



SCC

SCAP Compliance Checker
Version 5.7.1 User Manual
for Microsoft Windows

**Naval Information
Warfare Center**



ATLANTIC

Developed by:
NIWC Atlantic (formerly SPAWAR Atlantic)
P.O. Box 190022
North Charleston, SC 29419-9022
scc.fct@navy.mil
<https://www.niwcatlantic.navy.mil/scap/>

Distribution A: Approved for Public Release (16 Feb 2021) NIWCLANT SPR# 2021-57

Table of Contents

| | |
|--|----|
| 1. Introduction | 1 |
| 1.1 Background | 1 |
| 1.2 Platforms Supported | 2 |
| 1.3 SCAP Content Included | 2 |
| 1.4 Changelog for 5.7.1 | 4 |
| 1.5 Changelog for 5.7 | 4 |
| 2. Requirements | 6 |
| 2.1 Minimum Hardware/OS Requirements | 6 |
| 2.2 Scanning Requirements..... | 6 |
| 3. Install/uninstall | 8 |
| 3.1 Windows Software Installation | 8 |
| 3.2 Windows Software Uninstall | 10 |
| 3.3 Install/Remove software via zip file..... | 10 |
| 3.4 Install Details..... | 11 |
| 4. GUI Based Usage..... | 13 |
| 4.1 Launching the Graphical User Interface | 13 |
| 4.2 Installing & Configuring Content | 14 |
| 4.3 Performing a Scan | 18 |
| 4.4 Editing Options..... | 23 |
| 4.5 Viewing Results | 37 |
| 4.6 SCAP scanning with OCIL Manual Questions..... | 38 |
| 4.7 XCCDF Tailoring..... | 40 |
| 4.8 Cisco IOS / IOS XE Offline (Show Tech) File Scanning | 42 |
| 4.9 Standalone OVAL Usage..... | 44 |
| 4.10 Standalone OCIL Usage | 45 |
| 4.11 Post Scanning Report Generation | 47 |
| 4.12 File and Help Menus | 50 |
| 5. Command Line Usage | 52 |
| 5.1 Basic Command Line Usage | 52 |
| 5.2 Command Line Configuration Parameters | 53 |
| 5.3 Command Line Scanning Parameters | 58 |
| 5.4 Option Descriptions and Datatypes | 62 |
| 5.5 Generating Post Scan Reports from the Command Line | 72 |
| 5.6 Multiple Computer Deployment | 75 |
| 5.7 Manual Question Auto-Answer Files | 76 |
| 6. Understanding Scan Results..... | 78 |
| 6.1 Understanding Scan Reports..... | 78 |
| 6.2 Navigating the Results Directory | 81 |
| 6.3 Viewing Screen, Error or Debug Logs | 83 |
| 7. Running SCC as a Service | 85 |
| 7.1 Installing the SCC Service | 85 |
| 7.2 Configuring the SCC Service | 85 |
| 7.3 Update Service Configuration | 86 |
| 8. Running SCC as a non-Administrator | 87 |
| 8.1 Installing SCC | 87 |
| 8.2 Install directory non-writable by non-Administrators | 87 |
| 8.3 GUI usage as non-administrator | 87 |
| 8.4 Command line usage as non-administrator | 87 |
| 8.5 Uninstalling..... | 88 |
| APPENDIX A - FREQUENTLY ASKED QUESTIONS | 89 |
| A.1 Why can't I install a DISA STIG Manual XCCDF into SCC? | 89 |
| A.2 How can I scan CENTOS Linux, Rocky Linux, Alma Linux, Debian Linux etc. with an existing SCAP benchmark? | 89 |

| | |
|---|-----|
| A.3 I just installed new/updated SCAP content from DISA, why am I no longer seeing Manual Questions? | 89 |
| A.4 Can I scan Linux/Solaris/Mac from Windows? | 90 |
| A.5 Is SCC officially SCAP validated? | 90 |
| A.6 Who should I report SCAP content issues to? | 90 |
| A.7 Why does NIWC's 'Enhanced' content have a different version from DISA SCAP content? | 90 |
| A.8 Does SCC provide any remediation functionality? | 91 |
| A.9 Where can I learn more about creating my own SCAP content? | 91 |
| A.10 Why is SCC default SCAP content and application updates URL's hosted on a .com? .. | 91 |
| A.11 Can I create my own offline SCAP content repository for my isolated network? | 92 |
| A.12 Can SCC run directly from a CD-ROM? | 94 |
| A.13 Can SCC be run as a non-Administrator or non-root user? | 94 |
| A.14 How can I use RunAs (Secondary Logon) with SCC? | 94 |
| A.15 What type of network traffic does a remote Windows SCC scan generate? | 95 |
| A.16 Where can I download the DOD Root Certificates for Windows (InstallRoot)? | 95 |
| A.17 Why does SCC review all cached profiles to confirm that User profile settings are accurate | 96 |
| A.18 How do I make local users compliant with user level GPOs? | 96 |
| APPENDIX B - KNOWN ISSUES | 97 |
| B.1 Potential out of memory crashes with very large OVAL XML content files | 97 |
| B.2 Unable to scan RHEL8 systems via SSH with OS application white listing enabled (SCC failed to launch) | 97 |
| B.3 Host Key Check Failed when scanning RHEL7/8 and Ubuntu systems via SSH when changing between SCC 5.4 and 5.4.2 or later | 97 |
| B.4 Account lockout issues when scanning Ubuntu remotely via SSH with correct credentials | 97 |
| B.5 Command prompt closes when run with UAC | 97 |
| B.6 Maximum directory/file length error when copying SCC results | 98 |
| B.7 Reviewing Domain Controllers with numerous user accounts | 98 |
| B.8 Issues with WMI scanning if GPO is configured to block execution of all .bat files | 99 |
| B.9 Issues with remote scanning (Classic and WMI) if scanning PC is not fully patched | 99 |
| APPENDIX C - TROUBLESHOOTING | 100 |
| C.1 Troubleshooting UNIX SSH Remote Scanning | 100 |
| C.2 Troubleshooting Windows Remote Scanning | 101 |
| APPENDIX D – SCC AND SCAP | 107 |
| D.1 SCAP Validations & Capabilities | 107 |
| D.2 Standards Supported | 107 |
| D.3 SCAP Implementation | 108 |
| D.4 OVAL Probes Supported by SCC 5.7.1 for Windows | 117 |
| APPENDIX E - REFERENCES & DEFINITIONS | 120 |
| E.1 References | 120 |
| E.2 Definitions | 121 |
| APPENDIX F - LICENSES | 124 |
| F.1 End User License Agreement | 124 |
| APPENDIX G - TECHNICAL SUPPORT & Feedback | 125 |
| G.1 Technical Support | 125 |
| G.2 Tutorials | 125 |
| G.3 Software Releases | 125 |
| G.4 Provide Feedback on SCC | 125 |
| APPENDIX H - CREDITS AND FUNDING | 126 |
| H.1 Credits and Funding | 126 |
| H.2 SCC Funding for FY24 and Beyond | 126 |

1. INTRODUCTION

The Security Content Automation Protocol (SCAP) Compliance Checker (SCC) is a SCAP 1.2 Validated Authenticated Configuration Scanner, with support for SCAP versions 1.0, 1.1, 1.2 and 1.3, and an 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 Security Technical Implementation Guides (STIG) Viewer, please refer to DISA's (Defense Information Systems Agency) documentation, which is located at: <https://cyber.mil/stigs/srg-stig-tools/>

1.1.2 What is SCC?

SCC is an XML interpreter of SCAP content, meaning SCC performs automated security configuration checks based on the content that is installed and enabled. The end user can install SCAP content into SCC, and enable one or more SCAP content streams to perform compliance checking.

1.1.3 Who can use SCC?

Starting with SCC version 5.4, the application can be freely distributed and used by anyone. Refer to Appendix F for our legal disclaimer in our End User License Agreement.

1.1.4 Who funds the development and support of SCC?

Starting with FY24, we are hoping to crowdfund SCC. See Appendix H for details about historical funding, current FY23 funding, and future funding efforts.

1.1.5 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 targeted 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.

1.2 Platforms Supported

- Microsoft Windows 10 (x86 & x64)
- Microsoft Windows 11 (x64)
- Microsoft Windows Server 2012 (x64)
- Microsoft Windows Server 2012 R2 (x64)
- Microsoft Windows Server 2016 (x64)
- Microsoft Windows Server 2019 (x64)
- Microsoft Windows Server 2022 (x64)
- Microsoft SQL Server 2000/2005/2008/2008R2/2012/2014
- Cisco IOS
- Cisco IOS XE
- Platforms supported by remote SSH based scanning (with the UNIX Remote Scanning Plugin installed)
 - Red Hat Distributions
 - Red Hat Enterprise Linux 6 (x86 & x64)
 - Red Hat Enterprise Linux 7 (x64)
 - Red Hat Enterprise Linux 8 (x64 & aarch64)
 - Red Hat Enterprise Linux 8 (x64 & aarch64)
 - Red Hat Enterprise Linux 9 (x64)
 - SUSE Linux
 - Enterprise SUSE Linux 12 (x64)
 - Enterprise SUSE Linux 15 (x64 & aarch64)
 - Oracle Linux
 - Oracle Linux 7 (x64)
 - Oracle Linux 8 (x64 & aarch64)
 - Debian Distributions
 - Ubuntu 16.04 LTS (x86)
 - Ubuntu 16.04 LTS (amd64)
 - Ubuntu 18.04 LTS (amd64)
 - Ubuntu 20.04 LTS (amd64& arm64)
 - Raspberry Pi 3 (ARM7)
 - Raspberry Pi 4 (ARM7)
 - Raspberry Pi OS (arm64)
 - Solaris 10 (x86 & SPARC)
 - Solaris 11 (x86 & SPARC)
 - Mac OS X

Note 1: *There are separate SCC installers per architecture (Windows, Linux (RPM, DEB), Solaris, MacOS)*

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

1.3.1 SCAP Streams

- NIWC Manual Question "Enhanced" DISA STIG SCAP content obtained from:
<https://www.niwcatlantic.navy.mil/scap/scap-content-repository/>
 - Adobe Acrobat Reader DC Continuous
 - Google Chrome
 - Microsoft Edge
 - Internet Explorer 11
 - Mozilla Firefox
 - Microsoft .NET Framework
 - Windows Defender AV
 - Windows Firewall
 - Windows 2012 and 2012 R2 Domain Controller
 - Windows 2012 and 2012 R2 Member Server
 - Windows Server 2016
 - Windows Server 2019
 - Windows Server 2022
 - Windows 10
 - Windows 11
 - Cisco IOS XE Router RTR
 - Cisco IOS XE Router NTM
- NIWC Developed DISA STIG SCAP content obtained from:
<https://www.niwcatlantic.navy.mil/scap/scap-content-repository/>
 - Microsoft Internet Information Server (IIS) 8.5
 - Microsoft Internet Information Server (IIS) 10.0
 - Microsoft Office 365 ProPlus
 - Microsoft OneDrive

1.4 Changelog for 5.7.1

Below is an abbreviated list of the primary changes from version 5.6 to 5.7. Please refer to the release notes for a complete list of updates.

- For All Platforms
 - Fixed data interoperability issue with SCC's CKL file and eMASS
 - Disabled the creation of XCCDF Results for Manual Questions rules, if Manual Question processing option is disabled.
 - Updated upgrade feature on Windows to upgrade any Manual Question results from a previous installation
 - Improved functionality of Manual Question GUI, adding searching and sorting
 - Minor improvements to Manual Question autoanswer text file templates
- Windows
 - Fixed issue running on Windows when no network cards have IP Addresses
- Linux
 - Fixed issue running GUI at 1024 x 768 resolution
- MacOS
 - Fixed minor issues with incorrectly identifying NIST content as containing manual checks.

1.5 Changelog for 5.7

Below is an abbreviated list of the primary changes from version 5.6 to 5.7. Please refer to the 5.7 release notes for a complete list of updates.

- For All Platforms
 - Updated all SCAP content bundled with SCC to be enhanced with manual checks, providing 100% coverage of DISA STIG Manuals, using SCAP standard of Open Checklist Interactive Language (OCIL)
 - Updated default SCAP content repository to NIWC's repository located at <https://www.niwcatlantic.navy.mil/scap/scap-content-repository/>
 - Updated SCC GUI to provide interface for manual questions, refer to section 4.6 for details
 - Added manual question autoanswer files for command line automation, refer to section 5.7 for details
 - Added creation of DISA's Checklist (CKL) report output, for SCAP content that has been enhanced with manual questions.
 - Improved error reporting in HTML/Text/XML
 - Improved result details in XCCDF XML results, which should be supported by DISA STIG Viewer in the future
 - Now officially SCAP 1.3 validated by an independent lab
 - Added funding popup on GUI and text based message on cscs --config as SCC will be crowdfunded in FY24
- For Windows
 - Added prompting to upgrade configuration from previous installation on first launch.
 - Added NIWC developed SCAP content for
 - Microsoft Internet Information Server (IIS) 8.5
 - Microsoft Internet Information Server (IIS) 10.0
 - Microsoft Office 365 ProPlus

- Microsoft OneDrive

2. REQUIREMENTS

2.1 Minimum Hardware/OS Requirements

SCC can run on virtually any Windows based computer, however, below are some minimum specifications.

| HARDWARE | MINIMUM/RECOMMENDED |
|-------------------------|---|
| CPU | Intel/AMD x86 or x64 based processor. Recommend at least a 1.5 Ghz dual core or newer. |
| RAM | 1.0 GB Minimum, 2.0 GB or more is recommended. SCC uses about 250 MB to startup, and may use up to 1 GB or more during certain scans, especially WMI based remote scans from 64 bit Windows. |
| Disk space installation | The base install of SCC requires approximately 150 MB of disk space. Reviews may generate 100+ MB of results depending on content and logging options enabled. |
| Operating System | Windows 2012 or later |

2.2 Scanning Requirements

SCC has three scanning modes for Windows. Local, Classic Remote and WMI Remote. Each have slightly different requirements.

| SCANNING REQUIREMENT | LOCAL | CLASSIC REMOTE | WMI REMOTE |
|---|-------|----------------|------------------|
| Local Administrative Rights | X | X | * See Note Below |
| Manage Auditing and Security Logon User Right | X | X | X |
| Windows Management Instrumentation (WMI) Service | X | X | X |
| Domain Admin Rights | | X | X |
| File and Printer Sharing for Microsoft Networks | | X | X |
| Server Service | | X | X |
| Remote Procedure Call (RPC) Service <ul style="list-style-type: none">System dependency for Remote Registry and WMI | | X | X |
| Firewall Exceptions <ul style="list-style-type: none">If the client firewall is blocking WAN/LAN connectivity to the file shares, RPC or WMI, SCC will not be able to perform a remote review. Classic reviews also require firewall rules to allow Remote Registry access, and DCOM. | | X | X |
| "Access this computer from the network" User Right for the account running SCC (and not denied via "Deny access to this computer from the network") | | X | X |
| Remote Registry Service | | X | |
| DCOM (if content which uses WuaUpdateSearcher) | | X | |

| | | | |
|--|--|--|---|
| Ability to execute Windows 'makecab.exe' | | | X |
|--|--|--|---|

* WMI Note: Windows WMI mode can be run with SCC running as an administrator but can also be run as a non-administrator, and perform scans with alternate credentials, stored in SCC. Refer to section 4.4.1.7 WMI Remote Scanning Options for more information.

3. INSTALL/UNINSTALL

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

It is recommended to verify the SHA256 checksums of the downloaded zip files with the SCC checksum file from <https://www.niwcatlantic.navy.mil/scap/> before proceeding to install.

3.1 Windows Software Installation

Note: Installer should be run with an Administrator account.

3.1.1 Graphical Installation Method

1. Double click on the installer (SCC_5.7.1_Windows_Setup.exe).
2. Verify that the installer has been signed by a DOD trusted cert: CS.NIWC-ATLANTIC.001
Note: DOD Root certificates need to be installed to verify the certificate trust path.
3. Review the User Account Control prompt, and click Yes.
4. Read the License Agreement page, click "I accept the agreement", and click Next.
5. Choose the Destination Folder (or leave at the default) and click Next.
6. Select Components (or leave default)
 - a. Determine if pre-bundled SCAP content is desired.
 - b. Determine if installing as a service is desired. Refer to the section titled 'Running SCC as a Service' for additional information.
7. Select a desktop shortcut if desired
8. Read the Ready to Install page and click Install.

3.1.2 Command Line Installation Method

The Setup program accepts optional command line parameters. These can be useful to system administrators, and to other programs calling the Setup program.

`/HELP, /?`

Shows a summary of this information. Ignored if the UseSetupLdr [Setup] section directive was set to no.

`/SP-`

Disables the 'This will install... Do you wish to continue?' prompt at the beginning of Setup.

`/SILENT, /VERYSILENT`

Instructs Setup to be silent or very silent. When Setup is silent the wizard and the background window are not displayed but the installation progress window is. When a setup is very silent this installation progress window is not displayed. Everything else is normal so for example error messages during installation are displayed and the startup prompt is (if you haven't disabled it with DisableStartupPrompt or the '/SP-' command line option explained above).

`/SUPPRESSMSGBOXES`

Instructs Setup to suppress message boxes. Only has an effect when combined with '/SILENT' or '/VERYSILENT'.

The default response in situations where there's a choice is:

Yes in a 'Keep newer file?' situation.

No in a 'File exists, confirm overwrite.' situation.

Abort in Abort/Retry situations.

Cancel in Retry/Cancel situations.

Yes (=continue) in a

DiskSpaceWarning/DirExists/DirDoesntExist/NoUninstallWarning/ExitSetup Message/ConfirmUninstall situation.

Yes (=restart) in a FinishedRestartMessage/UninstalledAndNeedsRestart situation.

5 message boxes are not suppressible:

The About Setup message box.

The Exit Setup? message box.

The FileNotInDir2 message box displayed when Setup requires a new disk to be inserted and the disk was not found.

Any (error) message box displayed before Setup (or Uninstall) could read the command line parameters.

Any message box displayed by [Code] support function MsgBox.

`/DIR="x:\dirname"`

Overrides the default directory name displayed on the Select Destination Location wizard page. A fully qualified pathname must be specified. May include an "expand:" prefix which instructs Setup to expand any constants in the name. For example: '/DIR=expand:{pf}\My Program'.

`/TYPE=type name`

Overrides the default setup type. Options are Standard and Custom, selecting Custom is required to select components as listed below

`/COMPONENTS="comma separated list of component names"`

Overrides the default component settings. Using this command line parameter causes Setup to automatically select a custom type. If no custom type is defined, this parameter is ignored.

Only the specified components will be selected; the rest will be deselected.

If a component name is prefixed with a "*" character, any child components will be selected as well (except for those that include the dontinheritcheck flag). If a component name is prefixed with a "!" character, the component will be deselected.

The available components are:

Content\DISA_STIG_SCAP_Content

Other\SCC_Service

This parameter does not change the state of components that include the fixed flag.

Example:

Deselect all components, then select the "SCC Service" component:

`/COMPONENTS="Other\SCC_Service"`

Examples

Install SCC with default options silently with no GUI shown

```
SCC_5.7.1_Windows_Setup.exe /VERYSILENT
```

Install SCC to a given directory with default options silently with no GUI shown

```
SCC_5.7.1_Windows_Setup.exe /VERYSILENT /DIR="C:\SCC"
```

Install SCC with the Service and default content silently with no GUI shown

```
SCC_5.7.1_Windows_Setup.exe /VERYSILENT /TYPE=custom  
/COMPONENTS="Content\NIST_USGCB_SCAP_Content,Content\DISA_ST  
IG_SCAP_Content,Other\SCC_Service"
```

3.2 Windows Software Uninstall

Note: The uninstaller will not delete any files added after the installation, such as end user installed content, so the installation directory may exist and need to be manually removed.

3.2.1 Standard Method

1. Click Start -> Control Panel -> Programs -> Uninstall a program
2. Double click on SCAP Compliance Checker 5.7.1
3. Follow the prompts

3.2.2 Silent Uninstall

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

```
"C:\Program Files\SCAP Compliance Checker 5.7.1"\unins000.exe  
/SILENT
```

3.3 Install/Remove software via zip file

3.3.1 'Install' software via zip file

To install, simply extract file scc-5.7.1_Windows.zip to any directory.

3.3.2 Removal of software installed via zip file

To remove software 'installed' from the generic zip file, simply remove the installation directory and all sub-directories and files.

3.4 Install Details

3.4.1 Files Installed by the SCC

| FILE | DESCRIPTION |
|--------------------------------------|---|
| bin | SCC dependencies shared for 32 and 64 bit. |
| csc.exe | Launcher program for the command line version of SCC |
| csc-remote.exe | Launcher program for the command line version of SCC, used for remote WMI reviews. |
| scc.exe | Launcher program for the graphical version of SCC |
| scc.sig32 | Use for verifying the integrity of 32 bit installations |
| scc.sig64 | Use for verifying the integrity of 64 bit installations |
| lib32 | 32 bit version of SCC dependencies |
| lib64 | 64 bit version of SCC dependencies |
| options.xml | Default options file used by SCC |
| hosts.txt | Sample host file |
| unins000.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. |
| Documentation\ThirdPartyLicenses.txt | Contains list of third party libraries used in SCC and their respective licenses. |
| Documentation\ThirdPartyLicenses | Directory containing text formatted 3rd party licenses, referenced in ThirdPartyLicenses.txt |
| Local | Location in which SCC writes temporary files during execution. |
| RemotePlugin | Location in which remote UNIX and Windows scanning plugins may reside, empty by default. |
| Resources\Compiled* | Folder containing compiled library files for SCC use |
| Resources\Content* | Parent content folder for SCAP, SCAP 1.2, OVAL, OVAL External Variables, and OCIL content folders |
| Resources\Content\External_Variables | Contains any External Variables files associated with an OVAL content stream |
| Resources\Content\OVAL_Content | Contains any OVAL vulnerability content included with the installer or installed by the end user with the Install OVAL Content feature. |
| Resources\Content\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\Content\SCAP_Content | Contains any SCAP 1.0 or SCAP 1.1 content included with the installer or installed by the end user |
| Resources\Content\SCAP12_Content | Contains any SCAP 1.2 content included with the installer or installed by the end user |
| Resources\Content\TrustedPublicCerts | Contains known/trusted certificates to verify digital signatures in SCAP 1.2 content |
| Resources\Content\XCCDF_Tailoring | Contains XCCDF Tailoring files which can be used with SCAP 1.2 datastreams |
| Resources\DB | Database utilized when processing SCAP 1.2 data streams |
| Resources\DefaultFiles | Contains default files used by the SCC |
| Resources\Graphics* | Images and icons used with SCC.exe |
| 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 post scan HTML and text reports from the OVAL and XCCDF XML results |
| C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\SCAP Compliance Checker 5.7.1 | Start menu icons created during the installation process |

3.4.2 Registry Keys Created During SCC Installation

| REGISTRY KEY | DESCRIPTION |
|--|---|
| HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\SCAP Compliance Checker 5.7.1 | Standard uninstall information which allows the Add/Remove Programs to remove the SCAP Compliance Checker software. |

3.4.3 Files Created During Software Execution

| FILE | DESCRIPTION |
|--|---|
| <User Defined Directory>\Sessions Refer to Data Directory option in "Editing Options" for details. | XML, HTML and Text based results created during a review. Also contains Screen, Debug and Error logs that are specific to a scan session. |
| <User Defined Directory>\ApplicationLogs Refer to Data Directory option in "Editing Options" for details. | SCC Application Logs (not related to any SCAP scan session) including Screen, Error and Debug logs that could be created during a review depending on user preferences. |
| <User Defined Directory>\Config Refer to Data Directory option in "Editing Options" for details. | Contains scan session database and host credential database. |
| <User Defined Directory>\options.xml | Configuration settings from the SCC.exe |
| <SCC Install>\Local | Temporary files created during SCC execution |

4. GUI BASED USAGE

Section 4 of this document explains the basic Graphical User Interface (GUI) usage of SCC to perform SCAP based compliance scanning, standalone OVAL and OCIL scanning, and editing options.

Below is a quick overview of how SCC works.

1. Open the SCC GUI.
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. Select Scan Type
6. Scan Computer(s) with enabled SCAP content.
7. View reports.

4.1 Launching the Graphical User Interface

To start the application with a GUI, click:

Start -> All Programs -> SCAP Compliance Checker 5.7.1 -> SCAP Compliance Checker (SCC) 5.7.1

1. Review information on the User Account Control pop-up
2. Verify that the SCC application has been signed by a DOD trusted cert: CS.NIWC-ATLANTIC.001
Note: DOD Root certificates need to be installed to verify the certificate trust path.
3. Click "Yes"

4.2 Installing & Configuring Content

SCC's installer contains the latest publicly available SCAP content from DISA, NIWC and NIST, which was available at that time. However, new and updated content may need to be installed by end users, especially if the current SCC release is several months old.

4.2.1 Updating SCAP Content with SCC

If the computer and the user running SCC have Internet access, SCC has the ability to update the DISA and NIWC developed STIG SCAP content.

To check for updated SCAP content:

- Click Help -> Check For Content Updates

To view more information on any content stream:

- Right click
 - View Content Details

To install content:

- Either Left click on each check box to enable
- Or Right click
 - Enable All
 - Disable All
- Then click "Install Checked Content"

* See Editing Options -> Update Options for more information on content updates and repositories.

Refer to SCC's FAQs if you are interested in making your own offline copy of DISA's content repository, or to learn why SCC's default content repository XML file is located on github instead of cyber.mil.

4.2.2 Installing Content Manually

The steps below will guide you through installing content within SCC. Note that the steps are the same SCAP 1.0, 1.1, 1.2 and 1.3 data streams.

To obtain NIWC Enhanced DISA STIG SCAP content which contain automation and Manual Questions: <https://www.niwcatlantic.navy.mil/scap/scap-content-repository/>

OR

To obtain DISA STIG SCAP content which does not contain any Manual Questions, please download "benchmarks" from <https://cyber.mil/stigs/scap/>

1. Launch the SCC GUI
2. Content should be visible by default in the main window. If content is not visible, due to existing scan logs, click the "Show Content" button in the left column, "Select Content" pane.
3. Click on the "Install" button in the "Content" pane

- a. Select from the following options:
 - i. Validate XML on content install (Yes/No)
 - ii. Overwrite existing content (Yes/No)
 - iii. Enable content on install (Yes/No)
4. Browse to the content file you would like to install
 - a. For .zip files, the following is supported
 - Zip of all SCAP 1.0/1.1 files
 - Zip of all SCAP 1.2/1.3 files
 - Zip of all standalone OVAL files (not part of a SCAP stream)
 - For more information on installing OVAL External Variables, refer to Section 4.9 Standalone OVAL Usage
 - Zip of all standalone OCIL files (not part of a SCAP stream)
 - Mixing of content types (SCAP/SCAP1.2/OVAL/OCIL) is not supported
 - b. For .xml files, the following is supported
 - XML file that is a SCAP 1.2/1.3 datastream
 - XML file that is a valid OVAL file
 - XML file that is a valid OCIL file
5. After installation is complete, enable the content and choose the desired profile.

Note: DISA STIG "Manual" files are not SCAP content. They contain an XCCDF XML file, but do not contain any OVAL XML. They are intended for performing a manual review of the system.

4.2.3 Enabling/Disabling Content

To enable/disable a single Content stream:

1. **Left** click the check box to the left of the content stream name

To enable all Content streams:

1. **Right** click on any row
2. Click "Select All"

To disable all Content streams:

1. **Right** click on any row
2. Click "Clear All"

NOTE: *If multiple benchmarks are included in a SCAP 1.2 data stream, SCC splits each benchmark on the SCAP Content tab. This allows the end-user to enable/disable a specific benchmark within a larger data stream.*

4.2.4 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
- Disable Slow Rules
- CAT I Only

How many checks and results are impacted by changing the profile is completely dependent 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:

1. **Left** click on the Stream name to populate the "Stream Details" window on the right
2. Select the desired profile from the Profile dropdown.

4.2.5 Selecting a Profile to use with All SCAP Content

To select a single profile, and apply it to all SCAP content:

1. **Right** click on the row to delete
2. Click "Set All Profiles"
3. A new form will open, showing a dropdown of all profiles found in all content.
4. Left click to select the desired profile
5. Click Save to save and close the form

4.2.6 Deleting Content

To delete a single content row

1. **Right** click on the row to delete
2. Click "Delete Selected Content"

To delete several content rows

1. Select as many content rows as you would like to delete, with **Left click and Shift** or **Left click and Ctrl**.
2. Right click on any of the selected rows
3. Click "Delete Selected Content"

To delete ALL Content

1. **Right** click on any row

2. Click "Delete All"

4.2.7 Viewing Content Details

To view additional information about the SCAP Content:

1. **Left** click on the Content Name
2. View the "Content Details" information on the right pane, it contains the following fields:

| ITEM | DESCRIPTION |
|--------------|--|
| Title | The XCCDF "title" field, directly from the content. |
| Datastream | The SCAP 1.2/1.3 Datastream "data-stream id" field. This can be useful if there are multiple datastreams with the same benchmark ID. |
| Profile | A drop-down containing 1 or more profiles from the XCCDF content. |
| Release Info | The XCCDF "release-info" field, directly from the content. |
| Status | The XCCDF "status" field, directly from the content. |
| Validation | The end result of SCC's attempt to validate the content, either at install or scan time. |
| Signature | The end result of SCC's attempt to validate the digital certificate of SCAP 1.2/1.3 datastream (if found) |
| Platform | The CPE-Dictionary CPE Item Title, directly from the XML content |
| Publisher | The XCCDF "publisher" field, directly from the XML content. |
| Description | The XCCDF "description" field, directly from the XML content. |
| Notice | The XCCDF "notice" field, directly from the XML content. |

4.2.7.1 Saving SCAP Prose Reports

Once you have populated the Stream Details pane, 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.

The Prose report is a human readable representation of the SCAP content, very similar to the All Setting reports, but does not contain any scan data. It is meant to show the XCCDF rules and OVAL definitions in a logical tree structure format.

4.2.7.2 XCCDF Tailoring

This is a feature for advanced users wanting to modify how SCAP 1.2 and SCAP 1.3 benchmarks perform checks. Refer to the XCCDF Tailoring section 4.8 for details.

4.2.7.3 Manual Questions

Starting with SCC 5.7, if SCAP content that contains OCIL manual questions is installed, SCC provides the ability to answer manual questions from the DISA STIG. To use, select the desired SCAP content, click on "Manual Questions" in the content details pane, and answer the non-automated items from the STIG Manual, and those results, along with the automated checks will be included in SCC results. See section 4.6 "SCAP Scanning with Manual Questions" for more information.

4.3 Performing a Scan

After installing and enabling the desired content and profile, the application is ready to perform compliance scanning.

1. Launch the SCC GUI
2. Select Scan Type
 - Local Scan
 - Single Remote Scan (Windows)
 - Multiple Remote Scan (Windows)
 - Cisco IOS / IOS XE Offline Scan
 - Cisco IOS / IOS XE Remote SSH Scan
 - Remote UNIX SSH Scan
 - Windows WMI and UNIX SSH Remote Scan
3. Select Content Stream(s) and their respective applicable Profiles
4. Start Scan
5. View Reports

4.3.1 Select Scan Type

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

4.3.1.1 *Local Scan*

This option instructs SCC to scan the computer in which the SCC software is installed.

4.3.1.2 *Single Remote Computer (Windows)*

This option instructs SCC to scan a single remote Windows computer over the LAN/WAN.

- Choose remote scan mode
 - Classic
 - Scan to be performed with remote API calls, no agent on remote computer
 - WMI
 - Scan to be performed by command line agent temporarily installed to target computer, and started and monitored via WMI
- A single NetBIOS computername or IP Address should be entered into the text field provided.

4.3.1.3 *Multiple Remote Computers (Windows)*

This option instructs SCC to scan a list of remote Windows computer over the LAN/WAN.

- Choose remote scan mode
 - Classic

- Scan to be performed with remote API calls, no agent on remote computers
- WMI
 - Scan to be performed by command line agent temporarily installed to target computers, and started and monitored via WMI
 - Scans are performed in parallel decreasing scan times for large numbers of computers.
- Host File
 - Create a new host file
 - Create a host list by querying Active Directory for the current domain
 - Options exist for validating this file
 - Validate host list using NSLookup to ensure computername is in DNS
 - Validate host list using NSLookup and Ping to ensure computername is in DNS and computer is online
 - Choose an existing hosts file
 - This list should be in the form of a text file with a single computer listed per line.
- Organizational Unit (OU)
 - Select one or more OU's from Active Directory (shift + left click to select more than one OU)
 - List of hosts created each time a scan is performed.
- Entire Domain
 - Scan all computers in the domain, list of hosts created each time a scan is performed.

4.3.1.4 Cisco IOS / IOS XE Config File

Refer to section 4.9 "Cisco IOS Config Scanning" for usage.

4.3.1.5 Cisco IOS / IOS XE Remote SSH

This option instructs SCC to scan a list of remote CiscoIOS Routers/Switches over the LAN/WAN. Refer to Edit/Select SSH Hosts, for instructions on selecting hosts and credentials.

4.3.1.5.1 Edit/Select SSH Hosts (Cisco)

Note: If the host credential manager has not been used before, a popup window will appear prompting for a new master password and confirming the new password.

This opens a credential manager in which the end user can

- Add a new host
 - DNS name or IP Address
 - Description (optional)
 - SSH Port
 - Authentication Type
 - Enable: No additional authentication
 - Enable: Use same password as username

- Enable: Use 'Enable' password. This requires selecting a credential that has an 'Enable' password
 - Enable: Use 'Enable' username and 'Enable' password. This requires selecting a credential that has both an 'Enable' username and an 'Enable' password.
 - Select an existing credential, or add a new one
 - Test SSH connection to remote device using selected credential
- Add a new credential
 - Username
 - Nickname (optional)
 - Password
 - 'Enable' username (optional depending on how device is configured), this field is used if Authentication Type is "Use 'Enable' username and 'Enable' password.
 - 'Enable' password (optional depending on how device is configured), this field is used if Authentication Type is "Use 'Enable' username and 'Enable' password, or Use 'Enable' password.
- Import an existing host file, formatted as text with a single DNS name or IP Address per line
 - Each host in this file will have it's SSH connection tested after import
- Double click a host to edit it
- Right click on the host list to:
 - Edit host
 - Enable Selected Hosts (If SSH test passes)
 - Enable All hosts (If SSH test passes)
 - Disable Selected Hosts
 - Disable Hosts with Failed SSH Connections
 - Disable All Hosts
 - Test Selected SSH Connections
 - Test All SSH Connections
 - Delete SSH hostkey/SHA256 Fingerprint
 - Delete Selected Hosts
 - Delete All Hosts
- Double click on a credential to edit it
- Right click on credentials to:
 - Edit credential
 - Delete selected credential
 - Delete all credentials

4.3.1.6 UNIX Remote SSH

This option instructs SCC to scan a list of remote UNIX/Linux/Mac systems over the LAN/WAN. Refer to Edit/Select SSH Hosts, for instructions on selecting hosts and credentials.

Note: If the UNIX SSH Scanning Plugin has not been installed, an information message will appear in the left window, with a browse dialog to select the plugin, which can usually be obtained from the same location you obtained the SCC installers.

4.3.1.6.1 Edit/Select SSH Hosts (UNIX)

This opens a credential manager in which the end user can

- Add a new host
 - DNS name or IP Address
 - Local System Name (Read only, queried from remote system)
 - Description (optional)
 - SSH Port
 - Operating System
 - SCC Autodetect is default
 - If autodetect fails, manual selection can be used.
 - Authentication Type
 - SSH as 'root'
 - SSH as non-root user, then 'su' with root password
 - **Note:** If the remote host is Solaris, Ubuntu or Mac OS X, this method may not work, due to the implementation of 'su' in those operating systems. The recommended method is one of the 'sudo' options below.
 - SSH as non-root user, then 'sudo', no password
 - SSH as non-root user, then 'sudo', with user's password
 - Select an existing credential, or add a new one
 - Test SSH connection to remote device using selected credential
 - Tests to make sure the hostname/ip is valid
 - Checks remote server's hostkey
 - Tests authentication
 - Determines remote 'local system name'
 - Tests running commands as root level user
 - Determines remote Operating System
 - Checks freespace on remote /tmp and remote base SCC directory (user configurable, see scanning options for more information)
 - SHA256 fingerprint
 - The first time SCC SSH's to a remote UNIX host, it will download the remote system's hostKey, and display the SHA256 checksum of the hostkey for the end user to inspect.
 - If the remote hostKey changes in the future, SCC will warn the user about a potential man in the middle attack and disable the host.
 - If the new hostkey is to be trusted, SCC will allow you to re-trust and re-enable the host.
- Add a new credential
 - SSH Username
 - Nickname (optional)
 - SSH and/or sudo password
 - Enter the password associated with the username, it could be used for just the SSH connection, but also for sudo depending on the authentication type selected for the host.
 - Private Key (required if password is not present)
 - Note that SCC will use the private key first if both an SSH password and private key are present.
 - Passphrase (if required by private key)
- Import an existing host file, formatted as text with a single DNS name or IP Address per line
 - Each host in this file will have it's SSH connection tested after import

- Double click a host to edit it
- Right click on the host list to:
 - Edit host
 - Enable Selected Hosts (If SSH test passes)
 - Enable All hosts (If SSH test passes)
 - Disable Selected Hosts
 - Disable Hosts with Failed SSH Connections
 - Disable All Hosts
 - Test Selected SSH Connections
 - Test All SSH Connections
 - Delete SSH hostkey/SHA256 Fingerprint
 - Delete Selected Hosts
 - Delete All Hosts
- Double click on a credential to edit it
- Right click on credentials to:
 - Edit credential
 - Delete selected credential
 - Delete all credentials

4.3.1.7 Windows WMI and UNIX Remote SSH Scan

This is a Windows only feature that combines WMI scanning and UNIX SSH Remote scanning into a single scan. Refer to each individual method for instructions on selecting/enabling hosts.

Note: If the UNIX SSH Scanning Plugin has not been installed, an information message will appear in the left window, with a browse dialog to select the plugin, which can usually be obtained from the same location you obtained the SCC installers.

4.3.2 Select Content

Select content as described in section 4.2.

4.3.3 Performing Analysis

To perform a scan, click the '**Start Scan**' button.

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

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 SCC GUI
2. Click Options ->Show Options

4.4.1 Scan Options

4.4.1.1 SCAP Processing

| OPTION | DESCRIPTION |
|---|--|
| Run all content regardless of applicability | <p>This option will ignore the content's CPE-OVAL results and continue processing the content against the system. This option can be used to run content that is not normally applicable to the target system (e.g. Red Hat SCAP content on a Debian system).</p> <p>Note that this option alters the standard SCAP rules for gathering certain objects which can result in incomplete results and/or false positives.</p> |
| Process Manual Questions if found in SCAP content | <p>This option will ignore any manual questions in the content and cause any XCCDF rule that is a manual question to be excluded from XCCDF results.</p> <p>This will disable the creation of DISA CKL reports, as all rules are required for CKL reports.</p> <p>This will remove any warnings that SCC would normally print if manual question results were not found for a given content stream.</p> |
| Attempt to download external OVAL and XCCDF Tailoring files | <p>This option allows the user to disable the SCAP 1.2 requirement of attempting to download OVAL and/or XCCDF Tailoring files from the internet, if specified in the content.</p> <p>If this option is enabled (default) and the SCAP 1.2 datastream lists a http reference for the OVAL or XCCDF Tailoring component, SCC will attempt to download it, and store it locally. Once it has been downloaded, it does not attempt again.</p> <p>This feature is not currently used by any production NIST or DISA SCAP content, but the feature is required for SCC to obtain SCAP 1.2 validation.</p> |
| Force OVAL results to 5.10.1 for SCAP 1.2 interoperability | <p>SCC by default saves results in OVAL 5.12.1. However, this option could be enabled by the user for certain usage (primarily SCAP 1.2 validation) or tools that import OVAL results (but only support OVAL 5.10.1).</p> |
| Save results when content is not applicable for SCAP 1.3 interoperability | <p>This option is designed to force SCC to create XML results even when content is not applicable to the target. It could be used for troubleshooting debugging purposes, but is primarily intended to only be used as part of NIST SCAP 1.3 validation, which has a test case which mandates SCAP validated tools create results when content is not</p> |

| | |
|--|-------------|
| | applicable. |
|--|-------------|

4.4.1.2 OVAL Processing

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.

| OPTION | DESCRIPTION |
|---|--|
| Ignore remote file systems during OVAL file scans | <p>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.</p> <p>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.</p> <p>Until SCAP content is updated to ignore remote file systems, it is recommended to keep this option enabled in SCC.</p> |
| Treat the OVAL 'equals' operation as 'case insensitive equals' | <p>This option allows end users to override the instructions in the OVAL content and to ignore case of files and directories.</p> <p>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.</p> |
| Domain Controllers: Process the OVAL accesstoken_test by user right | <p>The Windows accesstoken_test will collect user right information for all user accounts even if the accounts have no rights. Under certain circumstances (domain controllers), this could result in the collection of thousands of user accounts which may lead to extremely large result files and/or memory errors. If this option is enabled, then user right information will be collected only for user accounts that actually have user rights assigned.</p> |
| Enable OVAL item creation threshold | <p>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.</p> <p>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.</p> <p>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</p> |

| | |
|--|--|
| | <p>pass/fail, and the end user will likely need to perform the check manually to determine true compliance.</p> <p>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.</p> <p>By default, the OVAL Item Creation Threshold is set at 50,000.</p> <p>This field is guarded by input validation and will only allow a user to enter an integer between 0 and 999999. Any input outside of those values will result in an error and the option will not be allowed to be saved.</p> |
|--|--|

4.4.1.3 Manual Question Processing

| OPTION | DESCRIPTION |
|--|---|
| Sort Questionnaires by DISA CAT (CAT I, CAT II etc..) | This option sorts Manual Questions, both in the SCC GUI and in the Manual Question text based autoanswer templates to be sorted by severity, displaying CAT I items first, followed by CAT II etc... If this option is disabled, questions will be displayed in the order they were found in the DISA STIG Manual. |
| Regenerate Templates | This option allows the end user to regenerate all Manual Autoanswer Templates. This does not update any existing completed autoanswer file |
| Backup Manual Question Results with datetime/username to a Backups sub-directory | This option only applies to SCC GUI when saving manual question results from SCC's Manual Question editing form. When enabled, this option causes SCC to create a backup of the Manual Question results to a subfolder of Completed_Files each time "Save Document and Close" is pressed. This creates a backup file with the date/timestamp and the username of the person logged into the computer. These files can be used to manually restore a backup, or show changes with diff utilities. Refer to Section 4.6.2.2 for more information. |

4.4.1.4 Manual Question AutoAnswer Completed Files Directory

| OPTION | DESCRIPTION |
|--|--|
| Obtain Manual Question AutoAnswer Files from the default directory | This option sets SCC to obtain manual question autoanswer files from <SCC Install>Resources/Content/Manual_Questions/Completed_Files/ |
| Obtain Manual Question Autoanswer files from a Custom Directory | This option sets SCC to obtain manual questions autoanswer files from any end user specified directory. This also instructs the SCC GUI to save Manual Questions to this custom directory. |

4.4.1.5 WMI/SSH Remote Scanning Options

| OPTION | DESCRIPTION |
|---|---|
| Maximum local threads for performing remote WMI or SSH scan | This option allows the end user to determine the number of local threads for parallel scanning with WMI and SSH based scanning. Each thread takes about 30 MB of RAM. More threads will speed up large remote scans, but could cause slowdowns or issues on the local computer. |
| Maximum minutes to allow SCC to start on remote system | This option allows the end user to specify a maximum amount of time to wait for SCC to be launched on the remote computer. This may fix issues on certain slow remote systems, especially with certain anti-virus products and features enabled that slow down extraction of zips and cabs. |

4.4.1.6 SSH Remote Scanning Options

| OPTION | DESCRIPTION |
|--|--|
| SSH: Remote Base Directory, SCC will make a sub-dir of 'scc-remote' | <p>Directory to copy a temporary copy of SCC for remote SSH based scans. This directory must exist, and should exist on it's own partition if possible. Default is /opt. SCC will create a subdirectory called 'scc-remote' in the specified directory, which it will install a temporary copy of SCC, and a results subdirectory for scanning logs and results.</p> <p>The <remote base directory>/scc-remote directory will be removed after each remote SSH scan.</p> |
| Uninstall Remote UNIX SSH Plugin | This allows for the removal of the remote plugin from the scanning computer. |
| SSH: Allow SCC to temporarily whitelist itself on target RHEL 8 and Oracle Linux 8 | <p>For RHEL 8 and Oracle Linux 8 targets:</p> <p>This option allows for remotely scanning STIG compliant RHEL 8 and Oracle Linux 8 computers, which requires enabling application whitelisting with fapolicy daemon.</p> <p>As this option temporarily change the configuration of the target system, this option is disabled by default. Below is an overview of what SCC does, should the end user want to enable this feature:</p> <ol style="list-style-type: none"> 1. From the scanning computer, after the temporary files are copied to the target computer in the user specified directory (default is /opt/scc-remote), the scanning computer runs the following command to whitelist csc-remote via SSH: <pre>fapolicy-cli -f add /opt/scc-remote/csc-remote fapolicyd-cli --update</pre> 2. Then csc-remote is called and it whitelists all of it's known binaries with the same method as #1 3. csc-remote scans the computer 4. When csc-remote completes, the scanning computer then removes the directory and all files/subdirectories with the following via SSH: |

| | |
|--|---|
| | <pre>fapolicyd-cli -f delete /opt/scc-remote/ fapolicyd-cli --update</pre> <p>To summarize, SCC uses the system command (if found) of fapolicyd-cli to whitelist a known list of binaries that comprise the SCC application before a scan starts, and when the scan completes, the whitelist is then removed from the target computers fapolicy database.</p> |
|--|---|

4.4.1.7 WMI Remote Scanning Options

| OPTION | DESCRIPTION |
|--------------------------------|---|
| WMI: Use Alternate Credentials | <p>This optional feature allows SCC to connect to target computers specifying alternate credentials. Please note that with this mode enabled, the command line interface of --wmi will prompt the user for the master password, in the same method as --ssh scanning, so any scripted usage of --wmi should have this option disabled.</p> <ul style="list-style-type: none"> ○ This feature allows SCC to scan from one active directory domain to another, and to scan systems that are not in any active directory domain. ○ This feature also allows for a non-administrator to launch SCC and perform remote WMI based reviews if they have a domain admin enter scanning credentials. The password stored in SCC is not reversible to the end user, and during the scan the end user should not have any admin level access to the target computer. |

4.4.2 Content Options

4.4.2.1 Installing Newer Versions of Existing SCAP Content

| OPTION | DESCRIPTION |
|--|--|
| Do Nothing, leave older content as-is when installing newer versions | This option leaves any older version of content as installed, and if it's enabled, it remains enabled. |
| Disable older versions of matching content | This options leaves the older version of content as installed, but disables it. |
| Archive older versions of matching content | This option moves the older version of content to <install>\Resources\Content\Archived_Content |
| Delete older versions of matching content | This option will delete any older version of matching content. |

4.4.2.2 XML Schema Validation

| OPTION | DESCRIPTION |
|--|---|
| Perform XML Schema Validation on Input Files during Installation | This option validates that the XML content is syntax error free before installing new content into SCC. |
| Perform XML Schema Validation on Input Files before scanning | This options validates that the XML content is syntax free before SCC uses it for each scan. |
| Perform XML Schema Validation on Output Files | This options validates that the XML result files are syntax and error free after creation. |

4.4.2.3 XML Digital Signatures

| OPTION | DESCRIPTION |
|--|---|
| Perform XML Digital Signature Validation before scanning | This option will validate signed XML content files prior to execution. |
| Cancel Scan(s) on XML Digital Signature Validation Failure | This option will automatically cancel a scan if the signed XML file(s) fail XML digital signature validation. |

4.4.2.4 Content Developer Mode

| OPTION | DESCRIPTION |
|--|--|
| Allow non schema validated content via manual installation | This option is reserved for content developers. As of 5.1, SCC strictly validates all content against the appropriate content schema prior to any scan (not just on installation). Since this security feature can be disruptive during content development testing with SCC, this option allows for a relaxation of that feature. |

4.4.3 Reporting Options

4.4.3.1 Select Reports

| 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 performed. |
| 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 failed checks |

4.4.3.2 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. |
|------|---|

4.4.3.3 XML Results

| OPTION | DESCRIPTION |
|--|--|
| Save 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 OVAL XML files - Full with System Characteristics | This option allows the user to enable saving the OVAL XML files, which contain the detailed results from each review, and can be very helpful in debugging problems, or recreating reports after scans occur. |
| Save OVAL XML files - Full without System Characteristics | This option allows the user to save a slightly less verbose version of OVAL results, which exclude the System Characteristics, and is required by SCAP 1.2. |
| Save OVAL XML files - Thin | This option allows the user to save even less data to OVAL results, which exclude the System Characteristics and Test results, and is required by SCAP 1.2. |
| Do Not Save OVAL Results | This option allows the user to not save OVAL XML results after each scan is complete. |
| Save OCIL Results | This option allows the user to disable saving OCIL XML files (if content includes OCIL content). |
| Save NIST ARF XML files | This option creates the NIST SCAP 1.2/1.3 Asset Reporting Format (ARF), which may be useful if an AFT results consumer is being used, or for testing official SCAP capabilities. |
| Save DISA Checklist 'CKL' file when using content enhanced with Manual Questions | When running NIWC Enhanced SCAP content, which contains Manual Questions, create the DISA Checklist 'CKL' report, which can be used by systems such as eMASS, and eliminates the need to use the STIG Viewer to import SCC results, answer manual questions and export CKL results. Creating CKL results from 'standard' DISA SCAP content is not supported, as DISA SCAP benchmarks do not contain all of the rules from the STIG Manual, only those that are automated. |
| Save Failed CPE XML result files | This option enables saving of Common Platform Enumeration (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. |

4.4.3.4 Summary Viewer

| OPTION | DESCRIPTION |
|------------------------|--|
| Save Summary Viewer | This option saves an HTML report that is created at the end of each scan, and provides an easy way to see all of the HTML/Text/XML results created by SCC during that scan session. |
| Summary Viewer Sorting | The summary viewer HTML report can be sorted by three fields. This report is primarily useful if more than one computer or content stream is used. Below is the default sort order and a description of each: |

| | |
|--|---|
| | <ol style="list-style-type: none"> 1. Session: The date/timestamp from when the scan started. 2. Stream : The SCAP content or OVAL datastream name being used 3. Host : The hostname for the target computer(s) being scanned. <p>Note: The Summary Viewer can also be sorted manually by clicking on any column of the report after it's generated.</p> |
|--|---|

4.4.3.5 Scan Sessions

| OPTION | DESCRIPTION |
|--|--|
| Save Scan Session Information (directory, scores, filenames) | This option enables creating a scan session database which resides in the root of the SCC results directory, and allows for easy viewing and searching and deleting of existing SCC scan sessions. |
| Double Clicking any log, report or XML file in the session viewer in SCC opens | This option instructs SCC to open SCC created files with a file viewer internal to SCC. If this option is disabled, SCC will attempt to open the file with the Operating System default file viewer based on the file type, although on many linux distributions, this may not work well, as SCC is run as root, and HTML and PDF viewers may not be allowed to run as root. |

4.4.4 Logging Options

4.4.4.1 Logging Options

| 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 | <p>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.</p> <p>Please refer to Appendix A.8 Debugging for additional information on SCC debug logs and their intended usage.</p> |
| Enable Verbose 'TRACE' Level Debug | This option saves even more debug at a very verbose level that is only be recommended to debug crash type issues, as it may generate GB of text and slowdown SCC in general. This option is only available if Save Debug Log is enabled. |
| Suppress Warnings | <p>This option will prevent warnings from being reported. As warnings are not critical, this option may be desired for certain users.</p> <p>This option may be useful in conjunction with 'ignore remote file systems' and 'ignore case' listed in the File Scanning section.</p> |

4.4.5 Output Options

4.4.5.1 Configuration Save Location

| OPTION | DESCRIPTION |
|---|---|
| Save Configuration to the User's Home Directory | <p>This option dynamically sets the base directory in which SCC saves its configuration (5.7.1_options.xml) on a per-user basis.</p> <p><i>Ex: C:\users\TestUser\SCC\Config\5.7.1_options.xml</i></p> |
| Save Configuration to the Running Application Directory | <p>This option sets the based directory in which SCC saves its configuration (options.xml) to the location SCC is running/installed.</p> <p><i>Ex: C:\Program Files\SCAP Compliance Checker 5.7.1\options.xml</i></p> |

4.4.5.2 SCC Security Configuration Directory Options

This is a new option for SCC 5.3, and currently contains the SSH Host Credential Database, SSH trusted keys, and other security related items related to SSH. In the future it could contain other security related configuration.

If SSH based scanning is not used, this directory may not exist, and the SSH Host Credential Database is not created until it is used.

| OPTION | DESCRIPTION |
|--|---|
| Save SCC's Security Configuration to the User Home Directory | <p>This option dynamically sets the base directory in which SCC saves its security configuration to each user's home directory. This option is recommended, both for increased security, and to prevent its accidental removal, as the host credential database is designed to work across multiple installations of SCC.</p> <p><i>Ex: C:\users\TestUser\SCC\Config</i></p> |
| Save SCC's Security Configuration to the Running Application Directory | <p>This option sets the based directory in which SCC saves its security configuration to the location SCC is running/installed.</p> <p>Note: This setting is not recommended, due to potential security issues, and loss of credential data if SCC is uninstalled/reinstalled into the same directory.</p> <p><i>Ex: C:\Program Files\SCAP Compliance Checker 5.7.1\Config</i></p> |
| Save SCC's Security Configuration to a Custom Directory | <p>This option allows the end user to specify any custom directory to save SCC's security configuration.</p> <p>This can be a local path such as C:\SomeDirectory or a network share but only with the UNC path of \\ServerName\ShareName\SomeDirectory. Using a mapped drive such as Z:\SomeDirectory is known to cause errors and is not officially supported.</p> <p>This field is guarded by input validation and will only allow a user to</p> |

| | |
|--|---|
| | enter an absolute directory path that exists. Any input outside of those values will result in an error and the option will not be allowed to be saved. |
|--|---|

4.4.5.3 SCC Results Directory Options

| OPTION | DESCRIPTION |
|---|---|
| Save Results to the User Home Directory | This option dynamically sets the base directory in which SCC saves all Logs and Results on a per-user basis. <i>Ex: C:\users\TestUser\SCC</i> |
| Save Results to the Running Application Directory | This option sets the based directory in which SCC saves all Logs and Results to the location SCC is running/installed. <i>Ex: C:\Program Files\SCAP Compliance Checker 5.7.1</i> |
| Save Results to a Custom Directory | This option allows the end user to specify any custom directory to save all SCC Results and Log. This can be a local path such as C:\SomeDirectory or a network share but only with the UNC path of \\ServerName\ShareName\SomeDirectory. Using a mapped drive such as Z:\SomeDirectory is known to cause errors and is not officially supported. This field is guarded by input validation and will only allow a user to enter an absolute directory path that exists. Any input outside of those values will result in an error and the option will not be allowed to be saved. |

4.4.5.4 SCC Results Subdirectory Options

| OPTION | DESCRIPTION |
|---|--|
| Create 'ApplicationLogs' subdirectory | This option creates a directory to store SCC application logs (those not related to performing a SCAP content scan session) |
| Create 'Sessions' subdirectory | This creates a base directory to store all scan sessions. |
| > Create 'Date/Timestamp' subdirectories | This option automatically creates a subfolder with the 'Date/Timestamp' within the results directory. (This option is highly recommended, as it's required for new scan session viewing feature.) |
| >> Create 'Results' subdirectory | This option automatically creates a subfolder of 'Results' within the Sessions directory |
| >> Create 'Logs' subdirectory | This option automatically creates a subfolder of 'Logs' within the Sessions directory, as a sibling of the 'Results' directory. These 'scan' logs will be directly related to the HTML/Txt/XML files in the 'Results' directory. |
| >>> Create 'SCAP', | This option automatically creates a subfolder based on the content |

| | |
|---|--|
| 'OVAL', 'OCIL' and 'ApplicationLog' directories | 'SCAP', 'OVAL', 'OCIL' within the results directory, and ApplicationLogs within the Logs directory |
| >>> Create 'Content Name' Subdirectories | This option automatically creates a subfolder with the 'Content Name' within the results directory. (This option is disabled by default.) |
| >>>> Create 'Target Name' Subdirectories | This option automatically creates a subfolder with the 'Target Name' within the results directory. (This option is disabled by default.) |
| >>>>> Create 'XML Subdirectory | This option automatically creates a subfolder called XML |

4.4.5.5 SCC Report Filename Options

| OPTION | DESCRIPTION |
|-----------------|---|
| Target Name | This option adds the target host name to resulting report filename. <i>Ex: Computer1_All-Settings_Mozilla_Firefox.html</i> |
| SCC Version | This option adds the SCC version to the report filename: <i>Ex: Computer1_SCC-5.7.1_All-Settings_Mozilla_Firefox.html</i> |
| Content Version | This option adds the content version to the report filename: <i>Ex: Computer1_SCC-5.7.1_All-Settings_Mozilla_Firefox-001.015.html</i> |
| Date/Timestamp | This option adds a date/timestamp to the report filename: <i>Ex: Computer1_SCC-5.7.1_2021-02-17_125008_All-Settings_Mozilla_Firefox-001.015.html</i> |

4.4.5.6 Permission Options

| OPTION | DESCRIPTION |
|---|--|
| Allow SCC to set restricted permissions on SCC created Logs and Results | <p>This option allows SCC to set restricted permissions on the Logs and Results (XML, Text, HTML) created by SCC. This can be useful especially if results are set to write back to the application install, or some other location where non-privileged users have read access.</p> <p>On Windows: SCC sets the permissions to be the user running SCC, Administrators, and System</p> <p>Disabling this option defaults back to the OS defaults.</p> |

4.4.6 SFTP Report File Transfer Options

SCC has the ability to copy results after each scan via SFTP to a centralized server for easier data collection. This option is not related to SSH based scanning, refer to section 4.3 for SSH based scanning of UNIX systems.

Note: *SSHv2 is supported, SSHv1 is not.*

4.4.6.1 SFTP File Transfer Options

| OPTION | DESCRIPTION |
|-------------------------------------|---|
| Enable File Transfers | Transfer any report/log that is enabled |
| Delete Local Results After Transfer | This option will delete the local results off of the machine after SCC has successfully transferred the files to the SSH server |

4.4.6.2 SFTP Server Information

| OPTION | DESCRIPTION |
|-------------|--|
| Hostname/IP | <p>Enter the DNS hostname or IP Address of the SFTP server to copy result to.</p> <p>This field is guarded by input validation and will only allow a user to enter a hostname or ip address. Any input outside of those values will result in an error and the option will not be allowed to be saved.</p> |
| Port | <p>Enter the port which the SFTP server is listening (normally 22)</p> <p>This field is guarded by input validation and will only allow a user to enter a port number between 0 and 65536. Any input outside of those values will result in an error and the option will not be allowed to be saved.</p> |
| Directory | <p>By default, this is set as the user's home directory (e.g. /home/<username>) but can be changed here to reflect the desired directory you would like the reports to be transferred to.</p> <p>This field is guarded by input validation and will only allow a user to enter an absolute directory path that exists. Any input outside of those values will result in an error and the option will not be allowed to be saved.</p> |

4.4.6.3 SFTP Connection Type

| OPTION | DESCRIPTION |
|--|--|
| Connection with Username/Password | Select this option if you plan to authenticate with username/password combination |
| Connection with Private Key/Passphrase | <p>Select this option if you plan to authenticate with a private key.</p> <p>Note: SCC only supports private keys that are secured with a private key passphrase</p> |
| Username | <p>Required for either Username/Password or Private key authentication</p> <p>This field is guarded by input validation and will only allow a user to enter a proper username (eg, nothing that starts with “;”). Any input outside of those values will result in an error and the option will not be allowed to be saved</p> |
| Password | Only required if Username/Password authentication has been selected |
| Private Key | Only required if Private Key/Passphrase authentication has been selected |
| Private Key | Only required if Private Key/Passphrase authentication has been |

| | |
|------------|----------|
| Passphrase | selected |
|------------|----------|

4.4.7 Update Options

4.4.7.1 HTTP Connection Options

| OPTION | DESCRIPTION |
|--|--|
| Use System Proxy | SCC should use the system configured proxy (or not) that has been configured as part of the OS and is used Internet Browsers |
| Use Environment Variable Defined Proxy | Primarily a UNIX/Linux method, but SCC looks for http_proxy or https_proxy environment variables |
| No Proxy | SCC connects without any proxy |
| Custom Proxy | Enter the proxy to be used by SCC, in the format of http://<proxy server>:<port> or https://<proxy server>:<port> |

4.4.7.2 SCC Application Updates

| OPTION | DESCRIPTION |
|--|--|
| Periodically Check for SCC Application Updates | Allow SCC to check for application updates when SCC launches. This feature does not download or install/upgrade SCC, it only notifies the user that an updated version is available. |
| Frequency (Days) | Number of days between SCC Application Checks. |
| SCC Update URL | Internet (or could be updated to an Intranet location) to query for SCC release information. |

4.4.7.3 SCAP Content Updates

| OPTION | DESCRIPTION |
|---|--|
| Periodically Check for SCAP Content Updates | Allow SCC to check for application updates when SCC launches. This feature allows the user to download and install updated content into SCC. |
| Frequency (Days) | Number of days between SCC Application Checks. |
| Include pre-release (Draft/Test) versions of SCAP Content | Internet (or could be updated to an Intranet location) to query for SCAP Content information. |

4.4.7.4 SCAP Content Repository Options

| OPTION | DESCRIPTION |
|--------------------|--|
| Add Repository URL | Press the Add Repository URL button to add a URL to the repository list. |
| Edit | Edit an existing URL by right clicking on it, and clicking Edit. |
| Delete | Delete repository URL by right clicking on it, and clicking Delete. |
| Delete All | Delete all repository URL's by right clicking and selecting Delete All. |

4.4.8 Service Options

Refer to Section 7 - SCC as a Service

4.5 Viewing Results

4.5.1 Viewing Scan Results

After the SCC software completes the review, reports, XML files and any scan related logs can be viewed within SCC by clicking:

'View Results' button on bottom left of main screen

or

Results -> View Results

Scan Sessions:

This section displays scan Sessions, which corresponds to each click of 'Start Scan' or each review performed by command line. Each session may contain many computers, with many different SCAP content streams. When opening this form, the most recent scan session is automatically selected. Left click to select any scan session, or right click for more options. After selecting a session, see Results and Reports below.

Results:

This section displays the high level results of a SCAP scan; it contains the hostname, scap content name, score, error count and warning count. Left click any row to select different Host/content combinations.

Reports/XML/Logs:

This section displays the reports, XML and Logs (if created) based on the Host/Content combination selected in the Results pane. Double click to open the report in SCC, or right click for more options.

4.5.2 Viewing Application Logs

If something unexpected occurs within the SCC GUI, which is not part of a SCAP scan, application logs can be useful in determining the cause.

Results -> View Application Logs

Application Logs:

This form displays any application logs (if any exist, such as screen, debug or error). Double click to open the log in SCC, or right click for more options.

4.6 SCAP scanning with OCIL Manual Questions

Starting with SCC 5.7, SCC includes NWIC 'Enhanced' STIG SCAP content by default, which converts non-automated requirements from the STIG Manual into manual questions in SCC, which are included as OCIL.

4.6.1 Answering Manual Questions in SCC's GUI

1. Click on the desired content in the SCAP content tree.
2. Click on 'Manual Questions' on the Content Details pane.
3. A new Manual Questions form should appear.
4. Click on any row in the tree on the left side of the page, the first question will be selected by default.
5. Select the desired answer from the available options.
6. Enter any comments in the Comments text field.
7. Click 'Save Answer and Comments'.
8. This should take you to the next unanswered question. Repeat until all questions are answered.

4.6.2.1 Save and Close

When you have completed all of the questions, or all that you want to change for now, click "Save Document and Close". This will save your answers and they will be applied to all future scans.

4.6.2.2 Automatic Backups of Manual Questions Results

If you have the option enabled to automatically backup manual question results, a new backup of the text based results will be stored to a subdirectory called Backups, each time you press Save Document and Close Form. If your Manual Question autoanswer results file in the Completed_Results directory somehow gets corrupt or lost, you can manually restore a backup version.

Backups will be in the format of
<BenchmarkID>_<BenchmarkVersion>.txt_<datetime>_<username>

Example:

```
MOZ_Firefox_Windows_6.3.2_Autoanswer.txt_2023-02-16_084507_testUser1
```

To restore a backup file, rename the file from:

```
MOZ_Firefox_Windows_6.3.2_Autoanswer.txt_2023-02-16_084507_testUser1  
to MOZ_Firefox_Windows_6.3.2_Autoanswer.txt
```

Then copy the renamed file from the Backups directory to the Completed_Files directory.

4.6.3 Interaction with Manual Question Autoanswer files

Starting with SCC 5.7, SCC supports a text based method for answering manual questions, via autoanswer text files. SCC's OCIL interface reads from and updates these files, so an end

user can update an autoanswer file, or answer questions via SCC GUI and the results should be the same. Refer to section 5.7 for more information on SCC's new text based manual question autoanswer support.

4.6.4 Upgrading manual question results from an older version of SCC

Starting with SCC 5.7 (on Windows) SCC will prompt to upgrade configuration and manual question results on first launch. If the manual question results are configured to be stored in the application installation directory (default), SCC will copy the files from 5.7 to 5.7.1 etc. If the manual question results directory has been configured to a custom directory, SCC 5.7.1 will use that custom directory, as a side effect of the configuration upgrade.

For Linux: When using package based installation, with the RPM or DEB upgrade method selected, SCC will install to the same directory as previous versions, upgrade the configuration to the current version, and have all of the manual questions results available.

4.6.4 Converting manual question results from one version of SCAP content to another

Starting with SCC 5.7.1, SCC now automatically converts manual question results to the latest SCAP content. Only questions that match the same XCCDF rule and version are updated, so if any change is made to an XCCDF rule in the updated STIG manual, answers will not be converted and those questions will need to be re-answered.

4.7 XCCDF Tailoring

SCAP 1.2 and SCAP 1.3 specifications allow for a separate 'tailoring' XML file which allows users to customize certain portions of the XCCDF stream, without modifying the source XML file.

Customizations include:

- Creation of a new profile
 - All modifications will be reported under a new profile, with the original profile name followed by "_tailored"
- Selecting and deselecting rules and groups
 - This allows users to disable rules that may cause incorrect results, or take too long to complete.
 - Results will be marked as 'not selected'
- Modifying refine-rules, values and refine-values
 - This allows users to modify certain rules to meet their organizational requirements. Note that not all rules will have modifiable values, and OVAL XML content may need to be edited.

SCC supports this feature, and provides a graphical interface for creating and editing the XCCDF tailoring file.

4.7.1 Selecting/Deselecting Groups and Rules

To enable/disable rules or groups:

1. Left click on the checkbox on the far left on any row listed with a Type of "Group" or "Rule".
2. Enabling or Disabling a group will cascade Enable/Disable to all sub-groups and rules.
3. Enabling/Disabling can also be performed by left clicking on the row, and clicking the check-box in the right hand window.

Note: Per XCCDF 1.2 specifications, if a Group is disabled, no sub-groups or rules under it are evaluated (even if they are enabled manually). If a group is enabled, the sub-groups and rules are processed based on their individual selected/deselected status.

4.7.2 Refine Rules

To refine a rule:

1. Left click on a row listed with a Type of "Refine-Rule"
2. Edit any of the available fields in the right hand window
 - a. Weight
 - b. Role
 - c. Severity
 - d. Selector
 - e. Remarks

Note: This feature has not been seen in any publicly available content, so end users may not see "Refine-Rules" in any rows.

4.7.3 Values and Refine-Values

To modify a value:

1. Click on any row in tree listed with a Type of "Value"
 - A. Enter the desired value in the 'Set Value To' field, and click "Apply Value"OR
 - B. Select the Refined Value Selector

Note that the Refine Value Selector may only have a single row, unless the SCAP content contains multiple options to choose from.

Note: Values and refine-values may not be present in content.

4.7.4 Saving XCCDF Tailoring

Click Save and Close. The selected profile on the main SCC form should be updated to reflect the new <Profile>_tailored profile.

4.7.5 Entering XCCDF Tailoring File Creator Info

After clicking Save, a form will appear with the following fields. These will all be saved to the resulting XML results and HTML/Text reports if enabled.

| Field | Description |
|---------------------|---|
| Agency/Organization | Enter your Agency/Organization Name |
| Full Name | Enter your full name |
| Notes | Enter any notes that help explain why this XCCDF Tailoring file was created. |
| Version | Enter a version for this XCCDF Tailoring file |
| Status | Select the status of this XCCDF Tailoring file (Draft, Accepted, Deprecated, Incomplete, Interim) |

4.8 Cisco IOS / IOS XE Offline (Show Tech) File Scanning

This option instructs SCC to scan an existing Cisco IOS/IOS-XE "show tech" file. The file format required for this type of assessment is very specific. To create a configuration file suitable for using in SCC:

1. Logon to the device with full (level 15) privileges (enable mode)
2. Type "show tech" saved to a single text file
3. Save the file as "<devicename>_<date>.txt"
NOTE: Save this file as Text Only with Line Breaks using a plain text editor such as Notepad. Do not use Microsoft Word or other document editor. Only one device per file
4. Disable any Windows or UNIX SCAP/OVAL content, otherwise many content errors will be reported
5. Enable just Cisco IOS specific SCAP/OVAL content

4.8.1 Browse for Cisco IOS / IOS XE Show Tech File

This option allows the end user to select a single file, either a text file (.txt) containing single Cisco IOS/IOS-XE "show tech" file, or a zip file containing a collection of Cisco IOS/IOS-XE "show tech" configuration file.

4.8.2 Browse for a directory containing Cisco IOS / IOS XE show tech files

This option allows the user to select a directory which contains a collection of text (.txt) based Cisco IOS/IOS-XE show tech files.

4.8.3 Appending other 'show' commands not included in 'show tech'

In the event that one or more IOS line tests error due to unsupported "show" commands, take note of the list of unsupported commands that are listed at the end of the analysis. Most Cisco IOS content is likely to attempt collection of "show" command output that is not provided by the "show tech" or "show tech-support" commands by default. The best recourse is to manually execute any unsupported commands and append their output to the "show tech" command output, or to perform the scan via SCC's SSH based scanning mode and let SCC collect all of the required show commands automatically.

To manually append additional 'show' command to an existing 'show tech' file:

1. Logon to the device with full (level 15) privileges (enable mode)
2. Execute the listed commands
3. Copy the output of each command and append it to the original "show tech" output file with a leading header on its own line that specifies the command that generated the output
4. Ensure each header consists of a sequence of 18 hyphens, a space, full show command (no shorthand notation), another space, and 18 more hyphens for consistency with the default "show tech" command output

Example:

```
<existing output of show tech> then
```

```
----- show startup-config -----  
Using 3130 out of 524284 bytes, uncompressed size = 8791 bytes  
!  
<output of show startup-config>
```

4.9 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. Follow instructions for Installing & Configuring Content (Section 4.2)
3. If standalone OVAL content is found during the content install, an OVAL content tab will appear for enabling/disabling content.

4.9.1 External Variables

If standalone OVAL content uses an external variables file, the file will need to match the name of the base oval document, but ending with "external-variables.xml". When installing standalone OVAL with external variables, just include the file in the zip file to be installed.

Example:

- MyContent.zip
 - myOVALContent.xml
 - myOVALContent_external-variables.xml

4.10 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.

4.10.1 Installing OCIL content

1. Launch the Graphical User Interface of SCC
2. Follow instructions for Installing & Configuring Content (Section 4.2)
3. If standalone OCIL content is found during the content install, an OCIL content tab will appear for enabling/disabling content.

SCC will also search 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. For more information please see section 4.4.

OCIL schema validation occurs during installation of the OCIL content. If the OCIL content is deemed invalid, SCC will inform the user via a dialog box but will continue the installation process. The user will be notified of the result of the installation process in a separate dialog box.

4.10.2 Performing a standalone OCIL analysis

4.10.2.1 Creating and Selecting OCIL Targets

Unlike the automated portions of SCC, which the target is always a computer, whose hostname is automatically populated by programmatic means during the scan, with OCIL, the target could be a computer/system or a user/person, and each will need to be manually entered.

To create a new system target, click on the 'add target system' in the in upper left corner of the form. Then enter in as much information as you have.

| FIELD | DESCRIPTION |
|--------------|---|
| System Name | The name of the system, generally a computer, which is the target for the checklist. This field is mandatory. |
| IP Address | Optional field to report on the IP Address associated with this system. |
| Organization | Optional field to document the organization that the system is a part of. |
| Description | Optional field to enter any other information about this system that might be relevant. |

To create a new user target, click on the 'add target user' in the in upper left corner of the form. Then enter in as much information as you have.

| FIELD | DESCRIPTION |
|--------------|---|
| Full Name | The name of full name of the person being interviewed. This field is mandatory. |
| Email | Optional field to report on the email address of the person being interviewed. |
| Organization | Optional field to document the organization that the person is a part of. |
| Description | Optional field to enter any other information about this person that might be relevant. |

After creating and selecting the desired targets, click "Continue".

4.10.2.2 Answering Questions on the OCIL Document Form

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.

4.10.2.3 Entering Artifacts

For each question, the user can manually enter an artifact which may help explain the results. To enter an artifact, click on the Add Artifact button.

4.10.2.4 Entering Content Mandated Artifacts

The OCIL content can also ask specifically for artifacts, which will cause a new form to appear, which contains:

| FIELD | DESCRIPTION |
|-------------|---|
| Title | Content provided title |
| Description | Content provided description, likely explaining what data the end user should provide |
| Artifact | Location for the end user to enter data as specified in the Description field. |
| Save | After entering Data, click Save to close this form. |

4.10.2.5 Save and Close

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

4.10.3 Generating Reports

If you have answered all of the OCIL Questionnaire, click "Create Reports" to proceed to creating reports with the results.

4.11 Post Scanning Report Generation

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

4.11.1 Select Directories

| OPTION | DESCRIPTION |
|--|---|
| Source Directory | Location for the application to scan for XCCDF and/or 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. |

4.11.2 Reports

4.11.2.1 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:

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.

4.11.2.1.1 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. |

4.11.2.2 Generate Detailed SCAP Reports (from ARF or XCCDF/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.

4.11.2.2.1 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. |

4.11.2.3 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.

4.11.2.3.1 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. |

4.11.3 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 |

4.11.4 Generate 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.

4.11.5 Viewing Reports

After Multi-Computer Summary Reports are created 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.

4.12 File and Help Menus

4.12.1 File Menu

| MENU ITEM | DESCRIPTION |
|-------------------------|---|
| Load Options | <p>This will delete your current options file and replace it entirely with the file you specify. This is only applicable to options files that match the same version of the SCC application as you are running. If an options file from an older version of SCC is specified, it quite likely will fail schema will fail, and errors will be reported.</p> <p>This is not intended as an upgrade feature.</p> |
| Save Options As | <p>This will make a copy of your options XML file for backup purposes or for sharing with another installation of SCC.</p> |
| Upgrade Options | <p>This will upgrade your current installation of SCC using an existing options xml from an existing installation of SCC. This will not delete your current options file, it will keep your current options, and overlay them with the matching configuration settings from the previous installation. There are exceptions to this, as specified below:</p> <ul style="list-style-type: none">○ Content is not upgraded, nor are the enabled/disabled status for content.○ appUpdateURL and contentRepository settings are intentionally excluded, as they may change in a future release of SCC and upgrading could cause issues. If you have your own SCAP content repository or SCC application update repository setup, these files can be manually configured after the upgrade is complete. |
| Restore Default Options | <p>This will delete your current options XML file, and restore them using the installation defaults.</p> |
| Exit | <p>Exits the SCC application.</p> |

4.12.2 Help Menu

| MENU ITEM | DESCRIPTION |
|---------------------------|---|
| Help | <p>Opens the SCC compiled help application (Windows Only).</p> |
| User Manual | <p>Opens this PDF.</p> |
| Online Tutorials | <p>Opens a web browser to https://www.niwcatlantic.navy.mil/scap/videos/</p> |
| Release Notes | <p>Displays SCC's Release Notes file.</p> |
| Check For Content Updates | <p>Downloads a small XML file from the URL(s) specified in the Options -> Update Options -> Content Repositories option, and then compares current content to that in the XML file and prompts the user to install any new or updated SCAP content.</p> |
| Check for SCC App Updates | <p>Downloads a small XML file from the URL(s) specified in the Options -> Update Options -> SCC Update URL option, and then compares current content to that in the XML file and informs the user if there is an</p> |

| | |
|----------------------------|---|
| | updated version of SCC available for download. |
| End User License | Displays SCC's End User License Agreement. |
| Third Party Licenses | Displays a listing of all Third Partly Licenses in use by SCC. |
| Rate SCC via Online Survey | Our survey is now online 24/7 and we get reports on a monthly basis, so you can rate what you think of the SCC application and our tech support anytime. The website is: https://usnavy.gov1.qualtrics.com/jfe/form/SV_4ZpXv8JkUIDs4lw |
| About | Lists SCC's version, build number and supported SCAP features, and contact information. |

5. COMMAND LINE USAGE

SCC has a separate executable for command line usage which is included in the installation package as 'csc.exe'. The Command-line SCAP Compliance Checker (CSCC) allows for scripted or automated reviews by other applications or scheduled tasks.

Any changes made via the SCC GUI 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.

```
csc.exe -? or csc.exe --help
```

5.1.1 Open a Command Prompt

Open an command prompt (admin for any local scanning) and change directory to the SCC installation directory.

Example:

```
Start -> Run -> cmd
```

```
c:
```

```
cd "\Program Files\SCAP Compliance Checker 5.7.1"
```


5.2 Command Line Configuration Parameters

5.2.1 Configuration Parameters

Below are the parameters available for installing content and configuring application options. All of the following options must be used individually, and are not compatible with any other parameter.

For descriptions of each option available to be edited, refer to section 4.4, Editing Options

To see the help related to configuration parameters run '**csc.exe --help config**'

```
#####  
CONFIGURATION PARAMETERS:
```

Below are the parameters available for installing content and configuring application options. All of the following options must be used individually, and are not compatible with any other parameter.

--config

Open a command line menu which displays several configuration options

-eb, --enableBenchmark BENCHMARK_ID [version]

Enable a benchmark based on its ID, with optional benchmark version.

Example: **csc.exe --enableBenchmark Windows_10_STIG**

Example: **csc.exe --enableBenchmark Windows_10_STIG 001.002**

See **--listAllBenchmarks** for a list of benchmarks.

-db, --disableBenchmark BENCHMARK_ID [version]

Disable a benchmark based on its ID, with optional benchmark version.

Example: **csc.exe --disableBenchmark Windows_10_STIG**

Example: **csc.exe --disableBenchmark Windows_10_STIG 001.002.**

See **--listAllBenchmarks** for a list of benchmarks.

-ea, --enableAll

Enable all SCAP and OVAL content.

-da, --disableAll

Disable all SCAP and OVAL content.

-ub, --uninstallBenchmark BENCHMARK_ID [version]

Uninstall a benchmark based on its ID, with optional benchmark version.

Example: cscce.exe --uninstallBenchmark Windows_10_STIG

Example: cscce.exe --uninstallBenchmark Windows_10_STIG 001.002

See --listAllBenchmarks for a list of benchmarks.

-ua, --uninstallAll

Uninstall all SCAP and OVAL content.

--setProfile PROFILE BENCHMARK_ID

Set a profile to be applied to a specified content stream.

See --listAllProfiles for a list of profiles.

See --listAllBenchmarks for a list of benchmarks.

Example: cscce.exe --setProfile MAC-3_Sensitive Windows_10_STIG

--setProfileAll PROFILE

Set a profile to be applied to all content installed in SCC, if applicable. If a profile cannot be applied to a content stream it is not applicable. See --listAllProfiles to obtain a list of profiles.

Example: cscce.exe --setProfileAll MAC-3_Sensitive

--setOpt OPTION VALUE

Advanced user setting which allows command line configuration of any SCC option to a user specified value.

--setOpt can be called multiple times in a single command if needed, see second example.

Available options can be found in --listOpt, and need to be specified exactly. To set a value to an empty string, enter the value as all caps

NULL

Example: cscce.exe --setOpt dirSessionEnabled 0

Example: cscce.exe --setOpt dirSessionEnabled 0 --setOpt debugEnabled 1

--generateOptionsFile

Delete the options file, restore default settings, and reinstall all content. Note that this may take a few minutes.

--generateAutoAnswerTemplates

Delete and regenerate all of the Manual Question auto-answer template files found in

Resources/Content/Manual_Questions/Templates

--restoreDefault

Restore all options to installation default.

-is FILE PROFILE [--force], --installScap FILE PROFILE [--force]

Install one or more SCAP content streams from an XML file or ZIP archive. Specifying an XCCDF benchmark profile name after the filepath will enable that profile for the given SCAP stream. Use the optional --force switch to reinstall

Example: cscs -is C:\Users\User1\SampleScapContent.zip

Example: cscs --installScap C:\Users\User1\SampleScapContent.zip

Example: cscs -is C:\Users\User1\SampleScapContent.zip MAC-3_Sensitive

Example: cscs -is --force C:\Users\User1\SampleScapContent.zip

Example: cscs --installScap --force
C:\Users\User1\SampleScapContent.zip MAC-3_Sensitive

-isr FILE PROFILE [--force], --installScapRun FILE PROFILE [--force]

Install, enable, and conduct an analysis with a SCAP Content stream from a zip file. Specifying an XCCDF benchmark profile name after the filepath will enable that profile for the given SCAP stream.

Use the optional --force switch to reinstall.

Example: cscs -isr C:\Users\User1\SampleScapContent.zip

Example: cscs --installScapRun C:\Users\User1\SampleScapContent.zip
MAC-3_Sensitive

Example: cscs -isr --force C:\Users\User1\SampleScapContent.zip

Example: cscs --installScapRun --force
C:\Users\User1\SampleScapContent.zip MAC-3_Sensitive

-iv FILE [--force], --installOval FILE [--force]

Install OVAL Content from a single xml file or a zip file containing multiple xml files. Use the optional --force switch to reinstall.

Example: cscs --installOval C:\Users\User1\sampleOval.xml

Example: cscs -iv --force C:\Users\User1\sampleOval.xml

-ivr FILE [--force], --installOvalRun FILE [--force]

Install, enable, and conduct an analysis with OVAL Content from a single xml file or a zip file containing multiple xml files. Use the optional --force switch to reinstall.

Example: cscs --installOvalRun C:\Users\User1\sampleOval.xml

Example: cscs -ivr --force C:\Users\User1\sampleOval.xml

--installTailoringProfile FILE

Install an existing XCCDF Tailoring Profile file from another installation of SCC, created by the SCC GUI Tailoring interface.

Installing a tailoring profile will set the selected profile for the matching content to be the tailored profile in the selected tailoring file

Example: `cscs --installTailoringProfile <filepath to tailoring xml>`

--checkForContentUpdates [--installUpdates | --installAll]

Check for SCAP content updates from an online content repository.

Additional settings may need to be pre-configured before usage.

refer to: `cscs --config -> Options -> Update Options`

Example: `cscs --checkForContentUpdates`

Example: `cscs --checkForContentUpdates --installUpdates`

Example: `cscs --checkForContentUpdates --installAll`

--installUnixPlugin FILE

Install the UNIX Plugin file, to allow SSH based scanning of remote UNIX hosts. The file below can be obtained from the same location you downloaded SCC: `SCC_5.5_UNIX_Remote_Scanning_Plugin.scc`

Example: `cscs --installUnixPlugin`

`<path>SCC_5.5_UNIX_Remote_Scanning_Plugin.scc`

Refer to `--installCredentialDB` if this computer does not have the ability to open the SCC GUI to update/maintain the hosts/credentials

--installCredentialDB FILE

If this computer is not able to open the SCC GUI to create/maintain the SCC Host Credential Database, which is used to enter hosts and credentials for SSH based remote scanning of UNIX and Cisco devices, this feature allows you to install a previously created Host Credential Database and use it for scanning.

*** NOTE 1: You will not be able to create new hosts, or edit credentials, just perform scans using the Master Password for the existing set of hosts/credentials. When host passwords expire, or the Master Password expires, you'll need to obtain an updated Host Credential DB and reinstall it via this command.

*** NOTE 2: This feature will always overwrite the existing host credential db (if found). You will need to manually copy the `hostCredentials.db` from another installation, by default it's found in `<your home directory>\SCC\Config`

--register EMAIL REGISTRATION_CODE

This command line argument is used to register your email address with a code

provided from the SCC team, obtained by emailing `scc.fct@navy.mil`, indicating

that your team/group/agency is planning to send some level of funding in the future.

Registering your email address makes the funding notice go away.

--upgrade FILE

Upgrade the configuration options from a previous installation of SCC.

SCC will load the current settings, and overlay the configuration settings from the selected option file, excluding content, appUpdateURL and contentRepository.

Example: `csc --upgrade <filepath to existing SCC options xml>`

5.3 Command Line Scanning Parameters

5.3.1 Scanning Parameters

Below are the parameters available for performing scans. Many of the options can be used in combination, unless indicated below. Any configuration change from a Scanning Parameter is temporary, and does not get saved for future use.

To see the help related to scanning parameters run '**cscce.exe --help scan**'

```
#####
```

SCANNING PARAMETERS:

Below are the parameters available for performing scans. Many of the options can be used in combination, unless indicated below. Any configuration change from a Scanning Parameter is temporary, and does not get saved for future use.

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

-d, --debug

Create a verbose debug log file in the Logs directory for troubleshooting purposes.

-ds, --debugToScreen

Debug to the Screen. This option will print a very large amount of data to the terminal, which can be captured and shared with our team, and should only be used to help diagnose crash type issues.

-ear, --enableAllRun

Enable all SCAP and OVAL content and run content.

-u DIRECTORY, --userDir DIRECTORY

Temporarily configure SCC to save user results and logs to the specified directory path.

Example: cscce -u C:\Users\User1

-cd DIRECTORY, --configDir DIRECTORY

Temporarily configure SCC to save application configuration files to the specified directory path.

Example: cscce -cd C:\Users\User1

-f FILE, --file FILE

Review all Windows computers specified in the new line delimited host file.

Example: `csc -f C:\Users\User1\sampleHosts.txt`

-h HOSTNAME, --host HOSTNAME

Review the specified computer.

Example: `csc -h testcomputer1`

--wmi --file FILE | --domain | --ou "OU=OU Name"

Review all computers specified with WMI method.

Note 1: Many command line parameters such as `-d`, `-q`, `-r`, `-mr`, `-ear` are not compatible with `--wmi` and should be configured via `--setOpt` or `--config` prior to calling `csc --wmi`

Note 2: If the WMI alternate credentials feature is enabled, you will be prompted for the master password. For any automated scripting, the alternate credentials mode will need to be disabled, which is the default.

Note 3: If using the `--ou` method, make sure to use the following format (including quotes) `"OU=Your Ou Name"` If the OU is a child of another OU, use the LDAP comma separated format of `"OU=OU Child,OU=OU Parent"`

To scan multiple OU's, separate OU declarations with a semicolon ; (no spaces)

`"OU=OU Child1,OU=OU Parent1;OU=OU Child2,OU=OU Parent2"`

Example: `csc --wmi --file C:\Users\User1\sampleHosts.txt`

Example: `csc --wmi --domain`

Example: `--wmi --ou "OU=Test Computers,OU=Lab"`

Example: `csc --wmi --ou "OU=Test Computers1,OU=Lab;OU=Test Computers2,OU=Lab"`

--scanDomain [nslookup ping]

Review the entire active directory domain using 'classic' mode.

Optionally verifying via nslookup and/or ping

--force32

Open the 32 bit version of SCC on 64 bit Windows

--ssh [cisco|unix]

Review all Cisco IOS/IOS-XE OR UNIX computers enabled in the Host Credential Manager, which is only available via the SCC GUI. You will be prompted to enter the SCC Host Credential Master Password in order to perform a remote command line SSH based scan.

Note that many command line parameters such as `-d`, `-q`, `-r`, `-mr`, `-ear` are not compatible with `--ssh` and should be configured via `--setOpt` or `--config` prior to calling `csc` `--ssh`

'`--ssh unix`' can be used in combination with `--wmi` to scan both UNIX and Windows remotely at the same time.

Refer to `--installCredentialDB` for installing an existing SCC Host Credential Database from another system which is able to use the SCC GUI

`--cisco FILE`

Conduct an offline review against a Cisco IOS/IOS XE configuration file or ZIP archive of multiple configuration files located at the given file path.

**** Configuration files should be created with the 'show tech' command

Example: `csc --cisco C:\Users\User1\sampleConfigFile.txt`

`-o FILE, --options FILE`

Review using the specified options file.

Example: `csc -o options.xml`

Example: `csc --options C:\Users\User1\myOptions.xml`

`-q, --quiet`

Review in quiet mode. No output will be displayed on the screen.

`-r XCCDF_RULE_OR_OVAL_DEF, --rule XCCDF_RULE_OR_OVAL_DEF`

Review a single Rule using the Rule ID from the XCCDF file or review a single definition from an OVAL document.

Example1: `csc -r account_lockout_duration`

Example2: `csc -r oval:mil.disa.stig.adobe.reader:def:1`

`-mr RULE_COUNT RULE_ID RULE_ID ..., --multipleRules RULE_COUNT RULE_ID...`

Review multiple rules using the Rule ID from the XCCDF file or review X definitions from an OVAL document.

Example1: `csc -mr 2 account_lockout_duration logon_as_service`

Example2: `csc --multipleRules 3`
`oval:mil.disa.stig.adobe.reader:def:1`
`oval:mil.disa.stig.adobe.reader:def:2`
`oval:mil.disa.stig.adobe.reader:def:3`

`-rr XCCDF_RULE_ID REGULAR_EXPRESSION --ruleRegex XCCDF_RULE_ID REGULAR_EXPRESSION`

Review all rule IDs in the selected profile that match the regular expression

Example1: `csc -rr rule_SV-213143r55.*`

Example2: `csc -ruleRegex mscp.content_rule_sysprefs_.*`

5.3.2 Command Line Examples

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

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

2. Review several computers from a text file of hostnames with customized report settings.

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

3. Review a single remote host 'computer1' in debug mode

```
csc.exe -h computer1 -d
```

5.4 Option Descriptions and Datatypes

Below are all of the options that can be configured via the --setOpt command line parameter, which is primarily designed for advanced users to automate command line reviews. This information (with the exception of the description) can be obtained by running the --listOpt command.

Example: `csc - --listOpt`

| OPTION | DESCRIPTION | DATATYPE |
|---|--|--|
| GENERAL SCANNING OPTIONS | | |
| <code>reviewType</code> | Type of review | String ('local', 'cisco', 'remote', 'multiremote' (remote/multiremote for Windows only)), cisco-remote, unix-remote, windows-unix-remote |
| <code>offlineConfigPath</code> | Target if 'reviewType' equals 'cisco', This is a fully qualified path to a valid CiscoIOS configuration text file | String |
| REMOTE SCANNING OPTIONS (WINDOWS ONLY) | | |
| <code>hostName</code> | Target of SCC scan if 'reviewType' equals 'remote' | String |
| <code>hostFile</code> | Fully qualified path to a text file containing NetBIOS names of Windows computers, one per line | String |
| <code>multiRemoteMode</code> | Mode to determine how to create/select host file. | String (Host File, Entire Domain, Selected OU) |
| <code>remoteWindowsOU</code> | Name of OU (or OU's), delimited by ; | String |
| <code>remoteWMIEnabled</code> | This option used to determine if remote Windows scans should be WMI based | Boolean (0/1) |
| <code>alternateWMICredentials</code> | Use other credentials for WMI bases scans. | Boolean (0/1) |
| WMI/SSH REMOTE SCANNING OPTIONS | | |
| <code>remoteScanHostCooldown</code> | Number of seconds between SSH/wmi connections. This will slow down refresh to the screen, but also decrease the number of auditable events for long running SSH scans. | Integer |
| <code>remoteBaseLocation_unix</code> | Base directory to which SCC | String |

| | | |
|--|---|-------------------------------|
| | should create sub-directories for SSH based scanning. This directory must exist on the target system. Default is /opt | |
| remoteStartupTimeout | Number of minutes to wait before assuming SCC is unable to start on target computer. | Integer |
| remoteMaxThreads | Maximum number of WMI scanning threads to create on 64 bit Windows | Integer |
| remoteMaxThreads32 | Maximum number of WMI scanning threads to create on 32 bit Windows | Integer |
| SCAP PROCESSING OPTIONS | | |
| ignoreCPEOVALResults | Run SCAP content even if CPE OVAL applicability fails | Boolean (0/1) |
| answerOCILwithSCAP | Enable answering OCIL manual questions if found in a SCAP Content Datastream. | Boolean (0/1) |
| filterSCAPContentPerFamily | Only display (and run) content that matches the family (windows/unix/cisco). | Boolean (0/1) |
| downloadExternalFiles | Download external SCAP 1.2 content files | Boolean (0/1) |
| forceOVAL510 | Force OVAL results be compliant with 5.10.1 for SCAP 1.2 validation purposes | Boolean (0/1) |
| saveResultsForNotApplicableContent | Force saving of results for non-applicable content to pass SCAP 1.3 validation. | Boolean (0/1) |
| OVAL PROCESSING OPTIONS | | |
| ignoreRemoteFileSystems | Do not perform any file searches on remote file systems | Boolean (0/1) |
| ignoreCase | Ignore case specific content requirements for searching files, paths, registry keys, etc | Boolean (0/1) |
| itemCreationThresholdEnabled | Enable setting a maximum number of items to create, to save memory usage in SCC | Boolean (0/1) |
| itemCreationThreshold | Numeric value for item creation threshold if itemCreationThresholdEnabled equals 1 | Integer between 0 and 999999. |
| OVAL PROCESSING OPTIONS (UNIX ONLY) | | |
| maskPasswords | Do not display UNIX password hashes to reports or XML files, does not impact test accuracy. | Boolean (0/1) |
| useGetpwent | Use the system command of getpwent instead of parsing /etc/passwd | Boolean (0/1) |

| | | |
|---|--|--------------------|
| ignoreFileExtendedACL | Do not collect extended ACL information which can be time consuming, and may not be acutally used in SCAP content | Boolean (0/1) |
| OVAL PROCESSING OPTIONS (WINDOWS ONLY) | | |
| onlyCollectSecurityPrinciplesThatHavePrivilegesAssigned | Only report on users/groups that have access token data assigned to them, used to save time when scanning large domain controllers | Boolean (0/1) |
| windowsRegistryUserAge | Obsolete, do not use. | n/a |
| OCIL PROCESSING OPTIONS | | |
| sortOCILQuestionsByDISACAT | Sort OCIL Questionnaires by DISA CAT level (CAT I, CAT II, CAT III) | Boolean (0/1) |
| backupManualQuestionResults | GUI only option to backup manual questions results when SCC GUI saves manual question data to file | Boolean (0/1) |
| customManualQuestionAutoAnswerDirectoryValue | Enable user selected autoanswer result directory | Boolean (0/1) |
| customManualQuestionAutoAnswerDirectory | Directory specified by the end user to obtain autoanswer | String (Directory) |
| SCAN REPORTING OPTIONS | | |
| allSettingsHTMLReport | Save the All Settings HTML report at the end of each scan | Boolean (0/1) |
| allSettingsTextReport | Save the All Settings Text report at the end of each scan | Boolean (0/1) |
| nonComplianceHTMLReport | Save the Non-compliance HTML report at the end of each scan | Boolean (0/1) |
| nonComplianceHTMLReport | Save the Non-compliance HTML report at the end of each scan | Boolean (0/1) |
| allSettingsSummaryHTMLReport | Save the All Settings Summary HTML report at the end of each scan | Boolean (0/1) |
| allSettingsSummaryTextReport | Save the All Settings Summary Text report at the end of each scan | Boolean (0/1) |
| nonComplianceSummaryHTMLReport | Save the Non-compliance Summary HTML report at the end of each scan | Boolean (0/1) |
| nonComplianceSummaryTextReport | Save the Non-compliance Summary Text report at the end of each scan | Boolean (0/1) |
| XML RESULTS OPTIONS | | |
| keepXCCDFXML | Save the XCCDF XML Results at the end of each scan | Boolean (0/1) |

| | | |
|-------------------------------|---|---|
| keepOVALXML | Save the OVAL XML Results at the end of each scan | Integer (0/1/2/3) 0 =Keep full oval 1= Keep oval without system characteristics 2 = Keep "thin" OVAL 3 = Do not keep OVAL XML |
| keepOCILXML | Save the OCIL XML Results at the end of each scan | Boolean (0/1) |
| keepARFXML | Save the ARF XML Results at the end of each scan | Boolean (0/1) |
| keepCPEXML | Save the CPE-OVAL results if CPE-OVAL results return false (not applicable to target) | Boolean (0/1) |
| SUMMARY VIEWER OPTIONS | | |
| enableSummaryViewer | Enable the Summary Viewer HTML report to provide hyperlinks to all results from a scan | Boolean (0/1) |
| summaryViewerSort1 | Set which field to sort the Summary Viewer Report by first | Case sensitive string (Session, Stream, Host) |
| summaryViewerSort2 | Set which field to sort Summary Viewer Report by second | Case sensitive string (Session, Stream, Host) |
| summaryViewerSort3 | Set which field to sort Summary Viewer Report by third | Case sensitive string (Session, Stream, Host) |
| LOGGING OPTIONS | | |
| keepScreenLogs | Save screen logs from each application/scan session | Boolean (0/1) |
| debugEnabled | Save debug logs from each application/scan session | Boolean (0/1) |
| suppress_warnings | Don't print warnings to the error log | Boolean (0/1) |
| debugExcludeDateTime | Do not print date/time stamps on every line of debug, which allows for easier comparison between debug logs | Boolean (0/1) |
| debugTraceEnabled | Print Trace level debug, which is more than default, enable with caution | Boolean (0/1) |
| maxLogFileSize | Maximum size for logs (primarily debug) before creating a new file | Integer (MB) |
| OUTPUT OPTIONS | | |

| | | |
|--|---|--|
| <code>sharedOptions</code> | Save options to SCC install directory? | Integer (1 = install to shared/install directory, 0 = install to users home directory) |
| <code>userResultsDirectory</code> | Path to which SCC will save results | String that is an absolute directory path |
| <code>userResultsDirectoryValue</code> | How 'userDataDirectory' is determined | Integer (0 = User's home directory, 1 = Running Application Directory, 2 = Custom Directory) |
| <code>userConfigDirectory</code> | Path to which SCC will save configuration information. | String that is an absolute directory path |
| <code>userConfigDirectoryValue</code> | How 'userConfigDirectory' is determined. | Integer (0 = User's home directory, 1 = Running Application Directory, 2 = Custom Directory) |
| <code>customPathLocal</code> | Path to which SCC will save temporary files. Default location will be <scc install>/Local directory. This setting can only be configured via command line with --setOpt | String (Absolute Directory Path, Empty String = default location" |
| OUTPUT SUBDIRECTORY OPTIONS | | |
| <code>dirApplicationLogsEnabled</code> | Create a subdirectory called 'ApplicationLogs' for application logs. | Boolean (0/1) |
| <code>dirAllSessionsEnabled</code> | Create a subdirectory called 'Sessions' for sessions. | Boolean (0/1) |
| <code>dirSessionEnabled</code> | Create a date/time subdirectory of the scan | Boolean (0/1) |
| <code>dirSessionResultsEnabled</code> | Create a results subdirectory of the date/time of the scan. | Boolean (0/1) |
| <code>dirSessionLogsEnabled</code> | Create a logs subdirectory of the date/time of the scan. | Boolean (0/1) |
| <code>dirContentTypeEnabled</code> | Create a results subdirectory based on content type (SCAP/OVAL/OCIL) | Boolean (0/1) |
| <code>dirTargetNameEnabled</code> | Create a results subdirectory based on the target hostname. | Boolean (0/1) |

| | | |
|--------------------------------|--|---|
| dirStreamNameEnabled | Create a results subdirectory based on the content stream name. | Boolean (0/1) |
| dirXMLEnabled | Create an results subdirectory called 'XML' for saving XML results. | Boolean (0/1) |
| OUTPUT FILENAME OPTIONS | | |
| fileTargetNameEnabled | Include the target hostname in the result filenames | Boolean (0/1) |
| fileSCCVersionEnabled | Include the SCC version in the result filenames | Boolean (0/1) |
| fileTimestampEnabled | Include scan date/timestamp in the result filenames | Boolean (0/1) |
| fileContentVersionEnabled | Include the Content version in the result filenames. | Boolean (0/1) |
| CONTENT OPTIONS | | |
| newerContentInstall | What to do when installing a newer version of the same SCAP benchmark. | 0 = Do nothing. 1 = Disable older content, 2 = Archive older content, 3 = deleted older content. Integer (0/1/2/3) |
| contentDevModeSkipValidation | Allow for developer mode. | Boolean (0/1) |
| validateContent | Perform XML schema validation before scanning | Boolean (0/1) |
| validateContentOnInstall | Perform XML schema when installing content | Boolean (0/1) |
| validateDigitalSignature | Perform XML digital signature validation on SCAP 1.2 content before scanning | Boolean (0/1) |
| failOnXMLDSig | Do not scan if XML digital signature validation fails | Boolean (0/1) |
| validateXMLResults | Perform XML schema validation on XML results generated by SCC | Boolean (0/1) |
| UPDATE OPTIONS | | |
| httpProxyType | The type of proxy to be used for HTTP request. 0 for system proxy, 1 for env proxy, 2 for no proxy, and 3 for custom proxy | Integer (0-3) |
| httpProxyURL | URL to use for a custom proxy. | String |
| appCheckForUpdates | Check for SCC application Updates. | Boolean (0/1) |
| appUpdateCheckFrequency | Days between checking for updated SCC. | Integer (>0) |
| appUpdateLastCheck | UNIX time of last SCC app update check. | Integer |
| appUpdateURL | URL to SCC update file. | String |

| | | |
|---|--|---|
| contentCheckForUpdates | Check for content Updates | Boolean (0/1) |
| contentUpdateCheckFrequency | Days between checking for updated content | Integer >0 |
| contentUpdateLastCheck | NIX time of last content update check. | Integer |
| includeDraftContent | Include pre-release (draft/test) content. | Boolean (0/1) |
| contentRepository | List of content repository URL's | String(s) |
| DEVELOPER OPTIONS: MISC THRESHOLDS | | |
| maximumRecentReports | Number of recent reports (or scan sessions) to save in the Recent Reports menu | Integer |
| freeSpaceThreshold | Minimum amount of free space before stopping scan | Integer (MB) |
| validationThreshold | Maximum file size of XML input or output to perform schema validation on | Integer (MB) |
| externalcmdTimeout | Number of seconds to wait for external commands to return data. | Integer (Seconds) |
| SSH RESULT FILE TRANSFER OPTIONS | | |
| sshEnabled | Enable sending of results via SSH after each scan | Boolean (0/1) |
| deleteOnTransferReports | Delete local results after sending to server via SSH | Boolean (0/1) |
| sshServer | Name of ssh server to send results to | String that is a hostname or ip address |
| sshPortNumber | Port number for SSH | Integer between 0 and 65536 |
| sshConnectionType | SSH Connection Type | Integer (0 = username, private key and passphrase; 1 = username and password) |
| username | SSH Username | String that is a proper username |
| sshUserPassword | Encrypted by SCC, cannot be edited manually | String |
| sshPrivateKey | Full path to user's private key for SSH connections | String |
| sshUserKeyFile | SCC generated keyfile for use with SSH | String |
| sshKeyPassphrase | Encrypted by SCC, cannot be edited manually | String |
| sshServerDirectory | Directory on the SSH in which to send results | String |
| POST SCAN SCAP SUMMARY REPORTING OPTIONS | | |

| | | |
|---|--|---|
| summarySourceDirectory | Source directory for post scan SCAP summary reports | String that is an absolute directory path |
| summaryDestinationDirectory | Destination directory for post scan SCAP summary reports | String that is an absolute directory path |
| openSummaryDestinationDirectory | Open Windows Explorer to the directory containing the reports (Windows only) | Boolean (0/1) |
| computerListHistoricalHTMLReport | Generate the Computer List Historical HTML report | Boolean (0/1) |
| computerListHistoricalExcelReport | Generate the Computer List Historical Excel report | Boolean (0/1) |
| computerListHTMLReport | Generate the Computer List HTML report | Boolean (0/1) |
| computerListExcelReport | Generate the Computer List Excel report | Boolean (0/1) |
| siteSummaryHTMLReport | Generate the Site Summary HTML report | Boolean (0/1) |
| siteSummaryNonComplianceHTMLReport | Generate the Site Summary Non Compliance HTML report | Boolean (0/1) |
| siteSummaryExcelReport | Generate the Site Summary Excel report | Boolean (0/1) |
| siteSummaryNonComplianceExcelReport | Generate the Site Summary Non Compliance Excel report | Boolean (0/1) |
| POST SCAN SCAP DETAILED REPORTING OPTIONS | | |
| detailSummarySourceDirectory | Source directory for post scan SCAP Detailed reports | String |
| detailSummaryDestinationDirectory | Destination directory for post scan SCAP Detailed reports | String |
| openDetailSummaryDestinationDirectory | Open Windows Explorer to the directory containing the reports (Windows only) | Boolean (0/1) |
| POST SCAN OVAL DETAILED REPORTING OPTIONS | | |
| detailSummaryOVALSourceDirectory | Source directory for post scan OVAL Detailed reports | String |
| detailSummaryOVALDestinationDirectory | Destination directory for post scan OVAL Detailed reports | String |
| openDetailSummaryOVALDestinationDirectory | Open Windows Explorer to the directory containing the reports (Windows only) | Boolean (0/1) |
| POST SCAN SCAP/OVAL SHARED REPORT GENERATION OPTIONS | | |
| allSettingsHTMLReportDetailSummary | Regenerate the All Settings HTML Report | Boolean (0/1) |
| allSettingsTextReportDetailSummary | Regenerate the All Settings Text Report | Boolean (0/1) |
| nonComplianceHTMLReportDetailSummary | Regenerate the Noncompliance HTML Report | Boolean (0/1) |
| nonComplianceTextReportDetailSummary | Regenerate the | Boolean (0/1) |

| | | |
|--|--|--|
| | Noncompliance Text Report | |
| <code>allSettingsSummaryHTMLReportDetailSummary</code> | Regenerate the All Settings Summary HTML Report | Boolean (0/1) |
| <code>allSettingsSummaryTextReportDetailSummary</code> | Regenerate the All Settings Summary Text Report | Boolean (0/1) |
| <code>nonComplianceSummaryHTMLReportDetailSummary</code> | Regenerate the Noncompliance Summary HTML Report | Boolean (0/1) |
| <code>nonComplianceSummaryTextReportDetailSummary</code> | Regenerate the Noncompliance Summary Text Report | Boolean (0/1) |
| THRESHOLD OPTIONS | | |
| <code>thresholdsEnabled</code> | Enable usage of thresholds | Boolean (0/1) |
| <code>thresholdsProfile</code> | Allows usage of a different thresholds file value of 'default' translates to 'default-thresholds.xml' | String |
| <code>thresholdsUnlockCode</code> | Code generated by SCC Unlocker, to allow end users to modify thresholds | String |
| SCC SERVICE OPTIONS (WINDOWS ONLY) | | |
| <code>frequency</code> | How frequently SCC Service should run | Integer (0 = Custom, 1 = Hourly, 2 = Daily, 3 = Weekly, 4 = Monthly) |
| <code>schedule</code> | Custom schedule if 'frequency' = 0 | Integer (Hours) |
| <code>randomizeSSHTransfer</code> | Delay SCC Service (and SSH transfer) by a random amount of time to prevent DDoS if numerous computers are configured with the SCC service and SSH transfer | Boolean (0/1) |
| <code>randomizeValue</code> | Max amount of time to delay starting SCC | Integer (seconds) |
| <code>timeout</code> | Programmatically calculated by SCC, do not edit | Integer |
| <code>lastServiceScan</code> | Programmatically calculated by SCC, do not edit | Integer |
| <code>nextServiceScan</code> | Programmatically calculated by SCC, do not edit | Integer |
| INTERNAL OPTIONS - DO NOT EDIT | | |
| <code>version</code> | Version of SCC, do not edit | String |
| <code>timeStamp</code> | date/timestamp of last write to options, do not edit | Integer |
| <code>expignore</code> | Over-ride software expiration for pre-release versions | Boolean (0/1) |
| <code>scap12DBFilepath</code> | Relative path to the SCAP 1.2 content database, do not Edit | String |

SCC Option Descriptions and Datatypes

| | | |
|---------------------|---|---------------|
| iaControlDBLoaded | Is the IA Control database loaded | Boolean (0/1) |
| iaControlDBFilepath | Relative path to the IA Control mappings database | String |
| nvdcceFile | Filename (no path) to the NVD CCE xml file | String |
| cciFile | Filename (no path) to the DISA CCI xml file | String |

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 time frame.

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.

To see the help related to informational parameters run '**csc.exe --help info**'

```
#####
```

```
POST SCAN 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.

-s OPTIONS_FILEPATH, --summaryReports OPTIONS_FILEPATH

Generate SCAP summary reports using the specified options file.

Example: csc.exe -s options.xml

Example: csc.exe --summaryReports myOptions.xml

-ts OPTIONS_FILEPATH, --detailedSCAP OPTIONS_FILEPATH

Generate detailed reports for SCAP using the specified options file.

Example: csc.exe -ts options.xml

Example: csc.exe --detailedSCAP myOptions.xml

-tv OPTIONS_FILEPATH, --detailedOVAL OPTIONS_FILEPATH

Generate detailed reports for OVAL results using the specified options file.

Example: csc.exe -tv options.xml

Example: csc.exe --detailedOVAL options.xml

5.5.2 Informational Parameters

Below are the parameters available for information purposes only. No configuration changes or scanning occur. All of the following options must be used individually, and are not compatible with any other parameter.

To see the help related to informational parameters run '**cscce.exe --help info**'

```
#####
```

INFORMATIONAL PARAMETERS:

Below are the parameters available for information purposes only. No configuration changes or scanning occur. All of the following options must be used individually, and are not compatible with any other parameter.

--checkForSCCUpdates

Check to see if newer SCC releases exist via online query. Additional settings may need to be pre-configured before usage. refer to: cscce.exe --config -> Options -> Update Options This does not download or update/install SCC, it just verifies it's current.

--getOpt OPTION

Advanced user setting to retrieve the value of any SCC option. Available options can be found with --listOpt, and need to be specified exactly.

Example: cscce.exe --getOpt debugEnabled debugEnabled = 0

--listOpt

Advanced user setting to retrieve the configurable values for use with --getOpt and --setOpt

--listAllProfiles

List all profiles according to the installed content. Note that not all profiles are available to all content streams.

--listAllBenchmarks

List all benchmarks according to the content installed on the system. Useful when setting a profile for specific content.

-v, --version

Display one liner version information.

-V, --verboseVersion

Display version information.

-?, --help [config scan post-scan info]

Display this help page, by default all sections will be displayed. With optional parameter(s) of config, scan, post-scan or info specific section(s) can be displayed.

5.5.3 Scheduling Command Line Generation of Summary Reports

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

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 5.7.1\csc.exe")
5. Choose the selected time frame (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 5.7.1\csc.exe" -s options.xml

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

5.6 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.

- csc.exe
- bin directory
- lib32 directory
- lib64 directory
- scc.sig32
- scc.sig64
- options.xml (or any custom named options file)
- "Resources" directory, subdirectories and all files

5.6.1 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 (depending on user preferences), such as:

- o SCC
 - o Sessions
 - o <Date Time Stamp>
 - o Results
 - o XML

The XML Directory will contain the resulting ARF, 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_5.7.1_<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.

5.7 Manual Question Auto-Answer Files

SCC supports answering of non-automated questions via Manual Question Auto-Answer Files.

These are text based templates based on OCIL (Open Checklist Interactive Language) XML files. SCC includes 'enhanced' STIG SCAP content, which is programmatically created from STIG Manuals and SCAP Benchmarks, to provide 100% coverage of the STIG Manual.

5.7.1 Templates Directory

Files in this directory are programmatically created by SCC when content is installed, or when an end user changes the sort order of manual questions. Files in this directory should not be manually updated, as they will be overwritten, and ignored. Files from this directory should be copied to the Completed Files directory

Templates are located in SCC's Resources/Content/Manual_Questions/Templates directory

5.7.2 Completed Files Directory

This directory contains all of the completed autoanswer files, either create by SCC's Manual Questions GUI interface, or edited manually by any text editor.

The default directory is SCC's Resources/Content/Manual_Questions/Completed_Files, but can be changed by the end user via SCC Options -> Scanning Options -> Manual Questions Autoanswer Completed Files Directory

5.7.3 Usage

1. Ensure that SCC's option to process manual questions is enabled SCC Options -> Scanning Options -> Process Manual Questions if found in SCAP content
2. Copy desired template(s) from the Templates directory to your Completed Files directory
 - o Important: Do not rename the file(s), or SCC will not find it.
3. Open template using a text editor
 - a. Mark answers with an X
 - b. Remove X from "Not Reviewed" line
 - c. Add any comments
 - d. Do not add/remove any other sections to this file. The only editable portions are selecting an answer with [X] and adding text based comments.
 - e. Save the file when complete
4. Run csc to perform a scan, answers to manual questions should be applied to all future scans.

Example:

```
=====
Select One of the following by entering an X in the brackets
[ ] Finding
[ ] Not a Finding
[X] Not Applicable
[ ] Not Reviewed
Enter any comments : This is a sample comment that will be
included in XCCDF XML, HTML, Text and CKL reports.
```


5.7.4 Warnings if autoanswer files are not found

If SCC finds enhanced content that contains Manual Questions, and no Manual Question autoanswer file is found, SCC will print a warning during each scan, and all manual question results will be reported as not reviewed.

5.7.5 Interaction with SCC GUI

SCC's graphical Manual Questions feature imports files from the Completed_Files directory before making updates, so editing either manually via text editor or SCC GUI, or both should work as expected, unless both methods are used at the same time, and then the last one to save will win.

5.7.6 Upgrading manual question results from an older version of SCC

Starting with SCC 5.7 (on Windows) SCC will prompt to upgrade configuration and manual question results on first launch. If the manual question results are configured to be stored in the application installation directory (default), SCC will copy the files from 5.7 to 5.7.1 etc. If the manual question results directory has been configured to a custom directory, SCC 5.7.1 will use that custom directory, as a side effect of the configuration upgrade.

For Linux: When using package based installation, with the RPM or DEB upgrade method selected, SCC will install to the same directory as previous versions, upgrade the configuration to the current version, and have all of the manual questions results available.

5.7.7 Converting manual question results from one version of SCAP content to another

Starting with SCC 5.7.1, SCC now automatically converts manual question results to the latest SCAP content. Only questions that match the same XCCDF rule and version are updated, so if any change is made to an XCCDF rule in the updated STIG manual, answers will not be converted and those questions will need to be re-answered.

6. UNDERSTANDING SCAN RESULTS

6.1 Understanding Scan Reports

6.1.1 Summary Viewer Report

By default, with each scan session, a summary viewer HTML report is created which provides hyperlinks for easy browsing of the results created from that scan session. It's saved to the root of the scan session directory.

Ex: SCC_Summary_Viewer_2017-01-06_112807.html

This report can be sorted by clicking on any column heading, or filtered by typing a hostname, content stream etc. in the 'search' box.

6.1.2 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 | <p>The <i><Computer>_SCC_5.7.1_All-Settings_<Content Name>.html</i> 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.</p> <p>The Scores section contains the calculated scores for the target system.</p> <p>The System Information section contains information about the target system (CPE Information), such as the host name, IP addresses, operating system, processor, memory, manufacturer, model, serial number, BIOS version, and Ethernet Interfaces.</p> <p>The Content Information section contains information about the XCCDF benchmark, such as the XCCDF filename used, status (if officially accepted content along with the date it was officially accepted), content installation date, the profile used, the testing start and end times, and the identity of the user who ran the benchmark.</p> <p>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.</p> <p>The Detailed Results section contains in-depth information on each rule performed in the benchmark. This section varies slightly between SCAP and standalone OVAL/OCIL, but contains fields such as Title, Result, CCE Identities, CVE Identities, severity, weight, definitions, tests, collected items</p> |
| 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 | The <i><Computer>_SCC_5.7.1_Non-Compliance_<XCCDF Content</i> |

| | |
|-------------------------------|---|
| Report | <i>Name>.html</i> 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. |

6.1.3 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. |
| Not Checked | The SCC was able to interpret the check in the XML content, however the XML content did not result in any evaluation to be performed. Also, if a probe is not supported, the check will show up as Not Checked. |
| 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. |

6.1.4 Understanding Color Coding in the HTML Reports

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

6.1.4.1 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 |

6.1.4.2 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. |

6.1.4.3 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 |

6.1.4.4 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

The User Data Directory, which contains both Application Logs and Scan Sessions, 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 default directory structure is as follows, but is user configurable.

ApplicationLogs

This directory contains SCC logs (screen, debug, error) related primarily to the SCC application itself, startup, forms, etc. and not specifically related to performing SCAP content scanning.

Sessions

<Date/Time Scan Session>

The Date/Time directory is created each time the Analyze Computer button is pressed, or a scan is completed via C SCC. This helps organize all scan related data for a single session.

SCC_Summary_Viewer_<Date/Time Scan Session>.html

The Summary Viewer report provides hyperlinks to all of the HTML, Text and XML based reports created from a single scan session.

Logs

This directory contains log files (screen, debug, error) specifically related to a scan session.

Results

<SCAP/OVAL/OCIL>

<Computer>_SCC_5.7.1_All-Settings_<Content>.html

<Computer>_SCC_5.7.1_Non-Compliance_<XCCDF Content>.html

XML

XML files (see table below)

Checklists

DISA Checklist (CKL) reports from any NIWC Enhanced SCAP Benchmark that contains Manual Questions

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.

***Note:** All filenames included in the table below are SCC's default result filenames*

| XML FILE | DESCRIPTION |
|--------------------|--|
| NIST ARF 1.1 | <p>The <Computer>_SCC_5.7.1_<DateTime>_ARF_<XCCDF Content Name>.xml file contains the ARF results in a machine readable format.</p> <p>This high level summary of the review including the asset information from each system and the pass/fail status of each check performed. This results file is required for SCAP 1.2 compliance.</p> |
| XCCDF Results | <p>The <Computer>_SCC_5.7.1_<DateTime>_XCCDF-Results_<XCCDF Content Name>.xml file contains the XCCDF results in a machine readable format.</p> <p>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.</p> |
| OCIL Results | <p>The <Computer>_SCC_5.7.1_<DateTime>_ocil-res-Results_<XCCDF Content Name>.xml file contains the detailed OCIL in a machine readable format.</p> <p>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.</p> |
| OVAL CPE Results | <p>The <Computer>_SCC_5.7.1_<DateTime>_CPE-Results_<XCCDF Content Name>.xml file contains the CPE results in a machine readable format.</p> <p>This contains platform information about the target system including the operating system, network interfaces and processor type.</p> |
| OVAL Patch Results | <p>The <Computer>_SCC_5.7.1_<DateTime>_OVAL-Patch-Results_<XCCDF Content Name>.xml file contains the detailed OVAL patch results in a machine readable format.</p> <p>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.</p> |
| OVAL Results | <p>The <Computer>_SCC_5.7.1_<DateTime>_OVAL-Results_<XCCDF Content Name>.xml file contains the detailed OVAL results in a machine readable format.</p> <p>This is a detailed report of pass/fail results from each OVAL definition performed during a review.</p> |
| OVAL Variables | <p>The <Computer>_SCC_5.7.1_<DateTime>_OVAL-Variables_<XCCDF Content Name>.xml file contains a list of OVAL variables in a machine readable format.</p> |

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, the following log files may be present:

6.3.1 Application Logs

Application Logs are logs that are created when the application is started, and during application execution outside of any scan (when the analyze button is pressed). Application Logs are created in the Logs\ApplicationLogs directory (unless that directory option is disabled) and then they are saved in the root of the Logs directory. The ApplicationLogs directory is only created when logs exist, so may not be created depending on user preferences.

Some of the following logs might be present, depending if screen or debug logs are enabled, or if any application errors occurred.

| REPORT | DESCRIPTION |
|------------|--|
| Screen Log | <p><i>SCC_5.7.1_<DateTime>_Screen_Log.txt</i></p> <p>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 Options.</p> |
| Error Log | <p><i>SCC_5.7.1_<DateTime>_Error_Log.txt</i></p> <p>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.</p> <p>If this file exists, and the error log does not provide enough information to resolve the issue, please contact NIWC (see appendix G for technical support) and provide the error log for our analysis.</p> |
| Debug Log | <p><i>SCC_5.7.1_<DateTime>_Debug_Log.txt</i></p> <p>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.</p> <p>Please refer to Appendix A.8 Debugging for additional information on SCC debug logs and their intended usage.</p> |

6.4.1 Scan Logs

Scan Logs are logs that are created when any SCAP/OVAL/OCIL content is used to scan a target computer. By default the logs are created in a date/timestamp 'session' directory within the Logs directory. Each time the Analyze button is pressed, a new scan log subdirectory is created. This directory name matches the same date/time session directory created in the Results directory.

| REPORT | DESCRIPTION |
|-----------------|---|
| Scan Screen Log | <p><i>SCC_5.7.1_<DateTime>_Screen_Log.txt</i></p> <p>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 Options.</p> |
| Scan Error Log | <p><i>SCC_5.7.1_<DateTime>_scan<number>_Error_Log.txt</i></p> <p>This report contains any errors that may have occurred during a GUI based scan. The scan<number>, such as scan001 or, scan002 corresponds to each review that is started by clicking the Analyze button. Normally this file will not exist.</p> <p>If this file exists, and the error log does not provide enough information to resolve the issue, please contact NIWC (see appendix G for technical support) and provide the error log for our analysis.</p> |
| Scan Debug Log | <p><i>SCC_5.7.1_<DateTime>_scan<number>_Debug_Log.txt</i></p> <p>This report contains any debug that occurred during a scan. The scan<number> such as scan001, scan002 corresponds to each review that is started by clicking the Analyze button.</p> <p>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.</p> <p>Please refer to Appendix A.8 Debugging for additional information on SCC debug logs and their intended usage.</p> |

7. 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.

7.1 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.

7.2 Configuring the SCC Service

The SCC application has a SCC Service Configuration component available, but only if the SCC Service was installed during application install.

Start -> Programs -> SCAP Compliance Checker 5.7.1 -> SCAP Compliance Checker 5.7.1 -> Options -> Show Options -> Service Options

7.2.1 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.

7.2.2 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 configuration options for scheduling scans:

| FREQUENCY | DESCRIPTION |
|--------------------------------|---|
| Daily | SCC will scan once per day |
| Weekly | SCC will scan once per week. |
| Monthly | SCC will scan once per month |
| 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. |

7.2.3 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 inherit all configuration settings from the SCC application, but only at the time the Save Service Configuration is pressed.*

7.2.4 Files/processes used in the SCC Service

The following process will appear in the process table, and will be running in the background:
SCC_Service32.exe

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

7.3 Update Service Configuration

7.3.1 Save Current Configuration to Service

This button saves the current configuration of SCC to the SCC service, then starts or restarts the SCC Service as needed.

7.3.1 Stop Service

This button stops and sets the startup of the SCC Service to 'Manual', effectively disabling the service. To re-enable the service, click the Save Current Configuration to Service button..

8. RUNNING SCC AS A NON-ADMINISTRATOR

This section of the manual is only applicable to installations of SCC on Windows. Starting with SCC 5.5, SCC allows for a limited operation of SCC without local Administrator rights.

8.1 Installing SCC

8.1.1 Installing as Administrator to Program Files

SCC can be installed by an Administrator in the normal location (C:\Program Files). If it is, then non-Administrators will not have write access to this installation directory and any files that need to be updated/added, etc. will be located in the home directory of the non-Administrator. See section 8.2 for more information.

8.1.2 Extracting Zipped version of SCC as a non-Administrator

SCC can be 'installed' to any directory by unzipping the zipped version of SCC. If the directory is writable by non-Administrators, it is not recommended to have this be a shared installation, because running the application as an Administrator will lock down a few of the subdirectories that contain sensitive data, and errors may occur when later attempting to run vis non-administrator. If the directory is not writable by non-Administrators, refer to Section 8.2.

8.2 Install directory non-writable by non-Administrators

If the non-Administrator who launched SCC cannot write to the installation directory, then a directory called "SCC" and a subdirectory called "SCC_5.7.1".will be created in the home directory of the non-Administrator.

Example: C:\Users\testuser\SCC\SCC_5.7.1

Launching SCC as a non-Administrator the first time may take a while as all of the SCAP content is copied from the SCC installation directory to the home directory of the non-Administrator..

8.3 GUI usage as non-administrator

SCC will launch as normal, and appear the same as when run as an Administrator, but will have limited scanning functionality. SCC will allow:

- SSH based Unix scanning
- SSH based Cisco IOS XE scanning
- Offline Configuration Scanning of Cisco IOS XE
- Post scan report generation

SCC will not allow any scanning of Windows (local or remote) because much of the data commonly queried in the Windows OS content is not available to standard users and the results would be inaccurate.

8.4 Command line usage as non-administrator

The command line interface of SCC will allow for the same limited scanning modes as the GUI, and the --help command will only show the command line parameters that are applicable when running as a non-administrator.

8.5 Uninstalling

If SCC was installed to C:\Program Files, then an Administrator will need to remove the software. For zip installations, just delete the directory that was extracted from the zip. Additionally, if a non-Administrator cannot write to the installation directory, then the home directory of the non-Administrator may need to be manually cleaned up by deleting the SCC\SCC_5.7.1 directory.

Example: C:\Users\testuser\SCC\SCC_5.7.1

APPENDIX A - FREQUENTLY ASKED QUESTIONS

A.1 Why can't I install a DISA STIG Manual XCCDF into SCC?

Below is a common question:

I tried to import a "Manual" STIG as a *.zip into the SCC and it gives me the following error:

```
"Unable to find OVAL document.*.zip Please ensure that all SCAP streams include a valid OVAL file that is named '<stream_name>-oval.xml'"
```

I then tried to import a manual STIG as a *-xccdf.xml into the SCC and gives me the following error:

```
"Error installing file, *-xccdf.xml: SCC did not find a valid SCAP 1.2 data-stream-collection"
```

Answer:

DISA STIG "Manual"s are not SCAP content. They contain an XCCDF XML file, with a xslt transform, meant to be viewed with Internet Explorer in order to perform a manual assessment of the system. They do not contain any OVAL xml, which is required for automation.

To obtain SCAP content from DISA, download "Benchmarks" from <https://cyber.mil/stigs/scap/>

A.2 How can I scan CENTOS Linux, Rocky Linux, Alma Linux, Debian Linux etc. with an existing SCAP benchmark?

SCAP content is designed to be applicable to a specific OS or application version, but SCC has a feature to ignore this.

GUI:

```
Options -> Show Options -> Scanning Options -> SCAP Options -> Run all content regardless of applicability
```

CSCC

```
csc --config -> 6. Configure Options -> Scanning Options -> 3. [X] Run all content regardless of applicability
```

A.3 I just installed new/updated SCAP content from DISA, why am I no longer seeing Manual Questions?

SCAP content from DISA does not contain any manual questions. The SCC team is maintaining a repository of "Enhanced" content, which contains all of the automated rules from the DISA content, along with manual questions from the DISA STIG Manual. In order to include manual questions in SCAP content, only install content from NIWC's repository located at:

<https://www.niwcatlantic.navy.mil/scap/scap-content-repository/>

Our "Enhanced" repository should be updated shortly after DISA posts new/updated benchmarks to their repository at cyber.mil.

A.4 Can I scan Linux/Solaris/Mac from Windows?

Yes. The SSH based scanning allows for UNIX (linux/solaris/mac) scans to be performed from Windows. Refer to section 4.3.

A.5 Is SCC officially SCAP validated?

Yes.

SCC version 4.1.1 was officially SCAP validated on August 26, 2016 against the SCAP 1.2 standards.

SCC version 5.6 was officially SCAP validated on November 4, 2022, against the SCAP 1.3 standards.

SCC currently supports SCAP versions 1.0, 1.1, 1.2 and 1.3.

<https://csrc.nist.gov/Projects/scap-validation-program/validated-products-and-modules/147-scc-scap-1-3-product-validation-record>

<https://csrc.nist.gov/projects/scap-validation-program/validated-products-and-modules/140-spawar-scap-1-2-product-validation-record>

A.6 Who should I report SCAP content issues to?

For content which lists the Publisher as DISA, please contact DISA:: disa.stig_spt@mail.mil

For content which lists the Publisher as NIWC LANT, please contact our team: scc.fct@navy.mil

A.7 Why does NIWC's 'Enhanced' content have a different version from DISA SCAP content?

In order to allow end users to be able to install both DISA content and NIWC Enhanced content at the same time, the benchmark version of our enhanced content needs to be different from DISA SCAP content. The Enhanced content will be based on the DISA STIG SCAP content version, but with an additional set of numbers for our Enhanced content release.

<DISA STIG SCAP Benchmark Version> + "." <NIWC Enhanced Content Version>, and the enhanced content is dropping the leading 00's for brevity.

Example:

DISA SCAP:

U_Adobe_Acrobat_Reader_DC_Continuous_V2R2_STIG_SCAP_1-2_Benchmark.xml
internally it's version 002.002

NIWC Enhanced SCAP:

U_Adobe_Acrobat_Reader_DC_Continuous_V2R2_STIG_SCAP_1-2_Benchmark-enhancedV1.xml internally it's version 2.2.1

If there were updates to the STIG Manual, but no updates to the DISA SCAP Benchmark after 2.2.1 was released, we would regenerate the content with updated manual questions and then the Enhanced content would be version 2.2.2.

A.8 Does SCC provide any remediation functionality?

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

A.9 Where can I learn more about creating my own SCAP content?

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

<http://ovalproject.github.io/> - OVAL

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

A.10 Why is SCC default SCAP content and application updates URL's hosted on a .com?

The default content repository URL included with SCC is an XML file maintained on github by DISA. The URL is part of DISA's <https://disa-stigs.github.io/> page, and updates are posted by an authorized DISA employee. It was decided to use DISA's github portal for the XML feed for two reasons.

1. To prevent any denial of service issues with their cyber.mil page, as we have thousands of end users, running SCC on millions of computers, and github has much more bandwidth, capability and reliability than cyber.mil.
2. Speed of updates. Any updated files posted to cyber.mil have to go through a lengthy approval process, and would delay content update availability by days or weeks.
3. Cyber.mil may be replaced with another website at some point, while github likely will remain a constant, and the XML file on github can then be updated to point to any cyber.mil replacement website.

Additionally, the XML file is just a pointer to cyber.mil, so if SCAP content or application updates are needed, they are downloaded directly from cyber.mil, but we assumed this would be much less frequent than end users checking for updates.

Below is an snip from the current XML feed located at:

<https://raw.githubusercontent.com/DISA-STIGS/DISA-STIGS.github.io/master/content-repository.xml>

```
<content-id>U_Adobe_Acrobat_Reader_DC_Continuous_V2R2_STIG_SCAP_1-
2_Benchmark-enhanced.zip</content-id>
<location>https://www.niwcatlantic.navy.mil/wp-
content/uploads/2022/12/U_Adobe_Acrobat_Reader_DC_Continuous_V2R2_ST
IG_SCAP_1-2_Benchmark-enhanced.zip</location>
<checksum
style="SHA512">6a8f8593d41c16807d483f272de24b5c7940348ce7ebf677928f4
dadf887ac5247be8b996bdba74cf4a4b0ab32435e09b0e1aaa0d87820998ae5f15cf
8a41276</checksum>
```

```

    <benchmarks>
      <benchmark>
        <benchmark-
id>xccdf_mil.disa.stig_benchmark_Adobe_Acrobat_Reader_DC_Continuous_
Track_STIG</benchmark-id>
        <title>Adobe Acrobat Reader DC Continuous
Track STIG SCAP Benchmark - NIWC Enhanced with Manual
Questions</title>
        <version>002.002</version>
        <style>SCAP_1.2</style>
        <status>accepted</status>
        <status-date>2021-06-22</status-date>
        <creator>DISA</creator>
        <publisher>DISA</publisher>
        <contributor>DISA</contributor>
        <source>STIG.DOD.MIL</source>
      </benchmark>
    </benchmarks>

```

As you can see, the actual content will be downloaded directly from cyber.mil, with SHA512 checksum being performed to ensure it's what is expected. SCC's application update XML feed works in the same manner.

A.11 Can I create my own offline SCAP content repository for my isolated network?

Yes, although you will need to have your own web server that you can write files to that doesn't require authentication.

Option 1: To make an offline copy of NWC's content repository;

1. Copy the following file from DISA's github repository to your computer:
<https://raw.githubusercontent.com/DISA-STIGS/DISA-STIGS.github.io/master/niwc-content-repository.xml>
2. Copy all of the SCAP Benchmark zip files from NIWC's content repository website:
<https://www.niwcatlantic.navy.mil/scap/scap-content-repository/>
3. Copy all of the SCAP Benchmarks to your own web server
4. Edit the content repository XML file URLs to match the URL's to your zip files
(ex: update

```

<location>https://www.niwcatlantic.navy.mil/wp-
content/uploads/2022/12/U_Adobe_Acrobat_Reader_DC_Continuous_V2
R2_STIG_SCAP_1-2_Benchmark-enhanced.zip</location>

```

to be

```

<location>https://your-
webserver/yourDirectory/U_Adobe_Acrobat_Reader_DC_Continuous_V2
R2_STIG_SCAP_1-2_Benchmark-enhanced.zip</location>

```
5. Copy the updated content repository to your server (ex: <https://your-webserver/content-repository.xml>)
6. Update SCC to use your webserver
 - a. via GUI:
 SCC -> Options -> Update Options -> Right click on the existing URL, and click edit, then edit and save to <https://your-webserver/content-repository.xml>
 - a. via CSCC Config


```
cscs --config -> 6. Configure Options -> 7. Update
Options -> Delete Repository URL, then Add new Repository
URL
```

a. scripted via CLUI:

```
cscs --setOption contentRepository https://your-
webserver/content-repository.xml
```

Options 2: To make an offline copy of DISA's content repository, that SCC can use for updating:

1. Copy the following file from DISA's github repository to your computer:
<https://raw.githubusercontent.com/DISA-STIGS/DISA-STIGS.github.io/master/content-repository.xml>
2. Copy all of the SCAP Benchmark zip files from DISA's Cyber.mil website:
<https://cyber.mil/stigs/scap/>
3. Copy all of the SCAP Benchmarks to your own web server
4. Edit the content repository XML file URLs to match the URL's to your zip files
(ex: update

```
<location>https://dl.dod.cyber.mil/wp-
content/uploads/stigs/zip/U_Adobe_Acrobat_Reader_DC_Classic_V2R
1_STIG_SCAP_1-2_Benchmark.zip</location>
```

to be

```
<location>https://your-
webserver/yourDirectory/U_Adobe_Acrobat_Reader_DC_Classic_V2R1_
STIG_SCAP_1-2_Benchmark.zip</location>
```
5. Copy the updated content repository to your server (ex: <https://your-webserver/content-repository.xml>)
6. Update SCC to use your webserver
 - a. via GUI:
SCC -> Options -> Update Options -> Right click on the existing URL, and click edit, then edit and save to <https://your-webserver/content-repository.xml>
 - a. via CCCC Config

```
cscs --config -> 6. Configure Options -> 7. Update
Options -> Delete Repository URL, then Add new Repository
URL
```
 - a. scripted via CLUI:

```
cscs --setOption contentRepository https://your-
webserver/content-repository.xml
```

To create your own custom content repository xml file, not based on the existing DISA repository, we suggest using the DISA STIG content repository xml feed as a template. The following checksum 'styles' are supported, SHA3_256 is recommended, but not easily available via windows/linux command line.

- SHA3_256
- SHA256
- SHA512

The following may also work but are not recommended

- SHA1
- MD5

A.12 Can SCC run directly from a CD-ROM?

Yes

A.13 Can SCC be run as a non-Administrator or non-root user?

On Windows, SCC offers limited functionality for non-Administrator users, including SSH based UNIX and Cisco scanning and alternate credentials Windows WMI remote scanning. Refer to section 8 for more information.

On Linux, Mac, and Solaris, root is required to run SCC.

A.14 How can I use RunAs (Secondary Logon) with SCC?

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 5.7.1 -> 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 5.7.1" (Install Folder)
```

3. Run the application

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

OS Requirements:

- The Secondary Logon 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.

A.15 What type of network traffic does a remote Windows SCC scan generate?

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 dependent 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.

Protocols:

- ICMP Echo (ping) requests/replies
- TCP NBSS session requests
- TCP SMB AndX requests/responses
- TCP WINREG OpenKey/CloseKey requests/responses
- TCP RPC/DCOM (for WMI queries)
- HTTP GET (for WindowsUpdateAgent content, which is rarely if ever used in SCAP content)

Ports

- RPC TCP 135
- SMB/NBSS/WINREG TCP 445, 139
- WMI/DCOM/RPC Randomly allocated high TCP ports¹ TCP random port number between 1024 - 4000 and random port number between 49152 - 65535²
- HTTP/HTTPS 80, 443 (but unlikely, unless SCAP content has WindowsUpdateAgent tests)

For more information on WMI/RPC/DCOM ports

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements>

A.16 Where can I download the DOD Root Certificates for Windows (InstallRoot)?

DISA provides the DOD Root Certificates for Windows via an installation package called InstallRoot. As of the release date of SCC 5.7.1, the URL is:

https://public.cyber.mil/installroot_5-6/

A.17 Why does SCC review all cached profiles to confirm that User profile settings are accurate

User based GPO's are applied on a per-user basis, meaning that each user can have different configurations, so the only way to know if the system is compliant is to check all users. Some tools just check the currently logged in user, which may only provide a false sense of security.

SCC uses the OVAL tested/vetted and approved 'ntuser' test to complete this task. SCC reviews the currently logged in user, and then finds any cached profile for all 'human' users and checks their ntuser.dat files. SCAP content can determine which users are in scope such as local, domain, enabled, disabled, and number of days since last login.

Making domain users compliant is generally very straight forward, and likely already implemented in your environment. Local users do not obtain security settings from any domain based GPO, and can be more challenging to configure. Usually the easiest answer is to disable all local users. If you need local users, please see FAQ 18, and how to make them compliant.

A.18 How do I make local users compliant with user level GPOs?

The Windows OVAL test called 'ntuser' is designed to review cached user profile ntuser.dat files to validate that they are compliant with policies. This test will be used for the NIWC developed Microsoft Office 365 SCAP content, and likely others. For Local users, applying User based GPO's can be less intuitive than Domain Users.

The LGPO tool included in the Microsoft Security Compliance Toolkit 1.0 can be used to apply GPOs (user and machine) to systems which are not domain-joined. There are likely other ways to accomplish this task, proceed at your own discretion.

Below is an example usage scenario:

To apply the Microsoft Office 365 (MS O365) DISA STIG GPOs (user and machine):

- 1) Obtain a copy of the LGPO tool from <https://www.microsoft.com/en-us/download/details.aspx?id=55319> (LGPO.zip)
- 2) Obtain a copy of the MS O365 DISA STIG GPO from <https://public.cyber.mil/stigs/gpo/> (which can be found in the Group Policy Objects (GPOs) - October 2022 download file (U_October_2022_STIG_GPO.zip))
- 3) Obtain a copy of the MS O365 DISA STIG from <https://public.cyber.mil/stigs/downloads/> (Microsoft Office 365 ProPlus STIG - Ver 2, Rel 7 (U_MS_Office_365_ProPlus_V2R7_STIG.zip))
- 4) Login to the non-domain system using a local Administrator account
- 5) Extract the contents of LGPO.zip, U_October_2022_STIG_GPO.zip, and U_MS_Office_365_ProPlus_V2R7_STIG.zip (or most recent Office GPO)
- 6) Run Command Prompt as Administrator and navigate to the LGPO\LGPO_30 directory
- 7) Execute the LGPO tool:
`LGPO.exe /g '<path>\U_October_2022_STIG_GPO\DoD Office 2019-M365 Apps v2r7\GPOs\{9D99357A-A462-40DB-A86E-AB358B4CB1AA}' /g '<path>\U_October_2022_STIG_GPO\DoD Office 2019-M365 Apps v2r7\GPOs\{DE620AC8-43FF-4123-8C7A-B589D92AC5F0}' /v > lgpo_o365_out.txt 2> lgpo_o365_err.txt`
- 8) User GPO's are applied on login, so any Local user will need to logoff and log back in to apply settings
- 9) Compare the users HKEY_CURRENT_USER registry keys/values against the MS O365 DISA STIG and verify that all policy settings have been properly applied (the DISA STIG can be viewed using the STIG Viewer)

APPENDIX B - KNOWN ISSUES

B.1 Potential out of memory crashes with very large OVAL XML content files

It is not recommended to install OVAL source content larger than 30 MB in size. When loading OVAL XML content, 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 1-2 GB, 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 CIS OVAL repository that could cause stability issues with SCC.

B.2 Unable to scan RHEL8 systems via SSH with OS application white listing enabled (SCC failed to launch)

Starting with SCC 5.5, we have added a new option, disabled by default, which can allow SCC to automatically whitelist itself and allow it to run remotely via SSH. See the SSH Remote Scanning Option to enable it, and for more information on how the temporary configuration change works.

B.3 Host Key Check Failed when scanning RHEL7/8 and Ubuntu systems via SSH when changing between SCC 5.4 and 5.4.2 or later

SCC's internal libssh2 module was updated for SCC 5.4.1, and this adds support for more modern/secure ssh host key exchanges. This causes the host key saved in SCC 5.4 to be different from SCC 5.4.2 on most modern Linux systems. There is an auto-negotiate that occurs, and the highest security method by both server and client is used. So for RHEL6 and Solaris 10, the keys will not change, but for anything more modern host keys will change.

To resolve this issue, using the Host Credential Manager, do a test connection on all hosts using 5.4.2 or later and accept the new host keys.

B.4 Account lockout issues when scanning Ubuntu remotely via SSH with correct credentials

Refer to the SSH Troubleshooting section for details.

B.5 Command prompt closes when run with UAC

With the update to csc.exe to automatically elevate to a privileged user, if you run csc.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 csc.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:

```
csc.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, csc.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:

- Open the command prompt as administrator prior to running csc.exe

B.6 Maximum directory/file length error when copying SCC results

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 5.7.1\Results\SCAP\LONG-  
COMPUTERNAME\U_Windows_7_VIR6_STIG_Benchmark\2\2011-12-23_160049\XML\LONG-  
COMPUTERNAME_SCC-5.7.1_2011-12-23_160049_OVAL-CPE-  
Results_U_Windows_7_VIR6_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  
5.7.1\Results\SCAP\LONG-COMPUTERNAME\U_Windows_7_VIR6_STIG_Benchmark\2\2011-12-  
23_160049\XML\LONG-COMPUTERNAME_SCC-5.7.1_2011-12-23_160049_OVAL-CPE-  
Results_U_Windows_7_VIR6_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 workarounds exist for this:

- In the Content and Options menu, on the Output Options tab you are able to reduce the folders created by SCC in the Output Subdirectory Options section and reduce the length of the filename using the Output Filename Options
- 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.

B.7 Reviewing Domain Controllers with numerous user accounts

Domain controllers with large numbers of users and computers (several thousand), may not be able to be reviewed using the current DISA STIG SCAP content. There are several checks that require .* operations, which take a long time to process and can generate GB's of results, and likely will cause SCC to crash before completion.

As a partial workaround, we have added an OVAL processing option to prevent Access Token (User Rights) from causing SCC to crash.

Other checks may still exist in the content that perform .* operations for User accounts and SID's, and the only workaround would be to manually disable these rules in the XCCDF XML file.

B.8 Issues with WMI scanning if GPO is configured to block execution of all .bat files

SCC's remote WMI scanning requires the ability to create an execute a batch file. Without it, the scan will fail. See the Requirements section for more details.

B.9 Issues with remote scanning (Classic and WMI) if scanning PC is not fully patched

At some point during 2022, Microsoft released a security patch that appears to have broken some remote API calls from outdated versions of Windows to patched computers. If you experience issues, and are also unable to connect to the target computer via Remote Desktop Protocol, the patch level of your scanning computer may be out of date. Updating the scanning computer to current appears to resolve this issue.

The error reported is

```
Failed to connect to <target computer> via WMI, Error  
Win32::OLE(0.1712) error 0x80070005: "Access is denied"      after  
character 0 in "WinMgmts:{impersonationLevel=impersonate}!//<target  
computer>" : Access is Denied
```

APPENDIX C - TROUBLESHOOTING

C.1 Troubleshooting UNIX SSH Remote Scanning

C.1.1 SSH Authentication Troubleshooting

C.1.1.1 For Password Authentication: Verify sshd_config is configured with "PasswordAuthentication yes"

This setting is disabled by default on SUSE Enterprise Linux 12, and could be configured to "PasswordAuthentication no" on any system. Some systems may have it commented out "# PasswordAuthentication yes". We recommend having it explicitly set, as each OS could have different default value.

SCC will not be able to SSH to the system, and the error returned from the system will appear the same as a bad username/password. To make debugging more challenging, manually SSH'ing outside of SCC will likely work as expected. This setting appears to make the connection mandate an interactive session, breaking any automation.

C.1.1.2 For Private Key Authentication: Verify private key is a RSA PRIVATE KEY

Putty generated keys are not support. The file should look like the following:

```
-----BEGIN RSA PRIVATE KEY-----  
large text block that is your private key...  
-----END RSA PRIVATE KEY-----
```

SCC 5.7.1 should log a specific error regarding this issue.

C.1.1.3 For direct root login: Verify sshd_config is configured with 'PermitRootLogin yes'

This method is not allowed in DISA STIG's so it's not a recommended method for SCC.

C.1.2 SSH Escalation Troubleshooting

C.1.2.1 SUDO: Verify that sudo is installed on Solaris 10/11

'sudo' is not installed by default, and will need to be installed if sudo scanning methods are enabled.

SCC 5.7.1 should log a specific error regarding this issue.

C.1.3 Verify target partitions exist and have sufficient freespace

SCC uses /tmp for pushing files to before moving them to their final directory (usually /opt/scc-remote), but /opt can be changed by the end user to any directory. SCC will create the 'scc-remote' subdirectory on each scan, and remove it when it's complete.

SCC requires at least 200 MB free in /tmp and 2048 MB in /opt/scc-remote

C.1.4 Known issues with remote RHEL targets and Application Whitelisting with fapolicy

Starting with SCC 5.5, we have added a new option, disabled by default, which can allow SCC to automatically whitelist itself and allow it to run remotely via SSH. See the SSH Remote Scanning Option to enable it, and for more information on how the temporary configuration change works.

C.1.5 Known issues with remote Ubuntu targets and pam_tally2 and account lockout (when using the correct password)

The STIG for Ubuntu 18 has the user add pam_tally2 to the /etc/pam.d/common-auth file, with the lockout being 3 wrong passwords. This affects SCC because of an oversight in the pam_tally2 functionality, where, upon a successful SSH login, an unsuccessful login attempt will be tallied. Remote scanning appears as several SSH scans at once, causing the user to be locked out immediately and preventing the scan. According to the man page for pam_tally2, the login attempt counter is incremented, then the password is checked, and afterwards pam_setcred should be called to reset the counter if successful. On a default install of Ubuntu 18, this pam_setcred is not installed, nor is it called in the etc/pam.d/common-auth file, meaning the attempt counter never gets reset. A fix for this issue is adding the line `account required pam_tally2.so` to the /etc/pam.d/common-account file before any other account statements.

The user is also advised to reset the tally counter on their account used to scan.
`pam_tally2 --user USERNAME --reset` where USERNAME is the account name.

The STIG is scheduled to be updated to resolve this issue in October 2021.

C.2 Troubleshooting Windows Remote Scanning

C.2.1 Verify Scanning Computer is Fully Patched

If the scanning computer is not at least as patched as the target computer, it is quite likely that any WMI based query may fail with an "Access is Denied" error. There appears to be a patch released in 2022 that breaks WMI (and RDP) unless both the scanning and target computers are at the same patch level. The easy solution is to ensure that the scanning computer (the one you are logged into) is fully patched.

C.2.2 Ensure Necessary Services are Enabled and Running

Refer to Section 2 - Requirements to determine the required services depending on the scanning mode selected.

C.2.3 Ensure a Client Firewall is not Blocking RPC, Registry, Shares or WMI

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

C.2.4 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.

C.2.5 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.

C.2.6 Verify "Access this computer from the network" User Right for target computer.

If the account you are logged into does not have access to the target computer over the network, remote scans will not be possible. In order to scan remotely, the Administrators or Domain Admins group(s) may need to have this user right. If you do not have this user right, you may receive 'access is denied' type errors.

C.2.7 Verify "Deny access to this computer from the network" User Right for target computer.

If the account you are logged into is a member of a group being denied access to the target computer over the network, then remote scans will not be possible. If the Administrators or Domain Admins group(s) are being denied access, this could be a reason for errors, especially 'access is denied' type errors.

C.2.8 Testing Connections

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

C.2.8.1 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.

C.2.8.2 Ensure Administrative Shares are enabled on the target computer

If the steps in C.6.1 do not allow you connect, but also do not prompt you for alternative connections, it's possible that the system has been configured to disable administrative shares.

1. On the target computer, login locally and open a command prompt
2. Type 'net share'
3. Verify that both the C\$ and ADMIN\$ shares appear

```
C:\>net share
Share name      Resource
-----
C$              C:\
IPC$            Remote IPC
ADMIN$          C:\Windows
Remote Admin
The command completed successfully.
```

If either the C\$ or ADMIN\$ shares do not appear, refer to the following MSDN article regarding the registry values in HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer and HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks

C.2.8.3 Remotely Connect to a Computer's Registry

For Classic remote scanning, verify that the Remote Registry is available, 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.

C.2.8.4 Testing the WMI Connection

WMI scanning requires WMI to operate at all, and even with classic mode WMI queries can be required to perform certain checks. To verify that WMI functional perform either of the following methods, where <Computername or IP is replaced with the computer you wish to test.

Powershell Method

1. Open an Admin Power Shell Prompt
2. Type Get-WmiObject Win32_ComputerSystem –ComputerName <Computername or IP>
3. If WMI is available remotely you should see the following:


```
Domain          : <your domain>
Manufacturer    : <Your manufacturer>
Model           : <your model>
Name            : <Computername>
PrimaryOwnerName : <some user>
```

```
TotalPhysicalMemory : <some number
```

If you see the following, WMI is not going to work remotely, and it could be caused by several conditions. Refer to the next section, Testing RPC Issues.

"Get-WmiObject : The RPC server is unavailable."

MMC Snap In Method

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 or IP>.
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, WMI is not going to work remotely, and it could be caused by several conditions. Refer to the next section, Testing RPC Issues.

C.2.8.4.1 Microsoft WMI Links

Below are some links maintained by Microsoft related to WMI.

- Troubleshooting and Tips <https://technet.microsoft.com/en-us/library/ee692772.aspx>

C.2.8.5 Testing RPC Issues

Several common issues can cause the RPC server unavailable error:

- The RPC service is stopped on the remote computer;
- The RPC Endpoint Mapper port TCP/135 is not accessible on the remote computer;
- The Dynamic RPC range is blocked by firewalls installed between your computer and the remote computer.

1. Make sure RPC Endpoint Mapper port 135 is listening on a remote computer.

- Login to the remote/target computer
- Use the following command: "netstat -ano | find "135"
- The following should be returned:

```
TCP      0.0.0.0:135          0.0.0.0:0
          LISTENING          924
TCP      [::]:135           [::]:0
          LISTENING          924
```

2. Verify that the RPC Service is enabled and running

- Login to the remote/target computer
- Run the following command: "sc query rpcss"
- The following should be returned:

```
SERVICE_NAME: rpcss
            TYPE                : 20  WIN32_SHARE_PROCESS
            STATE                : 4   RUNNING
                                (NOT_STOPPABLE,
NOT_PAUSABLE, IGNORES_SHUTDOWN)
            WIN32_EXIT_CODE      : 0   (0x0)
            SERVICE_EXIT_CODE   : 0   (0x0)
            CHECKPOINT           : 0x0
            WAIT_HINT            : 0x0
```

- If any errors are reported with the RPC Service , verify that the dependencies for RPC Service are running (DCOM Server Process Launcher and RPC Endpoint Mapper)
 - On the remote/target computer, run the following 2 command
 - sc query DcomLaunch
 - sc query RpcEptMapper
 - Both should return back

```
STATE                : 4   RUNNING
```

3. If the RPC Service is running, verify if remote connections report any errors

- From your local scanning computer (not the remote/target computer)
- Open an Admin Powershell Prompt
- Type Test-NetConnection <Computername or IP> -port 135

The command may take some time to return data, but should eventually return back

```
ComputerName      : <Computername>
RemoteAddress     : <Target IP>
RemotePort        : 135
InterfaceAlias    : Ethernet
SourceAddress     : <Your local IP>
TcpTestSucceeded  : True
```

4. 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.

5. Verify DCOM is enabled

- <http://msdn2.microsoft.com/en-us/library/ms687298.aspx>

C.2.8.7 Test ability to run auditpol.exe on target system

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

```
Auditpol /backup /file:<file>
```

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.

C.2.8.8 Re-scan with SCC

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

APPENDIX D – SCC AND SCAP

D.1 SCAP Validations & Capabilities

- SCAP Versions Supported
 - SCAP Version: 1.0
 - Validation Date: February 25, 2009
 - SCAP Version: 1.1
 - SCAP Version: 1.2
 - Validation Date: August 26, 2016
 - SCAP Version: 1.3
 - Validation Date: November 4, 2022
- SCAP Capabilities
 - Authenticated Configuration Scanner (ACS)
 - Common Vulnerability Enumeration (CVE)
 - Open Checklist Interactive Language (OCIL)

D.2 Standards Supported

| STANDARD | VERSION SUPPORTED |
|-------------------------------------|--------------------|
| SCAP | 1.0, 1.1, 1.2, 1.3 |
| OVAL | 5.3 -> 5.11.2 |
| OCIL | 2.0 |
| XCCDF | 1.1.4 and 1.2 |
| CPE | 2.2, 2.3 |
| CCE | 5.0 |
| CVE | |
| AI | 1.1 |
| ARF | 1.1 |
| TMSAD | 1.0 |
| Software Identification (SWID) Tags | 2015 |

D.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 Compliance 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 Compliance 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 Compliance 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 5.7.1 implements SCAP version 1.0, 1.1, 1.2 and 1.3.

D.3.1 How SCC Process SCAP 1.0/1.1 Data Streams

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_5.7.1_<Date-Time>_OVAL-CPE-Results_USGCB-Windows-XP.xml
<Computer>_SCC_5.7.1_<Date-Time>_OVAL-Patch-Results_USGCB-Windows-
XP.xml
<Computer>_SCC_5.7.1_<Date-Time>_OVAL-Results_USGCB-Windows-XP.xml
<Computer>_SCC_5.7.1_<Date-Time>_OVAL-Variables_USGCB-Windows-XP.xml
<Computer>_SCC_5.7.1_<Date-Time>_XCCDF-Results_USGCB-Windows-XP.xml
```

7. HTML and/or text based reports are generated based on end user options

D.3.2 How SCC Processes SCAP 1.2 or 1.3 Data Streams

SCAP 1.2 as defined in NIST 800-126 rev 2 introduces data-stream-collections, data-streams, and components which are used to combine SCAP 1.0/1.2 components into a single file. Each SCAP 1.2 stream must contain a single data-stream-collection which in turn must contain at least one data-stream and one component. A data-stream may contain dictionaries and checklists, but must contain at least one check.

Upon installation of a SCAP 1.2 stream, if the file contains multiple data-streams within the data-stream-collection SCC will create a new record in the SCAP Content options for each data-stream. The user is then able to select/de-select content based on the data-stream allowing the user to run one or more data-streams from the same data-stream-collection during any given analysis run.

The SCC order of operations with a SCAP 1.2 stream is as follows, and the USGCB 1.2.7.1 Internet Explorer 8 Stream is used as an example. SCAP 1.2 Stream Name = "scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip".

Note: *This is the data-stream name, not the data-stream-collection name*

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

```
scap_gov.nist_comp_USGCB-ie8-xccdf.xml
scap_gov.nist_comp_USGCB-ie8-OCIL.xml
scap_gov.nist_comp_USGCB-ie8-oval.xml
scap_gov.nist_comp_USGCB-ie8-cpe-oval.xml
scap_gov.nist_comp_USGCB-ie8-cpe-dictionary.xml
```

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

```
scap_gov.nist_comp_USGCB-ie8-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".)

```
xccdf_gov.nist_profile_united_states_government_configuration_baseline
_version_1.2.3.1
```

4. If SCC detects an OCIL Component, the user is prompted to fill out the questionnaire or skip the questions and continue analysis.

```
scap_gov.nist_comp_USGCB-ie8-OCIL.xml
```

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

```
scap_gov.nist_comp_USGCB-ie8-cpe-oval.xml
scap_gov.nist_comp_USGCB-ie8-cpe-dictionary.xml
```

6. 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.

```
scap_gov.nist_comp_USGCB-ie8-oval.xml
scap_gov.nist_comp_USGCB-ie8-patches.xml
```

7. XML results are created, based on user settings in the options form of the GUI or the --config from the command line. SCAP 1.2 specifies the use of the NIST Asset Reporting Format (ARF) 1.1 for results generation. SCC generates an ARF results file, but we also chose to include the old reports for our current user population.

```
<Computer>_SCC_5.7.1_<Date-Time>_ARF_ scap_gov.nist_datastream_USGCB-
ie8-1.2.3.1.zip.xml
<Computer>_SCC_5.7.1_<Date-Time>_OCIL-Results_
scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip.xml
<Computer>_SCC_5.7.1_<Date-Time>_OVAL-CPE-Results_
scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip.xml
<Computer>_SCC_5.7.1_<Date-Time>_OVAL-Patch-Results_
scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip.xml
<Computer>_SCC_5.7.1_<Date-Time>_OVAL-Results_
scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip.xml
<Computer>_SCC_5.7.1_<Date-Time>_OVAL-Variables_
scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip.xml
<Computer>_SCC_5.7.1_<Date-Time>_XCCDF-Results_
scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip.xml
```

8. HTML and/or text based reports are generated based on end user options.

D.3.3 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. It is important to distinguish that SCC does not contain any static CVE database and only imports CVE information from the content stream.

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.

CVE Specification - <https://cve.mitre.org>

D.3.4 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. If no CCE identifiers are found within the SCAP data stream, SCC will not provide CCE information in the result 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 (e.g. attack vectomy, dates, etc.) regarding the configuration issue.

SCAP Compliance Checker 5.7.1 implements CCE version 5.0, however the Detailed Results section of the reports displays the CCE version 4.0 as well.

CCE 5.0 Specification - <http://cce.mitre.org/>

D.3.5 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 5.7.1 implements CPE version 2.2, 2.3.

CPE 2.3 Specification - <https://csrc.nist.gov/publications/detail/nistir/7695/final>

D.3.6 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.

CVSS 2.0 Specification - www.first.org/cvss

D.3.7 ARF 1.1 Implementation

The ARF (Asset Reporting Format) is a data model to express the transport format of information about assets and the relationships between assets and reports. The standardized data model facilitates the reporting, correlating, and fusing of asset information. SCC automatically generates the results of all SCAP 1.2 data streams into the ARF 1.1 format. The file will be included in the same folder as the other XML result files.

ARF 1.1 Specification - <http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7694>

D.3.8 AI Implementation

The Asset Identification (AI) 1.1 specification provides a standardized model for representing and identifying assets. The specification provides the necessary constructs to uniquely identify and correlate assets based on known identifiers and/or information about the assets. SCC identifies all assets utilizing the AI 1.1 specification in the ARF 1.1. result files.

AI 1.1 Specification - <http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7693>

D.3.9 TMSAD Implementation

The Trusted Model for Security Automation Data (TMSAD) is a common trusted model that can be applied to specification within the security automation domain (e.g SCAP). The TMSAD is composed of recommendations on how to use existing specifications to represent signatures, hashes, key information, and identify information in the context of an XML document and permits users to establish integrity, authentication, and traceability for security automation data.

SCC implements the TMSAD by verifying digitally signed SCAP 1.2 data streams. The XML digital signature (XMLDSig) implementation is based on requirements from the TMSAD, which includes requirements from W3C (<http://www.w3.org/TR/xmlsig-core>), and the NIST SP800-126 (<http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf>).

Supported algorithms include:

- Digests: SHA1, SHA256, SHA384, SHA512
- Encryption: DSA_SHA1, RSA_SHA1, RSA_SHA256, ECDSA_SHA256
- ECDSA Named Curves: prime256v1, secp256k1, secp384r1, secp521r1
- Transforms: C14N, C14N11, EC14N (with and without comments), enveloped signature transform
- Canonicalization: C14N, C14N11, EC14N (with and without comments)

Note: *The current implementation only supports reference that point to elements within the same document (enveloped signatures)*

TMSAD 1.0 Specification - <http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7802>

D.3.10 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 5.7.1 implements XCCDF version 1.1.4 and 1.2.

XCCDF 1.1.4 - <https://csrc.nist.gov/publications/detail/nistir/7275/rev-3/final>

XCCDF 1.2 - <https://csrc.nist.gov/publications/detail/nistir/7275/rev-4/final>

D.3.11 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 5.7.1 implements OVAL version 5.3 -> 5.11.2.

OVAL 5.11.1 Specification - <https://github.com/OVAL-Community/OVAL>

D.3.12 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 5.7.1 implements OCIL version 2.0

OCIL 2.0 Specification - <http://scap.nist.gov/specifications/ocil/#resource-2.0>

D.3.12.1 OCIL CPE Implementation

SCAP validation requirement SCAP.V.1800.1 states:

“The vendor SHALL provide instructions on how the product indicates the applicability of the imported SCAP source data stream to a target platform. Instructions SHOULD also describe how the product indicates data streams are not applicable for a target platform. This requirement is testing the use of the OCIL questionnaire associated with a CPE name via the CPE dictionary and the platform id to determine applicability of the data stream.”

SCC allows the OCIL Questionnaire to be answered prior to running the CPE applicability check so that the end user does not have to answer the same questions multiple times if multiple systems are being scanned. This allows SCC to create an OCIL Results file into a temporary directory for each system. After finishing the OCIL Questionnaire and continuing the analysis, if a CPE applicability check is included in the SCAP stream, only the OCIL questionnaires deemed applicable will be included in the final ARF results file.

D.3.13 SWID Tags Implementation

SCAP 1.3 validation requirements state:

"SCAP.V.2850.1: The vendor SHALL provide instructions on how the product identifies SWID tags using OVAL inventory class definitions that are part of an SCAP source data stream.."

and

"SCAP.V.2860.1: The vendor SHALL provide instructions on how the product identifies SWID tags using OVAL inventory class definitions that are part of a standalone OVAL Definition file."

SCC has support for the OVAL independent XMLFileContent test, with which content authors can create SCAP/OVAL content to find and process SWID tag files and report them as OVAL inventory.

SWID 2015 specification: <https://csrc.nist.gov/Projects/Software-Identification-SWID/resources#resource-2015>

D.4 OVAL Probes Supported by SCC 5.7.1 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
- Cisco IOS
 - global
 - interface
 - line
 - snmp
 - version
 - version55
- Independent
 - EnvironmentVariable
 - EnvironmentVariable58
 - Family
 - FileHash
 - FileHash58
 - LDAP
 - SQL
 - SQL57
 - SQLEXT (SCC specific OVAL test, was submitted to the OVAL Board for inclusion in OVAL 5.12, but hasn't been approved)
 - TextFileContent
 - TextFileContent54
 - Variable
 - XMLFileContent
- Windows
 - AccessToken
 - ActiveDirectory
 - ActiveDirectory57
 - AppCmd
 - AuditEventPolicy
 - AuditEventPolicySubCategories
 - Cmdlet
 - DnsCache
 - File
 - FileAuditedPermissions
 - FileAuditedPermissions53
 - FileEffectiveRights
 - FileEffectiveRights53
 - Group
 - Group_SID
 - Interface
 - License
 - LockoutPolicy
 - Metabase
 - NTUser
 - PasswordPolicy
 - PeHeader

- Port
- PrinterEffectiveRights
- Process
- Process58
- Registry
- RegKeyAuditedPermissions53
- RegKeyEffectiveRights
- RegKeyEffectiveRights53
- Service
- ServiceEffectiveRights
- SharedResource
- SID
- SID_SID
- SystemMetric
- UAC
- User
- User_SID55
- UserSID
- UserRight
- Volume
- WMI
- WMI57
- WuaUpdateSearcher

D.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.

D.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.

APPENDIX E - REFERENCES & DEFINITIONS

E.1 References

DISA STIG SCAP Benchmarks

<https://cyber.mil/stigs/scap/>

NIWC SCAP Compliance Checker

<https://www.niwcatlantic.navy.mil/scap/>

NIST SCAP Specifications

<http://nvd.nist.gov/scap.cfm>

E.2 Definitions

| ACRONYM | DEFINITION |
|---------|---|
| ARF | The Asset Reporting Format (ARF) is a data model to express the transport format of information about assets and the relationships between assets and reports. |
| CCE | <p>Common Configuration Enumeration</p> <p>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]</p> |
| CIS | The Center for Internet Security. Current managers of the open source project which maintains OVAL. [6] |
| CPE | <p>Common Platform Enumeration</p> <p>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]</p> |
| CVE | <p>Common Vulnerability Enumeration</p> <p>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]</p> |
| DISA | <p>Defense Information Systems Agency</p> <p>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]</p> <p>With respect to SCC and SCAP, DISA creates and maintains SCAP content for the DISA STIGS.</p> |
| MITRE | <p>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]</p> <p>With regards to SCAP, MITRE develops and maintains several standards such as CPE, CCE and CVE (and formerly OVAL).</p> |
| NIST | National Institute of Standards and Technology |

| | |
|------------------------------|---|
| | NIST is a United States Government agency responsible for many government standards, including SCAP. |
| OCIL | <p>Open Checklist Interactive Language</p> <p>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]</p> |
| OVAL | <p>Open Vulnerability and Assessment Language</p> <p>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]</p> |
| SCAP | <p>Security Content Automation Protocol</p> <p>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]</p> <p>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]</p> |
| SCC | <p>SCAP Compliance Checker</p> <p>SCAP Validated Authenticated Configuration Scanner developed by NIWC Atlantic.</p> |
| NIWC (formerly SPAWAR) | <p>Naval Information Warfare Center</p> <p>NWIC 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]</p> |
| STIG | <p>Security Technical Implementation Guides</p> <p>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</p> |

| | |
|-------|--|
| | malicious computer attack. ^[5] |
| SWID | Software Identification (SWID) Tags 2015 revision, a format for representing software identifiers and associated metadata ^[6] [SWID]; Version: ISO/IEC 19770-2:2015 published in October 2015 |
| 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] - <https://cyber.mil/stigs/>

[6] - <http://cisecurity.org>

APPENDIX F - LICENSES

F.1 End User License Agreement

IN NO EVENT SHALL THE UNITED STATES NAVY (OR GOVERNMENT) OR ANY EMPLOYEES THEREOF BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THIS SOFTWARE AND/ OR ITS DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, NOR SHALL THE UNITED STATES NAVY (OR GOVERNMENT) OR ANY EMPLOYEES THEREOF ASSUME ANY LEGAL LIABILITY OR RESPONSIBILITY FOR THE ACCURACY, COMPLETENESS, OR USEFULNESS OF THIS SOFTWARE AND/OR ITS DOCUMENTATION.

THE UNITED STATES NAVY (OR GOVERNMENT) SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE AND ACCOMPANYING DOCUMENTATION, IF ANY, PROVIDED HEREUNDER IS PROVIDED "AS IS". THE UNITED STATES NAVY (OR GOVERNMENT) HAS NO OBLIGATION HEREUNDER TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS. ANY REPRODUCTION OF THIS WORK MUST INCLUDED THE ABOVE NOTICES AND THE FOLLOWING NOTICE: "PORTIONS OF THIS SOFTWARE ARE OFFICIAL WORKS OF THE U.S. GOVERNMENT. THE U.S. GOVERNMENT MAY PUBLISH OR REPRODUCE THIS SOFTWARE, OR ALLOW OTHERS TO DO SO, FOR ANY PURPOSE WHATSOEVER."

FOR MORE INFORMATION CONTACT:
OFFICE OF INTELLECTUAL PROPERTY
NAVAL INFORMATION WARFARE CENTER PACIFIC
SAN DIEGO, CA 92152

APPENDIX G - TECHNICAL SUPPORT & FEEDBACK

Technical support is available for government users and contractors to the federal government.

G.1 Technical Support

- For assistance with the SCC application (installation, usage, errors, crashes) please email: scc.fct@navy.mil

G.2 Tutorials

There are a series tutorials for SCC which can be viewed at:
<https://www.niwcatlantic.navy.mil/scap/videos/>

G.3 Software Releases

The latest official release information can be obtained from our website:
<https://www.niwcatlantic.navy.mil/scap/>

To be notified via email with updates on SCC, release notifications, customer support surveys, please email: scc.fct@navy.mil

G.3.1 Download Location

DISA maintains the authoritative download of SCC, and starting with SCC 5.4, no longer requires a CAC to obtain: <https://public.cyber.mil/stigs/scap/>

G.4 Provide Feedback on SCC

We ask for your feedback with an annual survey, but you can submit feedback anytime at the website below.

https://usnavy.gov1.qualtrics.com/jfe/form/SV_4ZpXv8JkUIDs4lw

APPENDIX H - CREDITS AND FUNDING

H.1 Credits and Funding

The development of SCC has been funded by several different agencies over the years:

- 2008 - 2010 Internal Revenue Service (IRS)
- 2010 - 2012 National Security Agency (NSA)
- 2013 - 2022 Defense Information Systems Agency (DISA).
- November 2022 - January 2023 Space Systems Command, MilComm & PNT Directorate, PNT Test and Evaluation Branch (SSC/CGEV).
- February 2023 - September 2023 Funded by a group of end users that preferred to remain anonymous.

H.2 SCC Funding for FY24 and Beyond

SCC is no longer funded by DISA (or any other individual agency). During FY23 we were graciously funded by two groups of end users, but they are unable to continue that level of funding for FY24 and beyond.

We are looking to find several agencies able to fund \$300K or more each, to share the costs of our labor (6 government GS-13 developers) along with materials and maintenance for the SCC development/test lab.

If we are not able to find sufficient funding, SCC will not be developed nor supported after 30 Sept 2023.

Please contact our team for more information.

| | |
|-------------|---|
| SCC Email | scc.fct@navy.mil |
| SCC Website | https://www.niwcatlantic.navy.mil/scap/ |