NetIQ Secure Configuration Manager SCAP Module

User's Guide

July 2018

NetIQ.

Legal Notice

Contents

About This Book

The *User's Guide* provides conceptual information about the Secure Configuration Manager SCAP Module. This book includes instructions for upgrading or installing as well as guidance for common tasks.

Intended Audience

This book provides information for individuals responsible for implementing the standards established by federal computer configuration initiatives: United States Government Configuration Baseline (USGCB) and Federal Desktop Core Configuration (FDCC).

Additional Documentation

The Secure Configuration Manager documentation library includes the following resources:

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

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

Contact Information

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

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

1 About this Release

NetIQ Secure Configuration Manager Module for SCAP 7.1 (the SCAP module) includes enhancements to stay aligned with Secure Configuration Manager.

For more information about Secure Configuration Manager, see the Secure Configuration Manager website.

What's New?

The SCAP module 7.1 includes the following enhancements:

Support for Secure Configuration Manager Components

Adds support for the following components of Secure Configuration Manager:

- Secure Configuration Manager 7.1
- Security Agent for UNIX 7.6
- Security Agent for UNIX 7.5 Service Pack 1
- Secure Configuration Manager Windows Agent 7.1

Infrastructure Update

This release includes a modification to the infrastructure of the SCAP Module so that it is not tied to a specific version of Secure Configuration Manager.

Version Requirements

The SCAP module 7.1 requires the following product versions, at a minimum:

- Secure Configuration Manager 7.1
- Security Agent for UNIX 7.6
- Security Agent for UNIX 7.5 Service Pack 1
- Secure Configuration Manager Windows Agent 7.1

For the most recently updated list of supported application versions, see the NetIQ Secure Configuration Manager Technical Information page. For detailed information on hardware requirements and supported operating systems, and browsers, see "Planning to Install the SCAP Module" on page 15 .

Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

CTRL-M Characters Prevent Running of the S-cat.sh file for an Offline Assessment

Issue: When you attempt to run the `s-cat.sh` file for an offline assessment on a UNIX server, the script might fail to run and the terminal displays the following error:

```
bash: ./s-cat.sh: /bin/sh^M: bad interpreter: No such file or directory
```

The script fails because the file contains `CTRL-M` (`^M`) characters. This issue might occur after you extract the offline assessment file from the SCAP package. (Bug 1073504, 1073947)

Workaround: To remove the `^M` characters from the file, run the following command:

```
Dos2unix s-cat.sh s-cat.sh
```

Cannot Import SCAP Templates after Installing the SCAP Module

Issue: After the installation, importing SCAP templates to Secure Configuration Manager console fails. `(Bug 937972)`

Workaround: Restart **NetIQ Core Services**.

Risk Score Might be Applied Inappropriately to Windows Server 2003 Endpoints

Secure Configuration Manager might inappropriately apply a risk score to Windows Server 2003 endpoints for security checks that do not apply to the endpoints or when the policy template report lists the endpoint as "unknown". This issue occurs when you run an SCAP policy template containing checks that apply to multiple endpoint types against multiple endpoints, including a Windows Server 2003 endpoint. `(Bug 953300)`

Workaround: There is no workaround at this time.

XCCDF Conversion Utility Displays Errors during Successful Conversion

Issue: The XCCDF Conversion utility incorrectly reports errors while converting XCCDF benchmark files to templates. The following messages are examples of the incorrect errors:

```
cpe USGCB-ie8-cpe-dictionary.xml Invalid Error on line 105 of document http://
cpe.mitre.org/files/cpe-dictionary_2.1.xsd: src-resolve: Cannot resolve the name
'xml:lang' to a(n) 'attribute declaration' component
```

```
cpe USGCB-Windows-7-firewall-cpe-dictionary.xml Invalid Error on line 105 of
document http://cpe.mitre.org/files/cpe-dictionary_2.1.xsd: src-resolve: Cannot
resolve the name 'xml:lang' to a(n) 'attribute declaration' component
```

```
cpe irm-10.8.10-cpe-dictionary.xml Invalid Error on line 105 of document http://
cpe.mitre.org/files/cpe-dictionary_2.1.xsd: src-resolve: Cannot resolve the name
'xml:lang' to a(n) 'attribute declaration' component
```

`(Bug 953314)`

Workaround: Ignore these errors. Even though the messages report errors, the utility successfully creates the policy templates. You can import the templates and run them against endpoints displaying valid data.

Exported XCCDF File Might Report an Inaccurate Number of Windows XP and Vista Endpoints

Issue: If a managed group contains a combination of Windows XP and Windows Vista endpoints, exported SCAP results inaccurately report the number of endpoints per operating system type. This issue occurs because, when generating the XCCDF file, Secure Configuration Manager applies the type of the first reported endpoint to all endpoints in the group, such as Windows Vista. For example, the South Texas managed group contains three Windows XP endpoints and two Vista ones. You run an assessment against the South Texas group, export the results as XCCDF, and then run the FDCC Reporting Utility to generate a compliance report. The final report lists five Windows Vista endpoints and zero Windows XP systems. `(Bug 953345)`

Workaround: Create managed groups for each operating system type. You can nest managed groups within higher-level groups. For example, **My Groups** > **South Texas** > **XP Laptops** and **My Groups** > **South Texas** > **Vista Laptops**. Then run separate jobs against the lower-level groups, such as one job for the XP Laptops.

Password Field for the Report Loader Might Not Display Asterisks for All Characters Entered

Issue: When you specify credentials for the Report Loader, Secure Configuration Manager displays asterisks for no more than 20 characters entered in the Password field. However, regardless of the asterisks displayed in the field, Secure Configuration Manager supports passwords up to 40 characters. `(Bug 953348)`

Workaround: There is no workaround at this time.

Cannot Create FDCC Compliance Reports

Issue: Creating FDCC compliance reports fails because you cannot export policy template reports to XCCDF format. `(Bug 891524)`

Workaround: There is no workaround at this time.

2 Introduction

The NetIQ Secure Configuration Manager SCAP Module (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.

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, UNIX, 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.

Understanding the SCAP Module Components

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

Component	Description
NetIQ SCAP Module for Secure Configuration Manager (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 "Installing or Upgrading on Secure Configuration Manager Computers" on page 19.
NetIQ SCAP Module for Windows Agent (Windows Agent)	Provides a setup program that enables the Windows agent to run SCAP policy template queries. For more information, see "Deploying or Updating the SCAP Module to a Remote Agent Computer" on page 20.
NetIQ SCAP Module for UNIX Agent (UNIX agent)	Provides `.zip` files containing patches that enable the UNIX agent to run SCAP policy template queries. For more information, see "Installing or Upgrading on Secure Configuration Manager Computers" on page 19.
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 "Assessing NetIQ-Monitored Computers" on page 25.
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 "Creating a Compliance Report" on page 30.
Offline Assessment Content - UNIX	Contains content that you can configure for performing an assessment on offline UNIX systems. For more information, see "Assessing Offline Computers" on page 27.
Offline Assessment Content - Windows	Contains content that you can configure for performing an assessment on offline Windows systems. For more information, see "Assessing Offline Computers" on page 27.
Report Loader	Enables you to import results of offline assessments. The module installation program automatically installs the `ReportLoader.exe` file. For more information, see "Importing Offline Assessment Results" on page 29.

Understanding How the SCAP Module Works

After you install the module components, Secure Configuration Manager automatically recognizes which NetIQ UNIX and Windows security agents are 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 "Assessing NetIQ-Monitored Computers" on page 25.

You can run the SCAP policy templates from the Secure Configuration Manager console to gather data on endpoints monitored by NetIQ UNIX and Windows security agents. 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 "Assessing Offline Computers" on page 27. After running offline assessments, you can import the results into the Secure Configuration Manager database.

When you complete a set of assessments, 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 "Creating a Compliance Report" on page 30.

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.

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 UNIX computer requires one endpoint license for the UNIX agent and one SCAP Module license, for a total of two licenses. For more information about licensing UNIX agents, see the *Security Agent for UNIX Installation and Configuration Guide*.
- 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 *Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

3 Planning to Install the SCAP Module

This section addresses planning considerations for installing or upgrading 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.

Considerations for Upgrading or Installing

Before upgrading on installing the SCAP Module, review the following considerations:

- You can upgrade to SCAP module 7.1 from version 7.0.
- If you have Windows agents at version 6.1 or later without an SCAP module installed, update the agents to version 7.1 then install the SCAP module.
- If you have Windows agents at version 7.1, you can deploy the SCAP module for Windows Agent from the Secure Configuration Manager console using the deployment wizard.

  Either install the SCAP module for Windows Agent component locally on the agent computer or use the console to deploy a `.nap` package to remote agent computers. For more information about installing and deploying the SCAP module for Windows agent component, see the “Checklist for Upgrading and Installing” on page 19.
- (Conditional) You can upgrade the SCAP Module for Secure Configuration Manager and the SCAP module for Windows Agent from version 6.1 or later to version 7.1 on a local computer only by using the command line. For more information, see the “Checklist for Upgrading and Installing” on page 19.

Default Ports

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

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.

Port Number	Component Computer	Port Use
8443	Core Services computer	Used by Core Services to listen to SCAP-enabled agents.

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

UNIX Agent Computer Requirements

The following table lists requirements for installing the SCAP module on a UNIX agent computer. You cannot install the SCAP module if you are using the Lightweight UNIX solution.

Category	Requirements
Disk Space	Minimum free space for the following operating systems: ◆ 200 MB for CentOS ◆ 144 MB for AIX ◆ 262 MB for HP-UX on PA-RISC ◆ 567 MB for HP-UX on Itanium ◆ 229 MB for Red Hat Enterprise Linux ◆ 229 MB for Solaris
Operating Systems	See the operating systems certified for Secure Configuration Manager in the Technical Information for Security Agent for UNIX page.
Additional Software	NetIQ UNIX Agent

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 Technical Information for Windows Agent for SCM page.
Additional Software	NetIQ Secure Configuration Manager Windows Agent

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 UNIX or 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	◆ **For Windows**: Include the software located in the `Offline Assessment > Windows` folder. ◆ **For UNIX or Linux**: Include the software located in the `Offline Assessment > UNIX` folder.

4 Installing or Upgrading the SCAP Module

This section provides instructions for installing or upgrading the SCAP module.

Checklist for Upgrading and Installing

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

	Steps	For More Information
□	Install or upgrade the SCAP module on the Secure Configuration Manager Core Services computer, as specified in the release notes.	Section 3, "Planning to Install the SCAP Module," on page 15.
□	Install or update the UNIX and Windows agent components on the endpoints that you want to assess.	- ***If you want to remotely deploy the SCAP module,*** see "Deploying or Updating the SCAP Module to a Remote Agent Computer" on page 20. - ***If you want to locally install the SCAP module***, see "Locally Installing or Upgrading the SCAP Module on an Agent Computer" on page 21.
□	Install the XCCDF Conversion Utility on each console computer.	"Installing the XCCDF Conversion Utility" on page 22.
□	Install the FDCC Reporting Utility on each console computer.	"Installing the FDCC Reporting Utility" on page 23.

Installing or Upgrading on Secure Configuration Manager Computers

Install or upgrade 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 or upgrade 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.

   Follow the instructions in the wizard until you have finished installing the module.
3. Restart **NetIQ Core Services** to import SCAP templates successfully to Secure Configuration Manager console.

Deploying or Updating 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 "Locally Installing or Upgrading the SCAP Module on an Agent Computer" on page 21. You can install the agent component of the SCAP module only on computers that have a UNIX agent or a Windows agent installed.

- "Deploying to a Remote UNIX Agent Computer" on page 20
- "Deploying to a Remote Windows Agent Computer" on page 21

Deploying to a Remote UNIX Agent Computer

The UNIX Agent Manager console enables you to deploy the SCAP module to UNIX agent computers.

To remotely deploy the SCAP module to a UNIX agent computer:

1. In the UNIX Agent Manager console, click **Agent Manager**.
2. Click **Hosts** > **Scan All Hosts** to verify all agents are active and registered.
3. Click **Hosts** > **Patch Mgr**.
4. In Patch Manager, install `p751p100.zip` to your agent computer.
5. Verify successful installation in the results window.
6. Re-register the agent in Secure Configuration Manager. For more information, see the *User's Guide for Secure Configuration Manager*.

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 *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_7.1_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 7.1 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.

Locally Installing or Upgrading the SCAP Module on an Agent Computer

Directly install or upgrade 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 "Deploying or Updating the SCAP Module to a Remote Agent Computer" on page 20. You can install or upgrade the SCAP module only on computers that have either the NetIQ Security Agent for Windows or the NetIQ UNIX Agent installed.

- "Locally Installing on a UNIX Agent Computer" on page 21
- "Locally Installing or Upgrading on a Windows Agent Computer" on page 22

Locally Installing on a UNIX Agent Computer

The UNIX Agent Manager console enables you to deploy the SCAP module to UNIX agent computers.

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

1. Copy the `.tar` files for your operating system and the `wcPatch` file to the `PSHOME/netiq/bin` directory on the computer where you want to install the module. You can find the value for PSHOME in the `/etc/vsaunix.cfg` file on the local computer.
2. Run the `su` command to switch to the root user account.
3. Change to the `PSHOME/netiq/bin` directory.

4 Run the command `./wcPatch APPLY <file name> <version> <temporary directory>` where:

- `<file name>` is the file name of the patch for the specific operating system, provided in the UNIX agent folder of the NetIQ Secure Configuration Manager Module for SCAP installation kit. For example, `p12p34.tar` provided in the `HP-UX_ia64` folder.
- `<version>` is the patch number of the patch provided in the UNIX agent folder of the installation kit. For example, `1.2.3.45`.
- `<temporary directory>` is the directory on a remote computer where you want to store temporary files during installation.

NOTE: If you want to use a directory on the computer where you are installing, you will need twice as much free disk space as normally required.

5 Perform Step 4 for patches provided in the UNIX agent folder of the installation kit.

6 Re-register the agent in Secure Configuration Manager. For more information, see the *User's Guide for Secure Configuration Manager*.

Locally Installing or Upgrading on a Windows Agent Computer

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

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

1 Log on to the local agent computer with a local administrator account.

2 Run the `NetIQSCAPModuleForWindowsAgent.msi` program from the Windows agent folder of the NetIQ Secure Configuration Manager Module for SCAP installation kit.

Follow the instructions in the wizard until you have finished installing the module.

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 "Assessing NetIQ-Monitored Computers" on page 25.

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_1.1.1.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.

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 "Creating a Compliance Report" on page 30.

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.

Verifying the Installation

Complete the following steps to verify that the installation was successful on the Core Services computer:

1. Log on to the Secure Configuration Manager console.
2. On the Help menu, click **About NetIQ Secure Configuration Manager**.
3. Under Patch Summary, click **Database**.
4. Verify that the Version tab lists **7.1** for the most recently installed SCAP Module.

5 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.

- "Assessing NetIQ-Monitored Computers" on page 25
- "Assessing Offline Computers" on page 27
- "Creating a Compliance Report" on page 30
- "Best Practice Recommendations" on page 32

Assessing NetIQ-Monitored Computers

You can convert and import the SCAP benchmarks you download from the NIST web site, including those with embedded NIST SCAP 1.2 certified binaries. You can run these policy templates in the Secure Configuration Manager console to assess endpoints monitored by NetIQ security agents for UNIX and Windows.

- "Using SCAP 1.2 Benchmarks for Assessment" on page 25
- "Converting and Importing an SCAP Benchmark" on page 26
- "Running SCAP Policy Templates" on page 27

Using SCAP 1.2 Benchmarks for Assessment

The SCAP 1.2 benchmarks that you download from the NIST site are in `.xml` format. You do not need to convert these to template format for Secure Configuration Manager to run. Instead, use the `s-cat` command to run assessments.

1. Copy the contents of the `Offline Assessment` folder from the Secure Configuration Manager Module for SCAP installation kit to the root directory of the computer where you want to run the assessments.
2. Download the SCAP 1.2 benchmarks to the computer.
3. (Conditional) On a Windows computer, launch `s-cat.exe`, by default in the `Offline Assessment\Windows` folder.
4. (Conditional) For UNIX and Linux computers, open `s-cat.sh`.
5. Enter one of the following commands:

   ```
   s-cat.exe evaluate -i <Source.xml> -o <Target.xml> -pid <ProfileID> -as +ra
   ```

   or

   ```
   s-cat.sh evaluate -i <Source.xml> -o <Target.xml> -pid <ProfileID> -as +ra
   ```

   Use the following parameters:

Source.xml

Specifies the path to the `.xml` file of the SCAP 1.2 benchmark that you want to run

Target.xml

Specifies the path where you want to save the `.xml` file that contains the assessment results

ProfileID

Specifies the profile ID that you use to run the assessments

For example:

```
s-cat.exe evaluate -i  U_Windows_Server_2016_V1R3_STIG_SCAP_1-2_Benchmark.xml
-o  C:\SCAP\2016.xml -pid xccdf_mil.disa.stig_profile_MAC-1_Public -as +ra
```

For more information, see the Help: `s-cat.exe evaluate –h`

Converting and Importing an SCAP Benchmark

Applies only to SCAP 1.0 and 1.1 content

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 the NetIQ Knowledgebase Article 7771203.

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 *User's Guide for Secure Configuration Manager*.

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**.

Running SCAP Policy Templates

Applies only to SCAP 1.0 and 1.1 content

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 28.

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

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.

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 "Running SCAP Policy Templates" on page 27.
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.

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 For Windows computers, open `s-cat.exe`.

   2c For UNIX and Linux computers, open `s-cat.sh`.

3 Once the assessment is complete, repeat Step 1 through Step 2 on page 29 for each offline computer you want to assess.

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 “Assessing NetIQ-Monitored Computers” on page 25.

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`, located by default 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.

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.

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.

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 *User's Guide for Secure Configuration Manager*.
3. (Conditional) To run an SCAP policy template on an offline computer, see "Assessing Offline Computers" on page 27.
4. View the completed policy template report. For more information about viewing a policy template report, see the *User's Guide for Secure Configuration Manager*.
5. (Conditional) To create an exception for a security check or endpoint, see the *User's Guide for Secure Configuration Manager*.
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**.

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
□	(Conditional) 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.
□	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.