NetIQ® Secure Configuration Manager™

User's Guide

July 2018

NetIQ

Legal Notice

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

Copyright © 2018 Micro Focus or one of its affiliates. All Rights Reserved.

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

Contents

About This Book 11

1 Introduction 13

Understanding Secure Configuration Manager Components . . . 13
Understanding Asset Categories . . . 15
Assets . . . 15
Agents . . . 15
Endpoints . . . 16
Groups . . . 16
Auditing and Evaluation Process Workflow. . . . 17
Understanding the Tools for Auditing Assets. . . . 18
Understanding Compliance Evaluation Tools . . . 19
Listing Reports, Actions, and Security Checks . . . 21

Part I Discovering and Managing Your IT Assets 23

2 Building Your Asset Map 25

Checklist for Building Your Asset Map . . . 25
Understanding Managed and Unmanaged Assets . . . 26
Adding Known, Unmanaged Assets . . . 26
Manually Adding Known Assets . . . 26
Using a Formatted File to Add Known Assets . . . 27
Discovering Unmanaged Assets in Your Environment . . . 27
Manually Discovering Unmanaged Assets. . . . 28
Automatically Discovering Unmanaged Assets . . . 28
Scheduling the Discovery Process. . . . 29
Deploying Windows Agents to the Managed Assets. . . . 30
Registering Managed Assets . . . 31
Registering an Agent Manually . . . 31
Registering an Endpoint. . . . 31
Adding Endpoints to Managed Assets . . . 32
Adding Known Endpoints to an Agent . . . 32
Discovering Endpoints on Managed Assets. . . . 33
Adding Discovered Endpoints to a Managed Asset . . . 34
Adding Network Device Endpoints. . . . 34

3 Managing Your Assets 37

Managing Asset Properties. . . . 37
Managing Your Agents . . . 37
Ensuring an Agent's Efficiency. . . . 38
Checking an Agent Heartbeat . . . 38
Updating Windows Agent Software . . . 38
Managing Your Endpoints. . . . 39
Managing Endpoints without Installing an Agent . . . 39
Assigning Importance to Endpoints . . . 39
Organizing Endpoints into Groups . . . 40
Creating a Managed Group . . . 41

Moving Existing Endpoints into Groups . . . 41
Removing Managed Assets . . . 42
Removing an Endpoint from an Agent . . . 42
Removing Agents . . . 42
Removing a Managed Asset . . . 43
Reporting Asset Map Information . . . 44

Part II Auditing Your Managed Assets 45

4 Using Security Checks to Assess Assets 47

Understanding Security Checks . . . 47
Understanding How Agents Identify Data to Collect . . . 49
Understanding Security Check Components . . . 49
Security Check Categories . . . 50
Security Check Filters . . . 50
Security Check Properties . . . 55
Understanding Risk Scoring . . . 56
Scoring Method . . . 56
Threat Factors . . . 57
Expected Number of Rows Returned . . . 57
Importance Factor . . . 58
Example of Risk Scoring . . . 59
Risk Scoring Distribution . . . 59
Modifying or Creating Custom Security Checks . . . 60
Checklist for Editing and Creating Security Checks . . . 60
Modifying Built-in Security Checks . . . 61
Creating Custom Security Checks . . . 61
Working with the Generic Network Device Security Check . . . 63
Custom Security Check Examples . . . 64
Accounts with Passwords More than 60 Days Old . . . 64
Kernel Parameters . . . 65
Registry Keys Modified Since Date . . . 66
Password Policy Violations . . . 67
Suspicious User . . . 68
Running Security Checks . . . 69
Web Console - Running Security Checks . . . 70
Windows Console - Running Security Checks . . . 70

5 Using Policy Templates to Assess Assets 71

Understanding Policy Templates . . . 71
Modifying and Creating Policy Templates . . . 72
Using Security Check Instances . . . 72
Translating a Technical Standard to a Policy Template . . . 73
Modifying Built-in Policy Templates . . . 74
Creating a Custom Policy Template . . . 74
Running Policy Templates . . . 75
Web Console - Running Policy Templates . . . 76
Windows Console - Running Policy Templates . . . 76

6 Configuring Assessment Options 77

Automating Out-of-Compliance Notifications . . . 77
Sending Email Notifications to Users . . . 77
Sending Email Notifications to Change Management Systems . . . 78
Running Assessments on a Schedule . . . 78

Web Console - Scheduling a Run . . . 78
Windows Console - Scheduling a Run . . . 78
Enabling Report Distribution . . . 79
Sharing Reports from the Web Console . . . 79
Distributing Reports to a File or Share . . . 79
Distributing Reports to an Email Recipient . . . 80

Part III Identifying Security Risks in Your Environment 83

7 Reviewing Results of Individual Runs 85

Viewing Assessment Results . . . 86
Understanding Assessment Results . . . 86
Exporting Assessment Results . . . 87
Re-assess Failed Endpoints . . . 88
Using the Web Console for Evaluation . . . 88
Using the Asset Compliance View for Evaluation . . . 89
Changing Asset Compliance View Settings . . . 91
Viewing Compliance Information . . . 91
Viewing Risks Information . . . 93
Viewing Trending Information . . . 94
Viewing Systems Information . . . 95
Viewing Summary Information . . . 97
Distributing Asset Compliance Information . . . 98
Using the Secure Configuration Manager Dashboard for Evaluation . . . 99
Accessing the Dashboard . . . 100
Viewing the Secure Configuration Manager Dashboard . . . 100
Viewing the Risk Compliance Dashboard . . . 102
Viewing the System Compliance Dashboard . . . 103
Viewing the Technical Compliance Dashboard . . . 103
Customizing the Dashboard . . . 104
Screen Capturing and Report Sharing . . . 105

8 Using Dynamic Reports to Evaluate Endpoints 107

Checklist for Using Dynamic Reports to Evaluate Assets . . . 107
Building Dynamic Reports . . . 108
Evaluating Endpoints with a Dynamic Report . . . 108
Snapshot Report - Evaluating Your Endpoints . . . 108
Compliance Report - Evaluating Your Endpoints . . . 108
Risk Report - Evaluating Your Endpoints . . . 109

9 Excluding Data from Runs and Reports 111

Excluding Values from a Run . . . 111
Using Saved Lists in an Existing Security Check . . . 112
Importing Saved Lists . . . 112
Exporting Saved Lists . . . 113
Excluding Data from Report Results . . . 113
Allowing Users to Create or Manage Exceptions . . . 114
Excepting Endpoints or Groups from a Policy Template Run . . . 115
Excepting Specific Data Returned by a Security Check . . . 116
Excepting all Data Returned by a Security Check . . . 117
Avoiding the Creation of Duplicate or Similar Batch Exceptions . . . 118
Requiring Approval before Applying Exceptions . . . 119
Applying Exceptions . . . 120
Editing an Exception . . . 121

Deleting an Exception . . . 121
View the Status of All Exceptions . . . 122
Enabling Managed Groups to Inherit Parent Group's Exceptions . . . 122

10 Comparing Results of Assessments 123

Using a Dynamic Report to Compare Endpoints . . . 123
Running Reports from the Database . . . 124
Comparing Security Check Results for Two Endpoints . . . 125
Comparing Policy Template Results . . . 125
Filtering a Delta Report . . . 126
Scheduling a Delta Report . . . 127
Distributing Delta Reports to a File Share or Folder . . . 128
Distributing Delta Reports to an Email Recipient . . . 129
Exporting a Delta Report . . . 130
Exporting a Full Delta Report . . . 130
Exporting Delta Report Data . . . 130

11 Predicting Vulnerability and Compliance Problems 133

Part IV Customizing Secure Configuration Manager 135

12 Customizing Secure Configuration Manager 137

Creating and Applying Tags . . . 137
Creating Custom Tasks and Reports . . . 137
Creating Custom Tasks . . . 138
Creating Groups of Custom Tasks . . . 138
Changing the Logo on the Report . . . 139
Customizing the Job Queues . . . 139
Setting the Retention Period . . . 140
Using Folders to Organize Completed Jobs . . . 140
Customizing Core Services . . . 141
Accessing the Advanced Tab . . . 141
Enabling Event Logging . . . 141
Enabling Interim Local Storage of Microsoft Excel Reports . . . 142
Enabling the Ability to Distribute Reports Only if the Score Is Greater Than Zero . . . 142
Configuring Scheduled Jobs Behavior when Core Services Restarts after a Downtime . . . 142
Enabling FIPS Communication . . . 143
Enabling FIPS Communication on the Operating System for the Console Computer . . . 143
Enabling Core Services to Communicate with Components in FIPS Mode . . . 143

13 Configuring the Consoles and Dashboard 145

Modifying the Session Timeout Settings . . . 145
Configuring the Web Console . . . 145
Ensuring Web Console Performance . . . 145
Launching the Dashboard from the Web Console . . . 145
Allowing Users to Batch-create Exceptions . . . 146
Logging Web Console Activity . . . 146
Configuring the Windows Console . . . 146
Changing the View of the Asset Map . . . 146
Modifying Windows Console Settings . . . 146
Improving Console Performance . . . 147
Configuring the Web-based and Asset Compliance Content . . . 147
Configuring Web Services . . . 148

Configuring Data Settings . . . 148
Setting up the Dashboard for Your Users . . . 149
Working with Authorization Settings . . . 149
Working with Geolocation Settings. . . . 149
Working with General Dashboard Settings . . . 150

14 Setting Security on the Secure Configuration Manager Console 153

Console Security Checklist . . . 153
Understanding Console Security . . . 154
Understanding Console Users . . . 154
Understanding Console Administrators . . . 154
Understanding Console User and Administrator Auditing . . . 155
Managing User Authentication . . . 155
Implementing External Authentication . . . 156
Configuring a Secure LDAP Authentication Source . . . 157
Managing Password Policy . . . 157
Managing Roles . . . 158
Default Roles . . . 158
Creating, Modifying, and Deleting Roles . . . 159
Assigning Session Limit to Roles . . . 159
Managing Permissions . . . 160
Resolving Permission Conflicts and Inheritance . . . 161
Modifying Permission Assignments . . . 162
Managing Console Users . . . 162
Creating a Console User . . . 163
Assigning Roles to a Console User . . . 163
Assigning Permissions to a Console User . . . 163
Working with Console User Accounts . . . 163

Part V Integrating with a SIEM Solution 165

15 Secure Configuration ManagerPreparing for Integration 167

Understanding Integration with a SIEM Solution . . . 167
Understanding the Component Architecture . . . 168
Understanding Data Storage Requirements . . . 168
Secure Configuration ManagerConfiguring for SIEM Integration. . . . 169
Configuring the Basic Settings for SIEM Integration . . . 169
Adding the SIEM Server to Core Services . . . 170
Specifying the Assessments to Include in Event Data . . . 170
Customizing the Event Data Sent to the SIEM Server . . . 170

16 Secure Configuration ManagerIntegrating with ArcSight 173

Configuring ArcSight . . . 173
Secure Configuration ManagerViewing Raw Events in ArcSight . . . 173
Viewing the ArcSight Dashboard. . . . 173
Secure Configuration ManagerGenerating Alerts on Events . . . 174

17 Integrating Secure Configuration Manager with Sentinel 175

Sending Events in FIPS Mode . . . 175
Sentinel is in FIPS Mode . . . 175
Secure Configuration Manager is in FIPS Mode . . . 176
Secure Configuration ManagerBoth and Sentinel are in FIPS Mode . . . 176
Viewing Assessment Events in Sentinel . . . 177

18 Integrating Secure Configuration Manager with Splunk 179

Configuring Splunk for Integration . . . 179
Secure Configuration ManagerViewing Raw Events in Splunk . . . 179
Viewing the Splunk Dashboard . . . 179
Secure Configuration ManagerGenerating Alerts on Events . . . 180

Part VI Maintaining Secure Configuration Manager 181

19 Maintaining Your Security Knowledge 183

Understanding the AutoSync Components . . . 184
Configuring a Standalone AutoSync Client . . . 184
Connecting the AutoSync Client to Core Services . . . 184
Connecting the AutoSync Client to Core Services in a FIPS-Enabled Environment . . . 185
Connecting to the AutoSync Server through Proxy . . . 185
Manually Checking for New Security Knowledge . . . 186
Scheduling Checks for New Security Knowledge . . . 186
Applying AutoSync Updates . . . 187
Updating Agent Content . . . 187
Updating Agent Content During a Security Check Run . . . 187
Scheduling Agent Content Updates . . . 188
Manually Updating Agent Content . . . 188
Understanding AutoSync Archive . . . 189
Archiving Unapplied Updates . . . 189
Restoring Archived Updates . . . 189
Viewing the History of an Archived Update . . . 190

20 Maintaining the Secure Configuration Manager Database 191

Database Maintenance Checklist . . . 191
Required Database Permissions and Settings . . . 192
How the Secure Configuration Manager Database Works . . . 193
Developing a Database Maintenance Strategy . . . 194
Identifying a Backup and Archive Plan . . . 194
Backing Up the Secure Configuration Manager Database . . . 194
Grooming the Secure Configuration Manager Database . . . 195
Identifying the Appropriate Recovery Model . . . 196

21 Disaster Preparation and Recovery 197

Disaster Preparation . . . 197
Disaster Preparation Checklist . . . 198
Backing Up the Secure Configuration Manager Database . . . 198
Storing Product Configuration Information . . . 199
Saving Asset Map Data . . . 200
Disaster Recovery . . . 201
Disaster Recovery Checklist . . . 201
Reinstalling Secure Configuration Manager . . . 202
Applying Service Packs and Hotfixes . . . 202
Restoring the Secure Configuration Manager Database . . . 202
Restoring Your Core Services Settings . . . 203
Linking Users to the Secure Configuration Manager Database . . . 203
Restoring Domain keys . . . 204
Restoring License Keys . . . 204
Re-Registering Agents and Endpoints . . . 204

Part VII Appendices 205

A Using the Lightweight UNIX Solution 207

Lightweight UNIX Solution Checklist . . . 207
Running the Data Collection Script . . . 208
Transferring the Data Files . . . 209
Installing the Data Files . . . 209
Running Security Checks for Lightweight UNIX . . . 209

B Working with Baselines 211

Understanding Baselines . . . 211
Understanding Baseline Permissions . . . 211
Creating and Managing Baselines . . . 212
- Working with Baseline Criteria . . . 213
- Working with Baseline Collections . . . 216
- Establishing a Baseline . . . 217
- Running a Baseline Comparison Check . . . 218
- Scheduling a Baseline Comparison Check . . . 219
- Deleting a Baseline . . . 219
- Updating a Baseline . . . 220
- Creating a List of Baselines for a Target Endpoint . . . 220

C Evaluating the Product in a Trial Environment 221

Evaluation Checklist . . . 221
Getting Started . . . 222
- Installing Secure Configuration Manager . . . 222
- Introducing the Console . . . 223
- Understanding Console Permissions . . . 224

Adding Assets to the Asset Map . . . 225
- Exploring the IT Assets Content Pane . . . 226
- Overview of System Discovery and Management . . . 227
- Deploying Windows Agents to Discovered Systems . . . 229
- Managing (Discovered) Windows Systems by Proxy . . . 230
- Managing (Discovered) UNIX and Linux Systems . . . 231
- Adding (Discovered) Endpoints to Managed Systems . . . 232
- Creating a Report about Managed Assets . . . 233

Auditing IT Assets . . . 233
- Exploring Security Knowledge Content . . . 234
- Updating Security Knowledge Content (AutoSync Service) . . . 236
- Running Policy Templates . . . 237
- Running Security Checks . . . 239
- Exploring the Report Viewer . . . 242

Evaluating IT Assets . . . 245
- Excluding Data from Report Results . . . 245
- Comparing an Endpoint's Results Over Time . . . 250
- Exploring the Asset Compliance View . . . 252
- Configuring Asset Compliance View Settings . . . 252
- Viewing Results with the Asset Compliance View . . . 253

Maintaining Environment Configuration Standards . . . 253
Applying Product Licenses . . . 254
- Using a Trial License . . . 254
- Changing from Trial to Production License . . . 254

D Checklists 255

About This Book

The *User's Guide* provides conceptual information about Secure Configuration Manager. This book includes procedural instructions for some common tasks.

- Chapter 1, "Introduction," on page 13
- Part I, "Discovering and Managing Your IT Assets," on page 23
- Part II, "Auditing Your Managed Assets," on page 45
- Part III, "Identifying Security Risks in Your Environment," on page 83
- Part IV, "Customizing Secure Configuration Manager," on page 135
- Part V, "Integrating with a SIEM Solution," on page 165
- Part VI, "Maintaining Secure Configuration Manager," on page 181
- Part VII, "Appendices," on page 205

Intended Audience

This book provides information for individuals responsible for assessing the risk and vulnerability of IT assets, such as Windows and UNIX servers, as well as the applications and databases that the servers host. This book includes information for individuals who must manage and configure the application and its components.

Additional Documentation

The Secure Configuration Manager documentation library includes the following resources:

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

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

Contact Information

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

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

1 Introduction

NetIQ Secure Configuration ManagerThe product 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.

- "Understanding Secure Configuration Manager Components" on page 13
- "Understanding Asset Categories" on page 15
- "Auditing and Evaluation Process Workflow" on page 17
- "Understanding the Tools for Auditing Assets" on page 18
- "Understanding Compliance Evaluation Tools" on page 19
- "Listing Reports, Actions, and Security Checks" on page 21

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 **consoles**. 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.
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, assessment results, and configuration data in the database
Database	Stores product configuration data and results from security checkup reports in Microsoft SQL Server format.

Component	Description
Web console	Secure Configuration ManagerServes as a browser-based interface for so you can perform the following functions: ◆ Get a high-level view of your IT assets, including the status of their health, compliance, and risk to your enterprise security ◆ Create dynamic reports that combine the results of multiple policy templates and endpoints ◆ View and manage endpoints and groups ◆ Execute security checks and run policy templates so you can perform a granular assessment of specific groups and endpoints ◆ Create and apply saved lists for security check parameters ◆ Create, apply, and edit exceptions for assessment results, including batch-created exceptions that apply to multiple policy templates ◆ Create and apply tags to endpoints and policy templates ◆ View the status of jobs ◆ Launch the Dashboard without having to log in again **NOTE:** With the introduction of Secure Configuration Manager 7.0, this console replaces some functionality provided by the Windows console.
Windows console	Secure Configuration ManagerServes as an interface for so you can perform the following functions: ◆ View, add, remove, and group your IT assets ◆ Execute security checks and run policy templates ◆ Create and apply saved lists for security check parameters ◆ Create and apply exceptions to assessment results ◆ Manage jobs ◆ Filter information ◆ Control automatic AutoSync updates ◆ Configure product settings ◆ Modify, import, and export security checks and policy templates **NOTE:** With the introduction of Secure Configuration Manager 7.0, the Web console replaces some of the console's functionality. Further references to this console will be prefaced with "Windows".
Dashboard	Provides a Web-based overview of your environment's compliance enables executives and managers to: ◆ View the overall compliance of 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 about modifying component settings and grooming the database, see Chapter 20, "Maintaining the Secure Configuration Manager Database," on page 191.

Understanding Asset Categories

Secure Configuration Manager interacts with your servers and network devices according to each asset's assignment within four specific categories: assets, also known as systems; agents; endpoints; and groups.

- "Assets" on page 15
- "Agents" on page 15
- "Endpoints" on page 16
- "Groups" on page 16

NOTE: The Web console uses the term *asset*, while the Windows console continues to use the older term *system*.

Assets

Assets, or **systems**, are physical computers on a network that run an operating system and host applications or databases. When you add an asset to Secure Configuration Manager, the computer hosts an agent, and possibly one or more endpoints. For more information, see "Agents" on page 15 and "Endpoints" on page 16.

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 asset** 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 assets on your network. For more information about automatically discovering systems, see "Discovering Unmanaged Assets in Your Environment" on page 27. 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 assets on your network according to the schedule you set.

Agents

Agents are hosted on assets 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 "Endpoints" on page 16.

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 "Registering an Agent Manually" on page 31.

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 Windows console, then view the agents listed in the content pane. For more information about deployment, see "Deploying Windows Agents to the Managed Assets" on page 30.

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 deleting and unregistering managed assets, endpoints, and agents, see "Removing Managed Assets" on page 42.

Endpoints

Secure Configuration Manager analyzes security risks and ensures policy compliance for your endpoints. An **endpoint** represents an agent-monitored operating system, application, web server, network device, or database instance. Endpoints are categorized into groups in the asset map according to the endpoint type, such as SQL Server 2012 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. An asset can have multiple endpoints.

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

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 2012. 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** under the **My Groups** tree in the console to facilitate management of your environment. The console nests these user-defined groups, 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 several data views. The Secure Configuration Manager Dashboard also displays policy template results according to your managed groups. For more information about the Asset Compliance View, see "Using the Asset Compliance View for Evaluation" on page 89. For more information about the Secure Configuration Manager Dashboard, see "Using the Secure Configuration Manager Dashboard for Evaluation" on page 99.

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.

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 "Understanding Managed and Unmanaged Assets" on page 26.
❑	2. Discover assets and endpoints in your environment. For more information, see "Discovering Unmanaged Assets in Your Environment" on page 27.

	Checklist Items
❑	3. Organize your assets into logical groups. For more information, see "Organizing Endpoints into Groups" on page 40.
❑	4. Specify the value of each asset to your organization. For more information, see "Assigning Importance to Endpoints" on page 39.
❑	5. Identify the corporate policies and technical standards that affect your IT assets.
❑	6. Map your policies and standards to the policy templates built into Secure Configuration Manager. For more information, see "Understanding Policy Templates" on page 71.
❑	7. (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 "Modifying Built-in Policy Templates" on page 74 or "Translating a Technical Standard to a Policy Template" on page 73.
❑	8. Run the policy templates to begin the assessment process. For more information, see "Running Security Checks" on page 69.
❑	9. Review policy template results to evaluate asset compliance. For more information, see Part III, "Identifying Security Risks in Your Environment," on page 83.
❑	10. Correct the configuration problems found in the report results.
❑	11. (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 "Assigning Importance to Endpoints" on page 39 and "Understanding Risk Scoring" on page 56.
❑	12. (Optional) To create a baseline using an asset which meets specific criteria and use that baseline as a standard for that particular asset, or run delta reports. For more information, see Chapter B, "Working with Baselines," on page 211 or Chapter 10, "Comparing Results of Assessments," on page 123.
❑	13. (Optional) To exclude some assets or results from policy template runs, create exceptions. For more information, see "Excluding Data from Report Results" on page 113.
❑	14. Regularly audit assets with the selected policy templates. For more information, see Chapter 6, "Configuring Assessment Options," on page 77.
❑	15. (Optional) To regularly compare policy template results, schedule delta reports. For more information, see "Scheduling a Delta Report" on page 127.
❑	16. Regularly update your policy templates as corporate and regulatory standards change. For more information, see Chapter 19, "Maintaining Your Security Knowledge," on page 183.

Understanding the Tools for Auditing Assets

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 "Understanding Policy Templates" on page 71. For more information about security checks, see "Understanding Security Checks" on page 47.

Understanding Compliance Evaluation Tools

The security check and policy template reports help you determine the risk areas in your enterprise, so you can prioritize the security risks that you find. 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
Web console	This browser-based tool provides **assessment reports** and **dynamic reports** that enable executives and managers to: ◆ View the overall status of your IT assets ◆ Visualize compliance and risk status your IT assets in tables or charts and graphs ◆ 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 ◆ Generate reports that combine results of multiple policy templates and endpoint types to observe trends in security compliance or compare the status of endpoints For more information, see "Using Dynamic Reports to Evaluate Endpoints" on page 107 and "Viewing Assessment Results" on page 86, as well as the Help in the Web console.
Dashboard	This Web-based overview of your environment's compliance enables executives and managers to: ◆ View the overall compliance of your IT assets ◆ Perform a granular assessment of specific groups and computers ◆ View the overall posture and trends of security compliance at a single glance For more information, see "Using the Secure Configuration Manager Dashboard for Evaluation" on page 99.
Asset Compliance View	In the Windows console, provides an overview of your environment's compliance that 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 "Using the Asset Compliance View for Evaluation" on page 89.

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 “Automating Out-of-Compliance Notifications” on page 77 and Part V, “Integrating with a SIEM Solution,” on page 165.

Listing Reports, Actions, and Security Checks

The Windows console 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 “Managing Permissions” on page 160.

Discovering and Managing Your IT Assets

This section helps you build and manage your IT assets map so that you can begin managing risk in your environment. You can discover Windows computers, install agents on them, then discover endpoints on each server. You can also add UNIX agents and endpoints.

- Chapter 2, “Building Your Asset Map,” on page 25
- Chapter 3, “Managing Your Assets,” on page 37

2 Building Your Asset Map

To manage an asset with Secure Configuration Manager, such as a computer or database, you must first add and 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 categories most appropriate for your organization. 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 managed assets to the asset map periodically.

NOTE: To discover, add, and register assets with Secure Configuration Manager, you must use the Windows console.

Checklist for Building Your Asset Map

Use the following checklist to help you discover, add, and organize your assets, 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 "Organizing Endpoints into Groups" on page 40.
❑	2. Create and organize your asset map groups. For more information, see "Creating a Managed Group" on page 41.
❑	3. Add known, unmanaged assets: ◆ To add individual assets, see "Manually Adding Known Assets" on page 26 ◆ To add multiple assets at once, see "Using a Formatted File to Add Known Assets" on page 27
❑	4. Find unmanaged assets in your environment. For more information, see "Discovering Unmanaged Assets in Your Environment" on page 27.
❑	5. Deploy Windows agent to unmanaged assets. For more information, see "Deploying Windows Agents to the Managed Assets" on page 30.
❑	6. Add the discovered assets to your asset map. For more information, see "Registering Managed Assets" on page 31.
❑	7. Register the discovered and added assets. See "Registering Managed Assets" on page 31.
❑	8. Find additional endpoints on your managed assets. For more information, see "Discovering Endpoints on Managed Assets" on page 33.
❑	9. Move your assets into the managed groups appropriate for your environment. See "Moving Existing Endpoints into Groups" on page 41.
❑	10. Store a copy of your asset map for future reference. "Saving Asset Map Data" on page 200

Understanding Managed and Unmanaged Assets

A **managed asset** comprises the host computer with a registered endpoint and, usually, a registered agent. You can run assessments only against managed assets. Until you add an asset, agent, or endpoint to **Managed Systems**, the asset is considered **unmanaged**. You can configure Secure Configuration Manager to discover unmanaged servers and endpoints in the specified domains. Alternatively, you can manually add assets to **Managed Systems**.

Secure Configuration Manager enables you to manually add assets or discover assets to manage. If the discovered or imported asset already has a valid security agent, you can manage the asset 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 "Deploying Windows Agents to the Managed Assets" on page 30 and the *Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

Adding Known, Unmanaged Assets

Available only in the Windows console.

If you already know the host name or IP addresses of assets that you to assess with Secure Configuration Manager, you can manually add them from the Windows console. Alternatively, if you have a large number of known assets, you can create a file to import the assets. You can add Windows or UNIX servers.

The assets do not need a security agent before you add them to Secure Configuration Manager. Instead, you can assign an existing agent to each asset as you manually add them or assign the agent later. However, the asset must have an agent before you can register the asset with Secure Configuration Manager and begin assessing it for vulnerabilities. For more information, see "Registering Managed Assets" on page 31.

Your console user account must have proper permissions to add assets. For more information about permissions, see "Managing Permissions" on page 160.

Manually Adding Known Assets

If you have a few servers for which you already know the IP address and host name, it might be easier to manually add them. This wizard enables you to add assets with or without an agent. If the asset has an agent, you can also register the asset ass you add it to Secure Configuration Manager. For more information about registeration, see "Registering Managed Assets" on page 31.

1. Log in to the Windows console.
2. Select **IT Assets > Managed Systems**.

   NOTE: You can also add assets in this same way from **IT Assets > Agents**.

3. Complete the wizard for adding assets.

NOTE: Secure Configuration Manager supports IPv4 and IPv6 addresses. For more information about IPv6 support, see "Discovering Unmanaged Assets in Your Environment" on page 27, the *Secure Configuration Manager Installation Guide*, and the *Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

Using a Formatted File to Add Known Assets

The Core Services Configuration Utility enables you to specify a file containing a list of computers that 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 "Scheduling the Discovery Process" on page 29. 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
```

Discovering Unmanaged Assets in Your Environment

Available only in the Windows console.

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 Windows 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 "Discovering Endpoints on Managed Assets" on page 33.

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. You must either deploy an agent to the discovered system to manage the asset, or use an agent on another asset to manage the endpoints by proxy. For more information about adding discovered systems to your asset map, see Chapter 3, “Managing Your Assets,” on page 37.

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 “Managing Permissions” on page 160.

Manually Discovering Unmanaged Assets

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.

Automatically Discovering Unmanaged Assets

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 "Discovering Endpoints on Managed Assets" on page 33.

- 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 "Deploying Windows Agents to the Managed Assets" on page 30.

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 "Scheduling the Discovery Process" on page 29.

Scheduling the Discovery Process

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 "Automatically Discovering Unmanaged Assets" on page 28.

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 "Discovering Endpoints on Managed Assets" on page 33.

Deploying Windows Agents to the Managed Assets

Available only in the Windows console.

After you discover or manually add Windows assets to Secure Configuration Manager, you can add a Windows agent to the assets. 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 *Secure Configuration Manager Windows Agent Installation and Configuration Guide* and the Help. For more information about finding computers to add to the asset map, see "Discovering Unmanaged Assets in Your Environment" on page 27.

Registering Managed Assets

Available only in the Windows console.

To “manage” an asset, you simply add the asset to the asset map. However, to run assessments, you must **register** the asset’s agent and endpoints with Secure Configuration Manager. Core Services cannot communicate appropriately with the agent until you register the agent. If you do not register the endpoints, the agent cannot gather data to assess the asset’s vulnerability to security risks.

In general, when you register an agent on a managed asset, Secure Configuration Manager automatically registers the managed endpoints on that asset. If you add an endpoint after registering the agent, though, you might need to register the added endpoint. For more information, see “Adding Endpoints to Managed Assets” on page 32.

If you have not added agents to your managed assets, consult the following table.

For more information about...	See...
Deploying a Windows agent	“Deploying Windows Agents to the Managed Assets” on page 30
Installing a Windows agent in a remote domain	*Secure Configuration Manager Windows Agent Installation and Configuration Guide*
Installing or deploying UNIX agents	*Installation and Configuration Guide for Secure Configuration Manager UNIX Agent*

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.

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.

Registering an Endpoint

In general, Secure Configuration Manager automatically registers an endpoint when you add it to a security agent.

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

Adding Endpoints to Managed Assets

Available only in the Windows console.

Many of the servers in your environment host more than one endpoint, such as the operating system and a database instance. When you register a Windows computer 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 managed asset, or you can configure Secure Configuration Manager to regularly probe managed assets for undiscovered endpoints.

- "Adding Known Endpoints to an Agent" on page 32
- "Discovering Endpoints on Managed Assets" on page 33
- "Adding Discovered Endpoints to a Managed Asset" on page 34
- "Adding Network Device Endpoints" on page 34

Adding Known Endpoints to an Agent

As your organization grows and changes, you might need to add endpoints that you want to assess. For example, you might install a database on a managed asset or add a network device to your environment.

1. Log in to the Windows console.
2. In the left pane, click **IT Assets**.
3. In the IT Assets tree pane, expand **Agents** and select the appropriate folder.
4. In the content pane, right-click the agent to which you want to add the endpoint, and then click **Add Endpoint**.
5. Click **Next**.
6. (Optional) To find an existing system on which to add an endpoint, click **Existing Systems**. Select a system and click **OK**.
7. In the **Name** field, type a name for the endpoint.
8. Select the appropriate endpoint type from the **Endpoint Type** field, such as Windows Machine or Active Directory, or accept the default endpoint type.
9. 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.
10. (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.
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.

Field	Description
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, or Oracle systems.
Service Pack	Microsoft Service Pack applied to the Windows operating system. 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.

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

11a Select the **Add Endpoint to a Group** check box.

11b Click **Groups**.

11c Select an existing group to which you want to add the endpoint, or create a new group.

11d (Optional) To create a new group, enter the new group name and description, and then click **Create New Group**.

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

12 (Optional) To add more than one endpoint, click **Add Endpoint**. Repeat Step 7 on page 32 through Step 11 on page 33 for each endpoint that you want to add.

13 Click **Finish**.

Discovering Endpoints on Managed Assets

When you add a server to your asset map, Secure Configuration Manager automatically recognizes the operating system as an endpoint. However, that server might have more endpoints that can be managed and assessed. You can configure Secure Configuration Manager to automatically discover the following types of endpoints referred to as **application endpoints**, on your managed assets:

- 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 asset, Core Services instructs the agent managing that asset 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 assets. For more information about jobs that discover application endpoints, see "Scheduling the Discovery Process" on page 29.

Adding Discovered Endpoints to a Managed Asset

Adding a discovered endpoint follows the same process as manually adding endpoints, except you start from **IT Assets > Discovered Systems**.

1. Log in to the Windows console.
2. In the left pane, click **IT Assets > Discovered Systems**.
3. In the content pane, right-click the endpoint that you want to add, and then click **Manage**.
4. Select the agent that you want to manage the endpoint, then complete the wizard for adding the endpoint.

   For more information, see "Adding Known Endpoints to an Agent" on page 32.
5. (Optional) Add the endpoint to a group, as described in Step 11 on page 33.
6. Click **Finish**.

Adding Network Device Endpoints

Secure Configuration Manager enables you to assess the configuration of network devices attached to a Windows environment. It's a two-step process to add network devices as endpoints. First, you add the network devices to the Network Device Endpoint Importer utility. Then you have the utility import the devices into Secure Configuration Manager.

The Network Device Endpoint Importer is a separate utility packaged with Secure Configuration Manger.

1. To launch the Network Device Endpoint Importer utility, go to **Start > Secure Configuration Manager > Network Device Endpoint Importer**.
2. Enter your Secure Configuration Manager login credentials.
3. Enter IP address and port number for Core Services.
4. Click **Login**.
5. Click **File > New Endpoint** or click the **+** option.
6. In the **Endpoint Name** field, specify a name for the endpoint that you want to add.
7. In the **Endpoint Properties** table, verify or specify the following required information:

Field	Description
Agent Name	Select the Windows agent to which you want to add the network device endpoint.
Endpoint Name	(Optional) Specify a name for the endpoint, if you have not specified already in Step 2.
Protocol	Select the type of protocol used to connect with the network device - Telnet or SSH.

Field	Description
Authentication Type	This field is displayed only if you have selected SSH as the protocol. Select one of the following options: ◆ **Password:** Select this option if you require password-based SSH authentication. ◆ **Key:** Select this option if you require key-based SSH authentication.
Network Device Type	Select the type of the network device for which you are configuring this endpoint. This drop-down list has following options: ◆ **IOS:** Select IOS if the network device is a Cisco device. ◆ **JUNOS:** Select UNOS if the network device is a Juniper device. ◆ **GENERIC:** Select GENERIC if the network device is not a Cisco or a Juniper device.
IP Address	Specify IP address of the network device.
IP Port	Specify the port through which the endpoint interacts with the network device.
User Name	Specify the user name to log in to the network device.
Password	This field is displayed only if you have selected Password as the **Authentication Type**. Specify 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 customize the values.

8 (Optional) Specify the following endpoint properties:

Field	Description
Passphrase	This field is displayed only if you 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 contact person.
Importance	Criticality level of the endpoint.
License Type	Product for which you are licensing this endpoint.
Location	Physical location of the endpoint computer hardware.
Version	Version of the SQL Server database that the endpoint represents.
Time Zone	Time zone in which the endpoint computer hardware is located.
Notes	Descriptive notes about the endpoint.

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

9 To register the endpoint with Secure Configuration Manager, select **True** in the Register field.

Alternatively, you can select **Register All** to register all the endpoints you have added.

10 (Optional) To add the endpoint to a group, select **Add Endpoint to a Group** option, and then select an existing group or type a new group name to which the endpoint should belong.

To easily add endpoints, you can do the following:

- 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.
- 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. You can use these configuration information files to add network device endpoints in future.

- 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.

After you add network device endpoints in the Network Device Endpoint Importer utility, click **Import All** to import all the network device endpoints to Secure Configuration Manager. You can view the log messages pertaining to the import operation in the Log Messages area. On completing the import operation successfully, a confirmation message is displayed.

3 Managing Your Assets

After building the asset map, you can manage and monitor the status of your agents and endpoints, as well as organize the endpoints into groups. Both consoles include a **Managed** view that contains all agents and endpoints that you have included in your asset map. These assets might 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 *Secure Configuration Manager Installation Guide*.

- "Managing Asset Properties" on page 37
- "Managing Your Agents" on page 37
- "Managing Your Endpoints" on page 39
- "Organizing Endpoints into Groups" on page 40
- "Removing Managed Assets" on page 42
- "Reporting Asset Map Information" on page 44

Managing Asset Properties

Available only in the Windows console.

You can change the properties of a managed asset, agent, or endpoint at any time after you have added the asset to your map. For example, you might want to modify the asset's contact email or physical location. To support compliance notifications, you should add an email account to each endpoint's properties.

You can also add customized properties for each managed asset, such as specifying the organizational unit to which the asset belongs or the number of endoints that the agent manages.

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

Managing Your Agents

To manage agents, you must use the Windows console.

Occasionally, you might need to check an agent's status or re-register the agent. You can also update the agent's software and limit the number of concurrent requests that Core Services submits to an agent.

- "Ensuring an Agent's Efficiency" on page 38
- "Checking an Agent Heartbeat" on page 38
- "Updating Windows Agent Software" on page 38

Ensuring an Agent's Efficiency

Secure Configuration Manager 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.

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.

Updating Windows Agent Software

Secure Configuration Manager enables you to push software updates to security agents on multiple systems concurrently. Once you have a 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.

Managing Your Endpoints

Available only in the Windows console.

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. 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 "Assigning Importance to Endpoints" on page 39.

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.

- "Managing Endpoints without Installing an Agent" on page 39
- "Assigning Importance to Endpoints" on page 39

Managing Endpoints without Installing an Agent

Secure Configuration Manager employs a process called **manage by proxy** to let you manage and assess some endpoints without installing an agent on the computer. Instead, an agent in the same domain as the agentless asset would managing the endpoints on othat asset.

The manage by proxy capability 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. The computers within the **domain** must share a common security account (user and group) database and policy.

To set up a proxy agent, add the agent to your asset map, and then add endpoints residing on agentless assets to the agent.

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 "Managing Permissions" on page 160.

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 "Understanding Risk Scoring" on page 56.

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.

Organizing Endpoints into 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. For an overview of groups, see "Groups" on page 16.

The entire set of groups is called a **forest**. Each top-level node is called a **tree**. Several rules apply to managing 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.

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 "Managing Permissions" on page 160.

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.

- "Creating a Managed Group" on page 41
- "Moving Existing Endpoints into Groups" on page 41

Creating a Managed Group

You can create managed groups in both the Web and Windows consoles. You can create empty managed groups so those groups are available when you add endpoints later.

- "Web Console - Creating a Managed Group" on page 41
- "Windows Console - Creating a Managed Group" on page 41

Web Console - Creating a Managed Group

To create a managed group in the Web console, start from **Manage > Endpoints**. For more information, see the Help in the Web console.

Windows Console - Creating 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**.

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.

- "Web Console - Creating a Managed Group" on page 41
- "Windows Console - Creating a Managed Group" on page 41

Web Console - Creating a Managed Group

To move or copy endpoints to a managed group in the Web console, start from **Manage > Endpoints**. For more information, see the Help in the Web console.

Windows Console - Creating a Managed 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**.

Removing Managed Assets

Available only in the Windows console.

On occasion, you might want to stop managing an agent or endpoint, or the full managed asset. Depending on the asset type, you can choose to either un-register the asset or delete the asset from the map.

- "Removing an Endpoint from an Agent" on page 42
- "Removing Agents" on page 42
- "Removing a Managed Asset" on page 43

Removing an Endpoint from an Agent

You can remove an endpoint from an agent. For example, you manage the endpoint by proxy and want a different agent to manage the endpoint.

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

2 Navigate to the agent that manages the endpoint you want to remove.

3 In the content pane, select the agent.

4 In the bottom pane, right-click the endpoint, then click **Remove from Agent**.

Removing Agents

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. Alternatively, you can choose to remove the agent from the asset map, but the agent continues to be registered.

- "Un-Registering an Agent" on page 42
- "Deleting an Agent from the Asset Map" on page 43

Un-Registering an Agent

We recommend that you un-register the agent before removing it from your asset map. Before deleting an agent, you must remove all attached endpoints. Deleting the agent without removing the endpoints leaves the endpoints unmanaged

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.

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 "Un-Registering an Agent" on page 42.

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.

Removing a Managed Asset

When you no longer need a managed asset, or when you remove the asset from the domain, you can delete that asset from your asset map. If the asset hosts an agent, deleting that asset also un-registers its hosted agent from the current Core Services. Before deleting an asset 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 asset from your asset map, the asset might be added to Discovered Systems again, depending on the settings for discovery.

---

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 asset that you want to delete, then click **Delete**.

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

Reporting Asset Map Information

The Windows console 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 “Managing Permissions” on page 160.

II Auditing Your Managed 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 that 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. You can also use the reports to predict the regulations, standards, and benchmarks that might result in vulnerabilities and compliance problems for your assets.

This section 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 Part III, “Identifying Security Risks in Your Environment,” on page 83.

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 19, “Maintaining Your Security Knowledge,” on page 183.

You can also customize the built-in security checks and policy templates or create your own.

- Chapter 4, “Using Security Checks to Assess Assets,” on page 47
- Chapter 5, “Using Policy Templates to Assess Assets,” on page 71
- Chapter 6, “Configuring Assessment Options,” on page 77

4 Using Security Checks to Assess Assets

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.

You can edit an existing security check or create a new one to meet your organization's security policies. For more information about editing a security check, see "Modifying Built-in Security Checks" on page 61.

- "Understanding Security Checks" on page 47
- "Understanding How Agents Identify Data to Collect" on page 49
- "Understanding Security Check Components" on page 49
- "Understanding Risk Scoring" on page 56
- "Modifying or Creating Custom Security Checks" on page 60
- "Custom Security Check Examples" on page 64
- "Running Security Checks" on page 69

Understanding Security Checks

To help you determine whether a security check meets your needs, the consoles provide an **explanation** of the security 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
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

Component	Explanation	Example
Report	Formal output of the checked results	Physical report in the Completed jobs queue

The following are 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

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. 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	“Excluding Values from a Run” on page 111
Modify a built-in security check	“Modifying Built-in Security Checks” on page 61
Create a custom security check	“Creating Custom Security Checks” on page 61
Learn more about security check components	“Understanding Security Check Components” on page 49
Learn more about the threat factor and scoring security check results	“Understanding Risk Scoring” on page 56
Compare the results for individual endpoints or security checks	Chapter 10, “Comparing Results of Assessments,” on page 123
Learn more about the Completed jobs queue	“Viewing Assessment Results” on page 86 and “Customizing the Job Queues” on page 139
Learn more about the AutoSync server	Chapter 19, “Maintaining Your Security Knowledge,” on page 183
Learn more about managing permissions in the console	“Managing Permissions” on page 160

Understanding How Agents Identify Data to Collect

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 “Custom Security Check Examples” on page 64.

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 “Understanding Risk Scoring” on page 56.

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.

- “Security Check Categories” on page 50
- “Security Check Filters” on page 50
- “Security Check Properties” on page 55

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.

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” on page 51
- “Filter Operators” on page 51
- “Filter Type” on page 52
- “Filter Criteria” on page 52
- “Regular Expressions in the Filter” on page 52
- “Combining Filter Sets” on page 53
- “User Parameters” on page 54

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 “Excluding Values from a Run” on page 111.
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 “Excluding Values from a Run” on page 111.
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 52.
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 52.

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 "Understanding Policy Templates" on page 71.

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.

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.

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.

- “Scoring Method” on page 56
- “Threat Factors” on page 57
- “Expected Number of Rows Returned” on page 57
- “Importance Factor” on page 58
- “Example of Risk Scoring” on page 59
- “Risk Scoring Distribution” on page 59

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 "Expected Number of Rows Returned" on page 57. For more information about applying the scoring method to a custom security check, see "Creating Custom Security Checks" on page 61.

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.

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 "Scoring Method" on page 56.

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 "Expected Number of Rows Returned" on page 57.

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 "Assigning Importance to Endpoints" on page 39.

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.

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.

Modifying or Creating Custom Security Checks

Available only in the Windows console.

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.

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 "Creating Custom Security Checks" on page 61. 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 "Understanding Security Checks" on page 47.

- "Checklist for Editing and Creating Security Checks" on page 60
- "Modifying Built-in Security Checks" on page 61
- "Creating Custom Security Checks" on page 61
- "Working with the Generic Network Device Security Check" on page 63

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 "Understanding How Agents Identify Data to Collect" on page 49.
❑	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 "Security Check Filters" on page 50.
❑	4. Identify the scoring method that you want to apply to the data.See "Scoring Method" on page 56.

	Checklist Items
❑	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 "Threat Factors" on page 57.
❑	6. Identify the amount of data 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 "Expected Number of Rows Returned" on page 57.
❑	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 "Security Check Categories" on page 50.
❑	9. Write a brief description, detailed explanation, and additional information describing the check and its uses. see "Security Check Properties" on page 55.

Modifying Built-in Security Checks

Available only in the Windows console.

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 "Managing Permissions" on page 160. 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 "Creating Custom Security Checks" on page 61.

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 "Managing Permissions" on page 160.

Creating Custom Security Checks

To create a custom security check, you must use the Windows console.

To meet your organization's specific security needs, you can create custom security checks that evaluate 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 "Custom Security Check Examples" on page 64. To create a custom check, your console user account needs the New Security Check permission. For more information, see "Managing Permissions" on page 160.

To create a custom security check:

1. Log in to the Windows console.
2. In the left pane, click **Security Knowledge**.
3. In the Security Knowledge tree pane, expand **Security Checks**.
4. Right-click **My Checks**, and then click **New Security Check**.
5. 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.

6. Click **Next**.
7. On the Select Returned Attributes window, select the attributes that you want to use as the columns of data returned by the query.
8. Click **Next**.
9. (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.

10. ***If you want to create multiple filters***, specify the items in Step 9 on page 62 and specify the AND/OR logic of how the filters combine. For more information about filter components and filter logic, see "Security Check Filters" on page 50.

    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.

11. Click **Next**.
12. (Conditional) If your custom check includes required parameters, specify the default values, and then click **Next**.
13. Select a method in the **Scoring Method** field.
14. Enter values in the **Threat Factor** and **Expected Number of Rows Returned** fields, or accept the defaults.
15. Click **Next**.
16. 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.

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

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

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

20 Type the remaining descriptive fields as necessary.

21 Click **Next**.

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

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

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

Working with the Generic Network Device Security Check

In addition to the device-specific security checks for Cisco and Juniper network devices endpoints, Secure Configuration Manager 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.

Custom Security Check Examples

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

- "Accounts with Passwords More than 60 Days Old" on page 64
- "Kernel Parameters" on page 65
- "Registry Keys Modified Since Date" on page 66
- "Password Policy Violations" on page 67
- "Suspicious User" on page 68

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**.

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**.

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**.

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**.

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**.

Running Security Checks

When you run a security check, Secure Configuration Manager compares all the endpoints you specify to all the preferred security settings listed in the security checks. 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 at any time. If you want to gather data for a specific period of time, you can run reports from the database rather than have the agent gather current data from the endpoint. The database maintains results from previous runs of each security check. You can compare results for each run using the delta report function. For more information about gathering security check data from the database, see "Running Reports from the Database" on page 124. For more information about delta reporting, see Chapter 10, "Comparing Results of Assessments," on page 123.

If you do not know which security checks you want to run, you can initiate a search based on several criteria. For example, you can search for checks based on keyword, platform, category, and other criteria.

The time it takes to run a security check 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 "Viewing Assessment Results" on page 86. For more information about distributing a copy of the report, see "Enabling Report Distribution" on page 79.

To run a security check, your console user account must have the Run Security Checks permission. For more information, see "Managing Permissions" on page 160.

- "Web Console - Running Security Checks" on page 70
- "Windows Console - Running Security Checks" on page 70

Web Console - Running Security Checks

To run a security check in the Web console, start from **Manage > Endpoints** or **Assess > Security Checks**. For more information, see the Help in the Web console.

To view the available security checks, see **Assess > Security Checks**.

Windows Console - Running Security Checks

To run a security check in the Windows console, select **Knowledge > Security Checks**. For more information, see the Help in the Windows console.

5 Using Policy Templates to Assess Assets

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 "Modifying Built-in Policy Templates" on page 74.

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 "Translating a Technical Standard to a Policy Template" on page 73. 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.

- "Understanding Policy Templates" on page 71
- "Modifying and Creating Policy Templates" on page 72
- "Running Policy Templates" on page 75

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.

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** 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 that 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.

You can modify the built-in policy templates or create new templates to express corporate technical standards and current industry standards.

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

If you want to ...	See ...
Understand how security checks score results	“Understanding Risk Scoring” on page 56
Modify a built-in policy template	“Modifying Built-in Policy Templates” on page 74
Create a custom policy template	“Translating a Technical Standard to a Policy Template” on page 73
Compare the results for policy template runs	Chapter 10, “Comparing Results of Assessments,” on page 123
Evaluate endpoints based on policy template results	Part III, “Identifying Security Risks in Your Environment,” on page 83
Learn more about the AutoSync server	Chapter 19, “Maintaining Your Security Knowledge,” on page 183
Learn more about managing permissions in the console	“Managing Permissions” on page 160

Modifying and Creating Policy Templates

Available only in the Windows console.

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.

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.

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 "Modifying Built-in Policy Templates" on page 74.
- ***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 "Using Security Check Instances" on page 72.
- ***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 "Modifying Built-in Security Checks" on page 61.
- ***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 "Creating Custom Security Checks" on page 61.

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.

Modifying Built-in Policy Templates

Available only in the Windows console.

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 "Managing Permissions" on page 160.

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, the jobs continue to run. However, when you attempt to view the report, the console displays the following error: `Core Services: You cannot run the policy template because it has been deleted. (template ids 376)`.

Creating a Custom Policy Template

Available only in the Windows console.

To meet your organization's specific security needs, you can create custom policy templates that evaluate 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 "Running Security Checks" on page 69.

To create a custom template, your console user account needs the New Policy Template permission. For more information, see "Managing Permissions" on page 160.

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 "Modifying Built-in Policy Templates" on page 74.

To create a custom policy template:

1. Log in to the Windows console.
2. In the left pane, click **Security Knowledge**.
3. In the Security Knowledge tree pane, expand **Policy Templates**.
4. Right-click **My Templates**, and then click **New Policy Template**.
5. On the Security Checks window, select the checks you want to include in the policy template.
6. (Optional) To use multiple instances of the same check, complete the following steps:
   - **6a** Highlight the security check in the Available Checks list.
   - **6b** Click the **>** button to move the check to the Selected Checks list.

6c 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.

6d Repeat this step for each instance of the security check that you want to include in the policy template.

7 Click **Next**.

8 On the Parameters window, enter the parameter specifications for each security check, and then click **Next**.

9 On the Properties window, enter a unique name and a description of the policy template, and then click **Next**.

10 Review the information on the Summary window, and then click **Finish**.

Running Policy Templates

When you run a policy template, Secure Configuration Manager compares all the endpoints you specify to all the preferred security settings listed in the security checks of the policy template. 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 policy templates at any time. To gather data for a specific period of time, you can run reports from the database rather than have the agent collect current data from the endpoint. The database maintains results from previous runs of each 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 “Running Reports from the Database” on page 124. For more information about delta reporting, see Chapter 10, “Comparing Results of Assessments,” on page 123. For more information about scheduling, see “Running Assessments on a Schedule” on page 78.

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 “Viewing Assessment Results” on page 86. For more information about distributing a copy of the report, see “Enabling Report Distribution” on page 79.

To run a policy template, your console user account needs the Run Policy Template permission. For more information, see “Managing Permissions” on page 160.

- “Web Console - Running Policy Templates” on page 76
- “Windows Console - Running Policy Templates” on page 76

Web Console - Running Policy Templates

To run a policy template in the Web console, start from **Manage > Endpoints** or **Assess > Policy Templates**. For more information, see the Help in the Web console.

To view the available policy templates, see **Knowledge > Policy Templates**.

Windows Console - Running Policy Templates

To run a policy template in the Windows console, select **Security Knowledge > Policy Templates**. For more information, see the Help in the Windows console.

6 Configuring Assessment Options

When you run an assessment, the wizards enable you to set up schedules for recurring runs and notify others of compliance failures. In the Windows console, you can also

- "Automating Out-of-Compliance Notifications" on page 77
- "Running Assessments on a Schedule" on page 78
- "Enabling Report Distribution" on page 79

Automating Out-of-Compliance Notifications

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.

For more information about sending notifications when you run a policy template, see the Help in the Web or Windows console.

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.

- "Sending Email Notifications to Users" on page 77
- "Sending Email Notifications to Change Management Systems" on page 78

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 "Managing Your Endpoints" on page 39.

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.
6. When you run a policy template or security check, select the option to send email notifications:
   - In the Web console, select **Enable e-mail compliance alerts**.
   - In the Windows console, click **Enable Distribution**, then specify the email options.

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.

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. When you run a policy template or security check, select the option to send a notification to the change management system:
   - In the Web console, select **Forward assessment report to destination server**.
   - In the Windows console, click **Enable Distribution**, then specify the file distribution options.

Running Assessments on a Schedule

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, specify the settings the Run Policy Template wizard.

Once you have scheduled a policy template, you can update the schedule properties using the Schedule Jobs wizard in the Windows console. If you are a console administrator, you can also reassign the owner of a scheduled policy template. For more information about console roles, see "Managing Roles" on page 158.

Web Console - Scheduling a Run

In the **Run Policy Template** wizard, select **Run Options > Run Type > Recurring**. Then specify whether you want the run to occur once at a specific date and time or on a recurring schedule.

For more information, see the Help in the Web console.

Windows Console - Scheduling a Run

In the **Run Policy Template** wizard, select **Schedule > Enable Schedule**. Then specify whether you want the run to occur once at a specific date and time or on a recurring schedule.

You can also instruct Secure Configuration Manager to include a delta report that compares the current results to a previous run. For more information, see "Comparing Policy Template Results" on page 125.

Enabling Report Distribution

When you run or schedule a run of a security check or policy template in the Windows console, you can specify whether you want to distribute a copy of the report to a file or file 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 *Secure Configuration Manager Installation Guide*.

- "Sharing Reports from the Web Console" on page 79
- "Distributing Reports to a File or Share" on page 79
- "Distributing Reports to an Email Recipient" on page 80

Sharing Reports from the Web Console

To share a completed assessment report with relevant users, such as system administrators and business management, you can export the report in PDF format. However, the Web console is designed to provide those users access directly to the assessment reports. In this way, the relevant users can interact with and drill down into the data, then export the PDF if needed. You can limit the access of these users to viewing assessment reports.

For more information about viewing assessment reports, see the Help in the Web console.

Also, when you run a security check or policy template, you can specify that you want out-of-compliance results to be sent to an individual or to notify a change management system. The Web console sends the information to the email addresses or change management system identified in the Core Services Configuration Utility.

Distributing Reports to a File or Share

This feature is available only in the Windows console.

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 "Managing Permissions" on page 160.

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 *Secure Configuration Manager Installation Guide*.

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**.

Distributing Reports to an Email Recipient

Available only in the Windows console.

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 *Secure Configuration Manager Installation Guide*.

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**.

III Identifying Security Risks in Your Environment

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 6, “Configuring Assessment Options,” on page 77. Next, use the reported results to evaluate asset compliance and establish a prioritized remediation plan to protect against the discovered vulnerabilities.

- Chapter 7, “Reviewing Results of Individual Runs,” on page 85
- Chapter 8, “Using Dynamic Reports to Evaluate Endpoints,” on page 107
- Chapter 9, “Excluding Data from Runs and Reports,” on page 111
- Chapter 10, “Comparing Results of Assessments,” on page 123
- Chapter 11, “Predicting Vulnerability and Compliance Problems,” on page 133

7 Reviewing Results of Individual Runs

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 Part II, "Auditing Your Managed Assets," on page 45. 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.

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.

Assessment Reports

Available only in the Web console.

Provides a web-based method for executives and system administrators to visualize the compliance and risk status of IT assets in tables or charts and graphs. Users can drill down into the specific security checks to identify where the endpoints fail and determine how to remediate the problems. They can also create and apply exceptions for endpoints and security checks in the viewed policy template results.

For more information, see "Using the Web Console for Evaluation" on page 88.

NOTE: The Web console also supports aggregated reports that combine the results of multiple policy templates run against a wide variety of endpoints. For more information, see Chapter 8, "Using Dynamic Reports to Evaluate Endpoints," on page 107.

Delta Reports

Available only in the Windows console.

Provides Windows 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

Available only in the Windows console.

Provides Windows 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.

Secure Configuration Manager Dashboard

Provides a Web-based interface 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.

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.

- "Viewing Assessment Results" on page 86
- "Using the Web Console for Evaluation" on page 88
- "Using the Asset Compliance View for Evaluation" on page 89
- "Using the Secure Configuration Manager Dashboard for Evaluation" on page 99

Viewing Assessment Results

As Secure Configuration Manager runs a security check or policy template, the consoles display a report in the **Pending** jobs queue. When the run completes, Secure Configuration Manager moves the report to a **Completed** queue. To access assessment results, perform one of the following actions:

Web Console

Select **Reports > Assessment Reports** or **Reports > Dynamic Reports**, then choose the report that you want to review. You can also click **View Report** in the **Completed** jobs queue. For more information, see "Using the Web Console for Evaluation" on page 88.

Windows Console

Select **Job Queues > Completed** in the left pane, then choose the report that you want to review.

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 "Exporting Assessment Results" on page 87. For more information about graphics in the report, see "Creating Custom Tasks and Reports" on page 137.

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 7, "Reviewing Results of Individual Runs," on page 85.

- "Understanding Assessment Results" on page 86
- "Exporting Assessment Results" on page 87
- "Re-assess Failed Endpoints" on page 88

Understanding Assessment 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 "Assigning Importance to Endpoints" on page 39. For more information about scoring, see "Understanding Risk Scoring" on page 56.

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.
- If you run an assessment that results in an error for an endpoint, the Web console displays a compliance or risk score of **-1** for the endpoint / security check combination that caused the error. The error might indicate that the endpoint needs to be re-registered, the security check failed to function appropriately, or the agent lost communication with the endpoint or Core Services. In the Windows console, you will continue see a compliance or risk score of **0** for the endpoint / security check combination.

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.

Exporting Assessment Results

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.

- "Exporting from the Web Console" on page 87
- "Exporting from the Windows Console" on page 87

Exporting from the Web Console

The Web console allows you to export the completed assessment report as a PDF file. For more information, see the Help in the Web console.

Alternatively, you can give users access to view the reports in the Web console, which enables them to more easily drill down into the data. For more information, see "Using the Web Console for Evaluation" on page 88.

Exporting from the Windows Console

Available only in the Windows console.

To export report data:

1. View the complete report. For more information about viewing reports, see "Viewing Assessment Results" on page 86.
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 *Secure Configuration Manager Installation Guide*.
6. Click **Save**.

Re-assess Failed Endpoints

If the completed report indicates one or more endpoints failed security checks, you can re-run the job or re-run just the failed checks on those endpoints. For information about evaluating report results, see Chapter 7, "Reviewing Results of Individual Runs," on page 85.

Run the assessment report again from **Jobs > Success** or **Jobs > Failed**.

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.

Using the Web Console for Evaluation

In the Web console, you can select to view a graphical snapshot of the overall health of your endpoints, assets, and agents. You can determine the number / percentage of endpoints, assets, or agents that are *online* and *offline*, then drill into the numbers to find the endpoints that might be offline.

Once you have run a policy template, you can view the results in an **assessment report**. Each assessment report includes three views:

Overview

Provides the overall compliance and risk state of the endpoints that were assessed. To help you determine which endpoints to examine first, the overview also contains the following lists:

- The endpoints that pose the highest risk to your environment
- The security checks that had the highest number of failures among the assessed endpoints

Endpoints & Groups

Provides a table that you can sort to quickly investigate the endpoints that might make your environment vulnerable. You can change the view to show all endpoints or only those that are at risk.

For each endpoint, the table lists the compliance status, importance, managed risk status, and the number of failed security checks. To view the failed security checks, you can select the listed value, then identify the settings that need to be updated.

You can also create exceptions for one or more of the endpoints. For more information about exceptions, see "Excluding Values from a Run" on page 111.

Security Checks

Provides high-level view of the pass/fail rate of the security checks as well as a table that you can sort to quickly investigate the security checks that caused the most failures.

For each security check, the table lists the number of compliant, non-compliant, and error-based endpoints. To view the endpoints in one of the categories, you can select the listed value, then review the settings that need to be updated.

You can also create exceptions for one or more of the security checks. For more information about exceptions, see "Excluding Values from a Run" on page 111.

For more information and instructions, see the Help in the Web console.

Using the Asset Compliance View for Evaluation

Available only in the Windows console.

The Asset Compliance View in the Windows console 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 "Changing Asset Compliance View Settings" on page 91.

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	"Understanding Policy Templates" on page 71
Learn about security checks	"Understanding Security Checks" on page 47
Learn about exceptions for policy template results	"Excluding Data from Report Results" on page 113
Compare the results of individual endpoints or security checks	Chapter 10, "Comparing Results of Assessments," on page 123
Learn more about endpoint risk scoring in security checks	"Understanding Risk Scoring" on page 56
Create user-defined groups	"Creating a Managed Group" on page 41

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.

- "Changing Asset Compliance View Settings" on page 91
- "Viewing Compliance Information" on page 91
- "Viewing Risks Information" on page 93
- "Viewing Trending Information" on page 94
- "Viewing Systems Information" on page 95
- "Viewing Summary Information" on page 97
- "Distributing Asset Compliance Information" on page 98

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 "Configuring Data Settings" on page 148 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 "Viewing Trending Information" on page 94.

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 range, change the start and end dates.
5. (Optional) To change the trend interval, select **Daily**, **Weekly**, or **Monthly**.
6. Click **OK**.

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" on page 91
- "Classifying Compliance Results" on page 92

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 "Configuring Data Settings" on page 148.
- 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 "Viewing Systems Information" on page 95.

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 "Understanding Security Checks" on page 47. Fore more information about evaluating asset compliance over time, see "Viewing Trending Information" on page 94.

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.

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 "Understanding Risk Scoring" on page 56.

- "Understanding Risk Status Charts" on page 93
- "Classifying Risk Results" on page 93

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 "Viewing Systems Information" on page 95.

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 "Understanding Risk Scoring" on page 56. For more information about evaluating risk score results over time, see "Viewing Trending Information" on page 94.

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.

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 "Changing Asset Compliance View Settings" on page 91.

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 "Changing Asset Compliance View Settings" on page 91.
7. Select the check box beside the policy templates for which you want to view results.
8. In the Asset Compliance View, click **Trending**.

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" on page 95
- "Viewing Detailed Data for an Endpoint" on page 96
- "Sending an Endpoint Compliance Email" on page 96

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 "Distributing Asset Compliance Information" on page 98.

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 "Distributing Asset Compliance Information" on page 98.

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**.

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 "Viewing Compliance Information" on page 91. For more information about risk results in the Asset Compliance View, see "Viewing Risks Information" on page 93.

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 "Distributing Asset Compliance Information" on page 98.

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 "Distributing Asset Compliance Information" on page 98.

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 *Secure Configuration Manager Installation Guide*.
- 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.

Using the Secure Configuration Manager Dashboard for Evaluation

The Secure Configuration Manager Dashboard provides a web-based interface for executives and managers to view both the overall compliance of their IT assets and to perform a more granular assessment of specific managed 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. The Dashboard displays compliance data based on the Secure Configuration Manager managed groups and scoring types you want each user role to see.

The Dashboard has a few default dashboards, consisting of charts that display compliance data. You can create your own dashboards, and save them. The data that you will see in the charts will depend on the access rights of your user role.

The Dashboard organizes the views into four logical groups, displayed in the following four dashboards:

- Secure Configuration Manager
- Risk Compliance
- System Compliance
- Technical Compliance

Click the **Load Saved Dashboard** icon on the menu bar to navigate to any of these dashboards.

- "Accessing the Dashboard" on page 100
- "Viewing the Secure Configuration Manager Dashboard" on page 100
- "Viewing the Risk Compliance Dashboard" on page 102
- "Viewing the System Compliance Dashboard" on page 103
- "Viewing the Technical Compliance Dashboard" on page 103
- "Customizing the Dashboard" on page 104
- "Screen Capturing and Report Sharing" on page 105

Accessing the Dashboard

All console users can log in to the Dashboard. However, the data that users can view depends on the privileges their role has been assigned by the Secure Configuration Manager administrator. For more information about Secure Configuration Manager users and roles, see "Setting up the Dashboard for Your Users" on page 149.

If your role has been configured with a session limit value, it will be applicable for your Dashboard session too. For more information about session limit, see "Assigning Session Limit to Roles" on page 159.

If your user account is deleted by the Secure Configuration Manager administrator while you are using the Dashboard, your session will be terminated whenever the session is revalidated. For more information about session revalidation interval, see the **Validate User in Every** field in "Working with General Dashboard Settings" on page 150.

You can launch the Dashboard in one of the following ways:

Web console

If the Web console and the Dashboard are installed in the same domain, click **Dashboard** in the Web console. You do not need to enter your credentials.

To enable single sign-on from the Web console, see "Launching the Dashboard from the Web Console" on page 145.

Start menu

Use the Dashboard shortcut in the **Start**Secure Configuration Manager menu of your computer where and the Dashboard are installed.

1. Go to **Start > Secure Configuration Manager Dashboard**.
2. Secure Configuration ManagerSpecify your user name and password.
3. Click **Log In**.

For quick and easy access, add the Dashboard URL to the Favorites tab of your browser. For more information about supported browsers, see the *Secure Configuration Manager Installation Guide*.

Viewing the Secure Configuration Manager Dashboard

The Secure Configuration Manager Dashboard is the default view displayed when you log in to the Dashboard. This dashboard is used to visualize the results of template runs over various endpoints/managed groups. This dashboard provides an overview of the compliance, risk status, and distribution of assets, endpoints, and groups added or created in Secure Configuration Manager.

Following are the charts in the Secure Configuration Manager Dashboard:

Chart Name	Description
Compliance Distribution	This is a pie chart that displays the distribution of the compliance information of the latest runs of templates over the network. The size of each slice indicates the number of template runs on the endpoints of the network, which ended with corresponding compliance level. Only unique template runs are considered for this chart; multiple runs of same templates are not considered. For example, if you run four different templates, the chart will have four slices. If you run two templates twice, the chart will have two slices.
Group Hierarchy	This is a multi-level pie chart created to visualize the hierarchy and size of the groups on which templates have been run. The size of each slice will be reflective of the number of endpoints that are part of the corresponding group.
Policy Template Risk Over Time	This is a trend chart that displays the trend of the sum of total risk of each run of a particular template. By default, the chart follows an interval of one day. The 10 templates with highest sum of total risk are shown in the chart. ALL templates run (including multiple runs of same templates) are considered for this chart.
Platform Distribution	This is a pie chart that displays the distribution of the network based on the platform of endpoints. The size of each slice reflects the number of endpoints of corresponding platform.
Endpoint Distribution	This is a pie chart that displays the distribution of the network in terms of the endpoints. Each slice represents one endpoint.
Policy Template Distribution	This is a pie chart that displays the templates that have been run over the network. Each slice represents one template.
Check Status Distribution	This is a pie chart that displays the collective status of the execution of the security checks that have been run over the network. Each slice represents a status such as “Passed”, “Failed”, and “Unknown”.
Group Compliance Detail	This is a bar graph that displays the distribution of compliance levels of the latest runs of the templates run over the groups. The groups are ordered in descending order according to the number of templates run on them.
Asset Compliance Detail	This is a bar graph that displays the distribution of compliance levels of the latest runs of the templates run over the assets. The assets are ordered in a descending order according to the number of templates run over them.

Chart Name	Description
Check Status Detail	This is a bar graph that displays the status of the execution of various security checks. The security checks will be visible in this graph only if they were executed as a part of a template run. The status of a security check can be “Passed”, “Failed”, “Excepted”, or “Unknown”. The security checks are ordered in the descending order of the number of times they have been run.
Risk Score Detail	This is a bar graph that displays the risk distribution of the latest runs of templates on respective endpoints. The size of each bar area indicates the number of template runs having that risk level. The endpoints are ordered in descending order based on the number of templates run on them.
Geolocation of Out of Compliance Endpoints	This is a world map (tile map) that shows the location of endpoints that have template runs which were out of compliance. **NOTE:** You must have internet connection in your computer to be able to view this chart.

Viewing the Risk Compliance Dashboard

The Risk Compliance Dashboard is used to visualize the important risk related information of your network. When a template is run on any endpoint, it can result in “Low Risk”, “Medium Risk”, “High Risk”, or “Unknown Risk”.

Following are the charts in the Risk Compliance Dashboard:

Chart Name	Description
Overall Risk Status	This is a pie chart that displays the distribution of the risk levels of all the latest runs of templates over the network. The size of each slice indicates the number of template runs having that risk level. Only unique template runs are considered for this chart; multiple runs of same templates are not considered. For example, if you run four different templates, the chart will have four slices. If you run two templates twice, the chart will have two slices.
Overall Risk Status Over Time	This is a bar chart that displays the risk distribution of templates over the network on specific dates. The size of each slice of the bar indicates the number of templates having corresponding risk level. ALL templates run (including multiple runs of same templates) are considered for this chart.
Risk Score Detail	This is a bar graph which displays the risk distribution of the latest runs of templates on respective endpoints. The size of each bar area indicates the number of template runs having that risk level. The endpoints are ordered in descending order of the number of template runs on them.

Chart Name	Description
Low Risk Score Over Time	This is a trend chart which displays the number of template runs which have resulted in low risk at a given point of time.

Viewing the System Compliance Dashboard

The System Compliance Dashboard is used to visualize the important compliance related information of your network. When a template is run over any endpoint, it can result in “In Compliance”, “Out of Compliance”, or “Unknown Compliance”.

Following are the charts in the System Compliance Dashboard:

Chart Name	Description
Overall Compliance Status	This is a pie chart that displays the compliance distribution of all the latest runs of templates over the network. The size of each slice indicates the number of template runs having corresponding compliance level. Only unique template runs are considered for this chart; multiple runs of same templates are not considered. For example, if you run four different templates, the chart will have four slices. If you run two templates twice, the chart will have two slices.
Overall Compliance Status Over Time	This is a bar chart that displays the risk distribution of templates over the network on specific dates. The size of each slice of the bar indicates the number of templates having corresponding compliance level. ALL templates run (including multiple runs of same templates) are considered for this chart.
System Compliance Detail	This is a bar chart which displays the compliance distribution of the latest runs of templates on respective endpoints. The size of each bar area indicates the number of template runs having that compliance level.
Passed Compliance Over Time	This is a trend chart that displays the number of templates that are in compliance at a given point of time.

Viewing the Technical Compliance Dashboard

The Technical Compliance Dashboard is used to visualize the check level information of the network. When the check is run on an endpoint it can either result in “Passed”, “Failed”, or “Excepted”.

Following are the charts in the Technical Compliance Dashboard:

Chart Name	Description
Overall Compliance Status	This is a pie chart that displays the distribution of all the check runs on the endpoints based on their returned status. The size of each slice of the chart indicates the number of checks that returned with that status. Only unique template runs are considered for this chart; multiple runs of same templates are not considered. For example, if you run four different templates, the chart will have four slices. If you run two templates twice, the chart will have two slices.
Overall Compliance Status Over Time	This is a bar chart which displays the risk distribution of templates over the network on the particular dates. The size of each slice of the bar indicates the number of checks having corresponding compliance level. ALL templates run (including multiple runs of same templates) are considered for this chart.
Compliance Detail	This is a bar chart that displays the distribution of the check results for all the checks that have been run on a particular endpoint. The size of each area of bar indicates the number of checks run on that endpoint, which returned in corresponding status. The endpoints are ordered in descending order of the number of checks that have run on them.
Passed Compliance Over Time	This is a trend chart that displays the number of passed or excepted checks over time. The trend is shown for each template that has such checks.

Customizing the Dashboard

You can perform the following tasks using the options in the menu bar, to customize the Dashboard:

Creating New Dashboard

If you need your own, customized dashboard apart from the four dashboards provided, click the **New Dashboard** icon to create it. When you click this icon, an empty dashboard is displayed. In this dashboard, you can add the charts based on your requirement.

Adding Charts to Existing Dashboard

You can add charts to your dashboard by clicking the **Add Visualization** icon.

Saving the Dashboard

If you have created you own dashboard, you can save it by clicking the **Save Dashboard** icon, and providing a name of your dashboard.

Select **Store time with dashboard** while saving the dashboard to change the time filter for the dashboard to the currently applied time filter.

Loading Saved Dashboard

You can load any default or saved dashboard by clicking the **Load Saved Dashboard** icon and selecting the dashboard you want to load.

Changing the Dashboard Theme

You can update the dashboard to use the dark theme by clicking the **Options** icon and then selecting the **Use dark theme** option.

NOTE: The Secure Configuration Manager Dashboard leverages Kibana, a browser-based analytics and search dashboard, that helps you to visualize and analyze data. Apart from the customizing functionality that the Dashboard offers, you can also use the Kibana functionality to customize the Dashboard. For more information, see the Kibana documentation.

Screen Capturing and Report Sharing

The Dashboard offers reporting capabilities, which enables you to take a screenshot of your dashboard and export it in multiple formats. NetIQ recommends FireShot as the screen-capturing and sharing tool. When you download FireShot and install it on your computer, you will see the FireShot icon in your browser bar. Click on that icon to start using FireShot for screen capturing and sharing tasks.

With FireShot, you can perform the following reporting tasks:

- Capture screenshot: You can capture entire dashboard screen, or a selected screen area.
- Save screenshots as image or PDF: You can save the captured screenshot in various formats: image (.jpg or .png) or as PDF.
- Print screenshot: You can directly print the screenshot, or copy it to a clipboard.

You can send the saved screenshot file (image or pdf) though email, and use it for any other report sharing purpose.

NOTE: You can also use any other screenshot capturing tool to achieve screen-capturing and reporting with the Dashboard.

---

8 Using Dynamic Reports to Evaluate Endpoints

Available only in the Web console.

Secure Configuration Manager allows you to combine the results of multiple policy templates into a **dynamic report**. This aggregated report can include results for a variety of endpoints, regardless of operating system or application type, rather than having an individual report for each policy template. You can create custom the report definitions from which users can generate dynamic reports.

Secure Configuration ManagerSecure Configuration ManagerWhen you generate a report, gathers the data from the database rather than collecting data in real-time from the specified endpoints. The data is always from the last successful run of the policy templates against the endpoints specified in the report definition. However, the reports can include a trend graph if data for multiple runs is available within the specified time frame for collecting report data.

- "Checklist for Using Dynamic Reports to Evaluate Assets" on page 107
- "Building Dynamic Reports" on page 108
- "Evaluating Endpoints with a Dynamic Report" on page 108

Checklist for Using Dynamic Reports to Evaluate Assets

The following checklist provides a guide for creating and reviewing dynamic reports to assess the state of compliance and risk in your environment.

	Checklist Items
❑	1. Run policy templates associated with your security policies against the endpoints or groups that you want to assess.
❑	2. Decide which type of dynamic report you want to build for each set of endpoints/groups or policy templates: compliance-based, risk-based, or a snapshot of endpoint status.
❑	3. (Optional) Create report definitions that match your various security needs so users can generate reports on demand. For more information, see "Building Dynamic Reports" on page 108.
❑	4. (Optional) Generate dynamic reports on demand from the **Endpoints** or **Policy Template** pages in the Web console. For more information, see the Help in the Web console.
❑	5. Review the generated dynamic reports to determine the status of your IT environment. For more information, see "Evaluating Endpoints with a Dynamic Report" on page 108.
❑	6. Resolve the issues that you identify in the reports, then run the reports again to ensure ongoing compliance to your security standards.

Building Dynamic Reports

You can generate a dynamic report at any time. However, before getting started, you might want to run policy templates associated with your security standards. A dynamic report can only display data for policy templates that have been run against the selected endpoints within the specified time frame. If the policy templates within the report have not been run against the specified endpoints, the Web console cannot display the report or the report will have incomplete data.

When you generate a dynamic report, you can save the configuration as a report definition. Each **report definition** contains a set of policy templates and endpoints associated with a particular need, such as PCI compliance. You also set the time frame from which you want to draw the data. For example, you want a snapshot of the compliance status for endpoints in the Finance department within the last 30 days, based on 10 different policy templates.

Once you create report definitions, console users can generate reports from the definition. They specify a name and description for their report without affecting the report definition.

For more information, see the Help in the Web console.

Evaluating Endpoints with a Dynamic Report

Dynamic reports align with three categories:

- "Snapshot Report - Evaluating Your Endpoints" on page 108
- "Compliance Report - Evaluating Your Endpoints" on page 108
- "Risk Report - Evaluating Your Endpoints" on page 109

For more information, see the Help in the Web console.

Snapshot Report - Evaluating Your Endpoints

Snapshot reports provide a high-level view of the state of risk and compliance for the specified endpoints or groups of endpoints, based on the selected endpoints. The report content is similar to the Asset Status view. However, the report focuses on the specific policy templates and endpoints rather than your entire set of assets.

While a **Snapshot** report contains the results of all the policy templates specified in the report definition, the **Overview** and **Endpoints** views display only the results for one policy template at a time. To help you identify endpoints that failed the policy template, the report lists the endpoints at risk. To determine which settings need to be corrected, you can select the high risk endpoints then view details of the security checks that they failed.

Compliance Report - Evaluating Your Endpoints

Compliance reports help you determine how the specified endpoints or groups of endpoints comply with your organization's security policies and technical standards.

- "Identify Security Policies that Need Attention" on page 109
- "Compare Compliance Results by Endpoint" on page 109

Identify Security Policies that Need Attention

In a compliance-based dynamic report, the **Policy Templates** view lists the combined results for all endpoints per policy template, so you can identify which security policies need the most attention.

For example, the report contains the results for Password Strength, PCI DSS, and CIS Benchmark policy templates run in the last 30 days on your financial servers. You can see that the Password Strength and CIS Benchmark policy templates are *In Compliance*, but the PCI DSS policy template is *Out of Compliance*. Now you can investigate your processes and endpoints that caused the non-compliant state.

Compare Compliance Results by Endpoint

The **Endpoints** view lists the compliance status of your endpoints for all policy templates in the report. This can help you compare known, good endpoints with new or questionable endpoints.

If you run the policy templates regularly for the selected endpoints, the report can display a trend graph that indicates changes in compliance over time.

Risk Report - Evaluating Your Endpoints

Risk reports help you determine whether the specified endpoints or groups of endpoints, pose a high, medium, or low security risk to your environment.

By default, the report lists the policy templates that report the highest level of risk, based on endpoint importance. You can select a policy template, then drill down to the specific endpoints to identify where they pose high, medium, and low risks in your environment.

9 Excluding Data from Runs and Reports

Secure Configuration Manager enables you to temporarily create exceptions for reported results to prevent conditions from causing a violation for a security check in a policy template. Alternatively, you can configure a security check to exclude results that match data from a saved list.

- "Excluding Values from a Run" on page 111
- "Excluding Data from Report Results" on page 113

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

- "Using Saved Lists in an Existing Security Check" on page 112
- "Importing Saved Lists" on page 112
- "Exporting Saved Lists" on page 113

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.

- "Web Console - Using Saved Lists" on page 112
- "Windows Console - Using Saved Lists" on page 112

Web Console - Using Saved Lists

When you run a security check, you can apply a saved list to any user-definable parameter in the security check, as long as the saved list's values match the parameter requirements. The Web console supports all saved lists that you create or import into the Windows console.

For more information about creating, modifying, and applying saved lists, see the Help in the Web console.

Windows Console - Using Saved Lists

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. In the Parameters window, click **Exclusion List** or **Inclusion List**, depending on the security check.
6. Type the name of the saved list or click the button at the end of the Exclusion List or Inclusion List line.
7. Select the saved list whose entries you want to exclude from or include in the security check.
8. Follow the instructions in the wizard to run the report.

Importing Saved Lists

Available only in the Windows console.

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 "Managing Permissions" on page 160.

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

Available only in the Windows console

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 "Managing Permissions" on page 160.

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**.

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 policy template run. 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.

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 "Excluding Values from a Run" on page 111.

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.

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 in the console.

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.

- "Allowing Users to Create or Manage Exceptions" on page 114
- "Excepting Endpoints or Groups from a Policy Template Run" on page 115
- "Excepting Specific Data Returned by a Security Check" on page 116

- “Excepting all Data Returned by a Security Check” on page 117
- “Avoiding the Creation of Duplicate or Similar Batch Exceptions” on page 118
- “Requiring Approval before Applying Exceptions” on page 119
- “Applying Exceptions” on page 120
- “Editing an Exception” on page 121
- “Deleting an Exception” on page 121
- “View the Status of All Exceptions” on page 122
- “Enabling Managed Groups to Inherit Parent Group’s Exceptions” on page 122

Regardless of whether you create and apply the exceptions in the Web console or Windows console, the assessment reports reflect the applied exceptions.

Allowing Users to Create or Manage Exceptions

Secure Configuration ManagerThe Web console is designed to be accessible to many individuals within your organization. However, most of these console users simply need to view the status of vulnerability and compliance. Usually, they would not need to modify asset properties or the results of assessment reports. Thus, helps you control who can make exceptions and how.

- “Allow Exceptions in the Web Console” on page 114
- “Assign Exception Permissions” on page 115

Allow Exceptions in the Web Console

In the Web console, you can specify whether users can create, edit, or delete batch exceptions, which are a combination of endpoints or groups and security checks for specified policy template runs. These exceptions apply every time the specified policy templates run against the designated endpoints or groups.

Note that users can always create exceptions for an endpoint, group, or security check within a single assessment report. However, these report-based excpetions do not affect other runs of the same policy template, endpoint, or security check.

For more information about configuring exceptions in the Web console, see the “Allowing Exceptions in the Web console” topic in the Help.

Assign Exception Permissions

Web and Windows console users must have appropriate permissions to create or manage exceptions, as shown in the following table.

User activity	Required permission
Create an exception	◆ Run Policy Template ◆ 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

For more information about assigning permissions, see "Managing Permissions" on page 160.

Excepting Endpoints or Groups from a Policy Template Run

You can except endpoints or group of endpoints from being assessed by a policy template. For example, an endpoint is under maintenance so you do not want the scheduled policy templates to run against that endpoint.

NOTE: This section provides instructions for creating the exception in the Windows console. The batch-created exceptions are an alternative method for excepting endpoints and groups from policy template runs.

1. In the Windows console, open an assessment report where the policy template has been run against the endpoints or group of endpoints.
2. Click **Data View**.
3. In the tree pane, expand **Target Endpoints** or **Target Groups** .
4. Locate the endpoint or group of endpoints that you want to except.

   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. Right-click the endpoint or group of endpoints, and then click **Create Exception**.
6. (Optional) To add selected endpoints or groups in the wizard, click the value after **from the endpoints** or **from the group**, respectively.

   The wizard lists all available endpoints or groups that you can include in the exception.
7. Complete the Exception Wizard.
8. (Conditional) If you have enabled exception approvals in the Core Services Configuration Utility, select **Needs Approval** in the wizard.

   If approvals are required, the exception must be approved before it can go into effect.

9 After completing the wizard, click **Apply Exceptions**.

The Windows console closes the report to apply the exceptions.

Excepting Specific Data Returned by a Security Check

Must be configured in the Windows console, but affects policy template runs in both consoles

Some security checks can return multiple data values, which the report displays as a combination of row and column data. For example, the **Accounts with passwords that never expire** security check in the **NetIQ Password Strength** policy template returns values for all user accounts on the `BANK_LONDON_1` endpoint. The accounts are `Guest`, `Administrator`, and `BSmith`. The security check scores each reported value separately. However, the **Total Risk** score for the security check combines the results of all the returned values. Even though the `Guest` account is disabled, it fails the check because its password is set to Never Expire. In this case, you might want to except that value from the policy template results for `BANK_LONDON_1`Secure Configuration Manager. applies the exception each time that you run the policy template against the specified endpoints or groups.

NOTE: If you create a security 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 "Understanding Risk Scoring" on page 56.

To create an exception, your console user account needs the **View Policy Template** and **New Exception** permissions.

To except specific data returned for a security check:

1 In the Windows console, open the completed report of a policy template run for which you want to create an exception.

The report must contain the endpoints or groups that you want to include in the exception.

2 Click **Data View**.

3 In the tree pane, expand **Security Checks**.

4 Select or expand the security check whose data you want to except.

5 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**.

For example, select the **Accounts with passwords that never expire** security check, then click `Guest`. If you run the policy template against multiple endpoints, ensure that you select the correct combination of endpoint and returned value. For example, select the `BANK_LONDON_1` endpoint.

6 Complete the steps in the Exception Wizard.

In the wizard you can add more data points to except for the security check. You can also add endpoints.

7 (Conditional) If you have enabled exception approvals in the Core Services Configuration Utility, select **Needs Approval** in the wizard.

If approvals are required, the exception must be approved before it can go into effect.

8 After completing the wizard, click **Apply Exceptions**.

The Windows console closes the report to apply the exceptions.

Excepting all Data Returned by a Security Check

You can create exceptions that apply to all data returned by one or more security checks in a policy template run for the specified endpoints or groups. However, the Windows and Web console provide different ways for you to create these exceptions.

Alternatively you can choose to except specific returned data only or create exceptions that apply to a single assessment report.

- "Windows Console - Exceptions that Apply to all Security Check Results for a Policy Template" on page 117
- "Web Console - Exceptions that Apply to a Single Assessment Report" on page 118
- "Web Console - Exceptions that Apply to all Security Check Results for a Policy Template" on page 118

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.

Windows Console - Exceptions that Apply to all Security Check Results for a Policy Template

Affects policy template runs in both consoles

You can exclude all results that a security check returns for endpoints or groups during a policy template. When creating the exception, you can choose to start with a security check then specify the endpoints you to to except or start specifying endpoints or groups then choose the security checks. In either case, it's the combination of endpoints or groups and security checks that are excepted when you run the policy template.

Secure Configuration Manager applies the exceptions every time that you run the specified policy template against the specified endpoints.

1. In the Windows console, open the completed report of a policy template run for which you want to create an exception.

   The report must contain the endpoints or groups that you want to include in the exception.
2. Click **Data View**.
3. In the tree pane, expand **Security Checks**.
4. Select or expand the security check whose data you want to except.
5. In the right pane, select an endpoint that you want to except for that security check.

   In the Exception Wizard, you can add more endpoints to the exception. You can also add more security checks.
6. Complete the Exception Wizard.
7. (Conditional) If you have enabled exception approvals in the Core Services Configuration Utility, select **Needs Approval** in the wizard.

   If approvals are required, the exception must be approved before it can go into effect.
8. After completing the wizard, click **Apply Exceptions**.

   The Windows console closes the report to apply the exceptions.

Web Console - Exceptions that Apply to a Single Assessment Report

When viewing a completed assessment report for a policy template, you can create exceptions that apply to a combination of the assessed endpoints or groups and security checks. These **report-based** exceptions affect only that assessment report. You can view the report and its exceptions in either console.

For example, you run the **NetIQ Audit Settings** policy template against endpoints `Texas_Bank_1` and `London_Bank_1`. In the completed report, you create an exception for the **RAS auditing** security check for the `London_Bank_1`Secure Configuration Manager endpoint. You can re-generate the report to apply the exceptions. However, if you run that policy template against the same endpoints at a later date, does not apply the exceptions. Instead of running the policy template again, you might want to re-run the assessment report to include the exceptions.

For more information, see the “Creating Exceptions within an Assessment Report” topic in the Web console Help.

Web Console - Exceptions that Apply to all Security Check Results for a Policy Template

Affects assessment reports run from the Web console only

In the Web console, you can create exceptions that apply to multiple policy templates. This **batch method** for creating exceptions requires you to specify the combination of endpoints or groups of endpoints and security checks in the chosen policy templates. Secure Configuration Manager applies the exceptions every time that you run one of the specified policy templates against the specified endpoints.

You can use this method to except an endpoint from a policy template run. When creating the exception, select the policy template then select all security checks within the template.

You can choose to enable or disable this feature. With this feature enabled, you do not have to run the policy templates against the relevant assets before creating the exceptions. However, Core Services might take longer to run a policy template because the service must first review all exceptions to determine if any need to be applied.

Secure Configuration ManagerWhen creating an exception, checks whether the exception already exists. The Web console then asks whether you want to edit the existing exception or create a new one.

For more information, see the “Creating an Exception that Contains Multiple Policy Templates” topic in the Web console Help.

Avoiding the Creation of Duplicate or Similar Batch Exceptions

Available only in the Web console

Secure Configuration ManagerIt is possible that, when you have multiple console users, those users might create exceptions that are similar or identical to existing exceptions. can help reduce the opportunity for creating duplicate or similar exceptions, thus also reducing the number of exceptions that need to be managed.

When you use the batch methodSecure Configuration Manager to create an exception in the Web console, reviews the properties of all current exceptions. If a similar exception exists, the Web console prompts you to decide whether you want to continue with the new exception or edit the existing one.

For example, an exception called `London 1 SoxCobit 3rd Party SMB Password` currently exists. This exception has the following properties:

Endpoint	BANK_LONDON_1
Policy template	NetIQ SOX/CobiT 4.1 for Windows Server
Security check	Third-party SMB server password connect setting
Reason	In Remediation

You want to create an exception for the *same* endpoint in the *same* policy template but for the **Automatic administrative logon** security check. The Web console informs you about the `London 1 SoxCobit 3rd Party SMB Password` exception and recommends that you add the **Automatic administrative logon** security check to the existing exception.

However, you can choose to create the new exception despite the similarity. For example, you might want to have a different time frame for applying the exception. Or the reason for the exception might be “Accepted Risk” rather than “In Remediation.” You cannot create a duplicate exception.

For more information about creating an exception, see the “Managing Data in Reports” topic in the Web console Help.

Requiring Approval before Applying Exceptions

By default, Secure Configuration Manager allows you to apply exceptions 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.

- “Enabling Exception Approvals” on page 119
- “Approving Exceptions” on page 120
- “Web Console - Approve Exceptions” on page 120
- “Windows Console - Approve Exceptions” on page 120

Enabling Exception Approvals

To require approvals before exceptions can go into effect, you must configure the approval process.

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

Approving Exceptions

If you enable exception approvals, users can specify **Needs Approval** while creating the exception. Core Services sends a notification email to users with the NetIQ Exception Approval Manager role. Users will also receive an email notification, which specifies the status of the approval. When the approval status of the exception changes (for example, the exception is approved), users will receive another email notification specifying the change in the approval status.

In this console...	Select...
Web	**Utilities > Exceptions**
Windows	**Exception Management > Exceptions**

Web Console - Approve Exceptions

1. Click **Utilities > Exceptions**.
2. On the **Needs Approval** or **Disapproved** tab, select the exceptions that you want to approve.
3. Click **... > Mark as approved**.

Windows Console - Approve Exceptions

1. Click **Exception Management > Exceptions**.
2. Select the exception that you want to approve.
3. On the Properties page of the wizard, click **Approved**, then click **Finish**.

Applying Exceptions

You can apply exceptions to security check results, endpoints, or groups of endpoints. When you apply the exceptions in an assessment report, the console automatically closes the report to regenerate with the applied exceptions.

- "Web Console - Applying Exceptions" on page 120
- "Windows Console - Applying Exceptions" on page 121

To apply exceptions, your console user account needs the Apply Exceptions permission. For more information about applying exceptions, see the Help in the console.

Web Console - Applying Exceptions

After you create exceptions in an assessment report, you can immediately apply the exceptions. The Web console generates the report again. In **Assessment Reports**, you can see that the Exceptions column indicates *Applied* for the re-generated report.

You can also enable and disable exceptions from **Utilities > Exceptions**.

For more information, see the Help in the Web console.

Windows Console - Applying 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**.

   Once Secure Configuration Manager applies all exceptions to the report, the report moves to the **Completed** jobs queue.

Editing an Exception

As you update your inventory and security policies, you might need to revise the exceptions that you use when assessing your environment. You can edit any property of the exception, including the defined endpoints, endpoint groups, security checks, and policy templates.

In this console...	Select...
Web	The assessment report - for a report-based exception
	Utilities > Exceptions - for a batch-created exception
Windows	**Exception Management > Exceptions**

To edit an exception, your console user account needs the View Policy Template and Edit Exception permissions.

NOTE: 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.

Deleting an Exception

Secure Configuration ManagerAs you update your inventory and security policies, you might need to remove the exceptions that you use when assessing your environment. When you delete an exception, removes the exception from the database. As an alternative to deleting an exception, you might want to disable that exception, which prevents the exception from functioning but keeps the properties in the database.

In this console...	Select...
Web	**Utilities > Exceptions**
Windows	**Exception Management > Exceptions**

To delete an exception, your console user account needs the Delete Exception permission. For more information, see “Managing Permissions” on page 160.

NOTE: Secure Configuration ManagerWhen you delete an exception, 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.

View the Status of All Exceptions

You must be a console administrator or have the Exception Approval Manager role to perform this task

Secure Configuration ManagerYou can review the status of all exceptions created in . For example, you might want to identify exceptions that await approval.

- "Web Console - View Exceptions" on page 122
- "Windows Console - View Exceptions" on page 122

Web Console - View Exceptions

Select **Utilities > Exceptions**.

You can review currently applied exceptions, those in need of approval, and those that have been disapproved. You can delete, edit, and enable/disable exceptions from this page. You can also export a CSV file that contains information about any exceptions that you specify.

For more information, see the Help in the Web console.

Windows Console - View 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 "Managing Permissions" on page 160.

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.

Enabling Managed Groups to Inherit Parent Group's Exceptions

You must be a console administrator to perform this task.

You can enable managed groups to inherit its immediate parent group's exceptions by performing the following steps:

1. Go to the **Advanced** tab in the Core Configuration Utility.
2. Set the value of the **gladiator/exception/parent/enabled** field to `true`.
3. Restart **NetIQ Core Services**.

10 Comparing Results of Assessments

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.

- "Using a Dynamic Report to Compare Endpoints" on page 123
- "Running Reports from the Database" on page 124
- "Comparing Security Check Results for Two Endpoints" on page 125
- "Comparing Policy Template Results" on page 125
- "Filtering a Delta Report" on page 126
- "Scheduling a Delta Report" on page 127
- "Distributing Delta Reports to a File Share or Folder" on page 128
- "Distributing Delta Reports to an Email Recipient" on page 129
- "Exporting a Delta Report" on page 130

Using a Dynamic Report to Compare Endpoints

Available only in the Web console.

Dynamic reports generated from the **Compliance** category help you compare known, good endpoints with new or questionable endpoints. As shown in the example below, the **Endpoints** view lists the compliance status of each endpoint assessed per each policy template in the dynamic report. Sort the results by any of the columns, such as Compliance or Name of the endpoint. Select **Change** to view the results for one of the other policy templates in the report.

Figure 10-1 *Excerpt from a compliance-based dynamic report*

If you run the policy templates regularly for the selected endpoints, the report displays a trend graph that indicates changes in compliance over time. So you can verify the rate of improvement as you resolve the discovered vulnerabilities.

Running Reports from the Database

Available only in the Windows console.

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.

Comparing Security Check Results for Two Endpoints

Available only in the Windows console.

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 "Filtering a Delta Report" on page 126.
9. To view the report, double-click the report name in the **Completed** jobs queue.

Comparing Policy Template Results

Available only in the Windows console.

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 "Filtering a Delta Report" on page 126.

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 "Filtering a Delta Report" on page 126.

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.

Filtering a Delta Report

Available only in the Windows console.

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 "Distributing Delta Reports to a File Share or Folder" on page 128 and "Distributing Delta Reports to an Email Recipient" on page 129.

Scheduling a Delta Report

Available only in the Windows console.

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 "Comparing Policy Template Results" on page 125.
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.

Distributing Delta Reports to a File Share or Folder

Available only in the Windows console.

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 "Managing Permissions" on page 160.

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 *Secure Configuration Manager Installation Guide*.
- 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 "Filtering a Delta Report" on page 126.

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 "Comparing Policy Template Results" on page 125.
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 create 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.

Distributing Delta Reports to an Email Recipient

Available only in the Windows console.

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 *Secure Configuration Manager Installation Guide*.
- 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 "Filtering a Delta Report" on page 126.

To distribute delta report results through email:

1. Ensure that at least one run of the policy template is complete. For more information, see "Comparing Policy Template Results" on page 125.
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 compress 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.

Exporting a Delta Report

Available only in the Windows console.

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" on page 130
- "Exporting Delta Report Data" on page 130

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 *Secure Configuration Manager Installation Guide*.
- 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 "Filtering a Delta Report" on page 126.

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 "Filtering a Delta Report" on page 126.

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**.

11 Predicting Vulnerability and Compliance Problems

Available only in the Web console.

Being able to predict vulnerability and compliance issues can help you reduce the number of policy templates that you must run and review to assess your assets.

Many policy templates use the same security checks to assess an endpoint's vulnerability to security breaches or compliance with a regulation, standard, or benchmark. If an endpoint fails security check instances in one policy template run, that endpoint will fail the same instances in another policy template. When you click **Vulnerability & Compliance Prediction** in an assessment report, Core Services identifies the security checks and check instances that the assessed endpoints failed, then reviews all policy templates that include the same security checks and instances. After completing the review, the Web console lists all regulations, standards, and benchmarks that the assessed endpoints might fail.

For example, you ran the **NetIQ SOX/CobiT 4.1 for Windows Server** policy template against your `BANK_LONDON_1` server. The endpoint failed the **Third-party SMB server password connect setting** security check. Core Services can predict that the endpoint will also fail the **NetIQ PCI DSS 2.0 for Windows Server** policy template, which includes that security check.

The prediction includes the following information:

- The regulations, standards, and benchmarks that might be affected.
- Number of policy templates that might be affected.
- Percent and number of security checks in all potential policy template runs that might be affected.
- Details about the affected security checks so you can determine whether those security checks are worth acting upon. If a security check is not important to the endpoint, you can create exceptions for the assessment.

For more information about applying the prediction algorithm, see the Help in the Web console.

IV Customizing Secure Configuration Manager

This section helps you customize Secure Configuration Manager for your IT enviroment. You manage who accesses the consoles, configure the default settings for Secure Configuration Manager, and manage the tags that can be applied to your assets.

- Chapter 12, “Customizing Secure Configuration Manager,” on page 137
- Chapter 13, “Configuring the Consoles and Dashboard,” on page 145
- Chapter 14, “Setting Security on the Secure Configuration Manager Console,” on page 153

12 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.

- "Creating and Applying Tags" on page 137
- "Creating Custom Tasks and Reports" on page 137
- "Customizing the Job Queues" on page 139
- "Customizing Core Services" on page 141
- "Enabling FIPS Communication" on page 143

Creating and Applying Tags

Available only in the Web console.

If you have an Administrator role, you can create **tags**Secure Configuration Manager to serve as customized labels that help users to identify, organize, and search for the followin objects in :

- endpoints
- policy templates

You can create and apply an unlimited number of tags. For example, you might create standard tags, such as *UNIX* and *SQL*, that apply to a large number of endpoints. Then you might add more specific identifiers for particular endpoints, such as *Web server* to indicate the endpoint's purpose or *HIPAA* to denote that an endpoint or group must meet the particular security policy.

You can also view which objects are associated with a particular tag. An **association** represents the link between a tag and the endpoints, groups, policy templates, and security checks mapped to that tag. When you delete a tag, you also remove all of the associations for that tag.

All Web console users can view the tags. They can also search for an object by a tag.

To create tags, select **Utilities > Tags**. To apply a tag, navigate to the object that you want to tag. For more information, see the Web console Help.

Creating Custom Tasks and Reports

Available only in the Windows console.

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 Part II, "Auditing Your Managed Assets," on page 45.

Secure Configuration Manager also enables you to customize the logo displayed on all reports. For more information about changing the logo, see "Changing the Logo on the Report" on page 139.

- "Creating Custom Tasks" on page 138
- "Creating Groups of Custom Tasks" on page 138
- "Changing the Logo on the Report" on page 139

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 "Creating Groups of Custom Tasks" on page 138.

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.

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 "Managing Roles" on page 158.

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 "Managing Permissions" on page 160.

Changing the Logo on the Report

Secure Configuration ManagerYou have the option of displaying your company logo or the NetIQ logo in your completed reports. By default, 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.

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.

Use the **Prev** and **Next** buttons at the bottom of the console to navigate to the previous and next set of records.

- "Setting the Retention Period" on page 140
- "Using Folders to Organize Completed Jobs" on page 140

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 "Exporting Assessment Results" on page 87, "Exporting a Delta Report" on page 130, and "Creating Groups of Custom Tasks" on page 138.

Using Folders to Organize Completed Jobs

Available only in the Windows console.

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.

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.

- "Accessing the Advanced Tab" on page 141
- "Enabling Event Logging" on page 141
- "Enabling Interim Local Storage of Microsoft Excel Reports" on page 142
- "Enabling the Ability to Distribute Reports Only if the Score Is Greater Than Zero" on page 142
- "Configuring Scheduled Jobs Behavior when Core Services Restarts after a Downtime" on page 142

Accessing the Advanced Tab

By default, the Core Services Configuration Utility does not display the **Advanced** tab.

1. Close the utility, if it is open.
2. Run the `config.bat` program, by default in the *`installation_directory`*`\Core Services\bin` folder.
3. Open the Core Services Configuration Utility.
4. Select the **Advanced** tab.

Enabling Event Logging

You can enable event logging in Secure Configuration Manager and use the event log file as input to any other application. Once you enable Core Services to log events, you can specify whether to gather data from Web console sessions.

- "Configuring Core Services to Log Events" on page 141
- "Enabling Logging for Web Console Sessions" on page 142

Configuring Core Services to Log Events

To enable event logging:

1. Go to the **Advanced** tab in the Core Configuration Utility.
2. Set the value of the **eventlog/enabled** field to `true`.
3. Restart **NetIQ Core Services**.

You can now find the events information in the `C:\Program Files (x86)\NetIQ\Secure Configuration Manager\Core Services\log\smevent.log` file.

NOTE: For more information, see the Core Services Configuration Utility online help.

Enabling Logging for Web Console Sessions

When you enable logging for the Web console, Secure Configuration Manager stores information such as error messages and warnings in the event log.

For more information about enabling logging in the Web console, see “Logging Web Console Activity” in the Help.

Enabling Interim Local Storage of Microsoft Excel Reports

You can enable interim local storage of Microsoft Excel reports to enhance the report distribution performance.

Secure Configuration Manager saves Microsoft Excel reports in a local directory (`C:\Program Files (x86)\NetIQ\Secure Configuration Manager\Core Services\tmp`) in the interim, while also saving them in a network location. If there is a network connectivity outage and reports are not saved in the network location, you can manually copy the reports from the local directory to the network location.

To enable Secure Configuration Manager to save Microsoft Excel reports in a local directory:

1. Go to the **Advanced** tab in the Core Configuration Utility.
2. Change the value of the **gladiator/report/Report Export Save Excel Locally/Enabled** field to `true`.
3. Restart **NetIQ Core Services**.

Enabling the Ability to Distribute Reports Only if the Score Is Greater Than Zero

You can configure Secure Configuration Manager to distribute reports only if the score is greater than zero.

Perform the following steps:

1. Go to the **Advanced** tab in the Core Configuration Utility.
2. Set the value of the **gladiator/EnableDistributionOnlyOnViolation** field to `true`.

   If you set this value to `false`, Secure Configuration Manager distributes all the reports, irrespective of the score.
3. Restart **NetIQ Core Services**.

NOTE: For more information, see the Core Configuration Utility online help.

Configuring Scheduled Jobs Behavior when Core Services Restarts after a Downtime

You can configure scheduled jobs to not run immediately when the Core Services restarts after a downtime. This helps you to avoid too many jobs simultaneously running after Core Services starts.

For example, if the Core Services computer has stopped at 9 a.m. because of an outage and restarts at 10.30 a.m., and you have scheduled 25 jobs to run at 10 a.m., those jobs might run immediately after Core Services restarts.

Perform the following step to configure scheduled jobs to not run immediately after Core Services restarts following a downtime:

1. Go to the **Advanced** tab in the Core Configuration Utility.
2. Set the value of the **scheduler/jobs/disabled** field to `True`.
3. Restart **NetIQ Core Services**.

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.

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 "Connecting the AutoSync Client to Core Services in a FIPS-Enabled Environment" on page 185.

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**.

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: 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.

13 Configuring the Consoles and Dashboard

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.

- "Modifying the Session Timeout Settings" on page 145
- "Configuring the Web Console" on page 145
- "Configuring the Windows Console" on page 146
- "Configuring the Web-based and Asset Compliance Content" on page 147
- "Setting up the Dashboard for Your Users" on page 149

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.

Configuring the Web Console

The Web console must connect to the Analytics Database to properly display asset results. Also, you can enable users to launch the Dashboard from the Web console without having to log in again.

- "Ensuring Web Console Performance" on page 145
- "Launching the Dashboard from the Web Console" on page 145
- "Allowing Users to Batch-create Exceptions" on page 146
- "Logging Web Console Activity" on page 146

Ensuring Web Console Performance

To perform appropriately, the Web console needs access to the Analytics Database. The installation process automatically informs the Web console of the location of the Analytics Dashboard.

To verify or update the database location, go to ***Your_ID*** **> Settings > Analytics Dashboard** in the Web console.

Launching the Dashboard from the Web Console

For Web console users to open the Dashboard without having to log in again, the Web console and Dashboard must be in the same domain. The Web console must also know the Dashboard's location.

To configure single sign-on:

1 In the Web console, go to ***Your_ID*** **> Settings > Dashboard**.

2 Specify the IP address or host name and the port for the Dashboard server.

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

Allowing Users to Batch-create Exceptions

You can specify whether Web console users can create an exception that includes multiple policy templates. If allowed, users with appropriate permissions can create, edit, delete, and change the enable or approval status for this batch method of creating exceptions.

For more information, see the Help in the Web console.

Logging Web Console Activity

When you enable logging for the Web console, the browser records data in the browser's console log, such as errors, warnings, and information messages. Technical Support can review this data to help diagnose problems that might occur in the Web console.

For more information, see the Help in the Web console.

Configuring the Windows 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.

- "Changing the View of the Asset Map" on page 146
- "Modifying Windows Console Settings" on page 146
- "Improving Console Performance" on page 147

Changing the View of the Asset Map

The Windows console displays the asset map 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.

Modifying Windows Console Settings

The Windows console options 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.

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**.

Configuring the Web-based and Asset Compliance Content

To properly display content, the Web console, Dashboard, and Asset Compliance View rely on settings in the Core Services Configuration Utility.

- “Configuring Web Services” on page 148
- “Configuring Data Settings” on page 148

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 Secure Configuration Manager Dashboard and the Web console. By specifying a port number, you can meet your unique environment needs. For example, your security policy might dictate that Web applications use specific ports or you might need to accommodate a network firewall.

Web services must be enabled for the Web console, Asset Compliance View, and the Secure Configuration Manager Dashboard to function.

1. On the Core Services computer, start the Core Services Configuration Utility, located by default in the NetIQ Secure Configuration Manager program folder.
2. On the **Web Services** tab, change **Enable Web Services** to **true**.
3. Click **OK** to save the changes and close the Configuration Utility.

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 Web console, Asset Compliance View, and the Secure Configuration Manager Dashboard.

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 "Understanding Risk Scoring" on page 56. For more information about email alerts, see "Automating Out-of-Compliance Notifications" on page 77.

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.

Setting up the Dashboard for Your Users

As a Secure Configuration Manager administrator, you can configure the Dashboard settings and assign access rights to other users.

Click your user name and select **Configuration** in the Kibana menu bar. The Dashboard Settings page has General Settings, Geolocation, and Authorization options.

- "Working with Authorization Settings" on page 149
- "Working with Geolocation Settings" on page 149
- "Working with General Dashboard Settings" on page 150

Working with Authorization Settings

As an administrator, you can configure authorization settings for other user roles.

To configure authorization settings for user roles:

1. Click **Authorization** in the Dashboard Settings page.
2. Select the user role for which you need to configure the authorizations settings from the **User Roles** list.
3. Click **Edit** in the **Groups** tab. The corresponding groups associated with the user role you have selected in step 1 are displayed in this list. Select the groups for which the user role you have selected can view the data, and click **Save**.
4. Click **Edit** in the **Templates** tab. The corresponding templates associated with the user role you have selected in step 1 are displayed in this list. Select the templates for which the user role you have selected can view the data, and click **Save**.

For example, if you are configuring authorization settings for the NetIQ Windows Admin user, you can select the Windows group from the Groups list, and select only the Windows templates from the Templates list. This results in the NetIQ Windows Admin users viewing only the data about Windows groups and from Windows templates.

NOTE: The Administrator role is not displayed in the **User Roles** list to select for configuring authorization settings, because the users belonging to this role will have full privileges. As an administrator, you can view the data from all the template runs on all the groups.

Working with Geolocation Settings

The Dashboard comprises three geolocation charts, which display compliance data in world map view. For these chart to be functional, you must set the geographical locations of your environment, so that the data is displayed in these charts.

To configure the geolocation settings as an administrator:

1. Click **Geolocation** in the Dashboard Settings page.

   A table with already existing geolocation mappings, if any, is displayed.
2. To add a new geolocation mapping, click the **New** icon adjacent to the table.

   Select geolocation window is displayed.

   2a Specify the following information:

   - Location: Name of the location that you want to add as a geolocation.

- IP Range: The IP address range of the endpoints that you want to monitor and view the data for.

  NOTE: You must specify a value for at least one of the above two fields.

- Latitude: Latitude of the location.
- Longitude: Longitude of the location.

2b Click the **Save** icon.

The geolocation mapping you added is displayed in the Geolocation Mapping table.

You can edit or delete the geolocation mappings in the table by clicking the **Edit** or **Delete** icons that are present adjacent to the geolocation mapping record.

You can also add multiple geolocation mappings to this table by following the same procedure.

You can also import and export geolocation mappings as Microsoft Excel files. Click the **Import** icon to import geolocation mappings that you might have already saved in your computer and want to apply those mappings to the Dashboard. Also, you can export the existing geolocation mappings by clicking the **Export** icon.

3 Click **Apply Geolocation** after adding the necessary geolocation mappings.

This updates the existing geolocation data, which is already synchronized to the Dashboard database from Secure Configuration Manager, and enables you to view the geolocation data in the charts. After a geolocation mapping is applied, any new data that is synchronized to the Dashboard database will be displayed in the geolocation charts.

4 A confirmation message is displayed. Click **Apply** to apply the geolocation mappings.

After configuring the geolocation settings, you can view the geolocation charts in the Dashboard populated with data whenever applicable.

Working with General Dashboard Settings

To configure the general Dashboard settings, click **General** in the Dashboard Settings page. You can configure the following settings:

Startup Dashboard

This is the name of the dashboard that will be displayed when users log in to the Dashboard. For more information about these dashboards, see "Viewing the Secure Configuration Manager Dashboard" on page 100.

Validate User in Every

This is the time interval at which the user sessions are revalidated. The Dashboard communicates with Secure Configuration Manager at this interval and validates the user whose session is presently on.

Data Pull Interval

This is the time interval at which the Dashboard connects to the Secure Configuration Manager database and receives fresh data.

Retain Data For

This is the time interval till which the Dashboard retains the data in the Dashboard Database.

NOTE: When you update the above three fields, the new value is applied only after the current intervals are completed. If you want to update the values immediately, restart the **Elasticsearch 2.0.0 (NetIQDatabaseService)** service.

Click **Save** after you update the value in any of these fields.

If you update these values, new values will be applied only for a new session of the Dashboard. If you want the new values to be applied immediately, log out of the Dashboard and log in again.

Resetting Built-in Dashboards

Click **Reset built-in dashboards** to reset any updates done to the four built-in dashboards. Any customization done to any of these dashboards will be overridden, and the dashboards will be set to the default configurations. Any custom dashboards you might have created will not be affected by this operation.

14 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.

- "Console Security Checklist" on page 153
- "Understanding Console Security" on page 154
- "Managing User Authentication" on page 155
- "Managing Password Policy" on page 157
- "Managing Roles" on page 158
- "Managing Permissions" on page 160
- "Managing Console Users" on page 162

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 "Understanding Console Administrators" on page 154.

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 "Understanding Console Security" on page 154.
❑	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 *Secure Configuration Manager Installation Guide*.
❑	3. Determine whether you want to implement an external authentication source to validate the console users. See "Managing User Authentication" on page 155.
❑	4. Determine whether you want Secure Configuration Manager to enforce password policy on the console user accounts. See "Managing Password Policy" on page 157.
❑	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 "Creating a Console User" on page 163.
❑	6. Determine which sets of roles and permissions you want to assign to those users. If needed, create the appropriate roles. See "Managing Roles" on page 158 and "Managing Permissions" on page 160.

	Checklist Items
❑	7. Assign the appropriate roles and permissions to the appropriate console users. See "Assigning Roles to a Console User" on page 163 and "Assigning Permissions to a Console User" on page 163.
❑	8. Assign limit to the number of concurrent web or console sessions for required roles. See section "Assigning Session Limit to Roles" on page 159

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.

- "Understanding Console Users" on page 154
- "Understanding Console Administrators" on page 154
- "Understanding Console User and Administrator Auditing" on page 155

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 "Managing Roles" on page 158 and "Managing Permissions" on page 160.

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 "Managing User Authentication" on page 155.

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.

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 "Managing Permissions" on page 160.

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 2012 or later domain controller or a Sun ONE Directory Server version 5.2 running on a Windows 2012 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 2012 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 "Implementing External Authentication" on page 156. 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 "Managing Console Users" on page 162.

- "Implementing External Authentication" on page 156
- "Configuring a Secure LDAP Authentication Source" on page 157

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**.

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 "Implementing External Authentication" on page 156, and enter `ldaps://ldap server:636` as the LDAP Server URL value in Step 3 on page 156.

Managing Password Policy

Available only in the Windows console.

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**.

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.

- "Default Roles" on page 158
- "Creating, Modifying, and Deleting Roles" on page 159
- "Assigning Session Limit to Roles" on page 159

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 "Understanding Console Administrators" on page 154.

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 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.

Creating, Modifying, and Deleting Roles

Available only in the Windows console.

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 “Managing Permissions” on page 160.

Assigning Session Limit to Roles

Available only in the Windows console.

You can limit the maximum number of concurrent web and client console sessions for each user in a role by assigning Session Limit to the role. You can specify Session Limit for any role. Users under that role can then launch the maximum number of concurrent console and web sessions the Session Limit allows. The default value of Session Limit is unlimited. If you do not specify the Session Limit for a role, users included in the role can use an unlimited number of concurrent sessions.

A user who reaches the Session Limit for a specific role and launches another session, the user receives a message on the active computer stating that maximum limit is reached and the user must 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. If the user chooses to keep the oldest session, then the user cannot launch a new session.

Session Limit for Users with Multiple Roles

Available only in the Windows console.

If a user has multiple roles and session limits, the precedence of the session limits is as follows:

- The Session Limit that has the highest numerical value among the roles is applicable for that user.

  If a user is added or removed from any role, the Session Limit that has the highest value among the remaining roles will be applicable for that user.
- The highest numeric value of Session Limit takes precedence over the default value. The default value (`Unlimited`) is not considered in the session limit calculation.

Managing Permissions

Available only in the Windows console.

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 "Managing Roles" on page 158.

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 "Resolving Permission Conflicts and Inheritance" on page 161. Be aware that permissions explicitly assigned to a console user can override permissions implicitly granted through roles.

- "Resolving Permission Conflicts and Inheritance" on page 161
- "Modifying Permission Assignments" on page 162

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 "Modifying Permission Assignments" on page 162 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

Modifying Permission Assignments

You can add or remove permission assignments from console users and roles. For more information, see "Assigning Permissions to a Console User" on page 163 and "Creating, Modifying, and Deleting Roles" on page 159.

Managing Console Users

Available only in the Windows console.

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

- "Creating a Console User" on page 163
- "Assigning Roles to a Console User" on page 163
- "Assigning Permissions to a Console User" on page 163
- "Working with Console User Accounts" on page 163

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 "Implementing External Authentication" on page 156.

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 "Creating, Modifying, and Deleting Roles" on page 159.

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 "Managing Permissions" on page 160.

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

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 "Modifying Permission Assignments" on page 162.

V Integrating with a SIEM Solution

Secure Configuration ManagerThis section helps you integrate with Security Information and Event Management (SIEM) solutions.

- Chapter 15, “Secure Configuration ManagerPreparing for Integration,” on page 167
- Chapter 16, “Secure Configuration ManagerIntegrating with ArcSight,” on page 173
- Chapter 17, “Integrating Secure Configuration Manager with Sentinel,” on page 175
- Chapter 18, “Integrating Secure Configuration Manager with Splunk,” on page 179

15 Secure Configuration ManagerPreparing for Integration

You must be a console administrator to perform this action

Knowledge of policy compliance in relation to assessment activity allows the SIEM administrator to:

- Verify that configuration compliance is in line with IT asset activity
- Verify compliance to configuration in times of anomalous activity
- Determine if IT asset activity resulted in changes that affect policy compliance

Secure Configuration ManagerTo send events to a SIEM solution, you must configure Core Services. You must also ensure policy template runs send the assessment results to the SIEM server.

- "Understanding Integration with a SIEM Solution" on page 167
- "Secure Configuration ManagerConfiguring for SIEM Integration" on page 169

Understanding Integration with a SIEM Solution

Secure Configuration Manager sends information about the compliance status of an endpoint as an event to the following SIEM solutions:

- Micro Focus ArcSight
- Micro Focus Sentinel
- Splunk Enterprise Server

Secure Configuration ManagerEach event contains applicable attributes of the endpoint, such as asset name and IP address. generates event data in near real-time, subject to latency factors such as network traffic and connectivity.

- "Understanding the Component Architecture" on page 168
- "Understanding Data Storage Requirements" on page 168

Understanding the Component Architecture

As shown in the following diagram, Core Services connects to the data receiver component of the SIEM solution through a TCP/IP or UDP connection. Then Core Services sends the compliance data in common event format (CEF) to ArcSight and Splunk. Core Services sends event data to Sentinel using a proprietary format that adheres to Sentinel's taxonomy.

Understanding Data Storage Requirements

Secure Configuration ManagerYou can configure to attach a detailed report to each event that it sends to Sentinel. To store assessment events and reports, you should plan to have an estimated 1.7MB per event .

To help you with calculating storage needs, you might want to review "System Sizing Information" for Sentinel.

Secure Configuration ManagerConfiguring for SIEM Integration

You can configure Core Services to send an event to the SIEM solution when an endpoint'Secure Configuration Managers assessment results exceed the risk score or compliance threshold. You can have attach a detailed report to each event it sends to the SIEM solution. For more information about how this might affect hardware requirements on the SIEM server, see "Understanding Data Storage Requirements" on page 168.

- "Configuring the Basic Settings for SIEM Integration" on page 169
- "Adding the SIEM Server to Core Services" on page 170
- "Specifying the Assessments to Include in Event Data" on page 170
- "Customizing the Event Data Sent to the SIEM Server" on page 170

Configuring the Basic Settings for SIEM Integration

1 Open the Core Services Configuration Utility in Advanced mode.

   For more information, see "Accessing the Advanced Tab" on page 141.

2 Click **Forward Assessment Report**, then complete the following steps:

   2a For **Forward Events of Assessment Result**, specify **Enabled**.

   2b For **Destination Server**, specify the URL of the SIEM server that will receive the events.

   2c For **Destination Server Credentials**, specify the user name and password of the SIEM server.

   2d (Conditional) If the SIEM server exists in a multi-tenant environment, specify the **Tenant Name** (or department name) for which you want to send events.

   Core Services uses the default value if you do not specify a tenant name.

   2e (Optional) Customize the settings for sending assessment events. For more information, see "Customizing the Event Data Sent to the SIEM Server" on page 170.

3 Click **Advanced**.

4 (Conditional) When integrating with ArcSight or Splunk, specify **true** for **assessment/Thirdparty/SIEM/AppIntegration/Enabled**.

5 (Conditional) When integrating with Sentinel, specify one of the following values for **assessment/Check/Include**:

   True

   Sends a report to the SIEM server for each security check that is run as part of a policy template.

   NOTE: Many of the commonly run policy templates include a large number of security checks. Some policy templates have more than 100 security checks.

   False

   Sends a consolidated report to the SIEM server for each policy template that you run.

6 Click **Apply** to apply the settings.

7 Restart the **NetIQ Core Services** service.

Adding the SIEM Server to Core Services

Core Services must know the connection settings for the SIEM server.

1 Open the `thirdpartysiem.csv` file, located by default in the `NetIQ\Secure Configuration Manager\Core Services\etc` folder.

2 Add entries to the file that specify the connection settings for each SIEM server to which you want to send event data. Use the following format:

```
IP_address:port,protocol
```

For example:

```
162.99.123.245:524,TCP
```

Specifying the Assessments to Include in Event Data

Secure Configuration ManagerYou can configure to always send event data for specific policy templates and security checks.

NOTE: When users run any policy template or a security check in the console, they can select the **Forward Assessment Report to Destination Server** option to send out-of-compliance results to the SIEM server. For more information, see "Automating Out-of-Compliance Notifications" on page 77.

---

1 Secure Configuration ManagerLog in to the Windows console.

2 Navigate to **Go > Assessment Configuration**.

3 Select the policy templates or security checks that you want to always trigger event data.

Customizing the Event Data Sent to the SIEM Server

1 Open the Core Services Configuration Utility.

2 For **Forward Assessment Events**, specify the type of data that you want to send as assessment events:

By Asset

Secure Configuration ManagerSends a report for each asset that assesses (for example, an endpoint).

Secure Configuration ManagerIf you run a policy template against 100 assets, sends 100 reports.

By Policy

Sends a report for each policy template run.

Secure Configuration ManagerIf you run two policy templates against 100 assets in your enterprise, sends two reports. Each report contains information about the endpoints that were assessed.

By Asset and Policy

Sends a report for each asset assessed and policy template run.

Secure Configuration ManagerIf you run two policy templates against 100 assets in your system, sends 102 reports: two reports that contain information about all the assets (generated for two policy templates) and 100 reports that contain information about each asset.

3 For **Enable Events for Compliant Results**, specify whether you want to send events when an endpoint's assessment results shows as in compliance.

4 For **Enable Events for Out Of Compliance Results With**, specify whether you want to send events when an endpoint's assessment results are out of compliance, based on the reported risk score:

False

Specifies that you do not want to send out-of-compliance assessment events.

Low Risk and Above

Specifies that you want to send events for assessment results that report at any risk level.

Medium Risk and Above

Specifies that you want to send events only for assessment results that report as a medium or high risk.

High Risk

Default value

Specifies that you want to send events only for assessment results that report as high-risk.

For more information about risk scores, see "Understanding Risk Scoring" on page 56.

5 For **Enable Events where Results are Incomplete**, specify whether you want to send events when an endpoint's assessment results show unknown compliance.

6 Click **Apply** to apply the settings.

7 Restart the **NetIQ Core Services** service.

16 Secure Configuration ManagerIntegrating with ArcSight

Secure Configuration Manager can send information to ArcSight Dashboard for Enterprise administrator reference as events, communicating whether the endpoint is in compliance, out of compliance, or of unknown compliance. Enterprise administrator can generate various reports on configuration compliance, and can also trigger alerts and actions such as sending emails for anomalous activity.

- "Configuring ArcSight" on page 173
- "Secure Configuration ManagerViewing Raw Events in ArcSight" on page 173
- "Viewing the ArcSight Dashboard" on page 173
- "Secure Configuration ManagerGenerating Alerts on Events" on page 174

Configuring ArcSight

Configure a receiver in ArcSight to accept events from Secure Configuration Manager server, as shown in the following figures.

1. Log in to ArcSight.
2. In **Configuration > Receivers**, select **Add**.
3. Specify the **Name** and **Type**Secure Configuration Manager of the receiver that you want to use for events.
4. Click **Next**, then complete the process.

Secure Configuration ManagerViewing Raw Events in ArcSight

Secure Configuration ManagerYou can view events in the ArcSight **Search**Secure Configuration Manager panel. Whenever runs a policy template, Core Services forwards the events to the ArcSight sever.

Viewing the ArcSight Dashboard

You can generate a number of reports in the ArcSight Dashboard using saved searches, such as top policies and compliance distribution.

Secure Configuration ManagerGenerating Alerts on Events

Secure Configuration ManagerYou can generate alerts on events based on saved searches. The alerts can include various actions, such as email notifications and syslog event source. To configure alert generation for saved searches, see the ArcSight documentation.

17 Integrating Secure Configuration Manager with Sentinel

Secure Configuration Manager can send information to Sentinel as events, communicating whether the endpoint is in compliance, out of compliance, or of unknown compliance.

- "Sending Events in FIPS Mode" on page 175
- "Viewing Assessment Events in Sentinel" on page 177

Sending Events in FIPS Mode

Secure Configuration Manager can send events to Sentinel when either or both of the applications are in FIPS mode. For more information about FIPS Mode, see "Enabling FIPS Communication" on page 143.

- "Sentinel is in FIPS Mode" on page 175
- "Secure Configuration Manager is in FIPS Mode" on page 176
- "Secure Configuration ManagerBoth and Sentinel are in FIPS Mode" on page 176

Sentinel is in FIPS Mode

For information about FIPS mode configuration in Sentinel, see the Sentinel Documentation.

Secure Configuration ManagerSecure Configuration ManagerBy default, Sentinel uses a NSS provider when FIPS mode is enabled. To connect to the server, you need to add the server certificate to Sentinel's NSS truststore.

Secure Configuration ManagerUse keytool to export the certificate to Sentinel NSS truststore from `vssl.keystore`. Keytool is located by default in the `C:\Program Files (x86)\NetIQ\Secure Configuration Manager\Core Services\jre\bin` folder.

1. Secure Configuration ManagerTo export the certificate, enter the following command:

   ```
   keytool.exe -export -keystore ..\..\etc\vssl.keystore -alias
   alias_of_keystore_server -file certificate_name.cer
   ```

   For example:

   ```
   keytool.exe -export -keystore ..\..\etc\vssl.keystore -alias vsskey  -file
   myserver.cer
   ```

2. On the Sentinel server, copy the certificate file to the `tmp` folder.
3. To import the certificate, run the following command:

   ```
   /usr/bin/certutil -A -d /etc/opt/novell/sentinel/3rdparty/nss -t "CT,CT,CT" -n
   "name_of_Secure_Configuration_Manager_server" -i /tmp/certificate_name.cer
   ```

4. When prompted, enter the password for the server.
5. Restart the Sentinel server.

Secure Configuration Manager is in FIPS Mode

Secure Configuration ManagerSecure Configuration ManagerWhen is in FIPS mode, it uses a NSS provider. You need to import the Sentinel certificate to the NSS database.

1 To export the Sentinel web server certificate, enter the following command:

```
/opt/novell/sentinel/jre/bin/keytool -export -keystore .webserverkeystore.jks
-alias webserver -file 200.cer
```

2 Secure Configuration ManagerTo import the certificate to the server, enter the following command:

```
certutil.exe -A -d c:\SCMNSS\etc -i "c:\200.cer" -n webserver  -t "CT,CT,CT"
```

3 Restart **NetIQ Core Services**.

Secure Configuration ManagerBoth and Sentinel are in FIPS Mode

Secure Configuration ManagerIf Sentinel and are both in FIPS mode, each uses a NSS provider. You need to add each application's certificate to the other application's NSS Keystore.

Use keytool to export the certificates. Keytool is located by default in the `C:\Program Files (x86)\NetIQ\Secure Configuration Manager\Core Services\jre\bin` folder.

Add the Certificate to Sentinel

1 Secure Configuration ManagerLog in to the server.

2 To export the certificate from the NSS store, enter the following command:

```
c:\Program Files\NetIQ\Secure Configuration Manager\Core
Services\jre\bin>keytool.exe -export -keystore ..\..\etc\vssl.keystore -alias
vsskey -file alias_of_keystore_server.cer
```

For example:

```
c:\Program Files\NetIQ\Secure Configuration Manager\Core
Services\jre\bin>keytool.exe -export -keystore ..\..\etc\vssl.keystore -alias
vsskey -file myserver.cer
```

3 Enter the password or PIN for the NSS FIPS certificate database.

You can also specify the credentials in the **nss/keystore/password** field in the **Advanced** tab of the **Core Services Configuration Utility**.

4 On the Sentinel server, copy the certificate file to the `tmp` folder.

5 To import the certificate, run the following command:

```
/usr/bin/certutil -A -d /etc/opt/novell/sentinel/3rdparty/nss -t "CT,CT,CT" -n
"alias_of_Secure_Configuration_Manager_server" -i /tmp/certificate_name.cer
```

For example:

```
/usr/bin/certutil -A -d /etc/opt/novell/sentinel/3rdparty/nss -t "CT,CT,CT" -n
"vsskey" -i /tmp/SCMserver.cer
```

6 To set the trust flags on Sentinel, enter the following command:

```
certutil -M -n server_name -t "CT,C,C" -d /etc/opt/novell/sentinel/3rdparty/
nss/
```

7 Restart the Sentinel server.

Secure Configuration ManagerAdd the Certificate to

1 Log in to the Sentinel server.

2 To export the certificate from the NSS store, enter the following command:

```
./keytool -export -keystore .webserverkeystore.jks -alias webserver -file
webserver.cer
```

3 Secure Configuration ManagerOn the , import the certificate with the following command:

```
c:\Program Files\NetIQ\Secure Configuration Manager\Core
Services\bin>certutil.exe -A -d c:\SCMNSS\etc -i "webserver.cer" -n webserver -
t "CT,CT,CT"
```

4 To set the certificate flag, enter the following command:

```
certutil -M -n webserver -t "CT,CT,CT" -d c:\SCMNSS\etc
```

5 Restart **NetIQ Core Services**.

Viewing Assessment Events in Sentinel

Secure Configuration ManagerFor information about settings required to enable Sentinel to receive assessment events from , see “Receiving Compliance Details from Secure Configuration Manager” in the *Sentinel Administration Guide*.

1 Open a browser to the Sentinel URL.

The URL must be in the format `https://<Sentinel IP Address>:<Port>`. For example, `162.99.123.245:1234`.

NOTE: This is the destination server specified in the **Destination Server** field for the integration configuration. For more information, see “Configuring the Basic Settings for SIEM Integration” on page 169.

---

2 Log in to Sentinel using valid Sentinel user credentials.

You can also use the credentials that you specified for **Destination Server Credentials**Secure Configuration Manager in the Core Services Configuration Utility. However, these credentials have administration privileges to enable configuration, and you do not need such privileges to view assessment events in Sentinel. Instead, you should create separate user accounts for users who only need to view events.

Secure Configuration ManagerFor more information about viewing events in Sentinel, see “Viewing Secure Configuration Manager Events and Compliance Details” in the *Sentinel User Guide*.

18 Integrating Secure Configuration Manager with Splunk

Secure Configuration Manager can send information to Splunk Enterprise Server (Splunk) as events, communicating whether the endpoint is in compliance, out of compliance, or of unknown compliance.

- "Configuring Splunk for Integration" on page 179
- "Secure Configuration ManagerViewing Raw Events in Splunk" on page 179
- "Viewing the Splunk Dashboard" on page 179
- "Secure Configuration ManagerGenerating Alerts on Events" on page 180

Configuring Splunk for Integration

Secure Configuration ManagerSplunk must be able to receive the data coming from .

1. Log in to Splunk.
2. For **TCP/UDP**, create an instance for a TCP or UDP listener with syslog source type.
3. Specify the **Port**Secure Configuration Manager you want to use to receive data from .
4. Specify values for **Source name override** and **Only accept connection from**, as needed.
5. To verify the data is correct, check whether the **TCP Data inputs** table lists your new syslog source.

Secure Configuration ManagerViewing Raw Events in Splunk

To view the raw syslog events, select **Search & Reporting**Secure Configuration Manager then look for .

Viewing the Splunk Dashboard

Secure Configuration ManagerYou can generate reports in Splunk Dashboard based on the event data. For example, you can use the following search string to create a report of top assets by **Risk**:

```
<searchString>source="104.23.456.189"  | top 5
cs3,cs1,cs2,dst,dhost,sourceServiceName,suser showcount=false showperc=false |
table dhost,dst,sourceServiceName,suser,cs1,cs2,cs3| sort -cs3 | rename cs3 as
"Managed Risk" | rename cs2 as "Excepted Risk" | rename suser as "User" | rename
dhost as "Asset Name" | rename dst as "Asset IP" | rename sourceServiceName as
"Platform" | rename cs1 as "Total Risk"</searchString>
```

Secure Configuration ManagerSimilarly, you can create a number of reports in various panels of the Splunk Dashboard, using the attributes of the events that sends.

Secure Configuration ManagerGenerating Alerts on Events

Secure Configuration ManagerYou can generate alerts for events on Splunk Server. Splunk Server has a provision to trigger alerts on a specific saved search condition. There are options for performing actions such as sending emails and running scripts. To configure saved searches, alert action, and other configurations, see the Splunk Server documentation.

VI Maintaining Secure Configuration Manager

This section helps you ensure that Secure Configuration Manager runs smoothly. You should check for and update the content in policy templates and security checks. You should also regularly groom the Secure Configuration Manager database. This section also provides guidance for disaster preparation and recovery.

- Chapter 19, “Maintaining Your Security Knowledge,” on page 183
- Chapter 20, “Maintaining the Secure Configuration Manager Database,” on page 191
- Chapter 21, “Disaster Preparation and Recovery,” on page 197

19 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.

- “Understanding the AutoSync Components” on page 184
- “Configuring a Standalone AutoSync Client” on page 184
- “Connecting to the AutoSync Server through Proxy” on page 185
- “Manually Checking for New Security Knowledge” on page 186
- “Scheduling Checks for New Security Knowledge” on page 186
- “Applying AutoSync Updates” on page 187
- “Updating Agent Content” on page 187
- “Understanding AutoSync Archive” on page 189

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.

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.

NOTE: While using the standalone AutoSync client, if the Secure Configuration Manager Core Services and the standalone AutoSync client are in two different computers, you must manually copy the patch database to the `\Program Files (x86)\NetIQ\Secure Configuration Manager\Core Services\SyncStore` folder in the Secure Configuration Manager Core Services computer.

- "Connecting the AutoSync Client to Core Services" on page 184
- "Connecting the AutoSync Client to Core Services in a FIPS-Enabled Environment" on page 185

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 "Connecting to the AutoSync Server through Proxy" on page 185.

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 *Secure Configuration Manager Installation Guide*.
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 "Connecting the AutoSync Client to Core Services in a FIPS-Enabled Environment" on page 185 and "Enabling FIPS Communication" on page 143.

---

8 Click **OK**.

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 "Enabling FIPS Communication" on page 143.

To configure the client for FIPS-enabled communication:

1 Complete the steps in "Connecting the AutoSync Client to Core Services" on page 184. 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.

Connecting to the AutoSync Server through Proxy

Available only in the Windows console.

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 "Configuring a Standalone AutoSync Client" on page 184.

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**.

Manually Checking for New Security Knowledge

Available only in the Windows console.

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 "Scheduling Checks for New Security Knowledge" on page 186.

After you check for updates, you can review the updates and choose the ones to apply. For more information, see "Applying AutoSync Updates" on page 187.

To manually check for AutoSync updates:

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

2 Click **Check for Updates**.

Scheduling Checks for New Security Knowledge

Available only in the Windows console.

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 "Manually Checking for New Security Knowledge" on page 186.

After a scheduled check completes, review the list of available updates and choose the updates to apply. For more information, see "Applying AutoSync Updates" on page 187.

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**.

Applying AutoSync Updates

Available only in the Windows console.

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.

Updating Agent Content

Available only in the Windows console.

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 "Viewing the History of an Archived Update" on page 190. To identify which of the patch databases have been applied to which agents, run the Applied Patch Databases administrative report. For more information, see "Listing Reports, Actions, and Security Checks" on page 21.

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.

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 "Applying AutoSync Updates" on page 187.
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**.

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 "Applying AutoSync Updates" on page 187.

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**.

Understanding AutoSync Archive

Available only in the Windows console.

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.

- "Archiving Unapplied Updates" on page 189
- "Restoring Archived Updates" on page 189
- "Viewing the History of an Archived Update" on page 190

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**.

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 "Viewing the History of an Archived Update" on page 190.

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 "Applying AutoSync Updates" on page 187.

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.

20 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.

- "Database Maintenance Checklist" on page 191
- "Required Database Permissions and Settings" on page 192
- "How the Secure Configuration Manager Database Works" on page 193
- "Developing a Database Maintenance Strategy" on page 194

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 "Required Database Permissions and Settings" on page 192.
❑	2. Understand how the Secure Configuration Manager database stores and manages data. See "How the Secure Configuration Manager Database Works" on page 193.
❑	3. Identify and implement the appropriate database maintenance strategy for your organization. See "Developing a Database Maintenance Strategy" on page 194.
❑	4. Ensure data preservation and history by scheduling routine backups.See "Backing Up the Secure Configuration Manager Database" on page 194.
❑	5. Ensure optimal database performance through routine grooming. See "Grooming the Secure Configuration Manager Database" on page 195.

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 *Secure Configuration Manager Installation Guide*.

For more information about Secure Configuration Manager requirements, see the *Secure Configuration Manager Installation Guide*.

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.

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.

- "Identifying a Backup and Archive Plan" on page 194
- "Backing Up the Secure Configuration Manager Database" on page 194
- "Grooming the Secure Configuration Manager Database" on page 195
- "Identifying the Appropriate Recovery Model" on page 196

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 "Identifying the Appropriate Recovery Model" on page 196.

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	"How the Secure Configuration Manager Database Works" on page 193
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

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 "Setting the Retention Period" on page 140.

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 "How the Secure Configuration Manager Database Works" on page 193.

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 "Identifying a Backup and Archive Plan" on page 194. For more information about recovery models, contact your database administrator or see SQL Server Books Online.

21 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.

- “Disaster Preparation” on page 197
- “Disaster Recovery” on page 201

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.

- “Disaster Preparation Checklist” on page 198
- “Backing Up the Secure Configuration Manager Database” on page 198
- “Storing Product Configuration Information” on page 199
- “Saving Asset Map Data” on page 200

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 "Backing Up the Secure Configuration Manager Database" on page 198 and Chapter 20, "Maintaining the Secure Configuration Manager Database," on page 191.
❑	2. Maintain a copy of the service pack and hotfix levels for Secure Configuration Manager components. See "Storing Version Level Information" on page 199.
❑	3. Maintain a copy of the Core Services folder. See "Storing Core Services Configuration Settings" on page 199.
❑	4. Maintain a copy of the domain keys. See "Storing a Copy of the Domain Keys" on page 199.
❑	5. Maintain a copy of the Secure Configuration Manager license keys. See "Storing a Copy of the Product License Keys" on page 200.
❑	6. Maintain a snapshot of your asset map. See "Exporting the Asset Map" on page 200.
❑	7. Maintain a snapshot of your managed groups. See "Exporting Managed Groups Data" on page 201.

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 20, "Maintaining the Secure Configuration Manager Database," on page 191.

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.

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" on page 199
- "Storing Core Services Configuration Settings" on page 199
- "Storing a Copy of the Domain Keys" on page 199
- "Storing a Copy of the Product License Keys" on page 200

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 and UNIX 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**.

Saving Asset Map Data

Available only in the Windows console.

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" on page 200
- "Exporting Managed Groups Data" on page 201

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**.

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.

- "Disaster Recovery Checklist" on page 201
- "Reinstalling Secure Configuration Manager" on page 202
- "Applying Service Packs and Hotfixes" on page 202
- "Restoring the Secure Configuration Manager Database" on page 202
- "Restoring Your Core Services Settings" on page 203
- "Linking Users to the Secure Configuration Manager Database" on page 203
- "Restoring Domain keys" on page 204
- "Restoring License Keys" on page 204
- "Re-Registering Agents and Endpoints" on page 204

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 "Reinstalling Secure Configuration Manager" on page 202.
❑	2. If you reinstalled a Secure Configuration Manager component, reapply service packs and hotfixes. See "Applying Service Packs and Hotfixes" on page 202.
❑	3. If you reinstalled the database, restore the backup Secure Configuration Manager database. See "Restoring the Secure Configuration Manager Database" on page 202.

	Checklist Items
❑	4. If you reinstalled Core Services, restore the backup Core Services folder. See "Restoring Your Core Services Settings" on page 203.
❑	5. If you reinstalled Core Services or the database, enable the database and Core Services to communicate with users.See "Linking Users to the Secure Configuration Manager Database" on page 203.
❑	6. If you reinstalled Core Services, restore the domain keys. See "Restoring Domain keys" on page 204.
❑	7. If you reinstalled Core Services, add additional license keys. See "Restoring License Keys" on page 204.
❑	8. If you reinstalled Core Services, re-register your agents and endpoints. For more information, see "Re-Registering Agents and Endpoints" on page 204.

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 *Secure Configuration Manager Installation Guide*.

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 199.

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.

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 20, "Maintaining the Secure Configuration Manager Database," on page 191. 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.

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.

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.

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.

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.

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 “Understanding Managed and Unmanaged Assets” on page 26.

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 “Saving Asset Map Data” on page 200.

VII Appendices

These Appendices provide additional information that might be useful in working with Secure Configuration Manager.

- Appendix A, “Using the Lightweight UNIX Solution,” on page 207
- Appendix B, “Working with Baselines,” on page 211
- Appendix C, “Evaluating the Product in a Trial Environment,” on page 221
- Appendix D, “Checklists,” on page 255

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 "Understanding Security Checks" on page 47. For more information about custom checks, see "Creating Custom Security Checks" on page 61.

- "Lightweight UNIX Solution Checklist" on page 207
- "Running the Data Collection Script" on page 208
- "Transferring the Data Files" on page 209
- "Installing the Data Files" on page 209
- "Running Security Checks for Lightweight UNIX" on page 209

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 "Running the Data Collection Script" on page 208.
❑	2. Transfer the Lightweight UNIX data files to a UNIX agent computer.See "Transferring the Data Files" on page 209.
❑	3. Install the Lightweight UNIX data files on the UNIX agent computer. See "Installing the Data Files" on page 209.
❑	4. Create a Lightweight UNIX endpoint on the UNIX agent computer in Secure Configuration Manager. See "Managing Your Endpoints" on page 39.
❑	5. Run a security check on the Lightweight UNIX endpoint. See "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 "Managing Your Endpoints" on page 39.

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.

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
```

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.

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 "Managing Your Endpoints" on page 39.

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 "Running Security Checks" on page 69. You can also create custom checks for Lightweight UNIX computers. For more information about custom checks, see "Creating Custom Security Checks" on page 61.

B Working with Baselines

Available only in the Windows console.

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.

- "Understanding Baselines" on page 211
- "Understanding Baseline Permissions" on page 211
- "Creating and Managing Baselines" on page 212

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.

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 "Managing Permissions" on page 160.

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 213 or "Creating Baseline Criteria Sets from Security Checks" on page 214.
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 216.
3. Establish baselines for your target endpoints using the baseline criteria sets and baseline collections. For more information, see "Establishing a Baseline" on page 217.
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 "Running a Baseline Comparison Check" on page 218.
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 "Updating a Baseline" on page 220.

   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 "Creating a List of Baselines for a Target Endpoint" on page 220.

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 "Understanding How Agents Identify Data to Collect" on page 49.

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 213 through Step 4 on page 214 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 216 and "Establishing a Baseline" on page 217.

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 "Updating a Baseline" on page 220.

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 216.

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**.

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**.

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.

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 “Scheduling a Baseline Comparison Check” on page 219.

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 "Understanding Policy Templates" on page 71.

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.

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.

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 215.

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 "Establishing a Baseline" on page 217.

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.

C Evaluating the Product in a Trial Environment

Secure Configuration ManagerThis section guides you through an evaluation of so you can explore the features and benefits of using the product. The product trial requires minimal configuration and focuses on the Windows console. To best experience the product's scalability, you can add up to 999 endpoints to manage during the 30-day evaluation period.

Secure Configuration ManagerSecure Configuration ManagerYou can install the components on the same computer for evaluation use, or perform a production-style installation where you place the database and Core Services components on separate computers. Use the evaluation checklist as a guide to installing, configuring, and exploring . For more information about installing the components, see the *Secure Configuration Manager Installation Guide*.

This chapter references the following documentation:

- *Secure Configuration Manager Installation Guide*
- *Secure Configuration Manager Windows Agent Installation and Configuration Guide*

- "Evaluation Checklist" on page 221
- "Getting Started" on page 222
- "Adding Assets to the Asset Map" on page 225
- "Auditing IT Assets" on page 233
- "Evaluating IT Assets" on page 245
- "Maintaining Environment Configuration Standards" on page 253
- "Applying Product Licenses" on page 254

Evaluation Checklist

The following checklist helps you track completed tasks in this product trial and provides a reference to detailed steps in the evaluation process.

	Checklist Items
❑	1. Review the terminology and components in Secure Configuration Manager. See "Getting Started" on page 222.
❑	2. Verify that your computer meets the requirements for the evaluation and plan how you want to set up the components. See "Installing Secure Configuration Manager" on page 222 and the *Secure Configuration Manager Installation Guide*.
❑	3. Secure Configuration ManagerInstall prerequisite software and on the evaluation computer or computers. See the *Secure Configuration Manager Installation Guide* and the *Secure Configuration Manager Windows Agent Installation and Configuration Guide*.
❑	4. Start the console and begin the guided tour. See "Adding Assets to the Asset Map" on page 225.

	Checklist Items
❑	5. Run policy templates and security checks to begin auditing the systems in your environment. See "Auditing IT Assets" on page 233.
❑	6. Review report results and create exceptions for some endpoints or data. See "Evaluating IT Assets" on page 245.
❑	7. Configure compliance alerts and schedule regular policy template and delta report runs. See "Maintaining Environment Configuration Standards" on page 253.
❑	8. Upgrade your trial installation to a production environment. See "Applying Product Licenses" on page 254.

Getting Started

Before delving into an evaluation, you should review information about the primary components and terminology in Secure Configuration Manager.

For more information about the...	See...
Purpose of and interaction among the database, console, Core Services, and agent	"Understanding Secure Configuration Manager Components" on page 13
Application of systems, agents, endpoints, and groups	"Understanding Asset Categories" on page 15
Tools that enable you to audit your IT assets	"Understanding the Tools for Auditing Assets" on page 18
Tools that enable you to evaluate your IT assets	"Understanding Compliance Evaluation Tools" on page 19

Installing Secure Configuration Manager

The *Secure Configuration Manager Installation Guide* provides detailed requirements and steps for installing Secure Configuration Manager. When determining the setup for your evaluation environment, consider how that setup might affect a smooth upgrade to a production environment:

- ***If your production environment contains fewer than 50 computers***, you can install the database, console, and Core Services on one server.
- ***If your production environment contains fewer than 50 computers and you want to audit resource-heavy data***, such as entitlements for files and shares for all users, install the database and Core Services on separate computers. In a data-rich environment, the database requires more disk space.
- ***If your production environment contains more than 50 computers***, install the database and Core Services on separate computers. In an environment supporting a large number of endpoints and agents, the database requires more disk space and server resources.

NOTE

- For optimal Core Services performance, you must install a console on the Core Services computer. You do not need to use that console for any operational work.

- You can install a console on more than one computer so multiple console users can audit and evaluate separate groups of managed systems.
- You do not need to install a Windows agent at this time. The setup program always installs a Windows agent on the Core Services computer. This tour walks you through deploying the agent to other computers.
- Use the NetIQ UNIX Agent Manager to deploy additional UNIX agents in your trial environment. You can add the UNIX systems manually or enable Secure Configuration Manager to discover them. For more information, see "Managing (Discovered) UNIX and Linux Systems" on page 231.

Introducing the Console

Secure Configuration ManagerWhen you complete the installation process, you can begin exploring the console. To start the console, you must know the administrator user name and password you provided during installation.

When you start the Secure Configuration Manager console, you can select from a list of common tasks, as well as click one of the navigation buttons. The following definitions describe the window items and their associated content in the console:

IT Assets

Allows you to view and manage security agents, endpoints, and systems. Displays the built-in managed groups of endpoints as well as My Groups, a container where you can group endpoints to match your organizational needs. For more information, see Chapter 2, "Building Your Asset Map," on page 25.

Security Knowledge

Displays containers that enable you to view, define, and run policy templates, security checks, and tasks. For ease of use, policy templates are organized in logical groups, such as Best Practices, Bulletins, and Regulations. Security checks are organized according to agent and endpoint types, such as UNIX, Windows, and SQL Server. The Task Suites and Custom Tasks containers enable you to create and run sets of reports and actions. For more information, see Chapter 6, "Configuring Assessment Options," on page 77 and "Creating Custom Tasks" on page 138.

Discovered Systems

Lists the systems discovered on your network as well as the unmanaged endpoints on your currently managed systems, depending on the settings for discovery. For ease of use, systems and endpoints are organized by the type of asset, such as SQL Server or UNIX computers. For more information, see "Discovering Unmanaged Assets in Your Environment" on page 27 and "Discovering Endpoints on Managed Assets" on page 33.

Job Queues

Displays report status and lets you view reports. Select a report in the Completed folder to display details or the current status of the report. You can organize completed reports into custom containers under My Reports. For more information, see "Viewing Assessment Results" on page 86 and "Customizing the Job Queues" on page 139.

Alerts

Allows you to view and manage alerts that are generated when a Secure Configuration Manager or an agent detects certain events or conditions on a managed endpoint. For example, upon installation, an alert announces that Secure Configuration Manager has discovered a new Windows domain. For more information, see the Help.

Audit History

Allows you to view and export a log of the tasks performed by console users and administrators in Secure Configuration Manager, such as logging on and off, adding exceptions, and modifying checks and policy templates. For more information, see Chapter 14, “Setting Security on the Secure Configuration Manager Console,” on page 153.

Baselines

Displays the containers for computer baseline management. Baselines allow you to identify and track changes to your computers. The Criteria and Collection containers are a list of defined baseline sets and a list of defined baseline collections. The Management container is a list of the pre-defined checks for managing baselines. For more information, see Chapter B, “Working with Baselines,” on page 211.

Exception Management

Displays the containers for exception management. Exceptions are temporary waivers you can create to prevent unnecessary security check report violations. The Exceptions container is a list of exceptions. The Saved Lists container is the list of values that can be used as a filter or exclusion list when running a security check or policy template. For more information, see “Excluding Data from Report Results” on page 113.

Console Permissions

Secure Configuration ManagerProvides administrators access to Console Users, Console Roles, and Authentication Sources. Enables you to set the password policy for console accounts. For more information, see Chapter 14, “Setting Security on the Secure Configuration Manager Console,” on page 153.

Understanding Console Permissions

When you install Secure Configuration Manager, the setup program creates an administrator account that can access all product functionality. However, if several individuals in your organization want to participate in this evaluation, you might want to assign an account to each person. In this way, you control who can access Secure Configuration Manager and which activities each user can perform. For example, you can specify whether a console role can deploy agents or run a delta report. You can use the built-in roles or create new ones, and then assign console users to the appropriate roles. Once you create console accounts, you can configure a password policy to protect the accounts against security attacks. You can also instruct Secure Configuration Manager to check user credentials against an external authentication source.

For more information about...	See...
Creating console user accounts	“Managing Console Users” on page 162
Creating or assigning console roles	“Managing Roles” on page 158
Using external authentication to validate console users	“Managing User Authentication” on page 155
Configuring the password policy settings	“Managing Password Policy” on page 157

Adding Assets to the Asset Map

Secure Configuration ManagerSecure Configuration Manager offers several methods for deploying, grouping, and viewing IT assets. In the following tours, you can explore the asset map and deploy agents to additional Windows computers in your evaluation environment. The asset map is a record of the endpoints you want to manage.

NOTE: The setup program automatically installs a Windows agent on your Core Services computer, registers the agent, and adds an endpoint to represent the computer in the asset map.

After installing Secure Configuration Manager, use this checklist to build your asset map.

	Checklist Items
❑	1. Review the Checklist for Building Your Asset Map to understand the steps involved in building your asset map.
❑	2. Check **IT Assets > Agents > Windows** for a Windows agent, which should be installed on the Core Services computer. You can use this agent as a Deployment Agent. For more information about Deployment Agents, see "Deploying Windows Agents to the Managed Assets" on page 30.
❑	3. Update the settings for system discovery so Secure Configuration Manager can find Windows and UNIX systems in your environment. For more information, see "Overview of System Discovery and Management" on page 227 and "Discovering Unmanaged Assets in Your Environment" on page 27.
❑	4. Add discovered systems to **IT Assets** by deploying Windows agents or managing discovered systems. For more information, see the following sections: ◆ "Deploying Windows Agents to Discovered Systems" on page 229 ◆ "Managing (Discovered) Windows Systems by Proxy" on page 230 ◆ "Managing (Discovered) UNIX and Linux Systems" on page 231
❑	5. Discover and add endpoints to your managed Windows systems. See "Adding (Discovered) Endpoints to Managed Systems" on page 232 and "Discovering Endpoints on Managed Assets" on page 33.
❑	6. Run policy templates to determine whether your assets pose a risk to enterprise security. For more information, see "Auditing IT Assets" on page 233 and "Evaluating IT Assets" on page 245.
❑	7. Create exceptions to temporarily waive the results for specific managed groups, endpoints, or data points. For more information, see "Excluding Data from Report Results" on page 245.
❑	8. Compare policy template results to ensure that risks have been mitigated. For more information, see "Comparing an Endpoint's Results Over Time" on page 250 and "Exploring the Asset Compliance View" on page 252.
❑	9. Schedule policy templates and delta reports to run at regular intervals to comply with auditing requirements. For more information, see "Maintaining Environment Configuration Standards" on page 253.
❑	10. Upgrade your trial installation to a production environment. See "Applying Product Licenses" on page 254.

Exploring the IT Assets Content Pane

The **IT Assets** content pane in the console lists all the managed systems, with agents and endpoints, that you have added to the asset map. You already have one system in IT Assets: When you installed Secure Configuration Manager, the setup program automatically installed and registered a Windows agent on the Core Services computer. You can manually add systems to the asset map without registering them with Core Services. However, this guide assumes that all managed systems, agents, and endpoints are registered.

To explore IT Assets:

1. Log on to the console using the credentials you created during installation.
2. In the console, click **IT Assets**, and then explore the **Agents** and **Managed Systems** content.
3. Expand **Agents > OS > Windows** to observe the Windows agent and its operating system endpoint.

   When you select an agent in the content pane, the lower pane lists the endpoints that the agent manages. An agent can manage multiple endpoints by proxy. For more information about management by proxy, see "Managing Your Agents" on page 37.
4. Individually right-click the agent and endpoint, and then click **Properties** to see the information automatically assigned to the assets. You can add information to the empty properties, such as a Contact Name and Email for the endpoint.
5. In the **Managed Systems** content pane, you right-click the system to view the same properties information.
6. In any of the panes, right-click a system, agent, or endpoint, and then click **Effective Permissions** to view the effective permissions automatically assigned to the assets.

   Effective permissions represent the permissions in effect for a console role, such as an Administrator. You can modify permissions for users and roles in the Console Permissions panel. For more information about permissions, see Chapter 14, "Setting Security on the Secure Configuration Manager Console," on page 153.
7. Expand **Managed Groups**. Secure Configuration Manager automatically creates folders, such as the Windows folder, to organize your endpoints.
8. To add a custom group to **Managed Groups**, complete the following steps:
   a. Right-click **My Groups**, and then click **Add Group**.
   b. For **New Group Name**, type `Test Group` and then click **Create New Group**.
   c. Continue adding custom groups to learn how Secure Configuration Manager allows you to create child groups under Test Group and My Groups.
   d. Click **Close** when you have finished exploring the Add Group option.
9. To add an endpoint to Test Group, complete the following steps:
   a. Expand **Managed Groups > My Groups > Test Group**.
   b. Expand **Agents > OS > Windows**.
   c. In the Windows content pane, select the Windows agent.
   d. In the lower content pane, drag and drop the endpoint to the **Test Group** folder. Alternatively, right-click the endpoint, click **Add to Group**, select **Test Group**, and then click **OK**.

e. Click **Test Group** to observe that the endpoint now resides in the folder.

   No matter which custom groups contain your endpoints, the endpoints continue to reside in the built-in groups, such as Windows.

10. Continue to explore **IT Assets** on your own. Observe that the right-click menu for some items allows you to perform additional actions, such as running policy templates and security checks.

Overview of System Discovery and Management

Secure Configuration Manager can discover UNIX, Linux, and Windows systems in your network. You can add the discovered systems to your environment by deploying Windows agents from the console, adding the UNIX and Linux systems that already have a UNIX agent, and managing Windows systems without deploying an agent.

The first Windows agent added to Secure Configuration Manager becomes the Deployment Agent for the agent's domain. Core Services uses the Deployment Agent to securely deploy Windows agents to remote computers, particularly to computers in untrusted domains. You can assign a different agent as the Deployment Agent once you have more than one agent registered with Core Services. Before you can deploy a Windows agent to a system, Core Services must know the system's domain. Otherwise, Core Services cannot assign a Deployment Agent for that system. For more information about Deployment Agents, see "Deploying Windows Agents to the Managed Assets" on page 30 and the *Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

Discovering Systems in Your Environment

This section guides you through the process of discovering UNIX, Linux, and Windows systems in your environment. You configure the automatic discovery settings in the Core Services Configuration Utility. You can specify Windows, Active Directory, and DNS domain.

By default, Core Services queries newly registered systems about their domain. Thus, when you install Secure Configuration Manager, Core Services verifies the domain of the agent added to the Core Services computer. The Alerts feature informs you when you register a system from a previously undiscovered domain. You can use the information in an alert to update your system discovery settings. For more information about discovering systems, see "Discovering Unmanaged Assets in Your Environment" on page 27.

Secure Configuration Manager includes two scheduled jobs that help you find systems that have been added to your environment after your initial set up. For more information about the discovery jobs, see "Scheduling the Discovery Process" on page 29.

NOTE: If you installed the Secure Configuration Manager database on the same computer as Core Services, then the Discovered Systems pane already includes a discovered SQL Server asset representing the database instance. For more information about adding the endpoint to your asset map, see "Adding (Discovered) Endpoints to Managed Systems" on page 232.

To discover systems in your environment:

1. In the console, click **Alerts**.
2. Right-click the **Discovered a new Windows domain** alert, and then click **View**.
3. Note the name of the discovered domain in the **Description** field.

   The listed domain represents the fully qualified name for the discovered Active Directory network.
4. Open the Core Services Configuration Utility.

By default, you can find this program under **Start > All Programs > NetIQ Secure Configuration Manager**.

5. On the **Discovery** tab, add the name of the discovered domain to the **Active Directory** field. To add multiple directories, separate the names with commas.
6. Change **Active Directory Discovery** to **enabled**.
7. (Optional) Enable DNS domain discovery, and then add domain names to the **DNS Domains** field. To add multiple domains, separate the names with commas.

   By default, the Windows discovery automatically discovers systems in the same domain as the Core Services computer. You must enable DNS domain discovery.
8. Click **OK** to close the utility.
9. In the console, click **Discovered Systems**.
10. In the navigation pane, right-click **Discovered Systems**, and then click **Discover Systems**.
11. Click **Yes**.

    The discovery process might take a while. You can skip to the next section, and then return here after Secure Configuration Manager adds discovered systems to the content pane. You might need to refresh the view to see the discovered systems.
12. Expand the **Asset Type** categories to observe the list of discovered systems.
13. (Optional) To add discovered assets to your asset map, continue to the following tours:
    - "Deploying Windows Agents to Discovered Systems" on page 229
    - "Managing (Discovered) Windows Systems by Proxy" on page 230
    - "Managing (Discovered) UNIX and Linux Systems" on page 231
    - "Adding (Discovered) Endpoints to Managed Systems" on page 232

Managing Discovered Systems

Managing a system usually means you register the system with Core Services, which then adds the system to **IT Assets**. A registered Windows system might have an agent installed on the computer. UNIX systems host an agent by default. To deploy a UNIX agent to a discovered system, see the *Installation and Configuration Guide for Security Agent for UNIX*.

To check the configuration and vulnerability status of managed systems, those systems must be registered with Core Services. When Core Services successfully registers a managed system, the system's agent and endpoints always appear within the **IT Assets** content pane. You can add systems to the Managed Systems content pane without actually registering those systems with Core Services. However, NetIQ Corporation recommends deploying agents first, and then managing systems. When you select a system in the Discovered Systems content pane, Secure Configuration Manager provides different options for adding the selected system to your asset map. The Deployment wizard enables you to deploy a Windows agent to a discovered system. The Manage System wizard walks you through the process for adding discovered systems to the asset map without deploying an agent. The Manage System wizard provides the following options for specifying the agent that you want to manage a selected system.

Use local agent already installed on this system

Uses the agent already installed on the selected system to manage the discovered system and all endpoints added to the system. Select this option when you have previously installed the agent on the computer and you do not want to manage the system remotely (by proxy).

Use remote agent installed on another system

Allows you to manage the selected system by proxy. Select this option when you want a Windows agent installed on a different computer to monitor the selected system. For more information about management by proxy, see the *Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

I will install agent later and then register

Allows you to add the selected system to your asset map and then deploy an agent to the system at a future time. NetIQ Corporation does not recommend using this option since Core Services does not register the system. You must install an agent, and then manually register the system to add it to **IT Assets**. If you use this option for a large volume of systems, the unregistered systems might get lost within the **Managed Systems** content pane. The **Managed Systems** content includes all systems that host an agent, registered and unregistered.

Deploying Windows Agents to Discovered Systems

Managing a system usually means you register the system with Core Services, which then adds the system to **IT Assets**. A registered Windows system might have an agent installed on the computer. UNIX systems host an agent by default. This section guides you through the process of deploying the Windows agent to discovered systems. To deploy a UNIX agent to a discovered system, see the *Installation and Configuration Guide for Security Agent for UNIX*.

To deploy an agent to discovered Windows systems:

1. In the console, click **Discovered Systems**.
2. Within the **Asset Type: Windows Machine** category, select the database computer and any additional systems that you want to manage.

   You can also select systems within the **Asset Type: Unknown** category. Secure Configuration Manager allows you to assume that an unknown system is a Windows system.
3. Right-click a selected system, and then click **Deploy** to begin the process for installing the Windows agent software on the systems.
4. In the **Computers** window, click **Edit Settings** to view the deployment configuration settings.

   You can select all the computers listed in the window, and then click **Edit Settings**. The values then apply to all the selected computers. Alternatively, you can select computers individually, and then modify the settings.

   The **Deployment Method** specifies whether Secure Configuration Manager communicates with the remote computer through the Deployment Agent or communicates directly with the remote computer.

   The deployment process uses the specified **Agent Deployment Credentials**Secure Configuration Manager to access the selected systems and install the software. If you specify a Deployment Agent for the method, uses, by default, the credentials for the NetIQ Security Agent for Windows service (Windows agent service) account running on the Deployment Agent computer. The Windows agent service account for the Deployment Agent must have rights to deploy to the target computer. For example, the account might be a member of the Domain Administrators group.

   The **Agent Service Credentials** specifies the type of account used to run the agent service on the selected systems.
5. (Optional) If you do not want the Windows agent service on the selected systems to use the LocalSystem account, change **Run Agent Service As** to **Custom**. Then enter an account name and password for the service account.
6. Click **OK**, and then click **Next**.

7 In the Packages window, select the NetIQ Security Agent for Windows package, and then click **Next**.

The setup program automatically added this package to the `SyncStore` folder on the Core Services computer. In future, this window might include packages for hotfixes and services packs that you can deploy to registered Windows agents.

8 (Optional) To deploy the agents at a future time, click **Enable Schedule** in the **Schedule** window, and then specify the date and time.

9 Click **Next**.

10 In the Distribution window, click **Next**.

11 Review the summary information. To deploy the Windows agent to the specified systems, click **Finish**.

12 Expand **Job Queues > Pending** and then click **Install/Update: NetIQ Security Agent for Windows**.

The Install/Update: NetIQ Security Agent for Windows job stays in the Pending jobs queue until all agents have been deployed. Observe that, if you deployed the agent to multiple systems, the status of each system updates dynamically from Pending to Success or Fail as results return to Secure Configuration Manager.

13 When the job finishes, click **Completed** and then open the **Install/Update: NetIQ Security Agent for Windows** job.

14 In the Task Viewer, expand the report result to view detailed information about the deployment for each system.

15 (Optional) To export the deployment results, on the File menu, click **Export** and then specify the file type, name, and path.

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

Observe the new agents added to your asset map. For more information about IT Assets, see "Exploring the IT Assets Content Pane" on page 226.

NOTE: Secure Configuration Manager always adds the targeted systems to IT Assets, even when deployment or registration is unsuccessful. Secure Configuration Manager assumes that you want to manage the selected systems. The icon to the left of the system name provides an indication of the system's status. For example, a red bar through the icon indicates that the system is unregistered. Check the job report to discover problems that might have occurred in the deployment process.

Managing (Discovered) Windows Systems by Proxy

A Windows agent can manage remote computers that do not host an agent. This process is called management by proxy. This tour enables you to add discovered Windows systems to the asset map without deploying agents to the systems. For more information about managing systems by proxy, see the *Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

To manage discovered UNIX and Linux systems:

1 In the console, click **Discovered Systems**.

2 Within the **Asset Type: Windows** category, select the systems that you want to manage by proxy.

3 Right-click a selected system, and then click **Manage**.

4 In the System Definition window, ensure that **Type** specifies **Windows**.

5 (Optional) Add information to the empty property fields.

6 Click **Next**.

7 In the Register Agent window, click **Use remote agent installed on another system**.

8 On the pull-down menu, select the computer for the agent that you want to manage the target systems.

9 (Optional) In the **Add Endpoint to Group** window, specify an existing custom group for the system or create a new group.

10 Click **Finish**.

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

Select the specified agent and then observe the new operating system endpoints added to your asset map. For more information about IT Assets, see "Exploring the IT Assets Content Pane" on page 226.

NOTE: Secure Configuration Manager always adds the target systems to IT Assets, even when deployment or registration is unsuccessful. Secure Configuration Manager assumes that you want to manage the system. The icon to the left of the system name provides an indication of the system's status. For example, a red bar through the icon indicate that the system is unregistered.

---

12 (Optional) Expand **IT Assets > Managed Groups > My Groups**.

Observe the custom groups that you created, and the new endpoints in their assigned custom groups.

Managing (Discovered) UNIX and Linux Systems

This tour walks you through the process for adding discovered UNIX and Linux systems. You must install the UNIX agent on the systems before completing these steps.

To manage discovered UNIX and Linux systems:

1 In the console, click **Discovered Systems**.

2 Within the **Asset Type: UNIX** category, select the systems that you want to manage.

3 Right-click a selected system, and then click **Manage**.

4 In the System Definition window, ensure that **Type** specifies **UNIX**.

5 (Optional) Add information to the empty property fields.

6 Click **Next**.

7 In the Register Agent window, click **Use local agent already installed on this system**, and then click **Next**.

8 (Optional) In the **Add Endpoint to Group** window, specify an existing custom group for the system or create a new group.

9 Click **Finish**.

10 Expand **IT Assets > Agents > OS > UNIX**.

Observe the new agents and operating system endpoints added to your asset map. For more information about IT Assets, see "Exploring the IT Assets Content Pane" on page 226.

NOTE: Secure Configuration Manager always adds the target systems to IT Assets, even when registration is unsuccessful. Secure Configuration Manager assumes that you want to manage the system. The icon to the left of the system name provides an indication of the system's status. For example, a red bar through the icon indicate that the system is unregistered.

---

11 (Optional) Expand **IT Assets > Managed Groups > My Groups**.

Observe the custom groups that you created, and the new endpoints in their assigned custom groups.

Adding (Discovered) Endpoints to Managed Systems

This tour guides you through the process of managing the endpoints that Secure Configuration Manager discovers in your environment. When you register a UNIX or Windows operating system endpoint, Core Services asks the agent managing the system whether the system supports additional endpoints. Secure Configuration Manager lists the discovered endpoints in the Discovered Systems pane and adds an alert for each endpoint.

If you perform an all-in-one installation, the Discovered Systems pane includes a discovered SQL Server asset. This asset represents the SQL Server instance for the Secure Configuration Manager database. Secure Configuration Manager discovered this asset while registering the Windows agent on the computer that hosts Core Services and the database.

To add discovered endpoints to managed systems:

1. In the console, click **Discovered Systems**.
2. Expand the Asset Type categories that represent Windows, UNIX, and Unknown application endpoints. For example, depending on your environment, you might see categories for Oracle, SQL Server, or IIS.

   Each discovered endpoint resides on a system currently managed by Secure Configuration Manager. Thus, when you add the endpoint, the system already has an assigned Windows agent.
3. Within one Asset Type category, right-click the endpoint or endpoints that you want to manage, and then click **Manage System**.

   NOTE: To select multiple endpoints, they must be in the same Asset Type category.
4. In the System Definition window, review the properties for the endpoint.

   Secure Configuration Manager updates the required property fields with information gathered during the discovery process. You can complete the optional fields, such as Contact Name and Contact Email.
5. Click **Next**.
6. In the Register Agent window, verify that **Use existing agent** is selected, and then click **Next**.
7. (Optional) In the **Add Endpoint to Group** window, specify an existing custom group for the system or create a new group.
8. Click **Finish**.
9. Expand **IT Assets > Agents** to review the new endpoints added to existing agents.
10. (Optional) Expand **IT Assets > Managed Groups** to review the additional built-in groups that represent the newly added endpoint types. If you also added the endpoints to custom groups, review the contents of **My Groups** to see the new endpoints.

Creating a Report about Managed Assets

The Admin Reports feature provides a group of reports that describe the Secure Configuration Manager configuration, such as a list of Deployment Agents and their domains, and systems that do not have an agent.

This tour enables you to find endpoints that have not been assigned to a user-defined managed group. NetIQ recommends that you assign all endpoints to one or more user-defined groups. Both the Asset Compliance View and the Security and Compliance Dashboard use your user-defined groups for displaying policy template results. For more information about assigning endpoints to managed groups, see "Organizing Endpoints into Groups" on page 40. For more information about reviewing policy template results for managed groups, see "Using the Asset Compliance View for Evaluation" on page 89 and "Using the Secure Configuration Manager Dashboard for Evaluation" on page 99.

To find endpoints that have not been assigned to a user-defined group:

1. On the Tools menu, click **Admin Reports Wizard**.
2. In the Available Reports window, click **Group Context for Endpoints**.
3. Click Next.

   This report allows you to specify whether to list results for a single endpoint or all endpoints. The default value is ***** for all reports.
4. Click **Run Report**.

   Observe that the results appear in the Admin Reports wizard, rather than in Job Queues. You can search the data to find a specific endpoint.
5. Sort the results by **Server Name**.

   Secure Configuration Manager provides a row of data for each group that applies to an endpoint. Each endpoint should have a row that includes `/IT Asset Map/Managed Groups/My Groups` in the **Group Context** column. The **My Groups** designation indicates that the endpoint resides in a user-defined group.
6. (Optional) Click **Print** or **Export** to save the report results.
7. (Optional) Scroll through the available administrative reports to discover the types of information that this feature provides.
8. Click **Close**.
9. (Optional) To assign an endpoint to a user-defined managed group, complete the steps in "Moving Existing Endpoints into Groups" on page 41.

Auditing IT Assets

To assess the vulnerability and misconfigurations of assets in your enterprise, you run **security checks** and **policy templates**. The resulting report lets you quickly determine how well each IT resource in your environment complies with your company security standards. These reports score each asset based on the threat they identify. Before you start running reports against your assets, you should review information about the asset auditing process.

For more information about...	See...
Ensuring that the database has the latest policy templates and security checks	"Scheduling Checks for New Security Knowledge" on page 186 and "Applying AutoSync Updates" on page 187

For more information about...	See...
Ensuring that your security agents have the latest patch database	"Updating Agent Content" on page 187
Auditing and evaluating assets	"Auditing and Evaluation Process Workflow" on page 17
Security checks that you can use as auditing tools	"Understanding Security Checks" on page 47 and "Modifying or Creating Custom Security Checks" on page 60
Policy templates that you can use as auditing tools	"Understanding Policy Templates" on page 71 and "Modifying or Creating Custom Security Checks" on page 60
Ensuring that a policy template matches your technical standards	"Translating a Technical Standard to a Policy Template" on page 73
Measuring the risk of a vulnerable endpoint	"Understanding Risk Scoring" on page 56

Exploring Security Knowledge Content

The Security Knowledge pane in the console contains hundreds of built-in security checks and policy templates to help you evaluate risks in your enterprise. You can add to the content by creating your own security checks and policy templates, based on your technical standards. However, it is likely that Secure Configuration Manager already contains the security checks that you need. To generate a report, you can run security checks individually against your assets or run a policy template that contains a group of checks. Policy templates let you quickly and easily determine the compliance of your entire enterprise with the security policies of your organization. This tour enables you to explore the Security Knowledge content.

To explore Security Knowledge content:

1. In the console, click **Security Knowledge**.
2. Expand **Security Checks > NetIQ Checks**.

   Observe that Secure Configuration Manager organizes security checks by asset type, such as UNIX and Oracle.
3. Select **Oracle**.

   When you select the Oracle categories, the content pane lists the security checks for that category only. The content pane further organizes the Oracle checks into subcategories for Files/Directories, System, and User/Groups. Other security check categories, such as Windows and UNIX, might have additional subcategories.

   Also, observe that some security checks display **Yes** in the Edit column, which means you can customize the check. If a security check cannot be edited within the console, you can export the check and then apply your changes. You must rename and import the modified check. Modified checks become custom checks and are listed under the **My Checks** category.
4. Click **Windows**.

   You can expand or contract the subcategories for the Windows checks. Observe that the content pane includes a brief description of the security check's purpose.
5. In the content pane, expand **Vendor Updates**.
6. Click **Missing Microsoft updates - security bulletins**.

Observe that the lower pane now displays information about the selected check. The Explanation, Risks, and Remedies data help you determine whether the security check meets your auditing needs. In general, the **Explanation** describes the concept behind the check to help you determine whether you should run the check and how the checked parameter or feature fits into the overall security scheme. The **Risks** section explains why the feature or setting value that the check evaluates can pose a security risk for the computer, network, or enterprise. The **Remedies** section explains how to configure the checked parameter or function to ensure endpoint compliance or to reduce the endpoint's vulnerability to the security risk.

7 Click **NetIQ Checks**.

Observe that the top of the content pane provides a search field.

8 In the search field, type `discovery`.

Observe that the content pane lists security checks for UNIX and Windows that meet the search criteria. NetIQ Corporation created the listed security checks to help you gather information about your registered agents and endpoints. When Secure Configuration Manager runs the Asset Details and Discovery scheduled job, the process actually initiates the NetIQ Endpoint and Agent Configuration policy template, which contains these discovery checks.

9 (Optional) To become more familiar with the type of security checks that Secure Configuration Manager offers, continue to explore the content within **NetIQ Checks**.

10 Expand **Policy Templates**.

Like the Security Checks pane, the Policy Templates content pane automatically lists all available policy templates. You can filter the content by typing a word or phrase in the search field.

Secure Configuration Manager divides the policy templates into four categories in the navigation pane: Regulations, Bulletins, Best Practices, and My Templates. The Help pane on the right provides an explanation for each category.

11 In the search field, type `vulnerabilities`.

Observe that the content pane lists policy templates specifically designed to check for high, medium, and low severity vulnerabilities on UNIX and Windows systems. Secure Configuration Manager regularly updates these policy templates to ensure that you have applied the most recent patches, hotfixes, and service packs to reduce software vulnerabilities. For more information about downloading the latest vulnerability data, see Chapter 19, "Maintaining Your Security Knowledge," on page 183.

12 Click **Best Practices**.

13 In the content pane, click one of the CIS benchmarks for Windows Server 2008.

Observe that the lower pane now lists the security checks included in the policy template. The **Security Check** column provides the actual name of the security check. Some security checks, such as Account Lockout Duration - Windows 2000 or Later, are designed to check one value setting and are listed once in the column. However, this column includes some security checks multiple times. These security checks can be used again and again, simply by changing the parameter and value that the check verifies. For example, the Advanced Audit Policy Setting Status check appears multiple times in the policy template. To help you determine the purpose for each instance of the security check, the **Security Check Alias** column lists the specific security setting that each instance verifies.

14 (Optional) To become more familiar with the type of policy templates that Secure Configuration Manager offers, continue to explore the content within **Policy Templates**.

Updating Security Knowledge Content (AutoSync Service)

NetIQ regularly updates and augments policy templates and security checks in direct response to security bulletins as they are published. To keep your Security Knowledge library current with corrections for the latest known vulnerabilities, NetIQ maintains an AutoSync update service Web site that Secure Configuration Manager can automatically access.

When you schedule Core Services to regularly poll the AutoSync server, the AutoSync Wizard automatically lists the latest content. Otherwise you must manually instruct Core Services to check for updates. For more information about enabling an AutoSync schedule, see "Scheduling Checks for New Security Knowledge" on page 186.

To explore the AutoSync Wizard:

1. In the console, click **AutoSync Wizard** on the **Tools** menu.

   The AutoSync Wizard contains all Security Knowledge content, regardless whether you have applied any updates. The wizard also includes a Notifications category to inform you about hotfixes, service packs, and new releases. Notifications are information-only, so Core Services does not apply these to Security Knowledge.

2. (Conditional) If the content pane is empty, click **Check for Updates**.

3. In the Available Updates tab, drag the **Platform** column heading to the area labeled **Drag a column header here to group by that column**.

   Observe that Secure Configuration Manager now organizes the content by endpoint type, such as MS SQL Server and UNIX. The **Common** category usually applies to Notifications. However, this category also would include policy templates that apply to multiple platforms.

   Browse through the list of available updates. The content that gets updated most often are the monthly vulnerability policy templates, such as NetIQ High Severity UNIX Vulnerabilities for 2012. Observe that the icon for this particular policy template indicates a high priority. NetIQ ranks the severity of the updates so you can quickly identify the content that must be applied to Security Knowledge to reduce security risks. You can sort or filter content by Severity to view the most important updates.

4. Drag the **Type** column heading to the left of **Platform**.

   You can now find the AutoSync content organized by type, such as policy templates and security checks, and then by the endpoint platform. Observe that all content is selected automatically for applying to Security Knowledge. To apply the selected updates, click **Apply Updates**. If you want to apply specific updates, such as those for a single platform, use the check box at the top of table to deselect the entire list and then select the individual updates.

5. (Optional) To view a brief summary of an update, click the **+** icon to the left of the update.

   You can also view this information by selecting the update and then clicking **Show Details**.

6. (Optional) To view detailed information about an update, click the name of the update, such as NetIQ High Severity UNIX Vulnerabilities for 2012.

   Secure Configuration Manager provides browser-based documentation for the updates. For example, when NetIQ releases new or modified security checks, the documentation explains the changes to or purpose of the checks. An IIS security check might be updated to work with a new version of Microsoft Internet Information Services.

7. Click **Archived Updates**, and then scroll through the content.

   You can archive updates without applying them to Security Knowledge. For example, your environment might not have SQL Server endpoints, so you might not want the content for this platform. You can also apply or reapply updates that you have previously archived. For more information about reapplying archived updates or to check the history of an update, see "Understanding AutoSync Archive" on page 189.

Observe that the content includes **Type: Database** for the UNIX and Windows platforms. Core Services automatically archives these updates after pushing the latest patch database to the agents. For more information about pushing the patch database to security agents, see "Updating Agent Content During a Security Check Run" on page 187 or click **AutoSync Settings** and then review the explanation for Push Patch Database to Agents in the Help.

8 (Optional) To view the AutoSync configuration, click **Settings**.

Browse through the settings. You can configure AutoSync to regularly check for updates. You can also specify which client computer contains the content downloaded from the AutoSync service. For more information about modifying the settings, see the Help and Chapter 19, "Maintaining Your Security Knowledge," on page 183.

Running Policy Templates

Secure Configuration Manager includes a number of policy templates that enable you to assess the security risks posed for your IT assets. You can run policy templates from the Security Knowledge navigation pane or from IT Assets. You can also schedule regular runs of your preferred policy template.

Running Policy Templates from Security Knowledge

This tour walks you through the process of running three policy templates so you can understand the variations available in the Secure Configuration Manager content. For example, some policy templates contains security checks for multiple platforms, such as Windows, SQL Server, and Oracle. Other policy templates query specific types of platforms, such as Red Hat Linux.

To explore and run policy templates:

1 In the console, click **Security Knowledge**.

2 Expand **Policy Templates > Best Practices**.

3 (Optional) In the search field, type `CIS`.

4 Right-click **CIS Benchmark for Windows Server 2008 and 2008 R2 Enterprise Security for Domain Member Servers**, and then click **Run Policy Template**.

You can select more than one policy template to run concurrently. However, this tour runs one policy template.

5 In the Targets window, click **Endpoints** and **Test Group** (or the name of your custom group containing the Windows endpoints that you want to check).

The **Groups** option returns results at the group level, while the **Endpoints** option allows you report results for all endpoints in a group or select specific endpoints.

6 Click **Next**.

7 In the Run Options window, click **Next**.

This window allows you to run results from the Secure Configuration Manager database rather than querying the endpoints in real-time. However, since you have not previously run this policy template, the database contains no information and will return a blank report if you enable **Run report from database**. For more information about generating aggregated reports from the database, see "Running Reports from the Database" on page 124.

8 (Optional) In the Report Options window, specify the report settings. For example, you can specify that the report includes violations only.

9 Click **Next**.

10 (Optional) In the Schedule window, click **Enable Schedule** and then specify the time frame for running the report.

11 Click **Next**.

12 In the Delta Report window, click **Next**.

   This window allows you to run an additional report that compares the current results with a previous run of the report. However, since you have not previously run this policy template, Core Services cannot run a delta report.

13 (Optional) In the Distribution window, click **Enable Distribution** and then specify whether you want to save the report to a file or share.

   To email the report, you must configure email settings in the Core Services Configuration Utility. Also, to distribute reports, you must have a console installed on the Core Services computer.

14 Click **Next**.

15 Review the summary information, and then click **Finish**.

   Secure Configuration Manager initiates a job for the policy template. You can track the status of the report in the Job Queues. For more information about evaluating the report results, continue to "Exploring Reports for Policy Template Runs" on page 243.

Running Policy Templates from IT Assets

This tour walks you through the process of running three policy templates so you can understand the variations available in the Secure Configuration Manager content. For example, some policy templates contains security checks for multiple platforms, such as Windows, SQL Server, and Oracle. Other policy templates check specific types of platforms, such as Red Hat Linux.

This process also is useful when you have a managed group that includes systems representing different endpoint types. Instead of individually selecting the endpoints for the policy template runs, you can tell Secure Configuration Manager to run the templates against the entire group. Secure Configuration Manager decides which security checks apply to which endpoint types.

To explore and run policy templates:

1 In the console, expand **IT Assets > Managed Groups > My Groups**.

2 Right-click **Test Group** (or the name of your custom group containing the endpoints that you want to check), then click **Run Policy Template**.

   This window lists all available policy templates. You can select more than one policy template to run concurrently. However, this tour runs one policy template.

3 In the search field, type `CIS`.

4 Click **CIS Benchmark for Windows Server 2008 and 2008 R2 Enterprise Security for Domain Member Servers**, and then click **Next**.

   If your environment does not contain Windows Server 2008 or 2008 R2 systems, select a CIS Benchmark policy template that closely matches your systems.

5 In the Run Options window, click **Next**.

   This window allows you to run results from the Secure Configuration Manager database rather than querying the endpoints in real-time. However, since you have not previously run this policy template, the database contains no information and will return a blank report if you enable **Run report from database**. For more information about generating aggregated reports from the database, see "Running Reports from the Database" on page 124.

6 (Optional) In the Report Options window, specify the report settings. For example, you can specify that the report includes violations only.

7 Click **Next**.

8 (Optional) In the Schedule window, click **Enable Schedule** and then specify the time frame for running the report.

9 Click **Next**.

10 In the Delta Report window, click **Next**.

This window allows you to run an additional report that compares the current results with a previous run of the report. However, since you have not previously run this policy template, Core Services cannot run a delta report.

11 (Optional) In the Distribution window, click **Enable Distribution** and then specify whether you want to save the report to a file or share.

To email the report, you must configure email settings in the Core Services Configuration Utility. Also, to distribute reports, you must have a console installed on the Core Services computer.

12 Click **Next**.

13 Review the summary information, and then click **Finish**.

Secure Configuration Manager initiates a job for the policy template. You can track the status of the report in the Job Queues. For more information about evaluating the report results, continue to "Exploring Reports for Policy Template Runs" on page 243.

Running Security Checks

This tour walks you through the process of running three different types of security checks so you can understand the variations available in the Secure Configuration Manager content. For example, some security checks enable you to gather information about an endpoint or system. Information-only checks do not assess a penalty for the returned data. For more information about creating a custom security check, see "Custom Security Check Examples" on page 64.

Running Security Checks from Security Knowledge

This tour starts from the Security Knowledge pane and walks you through running the Local - Agent Version security check. This check allows you to identify the version of the operating system, providers, and patch-level database on a Windows agent computer.

You can also run security checks from IT Assets. For more information, see "Running Security Checks from IT Assets" on page 240.

To run security checks from Security Knowledge:

1 Expand **Security Knowledge > Security Checks > NetIQ Checks > Windows**.

2 In the content pane, expand **System**.

3 Right-click **Local - Agent version**, and then click **Run Security Checks**.

You can also use the search field to quickly find the security check.

4 In the Parameters window, click **Next**.

5 (Optional) In the Properties window, specify a name for the report that appears in the Completed jobs queue.

6 Click **Next**.

7 In the Targets window, click **Endpoints** and **Test Group** (or the name of your custom group containing the Windows endpoints that you want to check).

   The Groups option returns results at the group level, while the Endpoints option allows you report results for all endpoints in a group or select specific endpoints.

8 In the Run Options window, click **Next**.

   This window allows you to run results from the Secure Configuration Manager database rather than querying the endpoints in real-time. However, since you have not previously run this security check, the database contains no information and will return a blank report if you enable **Run report from database**.

9 (Optional) In the Report Options window, specify the report settings.

10 Click **Next**.

11 (Optional) In the Distribution window, click **Enable Distribution** and then specify whether you want to save the report to a file or share.

   To email the report, you must configure email settings in the Core Services Configuration Utility. Also, to distribute reports, you must have a console installed on the Core Services computer.

12 Click **Next**.

13 Review the summary information, and then click **Finish**.

   Secure Configuration Manager initiates a job for the security check. You can track the status of the report in the Job Queues. For more information about evaluating the report results, continue to "Exploring Reports for Security Check Runs" on page 244.

Running Security Checks from IT Assets

This tour starts from the IT Assets pane and walks you through running two security checks concurrently. The Local - File and Directory Permissions security check allows you to identify the version of the operating system, providers, and patch-level database on a Windows agent computer. The Accounts That Can Shut Down System security check allows you to identify the user accounts that have the right to shut down the computer. This security check assesses a penalty for any account found with this right.

You can also run security checks from Security Knowledge. For more information, see "Running Security Checks from Security Knowledge" on page 239.

To run security checks from IT Assets:

1 Expand **IT Assets > Managed Groups > My Groups**.

2 Right-click **Test Group** (or the name of your custom group containing the Windows endpoints that you want to check), then click **Run Security Checks**.

   This window enables you to specify one or more security checks to run. However, this tour runs one security check.

3 Expand **Windows > Files/Directories**.

4 Select **Local - File and directory permissions**, and then click **>** to move the check to the **Selected Checks** pane.

5 Expand **User/Groups**.

6 Select **Accounts that can shut down system**, and then move the check to the **Selected Checks** pane.

7 Click **Next**.

8. In the Parameters window, observe that the Selected Checks pane lists both security checks. When a security check requires user intervention, Secure Configuration Manager lists the check name in red type. In this case, the Local - File and Directory Permissions check requires you to specify the file or directory that you want to check.

9. To specify settings for the Local - File and Directory Permissions check, complete the following steps:

   9a Click **Local - File and directory permissions**.

   In the Parameters pane, you can change the values for several parameters. Note that the FILDIR parameter requires a value entry. Select each parameter to view an explanation at the bottom of the pane.

   9b For **FILEDIR**, specify `C:\%Program Files%`.

   Observe that you cannot click Next until you press Tab or select another field. Also, observe that Secure Configuration Manager no longer lists the check name in red type.

   9c Specify `TRUE` for **EXISTFILES**.

   When you specify TRUE, the report lists the permissions per trustee for each file or directory in the specified directory.

   9d Specify `TRUE` for **SUBDIRS**.

   When you specify TRUE, the report lists the permissions per trustee for each file or directory within the specified directory.

10. To specify settings for the Accounts That Can Shut Down System check, complete the following steps:

   10a Click **Accounts that can shut down system**.

   10b In the Parameters pane, select each parameter to view an explanation at the bottom of the pane.

   While many security checks include the **Threat Factor** and **Expected Value** fields, the parameter values in the Settings section vary per security check. Also, when you see a **Saved List** or **Exclusion List** parameter, you can usually create a new list or select from a group of built-in lists.

   10c (Optional) To create a saved list, click the browse button beside ***Administrator**.

   You can specify all accounts that you want to exclude from the security check. Browse through the available saved lists to determine whether one contains the accounts that you want to exclude. The **Show Values** option allows you to see the contents of the selected list. Click **New List** to create a customized list of accounts.

11. In the Parameters window, click **Next**.

12. (Optional) In the Properties window, specify a name for the report that appears in the Completed jobs queue.

    When you run a single security check, Secure Configuration Manager names the report according to the check name. When you select multiple checks to run, the report name defaults to a more generic title.

13. Click **Next**.

14. In the Run Options window, click **Next**.

    This window allows you to run results from the Secure Configuration Manager database rather than querying the endpoints in real-time. However, since you have not previously run this security check, the database contains no information and will return a blank report if you enable **Run report from database**.

15. (Optional) In the Report Options window, specify the report settings.

16 Click **Next**.

17 (Optional) In the Distribution window, click **Enable Distribution** and then specify whether you want to save the report to a file or share.

   To email the report, you must configure email settings in the Core Services Configuration Utility. Also, to distribute reports, you must have a console installed on the Core Services computer.

18 Click **Next**.

19 Review the summary information, and then click **Finish**.

   Secure Configuration Manager initiates a job for the security checks. You can track the status of the report in the Job Queues. For more information about evaluating the report results, continue to "Exploring Reports for Security Check Runs" on page 244.

Exploring the Report Viewer

As soon as you install Secure Configuration Manager, a job appears in the Job Queues. This first job represents the discovery job run against the first registered Windows endpoint installed on the Core Services computer. As you follow the tours for deploying agents and enabling Active Directory discovery, Core Services adds jobs to the Completed jobs queue. Similarly, after you run the policy template and security check tours, you can check the status of the reports in Job Queues.

Secure Configuration Manager displays reports in two ways. When you open the Asset Details and Discovery or the Automatic System Discovery jobs, they appear in the task viewer. These reports provide simple amounts of information. However, security check and policy template reports provide considerably more information and require the Report Viewer. This tour walks you through the Report Viewer.

Overview of the Report Viewer

Secure Configuration Manager starts the Report Viewer with the Summary tab selected. This tab displays several top 10 lists and a pie chart that shows the distribution of systems in each risk category. The Report Viewer displays the following tabs in the upper-left portion of the viewer window.

Report Summary

Displays top 10 lists, including Risk Distribution by Platform, Risk Distribution by Group, Highest Scoring Endpoints, and Most Frequently Violated Security Checks. A pie chart in this window displays the distribution of assets in low, medium, and high risk categories.

Data View

Displays a tree view of the security checks included in the security check report, as well as the target endpoints and groups.

Detailed Graphs

Displays pie charts showing the distribution of assets in various risk categories.

Full Report

Displays the security check report using Adobe® Reader® as the Report Viewer. This view includes data from all tabs, including the summary, detailed data, and graphs. It provides all the navigation tools and options inherent with your version of Adobe Reader. You can customize this report by clicking **Tools > Full Report Options**.

You can print or export the displayed information to present compliance status results or to use as a remediation checklist. The Actions menu provides different print and export options, depending on the tab currently displayed.

Exploring Reports for Policy Template Runs

The Running Policy Templates tour walked you through the process for running a policy template. This tour explores the results.

To view a policy template report:

1. Expand **Job Queues > Completed**.

   The upper content pane contains a large amount of information about each job. Scroll to the right to see all the columns of data available for each job. You can rearrange the columns or group the jobs by a column heading. Note that if an endpoint failed a security check in the selected policy template, the Status column states Failed.

   The lower content pane enables you to quickly see the history and status of the completed report. The lower pane lists the endpoints that you specified to check, and indicates whether the agent successfully gathered data for the endpoint. The Status field also indicates whether the security check or policy template applies to the endpoint.

2. In the content pane, right-click **CIS Benchmark for Windows Server 2008 and 2008 R2 Enterprise Security for Domain Member Servers**.

   The shortcut menu provides several options, including the ability to run the report again for failed endpoints. This option allows you to check only those endpoints that had problems, rather than having the agent run the same queries against the entire group of endpoints. Secure Configuration Manager creates a second report for the run against the failed endpoints. You can then create a report that combines both report runs. For more information about creating an aggregated report, see "Running Reports from the Database" on page 124.

3. On the shortcut menu, click **View**.

4. Secure Configuration Manager opens the Report Viewer in a separate window.

   Observe that the default display provides a summary of the job results. You can see, at a glance, the managed risk for the endpoints, the endpoints that have the highest risk for vulnerability, and the security checks that reported the most frequent violations among the endpoints.

5. Click **Data View**.

6. In the left pane, click **Security Checks**.

   This view shows a summary of all the security checks that are included in the policy template, the expected value for each check, the actual value discovered on each checked system, the threat factor assigned to the check, and the resulting penalty for the system.

7. Drag the **Total Risk** column heading to the area labeled **Drag a column header here**.

   The Report Viewer regroups the data based on risk score ranges. Click the triangle in the Total Risk heading to sort the risk scores from highest to lowest. Observe that the Report Viewer groups the security checks by the total risk values. For more information about the way risk scores differ by endpoint, see "Example of Risk Scoring" on page 59.

   Security checks can score results in different ways, which you can observe with the **Scoring Method** column. In this policy template, most of the checks use *Single Value* scoring, which applies a penalty when the **Actual Value** for the setting on the endpoint does not match the **Expected Value** specified in the security check.

   The *Count* scoring method lists a violation for every row of returned data where the expected and actual values do not match. For example, the 1.8.21 Perform Volume Maintenance Tasks security check returns results for all user accounts with the rights to perform volume maintenance tasks. The CIS Benchmark recommends that only accounts in the Administrators group should have this capability. If the query discovers other accounts with these rights, then

each reported group counts as a penalty. Secure Configuration Manager calculates the Total Risk by multiplying the number of returned rows by the Threat Factor. For more information about scoring security check results, see "Understanding Risk Scoring" on page 56.

8 In the content pane, scroll through the list of checks to compare the Actual Value and Expected Value results.

If you see a difference in the expected and actual value columns, then the report adds a Total Risk value to the overall score. A Total Risk score of zero indicates that the endpoint passed the security check.

9 Expand **Security Checks**, and then scroll through the list.

Observe that if the Windows agent failed get a response from the endpoint for a security check, the Report Viewer lists the check name in red type with a large X icon beside the name. For example, the Windows agent service account might not have the right permissions to query the setting.

10 Expand **1.1.12 Maximum lifetime for service ticket**.

This view allows you to see the results of this check instance run against each endpoint. At the bottom of the right pane, you can view detailed descriptions, explanations, risks, and remedies for the selected check. This built-in security knowledge can help you understand the risks and make the changes you need to correct the vulnerability.

Continue to explore the results under **Data View > Security Checks**.

11 Collapse **Security Checks**, and then expand **Target Endpoints**.

12 Select an endpoint.

The content pane lists the results of all security check instances run against this endpoint. The **Expected Value or Count** and **Actual Value or Count** columns help you determine the reason the endpoint passed or failed a check. For example, if the password policy on the endpoint is set to 6 characters, then the endpoint fails the 1.1.4 Minimum Password Length standard because that check instance is looking for a value equal to or greater than 8.

Scroll the content pane to observe the risk scoring for the endpoints. A Managed Risk value of zero means the endpoint poses no risk to your enterprise. The Excepted Risk column indicates whether the security check result has been excluded for the endpoint. For more information about creating exceptions, see "Excluding Data from Report Results" on page 113.

13 When you finish exploring the report, close the Report Viewer window.

Exploring Reports for Security Check Runs

The Running Security Checks tour walked you through the process for running some security checks. This tour explores the results for those security checks.

To view a security check report:

1 Expand **Job Queues > Completed**.

The upper pane with the list of completed jobs contains a large amount of information about each job. Scroll to the right to see all the columns of data available for each job. You can rearrange the columns or group the jobs by a column heading. Note that if an endpoint failed a security check in the selected security check or policy template, the Status column states Failed.

The lower content pane enables you to quickly see the history and status of the completed report. The lower pane lists the endpoints you specified to check, and indicates whether the agent successfully gathered data for the endpoint.

2 In the content pane, right-click **Multiple Checks** or the report name that you specified in the tour for Running Security Checks from IT Assets.

   The shortcut menu provides several options, including the ability to run the report again for failed endpoints. This allows you to check only those endpoints that had problems, rather than having the agent run the same query against the entire group of endpoints. Secure Configuration Manager creates a second report for run against the failed endpoints. You can then create a report that combines both report runs. For more information creating an aggregated report, see "Running Reports from the Database" on page 124.

3 Click **View** to open the report.

   Observe that the reported **Managed Risk** summarizes the results for all endpoints and security checks in the job. If the report lists any endpoints as Unknown, then Secure Configuration Manager could not gather some data about that endpoint.

4 Click **Data View**.

   This view provides a summary of the security checks and endpoints that you specified to check. The summary includes the expected value, the actual value discovered on each checked system, the threat factor assigned to the check, and the resulting penalty for the managed risk of the system. Observe that the **Scoring Method** column for Local - File and Directory Permissions indicates that the security check is for informational purposes only. Secure Configuration Manager does not assess a penalty for returned results on these types of security checks.

5 In the left pane, expand **Accounts that can shut down system**, and then select an endpoint.

   The report lists the specific accounts that can shut down the system, if any exist on the endpoint. Observe that each reported account, if any, increase the Managed Risk by 10 points.

6 In the left pane, expand **File and directory permissions**, and then select an endpoint.

   The report lists useful information about the specified directory name and the trustees that can access the directory. Observe that the Report Viewer does not list information about risk status. This security check scores as information only, and thus Secure Configuration Manager does not apply penalties for returned results.

7 When you finish exploring the report, close the report viewer window.

8 (Optional) Click **Full Report** to create a `.pdf` file of the report.

Evaluating IT Assets

To streamline the audit and compliance process, Secure Configuration Manager provides a set of evaluation tools for you to determine how well IT assets in your environment comply with the policy templates that match your security policy standards. This tour shows you how evaluate your assets using the Exceptions Management, Delta Reports, and Asset Compliance View features.

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 in a policy template. You can apply the following types of exceptions each time you run the policy template:

Exclude a specified endpoint

Instructs Secure Configuration Manager to ignore the results for the specified endpoint. This option enables you to prevent offline or problematic systems from skewing report results.

Exclude a specified group of endpoints

Instructs Secure Configuration Manager to ignore the results for the specified managed group when you run the policy template. For example, the systems in the group might be under maintenance when you run the policy template. Alternatively, you might want to exclude a single check in the policy template that does not apply to the group. The specified group must be a user-defined group within **My Groups**, and you must run the policy template against the group. For an example, see "Excluding a Managed Group from a Security Check" on page 246.

Exclude a specified security check associated with an endpoint

Instructs Secure Configuration Manager to ignore the results of the specified security check for a specified endpoint. This option enables you to exclude failed results for the endpoint when the security check might not apply to the settings for that particular endpoint. For example, the check might look for files and directories that you do not allow on the endpoint. For an example, see "Excluding an Endpoint from a Security Check" on page 247.

Exclude a specified data point for a security check associated with an endpoint

Instructs Secure Configuration Manager to ignore the results for a particular data value for the specified security check run against the specified endpoint. For example, you might want an endpoint to accept inbound private connections, which violates the CIS security setting for the Windows Firewall: Inbound connections (Private) group policy. For an example, see "Excluding a Specific Data Point from a Security Check" on page 248.

For more information about creating these types of exceptions, see "Excluding Data from Report Results" on page 113. You can also configure Secure Configuration Manager to generate an approval process for exception management. This process requires that exceptions receive approval before being applied to report results. For more information, see "Enabling Exception Approvals" on page 119.

Excluding a Managed Group from a Security Check

This tour walks you through excluding the results of a managed group of endpoints for a particular security check.

To exclude results for a group of endpoints:

1. In the navigation pane, expand **Job Queues > Completed**.
2. In the content pane, open the report for the CIS Benchmark for Windows Server 2008 and 2008 R2 policy template that you ran in a previous tour.
3. Click **Data View**.
4. Expand **Target Groups**.
5. Right-click **Test Group** (or the name of your custom group against which you ran the policy template), and then click **Create Exception**.
6. In the Welcome window, click **Next**.

   The Criteria window automatically lists the policy template and selected group of endpoints. You must specify the security check(s) that you want to exclude from the report. Otherwise, Secure Configuration Manager assumes you want to exclude the selected group from policy template itself. For this tour, we will create an exception for specific checks.
7. In the Criteria window, select **generated by the '<checkname>' security check**, and then click **'<check name>)'**.

8 Select the following security checks:
   - 1.5.4 Windows Firewall: Apply Local Connection Security Rules (Private)
   - 1.5.7 Windows Firewall: Apply local firewall rules (Private)
   - 1.5.10 Windows Firewall: Display a notification (Private)
   - 1.5.13 Windows Firewall: Firewall state (Private)
9 Click **OK**, and then click **Next**.

   The Properties window allows you to specify a name and description for the exception. You can also include a reason for the exception and a duration for the exception to be in effect.
10 To create a custom reason, complete the following steps:

   10a Click **Edit**.

   10b In the IQ Exception Reasons window, click **User Defined**.

   10c Click **Add**, and then specify a name and description for your custom reason.

   10d Click **OK** and then **Close**.
11 Click **Next**.

   The Notes window allows you to track the changes to exceptions.
12 In the **Note** field, type `Created on` *[date]* where *[date]* is the current date.
13 Click **Next**.
14 Review the summary of the exception, and then click **Finish**.
15 In the Report Viewer, click **Apply Exceptions**, and then click **Yes**.
16 In **Job Queues > Completed**, open the report again.
17 In the Data View pane, scroll to the Windows Firewall security checks that start with 1.5.

   Observe that the security checks that you specified in the exception have a different icon beside their names to indicate the presence of an exception.
18 Expand **1.5.10 Windows Firewall: Display a notification (Private)**.

   Observe that the endpoints from the managed group for which you created an exception are now grayed out.
19 Select one of the excepted endpoints.
20 In the lower content pane, click **Exceptions** to observe the exception name.
21 (Optional) To review all the exceptions applied to the policy template, scroll to the end of the Data View pane, and then click **Exceptions**.

Excluding an Endpoint from a Security Check

This tour walks you through excluding the results of a single endpoint for a particular security check.

To exclude results for a single endpoint:

1 In the navigation pane, expand **Job Queues > Completed**.
2 In the content pane, open the report for the CIS Benchmark for Windows Server 2008 and 2008 R2 policy template that you ran in a previous tour.
3 Click **Data View**.
4 Expand **Security Checks > 1.5.16 Windows Firewall: Inbound connections (Private)**.
5 Right-click an endpoint listed under the check name, and then click **Create Exception**.

6 In the Welcome window, click **Next**.

The Criteria window shows the exception information. Observe that this exception will be for the security check and the endpoint that you selected.

7 (Optional) In the Criteria window, click **'1.5.16 Windows Firewall: Inbound connections (Private)'**.

Observe that the Select Check window allows you to select other security checks in the policy template that you want to except for this endpoint.

8 (Optional) In the Criteria window, click the endpoint name.

Observe that the Select Endpoint window allows you to select endpoints that you want to include in the exception.

9 Click **Next**.

The Properties window allows you to specify a name and description for the exception. You can also include a reason for the exception and a duration for the exception to be in effect.

10 To create a custom reason, complete the following steps:

10a Click **Edit**.

10b In the IQ Exception Reasons window, click **User Defined**.

10c Click **Add**, and then specify a name and description for your custom reason.

10d Click **OK** and then **Close**.

11 Click **Next**.

The Notes window allows you to track the changes to exceptions.

12 In the **Note** field, type `Created on` *[date]* where *[date]* is the current date.

13 Click **Next**.

14 Review the summary of the exception, and then click **Finish**.

15 In the Report Viewer, click **Apply Exceptions**, and then click **Yes**.

16 In **Job Queues > Completed**, open the report again.

17 In the Data View pane, expand **1.5.16 Windows Firewall: Inbound connections (Private)**.

Observe that the endpoint for which you created an exception is now grayed out. If you click the endpoint, the lower content pane lists the exception name. Click the exception name to observe information about the exception.

18 (Optional) To review all the exceptions applied to the policy template, scroll to the end of the Data View pane, and then click **Exceptions**.

Excluding a Specific Data Point from a Security Check

This tour walks you through excluding a particular data value for a specified security check run against the an endpoint.

To exclude a specific data value for an endpoint:

1 In the navigation pane, expand **Job Queues > Completed**.

2 In the content pane, open the report for the CIS Benchmark for Windows Server 2008 and 2008 R2 policy template that you ran in a previous tour.

3 Click **Data View**.

4 Expand **Security Checks > 1.8.1 Access this computer from the network**.

5. Select an endpoint under the check name.

   For this tour, assume that the endpoint fails the security check because of a returned value in the **Well-known group list** column. You want to create an exception for that set of data.

6. In the content pane, right-click the data cell in the **Well-known group list** column, and then click **Create Exception**.

7. In the Welcome window, click **Next**.

   The Criteria window shows the exception information. Observe that every box is checked. This exception will be for the combination of the endpoint, the security check, and the selected data in the policy template.

8. In the **where returned data matches** row, click the endpoint name.

   In the Select Check Data window, observe that you can change the columns of data that you want to include in the exception. To add or remove a data column, select the column name and then click the add or delete button on the menu.

9. Click **OK**, and then click **Next**.

   The Properties window allows you to specify a name and description for the exception. You can also include a reason for the exception and a duration for the exception to be in effect.

10. To create a custom reason, complete the following steps:

    10a Click **Edit**.

    10b In the IQ Exception Reasons window, click **User Defined**.

    10c Click **Add**, and then specify a name and description for your custom reason.

    10d Click **OK** and then **Close**.

11. Click **Next**.

    The Notes window allows you to track the changes to exceptions.

12. In the **Note** field, type `Created on` *[date]* where *[date]* is the current date.

13. Click **Next**.

14. Review the summary of the exception, and then click **Finish**.

15. In the Report Viewer, click **Apply Exceptions**, and then click **Yes**.

16. In **Job Queues > Completed**, open the report again.

17. In the Data View pane, click **Exceptions**.

    Observe that the report lists all the exceptions applied to the policy template. You can also view the exception by selecting the security check.

Comparing an Endpoint's Results Over Time

The Delta Report function enables you to build a trend of results for an asset over time, based on the results for a policy template. For more information about delta reporting, see Chapter 10, "Comparing Results of Assessments," on page 123.

Creating a Delta Report

Before you can compare endpoint results, you must have at least one completed run of the policy template. You can run a delta report once from the Job Queues or you can configure a delta report to run concurrently with a scheduled policy template run.

To compare an endpoint's results over time:

1. Run the CIS Benchmark for Windows Server 2008 and 2008 R2 Enterprise Security for Domain Member Servers policy template as directed in the tour for Running Policy Templates.

   To have the delta report list changes for an endpoint, you must modify the endpoint's setting in a way that a security check in the policy template would recognize. For this tour, we will change the settings for the Local Policy: Audit process tracking. In the policy template, the 1.2.8 Audit Process Tracking security check verifies whether this local audit policy is set to **Success,Failure**.

2. To change the Local Policy setting for Audit process tracking, complete the following steps:

   2a Open the Local Security Policy.

   2b Expand **Security Settings > Local Policies > Audit Policy**.

   2c Right-click **Audit process tracking**, and then click **Properties**.

   2d Select **Success**, and then click **Close**.

3. In the console, expand **Job Queues > Completed**.

4. Right-click the job for the policy template that you ran in Step 1 on page 250, and then click **Run Again**.

5. When the second policy template run finishes, select the job in the content pane.

6. In the lower content pane, click **All Runs of this report**.

   Observe that Secure Configuration Manager lists a report corresponding to each run of the selected policy template. If any endpoint failed any security check in the template, the **Status** field indicates **Failed**.

7. Select the two runs of the report, right-click one of the runs, and then click **Run Delta Report**.

   In the Comparison window, observe that you can choose which report serves as the basis for comparison. By default, Secure Configuration Manager selects the older report as the base report.

8. Click **Next**.

9. In the Security Checks window, click **Select All**.

   You can choose to include specific security checks in the delta report. For example, you might care about the changes for specific settings rather than every setting that the policy template checks.

   Observe that some security checks might not be selected, even though you clicked Select All. Secure Configuration Manager does not perform a delta comparison for security checks that do not apply to the endpoints. If you review the original policy template report, you can see that the report includes wording such as "No data matched your criteria" for the checks not selected in the Delta Report wizard.

10. Click **Next**.

11 In the Delta Criteria window, you select individual checks to view the method for comparing results. Since each security check returns columns of data, Secure Configuration Manager compares information within those columns.

   By default, Secure Configuration Manager uses the column for the setting name, or the value being checked, as the unique item to find in each report. Then, Secure Configuration Manager compares the Actual Value for that unique setting in the base report to compare with the same value in the second report.

12 Keep the default settings, and click **Next**.

13 In the Report Options window, click **Layout**.

   You can specify whether the delta report includes a combination of added, deleted, modified, and unchanged data. Note that Microsoft Windows might interpret *modified* 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. So, choosing to show only Modified settings might result in an inaccurate delta report.

14 (Optional) To discover changed settings only, click **Added**, **Deleted**, and **Modified**.

15 Click **Next**.

16 Review the summary of the delta report, and then click **Finish**.

17 On the Schedule window, click **Next**.

18 On the Delta Reporting window, click **Enable Delta Reporting**.

19 (Optional) Reinstate the settings for the Local Policy: Audit process tracking.

Reviewing a Delta Report

By default, names for delta reports start with the “Delta-” prefix. For example, the job name might be Delta - CIS Benchmark for Windows Server 2008 and 2008 R2 Enterprise Security for Domain Member Servers.

To review a delta report:

1 In the console, expand **Job Queues > Completed**.

2 Open the job for the delta report that you initiated in the tour for Creating a Delta Report.

3 In the Report Viewer, observe that the content pane lists **Unchanged** in the **Delta** column for all the security checks in the policy template.

   When you select Security Checks at the top level of the Delta Comparison View, a value of “Unchanged” might indicate that 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.

4 In the left pane, click **1.2.8 Audit process tracking** and expand to show the tested endpoints.

   This security check verifies the setting that you changed in the tour for Creating a Delta Report. Observe that both the check name and the endpoint that you changed appear in bold type. The content pane lists the delta results for the endpoints. For the endpoint that you changed, the **Delta** column should list **Modified** or **Added**, depending on the operating system version.

5 To view the actual changes in settings, click the endpoint name in the left pane.

   Observe that the Actual Value column splits into two columns that represent each report. The report uses colored text to indicate values that changed between report runs.

   To share the delta results with system administrators, you can print or export the data at either the security check level or as a full report.

6 (Optional) To export the delta results at the security check level, complete the following steps:

   6a In the Delta Comparison View pane, click the check whose results you want to export.

   6b On the Action menu, click **Export**.

   6c Specify the file type, name, and path, and then click **OK**.

Exploring the Asset Compliance View

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 in the view only after you run policy templates.

These tours assume you have already run the NetIQ CIS Benchmark for Windows Sever 2008 and 2008 R2 Domain Member Servers policy template as described in the Running Policy Templates tour. You might also have created exceptions as described in the for Excluding Data from Report Results tour.

Configuring Asset Compliance View Settings

The information displayed in Asset Compliance View depends on both the Managed Group selected in the IT Assets pane and the policy template that you specify in the Settings window. For more information about the Asset Compliance View settings, see "Changing Asset Compliance View Settings" on page 91.

To configure the Asset Compliance View:

1 Expand **IT Assets > Managed Groups > My Groups**.

2 Click **Test Group** (or the name of your custom group containing the Windows endpoints that you want to evaluate).

3 On the View menu, click **Compliance Overview**.

4 Click **Settings**.

5 To filter the list of policy templates, type `"domain member servers"` in the search pane.

   Alternatively, if you ran a different policy template in the tour for "Running Policy Templates" on page 237, enter search criteria related to that template.

6 Select **CIS Benchmark for Windows Server 2008 and 2008 R2 Enterprise Security for Domain Member Servers** (or the template that you previously ran).

   Observe that you can select more than one policy template. The Asset Compliance View aggregates results for the most recent run of all selected policy templates.

7 For **Time Range** specify the date that you first ran the policy template, and then click **No End Date**.

8 Set **Trend Interval** to **Daily**.

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.

9 Click **OK**.

Viewing Results with the Asset Compliance View

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 configuration of those computers poses a high, medium, or low risk. For more information, see "Using the Asset Compliance View for Evaluation" on page 89.

NOTE: This section does not include a tour of the NetIQ Secure Configuration Manager Dashboard, which provides a Web-based interface for executives and managers to view the overall compliance of IT assets. Like the Asset Compliance View, the Dashboard enables you to perform a granular assessment of specific groups and computers. For more information, see "Using the Secure Configuration Manager Dashboard for Evaluation" on page 99. For a trial version of the Dashboard, contact NetIQ Sales.

Maintaining Environment Configuration Standards

Secure Configuration Manager can notify you or a change management system when an endpoint no longer complies with your technical standards. Automated notifications are useful when the endpoint's system contains sensitive information or must be continuously operational. Core Services generates the alerts based on results from scheduled policy template runs. You can schedule policy templates to run at regular intervals. You can also configure a delta report to run concurrently with the scheduled policy template so you can quickly discover changes in an endpoint's configuration.

As a best practice, your scheduled runs of tasks, policy templates, delta reports, and security checks should occur at different times to reduce the load on the database and Core Services. Secure Configuration Manager runs built-in jobs, such as purging old reports, at specific times of the day. By default, Core Services purges the database at 1 a.m., local time. At 3 a.m., Core Services takes snapshots of policy template results to use in the Asset Compliance View trending reports.

Also, when scheduling jobs, keep in mind that Secure Configuration Manager runs those jobs according to the local time on the Core Services computer. For example, a console user in London schedules a job to run at 4 a.m., with the assumption that the job runs according to Greenwich Mean Time. However, the Core Services computer in New York City runs the job at 4 a.m. Eastern Daylight Time, which is five hours later than the user planned.

For more information about...	See...
Scheduling regular runs of a policy template	"Running Assessments on a Schedule" on page 78
Scheduling a delta report with a policy template run	"Scheduling a Delta Report" on page 127
Creating alerts when endpoints are out of compliance	"Automating Out-of-Compliance Notifications" on page 77

Applying Product Licenses

When you install Secure Configuration Manager, the setup program automatically installs a trial license key unless you specify a production license. You can upgrade your trial installation to a full production installation by changing the license key.

Using a Trial License

The trial license key allows you to monitor the locally installed Windows agent, add more Windows agents, and manage up to 999 endpoints. You can explore all features in Secure Configuration Manager for 30 days.

To determine the time remaining on a trial license, click **License Status** on the **Tools** menu in the Secure Configuration Manager console. The License Status window reports the number of licenses available for each installed product, the number of licenses in use, and the license expiration dates. To add licenses or extend your trial license, contact your NetIQ sales representative.

Changing from Trial to Production License

To upgrade your trial installation to a production environment, you must change the license key listed in the Core Services Configuration Utility > License Key tab. For more information, see "Customizing Core Services" on page 141.

NOTE: Secure Configuration Manager supports multiple license keys.

D 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	Checklist for Building Your Asset Map
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