NetIQ Secure Configuration Manager

Help for the Web Console

January 2018

Legal Notice

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

About This Book

These Help files provide conceptual information and instructions for the Web console of Secure Configuration Manager.

Intended Audience

This book provides information for individuals responsible for running assessment against endpoints in your IT environment, as well as for individuals who review the assessment reports or want to build customizing reports based on policy template runs.

Additional Documentation

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

Contact Information

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

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

Contents

1 Welcome to Secure Configuration Manager

Secure Configuration Manager is a security configuration and compliance monitoring solution that pro actively assesses your server configurations against regulatory requirements, security best practices, and corporate IT policies to demonstrate compliance and manage information security risk.

Secure Configuration Manager deploys **agents** to collect information about your IT assets, 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.

NOTE: Secure Configuration Manager supports two consoles for users to interact with the product: this Web console and the original Windows console. While this Web console helps you use many of the features in Secure Configuration Manager, some functionality currently remains in the Windows console. When necessary, this Help will direct you to actions that must be performed in the Windows console.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Managing Your Assets

Select **Manage > Assets**

Assets are physical computers on a network that run an operating system and host applications or databases. Assets also host agents or endpoints. An **agent** resides on an asset and monitors endpoints such as computers, devices, and applications. An **endpoint** represents an agent-monitored operating system, application, web server, database instance, or network device.

NOTE: To successfully communicate and collect security information from the managed endpoints, you must first register the agents and endpoints with Core Services.

To **manage agents**, use the Windows console.

For more information about tagging, re-registering, or heartbeat, see Chapter 3, “Managing Endpoints,” on page 15. For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

2 Status of Your Assets

Select 

The Endpoint, Asset, and Agent overviews provide a snapshot of the overall health of your endpoints, assets, and agents, respectively. **Health** indicates whether the endpoint, asset, or agent is *online* or *offline*. If Secure Configuration Manager cannot accurately determine their state, the overviews lists them as *unknown*. Secure Configuration Manager also organizes endpoints by operating system and endpoint type, such as database version or application.

To view more specific information about the displayed data, you can select the numeric values that represent the endpoint, agent, or asset state. For example, two endpoints are offline. To identify the endpoints, select **Offline 2** under **Endpoints by Health**. The Web console displays a list of the offline endpoints. You can then select one or more endpoint to check its heartbeat or re-register it.

NOTE: To successfully communicate and collect security information from the managed endpoints, the agents and endpoints must be registered with Core Services.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

3 Managing Endpoints

Select **Manage > Endpoints**

Endpoints are the operating systems, devices, and applications that agents help Secure Configuration Manager to assess for vulnerabilities. You can organize your endpoints into **groups** so that Secure Configuration Manager knows what assets to manage and where to find them.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Assess Endpoints

You can initiate an assessment of one or more endpoints.

1. In the **Endpoints** tab, select the managed group that contains the endpoints that you want to assess.

   To run a policy template or security check against endpoints in more than one group, you must be in the **Groups** tab. For more information, see "Audit Groups of Endpoints" on page 21.
2. Select one or more endpoints in the chosen group.
3. Select **Run Policy Template** or **Run Security Check**, then complete the run process.

   For more information, see Part II, "Assessing Your Managed Assets," on page 23.

NOTE: Secure Configuration Manager cannot communicate with agents that are not registered. If an unregistered agent manages any of the selected endpoints, Secure Configuration Manager will not collect data from those specific endpoints.

Organize Endpoints in Groups

Groups contain collections of endpoints and other groups. By default, Secure Configuration Manager organizes your endpoints by the computer's operating system. However, you can create customized groups. For more information, see "Organize Endpoints in Groups" on page 21.

Tag Endpoints

You can create and add tags to an endpoint to improve identification and understanding of that endpoint. You can search your assets according to these tags.

For example, you might have standard tags such as *UNIX* and *SQL* that apply to several 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 the endpoint must meet the particular security policy.

For more information about adding tags to endpoints, see "Create and Apply Tags" on page 88.

Check the Heartbeat

A **heartbeat** is a periodic pulse from the endpoint that contains information related to the endpoint's viability and status. Checking the heartbeat of an endpoint is crucial in determining whether the selected endpoint is online and can be assessed. If a endpoint is offline, you might need to re-register the endpoint.

1. Select the endpoints that you want to check.

   To ensure peak product performance, you can select a maximum of 50 endpoints at a time.
2. Click **... > Check heartbeat**.
3. Refresh the page to view the results.

NOTE: It might take a while for Core Services to complete the heartbeat check.

Re-register

When Secure Configuration Manager registers an endpoint, it gathers information such as major and minor versions of the operating system or application that the endpoint represents. If an endpoint appears offline but is running, you might need to re-register it with Secure Configuration Manager.

1. Select the endpoints that you want to re-register.

   To ensure peak product performance, you can select a maximum of 50 endpoints at a time.
2. Click **... > Re-register**.

Review Endpoint Status and Properties

The Web console lists basic information about each endpoint to help you chose the appropriate policy templates to run against it and to determine whether the endpoint is communicating with Core Services.

To **view the details** about an endpoint, such as recent policy template runs, select the endpoint. For more information, see Chapter 4, "Understanding Endpoint Properties," on page 19.

Search for Endpoints

You can search for endpoints or filter the list of endpoints, based on a wide variety of criteria including user-defined tags. For more information, see "Search Query Criteria" on page 91.

Generate a Dynamic Report

You can create a dynamic report for the selected endpoints. For more information, see Chapter 13, “Generating a Dynamic Report,” on page 49.

4 Understanding Endpoint Properties

Select **Manage > Endpoints > *selected endpoint***

Endpoints are the operating systems, devices, and applications that agents help Secure Configuration Manager to assess for vulnerabilities. You can review the current state of a selected endpoint, including results of recent policy template runs.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

“Configurable Properties” on page 19

Details that you can change, such as the endpoint’s importance to your organization or the tags associated with that endpoint

“Descriptive Properties” on page 20

System-generated information about the endpoint, such as its software version and the agent that manages the endpoint

Configurable Properties

When you add an endpoint, you can provide details about the endpoint’s properties. You can add or remove tags in this Web console. However, to **edit properties** other than tags, you must use the Windows console.

Importance

Identifies the level of criticality that the endpoint might pose to the security of your organization.

Location

Describes the place where the server resides. For example, *Houston, Texas* or *ABC Finance*.

Online / Offline

Indicates whether the endpoint is connected to Core Services, and thus available for gathering data.

Registered

Indicates whether the endpoint has been registered with Core Services. You can add endpoints without registering them. However, you cannot gather data from an unregistered endpoint.

Tag

Serves as customized labels that help users identify, organize, and search for endpoints. For more information, see “Tag Endpoints” on page 16.

Descriptive Properties

The Web console also gives you version information regarding the endpoint's type, such as version of operating system or SQL Server so you know exactly which security checks and policy templates to run.

Also, you can view the policy templates that have been run most recently against the endpoint, as well as the results of those runs. At a glance, you can tell whether the endpoint is out of compliance or poses a high risk to your environment.

5 Managing Groups

Select **Manage > Endpoints > Groups**

Groups contain collections of endpoints and other groups. By default, Secure Configuration Manager organizes your endpoints by the computer's operating system.

To more easily specify which IT assets you want to analyze when you run assessments, you can create custom groups. Secure Configuration Manager then displays policy template results according to your custom groups. Ensure that you assign all endpoints to one of your custom groups.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Audit Groups of Endpoints

You can run a policy template or security check against one or more groups. Select the group or groups, then specify whether you want to run a policy template or security check.

1. Select the group(s) containing the endpoint(s) that you want to audit.
2. Select **Run Policy Template** or **Run Security Check**, then complete the run process.

   For more information, see Part II, "Assessing Your Managed Assets," on page 23.

NOTE: Secure Configuration Manager cannot communicate with agents that are not registered. If an unregistered agent manages any endpoints in the selected group(s), Secure Configuration Manager will not collect data from those specific endpoints.

Organize Endpoints in Groups

Adding a **group** to the **My Groups** folder allows you to organize endpoints according to your preferred criteria. You can nest your customized groups such that you have groups within groups.

The entire set of endpoint groups is called a **forest**. Each top-level node, such as the **My Groups** folder, is called a **tree**. The following rules apply to endpoint groupings:

- An endpoint can belong to many trees, but can be a member of only one group in any given tree
- A group can contain endpoints and other groups
- You can **move** or remove endpoints in a group at any time
- You can add endpoints to groups and move endpoints from one group to another within **My Groups**
- To place an endpoint in groups in other trees, you can **copy** the endpoint to the additional groups.

Place Endpoints in a Group

1. Select the endpoint(s) that you want to place in a group.
2. Click **... > Move**.
3. (Conditional) to the move endpoint(s) to an existing group, specify the group.
4. (Conditional) to move the endpoints to a new group, complete the following steps:
   - **4a** Select the location within My Groups where you want to place the new group.
   - **4b** Click **Create New Group & Move**.
   - **4c** Specify the name of the new group.

   For more information creating groups, see “Organize Endpoints in Groups” on page 21.
5. Select **Move**.

Move Endpoints to a Different Group

1. Expand the group containing the endpoints that you want to move or copy to a different group.
2. (Conditional) To keep the endpoints in the current group but also add them to a different group, click **... > Copy**.

   When you copy an endpoint to a group, the target group must be in a different tree than the current group. For example, the endpoint is currently in `My Groups > Finance > New York`. You can copy the endpoint to any branch within `My Groups` except to `Finance > [child groups]`.
3. (Conditional) To move the endpoints from the current group to a different group, click **... > Move**.
4. Specify the group where you want to place the endpoints that you selected.
5. Select **Move**.

Search for Groups

You can search for groups, based on a wide variety of criteria. For more information, see “Search Query Criteria” on page 91.

Assessing Your Managed Assets

Select **Assess**

Secure Configuration Manager lets you perform security audits of your IT assets by running security checks and policy templates. These assessments enable you to determine how well each asset in your IT environment complies with your company security policies and technical standards.

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** are a collection of security checks that your assets for a specific set of issues, such as those defined by the PCI DSS standards.

When you run a policy template against an endpoint or a group of endpoints, 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.

- Chapter 6, “Running a Policy Template,” on page 25
- Chapter 7, “Running a Security Check,” on page 27
- Chapter 8, “Selecting Assets to Audit,” on page 31
- Chapter 9, “Specifying Run Options,” on page 33

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

6 Running a Policy Template

Select **Assess > 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 more information about policy templates, see Part VII, “Understanding Policy Templates,” on page 69.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Run a Policy Template

You can run one or more policy templates against one or more endpoints or groups. Each policy template that you run results in a single assessment report.

1. Select the policy template that you want to use for the assessment, then click **Run Policy Template**.

   You can also start a policy template run from **Manage > Endpoints**, then click **Run Policy Template**.
2. Select the endpoints or groups of endpoints that you want to assessment, then click **Next**.

   For more information, see Chapter 8, “Selecting Assets to Audit,” on page 31.
3. Specify how you want the assessment report to be configured.

   For more information, see Chapter 9, “Specifying Run Options,” on page 33.
4. (Conditional) To run the policy template immediately, click **Run Now**.
5. (Conditional) To run the policy template in the future or on a regularly basis, click **Schedule**.

   For more information, see “Create a Recurring Schedule for Policy Templates” on page 34.
6. When the run completes, evaluate the status of your endpoints.

   For more information, see Part III, “Using Assessment Reports to Identify Risks and Vulnerabilities,” on page 37.

Schedule Policy Template Runs

You can schedule regular runs of your preferred policy templates. For more information about scheduling a policy template run, see Chapter 9, “Specifying Run Options,” on page 33.

View Results of a Run

Secure Configuration Manager saves the policy template results in a report - one report per policy template.To help you resolve vulnerabilities, the report lists the expected value for each security check versus the actual value found on the endpoint.

For more information, see Part III, “Using Assessment Reports to Identify Risks and Vulnerabilities,” on page 37.

Configure the Run Options

When you run a policy template, the wizard enables you to specify whether you want to notify a person or change management system when an endpoint is out of compliance. You can also specify the timing of the and whether you want it to run on a regular basis.

For more information, see Chapter 9, “Specifying Run Options,” on page 33.

7 Running a Security Check

Select **Assess > Security Checks**

Secure Configuration Manager provides hundreds of built-in security checks to ensure policy compliance. A **security check** is a query that an agent performs on an endpoint to test for potential vulnerabilities in the endpoint's configuration settings, such as who has user privileges for an Oracle database.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Start a Security Check Run

You can run one or more security checks against one or more endpoints or groups.

1. Select **Assess > Security Checks**.
2. Select the security checks that you want to run, then click **Run Security Check**.
3. Select the endpoints or groups that you want to assess, then click **Next**.
4. (Conditional) For security checks with user-definable parameters, specify values or apply a saved list of values.

   For more information, see "Specify Values for User-Definable Parameters" on page 28.
5. Click **Next**.
6. (Optional) Modify the default values for the severity range if they do not suit your environment.

   For more information, see "Modify the Severity Range for a Security Check" on page 35.
7. (Optional) Specify whether you want to send notifications about the results of the assessment to individual email accounts and to a change management system.

   For more information, see "Email Notifications about Assessment Results" on page 33.

You can also start a security check run from **Manage > Endpoints**, then click **Run Security Check**.

Specify Values for User-Definable Parameters

Some security checks include **user-definable parameters** so you can customize the security check for each particular run. For example, the *AD Group Changes Within X Days* security 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* security check, the default value is 14 days. However, some parameters are **mandatory** but do not have default values. When this occurs, the console prompts you to specify a value before you can run the security check. For some parameters, you can also create and apply a **saved list** of values.

- "Specify Parameter Values" on page 28
- "Apply a Saved List to a Parameter" on page 28

Specify Parameter Values

You can specify parameter values in one of the following ways:

Customize parameter values

Select the security check then deselect **Use default values**. Modify the values as desired.

Specify values only for mandatory parameters

Click **... > Show checks with missing mandatory fields**, then select each security check to specify the values.

The console prompts you when one of the displayed security checks requires you to specify mandatory values. However, the console displays no more than 10 of your selected security checks at a time. If you are running more than 10 security checks, click through the full list to ensure that you specify all mandatory values.

Apply a saved list to a value

See "Apply a Saved List to a Parameter" on page 28.

Apply a Saved List to a Parameter

Many security checks return a set of results containing multiple rows of data. To simplify the returned results, you can exclude or include some values by using a saved list. **Saved lists** are lists of values that you can reuse in security checks as a filter. Saved lists can include values such as user names, file names, registry keys, ports, or services.

You can apply a saved list to any user-definable parameter in a security check.

1. On the **Run Security Checks > Parameters** page, select the check where you want to apply a saved list.
2. For the parameter that will use the saved list, click **Add a saved list**.
3. Specify one or more saved lists, then click **Apply**.

For more information, see Chapter 18, "Including or Excluding Values in a Security Check Parameter," on page 63.

View Results of a Run

Secure Configuration Manager saves the check results in a report - one report per security check. To help you resolve vulnerabilities, the report lists the expected value for each security check versus the actual value found on the endpoint.

For more information, see Part III, “Using Assessment Reports to Identify Risks and Vulnerabilities,” on page 37.

Group Security Checks in a Policy Template

If you regularly run several security checks as a group, you might want to create a custom policy template for those security checks. For more information, see the *Administrator's Guide for NetIQ Secure Configuration Manager*.

8 Selecting Assets to Audit

When you run a policy template or security check, you can choose to assess one or more endpoints or groups of endpoints. You can initiate the run from **Manage > Endpoints**, **Policy Templates**, or **Security Checks**.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

9 Specifying Run Options

When you run a policy template or security check, the wizard enables you to specify whether you want to notify a person or change management system when an endpoint is out of compliance. You can also specify the timing of the assessment and whether you want it to run on a regular basis.

For more information about running a policy template or security check, see Chapter 6, "Running a Policy Template," on page 25 and Chapter 7, "Running a Security Check," on page 27.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Email Notifications about Assessment Results

Secure Configuration Manager can send notifications about the results of an assessment to individual email accounts and to a change management system. For example, you might want to notify the server manager when the results of a policy template indicate that the SQL Server endpoint on the server is out of compliance.

Enable email compliance alerts

Secure Configuration Manager sends an email notification to specified users when an endpoint's results are out of compliance. By default, Secure Configuration Manager uses the email addresses listed in the **Contact Email** field of the endpoint's properties.

For more information, see "Automating Out-of-Compliance Notifications" in the *Secure Configuration Manager User Guide*.

Forward assessment report to destination server

Every organization has complex workflows and change management processes that require adherence. Secure Configuration Manager can send the results of the assessment report to a server, such as your change management system. For more information, see "Integrating with a SIEM Solution" in the *Secure Configuration Manager User Guide*.

When to Run a Policy Template

Secure Configuration Manager provides the following options for running the selected policy template:

Run Now

Runs the policy template immediately, and runs the policy template once only.

Once

Starts the run at the specified time, and runs the policy template once only.

Recurring

Runs on a periodic schedule, based on the specified settings. For more information, see “Create a Recurring Schedule for Policy Templates” on page 34.

Create a Recurring Schedule for Policy Templates

To run a policy template on a recurring schedule, use the following settings:

Occurrence pattern

Specifies whether you want the schedule to run daily, weekly, monthly, or continuously

Every *n* days or *n* weeks

Applies only when you specify a daily or weekly occurrence pattern

Specifies how often the schedule reoccurs. For example, every two weeks.

(Conditional) For a **Weekly** occurrence, you must also specify the days of the week on which the run occurs.

Frequency > Occurs once at

Specifies when in the specified **Occurrence pattern** that the run occurs. For example, the time of day for a daily occurrence.

Frequency > Every

Specifies how often you want to run the policy template on the scheduled day. For example, every six hours.

You must also specify the time of day during which the runs occur. For example, starting at 08:00 and ending at 15:30.

Day of the month

Applies only when you specify a monthly occurrence pattern

Specifies how often the schedule reoccurs during the month. For example, every 11 days.

You must also specify how often the schedule repeats on a monthly basis. For example, every two months.

Day of the week

Applies only when you specify a monthly occurrence pattern

Specifies the days of the week on which the schedule occurs, as well as which week of the month. For example, on the first and third Monday and Thursday of the month.

You must also specify how often the schedule repeats on a monthly basis. For example, every two months.

Duration

Specifies the beginning and ending dates of the schedule. To run the schedule perpetually, specify a start date, then select **Repeat forever**.

Modify the Severity Range for a Security Check

Security checks let you score each asset to determine vulnerabilities. The **severity range** specifies the level of risk that the security check might pose to your environment. In the report, Secure Configuration Manager displays a pie chart showing the distribution of endpoints in each risk score range. You can modify the default values for the severity range if they do not suit your environment.

II Using Assessment Reports to Identify Risks and Vulnerabilities

Select **Reports > Assessment Reports**

To help you evaluate how the endpoints in your environment adhere to the security and system configuration policies you want to enforce, you can review the results of policy templates and security checks run on those endpoints.

When you run a policy template or security check, Secure Configuration Manager generates a **job**. Each job runs asynchronously so you can initiate or schedule concurrent runs of policy templates and security checks. In **Jobs**, you can view the status of the scheduled, pending, and completed jobs. You can also view an **assessment report** for each policy template or security check that runs successfully.

To simplify the results of your assessments, you can **include or exclude data** for specific security checks or endpoints and groups. Depending on how you want to filter the data in report results, you can create and apply saved lists or exceptions. For more information, see Part V, “Managing Data in Reports,” on page 59.

- Chapter 10, “Choosing an Assessment Report to Review,” on page 39
- Chapter 11, “Reviewing an Assessment Report,” on page 41

You can also combines the results of multiple policy templates into a **dynamic report**. For more information, see Part IV, “Using Dynamic Reports to Identify Risks and Vulnerabilities,” on page 45.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

10 Choosing an Assessment Report to Review

Select **Reports > Assessment Reports**

The Web console lists the assessment and dynamic reports that you can view. **Assessment reports** contain results of a single policy template or security check run.

- “View an Assessment Report for a Single Policy Template” on page 39
- “View the Results of Multiple Policy Templates” on page 39

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

View an Assessment Report for a Single Policy Template

You can view an assessment report from **Reports > Assessment Reports** or **Jobs > Completed**.

Select any report to view its contents. You can drill down into the results to determine which endpoints and groups failed security checks, and how. For more information, see Chapter 11, “Reviewing an Assessment Report,” on page 41.

View the Results of Multiple Policy Templates

The Web console provides **dynamic reports** that allow you to combine the results of multiple policy templates and endpoint types. For more information, see Part IV, “Using Dynamic Reports to Identify Risks and Vulnerabilities,” on page 45.

11 Reviewing an Assessment Report

Select **Reports > Assessment Reports**

When an assessment report for a policy template or security check run completes, you can view the results in Assessments Reports.

Depending on the type of assessment, you can drill down into the results to determine which endpoints and groups failed security checks, and how. You can select endpoints, then re-run the failed checks for those endpoints only.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Understand the Report Overview

Assessment reports contain results for a single policy template or security check run. The **Overview** provides a high-level view of how the selected assets comply with the technical standards and organizational policies represented by the policy template.

NOTE: If an assessment 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.

Depending on the type of policy template run, you might see the following data in the report:

Compliance status

Displays the overall compliance of the endpoints based on the data collected for the policy template. A **compliant** asset meets your organization's policies for assessment, operation, and control of systems and resources according to security standards, best practices, and regulatory requirements.

Each policy template has a specific range of compliance risk scores that Secure Configuration Manager uses as a baseline when calculating endpoint results. If an endpoint is **compliant**, then its risk score is lower than the out-of-compliance risk score range. An **unknown** compliance indicates incomplete data for the endpoint. Data might not be available because the some security checks do not apply to an endpoint, Secure Configuration Manager was unable to connect to the agent, or an endpoint returned errors.

Overview of risk or vulnerability

Summarizes the risk or vulnerability state of the endpoints and groups associated with the report.

The report displays **risk-based** results when the policy template tests endpoints for a specific configuration setting or security risk on a specific platform, such as user privileges for an Oracle database.

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. An endpoint's **importance** represents the criticality level of that endpoint in your organization. For example, a database endpoint containing customer financial data might have a higher importance level than a database of customer references.

Endpoints with the highest risk or vulnerability

Lists the endpoints that most likely pose a security threat to your environment.

Security checks most likely to pose a risk or vulnerability

Lists the security checks that endpoints failed, which might pose a security issue.

Endpoints at Risk (by location)

Provides a map-based view of endpoints with the highest risk results.

Export Assessment Results

You can export a completed assessment in PDF format.

1. Navigate to **Reports > Assessment Reports**.
2. Select the report.
3. Click **... > Download**.

   Depending on your browser settings, the browser might prompt you for the file name and download location.

Identify Areas that Cause Security Risks

Depending on the policy template, you can view results based on the security checks in the policy template, common vulnerabilities and exposures (CVEs), or requirements associated with a security standard.

You can quickly determine the overall number of security checks with failed and successful results. Then you can delve into a detailed view any particular security check to determine which endpoints failed and how.

- "Endpoints that Pose a Security Risk" on page 42
- "Security Checks that Result in the Most Failures" on page 43

It is possible that an endpoint might temporarily be causing a problem or some results returned might not be relevant for your security policies and standards. To remove this information from the assessment report, see "Simplify the Data in a Report" on page 44.

Endpoints that Pose a Security Risk

In the report view, click **Endpoints & Groups**.

To quickly find endpoints that might pose a security risk, you can select **Endpoints at Risk**. You can also sort the table by **Failed Security Checks** or **Compliance**.

Select an endpoint to view its compliance per security check. Then review the **Expected Value** and **Actual Value** columns to identify why the endpoint failed the security check.

Example

The completed assessment for the *NetIQ Password Strength* policy template indicates that endpoint `ABCTest` failed two security checks. You select the endpoint to identify where the risks occurred. You observe the following results:

Security Check	Compliance Status	Expected Value	Actual Value	Check Result
Accounts with passwords that never expire	Failed	0	1	Description: Built-in account for guest access to the computer/domain Status: Disabled Last login date: Never logged on
Minimum number of passwords remembered	Failed	greater than or equal to 24	0	Status: 0

The endpoint has one account with a password that never expires, which might pose a security risk if malicious users know about this built-in account. The security check expects to find no such accounts. Moreover, another security check discovered that the server fails to store previously used passwords, which is a safeguard to prevent the re-use of old passwords.

For more information about resolving these failures, see "Resolve the Discovered Security Risks" on page 43.

Security Checks that Result in the Most Failures

In the report view, click **Security Checks**.

You can identify the security settings that resulted in the most failures among your endpoints. From there, you can determine which endpoints might pose the greatest risk to your environment.

Identify the security checks that one or more endpoints failed

Select the value below **Failed**. You can clear this filter as needed.

Determine which endpoints are at risk

Select a security check from the **Failed** list, then click **Endpoints**.

For more information about security check **Properties**, see Chapter 24, "Viewing Details of a Security Check," on page 81.

Resolve the Discovered Security Risks

Secure Configuration Manager helps you to resolve the security risks reported by an assessment in the following ways:

Notify the system administrator

In the assessment report, you identified the endpoints that failed a security check. The assessment also tells you the value for the configuration setting value that would result in a successful result. You can now ask the endpoint's administrator to resolve the failures. For ease of communication, you send the relevant information from the assessment report to the administrator. For more information, see "Export Assessment Results" on page 42.

Create an exception

You know that the settings that caused the failed security checks are acceptable for that particular server or endpoint. So you create an **exception** for the endpoint or the security checks to prevent the failed conditions from causing a violation. For more information, see Chapter 17, "Excluding Data from Reports," on page 61.

Simplify the Data in a Report

When you run policy templates against a large number of endpoints or groups of endpoints, the results can be overwhelming. You might want to reduce the amount of data returned by applying exceptions to a certain set of values. Alternatively, some results returned might not be relevant for your security policies and standards. To simplify assessment results, you can exclude or include specific data for specific endpoints or groups.

To view data that has already been excluded from the report, select **Exceptions**. For more information, see Chapter 17, "Excluding Data from Reports," on page 61.

NOTE: The individual who ran the policy template or security check might also have pre-filtered the security check's results by applying a saved list. For more information, see "Including or Excluding Values in a Security Check Parameter" on page 63.

IV Using Dynamic Reports to Identify Risks and Vulnerabilities

Select **Reports > Dynamic Reports**

To get a clear understanding of the state of your assets, you can combine the results of multiple policy templates and endpoints into a single **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.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

12 Understanding Dynamic Reports

Select **Reports > Dynamic Reports**

To get a clear understanding of the state of your assets, you can combine the results of multiple policy templates and endpoints into a single **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.

- "Elements of a Dynamic Report" on page 47
- "Types of Dynamic Reports" on page 47

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Elements of a Dynamic Report

The Web console builds a dynamic report according to the following elements, which you specify in the report definition:

Assets

Helps you identify which IT assets are important for the particular dynamic report.

You can specify individual endpoints or groups of endpoints. The endpoints can be of different types, such as UNIX operating systems, Windows operating systems, SQL Server database, and Oracle database.

Policy Templates

Helps you define the type of security check results that you want to review for the specified assets.

Depending on your chosen assets, you might specify policy templates. As a best practice, you might want to narrow the scope to a specific technical standard or security policy, such as PCI compliance.

Time range

Narrows the scope of the policy template results to data returned within a specific range of time. For example, the last seven days.

If a chosen policy template has run more than once during the specified time frame, the Web console gathers results from the most recent run.

NOTE: If you have recently added assets or just begun using Secure Configuration Manager, it is possible that the chosen policy templates might not have run in the specified time frame. When this occurs, the generated report would not contain data or not have data for all of the chosen endpoints.

Types of Dynamic Reports

Each report definition aligns with one of the following categories:

Compliance

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

Risk

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

Snapshot

Gives you a high-level view of the state of risk and compliance for the specified endpoints or groups of endpoints.

NOTE: If an assessment 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.

You can create new report definitions by modifying an existing definition or by starting with no base definition setting other than one of these types. For more information, see Chapter 14, "Creating a Report Definition," on page 51.

13 Generating a Dynamic Report

When you generate a dynamic report, the Web console gathers the data from the Secure Configuration Manager 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 in the specified time frame for the endpoints specified in the report definition.

- “Generate a Report without a Report Definition” on page 49
- “Generate a Report from an Existing Definition” on page 50

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Generate a Report without a Report Definition

You can generate a report without an existing report definition from one of the following locations in the Web console:

- **Assets > Endpoints**
- **Assess > Policy Templates**
- **Reports > Dynamic Reports > Create Custom Report**

  For more information about creating a custom report definition, see Chapter 14, “Creating a Report Definition,” on page 51.

As you generate the report, you can save your settings as a new report definition. The following procedure provides an example of starting from **Assets > Endpoints**.

1. Click **Assets > Endpoints**.
2. Select the endpoints that you want to include in the dynamic report.

   You can select any combination of endpoints, regardless of their operating system or endpoint type.
3. Click **Generate Dynamic Report**.
4. Specify the category of dynamic report that you want to use, then click **Next**.

   For more information about the report categories, see “Types of Dynamic Reports” on page 47.
5. Select the policy templates that you want to include in the dynamic report, then click **Next**.
6. Specify the **Report Name** and (optional) **Report Description**.
7. For **Time Range**, specify the range of time within which you want to gather assessment results associated with the selected endpoints and policy templates.
8. (Optional) To save these settings as a report definition, complete the following steps:

   8a Click **Save definition as**, then specify a name and description.

   8b Click **Save**.
9. Click **Preview**.

If the policy templates have not been run against the endpoints in the specified time frame, then the Web console responds with “No data found.” You can modify the time frame, endpoints, or policy templates.

10. (Optional) In the preview, select **Change** to preview the results for each policy template included in the dynamic report.
11. (Optional) Modify the report settings and preview again until you are satisfied with the results.
12. In the Preview, click **Save Report**.

    The Web console automatically displays the report.
13. (Conditional) To view the report results at a future time, click **Reports > Dynamic Reports**, then open the saved report.

Generate a Report from an Existing Definition

Report definitions contain a specific combination of endpoints and policy templates, as well as particular time frame. You cannot modify those values.

1. Click **Reports > Dynamic Reports**.
2. Click **Choose a Definition** within the desired category.

   For more information about report categories, see “Types of Dynamic Reports” on page 47.
3. Select the report definition that you want to use, then click **Next**.
4. Specify the **Name** and (optional) **Description** for the report.
5. Click **Save**.

   The Web console automatically displays the report.
6. (Conditional) To view the report results at a future time, click **Reports > Dynamic Reports**, then open the saved report.

14 Creating a Report Definition

Select **Reports > Dynamic Reports**

Each **report definition** includes a set of policy templates and endpoints, as well as the time frame from which to draw the data. To meet your organization's specific security needs, you can create custom report definitions. For example, you might want a report that shows the compliance status for all endpoints, based on 10 different policy templates.

1. Select **Reports > Dynamic Reports**.
2. In the appropriate category, click **Create your own**.

   For more information about the report categories, see "Types of Dynamic Reports" on page 47.
3. Select the endpoints that you want to include, then click **Next**.
4. Select the policy templates that you want to use for assessing the assets, then click **Next**.
5. Enter a name and description for the report.

   Report Name and **Report Description** help you more easily find the report in the Assessment Reports list. These values do not affect the name or description of the report definition that you used as the basis for the generated report.
6. For **Time Range**, specify the range of time within which you want to gather assessment results associated with the selected endpoints and policy templates.
7. Click **Save definition as**, then specify a name and description for the new report definition.
8. Click **Save**.
9. Click **Preview**.

   If the policy templates have not been run against the endpoints in the specified time frame, then the Web console responds with "No data found." You can modify the time frame, endpoints, or policy templates. If you make changes, you should create a new report definition with those changes.
10. (Optional) In the preview, select **Change** to preview the results for each policy template included in the dynamic report.
11. (Optional) Modify the report settings and preview again until you are satisfied with the results.
12. In the Preview, click **Save Report**.

    The Web console automatically displays the report.
13. (Conditional) To view the report results at a future time, click **Reports > Dynamic Reports**, then open the saved report.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

15 Reviewing a Dynamic Report

Select **Reports > Dynamic Reports > *selected_report***

Depending on the type of dynamic report that you generate, you can drill down into the results to determine which endpoints and groups failed security checks, and how. This section provides information about **viewing** a saved dynamic report. To **run** a new dynamic report, see Chapter 13, “Generating a Dynamic Report,” on page 49.

Dynamic reports include charts and graphs to help you visualize changes in endpoint status. However, the Web console does not display a graph or chart when the report results contain a single set of data. For example, Secure Configuration Manager calculates trend data based on at least two sets of policy template runs. If only one run has been completed, the Web console cannot display the trend.

For more information about dynamic reports, see Chapter 12, “Understanding Dynamic Reports,” on page 47. For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Find a Saved Report

If more than 10 reports have been saved in one of the categories, you might need to click **View all** to find your report.

If no reports have been saved for a category, the Web console displays only the **Choose a Definition** and **Create Your Own** categories. From these, you can create a dynamic report or report definition. For more information, see Chapter 13, “Generating a Dynamic Report,” on page 49.

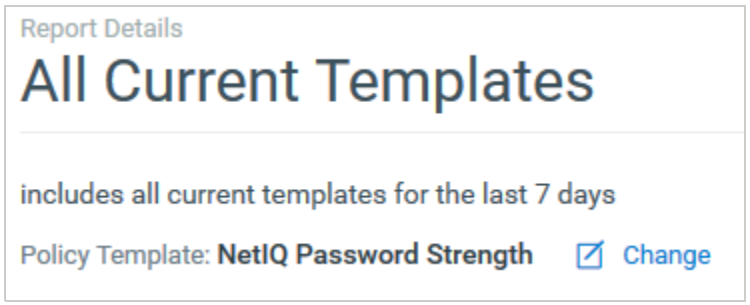
Snapshot Reports

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.

View Results for a Specific Policy Template

While a **Snapshot** report contains the results of all the policy templates specified in the report definition, the **Overview** displays only the results for one policy template at a time.

1 Click **Change**, which is to the right of the name of the currently displayed policy template.



2 Select the next policy template that you want to view.

3 To identify endpoints that failed the policy template, click **Endpoints > Endpoints at Risk**.

4 To identify the settings that need to be corrected, click **Check Details** for an endpoint.

View Endpoint Status for All Policy Templates

You can also view the status of an endpoint based on all policy templates included in the dynamic report.

1 Click **Overview**, then scroll to **Top 5 - Endpoints at Risk**.

2 Click the endpoint that you want to review.

3 In the policy templates table, review the compliance and risk status for the endpoint.

4 (Optional) To apply a **tag** to help you identify the endpoint at a later time, complete the following steps:

4a Click **Add Tags**.

4b Complete the wizard for applying a tag.

For more information, see “Create and Apply Tags” on page 88.

Compliance Reports

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

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 per policy template. 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 Reports

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. To drill down to the specific endpoints, click the desired risk category for one of the policy templates.

16 Managing Report Definitions

You must have an Administrator role to perform this function.

Select **Reports > Dynamic Reports > Manage Definitions**

You can **delete** existing report definitions.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

V Managing Data in Reports

You must have specific permissions to perform this function. For more information, speak to the Secure Configuration Manager administrator.

Secure Configuration Manager allows you to create **exceptions** for all data returned by a security check for endpoints or a group of endpoints, or to except specific data returned by the security check. You can also use **saved lists** to exclude or include values from security checks.

- Chapter 17, “Excluding Data from Reports,” on page 61
- Chapter 18, “Including or Excluding Values in a Security Check Parameter,” on page 63

For more information, see the NetIQ Secure Configuration Manager documentation.

17 Excluding Data from Reports

You must have specific permissions to perform this function. For more information, speak to the Secure Configuration Manager administrator.

You can create temporary waivers, or **exceptions**, to prevent conditions from causing a violation in the reported results for a security check associated with a policy template.

You can also run a security check that contains a saved list, then modify the values in the list. For more information, see "Including or Excluding Values in a Security Check Parameter" on page 63.

Understand Exceptions

You can create and apply the following types of exceptions:

- Endpoints or a group of endpoints for individually run security checks
- Endpoints or a group of endpoints for security checks in a policy template run

Typically, you create an exception when you do not want a particular violation to display in the assessment report, or when you want to prevent a particular security check from running for an endpoint or a group of endpoints. For example, if a server in your environment is currently undergoing maintenance, you might want to create an exception to suspend monitoring that server with certain security checks.

When creating an exception, you can specify a **reason** for excepting that security check or endpoint. The Web console provides default reasons for the exception, or you can create your own. You can also specify the time frame during which the exception will be active.

Create and Apply Exceptions

After you apply an exception, the Web console re-generates the report. The updated report shows *Applied* in the **Exceptions** column.

NOTE: In some organizations, exceptions must be approved before they can go into effect in an assessment report. For more information, see "Manage Exceptions with an Approval Process" on page 62.

---

1. Open the assessment report where you want to make the exception.
2. (Conditional) To make an exception based on a security check, select the **Security Checks** tab.

   The Create exception wizard prompts you later to specify the endpoints or groups that you want to associate with the selected security checks.
3. (Conditional) To make an exception based on an endpoint or group, select the **Endpoints** tab.

The Create exception wizard prompts you later to specify the security checks that you want to associate with the selected endpoints or groups.

4. Select the security checks or endpoints that you want to except, then click **Create exception**.
5. (Conditional) If you selected security checks in Step 4, specify the endpoints that you want to except from the security check results.
6. (Conditional) If you selected endpoints or groups in Step 4, specify the security checks whose results you want to exclude from the report.
7. Click **Next**.
8. Specify a name, description, and reason for the exception.
9. (Conditional) If you create a custom **Reason** for the exception, ensure that you also enter a description of the reason so that other users can understand the reason's purpose.
10. Click **Enable** to activate the exception.
11. (Optional) To set a time limit on the exception, specify start and end dates.

    If you do not specify a value for **End date**, the exception never expires.
12. Click **Create**.
13. (Optional) Create another exception.
14. To apply the exceptions, click **... > Apply exceptions**.
15. To view the report with exceptions applied, return to **Reports > Assessments** and open the report, which should now say *Applied* in the **Exceptions** column.

Manage Exceptions with an Approval Process

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

If you enable the approval process, the exceptions created and applied in the Web console must be approved in the Windows console before they can go into effect. For more information, see "Enabling Exception Approvals" in the *User's Guide to Secure Configuration Manager*.

Delete an Exception

When you delete an exception from an assessment report, you cannot re-apply it. Instead, everything associated with that exception is removed from the database.

As an alternative, to save the exception for later use, use the Windows console to revoke the exception. For more information, see the Help for the Windows console.

1. Select the **Utilities > Exceptions**.
2. Select one or more exceptions that you want to delete.
3. Select **Delete**.

18 Including or Excluding Values in a Security Check Parameter

You must have specific permissions to perform this function. For more information, speak to the Secure Configuration Manager administrator.

Many security checks in Secure Configuration Manager return a set of results that contain multiple rows of data. When you run a policy template, the resulting set of returned rows of data can be difficult to review. To simplify the returned results, you can exclude or include some values by using a saved list. **Saved lists** are lists of values that you can reuse in security checks as a filter.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Understand Saved Lists

Saved lists can include values such as user names, file names, registry keys, ports, or services. The content in a security check depends on the parameter values that you want to filter. Saved lists include the following settings:

Data Type

Specifies the type of value that the saved list contains, such as an integer (number) or string (text). All values in a saved list use the same data type. You cannot mix data types in a saved list.

Attribute

Specifies which attributes in the security check that the saved list should as filter criteria.

Value

Specifies all values associated with the saved list.

Create or Modify a Saved List

You can create and apply a saved list when you run a policy template that contains a user-configurable parameter that supports saved lists. For example, the *Entitlement for drives and shares for specific users and groups* security check.

1. Select **Assess > Security Checks**.
2. Select the security checks for which you want to create or modify a saved list, then click **Run**.

   The Web console lists 10 of the selected security checks at a time. You might need to scroll through the list to reach all of the security checks with user-configurable parameters.
3. Select the security check that the Web console highlights as having user-configurable parameters.

4. If the security check supports a saved list, select **Add Saved List**.
5. Select the **Edit** icon.
6. Specify values for the saved list.

   NOTE: Saved lists do not support wildcard characters.

7. Select **Create** or **Edit**.
8. Select **Apply**.

Apply a Saved List to a Security Check

You can use any saved list that you create in any security check, as long as the saved list's values match the parameter requirements. For example, you cannot apply a saved list that contains integers to a parameter that requires user account names.

When running a built-in security check, apply a saved list using the **Exclusion List** field. When running a custom security check, you can use a saved list in the **Criteria** field for the filter.

1. Select **Assess > Security Checks**.
2. Select the security check to which you want to apply a saved list.

   The Web console lists 10 of the selected security checks at a time. You might need to scroll through the list to reach all of the security checks with user-configurable parameters.
3. Select the security check in the left pane.
4. Select **Add Saved List**.
5. Select one or more saved lists to apply to the security check.
6. Select **Apply**.

VI Understanding Jobs

Select **Jobs**

Secure Configuration Manager provides a queue of scheduled, in progress, and completed jobs.

For more information about **creating an assessment report** from a job, see Chapter 10, “Choosing an Assessment Report to Review,” on page 39.

- Chapter 19, “Determining the Status of a Job,” on page 67

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

19 Determining the Status of a Job

Select **Jobs**

Secure Configuration Manager enables you to track the status and history of all jobs run and pending a run. You can delete jobs, mark them as read, and re-run them. If you have console administrator permissions, you can view jobs for specific console users.

Jobs are organized in the following categories:

- “Does Not Apply” on page 67
- “Failed” on page 67
- “In Progress” on page 67
- “Scheduled” on page 68
- “Successful” on page 68

For more information about **creating an assessment report** from a job, see “Choosing an Assessment Report to Review” on page 39.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Does Not Apply

Failed jobs that occur when the selected policy template or security check does not match the selected endpoints.

For example, you inadvertently run a UNIX policy template against a Windows endpoint. Rather than reporting the policy template as a failure for that endpoint, which could be mistaken for a violation, Secure Configuration Manager labels the job results as ‘does not apply’.

To help you validate why a job does not apply, you can view a report for jobs in this category.

Failed

Jobs that did not complete successfully.A job might fail because the agent returned an error, Core Services could not connect to the agent, or the job timed out.

You can re-run a failed job. Select the job, then **Re-run**.

To determine why a job might have failed, you can view a report for jobs in this category.

In Progress

Jobs that are in progress but have not completed. Jobs remain here until the job successfully completes or fails. Select a job to see details about each of the endpoints the job is running against.

You can also cancel a job that is in progress.

Scheduled

Jobs that are scheduled to run in the future, such as a policy template that runs every month.

You can enable, disable, and delete scheduled jobs. When you disable a scheduled job, it remains in the queue but does not run. If the user account that created the scheduled job is disabled or deleted, Secure Configuration Manager no longer runs the scheduled job.

NOTE: Any previously run versions of a scheduled job will be in the other job queues, depending on the job's state.

Secure Configuration Manager automatically includes the following scheduled jobs:

Asset details and discovery

Enabled by default.

Allows you to gather information about currently managed UNIX and Windows endpoints and their security agents.

If you enable **Application Endpoint Discovery** 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 by querying 50 systems each run until all systems in your asset map have been checked. When the last managed asset has been scanned, Core Services restarts the process with the first managed asset.

Automatic system discovery

Disabled by default.

Enables you to regularly scan your environment for unmanaged assets, based on the settings for discovery in the Core Services Configuration Utility.

To view discovered systems, use the Windows console.

CyberScope Data Feed

includes aggregated data on all SCAP-enabled endpoints.

When you run this job, Secure Configuration Manager gathers from the database the results of the most recent SCAP policy template runs, including offline assessments imported to the database. Secure Configuration Manager compiles this data into an `.xml` file.

You can specify whether the `.xml` file is exported to a specific folder or email address.

Secure Configuration Manager gathers only for the endpoints and the benchmark IDs that you specify in the **SCAP** tab in the Core Services Configuration Utility. To meet CyberScope reporting standards, you must also provide information about your reporting department.

Benchmark IDs correlate to specific SCAP policy templates. SCAP policy templates are available only if you have the SCAP Module for Secure Configuration Manager installed.

Successful

Jobs that completed successfully. To launch a report based on a completed job, select **View Report**. You can also go to **Reports**, then select the report.

VII Understanding Policy Templates

Select **Assess > Policy Templates**

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** are a collection of security checks that audit your assets for a specific set of issues, such as those defined by the PCI DSS standards.

You can **delete** a policy template, run one or more policy templates, or generate a dynamic report from one or more policy templates. To **run a policy template**, see Chapter 6, “Running a Policy Template,” on page 25. To **generate a dynamic report**, see Part IV, “Using Dynamic Reports to Identify Risks and Vulnerabilities,” on page 45.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

20 Understanding the Categories

For ease of use, Secure Configuration Manager organizes policy templates in logical groups:

Regulations

Policy templates that assess whether your security configurations and policies conform to the policies recommended by rules and legislation, such as HIPAA and the Sarbanes-Oxley Act.

Bulletins

Templates that use information based on recent updates, such as critical patches to assess your security configuration. These templates also provide vulnerability announcements.

Best Practices

Policy templates that assess whether your security configurations and policies conform to best practices for specific areas of concern, such as account passwords and security patches.

SCAP

Available only when you have the SCAP Module for Secure Configuration Manager installed

Policy templates that assess whether your security configuration and policies conform to the policies specified in the imported SCAP content, such as FDCC.

My Templates

Policy templates created or imported by Secure Configuration Manager users.

For more information about a specific policy template, see Chapter 21, “Viewing the Details of a Policy Template,” on page 73. For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

21 Viewing the Details of a Policy Template

Select **Assess > Policy Templates > *selected policy template***

NOTE: To change the properties of a policy template, you must use the Windows console. For more information, see the NetIQ Secure Configuration Manager documentation.

Description

Provides an explanation of the policy template's purpose to help users determine whether they want to run the policy template.

Status

Indicates whether the administrator has enabled the policy template for use.

Type

Indicates the category for the policy template. For more information, see Chapter 20, "Understanding the Categories," on page 71.

Tags

You can create, view, and manage the tags associated with a policy template to improve identification and understanding. You can search for policy templates based on these tags.

For more information about adding tags to a policy template, see "Create and Apply Tags" on page 88.

Severity Ranges

Specifies the range of risk scores that apply to each Risk level. By default, a range of 0-100 represents a minor risk.

Be cautious when changing severity ranges, as any change to the range affects all policy templates.

Security Checks

Lists the security checks included in the policy template.

The **Alias Name** specifies alternate names that describe the unique instances of the security checks in the policy template. Usually, each instance verifies the status of different policies or requirements. The aliases are designed to help you review the audit report more effectively.

For example, the *CIS Level Two Benchmark for RHEL* policy template includes multiple instances of the *Software not installed* security check. Each instance has a unique name that indicates its purpose:

Security check name	Alias name
Software not installed	1.4.4 Remove SETroubleshoot
Software not installed	1.4.5 Remove MCS Translation Service (mcstrans)
Software not installed	2.1.11 Remove xinetd

In this example, the alias also includes a numerical reference to the particular CIS requirement.

22 Excluding Data from Policy Template Results

As you review endpoint assessments based on policy template runs, you can simplify the results in one of the following ways:

- Replace the default values in a security check with a specific set of values, such as a list of high-profile users
- Create exceptions that exclude the results of a combination of specific security checks, endpoints, and groups

For more information, see Chapter 17, “Excluding Data from Reports,” on page 61.

For more information about this software product, see the Secure Configuration Manager documentation.

23 Updating a Policy Template

Accurately assessing your computers requires regularly updating the security checks and policy templates in Secure Configuration Manager. The **AutoSync** service delivers new and updated security checks and policy templates when new vulnerabilities emerge.

AutoSync can provide automatic or manual downloads of the latest audit policies and standards. To configure AutoSync, use the Windows console.

For more information about AutoSync, see the NetIQ Secure Configuration Manager documentation and the Windows console Help.

VIII Understanding Security Checks

Select **Assess > Security Checks**

A **security check** is a query that an agent performs on an endpoint to test for potential vulnerabilities in the endpoint's configuration settings, such as who has user privileges for an Oracle database. Secure Configuration Manager provides hundreds of built-in security checks to ensure policy compliance.

- Chapter 24, "Viewing Details of a Security Check," on page 81
- Chapter 25, "Excluding Data from Security Check Results," on page 83

For more information about **running a security check**, see Chapter 7, "Running a Security Check," on page 27.

To receive **updated or new security checks**, use the AutoSync feature. To **modify** a security check or **import** a new or updated security check, use the Windows console. For more information, see the NetIQ Secure Configuration Manager documentation.

24 Viewing Details of a Security Check

Select **Assess > Security Checks > *selected security check***

Each security check includes the following properties:

Category

Specifies the type of information that the security check gathers based on the endpoint type, such as SQL Server or IIS. The following are examples of 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 in the Windows console, you can specify one of the available categories, create a new category, or leave the security check uncategorized.

Description

Provides specific information about how the security check functions.

Explanation

Describes the concept behind the security check to help you understand why you should run the security check and how the checked parameter or feature fits into the overall security scheme.

Risks

Describes the risks that you face by not mitigating the issues that the security check verifies.

Remedies

Help you solve the risks to bring non-compliant endpoints into compliance with the selected security check.

To **filter** the list of available security checks, use the **Search** function and the pull-down menu. For more information, see “Search Query Criteria” on page 91.

To **modify** or **import** a security check, use the Windows console.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

25 Excluding Data from Security Check Results

As you review endpoint assessments based on security checks, you can simplify the results in one of the following ways:

- Replace the default values in a security check with a specific set of values, such as a list of high-profile users.
- Create exceptions that exclude the results of a combination of specific security checks, endpoints, and groups

For more information, see Chapter 17, “Excluding Data from Reports,” on page 61.

To change the properties of a security check, you must use the Windows console. For more information, see the NetIQ Secure Configuration Manager documentation.

IX Managing the Web Console

You must have an Administrator role to perform the functions in **Utilities***.*

For most configuration settings, select **Utilities > *administrator function***. To configure single sign-on access between the Web console and the Dashboard, select ***Your ID*** **> Settings**.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

26 Managing Tags

You can create **tags** to serve as customized labels that help users identify, organize, and search the following objects in Secure Configuration Manager:

- endpoints
- policy templates

Your console administrator might create a common set of tags or allow console users to create their own tags.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Understand Tag Names

To reduce confusion and the potential for duplicate tags, tag names are not case-sensitive. For example, if you create a tag named *PCI*, Secure Configuration Manager will not allow you to create a second tag named *pci*.

Tag names are limited to 64 characters, including spaces and underscores (_). Tag descriptions can be no more than 255 characters.

View the Tag Associations

You can view which objects are associated with a particular tag. An **association** represents the link between a tag and the objects mapped to that tag.

NOTE: When you delete a tag, you also remove all of the associations for that tag.

---

1. Select **Utilities > Tags**.
2. For the tag whose associations you want to view, select the numeric value in the **Associations** column.

   For example, if you have a *UNIX* tag with 18 associations, select **18**.

Create and Apply Tags

Any console user can create and apply a tag. You can also apply multiple tags to each object.

1. Select one or more endpoints or policy templates.
2. Click **Tag**.
3. (Conditional) To apply an existing tag, complete the following steps:
   - **3a** Select a tag from the list or search for the tag.

     For more information, see “Search Query Criteria” on page 91.
   - **3b** Click **+**.
4. (Conditional) To apply a new tag, click **Create tag & apply**.
   - **4a** Specify a name and description for the tag.

     For more information, see “Understand Tag Names” on page 87.
   - **4b** Click **Create**.
5. Click **Apply**.

For more information, see “Tag Endpoints” on page 16 and “Tags” on page 73 for policy templates.

Modify and Delete Tags

To modify or delete tags, select **Utilities > Tags**.

You can always modify or delete the tags that you create. If you have an Administrator role, you can modify or delete tags created by any console user.

For more information about modifying a tag name, see “Understand Tag Names” on page 87.

Search for Tags

You can search for tags or items by their associated tags, based on a wide variety of criteria. For more information, see “Using Search” on page 91.

27 Managing Exceptions

You must have an Administrator role to perform this action.

When creating an exception, you can specify that the exception needs 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. By default, Secure Configuration Manager allows you to apply exceptions to security check results or endpoints immediately. For more information about establishing an approval process, see "Enabling Exception Approvals" in the *User's Guide to Secure Configuration Manager*.

To review and delete exceptions, click **Utilities > Exceptions**.

To create and apply exceptions, see Chapter 17, "Excluding Data from Reports," on page 61.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Review Exceptions

To review the current exceptions, select **Utilities > Exceptions**.

Secure Configuration Manager categorizes the exceptions according to their current status: approved, needs approval, and disapproved. For each exception, you can observe its purpose or reason for use, who created or last modified it, and the affected endpoints, groups, or security checks.

28 Using Search

Depending on the page, the Search function helps you find the following types of items in Secure Configuration Manager:

- Endpoints
- Jobs
- Policy templates
- Reports
- Security Checks
- Tags

You can search for these items or filter a list of items, based on a wide variety of criteria. If the item, such as an endpoint, supports user-defined tags, you can also search for the item by its tags.

- “Search Query Criteria” on page 91
- “Search for Items by their Tags” on page 92

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

Search Query Criteria

For your search terms, consider the following criteria:

Multiple values

Use spaces to separate multiple values. For example:

```
SQL Windows Finance
```

Special characters

You can use the following special characters in the search string:

```
@ $ - _ . | " ; < >
```

However, you must include the escape character \ before the following special characters:

```
| " ; < >
```

For example:

```
Finance \> Texas, Finance\|Texas
```

Phrases

You can search for phrases, such as `Finance_Dept` or `NetIQ Password Settings`. However, if the phrase includes a space, you might need to enclose the phrase in double quotation marks (“”):

- Use quotation marks when searching for a policy template or security check in **Assess > Policy Templates** or **Assess > Security Checks**. For example:

  ```
  "AD Domain", "NetIQ Password Settings"
  ```

- Use quotation marks when searching for an endpoint or group in **Manage > Endpoints**. For example:

  ```
  "Finance Dept", "Finance \> Texas"
  ```

- Do not use quotation marks when searching for security check or endpoint names in the tables of an assessment or dynamic report. For example:

  ```
  AD Domain
  ```

The Web console reports an error or “no data found” if your search does not meet the query criteria.

For more information about queries for finding a policy template or endpoint by its tag, see “Search for Items by their Tags” on page 92.

Search for Items by their Tags

You can find a policy template or endpoint by searching for its associated tags in the following locations:

- Manage > Endpoints
- Assess > Policy Templates
- Utilities > Tags

In the search field, enter `tagList:<tagName>`. For example:

```
tagList: windows, tagList: Finance
```

X Configuring the Web Console

You must have an Administrator role to perform the functions in **Settings***.*

You can enable users to launch the Dashboard from the Web console. To do so, you must configure the following settings:

- Chapter 29, “Enabling Users to Launch the Dashboard,” on page 95
- Chapter 30, “Connecting to the Analytics Database,” on page 97

To modify these settings, select ***Your_ID*** **> Settings**.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

29 Enabling Users to Launch the Dashboard

Select *Your_ID* > **Settings** > **Dashboard**

You must have an Administrator role to perform this action.

Web console users can launch the Dashboard without entering their credentials. To support a single sign-on process, provide one of the following scenarios in your environment:

- Install the Dashboard on the Core Services computer. The Analytics Database component can be on a separate server.
- Specify the **Port** and the IP address or name of the Dashboard's **Host** server. This assumes that the Dashboard is installed in the same domain as Core Services.

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`.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.

30 Connecting to the Analytics Database

Select ***Your_ID*** **> Settings > Analytics Database**

You must have an Administrator role to perform this action.

To properly display asset data, the Web console must connect to the Analytics Database, which is installed with the Dashboard. Specify the **Port** and the IP address or name of the database's **Host** server.

For more information about this software product, see the NetIQ Secure Configuration Manager documentation.