NetIQ Secure Configuration Manager SCAP Module

Module Guide

May 2016

Legal Notice

Contents

About This Book and the Library

This document provides information about installing the NetIQ Secure Configuration Manager Module for SCAP on Secure Configuration Manager computers. This document also covers importing SCAP policy templates, performing SCAP assessments on offline computers, and exporting aggregated reports.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

Other Information in the Library

The library provides the following information resources:

Installation Guide

Provides detailed information for planning for and installing Secure Configuration Manager.

User Guide

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

Windows Agent Guide

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

Help

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

Conventions

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

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

About NetIQ Corporation

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

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

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

Enabling critical business services, better and faster

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

Our Philosophy

Selling intelligent solutions, not just software

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

Driving your success is our passion

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

Our Solutions

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

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

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

Contacting the Online User Community

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

1 Introduction

The NetIQ Secure Configuration Manager Module for SCAP (SCAP module) enables your organization to implement the standards established by federal computer configuration initiatives: United States Government Configuration Baseline (USGCB) and Federal Desktop Core Configuration (FDCC). Using the components of the SCAP module, you can assess desktops and identify which systems are out of compliance. You can also create the necessary reports required by the U.S. Office of Management and Budget to demonstrate compliance with the standards.

1.1 What is SCAP?

Security Content Automation Protocol (SCAP) is a collection of six open standards, developed jointly by the government and the private sector, that specify the format of the content used to assess computer security. This common standard provides regulatory authorities and configuration managers a consistent way to construct a definitive guidance for system security. The standard specifies the content for platforms such as Windows and Internet Explorer, using the Extensible Configuration Checklist Description Format (XCCDF).

The SCAP module enables you to import properly formatted XCCDF content, and then use the content in Secure Configuration Manager as policy templates. For example, you can download the XCCDF content from the National Institute of Standards and Technology (NIST) website.

NIST was one of the driving forces behind the National Information Assurance Program (NIAP) Common Criteria program. At the heart of the Common Criteria is the concept of a protection profile, which is constructed to protect against all known threats for a proposed system. While these NIST efforts have been rooted in the traditional approach of focusing on a list of known vulnerabilities, NIST has placed a renewed focus on a gold standard configuration for systems deployed within the federal government. The FDCC standard establishes a single gold standard configuration for Windows XP and Vista systems, based on computer configurations at the United States Air Force that resulted in substantial cost savings. The USGCB standard evolved from the FDCC configuration and applies to a wider variety of computing systems.

1.2 Understanding the SCAP Module Components

The following table describes the components in the SCAP module installation kit.

Component	Description
Setup Program	Enables Secure Configuration Manager to do the following: ◆ Recognize SCAP-enabled agents ◆ Provide SCAP policy templates in the console ◆ Load assessment reports from offline computers For more information about running the setup program, see Section 2.2.1, “Installing the SCAP Module on Secure Configuration Manager Computers,” on page 15.
NetIQ Secure Configuration Manager Windows Agent (Windows agent)	Provides a setup program that enables the Windows agent to run SCAP policy template queries. For more information, see Section 2.2.2, “Deploying the SCAP Module to a Remote Agent Computer,” on page 16.
XCCDF Conversion Utility	Enables you to convert content in XCCDF format to an SCAP policy template that Secure Configuration Manager can run in the console. For more information, see Section 3.1, “Assessing NetIQ-Monitored Computers,” on page 19.
FDCC Reporting Utility	Enables you to convert policy template reports exported in XCCDF format to a `.csv` file for compliance reporting. For more information about reporting, see Section 3.3, “Creating a Compliance Report,” on page 23.
Offline Assessment Content - Windows	Contains content that you can configure for performing an assessment on offline Windows systems. For more information, see Section 3.2, “Assessing Offline Computers,” on page 20.
Report Loader	Enables you to import results of offline assessments. The module installation program automatically installs the `ReportLoader.exe` file. For more information, see Section 3.2.3, “Importing Offline Assessment Results,” on page 22.

1.3 Understanding How the SCAP Module Works

After you install the module components, Secure Configuration Manager automatically recognizes which NetIQ Windows security agent is enabled for SCAP queries, and then sets a flag in the asset map for these agents and their corresponding endpoints.

The SCAP module also adds an **SCAP Templates** option to the **Security Knowledge** > **Policy Templates** node in the console. The SCAP Templates option contains all SCAP policy templates you convert and import. To import content from the NIST site, you must convert the files from XCCDF format to `.tpl` format using the XCCDF Conversion Utility. For more information about converting and importing content, see Section 3.1, “Assessing NetIQ-Monitored Computers,” on page 19.

You can run the SCAP policy templates from the Secure Configuration Manager console to gather data on endpoints monitored by NetIQ Windows security agent. However, some endpoint computers might be offline, either because they are mobile workstations or they reside behind a high-security firewall. You can copy the SCAP files in their original XCCDF format to a read/write medium to assess systems not currently monitored by a NetIQ security agent. For more information about assessing offline systems with the SCAP benchmarks, see Section 3.2, “Assessing Offline Computers,” on page 20. After running offline assessments, you can import the results into the Secure Configuration Manager database.

When you complete a set of assessments, the Secure Configuration Manager and the SCAP module provide two methods for generating compliance reports. You can create and run a scheduled job in the console that automatically compiles and exports results in a format supported by the CyberScope data feeds. Alternatively, you can use the FDCC Reporting Utility to convert report results to `.csv` format for submitting reports in Microsoft Excel. For more information about reporting assessment results, see Section 3.3, “Creating a Compliance Report,” on page 23.

The SCAP module enables you to assess the subset of endpoint types available in Secure Configuration Manager. For information about supported endpoint types and versions, see the Secure Configuration Manager Technical Information page.

1.4 Understanding SCAP Module Licensing

To run SCAP assessments, you must have an endpoint license and an SCAP module license for each computer where you want to run SCAP assessments. For example:

A Windows computer with one Windows proxy agent managing six remote Windows computers requires six Windows endpoint licenses and six SCAP module licenses, for a total of 12 licenses. For more information about licensing Windows agents, see the *NetIQ Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

2 Installing the SCAP Module Components

This section addresses planning considerations and instructions for installing the SCAP module. This document provides a description of supported platforms at the time of release. For the most recent information about supported configurations, see the latest Secure Configuration Manager Documentation and the Secure Configuration Manager Technical Information page.

2.1 Planning to Install the SCAP Module Components

This section provides requirements for installing the SCAP module on Secure Configuration Manager Core Services, console, and agent computers, and for running offline assessments.

2.1.1 Default Ports

Open the ports listed in the following table for proper communication between the Core Services computer and the NetIQ Security Agent for Windows running SCAP policy templates.

Port Number	Component Computer	Port Use
8044	Web server	Used by the Web server that is embedded in Core Services to listen to SCAP-enabled agents. The Web server uses port 8044 by default, but this port is configurable.
8443	Core Services computer	Used by Core Services to listen to SCAP-enabled agents.

2.1.2 Secure Configuration Manager Computer Requirements

The following table lists requirements for installing the SCAP module on the Secure Configuration Manager Core Services computer.

Category	Requirements
Disk Space	Minimum of 60 MB of free space
Operating Systems	See the operating systems certified for Secure Configuration Manager Core Services in the Secure Configuration Manager Technical Information page.
Additional Software	NetIQ Secure Configuration Manager

2.1.3 Windows Agent Computer Requirements

The following table lists requirements for installing the SCAP module on a Windows agent computer.

Category	Requirements
Disk Space	Minimum of 100 MB of free space
Operating Systems	See the operating systems certified for Secure Configuration Manager Windows Agent in the Secure Configuration Manager Technical Information page.
Additional Software	NetIQ Secure Configuration Manager Windows Agent

2.1.4 Offline Assessment Requirements

The following table lists requirements for portable a read/write medium, such as a USB flash drive, for offline computer assessment. You must include the following Windows software when preparing the read/write medium for offline assessments.

Category	Requirements
Storage Capacity	◆ 128 MB of free space for required files. ◆ 1.5 MB of free space for each assessment result. For example, a 256 MB USB flash drive can hold assessment results for over 130 endpoints.
Software	The following software is located in the `Offline Assessment` folder of the NetIQ Secure Configuration Manager Module for SCAP installation kit: ◆ `JavaAccessBridge.DLL` ◆ `JAWTAccessBridge.DLL` ◆ `WindowsAccessBridge.DLL` ◆ `oem.conf` ◆ `scat-config.xml` ◆ `Slylog.conf` ◆ `autorun.inf` ◆ `s-cat.exe` ◆ `TADLib.dll` ◆ `TADLib_x64.dll` ◆ `TGMGT.dll` ◆ `TGMGT_x64.dll` ◆ `TGVista.dll` (Windows Vista only) ◆ `TGVista_x64.dll` (Windows Vista only) ◆ `TGWmi.dll` ◆ `TGWmi_x64.dll` ◆ vm - localized Java environment

2.2 Installing the SCAP Module Components

The following table provides an overview of tasks to install the SCAP module components and configure support for the module.

	Steps	For More Information
☐	Install the SCAP module on the Secure Configuration Manager Core Services computer, as specified in the release notes.	Section 2.1, “Planning to Install the SCAP Module Components,” on page 13.
☐	Install the Windows agent components on the endpoints that you want to assess.	◆ ***If you want to remotely deploy the SCAP module,*** see Section 2.2.2, “Deploying the SCAP Module to a Remote Agent Computer,” on page 16. ◆ ***If you want to locally install the SCAP module***, see Section 2.2.3, “Locally Installing the SCAP Module on an Agent Computer,” on page 16.
☐	Install the XCCDF Conversion Utility on each console computer.	Section 2.2.4, “Installing the XCCDF Conversion Utility,” on page 17.
☐	Install the FDCC Reporting Utility on each console computer.	Section 2.2.5, “Installing the FDCC Reporting Utility,” on page 17.

2.2.1 Installing the SCAP Module on Secure Configuration Manager Computers

Install the SCAP module on the Secure Configuration Manager Core Services computer.

NOTE

- When you install the module on the Core Services computer, the installation program automatically connects to and updates the Secure Configuration Manager database.
- If you have installed the Secure Configuration Manager database and Core Services on different computers, your logon account must be a local administrator account on the Core Services computer and a member of either the local Administrator group or the SQL Server user role on the database computer.

To install this module on Secure Configuration Manager computers:

1. Log on to the Core Services computer with a local administrator account.
2. Run the **NetIQSCAPModuleForSecureConfigurationManager** setup program locally from the root folder of the NetIQ Secure Configuration Manager Module for SCAP installation kit.
3. Follow the instructions in the wizard until you have finished installing the module.
4. Restart **NetIQ Core Services** to import SCAP templates successfully to Secure Configuration Manager console.

2.2.2 Deploying the SCAP Module to a Remote Agent Computer

Remotely deploy the SCAP module component to an agent computer by completing the following steps. If you want to install the SCAP module manually, see Section 2.2.3, “Locally Installing the SCAP Module on an Agent Computer,” on page 16. You can install the agent component of the SCAP module only on computers that have a Windows agent installed.

Deploying to a Remote Windows Agent Computer

You can use the Secure Configuration Manager console to deploy the SCAP module to a registered Windows agent. Before you deploy the Windows agent component for the SCAP module, you must update the Windows agent component on the Core Services computer and copy the `.nap` file to a special folder. For more information about deployment, see the *NetIQ Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

To deploy the SCAP module to a Windows agent:

1. Log on to the Core Services computer with a local administrator account.
2. In the SCAP module installation kit, open the folder containing the Windows agent component.
3. Copy the SCAP module `.nap` file to the `SyncStore` folder on the Core Services computer, by default `%Program Files (x86)%\NetIQ\Secure Configuration Manager\Core Services\SyncStore`. For example, copy the `SCAP_2.3_for_Windows_Agents.nap` file.
4. Log on to the console with an account that has rights to deploy Windows agents.
5. Expand **IT Assets > Agents > OS > Windows**.
6. Right-click the agents that you want to update, and then click **Deploy or Update**.
7. Complete the steps in the Deployment wizard. When specifying the deployment package, select the SCAP module package. For example, select **NetIQ SCAP Module 2.3 for Windows Agent**.

NOTE: If the Packages window of the Deployment wizard does not list the SCAP module package, you can browse to the `SyncStore` folder to add the `.nap` file.

2.2.3 Locally Installing the SCAP Module on an Agent Computer

Directly install the SCAP module on the local agent computer by completing the following steps. If you want to install the SCAP module remotely from Secure Configuration Manager, see Section 2.2.2, “Deploying the SCAP Module to a Remote Agent Computer,” on page 16. You can install the SCAP module only on computers that have either the NetIQ Security Agent for Windows installed.

Locally Installing on a Windows Agent Computer

You can install the SCAP module on a local Security Agent for Windows computer.

To locally install the SCAP module on a Windows agent computer:

1. Log on to the local agent computer with a local administrator account.
2. Run the `NetIQSCAPModuleForWindowsAgents.msi` program from the Windows agent folder of the NetIQ Secure Configuration Manager Module for SCAP installation kit.
3. Follow the instructions in the wizard until you have finished installing the module.

2.2.4 Installing the XCCDF Conversion Utility

To import properly formatted XCCDF content into Secure Configuration Manager, you must use the XCCDF Conversion Utility to convert the XCCDF content into SCAP policy templates that use the `.tpl` format. For more information about SCAP policy templates, see Section 3.1, “Assessing NetIQ-Monitored Computers,” on page 19.

To install the XCCDF Conversion Utility:

1. Log on to the Secure Configuration Manager console computer with a local administrator account.
2. Run the `Setup_XCCDF_Conversion_Utility_1.1.4.exe` file from the `Utilities` folder of the NetIQ Secure Configuration Manager Module for SCAP installation kit.
3. Follow the instructions in the wizard until you have finished installing the XCCDF Conversion Utility.

2.2.5 Installing the FDCC Reporting Utility

To create an FDCC compliance report, you must use the FDCC Reporting Utility to convert the exported policy template report from XCCDF format to a `.csv` file. For more information about FDCC compliance reports, see Section 3.3, “Creating a Compliance Report,” on page 23.

To install the FDCC Reporting Utility:

1. Log on to the Secure Configuration Manager console computer with a local administrator account.
2. Run the `Setup_FDCC_Reporting_Utility.exe` file from the `Utilities` folder of the NetIQ Secure Configuration Manager Module for SCAP installation kit.
3. Follow the instructions in the wizard until you have finished installing the FDCC Reporting Utility.

3 Using the SCAP Module

The SCAP module enables you to assess desktop computers and identify the systems that are out of compliance with the USGCB and FDCC standards. You can also create reports to demonstrate compliance with these standards. This section provides information about converting and importing SCAP content from the NIST Web site, running policy templates on monitored and offline computers, and generating reports specifically for compliance reporting.

3.1 Assessing NetIQ-Monitored Computers

You can convert and import the SCAP benchmarks you download from the NIST web site. You can run these policy templates in the Secure Configuration Manager console to assess endpoints monitored by NetIQ security agent for Windows.

3.1.1 Converting and Importing an SCAP Benchmark

You can import any properly formatted SCAP content for the supported endpoint types, and then use the content within Secure Configuration Manager. You can download SCAP content from the NIST Web site. For a current list of sources with SCAP content, see NetIQ Knowledge Base article NETIQKB71203 at www.netiq.com/support.

Some data files for SCAP benchmarks contain multiple profiles that specify which security checks are included in the policy template and their associated parameter values. When importing a converted SCAP policy template into Secure Configuration Manager, you can specify which profile you want to import. Secure Configuration Manager places the imported policy templates under the **Security Knowledge > Policy Templates > SCAP Templates** heading. For more information about working with policy templates, see the *NetIQ Secure Configuration Manager User Guide*.

NOTE: When using the XCCDF Conversion Utility to import properly formatted XCCDF content into Secure Configuration Manager, if you select the **Perform schema validation on selection** check box, the console computer must have Internet access.

To convert and import an SCAP benchmark:

1. Run the `XCCDF Conversion Utility.exe` file where you installed the component. By default, this file is located in the `C:\Program Files (x86)\NetIQ\Secure Configuration Manager\Core Services\XCCDF Converter` folder.
2. In the **Source** field, browse to the SCAP benchmark that you want to import and click **Import**.
3. In the **Destination** field, browse to the folder where you want to save the specified SCAP template in `.tpl` format and click **Accept**.
4. Double-click the profiles that you want to associate with the SCAP template.
5. Click **Process Content**.
6. Log on to a Secure Configuration Manager console computer with a console user account that has the Import Policy Template permission.
7. Expand **Security Knowledge > Policy Templates**.

8 Right-click **Policy Templates**, then click **Import Policy Template**.

9 Select the policy template that you want to import, then click **Open**.

3.1.2 Running SCAP Policy Templates

Once you determine which policy templates you need to run to generate compliance reports, you can schedule one-time or recurring jobs for each template. Secure Configuration Manager generates a report for each job you run, which you can review in the **Job Queues > Completed Jobs** pane.

The SCAP module adds an option to the Run Policy Template wizard and the offline assessment feature that enables you to exclude Open Vulnerability and Assessment Language (OVAL) notes for successful checks from the report results. OVAL is a set of standards created by the information security community for assessing and reporting consistent and actionable information about the machine state of a computer system. When you run an SCAP policy template, the OVAL notes in the report provide the logic underlying the pass/fail result for each technical control assessed by the template. For example, if you run the policy template for the first time, you might consider including the OVAL notes to help determine why endpoints fail certain checks. Alternatively, if you have remediated all issues and want to submit a streamlined compliance report, you can select **Suppress OVAL Notes** in the Policy Template Wizard when you run the template. To suppress the OVAL notes in offline assessment results, see Step 4 on page 21.

For more information about working with policy templates, see the *NetIQ Secure Configuration Manager User Guide*.

3.2 Assessing Offline Computers

Auditors and security personnel rely heavily on automated tools to gather and centralize compliance information for aggregation and analysis. Since automated tools have no means of connecting to offline computers, you cannot determine whether the offline computers comply with security standards, best practices, and regulatory requirements.

If you have physical access to offline computers, the SCAP module allows you to run SCAP policy templates on those computers using portable read/write media, such as a USB flash drive. You can import these assessment results into Secure Configuration Manager to view, print, or export the results. You can get the latest version of XCCDF content from the National Institute of Standards and Technology (NIST) (http://scap.nist.gov).

NOTE

- If you run an offline assessment on a computer that is not running the operating system specified in the benchmark, Secure Configuration Manager does not create an `.xml` file.
- To ensure Secure Configuration Manager can connect to desktop computers, set the **Is DHCP Client** field of the Endpoint Properties window to **True** for all desktop computers.

3.2.1 Configuring the Read/Write Medium

To assess offline computers, you must insert a read/write medium, such as a USB flash drive, containing appropriately formatted policy templates in the computer. These files must correspond with policy templates imported to the SCAP Templates node in the Secure Configuration Manager console. The files must be in `.xml` format.

To configure a read/write medium for offline assessments:

1. Copy the contents of the `Offline Assessment` folder from the NetIQ Secure Configuration Manager Module for SCAP installation kit to the root directory of the read/write media.
2. Ensure the `oem-content` folder includes the XCCDF content files for which you want to run assessments.
3. Specify the profile that you want to run by opening the `scat-config.xml` file and updating the following line:

   ```
   <profile>profile_name</profile>
   ```

   where *profile_name* is the name of the profile you want to use while running the assessments.
4. ***If you want to include OVAL notes in the report***, open the `scat-config.xml` file and edit the OVAL notes tag as follows:

   ```
   <suppress_oval_notes>false</suppress_oval_notes>
         <force_32bit_mode>false</force_32bit_mode>
         <xml_oval_notes>true</xml_oval_notes>
   ```

   For more information about OVAL notes, see Section 3.1.2, “Running SCAP Policy Templates,” on page 20.
5. ***If you want to run a specific benchmark***, specify the benchmark that you want to run by opening the `scat-config.xml` file and updating the `<xccdf_file>` tag with the benchmark name. For example, if you want to run the `fdcc-winxp-xccdf.xml` benchmark, update the tag as follows:

   ```
   <xccdf_file>fdcc-winxp-xccdf.xml</xccdf_file>
   ```

   You can find the benchmarks (those you have copied in Step 2) listed in the `oem-content` folder.
6. ***If you want to automatically determine all applicable benchmarks in the*** `oem-content` ***folder and perform an assessment of each one***, open `scat-config.xml` and remove the following line:

   ```
   <xccdf_file>benchmarkfilename.xml</xccdf_file>
   ```

   where `benchmarkfilename.xml` is the name of a specific benchmark.
7. ***If you want to create a log file***, open `Slylog.conf` and delete the pound sign (`#`) from `#LogFile=scat.log`.

8 ***If you want to change the logging level***, open `Slylog.conf` and change the LogLevel parameter to one of the following values:

Logging Level	Description
`FATAL`	Show errors that cause S-CAT to abort an assessment.
`ERROR`	Show run time errors, including content errors.
`WARNING`	Show warning messages.
`INFO`	Show informational messages.
`DEBUG`	Show detailed debug output.

These settings are cumulative. For example, a logging level setting of `DEBUG` displays fatal, error, warning, info, and debug messages.

3.2.2 Running Assessments on Offline Computers

Once you prepare the read/write medium, you can run assessments on offline computers. The content files on the read/write medium should correspond with the aspects of offline computer that you want to assess, such as the Windows operating system or an Oracle database.

To run an SCAP assessment on an offline computer:

1 Insert the read/write medium into the computer on which you want to run an assessment.

2 ***If the computer is configured to not take automatic action when read/write media is inserted***, complete the following steps:

2a Access the read/write medium.

2b Open `s-cat.exe`.

3 Once the assessment is complete, repeat Step 1 through Step 2 on page 22 for each offline computer you want to assess.

3.2.3 Importing Offline Assessment Results

You can import only completed offline assessments for SCAP content that corresponds with SCAP policy templates you imported into Secure Configuration Manager. For more information about importing SCAP policy templates, see Section 3.1, “Assessing NetIQ-Monitored Computers,” on page 19.

To import results of an offline assessment:

1 Log on to a Secure Configuration Manager Core Services computer with a Secure Configuration Manager administrator account.

2 Insert the read/write medium used to gather offline assessments.

3 Run `ReportLoader.exe`. By default, this file is located in the `C:\Program Files (x86)\NetIQ\Secure Configuration Manager\Core Services\bin` folder.

4 Specify the user name and password of your Secure Configuration Manager administrator account and click **Logon**.

5 In the **Import Folder** field, browse to the location of the completed SCAP assessments that you want to import. Completed SCAP assessments have an `.xml` file type. By default, you can find the completed SCAP assessments in the `Products` folder.

NOTE: You can import only completed offline assessments that correspond with SCAP policy templates previously imported into Secure Configuration Manager.

6 Click **Run**.

7 Click **Close**.

NOTE: The Report Loader continues to import the completed SCAP assessments even if you click **Close**.

8 Log on to a Secure Configuration Manager console computer with your console user account.

9 Expand **Job Queues > Completed**.

10 In the content pane, double-click the policy template report that you want to view.

11 When you are finished viewing or printing the report, close the Report Viewer.

3.3 Creating a Compliance Report

The U.S. Office of Management and Budget requires the agency or department CIO to report compliance for the associated organization. The SCAP module provides two methods for generating reports that meet the NIST guidelines: the CyberScope Data Feed scheduled job and the FDCC Reporting Utility.

3.3.1 Creating a CyberScope Data Feed Report

NIST collaborated with CyberScope to create a web-based program that automatically processes the data feeds from agencies reporting under the Federal Information Security Management Act (FISMA) standards. The SCAP policy templates that you import to Secure Configuration Manager are associated with specific SCAP benchmarks. The CyberScope program can process reports sent in a designated format that uses the following content in the SCAP benchmarks:

Content Format	Description
Common Configuration Enumeration (CCE)	Represents a unique identifier for common system configuration issues, such as a specific security setting.
Common Vulnerabilities and Exposures (CVE)	Represents unique identifiers that map to standard names for publicly known information security vulnerabilities and exposures.
Common Platform Enumeration (CPE)	Represents a structured naming scheme for information technology systems, platforms, and packages, based upon the Uniform Resource Identifiers (URI) syntax.

The CyberScope Data Feed report in the Scheduled Jobs queue includes aggregated data on all specified SCAP-enabled endpoints, such as the number of non-compliant computers for each CVE point listed in the SCAP template. When you run the CyberScope 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. Then, Secure Configuration Manager compiles this information into an `.xml` file for the aggregated report and exports the file to a specified folder or email address.

You must specify the managed groups and SCAP benchmarks to include in the report, as well as the component, agency, and enclave names for the reporting department. Complete the following steps to configure the content that you want to include in the report.

To configure the content in the CyberScope Data Feed report:

1. Log on to the Core Services computer with a Secure Configuration Manager administrator account.
2. Open the Core Services Configuration Utility.
3. On the SCAP tab, specify the managed groups and SCAP benchmarks that you want to include in the report.
4. Specify the names that CyberScope associates with your organization, agency, and enclave.
5. Click **OK**.
6. (Optional) As a best practice, schedule the CyberScope Data Feed job to regularly export the aggregated data report.

3.3.2 Creating an FDCC Compliance Report

The Office of Management and Budget mandates that federal agencies with desktop and laptop computers running the Windows XP operating system adopt the FDCC standard. If you cannot implement some settings in the FDCC standard, you can report deviations from the FDCC settings in your compliance report to NIST.

To create an FDCC compliance report:

1. In the Secure Configuration Manager console, assign an FDCC role to each endpoint that you want to include in the report using the Endpoint Properties window **Use** field. Select one of the following FDCC roles:
   - Centrally Managed General Purpose Desktop
   - Centrally Managed General Purpose Laptop
   - Development System
   - Special Use System
   - Other
2. Run the SCAP policy template against the endpoints that you want to assess. For more information about running policy templates, see the *NetIQ Secure Configuration Manager User Guide*.
3. ***If you want to run an SCAP policy template on an offline computer***, see Section 3.2, “Assessing Offline Computers,” on page 20.
4. View the completed policy template report. For more information about viewing a policy template report, see the *NetIQ Secure Configuration Manager User Guide*.
5. ***If you want to create an exception for a security check or endpoint***, see the *NetIQ Secure Configuration Manager User Guide*.

6 Export the policy template report to XCCDF format by performing the following steps:

NOTE

- To export a policy template report in XCCDF format, you must specify the major and minor version of the operating system in the Endpoint Properties window for each endpoint in the report.
- When you export an SCAP policy template report to XCCDF format, the Secure Configuration Manager validates the XML against the XCCDF schema. If you export a non-SCAP policy template report, Secure Configuration Manager does not validate the XML against the XCCDF schema.

6a On the Action menu, click **Export Full Report**.

6b Type the file name.

6c Select the `XCCDF` file format.

6d Click **Save**.

7 Run the `FDCCReporter.exe` file. By default, this file is located in the `C:\Program Files (x86)\NetIQ\ Secure Configuration Manager\FDCC Reporting Utility` folder.

8 In the **Source Directory** field, browse to the directory location of the policy template for which you want to create a compliance report.

9 In the **Destination File** field, browse to the folder where you want to save the compliance report and specify a file name.

10 Click **Accept**.

11 In the **Agency Name** field, specify the agency to which you are submitting the compliance report.

12 In the **Chief Information Officer (CIO)** field, specify the name of the CIO reporting the compliance of the agency.

13 Click **Create**.

3.4 Best Practice Recommendations

NetIQ recommends scheduling the SCAP policy templates and report output to run on a regular basis. However, the CyberScope Data Feed scheduled job requires that the Secure Configuration Manager database contain the latest policy template results for your SCAP endpoints. To avoid running SCAP policy templates at the same time that the CyberScope Data Feed job queries data results, ensure that the endpoint results already exist in the database. Use the following checklist as a guide to properly configure Secure Configuration Manager to report the latest endpoint results.

	Checklist Items
☐	***To determine the average interval of time required between running policy templates and running the data feed report***, run the SCAP policy templates for your online endpoints. Note the elapsed time between the start and completion of the runs. You can choose to run multiple templates concurrently.
☐	Schedule the runs for the SCAP policy templates.
☐	Determine the dates and times that you want to assess offline computers and to import the results to the Secure Configuration Manager database.

	Checklist Items
❑	Schedule the CyberScope Data Feed job to run after the completion of the SCAP policy template runs and after the planned import of offline assessment data.