SCAP Compliance Checker Version 3.1 for Windows

February 12, 2012

Developed by:
Space and Naval Warfare (SPAWAR) Systems Center Atlantic
P.O. Box 190022
North Charleston, SC 29419-9022
ssc_lant-scc@navy.mil

Table of Contents

1. INTRODUCTION

The Security Content Automation Protocol (SCAP) Compliance Checker (SCC) is a SCAP Validated FDCC Scanner and Open Vulnerability Assessment Language (OVAL) adopter, capable of performing compliance verification using SCAP content, and authenticated vulnerability scanning using OVAL content.

1.1 Background

1.1.1 About this Manual

This User Manual is intended to explain all of the features and functionality of the SCC application, along with some basic information regarding the SCAP standards. As SCC is used by thousands of people across hundreds of government agencies, a single Standard Operating Procedure (SOP) is not feasible. Each agency may need to create their own SOP based on their intended usage of SCC.

For DOD Usage, and integration with the STIG Viewer, please refer to DISA's (Defense Information Systems Agency) documentation, which is located at:
http://iase.disa.mil/stigs/scap/index.html
http://iase.disa.mil/stigs/stig_viewing_guidance.html

1.1.2 What is SCC?

SCC is a SCAP Validated FDCC Scanner and OVAL interpreter. Essentially SCC is an XML interpreter of SCAP content, meaning SCC does not perform any checks without SCAP/OVAL XML content. The end user can install SCAP content into SCC, and enable one or more SCAP content streams to perform compliance checking.

1.1.3 What is SCAP and SCAP Content?

At a very high level, SCAP is a set of XML standards, primarily XCCDF and OVAL, which include policy settings and technical instructions to perform automated checking.

SCAP Content is a collection of XML files, usually bundled in a zip file, which defines the checks to be evaluated on a target system or systems. This bundle, or 'stream', instructs what checks to perform, provides all text fields such as titles, references, descriptions, and to some extent, how to perform them. SCAP validated scanners such as SCC ingest the stream and perform the checks listed therein.

The SCC application has some SCAP content pre-bundled with it from DISA and NIST (National Institute of Standards and Technology). However, SPAWAR, does not own nor maintain the content, it is only included for end user convenience. This content may need to be manually replaced periodically by the user, when content authors publish updates.

1.2 Platforms Supported

- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- SQL Server 2000/2005/2008/2008R2

Note 1: There are separate installers per architecture (Windows, Linux (RPM, DEB), Solaris, Mac) and cross platform scanning is not supported.

Note 2: 'Supported' is defined as the application has been designed to run on the Operating System and architecture, and has been tested in our lab to execute as expected. Content may not be provided, but end users could obtain content from other sources, or write their own, and install and run in the application. See below for the list of content included in the installer.

1.3 SCAP Content Included

NIST USGCB content obtained from: http://usgcb.nist.gov/index.html
DISA STIG content obtained from: http://iase.disa.mil/stigs/scap/index.html

- NIST USGCB
  - Version: 2.0.0.0
    - Release Date: 2013.01.22
    - Windows XP Operating System
    - Windows XP Firewall
    - Windows Vista Operating System
    - Windows Vista Firewall
    - Internet Explorer 7
  - USGCB Version: 1.2.0.0
    - Release Date: 2013.01.22
    - Windows 7 Operating System
    - Windows 7 Energy
    - Windows 7 Firewall
    - Internet Explorer 8

- DISA STIG SCAP Benchmarks
  - Internet Explorer 8 Version 1, Release 8
  - Internet Explorer 9 Version 1, Release 3
  - Windows 2003 Member Server Version 6, Release 1.27
  - Windows 2003 Domain Controller Version 6, Release 1.27
  - Windows 2008 Member Server Version 6, Release 1.20
  - Windows 2008 Domain Controller Version 6, Release 1.20
  - Windows 2008 R2 Member Server Version 1, Release 6
  - Windows 2008 R2 Domain Controller Version 1, Release 6
  - Windows 7 Version 1, Release 14
  - Windows XP Version 6, Release 1.27
  - Windows Vista Version 6, Release 1.28

1.4 Changelog

Below is an abbreviated list of the primary changes from version 3.0 to 3.1. Please refer to the release notes for a complete list of updates.

- For All Platforms
    - Updated default location for Logs and Results to be dynamic based on each user's profile/home directory.
    - Added applicable DISA STIG SCAP Benchmarks to each installer.
    - Added new OVAL Processing Options, which allows the user to exclude certain OVAL features which known to cause system resource issues.
    - Added support for OVAL 'unique' function.
    - Added support for OVAL 'count' function.
    - Added ability to copy results via SSH to a centralized server.
    - Improved OCIL functionality to allow for resuming of partially completed questionnaires.
    - Improved documentation in the User Manual.
- For Windows
    - Added ability to install and run as a service.
    - Added support for case insensitivity to several OVAL tests
    - Added support for OVAL windows cmdlet test, object, state.
    - Updated registry tests to support OVAL 5.10 'windows_view'.
    - Updated file test to support OVAL 5.10 'windows_view'.

2. REQUIREMENTS

2.1 Scanning Requirements (Local and Remote)

2.1.1 Administrative Rights

The SCC requires the user to have administrative rights on the computer to be reviewed.

2.1.2 Manage auditing and security logon

On Windows Vista and later, SCC uses the auditpol.exe application to obtain the system's audit configuration. In order to run this command, the user running the software must have the User Right, "Manage auditing and security log". By system default, the Administrators group is a member of this right. However, if the security is modified and the Administrators group is removed, errors will be reported, any check related to the Windows 'Audit Policy' will error out.

2.1.3 Windows Management Instrumentation (WMI) Service

Several checks in the SCAP content require performing checks by querying WMI data. For both local and remote reviews, the WMI service must be enabled and running. This service is installed and enabled by default.

2.2 Scanning Requirements (Windows Remote Only)

2.2.1 Domain Admin Rights

When performing remote scans of Windows computers, the user of the software must have Local Administrator rights on both the scanning and target computers. The preferred method for this is to login to the computer with SCC installed as a Domain Admin. SCC does not currently allow any credential caching or storing.

2.2.2 File and Printer Sharing for Microsoft Networks

When performing a review of a remote system, the remote File and Printer Sharing for Microsoft Networks must be installed and enabled in order to connect to the Administrative shares. This Network component is installed and enabled by default on Windows XP, but may need to be enabled on Windows Vista and later.

2.2.3 Server Service for Remote Reviews

When performing a review of a remote system, the remote Server Service must be enabled and running in order to connect to the Administrative shares. This service is installed and enabled by default.

2.2.4 Remote Registry for Remote Reviews

When performing a review of a remote system, the remote system must have the Remote Registry service enabled and running. This service is installed and enabled by default.

2.2.5 Firewall Exceptions for Remote Reviews

When performing a review of a remote system, the remote system's firewall settings may prohibit SCC from scanning. If the client firewall is blocking WAN/LAN connectivity to the file shares, remote registry or WMI, SCC will not be able to perform a remote review.

2.2.6 DCOM for Remote Reviews and content which uses WuaUpdateSearcher

If content is selected which uses WuaUpdateSearcher OVAL probes, and the target system is remote, SCC uses DCOM to obtain this information. DCOM is enabled by default, but might be disabled due to agency security policies. If DCOM cannot be enabled, then the review will need to be performed locally to obtain WuaUpdateSearcher data.

2.3 Report Generation and XML Validation Requirements

2.3.1 Microsoft Core XML Services (MSXML) 6.0

Microsoft Core XML Services (MSXML) 6.0 is required by SCC to validate and transform XML documents. Most Windows systems should have this installed.

If the MSXML 6.0 is not installed on the system, the review can still complete and create the XCCDF and OVAL XML files, but it will not be able to create any HTML or text-based reports.

A download is available at:
http://www.microsoft.com/downloads/details.aspx?FamilyID=993C0BCF-3BCF-4009-BE21-27E85E1857B1&displaylang=en

3. INSTALL/UNINSTALL

To obtain a copy of the SCAP Compliance Software please refer to the Technical Support section of this manual.

3.1 Windows Software Installation

Note: Installer should be run with an Administrator account.

3.1.1 Standard Installation Method

1. Double click on the installer (SCC_3.1_Setup.exe).
2. Read the Welcome Screen and click Next.
3. Read the License Agreement page, click "I agree", and click Next.
4. Choose the Destination Folder (or leave at the default) and click Next.
5. Select "Install for all users" or "Install for the current user only" and click Next. The "Install for the current user only" option may allow a non-administrator to install the software; however, the Start Menu icons will only appear on that user's Start Menu.
6. Determine if installing as a service is desired. Refer to the section titled 'Running SCC as a Service' for additional information.
7. Read the final page and click Finish.

3.1.2 Silent Installation Method

To perform an automatic, silent installation based on default settings, run the installer via command line with a /S flag.

```
SCC_3.1_Setup.exe /S
```

Other silent installation options:

Install the SCC Service

```
/svc=yes
```

Install the SCC Service Editor

```
/edit=yes
```

Install SCC to a specific directory

```
/D=<Path>
```

To perform an automatic, silent installation and specify the installation directory, run the installer via command line with a /S and /D flag.

```
Example: SCC_3.1_Setup.exe /S /D=<Path>
```

To perform a silent installation including the SCC Service and the SCC Service Editor, run the installer with a /S, /svc and /edit

```
Example: SCC_3.1_Setup.exe /S /svc=yes /edit=yes
```

Note 1: All command line parameters are case sensitive.

Note 2: In regards to specifying the installation directory, when defining the path, even if the path includes spaces, do not wrap that path in quotes. Also do make sure there are no spaces around the

equals sign. Finally, if the /D flag is used with other parameters such as /svc or /edit, it must be specified last.

.

```
Example: SCC_3.1_Setup.exe /S /svc=yes /D=D:\Some Directory\
```

3.1.3 Running software directly from a CD-ROM

Refer to the FAQ 22 for instructions.

3.2 Windows Software Uninstall

3.2.1 Standard Method

1. Click Start -> Programs -> SCAP Compliance Checker 3.1 -> Uninstall.
2. Read the Welcome Screen and click Next.
3. Read the list of Files not Deleted and determine if the files should be deleted or kept. By default, the uninstaller does not remove any file created after the installation. Click Delete, Delete All, or Next.
4. Click Finish.

3.2.2 Silent Uninstall

To perform an automated, silent uninstallation, run the uninstaller via command line with a /S flag

```
"C:\Program Files\SCAP Compliance Checker 3.1"\uninstall.exe /S
```

4. GUI BASED SCAP COMPLIANCE SCANNING

Section 4 of this document explains the basic graphical user interface (GUI) usage of SCC to perform SCAP based compliance scanning. For additional features, such as standalone OVAL and OCIL, please review section 8.

4.1 Overview of Graphical SCAP Scanning with SCC

Below is a quick overview of how SCC works.

1. Open the SCC Graphical User Interface.
2. View available SCAP content included with SCC.
3. Install any additional SCAP content into SCC.
4. Enable SCAP content and select the desired profile from each SCAP content stream.
5. Scan Computer(s) with enabled SCAP content.
6. View reports.

4.1.1 Launching the Graphical User Interface

To start the application with a Graphical User Interface (GUI), click:

Start -> Programs -> SCAP Compliance Checker -> SCAP Compliance Checker 3.1

4.2 Installing & Configuring SCAP Content

The SCAP Content selection form lists all of the SCAP streams available to the user.

4.2.1 Installing SCAP Content

1. Launch the Graphical User Interface of SCC
2. Click Edit -> SCAP Content
3. Click on the "Install Content" button on the upper left corner of the form.
4. Browse to the zip file containing the SCAP stream
5. After installation is complete, enable the content and choose the desired profile.

4.2.2 Enabling/Disabling SCAP Content

1. To enable/disable a single SCAP Content stream, **left** click the checkbox to the left of the SCAP stream name
2. To enable all SCAP Content streams, **right** click in the Content column, and click "Select All Streams"
3. To disable all SCAP Content streams, **right** click in the Content column, and click "Clear All Selected Streams"

4.2.3 Selecting a Profile

A profile is a collection of rules and is designed to allow the same set of SCAP content (XML) to perform different sets of checks based on end user need. SCAP content can contain one or more different profiles. By default, SCC enables the first profile found.

For USGCB, there is only one profile in the content, but for other content such as DISA, the end user will need to select the appropriate profile, according to the sensitivity of the computer being scanned. For DISA STIGS, below is the normal list of available profiles in each SCAP content stream.

- MAC 1 Public
- MAC 1 Sensitive
- MAC 1 Classified
- MAC 2 Public
- MAC 2 Sensitive
- MAC 2 Classified
- MAC 3 Public
- MAC 3 Sensitive
- MAC 3 Classified

How much the checks and results are impacted by changing profiles is completely dependant on the intent of the SCAP Content Author (not SCC). The checks in all profiles could be all the same, or they could differ greatly.

To select a profile, **left** click on the Profile Column for the desired stream, if there is more than one profile available for a given SCAP stream, such as DISA STIG content, you will see a list of available profiles.

4.2.4 Deleting SCAP Content

To delete a SCAP Content Stream, **right** click on the Content column and click "Delete -<stream name>".

To delete ALL SCAP Content Streams, **right** click on the Content column and click "Delete all Streams".

4.2.5 Viewing SCAP Stream Details

To view additional information about the SCAP Content, Right click on the SCAP Stream name, and click "View Details". A new form will appear with the Stream, Version, Status, Profile, OVAL Version, XCCDF Date, Patches Date, Title, Platform, Publisher, Description and Notice.

4.2.5.1 Saving SCAP Prose Reports

Once you have opened the Content Details form, a human readable 'prose' version of the XCCDF and OVAL files to either HTML or Text format may be produced. To use, a profile must be selected on the SCAP Content form. If no profile is selected, the buttons will be disabled.

4.2.6 Configuring SCAP Patch Content Update Options

Note: This functionality only works for Patch content, not for SCAP content in general.

1. Click Edit -> SCAP Content
2. Click Content Updates

The SCC can be configured to periodically check for updated SCAP patch content XML files. For the USGCB content maintained by NIST, the XCCDF files contain external references to the current patch content files online. By default the SCC will not attempt to download patch content. It will use the copy which is provided with the SCC installer, or any additional SCAP stream bundles that are installed by the end user. As the patch content should change periodically it is recommended to either manually replace the patch content on a periodic basis, or configure SCC by the use of a local Intranet patch content website.

To prevent potential bandwidth issues and fingerprinting of your network, it is highly recommended to use a website on your Intranet to obtain updated patch content. When NIST releases revised content, which is about once a month, these files will need to be replaced by a system administrator.

The patch content website can be obtained by viewing the XCCDF XML file with an XML or Text editor.

4.2.6.1 Patch Content Update Process

1. SCC determines if the user has selected downloading from an Intranet or Internet website.
2. SCC checks the user specified Update Frequency against the file modified time of the local copy of the patch content.
3. If the primary or secondary Intranet download succeeds, then the Internet download is not attempted, even if the option is enabled.
4. After the patch content XML file has been downloaded, an XML validation is performed to ensure the XML is valid.
5. If the downloaded content is valid and newer than the local copy, then the local copy is replaced.

4.2.6.2 Update Frequency

Option	Description
Download updated patch content if local file is older than [] days.	The SCC will check the modified date of the patches file referenced in the XCCDF file. For example, in the usgcb-winxp stream, the patches file is called USGCB-Windows-XP-patches.xml'. If the date modified of the file is greater than the user specified threshold, then the SCC will attempt to download an updated version from a user specified Intranet site, or use the URL specified in the XCCDF, which is likely an Internet reference.

4.2.6.3 Intranet Settings

Option	Description
Download from Intranet Site	This checkbox is used to enable the functionality of downloading patch content from the users local Intranet.
Primary Intranet Site URL (http only)	URL to an HTTP (not HTTPS) website on the users Intranet LAN/WAN. Example: http://yourintranet.gov SCC will then lookup the file names for the patch content and attempt to download the local files. If the end user is reviewing Windows XP and Vista computers, the SCC will lookup the patch content information from the USGCB XCCDF file and attempt to download the following: http://yourintranet.gov/USGCB-Windows-Vista-patches.xml http://yourintranet.gov/USGCB-Windows-XP-patches.xml http://yourintranet.gov/USGCB-ie7-patches.xml
Secondary Intranet Site URL (http only)	This is an optional backup URL incase the first local website is not available. This only is performed if the primary Intranet download is not successful.

4.2.6.4 Internet Settings

Option	Description
Download from URL specified in each XCCDF File	Most XCCDF XML files contain a URL to the current patch content XML file. Since this file will very likely be an Internet URL, this option should be used with caution as it will cause the application to download from the Internet. If the application is being run via a scheduled task or other method across an enterprise, this could cause bandwidth issues for your agency or potentially cause a denial of service to the hosted website. For example, if an agency has 10,000+ computers running the SCC at the same time, it could cause some significant bandwidth problems.

4.3 Performing SCAP Scanning

After installing and enabling the desired SCAP content and profile, documented in section 4.2, the application is ready to perform compliance scanning.

4.3.1 Quick Overview

1. Launch the Graphical User Interface of SCC
2. Select SCAP Content Stream(s) and Profile per Content Stream
3. Select Computer(s) to Review
4. Review Computer(s)
5. View Reports

4.3.2 Select Computer(s) to Review

The SCC can review the local computer or remote computers over LAN/WAN connections. Select one of the following options:

4.3.2.1 Local Computer

This option instructs SCC to scan the computer in which the SCC software in installed. Please refer to the Requirements section for additional information on what is required to perform a local scan.

4.3.2.2 Single Remote Computer

This option instructs SCC to scan a single remote Windows computer over the LAN/WAN. To use, enter a single NetBIOS computername or IP Address into the text field provided.

Please refer to the Requirements section for additional information on what is required to perform a remote scan.

4.3.2.2 Multiple Remote Computers

This option instructs SCC to scan a list of remote Windows computer over the LAN/WAN. This list should be in the form of a text file with a single computer listed per line.

Please refer to the Requirements section for additional information on what is required to perform a remote scan.

4.3.2.2.1 Create Host file from Domain

This option allows the end user to automatically generate a host file based on the Active Directory Domain that the end user's computer resides in. Note that this may take a long time, and could cause IDS alerts depending on the option chosen such as "Ping".

4.3.3 Enabling SCAP Scanning

By default, SCC is enabled to perform SCAP Scanning. SCC can perform SCAP content analysis, 'raw' OVAL analysis, 'raw' OCIL analysis, or combinations there of. The majority of SCC users will only require SCAP Analysis, which contains SCAP Benchmarks such as USGCB, DISA STIGS etc...

This option can be configured by clicking the Button to the left of "SCAP Streams Enabled" and ensuring a Check is listed and not an X. Additionally it can be enabled by clicking Edit -> SCAP Analysis.

4.3.4 Performing Analysis

To perform a scan, click the '**Analyze Selected Computers**' button.

To cancel a review, click the '**Cancel Analysis**' button.

4.3.5 Saving Options to a custom XML File

SCC will automatically save any customization to the default options.xml file on each run. However options in the GUI can be saved to an XML file by clicking:

File -> Save Options As

The resulting XML file can be used when running via command line. Refer to the Command Line Parameters section of the Using the Software - via Command Line for additional information.

4.4 Editing Options

The SCC application has many end user customizable options, although the installation defaults are those most frequently used. After using SCC a few times, the end user may want to adjust some of these options, depending on their personal preferences.

1. Launch the Graphical User Interface of SCC
2. Click Edit -> Options

4.4.1 Reporting

Option	Description
Maximum Number of Recent Reports	This option specifies the number of "Recent Reports" to list in the GUI under Results -> Recent Reports. The available options are from 10 to 30.
Clear All Recent Reports	Clear the last X number of reports from the Results -> Recent Reports menu. This does not delete any of the source HTML/XLS/Text reports from disk, it just deletes this history in the menu.

4.4.2 Select Reports

Select the Reports to be created during the analysis.

Report	Description
All Settings	This report contains detailed pass and fail results from each check performed. It is a large report and is not intended for printing.
All Settings Summary	This report contains a summary of pass and fail results from each check.
Non-Compliance	Non-compliance reports contain detailed results from each failed check. It is a large report and is not intended for printing.
Non-Compliance Summary	This report contains a summary of the failed checks.

4.4.3 Report File Types

Format	Description
HTML	HTML formatted reports for viewing with a web browser
Text	Plain Text reports for viewing with a text editor such as Notepad or Wordpad.

4.4.4 Data Directory

Option	Description
User Home Directory	This option dynamically sets the base directory in which SCC saves all Logs and Results on a per-user basis. Example: C:\users\TestUser\SCC
Running Application Directory	This option sets the based directory in which SCC saves all Logs and Results to the location SCC is running/installed. Example: C:\Program Files\SCAP Compliance Checker 3.1

Custom Directory	This option allows the end user to specify any custom directory to save all Results and Logs to.

4.4.5 Logging and Debug

Option	Description
Save Screen Log	This option saves the analysis log printed to the "Status" screen to a text file for viewing after the review.
Save Debug Log	This option saves a large amount of additional information related to what occurred during a review. This option is disabled by default and should only be used when attempting to resolve errors in the application, as it will slow down the application and potentially use large amounts of disk space. Please refer to Appendix A.8 Debugging for additional information on SCC debug logs and their intended usage.
Suppress Warnings	This option will prevent warnings from being reported. As warnings are not critical, this option may be desired for certain users. This option may be useful in conjunction with 'ignore remote filesystems' and 'ignore case' listed in the File Scanning section.

4.4.6 XML Results

Option	Description
Save Generated XCCDF XML Files	This option allows the user to disable saving the XCCDF XML files after the review. It should always be enabled unless drive space is limited. If this option is not enabled, multiple computer summary reports cannot be created.
Save Generated OVAL XML Files	This option allows the user to disable saving the OVAL XML files, which contain the detailed results from each review, and can be very helpful in debugging problems.
Create ARF XML Output File	This option creates the Assessment Results Format (ARF) XML results based on ARF version 0.41.1
Validate XML Output Files	This option enables validating the XML results created by SCC.
Failed CPE XML Result Files(s)	This option enables saving of CPE results for SCAP streams that are not applicable to the target system. This option should only be enabled for debugging why a SCAP stream is not performed against a target system. Enabling it will create numerous small XML files, which are not required for any other reporting purpose.

4.4.7 File Scanning

Option	Description
Ignore remote filesystems	This option allows end users to override the instructions in the OVAL content and to skip scanning any remotely mounted filesystems such as NFS or Windows shares. Ideally this should be specified in the OVAL content, and enabling this option will likely cause warnings that results may not be as intended by the content author.
Ignore case	This option allows end users to override the instructions in the OVAL content and to ignore case of files and directories.

	Ideally this should be specified in the OVAL content, and enabling this option will cause warnings that results may not be as intended by the content author.

4.4.8 Content Processing

Option	Description
Validate content Stream(s) XML Files	This option validates that the XML content is syntax error free before performing the review.

4.4.9 Free Disk Space Threshold

Option	Description
Minimum Free Disk Space (MB)	If debugging is enabled, and OVAL content specifies to perform recursive file system and/or registry checks, the amount of disk space used by SCC can grow dramatically. To prevent running out of free disk space, SCC periodically checks the user specified free disk threshold to determine if processing can continue. If the threshold is met, the SCC will write an error to the screen, error log, and debug log (if enabled) and stop the scan.

4.4.10 Warnings

Option	Description
Patch Warning Threshold (Days)	This option allows the user to determine when SCC should print a warning regarding the age of the patch content. Since patch content is normally updated on a regular basis, this option will inform the end user if updated patch content should be obtained.

4.5 Viewing Reports

4.5.1 Viewing Single Computer Reports

After the software completes the review, the reports can be viewed by clicking:

Results -> Open Results Directory
or
Results -> Recent Reports

The Data Directory, which contains both the results and logs, is configurable based on user preferences. Refer to "Editing Options" for details. By default, the data is stored in a subdirectory called "SCC" in the user's home directory, but can be configured to store results to the installation directory, or any custom directory.

4.5.2 Viewing Recent Reports From the GUI

The feature of "Results -> Recent Reports" allows the user to quickly view recently created reports without having to browse through the directory structure.

To increase the number of recent reports listed, refer to the "Editing Options" section of this manual.

5. COMMAND LINE USAGE

SCC has a separate executable for command line usage which is included in the installation package as 'cscc.exe'. CSCC allows for scripted or automated reviews by other applications or scheduled tasks.

Any changes made via the Graphical User Interface such as content installation, or application preferences impact the command line interface and vice versa, as the options for both interfaces are saved to the same 'options.xml' file located in the SCC installation directory.

5.1 Basic Command Line Usage

Below is a quick overview of how CSCC works.

1. Open a Command Prompt with an account that has Administrator privileges.
2. Install any additional SCAP Content into CSCC.
3. Run the Configuration Menu option of CSCC (--config).
4. View available SCAP content included with CSCC.
5. Enable SCAP Content and Select the desired profile from each SCAP Content stream.
6. Scan Computer(s) with Enabled SCAP Content.
7. View reports.

To view all available command line options, use the -? parameter.

```
cscc.exe -?
```

5.1.1 Open a command prompt and change directories to the installation directory.

Example:

```
Start -> Run -> cmd
c:
cd "\Program Files\SCAP Compliance Checker 3.1"
```

5.1.2 Optional: Install new SCAP content

```
cscc.exe -is <path to new scap content.zip>
```

Note: Once content has been installed into SCC by either the GUI or command line, it does not need to be re-installed for each use. However, after installing new content, you will need to enable it and select the desired SCAP Profile before performing any reviews.

5.1.3 Determine what SCAP Content is currently installed and enabled

```
cscc.exe --config
1.  Configure SCAP Content
-->  Follow on screen instructions for enabling SCAP streams

2.  Configure SCAP Profiles
-->  Follow on screen instructions for selecting SCAP profiles
```

Note: Each SCAP Content stream has one or more SCAP Profiles. SCAP Profiles are collections of rules to be performed, and for content such as DISA STIG SCAP Benchmarks, may impact the number of checks performed.

5.1.4 Run the command line version of the software without command-line parameters to perform a scan.

```
cscc.exe
```

This mode will automatically review the local computer based on the options you have selected via the --config menu or the GUI.

5.1.5 View Resulting Reports

After the scan completes, SCC displays the path to which the results or logs were saved.

5.2 Installing Content & Configuring SCC Configuration via Command Line

5.2.1 Installing Content into SCC

Below are the parameters for installing content and configuring application options. All of the following options must be used individually, and are not compatible with any other parameter. These parameters are designed to be performed before scanning occurs.

All command line usage requires Administrator privileges.

`-is <path>`

Install SCAP content stream from a zip file.
Example: `cscc.exe -is <path>`

Note: After installing SCAP content, you will need to enable it and select the desired profile, which can be performed via the --config command line parameter.

`-iv <path>`

Install OVAL content or optional External Variables Files from a single xml file or a zip file containing multiple xml files.
Example: `cscc.exe -iv <path>`

Note: After installing OVAL content, you will need to enable it, which can be performed via the --config command line parameter.

5.2.2 Editing Options for Command Line Use

Many of the options for SCC can be edited via the --config command line parameter of cscc. Any changes made with the --config menu will be saved to the 'options.xml' file which is located in the installation directory of SCC.

For more in-depth descriptions of each option available for configuration, please refer to section 4.4, "Editing Options".

```
cscc.exe --config

 SCC 3.1 configuration edit menu.
 Make menu selection:

 1. Configure SCAP content
 2. Configure SCAP profiles
 3. Delete SCAP content
 4. Configure OVAL content
 5. Delete OVAL content
 6. Configure Options
 7. Configure SSH Options
 8. Exit and save changes
 9. Exit without saving changes
 SCAP Processing is Enabled

 - 4 of 25 SCAP streams are enabled
 OVAL Processing is Disabled

 - 0 of 0 OVAL streams are enabled
```

```
Enter menu selection:
```

1. Configure SCAP content

```
SCAP Content X of Y enabled.
Enter content number to enable or disable content.
('all', 'clear', or ranges N-N are allowed, type 'back' or '0' to
return):
```

2. Configure SCAP profiles

```
Enter content number to view available profiles (type 'back' or
'0' to return):
```

After selecting the content number from the list provided, a screen appears listing all available profiles for the selected SCAP Content

```
Enter profile number to set selected profile (type 'back' or '0'
to return):
```

3. Delete SCAP content

```
Enter content number to delete content.
('all' is allowed, type 'back' or '0' to return):
```

4. Configure OVAL content

5. Delete OVAL Content

6. Configure options

```
Content Scan Methods
    1.  Perform SCAP Scan
    2.  Perform OVAL Scan

Select Reports
    3.  Generate 'All Settings' report
    4.  Generate 'All Settings Summary' report
    5.  Generate 'Non-Compliance' report
    6.  Generate 'Non-Compliance Summary' report

Report File Types
    7.  Generate reports as HTML
    8.  Generate reports as Text

Logging and Debugging
    9.  Save screen logs
    10.  Save debug logs
    11.  Suppress warnings

XML Results
    12.  Save generated XCCDF XML files
    13.  Save generated OVAL XML files
    14.  Create ARF XML output
    15.  Validate XML output files
    16.  Save failed CPE XML results files
```

```
Content Processing
    17.  Scan content directories on application load
    18.  Validate content stream(s) XML files

Data Directory
    19.  Path to directory where SCC should write Results and Logs

OVAL Processing Options
    20. Ignore Remote Filesystems
    21. Enable item creation threshold
    22. Item creation threshold [50000]
    23. Ignore Case
```

Refer to section 8.7 'Editing OVAL Processing Options' for additional information on options 20-23.

7. Configure SSH Options

This set of options is used to enable sending of the XML, HTML and/or Text reports via SSH to a centralized server.

```
SCC 3.1 SSH Options menu.
Make menu selection *Note: only SSHv2 is supported

File Transfer Options
    1. Enable file transfers
    2. Delete local reports after transfer

Reports to Transfer
    3. XML
    4. HTML
    5. Text

Server Information
    6. Hostname/IP Address: irsnet
    7. Port: 22

Select either Username/Password connection, or Private Key
connection
    8. Connect using Username/Password
    9. Connect using Private Key and Passphrase

Directory Information
    10. Local results directory: <Local Path>
    11. Remote SSH directory: <Remote Path>

Enter menu selection (type 'back' or '0' to return):
```

8. Exit and save changes

9. Exit without saving changes

5.3 Command Line Scanning

Before performing a scan via command line, it is recommended to view the configuration by the --config parameter, documented in section 5.2.

5.3.1 Scanning Parameters

Below are the parameters available for performing scans. Many of the options can be used in combination, as indicated in the usage below.

```
cscc.exe [-f <file> | -h <host>] [-o <file>][-drqx]
```

`no parameters`
: Review the local computer based on the configuration settings found in options.xml. If options.xml does not exist in the installation directory, it will be created based on application defaults. The desired method for editing the options is via the --config command line parameter.

`-d`
: Create verbose debug logs in the Logs directory for troubleshooting purposes. Note that this option will generate a large amount of text based data (MB's to GB's) and will cause the application to run slower, so is not recommended for normal usage.

  Please refer to Appendix A.8 Debugging for additional information on SCC debug logs and their intended usage.

`-f <file name>`
: Review all computers specified in the file. This text file should contain one computer name per line.

  Example: `cscc.exe -f hosts.txt`

`-h <host name>`
: Review the specified computer.

  Example: `cscc.exe -h <hostname>`

`-o <file name>`
: Review using the specified options file. If the file specified does not exist, the application will report an error that it does not exist. A new options file will not be created.

  Example: `cscc.exe -o myoptions.xml`

`-r <rule id>`
: Review a single rule using the Rule ID from the XCCDF file

  Example: `cscc.exe -r account_lockout_duration`

`-q`
: Review in quiet mode. No output will be displayed on the screen.

`-x`
: Perform schema validation on all input and output XML files.

5.3.2 Other Parameters

Below are other informational parameters. All of the following options must be used individually, and are not compatible with any other parameter.

`-v`
Displays simple version information.

`-V`
Displays verbose version information.

`-?`
Displays help.

`--help`
Displays help.

5.3.3 Command Line Examples

1. Review the local computer with customized report settings and do not display any data to the screen.

```
cscc.exe -o myoptions.xml -q
```

2. Review several computers from a host with customized report settings.

```
cscc.exe -f test.txt -o myoptions.xml
```

3. Review a single remote host 'computer1' in debug mode and validate the XML files

```
cscc.exe -h computer1 -d -x
```

5.4 Multiple Computer Deployment

If the end user is automating the process of running the SCC software locally on multiple remote computers, below is the list of files that must be present for the application to run via command line.

- cscc.exe
- options.xml (or any custom named options file)
- "Resources" directory, subdirectories and all files

5.4.1 Collecting Resulting Files

If the end user is pushing the command line version of the software out to the target computers, and would like to collect the results in a consolidated directory for generating multi-computer summary reports, below is documentation explaining which files to copy.

A directory structure will be created in the format:

SCAP
<Computer>
<SCAP Stream>
<SCAP Stream Version>
<Date Time Stamp>
<XML>

The Date Time Stamp directory will contain any Text or HTML reports created, based on user preferences. The XML Directory will contain the resulting OVAL and XCCDF XML files based on user preferences.

The only file required for generating the multi-computer reports is the XCCDF file, which will be in the XML directory, in the format:

`<Computer>_SCC_3.1_<DateTime>_**XCCDF-Results**_<Stream>.xml`

After all of the XCCDF XML files have been collected and copied to a centralized share, multi-computer summary reports can be created. Please refer to "Generating Multi-Computer Summary Reports" section of the documentation for additional information.

5.5 Generating Post Scan Reports from the Command Line

If a large number of files are collected on a share that is accessed via a LAN or WAN, it may be most time effective to generate the reports via command line on the server that contains the collection of files. This allows for a scheduled task to be created that can be run on a user specified timeframe.

For example, if 100,000 computers are reviewed, it will likely take many hours to generate the summary reports. Ideally, this could be run during an evening a day after all of the results are created.

This functionality requires configuring a custom options.xml file with the GUI, and calling the application via command line with specific parameters. Refer to section 7 "Post Scan Report Generation" for details.

5.5.1 Post Scanning Report Generation Parameters

Below are the parameters available for creating reports after XML results have been created. All of the following options must be used individually, and are not compatible with any other parameter.

`-c <options file name>`

Generate the Cyberscope auto-feed XML report using the specified options file.

Example: `cscc.exe -c options.xml`

This option corresponds to the Generate Cyberscope Report feature in the GUI, which can be accessed via "Results-> Generate Cyberscope Report".

This command line feature uses all of the configurable options on the Generate Cyberscope Report form including the Source and Destination Directories.

`-s <options file name>`

Generate summary SCAP reports using the specified options file.

Example: `cscc.exe -s options.xml`

This option corresponds to the Generate Summary Reports feature in the GUI, which can be accessed via "Results-> Generate Summary SCAP Reports".

This command line feature uses all of the configurable options on the "Generate Summary SCAP Reports" form including the Source and Destination Directories along with all available reports.

This command line feature is available for generating summary reports from very large numbers of computers, which may take hours to complete. This command could be scheduled to run weekly or monthly, and have reports available the next day.

`-ts <options file name>`

Generate detailed SCAP reports using the specified options file.

Example: `cscc.exe -ts options.xml`

This option corresponds to the Generate Detailed SCAP Reports feature in the GUI, which can be accessed via Results-> Generate Detailed SCAP Reports.

This command line feature uses all of the configurable options on the Generate Detailed SCAP Reports form including the Source and Destination Directories along with all available reports.

This command line feature is available for generating detailed reports from very large numbers of computers, which may take hours to complete. This command could be scheduled to run weekly or monthly, and have reports available the next day.

`-tv <options file name>`

Generate detailed OVAL reports using the specified options file.

Example: `cscc.exe -tv options.xml`

This option corresponds to the Generate Detailed OVAL Reports feature in the GUI, which can be accessed via Results-> Generate Detailed OVAL Reports.

This command line feature uses all of the configurable options on the Generate Detailed OVAL Reports form including the Source and Destination Directories along with all available reports.

This command line feature is available for generating detailed reports from very large numbers of computers, which may take hours to complete. This command could be scheduled to run weekly or monthly, and have reports available the next day.

5.5.2 Scheduling Command Line Generation of Summary Reports

The process for scheduling cscc.exe via the Windows Task Scheduler is the same as any other application, except the parameters listed above will need to be included.

1. Click Start -> Programs -> Accessories -> System Tools -> Scheduled Tasks.
2. Click "New".
3. Click "Browse".
4. Select the command line version of the file (Example "C:\Program Files\SCAP Compliance Checker 3.1\cscc.exe"
5. Choose the selected timeframe (Daily, Weekly, Monthly, etc..).
6. Enter the credential for the software to run.
7. Click "Open Advanced Properties for this task when I click Finish".
8. Click "Finish".
9. In the Run line add the desired parameters after the double quotes. Example:

```
"C:\Program Files\SCAP Compliance Checker 3.1\cscc.exe" -s options.xml
```

Test the scheduled task by right clicking and selecting "Run."

6. UNDERSTANDING SCAN RESULTS

6.1 Understanding Scan Reports

6.1.1 Single Computer HTML and Text Reports

Depending on the user selected options, the following reports may be available in both HTML and/or text based formats:

Report	Description
All Settings Report	The <Computer>_SCC_3.1_All-Settings_<XCCDF Content Name>.htm report contains the XCCDF results in a human readable format. The report is divided into five sections: Score, System Information, Stream Information, Results and Detailed Results. The **Scores** section contains the calculated scores for the target system. The **System Information** section contains information about the target system, such as the host name, IP addresses, operating system, processor, memory, manufacturer, model, serial number, BIOS version, and Ethernet Interfaces. The **Stream Information** section contains information about the XCCDF benchmark, such as the XCCDF filename used, the profile used, the testing start and end times, and the identity of the user who ran the benchmark. The **Results** section contains the individual rule results, comprised of the CCE reference and the check title. To view the "Detailed Results" for an individual item, just click on the text. The **Detailed Results** section contains in-depth information on each rule performed in the benchmark.
All Settings Summary Report	Contains the same information as the "All Settings Report", except excludes the Detailed Results, which allows for easier printing.
Non-Compliance Report	The <Computer>_SCC_3.1_Non-Compliance_<XCCDF Content Name>.htm report contains same results in the same format as the "All Settings Report", but only includes the Failed, Error, and Unknown checks.
Non-Compliance Summary Report	Contains the same information as the "Non-Compliance Report", except excludes the Detailed results, which allows for easier printing.

6.1.2 Understanding the Result Status Information

All of the reports show the number of checks performed, and the result for each. The result types are specified by the SCAP standards and are summarized below.

Result	Explanation
Pass	The SCC was able to correctly interpret the check in the XML content, perform the check on the target system, and all check requirements were met. Example: Password Length Requirement 12 Characters, Target Computer: 12 Characters
Fail	The SCC was able to correctly interpret the check in the XML content, perform the check on the target system, and one or more of check requirements were not met.

	Example: Password Length Requirement 12 Characters, Target Computer: 8 Characters
Error	The SCC was able to correctly interpret the check in the XML content, however an error occurred while performing the check. This is typically due to a configuration of the target system, or insufficient permissions of the user running the software.
Unknown	The SCC was not able to interpret the check in the XML content. This could be due to a flaw in the XML content, or an incompatibility between the SCC and the XML content such as OVAL version.
Not Applicable	The SCC was able to interpret the check in the XML content, but it was not applicable to the target system. For example, Internet Explorer 7 checks performed against a system that only has Internet Explorer 6..
Not Checked	The SCC was able to interpret the check in the XML content, however the XML content instructed the SCC not to perform this check.
Not Selected	The SCC was able to interpret the check in the XML content, however the XML content instructed the SCC not to perform this check.
Total	Numeric sum of Pass, Fail, Error, Unknown, Not Applicable, Not Checked, and Not Selected.

6.1.3 Understanding Color Coding in the HTML Reports

The HTML reports have color coding to assist in understanding what failed, and why it failed.

6.1.3.1 Color Coding in the 'Results' Section

Color	Description
Blue	The overall rule passed all of the required tests. Example: "Account Lockout Duration - (CCE-2928-0) - Pass
Red	The overall rule failed one or more of the required tests. Example: "Account Lockout Duration - (CCE-2928-0) - Fail

6.1.3.2 Color Coding in the 'Detailed Results' Section for Class = Compliance

Per OVAL specifications, for compliance checks, a test result of "True = Compliant", and "False = Not Compliant".

Color	Description
Blue	The individual test result was True, or the result was False but did not cause the overall test to fail.
Red	The individual test was False and contributed to the overall rule being marked as Fail.

6.1.3.3 Color Coding in the 'Detailed Results' Section for Class = Patch

Color	Description
Blue	SCC was able to verify that the patch was installed as required in the underlying tests. Result = Pass
Red	SCC was not able to confirm that the patch was installed as required, as one or more of the underlying tests failed. Result = Fail

6.1.3.4 Color Coding in the 'Detailed Results' Section for Class = Vulnerability

Per OVAL specifications, for Compliance checks, a test result of True = Vulnerable and False = Not Vulnerable.

Color	Description
Blue	The individual test result was False (meaning not vulnerable), or the result was Pass (vulnerable) but did not cause the overall test to fail.
Red	The individual test was True (Vulnerable) and contributed to the overall rule being marked as Fail.

6.2 Navigating the Results Directory

If Results -> Open Results Directory is selected, Windows Explorer opens to the directory containing the HTML and text reports along with other files created during the review.

The Data Directory, which contains both the Results and Logs, is configurable, see "Editing Options" for details. By default the data is stored a subdirectory called "SCC" in the user's home directory, but can be configured to store results to the installation directory, or any custom directory.

The Results directory structure is as follows:

SCAP
- <Computer>
  - <SCAP Content>
    - <SCAP Content Version> (Such as v1.2.0.0)
      - <Date_Time>
        - XML
        - <Computer>_SCC_3.1_All-Settings_<XCCDF Content>.htm
        - <Computer>_SCC_3.1_All-Settings-Summmary_<XCCDF Content>.htm
        - <Computer>_SCC_3.1_Non-Compliance_<XCCDF Content>.htm
        - <Computer>_SCC_3.1_Non-Compliance-Summary_<XCCDF Content>.htm

OVAL (only if standalone OVAL is enabled)
- <Computer>
  - <OVAL Content>
    - <OVAL Version> (Such as 5.10.1)
      - <Date_Time>
        - XML
        - <Computer>_SCC_3.1_All-Settings_<OVAL Content>.htm
        - <Computer>_SCC_3.1_All-Settings-Summmary_<OVAL Content>.htm
        - <Computer>_SCC_3.1_Non-Compliance_<OVAL Content>.htm
        - <Computer>_SCC_3.1_Non-Compliance-Summary_<OVAL Content>.htm

OCIL (only if standalone OCIL is Enabled)
- <Computer>
  - <OCIL Content>
    - <OCIL Version> (Such as 2.0)
      - <Date_Time>
        - XML
        - <Computer>_SCC_3.1_All-Settings_<OCIL Content>.htm
        - <Computer>_SCC_3.1_All-Settings-Summmary_<OCIL Content>.htm
        - <Computer>_SCC_3.1_Non-Compliance_<OCIL Content>.htm
        - <Computer>_SCC_3.1_Non-Compliance-Summary_<OCIL Content>.htm

6.2.1 Contents of the XML Directory

The XML folder contains XML output generated by SCC. This output can be XCCDF results, OVAL results and OVAL variables files. Refer to the "Editing Options" for enabling or disabling saving the XCCDF and OVAL XML files after each review.

These files are not designed to be human readable, but are intended to be read into another SCAP, XCCDF or OVAL compatible software product to provide consolidated results.

XML File	Description
ARF	The <Computer>_SCC_3.1_ARF_<XCCDF Content Name>.xml file contains the DOD ARF 0.41 (Assessment Results Format) results in a machine readable format. This is a high level summary of the review including the asset information from each system and the pass/fail status of each check performed.
XCCDF Results	The <Computer>_SCC_3.1_XCCDF-Results_<XCCDF Content Name>.xml file contains the XCCDF results in a machine readable format. This is a high level summary of the review including the asset information from each system and the pass/fail status of each check performed.
OCIL Results	The <Computer>_SCC_3.1_ocil-res-Results_<XCCDF Content Name>.xml file contains the detailed OCIL in a machine readable format. This is a detailed report pass/fail results from each OCIL patch check performed during a review. This file only exists if SCAP content contains an OCIL questionnaire.
OVAL CPE Results	The <Computer>_SCC_3.1_CPE-Results_<XCCDF Content Name>.xml file contains the CPE results in a machine readable format. This contains platform information about the target system including the operating system, network interfaces and processor type.
OVAL Patch Results	The <Computer>_SCC_3.1_OVAL-Patch-Results_<XCCDF Content Name>.xml file contains the detailed OVAL patch results in a machine readable format. This is a detailed report of pass/fail results from each OVAL patch check performed during a review. This file only exists if the SCAP content contained an OVAL patch file.
OVAL Results	The <Computer>_SCC_3.1_OVAL-Results_<XCCDF Content Name>.xml file contains the detailed OVAL results in a machine readable format. This is a detailed report of pass/fail results from each OVAL check performed during a review.
OVAL Variables	The <Computer>_SCC_3.1_OVAL-Variables_<XCCDF Content Name>.xml file contains a list of OVAL variables in a machine readable format.

6.3 Viewing Screen, Error or Debug Logs

The directory containing SCC Logs (if any exist) can be opened in the Windows Explorer by clicking:

Results -> Open Log Directory

Depending on the user selected preferences are selected, the following log files may be present:

Report	Description
Screen Log	SCC_3.1_<DateTime>_Screen_Log.txt This option saves the analysis log printed to the "Status" screen to a text file for viewing after the review. This file is not saved by default, but can be enabled in the Options.
Error Log	SCC_3.1_<DateTime>_Error_Log.txt This report contains any errors that may have occurred while SCC is running, but not during a specific scan. This also contains any errors that may have occurred during command line usage. If this file exists, and the error log does not provide enough information to resolve the issue, please contact SPAWAR and provide the error log for our analysis.
Scan Error Log	SCC_3.1_<DateTime>_scan<number>_Error_Log.txt This report contains any errors that may have occurred during a GUI based scan. The scan<number> such as scan001, scan002 corresponds to each review that is started by clicking the Analyze button. Normally this file will not exist. If this file exists, and the error log does not provide enough information to resolve the issue, please contact SPAWAR and provide the error log for our analysis.
Debug Log	SCC_3.1_<DateTime>_Debug_Log.txt This option saves a large amount of additional information related to what occurred during a primary SCC operation, or when run via command line.. This option is disabled by default and should only be used when attempting to resolve errors in the application, as it will slow down the application and potentially use large amounts of disk space. Please refer to Appendix A.8 Debugging for additional information on SCC debug logs and their intended usage.
Scan Debug Log	SCC_3.1_<DateTime>_scan<number>_Debug_Log.txt This report contains any debug that occurred during a GUI based scan. The scan<number> such as scan001, scan002 corresponds to each review that is started by clicking the Analyze button. This option saves a large amount of additional information related to what occurred during a review. This option is disabled by default and should only be used when attempting to resolve errors in the application, as it will slow down the application and potentially use large amounts of disk space. Please refer to Appendix A.8 Debugging for additional information on SCC debug logs and their intended usage.

7. POST SCANNING REPORT GENERATION

SCC, by default, creates most of the commonly used reports during each scan. However, additional reports can be created after the fact. These are completely optional depending on your desired usage.

7.1 Generate Summary SCAP Reports (from XCCDF results)

SCC can generate multi-computer summary reports from the XCCDF XML (SCAP) results created by the SCC or other SCAP Validated applications.
To generate summary reports from existing XCCDF XML files:

1. Launch the Graphical User Interface of SCC.
2. Click Results -> Generate Summary Reports.
3. Select the Source Directory containing existing XCCDF XML results from previous SCC scans.
4. Select the Destination Directory to save report to.
5. Select Report and Report Formats.
6. Click Generate.

7.1.1 Select Directories

Option	Description
Source Directory	Location for the application to scan for XCCDF XML results from previous reviews. This option is recursive (all subfolders will be scanned for files to use).
Destination Directory	Location where summary reports are to be saved.
Open Destination Directory when processing is complete	This opens Windows Explorer to the directory containing the new summary reports, when the processing is complete.

Note: To create reports based on a subset of computers in the organization, organize the consolidated data in a directory structure similar to the example listed below:

/Entire Organization
/ Sub Organization 1
/ Sub-Sub Organization
/ Sub Organization 2
/ etc..

If the SCC is pointed at the entire organization, or any subset, the summary reports will only contain the desired subset of computers.

7.1.2 Select Reports to Generate

Option	Description
Site Summary	This report provides a consolidated list of checks, with a single CCE reference and the Pass, Fail, Error, Unknown, Not Applicable, Not Checked, and Not Selected occurrences for each check.
Site Summary Non-Compliance	This report provides a consolidated list of checks, with a single CCE reference and the Fail, Error and Unknown occurrences for each check that had a fail or an error status.

Computer List	This report lists the latest results for all computers reviewed and the Review Time, Pass, Fail, Error, Unknown, Not Applicable, Not Checked, Not Selected, Total along with the Original and Adjusted Scores.
Computer List Historical	This report lists all results for all computers reviewed, and the Review Time, Pass, Fail, Error, Unknown, Not Applicable, Not Checked, Not Selected, Total along with the Original and Adjusted Scores.

7.1.3 Select File Format(s) of Generated Reports

Format	Description
HTML	HTML formatted reports for viewing with a web browser
Excel	Excel Spreadsheet versions with separate tabs per SCAP stream

7.1.4 Creating the Summary Reports

To create the summary reports, click Generate. The status window will display the progress.

Note: Summary reports can also be created with a command line parameter, based on the settings configured in the GUI. Please refer to the Using the Software via Command Line for additional information.

7.1.5 Saving Settings for Future Use

To save the current configuration without generating reports, click the Save button. This will save the current configuration, which could be useful for creating a custom options XML file for generating reports via the command line.

7.1.6 Viewing Multi-Computer HTML and Excel Reports

After Multi-Computer Summary Reports are created (refer to Using the Software -> Generating Summary Reports) a Windows Explorer window may open (based on user preferences), and the reports specified to be created will be available in HTML and/or Excel spreadsheets. To view, double click on any of the files.

7.2 Generate Detailed SCAP Reports (from XCCDF and OVAL results)

SCC can regenerate single computer detailed reports from the XCCDF XML and OVAL XML (SCAP) results created by the SCC or other SCAP Validated applications.
To re-generate detailed reports from existing XCCDD/OVAL XML files:

1. Launch the Graphical User Interface of SCC
2. Click Results -> Generate Detailed Reports
3. Select the Source Directory containing existing XCCDF and OVAL results from previous SCC Scans
4. Select the Destination Directory to save report to.
5. Select Report and Report Formats
6. Click Generate

7.2.1 Select Directories

Option	Description
Source Directory	Location for the application to scan for XCCDF and OVAL XML results from previous reviews. This option is recursive (all subfolders will be scanned for files to use).
Destination Directory	Location where summary reports are to be saved.
Open Destination Directory when processing is complete	This opens Windows Explorer to the directory containing the new summary reports, when the processing is complete.

7.2.2 Select Reports to Generate

Report	Description
All Settings	This report contains detailed pass and fail results from each check performed. It is a large report and is not intended for printing.
All Settings Summary	This report contains a summary of pass and fail results from each check.
Non-Compliance	Non-compliance reports contain detailed results from each failed check. It is a large report and is not intended for printing.
Non-Compliance Summary	This report contains a summary of the failed checks.

7.2.3 Select File Format(s) for Reports

Format	Description
HTML	HTML formatted reports for viewing with a web browser
Text	Plain Text reports for viewing with a text editor such as Notepad or Wordpad.

7.2.4 Generate ARF XML Output

SCC can generate and validate the DoD Assessment Results Format (ARF) XML results based on ARF version 0.41.1 located at:

http://metadata.dod.mil/mdr/ns/netops/shared_data/arf_index_page/0.41
http://measurablesecurity.mitre.org/incubator/arf

7.2.5 Creating SCAP Detailed Reports

To create the detailed reports, click Generate. The status window will display the progress.

Note: Detailed reports can also be created with a command line parameter, based on the settings configured in the GUI. Please refer to the Using the Software via Command Line for additional information.

7.2.6 Saving Settings for Future Use

To save the current configuration without generating reports, click the Save button. This will save the current configuration, which could be useful for creating a custom options XML file for generating reports via the command line.

7.3 Generate Detailed OVAL Reports (from standalone OVAL results)

SCC can regenerate single computer detailed reports from the standalone OVAL XML results created by the SCC or other SCAP Validated applications.
To re-generate detailed reports from existing OVAL XML files:

1. Launch the Graphical User Interface of SCC
2. Click Results -> Generate Detailed Reports
3. Select the Source Directory containing existing Standalone OVAL results from previous SCC Scans
4. Select the Destination Directory to save report to.
5. Select Report and Report Formats
6. Click Generate

7.3.1 Select Directories

Option	Description
Source Directory	Location for the application to scan for OVAL XML results from previous reviews. This option is recursive (all subfolders will be scanned for files to use).
Destination Directory	Location where summary reports are be saved.
Open Destination Directory when processing is complete	This opens Windows Explorer to the directory containing the new summary reports, when the processing is complete.

7.3.2 Select Reports to Generate

Report	Description
All Settings	This report contains detailed pass and fail results from each check performed. It is a large report and is not intended for printing.
All Settings Summary	This report contains a summary of pass and fail results from each check.
Non-Compliance	Non-compliance reports contain detailed results from each failed check. It is a large report and is not intended for printing.
Non-Compliance Summary	This report contains a summary of the failed checks.

7.3.3 Select File Format(s) for Reports

Format	Description
HTML	HTML formatted reports for viewing with a web browser
Text	Plain Text reports for viewing with a text editor such as Notepad or Wordpad.

7.3.5 Creating the Detailed Reports

To create the detailed reports, click Generate. The status window will display the progress.

Note: Detailed reports can also be created with a command line parameter, based on the settings configured in the GUI. Please refer to the "Using the Software via Command Line" for additional information.

7.3.6 Saving Settings for Future Use

To save the current configuration without generating reports, click the Save button. This will save the current configuration, which could be useful for creating a custom options XML file for generating reports via the command line.

7.4 Generate Cyberscope Report (from XCCDF results)

SCC can generate the Cyberscope Autofeed report based on the DRAFT 1.0.0 Early Access Release specifications.

http://scap.nist.gov/use-case/cyberscope/index.html

SCC creates this report using XCCDF XML results created by the SCC or other SCAP Validated applications. To generate summary reports from existing XCCDF XML files:

1. Launch the Graphical User Interface of SCC.
2. Click Results -> Generate Cyberscope Reports.
3. Select the Source Directory containing existing XCCDF XML results from previous SCC Scans.
4. Select the Destination Directory to save report to.
5. Enter Agency, Department, Enclave and Contact Information.
6. Click Generate.

7.4.1 Select Directories

Option	Description
Source Directory	Location for the application to scan for XCCDF XML results from previous reviews. This option is recursive (all subfolders will be scanned for files to use). ***Note:*** OVAL XML Results are not required, nor used for creating the Cyberscope report. The only XML results required are XCCDF.
Destination Directory	Location where summary reports are to be saved.
Open Destination Directory when processing is complete	This opens Windows Explorer to the directory containing the new summary reports, when the processing is complete.

Note: To create reports based on a subset of computers in the organization, organize the consolidated data in a directory structure similar to the example listed below:

/Entire Organization
/ Sub Organization 1
/ Sub-Sub Organization
/ Sub Organization 2
/ etc..

If the SCC is pointed at the entire organization, or any subset, the Cyberscope Autofeed XML reports will only contain the desired subset of computers.

7.4.2 XCCDF Input File Age Filter

Option	Description
Use All - No File Age Threshold	Use all data files regardless of age, and do not print any warning information.
Use All - Print Warnings Based on File Age Threshold	Print an error message for each file found which is older than the user specified threshold. Results from files older than the threshold will be included in the data aggregation.

Exclude Files Older Than File Age Threshold	Print an error message for each file found which is older than the user specified threshold. Results from files older than the threshold will not be included in the data aggregation.
File Age Threshold (days)	Enter a numeric value for the number of days old that files should be warned or excluded. This option is ignored if "Use All - No File Age Threshold" is chosen.

7.4.3 Specify missing CCE Warning option

Option	Description
Suppress printing errors for missing CCE references	CCE (Common Configuration Enumeration) identifiers are the primary key for data aggregation in the Cyberscope XML schema. Any test result without a CCE reference cannot be included in any Cyberscope results. This option allows the end user to suppress error messages for each result which does not include a CCE reference, and was excluded from the report. Since the USGCB content for Windows 7 as of February 12, 2012 contains 7 tests which do not include CCE references, the number of errors this can generate can be very large, and may cause undo concern with the user. This option does not impact the result generated in the autofeed XML.

7.4.4 Specify Organizational Information

The following organizational data elements are required for Cyberscope, but cannot be obtained from the XCCDF XML results and will need to be manually entered prior to generating the Cyberscope report.

Field	Example	Default
Agency Name	Department of Defense	
Department Name	US Navy	
Enclave	SPAWAR	
Contact Email	example@navy.mil	
Contact Telephone	555-555-5555	
Web Site	http://www.public.navy.mil	
FISMA Auto Feed ID	FISMA_auto_feed_fy11	FISMA_auto_feed_fy10
FISMA Auto Feed Version	1.0beta1	1.0beta1

Note: Be sure to enter the Agency Name, Department Name, Enclave, FISMSA Auto Feed ID and FISMA Autofeed Version exactly as specified by Cyberscope, or the auto-feed upload will likely have errors. For assistance on the Cyberscope reporting, please contact the Cyberscope Helpdesk.
cyberscopehelp@usdoj.gov

7.4.5 Creating the Cyberscope Report

To create the Cyberscope XML Autofeed report, click Generate. The status window will display the progress.

Note: Cyberscope reports can also be created with a command line parameter, based on the settings configured in the GUI. Please refer to the Using the Software via Command Line for additional information.

7.4.6 Saving Settings for Future Use

To save the current configuration without generating reports, click the Save button. This will save the current configuration, which could be useful for creating a custom options XML file for generating reports via the command line.

8. ADVANCED USAGE

Below are several features of SCC which are not required for 'standard' SCAP compliance scanning. They have been grouped together as advanced usage, to prevent confusing with new users of the application.

8.1 Editing Deviations

Deviations will change the status of deviated checks from Fail, Error or Unknown to Pass and will update the computer's compliance score. Only enter deviations that have been approved for your organization.

Deviations are only applied at review time, so deviations entered will not have any impact on past review results. To edit user specified deviations:

1. Launch the Graphical User Interface of SCC
2. Edit -> Deviations

8.1.1 Enabling Deviations

To enable the use of Deviations, click the check box next to "Enable Deviations." This does not mean that deviations are currently defined, just that the functionality has been enabled or disabled.

8.1.2 Select a SCAP Stream

Select the desired SCAP Stream from the drop down on the upper left of the form. The list will be in the format of <scap stream>-<version>. Examples:

USGCB-xpfirewall-v2.0.0.0
USGCB-winxp-v2.0.0.0

8.1.3 Select a Stream Profile

If more than one than one Profile is available in the selected SCAP Stream, select the Profile from the drop down on the upper right corner of the form. The first available profile will automatically be populated into the drop down.

8.1.4 Select a Check

To edit a deviation, click on the desired row containing the CCE reference or check tile in the white list box in the center of the form. This will populate the fields on the bottom half of the form.

8.1.5 Activating Deviations

Activating deviations requires obtaining a specific unlock code from a separate application called the SCC Unlocker, which provides the unlock codes for all SCAP content. This application is separate from the SCC and must be obtained directly from SPAWAR. This application is designed to be available only to person(s) in your organization that can officially approve deviations.

In order for deviations to be used to change the pass/fail status of checks, the "Authority" field must contain the person who authorized the deviation and the "Unlock Code" field must contain the correct code from SCC Unlocker application. Additionally, the "Remark" field should be used to explain why the deviation is necessary. Justification for any deviations is included in the application reports.

After the "Authority" field is populated with any text and the correct code is entered into the "Unlock Code" field, the check box next to "Deviation is Active" will be selected, and the text in the Deviation box will change from grey to blue.

Note: Unlock Codes are unique per check performed. In other words, an Unlock Code for Check1 will not work for Check2.

Note: Unlock Codes are unique per each version of SCAP content. In other words, an Unlock Code for Check1 of content version 1.2.0.0 will not be valid for Check1 of content version 1.3.0.0, as the requirements for this check may have changed with revised version.

8.2 Customizing Compliance Thresholds

The compliance thresholds can be customized based on the organization's requirements. To edit the compliance thresholds:

1. Launch the Graphical User Interface of SCC
2. Edit -> Thresholds.

Both the percentage levels and the titles given to each level can be customized. The default settings are listed below.

Threshold	Operation	Score
BLUE	Equal to	100
GREEN	Greater than or equal to	90
YELLOW	Greater than or equal to	80
RED	Greater than or equal to	0

To maintain a consistent threshold across the organization, an unlock code is required to modify the compliance thresholds. To obtain the unlock code, contact the SCC Point of Contact for your organization, or contact SPAWAR directly via email: ssc_lant-scc@navy.mil.

The order in which the thresholds are listed may impact the end result, so it is important to place them in the order you want it processed. To change the order, highlight the threshold on the left and click "Up" or "Down."

Higher thresholds take precedence over lower.

8.3 SCAP 1.1 Scanning which contains an OCIL Questionnaire

Note: Very little if any publicly available SCAP content currently exists which contains an OCIL (Open Checklist Interactive Language) checklist, so most users may never see the following screens, as they only appear if a OCIL checklist is found in SCAP stream.

8.3.1 Process Overview

The order of operations for a SCAP 1.1 data stream with OCIL is as follows:

1. OCIL Questionnaire form opens displaying OCIL content and target computers
2. User answers questionnaires for all selected computers
3. After questionnaires have been completed, the OVAL scanning proceeds
4. OVAL and OCIL results are collected into the XCCDF results
5. HTML/Text reports are created which contain both the OVAL and OCIL results

8.3.2 OCIL Questionnaire

This form contains a list of SCAP streams which were selected on the Edit -> SCAP Content form, which contain an OCIL checklist. It also lists all of the target computers listed any computers the user has selected on the main form.

- To answer questions for the OCIL questionnaire that are enabled, click "Start OCIL Questionnaire".

- To skip answering OCIL questionnaire and proceed with automated scanning, press "Continue Analysis". This will cause SCC to list all of the questions as "Not Checked".

8.3.3 OCIL Questionnaire

This form allows you to answer any questions in the OCIL questionnaire. All of the question titles will be listed in the tree on the left hand side. To answer a question, click at the leaf node, which has a grey circle. This will populate the associated question on the right hand side.

When you have completed all of the questions, click "Save & Close". This will take you back to the OCIL Questionnaire Form, or to the next Questionnaire if more than one has been enabled.

8.3.4 Proceeding to the automated OVAL checks

If you have answered all of the OCIL Questionnaire, click "Continue Analysis" to proceed to the automated OVAL tests.

8.4 Standalone OVAL Usage

Standalone OVAL content usage is designed primarily for advanced SCC users, such as content authors who wish to run OVAL content without creating an entire SCAP benchmark. It can also be used to perform vulnerability scanning using existing OVAL vulnerability content. No standalone OVAL content is currently bundled with SCC.

1. Launch the Graphical User Interface of SCC
2. Click Edit -> OVAL Content

The Content Selection form lists all of the OVAL content available to the user. The SCC searches the <SCC Install>\Resources\OVAL_Content directory and subdirectories for OVAL XML files.

Note: OVAL content that is part of a SCAP Stream, such as USGCB, or DISA STIGS should be installed into the SCAP Content, not in the OVAL content. OVAL content included in a SCAP Stream is designed to work with XCCDF and CPE. SCC might be able to process the OVAL file as 'raw OVAL' but unexpected errors may exist.

8.4.1 Select All, Clear All & Install Content Options

Option	Description
Select All	This option allows you to quickly enable all OVAL content To use, **right** click in the OVAL content column, and click "Select All Streams"
Clear All	This option allows you to quickly disable all OVAL content To use, **right** click in the OVAL content column, and click "Clear All Selected Streams"
Install OVAL Content	This feature allows the user to install OVAL content files to the <SCC Install>\Resources\OVAL_Content directory. To use, click the “Install Content” button and browse to an OVAL XML file or a ZIP archive containing one or more OVAL XML files; the latter option will install multiple OVAL Content files simultaneously. This feature also allows the user to install OVAL External Variables files to the <SCC Install>\Resources\External_Variables directory. OVAL External Variables files are distinguished by a file name that ends with “_external-variables.xml,” and are installed in the same fashion as OVAL Content files. They may be installed individually or bundled in a ZIP archive with other OVAL External Variables files and/or OVAL content files. After the OVAL Content files are installed, the OVAL content (based on the file name) should be listed along with the internal date modified and OVAL version. To enable it, click the Enable checkbox.
Display OVAL Version	This dropdown allows you to filter what is displayed on the form based on OVAL version.

8.4.2 Select OVAL Content Options

Option	Description
Enable	This checkbox is used to enable the usage of the OVAL XML file.
OVAL Content	OVAL content is a single OVAL XML file, either manually created, or downloaded from the MITRE OVAL repository.

Delete OVAL Content	This button will delete the OVAL XML file.

8.4.3 Configuring OVAL Content Update Options

1. Click Edit -> OVAL Content
2. Click the Patch Content Update tab

The SCC can be configured to periodically check for updated OVAL vulnerability XML files.

To prevent potential bandwidth issues and fingerprinting of your network, it is highly recommended to use a website on your Intranet to obtain updated patch content.

8.4.3.1 OVAL Content Update Process

1. SCC Determines if the user has selected downloading from an Intranet or Internet website.
2. SCC Checks the user specified Update Frequency against the file modified time of the local copy of the patch content.
3. If the Primary or Secondary Intranet download succeeds, then the Internet download is not attempted, even if the option is enabled.
4. After the patch content XML file has been downloaded, an XML validation is performed to ensure the XML is valid.
5. If the downloaded content is valid and newer than the local copy, then the local copy is replaced.

8.4.3.2 Update Frequency

Option	Description
Download updated OVAL content if local file is older than [] days.	The SCC will check the modified date of each OVAL content file if an OVAL content file is enabled, and the "Perform OVAL Analysis" is enabled. If the date modified of the file is greater than the user specified threshold, then the SCC will attempt to download an updated version from a user specified Intranet or Internet site.

8.4.3.3 Intranet Settings

Option	Description
Download from Intranet Site	This checkbox is used to enable the functionality of downloading patch content from the users local Intranet.
Primary Intranet Site URL (http only)	URL to an HTTP (not HTTPS) website on the users Intranet LAN/WAN. Example: http://yourintranet.gov SCC will then lookup the file names for the OVAL content and attempt to download the local files. http://yourintranet.gov/any-oval-content.xml
Secondary Intranet Site URL (http only)	This is an optional backup URL incase the first local website is not available. This only is performed if the primary Intranet download is not successful.

8.4.3.4 Internet Settings

Option	Description
Download from	This can be any http (not https) based Internet URL, which contains the same file

Internet Site URL	names as the OVAL content installed on the "OVAL Content" form.

8.4.3.5 Default Settings

By default the SCC will not attempt to download OVAL content. It will use the copy which is provided with the SCC installer.

As OVAL vulnerability content at the MITRE repository changes daily it is recommended to either manually replace the OVAL content on a periodic basis, or configure SCC by the use of a local Intranet patch content website.

8.5 Standalone OCIL Usage

Standalone OCIL (Open Checklist Interactive Language) content usage is designed primarily for advanced SCC users, such as content authors who wish to run OCIL content without creating an entire SCAP benchmark. No OCIL content is currently bundled with SCC.

1. Launch the Graphical User Interface of SCC
2. Click Edit -> OCIL Content

The Content Selection form lists all of the OCIL content available to the user. The SCC searches the <SCC Install>\Resources\OCIL_Content directory and subdirectories for OCIL XML files.

Note: OCIL content that is part of a SCAP Stream, such as DISA STIGS, should be installed into the SCAP Content, not in the OCIL content. OCIL content included in a SCAP Stream is designed to work with XCCDF, OVAL and CPE. SCC might be able to process the OCIL file as 'raw OCIL' but unexpected errors may occur.

8.5.1 Select All, Clear All & Install OCIL Content Options

Option	Description
Select All	This option allows the user to quickly enable all OCIL content To use, **right** click in the OCIL content column, and click "Select All Streams"
Clear All	This option allows the user to quickly disable all OCIL content To use, **right** click in the OCIL content column, and click "Clear All Selected Streams"
Install OCIL Content	This feature allows the user to install OCIL Content files to the <SCC Install>\Resources\OCIL_Content directory. To use, just click the “Install Content” button and browse to an OCIL XML file or a ZIP archive containing one or more OCIL XML files; the latter option will install multiple OCIL Content files simultaneously. After the OCIL content files are installed, the OCIL content (based on the file name) should be listed along with the internal date modified and OCIL version. To enable it, click the Enable checkbox.

8.5.2 Select OCIL Content Options

Option	Description
Enable	This checkbox is used to enable the usage of the OCIL content file
OCIL Content	OCIL content is a single OCIL XML file.
Delete OCIL Content	This button will delete the OCIL content file.

8.6 SSH Result Copying Options

SCC, starting with release 3.1, has the ability to copy results after each scan via SSH to a centralized server for easier data collection. This feature is disabled by default. To enable:

1. Launch the Graphical User Interface of SCC
2. Click Edit -> SSH Options
3. Enable File Transfer
4. Select Reports to Transfer
5. Enter Hostname or IP Address
6. Enter credentials
7. Enter remote SSH directory
8. Click Test Connection
9. Click Save

Note: SSHv2 is supported, SSHv1 is not.

8.6.1 File Transfer Options

- Enable - Enables transferring of result files via SSH
- Disable - Disables file transfer

- Reports To Transfer - Enables coping of results/reports
  - XML
  - HTML
  - Text

- Delete Local Results After Transfer
  - On - Deletes local results after transferring via SSH
  - Off - Leaves local data after transferring data

8.6.2 Server Information

Option	Description
Hostname/IP Address	Enter the DNS hostname or IP Address of the SSH server to copy result to
Port	Enter the port which the SSH server is listening (normally 22)

8.6.3 SSH User Information

Option	Description
Username/Password	Select this option if you plan to authenticate with username/password combination
Private Key/Passphrase	Select this option if you plan to authenticate with a private key. Note: SCC only supports private keys that are secured with a private key passphrase
SSH Username	Required for either Username/Password or Private key authentication
User Password	Only required if Username/Password authentication has been selected
User Private Key	Only required if Private Key/Passphrase authentication has been selected
Private Key Passphrase	Only required if Private Key/Passphrase authentication has been selected

8.6.4 Directory Information

Option	Description
Local Results Directory	Read only field which shows where local data is stored.
Remote SSH Directory	Enter the full path on the remote SSH server, which SCC should copy results. Example: /export/home/scc/ If this field is left blank, it will default to the user's home directory.

8.7 Editing OVAL Processing Options

This set of options allows SCC to process currently available content in an efficient and accurate manner, however it does not comply with the letter of the law when it comes to the OVAL standard. Previous releases of SCC (1.0 - 3.0.x) ignored these OVAL directives, but they are now offered up as options, should end users want to comply completely with the OVAL standards.

Note: Disabling any of these items could cause a dramatic slowdown in SCC's processing of SCAP content, and could cause certain SCAP content to return false positives.

8.7.1 Ignore Remote File Systems

This option will ignore remote file systems, such as Windows shares, and UNIX NFS mount points. This option could be specified in the SCAP content as well, but in all of the publicly available SCAP content to date, the content authors have not specified to skip scanning of remote file systems.

If this option is disabled, and the SCAP content does not specify to exclude remote file systems, SCC will scan all drives/mount points on the system, and will likely cause the application to slow down, dramatically in certain cases, and the results will potentially include issues from the server hosting the remote files.

Until SCAP content is updated to ignore remote file systems, it is recommended to keep this option enabled in SCC.

8.7.2 Item Creation Threshold

In certain circumstances, a combination of content issues, or system configuration can cause large numbers of OVAL items to be created. This causes two primary issues, the first being SCC's memory and CPU usage during the scan will increase, potentially to the point of crashing. Secondly, if SCC is able to complete the scan, the resulting XML files will be too large to create any Text or HTML reports from.

This option caps the number of OVAL items created, on a per OVAL test basis, to the number specified in the form. This option can be updated by the user depending on their preference. If SCC runs out of memory and crashes even with this option enabled, it is recommended to lower the threshold by a sizable amount and re-run.

If SCC reaches the threshold for a single test, the end result of the test will be 'error' as SCC will skip processing any additional items, and will not be able to make a final determination of compliance with regards to pass/fail, and the end user will likely need to perform the check manually to determine true compliance.

This should not be a common occurrence, and the content author may need to be contacted, to determine if the test can be written in a method which does not create such a large volume of results.

This option is enabled by default.

8.7.3 Ignore Case

This option will ignore case for all Windows OVAL tests, which may prevent certain false positives in SCAP content. This option could be specified in SCAP content, but currently many SCAP content authors have assumed that since the Windows operating system is case insensitive, that OVAL was as well.

Until SCAP content is updated to ignore case on Windows, it is recommended to keep this option enabled in SCC.

8.8 Running SCC as a Service

This section of the manual is only applicable to installations of SCC on Windows. Automated command line usage of SCC on Linux, Solaris and Mac OS X is possible, but requires end users to script the command line interface by methods such as cron.

Installing SCC as a service, is completely optional, and only provided to allow easier automated scanning. It is recommended to configure sending results via SSH with running SCC as a service, to automate data collection as well. Refer to the SSH section for instructions on its usage.

8.8.1 Installing the SCC Service

During the installation of SCC on Windows, the installer provides an option to install the SCC Service component. If this was not selected at install, re-install the software and enable this option.

8.8.2 Configuring the SCC Service

The SCC Service installation contains a graphical editor for configuring the SCC service options. To use click:

Start -> Programs -> SCAP Compliance Checker 3.1 -> SCC Service Options Editor

Note: Configuring the SCC service requires local administrator rights.

8.8.2.1 Service Status

This option displays the current status of the service. However this does not indicate that the SCC application is actively scanning the computer, just that the service itself is running.

To start or stop the service click Enable/Disable.

8.8.2.1 Scan Scheduling

This option allows the frequency at which SCC should perform scans, based on the options specified on this form.

Last Scan: Displays the date/time of the last scan performed by SCC as a service
Next Scan: Displays the date/time of the next scheduled scan, assuming the SCC service is Enabled and running.

Below are the user configurable options for scheduling scans:

- **Custom** (Number of Hours) Enter a numeric value say N (1-1000 etc..) for the frequency to at which SCC should scan. SCC will then scan the computer every N hours.
- **Hourly** - SCC will scan once per hour.
- **Daily** - SCC will scan once per day.
- **Weekly** - SCC will scan once per week.
- **Monthly** - SCC will scan once per month.

8.8.2.2 Other Options

All of the remaining options available for configuration are the same as SCC's options and include Reports, File Types, Logging, SCAP Content, OVAL Content, SSH Options. Refer to 'Using the Software via GUI' for documentation for each option.

Note: The options saved for the SCC service will not have any impact on the graphical usage of SCC or vise versa.

8.8.2.3 Files/processes used in the SCC Service

The following process will appear in the process table, and will be running in the background:
SCC_Service.exe

Depending on the scan frequency, periodically, the command line version of SCC will also be present in the process table: cscc.exe

9. FREQUENTLY ASKED QUESTIONS (FAQS)

9.1 WHAT IS SCAP/FDCC/USGCB AND WHY DO I NEED TO REPORT COMPLIANCE WITH IT?

The Security Content Automation Protocol (SCAP) is a method for using specified standards to enable automated vulnerability management, measurement, and policy compliance evaluation.

The Federal Desktop Core Configuration (FDCC) is a set of configuration settings for Windows XP and Vista which has been mandated by the Office of Management and Budget (OMB) for all government agencies. Additionally, all government agencies must use SCAP validated tools with FDCC Scanner capabilities to certify compliance with the FDCC standards.

Refer to the SCAP Implementation section for additional information.

9.2 WHERE CAN I FIND OUT MORE INFORMATION REGARDING FDCC AND SCAP?

NIST has a detailed page regarding FDCC Technical FAQ's that can be very helpful.

http://nvd.nist.gov/fdcc/fdcc_faq.cfm

9.3 IS THE SCC OFFICIALLY SCAP VALIDATED?

Yes. The SCAP Compliance Checker version 1.0 was officially SCAP Validated on February 25, 2009 to SCAP version 1.0.

http://nvd.nist.gov/validation_spawar.cfm

The SCAP validation is listed as expired as of December 31, 2010, however in email discussions with NIST in December 2011, they have agreed to leave our validation up on the website, since the SCAP 1.1 validation process was never established.

In 2013, SCC will be validated against SCAP 1.2.

9.4 HOW DOES THE SOFTWARE USE THE SCAP XML FILES TO PERFORM CHECKS AND CREATE REPORTS?

The SCAP Compliance Checker uses the SCAP XML files to perform checks. The XML files are read into the software, and the checks are performed exactly as specified by the content. The pass/fail status, method for checking, and all text reported in the reports is pulled directly from the XML content.

Refer to the SCAP Implementation section for additional information.

9.5 WHY ARE THE DETAILED RESULTS IN THE REPORTS LONG AND COMPLICATED?

The results are based on the SCAP content, which is very specific in the method for testing the results, which makes creating detailed, but easily understandable reports a challenge. If you have suggestions on report format improvements, please provide us with recommendations.

9.6 WHY DO SOME CHECKS HAVE MULTIPLE PASS/FAIL CHECKS?

Many of the requirements in the SCAP content contain several requirements such as the OS = 5.1 (XP), some registry keys must exist, and the registry value must be equal to a specified value. Additionally, some of the requirements allow for multiple settings, such as a registry key value must be greater than 900 or equal to -1.

9.7 I THINK A CHECK IS REPORTING INCORRECTLY. IS THIS DUE TO THE SCC OR THE SCAP CONTENT?

This will need to be determined on a case-by-case basis, as false positive and false negatives could be due to faulty SCAP content or from a bug in the SCC software.

Please report your issue along with the detailed HTML files for analysis.

9.8 IF THERE IS AN ISSUE WITH THE SCAP CONTENT, WHAT CAN BE DONE TO RESOLVE IT?

Since the SCAP Compliance Checker is required to use SCAP content for all of the compliance checks, there is nothing that can be done with the SCC to resolve this issue. It may be possible to manually edit the SCAP content to resolve the problem, but the long term solution will be to obtain revised content from the original content author.

9.9 HOW CAN I REPORT AN ISSUE WITH USGCB SCAP CONTENT TO NIST?

Since any issue with a check could be due to an issue with the SCAP content or the SCAP Compliance Checker, we ask that you report issues directly to us. We can confirm if there are SCAP issues and report them to NIST.

However, should you want to report an issue directly to NIST, issues can be reported by sending an email to: usgcb@nist.gov

9.10 WHAT IS THE "WEIGHT" LISTED IN THE REPORTS?

The weights are included in the NIST SCAP content and are based on CVSS.

http://www.first.org/cvss/cvss-guide.html

9.11 DOES THIS SOFTWARE "FIX" ANY OF THE SETTINGS TO BE COMPLIANT WITH FDCC/USGCB/DISA/ETC?

No. This software only analyzes the system, it does not modify any setting.

9.12 DO DEVIATIONS APPLY TO PREVIOUS OR FUTURE REVIEWS?

Deviations only apply to future reviews, and are applied at review time. If a deviation entered today for a specific requirement, all future reviews will have this deviation applied.

9.13 WHY DO NON-PRODUCTION VERSIONS OF THIS SOFTWARE EXPIRE AFTER A SET NUMBER OF DAYS?

Per requirements from the agency that funded the development of SCC, the non-production release versions (Dev, Alpha, Beta, Release Candidate) should expire after a fixed number of days, normally 90. This is to ensure that all users enterprise wide are running the same, current production release of the software.

During the development cycle, new non-productions releases are created at least once a month if not more often. The software expiration ensures that all software testers are using the latest code, and also prevents most production usage of an application that may not be ready for productions use.

9.14 WHY DOES THE SCC NOT PERFORM CHECKS FROM SELECTED SCAP CONTENT AGAINST ALL TARGET SYSTEMS?

The SCC uses the CPE OVAL definitions located in the SCAP content files to determine if the SCAP stream is applicable to the target system.

9.15 IS IT POSSIBLE TO WRITE CUSTOM SCAP CONTENT AND USE IT WITH SCC?

Yes, although creating content is not a trivial process.

9.16 WHERE CAN I LEARN MORE ABOUT CREATING SCAP CONTENT?

http://csrc.nist.gov/publications/PubsSPs.html - (SP800-126 and SP 800-117)

http://oval.mitre.org/ - OVAL

http://oval.mitre.org/language/version5.10/index.html#downloads – OVAL documentation

http://oval.mitre.org/repository/data/AdvancedSearch.jsp - OVAL Repository Search

http://scap.nist.gov/specifications/xccdf/ - XCCDF documentation

9.17 ARE THERE ANY TOOLS AVAILABLE FOR CREATING SCAP CONTENT?

Yes, although many are still in development, and may not be 100% feature complete.

The Enhanced SCAP Editor (eSCAPe) from G2:

http://www.g2-inc.com/escape

Benchmark Editor from MITRE:

http://benchmarkeditor.mitre.org

Microsoft Security Compliance Manager (SCM):

http://technet.microsoft.com/en-us/library/cc677002.aspx

See FAQ 9.28 for caveats.

9.18 ARE THERE ANY TOOLS AVAILABLE FOR CHECKING CONTENT FOR VALIDITY/CORRECTNESS?

Yes.

SCAP Content Validation Tool from NIST

http://scap.nist.gove/revision/1.0/index.html#tools

9.19 HOW DOES SCC PROCESS A SCAP CONTENT STREAM?

SCC follows the Use Case Requirements in NIST 800-126 which document the following:

Component	Stream Locator	Required/Optional
XCCDF Benchmark	xxxx-xccdf.xml	Required
OVAL Compliance	xxxx-oval.xml	Required
OVAL Patch	xxxx-patches.xml	Optional
CPE Dictionary	xxxx-cpe-dictionary.xml	Required
CPE Inventory	xxxx-cpe-oval.xml	Required

Where "xxxx" indicates the SCAP stream name, which must be consistent across all files in the SCAP Stream.

From 800-126: "The notation "xxxx" designates a locator prefix that SHALL be associated with a use case specific data source component stream.

The SCC order of operations with a SCAP stream is as follows, and the USGCB 2.0.0.0 Windows XP Stream is used as an example. SCAP Stream Name = "USGCB-Windows-XP"

1. SCC verifies if the XCCDF Benchmark, OVAL Compliance, CPE Dictionary and the CPE Inventory exist for the specified SCAP stream.

USGCB-Windows-XP-xccdf.xml
USGCB-Windows-XP-oval.xml
USGCB-Windows-XP-cpe-dictionary.xml
USGCB-Windows-XP-cpe-oval.xml

2. If all required files are present, SCC then loads the XCCDF file to gather platform information.

USGCB-Windows-XP-xccdf.xml

3. Based on the Profile that was selected in the options form, the SCC then finds the matching profile, and then checks to ensure the profile is not an abstract profile. (<Profile> element doesn't have an "abstract" attribute or the attribute is set to "false".)

united_states_government_configuration_baseline_version_2.0.0.0

4. Next the CPE Dictionary is processed. The platform element from the XCCDF is used to determine what CPE items the target system is part of.

USGCB-Windows-XP-cpe-oval.xml
USGCB-Windows-XP-cpe-dictionary.xml

5. If the content is applicable to the target computer based on the CPE OVAL tests, the XCCDF content is then traversed and loads the OVAL file and/or the OVAL patches files (from filename) and definitions are processed. The definitions that get processed come from the XCCDF rules found during the XCCDF traversal.

USGCB-Windows-XP-oval.xml
USGCB-Windows-XP-patches.xml

6. XML results are created, based on user settings in the options form of the GUI or the --config from the command line.

<Computer>_SCC_3.1_<Date-Time>_OVAL-CPE-Results_USGCB-Windows-XP.xml
<Computer>_SCC_3.1_<Date-Time>_OVAL-Patch-Results_USGCB-Windows-XP.xml
<Computer>_SCC_3.1_<Date-Time>_OVAL-Results_USGCB-Windows-XP.xml
<Computer>_SCC_3.1_<Date-Time>_OVAL-Variables_USGCB-Windows-XP.xml
<Computer>_SCC_3.1_<Date-Time>_XCCDF-Results_USGCB-Windows-XP.xml

7. HTML and/or text based reports are generated based on end user options, and the installation of the MS XML Parser 6.0.

9.20 CAN SCC PROCESS CONTENT THAT DOES NOT CONTAIN ALL OF THE REQUIRED XML FILES?

Yes. If the CPE-OVAL and the CPE-Dictionary files are missing, SCC will attempt to use default files included with the application. However it is recommended to have a full SCAP stream.

9.21 CAN THE END USER INSTALL OTHER OVAL CONTENT?

Yes. The SCC can process any content designed with OVAL specifications 5.10.1 or prior. Additionally, it is possible to download OVAL content directly from the OVAL repository, which can be installed and used by SCC.

http://oval.mitre.org/repository

9.22 CAN THE SOFTWARE RUN DIRECTLY FROM A CD-ROM?

On Windows: Yes
On Linux, Solaris & Mac OS X: No

For Windows:

> To use from a CD-ROM, just install the software to your hard drive and burn the resulting installation directory to a blank CD-R.
>
> > Ex: C:\Program Files\SCAP Compliance Checker 3.1
>
> If you need to install or update any SCAP or OVAL content, make sure to do this before you burn to CD-ROM, as only the content on the CD-ROM will be available.
>
> The results will be saved by default to your user temp directory, but can be changed in the preferences form to any directory on the system.

For Linux, Solaris & Mac OS X:

> The recommended method is to extract the software from the tar.gz file to a temporary directory on the system, run the application, and then remove delete the software.

9.23 CAN THE SOFTWARE RUN DIRECTLY FROM A USB THUMB DRIVE?

Yes.

To use from a thumb drive, just install the software and copy the resulting installation directory to the USB Drive

> Ex: C:\Program Files\SCAP Compliance Checker 3.1

If the USB Drive is set as Read Only, the software will treat it as a CD-ROM, and will save the results to a local temp directory. If you are able to write to the USB Drive, the software should function as normal when running from USB, although performance will be slower.

Note: As the DOD does not allow any USB drives, we have not tested this method.

9.24 WHAT IS CYBERSCOPE AND WHO WOULD CREATE A CYBERSCOPE AUTOFEED REPORT?

http://scap.nist.gov/use-case/cyberscope/

CyberScope is a secure online portal used by federal agencies for compliance reporting. The system can accept manual and automated compliance (FISMA) input.

In October 2009, the US federal Office of Management and Budget (OMB) released CyberScope, a reporting tool for federal agencies. Under the FISMA (the Federal Information Security Management Act of 2002), agencies are obliged to report on their information security statuses.

The Department of Homeland Security operates the web site on behalf of OMB. Its use as the sole reporting mechanism for FISMA was mandated in FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy on April 21, 209.

The introduction of CyberScope is closely tied to a directive by NIST requiring that FISMA compliance be supported by agency-level programs for continuous infrastructure monitoring. NIST Special Publication 800-137 established a goal of near real-time insight into the security status of IT infrastructures so corrections can be made quickly when systems fall out of compliance. NIST data models use the underlying Security Content Automation Protocol (SCAP) primitives including common vulnerabilities and exposures (CVE), common configuration enumeration (CCE) and common platform enumeration (CPE) to produce data feeds from security management tools that can be sent directly into CyberScope.

Users who are responsible for reporting their Federal Information Security Management Act (FISMA) results for an agency, department or enclave would be the target audience for this functionality.

If you have specific questions on Cyberscope, please contact the Cyberscope Help Desk:
cyberscopehelp@usdoj.gov

9.25 HOW CAN I USE THE XML RESULTS FROM SCC WITH DOD VMS?

SCC, and all SCAP validated applications create SCAP required XML results (XCCDF and OVAL). The SCAP XML results are not directly supported by the DOD Vulnerability Management System (VMS), but can be converted to VMS format by using the DISA developed STIG Viewer. The STIG Viewer can read in XCCDF source STIG policies and XCCDF results from SCAP Validated applications.

For additional information regarding the STIG Viewer:
http://iase.disa.mil/stigs/stig_viewing_guidance.html

9.26 HOW CAN I USE THE RUNAS (SECONDARY LOGON) WITH THIS APPLICATION?

Background: Why would a user need to do this?

If a user is logged on a non-administrative account or to one domain and wishes to review computers in a different domain, the use of the RunAs command can allow the user to complete this task without having to logon to the computer as domain administrator of the target domain.

Option 1: Run via Start Menu Shortcut as privileged user

1. Click Start -> Programs -> SCAP Compliance Checker 3.1 -> then Right click on SCAP Compliance Checker.
2. Click on “RunAs”.
3. Type the "Domain\Username" and "Password", and then Click "OK".

Option 2: Run Command Prompt as a privileged user

1. Open the command prompt as another user and then run the application from the installation directory from the command prompt.

```
RunAs /env /user:domain_name\username "cmd"
```

A new command window will appear with a header of cmd (running as domain_name\username)

2. Change the directory to the installation directory.

```
c:  (or drive application is installed to)
cd\
cd "Program files\SCAP Compliance Checker 3.1" (Install Folder)
```

3. Run the application

```
SCC.exe
or
CSCC.exe
```

OS Requirements:

- For Windows XP/2003 the Secondary Logon Service must be running.
- For Windows 2000 the RunAs Service must be running.

Known Issue:

- The feature in the SCC software which opens the results directory (Results -> Open Results Directory) will not function as expected when running via RunAs. The Windows Explorer cannot be called while running from RunAs, this is a limitation of Microsoft Windows.

9.27 WHAT TYPE OF NETWORK TRAFFIC CAN I EXPECT TO SEE AS A RESULT OF A REMOTE SCC SCAN?

SCC performs a variety of system calls as it attempts to perform compliance checks from the SCAP XML content. If the target computer is a remote computer, the SCC will generate network traffic to perform the checks. The volume and variety of network traffic will be dependant on the XML content, however, below is a list of various types of network traffic you can expect to see as a result of running SCC with the default USGCB SCAP content included in the SCC installer.

- ICMP Echo (ping) requests/replies
- TCP NBSS session requests
- TCP SMB AndX requests/responses
- TCP WINREG OpenKey/CloseKey requests/responses
- TCP IOXIDRes ServerAlive requests/responses

10. TROUBLESHOOTING

There are several issues that can prevent the SCC from successfully reviewing a computer, especially remote reviews over a LAN or WAN connection. Below are some basic troubleshooting suggestions.

10.1 VERIFY SCANNING AND TARGET COMPUTER ARE IN THE SAME ACTIVE DIRECTORY DOMAIN

SCC only officially supports remote authenticated scanning of computers in the same domain. Certain tests require the usage of WMI calls, which only work when both computers are in the same domain. Certain content that does not require WMI may work correctly across domains, but most SCAP content such as USGCB and DISA will have several checks that will be unable to obtain information, and will error out if attempted from one Active Directory Domain to another.

10.2 ENSURE NECESSARY SERVICES ARE ENABLED AND RUNNING

The Server Service, Remote Registry and Windows Management Instrumentation (WMI) are required for the SCC to run. Additionally DCOM is required if the content contains any WuaUpdateSearcher OVAL tests.

10.3 ENSURE A CLIENT FIREWALL IS NOT BLOCKING THE REGISTRY, SHARES OR WMI

If a client firewall is blocking LAN/WAN access to the Remote Registry, File Shares or WMI, remote reviews with SCC will not possible. Enabling these port exceptions will vary for each firewall product. Please refer to your firewall software documentation regarding opening specific ports.

10.4 VERIFY ADMINISTRATIVE RIGHTS

This issue should only occur for a user wanting to review a computer that is not part of a domain for which that person is a domain administrator. In order to attain local administrative rights on a single remote computer, the user may need to map an administrative share or connect to the remote registry of that system.

10.5 VERIFY "MANAGE AUDITING AND SECURITY LOG" USER RIGHT CONTAINS THE ADMINISTRATORS GROUP

On Windows Vista and later, SCC uses the auditpol.exe application to obtain the system's audit configuration. In order to run this command, the user running the software must have the User Right, "Manage auditing and security log". By system default, the Administrators group is a member of this right. However, if the security setting is modified and the Administrators group is removed, errors will be reported, any check related to the Windows 'Audit Policy' will error out.

10.6 TESTING CONNECTIONS

If SCC is unable to perform a remote review of a system, please perform the following tests before reporting any issues.

10.6.1 Map an Administrative Share

To map an administrative share to a target computer:

1. Right Click on My Computer.
2. Click on Map Network Drive. The Map Network Drive window will open.
3. In the Folder field, type in the drive you are wishing to access, most likely the C drive.
   \\servername\C$
4. Deselect the “Reconnect at logon” option.
5. Click on Finish.

6. If prompted to enter Username and Password, do so using an account with administrative rights on that system.

10.6.2 Remotely Connect to a Computer's Registry

To Remotely Connect to Computer's Registry:
1. Click on Start – Run. The Run window will open.
2. Type in Regedit and click OK. The Registry Editor will open.
3. Select File – Connect Network Registry…
4. Type in the NetBIOS computer name in the window provided. Select OK.
5. If prompted to enter Username and Password, do so using an account with administrative rights on that system.

10.6.3 Testing the WMI Connection

Several checks in the USGCB SCAP content required WMI queries to verify data. If any checks are listed as error, it could be due to WMI configuration issues on the target computer. To test the WMI connection, perform the following:

1. Click Start -> Run.
2. Type mmc.exe.
3. Click File - > Add/Remove Snap-In.
4. Click the Add button.
5. Scroll Down to WMI Control and Click on it.
6. Click the Add button.
7. Click the radio button next to "Another Computer".
8. Type the computer you want to test.
9. Click Finish.
10. Click Close.
11. Click OK.
12. Right Click on WMI Control for <Computername>.
13. Click Properties.
14. If the General Tab states "Successfully Connected to: \\<Computername>, then a WMI based review should be possible.
15. If any errors are listed on this tab, the troubleshooting is outside the scope of this manual.

10.6.3.1 Microsoft WMI Links

Below are some links maintained by Microsoft related to WMI.

- WMI FAQ: http://www.microsoft.com/technet/scriptcenter/resources/wmifaq.mspx
- How to enabled DCOM: http://msdn2.microsoft.com/en-us/library/ms687298.aspx

10.6.3.2 Verify 'Restrictions for Unauthenticated RPC Clients Setting' is not set to 'Enabled: Authenticated Without Exception'

Review the following setting: Policies\Administrative Templates\System\Remote Procedure Call "Restrictions for Unauthenticated RPC Clients". This can be set to either "Not Configured" (default) or "Enabled: Authenticated". If it is set to the highest setting "Enabled: Authenticated Without Exception" we have seen instances where this will no longer allow review of a system via WMI.

10.6.4 Test DCOM connections

The easiest way to test remote DCOM connections may be to run SCC with any WuaUpdateSearcher content, and review the errorlog. Additionally, there is a DCOM testing tool available from Microsoft.

http://support.microsoft.com/kb/259011

10.6.5 Test ability to run auditpol.exe

To test run the following command, which should return back all of the audit configuration of the local computer:

```
Auditpol /get /category:*
```

If this returns any error messages, SCC will not be able to check the audit configuration of the computer. In order to allow SCC or most applications to view the audit configuration, the Administrators group will need to be added back to the "Manage auditing and security log" User Right.

10.6.6 Test ability to run Power Shell cmdlets remotely

No publicly available content currently uses the Power Shell cmdlet oval test, so this is only useful if you are running OVAL 5.10 or later content, and have content that uses cmdlet tests.

1. Open an Administrator command prompt
2. Type powershell
3. enter-pssession <targetsystemname>

If any errors occur, you will need to configure both the scanning computer and target computer to allow remote power shell. Refer to the Known Issue related to remote cmdlet usage for additional information.

10.6.7 Re-scan with SCC

If all of the above tests were successful, please re-scan the target computer with SCC.

11. KNOWN ISSUES

11.1 USGCB (WINDOWS XP AND VISTA) SCAP CONTENT ISSUES

Since the SCC uses SCAP XML content to perform all of the compliance checks, issues with check accuracy are often based on issues with SCAP content. As of USGCB SCAP content version 2.0.0.0, the following known issues can occur.

11.1.1 SCAP content does not always allow for more restrictive User Rights and File Permissions to pass

There are many checks that fail if the setting is not set exactly to the SCAP specified setting, even if that setting is the least secure option.

- Deny User Right fail if a superset of user rights are configured
- Several Deny User Rights fail if the built in Support account is renamed or deleted

11.1.2 Some SCAP content requires checks to fail based on case sensitivity

Several checks may fail based on the case sensitivity of registry keys, or the registry values. Since Windows does not utilize case sensitivity, these checks should be allowed to pass.

11.2 USGCB (WINDOWS 7) SCAP CONTENT ISSUES

As of USGCB SCAP content version 1.2.0.0, the following known issues can occur.

11.2.1 SCAP content does not allow for more restrictive User Rights

This is the same issue found in the Windows XP/Vista USGCB content. If the user right is not set exactly to the USGCB setting, it will very likely fail the check based on the tests required in the content.

11.2.2 Several registry key checks fail when set to a more secure value

Several of the requirements in the USGCB mandate the least secure option, and the checks fail if the setting is configured to a more secure value.

11.2.3 Incorrect results with Network access: Allow anonymous SID-Name translation - (CCE-9531-5)

If the target computer is not in a domain, this check will always fail, due to the required RSOP check, which is only possible when joined to an Active Directory domain.

11.3 COMMAND PROMPT CLOSES WHEN RUN WITH UAC

With the update to cscc.exe to automatically elevate to a privileged user, if you run cscc.exe as a standard user, and pass in command line arguments that are invalid, Windows Vista/7 etc.. will spawn a new command prompt as administrator, in which cscc.exe runs. When the application closes, Windows closes this command prompt, and the end user will not be able to see the usage statement.

Example:
Running as a non-administrator:

```
cscc.exe -z
```

Windows will prompt the user with a User Account Control prompt, then open a new command prompt. Since the -z is not a valid parameter, cscc.exe will print the usage statement to the screen, however Windows will close the elevated command prompt before you are able to read it.

Workaround:

1. Open the command prompt as administrator prior to running cscc.exe

11.4 POTENTIAL OUT OF MEMORY CRASHES WITH VERY LARGE OVAL SOURCE FILES

It is not recommended to install OVAL source content larger than 30 MB in size. When loading OVAL source files, it's common for SCC to use 20-30 times the XML file size in RAM. This means that a 20 MB source OVAL XML file could use 400-600 MB of RAM to load and use. When memory usage goes above 1 GB, both system and SCC stability issues may occur.

Source OVAL XML files larger than 10 MB are not include in any SCAP content currently available, but it is possible to download raw OVAL files, such as the entire MITRE OVAL repository that could cause stability issues with SCC.

11.5 WINDOWS EXPLORER DOES NOT OPEN WHEN RUNNING SCC VIA RUNAS

If SCC is run via the RunAs functionality of Windows XP/2003, the Results -> Open Logs Directory, and Results -> Open Results Directory will not open Windows Explorer. This is a limitation of Windows, and there does not appear to be anything the application can do to fix it.

The results are normally stored in the <SCC Install>\Results directory, and the Logs are saved in the <SCC Install>\Logs

11.6 WINDOWS SERVER 2003 DOMAIN CONTROLLER DOS WITH SPECIFIC WMI QUERIES

This issue has not been found in any publicly available content, but was found in our internal testing. If any WMI queries are used against Server 2003 Domain controllers, caution is advised. Below is the issue we found.

Symptom: On Server 2003 (x86 and 64) domain controllers, WMI query for" Select Name from Win32_UserAccount where LocalAccount=True" will hang for hours on end, causing a DoS against that Domain Controller. The issue appears to be related to the "LocalAccount=True" portion of the query..

Workaround: Do not run content that contains a WMI query with "LocalAccount=True" against Server 2003 Domain Controllers.

Fix: Microsoft has an "unpublished" patch that needs to be installed to solve this issue. Patch can be downloaded from http://support.microsoft.com/kb/933593 Once the patch is installed and DC has been rebooted, the check now works without issue

11.7 POTENTIAL MAXIMUM DIRECTORY/FILE LENGTH ISSUES WHEN COPYING SCC RESULTS TO OTHER DIRECTORIES OR NETWORK SHARES.

SCC creates an organizational tree structure of the results from each scan, in order to allow the data to be easier to find by the end user. However, as the directory and file paths contain the SCAP Stream Name, this path can be very long, such as the following example:

C:\Program Files\SCAP Compliance Checker 3.0 Beta1\Results\SCAP\LONG-COMPUTERNAME\U_Windows_7_V1R6_STIG_Benchmar\2\2011-12-23_160049\XML\LONG-COMPUTERNAME_SCC-3.0_Beta1_2011-12-23_160049_OVAL-CPE-Results_U_Windows_7_V1R6_STIG_Benchmark.xml

The path above is 240 characters, which is allowable by the Windows OS, however if a user tries to copy the results to a network share, with a longer starting path, such as

\\somenetworkpath\some-long-sub-directory\some-other-sub-directory\SCAP Compliance Checker 3.0 Beta1\Results\SCAP\LONG-COMPUTERNAME\U_Windows_7_V1R6_STIG_Benchmar\2\2011-12-23_160049\XML\LONG-COMPUTERNAME_SCC-3.0_Beta1_2011-12-23_160049_OVAL-CPE-Results_U_Windows_7_V1R6_STIG_Benchmark.xml

The new path is 290 characters long, which exceeds the limit of 260 set by Windows
http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247%28v=vs.85%29.aspx#maxpath

Several workaround exist for this:

- Only copy the results to a directory path that has less length than the SCC install path
- Only copy the results subdirectory that you need, such as SCAP
- Write a script to copy just the files you need without any directory structure into a flat directory. Since SCC includes the computername, date timestamp and SCAP stream name in the resulting files, the likelihood of conflicts is low.

11.8 ISSUES WHEN SCANNING REMOTE COMPUTER WITH CONTENT THAT CONTAINS WINDOWS CMDLET TESTS

If the SCAP/OVAL content being used contains any cmdlet tests (aka Power Shell, which was added in OVAL 5.10), the following error may occur:

> "Connecting to remote server failed with the following error message : The client cannot connect to the destination specified in the request"

In order to use the cmdlet probe for reviewing a remote windows server, Powershell Remoting must be enabled on both the target and the scanning system. Below is the process required to enable Powershell Remoting:

1. Configure the local scanning computer
Open Powershell with administrative rights and perform the following two commands:

```
Enable-PSRemoting -force
winrm quickconfig
```

2. Test Remote Power Shell Command
Now that your reviewing system is configured to perform remote powershell commands, you can test to see if a target system can be accessed remotely using the following powershell command:

```
enter-pssession <targetsystemname>
```

If that is successful, then you should be able to use SCC with cmdlet content to review target system remotely.

3. Configure remote/target computer to accept remote Powershell connections (if necessary)
If it is not successful you will need to log into target system, open Powershell with administrative rights and perform the following commands:

```
Enable-PSRemoting -force
winrm quickconfig
```

4. Retest Remote Power Shell Command

Now go back to the first scanning system with SCC installed and again attempt the following commend via Powershell:

```
enter-pssession <targetsystemname>
```

This should now be successful and the SCC should now be able to attempt the remote cmdlet check from the local scanning computer to the remote target computer.

11.9 FATAL ERROR WHEN SELECTING ANY FILE LOCATED IN THE WINDOWS 7 OR LATER "LIBRARIES"

If a Host file, or SCAP Content is selected via one of SCC's browse for file dialogs, a fatal error occurs if any file is selected from the "Libraries" location, as it is not a valid full path.

Example: Selecting a Host file from :"Libraries\Documents\test.txt" will cause a fatal error.

However, if a select the same file via the true path of C:\Users\TestUser\Documents\test.txt it works fine.

11.10 WINDOWS REGISTRY PERMISSIONS CHECKS NOT FULLY SUPPORTED ON X64

If any content checks for registry Access Controls Lists (ACL) using the RegKeyEffectiveRights53 OVAL test, and the Windows View is not set to 32 bit, the check will error out. We have not yet found a method which will allow the 32 bit SCC application to obtain the ACL of the 64 bit portions of the Windows registry.

This OVAL test is not frequently used in SCAP content, so may not impact most end users.

11.11 DISA STIG SCAP CONTENT FAILS XML VALIDATION

All of the Windows Operating System STIG SCAP Benchmarks, current at the SCC 3.1 release date of: February 12, 2012, contained XML schema errors in the CPE Dictionary file. If the XML schema validation option is enabled in SCC, errors like the example from Windows 2008 DC will occur:

```
[ERROR] CPE invalid: Failed to load schema, C:\Program Files (x86)\SCAP
Compliance Checker 3.1\Resources\Schemas\cpe-dictionary_2.2.xsd to
validate file: C:\Program Files (x86)\SCAP Compliance Checker
3.1\Resources\Content\U_Windows_2008_DC_V6R1.20_STIG_Benchmark-cpe-
dictionary.xml.  See debug log for more details.

[WARN] Stream <U_Windows_2008_DC_V6R1.20_STIG_Benchmark>. Validation of
input XML has failed. SCAP Checker will attempt to process this stream
but content related errors may occur.
```

From pur testing, these do not impact the accuracy of the results, but should be fixed by DISA in a future release of the STIG SCAP benchmarks.

12. TECHNICAL SUPPORT

Technical support is available if a support contract has been setup between your agency and SPAWAR Atlantic. Please contact your management chain regarding any specific methods for reporting technical issues, and to determine if there is a support contract in place for your agency.

12.1 Point of Contact

To contact SPAWAR directly, please email: ssc_lant-scc@navy.mil

12.2 Software Releases

Users who have contacted SPAWAR at the email address listed above will be notified of software releases via email. Additionally, the latest official release information can be obtained from the following SPAWAR website:

www.public.navy.mil/spawar/Atlantic/ProductsServices/Pages/SCAP.aspx

12.2.1 DISA Hosted Download for DoD users

Department of Defense (DoD) users with a valid Common Access Card (CAC), can download the software directly from the following location:

http://iase.disa.mil/stigs/scap/index.html

Then click on "SCAP Tools", and click on the platform specific release of SCC to download.

13. CREDITS

The development of SCC was funded and developed by a joint effort between the Internal Revenue Service (IRS), National Security Agency (NSA) and SPAWAR.

IRS Cybersecurity Security Policy

- Janice F. Harrison
- Denise Crisco

National Security Agency

- Michael Kinney
- Edward Wienholt
- James K Ronayne

SPAWAR Atlantic

- Jack Vander Pol
- Kyle Stone
- Andy Deese
- Doug Tanner
- Richard Kelly
- Bryan Wilson
- Doug McIlroy

SAIC

- John Ulmer
- William F. Arens
- Brandon Gonzalez
- James Bradley
- Joe McEntire
- Glenn Johnson

And a big 'thank you' to all of our Beta testers, and anyone who has sent us suggestions and feedback on the application!

APPENDIXES

A.1 SCAP Validations

- SCAP Version: 1.0
    - FDCC Scanner
    - SCAP Validation Date: February 25, 2009

A.2 Standards Supported

Standard	Version Supported
SCAP	1.0
OVAL	5.10.1
OCIL	2.0
XCCDF	1.1.4
CPE	2.2
CCE	5.0
DOD ARF	0.41
Cyberscope	DRAFT 1.0.0 Early Access Release

A.3 SCAP Implementation

SCAP (Security Content Automation Protocol) is a suite of standards used to determine the presence of vulnerabilities, patches and configuration issues on a target system. SCAP content consists of machine readable XML files that contain configuration data, checklist data and logic used to scan a system. The standards include CVE (Common Vulnerabilities and Exposures), CCE (Common Configuration Enumeration), CPE (Common Platform Enumeration), XCCDF (eXtensible Configuration Checklist Description Format), OVAL (Open Vulnerability and Assessment Language) and CVSS (Common Vulnerability Scoring System).

SCAP Configuration Checker processes SCAP content on a target system and produces HTML and text reports, XCCDF results and OVAL results. The HTML and text reports provide benchmark scores and information that a system administrator can use to make the target system more secure. The XCCDF results and OVAL results can be used by other tools in a variety of ways since they are generated using the industry standard XCCDF and OVAL results formats.

SCAP Configuration Checker reads in a SCAP stream which includes XML files written in the XCCDF, OVAL and CPE Dictionary schemas. SCAP Configuration Checker then generates XML results files using the XCCDF and OVAL results schemas. The HTML reports are generated by transforming the generated XCCDF and OVAL XML results files into human readable output. This output contains detailed scoring and results information, as well as CVE, CCE and CPE identifiers.

SCAP Configuration Checker is capable of validating SCAP streams against the industry standard XCCDF and OVAL schemas. All output generated by SCAP Configuration Checker can also be validated.

SCAP Compliance Checker was designed specifically to process SCAP content. This includes the USGCB Windows Firewall content (Windows XP, Vista and 7), the Internet Explorer 7 & 8 content, and the Windows XP, Vista and 7 operating system content for Windows, and the USGCB Red Hat Enterprise Linux 5 content for Linux.

SCAP Compliance Checker 3.1 implements SCAP version 1.0.

A.3.1 CVE IMPLEMENTATION

The CVE (Common Vulnerabilities and Exposures) standard links unique identifiers with known security vulnerabilities and/or exposures. CVE identifiers are typically found in the OVAL patch definition content of a SCAP data stream. An OVAL patch definition may contain a reference element that associates the definition with a CVE identifier. Links to various websites containing more information about the vulnerability and/or exposure may also be provided in the reference element.

When the SCAP Compliance Checker processes a SCAP data stream against a target system, any CVE identifiers associated with entities in the stream will be found and provided in the results HTML and text files.

In the SCAP Compliance Checker results HTML files, CVE identifiers can typically be found in the OVAL results HTML file for the patch content. Detailed information on each definition processed can be found in the Definitions section of the HTML file. For each definition, there is a "CVE" row that displays any CVE identifiers that are associated with the definition.

It is important to note that when SCC finds a CVE identifier, it automatically creates a link in the CVE row to the NVD (National Vulnerability Database) webpage for that particular CVE identifier. This allows the user to determine the impact that a particular CVE has based on CVSS impact metrics. This also allows the user to prioritize different vulnerabilities found by comparing vulnerability scores with each other.

A.3.2 CCE IMPLEMENTATION

The CCE (Common Configuration Enumeration) standard links unique identifiers with known system configuration issues.

When the SCAP Compliance Checker processes a SCAP data stream against a target system, any CCE identifiers associated with Rules and/or definitions in the stream will be found and provided in the results HTML files.

CCE identifiers are typically found in the OVAL definition content and the XCCDF content of a SCAP data stream. An OVAL definition may contain a reference element that associates the definition with a CCE identifier. A link to the CCE website containing more information about the system configuration issue is also provided in the reference element. An XCCDF Rule may contain an ident element that associates the Rule with a CCE identifier.

In the SCAP Compliance Checker results HTML files, CCE identifiers can typically be found in the HTML reports. For OVAL results HTML files, detailed information on each definition processed can be found in the Definitions section of the HTML file. For each definition, there is an "Identities" row that displays any CCE identifiers that are associated with the definition, in addition to the CCE identifier.

It is important to note that CCE identifiers in the Detailed Results section of the reports, provides a link to the CCE website to allow the user to gather additional information regarding the configuration issue.

SCAP Compliance Checker 3.1 implements CCE version 5.0, however the Detailed Results section of the reports displays the CCE version 4.0 as well.

A.3.3 CPE IMPLEMENTATION

The CPE (Common Platform Enumeration) standard is a structured naming scheme for hardware, operating systems and applications. It allows different tools to specify names for IT platforms in a consistent way. The XCCDF file included in a typical SCAP data stream contains one or more platform elements. The platform element contains a CPE identifier that associates an XCCDF Benchmark, Rule or Group with a target platform. If the target system is not an instance of the CPE identifier specified in a platform element, then the XCCDF Benchmark, Rule, or Group associated with that platform element is not applicable to the target system and will not be processed.

In order to determine if the target system is an instance of a CPE identifier, SCAP Compliance Checker processes the CPE dictionary and the CPE OVAL content in the SCAP data stream. The CPE dictionary contains one or more CPE identifiers, each associated with an OVAL definition that resides in the CPE OVAL content. If SCAP Compliance Checker processes the OVAL definition and the definition returns a result of "true", then the target system is said to be an instance of the associated CPE identifier. A list of CPE identifiers that the target system is an instance of is compiled in this fashion from the CPE dictionary, then used when processing the XCCDF file. If the CPE identifier specified by a platform element in the XCCDF file is not in the compiled CPE instance list, then the Benchmark, Rule or Group associated with that CPE identifier is not applicable to the target system and will not be processed. Rules that are not applicable to the target system will have a result of "not applicable".

SCAP Compliance Checker 3.1 implements CPE version 2.2.

A.3.4 CVSS IMPLEMENTATION

The CVSS (Common Vulnerability Scoring System) standard is a system used to assign scores to vulnerabilities. By assigning a score to a vulnerability, one can determine its relative severity when compared to other vulnerabilities.

In the SCAP Compliance Checker the CVE identifiers can typically be found in the security patches section of the HTML reports. For each security patch check, there is a "References" row that displays any CVE identifiers that are associated with the definition. Each CVE identifier will have a link to the NVD database webpage for that CVE. Each link can then be used to obtain the CVSS information from

the National Vulnerability Database (NVD) site, including the NIST-calculated CVSS score, the full CVSS vector, and the CVSS calculator.

A.3.5 XCCDF IMPLEMENTATION

XCCDF (Extensible Configuration Checklist Description Format) is a language used for writing security checklists and benchmarks. SCAP Compliance Checker loads XCCDF content from a SCAP stream and determines if the Rules specified by the XCCDF content are satisfied by a target system.

SCAP Compliance Checker validates XCCDF content, imports it and allows the user to select a profile from the content. Rules are automatically selected and unselected based on the profile the user selects.

The SCAP stream's CPE dictionary and its associated OVAL definitions are then processed to determine which XCCDF Rules are applicable to the target system. Rules that are found to be inapplicable to the target system based on CPE identifiers are automatically unselected.

SCAP Compliance Checker then traverses the XCCDF content, processing all selected XCCDF Rules against a target system. Scores are calculated using all of the current XCCDF scoring models including the default, flat, flat unweighted and absolute models. Additionally two custom scoring methods are calculated, the spawar-original and spawar-adjusted.

A benchmark results XML document is generated using the XCCDF Results schema. This results file is then transformed into an HTML report, along with more in depth reports generated from the SCAP stream's OVAL content. The benchmark results XML document can be imported into other tools since it uses the industry standard XCCDF Results schema.

SCAP Compliance Checker 3.1 implements XCCDF version 1.1.4.

http://scap.nist.gov/specifications/xccdf/index.html#resource-1.1.4

A.3.6 OVAL IMPLEMENTATION

OVAL (Open Vulnerability and Assessment Language) is a language used to standardize the transfer of security content among different tools. SCAP Compliance Checker loads OVAL content in conjunction with an XCCDF checklist and processes the OVAL definition content against a target system.

SCAP Compliance Checker is able to process all four of OVAL's schemas: the Definitions schema, the System Characteristics schema, the Results schema and the Variables schema.

The Definitions schema is used to define definitions that test a machine's state. This schema is used in SCAP streams to specify patch, vulnerability and configuration content. SCAP Compliance Checker imports OVAL Definitions files and processes the OVAL definitions against a target system.

The System Characteristics schema is used to store data collected from a system. SCAP Compliance Checker uses Object data from OVAL Definitions content and generates System Characteristics data that is later used for testing purposes. This data is stored in an XML file using the OVAL System Characteristics schema.

The Results schema takes State data from OVAL Definitions content along with System Characteristics data and produces Definition and Test results. These results are stored in an XML file that follows the OVAL Results schema. SCAP Compliance Checker then transforms this XML file and produces human readable HTML report documents.

The Variables schema is used to import external variable data into the OVAL engine during processing of an OVAL definition. SCAP Compliance Checker processes the XCCDF content of a SCAP stream and extracts any variables that need to be imported into the OVAL engine. It then creates an XML file using

the OVAL Variables schema that contains these variables. The OVAL engine later uses this file during OVAL processing.

By using the industry standard OVAL schemas, SCAP Compliance Checker can share data with any tool that understands OVAL.

SCAP Compliance Checker 3.1 implements OVAL version 5.10.1.

http://oval.mitre.org/language/version5.10.1/

A.3.7 OCIL IMPLEMENTATION

The Open Checklist Interactive Language (OCIL) defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions. SCAP Compliance Checker loads OCIL content in conjunction with an XCCDF checklist and processes the OCIL questionnaires against a target system. SCAP Compliance Checker can also process OCIL outside of a SCAP 1.1 data stream.

SCAP Compliance Checker 3.1 implements OCIL version 2.0

http://scap.nist.gov/specifications/ocil/

A.4 OVAL Probes Supported by SCC 3.1 for Windows

The following OVAL probes are supported in the Windows version of SCC. For probe support on other platforms, please refer to the platform specific documentation for each release of SCC.

- **Apache**
  - httpd
- **Independent**
  - EnvironmentVariable
  - EnvironmentVariable58
  - Family
  - FileHash
  - FileHash58
  - LDAP
  - SQL
  - SQL57
  - TextFileContent
  - TextFileContent54
  - Variable
  - XMLFileContent
- **Windows**
  - AccessToken
  - ActiveDirectory
  - ActiveDirectory57
  - AuditEventPolicy
  - AuditEventPolicySubCategories
  - cmdlet
  - DnsCache
  - File
  - FileAuditedPermissions53
  - FileEffectiveRights53
  - Group
  - Group_SID
  - Interface
  - LockoutPolicy
  - Metabase
  - PasswordPolicy
  - Port
  - PrinterEffectiveRights
  - Process
  - Process58
  - Registry
  - RegKeyAuditedPermissions53
  - RegKeyEffectiveRights53*
  - Service
  - ServiceEffectiveRights
  - SharedResource
  - SID
  - SID_SID
  - UAC
  - User
  - User_SID55

- UserSID
- Volume
- WMI
- WMI57
- WuaUpdateSearcher

* RegKeyEffectiveRights53 is not currently supported for x64 Windows, unless the 32 bit view is specified in the content.

A.4.1 SQL DATABASE MANAGEMENT SYSTEM SUPPORT

SCC supports reviews against the following SQL database configurations:

Database Management System	Windows 2003 and Later	Solaris	Red Hat Enterprise Linux	Debian Linux
Microsoft SQL Server 2000 and Later	Yes			
Oracle Database 10g and 11g, Enterprise Edition		Yes	Yes	Yes
Oracle Database 10g and 11g, Express Edition		Yes	Yes	Yes

Local review capability is available for supported Oracle Database installations while local and remote review capabilities are available for supported Microsoft SQL Server installations.

A.4.2 SCAP CONTENT AUTHOR NOTE ON SQL AND SQL57 IMPLEMENTATION IN SCC

SCC can recognize several common representations of the SQL Server and Oracle Database versions it supports. Such representations include chronological (SQL Server: 2005, 2008, 2008 R2; Oracle DB: 10g, 11g), short numerical (SQL Server: 9.0, 10.0; Oracle DB: 10, 11), and long numerical (SQL Server: 9.00.x, 10.00.x, 10.05.x; Oracle DB: 10.1, 11.2.0.x). Declaring multiple versions in a pattern match operation (e.g. "2005|2008", "10g|11g", or ".*") will enable SCC to concurrently analyze instances from all matching and supported versions of SQL Server or Oracle Database installed on the target system.

SCC's handling of the "connection_string" element does not treat it as a literal connection string. Rather, it is treated as a form for specifying which instances and, if reviewing a SQL Server installation, databases on the target system should be inspected. Disregarding the quotation marks, it has one required field, "server=<instance>" where <instance> is a literal instance name or a regular expression, and one optional field, "database=<database>" where <database> is a literal database name or a regular expression. When both fields are declared, they are separated by a semicolon (;). When reviewing a SQL Server installation, declaring the "server" field as "server=MSSQLServer" will enable SCC to submit database queries against the default instance. Omitting the "database" field for a SQL Server review will cause all queries to be submitted against the default database of the specified instance(s). When reviewing an Oracle Database installation, any database declaration in the "connection_string" entity will be ignored since it would not be applicable to the Oracle Database review process. Leveraging the pattern match operation of the "connection_string" element allows SCC to analyze multiple instances and multiple matching databases, where applicable, on each instance with a single SQL or SQL57 OVAL probe.

Due to SCC's dependency upon the Oracle SQL*Plus utility for conducting Oracle Database reviews, any SQL queries specified by Oracle Database specific OVAL probes are limited to a length of 257 characters.

A.5 List of Files and Registry keys

A.5.1 FILES INSTALLED BY THE SCC

File	Description
scc.exe	Graphical User Interface to the SCC
cscc.exe	Command Line Interface to the SCC
hosts.txt	Sample host file
uninstall.exe	Uninstaller for this application
Documentation\ReleaseNotes.txt	Summary of changes for this version of the software.
Documentation\SCC_Help.chm	Compiled, searchable help file
Documentation\SCC_UserManual.pdf	PDF version of the User Manual
Documentation\TermsOfUse.txt	Text file containing the Usage, which is displayed during the installation.
Resources\Content*	Contains any SCAP content included with the installer or installed by the end user with the Install SCAP Content feature.
Resources\DefaultFiles	Contains default files used by the SCC
Resources\Deviations*.xml	Contains any user created deviations
Resources\Graphics*	Images and icons used with SCC.exe
Resources\OCIL_Content	Contains any stand alone OCIL content included with the installer or installed by the end user with the Install OCIL Content feature.
Resources\OVAL_Content	Contains any OVAL vulnerability content included with the installer or installed by the end user with the Install OVAL Content feature.
Resources\Schema*	Files used to validate the SCAP XML content
Resources\Thresholds*.xml	Contains the default and any user customized compliance thresholds
Resources\Transforms*	Files used to create the HTML and text reports from the OVAL and XCCDF XML results
Documents and Settings\All Users\Start Menu\Programs\SCAP Compliance Checker 3.1	Start menu icons created during the installation process

A.5.2 REGISTRY KEYS CREATED DURING SCC INSTALLATION

Registry Key	Description
HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\SCAP Compliance Checker 3.1	Standard uninstall information which allows the Add/Remove Programs to remove the SCAP Compliance Checker software.

3 FILES CREATED DURING SOFTWARE EXECUTION

File	Description
<User Defined Directory>\Results Refer to Data Directory option in "Editing Options" for details.	XML, HTML and Text based results created during a review

<User Defined Directory>\Logs Refer to Data Directory option in "Editing Options" for details.	Screen, Error and Debug logs that could be created during a review depending on user preferences.
<SCC Install>\options.xml	Configurable settings from the SCC.exe
<SCC Install>\Temp	Temporary files created during SCC execution
%Temp%\pdk-<username> or %SystemRoot%\Temp\pdk-system	Temporary files used by the SCC.exe and CSCC.exe during software execution.

A.6 Debugging

A.6.1 SCC Debug Introduction

The debug file(s) contains information produced by the application and consists of DEBUG, ERROR, NOTICE, INFO and WARNING categories. If the application is work as expected the only entries would be DEBUG and NOTICE, where DEBUG is the most frequent entry.

Log files are inherently large because the system is communicating all the events, providing the developer with as complete of a description as possible. The sizes of these files, however, are limited to 20MB, and this setting is specified in the options.xml MaxLogFileSize entry. We recommend keeping the 20MB limit although decreasing the limit might be more advantages for sharing these log files with the development team.

As the file reaches the 20MB threshold a new file is created that the system writes too. The files are differentiated by a trailing sequence number (SEQNUM) starting at 001 and concluding when the application terminates, and no more messages are written to the file(s).

A good assumption when specifying the application to create debug files is that the larger the SCAP content the greater quantity of debug files can be expected at 20MB apiece. For a simple SCAP run that terminates based on a Common Platform Enumeration (CPE) failed test the debug file will be around 176 K or approximately two thousand lines of text. A successful run against a moderate amount of rules, for this example 46 compliance rules, the debug file will be several MB in size or approximately 26 thousand lines. The log and results files produced by SCC can be very large and you need to make sure that the platform being tested has adequate file capacity to generate and store the applications output.

A.6.2 Resolving issues using the Debug file

The debug file is not intended for end users of the SCAP Compliance Checker (SCC). It is a configurable feature so that end users can capture unexpected application behaviors or events and communicate, to the product development team, those issues related to the applications performance.

At 20MB a file, it can be difficult to know which file to send. Assuming that there are a number of files generated (001 … n+1) then which file contains the error that the developers need to see? The easy answer is that if the application CRASHED the last file generated will generally have the ERROR that will illuminate the reason for the fault. All other issues, it will have to be assumed that all the debug files need to be sent to developers.

A.6.3 Sending Debug Information

Every circumstance is unique so please contact the product Point-Of-Contact explaining the problem. You should receive instructions on what debug files will need to be provided and how to transfer the files to the product support team. A typical method is to e-mail a zip file containing the requested data, if you are in a windows dominated environment, or compressed tape archive (tar.gzip) format for non-windows environments, although pkzip and gzip compressed files are perfectly acceptable.

A.7 References

NIST SCAP
http://nvd.nist.gov/scap.cfm

NIST FDCC (Federal Desktop Core Configuration)
http://nvd.nist.gov/fdcc/index.cfm

NIST USGCB (United States Government Configuration Baseline)
http://usgcb.nist.gov

NIST XCCDF (The Extensible Configuration Checklist Description Format)
http://scap.nist.gov/specifications/xccdf/

MITRE OVAL (Open Vulnerability Assessment Language)
http://oval.mitre.org

NIST OCIL (Open Checklist Interactive Language)
http://scap.nist.gov/specifications/ocil/

NIST Cyberscope
http://scap.nist.gov/use-case/cyberscope

DISA STIG SCAP Benchmarks
http://iase.disa.mil/stigs/scap/index.html

SCAP Compliance Checker SCAP Validation Page
http://nvd.nist.gov/validation_spawar.cfm

SPAWAR's SCC Page
www.public.navy.mil/spawar/Atlantic/ProductsServices/Pages/SCAP.aspx

A.8 Definitions

Acronym	Definition
CCE	Common Configuration Enumeration CCE™ provides unique identifiers to system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. For example, CCE Identifiers can be used to associate checks in configuration assessment tools with statements in configuration best-practice documents and security guides, are the main identifiers used for the settings in the U.S. Federal Desktop Core Configuration (FDCC) data file downloads, and are a key component for enabling security content automation. [1]
CPE	Common Platform Enumeration CPE™ is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets. CPE can be used as a source of information for enforcing and verifying IT management policies relating to these assets, such as vulnerability, configuration, and remediation policies. IT management tools can collect information about installed products, identify products using their CPE names, and use this standardized information to help make fully or partially automated decisions regarding the assets.[1]
CVE	Common Vulnerability Enumeration CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures. CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.[1]
DISA	Defense Information Systems Agency The Defense Information Systems Agency (DISA) is a United States Department of Defense agency that provides information technology (IT) and communications support to the President, Vice President, Secretary of Defense, the military Services, and the Combatant Commands.[2] With respect to SCC and SCAP, DISA creates and maintains SCAP content for the DISA STIGS.
FDCC	Federal Desktop Core Configuration FDCC has been replaced by the USGCB.
MITRE	MITRE is a not-for-profit corporation, chartered to work solely in the public interest. MITRE operates multiple Federally Funded Research and Development Centers (FFRDCs).[1] With regards to SCAP, MITRE develops and maintains several standards such as OVAL, CPE, CCE and CVE.
NIST	National Institute of Standards and Technology NIST is a United States Government agency responsible for many government standards, including SCAP.
OCIL	Open Checklist Interactive Language The Open Checklist Interactive Language (OCIL) defines a framework for expressing a

	set of questions to be presented to a user and corresponding procedures to interpret responses to these questions. Although the OCIL specification was developed for use with IT security checklists, the uses of OCIL are by no means confined to IT security. Other possible use cases include research surveys, academic course exams, and instructional walkthroughs.[3]
OVAL	Open Vulnerability and Assessment Language Open Vulnerability and Assessment Language (OVAL®) is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment. The repositories are collections of publicly available and open content that utilize the language.[1]
SCAP	Security Content Automation Protocol SCAP (pronounced S-CAP) consists of a suite of specifications for standardizing the format and nomenclature by which security software communicates information about software flaws and security configurations. [3] NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems.[3]
SCC	SCAP Compliance Checker SCAP Validated FDCC Scanner developed by SPAWAR Atlantic.
SPAWAR	Space and Naval Warfare SPAWAR Systems Center Atlantic is a Department of the Navy organization. We meet our nation's demands for uninterrupted vigilance, fail-safe cybersecurity, adaptive response and engineering excellence by delivering secure, integrated and innovative solutions to many naval, joint and national agencies. [4]
STIG	Security Technical Implementation Guides The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA Field Security Operations (FSO) has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. [5]
USGCB	United States Government Configuration Baseline The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. The USGCB is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security. [3]
XCCDF	The Extensible Configuration Checklist Description Format

	XCCDF is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. The specification also defines a data model and format for storing results of benchmark compliance testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices.
XML	Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. [2]

[1] - http://www.mitre.org/
[2] - http://www.wikipedia.org/
[3] - http://www.nist.gov/
[4] - http://www.public.navy.mil/
[5] - http://iase.disa.mil

A.9 End User License Agreement

Any usage or distribution of this software outside of the U.S. Federal Government shall be reviewed by the agency distributing the software to ensure the distribution complies with the government purpose rights listed below, and is in the best interest of the U.S. Federal Government.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The U.S. Federal Government has at least "government purpose rights" for this computer software under DFARS 252.227-7014. This computer software is to be used only for a "government purpose" as generally defined in DFARS 252.227-7014, and specifically defined below.

The U.S Federal Government's rights to use, modify, reproduce, release, perform, display, or disclose this software are restricted by paragraph (b)(2) of the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation. Any reproduction of the software or portions thereof marked with this legend must also reproduce the markings.

This software is designed to review computer security settings and can be installed on any U.S. Federal Government computer or any computer that is mandated to comply with U.S. Federal Government security regulations such as OMB M-08-22, FISMA, HIPPA, NIST FDCC, NIST USGCB, DISA STIGs and IRS.

The U.S Federal Government purpose in distributing this software is to increase computer security and awareness for U.S entities interfacing with the U.S Federal Government.