User Guide

Secure® Configuration Manager™

January 2015

Legal Notice

About this Book and the Library

The *User Guide* provides conceptual information about the NetIQ Secure Configuration Manager product (Secure Configuration Manager). This book also defines terminology and provides step-by-step guidance for some tasks.

Intended Audience

This book provides information for individuals responsible for understanding Secure Configuration Manager concepts.

Other Information in the Library

The library provides the following information resources:

Installation Guide

Provides detailed planning and installation information.

Windows Agent Installation and Configuration Guide

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

Help

Provides context-sensitive information and step-by-step guidance for common tasks.

About NetIQ Corporation

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

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

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

Enabling critical business services, better and faster

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

Our Philosophy

Selling intelligent solutions, not just software

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

Driving your success is our passion

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

Our Solutions

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

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **comment on this topic** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

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

Contents

1 Introduction

The NetIQ Secure Configuration Manager product (Secure Configuration Manager) is a security configuration and compliance monitoring solution that proactively assesses system configurations against regulatory requirements, security best practices, and corporate IT policies to demonstrate compliance and manage information security risk. For more information, see the Secure Configuration Manager web site.

1.1 Understanding Secure Configuration Manager Components

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.

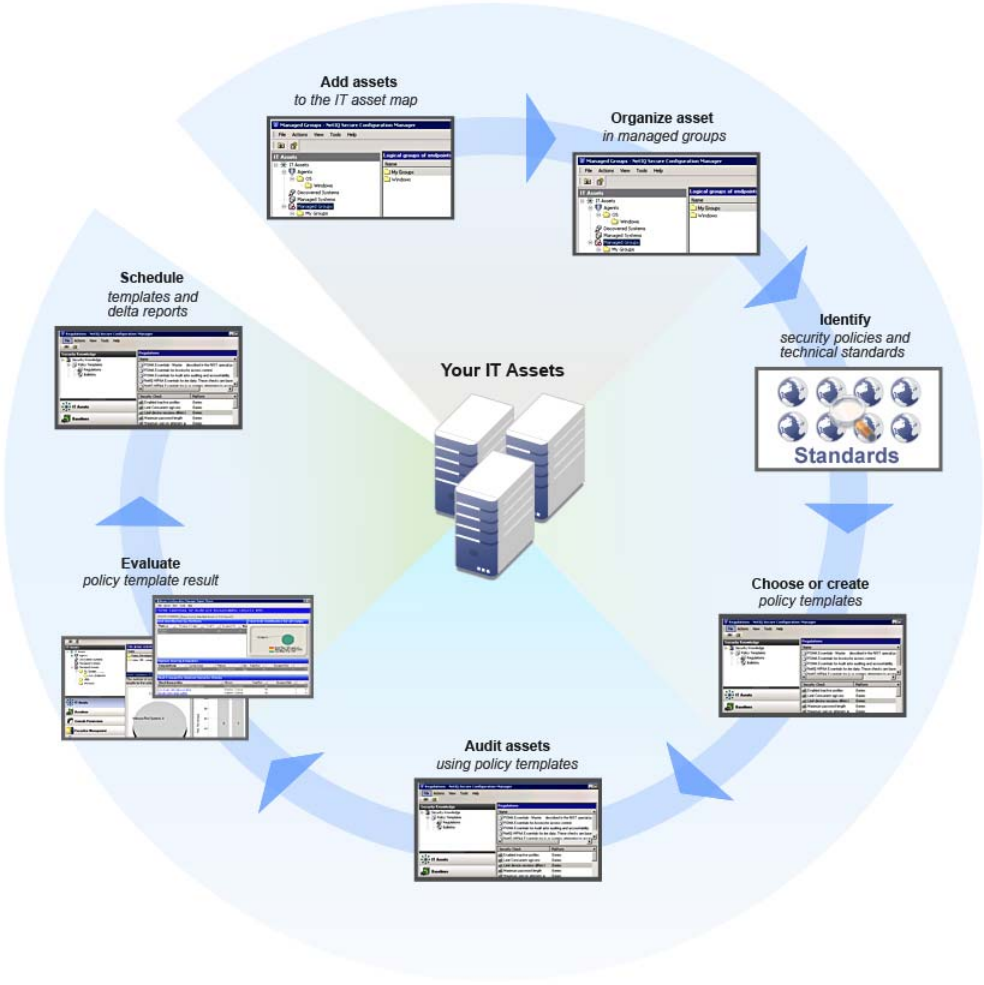
Component	Description
Agents	Receive requests from Core Services and run commands or respond by returning data, status, or results. Agents run platform-specific software locally on assets throughout your enterprise.
Database	Stores product configuration data and results from security checkup reports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

For more information about modifying component settings and grooming the database, see Chapter 9, “Maintaining the Secure Configuration Manager Database,” on page 129.

1.2 Auditing and Evaluation Process Workflow

Secure Configuration Manager simplifies and automates the process for demonstrating compliance and managing information security risk. Policy compliance is the assessment, operation, and control of systems and resources according to security standards, best practices, and regulatory requirements. Complex environments, industry standards, and government regulations can make compliance with so many policies a challenge, even for highly-experienced security teams. In most organizations, a variety of individuals perform the complex tasks required to maintain asset compliance.

The following workflow shows how you can streamline the asset auditing and evaluation processes by workflow tasks.



Use the following checklist to guide you through the auditing and evaluation process.

	Checklist Items
❑	1. Identify the IT assets that you want to monitor, and then add them to the Secure Configuration Manager asset map. See Section 2.2, “Building and Managing Your Asset Map,” on page 21.
❑	2. Organize your assets into logical groups. For more information, see Section 2.3, “Working with Managed Groups,” on page 28.

	Checklist Items
❑	3. Specify the value of each asset to your organization. For more information, see Section 2.5.2, “Assigning Importance to Endpoints,” on page 34.
❑	4. Identify the corporate policies and technical standards that affect your IT assets.
❑	5. Map your policies and standards to the policy templates built into Secure Configuration Manager. For more information, see Section 4.2, “Understanding Policy Templates,” on page 49.
❑	6. (Conditional) If the built-in policy templates do not specifically map to your corporate policies and standards, modify the built-in templates or create new ones. For more information, see Section 6.6.3, “Modifying Built-in Policy Templates,” on page 108 or Section 6.6.2, “Translating a Technical Standard to a Policy Template,” on page 107.
❑	7. Run the policy templates to begin the auditing process. For more information, see Section 4.3, “Running Security Checks and Policy Templates,” on page 50.
❑	8. Review policy template results to evaluate asset compliance. For more information, see Chapter 5, “Evaluating Audit Results,” on page 57.
❑	9. Correct the configuration problems found in the report results.
❑	10. (Optional) To adjust how Secure Configuration Manager scores asset results, modify the asset’s importance or adjust the threat factor and risk ranges for the security checks in the policy template. For more information, see Section 2.5.2, “Assigning Importance to Endpoints,” on page 34 and Section 6.3, “Understanding Risk Scoring,” on page 94.
❑	11. (Optional) To use a specific asset as a standard from which to compare other assets, establish a baseline or run delta reports. For more information, see Chapter 7, “Working with Baselines,” on page 111 or Section 5.3, “Comparing Report Results,” on page 63.
❑	12. (Optional) To exclude some assets or results from policy template runs, create exceptions. For more information, see Section 5.2, “Excluding Data from Report Results,” on page 58.
❑	13. Regularly audit assets with the selected policy templates. For more information, see Section 4.3.2, “Scheduling a Policy Template Run,” on page 51.
❑	14. (Optional) To regularly compare policy template results, schedule delta reports. For more information, see Section 5.3.4, “Scheduling a Delta Report,” on page 65.
❑	15. Regularly update your policy templates as corporate and regulatory standards change. For more information, see Chapter 8, “Maintaining Your Security Knowledge,” on page 121.

1.3 Understanding Asset Auditing Tools

At some point, corporate security policies should be mapped into documents that define the recommended configurations for an array of technologies. These documents are often called **Technical Standards**. In Secure Configuration Manager, **policy templates** let you define secure configuration standards for your IT assets. You can use these policy templates to express corporate

technical standards and current industry standards. Policy templates include many **security checks** or queries that you use to audit a series of IT controls on a variety of platforms. These audits generate:

- A list of security checks that identify non-compliant systems.
- A list of policy violations per security check. **Violations** are results returned by the security check that vary from the expected value and indicate a potential vulnerability. The **expected value** specifies the results you expect a security check to return.
- An aggregate score reflecting the state of compliance.
- A color code that indicates vulnerability based on risk score ranges.

NOTE: Security checks test for potential vulnerability. To help you determine which security checks to use, each check provides an explanation, the potential risks you face in not running the check, and remedies you can perform to reduce vulnerabilities.

Secure Configuration Manager lets you perform security audits by running security checks and policy templates. When you run a policy template, the resulting report contains a set of security checks, actual values for those checks, and scores. This capability provides a clear view of the current exposures in your enterprise. You can immediately use the default NetIQ policy templates to check the status of your systems against industry regulations and best practices. For more information about policy templates, see Section 4.2, “Understanding Policy Templates,” on page 49. For more information about security checks, see Section 4.1, “Understanding Security Checks,” on page 47.

1.4 Understanding Compliance Evaluation Tools

The security check and policy template reports help you determine the risk areas in your enterprise, and then prioritize the security risks that you found. You can use the reported scores to determine whether your systems are trending toward or away from the security policies and baselines set by your organization. Secure Configuration Manager provides tools to help you evaluate the report results. You can use these tools to browse the data for the asset out of compliance to see exactly how the asset failed and how to remediate the issue.

Tool	Description
Asset Compliance View	This console-based overview of your environment’s compliance enables console users to: ◆ View the overall compliance of their IT assets ◆ Perform a granular assessment of specific groups and computers ◆ Identify which IT assets are out of compliance with the enterprise’s security standard ◆ Determine whether the exposed system vulnerability poses a high, medium, or low risk For more information, see Section 5.4, “Using the Asset Compliance View for Evaluation,” on page 69.

Tool	Description
Security and Compliance Dashboard	This Web-based overview of your environment's compliance enables executives and managers to: ◆ View the overall compliance of their IT assets ◆ Perform a granular assessment of specific groups and computers ◆ View the overall posture and trends of security compliance at a single glance For more information, see Section 5.5, "Using the Security and Compliance Dashboard for Evaluation," on page 78.
Security Checkup Results Viewer	This Web-based tool enables managers and console users to remotely audit enterprise security by reviewing which assets are in compliance, out of compliance, or have an unknown compliance. For more information, see Section 5.6, "Using the Security Checkup Results Viewer for Evaluation," on page 78.

Secure Configuration Manager can notify you automatically when an asset falls out of compliance. Receiving notifications can help you expedite the remediation process. Also, every organization has complex workflows and change management processes that require adherence. Sending out-of-compliance alerts to a change management ticketing system uses your company-defined workflow to quickly address assets that fall out of compliance. For more information about automatic notifications, see Section 5.8, "Automating Compliance Notification," on page 84.

1.5 Listing Reports, Actions, and Security Checks

Secure Configuration Manager provides an Admin Reports wizard that lets you run reports to list Secure Configuration Manager administrative data. For example, you can run a report to list all reports, actions, and security checks for all endpoint types. Once you run an administrative report, you can print it or export it to a file. To run administrative reports, your console user account needs the Admin Reports permission. For more information, see Section 3.6, "Managing Permissions," on page 42.

2 Organizing Computers in Your Asset Map

To manage an asset with Secure Configuration Manager, such as a computer or database, you must first register the asset in the asset map. The **asset map** identifies all systems, agents, and endpoints that you want to monitor. The asset map is flexible and lets you group assets using the method most appropriate for your organization. After you have set up your asset map and organized your assets into groups, you can run templates to generate reports for those groups.

2.1 Understanding IT Assets

Secure Configuration Manager interacts with your IT assets according to each asset's assignment within four specific categories: systems, agents, endpoints, and groups.

2.1.1 Systems

Systems are physical computers on a network that run an operating system and host applications or databases. Systems also host agents or endpoints. An **agent** resides on a system and monitors endpoints such as computers, devices, and applications. An **endpoint** represents an agent-monitored operating system, application, web server, or database instance. For more information, see Section 2.1.2, "Agents," on page 19 and Section 2.1.3, "Endpoints," on page 20.

When you install Secure Configuration Manager, the setup program installs and registers a Windows agent on the Core Services computer. This agent and the endpoint representing the computer's operating system become the first **managed system** in your asset map. If you upgrade your Secure Configuration Manager environment, the setup program either updates the existing agent on the Core Services computer or installs and registers a new agent.

You can automatically discover systems on your network. For more information about automatically discovering systems, see Section 2.2.3, "Discovering Systems in Your Environment," on page 23. You can also periodically discover systems on your network by enabling the Automatic System scheduled task. When you enable this task, Secure Configuration Manager automatically discovers available systems on your network according to the schedule you set.

2.1.2 Agents

Agents are hosted on systems and manage endpoints such as computers, devices, and applications. Secure Configuration Manager runs actions and reports on endpoints and groups of endpoints. For more information about endpoints, see Section 2.1.3, "Endpoints," on page 20.

When you add an agent to the asset map, Secure Configuration Manager attempts to register the agent. Registration of an agent assigns a unique identifier to the agent. If an agent is not registered, Secure Configuration Manager cannot communicate with the agent, preventing the product from collecting security information from the managed endpoints. If you add an agent, but the agent is not registered at that time, you can manually register the agent later. The agent could fail registration when you add it to the asset map for several reasons:

- The network link to the agent is down.

- A firewall exists between the agent and Core Services.
- The agent is not running.
- The agent is using a different port than what is configured in Secure Configuration Manager.
- The agent requires a communication protocol that is not enabled in Secure Configuration Manager. For more information, see Section 2.4.2, “Registering an Agent Manually,” on page 30.

Any Windows agent can be assigned as a Deployment Agent by modifying the settings in the Agent Component Properties window. To see which agents are Deployment Agents, expand **IT Assets > Agents** in the navigation pane and view the agents listed in the content pane. For more information about deployment, see Section 2.2.7, “Deploying and Updating Agents,” on page 27.

Any time you are no longer using an agent, you should un-register the agent from Core Services and delete the agent from the asset map. If you no longer monitor a system’s security, you can delete the managed system, which removes all endpoints and agents on that system from the asset map. For more information about removing agents from Core Services, see Section 2.4.3, “Un-Registering an Agent,” on page 30. For more information about deleting managed systems, see Section 2.2.6, “Managing Systems in Your Asset Map,” on page 26.

2.1.3 Endpoints

Secure Configuration Manager analyzes security risks and ensures policy compliance for your endpoints and groups of endpoints. An **endpoint** is an entity that an agent manages and audits, and can be computers, databases, and applications. Endpoints are categorized into groups in the asset map according to the endpoint type, such as SQL Server 2000 or Windows. Each endpoint is mapped to one agent.

When you want to manage a specific computer, add that computer as an endpoint in the asset map. A computer can be a physical computer on a network that runs an operating system and hosts applications or databases. A system can have multiple endpoints, such as the operating system and a SQL Server database, and is referred to as a **managed system**.

Any time you are no longer managing or using an endpoint, you can delete that endpoint. You can also delete the managed system, which removes all endpoints and agents on that system from the asset map.

2.1.4 Groups

Groups contain collections of endpoints and other groups. By default, when you add an endpoint to the asset map, Secure Configuration Manager groups that endpoint by its platform. In Secure Configuration Manager, a **platform** refers to the endpoint type, such as Windows, UNIX, or SQL Server 2005. These built-in groups help you start to categorize your endpoints and cannot be modified. Secure Configuration Manager displays only the built-in groups that correspond with the agent and operating system types within your asset map.

You can create your own **managed groups** in Secure Configuration Manager to facilitate management of your environment. These user-defined groups in Secure Configuration Manager are nested, which means you can have groups within groups.

Ensure that you assign all endpoints to a managed group. Secure Configuration Manager uses your managed groups for the Asset Compliance View data. The Security and Compliance Dashboard also displays policy template results according to your managed groups. For more information about the Asset Compliance View, see Section 5.4, “Using the Asset Compliance View for Evaluation,” on page 69. For more information about the Security and Compliance Dashboard, see the *NetIQ Security and Compliance Dashboard Installation and Configuration Guide.*

The entire set of groups is called a **forest**. Each top-level node is called a **tree**. Several rules apply to groups in Secure Configuration Manager:

- A group can contain endpoints and other groups.
- You can add an endpoint to a group, or remove an endpoint from a group at any time.
- You can remove a group from another group at any time.
- An endpoint can belong to many trees, but that endpoint can be a member of only one group in any given tree.

Any time your IT infrastructure changes, you can change or delete existing user-defined groups, and remove endpoints from those groups to add to other groups.

2.2 Building and Managing Your Asset Map

The asset map provides an overview of all IT resources that you manage with Secure Configuration Manager. You use the asset map to run all reports and actions. You can grant or deny access to these assets through roles in Secure Configuration Manager. As your IT environment changes, you will need to add new systems, agents, and endpoints to the asset map periodically.

Secure Configuration Manager enables you to review your asset map in two ways. The Asset Compliance View provides an overview of your IT assets and their policy template results. The Admin Reports function enables you to review all your IT assets or the group context for specified endpoints. You can print or export the Asset Compliance and Admin Reports information. For more information about the Asset Compliance View, see Section 5.4, “Using the Asset Compliance View for Evaluation,” on page 69. For more information about the Admin Reports, see Section 2.2.8, “Reporting Asset Map Information,” on page 27.

You can change a system’s properties, such as contact email and system location, at any time after you have added the system to the asset map. You can also add customized properties for each system, such as specifying the organizational unit to which the system belongs.

NOTE: After you have added the customized property, the property cannot be deleted.

You can view your asset map in the console in two view styles. The **List View** lists your assets in table format. The **Flex Grid** view lists your assets so you can see the hierarchical relationships among systems, agents, and endpoints. For example, you can more easily determine which agents manage which endpoints by proxy. The Flex Grid view style might take a long time to load, depending on the number of assets in your asset map.

2.2.1 Asset Map Checklist

Use the following checklist to help you organize your asset map of groups, systems, agents, and endpoints. While you can add assets at any time, the most efficient way to set up your asset map initially is to follow these steps.

	Checklist Items
❑	1. Determine how you want to group your assets in the asset map. See Section 2.3, “Working with Managed Groups,” on page 28.
❑	2. Create and organize your asset map groups. See Section 2.3.1, “Creating a Managed Group,” on page 28.

	Checklist Items
❑	3. To add known systems, you can add them individually or create a file containing a list of systems.See Section 2.2.2, “Manually Adding Systems,” on page 22.
❑	4. To find systems in your environment, use the system discovery feature. See Section 2.2.3, “Discovering Systems in Your Environment,” on page 23.
❑	5. To find additional endpoints on your managed systems, use the endpoint discovery feature. See Section 2.2.4, “Discovering Application Endpoints,” on page 25.
❑	6. To deploy or update a Windows agent, use the Deployment wizard. See Section 2.2.7, “Deploying and Updating Agents,” on page 27.
❑	7. Add the discovered systems and endpoints to your asset map. See Section 2.2.6, “Managing Systems in Your Asset Map,” on page 26.
❑	8. Move your assets into the managed groups appropriate for your environment. See Section 2.3.2, “Moving Existing Endpoints into Groups,” on page 29.
❑	9. Maintain your asset map as needed.

2.2.2 Manually Adding Systems

Secure Configuration Manager enables you to add individual systems or a group of systems listed in a formatted file. These systems do not need a security agent before you add them to the asset map. You can assign an existing agent to the system or add the agent later. For more information about deploying a Windows agent, see Section 2.2.7, “Deploying and Updating Agents,” on page 27.

Your console user account must have proper permissions to add systems. For more information about permissions, see Section 3.6, “Managing Permissions,” on page 42.

Adding Individual Systems

When you have a few systems for which you already know the IP address and host name, it might be easier to manually add them. In the console, you can add systems from **IT Assets > Agents** and **IT Assets > Managed Systems**. When you add a system without registering the agent, Core Services adds the system to the Managed Systems content pane.

NOTE: Secure Configuration Manager supports IPv4 and IPv6 addresses. For more information about IPv6 support, see Section 2.2.3, “Discovering Systems in Your Environment,” on page 23, the *Installation Guide for NetIQ Secure Configuration Manager*, and the *Installation and Configuration Guide for NetIQ Secure Configuration Manager Windows Agent*.

Importing Systems Using a Formatted File

The Core Services Configuration Utility enables you to specify a file containing a list of computers you want to manage. Core Services reads the file and adds the listed computers to the Discovered Systems content pane. In the configuration utility, you must set the **File Import Discovery** field to `True` and specify the type and name of file to import. Secure Configuration Manager imports the systems from the file on a scheduled basis. The import runs on the same schedule as the Automatic System Discovery scheduled job. For more information about this job, see Section 2.2.5, “Using Scheduled Jobs to Discover Assets,” on page 25. For more information about the file import settings, see the Help for the Core Services Configuration Utility.

NOTE: Secure Configuration Manager supports IPv4 and IPv6 addresses.

The file must be an `NMAP XML` file, or a file in the proprietary format used by Secure Configuration Manager. If you are using the proprietary format, the complete format required for importing systems from a text file into Secure Configuration Manager is as follows:

```
HostName<Tab>IPAddress<Tab>Domain<Enter>
```

However, you can use any of the following formats as well:

```
HostName<Tab>IPAddress<Enter>
HostName<Tab>null<Tab>Domain<Enter>
HostName<Enter>
```

The following lines are examples from an import host file:

```
Host1    163.28.152.2    company.com
Host2    138.25.918.4
Host3    null    company.com
Host4    2001:db8:85a3:8d3:1319:8a2e:37:7334    company.com
Host5    2001:0db8:85a3:08d3:1319:8a2e:0370:7334
```

2.2.3 Discovering Systems in Your Environment

Discovered systems are computers that Core Services is aware of, but that have not been added to the Secure Configuration Manager asset map. You can manually initiate the discovery process in the console or enable Secure Configuration Manager to automatically discover systems on a scheduled basis. You can also discover unregistered endpoints on systems that you currently manage. For more information about discovering endpoints, see Section 2.2.4, “Discovering Application Endpoints,” on page 25.

To enable discovery and specify the domains that you want to search, update the settings on the Discovery tab in the Core Services Configuration Utility. By default, Windows domain discovery is enabled, which enables Secure Configuration Manager to find systems in the local domain of the Core Services computer. However, when searching the specified Windows or DNS domains, Core Services might categorize some discovered systems as an unknown asset type. To discover only computers that run a Windows operating systems, NetIQ Corporation recommends using Active Directory discovery.

Once you have discovered systems in your environment, you can register them with Core Services and begin managing them. For more information about adding discovered systems to your asset map, see Section 2.2.6, “Managing Systems in Your Asset Map,” on page 26.

NOTE

- Secure Configuration Manager cannot discover systems with IPv6-only addresses using the Windows domain discovery function. If you want to find systems with IPv6-only addresses, ensure that the systems are in an Active Directory or DNS domain and that these domains are enabled on the Discovery tab in the Core Services Configuration Utility.
- When Secure Configuration Manager discovers an IPv6-only system in a DNS domain, Discovered Systems could display an older IPv4 address for that computer. Discovering older addresses occurs when a computer was changed from dual-stack to IPv6-only and the older IPv4 address was not deleted from the WINS server.

Your console user account must have proper permissions to discover systems. For more information about permissions, see Section 3.6, “Managing Permissions,” on page 42.

Discovering Systems Manually

To initiate a manual discovery process, right-click **Discovered Systems** in the Discovered Systems navigation pane. By default, Secure Configuration Manager searches for all systems in the local domain. However, you can configure Core Services in the Core Services Configuration Utility to discover systems in specific DNS and Windows domains. The manual discovery process can also find systems in Active Directory, if you enable that functionality in the configuration utility. For more information about these settings, see the Help for the Core Services Configuration Utility.

Discovering Systems Automatically

Secure Configuration Manager can run processes in the background that enable you to automatically discover systems that have been added to your environment, as well as gather information about existing systems and endpoints. These processes can be triggered by registering endpoints and agents, as well as by running scheduled jobs.

When you register or re-register a UNIX or Windows operating system endpoint, Secure Configuration Manager can run the following types of queries:

- The first query gathers more information about the endpoint and its agent. For example, the query reports the fully qualified domain name for the agent computer, which is useful for agent deployment. This query occurs regardless of any configuration settings for discovery. Core Services uses the reported results to update the Properties fields for the agent and endpoint.
- A more in-depth query scans UNIX and Windows endpoints for additional, unmanaged applications such as Internet Information Services (IIS), Microsoft SQL Server, and Oracle. This in-depth query occurs only when you enable **Application Endpoint Discovery** in the Core Services Configuration Utility. Core Services uses the reported results to update the Properties fields for the endpoint, such as the protocol and authentication mode for an instance of SQL Server. For more information about application endpoint discovery, see Section 2.2.4, “Discovering Application Endpoints,” on page 25.
- If the Windows agent is also a Deployment Agent, Core Services instructs the agent to query Active Directory in the agent’s domain to find computers not currently managed by Secure Configuration Manager. This query occurs only when you enable **Active Directory Discovery** in the Core Services Configuration Utility. For more information about Deployment Agents, see Section 2.2.7, “Deploying and Updating Agents,” on page 27.

These queries run in the background. To view results, you might need to refresh the Discovered Systems pane or view the Audit History. Secure Configuration Manager adds a notification in the **Alerts** content pane when Core Services discovers a new endpoint, system, or domain.

Secure Configuration Manager includes built-in jobs that perform discovery queries similar to the discovery during asset registration. One of these jobs can continuously scan your environment for unmanaged endpoints. For more information about scheduled jobs for discovery, see Section 2.2.5, “Using Scheduled Jobs to Discover Assets,” on page 25.

2.2.4 Discovering Application Endpoints

Many of the systems in your environment support more than one endpoint, such as the operating system and a database instance. When you register a Windows system with Secure Configuration Manager, only the endpoint representing the operating system gets registered with Core Services. You can manually add the other endpoints to the system, or you can configure Secure Configuration Manager to regularly probe managed systems for undiscovered endpoints.

Secure Configuration Manager can discover the following endpoint types, referred to as **application endpoints**:

- Internet Information Services (IIS)
- Microsoft SQL Server
- Oracle (UNIX)
- Oracle (Windows)

By default, the **Application Endpoint Discovery** setting in the Core Services Configuration Utility is enabled, which allows Secure Configuration Manager to automatically discover application endpoints. When you register a new system, Core Services instructs the agent managing that system to run a check that looks for application endpoints. You can also schedule a job that continuously looks for unmanaged application endpoints on currently managed systems. For more information about jobs that discover application endpoints, see Section 2.2.5, “Using Scheduled Jobs to Discover Assets,” on page 25.

2.2.5 Using Scheduled Jobs to Discover Assets

Secure Configuration Manager provides the following scheduled jobs that enable you to easily discover unmanaged systems and endpoints:

Automatic system discovery

Enables you to regularly scan your environment for unmanaged systems, based on the settings for Windows, Active Directory, and DNS discovery in the Core Services Configuration Utility. This job is disabled by default. For more information about system discovery, see “Discovering Systems Automatically” on page 24.

Asset details and discovery

Enables you to gather information about the agents on currently managed UNIX and Windows endpoints. With **Application Endpoint Discovery** enabled in the Core Services Configuration Utility, this job also scans UNIX and Windows endpoints for additional unmanaged applications, such as Internet Information Services (IIS), Microsoft SQL Server, and Oracle.

This job runs continuously, using the NetIQ Endpoint Discovery and Agent Configuration policy template as the query basis. The job queries 100 endpoints each run until all endpoints in your asset map have been checked. The job runs on a 30-day schedule. Thus, Core Services does not restart the job until 31 days after the previous start, even if all assets have been checked within the 30-day window. Core Services starts the process with the endpoints that have the oldest last-run date for the template. If you manually register an endpoint, Core Services marks that endpoint as queried, as if the job had run against the endpoint that day. If you manually run the NetIQ Endpoint Discovery and Agent Configuration policy template against a group of endpoints, Core Services sets that run as the most recent run of the job for those endpoints.

This job is enabled by default. You can verify job runs in the Audit History pane. Secure Configuration Manager adds a notification in the **Alerts** content pane when Core Services discovers a new endpoint or system. For more information about endpoint discovery, see Section 2.2.4, “Discovering Application Endpoints,” on page 25.

2.2.6 Managing Systems in Your Asset Map

Once you have discovered systems and endpoints on your network or imported systems into the Discovered Systems pane, you can add them to your asset map and begin managing them. The Managed Systems pane in the console lists all systems, comprising agents and multiple endpoints, that you have registered for inclusion in your asset map. Managed Systems can also include endpoints or agents that have not been registered with Secure Configuration Manager. For example, you might have manually added a system but did not install an agent or did not register the system during agent installation.

Each endpoint that you register with Secure Configuration Manager requires an endpoint license. To view your current license count, click **License Status** on the **Tools** menu. For more information about endpoint licensing, see the *Installation Guide for NetIQ Secure Configuration Manager*.

Adding Managed Systems

Secure Configuration Manager enables you to manually add systems in the Managed Systems pane or select systems to manage from the Discovered Systems content pane. If the discovered or imported system already has a valid security agent, you can manage the system immediately. For Windows systems that do not have an agent, you can deploy a Windows agent to the computer or specify a Windows agent that will manage the system by proxy. For more information about deploying Windows agents, see Section 2.2.7, “Deploying and Updating Agents,” on page 27 and the *Installation and Configuration Guide for NetIQ Secure Configuration Manager Windows Agent*.

Deleting Managed Systems

When you no longer need a system, or when you remove the system from the domain, you can delete that system from your asset map. If the system hosts an agent, deleting that system also un-registers its hosted agent from the current Core Services. Before deleting a system that hosts an agent, you must remove all attached endpoints. Otherwise, the endpoints will be deleted as well as the agent and the system. Also, if the system hosts a Deployment Agent, you must assign a different agent as the Deployment Agent for that domain before you can delete the system.

NOTE: When you remove a managed system from your asset map, the system might be added to Discovered Systems again, depending on the settings for discovery.

To delete a system:

1. In the left pane, click **IT Assets**.
2. In the IT Assets tree pane, select **Managed Systems**.
3. In the content pane, right-click the system you want to delete, and then click **Delete**.
4. Click **Yes** on the confirmation message.

2.2.7 Deploying and Updating Agents

Secure Configuration Manager provides a deployment feature that enables you to easily install and uninstall Windows agents on remote computers. You can also push service packs and hotfixes to existing Windows agents. Once you install an agent on a remote computer, Secure Configuration Manager automatically adds the agent, its corresponding endpoint, and system to the asset map.

The functionality of the deployment feature varies, depending on where you initiate the wizard. For example, the wizard can include computers found by the Discovered Systems feature. Use the following table to determine where you want to start the Deployment wizard.

If you want to...	Start the deployment process from...
Upgrade, apply a hotfix or service pack to, or uninstall an existing agent	IT Assets > Agents IT Assets > Managed Systems
Install a new agent on systems already discovered by Secure Configuration Manager	Discovered Systems
Install a new agent on systems that Secure Configuration Manager does not manage or has not discovered	Tools menu

Secure Configuration Manager allows you to designate agents as **Deployment Agents**, which serve as intermediaries between Core Services and the target computer. The Deployment Agents enable you to deploy to computers in untrusted domains or highly secure networks. The deployment process uses the credentials of the agent service account on the Deployment Agent computer for permission to deploy to the target computers. You can also designate alternate credentials for accessing the target computers. By default, the Windows agent installed on the Core Services computer is a Deployment Agent. You must have a Deployment Agent in each domain. Secure Configuration Manager designates the first registered agent in a domain as the Deployment Agent for that domain. To determine which agents have been assigned as Deployment Agents and their respective domains, run the Deployment Agents administrative report.

You must specify a fully qualified host name for the endpoint that represents the Deployment Agent. Otherwise, Core Services cannot use the agent for deployment. You specify the host name in the endpoint Properties window. To see which agents are Deployment Agents, expand **IT Assets > Agents** in the navigation pane. You can sort the view using the **Is Deployment Agent** column in the content pane.

For more information about Deployment Agents and using the deployment feature, see the *Installation and Configuration Guide for NetIQ Secure Configuration Manager Windows Agent* and the Help. For more information about finding computers to add to the asset map, see Section 2.2.3, “Discovering Systems in Your Environment,” on page 23.

2.2.8 Reporting Asset Map Information

Secure Configuration Manager provides **administrative reports** that list information such as all IT resources in your asset map or the group context for specified endpoints, security checks, users, and roles. Use the Admin Reports wizard to run the administrative reports. You can print or export a report to a file for future reference. Your console user account needs the Admin Reports permission. For more information, see Section 3.6, “Managing Permissions,” on page 42.

2.3 Working with Managed Groups

Nested groups let you define different models of your company structure. Each of these top-level groups represents one view of your organization, such as organizational hierarchy, physical location of computers, or type of service the computers perform. Choose a managed group structure that maps to the setup of your organization. If your company IT infrastructure changes, you can drag and drop endpoints from group to group. Alternatively, you can organize your assets by vulnerability risk. For example, group all high-risk assets in one managed group so you can schedule pertinent policy templates to run against your most vulnerable systems more often than against lower-risk assets.

Ensure that you assign all endpoints to a managed group. Both the Asset Compliance View and the Security and Compliance Dashboard use your user-defined managed groups for displaying policy template results. For more information about the Asset Compliance View, see Section 5.4, “Using the Asset Compliance View for Evaluation,” on page 69. For more information about the Security and Compliance Dashboard, see the *NetIQ Security and Compliance Dashboard Installation and Configuration Guide.*

Your **console user account**, which enables you to log on to the Secure Configuration Manager console, must have proper permissions to create and modify groups. You can also set permissions for viewing managed groups. For more information about permissions, see Section 3.6, “Managing Permissions,” on page 42.

NOTE: Users must have the Access IT Assets permission with the **Allow for All Groups** setting enabled to add groups and see those groups they created. For example, console user John can add groups, such as Group C and Group D, but does not see the groups because he does not have the Allow for All Groups permission. Another user with the Allow for All Groups setting enabled must grant John access to the managed groups he created.

2.3.1 Creating a Managed Group

You can create empty managed groups so those groups are available when you add endpoints later.

To create a managed group:

1. In the left pane, click **IT Assets**.
2. In the IT Assets tree pane, expand **Managed Groups** and select **My Groups**.
3. Right-click and then click **Add Group**.
4. (Optional) To make your new group a child of an existing group, select the existing group in the **Available Groups** list.
5. Specify the appropriate values.

   NOTE: Managed Group names must be unique, but also are case-sensitive.

   ---

6. Click **Create New Group**.
7. Click **Finish**.

2.3.2 Moving Existing Endpoints into Groups

After deploying your agents and endpoints, move those existing endpoints into groups for easier categorization. Moving endpoints from one group to another does not affect scheduled jobs.

To add endpoints to a group:

1. In the left pane, click **IT Assets**.
2. In the IT Assets tree pane, expand **Managed Groups** and select the folder in which the endpoints currently exist.
3. In the content pane, select the endpoints you want to add to the group.
4. Right-click and then click **Add to Group**.
5. In the **Available Groups** list, select the group to which you want to add the endpoints.
6. Click **OK**.

2.4 Working with Agents

Secure Configuration Manager employs a process called **manage by proxy** to let you manage and audit some endpoints without installing an agent on the computer. The manage by proxy capability greatly simplifies deployment. For example, a single instance of the Windows agent is capable of managing any endpoint that is a member of the domain in which the agent service is installed. A **domain** is a set of computers sharing a common security account (user and group) database and policy. Each domain has a unique name.

To set up a proxy agent, add the agent to your asset map, and then add multiple endpoints to the agent. You can change an agent's properties, such as the agent version, at any time after you have added the system to the asset map. You can also add customized properties for each system, such as specifying the number of endpoints that the agent manages.

NOTE: After you have added the customized property, the property cannot be deleted.

Secure Configuration Manager also lets you control the flow of information through an agent by limiting the number of requests that Core Services submits to an agent concurrently. For example, if you have an agent installed on a shared server supporting many proxies, you can set the Maximum Concurrent Requests to a low value. This enables the server's resources to be shared with other applications since less data will flow through the agent at any given time. Alternatively, you can increase the number of concurrent requests if the agent is installed on a server with no proxy reporting or is installed on a dedicated server monitoring multiple endpoints by proxy. To specify the number of requests Core Services sends to the agent concurrently, change the agent property for **Maximum Concurrent Requests**. The default value is 5, and the maximum value is 100.

2.4.1 Checking an Agent Heartbeat

To determine whether an agent is started, running, and registered, check the agent heartbeat. The **heartbeat** indicates the agent's status. If an agent is not running, you may need to start the agent service and register the agent again.

To check an agent heartbeat:

1. In the left pane, click **IT Assets**.
2. In the IT Assets tree pane, expand **Agents**.
3. Right-click the folder that contains the agent whose heartbeat you want to check, and then click **Check Heartbeat**.
4. Click **OK** on the confirmation message.

2.4.2 Registering an Agent Manually

If you add an agent, but do not register the agent at that time, you can manually register the agent later. Secure Configuration Manager shows an unregistered agent as being offline.

To register an agent manually:

1. In the left pane, click **IT Assets**.
2. In the IT Assets tree pane, expand **Agents** and select the folder that contains the agent you want to register.
3. In the content pane, right-click the agent that you want to register, and then click **Register Agent or Endpoint**.
4. Follow the instructions in the wizard.

2.4.3 Un-Registering an Agent

When you delete an agent from your asset map, it is still registered by Core Services. To ensure that an unused agent does not cause a problem with future versions of Core Services, you can permanently remove the agent from Core Services. This process both un-registers the agent from Core Services and deletes it from your asset map. For more information about simply deleting an agent, see Section 2.4.5, "Deleting an Agent from the Asset Map," on page 31.

NOTE: Before deleting an agent, you must remove all attached endpoints. Deleting the agent without removing the endpoints leaves the endpoints unmanaged.

To un-register an agent:

1. In the left pane, click **IT Assets**.
2. (Conditional) If the agent has endpoints attached to it, complete the following steps:
   - **2a** In the IT Assets tree pane, expand **Agents** and select the appropriate folder.
   - **2b** In the content pane, select the agent you want to un-register.
   - **2c** In the lower content pane, right-click the endpoints associated with the agent, and then click **Remove from Agent**.
3. In the IT Assets tree pane, select **Managed Systems**.

4 In the content pane, right-click the agent that you want to un-register, and then click **Delete**.

5 Click **Yes** on the confirmation message.

2.4.4 Updating Windows Agent Software

Secure Configuration Manager enables you to push software updates to security agents on multiple systems concurrently. Once you have a Secure Configuration Manager Windows Agent registered in your asset map, you can use the Deployment wizard in the console to apply a hotfix, service pack, or new version of the agent.

Secure Configuration Manager adds a report to the Completed Jobs queue when the deployment process finishes. You can also save a copy of the report to a folder or file share. The report provides a list of successful and failed agent updates.

You can apply only the Windows installation and update packages stored on the Core Services computer. By default, the packages are stored as `.nap` files in the `%ProgramFiles%\NetIQ\Secure Configuration Manager\Core Services\SyncStore` folder. Some `.nap` files might contain an update for both the Windows agent and Secure Configuration Manager components. The Deployment wizard enables you to import the file.

To update software for an existing Windows agent:

1 In the IT Assets tree pane, expand **Agents > OS > Windows**.

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

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

4 Follow the instructions in the wizard until you finish updating the agents on the target computers. For more information about deploying your Windows agents, see the Help in the console.

2.4.5 Deleting an Agent from the Asset Map

Any time you no longer need an agent, or when you have removed the agent from the domain, you can delete that agent from your asset map. However, the agent is still registered by Core Services. Leaving an unused agent registered by a specific version of Core Services can cause problems in the future if you want to use that agent again, but with an updated or different Core Services.

The following steps explain how to delete the agent from your asset map. For more information about permanently removing an agent from Core Services, see Section 2.4.3, “Un-Registering an Agent,” on page 30.

NOTE: Before deleting an agent, you must remove all attached endpoints. Deleting the agent without removing the endpoints leaves the endpoints unmanaged.

To delete an agent from the asset map:

1 In the left pane, click **IT Assets**.

2 In the IT Assets tree pane, expand **Agents** and select the appropriate folder.

3 (Conditional) If the agent has endpoints attached to it, complete the following steps:

3a In the content pane, select the agent you want to delete.

3b In the lower content pane, right-click the endpoints associated with the agent, and then click **Remove from Agent**.

4 In the content pane, right-click the agent you want to delete, and then click **Delete**.

5 Click **Yes** on the confirmation message.

2.5 Working with Endpoints

If you add an endpoint, but the endpoint is not registered at that time due to a network problem or the computer being inaccessible, you can manually register the endpoint. Any time you no longer need an endpoint, you can delete that endpoint.

You can also change endpoint properties, such as a contact email, at any time after you have added the endpoint. Some endpoint properties apply to specific operating systems. For example, the CUM PTF property applies only to iSeries endpoints. The endpoint properties include importance level, which allows you to indicate each endpoint's value to your organization. For more information about modifying the importance level property, see Section 2.5.2, "Assigning Importance to Endpoints," on page 34.

NOTE

- After you have added a custom endpoint property, the property cannot be deleted.
- Deleting an endpoint does not remove the Secure Configuration Manager software installed on the agent computer.

2.5.1 Adding Endpoints to the Asset Map

As your organization grows and changes, you might need to add endpoints to the asset map in the console.

To add an endpoint to an existing agent:

1 In the left pane, click **IT Assets**.

2 In the IT Assets tree pane, expand **Agents** and select the appropriate folder.

3 In the content pane, right-click the agent to which you want to add the endpoint, and then click **Add Endpoint**.

4 Click **Next**.

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

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

7 Select the appropriate endpoint type from the **Endpoint Type** field, such as Windows Machine or Active Directory, or accept the default endpoint type.

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

9 (Optional) To add more information about the computer that you are adding as an endpoint, update the optional property fields. Some endpoint types might have a subset of the following optional property fields.

Field	Description
Contact Email	Email address of the contact person.
Contact Name	Name of the contact person.

Field	Description
Cumulative PTF	Cumulative PTF (program temporary fix) applied to the iSeries operating system.
Database Port	Port that the agent is using to communicate with Core Services, if you are adding a database endpoint.
Importance	Criticality level of the endpoint.
Instance Name	Name of the database instance, if you are adding a database endpoint.
Is DHCP Client	Whether this computer has its IP address dynamically assigned by a DHCP server.
License Type	Product for which you are licensing this endpoint.
Location	Location of the computer hardware.
Major Version	Major version of the operating system. Secure Configuration Manager automatically updates this information when registering Windows, SQL Server, NAS Server, IIS, and Active Directory endpoints. Not available for Lightweight UNIX or Oracle systems.
Minor Version	Minor version of the operating system. The list of available minor versions depends upon the selected major version. Secure Configuration Manager automatically updates this information when registering Windows, NAS Server, and Active Directory endpoints. Not available for SQL Server, IIS, Lightweight UNIX, or Oracle systems.
Notes	Descriptive notes about the computer. Not available for Lightweight UNIX, UNIX, iSeries, or Oracle systems.
Service Pack	Microsoft Service Pack applied to the Windows operating system. For example, Windows XP Service Pack 3. Not available for NAS servers.
Time Zone	Time zone in which the physical computer on which the endpoint is located is found. An endpoint computer can be in a different time zone than the Core Services computer or the managing agent.
Use	The purpose of the endpoint computer.

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

10a Select the **Add Endpoint to a Group** check box.

10b Click **Groups**.

10c Select an existing group to which you want to add the endpoint, or create a new group.

10d (Optional) To create a new group, enter the new group name and description, and then click **Create New Group**.

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

11 (Optional) To add more than one endpoint, click **Add Endpoint**. Repeat Step 6 on page 32 through Step 10 on page 33 for each endpoint that you want to add.

12 Click **Finish**.

2.5.2 Assigning Importance to Endpoints

When a minor vulnerability occurs on a high-value asset, you may consider the vulnerability a high risk in your environment. Secure Configuration Manager lets you assign an **importance** value to each endpoint so you can weight resulting risk scores based on the value of the asset to your organization. An endpoint's importance level represents the criticality of that asset to your company business and applications. For example, you may consider a corporate mail server a greater security risk than a desktop workstation with a very critical vulnerability, even if the mail server has a less critical vulnerability. You can change the importance level by modifying the endpoint's properties. To assign an importance level to an endpoint, your console user account needs the Assign Importance permission. For more information, see Section 3.6, "Managing Permissions," on page 42.

Importance levels range from Very Low to Very High. By default, an endpoint has a Medium importance when it is created. Secure Configuration Manager maps each level to a percentage that is ultimately multiplied by the exposure score to determine the **risk score**, which numerically expresses the current level of an endpoint's vulnerability. Secure Configuration Manager calculates the **exposure score** for each endpoint by using the scoring method, threat factor, and number of violations for a security check. The **threat factor** serves as an approximate penalty value, greater than 0, used to calculate the exposure score of a security check. Secure Configuration Manager maps each importance level to a **multiplier value**. The multiplier value serves as the percentage ultimately multiplied by the exposure score to determine the risk score. For more information about scoring, see Section 6.3, "Understanding Risk Scoring," on page 94.

NOTE: An endpoint may belong to more than one group. Since an endpoint can have only one importance level, you should assign the highest level to the endpoint when you view the endpoint across all groups. For example, if an endpoint has "Medium" importance in the Sales group, but has "High" importance in the Managers group, assign a "High" importance level to that endpoint.

---

3 Setting Security on the Secure Configuration Manager Console

Console security settings control who can access Secure Configuration Manager and which activities each user can perform. You can configure console security to control user access to Secure Configuration Manager functions. Secure Configuration Manager provides a powerful, role-based security model that helps you streamline permissions management. A **role** represents a title or responsibility placed on an individual user ID or a group of user IDs that may have permissions assigned to it.

3.1 Console Security Checklist

To define and manage security controls on the Secure Configuration Manager console, you must be a **console administrator**, which is a console user assigned to the Secure Configuration Manager Administrator's role. For more information, see Section 3.2.2, "Understanding Console Administrators," on page 36.

The following checklist outlines the workflow for configuring Secure Configuration Manager console security settings. You can modify this workflow to accommodate your specific security needs.

	Checklist Items
❑	1. Understand the console security components. See Section 3.2, "Understanding Console Security," on page 36.
❑	2. Log on to Secure Configuration Manager using a console administrator account. By default, you can specify a console administrator account during installation.See the *Installation Guide for Secure Configuration Manager*.
❑	3. Determine whether you want to implement an external authentication source to validate the console users. See Section 3.3, "Managing User Authentication," on page 37.
❑	4. Determine whether you want Secure Configuration Manager to enforce password policy on the console user accounts. See Section 3.4, "Managing Password Policy," on page 39.
❑	5. Identify which personnel you want to give permissions in Secure Configuration Manager, and then create a user account in Secure Configuration Manager for each console user and administrator. See Section 3.7.1, "Creating a Console User," on page 44.
❑	6. Determine which sets of roles and permissions you want to assign to those users. If needed, create the appropriate roles. See Section 3.5, "Managing Roles," on page 40 and Section 3.6, "Managing Permissions," on page 42.
❑	7. Assign the appropriate roles and permissions to the appropriate console users. See Section 3.7.2, "Assigning Roles to a Console User," on page 44 and Section 3.7.3, "Assigning Permissions to a Console User," on page 44.
❑	8. Assign limit to the number of concurrent web or console sessions for required roles. See section Section 3.5.3, "Assigning Session Limit to Roles," on page 41

3.2 Understanding Console Security

Console security includes the following components:

- Authentication
- Console users and administrators
- Password policy
- Roles and permissions

By setting console security, you determine appropriate access, enforcing secure management of vulnerabilities across your enterprise. You ensure that the appropriate personnel can identify vulnerabilities and perform the necessary corrective actions.

3.2.1 Understanding Console Users

A console user is any user who uses the Secure Configuration Manager console. Console users, including console administrators, need the appropriate roles or permissions to perform activities through Secure Configuration Manager. For example, ensure that each console user has the **Access IT Assets** permission to read reports or perform actions on endpoints in your asset map. For more information, see Section 3.5, “Managing Roles,” on page 40 and Section 3.6, “Managing Permissions,” on page 42.

Each console user requires a Secure Configuration Manager account. You can use the Secure Configuration Manager database to authenticate the console user account or configure Secure Configuration Manager to use an external authentication source. For more information, see Section 3.3, “Managing User Authentication,” on page 37.

3.2.2 Understanding Console Administrators

A console administrator is a console user who has administrator permissions in Secure Configuration Manager. For example, you can create a console administrator by assigning the Administrators role to a console user. A console administrator is not required to be an administrator or super user on a specific endpoint or platform. You do not need to grant escalated permissions on remote systems that Secure Configuration Manager is monitoring.

Console administrators can perform the following console security activities:

- Implement and modify external authentication
- Implement and modify password policy
- Reset console user and console administrator account passwords
- Create console user accounts
- Create, copy, and modify roles
- Assign permissions to roles or console users

Console administrators can also perform actions and generate reports through Secure Configuration Manager.

3.2.3 Understanding Console User and Administrator Auditing

To help ensure that users and administrators are assigned the appropriate permissions, you can audit all actions users perform in Secure Configuration Manager using the Audit History log. Audit History lets you view and export actions that console users and administrators perform, such as logging on

and off, adding exceptions, and modifying policy templates. Identifying when users perform non-job related tasks in Secure Configuration Manager helps you assess user permissions and role membership. To view audit history, your console user account needs the View Audit History permission. For more information, see Section 3.6, “Managing Permissions,” on page 42.

3.3 Managing User Authentication

User authentication ensures that a console user logs on to Secure Configuration Manager using valid credentials. **Credentials** represent a combination of user name and password to provide a user the authorization to log on to a computer. When Secure Configuration Manager authenticates a console user account, Secure Configuration Manager validates the account credentials against either the Secure Configuration Manager database or an external database that is LDAP compliant, such as Active Directory. You can configure a console user account for console authentication or external authentication. To successfully implement external authentication, identify an available LDAP server, such as a Windows 2000 or later domain controller or a Sun ONE Directory Server version 5.2 running on a Windows 2000 Server computer.

Secure Configuration Manager supports the following authentication settings:

Console Authentication

When a console user logs on to Secure Configuration Manager, Secure Configuration Manager validates the specified user name and password against encrypted credentials stored in the Secure Configuration Manager database.

External Authentication

When a console user logs on to Secure Configuration Manager, Secure Configuration Manager connects to the external authentication source associated with this account and validates the specified user name and password against credentials stored in the external authentication source. For example, if a console user account belongs to a Windows 2000 or later domain, Secure Configuration Manager validates the account user name and password against the credentials stored in Active Directory on the domain controller for that domain. External authentication allows you to leverage your existing authentication settings.

You can add, modify, verify, and delete authentication sources and the properties of each source. Before you associate console user accounts with an external authentication source, configure Secure Configuration Manager to support external authentication. For more information, see Section 3.3.1, “Implementing External Authentication,” on page 38. You can verify an authentication source to ensure that the specified LDAP server is available and the authentication credentials are valid. When you modify the authentication source properties, ensure that the specified LDAP server is available and the authentication credentials are valid.

Before you delete an authentication source from the Secure Configuration Manager database, ensure that no console users associated with this source are logged on to the Secure Configuration Manager console.

WARNING: Deleting an external authentication source prevents Secure Configuration Manager from validating the associated user accounts. When you delete an authentication source, assign another authentication source to the affected console users. For more information, see Section 3.7, “Managing Console Users,” on page 43.

3.3.1 Implementing External Authentication

You can configure Secure Configuration Manager to authenticate a console user using credentials stored in an external database. For example, Secure Configuration Manager can authenticate a console user account using credentials stored on a specific Active Directory domain controller.

To implement external authentication:

1. In the left pane, click **Console Permissions**.
2. In the Console Permissions tree pane, right-click **Authentication Sources**, and then click **New Authentication Source**.
3. On the General tab, specify the external authentication source by completing the following steps:
   - **3a** Under **Source Identification**, type the source name in the **Source Name** field (for example, Active Directory).
   - **3b** In the **LDAP Server URL** field, type the fully qualified URL of the appropriate LDAP server. Use either of the following formats:

     `ldap://server_name:port_number`
     `ldap://domain_controller.DNS_suffix`

     NOTE: You can search for the correct LDAP server using the browse button, and enter specifics in the LDAP Server URL window. To change the LDAP root path, click **Change** and enter the credentials used to access the specified Active Directory domain indicated in the LDAP Path.
   - **3c** Type the distinguished name of the container or organizational unit to which this LDAP server adds new user accounts in the **User Base DN** field. Use the following format:

     `CN=users,DC=DomainComponent1,DC=DomainComponent2`
   - **3d** Type the name of an LDAP attribute (such as `displayname`) that the LDAP server uses to uniquely identify this user account in the **Username Attribute** field. To map to the logon ID, use the attribute `SAMAccountName`.
4. Specify the authentication credentials Secure Configuration Manager should use to connect to this source.
   - **4a** (Optional) To allow anonymous access, under **Binding Credentials** select **Use Anonymous Binding**. To fully implement anonymous binding for Active Directory, configure the appropriate domain controller to support anonymous authentication. Anonymous binding allows console users to authenticate without specifying their Active Directory credentials.
   - **4b** In the **Username** field, type the full distinguished name of the account that Secure Configuration Manager should use when binding to the server. Use the following format:

     `CN=AccountName,OU=Users,DC=DomainComponent1,DC=DomainComponent2`

     NOTE: Active Directory credentials are case-sensitive. Ensure that you enter the information in the **Username** and **Password** fields in the appropriate case. For example, if the Active Directory account name is JMcNetIQ, the console user name must also be JMcNetIQ.
   - **4c** In the **Password** and **Confirm Password** fields, type the password used to log on to the LDAP server.

5 To ensure that the specified LDAP server is available and the authentication credentials are valid, click **Verify**.

6 Click **OK**.

3.3.2 Configuring a Secure LDAP Authentication Source

You can configure a secure LDAP authentication source, but you must first have a public key infrastructure running in your environment. For more information about setting up a Windows-based PKI, including issuing a certificate for your secure LDAP service and exporting your root certificate authority, see the Microsoft Windows Server 2003 Technology Center Web site.

To configure a secure LDAP authentication source:

1 On your Secure Configuration Manager Core Services computer, use the following command to add the CA root certificate to the cacerts keystore:

```
keytool -import -trustcacerts -alias rootca -file rootca.cer -keystore "Secure Configuration Manager Installation Folder\Core Services\jre\lib\security\cacerts"
```

2 Use the procedure described in Section 3.3.1, “Implementing External Authentication,” on page 38, and enter `ldaps://ldap server:636` as the LDAP Server URL value in Step 3 on page 38.

3.4 Managing Password Policy

To ensure that console user and administrator accounts are protected against security attacks, Secure Configuration Manager provides an integrated password policy. Password policy is enabled by default and offers complex password rules that apply to all console user and administrator accounts that use console authentication. Password policy also supports password history and console lockout settings. You can modify the default policy settings to address your specific security needs. You can also reset your password policy to the default settings in Secure Configuration Manager.

Secure Configuration Manager applies an updated policy to passwords created or reset after you enable or modify the password policy. For example, Secure Configuration Manager applies the new password policy the next time a console administrator resets a password.

These rules apply to passwords set through Secure Configuration Manager, and do not replace or overwrite native password rules. If you implement external authentication, ensure that the authentication source applies complex password policy rules to account credentials stored in the external authentication directory.

To configure the password policy:

1 In the console, click **Console Permissions**.

2 In the navigation pane, right click **Console Permissions**, and then click **Password Policy**.

3 (Optional) To return to the default settings, click **Reset**.

4 Modify the settings and then click **OK**.

3.5 Managing Roles

A **role** is a set of permissions that controls access to specific Secure Configuration Manager features. You can use roles to allow or deny a console user the ability to perform particular actions or run particular reports. A role allows you to quickly and easily assign permissions related to a specific job function or workflow, such as auditing all UNIX servers. You can use a single role multiple times by assigning the role to different console users. This approach ensures that consistent application of permissions, enforcing the same level of security across your organization. Likewise, when you update the role, all assigned console users automatically receive the same change.

3.5.1 Default Roles

Secure Configuration Manager provides several default roles that allow you to quickly and easily set up your system administrators. These default roles include the following administrator and platform-specific roles:

Administrators

Provides administrative rights to any console user assigned this role. Assign this role to console users responsible for Secure Configuration Manager configuration and security activities, such as creating policy templates and setting console passwords. For more information, see Section 3.2.2, “Understanding Console Administrators,” on page 36.

NetIQ Auditor

Provides permissions to run all reports across all platforms, agents, and systems. Assign this role to console users responsible for network-wide reporting. This role lets you immediately begin identifying vulnerabilities.

NetIQ Database Legacy Admin

Provides permissions to run all reports and actions on the legacy database platforms. Assign this role to console users who are responsible for database security.

NetIQ Exception Approval Manager

Provides permissions to approve or disapprove security check exceptions created in Secure Configuration Manager. Assign this role to console users who are responsible for approving and disapproving exceptions.

NetIQ Exception Manager

Provides permissions to manage security check exceptions created in Secure Configuration Manager. Assign this role to console users who are responsible for maintaining exceptions.

NetIQ Help Desk

Provides permissions to run all reports and actions related to Help Desk activities. Assign this role to console users who are responsible for Help Desk activities.

NetIQ iSeries Admin

Provides permissions to run all reports and actions on an iSeries platform. Assign this role to console users who are responsible for iSeries security.

NetIQ UNIX Admin

Provides permissions to run all reports and actions on a UNIX platform. Assign this role to console users who are responsible for UNIX security.

NetIQ Windows Admin

Provides permissions to run all reports and actions on a Windows platform. Assign this role to console users who are Domain Admins or are responsible for Windows security.

3.5.2 Creating, Modifying, and Deleting Roles

You can create, modify, and delete custom roles or copy the default NetIQ roles to create new roles. You can also create a new role by copying an existing role. Copying a role provides a quick and easy way to create multiple new roles. For example, you can create a template role that contains particular platform security settings, and then copy this role to ensure consistent settings across multiple roles. You can modify role assignments by adding or removing console users from an existing role. You can also add permissions to a role. Deleting a role removes a set of permissions granted to console users assigned to this role. You can also remove permissions from console users by modifying the role assignments.

When you add a new role in your console security, you must add permissions to the role. By default, most permissions are denied. You can add multiple permissions to a role by allowing or denying access to specific actions, security checks, task suites, and reports in Secure Configuration Manager. For more effective and efficient security settings, ensure that these permissions allow a set of activities that fulfill a particular job function. For more information, see Section 3.6, “Managing Permissions,” on page 42.

3.5.3 Assigning Session Limit to Roles

You can limit the maximum number of concurrent web and client console sessions for each user in a role by using Session Limit for the role. Session Limit can be specified for any role and the users under that role can launch the maximum number of concurrent console and web sessions as specified in the Session Limit of that role. The default value of Session Limit is unlimited. So, if the value of Session Limit is not specified for a role, then the users included in that role can use unlimited number of concurrent sessions.

When a user in a specific role reaches the limit as specified in Session Limit of the role, and launches another session, the user receives a message on the active computer stating that maximum limit is reached and the user needs to select an option to terminate or keep the oldest session. If the oldest session is not running on the active computer then, the oldest session is terminated with a logout message and a new session is launched on the active computer. If the oldest session is running on the same computer, then the oldest session is terminated without any logout message and a new session is launched.

Session Limit for Users with Multiple Roles

If a user is added to multiple roles then the user can have the maximum session limit as mentioned in the following:

- The Session Limit that has the highest numerical value among the roles will be applicable for that user.
- The highest numeric value of Session Limit takes precedence over the default value.
- If a user is added or removed from any role, the Session Limit that has the highest value among the existing roles will be applicable for that user.

3.6 Managing Permissions

Permissions control activities that a console user can perform through Secure Configuration Manager. You can assign permissions to run a report, perform an action, or maintain security checks and task suites. You can also assign permissions to run individual task suites or categories of task suites. Permissions also let you allow or deny access to specific Secure Configuration Manager features.

To quickly and easily assign permissions, consider grouping permissions into roles. Roles let you assign a set of permissions that represent a particular job function while enforcing consistent console security. For more information, see Section 3.5, “Managing Roles,” on page 40.

NOTE: Each console user requires the Access IT Assets permission to run reports or perform actions on endpoints in your asset map.

You can specify permissions according to the type of tasks you expect a role or console user to perform. For example, if a role performs one or more tasks, specify the All Tasks permission. If the user prints reports, specify the Reports Only permission. Refer to the following table when allowing or denying permissions from the list of actions, activities, and reports.

To assign these permissions ...	Complete the following steps ...
Allow selected permissions on all endpoints	Under **All Endpoints**, click **Allow for All**.
Allow selected permissions on individual endpoints	Click **Assign Individual Permissions**, select **Endpoints**, and then click **Allow** for each endpoint.
Allow selected permissions on individual groups	Click **Assign Individual Permissions**, select **Groups**, and then click **Allow** for each group.
Deny selected permissions on all endpoints	Under **All Endpoints**, click **Deny for All**.
Deny selected permissions on individual endpoints	Click **Assign Individual Permissions**, select **Endpoints**, and then click **Deny** for each endpoint.
Deny selected permissions on individual groups	Click **Assign Individual Permissions**, select **Groups**, and then click **Deny** for each group.

You can verify how Secure Configuration Manager applies the selected permissions by clicking **Show Effective Permissions**. For more information, see Section 3.6.1, “Resolving Permission Conflicts and Inheritance,” on page 42. Be aware that permissions explicitly assigned to a console user can override permissions implicitly granted through roles.

3.6.1 Resolving Permission Conflicts and Inheritance

Console users receive permissions from assigned roles as well as individual permissions you explicitly allow or deny. When a console user attempts to run a policy template or task suite, Secure Configuration Manager checks the roles and permissions assigned to the account. Permissions explicitly assigned to a console user override permissions implicitly granted through roles.

As you assign multiple roles or explicitly grant multiple permissions to a console user, conflicts can occur. You can verify how Secure Configuration Manager applies assigned permissions by reviewing the effective permissions for each user and role. **Effective permissions** represent the permissions in effect for the console user, as well as any permissions inherited from assigned console roles. For more information about changing permissions, see Section 3.6.2, “Modifying Permission Assignments,” on page 43 and the Help.

NOTE

- If you assign permissions to a group of endpoints, and then later add a child group, Secure Configuration Manager applies those permissions to the endpoints in the child group.
- If you assign permissions to one or more activities in a category, and then later assign additional permissions to the entire category, Secure Configuration Manager applies both sets of permissions. If the permissions assigned to the category conflict with the permissions assigned to the activities, Secure Configuration Manager applies the permissions assigned to the category.

The following table shows how Secure Configuration Manager applies permissions in response to particular permission settings. Use this table to help you identify and resolve permission conflicts and inheritance.

If you assign ...	Secure Configuration Manager applies as ...
No permissions	Deny
One or more permissions that allow the same activity	Allow
One or more permissions that deny the same activity	Deny
One permission that allows the activity and another permission that denies the same activity	Deny
One or more permissions set on a category of tasks, reports, or actions	Allow or deny each task, report, or action in the category
One or more permissions set on a group of endpoints	Allow or deny activities for each endpoint in the group
One or more permissions set on a group of endpoints that contains another group	Allow or deny activities for each endpoint in the parent group
Conflicting permissions set on two or more groups that contain the same endpoint	Deny
Two or more roles that contain conflicting permissions for the same activity	Deny

3.6.2 Modifying Permission Assignments

You can add or remove permission assignments from console users and roles. For more information, see Section 3.7.3, “Assigning Permissions to a Console User,” on page 44 and Section 3.5.2, “Creating, Modifying, and Deleting Roles,” on page 41.

3.7 Managing Console Users

Managing console users is an important aspect of console security. Successful management of console users includes the following activities:

- Creating the appropriate number of console user accounts
- Maintaining complex passwords
- Assigning the appropriate roles and permissions
- Deleting unused console user accounts

3.7.1 Creating a Console User

When you create a console user, you are creating an account in the Secure Configuration Manager database. For each console user, you can specify the following attributes:

- General properties, such as user name and email address
- Type of authentication you want Secure Configuration Manager to enforce when this user logs on to the console
- Role assignments

By default, Secure Configuration Manager uses console authentication to validate this account. However, you can configure Secure Configuration Manager to use an external authentication source, such as Active Directory, to validate this account upon logon. When creating a console user account that requires external authentication, ensure that the specified user name matches the logon name of the corresponding account in the external authentication source. For more information, see Section 3.3.1, “Implementing External Authentication,” on page 38.

3.7.2 Assigning Roles to a Console User

You can grant permissions to use a set of Secure Configuration Manager features by assigning roles to a console user. Each role contains the appropriate permissions for a particular task. You can create roles that fit your specific needs or assign one of the provided NetIQ roles. For more information about creating roles, see Section 3.5.2, “Creating, Modifying, and Deleting Roles,” on page 41.

3.7.3 Assigning Permissions to a Console User

You can assign permissions based on the type of task you want the console user to perform. You can allow or deny platform-specific permissions for each endpoint or group in your asset map. For example, you can allow one set of permissions, such as User/Groups permissions, and deny another set of permissions, such as System permissions. For more information about assigning permission, see Section 3.6, “Managing Permissions,” on page 42.

NOTE: You must assign console permissions to all endpoints at once. You cannot assign console permissions to specific endpoints.

3.7.4 Working with Console User Accounts

When working with console user accounts, you may need to unlock an account that is locked out of the Secure Configuration Manager console. Secure Configuration Manager provides a real-time status that indicates whether a console user account is locked. Use this information to diagnose logon issues.

NOTE: A locked console user is not locked by the external authentication source. For example, if a console user account requires Active Directory authentication, Secure Configuration Manager can lock the user out of the Secure Configuration Manager console, but not out of Active Directory.

You can reset the password for any console user’s account, if Secure Configuration Manager uses console credentials to authenticate your console user account. If an account is configured for external authentication, use other solutions, such as NetIQ Secure Password Administrator, to reset the account password.

You can also delete a console user account to prevent the console user from logging on to Secure Configuration Manager. Regularly delete user accounts to prevent security risks and groom the Secure Configuration Manager database of inactive or old accounts. When you delete a console user account, Secure Configuration Manager transfers ownership of task suites, custom tasks, security checks, and policy templates to the default console administrator. The default console administrator is the administrator you specified during installation. To prevent a user from accessing specific Secure Configuration Manager features, remove permissions from the user account. For more information, see Section 3.6.2, “Modifying Permission Assignments,” on page 43.

4 Auditing Your IT Assets

Secure Configuration Manager enables you to quickly determine how well each IT resource in your environment complies with your company security standards. To identify misconfigured assets, you can run individual **security checks** or combine security checks into a **policy template** to run against an endpoint or a group of endpoints. Security checks test endpoints for a specific configuration setting or security risk on a specific platform, such as user privileges for an Oracle database. Policy templates group multiple security checks to test for a specific set of issues, such as those defined by the PCI DSS standards.

When you use Secure Configuration Manager to assess the level of configuration compliance in your enterprise, first identify the endpoints or groups of endpoints you want to assess. Next, create or select a security check or policy template that represents the security and system configuration policies you want to enforce. The resulting reports help you prioritize a remediation plan to protect against the vulnerabilities the security checks identify. This chapter explains the purpose for security checks and policy templates, and helps you establish a schedule of policy template runs. For more information about assessing security check and policy template results, see Chapter 5, “Evaluating Audit Results,” on page 57.

Accurately assessing your computers requires regularly updating your security knowledge. The AutoSync vulnerability content service delivers new and updated security checks and policy templates when new vulnerabilities emerge. The AutoSync feature lets you regularly download and apply this security knowledge to your policy templates to ensure protection from the latest vulnerabilities. Update your security knowledge regularly using the AutoSync feature of Secure Configuration Manager. For more information about using the AutoSync server, see Chapter 8, “Maintaining Your Security Knowledge,” on page 121.

4.1 Understanding Security Checks

Secure Configuration Manager provides hundreds of built-in security checks to ensure policy compliance. With the AutoSync feature of Secure Configuration Manager, you can receive updates of new security checks when new vulnerabilities or new security issues emerge. Examples of built-in security checks are as follows:

- Accounts with short passwords
- Anti-virus software installed
- Determine if registry key exists
- Minimum password length

To help you determine whether a security check meets your needs, the console provides an **explanation** of the check, the **risks** you face by not mitigating the issue, and recommended **remedies** to solve the risks. Each security check contains some or all of the following components.

Component	Explanation	Example
Settings	Information the check should gather from an endpoint	List of accounts with expired passwords

Component	Explanation	Example
Expected Value *or* Expected number of rows returned	Settings expected to maintain endpoint security or meet policy requirements	0 (no accounts with expired passwords)
Scoring (comparator)	How Secure Configuration Manager compares the actual results to the Expected Value	The number of accounts with expired passwords is “less than or equal to” the Expected Value
Threat factor	Numeric penalty if the endpoint fails the check	10
Exclusion list	Values that are allowed to vary from the Expected Value without penalizing the endpoint	A saved list of accounts that are allowed to have expired passwords
Severity range	Ranges for the three risk states (low, medium, and high) that Secure Configuration Manager uses to graph results	0 to 100 = Low Risk 101 to 200 = Medium Risk 201 and up = High Risk
Report	Formal output of the checked results	Physical report in the Completed jobs queue

Some security checks include user-definable parameters so you can customize the check for each particular run. For example, the AD Group Changes Within X Days check looks for changes made to the AD group within a user-specified number of days. Most parameters have a default value. In the AD Group Changes Within X Days check, the default value is 14 days.

You can modify many built-in security checks or create custom checks to match specific policies. You can also use custom checks to respond to more complex vulnerabilities as they arise. If you create custom security checks or modify built-in security checks in the Secure Configuration Manager console, you can export those checks as XML-formatted files with a `.chk` extension. You can also export some built-in checks. In the content pane where checks are listed, a value of **Yes** in the Export column indicates that you can export that check. To export security checks, your console user account needs the Export Security Check permission. You can import security checks that were previously exported or custom checks created outside of the console. You can also use the import feature to restore a security check that was changed incorrectly. If a check with the same name already exists, Secure Configuration Manager gives you the option to overwrite the existing check. To import security checks, your console user account needs the Import Security Check permission.

The following table shows where you can learn more about security checks.

If you want to ...	See ...
Create an exclusion list	Section 4.3.3, “Excluding Values from a Run,” on page 51
Modify a built-in security check	Section 6.4.2, “Modifying Built-in Security Checks,” on page 98
Create a custom security check	Section 6.4.3, “Creating Custom Security Checks,” on page 99
Learn more about security check components	Section 6.2, “Understanding Security Check Components,” on page 87
Learn more about the threat factor and scoring security check results	Section 6.3, “Understanding Risk Scoring,” on page 94

If you want to ...	See ...
Compare the results for individual endpoints or security checks	Section 5.3, “Comparing Report Results,” on page 63
Learn more about the Completed jobs queue	Section 4.5, “Viewing Report Results,” on page 55 and Section 10.2, “Customizing the Job Queues,” on page 137
Learn more about the AutoSync server	Chapter 8, “Maintaining Your Security Knowledge,” on page 121
Learn more about managing permissions in the console	Section 3.6, “Managing Permissions,” on page 42

4.2 Understanding Policy Templates

Policy templates let you quickly and easily determine the compliance of your entire enterprise with your security policies. Each policy template contains multiple security checks designed to search for a specific set of issues. Secure Configuration Manager includes a large number of built-in policy templates, organized in the following categories: Regulations, Bulletins, and Best Practices. For example, under Best Practices, the CIS Benchmark policy templates include security checks based on recommendations from the Center for Internet Security (CIS) and are certified by CIS.

You can modify the built-in policy templates or create new templates to express corporate technical standards and current industry standards. To determine whether a particular policy template meets your enterprise’s needs, you can print information about the security checks in that policy template. To print policy template information, your console user account needs the Print Policy Template Information permission. You must also have Adobe® Reader® installed on the console computer to print and view the report.

Occasionally, you might want to save a specific version of a policy template before downloading a newer version from the AutoSync server. You can export templates as XML-formatted files with a `.tpl` extension. To export a policy template, your console user account needs the Export Policy Template permission. You can import one or more policy templates you have previously exported from the current Core Services or another Secure Configuration Manager Core Services. You can also use the import feature to restore a policy template that was changed incorrectly. If a policy template with the same name already exists, you have the option to overwrite the existing template. To import a policy template, your console user account needs the Import Policy Template permission.

Many built-in policy templates use the same security check multiple times to validate different system settings. When the template contains multiple **instances** of the same check, each instance can be identified by a unique name, or Check Alias. For example, the CIS Level One Benchmark for Windows Server 2003 policy template includes multiple instances of the User rights security check. The alias for the first User rights instance is “4.2.1 Access this computer from the network” to indicate the check validates the status of network logon privileges on the endpoint. The second instance, “4.2.10 Create a pagefile,” validates privileges for creating page files.

The following table shows where you can learn more about policy templates.

If you want to ...	See ...
Modify a built-in policy template	Section 6.6.3, “Modifying Built-in Policy Templates,” on page 108
Create a custom policy template	Section 6.6.2, “Translating a Technical Standard to a Policy Template,” on page 107

If you want to ...	See ...
Compare the results for policy template runs	Section 5.3, “Comparing Report Results,” on page 63
Evaluate endpoints based on policy template results	Section 5.3.2, “Comparing Policy Template Results,” on page 63
Learn more about the AutoSync server	Chapter 8, “Maintaining Your Security Knowledge,” on page 121
Learn more about managing permissions in the console	Section 3.6, “Managing Permissions,” on page 42

4.3 Running Security Checks and Policy Templates

When you run a security check or policy template, Secure Configuration Manager compares all the endpoints you specify to all the preferred security settings listed in the security checks. When running a policy template against a group of endpoints, Secure Configuration Manager checks each endpoint in the group for each security check in the policy template. Secure Configuration Manager runs only the security checks that apply to the endpoint type. For example, security checks related to Active Directory run only on Windows computers.

You can run security checks and policy templates at any time. If you want to gather data for a specific period of time, you can run reports from the database rather than from the agent computer. The database maintains results from previous runs of each security check and policy template. If you want to detect changes to systems in your enterprise and ensure that a positive trend for compliance with your organizational security policies, you can schedule policy templates to run on a regular basis. You can compare results for each run using the delta report function. For more information about gathering security check or policy template data from the database, see Section 4.3.1, “Running Reports from the Database,” on page 50. For more information about delta reporting, see Section 5.3, “Comparing Report Results,” on page 63. For more information about scheduling, see Section 4.3.2, “Scheduling a Policy Template Run,” on page 51.

If you do not know which policy templates or security checks you want to run, you can initiate a search based on several criteria. For example, you can search for policy templates based on keywords in the name or description, or in the name, description, or explanation of the security checks in the template. You can also search for security checks based on keyword, platform, category, and other criteria.

The time it takes to run a security check or policy template varies, depending on the number of checks and endpoints you select. Ensure that the report is complete before you view the resulting report in the Completed jobs queue. You can print or distribute the completed report to present compliance status results or to use as a remediation checklist. For more information about completed reports, see Section 4.5, “Viewing Report Results,” on page 55. For more information about distributing a copy of the report, see Section 4.4, “Enabling Report Distribution,” on page 53.

To run a policy template, your console user account needs the Run Policy Template permission. To run a security check, your console user account must have the Run Security Checks permission. For more information, see Section 3.6, “Managing Permissions,” on page 42.

4.3.1 Running Reports from the Database

Secure Configuration Manager provides the Run from Database option for creating an aggregated report about your assets. When you run a security check or policy template, Secure Configuration Manager compiles the results into a report. Each run against your endpoints adds a unique report to the Completed jobs queue and updates the database. The Run from Database option enables you to

collect the results from multiple runs into one report. The database always provides the results for the most recent run of the selected policy template or security check during the time period you specify for the aggregated results.

Running reports from the database can be beneficial in certain circumstances. For example, you have a large environment with assets in Texas, New York, and Florida. You organized your assets into managed groups to represent the regional areas. Then you scheduled a CIS Benchmark policy template to run against each of the groups every Friday night at staggered times. This means you have a separate report for each group. However, management wants to review the status of the systems in Texas, Florida, and New York as a whole. You can use the Run from Database option to aggregate the policy template results into a single report.

In a different scenario, you run a policy template against a group of endpoints. The report lists some endpoints as failed, indicating that they might have been offline. You run the template again for the failed endpoints. You now have separate reports for the same policy template and the same group of endpoints. Once you are satisfied you have results for all endpoints, you can run the template against the database for an aggregated report.

NOTE: The Run from Database option applies only to multiple runs of the same security check or policy template. Each run must use identical parameter settings to ensure accurate reporting.

For more information about running reports from the database, see the Help in the Run Security Check and Run Policy Template wizards.

4.3.2 Scheduling a Policy Template Run

If you want Secure Configuration Manager to continuously assess your IT environment, you can regularly run a policy template against the same endpoint or group of endpoints. To schedule a policy template run, use the Schedule tab in the Run Policy Template wizard. When you schedule a run, you can instruct Secure Configuration Manager to include a delta report that compares the current results to a previous run. For more information about running a policy template, see Section 4.3, “Running Security Checks and Policy Templates,” on page 50. For more information about delta reporting, see Section 5.3.2, “Comparing Policy Template Results,” on page 63.

Once you have scheduled a policy template, you can update the schedule properties using the Schedule Jobs wizard. If you are a console administrator, you can also reassign the owner of a scheduled policy template. For more information about console roles, see Section 3.5, “Managing Roles,” on page 40.

4.3.3 Excluding Values from a Run

Many security checks in Secure Configuration Manager return a set of results containing multiple rows of data. When you run a policy template with many security checks, the resulting list of returned rows can be difficult to review. If you want to exclude some values from the returned results, use a **saved list**. Saved lists are lists of values that you can reuse in security checks as a filter or exclusion list. Saved lists can include values such as user names, file names, registry keys, ports, or services. For example, administrators often exclude user accounts such as SYS, SYSDBA, sa, and root from security checks. You can create a saved list that includes these user accounts, and use the saved list to filter the user accounts from the security check results. You can also have a list of values you want to include in checks, such as a specific list of files and directories.

NOTE: Saved lists do not support wildcard characters.

You can use any saved list you create in any security check that provides an Exclusion List or Inclusion List parameter. As you update your inventory and security policies, you can revise the saved lists used in your security checks. You cannot delete saved lists that are part of a security check. Refer to the following table when assigning permissions to console users who work with saved lists.

User activity	Required permission
Create a saved list	New Saved List
Edit a saved list	Edit Saved List
Delete a saved list	Delete Saved List
Import a saved list	Import Saved List
Export a saved list	Export Saved List

For more information about importing saved lists, see “Importing Saved Lists” on page 53. For more information about exporting a saved list, see “Exporting Saved Lists” on page 53. For more information about assigning permissions, see Section 3.6, “Managing Permissions,” on page 42.

Using Saved Lists in an Existing Security Check

You can use saved lists to exclude or include values from existing security checks when you run those checks. If you have values in an exclusion or inclusion list that you entered in a previous version of Secure Configuration Manager, you can easily migrate those values to be part of a saved list.

To use a saved list as a list in a security check:

1. In the left pane, click **Security Knowledge**.
2. In the Security Knowledge tree pane, expand **Security Checks > NetIQ Checks**.
3. Expand the platform folder and select the category folder that contains the check that you want to run.
4. In the content pane, right-click the security check that you want to run, and then click **Run Security Check**.
5. On the Parameters window, click **Exclusion List** or **Inclusion List**, depending on the check.
6. Type the name of the saved list or click the button at the end of the Exclusion List or Inclusion List line, and then select the saved list whose entries you want to exclude from or include in the security check.
7. Follow the instructions in the wizard to run the report.

Importing Saved Lists

You can import saved lists to use in Secure Configuration Manager. If a saved list with the same name already exists, Secure Configuration Manager gives you the option to overwrite the existing saved list. For example, your organization might have a technical security specification that includes a list of files to secure through appropriate file permissions. You can create a saved list by copying the list of files from the technical specification to a text file, and then importing the text file.

To import a saved list, your console user account needs the Import Saved List permission. For more information, see Section 3.6, “Managing Permissions,” on page 42.

To import a saved list:

1. In the left pane, click **Exception Management**.
2. In the Exception Management tree pane, right-click **Saved Lists**, and then click **Import**.
3. Select the saved list file you want to import and click **Open**.

Exporting Saved Lists

After you have created saved lists, you can export those saved lists as XML-formatted files with an `.slt` extension. For example, you can run a report of powerful users and export the list to a file. You can then create a saved list to use the powerful users in other queries as either an inclusion or exclusion list.

To export a saved list, your console user account needs the Export Saved List permission. For more information, see Section 3.6, “Managing Permissions,” on page 42.

To export a saved list:

1. In the left pane, click **Exception Management**.
2. In the Exception Management tree pane, select **Saved Lists**.
3. Right-click the saved list that you want to export, and then click **Export**.
4. Enter a file name for the saved list and click **Save**.

4.3.4 Running Network Device Security Checks

4.4 Enabling Report Distribution

When you run or schedule a run of a security check or policy template, you can specify whether you want to distribute a copy of the report to a file or share or to specific users through email.

NOTE

- To distribute a report, you must install the Secure Configuration Manager console on the same drive where you installed Core Services.
- To distribute a report in Excel format, Microsoft Excel must be installed on the Core Services computer. For more information, see the *Installation Guide for NetIQ Secure Configuration Manager*.

4.4.1 Distributing Reports to a File or Share

When you run a security check or policy template in the run wizards, you can distribute a copy of the report to a file or share. To distribute a report, your Core Services account needs the Full Control permissions to the file or share where you want to save the report. By default, Core Services runs under the LocalSystem account. For more information, see Section 3.6, “Managing Permissions,” on page 42.

NOTE

- To distribute a report, you must install the Secure Configuration Manager console on the same drive where you installed Core Services.
- To distribute a report in `Excel` format, Microsoft Excel must be installed on the Core Services computer. For more information, see the *Installation Guide for NetIQ Secure Configuration Manager*.

To distribute reports to a file or share:

1. In the left pane, click **Security Knowledge**.
2. In the Security Knowledge tree pane, expand the tree to locate the security check or policy template that you want to run.
3. In the content pane, right-click the security check or policy template you want to run, and then click the Run option.
4. In the run wizard, click **Targets**, and then select the group or individual endpoints that you want to check.
5. Click **Distribution**.
6. Select **Enable Distribution**.
7. Click **Add**, and then select **File distribution**.
8. In the File Distribution window, complete the required fields.
9. (Optional) To overwrite an existing file, select **Overwrite existing file**.
10. (Optional) To create a new file for each report run, select **Save all runs of the report**.
11. (Optional) To compress the report, select **Compress this file before distributing** and then specify the file extension for the compressed file.
12. Click **OK**.
13. Click **Finish**.

4.4.2 Distributing Reports to an Email Recipient

When you run a security check or policy template in the run wizards, you can distribute a copy of the report to an email recipient. To distribute a report through email, ensure that you have specified a mail server for Secure Configuration Manager to use to send email. You can specify a mail server using the Core Services Configuration Utility.

NOTE

- To distribute a report, you must install the Secure Configuration Manager console on the same drive where you installed Core Services.
- To distribute a report in `Excel` format, Microsoft Excel must be installed on the Core Services computer. For more information, see the *Installation Guide for NetIQ Secure Configuration Manager*.

To distribute reports through email:

1. In the left pane, click **Security Knowledge**.
2. In the Security Knowledge tree pane, expand the tree to locate the security check or policy template you want to run.
3. In the content pane, right-click the security check or policy template that you want to run, and then click the Run option.
4. In the wizard, click **Targets**, and then select the group or individual endpoints that you want to check.
5. Click **Distribution**.
6. Select **Enable Distribution**.
7. Click **Add**, and then select **Email distribution**.
8. In the Email Distribution window, complete the required fields.
9. (Optional) To compress the report, select **Compress this file before distributing** and then specify the file extension for the compressed file.
10. Click **OK**.
11. Click **Finish**.

4.5 Viewing Report Results

As Secure Configuration Manager runs a security check or policy template, the console displays a report in the Pending jobs queue. When the run completes, Secure Configuration Manager moves the report to the Completed jobs queue. To view available reports, select **Job Queues** in the left pane, and then **Completed** in the content pane. When you open a report, Secure Configuration Manager launches the Report Viewer. From the Report Viewer, you can export results in a variety of file formats. For more information about exporting report results, see Section 4.6, “Exporting Reports,” on page 56. For more information about graphics in the report, see Section 10.1, “Creating Custom Tasks and Reports,” on page 135.

NOTE: When you attempt to view large reports in the Report Viewer, the console might time out and disconnect from the database. To prevent this issue, change the **Database Timeout for Console** setting in the **Tools > Options** window to a longer period of time.

If the completed report indicates one or more endpoints failed security checks, you can re-run the failed checks for those endpoints only. To re-run checks for failed endpoints, right-click the completed report, and then click select **Re-run for Failed Endpoints**. Secure Configuration Manager generates a new report in the Completed jobs queue. For information about evaluating report results, see Chapter 5, “Evaluating Audit Results,” on page 57.

4.6 Exporting Reports

Once Secure Configuration Manager completes a security check or policy template run, you can export the completed report to a variety of file formats. For policy template reports, you can specify whether the full report lists security checks according to their order in the template or alphabetically by their names or specified aliases. The check sort order applies to reports exported in `.pdf`, `.rtf`, `.tsv`, `.xml`, `.xls`, and `.xlsx` formats.

To export report data:

1. View the complete report. For more information about viewing reports, see Section 4.5, “Viewing Report Results,” on page 55.
2. Click **Full Report**.
3. (Optional) To change the sort order of the checks in the policy template, click **Full Report Options**, and then select the appropriate option from the Check Sort Order menu.
4. On the Actions menu, click **Export Report**.
5. Type the file name, and then select one of the following file formats:
   - `.pdf`
   - `.tsv`
   - `.rtf`
   - `.xml` (XML or XCCDF)
   - `.xls` or `.xlsx` (depending on the Excel version that you use)

   NOTE: To export a report in Excel format from the Report Viewer, Microsoft Excel must be installed on the Secure Configuration Manager console computer from which you are exporting the report and installed on the Core Services computer. For more information, see the *Installation Guide for NetIQ Secure Configuration Manager*.
6. Click **Save**.

5 Evaluating Audit Results

Secure Configuration Manager enables you to manage the risks inherent in an IT landscape. First, you must identify and run the security checks and policy templates representing the security and system configuration policies you want to enforce. For more information about running security checks and policy templates, see Chapter 4, “Auditing Your IT Assets,” on page 47. Next, use the reported results to evaluate asset compliance and establish a prioritized remediation plan to protect against the discovered vulnerabilities. Secure Configuration Manager provides a set of evaluation tools to help you determine how well each IT asset in your environment complies with your policies and to streamline the evaluation and remediation process.

Delta Reports

Provides console users a method for determining which settings on an unknown or noncompliant endpoint vary from a known, secure endpoint so IT managers can more efficiently remediate the issues. Console users can also evaluate changes to an endpoint’s results between policy template runs.

Asset Compliance View

Provides console users a starting point in the Secure Configuration Manager console for identifying which IT assets are out of compliance with the enterprise’s security standards, and whether the vulnerability of those systems poses a high, medium, or low risk.

Security and Compliance Dashboard

Provides a Web-based method for executives and managers to view the overall compliance of their IT assets and to perform a more granular assessment of specific groups and computers.

Security Checkup Results Viewer

Allows managers and console users to remotely audit enterprise security by reviewing which assets are in compliance, out of compliance, or have an unknown compliance for each policy template.

With each of these tools, you can browse endpoint data to see exactly which checks in the policy template failed and learn how to remediate the issue. You can also configure Secure Configuration Manager to automatically notify you when an asset falls out of compliance. Receiving notifications can help you expedite the remediation process. If your company uses a change management ticketing system to manage remediation efforts, you can configure Secure Configuration Manager to send an email to your change management system when an asset falls out of compliance.

5.1 Understanding Report Results

When you run a security check or policy template, the resulting report provides a snapshot of each endpoint’s condition at the time you ran the check or template. The results include discovered configuration violations and a **risk score** for each selected endpoint for each applicable security check run. Secure Configuration Manager calculates the risk score based on two factors: the threat level of the discovered violations and the importance of the asset to the company. For more information about endpoint importance, see Section 2.5.2, “Assigning Importance to Endpoints,” on page 34. For more information about scoring, see Section 6.3, “Understanding Risk Scoring,” on page 94.

NOTE: When you assign importance levels to all endpoints, the weighted report results help you identify which computers have the most serious exposures and need remedial attention first.

You can view and print the report results. Secure Configuration Manager places the completed report in the Completed jobs queue. You can use the printed reports for presenting compliance status results or as a remediation checklist. When you view a completed report, the Report Viewer opens in the Report Summary view. This view gives you a thorough overview of the report, providing you with important information such as the endpoints with the highest risk scores, and the most frequently violated security checks.

Once you have completed security check and policy template runs, you can use the available evaluation tools to assess compliance trends and report asset compliance to auditors and management. You can also use the delta report function to identify changes in your environment and determine which endpoints need to be updated.

5.2 Excluding Data from Report Results

Secure Configuration Manager enables you to create temporary waivers, or **exceptions**, to prevent conditions from causing a violation in the reported results for a security check in a policy template. Typically, you create an exception when you do not want a particular violation to display in the report, or when you want to prevent a particular security check from running for an endpoint or a group of endpoints. For example, if a server in your environment is currently undergoing maintenance, you might want to create an exception to suspend monitoring that server with certain security checks.

Secure Configuration Manager applies exceptions consistently. If you create an exception for a security check within a policy template, Secure Configuration Manager applies that exception to all other runs of that policy template where the same violation is returned or the same security check runs for that endpoint or group of endpoints. Exceptions continue to affect the total risk score for an endpoint, even when the violation is excluded.

NOTE: You can also use a saved list to filter returned values from a security check run. For more information about using saved lists, see Section 4.3.3, “Excluding Values from a Run,” on page 51.

To create an exception in Secure Configuration Manager, you must base it on a report that contains the exception. This means you must create a report that includes the exception to be able to edit the exception. If you delete all reports that include a particular exception, you cannot edit the exception. To edit the exception, you must run a new report that includes the exception.

When you create an exception, you can assign a reason code to explain why you created the exception. For example, a reason code of Mitigated Risk means the risk is no longer present. You can also specify the reason code of Accept Risk, which indicates the risk is still present but acceptable. You can create your own reason codes to explain why you created the exception. For more information about reason codes for exceptions, see the Help.

Secure Configuration Manager also gives you the option to require approvals for exceptions before applying them to a security check in a policy template or to an endpoint or group of endpoints. This option facilitates a secure method of managing the exception review and approval process.

Refer to the following table when assigning permissions to console users who work with exceptions.

User activity	Required permission
Create an exception	◆ View Policy Template ◆ New Exception
Apply an exception	Apply Exception
Approve or disapprove an exception	Approve Exceptions
Edit an exception	◆ View Policy Template ◆ Edit Exception
Delete an exception	Delete Exception

kFor more information about assigning permissions, see Section 3.6, “Managing Permissions,” on page 42.

5.2.1 Exceptions for Security Checks

Secure Configuration Manager applies exceptions to security checks when the combination of the selected security check and the selected endpoint or group of endpoints occurs within the policy template. You can create an exception from a security check in the Data View tree pane of the Report Viewer, or from any of the rows in the Data View right pane of the Report Viewer.

When you create an exception for a security check, you have the option to except all data returned by the security check for the selected endpoints or group of endpoints, or to except specific data returned by the security check.

5.2.2 Exceptions for Endpoints and Groups

You can create exceptions for endpoints or groups of endpoints in several ways. Secure Configuration Manager can except an endpoint or group of endpoints across your environment, regardless of the policy template or security checks run for the endpoint. You can also create an exception for an endpoint for a specific policy template. When you create an exception in a completed report, you must start by selecting a single endpoint or the endpoint group. You can also except additional endpoints for which the report was run. For more information, see Section 5.2.3, “Creating an Exception,” on page 59.

5.2.3 Creating an Exception

In addition to excepting a specific endpoint, a group of endpoints, or a security check, you can create exceptions for a combination of row and column data in a security check. The information per column and row varies by security check and endpoint type. For example, you can except an endpoint whose account status is disabled for the Accounts That Have Never Logged In security check.

NOTE: If you create a check with a unique count, simple value, or single value scoring type and then apply exceptions for row or column data, such as one data point in the check, Secure Configuration Manager might return unexpected managed risk and excepted risk scores. For more information about scoring security check violations, see Section 6.3, “Understanding Risk Scoring,” on page 94.

To create an exception, your console user account needs the View Policy Template and New Exception permissions. For more information, see Section 3.6, “Managing Permissions,” on page 42.

To create an exception:

1. Open the report for which you want to create an exception.
2. Click the Data View tab.
3. (Conditional) To except a security check, complete the following steps:
   - **3a** Expand **Security Checks** in the tree pane, and then expand the security check that you want to except from the report results.
   - **3b** Right-click any endpoint listed under the security check, and then click **Create Exception**.
4. (Conditional) To except an entire endpoint or a group of endpoints, complete the following steps:
   - **4a** Expand **Target Endpoints or Target Groups** in the tree pane.
   - **4b** Locate the endpoint or group of endpoints you want to except from the report results.
   - **4c** Right-click the endpoint or group of endpoints, and then click **Create Exception**.

   NOTE: You can create an exception for either an individual endpoint or for a group of endpoints in a report. However, you cannot except both an endpoint and a group of endpoints in the same report at the same time.

   ---
5. (Conditional) To except only one datapoint for an endpoint in a security check, complete the following steps:
   - **5a** Expand **Security Checks** in the tree pane, and then select the security check.
   - **5b** In the right pane, right-click the data point corresponding to the appropriate row and column you want to except from the security check, and then click **Create Exception**.
6. (Conditional) To except multiple data points for an endpoint in a security check, complete the following steps:
   - **6a** Select **Security Checks** in the tree pane.
   - **6b** In the right pane, select the security check name or alias.
   - **6c** Right-click the check name or alias, and then click **Create Exception**.
   - **6d** On the Criteria tab, select **where returned data matches ‘<returned data>’**.
   - **6e** Select **‘<returned data>’**, then click the columns and rows you want to except from the report results.
7. Follow the instructions in the wizard until you have finished creating the exception.

5.2.4 Enabling and Approving Exceptions

By default, Secure Configuration Manager allows you to apply exceptions to security check results or endpoints immediately. You can also require that exceptions receive approval before being applied to security check results, an endpoint, or a group of endpoints. This option gives you the flexibility to add an exception approval level to your change management workflow.

If you enable exception approvals, exceptions must be approved before you can apply them. To approve or disapprove exceptions, your console user account needs the Approve Exceptions permission. For more information about permissions, see Section 3.6, “Managing Permissions,” on page 42.

To enable exception approvals:

1. On the Core Services computer, start the Core Services Configuration Utility in the NetIQ Secure Configuration Manager program folder.
2. On the Exception Approvals tab, select `True` in the **Enable Exception Approvals** field.
3. Click **OK** to save the changes and close the Core Services Configuration Utility.

5.2.5 Applying Exceptions

You can apply approved exceptions to security check results, endpoints, or groups of endpoints. When you apply exceptions, the report returns to the Pending jobs queue. Once Secure Configuration Manager applies all exceptions to the report, the report moves to the Completed jobs queue.

To apply exceptions, your console user account needs the Apply Exceptions permission. For more information, see Section 3.6, “Managing Permissions,” on page 42.

To apply exceptions:

1. (Conditional) If you are currently viewing a completed report, click **Apply Exceptions** on the toolbar and click **OK** on the confirmation message.
2. In the left pane, click **Job Queues**.
3. In the Job Queues tree pane, select **Completed**.
4. In the content pane, select the report to which you want to apply exceptions.
5. Right-click the report, and then click **Apply Exceptions**.
6. Click **Yes**.

5.2.6 Editing an Exception

As you update your inventory and security policies, you may need to revise the exceptions that you use when assessing your environment. To edit an exception, including all defined endpoints, endpoint groups, security checks, and policy templates, your console user account needs the View Policy Template and Edit Exception permissions. For more information, see Section 3.6, “Managing Permissions,” on page 42.

NOTE

- You can update exception scheduling options and approval status through the **Exception Management > Exceptions** node in the tree pane.
- When you edit an approved exception, it must be approved again before you can apply it to a security check, an endpoint, or a group of endpoints. However, until the edited exception is approved again, Secure Configuration Manager continues to apply the original exception.

5.2.7 Deleting an Exception

As you update your inventory and security policies, you may need to revise the exceptions that you use when assessing your environment. To delete an exception, your console user account needs the Delete Exception permission. For more information, see Section 3.6, “Managing Permissions,” on page 42.

NOTE: When you delete an exception, Secure Configuration Manager does not automatically update the reports to which the exception is already applied. You must rerun the policy template to see results without the exception applied.

5.2.8 Listing Exceptions

The Admin Reports wizard lets you run reports to list Secure Configuration Manager administrative data. For example, you can list all exceptions created in the product, then you can either print an administrative report, or export it to a file. To run administrative reports, your console user account needs the Admin Reports permission. For more information, see Section 3.6, “Managing Permissions,” on page 42.

To list exceptions:

1. On the Tools menu, click **Admin Reports Wizard**.
2. Select the Exceptions report.
3. Follow the instructions until you have run the administrative report.
4. (Optional) Print or export the report.

5.3 Comparing Report Results

You can use the Secure Configuration Manager delta reporting feature for comparing report results to easily identify and monitor changes to systems. For example, if you regularly run a policy template, you can observe changes to an endpoint's results from run to run. You can also compare a known, good endpoint's results against those of another endpoint for the same policy template run. Similarly, you can compare the results of two endpoints from a single security check run.

Since delta reports compare specific data fields, those fields must match in the two reports you want to compare. Therefore, you can run delta reports only for security check and policy template reports generated for endpoints managed by the same agent version. Also, if a security check was edited between runs, Secure Configuration Manager can only compare the unchanged fields in the check.

You can schedule a delta report to run on a recurring basis. You can also distribute a delta report using email or save it to a folder or file share. For more information about the Delta Comparison wizard, see the Help.

The Delta Comparison View in the delta report can indicate both a change in the managed risk at the security check level and differences in the endpoint results. That is, when you select Security Checks at the top level of the view, the report might indicate "Unchanged" because the overall scoring for the endpoints did not change for the selected runs. For example, information-only security checks always indicate "Unchanged" at the top level of the view because the managed risk value does not vary with endpoint results. However, the data results for individual endpoints might have changed between runs. To view whether endpoint results changed, you must expand the selected check in the navigation pane of the Delta Comparison View. The content pane then lists endpoint results, such as "Added" or "Deleted" if a change occurred between runs.

5.3.1 Comparing Security Check Results for Two Endpoints

Once you run a security check against a group of endpoints, you can create delta reports to compare the security check's results for two of those endpoints. For example, you may have a known, good endpoint to use as a base to compare a newer, unknown endpoint.

To create a delta report comparing two endpoints:

1. In the left pane, click **Job Queues**.
2. In the Job Queues tree pane, select **Completed**.
3. In the content pane, select the report for which you want to compare runs.
4. In the bottom of the content pane, click the Endpoints tab.
5. Hold down Shift or Ctrl and select the two endpoints you want to compare.
6. Right click the selections, then click **Run Delta Report**.
7. Follow the instructions in the wizard to run the report.
8. (Optional) To include specific data in the Delta Report, click the **Layout** tab in the Report Options window and select the boxes for *Same* or *Different*. For more information, see Section 5.3.3, "Filtering a Delta Report," on page 64.
9. To view the report, double-click the report name in the **Completed** jobs queue.

5.3.2 Comparing Policy Template Results

When you compare policy template results, you can observe changes to an endpoint's results from run to run. You also can compare the results for a known, good endpoint against those of another endpoint for the same policy template run.

NOTE: To create, schedule, or distribute a delta report for a policy template, at least one run of the policy template must be complete.

Secure Configuration Manager provides two methods for running a delta report to compare policy template results: from the Run Policy Template wizard and from completed report in the Completed jobs queue. If you only have one run of the policy template, you can enable delta reporting as you set up another run of the policy template. Also, you can schedule automatic runs of the delta report from the Run Policy Template wizard. Alternatively, if you only need one delta report and already have two or more completed runs of the same policy template, you can generate the delta report from the Completed jobs queue.

To create a delta report comparing policy template results:

1 (Conditional) If two runs of the policy template are complete, complete the following steps:

- **1a** In the left pane, click **Job Queues**.
- **1b** In the Job Queues tree pane, select **Completed**.
- **1c** In the content pane, select the policy template report for which you want to compare runs.
- **1d** In the bottom of the content pane, click the All Runs of this Report tab.
- **1e** Hold down **Shift** or **Ctrl** and select the two report runs you want to compare.
- **1f** Right-click the selections, then click **Run Delta Report**.
- **1g** Follow the instructions in the wizard to run the report.
- **1h** (Optional) To include specific data in the Delta Report, click the Layout tab in the Report Options window and select the boxes for **Added**, **Deleted**, **Modified**, or **Unchanged**. For more information, see Section 5.3.3, “Filtering a Delta Report,” on page 64.
- **1i** Click **Finish**.

2 (Conditional) If only one run of the policy template is complete, complete the following steps:

- **2a** In the left pane, click **IT Assets**.
- **2b** In the IT Assets tree pane, expand **Managed Groups** and select the same managed group or individual endpoints that the previous run of the policy template ran against.
- **2c** Right-click the group or endpoints, then click **Run Policy Template**.
- **2d** Follow the instructions in the wizard, ensuring you select the same policy template.
- **2e** On the Delta Reporting window, select **Enable Delta Reporting**.
- **2f** Click **Setup**.
- **2g** Follow the instructions in the Delta Comparison wizard.
- **2h** (Optional) If you want to include specific data in the Delta Report, click the **Layout** tab in the Report Options window and select the boxes for **Added**, **Deleted**, **Modified**, or **Unchanged**. For more information, see Section 5.3.3, “Filtering a Delta Report,” on page 64.
- **2i** Click **Finish**.
- **2j** Follow the remaining instructions in the Run Policy Template wizard.

3 To view the report, double-click the report name in the **Completed** jobs queue.

5.3.3 Filtering a Delta Report

When comparing policy templates, you can specify whether the delta report includes added, modified, deleted, or unchanged data. Alternatively, if you compare endpoints, you can specify whether you want to include data that is the same or different between the endpoints. You can apply this filter

when generating a report and when viewing a completed report. For example, you might want a delta report to include all differences compared to the base report but print the delta report with the added data only.

NOTE

- Filters apply at the data level only. The delta comparison function cannot compare changes made to a check, such as modifications to attribute criteria. To determine if a check has been modified, review the Audit History log.
- Some operating systems might interpret modifications as additions and deletions. For example, if you modify the user name ADMINISTRATOR to ADMIN, the system reports that ADMINISTRATOR was deleted and ADMIN was added. To ensure that similar changes are included in the delta report, you might want to enable the Added and Deleted options.
- The report displays a message when data results do not match the chosen filters.

To filter a delta report:

1 (Conditional) To generate a new delta report, complete the following steps:

1a Follow the instructions in the Delta Comparison wizard.

1b In the Report Options window, click the Layout tab.

1c Specify the filters you want to apply to the data.

1d Click **Finish**.

1e Follow the remaining instructions in the wizard.

2 (Conditional) To view a delta report, complete the following steps:

2a Click the Full Report tab.

2b Click **Full Report Options**.

2c On the Report Options window, click the Layout tab.

2d Specify the filters you want to apply to the data.

2e Click **Finish**.

3 (Optional) To distribute the filtered delta report to a folder, file share, or email recipient, see Section 5.3.5, “Distributing Delta Reports to a File Share or Folder,” on page 66 and Section 5.3.6, “Distributing Delta Reports to an Email Recipient,” on page 67.

5.3.4 Scheduling a Delta Report

You can schedule a delta report to run each time a scheduled policy template runs for the same endpoint. This method provides two reports at runtime: the report containing results for the policy template run and the delta report.

NOTE: To distribute a report, you must install the Secure Configuration Manager console on the same drive where you installed Core Services.

To schedule a delta report with a policy template:

1 Ensure that at least one run of the policy template is complete. For more information, see Section 5.3.2, “Comparing Policy Template Results,” on page 63.

2 In the left pane, click **IT Assets**.

3 In the IT Assets tree pane, expand **Managed Groups** and select the same managed group or individual endpoints that the previous run of the policy template ran against.

4 Right-click the group or endpoints, then click **Run Policy Template**.

5 Follow the instructions in the wizard, ensuring you select the same policy template.

6 In the Schedule window, specify how often you want the report to run on a recurring basis.

7 In the Delta Reporting window, select **Enable Delta Reporting**.

8 Click **Setup**.

9 Follow the instructions in the Delta Comparison wizard, and then follow the remaining instructions in the Run Policy Template wizard.

5.3.5 Distributing Delta Reports to a File Share or Folder

When distributing a scheduled delta report, you can choose to overwrite the existing report so only the latest copy of the report is in the folder or share. Your Core Services account needs the Full Control permissions to the file share where you want to save the report. By default, Core Services runs under the LocalSystem account. For more information, see Section 3.6, “Managing Permissions,” on page 42.

NOTE

- To distribute a report, you must install the Secure Configuration Manager console on the same drive where you installed Core Services.
- To distribute a delta report, at least one run of the policy template must be complete.
- To distribute a report in Excel format, Microsoft Excel must be installed on the Core Services computer. For more information, see the *Installation Guide for NetIQ Secure Configuration Manager*.
- When you distribute a report in `.xml` format, Secure Configuration Manager does not apply filters that were applied to the viewed report. For more information, see Section 5.3.3, “Filtering a Delta Report,” on page 64.

To distribute a delta report to a file share or folder:

1 Ensure that at least one run of the policy template is complete. For more information, see Section 5.3.2, “Comparing Policy Template Results,” on page 63.

2 In the left pane, click **IT Assets**.

3 In the IT Assets tree pane, expand **Managed Groups** and select the same managed group or individual endpoints that the previous run of the policy template ran against.

4 Right-click the group or endpoints, then click **Run Policy Template**.

5 Follow the instructions in the wizard, ensuring you select the same policy template.

6 In the Delta Reporting window, select **Enable Delta Reporting**.

7 Click **Setup**.

8 Follow the instructions in the Delta Comparison wizard.

9 In the Distribution window, select **Enable Distribution**.

10 Click **Add**, and select **File distribution**.

11 In the File Distribution window, complete the required fields.

12 (Optional) To overwrite an existing file, select **Overwrite existing file**.

13 (Optional) To ceate a new file for each report run, select **Save all runs of the report**.

14 (Optional) To compress the report, select **Compress this file before distributing** and then specify the file extension for the compressed file.

15 Click **OK**.

16 Click **Finish**.

17 Follow the remaining instructions in the Run Policy Template wizard.

5.3.6 Distributing Delta Reports to an Email Recipient

To distribute delta report results to specified users through email, ensure that you have specified a mail server for Secure Configuration Manager to use to send email. You can specify a mail server using the Core Services Configuration Utility.

NOTE

- To distribute a report, you must install the Secure Configuration Manager console on the same drive where you installed Core Services.
- To distribute a delta report, at least one run of the policy template must be complete.
- To distribute a report in Excel format, Microsoft Excel must be installed on the Core Services computer. For more information, see the *Installation Guide for NetIQ Secure Configuration Manager*.
- When you distribute a report in `.xml` format, Secure Configuration Manager does not apply filters that were applied to the viewed report. For more information, see Section 5.3.3, “Filtering a Delta Report,” on page 64.

To distribute delta report results through email:

1 Ensure that at least one run of the policy template is complete. For more information, see Section 5.3.2, “Comparing Policy Template Results,” on page 63.

2 In the left pane, click **IT Assets**.

3 In the IT Assets tree pane, expand **Managed Groups** and select the same managed group or individual endpoints that the previous run of the policy template ran against.

4 Right-click the group or endpoints, then click **Run Policy Template**.

5 Follow the instructions in the wizard, ensuring you select the same policy template.

6 In the Delta Reporting window, select **Enable Delta Reporting**.

7 Click **Setup**.

8 Follow the instructions in the Delta Comparison wizard.

9 In the Distribution window, select **Enable Distribution**.

10 Click **Add**, and select **Email distribution**.

11 In the Email Distribution window, complete the required fields.

12 (Optional) To compres the report, select **Compress this file before distributing** and then specify the file extension for the compressed file.

13 Click **OK**.

14 Click **Finish**.

15 Follow the remaining instructions in the Run Policy Template wizard.

5.3.7 Exporting a Delta Report

Once you have run a delta report, you can export the full report for detailed viewing or simply export the data from the tables for a simplified view.

Exporting a Full Delta Report

You can export the full delta comparison report, including the cover page, for detailed viewing later or to share with others.

NOTE

- To export a report in Excel format, Microsoft Excel must be installed on the Core Services computer. For more information, see the *Installation Guide for NetIQ Secure Configuration Manager*.
- When you export a report in `.xml` format, Secure Configuration Manager does not apply filters that were applied to the viewed report. For more information, see Section 5.3.3, “Filtering a Delta Report,” on page 64.

To export delta comparison report data:

1. Open the delta comparison report you want to export.
2. Right-click the report, then click **Export Full Report**.
3. Type the file name and select one of the following file formats:
   - `.pdf`
   - `.tsv` (tab-separated values)
   - `.rtf` (rich-text format)
   - `.xml`
   - `.xls` or `.xlsx` (depending on the Excel version that you use)
4. Click **Save**.

Exporting Delta Report Data

You can export the table data from the delta comparison report for a simplified view.

NOTE: When you distribute a report in `.xml` format, Secure Configuration Manager does not apply filters that were applied to the viewed report. For more information, see Section 5.3.3, “Filtering a Delta Report,” on page 64.

To export delta comparison report data:

1. Open the delta comparison report you want to export.
2. Right-click the report, then click **Export Data View**.
3. Type the file name and select one of the following file formats:
   - `.xml`
   - `.html`

- `.txt` (tab-delimited text file)
- `.xls` or `.xlsx` (depending on the Excel version that you use)

4 Click **Save**.

5.4 Using the Asset Compliance View for Evaluation

The Asset Compliance View serves as a starting point for identifying where you might have security issues and provides an overview of your IT assets in relation to policy template results. You can quickly determine which computers or managed groups are not in compliance with your company's security standards, and whether the vulnerability of those computers poses a high, medium, or low risk.

Once you select a managed group to assess, the Asset Compliance View displays the group's results on the following tabs:

Compliance

Identifies the number of systems that are in compliance, in compliance with exceptions, or out of compliance for the selected policy templates.

Risks

Identifies the number of systems with high, medium, and low risk score results for the selected policy templates.

Trending

Displays asset compliance and risk score results over time for the selected policy templates.

Systems

Provides a table of each system's risk and compliance status for the selected policy templates, plus access to detailed data per endpoint.

Summary

Categorizes system results by security check, policy template, and risk score.

The Asset Compliance View displays your assets according to their location in your user-defined managed groups. You must create managed groups and assign all relevant endpoints to those groups. Also, Secure Configuration Manager populates the graphs and tables only after you run policy templates.

If you assign endpoints of one system to separate managed groups, the Asset Compliance View displays the system's total policy template results when you select any managed group containing an endpoint from that system. This total includes results from endpoints on this system not included in the managed group. That is, the Asset Compliance View displays results for endpoints that may not be in the selected managed group because those endpoints are part of a system included in the selected managed group. For example, you placed System A's operating system endpoint into group Houston and System A's SQL Server endpoint into group Dallas. If you choose to view results for Houston, the Asset Compliance View includes the results for the SQL Server endpoint because it is part of System A.

You can choose to display results from all policy templates or particular templates and specify the time frame for trending results. The Asset Compliance View displays results only for the most recent run of the selected policy template. For example, if you run the NetIQ Audit Settings policy template four times against the same managed group, Secure Configuration Manager displays results only for the fourth template run. For more information about selecting policy templates to view, see Section 5.4.1, "Changing Asset Compliance View Settings," on page 70.

The following table shows where you can learn more about Secure Configuration Manager features related to the Asset Compliance View.

If you want to ...	See ...
Learn about policy templates	Section 4.2, “Understanding Policy Templates,” on page 49
Learn about security checks	Section 4.1, “Understanding Security Checks,” on page 47
Learn about exceptions for policy template results	Section 5.2, “Excluding Data from Report Results,” on page 58
Compare the results of individual endpoints or security checks	Section 5.3, “Comparing Report Results,” on page 63
Learn more about endpoint risk scoring in security checks	Section 6.3, “Understanding Risk Scoring,” on page 94
Create user-defined groups	Section 2.3.1, “Creating a Managed Group,” on page 28

To display or hide the Asset Compliance View, click **Compliance Overview** on the View menu. You can also dock the Asset Compliance View as a tab at the base of the console display by clicking the thumbtack icon.

5.4.1 Changing Asset Compliance View Settings

You can specify whether the Asset Compliance View includes results for particular policy templates or all policy templates. The Asset Compliance View reports results as *unknown* if you choose to view a policy template that has not been run against the selected managed group.

The Compliance, Risks, Systems, and Summary tabs display the most recent policy template results according to the data retention settings in the Core Services Configuration Utility. By default, Secure Configuration Manager retains results for 90 days. For more information about adjusting the data retention setting, see Section 5.7.2, “Configuring Data Settings,” on page 83 and the Help for the Core Services Configuration Utility. Also, the Asset Compliance View displays results for the most recent run of the selected policy template. For example, if you run the NetIQ Audit Settings policy template four times against the same managed group, Asset Compliance View displays results only from the fourth template run.

You can also specify the date range and interval (daily, weekly, or monthly) for the trending information. Secure Configuration Manager processes trending data daily at 3:00 a.m. However, the Asset Compliance View displays trend data only for a completed trend interval. That is, if you set the interval to monthly, results for the current month are not included in the trend because the current month is not complete. For more information, see Section 5.4.4, “Viewing Trending Information,” on page 73.

To change the Asset Compliance View settings:

1. On the Go menu, click **Asset Overview Pane**.
2. In the Asset Compliance View, click **Settings**.
3. Check the check box beside the policy templates whose results you want to view.
4. (Optional) To view trend data for a specific date rante, change the start and end dates.
5. (Optional) To change the trend interval, select **Daily**, **Weekly**, or **Monthly**.
6. Click **OK**.

5.4.2 Viewing Compliance Information

The Compliance tab provides a starting point for determining how well your assets comply with your company's security standards. You can also compare results on the Compliance and Risks tabs to evaluate the vulnerability of assets in your enterprise.

Understanding Compliance Status Charts

The Compliance Status chart summarizes the policy compliance of all IT assets in the selected managed group, while the Compliance Details graph displays the compliance results for the next lower level of the managed group. The next lower level can be more managed groups or individual endpoints, depending on the selected managed group. You can drill down to the endpoint level. For example, you have a managed group called Texas which includes managed groups for Houston, Dallas, and San Antonio and each of these managed groups includes many systems. If you select Texas, the Compliance Status chart summarizes the status of all systems in Texas and the Compliance Details graph displays compliance for the Houston, Dallas, and San Antonio groups. If you want to review more specific compliance results, select one of the lower level managed groups, such as Houston. The Compliance Details graph then displays details for the systems or groups within the Houston managed group. You can drill down to the endpoint level on the Compliance Details graph.

Classifying Compliance Results

Secure Configuration Manager classifies compliance results as in compliance, in compliance with exceptions, out of compliance, or unknown compliance. Secure Configuration Manager defines these classifications as follows:

- An **in compliance** score indicates the system's risk score is lower than the out-of-compliance risk score range defined for each policy template.
- An **in compliance with exceptions** score applies when an endpoint, group, or security check includes waivers to prevent conditions from causing a violation in the reported results.
- If a system is **out of compliance**, its risk score is equal to or greater than the out-of-compliance risk score range defined for each policy template. For more information about out-of-compliance settings, see Section 5.7.2, "Configuring Data Settings," on page 83.
- An **unknown compliance** score applies to systems that do not have data collected during the specified time period. Data may not be available because the policy template was not run for an endpoint, Secure Configuration Manager was unable to connect to the agent, or an endpoint returned errors.

The Compliance Status and Details charts display results per system, not endpoint. Therefore, if a system has multiple endpoints, such as an operating system and a database, and one of those endpoints fails a security check within the selected policy template, the system is labeled *out of compliance*. Similarly, if Secure Configuration Manager reports unknown results for one endpoint in a system, the Asset Compliance View labels the system's results as *unknown compliance*. To determine exactly where an endpoint falls out of compliance or has unknown results, click the Systems tab. For more information, see Section 5.4.5, "Viewing Systems Information," on page 74.

If you run a policy template for a non-applicable endpoint, the Asset Compliance View ignores results for that endpoint. For example, you created a managed group including both SQL Server and UNIX endpoints. Secure Configuration Manager ignores the UNIX endpoints when running checks against the SQL Server endpoints in that managed group. The report indicates the checks do not apply to the UNIX endpoints.

For more information about security check and policy template results, see Section 4.1, “Understanding Security Checks,” on page 47. Fore more information about evaluating asset compliance over time, see Section 5.4.4, “Viewing Trending Information,” on page 73.

To view Asset Compliance information:

1. On the Go menu, click **Asset Overview Pane**.
2. In the left pane, click **IT Assets**.
3. In the IT Assets tree pane, expand **Managed Groups > My Groups**.
4. Under My Groups, select the group for which you want to view assets. You can drill down to an endpoint to obtain details about that particular system.
5. In the Asset Compliance View, click **Settings**.
6. Select the check box beside the policy templates whose results you want to view.
7. In the Asset Compliance View, click **Compliance**.
8. (Conditional) If you have run policy templates recently, click **Refresh** to update the displayed information.
9. (Optional) To determine the number of systems in or out of compliance for the selected group and policy templates, place your cursor over the appropriate section of the Compliance Status chart.

5.4.3 Viewing Risks Information

When you run a policy template, Secure Configuration Manager evaluates each selected endpoint for each applicable security check in the template, and assigns a risk score for each endpoint. With the Asset Compliance View, you can review risk score results for multiple policy templates run against multiple endpoints. The Risks tab helps you determine how many systems in the selected asset group constitute a high risk to your security. You can also compare these results with the number of non-compliant systems to evaluate the vulnerability of assets in your enterprise. For more information about risk scores, see Section 6.3, “Understanding Risk Scoring,” on page 94.

Understanding Risk Status Charts

The Risk Status chart summarizes the risk results of all computers in the selected managed group, while the Risk Details graph displays the risk results for the next lower level of the managed group. The next lower level can be more managed groups or individual endpoints, depending on the selected managed group. For example, you have a managed group called Texas which includes managed groups for Houston, Dallas, and San Antonio, and each of these managed groups includes many systems. If you select Texas, the Risk Status chart summarizes the status of all systems in Texas and the Risk Details graph displays risk status for Houston, Dallas, and San Antonio. If you want to review more specific risk results, select one of the lower level managed groups, such as Houston. The Risk Details graph then displays details for the systems or groups within the Houston managed group.

You can drill down to the endpoint level on the Risk Details graph. If you want to view the importance assigned to an endpoint in the selected managed group, you can select that endpoint on the pane above the Asset Compliance View in the console. Then, right-click the endpoint and select **Properties**. In addition, the Systems tab enables you to determine exactly where the endpoint falls out of compliance and poses a high risk. For more information, see Section 5.4.5, “Viewing Systems Information,” on page 74.

Classifying Risk Results

The Risk Status and Details charts display results per system, not endpoint. Therefore, if a system has multiple endpoints, such as an operating system and a database, and one of those endpoints poses a high risk for the selected policy template, the system's risk is labeled `high` to ensure that the system receives appropriate attention for its potential vulnerability. For example, if a system includes a SQL Server database with a high risk and a Windows operating system with a medium risk, the system's managed risk is reported as *high*. Similarly, if Secure Configuration Manager reports unknown results for one endpoint in a system and no endpoint in the system is a high risk, the Asset Compliance View labels the system's results as *unknown*. To determine exactly where an endpoint has a high risk or unknown results, click the Systems tab.

If you run a policy template against a non-applicable endpoint, the Asset Compliance View ignores results for that endpoint. For example, you created a managed group including both SQL Server and UNIX endpoints. Secure Configuration Manager ignores the UNIX endpoints when running checks against the SQL Server endpoints in that managed group. The report indicates the checks do not apply to the UNIX endpoints.

For more information about risk scores, see Section 6.3, "Understanding Risk Scoring," on page 94. For more information about evaluating risk score results over time, see Section 5.4.4, "Viewing Trending Information," on page 73.

To view Risks information:

1. On the Go menu, click **Asset Overview Pane**.
2. In the left pane, click **IT Assets**.
3. In the IT Assets tree pane, expand **Managed Groups > My Groups**.
4. Under My Groups, select the managed group for which you want to view assets.
5. In the Asset Compliance View, click **Settings**.
6. Select the check box beside the policy templates for which you want to view results.
7. In the Asset Compliance View, click **Risks**.
8. (Conditional) If you have recently run policy templates, click **Refresh** to update the displayed information.
9. (Optional) To determine the number of systems per risk type for the selected group and policy templates, place your cursor over the appropriate section of the Risks Status chart.

5.4.4 Viewing Trending Information

Secure Configuration Manager allows you to quickly review asset compliance and risk scoring results over time. The Trending tab in the Asset Compliance View displays the change in risk scores and policy template compliance for the computers in the selected asset group. The trend interval can be daily, weekly, or monthly. For more information about adjusting the trend interval or date range, see Section 5.4.1, "Changing Asset Compliance View Settings," on page 70.

Secure Configuration Manager calculates trend data only for a completed trend interval. For example, if you set the interval to monthly, results for the current month are not included in the trend because the current month is not complete. Also, Secure Configuration Manager does not display trend data for a managed group when you create the group. Instead, you must wait for one trend interval to pass after creating the group before you can see the data in the Asset Compliance View.

To help you identify trends per risk and compliance status, the Trending tab color-codes the results.

To view Trending information:

1. On the Go menu, click **Asset Overview Pane**.
2. In the left pane, click **IT Assets**.
3. In the IT Assets tree pane, expand **Managed Groups > My Groups**.
4. Under My Groups, select the group whose assets you want to view.
5. In the Asset Compliance View, click **Settings**.
6. Update the trend interval and date range. For more information, see Section 5.4.1, “Changing Asset Compliance View Settings,” on page 70.
7. Select the check box beside the policy templates for which you want to view results.
8. In the Asset Compliance View, click **Trending**.

5.4.5 Viewing Systems Information

The Systems tab provides a table of each system’s risk and compliance status for each selected policy template. From the Systems table, you can drill down to security check results per endpoint to determine exactly how the endpoint falls out of compliance or poses a high risk. You can export the Systems table to a printer, email recipient, or file. You can also email policy template results for a specific endpoint.

Viewing the Systems Table

The Systems tab provides a sortable table of the systems, endpoints, templates, and security checks associated with the selected managed group and policy templates. The table includes the risk and compliance status per endpoint. With this view, you can identify the endpoints with high risks scores or that failed security checks. Once you identify problem systems, you can develop a plan to mitigate their misconfigurations.

To help you quickly identify whether a system complies with the selected policy templates, the Systems table uses color to indicate compliance (green), compliance with exceptions (yellow), non-compliance (red), and unknown status (gray). The table identifies each system, endpoint, and policy template by name. It also specifies the risk and compliance status for each endpoint-policy template combination. *Total risk* indicates the exposure score of the endpoint multiplied by the asset importance ranking. The *Managed risk* indicates the total risk score for an endpoint based on how well the endpoint matches expected security settings

You can organize the table by dragging a column header to the top of the table. For example, if you want to view all computers according to their compliance status, you can drag the Compliance header to the space above the table.

Also, you can export the Systems table to a printer, email recipient, or file. For more information, see Section 5.4.7, “Distributing Asset Compliance Information,” on page 77.

To view the Systems table:

1. On the Go menu, click **Asset Overview Pane**.
2. In the left pane, click **IT Assets**.
3. In the IT Assets tree pane, expand **Managed Groups > My Groups**.
4. Under My Groups, select the group whose assets you want to view.
5. In the Asset Compliance View, click **Settings**.

6 Select the check box beside the policy templates for which you want to view results.

7 In the Asset Compliance View, click **Systems**.

8 (Conditional) If you have run policy templates recently, click **Refresh** to update the displayed information.

9 (Optional) To distribute the Systems table to a printer, email recipient, or file, click **Print**. For more information, see Section 5.4.7, “Distributing Asset Compliance Information,” on page 77.

Viewing Detailed Data for an Endpoint

From the Systems table, you can select a specific endpoint to evaluate results for all security checks in the selected policy template. The detailed data identifies the endpoint and policy template and provides a list of security checks included in the policy template. You can select a security check in the left pane to display such details as the expected and actual values, the managed and total risk scores, and the threat factor.

To view endpoint details:

1 On the Go menu, click **Asset Overview Pane**.

2 In the left pane, click **IT Assets**.

3 In the IT Assets tree pane, expand **Managed Groups > My Groups**.

4 Under My Groups, select the group whose assets you want to view.

5 In the Asset Compliance View, click **Settings**.

6 Select the check box beside the policy templates for which you want to view results.

7 In the Asset Compliance View, click **Systems**.

8 (Conditional) If you have run policy templates recently, click **Refresh** to update the displayed information.

9 Double-click the endpoint for which you want to view details.

Sending an Endpoint Compliance Email

To quickly act upon misconfigurations found in the Asset Compliance View, you can send an email about an endpoint’s compliance status. The email text contains the endpoint name, policy template name, and the endpoint’s compliance status for the selected template.

NOTE: To send asset compliance information to an email recipient, ensure that you have specified a mail server for Secure Configuration Manager to use to send email. You can specify a mail server using the Core Services Configuration Utility.

To send an endpoint compliance email:

1 On the Go menu, click **Asset Overview Pane**.

2 In the left pane, click **IT Assets**.

3 In the IT Assets tree pane, expand **Managed Groups > My Groups**.

4 Under My Groups, select the group whose assets you want to view.

5 In the Asset Compliance View, click **Settings**.

6 Select the check box beside the policy templates for which you want to view results.

7 In the Asset Compliance View, click **Systems**.

8 Right-click the endpoint whose policy template status you want to send to an email recipient, and then click **Email**.

9 Enter the recipient's email address, and then click **Send**.

5.4.6 Viewing Summary Information

The Asset Compliance View includes a numerical assessment for groups of systems so you can determine how many systems meet your secure configuration policies. The Summary tab enables you to determine the quantity of systems in the selected managed group that:

- Passed or failed the security checks in the selected policy templates
- Pose a high security risk
- Do or do not comply with the selected policy templates

To help you quickly identify a system's status for the selected policy templates, the summary table rows are color-coded. The table below shows the colors associated with the status of security checks, policy template compliance, and risk scores.

Row Color	Indicates
Green	Passed, in compliance, or low risk
Yellow	Passed with exceptions, in compliance with exceptions, or medium risk
Red	Failed, out of compliance, or high risk
Gray	Unknown status

The Summary table displays cumulative values for the selected policy templates. Secure Configuration Manager calculates the *Policy Compliance* values by counting the total number of systems per compliance status for all selected policy templates. For example, you ran a policy template on 100 systems. Of those systems, 12 are in compliance, 40 are out of compliance, 28 are in compliance with exceptions, and 20 are unknown. Similarly, *Security Risks* values equal the total number of systems per risk status for all the selected policy templates. Secure Configuration Manager calculates the *Failed Checks* value as expressed in the following equation:

```
Failed Checks = Number of systems * Number of checks
```

For example, you ran a policy template on 100 systems and 20 of those systems failed two checks each for a total of 40 failed checks. The Failed Systems and Check Count is 100 * 40 = 4,000. Secure Configuration Manager applies the equation for each type of check result: passed, passed with exceptions, failed, and unknown.

All endpoints, such as an operating system and a database, on one computer qualify as one system and are scored as one unit. If the database endpoint fails a security check while the operating system endpoint passes the same check, the system is counted as failed or out of compliance. Similarly, if one of the endpoints scores a high risk value, the system is considered a high risk. For more information about compliance results in the Asset Compliance View, see Section 5.4.2, "Viewing Compliance Information," on page 71. For more information about risk results in the Asset Compliance View, see Section 5.4.3, "Viewing Risks Information," on page 72.

You can export the Summary table to a printer, email recipient, or file. For more information about printing, emailing, or exporting the Summary data, see Section 5.4.7, “Distributing Asset Compliance Information,” on page 77.

To view summary information:

1. Enable the Asset Compliance View tab.
2. In the left pane, click **IT Assets**.
3. In the IT Assets tree pane, expand **Managed Groups > My Groups**.
4. Under My Groups, select the group for which you want to view.
5. In the Asset Compliance View, click **Settings**.
6. Select the box beside the policy templates for which you want to view results.
7. In the Asset Compliance View, click **Summary**.
8. (Conditional) If you have run policy templates recently, click **Refresh** to update the displayed information.
9. (Optional) To distribute the Summary table to a printer, email recipient, or file, click **Print**. For more information, see Section 5.4.7, “Distributing Asset Compliance Information,” on page 77.

5.4.7 Distributing Asset Compliance Information

Secure Configuration Manager allows you to export the Systems and Summary tables to a printer, email recipient, or file that you can then distribute to your organization.

NOTE

- To distribute asset compliance information, you must install the Secure Configuration Manager console on the same drive where you installed Core Services.
- To distribute asset compliance information in Excel format, Microsoft Excel must be installed on the Core Services computer. For more information, see the *Installation Guide for NetIQ Secure Configuration Manager*.
- To send asset compliance information to an email recipient, ensure that you have specified a mail server for Secure Configuration Manager to use to send email. You can specify a mail server using the Core Services Configuration Utility.

To distribute Asset Compliance information:

1. Enable the Asset Compliance View tab.
2. In the left pane, click **IT Assets**.
3. In the IT Assets tree pane, expand **Managed Groups > My Groups**.
4. Under My Groups, select the managed group for which you want to distribute information.
5. In the Asset Compliance View, click **Settings**.
6. Select the box beside the policy templates for which you want to view results.
7. In the Asset Compliance View, click **Summary** or **Systems**, depending on which table you want to distribute.
8. (Conditional) If you have run policy templates recently, click **Refresh** to update the Asset Compliance View information.
9. Click **Print** to display a preview of the data.

10 (Optional) To export the data to a file, complete the following steps:

10a On the Preview File menu, click the arrow beside **Export Document**, and then select the appropriate file format. For example, select **PDF File**.

10b Complete the export options associated with your chosen file format, and then click **OK**.

10c Choose a file name, and then click **Save**.

10d Specify whether you want to open the file.

11 (Optional) To send the data to an email recipient, complete the following steps:

11a On the Preview File menu, click the arrow beside **Send via E-Mail**, and then select the appropriate file format. For example, select **RTF File**.

11b Complete the export options associated with your chosen file format, and then click **OK**.

11c Choose a file name, and then click **Save**.

11d Follow the steps in the email wizard.

12 (Optional) To print the data, click **Print** on the Preview File menu.

5.5 Using the Security and Compliance Dashboard for Evaluation

The Security and Compliance Dashboard provides a Web-based method for executives and managers to view both the overall compliance of their IT assets and to perform a more granular assessment of specific groups and computers. This high-level overview of your environment's compliance allows you to see the overall posture and trends of security compliance at a single glance.

You can create tabs based on your Secure Configuration Manager console user account permissions to filter Secure Configuration Manager compliance information and provide the status of various levels of management in your organization. You can launch the Security and Compliance Dashboard from any computer with connectivity to the Internet. For more information, see the *NetIQ Security and Compliance Dashboard Installation and Configuration Guide*.

5.6 Using the Security Checkup Results Viewer for Evaluation

The Security Checkup Results Viewer allows you to view results generated from policy template runs. For more information about reports and policy templates, see Chapter 4, "Auditing Your IT Assets," on page 47. Based on your Secure Configuration Manager console user account permissions, you can remotely audit your enterprise security by reviewing which assets are in compliance, out of compliance, or have an unknown compliance for each policy template. In addition, you can review details from the Data View tab of the Report Viewer.

5.6.1 Implementing SSL and Digital Certificates

To ease implementation of Secure Sockets Layer protocol (SSL) on the Web server, the setup program installs a demo security certificate. While the demo certificate provided allows for the configuration of your server, consider upgrading to a certificate provided by a certificate authority or creating a self-signed certificate. For example, both VeriSign and Thawte can provide valid, secure certificates and are considered certificate authorities.

Secure Configuration Manager provides the same demo certificate in every installation kit. Because the certificate is not unique, other people may share the same key and possibly eavesdrop on your encrypted traffic. If you do not want to immediately purchase a security certificate, create a self-signed certificate to eliminate the certificate uniqueness issue.

Whether you plan to install a purchased security certificate or want to permanently implement a self-signed certificate within your environment, you need to create an RSA key pair and a self-signed certificate. Secure Configuration Manager provides the required tools to complete these tasks.

Creating a Self-Signed Security Certificate

The following procedure guides you through implementing a self-signed security certificate:

- Creating a 1024-bit key pair
- Creating a self-signed security certificate
- Installing a self-signed security certificate

Secure Configuration Manager provides all the tools you need to quickly create both a 1024-bit key pair and your self-signed security certificate, and then install this certificate. After completing this procedure, you will have a unique and secure HTTPS site. You can then decide whether to purchase a certificate from a certificate authority or continue to use your own, self-signed certificate.

To create and install a server certificate key pair and self-signed certificate:

1. Log on to the Core Services computer with an administrator account.
2. Use Windows Explorer to open the `etc` folder. By default, you can locate the `etc` folder in:

   `\Program Files\NetIQ\Secure Configuration Manager\Core Services\web\`
3. Delete the `keystore.dat` file.
4. Use Windows Explorer to open the `bin` folder. By default, you can locate the `bin` folder in:

   `Program Files\NetIQ\Secure Configuration Manager\Core Services\`
5. Double-click `sslkey.bat`.
6. Enter all requested information in lower case and refrain from using commas.
7. Copy the self-signed certificate you created to the `etc` folder. By default, you can locate the `etc` folder in:

   `\Program Files\NetIQ\Secure Configuration Manager\Core Services\web\`
8. On the Core Services computer, start the Core Services Configuration Utility in the NetIQ Secure Configuration Manager program folder.
9. On the Web Services tab, update the key store and key passwords.
10. Stop and restart the NetIQ Core Services service.

Installing a Purchased Security Certificate

Secure Configuration Manager can also implement a security certificate provided by a certificate authority. To install a purchased security certificate, complete the steps in the following sections.

NOTE: If you want to use VeriSign as your certificate authority, ensure that you request a Secure Site certificate for ApacheSSL. The Secure Site Pro certificate for ApacheSSL is not compatible with Secure Configuration Manager.

Creating a Certificate Signing Request

Secure Configuration Manager provides tools to create a certificate signing request that you submit to your certificate authority.

To create a certificate signing request:

1. Ensure that you have created and installed a self-signed security certificate. For more information, see "Creating a Self-Signed Security Certificate" on page 79.
2. Log on to the Core Services computer with an administrator account.
3. Click **Start > Run**, and then enter `cmd`.
4. Use the `cd` command to navigate to the `bin` folder. By default, you can locate the `bin` folder in:

   ```
   Program Files\NetIQ\Secure Configuration Manager\Core Services\
   ```

5. Enter `sslkey request > request.txt`.
6. When your certificate authority asks you to provide your certificate signing request, open the `request.txt` file and copy the information into the appropriate form. You can often send the entire file to your certificate authority.

Installing a Purchased Certificate

Secure Configuration Manager also provides the tools to import the certificate you receive from your certificate authority. Ensure that you have read and understand the information provided by your certificate authority before installing your certificate.

NOTE: You can download an intermediate CA certificate from VeriSign (http://www.verisign.com/support/install/index.html).

To install the certificate provided by your certificate authority:

1. Log on to the Core Services computer with an administrator account.
2. Save a copy of your security certificate to the `bin` folder. ***If you received an intermediate CA certificate***, save a copy of the intermediate CA certificate to the `bin` folder. By default, you can locate the `bin` folder in:

   ```
   Program Files\NetIQ\Secure Configuration Manager\Core Services\
   ```

3. Click **Start > Run**, and then enter `cmd`.
4. (Conditional) If you have purchased a VeriSign security certificate and received both an intermediate CA certificate and your purchased certificate, complete the following procedure:

   4a Use the `cd` command to navigate to the Secure Configuration Manager Core Services folder. By default, the Core Services folder is:

   ```
   Program Files\NetIQ\Secure Configuration Manager\Core Services\
   ```

4b Enter the following command:

```
Jre\bin\keytool -import -trustcacerts -file
bin\IntermediateCACertificate.cer -keystore server\conf\keystore.dat -
storepass secure
```

where *IntermediateCACertificate.cer* is the name of the intermediate CA certificate.

4c When prompted whether to trust this certificate, enter `y`.

5 (Conditional) If you are unsure whether your certificate is encoded using the X.509 format or you receive an `unsupported encoding` error when attempting to install your certificate, complete the following procedure:

5a Use Windows Explorer to open the `bin` folder. By default, you can locate the `bin` folder in:

```
Program Files\NetIQ\Secure Configuration Manager\Core Services\
```

5b Double-click the certificate you saved in Step 2 on page 80.

5c On the Certificate window, select the General tab, and then click **Install Certificate**.

5d Complete the Certificate Import wizard. On the Certificate Store window, ensure that you click **Place all certificates in the following store**, and then use **Browse** to select the Other People certificate store.

5e Start Internet Explorer.

5f Click **Tools > Internet Options**.

5g On the Internet Options window, select the Content tab, and then click **Certificates**.

5h On the Certificates window, select the Other People tab and then select the certificate you installed in Step 5b on page 81.

5i Complete the Certificate Export wizard. On the Export File Format window, ensure that you check **DER encoded binary X.509 (.CER)**.

6 At the command prompt, use the `cd` command to navigate to the `bin` folder. By default, you can locate the `bin` folder in:

```
Program Files\NetIQ\Secure Configuration Manager\Core Services\
```

7 Enter `sslkey import < NameOfCertificateFile.cer`.

Viewing Your Installed Security Certificate

You can use the sslkey tool provided with Secure Configuration Manager to view your security certificate.

To view your security certificate:

1 Log on to the Web server with an administrator account.

2 Click **Start > Run**, and then enter `cmd`.

3 At the command prompt, use the `cd` command to navigate to the `bin` folder. By default, you can locate the `bin` folder in:

```
Program Files\NetIQ\Secure Configuration Manager\Core Services\
```

4 Enter `sslkey list`.

5 Review the information displayed and ensure that it is correct.

5.6.2 Logging in to the Security Checkup Results Viewer

You can launch the Security Checkup Results Viewer from the Secure Configuration Manager console task pane, or from any computer running Internet Explorer. The **task pane** provides access to common tasks you might want to perform in the Secure Configuration Manager console. For quick and easy access, add the Security Checkup Results Viewer URL to the Favorites list of your browser. To access the Security Checkup Results Viewer, your console user account needs the Access Security Checkup Results Viewer permission. For more information, see Section 3.6, “Managing Permissions,” on page 42.

To log in to the Security Checkup Results Viewer remotely:

1. Start Internet Explorer.
2. Specify the following URL, where *hostcomputer* is the name of the Core Services computer:

   `https://`*hostcomputer*`:8044`

   The URL specified uses the default port number. You can configure the Security Checkup Results Viewer to use a different port. For more information, see Section 5.7.1, “Configuring Web Services,” on page 83.
3. Specify the name and password of your console user account.
4. Click **Log In**.

5.6.3 Filtering the Security Checkup Results Viewer

Secure Configuration Manager console administrators can filter the Security Checkup Results Viewer to display results from only specified policy templates.

To filter results:

1. From the Security Checkup Results Summary page, click **Filtering**.
2. In the **Available** list, select the policy templates for which you want to see results.
3. Click the right arrow to move the templates to the **Selected** list.
4. Select **Show only Templates Listed under Selected**.
5. Click **Save and Close**.

5.7 Configuring Evaluation Settings

This section provides step-by-step instructions that you can follow to configure Secure Configuration Manager when you want to work with the evaluation tools.

5.7.1 Configuring Web Services

You can configure Secure Configuration Manager to use a particular port and protocol to communicate with client computers, such as those used for the Security and Compliance Dashboard and the Security Checkup Results Viewer. By specifying a port number, you can meet your unique environment needs. For example, your security policy may dictate that Web applications use specific ports or you may need to accommodate a network firewall.

Web services must be enabled for the Asset Compliance View and the Security and Compliance Dashboard to function. Similarly, you must enable the Web Site feature for the Security Checkup Results Viewer to display results and for Out of Compliance email alerts to link to the Security Checkup Results Viewer.

To configure the Web services:

1. On the Core Services computer, start the Core Services Configuration Utility in the NetIQ Secure Configuration Manager program folder.
2. Click the **Web Services** tab.
3. (Optional) To enable users to access the Asset Compliance View or Security and Compliance Dashboard, change **Enable Web Services** to **true**.
4. (Optional) To enable users to access the Security Checkup Results Viewer, change **Enable Web Site** to **true**.
5. Click **OK** to save the changes and close the Configuration Utility.

5.7.2 Configuring Data Settings

Secure Configuration Manager has a pool of available reporting content that consists of all recently run reports. Using the Core Services Configuration Utility, you can specify how many days of report data are available for use with the Asset Compliance View, the Security and Compliance Dashboard, and the Security Checkup Results Viewer.

You can also configure Secure Configuration Manager to send alerts when endpoints fall below compliance levels based on risk scores. By changing the acceptable risk score range, you can decide the level of vulnerability that results in an email alert according to your company policy. For more information about risk scores, see Section 6.3, “Understanding Risk Scoring,” on page 94. For more information about email alerts, see Section 5.8, “Automating Compliance Notification,” on page 84.

To configure data settings:

1. On the Core Services computer, start the Core Services Configuration Utility in the NetIQ Secure Configuration Manager program folder.
2. Click the **Out of Compliance Alerts** tab.
3. In the **Out of Compliance When Endpoint Scores** field, select the risk score range that determines whether endpoints are out of compliance.
4. In the **Collect Data for N Days** field, specify the number of days for which you want to view report results.

   For example, if you specify `30` in the **Collect Data for N Days** field, Secure Configuration Manager displays results for policy templates run during the past 30 days. If a policy template is not run during this time period, Secure Configuration Manager reports the policy compliance as *unknown*.
5. Click **OK** to save the changes and close the Core Services Configuration Utility.

5.8 Automating Compliance Notification

Secure Configuration Manager can help you automate much of the policy compliance effort through scheduled policy templates and automatic out-of-compliance notifications. To help your remediation efforts when endpoints fall out of compliance, Secure Configuration Manager can send emails to users, distribution lists, and change management systems.

NOTE: A console user can override the settings for compliance notifications in the Core Services Configuration Utility by selecting or deselecting the **Enable e-mail compliance alerts** option in the Run Policy Template and Run Security Check wizards.

5.8.1 Sending Email Notifications to Users

If your organization includes systems that contain highly sensitive information or that must be continuously operational, you might want to be notified when report results indicate that an endpoint poses a security or operational risk. You can configure Secure Configuration Manager to send email notifications to individuals and distribution lists when endpoints become out of compliance with policy templates. By default, Secure Configuration Manager sends out-of-compliance notifications to the email address in the endpoint properties **Contact Email** field. For more information about adding an email address to an endpoint, see Section 2.5, “Working with Endpoints,” on page 32.

NOTE: Out of Compliance email alerts include a link to the specified endpoint’s results in the Security Checkup Results Viewer. For more information, see Section 5.6, “Using the Security Checkup Results Viewer for Evaluation,” on page 78.

To send email notifications to users:

1. On the Core Services computer, start the Core Services Configuration Utility in the NetIQ Secure Configuration Manager program folder.
2. On the Out of Compliance Alerts tab, set the **Enable Email Alerts** field to `True`.
3. Specify the appropriate value for each field.
4. Click **OK** to save the changes and close the Configuration Utility.
5. For best performance, restart both the NetIQ Core Services service and the console.

5.8.2 Sending Email Notifications to Change Management Systems

Every organization has complex workflows and change management processes that require adherence. Sending out-of-compliance alerts to a change management ticketing system uses your company-defined workflow to quickly address assets that fall out of compliance with policy templates.

NOTE: Out of Compliance email alerts include a link to the specified endpoint’s results in the Security Checkup Results Viewer. For more information, see Section 5.6, “Using the Security Checkup Results Viewer for Evaluation,” on page 78.

To send an email notification to a change management system:

1. On the Core Services computer, start the Core Services Configuration Utility in the NetIQ Secure Configuration Manager program folder.

2 On the Out of Compliance Alerts tab, set the **Enable Email Alerts** field to `True`.

3 In the **Email Change Management System** field, specify the email address of the third-party change management system you want to notify when endpoints are out of compliance.

4 Click **OK** to save the changes and close the Configuration Utility.

5 For best performance, restart both the NetIQ Core Services service and the console.

6 Customizing Security Checks and Policy Templates

Secure Configuration Manager effectively manages your heterogeneous enterprise by using agents to mine data from your IT assets: operating systems, databases, application servers, and web servers. Secure Configuration Manager provides a number of security checks and policy templates that use mined data to determine vulnerabilities on those assets. You can also create custom checks and templates to address unique, site-specific policies and regulations and to respond to complex vulnerabilities for which the pre-defined security checks are unsuitable.

6.1 Namespaces, Objects, and Attributes

Secure Configuration Manager provides security management functions from a central location, with distributed agents collecting data from endpoints. Agents store collected endpoint data in a data structure called the **namespace**, which represents a collection of unique related objects and their attributes. An **object** is the logical representation of security data collected by agents and stored in the namespace. **Attributes** describe the qualities of each object. For example, Secure Configuration Manager has separate namespaces for Microsoft SQL Server and UNIX because these providers support different objects and attributes.

Objects typically have several attributes, stored as a name-value pair such as `computer_name:comp5`. For example, the Windows agent can gather data from its host computer about the Windows_Workstation object, with the attributes Computer Name, IP Address, Operating System (OS), and Currently Logged On Users. Similarly, a UNIX agent has an object called Unix_Host with attributes IP Address, Operating System, and OS Version.

Each agent has a uniquely defined set of objects and attributes. Built-in security checks automatically access this data. You can use the namespace by creating custom security checks. In the custom check, you identify the object you want to query, and then specify the values you expect to find for the attributes associated with the object.

Some object types can have many different instances in a given namespace. For example, while there is one Unix_Host object per UNIX endpoint, there are many instances of the Unix_File object. Security checks allow you to filter out unimportant instances of many of these objects, so you can highlight the instances most likely to be sources of vulnerabilities. For example, a security check can evaluate the Windows_RegistryKey objects, filtering out everything but specific registry keys entered by known viruses. For more information, see Section 6.5, “Custom Check Examples,” on page 101.

6.2 Understanding Security Check Components

A security check is a query against the Secure Configuration Manager database represented by the namespace. You can query for a list of users, a list of registry keys, or any object defined in the namespace. You can select the attributes of the object you want returned in the list. You can also filter the list by selecting values of interest for any or all of the attributes available.

The query returns a list of all objects and their attributes that meet the filter criteria. You can view the information as a full report. If you do not want the details, you can request a simple count, or weighted score, of the number of items that fit the criteria. If each item represents a point of vulnerability, then

the resulting score is a measure of the endpoint's total vulnerability for that security issue. For more information about risk scoring, see Section 6.3, "Understanding Risk Scoring," on page 94.

For example, you can create a custom security check that allows you to query for a list of users, but limit that list to users without passwords. You can report these users as a number, or score, identifying the magnitude of the threat. You can also return the users in a list. You can then issue warnings or lock accounts to remedy the vulnerability.

6.2.1 Security Check Categories

For convenience and efficient identification, Secure Configuration Manager organizes security checks by platform and **category**. The category specifies the type of security check. Secure Configuration Manager automatically includes the following categories:

- Audit/Auth Analysis
- Data/Databases
- Files/Directories
- GPO
- Internet/Network
- Software/Apps
- System
- User/Groups

When you edit or create a custom security check, you can specify one of the available categories, create a new category, or leave the check uncategorized.

6.2.2 Security Check Filters

When editing or creating custom security checks, you can add a filter to the check to reduce the amount of data returned in a query. A **filter** is a logical expression built using specified values of an attribute of an object. These attributes do not have to be the same attributes that you have selected to return as columns. Each instance of the object that satisfies the criteria set by the filters becomes a row returned from the query.

When creating a single filter, specify the following items:

- Attribute
- Operator
- Type
- Criterion

When you create a set of filters, also specify the following logic of how the filters combine:

- AND/OR
- Left and right parentheses

  NOTE: Parentheses can be nested. There is a limit of ten nested parentheses.

- NOT

Filter Attributes

When used in a filter, attributes are the characteristics of an object that determine whether rows of data are included in the returned data set. For example, a query on the Unix_Process object returns a list of all running processes. If you are concerned only with those processes owned by certain users, you can use the Owner Name attribute to limit the returned data.

Filter Operators

An operator is the comparator between the attribute and the value of the criterion. Certain operators are available only to specific data types. The Security Check wizard provides the following operators.

Operator	Function
equals	Select all objects for which the value of an attribute is equal to the criterion.
not equal to	Select all objects for which the value of an attribute is not equal to the criterion.
less than	Select all objects for which the value of an attribute is less than the criterion.
less than or equal to	Select all objects for which the value of an attribute is less than or equal to the criterion.
greater than	Select all objects for which the value of an attribute is greater than the criterion.
greater than or equal to	Select all objects for which the value of an attribute is greater than or equal to the criterion.
contains	Select all objects for which an attribute contains the criterion. Using this operator to compare strings, the comparison is true if the criterion is a substring of the attribute. For example, `File/Dir Name contains .ini` would return all initialization files.
not contains	Select all objects for which an attribute does not contain the criterion.
is any one of	Select all objects for which an attribute matches any one of the criteria.
is not any one of	Select all objects for which an attribute does not match any one of the criteria.
is included in saved list	Select all objects for which an attribute is included in the saved list specified by the criterion. For more information about saved lists, see Section 4.3.3, “Excluding Values from a Run,” on page 51.
is not included in saved list	Select all objects for which an attribute is not included in the saved list specified by the criterion. For more information about saved lists, see Section 4.3.3, “Excluding Values from a Run,” on page 51.
matches regular expression	Select all objects for which an attribute matches the regular expression described by the criterion. For more information about regular expressions, see “Regular Expressions in the Filter” on page 90.
does not match regular expression	Select all objects for which an attribute does not match the regular expression described by the criterion. For more information about regular expressions, see “Regular Expressions in the Filter” on page 90.

Filter Type

The filter type category refers to the choice between using a value or a user parameter for the criterion. When you set a criterion as a value in a security check, you cannot modify it without altering the security check itself. When you set a criterion as a user parameter, you can modify the value each time you run the policy template that contains the security check. For more information about policy templates, see Section 4.2, “Understanding Policy Templates,” on page 49.

Filter Criteria

The query compares the value of the attribute to the criterion listed for the filtered attribute. The criterion must be of the appropriate input type and in the appropriate format for the attribute in question for the comparison to be valid. For example, if you select Owner Name as the attribute, the matching criterion must be in the format of a user name: `root`, `johnd`, or `projmgr`.

Regular Expressions in the Filter

Regular expressions are a criteria type that allow you to perform advanced text pattern matching against string data types. Regular expressions provide more flexibility than simple wildcard characters. To match an exact regular expression symbol, precede the symbol with a backslash (\).

Regular Expression Symbol	Description
.	Matches any single character.
[ ]	Matches any single character from within the bracketed list. Within square brackets, most characters are interpreted literally.
[^]	Specifies a set of characters not to be matched.
^	Matches the beginning of a line.
$	Matches the end of a line.
|	Matches either the regular expression preceding it or the regular expression following it.
( )	Groups one or more regular expressions to establish a logical regular expression consisting of sub-regular expressions. Used to override the standard precedence of specific operators.
!	Specifies that the following regular expression is not matched.
?	Specifies that the preceding regular expression is matched 0 or 1 time.
*	Specifies that the preceding regular expression is matched 0 or more times.
+	Specifies that the preceding regular expression is matched 1 or more times.
{*n*}	Specifies that the preceding regular expression is matched exactly *n* number of times.
{*n*,}	Specifies that the preceding regular expression is matched *n* or more times.
{,*n*}	Specifies that the preceding regular expression is matched *n* or fewer times.
{*n*,*m*}	Specifies that the preceding regular expression is matched a maximum of *m* times and a minimum of *n* times.

Regular Expression Symbol	Description
\n	Matches a new line.
\t	Matches a tab character.

The following table provides examples of regular expressions and their matches.

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

Combining Filter Sets

You can logically combine individual filters in two ways. You can combine consecutive filters with the logical tags of AND or OR, and you can combine groups of consecutive filters with parentheses to separate groups of filters from each other.

For example, if A, B, C and D are your filters, the following examples illustrate various logical combinations:

- A **AND** B **AND** C **AND** D
- (A **AND** B) **OR** (C **AND** D)
- (A **OR** B) **AND** (C **OR** D)
- (A **OR** B **OR** C) **AND** D

Another example is the following filter requirement: “Check for all remote users without administrative accounts who have umask values not equal to 027 or 077, or whose password strengths are greater than 0.” This filter requirement can be represented logically as:

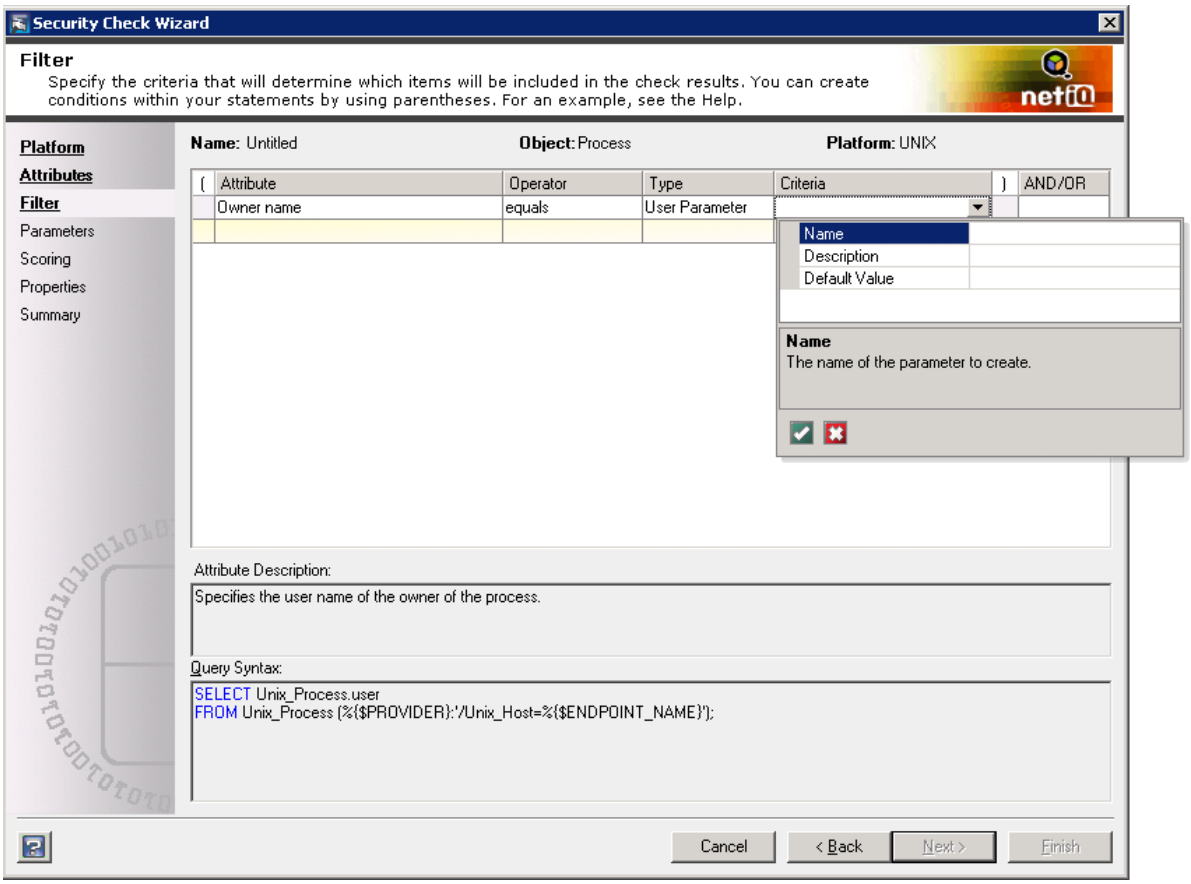
```
((Primary Group ID > 10) AND (Local or Remote Account = Remote)) AND (((umask Value
!= 027) OR (umask Value != 077)) OR (Password Strength != 0))
```

User Parameters

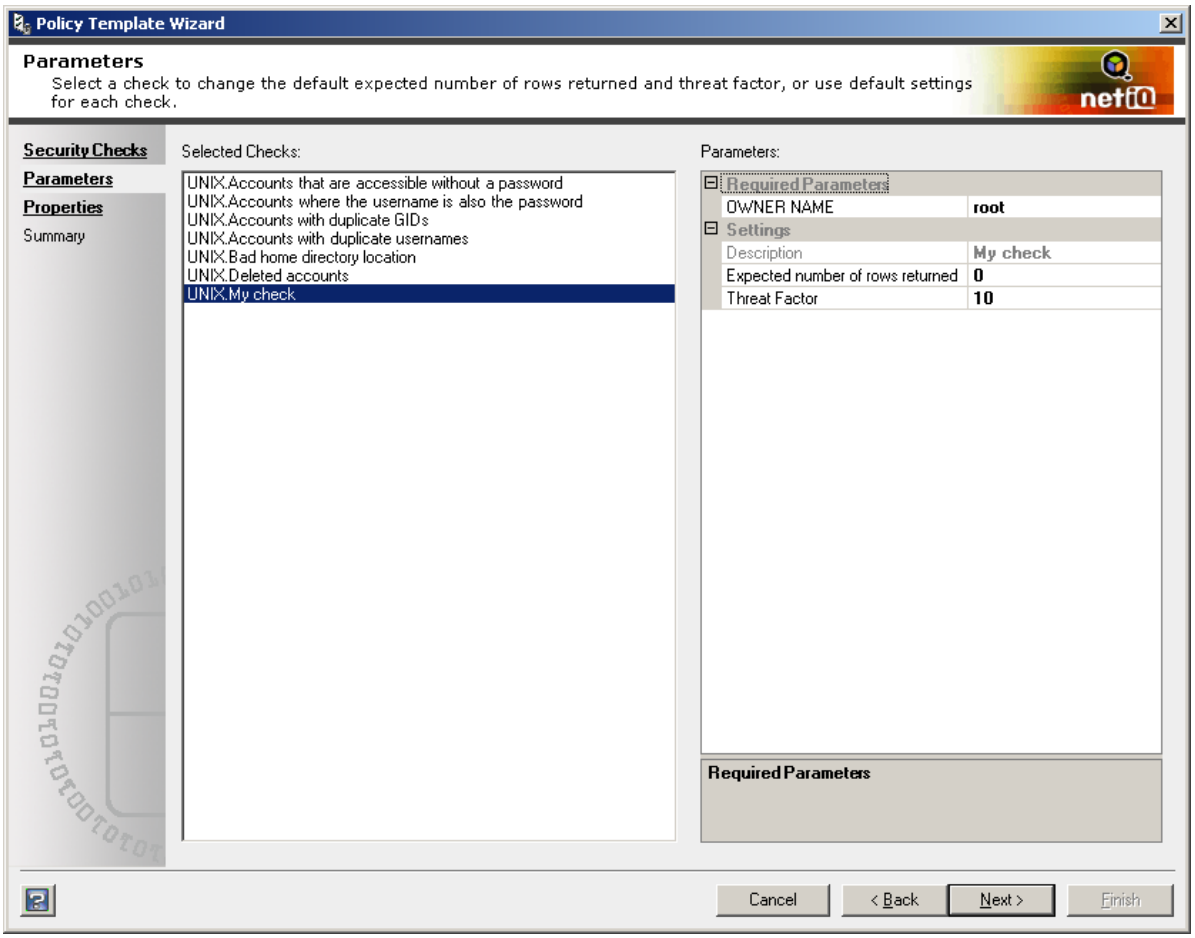
When creating a filter for a custom check, you can set a criterion as a value for every run of the security check level, or you can set the criterion as a user parameter to be selected each time you run the security check. For example, you can create a security check with the Owner Name attribute of the Unix_Process object as a filter. If you save the check with the specific value of root, when you add the security check to a policy template, the check always run with the filter criteria set as root. If you save the attribute as a user parameter, you can edit the value within the policy template and run the same check multiple times with multiple filter criteria for that attribute.

In other words, instead of creating several similar security checks for use in a custom policy template, you can create one generic security check with the attribute saved as a user parameter. Then, when you create the policy template, you include multiple instances of the generic security check where each instance specifies a different value for the user parameter.

The following figure shows the creation of a user parameter within a custom security check.



The following figure shows the security check and the user parameter as it would appear in a policy template.



Verify all entered values for data type and format. The wizard does not validate user-specified parameter values.

6.2.3 Security Check Properties

The property data of a security check is the information about the check that is visible in the Secure Configuration Manager console and at the policy template level. The data consists of the following properties:

- Check name
- Category
- Brief description
- Detailed explanation
- References
- Risks associated with this check and the environment when the violations are not remedied
- Remedies for violations of this check

When you modify or create a custom security check, ensure that you include relevant information for each check property. These properties provide other users with the information they need to decide whether this security check is appropriate.

6.3 Understanding Risk Scoring

Risk scores measure endpoint vulnerability and help you identify which endpoints have the most serious exposures based on two factors: threats discovered and endpoint importance. When you run a security check against an endpoint, Secure Configuration Manager evaluates the endpoint and includes a risk score in the report. When you run a policy template, Secure Configuration Manager assigns a risk score for each selected endpoint for each applicable security check in the template. Except for information-only security checks, Secure Configuration Manager assigns the risk score as expressed in the following equation:

Risk Score = Threat * Vulnerability

You can control how Secure Configuration Manager calculates its weighted risk scores by adjusting the following settings:

- Threat factors for each security check
- Endpoint importance
- Importance weighting factors

When you edit or create a security check, you can specify the way the score is determined so each check can satisfy a specific need.

6.3.1 Scoring Method

Every security check follows a specific method for reporting the number of violations found for each endpoint. The **scoring method** is the manner in which you want to accumulate the violations. When you create a custom check, you must assign the check to one of the following scoring methods:

Count

Counts violations for every row returned by the check that exceeds the value for the **Expected number of rows returned**. For example, the Local - Powerful Groups security check returns three rows of groups: Administrators, Domain Admins, and Enterprise Admins. The check counts three violations.

Unique Count

Counts each unique row of returned data as a violation and ignores duplicate results. The number of unique rows must exceed the value for the **Expected number of rows returned**. Secure Configuration Manager uses the first column of information in the report to determine whether a returned row contains unique data. For example, the Port Scan security check returns four rows of data, reporting the same process on different ports. The check counts four violations because each port number is unique.

Simple Value

Counts all returned violations as only one violation for a more simplified result. For example, the Accounts With Passwords More Than 90 Days Old security check returns 50 rows of data (that is, 50 accounts with old passwords). The check counts all rows as one violation. If you want no rows found to count as a violation, you can use this option, and then set the **Expected number of rows returned** value to greater than zero. Simple Value scoring applies to checks written in VQL programming language.

Single Value

Counts a single violation when the actual returned value does not match the specified **Expected value**. For example, the Advanced Audit Policy security check returns a result of *Not Compliant* when the specified policy is not set to the specified value. Single Value scoring applies to checks written in TCL programming language. TCL checks cannot be edited.

Information only

Sets the vulnerability to zero regardless of the number of violations. This option is useful when you want to create a report showing the attributes for an object.

For more information about rows returned by the check, see Section 6.3.3, “Expected Number of Rows Returned,” on page 95. For more information about applying the scoring method to a custom security check, see Section 6.4.3, “Creating Custom Security Checks,” on page 99.

6.3.2 Threat Factors

Each security check measures different attributes that can put your system at risk. Secure Configuration Manager lets you assign a **threat factor,** or penalty, for each discovered compliance or configuration risk the checks find, based on the importance of the threat in your environment. The threat factor is the relative weight, or numeric penalty, you associate with the compliance or configuration issue.

For example, you may consider the presence of a virus signature, indicating that a system has been exploited, an extremely threatening risk. Another vulnerability, such as remote access to a floppy disk, might be considered less risky. Both examples are threats, but by increasing the penalty for the presence of a virus signature you increase the resulting risk score for systems that test positive.

By default, Secure Configuration Manager assigns a threat factor of 10 to each security check. You can change the threat factor of any security check on the Parameters window in the Policy Template wizard.

6.3.3 Expected Number of Rows Returned

Each security check tests for a specific potential vulnerability in an endpoint’s configuration. For each endpoint response that varies from the expected configuration (a discovered threat or violation), Secure Configuration Manager adds a row of data to the report. The **expected number of rows returned** is the number of rows of data you allow in the report before you begin penalizing the endpoint or system for the discovered violations. The resulting **total exposure score** indicates the system’s exposure to potential vulnerabilities or threats.

The calculation for the total exposure score varies by the scoring method of the security check:

Scoring Method	Total Exposure Score Calculation
Count	Total exposure score = Threat factor * (Number of rows returned - Expected number of rows returned)
Unique Count	Total exposure score = Threat factor * (Number of rows returned - Expected number of rows returned)
Simple Value	Total exposure score = Threat factor ***if*** Number of rows returned ***does not match*** Expected number of rows returned
Single Value	Total exposure score = Threat factor ***if*** Actual value ***does not match*** Expected value
Information only	Total exposure score = 0

For example, you create a security check to determine whether all user accounts on a specific system have a password expiration date. You specify Count scoring method and a threat factor of 10 for the security check. You expect only two accounts to return without expiration dates, so you set the expected number of rows returned to a value of 2. When you run the check, Secure Configuration Manager does not count the first two returned rows when calculating the exposure score. If the report contains seven rows of returned data, the system's total exposure score is 50, as expressed in the following equation:

50 = 10 * (7 - 2)

The expected number of rows returned applies to security checks using the Count, Unique Count, and Simple Value scoring methods. For more information, see Section 6.3.1, "Scoring Method," on page 94.

6.3.4 Importance Factor

When you run a security check, Secure Configuration Manager first totals all threat factors for discovered violations on each asset. To calculate the risk score, Secure Configuration Manager multiplies the total exposure score by the **importance factor** associated with each asset importance rank, using the following equation:

Risk score = Total exposure score * Importance factor

Each asset importance rank corresponds to an importance factor that you can specify. By default, Secure Configuration Manager applies the following factors.

Asset Importance	Importance Factor
Very Low	25%
Low	50%
Medium	100%
High	125%
Very High	150%

For example, you run a security check to determine whether all user accounts have a password expiration date. An endpoint with a Very High importance factor reports five accounts without an expiration date, for a total exposure score of five. Secure Configuration Manager calculates the endpoint's risk score as 7.5 based on Total exposure score (5) * Importance factor (150%). For more information about calculating the total exposure score, see Section 6.3.3, "Expected Number of Rows Returned," on page 95.

You can change the importance factors on the **Tools > Assign Importance** menu. Factors under 100% result in lower overall risk scores. For more information about ranking the importance of an endpoint, see Section 2.5.2, "Assigning Importance to Endpoints," on page 34.

6.3.5 Example of Risk Scoring

As an example of risk scoring, suppose you create a policy template that includes only one security check, the TCP/IP Security check. When you run the policy template on two endpoints, Secure Configuration Manager determines that neither endpoint has TCP/IP Security enabled. The threat factor, or penalty, for not having TCP/IP security enabled is 10.

However, one endpoint is rated *medium* importance and the other endpoint is rated *very high* importance. The following table displays the resulting risk score for the endpoints included in this check.

Threat Factor	Importance Factor	Risk Score
10	100% (medium)	10
10	150% (very high)	15

An asset with a higher importance factor tends to result in higher overall risk scores. Highest-scoring assets appear in the report summary at the top of reports, making it easy for you to identify high-exposure assets.

6.3.6 Risk Scoring Distribution

When you run a security check or policy template, the completed report displays a pie chart showing the distribution of endpoints in each risk score range. By default, Secure Configuration Manager assigns the following risk scoring distribution levels.

Risk Level	Risk Score Range
Low Risk	0 - 100
Medium Risk	101 - 200
High Risk	201 or higher

You can change the risk scoring levels on the Properties window in the Policy Template wizard.

6.4 Working with Security Checks

Secure Configuration Manager provides hundreds of built-in security checks to ensure policy compliance. The built-in security checks and the updates provided with the AutoSync feature provide thorough vulnerability coverage. You can edit an existing security check to meet your organization's security policies. For more information about editing an existing check, see Chapter 6, "Customizing Security Checks and Policy Templates," on page 87.

You can also create your own security checks to meet your specific needs. Custom security checks are queries that you define. Secure Configuration Manager provides a wizard to guide you through the process of building custom checks. Because these custom checks are flexible, you can tailor them to meet the technical policies and regulations specific to your workplace. For more information about creating a custom check in the Security Check wizard, see Section 6.4.3, "Creating Custom Security Checks," on page 99. You can also use programming languages such as TCL to create queries outside of the wizard. For more information about advanced custom check development, contact NetIQ Professional Services.

After you create custom checks, you can export those checks as XML files. You can also export some built-in checks. You can import security checks that were previously exported from your current Core Services computer, from another Secure Configuration Manager Core Services computer, or from custom checks created outside of the console. For more information about working with existing security checks, see Section 4.1, “Understanding Security Checks,” on page 47.

6.4.1 Checklist for Editing and Creating Security Checks

Each security check is equivalent to asking a question about a particular attribute of a particular object on a particular platform. For example, does every User attribute of the Windows_Workstation object have a proper password? Are all Unix_Process objects running under the appropriate User attribute?

Use the following checklist as a guide for building the question, and then editing and creating security checks.

	Checklist Items
❑	1. Identify the platform of the agents and endpoints that you want to assess. For example, is the endpoint an Oracle database?
❑	2. Identify the objects and attributes for which you want information. For example, do all passwords have an expiration date? See Section 6.1, “Namespaces, Objects, and Attributes,” on page 87.
❑	3. Identify the values of the attributes by which you want to filter the data. For example, at what interval do we require users to change their passwords? See Section 6.2.2, “Security Check Filters,” on page 88.
❑	4. Identify the scoring method that you want to apply to the data.See Section 6.3.1, “Scoring Method,” on page 94.
❑	5. Identify the numeric penalty that you want to assign to the endpoint if the security check returns violations. For example, each violation scores 10 points. For more information about the numeric penalty, see Section 6.3.2, “Threat Factors,” on page 95.
❑	6. Identify the amount of data rhR you expect the security check to return for each endpoint. For example, you expect to see no returned data when querying the number of passwords without an expiration date. See Section 6.3.3, “Expected Number of Rows Returned,” on page 95.
❑	7. (Conditional) If you have a naming convention for your custom security checks, review the convention to create a new security check name.
❑	8. Identify the category in which you want to place your security check. See Section 6.2.1, “Security Check Categories,” on page 88.
❑	9. Write a brief description, detailed explanation, and additional information describing the check and its uses. see Section 6.2.3, “Security Check Properties,” on page 93.

6.4.2 Modifying Built-in Security Checks

Occasionally, you might want to customize a built-in security check to better suit your organizational needs. For example, you can change the way the check scores or add another column of returned data. Secure Configuration Manager enables you to edit some security checks and save the revised check under a new name. In the content pane where checks are listed, a value of **Yes** in the Edit column indicates that you can edit that check. To edit a check, your console user account needs the Edit Security Check permission. For more information, see Section 3.6, “Managing Permissions,” on page 42. When you edit a built-in security check, Secure Configuration Manager displays the same

wizard as used for creating a custom check. For more information about editing a check, see Section 6.4.3, “Creating Custom Security Checks,” on page 99.

As you update your inventory and security policies, you may need to delete the custom checks and policy templates you use to assess your environment. You cannot delete any security checks that are part of a policy template. To delete a security check, your console user account needs the Delete Security Check permission. For more information, see Section 3.6, “Managing Permissions,” on page 42.

6.4.3 Creating Custom Security Checks

To meet your organization’s specific security needs, you can create custom security checks that evaluate iSeries, Microsoft Internet Information Services (IIS), Oracle, SQL Server, UNIX, Lightweight UNIX, and Windows endpoints. For more information about supported versions of these endpoint types, see the NetIQ Support site. Secure Configuration Manager provides a wizard to guide you through the process of building your custom checks. Once you create a security check, you can save that check and include it in one or more policy templates.

In addition to the wizard provided in the Secure Configuration Manager console, you can use a programming language such as TCL to create queries outside of the console. You can then import those custom checks into the console to include them in policy templates. For more information about using programming languages to create custom checks, contact NetIQ Corporation Professional Services.

For examples of custom security checks, see Section 6.5, “Custom Check Examples,” on page 101. To create a custom check, your console user account needs the New Security Check permission. For more information, see Section 3.6, “Managing Permissions,” on page 42.

To create a custom security check:

1. In the left pane, click **Security Knowledge**.
2. In the Security Knowledge tree pane, expand **Security Checks**.
3. Right-click **My Checks**, and then click **New Security Check**.
4. On the Select Platform window, select a platform and an object.

   NOTE: For queries that require a Windows agent, NetIQ recommends that you expand the top-level objects and select objects at a lower level. If you select a top-level object, such as Windows > Workstation, the security check report includes results for all endpoints associated with the specified Windows agent, rather than limiting the results to the endpoint specified for the security check run.

5. Click **Next**.
6. On the Select Returned Attributes window, select the attributes that you want to use as the columns of data returned by the query.
7. Click **Next**.
8. (Optional) To create a single filter, specify the following items:
   - Attribute
   - Operator
   - Type
   - Criteria

   NOTE: The Filter page of the wizard does not support wildcard characters.

9 ***If you want to create multiple filters***, specify the items in Step 8 on page 99 and specify the AND/OR logic of how the filters combine. For more information about filter components and filter logic, see Section 6.2.2, “Security Check Filters,” on page 88.

NOTE: To view the format of an attribute value, run an unfiltered check. The unfiltered check returns data in the correct format, providing you an explicit example.

---

10 Click **Next**.

11 (Conditional) If your custom check includes required parameters, specify the default values, and then click **Next**.

12 Select a method in the **Scoring Method** field.

13 Enter values in the **Threat Factor** and **Expected Number of Rows Returned** fields, or accept the defaults.

14 Click **Next**.

15 Type a unique name for the custom check in the **Check Name** field. Ensure that the name is consistent with your naming convention.

NOTE: Secure Configuration Manager does not support using colon (:) and semicolon (;) characters in security check names.

---

16 Select the appropriate category in the **Category** field.

17 (Optional) To modify the available categories or add a new one, click **Edit Categories**, make changes, and then click **OK**.

18 Type a description of your custom check in the **Brief Description** field.

19 Type the remaining descriptive fields as necessary.

20 Click **Next**.

21 Review the summary of your custom check. To make changes, select the appropriate window in the tree pane.

22 (Optional) To run the custom security check at this time, select the **Run this security check now** check box.

23 Click **Finish** to save the custom check and close the wizard.

6.4.4 Working with the Generic Network Device Security Check

In addition to the device-specific security checks for Cisco and Juniper network devices endpoints, SCM provides a generic check called **Execute Command on Network Device**. You can run this check against any type of network device, and you can use check during configuration of a generic network device endpoint.

You can customize the **Execute Command on Network Device** check by specifying values for the following parameters in the **Run Security Check** window while running this check:

Classification	Parameter	Description
Parameters	Command	Specify the command that you want to execute on the generic network device.
	IsScorable	Specify whether you want to make the check scorable.
	Regular Expression	Specify the regular expression to be used on the command output.
Scoring	Comparator	Displays the comparator that is used in the security check. This parameter is displayed only when **IsScorable** is set to true.
	Expected Value	Specify the expected return value.
	Threat Factor	Specify the approximate penalty value for calculating the exposure score of the security check. This value must be greater than zero.
Description		Specify the description of the security check.

IMPORTANT: There is no restriction on the type of commands that can be executed by this check. NetIQ recommends that you exercise caution while executing commands that can modify the device content.

6.5 Custom Check Examples

This section provides custom check examples you can create using the wizard.

6.5.1 Accounts with Passwords More than 60 Days Old

Secure Configuration Manager provides the Accounts with Passwords More than 90 Days Old security check. You can edit this check to create the Accounts with Passwords More than 60 Days Old custom check.

The Accounts with Passwords More than 60 Days Old custom check has the following properties:

Description Lists accounts with passwords older than 60 days.

Explanation Users should change account passwords frequently to prevent passwords from being stolen or viewed.

Risks Once malicious users have guessed a password, they can use that password until it is changed. The longer the interval between password changes, the more damage is possible by a compromised password.

Remedies Require users to change their passwords every 60 days at a minimum.

To create the Accounts with Passwords More than 60 Days Old custom check:

1. In the left pane, click **Security Knowledge**.
2. In the Security Knowledge tree pane, expand **Security Checks > NetIQ Checks > Windows**.
3. Select **User/Groups**.
4. In the content pane, right-click **Accounts with Passwords more than 90 days old**, and then click **Edit Security Check**.
5. In the left pane, click **Attributes**.
6. Select `Password Policy` in the **Available Attributes** pane.
7. Click the right arrow to move `Password Policy` to the **Attributes to Check** field.
8. In the left pane, click **Filter**.
9. Type `5184000` in the **Criteria** list.
10. Click **Save As**.
11. Type `Accounts with passwords more than 60 days old`.
12. Click **OK**.

6.5.2 Kernel Parameters

The following example shows how to create a simple informational check for a UNIX or Linux computer.

The Kernel Parameters custom check has the following properties:

Description	Lists kernel parameters.
Explanation	Provides a list of editable kernel parameters.
Risks	This security check is for information only.
Remedies	This security check is for information only.

To create the Kernel Parameters custom check:

1. In the left pane, click **Security Knowledge**.
2. In the Security Knowledge tree pane, expand **Security Checks**.
3. Right-click **My Checks**, and then click **New Security Check**.
4. Select `UNIX` in the **Platform** field.
5. Expand `Host` in the **Object** field to show the list of child objects.
6. Select `Kernel Parameter`.
7. Click **Next**.
8. Click the right double arrow button.
9. To create an unfiltered security check, click **Next**.
10. Click **Next**.
11. In the **Scoring Method** field, select `Information Only`.
12. Click **Next**.
13. Type `Kernel Parameters` in the **Check Name** field.
14. Select `System` in the **Category** field.

15 Type a description of your custom check in the **Brief Description** field.

16 Click **Next**.

17 Review the summary of your custom check.

18 Click **Finish**.

6.5.3 Registry Keys Modified Since Date

The following example shows how to create a custom check for registry keys on a Windows computer.

The Registry Keys Modified Since Date custom check has the following properties:

Description	Checks for registry keys modified since specified date.
Explanation	Checks to identify any registry keys that have been modified since a specified date.
Risks	Unapproved modified registry keys may indicate an intruder or virus has tampered with your computer.
Remedies	Verify that all modified registry keys are from approved processes. Follow with other security checks to identify other evidence of tampering.

To create the Registry Keys Modified Since Date custom check:

1 In the left pane, click **Security Knowledge**.

2 In the Security Knowledge tree pane, expand **Security Checks**.

3 Right-click **My Checks**, and then click **New Security Check**.

4 Select `Windows` in the **Platform** field.

5 Expand `Workstation` in the **Object** field to show the list of child objects.

6 Select `Registry Key`.

7 Click **Next**.

8 Select `Key Name` and `Modification Date` and click the right arrow button.

9 Click **Next**.

10 Select `Modification Date` in the **Attribute** list.

11 Select `greater than` in the **Operator** list.

12 Select `User Parameter` in the **Type** list.

13 Click the **Criteria** field to open the User Parameter window.

14 Type `MODIFIED SINCE` in the **Name** field.

15 Type `Modified keys since this date` in the **Description** field.

16 Click the checkmark button.

17 Click **Next**.

18 Type a default date in the **Modified Since** field using the `MM/DD/YY HH:MM:SS` format.

19 In the **Registry Key Name** field, type an asterisk (`*`), and then click **Next**.

20 Select `Unique Count` in the **Scoring Method** field.

21 Click **Next**.

22 Type `Registry Keys Modified Since Date` in the **Check Name** field.

23 Select `System` in the **Category** field.

24 Type a description of your custom check in the **Brief Description** field.

25 Click **Next**.

26 Review the summary of your custom check.

27 Click **Finish**.

6.5.4 Password Policy Violations

The following example shows how to create a custom check with multiple filters.

The Password Policy Violations custom check has the following properties:

Description	Checks for simple password violations.
Explanation	Checks for users' passwords being too short, empty, or in the dictionary.
Risks	Passwords that violate simple policy regulations are easy to break and are considered system vulnerable.
Remedies	Identify users with password violations and force password changes.

To create the Password Policy Violations custom check:

1 In the left pane, click **Security Knowledge**.

2 In the Security Knowledge tree pane, expand **Security Checks**.

3 Right-click **My Checks**, and then click **New Security Check**.

4 Select `Windows` in the **Platform** field.

5 Expand `Workstation` in the **Object** field to show the list of child objects.

6 Select `Password`.

7 Click **Next**.

8 Click the right double arrow button.

9 Click **Next**.

10 Select `Password found in dictionary` in the **Attribute** list.

11 Select `equals` in the **Operator** list.

12 Select `Value` in the **Type** list.

13 Select `True` in the **Criteria** list.

14 Select `Or` in the **AND/OR** list.

15 On the next line, select `Password is blank` in the **Attribute** list.

16 Select `equals` in the **Operator** list.

17 Select `Value` in the **Type** list.

18 Select `True` in the **Criteria** list.

19 Click **Next**.

20 Click **Next**.

21 Select `Count` in the **Scoring Method** field.

22 Click **Next**.

23 Type `Password Policy Violations` in the **Check Name** field.

24 Select `User/Groups` in the **Category** field.

25 Type a description of your custom check in the **Brief Description** field.

26 Click **Next**.

27 Review the summary of your custom check.

28 Click **Finish**.

6.5.5 Suspicious User

The following example shows how to create a custom check with multiple filters combined in complex ways.

The Suspicious User custom check has the following properties:

Description	Checks for remote suspicious users.
Explanation	Checks for remote users with poor password protection.
Risks	These accounts may be compromised.
Remedies	Verify accounts belong to trusted users and ensure that password policies are enforced.

To create the Suspicious User custom check:

1 In the left pane, click **Security Knowledge**.

2 In the Security Knowledge tree pane, expand **Security Checks**.

3 Right-click **My Checks**, and then click **New Security Check**.

4 Select `UNIX` in the **Platform** field.

5 Expand `Host` in the **Object** field to show the list of child objects.

6 Select `User`.

7 Click **Next**.

8 Select `User name`, `Primary Group ID`, `umask Value`, `Last logon date and time`, and `Password strength` in the Available Attributes pane.

9 Click the right arrow button.

10 Click **Next**.

NOTE: The following filters are the logical equivalent to the following statement: “Check for all remote users without administrative accounts who have either umask values not equal to 022 or 033, or whose password strength is greater than 0.”

---

11 Select `Primary Group ID` in the **Attribute** list.

12 Select `not equal to` in the **Operator** list.

13 Select `Value` in the **Type** list.

14 Type `1` in the **Criteria** field.

15 Select `AND` in the **AND/OR** list.

16 On the next line, select `Local or Remote Account` in the **Attribute** list.

17 Select `equals` in the **Operator** list.

18 Select `Value` in the **Type** list.

19 Select `Remote` in the **Criteria** list.

20 Select `AND` in the **AND/OR** list.

21 To select the first two filters, click in the **(** or **)** column of the first filter, press and hold Shift, and click in the **(** or **)** column of the second filter.

22 To enclose the selected filters in parentheses, right click the highlighted area, and select **Add ( )**.

23 On the next line, select `umask Value` in the **Attribute** list.

24 Select `not equal to` in the **Operator** list.

25 Select `Value` in the **Type** list.

26 Type `022` in the **Criteria** field.

27 Select `AND` in the **AND/OR** list.

28 On the next line, select `umask Value` in the **Attribute** list.

29 Select `not equal to` in the **Operator** list.

30 Select `Value` in the **Type** list.

31 Type `033` in the **Criteria** field.

32 Insert parentheses to group the second and third filters.

33 Select `OR` from the **AND/OR** list.

34 On the next line, select `Password Strength` from the **Attribute** list.

35 Select `greater than` from the **Operator** list.

36 Select `Value` from the **Type** list.

37 Type `0` in the **Criteria** field.

38 To select the remaining filters, click in the **(** or **)** column of the umask Value filter, hold **Shift**, and click in the **(** or **)** column of the Password Strength filter.

39 To enclose the selected filters in parentheses, right click in the highlighted area, and then select **Add ( )**.

(	Attribute	Operator	Type	Criteria	)	AND/OR
(	Primary Group ID	not equal to	Value	1		AND
	Local or Remote Account	equals	Value	Remote	)	AND
(	umask Value	not equal to	Value	22		OR
	umask Value	not equal to	Value	33		OR
	Password Strength	greater than	Value	0	)	

40 Click **Next** three times.

41 Type `Suspicious User` in the **Check Name** field.

42 Select `User/Groups` in the **Category** field.

43 Type a description of your custom check in the **Brief Description** field.

44 Click **Next**.

45 Review the summary of your custom check.

46 Click **Finish**.

6.6 Working with Policy Templates

Secure Configuration Manager provides dozens of built-in policy templates to ensure policy compliance. The built-in templates and the updates provided with the AutoSync feature provide thorough vulnerability coverage. You can edit an existing policy template to meet your organization's security policies. For more information about editing a template, see Section 6.6.3, "Modifying Built-in

Policy Templates," on page 108.

You can also create your own policy templates tailored to meet the technical policies and regulations specific to your workplace. Custom templates can include any combination of built-in and custom security checks. Secure Configuration Manager provides a wizard to guide you through the process of building a policy template. For more information about creating a policy template in the Policy Template wizard, see Section 6.6.2, "Translating a Technical Standard to a Policy Template," on page 107. After you create custom templates, you can export those templates as `.tpl` files. You can also export a built-in template, modify it, and then import it using a new name.

NOTE: The console might require extra time to import and display a policy template that contains a large volume of security checks. For example, a policy template with more than 1,000 security checks might require more than five minutes to import.

By default, Secure Configuration Manager applies the same parameter values to a security check every time the security check runs. However, when you create or edit a policy template, you can customize the parameter values for the security checks within that policy template without affecting the security check's default values.

6.6.1 Using Security Check Instances

When creating policy templates, you can use multiple instances of a security check to verify different parameter values on the endpoint. You must specify a unique name for each instance of a security check using the **Check Alias** field in the Policy Template wizard. For example, you want to use the Service Status and Permissions Settings Minimum security check to verify whether both the Microsoft POP3 and the Messenger services are disabled. Add the security check twice to the policy template. In the first check instance, enter `Microsoft POP3` for the alias and `POP3SVC` for the service name. In the second check instance, enter `Messenger` for the alias and `MESSENGER` for the service name.

When you view the report, Secure Configuration Manager displays the check alias instead of listing the security check title. To view the check alias with its associated security check title, see the appendix on the Full Report tab.

6.6.2 Translating a Technical Standard to a Policy Template

Security policies are essential for effective security management. These policies define roles and responsibilities, and make employees aware of required security procedures. The establishment and enforcement of security policies helps reduce security incident costs and ensure consistency in standards across an organization. Most organizations map corporate security policies to technical standards that define the recommended configurations for an array of technologies.

To translate your corporate technical standards to a custom policy template, you must first identify the corporate policies and technical standards that specifically affect your IT assets. You can organize the technical standards and policies by their required configuration settings. Next, review the policy templates available in Secure Configuration Manager. Some or all security checks within a template might map to the individual settings that you want to verify. You can also review all security checks available in Secure Configuration Manager to find ones that map to the individual settings. Consider the following scenarios when determining which security checks to include in your policy template:

- ***If a built-in policy template contains some check instances that map to your technical standards***, you can modify the template to use as the base for your new policy template. Keep the security check instances that meet your needs and remove those instances that do not map to your standards. For more information about editing an existing policy template, see Section 6.6.3, "Modifying Built-in Policy Templates," on page 108.

- ***If a built-in security check allows you to enter a parameter and value pair***, you can include multiple instances of the check in your policy template. For example, you might want to use the Audit Policy check to verify settings for logon events, object access, and system events. Each setting that you want to verify would be a different check instances in the policy template. For more information about using one check multiple times in a template, see Section 6.6.1, “Using Security Check Instances,” on page 107.
- ***If a security check assesses the setting that you want to check but looks for a different value than your policy requires***, you can edit the security check. For more information about editing security checks, see Section 6.4.2, “Modifying Built-in Security Checks,” on page 98.
- ***If you cannot find a built-in security check that maps to your technical standards***, create a new check. For more information about creating security checks, see Section 6.4.3, “Creating Custom Security Checks,” on page 99.

For example, your technical standard AA123-2129-5 requires that you follow CCE-2129-5, which is a Common Configuration Enumeration guidance for restricting the number of users who can modify the audit records in the Security log on a Windows system. You can use the User Rights security check to verify that the Generate Security Audits local policy is set to Local Service or Network Service. In your policy template, you add the User Rights check, and then create the following alias: *AA123-2129-5 Generate Security Audits*. The alias links the check instance to your technical standard and the particular requirement in the standard, and also provides a quick description of the setting to be checked. For another example of mapping the check alias to the technical standard number, see the CIS Benchmark for Windows Server 2008 and 2008 R2 SSLF for Domain Controllers policy template. The template includes this same requirement under the alias *1.8.34 Generate Security Audits*. The 1.8.34 suffix for the alias maps to the CIS Benchmark requirement.

NOTE: Some parameters and their settings are case-sensitive. When you add the parameter names and values to a security check, ensure that you enter the same format and style that the queried operating system or application uses.

6.6.3 Modifying Built-in Policy Templates

You can edit user-created and selected NetIQ policy templates, then save the template under a new name. To edit a policy template, your console user account needs the Edit Policy Template permission. For more information about permissions, see Section 3.6, “Managing Permissions,” on page 42.

As you update your inventory and security policies, you might need to revise the custom checks and policy templates that you use to assess your environment. To delete a policy template, your console user account needs the Delete Policy Template permission.

WARNING: If the policy template that you want to delete is part of any scheduled jobs, those scheduled jobs will be deleted as well. For more information about scheduled policy templates, see Section 4.3.2, “Scheduling a Policy Template Run,” on page 51.

6.6.4 Creating Custom Policy Templates

To meet your organization's specific security needs, you can create custom policy templates that evaluate iSeries, Microsoft Internet Information Services (IIS), Oracle, SQL Server, UNIX, Lightweight UNIX, and Windows endpoints. For more information about supported versions of these endpoint types, see the NetIQ Support site. Secure Configuration Manager provides a wizard to guide you through the process of building your custom checks.

Once you create a policy template, you can save that template and run it against groups of heterogeneous endpoints. For more information about running a policy template, see Section 4.3, "Running Security Checks and Policy Templates," on page 50.

To create a custom template, your console user account needs the New Policy Template permission. For more information, see Section 3.6, "Managing Permissions," on page 42.

NOTE: When the account for the owner of a policy template is disabled or deleted, Secure Configuration Manager no longer runs the scheduled job. For more information about changing the owner of a scheduled policy template, see Section 6.6.3, "Modifying Built-in Policy Templates," on page 108.

To create a custom policy template:

1. In the left pane, click **Security Knowledge**.
2. In the Security Knowledge tree pane, expand **Policy Templates**.
3. Right-click **My Templates**, and then click **New Policy Template**.
4. On the Security Checks window, select the checks you want to include in the policy template.
5. (Optional) To use multiple instances of the same check, complete the following steps:
   - **5a** Highlight the security check in the Available Checks list.
   - **5b** Click the **>** button to move the check to the Selected Checks list.
   - **5c** Enter a unique name in the **Check Alias** field for the check instance.

     NOTE: When assigning the unique name, NetIQ Corporation recommends referencing the specific technical standard number or setting value.

   - **5d** Repeat this step for each instance of the security check that you want to include in the policy template.
6. Click **Next**.
7. On the Parameters window, enter the parameter specifications for each security check, and then click **Next**.
8. On the Properties window, enter a unique name and a description of the policy template, and then click **Next**.
9. Review the information on the Summary window, and then click **Finish**.

7 Working with Baselines

To help you manage and audit your assets more effectively, Secure Configuration Manager provides a mechanism for establishing baselines for your endpoints. A **baseline** is a snapshot representing the state of an endpoint using selected criteria. You establish a baseline to set an initial standard. Once you have established baselines, you can run baseline comparison checks to determine what changes have been made to your target endpoints, and then take the appropriate action according to your security policies.

7.1 Understanding Baselines

The purpose of establishing a baseline is to set a standard for future comparison and correlation. Baselines do not have to represent the ideal state of your endpoints or asset groups. They are just intended to provide an initial snapshot so you can see what has changed.

The baseline process includes defining baseline criteria sets for objects to be monitored on target endpoints, taking snapshots of those target endpoints or asset groups using the criteria, and then using those snapshots for future comparison and reporting. A **baseline criteria set** represents the criteria you define for a target endpoint that you want to use in establishing a baseline.

You can establish a single baseline or multiple baselines for each endpoint, using a single set of criteria or multiple sets of criteria. For example, you might establish a baseline for the UNIX files in a particular directory, noting file size and last modification time. When you run the baseline comparison check, you can see if any files have been added, deleted, or otherwise modified. You can also combine one or more baseline criteria sets to form a **baseline collection**. In a baseline collection, each criteria set represents a separately named baseline, but you can run a single report for multiple baselines at the same time.

NOTE: To use the baselines feature, you must install the appropriate Secure Configuration Manager agents for your target endpoints.

7.2 Understanding Baseline Permissions

You do not need to set up special permissions to enable console users to use the baseline feature in Secure Configuration Manager. The same permissions and roles you have assigned to users to work with security checks and policy templates also apply to baseline criteria, baseline collections, and baseline management checks and reports. However, you should review those permissions to ensure that they are appropriate for the users who will be performing baseline tasks. For more information about permissions, see Section 3.6, “Managing Permissions,” on page 42.

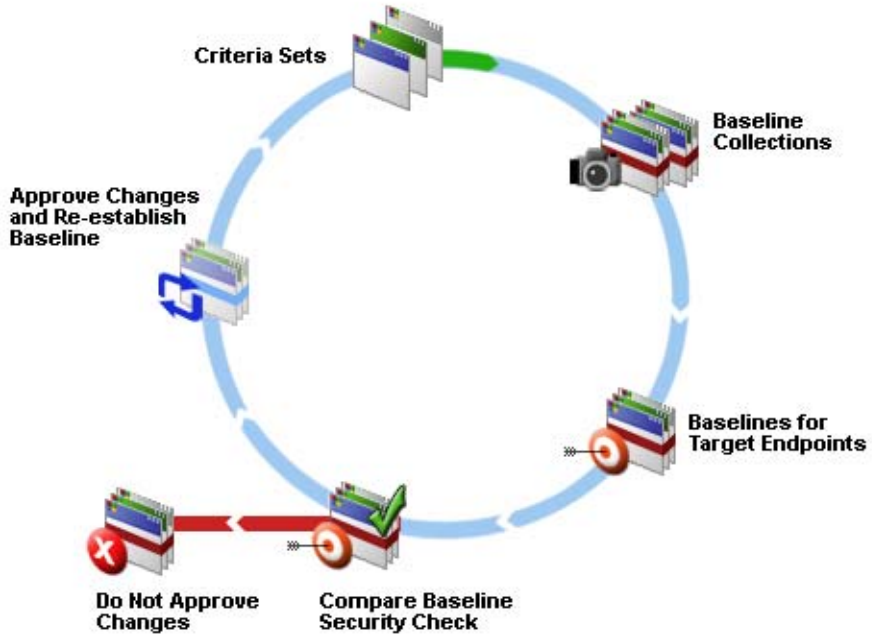
7.3 Creating and Managing Baselines

Creating and managing baselines is an ongoing process. Review the following steps for working with baselines in your Secure Configuration Manager environment:

1. Determine the criteria you are interested in monitoring on your target endpoints and use those criteria to define the necessary baseline criteria sets. You can create baseline criteria sets from scratch, or you can use existing security checks as the basis for a new baseline criteria set. For more information, see “Defining Baseline Criteria” on page 113 or “Creating Baseline Criteria Sets from Security Checks” on page 114.
2. Create one or more baseline collections. A baseline collection includes one or more baseline criteria sets. For more information, see “Creating Baseline Collections” on page 116.
3. Establish baselines for your target endpoints using the baseline criteria sets and baseline collections. For more information, see Section 7.3.3, “Establishing a Baseline,” on page 117.
4. Run the Compare Baseline security check on your target endpoints on a regular basis to report changes from the established baseline. You can set a schedule for the check by adding the check to a policy template. For more information, see Section 7.3.4, “Running a Baseline Comparison Check,” on page 118.
5. Evaluate the data from the baseline comparison report. Depending on the results of the baseline comparison, do one of the following:
   - **5a** (Conditional) If you approve the changes that have been made to your endpoints, you can update the established baseline. Re-establishing a baseline sets a new standard for future comparison. For more information, see Section 7.3.7, “Updating a Baseline,” on page 120.
   - **5b** (Conditional) If you do not approve the changes that have been made to your endpoints, you can take the appropriate action according to your security policies to address those changes. For example, you can correct vulnerabilities by creating and running tasks on specific resources using Secure Configuration Manager, or you can use native tools.
6. As you add or remove endpoints or make changes to asset groups in your environment, review your scheduled baseline checks to ensure that they are collecting data from all appropriate endpoints.

NOTE: The baseline check resides on the agent. If you establish a baseline against an asset group and then add endpoints to that group, by default the Compare Baseline check continues to run against the original group because the check is not aware of changes to the group. If you make frequent changes to your asset groups, it is a good idea to run the Compare Baseline check against individual endpoints instead of asset groups.

You should run the List Baselines check on a regular basis to review the established baselines on your endpoints and make any necessary changes to your criteria sets. For more information, see Section 7.3.8, “Creating a List of Baselines for a Target Endpoint,” on page 120.



7.3.1 Working with Baseline Criteria

Baseline criteria are the building blocks for **baseline collections**. When creating baseline criteria sets, it is a good idea to experiment and run baseline criteria sets individually to ensure that they are collecting the appropriate information. However, in your production environment, adding criteria sets to a baseline collection is a more efficient approach. When you combine criteria sets in a collection, each criteria set represents a separate named baseline, but you can run a single report for multiple baselines at the same time.

Defining Baseline Criteria

The first step in the baseline process is to define the set of criteria or attributes you want to use to establish a baseline standard for your target endpoints. You select the platform and the object (for example, files or kernel parameters) that you want to check. Then you select the attributes to be displayed in the report, as well as the attributes to be used for correlation and comparison. An **object** is the logical representation of security data collected by agents. **Attributes** describe the quality of each object. For more information about objects and attributes, see Section 6.1, “Namespaces, Objects, and Attributes,” on page 87.

To define a baseline criteria set:

1. In the left pane, click **Baselines**.
2. In the Baselines pane, right-click **Criteria**, and then click **New Baseline Criteria**.
3. Select the appropriate platform for the baseline criteria based on your target endpoints.

4 Follow the instructions in the wizard to define the baseline criteria set.

NOTE: Do not use the special characters ?>"|< in the baseline criteria set name. When you use one of these special characters, the completed baseline report displays an error rather than baseline data.

5 Repeat Step 1 on page 113 through Step 4 on page 114 as needed to create additional baseline criteria sets.

Once you have defined a single baseline criteria set, you can establish a baseline. Or, you can create additional baseline criteria sets and then combine them in a baseline collection. For more information, see “Creating Baseline Collections” on page 116 and Section 7.3.3, “Establishing a Baseline,” on page 117.

Creating Baseline Criteria Sets from Security Checks

In addition to creating baseline criteria sets from the Baselines section of the tree pane, you can create baseline criteria sets directly from security checks. This capability allows you to leverage the object types, attributes, and parameters already specified in security checks as the basis for a new baseline criteria set. Your baseline criteria set can match the security check precisely, or you can use it as a starting point, and make any necessary adjustments using the Baseline Criteria Set wizard.

You can create a baseline criteria set from any editable check, including those that are part of a policy template. However, you cannot create a baseline criteria set directly from a policy template.

NOTE

- You cannot name your baseline criteria set the same as the security check on which it is based. The name of the baseline criteria set must be unique.
- Do not use the special characters ?>"|< in the baseline criteria set name. When you use one of these special characters, the completed baseline report displays an error rather than baseline data.

To create a baseline criteria set from a security check:

1 In the left pane, click **Security Knowledge**.

2 In the Security Knowledge tree pane, expand **Security Checks > NetIQ Checks**.

3 Select the appropriate platform and node.

4 In the content pane, right-click the security check for which you want to create a baseline criteria set, then click **Create Baseline Criteria**.

5 Follow the instructions in the wizard to create the baseline criteria set.

Once you complete the wizard, you can see your new baseline criteria set in the **Baselines > Criteria** section of the tree pane.

Modifying Baseline Criteria

After you define baseline criteria sets, you can modify them any time to meet the unique auditing requirements of your company assets.

You can also revise an existing baseline to match the current characteristics of a target endpoint. For more information, see Section 7.3.7, “Updating a Baseline,” on page 120.

To modify a baseline criteria set:

1. In the left pane, click **Baselines**.
2. In the Baselines pane, select **Criteria**.
3. Select the appropriate platform and category for the criteria set.
4. In the content pane, right-click the named criteria set you want to modify and then click **Edit**.
5. Follow the instructions to edit the baseline criteria set.

Deleting Baseline Criteria

You can delete a baseline criteria set if you no longer need it, for example, if changes to your assets make a criteria set obsolete.

NOTE: If you want to delete a baseline criteria set that is part of a baseline collection, you must first edit the baseline collection to remove the unnecessary baseline criteria set. Once the baseline criteria set is no longer part of any collection, you can delete the baseline criteria set. For more information about editing the baseline collection, see “Modifying Baseline Collections” on page 116.

To delete a baseline criteria set:

1. In the left pane, click **Baselines**.
2. In the Baselines pane, select **Criteria**.
3. Select the appropriate platform and category for the criteria set.
4. In the content pane, right-click the baseline criteria set you want to delete, and then click **Delete**.
5. Click **Yes** on the confirmation message.

Exporting Baseline Criteria

After you have created baseline criteria sets, you can export them as `.bsl` files. Exporting baseline criteria sets allows you to restore this data in case it is changed incorrectly. You can also import this data to a different Core Services computer.

To export a baseline criteria set:

1. In the left pane, click **Baselines**.
2. In the Baselines pane, select **Criteria**.
3. Select the appropriate platform and category for the criteria set.
4. In the content pane, right-click the baseline criteria set you want to export, and then click **Export Baseline Criteria**.
5. Select a folder in which you want to save the exported baseline criteria set.
6. Click **Save**.

Importing Baseline Criteria

You can import baseline criteria sets that you previously exported from the current Core Services computer, or from another Core Services computer. You can use this feature, for example, to restore a baseline criteria set that was changed incorrectly. If a baseline criteria file with the same name already exists, Secure Configuration Manager gives you the option to overwrite the existing file.

To import a baseline criteria set:

1. In the left pane, click **Baselines**.
2. In the Baselines pane, right-click **Criteria**, and then click **Import Baseline Criteria**.
3. Select the baseline criteria (`.bsl`) files you want to import and click **Open**.

7.3.2 Working with Baseline Collections

Once you have defined one or more baseline criteria sets, you can create a baseline collection. Baseline collections are not required, but they offer the same benefits as working with policy templates. For example, you could use more than one instance of the same criteria set in a single baseline collection to check different parameters.

Creating Baseline Collections

You can create a baseline collection from a single set or multiple sets of baseline criteria.

To create a baseline collection:

1. In the left pane, click **Baselines**.
2. In the Baselines tree pane, right-click **Collection**, and then click **New Baseline Collection**.
3. Follow the instructions in the wizard to build the baseline collection.

NOTE: Do not use the special characters `?>"|<` in the baseline name. When you use one of these special characters, the completed baseline report displays an error rather than baseline data.

Modifying Baseline Collections

After you create a baseline collection, you can modify it any time to meet the changing needs of your environment. For example, you may need to add baseline criteria sets to a collection you created for a group of assets after you install new software on those computers.

To modify a baseline collection:

1. In the left pane, click **Baselines**.
2. In the Baselines tree pane, select **Collection**.
3. In the content pane, right-click the baseline collection you want to modify, and then click **Edit**.
4. Follow the instructions in the wizard to modify the baseline collection.

Deleting Baseline Collections

You can delete a baseline collection if you no longer need it, for example, if changes in your environment have made the collection obsolete.

To delete a baseline collection:

1. In the left pane, click **Baselines**.
2. In the Baselines tree pane, select **Collection**.
3. In the content pane, right-click the baseline collection you want to delete, and then click **Delete**.
4. Click **Yes** on the confirmation message.

Exporting Baseline Collections

After you have created baseline collections, you can export them as .bcl files. Exporting baseline collections allows you to restore this data in case it is changed incorrectly. You can also import this data to a different Core Services computer.

To export a baseline collection:

1. In the left pane, click **Baselines**.
2. In the Baselines tree pane, select **Collection**.
3. In the content pane, select the baseline collection you want to export, and then click **Export Baseline Collection**.
4. Select a folder in which you want to save the exported baseline collection.
5. Click **Save**.

Importing Baseline Collections

You can import baseline collections that you previously exported from the current Core Services computer, or from another Secure Configuration Manager Core Services computer. You can also use this feature to restore a baseline collection that was changed incorrectly. If a baseline collection file with the same name already exists, Secure Configuration Manager gives you the option to overwrite the existing file.

To import a baseline collection:

1. In the left pane, click **Baselines**.
2. In the Baselines tree pane, right-click **Collection** and then click **Import Baseline Collection**.
3. Select the baseline collection (.bcl) files you want to import and click **Open**.

7.3.3 Establishing a Baseline

After creating a baseline criteria set or a baseline collection, you can establish a baseline for target endpoints. You can use either or both of the following methods as appropriate:

- Add a single set or multiple sets of baseline criteria to a baseline collection and then establish the baseline using that baseline collection.
- Create a baseline criteria set and then establish the baseline directly from that criteria set.

When you establish a baseline, ensure that you enter a unique and easily identifiable name for the baseline. If you do not enter a name, Secure Configuration Manager provides a default name using the name of the criteria set and the current date and time. In a large environment with multiple baselines, being able to easily identify your baselines simplifies management and reporting tasks.

NOTE: Do not use the special characters `?>"|<` in the baseline name. When you use one of these special characters, the completed baseline report displays an error rather than baseline data.

It is also a good idea to note which endpoints you are using when you establish a baseline. Since baselines reside on the agents, when you run the Compare Baseline check, Secure Configuration Manager does not automatically populate the check with the endpoints you selected for the original baseline. However, you can generate a list of the baselines established on all your endpoints by running the List Baselines check if necessary.

To establish a baseline:

1. (Conditional) To establish a baseline from a baseline collection, perform the following steps:
   - **1a** In the left pane, click **Baselines**.
   - **1b** In the Baselines tree pane, select **Collection**.
   - **1c** In the content pane, right-click the collection you want to use and then click **Establish Baseline**.
   - **1d** Follow the instructions in the wizard to establish the baseline.
2. (Conditional) To establish a baseline from a single criteria set, perform the following steps:
   - **2a** In the left pane, click **Baselines**.
   - **2b** In the Baselines tree pane, select **Criteria**.
   - **2c** Select the appropriate platform and category for the criteria set.
   - **2d** In the content pane, right-click the criteria set you want to use and then click **Establish Baseline**.
   - **2e** Follow the instructions in the wizard to establish the baseline.
3. Review your asset groups and establish additional baselines as needed.

For more information about baseline collections, see the Baseline Collection wizard Help. For more information about baseline criteria, see the Baseline Criteria wizard Help.

7.3.4 Running a Baseline Comparison Check

Secure Configuration Manager provides a built-in, platform-independent security check called **Compare Baseline**. Running the Compare Baseline check generates a report on any changes on your target endpoints or asset groups against your established baselines. You can report on a single baseline or multiple baselines.

You can run baseline comparison checks as needed, or you can create a regular schedule by adding them to a policy template. For more information about scheduling a baseline comparison check, see Section 7.3.5, “Scheduling a Baseline Comparison Check,” on page 119.

NOTE: When running a baseline comparison check, you must enter the Baseline Name parameter in the proper text case for the check to recognize the existing baseline.

To run a baseline comparison:

1. (Conditional) To report on a single baseline immediately, run the Compare Baseline check as an individual security check:
   - **1a** In the left pane, click **Baselines**.
   - **1b** In the Baselines tree pane, select **Management**.
   - **1c** In the content pane, right-click **Compare Baseline** and then click **Run Security Checks**.
   - **1d** Follow the instructions in the wizard to select the established baseline and the endpoints against which you want to run the baseline comparison.
2. (Conditional) To report on multiple baselines, add multiple instances of the Compare Baseline check to a policy template and then run the policy template. For more information about using policy templates, see Section 4.2, “Understanding Policy Templates,” on page 49.

7.3.5 Scheduling a Baseline Comparison Check

To run a baseline comparison check on a regular schedule, you must perform two steps: add the baseline comparison check as a policy template, and then set the scheduling parameters using the Run Policy Template wizard.

To schedule a Baseline Comparison check:

1. In the left pane, click **Security Knowledge**.
2. In the Security Knowledge pane, right-click **Policy Templates** and then click **New Policy Template**.
3. Select **Baseline Management** from the options list.
4. In the Available Checks pane, expand **Common > Baseline Management**.
5. Select **Compare Baseline** and click **>** to add the security check to the Selected Checks pane, and then click **Next**.
6. Follow the remaining instructions to complete the Policy Template wizard.
7. In the left pane, select **Security Knowledge**.
8. In the Security Knowledge pane, expand **Policy Templates > My Templates**.
9. Right-click the appropriate baseline comparison template, and then click **Run Policy Template**.
10. Follow the instructions in the wizard.
11. In the Schedule window, select **Enable Schedule**, and then specify the scheduling parameters.
12. (Optional) To have the baseline comparison run on a recurring basis, click **Recurring**.
    - **12a** Click **Schedule Recurrence** to define how often you want to run the baseline comparison.
    - **12b** In the Recurrence Job Schedule window, specify the frequency and duration for which the baseline comparison will run.
13. Follow the remaining instructions in the Run Policy Template wizard.

7.3.6 Deleting a Baseline

When you no longer need a baseline, you can delete that baseline.

To delete a baseline:

1. In the left pane, click **Baselines**.
2. In the Baselines pane, select **Management**.

3 In the content pane, right-click **Remove Baseline** and then click **Run Security Checks**.

4 Follow the instructions to delete the baseline.

7.3.7 Updating a Baseline

Once you have established a baseline, you may need to update it to set a new standard for your target endpoints using the target endpoints' current characteristics. When you update a baseline, you re-establish the baseline with the same criteria sets. For example, you originally established a baseline for Endpoint A with four active user accounts, but that endpoint now supports eight user accounts. Rather than having Endpoint A regularly fail the established baseline, you can update the baseline for Endpoint A so that eight user accounts become the standard for the baseline.

You can also edit the baseline's criteria. For more information, see "Modifying Baseline Criteria" on page 115.

To update an established baseline:

1 In the left pane, click **Baselines**.

2 In the Baselines tree pane, select **Management**.

3 In the content pane, right-click **Update Baseline** and then click **Run Security Checks**.

4 Using the same baseline criteria sets or collections, establish a new baseline on the same target endpoints. For more information, see Section 7.3.3, "Establishing a Baseline," on page 117.

7.3.8 Creating a List of Baselines for a Target Endpoint

In a large or complex environment, you may have several baselines for a single endpoint. Secure Configuration Manager provides the List Baselines check you can run to generate a list of all established baselines for a target endpoint. You can also use this check to report on baselines for multiple endpoints.

To create a list of all baselines for a target endpoint:

1 In the left pane, click **Baselines**.

2 In the Baselines tree pane, select **Management**.

3 In the content pane, right-click **List Baselines** and then click **Run Security Checks**.

4 Follow the instructions to select the target endpoints and run the report.

8 Maintaining Your Security Knowledge

Secure Configuration Manager provides hundreds of built-in security checks to help you evaluate risks in your enterprise. To properly maintain your enterprise, you need up-to-date security knowledge. Secure Configuration Manager includes an automated security content update service that delivers new security checks, policy templates, and patch-level databases as new vulnerabilities emerge.

The Secure Configuration Manager AutoSync feature lets you regularly download and apply newly developed security knowledge in the following formats:

- Secure Configuration Manager security checks
- Patch-level database files
- Secure Configuration Manager policy templates, which include security bulletins representing vulnerability and malicious code alerts

The patch-level database files ensure that the computers in your enterprise are running with the latest recommended patches when checking for vulnerabilities.

Downloading the latest security knowledge arms Secure Configuration Manager with updated vulnerability assessment techniques to keep your enterprise protected. Use the AutoSync service to regularly download this important security content to ensure that Secure Configuration Manager agents always audit with the latest security intelligence. The **AutoSync service** is a Web site-based update service.

To deliver current, reliable security content, NetIQ Corporation partners with a trusted leading security content provider. NetIQ Corporation is committed to providing timely vulnerability alerts and other security content so you can immediately use and benefit from current security expertise. You can easily download the latest security knowledge using the built-in AutoSync service.

8.1 Understanding the AutoSync Components

NetIQ Corporation provides a Secure Configuration Manager library of policy templates and security checks to test for current known vulnerabilities. NetIQ regularly updates and augments the library in direct response to security bulletins as they are published. To keep your library current with corrections for the latest known vulnerabilities, NetIQ maintains an AutoSync update service Web site that Secure Configuration Manager can automatically access.

The updates listed in the AutoSync wizard include release notes for available hotfixes and service packs. The wizard labels these updates as Notifications. The AutoSync wizard does not apply Notification updates to Secure Configuration Manager.

When Secure Configuration Manager connects to the AutoSync Web site, the product compares your locally-stored security files with the files on the AutoSync Web site and provides you the option to download to your local library any new or changed files. An icon in your Windows task bar indicates that updates are available. You can update your library on demand or schedule AutoSync to check for updates to the library regularly.

8.2 Configuring a Standalone AutoSync Client

Use a standalone AutoSync client when your Core Services computer is not directly connected to the Internet, or when you do not want that computer to download from the Internet. The standalone **AutoSync client** runs separately from Core Services and queries the AutoSync server for security knowledge updates.

8.2.1 Connecting the AutoSync Client to Core Services

To use a standalone AutoSync client, you need to specify configuration information so the AutoSync client can query and receive updates from the NetIQ AutoSync server. The **AutoSync server** is a NetIQ Corporation server that provides security knowledge updates when queried by an AutoSync client. In addition to basic AutoSync settings, you can also set up a connection to a proxy Internet server. For more information, see Section 8.3, “Connecting to the AutoSync Server through Proxy,” on page 123.

To configure Core Services to communicate with a standalone AutoSync client:

1. Install the Standalone AutoSync client. For more information about installing the client, see the *Installation Guide for NetIQ Secure Configuration Manager*.
2. Log on to a console computer and open the console.
3. On the Tools menu, click **AutoSync Wizard**.
4. Click **Settings**.
5. Expand **AutoSync Client System**.
6. Specify the **Host Name/IP address** of the AutoSync client computer. Secure Configuration Manager supports IPv4 and IPv6 addresses.
7. Specify the **Port number** for communications with the AutoSync client computer.

   NOTE: If Core Services runs in a FIPS-enabled environment, you must set the port to 1621. For more information, see Section 8.2.2, “Connecting the AutoSync Client to Core Services in a FIPS-Enabled Environment,” on page 122 and Section 10.5, “Enabling FIPS Communication,” on page 139.
8. Click **OK**.

8.2.2 Connecting the AutoSync Client to Core Services in a FIPS-Enabled Environment

If you run Secure Configuration Manager in an environment that uses Federal Information Processing Standard (FIPS) algorithms for secure communication, you must configure the AutoSync client to communicate with Core Services. For more information about FIPS, see Section 10.5, “Enabling FIPS Communication,” on page 139.

To configure the client for FIPS-enabled communication:

1. Complete the steps in Section 8.2.1, “Connecting the AutoSync Client to Core Services,” on page 122. However, ensure that the port number is set to 1621.
2. Using an Administrator account, log on to the computer where you installed the standalone AutoSync client.
3. Run the `config.bat` file. By default, the file is located in the `%Program Files%\NetIQ\Secure Configuration Manager\AutoSync Client\bin` folder.

4 On the Network tab of the NetIQ AutoSync Client Configuration Utility, change **Enable FIPS Support** to **true**.

5 Click **OK**.

6 Restart the NetIQ AutoSync Client service.

8.3 Connecting to the AutoSync Server through Proxy

You can access the AutoSync Web site through an Internet proxy server. If you are using a standalone AutoSync client, ensure that you have configured that client before you complete the following steps. For more information, see Section 8.2, “Configuring a Standalone AutoSync Client,” on page 122.

NOTE: AutoSync does not support NTLM authentication.

To configure a proxy Internet server:

1 (Conditional) If you are using a standalone AutoSync client, ensure that you have configured the client.

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

3 Click **Settings**.

4 In the **Proxy Enabled** field, select **Yes**.

5 (Conditional) If your local environment requires a user name and password for the proxy server, complete the following steps:

5a Expand **Proxy User**.

5b Specify a user name to access the proxy server.

5c Specify a password for the user.

6 Expand **Proxy Server**.

7 Specify the **Host Name/IP address** of the computer acting as the proxy Internet server. Secure Configuration Manager supports IPv4 and IPv6 addresses.

8 Specify the **Port number** of the computer acting as the proxy Internet server.

9 Select the **Proxy Type**.

10 Click **OK**.

8.4 Manually Checking for New Security Knowledge

You can check for updates on the AutoSync server any time after you have configured the AutoSync settings. You can also schedule regular updates. For more information, see Section 8.5, “Scheduling Checks for New Security Knowledge,” on page 124.

After you check for updates, you can review the updates and choose the ones to apply. For more information, see Section 8.6, “Applying AutoSync Updates,” on page 124.

To manually check for AutoSync updates:

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

2 Click **Check for Updates**.

8.5 Scheduling Checks for New Security Knowledge

You can schedule the AutoSync client to regularly check for new AutoSync updates. You can also check for updates manually any time. For more information, see Section 8.4, “Manually Checking for New Security Knowledge,” on page 123.

After a scheduled check completes, review the list of available updates and choose the updates to apply. For more information, see Section 8.6, “Applying AutoSync Updates,” on page 124.

To schedule regular AutoSync checks:

1. On the Tools menu, click **AutoSync Wizard**.
2. Click **Settings**.
3. Expand **Schedule AutoSync**.
4. Complete the scheduling fields to set up the frequency to check for AutoSync updates.
5. Click **OK**.

8.6 Applying AutoSync Updates

When an AutoSync check is complete, Secure Configuration Manager lets you review the updates and select the updates that you want to apply. When you apply an update, Secure Configuration Manager is updated with the new information from the AutoSync server. New information includes new policy templates, security checks, and patch-level database files.

When using AutoSync to add security checks, Secure Configuration Manager stores the checks in the appropriate operating system folder under **Security Checks > NetIQ Checks**. Secure Configuration Manager stores new templates in the appropriate folder under **Policy Templates**.

To review and apply AutoSync updates:

1. On the Tools menu, click **AutoSync Wizard**.
2. (Optional) To view details about the update packages, click **Show Details**.
3. (Optional) To view detailed information about a specific update and the associated vulnerability, click the update name to display more detailed information.
4. Select the check box for each security update that you want to apply.
5. Click **Apply Updates**.
6. Click **Finish**.

NOTE: The update download may take a few minutes to complete.

8.7 Updating Agent Content

When the UNIX or Windows security agent runs a security check or policy template that performs a patch assessment, such as the Security Patches Not Applied check, the agent uses the list of patches in the patch-level database to compare against patches found on the target endpoint. The AutoSync service provides monthly updates for the patch-level content to ensure that Secure

Configuration Manager and the agents always audit with the latest security information. After downloading the latest patch database from the AutoSync server, you have three options for updating agents:

- Update agents when you run a patch assessment security check
- Schedule the agent updates
- Manually update each agent

To view the downloaded and applied updates, click the Archived Updates tab in the AutoSync wizard. For more information, see Section 8.8.3, “Viewing the History of an Archived Update,” on page 127. To identify which of the patch databases have been applied to which agents, run the Applied Patch Databases administrative report. For more information, see Section 1.5, “Listing Reports, Actions, and Security Checks,” on page 17.

8.7.1 Updating Agent Content During a Security Check Run

If you enable the **Push Patch Database** option in the AutoSync settings, Secure Configuration Manager automatically updates the patch-level content on each Windows agent. Each time you run a security check or policy template that performs a patch assessment, Core Services checks whether the specified agent has the most recent patch-level content. If the agent does not have the latest version of the patch-level content, Core Services sends the content files to the agent with the security check or policy template.

The **Push Patch Database** option ensures that all security agents have the latest patch-level content without your having to schedule a task for updating each agent or your having to manually update each agent every month.

NOTE: Secure Configuration Manager can push content only to Windows agents.

To update agent content during a security check run:

1. On the Tools menu, click **AutoSync Wizard**.
2. Click **Settings**.
3. Change the **Push Patch Database To Agents** option to **Yes**.
4. Click **OK**.
5. Close the AutoSync wizard.
6. Regularly download and apply the latest patch databases, such as NetIQ Windows Agent Patch Database, from the AutoSync server.

8.7.2 Scheduling Agent Content Updates

You can run the Update Agent Content task on a scheduled basis to frequently and automatically update your agents. For optimum performance, run the task against groups of 30 to 50 agents at a time.

To schedule updates for agent content:

1. Download and apply the latest patch database, such as NetIQ Windows Agent Patch Database, from the AutoSync server. For more information, see Section 8.6, “Applying AutoSync Updates,” on page 124.
2. In the tree pane, expand **IT Assets > Managed Groups** to display the group folder that contains the endpoints whose associated agents you want to update.

3 (Optional) To schedule updates for the agent content for a group, select the group in the tree pane or content pane.

4 (Optional) To schedule updates for the agent content for a single endpoint, select the associated group in the tree pane, and then select the endpoint in the content pane.

5 On the right-click menu, click **Update Agent Content**.

6 In the Run Task Suite wizard, click **Schedule**.

7 In the Scheduled Task wizard, configure the schedule settings.

8 Click **OK**, and then click **Finish**.

8.7.3 Manually Updating Agent Content

You can manually run the Update Agent Content task to update your agents. For example, you might add an agent to IT Assets and want to ensure that the agent has the latest patch-level content.

To manually update agent content:

1 Download and apply the latest patch database, such as NetIQ Windows Agent Patch Database, from the AutoSync server. For more information, see Section 8.6, “Applying AutoSync Updates,” on page 124.

2 In the tree pane, expand **IT Assets > Managed Groups** to display the group folder that contains the endpoints whose associated agents you want to update.

3 (Optional) To update the agent content for a group, select the group in the tree pane or content pane.

4 (Optional) To update the agent content for a single endpoint, select the associated group in the tree pane, and then select the endpoint in the content pane.

5 On the right-click menu, click **Update Agent Content**.

6 When the wizard has finished updating the agent content, click **Finish**.

When the update completes, Secure Configuration Manager stores the completed update job in **Completed** under **Job Queues**.

8.8 Understanding AutoSync Archive

Secure Configuration Manager automatically moves updates you have applied or approved to the AutoSync Archive. You can also move declined updates to the Archive. You can decline to apply any of the security checks, policy templates, or patch level database files available in AutoSync. For example, you may not need updates for an operating system not supported by your environment.

8.8.1 Archiving Unapplied Updates

You can move updated items to the Archive without applying them. For example, if your environment does not include UNIX systems, you do not need to apply policy templates for those systems.

To archive unapplied updates:

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

2 Select the check box next to the files you want to archive.

3 Click **Move to Archive**.

8.8.2 Restoring Archived Updates

Secure Configuration Manager allows you to apply the same update more than once. For example, you may need to restore and re-apply updates after disaster recovery. To ensure continuity, the Archive maintains a history of each update's application. For more information, see Section 8.8.3, "Viewing the History of an Archived Update," on page 127.

To restore archived updates:

1. On the Tools menu, click **AutoSync Wizard**.
2. Click the Archived Updates tab.
3. Select the check box next to the files you want to restore.
4. Click **Restore Updates**.
5. Click the Available Updates tab, and then follow the instructions for applying updates. For more information, see Section 8.6, "Applying AutoSync Updates," on page 124.

8.8.3 Viewing the History of an Archived Update

Because you can apply an update multiple times, AutoSync lists the dates and times an update has been applied. Archive history details apply only to updates added to AutoSync since upgrading or installing Secure Configuration Manager version 5.8.

To view the history of an archived update:

1. On the Tools menu, click **AutoSync Wizard**.
2. Click the Archived Updates tab.
3. Select the check box next to the file you want to view.
4. Click **Show Details**.
5. Click the History tab.

9 Maintaining the Secure Configuration Manager Database

Database maintenance is important to the health of your network security and Secure Configuration Manager data. By establishing a diligent and thorough database maintenance strategy, you can ensure optimal performance on a daily basis as well as successful data recovery in response to an emergency. Database maintenance includes routine backups, supported by data archival and grooming.

On occasion, you also need to modify settings in the console and Core Services to improve performance and enhance Secure Configuration Manager capabilities.

9.1 Database Maintenance Checklist

The following checklist outlines the typical database maintenance workflow. Use this checklist to understand the database maintenance process and help you implement the best maintenance strategy for your organization.

	Checklist Items
❑	1. Verify the appropriate permissions in Microsoft SQL Server and Secure Configuration Manager. See Section 9.2, “Required Database Permissions and Settings,” on page 129.
❑	2. Understand how the Secure Configuration Manager database stores and manages data. See Section 9.3, “How the Secure Configuration Manager Database Works,” on page 131.
❑	3. Identify and implement the appropriate database maintenance strategy for your organization. See Section 9.4, “Developing a Database Maintenance Strategy,” on page 132.
❑	4. Ensure data preservation and history by scheduling routine backups.See Section 9.4.2, “Backing Up the Secure Configuration Manager Database,” on page 132.
❑	5. Ensure optimal database performance through routine grooming. See Section 9.4.3, “Grooming the Secure Configuration Manager Database,” on page 133.

9.2 Required Database Permissions and Settings

The Secure Configuration Manager database requires the following permissions and authentication settings:

Accounts

Core Services uses the VigilEntService account to connect to the SQL Server computer on which the Secure Configuration Manager database is installed. The Secure Configuration Manager console uses either the VSMConsole or VigilEnt_Users account to read and write data from the Secure Configuration Manager database. Secure Configuration Manager creates these accounts during installation.

Roles

By default, the VigilEntService, VSMConsole, and VigilEnt_Users accounts are granted the VigilEnt User Access role in SQL Server. Secure Configuration Manager creates this role during installation. Use the Microsoft SQL Server Enterprise Manager tool to verify permissions.

Microsoft SQL Server automatically grants the `sysadmin` role to Windows user accounts that belong to the Administrators group.

Authentication

Secure Configuration Manager supports both Windows authentication and mixed-mode authentication. You can choose to use SQL authentication when you log onto the Secure Configuration Manager console.

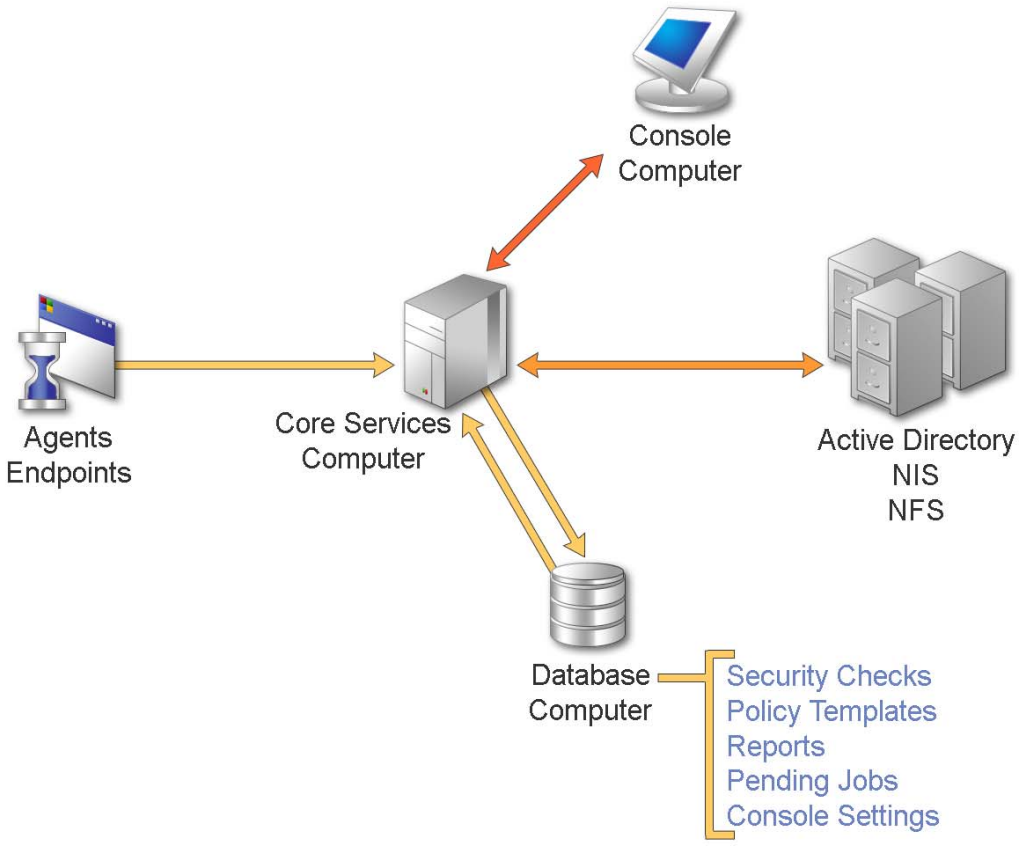
Depending on which authentication you configure Core Services to support, the Secure Configuration Manager console can accept different account credentials at logon. If Core Services is configured to support SQL authentication, the console can accept either the VSMConsole or the VigilEnt_Users account credentials. If Core Services supports Windows authentication, the console can accept the Windows credentials of the console user. For more information, see the *Installation Guide for NetIQ Secure Configuration Manager*.

For more information about Secure Configuration Manager requirements, see the *Installation Guide for NetIQ Secure Configuration Manager*.

9.3 How the Secure Configuration Manager Database Works

The **Secure Configuration Manager database** contains all Secure Configuration Manager data, including policy templates and task suites, report results, console user properties, domain keys, and Core Services security settings. The Secure Configuration Manager database also stores relevant data and Microsoft SQL Server settings.

The following figure shows the relationship between the Secure Configuration Manager database, the Core Services computer, and the Secure Configuration Manager console.



When you run a security check, a task suite, or a policy template, the Secure Configuration Manager console gathers data and then writes the results to the Secure Configuration Manager database. Secure Configuration Manager appends the new data to an existing table, writing one row of data per report run by the current console user. When you create console users or reset console user passwords, Secure Configuration Manager adds or changes these credentials in the database.

9.4 Developing a Database Maintenance Strategy

Because the Secure Configuration Manager database contains sensitive data, consider a database maintenance strategy that provides optimal performance and supports your data management goals. A database maintenance strategy determines the health of your database, ensures data integrity, and helps you better meet the data security needs of your organization.

A database maintenance strategy consists of the following key items:

- Database backup and archival
- Database grooming
- Database recovery

For each Secure Configuration Manager database you manage, develop a database maintenance strategy that addresses these key items.

9.4.1 Identifying a Backup and Archive Plan

How frequently you should back up and archive the Secure Configuration Manager database depends on your answers to the following questions:

- How often do you capture important data?
- How quickly does your database grow?
- How stable is your environment?

For example, if you run multiple daily policy templates and task suites, you may want to back up and archive the Secure Configuration Manager database each night. Daily backups ensure that you keep the most current copy of the database available. If your environment requires routine upgrades and security patches, you may want to implement a regular backup and archive schedule to mitigate potential data loss. Your backup frequency also influences your recovery model. For more information, see Section 9.4.4, “Identifying the Appropriate Recovery Model,” on page 134.

9.4.2 Backing Up the Secure Configuration Manager Database

You can back up the Secure Configuration Manager database to address the following goals:

- Ensure the security of your data
- Archive a data set
- Prevent data loss during upgrades
- Move the database from one Microsoft SQL Server computer to another

Backing up the Secure Configuration Manager database on a routine, scheduled basis helps achieve these goals. You can perform different types of backups, such as a full backup or an incremental backup. When selecting the backup type, consider the database size, the importance of your data, and how long you intend to keep the archived data. For example, Microsoft SQL Server supports full database backups as well as partial transaction log backups, allowing for more flexible and thorough recovery. This strategy is ideal if your transaction rate is high but can strain resources if your database is large. Nightly full backups can meet the security and data recovery needs of most organizations.

The following table provides additional information sources.

For more information about ...	See ...
Understanding how the Secure Configuration Manager database works	Section 9.3, “How the Secure Configuration Manager Database Works,” on page 131
Backing up the Secure Configuration Manager database	SQL Server Books Online
Moving the Secure Configuration Manager database to a different Microsoft SQL Server computer	NetIQ Technical Support
Managing distributed Secure Configuration Manager databases	NetIQ Professional Services

9.4.3 Grooming the Secure Configuration Manager Database

Secure Configuration Manager includes an automated, system-wide task to purge completed job record data from the database at the conclusion of the defined retention period. By default, the record retention setting is 90 days. You can specify that Secure Configuration Manager should never purge data by configuring **System Purge Time of Day** and **System Purge Period** in the Core Services Configuration Utility. Once you have configured the purge period, Secure Configuration Manager does not begin the purge immediately, but purges the database based on those settings. For more information, see the Core Services Configuration Utility Help. You can also configure purges for completed jobs, alerts, and job history log data. For more information about purging the Jobs Queues, see Section 10.2.1, “Setting the Retention Period,” on page 137.

You can manually groom the database to remove old and unused data. The Secure Configuration Manager database supports **script-based grooming**. Script-based grooming uses a script to search the database for old data and then deletes the appropriate columns, rows, or tables. You can also write scripts to export selected data, and then remove this archived data from the database.

Grooming scripts typically use Structured Query Language (SQL) to read and write data to the database, and VBScript or Java to connect to the SQL Server computer. You can also write SQL transactions, queries, and deletes using SQL commands from the Microsoft SQL Query Analyzer. For more information about developing a grooming script that best meets the needs of your organization, contact NetIQ Professional Services.

Secure Configuration Manager provides the Core Services Configuration Utility, which allows you to perform limited grooming. This utility lets you specify how often you want Secure Configuration Manager to delete report and asset map data. To decide how often you should purge the Secure Configuration Manager database, run the Task History Report. As the database grows, you may want to perform database consistency checks through Microsoft SQL Enterprise Manager.

Always back up the Secure Configuration Manager database before running a grooming script or SQL commands. For more information about database maintenance, see SQL Server Books Online. For more information about the Secure Configuration Manager database, see Section 9.3, “How the Secure Configuration Manager Database Works,” on page 131.

9.4.4 Identifying the Appropriate Recovery Model

Although you may routinely back up the Secure Configuration Manager database, your database data is only as current as the last backup. A successful database maintenance strategy balances the need for current data with the ability to quickly and accurately restore a database when required. Identifying the appropriate recovery model ensures efficient and effective disaster recovery.

Although the simple recovery model can address the needs of most organizations, your recovery model depends on the backup process you implement. For more information about determining the best backup and archive frequency for your organization, see Section 9.4.1, “Identifying a Backup and Archive Plan,” on page 132. For more information about recovery models, contact your database administrator or see SQL Server Books Online.

10 Customizing Secure Configuration Manager

You can customize the performance of Secure Configuration Manager components, particularly in the Job Queues, the console, and Core Services. You can also generate reports about your resources without running a security check or policy template when you simply want a quick, informational report.

10.1 Creating Custom Tasks and Reports

Secure Configuration Manager provides built-in tasks for running simple reports or actions against endpoints in your asset map, such as identifying accounts with weak passwords. You can edit these built-in tasks or create tasks to meet your organization's specific needs. For efficiency, you can group similar tasks to get one report. Tasks provide informational data only and cannot measure the potential vulnerability of your IT assets. For more information about measuring asset vulnerability, see Chapter 4, "Auditing Your IT Assets," on page 47.

Secure Configuration Manager also enables you to customize the logo displayed on all reports. For more information about changing the logo, see Section 10.1.3, "Changing the Logo on the Report," on page 136.

10.1.1 Creating Custom Tasks

A **custom task** is a report or action with pre-defined parameters. You can run the task against multiple groups of heterogeneous endpoints. Only the console user who created the task and the console administrator can see the custom task. Secure Configuration Manager includes a set of standard custom tasks that you can run immediately after you install the product.

After you have created a custom task, you can include that custom task in a task suite. You can also edit custom tasks and the built-in tasks. If the edited custom task is part of any task suite, the new custom task definition takes effect immediately in all referenced task suites. You can delete an existing custom task at any time. For more information about task suites, see Section 10.1.2, "Creating Groups of Custom Tasks," on page 136.

WARNING: If the custom task is a member of one or more task suites, and you delete the custom task, all task suite references to this custom task are also deleted.

10.1.2 Creating Groups of Custom Tasks

Secure Configuration Manager enables you to easily create, edit, schedule, import, export, and delete task suites. A **task suite** is a combination of multiple reports and actions, the parameters for each report and action, the unique values input for each parameter, and a sequence of execution. You can also include custom tasks in task suites. Secure Configuration Manager includes a set of standard task suites that you can run immediately after you install the product.

After creating the appropriate task suites to meet your company's security standards, you can schedule those task suites to allow Secure Configuration Manager to continuously assess your IT environment. Running a task suite for a managed group checks each endpoint in the group for each report or action in the task suite, and then generates a report. Once you have scheduled a task, you can update the schedule properties using the Scheduled Jobs wizard.

The console user who creates each task suite owns the task suite. By default, you are the only console user who can see a task suite that you create. To make a task suite visible to all other console users, select the **Share this Task Suite** check box in the Task Suite wizard. If you are a console administrator you can also reassign the owner of a scheduled task suite. For more information about roles, see Section 3.5, "Managing Roles," on page 40.

NOTE: When the account for the owner of a task suite is disabled or deleted, Secure Configuration Manager no longer runs the scheduled job.

You can import one or more task suites that you have previously saved. You can also import task suites to restore a suite that was changed incorrectly. If a task suite with the same name already exists, Secure Configuration Manager gives you the option to overwrite the existing task suite. To save a specific task suite version, you can export the task suite in `.xml` format.

Refer to the following table when assigning permissions to console users who work with task suites.

User activity	Required permission
Run a task suite	Run Tasks and Task Suites
Import a task suite	Import Task Suites
Export a task suite	Export Task Suites

For more information about assigning permissions, see Section 3.6, "Managing Permissions," on page 42.

10.1.3 Changing the Logo on the Report

You have the option of displaying your company logo or the NetIQ logo in your completed reports. By default, Secure Configuration Manager displays the NetIQ logo the header on each page and on the title page.

The following table shows the file names for the graphics that appear in the reports.

File Name	Location of Graphic
SCPageHeader.jpg	Header of each report page
SCTitlePageHeader.jpg	Header of title page

To replace the NetIQ logo with your company logo or another graphic file:

1. Browse to the `Program Files\NetIQ\Secure Configuration Manager\VSOC\images` folder on your computer.
2. Rename the `SCPageHeader.jpg` and the `SCTitlePageHeader.jpg` files.
3. Save your company logo files with the file names `SCPageHeader.jpg` and `SCTitlePageHeader.jpg`.

   NOTE

   - The dimensions of the default files are 1020 x 100 pixels. Make sure your company logo files are the same size.
   - If you remove or rename these files, Secure Configuration Manager displays the reports without a graphic.

4. View the report containing the new graphics.

10.2 Customizing the Job Queues

Secure Configuration Manager handles all reports and actions as jobs that run asynchronously and then stores the scheduled and completed reports in **job queues**. Once you submit a job to Core Services, you can perform other jobs in the console.

From the Job Options window, you can change settings for how long the console retains data in the Completed and Job History queues and the Alerts window. In addition, you can set the console to filter all job queues by a specified user.

You can display up to 1,000 records on a page when viewing the items in a queue or log. If the queue contains more than 1,000 records, use the **Prev** and **Next** buttons at the bottom of the console to navigate to the previous and next set of records.

10.2.1 Setting the Retention Period

Secure Configuration Manager purges completed jobs, alerts, and job history log data at the conclusion of the defined retention period. By default, the retention period is global and not saved by the user. However, you can set the retention period for completed jobs on a per-session basis in the Job Options window. In the Jobs Queue, right-click **Completed** and then click **Options**.

You can indicate specifically how long Secure Configuration Manager keeps job queue, history log, or alert information on the Job Options window. You can set the console to retain job queue information for completed jobs based on the session. You can also specify when Secure Configuration Manager deletes Job History queues and Alert logs on a global basis from this window. In addition, you can set the console to filter these windows to show all job queue windows for only a specified user.

WARNING: Secure Configuration Manager purges data from the database after the time specified in the purge settings in the Configuration Utility or in the Job Options retention fields. To preserve this information, run reports before the report retention period elapses, and then export the report data to a file. For more information about exporting report data to a file, see Section 4.6, “Exporting Reports,” on page 56, Section 5.3.7, “Exporting a Delta Report,” on page 68, and Section 10.1.2, “Creating Groups of Custom Tasks,” on page 136. For more information about purging the database, see .

10.2.2 Using Folders to Organize Completed Jobs

Secure Configuration Manager allows you to organize completed jobs such as policy template reports. In Job Queues, you can create folders, move jobs from the Completed jobs queue to user-defined folders, and delete jobs and folders. For example, you can create a folder called `Passwords` to contain reports generated from password-related security checks and policy templates.

You can create an unlimited number of user-defined folders to organize completed jobs. Once you have created folders, you can move jobs from the Completed jobs queue or move jobs from user-defined folder to user-defined folder by right-clicking the job and selecting **Move to** from the options.

NOTE

- You cannot rename a user-defined folder, so ensure that you name the folder appropriately.
- You cannot use special characters, such as @”#$), in the user-defined folder name.
- You can change a user-defined folder description.
- Before deleting a user-defined folder, you must remove or delete the jobs within the folder.

Although you cannot edit a user-defined folder name, you can create a new folder with the name you want, then move all jobs from the current folder to the new folder. After all jobs are removed, you can delete the unneeded folder.

10.3 Customizing the Console

You can modify console settings to point to a different Core Services computer and enable SQL authentication. You can also adjust the settings to improve console performance.

10.3.1 Modifying Console Settings

The console options settings enable you to point to a different Core Services computer, by changing the specified IP address and port number. You can also enable SQL authentication. To modify console settings, click **Tools > Options**.

NOTE: 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.

10.3.2 Improving Console Performance

The size of your Secure Configuration Manager database and number of concurrent connections can affect console performance. Secure Configuration Manager automatically refreshes data in the console to ensure that you view the most up-to-date information. However, if the console tries to obtain more data than can be pulled from the database within the specified refresh period, the console can pause or stop responding instead of displaying the requested data. This usually occurs

when the database contains a large volume of data, your enterprise has more than 500 endpoints, there are multiple concurrent console connections to the database, or a combination of all these factors.

To remediate the issue, you can increase the refresh period to improve console performance. You can also disable the automatic refresh period and use only the F5 function to manually refresh the console.

To change the console refresh period:

1. On the Tools menu, click **Options**.
2. On the Options window, click **Other**.
3. (Optional) To increase the time between refresh intervals, enter a new value in the **Refresh Period (seconds)** field up to 60 seconds.
4. (Optional) To disable the refresh rate, deselect the **Enable Automatic List Refreshes** check box. To manually refresh the console, you must press F5.
5. Click **OK**.

10.3.3 Modifying the Session Timeout Settings

You can specify whether Core Services terminates a console session that has been idle for a designated amount of time. You can also specify how often Core Services checks for idle sessions. When a session times out, the console user must log on again. Processes that the user starts before the timeout occurs continue to function. For more information about modifying timeout settings, see the Help for the Database tab of the Core Services Configuration Utility.

10.4 Customizing Core Services

Use the Core Services Configuration Utility to specify settings such as types of domains you want to include when discovering systems, types of alerts, and email addresses to receive alerts. The Core Services Configuration Utility resides on the same computer on which you installed Core Services. For more information about this utility and customizing Core Services, see the Help for the Core Services Configuration Utility.

10.5 Enabling FIPS Communication

Secure Configuration Manager components use secure TLS/SSL communication. Secure Configuration Manager also supports Federal Information Processing Standard (FIPS 140-2) communication between the product components. FIPS 140-2 standards regulate the implementation and communication of cryptographic software. Users working under FIPS guidelines must operate using Secure Configuration Manager within a secure FIPS-enabled environment.

Secure Configuration Manager features FIPS-migration mode functionality, which allows Core Services to communicate with Windows or UNIX security agent computers that are either in or out of FIPS mode. During agent registration, Core Services queries the agent operating system registry to determine whether FIPS communication is enabled. If the agent is already in FIPS mode, Core Services establishes a secure FIPS connection with the agent. Core Services cannot communicate with security agents on iSeries systems when you enable FIPS mode functionality.

If you use a standalone AutoSync client, you must enable the client to communicate with Core Services. For more information about configuring the AutoSync client, see Section 8.2.2, “Connecting the AutoSync Client to Core Services in a FIPS-Enabled Environment,” on page 122.

10.5.1 Enabling FIPS Communication on the Operating System for the Console Computer

Enable FIPS communication on every computer hosting a Secure Configuration Manager console, including the Core Services computer.

To enable FIPS on the console operating system:

1. Open the Local Security Policy application in Administrative Tools.
2. Under Security Settings, expand **Local Policies**.
3. Click **Security Options**.
4. Open the policy for **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.
5. Click **Enabled**, and then click **Apply**.
6. Click **OK**.

10.5.2 Enabling Core Services to Communicate with Components in FIPS Mode

This section provides instructions for configuring Core Services to operate in FIPS-migration mode for FIPS communication with other Secure Configuration Manager components. For more information about the security agents communicating in FIPS mode, see the guides for each security agent.

NOTE

- Core Services cannot communicate with iSeries security agents when you enable FIPS mode functionality.
- If Core Services does not appear to be communicating with an agent in FIPS mode, refer to the `core.log` file in the `\Core Services` folder of the Secure Configuration Manager installation folder to verify that Core Services is in FIPS mode.

To enable FIPS communication on the Core Services computer:

1. Start the Core Services Configuration Utility in the NetIQ Secure Configuration Manager program folder.
2. On the Network tab of the Core Services Configuration Utility, enable FIPS mode by setting **Enable FIPS Support** to **true**.
3. Click **OK** to save the changes and close the utility.
4. Restart the NetIQ Core Services service.

11 Integrating Secure Configuration Manager with Sentinel

This chapter describes how Secure Configuration Manager is integrated with NetIQ Sentinel.

This integration helps the Sentinel administrators determine if their environment complies to configuration policy. Knowledge of compliance to policy in relation to activity on systems can benefit in the following ways:

- Record configuration compliance in line with system activity
- Inform administrators of compliance to configuration in times of anomalous activity
- Inform administrators if system activity resulted in changes affecting policy compliance

Integration of SCM with Sentinel enables SCM to send compliance information to Sentinel. SCM sends information to Sentinel as events, communicating if the system is in compliance, out of compliance, or unknown compliance.

SCM administrator configures what produces an event for any of the following:

- Risk score threshold reached
- Compliance threshold reached

The event that SCM sends to Sentinel contains applicable attributes of the endpoint known by SCM, such as asset name and IP address.

Assessment events generated in SCM are forwarded to Sentinel in “near real time”. The actual latency for events in Sentinel might be affected by factors such as network traffic and connectivity.

The events that SCM sends to Sentinel may or may not have a detailed report as an attachment, based on the configuration you have done in SCM. NetIQ recommends that you consider the estimate of 1.7MB per event to calculate the additional storage you might need in Sentinel for storing assessment events forwarded by SCM. For more information about Sentinel hardware requirements, see System Sizing Information in the *NetIQ Sentinel Installation and Configuration Guide*.

11.1 Configuring the Integration

To configure Sentinel integration with SCM:

1. Go to **Core Services Configuration Utility** and click the **Forward Assessment Report** tab.
2. Provide the following information:
   - **Forward Events of Assessment Result**: Select *Enabled* to enable sending assessment events to Sentinel.
   - **Destination Server**: Specify the Sentinel Server URL, which needs to be configured to receive assessment events.
   - **Destination Server Credentials**: Specify the following login credentials of the destination server:
     - **User Name**: Specify the user name for the destination server you have specified.
     - **Password**: Specify the password for the destination server you have specified.

NOTE: You must restart the Core Service if you change the above settings.

3 (Optional) Provide the following additional information. The default values will be considered if you do not provided any information in these fields.

- **Forward Assessment Events**: Select the component(s) on which assessment events should be sent. This drop-down list has three options - By Asset, By Policy, and By Asset and Policy. The default value is By Asset.
  - When you select **By Asset**, a report for every asset (for example, an endpoint) is sent to Sentinel. If you run a policy against 100 assets, 100 reports are sent.
  - When you select **By Policy**, a report is sent per policy template. If you run two policy templates against 100 assets in your system, two reports are sent, and each report consists of information about relevant assets.
  - When you select **By Asset and Policy**, reports are sent for both assets and policies.
- **Assessment Conditions to Forward**: The following are assessment conditions you can select, to forward events to the destination server:
  - **Enable Events for Compliant Results**: Select True to receive in-compliance assessment events.
  - **Enable Events for Out Of Compliance Results With**: Select an option in this drop-down list to notify as when you want to receive out-of-compliance assessment events. This list has the following options:
    - False: Select this option if you do not want to receive out-of-compliance assessment events.
    - Low Risk and Above: Select this option if you want to receive assessment events for any kind of risk.
    - Medium Risk and Above: Select this option if you want to receive assessment events only for medium risk and above.
    - High Risk: Select this option if you want to receive assessment events only for high-risk. This is the default option.

    See Section 4.1, “Understanding Security Checks,” on page 47 to understand how risk scoring done in security checks.
  - **Enable Events where Results are Incomplete**: Select *True* if you want to receive assessment events for unknown compliance.
- **Tenant Name**: If the destination server is in a multi-tenant environment, specify the department or the tenant name for which you want to send events.

4 Click **Apply** to apply the settings. You must restart Core Services, so that the updated settings are saved and applied.

5 In the SCM console, click **Go** > **Assessment Configuration**. In the Assessment Configuration Settings window, you can select the policy templates or the security checks for which assessment events must be sent to the destination server.

Additionally, When you run a policy template or a security check in SCM console, you can select the **Forward Assessment Report to Destination Server** option in the **Run Policy Template Wizard** to enable sending assessment events to the destination server.

11.2 Viewing Assessment Events in Sentinel

For information about settings required to enable Sentinel to receive assessment events from SCM, see Receiving Compliance Details from Secure Configuration Manager in the *NetIQ Sentinel Administration Guide*.

To view assessment events in Sentinel:

1. Log in to the Sentinel URL you have configured to receive assessment events from SCM:
   - **1a** The URL must be same as the URL you have specified in the **Destination Server** field in Step 2 in Section 11.1, "Configuring the Integration," on page 141. The URL must be in the `https://<Sentinel IP Address>:<Port>` format. For example, `https://255.0.0.0:1234`.
   - **1b** Log in to Sentinel using valid Sentinel user credentials.

   NOTE: You can also use the credentials you specified in the **Destination Server Credentials** fields in Step 2 in Section 11.1, "Configuring the Integration," on page 141 to log in to Sentinel. However, these credentials have administration privileges to enable configuration, and you do not need such privileges to view assessment events in Sentinel. NetIQ recommends that you create separate user accounts for SCM users who only need to be able to view events.
2. You can view assessment events received by SCM in Sentinel now. For more information, see Viewing Secure Configuration Manager Events and Compliance Details in the *NetIQ Sentinel User Guide*.

11.3 Configuring Sending Events in FIPS Mode

This section describes how to configure Sentinel integration when Sentinel, SCM, or both the Sentinel and SCM are in FIPS mode.

11.3.1 When Sentinel is in FIPS Mode

For information about FIPS mode configuration in Sentinel, see the Sentinel Documentation.

By default, FIPS mode enabled Sentinel uses NSS provider. So, to connect to the SCM server, you need to add the SCM server certificate to the NSS truststore of Sentinel.

To add the SCM server certificate to the NSS truststore of Sentinel:

1. Export the SCM certificate to Sentinel NSS truststore from `vtls.keystore` using `keytool`.
2. Import the SCM certificate to FIPS mode enabled Sentinel.

11.3.2 When SCM is in FIPS Mode

When SCM is in FIPS mode, SCM uses NSS provider. So, you need to import the Sentinel certificate to SCM NSS database.

To export a Sentinel Server certificate and import it to SCM Server:

1. Export the Sentinel web server certificate.
2. Import the certificate to SCM server.

11.3.3 When Both SCM and Sentinel are in FIPS Mode

If Sentinel and SCM are in FIPS mode, both use NSS provider. So, you need to import each application's certificate into the other application's NSS Keystore.

To import the SCM certificate to Sentinel:

1. Export the certificate from SCM NSS Store.
2. Enter Password or PIN for the NSS FIPS Certificate DB. You can also specify it in the **nss/keystore/password** field in the **Advanced** tab of the **Core Services Configuration Utility**.
3. Import the certificate to Sentinel server.
4. Set the trust flags.

To import the Sentinel certificate to SCM:

1. Export the certificate from Sentinel NSS Store.
2. Import the certificate to SCM.
3. Set the certificate flag.

12 Network Device Endpoint Importer Utility

The Network Device Endpoint Importer utility helps you to import network device endpoints to Secure Configuration Manager. You can add network device endpoints in the Network Device Endpoint Importer utility and import multiple endpoints to Secure Configuration Manager with a single click. This makes adding network device endpoints to Secure Configuration Manager easy, specially when you have a large number of endpoints in your network.

12.1 Working with Network Device Endpoint Importer Utility

The Network Device Endpoint Importer is a separate utility packaged with Secure Configuration Manger. To start working with the Network Device Endpoint Importer:

1. Go to the **Start** menu of your computer and select **Network Device Endpoint Importer** in your **Secure Configuration Manager** installation.
2. In the Login window, specify your SCM login credentials and the IP address and port number of SCM Core Services.
3. Click **Login**.

12.2 Adding Endpoints

To add a network device endpoint using the Network Device Endpoint Importer utility:

1. In the Network Device Endpoint Importer utility, click **File** > **New Endpoint** or click the **+** button.
2. In the Endpoint Name field, type a name for the endpoint you want to add.
3. In the endpoint properties table, verify or type the following required information:

Field	Description
Agent Name	Select the Windows agent to which you want to add the network device endpoint.
Endpoint Name	Specify a name for the endpoint.
Protocol	The type of protocol used to connect with the network device - Telnet or SSH.
Authentication Type	This field is displayed only if you have chosen SSH as the protocol. Options are Password and Key. Select Password if you require password-based SSH authentication; select Key if you require key-based SSH authentication.
Network Device Type	Type of the network device for which you are configuring this endpoint. This drop-down list has three options - IOS, JUNOS, and GENERIC. Select IOS if the network device is a Cisco device, JUNOS if it is a Juniper device, and GENERIC if it is any other device.
IP Address	IP address of the network device.

Field	Description
IP Port	The port through which the endpoint interacts with the network device.
User Name	User name to log in to the network device.
Password	This field is displayed only if you have selected Password as the authentication type. Enter the password of the network device.
Key	This field is displayed only if you have selected Key as the authentication type. Specify the private key file path.
Expect Script Name	This field is displayed only if you have selected Generic as the network device type. Specify the name of the scripting file that interacts with the network device.

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

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

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

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

5 To register the endpoint with SCM, select **True** in the Register field. Alternatively, you can select **Register All** to register all the endpoints you have added.

6 (Optional) To add the endpoint to a group, select **Add Endpoint to a Group** check box and then select an existing group or type a new group name to which the endpoint should belong.

In addition to the above process for adding endpoints, the following capabilities are provided, that make addition of endpoints easier:

- You can save the configuration of endpoints you want to add in a `.xml` or a `.csv` file, and then load the configuration file by clicking **File** > **Load Configuration** and selecting the file.

- You can save the configuration of the endpoint you have added, by clicking **File** > **Save Configuration**. This saves the configuration of the endpoint in a `.xml` or `.csv` file. You can use the same configuration in the future while adding endpoints, by using the **Load Configuration** option.

  NOTE: You can use the schema of the `.xml` file that you create here to create your own `.xml` files that contain endpoint configuration information. And then, you can use those configuration information files to add network device endpoints in future.

- You can clone an endpoint by clicking the **>** button. This creates a new endpoint with the same configuration as the endpoint you are cloning. You can then modify the configuration of the clones endpoint as required. This makes it easy to add endpoints.

12.3 Importing Network Device Endpoints to Secure Configuration Manager

To import all the network device endpoints to SCM, click **Import All**. you can view the log messages pertaining to the import operation in the Log Messages area. You will get a confirmation when the import operation completes successfully.

A Using the Lightweight UNIX Solution

The Lightweight UNIX solution lets you run built-in security checks or create custom checks for UNIX or Linux computers that *do not* have agents installed on them. UNIX or Linux computers that do not have agents are called **Lightweight UNIX computers**. You can perform these tasks on Lightweight UNIX computers for the most popular UNIX and Linux distributions, including distributions that are not currently supported by agents.

The Lightweight UNIX solution uses a single UNIX agent computer to act as a repository for audit data collected by a script. You run the data collection script on each Lightweight UNIX computer you want to audit, and then install the files generated by the script on a UNIX agent computer. The data collection script does not leave a footprint and allows you to perform security audits without making changes to the system. Many of the security checks for Lightweight UNIX computers are identical to the checks for UNIX agent computers, which helps you make accurate comparisons.

You can also run security checks for any computer that has a UNIX agent installed on it. Security checks for UNIX agent computers include audit reports and many other comprehensive security checks. You can also create custom checks for UNIX agent computers. For more information about security checks, see Section 4.1, “Understanding Security Checks,” on page 47. For more information about custom checks, see Section 6.4.3, “Creating Custom Security Checks,” on page 99.

A.1 Lightweight UNIX Solution Checklist

The following checklist provides an overview of how to obtain data and run a security check for a Lightweight UNIX computer.

	Checklist Items
❑	1. Run the data collection script on the Lightweight UNIX computer you want to audit. See Section A.2, “Running the Data Collection Script,” on page 150.
❑	2. Transfer the Lightweight UNIX data files to a UNIX agent computer.See Section A.3, “Transferring the Data Files,” on page 150.
❑	3. Install the Lightweight UNIX data files on the UNIX agent computer. See Section A.4, “Installing the Data Files,” on page 151.
❑	4. Create a Lightweight UNIX endpoint on the UNIX agent computer in Secure Configuration Manager. See Section 2.5, “Working with Endpoints,” on page 32.
❑	5. Run a security check on the Lightweight UNIX endpoint. See Section 4.1, “Understanding Security Checks,” on page 47.

After setting up the endpoint, you can repeat the first three steps in the checklist to provide current data for reports. You can collect, transfer, and install data as often as you want, as long as you install the data files to the same UNIX agent computer each time. If you change the UNIX agent computer

where you install the data files, you must set up a new Lightweight UNIX endpoint in Secure Configuration Manager. For more information about setting up an endpoint, see Section 2.5, “Working with Endpoints,” on page 32.

A.2 Running the Data Collection Script

To collect Lightweight UNIX data for reports, run the data collection script on the Lightweight UNIX computer you want to audit. The data collection script creates Lightweight UNIX data files containing audit data. You will need the root password for the Lightweight UNIX computer that you want to audit, and a copy of the `build_luau_files` script that is located on the UNIX agent CD-ROM.

NOTE: Ensure that you have adequate disk space on the Lightweight UNIX computer before running the data collection script. The data collection script creates data files that require an average of 150 bytes for each file or directory in the file system. For example, if the file system contains 100,000 files or directories, the data collection script requires at least 15 MB of disk space.

To collect the required data:

1. Log on to the Lightweight UNIX computer as `root`, or `su` to root.
2. Create a temporary directory by entering the following:

   ```
   mkdir /tmp/luautmp
   ```

3. Change directories to the temporary directory by entering the following:

   ```
   cd /tmp/luautmp
   ```

4. Copy the `build_luau_files` script to the temporary directory. For example, if the script is on a floppy disk, enter the following and replace */mnt/floppy* with the floppy mount point:

   ```
   cp /mnt/floppy/build_luau_files ./
   ```

5. Make sure the build files script has proper permissions by entering the following:

   ```
   chmod 555 ./build_luau_files
   ```

6. Run the script by entering the following:

   ```
   ./build_luau_files
   ```

7. Enter `./` to create the data files in the current directory.
8. Enter any additional information the script requires to build the data files. You may be prompted to enter the path to certain files and directories. The build cycle is complete when the prompt reappears.
9. Log off the Lightweight UNIX computer.

A.3 Transferring the Data Files

After running the data collection script on the Lightweight UNIX computer, transfer the Lightweight UNIX data files to a UNIX agent computer. Consider selecting one UNIX agent computer to use as the data file repository for all Lightweight UNIX computers.

Using one UNIX agent computer simplifies the process of archiving all data files for your records and repeating data collection for reports. As part of the process of supporting Lightweight UNIX computers, you will set up a Lightweight UNIX endpoint and associate it with the UNIX agent

computer where you install Lightweight UNIX data files. You can collect, transfer, and install Lightweight UNIX data files as many times as you want. However, you must install the files on the same UNIX agent computer where you specify the Lightweight UNIX endpoint. If you change the UNIX agent computer on which you install the data files, you will need to set up a new Lightweight UNIX endpoint.

You can transfer the `.txt` files to a UNIX agent computer by FTP, floppy disk, or another method. It does not matter where you put the data files on the UNIX agent computer, but you may want to put them in an archive directory for your records.

After you transfer the data files, you can delete them from the Lightweight UNIX computer. To delete the data files, log on to the Lightweight UNIX computer and enter the following:

```
rm -rf /tmp/luautmp
```

A.4 Installing the Data Files

After transferring the Lightweight UNIX data files, run a script to install them on the UNIX agent computer you selected to be the Lightweight UNIX data file repository. Installing the Lightweight UNIX data files makes them available for security checks.

To install the Lightweight UNIX data files:

1. Log on to the UNIX agent computer on which you want to install the data files.
2. Change directories to the *$os*`/bin` directory.

   For example, `cd /usr/vsaunix/Linux/bin`.
3. Run the installation script by entering the following:

   ```
   ./install_luau
   ```
4. Enter the path to the floppy disk or the directory where you copied the data files. The data files are installed when the prompt reappears.
5. Log off the UNIX agent computer.

A.5 Running Security Checks for Lightweight UNIX

Before running a security check against Lightweight UNIX data you installed on a UNIX agent computer, create a Lightweight UNIX endpoint. For more information about creating an endpoint, see Section 2.5, “Working with Endpoints,” on page 32.

After you create the endpoint, you can run security checks as you would for any other endpoint. For more information about running security checks, see Section 4.3, “Running Security Checks and Policy Templates,” on page 50. You can also create custom checks for Lightweight UNIX computers. For more information about custom checks, see Section 6.4.3, “Creating Custom Security Checks,” on page 99.

B Disaster Preparation and Recovery

As your organization grows and changes, you perform many of the following activities in Secure Configuration Manager:

- Customize settings in Core Services
- Add agents and endpoints to the asset map in the console
- Run reports against your IT assets
- Update security knowledge through AutoSync and custom security checks
- Create, modify, and delete user profiles

Each of these activities affects the information stored in the Secure Configuration Manager database, Core Services, and the consoles. If your organization experiences a hardware or software problem, you could lose these incremental revisions. Sometimes, you can reinstall software on a server. On the other hand, a catastrophic failure might require you to restore backed up databases and Secure Configuration Manager components at a different site, and then reapply customized settings.

In general, organizations create a business continuity plan to ensure functionality during and after a disaster. Organizations demonstrate different levels of resilience when responding to and recovering from catastrophic events. Most business continuity plans account for four facets of organizational resilience: preparedness, protection, response, and recovery. This chapter helps you prepare for an infrastructure failure and determine whether restoring that infrastructure can be completed within company goals for an acceptable recovery time.

B.1 Disaster Preparation

When establishing your disaster preparedness process, you should consider which incremental changes in Secure Configuration Manager you want to maintain. For example, if you add, delete, or move a large volume of endpoints each month, you probably also should back up the database just as frequently. If you run reports daily, you should consider how many days' worth of data you can afford to lose.

This section provides steps to help you maintain current data and settings for a faster recovery if your organization experiences a catastrophic event.

B.1.1 Disaster Preparation Checklist

The following checklist provides an overview of activities you should regularly perform to maintain current copies of your Secure Configuration Manager data and settings.

	Checklist Items
❑	1. Back up the Secure Configuration Manager database. See Section B.1.2, "Backing Up the Secure Configuration Manager Database," on page 154 and Chapter 9, "Maintaining the Secure Configuration Manager Database," on page 129.
❑	2. Maintain a copy of the service pack and hotfix levels for Secure Configuration Manager components. See "Storing Version Level Information" on page 155.

	Checklist Items
❑	3. Maintain a copy of the Core Services folder. See “Storing Core Services Configuration Settings” on page 155.
❑	4. Maintain a copy of the domain keys. See “Storing a Copy of the Domain Keys” on page 155.
❑	5. Maintain a copy of the Secure Configuration Manager license keys. See “Storing a Copy of the Product License Keys” on page 156.
❑	6. Maintain a snapshot of your asset map. See “Exporting the Asset Map” on page 156.
❑	7. Maintain a snapshot of your managed groups. See “Exporting Managed Groups Data” on page 156.

B.1.2 Backing Up the Secure Configuration Manager Database

Once you have an idea of the frequency with which you should back up your data, you should consider other factors. The volume of data you require may dictate the time frame in which you can run a backup. Data volume also affects the method for backups. For more information about grooming and backing up your database, see Chapter 9, “Maintaining the Secure Configuration Manager Database,” on page 129.

SQL Server provides several types of backups that can be combined to serve a variety of requirements.

Full Backup

A full backup is the simplest type of SQL Server backup. When you run a full backup, SQL Server creates a copy of all data in the database, tables, indexes, and logs for transactions occurring during the backup. Full backups can be performed while the database is in use. Full backups can require a lot of disk space and time to complete, depending on the volume of data you want to save.

Differential Backup

The differential backup copies pages that have changed since the previous backup, plus the parts of the log necessary to retain data integrity for transactions during the backup. You can use the differential backup between full backups when you may not have time or disk space to perform a full backup.

Transaction Log Backup

The SQL Server transaction log contains almost every change that occurs within the database and aids in recovering the database. The log backup copies the database transaction log file and can be run during a full or differential backup. To protect your data and prevent the transaction log from filling, you should regularly run a log backup.

B.1.3 Storing Product Configuration Information

Secure Configuration Manager stores a variety of settings you customize upon installation. These settings may change over time. To ensure rapid recovery, NetIQ recommends regularly saving copies of your product configuration settings and version levels for the Secure Configuration Manager components.

Storing Version Level Information

To ensure that you can restore the Secure Configuration Manager components to the current hotfix and service pack version levels, you should regularly export a copy of the patch summary information.

To store version level information:

1. On the Help menu, select **About NetIQ Secure Configuration Manager**.
2. Click **Export**.
3. Enter a file name, and then click **Save**.

Storing Core Services Configuration Settings

Core Services contains a variety of special settings to ensure communication among Secure Configuration Manager components, agents, and your IT environment. Core Services also stores custom information such as email addresses for reports and compliance alerts and settings. For faster product recovery, you should maintain a copy of Core Services settings.

To store current Core Services settings, regularly back up the Core Services folder to your disaster recovery location. By default, this folder is located in the `Program Files\NetIQ\Secure Configuration Manager` folder.

Storing a Copy of the Domain Keys

Core Services uses a set of authentication keys, called **domain keys**, for shared secret authentication with the registered Windows, UNIX, and iSeries agents. When you move the Secure Configuration Manager infrastructure to a new system after a disaster, you must transfer the domain keys to enable the new Core Services to access agents registered to the previous Core Services. Secure Configuration Manager requires a password for importing the domain keys from a different Core Services computer.

NOTE: ensure that you retain a copy of the password used to access the `ExportDomainKeys.bat` file. The file does not allow any alternative methods of access.

To back up the domain keys:

1. On the Core Services computer that registered the Secure Configuration Manager 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 in which to store the domain keys.

   By default, Secure Configuration Manager saves the file in the same folder. To save the file to another location, enter a full path and file name.
3. Press Enter.

4 At the Password prompt, type a password, and then press Enter.

5 Store the specified password and saved file in your disaster recovery location.

Storing a Copy of the Product License Keys

Product license keys enable Secure Configuration Manager to function in your environment. NetIQ recommends you maintain a copy of the product license keys in your disaster recovery location. The License Keys tab in the Core Services Configuration Utility contains all current product license keys. You can copy and paste the displayed information in a separate file. You can also print a copy of your license status. In the Secure Configuration Manager console, expand **Tools > License Status**, and then click **Print**.

B.1.4 Saving Asset Map Data

If you reinstall Secure Configuration Manager after a catastrophic event, you must re-register managed systems, agents, and endpoints with the new Core Services. To ensure a more efficient return to operation, you should maintain copies of your current asset map and managed groups.

Exporting the Asset Map

Regularly exporting the asset map ensures that you have a current snapshot of all systems, agents, and endpoints to use as a visual reference when rebuilding the map in the recovery stage. You can save the exported file in `.xlsx`, `.html`, `.txt`, or `.xml` format.

To export the asset map:

1 On the Tools menu, click **Admin Reports Wizard**.

2 In the Available Reports list, click **All Systems, Agents, and Endpoints**.

3 Click **Run Report**.

4 In the Results window, click **Export**.

5 In the Save As window, navigate to the location where you want to save the exported file.

6 Enter a file name.

7 Select the file type, and then click **Save**.

Exporting Managed Groups Data

During the recovery stage, you might want to return endpoints to their original managed groups. Secure Configuration Manager enables you to export a snapshot of each managed group for future reference. You can save the exported file in `.xlsx`, `.html`, `.txt`, or `.pdf` format.

To export managed group data:

1 In the IT Assets tree pane, expand **Managed Groups > My Groups**.

2 Under My Groups, select the group whose data you want to export.

3 Right-click the group in the IT Assets tree, and then click **Export List**.

4 In the window, navigate to the location where you want to save the exported file.

5 Enter a file name.

6 Select the file type, and then click **Save**.

B.2 Disaster Recovery

Disaster recovery can range from re-registering agents and endpoints lost during a server crash to a complete restoration of your IT infrastructure. This section provides procedures for recovering the Secure Configuration Manager components, especially the database, connecting to your IT assets, and restoring configuration settings.

NOTE: This section assumes you will install the same version of Secure Configuration Manager as you had before the infrastructure failure.

B.2.1 Disaster Recovery Checklist

The following checklist provides an overview of the disaster recovery steps.

	Checklist Items
❑	1. If you must move to a new infrastructure, install the Secure Configuration Manager components. See Section B.2.2, “Reinstalling Secure Configuration Manager,” on page 157.
❑	2. If you reinstalled a Secure Configuration Manager component, reapply service packs and hotfixes. See Section B.2.3, “Applying Service Packs and Hotfixes,” on page 157.
❑	3. If you reinstalled the database, restore the backup Secure Configuration Manager database. See Section B.2.4, “Restoring the Secure Configuration Manager Database,” on page 158.
❑	4. If you reinstalled Core Services, restore the backup Core Services folder. See Section B.2.5, “Restoring Your Core Services Settings,” on page 158.
❑	5. If you reinstalled Core Services or the database, enable the database and Core Services to communicate with users.See Section B.2.6, “Linking Users to the Secure Configuration Manager Database,” on page 159.
❑	6. If you reinstalled Core Services, restore the domain keys. See Section B.2.7, “Restoring Domain keys,” on page 159.
❑	7. If you reinstalled Core Services, add additional license keys. See Section B.2.8, “Restoring License Keys,” on page 160.
❑	8. If you reinstalled Core Services, re-register your agents and endpoints. For more information, see Section B.2.9, “Re-Registering Agents and Endpoints,” on page 160.

B.2.2 Reinstalling Secure Configuration Manager

In some recovery situations, you will need to reinstall the Secure Configuration Manager consoles, database, and Core Services. Follow the installation instructions provided in the *Installation Guide for NetIQ Secure Configuration Manager*.

B.2.3 Applying Service Packs and Hotfixes

To ensure that the Secure Configuration Manager components synchronize properly after you reinstall, you must restore the consoles, database, and Core Services to the same hotfix and service pack version levels as were in use before the disaster. For more information about exporting a patch level summary, see “Storing Version Level Information” on page 155.

NOTE

- All Secure Configuration Manager components must be restored to the same release level, such as version 5.8.1.
- The security agents do not need to be at the same release level as Core Services.

B.2.4 Restoring the Secure Configuration Manager Database

If an infrastructure failure causes your organization to move to a new location or servers, you will need to restore the Secure Configuration Manager database. This process assumes you have a current, usable backup of the database. For more information about backing up the database, see Chapter 9, “Maintaining the Secure Configuration Manager Database,” on page 129. You must have administrative permissions to restore the database. You must install the generic Secure Configuration Manager database before restoring your backup data.

To restore the database:

1. Log on with an Administrator account to the computer where you want to restore or you installed the Secure Configuration Manager database.
2. (Conditional) If you have not installed the Secure Configuration Manager database in the new location, complete the instructions in the Secure Configuration Manager installation wizard for database installation.
3. (Conditional) If the NetIQ Core Services service is running, stop the service.
4. Restore the backup Secure Configuration Manager database.
5. Restart the NetIQ Core Services service.

B.2.5 Restoring Your Core Services Settings

If you have saved a current copy of the Core Services folder, you can copy the `mk.options` and `mk.properties` files from the saved folder to the same location where you reinstalled Secure Configuration Manager. By default, the Core Services folder is located in the `Program Files\NetIQ\Secure Configuration Manager` folder.

NOTE: Your backup Core Services folder and contents must be at the same hotfix and service pack level as the restored Core Services component for which you want to replace the `mk.options` and `mk.properties` files.

To restore the Core Services folder:

1. Log on with an Administrator account to the Core Services computer.
2. (Conditional) If the NetIQ Core Services service is running, stop the service.
3. Copy the `mk.options` and `mk.properties` files from your saved Core Services folder to the `Program Files\NetIQ\Secure Configuration Manager\Core Services` folder.
4. Click **Yes** on the confirmation message.
5. Restart the NetIQ Core Services service.

B.2.6 Linking Users to the Secure Configuration Manager Database

After database restoration you must link the existing Secure Configuration Manager console and VigilEnt Service users to the database and the database to Core Services.

To link users to the database and Core Services:

1. Log on with an Administrator account to the computer where you installed Core Services.
2. (Conditional) If the NetIQ Core Services service is running, stop the service.
3. Open the `PasswordUtility.exe` file. By default, this file is located in the `C:\Program Files\NetIQ\Secure Configuration Manager\Core Services\bin` folder.

   WARNING: Do not modify the `PasswordUtility.exe` file except as directed in these steps. Revising this file can adversely affect Core Services performance.
4. On the Welcome screen, click **Next**.
5. Type the SQL Server name, and then click **Next**.
6. Select the type of authentication used to connect to SQL Server, and then click **Next**.
7. In the **Login Name** field, type the same login account as used for installing the database, and then click **Next**.

   NOTE: Secure Configuration Manager also uses the Login Name for the administrative account for accessing Core Services.
8. In the **Password** and confirmation fields, enter a temporary password, and then click **Next**.
9. Click **Next**, and then click **Finish**.
10. Restart the NetIQ Core Services service.

B.2.7 Restoring Domain keys

Secure Configuration Manager generates a set of authentication keys called **domain keys**. Core Services uses the domain keys to authenticate communication with registered agents. When you move the Secure Configuration Manager infrastructure to a new system after a disaster, you must transfer the domain keys to enable the new Core Services to access agents registered to the previous Core Services.

This procedure assumes you have a backup copy of the domain keys. You must perform this procedure on each Core Services computer that requires access to the agents registered to the original Core Services.

To restore domain keys:

1. Run the `ImportDomainKeys.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 where the domain keys are stored and press Enter.
3. At the Password prompt, type the password to access the domain keys, and then press Enter.
4. Restart the NetIQ Core Services service.

B.2.8 Restoring License Keys

When you install Secure Configuration Manager, the installation program prompts you to enter the license key. Some organizations use more than one license key, which must be entered after installation.

To add license keys:

1. Open the Core Services Configuration Utility.
2. Click the License Keys tab.
3. In the **Additional Secure Configuration Manager License Keys** field, type the extra license keys separated by commas.
4. Restart the NetIQ Core Services service.

B.2.9 Re-Registering Agents and Endpoints

Once you have the database and Core Services running, you can re-register your existing agents and endpoints. For more information about discovering and managing systems, see Section 2.2, “Building and Managing Your Asset Map,” on page 21.

To ensure that you restore all systems, agents, and endpoints in their previous managed groups in the Secure Configuration Manager console, refer to the asset status files you most recently exported. For more information about exporting asset and managed group data, see Section B.1.4, “Saving Asset Map Data,” on page 156.

C Checklists

This section provides links to checklists that can guide you through the complex processes associated with assessing and maintaining asset configuration security. These checklists help you identify and review the related concepts and considerations.

If you want to...	Review this check list
Review the workflow for the audit and evaluation process	Auditing and Evaluation Process Workflow
Organize your asset map of groups, systems, agents, and endpoints	Asset Map Checklist
Define and manage security controls on the console	Console Security Checklist
Edit existing or create new security checks	Checklist for Editing and Creating Security Checks
Review the workflow or maintaining your Secure Configuration Manager database	Database Maintenance Checklist
Review the process for run a security check for a Lightweight UNIX computer	Lightweight UNIX Solution Checklist
Review the steps for disaster preparation	Disaster Preparation Checklist
Review the steps for disaster recovery	Disaster Recovery Checklist

D Port Usage

The following table summarizes the ports used by Secure Configuration Manager to communicate with agents and other NetIQ security products.

Table D-1 *Ports used by Secure Configuration Manager components*

Port Number	Component Computer	Port Use
700	Secure Configuration Manager Windows Agent (Deployment Agent)	Used by the Deployment Agent and remote computer during deployment.
1433	Database computer	Used by Microsoft SQL Server or SQL Server Express if you are using a default instance of SQL Server. 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 computer	Used by Core Services as a service port to listen for communication from the Secure Configuration Manager Windows Agent when both the agent and Core Services are in FIPS mode. This port requires, at a minimum, Secure Configuration Manager 5.9 and Secure Configuration Manager Windows Agent 5.9 with FIPS mode enabled on both the Core Services and Windows agent computers.
1622	Secure Configuration Manager Windows Agent	Used by the Secure Configuration Manager Windows Agent as a service port 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 as a service port to listen for communications from Core Services. Core Services uses this port to run reports and actions. This port uses bi-directional communications.
1622	userv	Used by the UNIX audit and secure agent as a service port to listen for communications from Core Services. Core Services uses this port to run reports and actions. This port uses bi-directional communications.

Port Number	Component Computer	Port Use
1626	Core Services computer	Used by Core Services to communicate with SSL (Secure Sockets Layer) agents. SSL agents include Windows (5.8 or earlier), UNIX (7.1, at a minimum), and iSeries (8.0, at a minimum) 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. Used by Core Services (version 5.8 or 5.9) to listen for communications from the Security Agent for Windows 5.8.2 or earlier.
1627	Core Services computer	Used by Core Services to listen for communication from the Windows or UNIX security agent. This port requires Secure Configuration Manager 5.9 and Secure Configuration Manager Windows Agent 5.9, at a minimum.
8044	Core Services computer	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.