Revision 3.10

National Institute of
Standards and Technology
U.S. Department of Commerce

Security Content Automation Protocol (SCAP) Version 1.3 Validation Program

Quick guide for using the consolidated data streams

Dragos Prisaca

Introduction

The information contained in this guide is intended for vendors of the SCAP product and module that are preparing for the SCAP Validation Program testing.

Please send questions or comments about information provided in this guide to scap-validation@nist.gov.

NOTE: This document is intended to support and provide additional clarification to NIST IR 7511. In the event of a conflict between the information presented in this document and the information presented in NIST IR 7511, IR 7511 takes precedence.

Test Systems

This section provides guidance and instructions on the creation and configuration of test systems for the purposes of product testing.

Platforms

Each product seeking SCAP validation for one or more of the following Microsoft platforms[1] MUST be fully tested within a domain connected configuration.

- Microsoft Windows Vista with Service Pack 2 or later
- Microsoft Windows 7 SP1 or later, 32 bit Edition
- Microsoft Windows 7 SP1 or later, 64 bit Edition
- Microsoft Windows 8.1 SP0 or later, 32-bit edition
- Microsoft Windows 8.1 SP0 or later, 64-bit edition
- Microsoft Windows Server 2012 R2 SP0 or later, 64-bit edition (**Domain Controllers and member servers SHALL be tested**)
- Microsoft Windows 10 SP0 or later, 32-bit edition
- Microsoft Windows 10 SP0 or later, 64-bit edition

NOTE: Only the Windows 7, 8.1, and 10 platforms are further defined by 32 bit and 64 bit editions.

Each product seeking SCAP validation for one or more of the following Red Hat or Apple Mac OS platforms[2] MUST be tested in standalone configuration.

- Red Hat Enterprise Linux 6, 32-bit edition
- Red Hat Enterprise Linux 6, 64-bit edition
- Red Hat Enterprise Linux 7, 32-bit edition
- Red Hat Enterprise Linux 7, 64-bit edition

- Apple Mac OS 10.11 (OS X El Capitan)

[1] Any edition of Windows which have support for domain environments is accepted (i.e. Professional, Enterprise, etc.) and will be listed in the validation record.
[2] Any edition of RHEL is accepted (i.e. Client, Workstation, Desktop, Server, etc.) and it will be listed in the validation record.

System Configurations

The vendor SHOULD exercise the product being validated on a variety of system configurations to ensure the desired results are obtained in real world scenarios.

The vendor SHOULD create a set of configurations for the SCAP 1.3 Validation Program. These configurations MAY include USGCB test systems for Windows and Red Hat Enterprise Linux platforms if the USGCB testing is performed by the vendor. The configurations for OVAL Test Data testing SHALL match the required configurations.

A newly imaged system SHOULD be used when starting the test process for a vendor product. The Implementation section in this document provides guidelines and suggestions for creating system configurations. Automated methods are suggested; however, the vendors MAY choose any method as long as the test systems meet the requisite configurations as defined in the OVAL Test Data content spreadsheets.

For applying the required configuration, users may use the individual scripts or commands provided in the ..\validationTestSuites\Consolidated \<Platform>\ configurationTools folder.

Windows systems

The Windows platform(s) SHALL be tested in a domain connected configuration. The tester must configure the following environment:

I. A windows domain controller running Windows Server 2012 R2. The name of the domain MUST be set to: "SCAPLAB" or "SCAPLAB[01-99]" (i.e. SCAPLAB11.local)

II. Configure the domain members. The domain members SHALL be configured as members of the "SCAPLAB" or "SCAPLAB[01-99]" domain.

The following requirements apply to all the Windows targets that are tested:

1. Ensure that the following pre-requisites are met:

   1.1 The test systems shall be named TESTMACHINE, TESTMACHINE01, TESTMACHINE02, up to TESTMACHINE199.

   1.2 Python 3.2 is installed

   - On Windows x86 platforms, download and install: http://www.python.org/ftp/python/3.2.5/python-3.2.5.msi

- On Windows x64 platforms, download and install: http://www.python.org/ftp/python/3.2.5/python-3.2.5.amd64.msi

1.3 The Python extensions for Windows (PyWin32 Build 220 is recommended) are installed

- On Windows x86 platforms, download and install: http://sourceforge.net/projects/pywin32/files/pywin32/Build%20220/pywin32-220.win32-py3.2.exe/download

- On Windows x64 platforms, download and install: http://sourceforge.net/projects/pywin32/files/pywin32/Build%20220/pywin32-220.win-amd64-py3.2.exe/download

1.4 The Microsoft Visual C++ 2010 and 2012 runtimes are installed

- On Windows x86 platforms, download and install: https://www.microsoft.com/en-us/download/details.aspx?id=8328 and https://www.microsoft.com/en-us/download/details.aspx?id=30679

- On Windows x64 platforms, download and install: https://www.microsoft.com/en-us/download/details.aspx?id=13523 and https://www.microsoft.com/en-us/download/details.aspx?id=30679

1.5 Windows PowerShell 3.0[3] or later shall be installed on Windows 7, 8.1, 10 and Server 2012 R2.

1.6 Please ensure the system is fully patched.

1.7 The test machine must be member of a domain and it is recommended to block the GPO inheritance:
- On the AD server: Start Group Policy Management -> Right Click on your domain -> New Organizational Unit: "OU-NO-GPOs" -> right click on "OU-NO-GPOs" -> Block Inheritance

- Start Active Directory Users and computers -> Drag and drop your test system to "OU-NO-GPOs"

- On the test system: Restart the test system

2. Create c:\validationTestSuites\ folder. Copy the combinedDataStreams_<version>.zip file to the test system and extract it to c:\validationTestSuites\. For the next steps we will assume that the zip file has been extracted to “c:\validationTestSuites\”. If you extract the files to a different location substitute that location in the following instructions.

[3] Requirements for Windows PowerShell system: https://docs.microsoft.com/en-us/powershell/scripting/install/windows-powershell-system-requirements?view=powershell-6

The content of the c:\validationTestSuites\ folder should be as follows:

Parent folder	Folder or File name	Description
..\Windows\	ValidationFiles	SCAP datastream validation results
	Documents	OVAL Test Data and configuration spreadsheet
	configurationTools	Tools for configuring the system
	Windows-datastream.xml	SCAP datastream
	catalog.xml	Expected results
..\tools\	compare.py	Python program used to compare the actual scan results with the expected results

3. Configure the target system(s), either using the provided tools and instructions below or using an alternate method of your choice:

   3.1 From a command prompt, change to the folder to "c:\validationTestSuites\Windows\configurationTools"

   3.2 Execute the **config#.bat** file from the folder, where # is the configuration number that you wish to execute. This script shall be run with administrator privileges. There are 4 different configurations for Windows Vista, 7, 8.1, 10, and Server 2012 (config 1 to 4).

If the product is validated for Windows Server 2012, two servers MUST be configured: a Windows Server 2012 R2 Domain Controller and a member server.

Examples:

- to apply the Configuration 1 on Windows Server 2012 R2 64bit Domain Controller, run as Administrator: "**config1.bat Win2012DC-64bit**" or just run config1.bat and select the option for Windows Server 2012 R2 64bit Domain Controller.
- to apply the Configuration 1 on Windows Server 2012 R2 64bit Domain Member, run as Administrator: "**config1.bat in7-8-10-2012-64bit**" or just run config1.bat and select the option for Windows 7, 8, 10, 2012 64bit.

The following options are available for the config#.bat scripts:
config[1-4].bat { WinVista-32bit | Win7-8-10-32bit | Win7-8-10-2012-64bit | Win2012DC-64bit }

4. Import the validation test content data stream for Windows (c:\validationTestSuites\Windows\Windows-datastream.xml) into the product/module following the vendor's instructions.

5. Perform configuration scans and export the evaluation results following the vendor's instructions. The result file format may look like:

   [arf | xccdf | oval | ocil | sc]-[OS]-[platform]-config[1-4].xml

   Where:
   arf = ARF results
   xccdf = XCCDF results
   oval = OVAL results
   ocil = OCIL results
   sc = systems characteristics
   OS = wvista, w7, wvista, w8.1, w10 or w2012
   Platform = 32 or 64

   For instance, the results file for consolidated data stream on Windows 7 64, configuration 1 may look like:
   arf-w7-64-config1.xml

   If you're exporting results from an USGCB data stream, replace "config[1-4]" with "exact", "reduced" or "enhanced":

   xccdf-win7-64-exact.xml

6. Compare the results produced by the product/module with the expected results from the spreadsheets or catalog.xml file. You may use the provide **compare.py** tool or an alternate method. The instructions below apply to the use of compare.py:

   - From a command prompt, change the directory to c:\validationTestSuites\tools or the directory where the compare.py tool is located.
   - Run: **python compare.py {RESULTSFILE} {CATALOGFILE} -i {SuiteID_from_catalog.xml} -o {Output_file}**
     - The compare.py script expects an ARF file. If you want to use it to parse an XCCDF file you must specify the **-x** switch. If the version of XCCDF is something other than 1.2 use the **-xv** {XccdfVersion} switch specify the version. For additional help or to see all available option run compare.py with the **-h** switch.

   For instance, using the catalog.xml file available for the Windows datastream (c:\validationTestSuites\Windows\catalog.xml), run:

   python compare.py arf-w7-64-config1.xml catalog.xml -i G2.w7_configuration1 -o arf-w7-64-config1.output

   The script will flag all the differences between the results obtained by the product/module and the expected results from the catalog.xml and save it to a

file (arf-w7-64-config1.output). If there are any differences, please verify all the configuration settings have been successfully applied to the system.

7. If you plan to use the same system for testing another configuration you should create a snapshot and clean up the configuration changes made in step 3. You can do this using the provided **cleanup.bat** tool or an alternate method. Run the cleanup.bat from the "c:\validationTestSuites\Windows\configurationTools" to restore a default configuration to the test system (as much as possible). Please note that the cleanup.bat file attempts to restore the system to an out-of-the-box state, not the state that was present before running the configuration scripts. As such, if you are testing a product/module that requires a specific configuration on the system you may need to manually clean up the settings and/or modify the cleanup process to work with the vendor's product/module.
8. Repeat steps 3 - 7 for each of the 4 configurations.

RHEL systems

1. Ensure that the following pre-requisites are met:

    1.1 The /tmp must be created as separate partition and not as a folder on the root partition.

    1.2 The test systems shall be named localhost.localdomain

    1.3 The dos2unix command shall be installed (i.e. yum install dos2unix)

    1.4 Python 3.2 is installed

    Instruction for installing Python 3.2.6 on RHEL:

    ```
    # yum groupinstall "Development Tools"
    # wget https://www.python.org/ftp/python/3.2.6/Python-3.2.6.tgz
    # tar xvf Python-3.2.6.tgz
    # cd Python-3.2.6
    # ./configure
    # make
    # make install
    ```

    Verify if Python was installed successful:
    # python3 -V
    (it should print out: Python 3.2.6)

    1.5 Set SELINUX to permissive mode: edit /etc/selinux/config, replace "SELINUX=enforcing" with "SELINUX=permissive" and reboot the system.

    1.6 The Red Hat Network Daemon (rhnsd) should be installed as default. Please verify that this service is present on your test system.

    1.7 Ensure the xinetd is installed:

    ```
    # yum install xinetd
    ```

2. Create /validationTestSuites folder directly on the / partition. Copy the combinedDataStreams_<version>.zip file to the /validationTestSuites folder and extract it there. For the next steps we will assume that the zip file has been extracted to "/validationTestSuites". If you extract the files to a different location substitute that location in the following instructions.

The content of the /validationTestSuites folder should be as follows:

Parent folder	Folder or File name	Description

../RHEL/	ValidationFiles	SCAP datastream validation results
	Documents	OVAL Test Data and configuration spreadsheet
	configurationTools	Tools for configuring the system
	RHEL-datastream.xml	SCAP datastream
	catalog.xml	Expected results
	README.txt	Readme file
../tools/	compare.py	Python program used to compare the actual scan results with the expected results

3. Configure the target system(s), either using the provided tools and instructions below or using an alternate method of your choice:

3.1 Run the following commands as root:
cd /validationTestSuites/RHEL/configurationTools/

dos2unix *.sh

dos2unix *.py

chmod +x *.sh

3.2 Apply Configuration 1 to System 1

Depending on the RHEL version, run as root:

RHEL5: # source config1_rhel5.sh

or

RHEL6: # source config1_rhel6.sh

or

RHEL7: # source config1_rhel7.sh

3.3 Apply Configuration 2 to System 2

Depending on the RHEL version, run as root:

RHEL5: # source config2_rhel5.sh

or

RHEL6: # source config2_rhel6.sh

or

RHEL7: # source config2_rhel7.sh

4. Import the consolidated data stream for RHEL (/validationTestSuites/RHEL/RHEL-datastream.xml) into the product/module

5. Perform configuration scans and export the evaluation results following the vendor's instructions. The result file format may look like:

[arf | xccdf | oval | ocil | sc]-[OS]-[platform]-config[1-2].xml

Where:

arf = ARF results

xccdf = XCCDF results

oval = OVAL results

ocil = OCIL results

sc = systems characteristics

OS = rhel5

Platform = 32 or 64

For instance, the results file for consolidated data stream on RHEL 5 64 bit, configuration 1 may look like: arf-rhel5-64-config1.xml

6. Compare the results with the expected results from the catalog.xml using the compare.py tool:

- From a command prompt, change the directory to /validationTestSuites/tools or the directory where the compare.py tool is located.
- Run: **python3 compare.py {RESULTSFILE} {CATALOGFILE} -i {SuiteID_from_catalogfile} -o {Output_file}**
- The compare.py script expects an ARF results file by default, if you want to use it to parse and XCCDF results file then you must also specify the -x switch to indicate that the file is XCCDF. If the XCCDF version is not version 1.2 you must use the -xv VersionNumber switch to specify the XCCDF version. For additional help or to see all available option run compare.py with the -h switch.

For instance, using the catalog.xml file available for the RHEL datastream (/validationTestSuites/RHEL/catalog.xml), run:

```
python3 compare.py arf-rhel5-64-config1.xml catalog.xml  -i
G2.configuration1 -o arf-rhel5-64-config1.output
```

The script will flag all the differences between the results obtained by the product/module and the expected results from the catalog.xml and save it to output file (arf-rhel5-64-config1.output). If there are any differences, please verify all the configuration settings have been successfully applies to the system.

MAC OS X systems

1.Ensure that the following pre-requisites are met:

1.1 Mac OS 10.11 (OS X El Capitan) is installed with default settings

1.2 The test systems shall be named TESTMACHINE, TESTMACHINE01, TESTMACHINE02, up to TESTMACHINE199.

1.3 Python 3.5.1 is installed

Download and install
https://www.python.org/ftp/python/3.5.1/python-3.5.1-macosx10.6.pkg

Verify if Python was installed successful:
$ python3 -V
(it should print out: Python 3.5.1)

2. Create /validationTestSuites folder directly on the / partition. Copy the combinedDataStreams_<version>.zip file to the /validationTestSuites folder and extract it there. For the next steps we will assume that the zip file has been extracted to "/validationTestSuites". If you extract the files to a different location substitute that location in the following instructions.

The content of the /validationTestSuites folder should be as follows:

Parent folder	Folder or File name	Description
../MacOS/	ValidationFiles	SCAP datastream validation results
	Documents	OVAL Test Data and configuration spreadsheet
	configurationTools	Tools for configuring the system
	MacOS-datastream.xml	SCAP datastream
	catalog.xml	Expected results
	README.txt	Readme file
../tools/	compare.py	Python program used to compare the actual scan results with the expected results

3. Configure the target system(s), either using the provided tools and instructions below or using an alternate method of your choice:

3.1 Run the following commands:

$ cd /validationTestSuites/MacOS/configurationTools/

$ sudo chmod +x *.sh

1.1 Apply Configuration 1 to System 1

$ sudo ./config1_macosx.sh

1.2 Apply Configuration 2 to System 2

$ sudo ./config2_macosx.sh

4. Import the consolidated data stream for MacOS (/validationTestSuites/MacOS/MacOS-datastream.xml) into the product/module

5. Perform configuration scans and export the evaluation results following the vendor's instructions. The result file format may look like:

[arf | xccdf | oval | ocil | sc]-[OS]-[platform]-config[1-2].xml

Where:

arf = ARF results

xccdf = XCCDF results

oval = OVAL results

ocil = OCIL results

sc = systems characteristics

OS = rhel5

Platform = 32 or 64

For instance, the results file for consolidated data stream on MacOS 5 64 bit, configuration 1 may look like: arf-macosx-64-config1.xml

6. Compare the results with the expected results from the catalog.xml using the compare.py tool:

- From a command prompt, change the directory to /validationTestSuites/tools or the directory where the compare.py tool is located.
- Run: **python3 compare.py {RESULTSFILE} {CATALOGFILE} -i {SuiteID_from_catalogfile} -o {Output_file}**

- The compare.py script expects an ARF results file by default, if you want to use it to parse and XCCDF results file then you must also specify the -x switch to indicate that the file is XCCDF. If the XCCDF version is not version 1.2 you must use the -xv VersionNumber switch to specify the XCCDF version. For additional help or to see all available option run compare.py with the -h switch.

For instance, using the catalog.xml file available for the MacOS datastream (/validationTestSuites/MacOS/catalog.xml), run:

$ python3 compare.py arf-macosx-64-config1.xml catalog.xml -i G2.macos_configuration1 -o arf-macosx-64-config1.output

The script will flag all the differences between the results obtained by the product/module and the expected results from the catalog.xml and save it to output file (arf-rhel5-64-config1.output). If there are any differences, please verify all the configuration settings have been successfully applies to the system.

Table 0-1: Test Case Guidance

Based on IR 7511 Revision 5 - April 2018

REF	REQ ID	DESCRIPTION	STATUS
1.	**SCAP.R.100**	**The product's documentation (printed or electronic) MUST assert that it uses SCAP and its component specifications and explain relevant details to the users of the product.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.100.1	The vendor SHALL indicate where in the product documentation information regarding the use of SCAP and its components can be found. This MAY be a physical document or an electronic document (e.g., a PDF, help file, etc.).	FAIL PASS N/A
	SCAP.T.100.1	The tester SHALL visually inspect the product documentation to verify that information regarding the product's use of SCAP and its components is present and verify that the SCAP documentation is in a location accessible to any user of the product. This test does not involve judging the quality of the documentation or its accuracy.	
	Guidance	Identify the location and provide either the actual documentation file(s) and/or a sample screenshot of the product's documentation.	
		Source Data Stream(s): N/A Expected Scan Results: N/A	
2.	**SCAP.R.200**	**The vendor MUST assert that the product implements SCAP and its component specifications and provide a high-level summary of the implementation approach as well as a statement of backward compatibility with earlier versions of SCAP and related components.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.200.1	The vendor SHALL provide to the lab a separate, 150- to 2500- word explanation written in the English language asserting that the product implements SCAP and its	

		component specifications for the capabilities claimed in Table 5-1[4]. This document SHALL include a high-level summary of the implementation approach and an assertion of backwards compatibility with SCAP 1.1 and SCAP 1.2. This content will be used on NIST web pages to explain details about each validated product and thus SHOULD contain only information that may be publicly released.	
	SCAP.T.200.1	The tester SHALL inspect the provided documentation to verify that the documentation asserts that the product implements SCAP and its component specifications and provides a high-level summary of the implementation approach and an assertion of backwards compatibility with SCAP 1.1 and SCAP 1.2. This test does not judge the quality or accuracy of the documentation, nor does it test how thoroughly the product implements SCAP or backwards compatibility with previous versions.	
	Guidance	The product vendor SHOULD complete the Vendor Assertions Document (v3.2 or later) and submit it to the lab. The product vendor MAY optionally want to write protect or digitally sign the PDF file. This PDF will be referenced by the SCAP Validated Products detail page which is available to the general public.	
		Source Data Stream(s): N/A Expected Scan Results: N/A	
	SCAP.T.200.2	The tester SHALL verify that the provided documentation is an English language document consisting of 150 to 2500 words.	
	Guidance	Several tools offer word counting options including Microsoft Word. With the MS Word status bar enabled, one can highlight text and quickly see how many words are currently selected. A count of the number of words provided is adequate. Other word counting tools are available as well.	
		Source Data Stream(s): N/A Expected Scan Results: N/A	

[4] Table 5-1. "Required SCAP Components for Each SCAP Capability" of the NIST IR 7511 revision 5

3.	**SCAP.R.300**	**The SCAP capabilities claimed by the vendor for the product under test MUST match the scope of the product's asserted capabilities for the target platform.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.300.1	The vendor SHALL indicate the defined SCAP capabilities (one or more) for which their product is being tested.	
	SCAP.T.300.1	The tester SHALL ensure that all tests associated with the asserted SCAP capabilities of the product are conducted.	
	Guidance	The test report SHALL provide a list of all tests to be conducted and corresponding test results. All tests MUST pass or be not applicable. A failed test will rarely, if ever, be accepted. Use the template in Appendix A of this document.	
		Source Data Stream(s): N/A Expected Scan Results: N/A	
	SCAP.T.300.2	The tester SHALL review product documentation to ensure that the product has implemented the SCAP capabilities for which it is being tested (e.g., Authenticated Configuration Scanner).	
	Guidance	The test report needs to clearly identify the SCAP capabilities the product vendor is claiming. The capabilities currently include: ☐ ACS = Authenticated Configuration Scanner ☐ CVE = Common Vulnerabilities and Exposures ☐ OCIL = Open Checklist Interactive Language	
		Source Data Stream(s): N/A Expected Scan Results: N/A	
4.	**SCAP.R.400**	**The product SHALL be able to import SCAP source data streams for the target platform and correctly load the included Rules and their associated Check System Definitions, rejecting any invalid content.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	

	SCAP.V.400.1	The vendor SHALL provide documentation and instruction on how to import SCAP source data streams for the target platform.	
	SCAP.T.400.1	The tester SHALL import valid SCAP source data streams for the target platform into the vendor product and execute the data streams on a target system. Results of the scan SHALL be inspected to ensure actual results match expected results.	
	Guidance	For a Microsoft Windows validation, import the signed r800-win-datastream.xml data stream. This data stream is applicable to all Windows platforms. For a Red Hat Linux validation, import the signed r800-rhel-datastream.xml data stream. For a Mac OS validation, import the signed r800-macos-datastream.xml data stream. For all the platforms, import the unsigned r400.1.1-datastream.xml data stream, execute it and include the scan results. The tester SHALL follow the vendor provided instructions to validate the signature and scan the target systems. The test report SHOULD indicate the name of the data stream imported. The data stream that was imported SHOULD be included in the submission. The test report SHALL provide evidence that the content was correctly imported, executed, and provide evidence of the comparison between actual results and expected results using the compare.py script. Any exceptions need to be justified.	
		Source Data Stream(s): r800-win-datastream.xml, r800-rhel-datastream.xml, r800-macos-datastream.xml, and r400.1.1-datastream.xml. Artifact(s): - Expected Scan Results: One ARF report for each platform family. - compare.py output	
	SCAP.T.400.2	The tester SHALL import an invalid SCAP source data stream into the vendor product and ensure that the imported content is not	

		available for execution.	
	Guidance	This requirement requires an unsigned data stream applied to the product under test. The r400.2.1-datastream.xml data stream is invalid according to the SCAP source data stream collection schema; the r400.2.2-datastream.xml is not well formed XML; and r400.2.3-datastream.xml is invalid according to the SCAP source data stream collection schematron schema. This requirement is intended to identify, communicate, and prevent software failure due to errors that MAY exist in content. The tester SHALL attempt to import the data stream and the test report SHALL indicate the cause (corruption) of the error and provide evidence of the error. The test report SHALL provide evidence indicating the error. The invalid content SHOULD NOT be available for execution.	
		Source Data Stream(s): r400.2.1-datastream.xml, r400.2.2-datastream.xml, and r400.2.3-datastream.xml Artifact(s): - Expected Scan Results: N/A - Evidence that the product reports the error(s). One report for each platform family.	
5.	**SCAP.R.500**	**The product SHALL be able to select a specific SCAP source data stream when processing an SCAP data stream collection.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.500.1	The vendor SHALL provide documentation and instruction on how to select a specific data stream (by ID) when processing an SCAP data stream collection.	
	SCAP.T.500.1	The tester SHALL validate that the vendor product can selectively choose and apply a specific valid SCAP data stream.	
	Guidance	Use the "requirements\R500" content for testing. This capability need only be tested once to satisfy the requirement. That is, it is not necessary to test this requirement on more than one platform. The test report SHALL provide evidence from the product output that the selected data stream was in fact executed.	
		Source Data Stream(s): r500-datastream.xml Expected Scan Results: One ARF report for each platform	

		family.	
6.	**SCAP.R.600**	**The product SHALL be able to select a specific XCCDF benchmark within an SCAP source data stream or data stream collection when multiple XCCDF benchmarks are present.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.600.1	The vendor SHALL provide documentation and instruction on how to select a specific XCCDF benchmark (by ID) when processing an SCAP data stream or data stream collection with multiple benchmarks.	
	SCAP.T.600.1	The tester SHALL validate that the vendor product can selectively choose and apply a specific valid XCCDF benchmark.	
	Guidance	Use the "requirements\R600" content for testing. This requirement requires multiple XCCDF benchmarks within a single data stream. Import "r600-datastream.xml" which includes two benchmarks and verify the user can select a specific XCCDF benchmark. The test report SHALL provide evidence from the product output that the selected XCCDF benchmark was in fact executed.	
		Source Data Stream(s): r600-datastream.xml Expected Scan Results: One ARF report for each platform family. Note: The tester SHALL select the benchmark with id: "xccdf_gov.nist_benchmark_2" and execute it.	
7.	**SCAP.R.700**	**The product SHALL be able to select a specific XCCDF profile within an SCAP source data stream or data stream collection when multiple XCCDF profiles are present.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.700.1	The vendor SHALL provide documentation and instruction on how to select a specific XCCDF profile (by ID) when processing an SCAP data stream or data stream collection.	

	SCAP.T.700.1	The tester SHALL validate that the vendor product can selectively choose and apply a specific valid XCCDF profile.	
	Guidance	Use the "requirements\R700" content for testing. This requirement requires multiple XCCDF Profiles within a single data stream. Import "r700-datastream.xml" and verify the user can select a specific XCCDF Profile. This benchmark SHALL be tested on configuration 1. The test report SHALL provide evidence that the selected XCCDF profile was in fact executed.	
		Source Data Stream(s): r700-datastream.xml Expected Scan Results: One ARF report for each platform family.	
8.	**SCAP.R.800**	**The product SHALL enable the user to import signed and unsigned SCAP source data streams.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.800.1	The vendor SHALL provide documentation explaining how an SCAP source data stream can be imported into the product and subsequently executed.	
	SCAP.T.800.1	The tester SHALL verify that the product documentation includes instructions on how the end user can import an SCAP source data stream.	
	Guidance	The test report SHALL identify the document providing import instructions. This can be a document title, filename, URL, menu path, actual excerpt, or screenshot.	
		Source Data Stream: N/A Expected Scan Results: N/A	
	SCAP.T.800.2	The tester SHALL import a valid unsigned SCAP source data stream into the vendor product and ensure that the imported content is available for execution.	
	Guidance	The tester MAY import any of the unsigned data streams in the test suite. The test report SHALL identify the data stream(s) and provide evidence indicating the unsigned content is	

		available for execution. Examine the content to ensure it is not signed.	
		Source Data Stream(s): Windows-datastream.xml; RHEL-datastream.xml; or MacOS-datastream.xml Expected Scan Results: One ARF report for each platform family.	
	SCAP.T.800.3	The tester SHALL import a valid signed SCAP source data stream into the vendor product and ensure that the imported content is available for execution.	
	Guidance	For a Microsoft Windows validation, import the signed r800-win-datastream.xml data stream; for a Red Hat Linux validation, import the signed r800-rhel-datastream.xml data stream; and for Mac OS validation, import the signed r800-macos-datastream.xml data stream The test report SHOULD identify the data stream(s) and provide evidence indicating the signed content is available for execution. The scan results SHALL be submitted as artifacts.	
		Source Data Stream(s): r800-win-datastream.xml; r800-rhel-datastream.xml; and r800-macos-datastream.xml Expected Scan Results: One ARF report for each platform family.	
9.	**SCAP.R.900**	**The product SHALL be able to validate digitally signed SCAP source data streams and MAY reject source content that has an invalid signature.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.900.1	The vendor SHALL provide documentation explaining how validation of digital signature validation is performed and where errors from validation will be displayed within the product output.	

	SCAP.T.900.1	The tester SHALL verify that the product documentation includes instructions on how the digital signature is validated.	
	Guidance	The test report SHALL identify the document providing instructions on how the digital signatures are validated.	
		Source Data Stream(s): N/A Expected Scan Results: N/A	
	SCAP.T.900.2	The tester SHALL verify that the vendor product can correctly validate the digital signature of a source data stream.	
	Guidance	The tester SHALL follow the vendor's instructions to validate the digital signature for the following source data streams: r800-win-datastream.xml for Windows; r800-rhel-datastream.xml for RHEL; and r800-macos-datastream.xml for Mac OS platforms. The tested SHALL provide evidence indicating the digital of the signed content was validated.	
		Source Data Stream(s): r800-win-datastream.xml; r800-rhel-datastream.xml; and r800-macos-datastream.xml Expected Scan Results: N/A	
	SCAP.T.900.3	The tester SHALL verify that the vendor product correctly identifies and reports an error when processing a data stream with an invalid digital signature.	
	Guidance	The tester SHALL follow the vendor's instructions to validate the digital signature for the following source data streams that have an invalid signature: r900.3-win-datastream.xml for Windows; r900.3-rhel-datastream.xml for RHEL; and r900.3-macos-datastream.xml for Mac OS platforms. The tested SHALL provide evidence indicating the digital of the signed content was validated and an error was reported.	
		Source Data Stream(s): r900.3-win-datastream.xml; r900.3-rhel-datastream.xml; and r900.3-macos-datastream.xml Expected Scan Results: N/A	

10.	**SCAP.R.1100**	**The product SHALL be able to correctly import all earlier versions of SCAP content supported by [Error! Reference source not found.][5].**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.1100.1	The vendor SHALL provide documentation explaining how earlier versions of SCAP content can be imported into the product and subsequently executed.	
	SCAP.T.1100.1	Using the vendor product, the tester SHALL execute a valid SCAP source data stream based on SCAP 1.1 and SCAP 1.2 content.	
	Guidance	The tester SHALL import the source data streams from the R800 folder and execute them on Configuration 1. The tester SHALL provide evidence that the SCAP 1.1 and SCAP 1.2 benchmarks were in fact processed. SCAP 1.1: • r1100-scap11-win_rhel_macos-cpe-dictionary.xml • r1100-scap11-win_rhel_macos-cpe-oval.xml • r1100-scap11-win_rhel_macos-ocil.xml • r1100-scap11-win_rhel_macos-oval.xml • r1100-scap11-win_rhel_macos-patches.xml • r1100-scap11-win_rhel_macos-xccdf.xml SCAP 1.2: • r1100-scap12-win-datastream.xml • r1100-scap12-rhel-datastream.xml • r1100-scap12-macos-datastream.xml	
		Source Data Stream(s): SCAP 1.1: • r1100-scap11-win_rhel_macos-cpe-dictionary.xml • r1100-scap11-win_rhel_macos-cpe-oval.xml • r1100-scap11-win_rhel_macos-ocil.xml • r1100-scap11-win_rhel_macos-oval.xml • r1100-scap11-win_rhel_macos-patches.xml • r1100-scap11-win_rhel_macos-xccdf.xml Expected Scan Results for SCAP 1.1: One XCCDF or ARF results report for each platform family. SCAP 1.2: • r1100-scap12-win-datastream.xml • r1100-scap12-rhel-datastream.xml	

Deleted: NIST SP 800-126 R3

[5] The products supporting SCAP 1.3 SHALL be capable of processing the legacy SCAP 1.2 and 1.1 content versions.

		• r1100-scap12-macos-datastream.xml Expected Scan Results for SCAP 1.2: One ARF report for each platform family.	
11.	**SCAP.R.1200**	**The product SHALL be able to determine the applicability of an imported SCAP source data stream by evaluating the associated OVAL definition for the CPE Name on an XCCDF <Benchmark>, <Profile>, <Group>, or <Rule> and verifying that the associated XCCDF content applies to the target system.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.1200.1	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 imported data stream is indicated to not be applicable for a target platform. This requirement is testing the use of the OVAL check associated with a CPE name via the CPE dictionary and platform id to determine applicability of the data stream.	
	SCAP.T.1200.1	The tester SHALL import an SCAP source data stream into the product that contains a CPE Name and platform ID and related OVAL definition not applicable for the target system. The tester SHALL verify that the product declines to execute the non-applicable tests.	
	Guidance	For Windows, Red Hat, and Mac OS validations, the tester SHALL use the r1200-datastream.xml and r1200-na-datastream.xml data streams. The test report SHALL indicate which platform the tested was executed on and which CPE was rejected; providing evidence that the product declined to execute the non-applicable tests.	
		Source Data Stream(s): r1200-datastream.xml Expected Scan Results: 1. ARF reports for test cases (1.a, 1.b, 1.c, 1.d, and 1.e) or (1.f, 1.g, 1.h, 1.i, and 1.j) 2. ARF reports for test cases 2.a, 2.b, and 2.c	

		3. ARF reports for test cases 3.a, and 3.b Source Data Stream(s): r1200-na-datastream.xml Expected Scan Results: ARF reports for each platform family using r1200-datastream.xml and r1200-na-datastream.xml.	
	SCAP.T.1200.2	The tester SHALL import an SCAP source data stream into the product that contains a CPE Name and platform ID and related OVAL definition applicable for the target system. The tester SHALL verify that the product executes the applicable tests.	
	Guidance	This SHALLbe demonstrated using any of the consolidated data streams.	
		Source Data Stream(s): Windows-datastream.xml, RHEL-datastream.xml, and MacOS-datastream.xml Expected Scan Results: One ARF report for each platform family.	
12.	**SCAP.R.1300**	**The product SHALL report and MAY reject SCAP source data stream collection content that is invalid according to the SCAP source data stream and\or its component XML schemas and Schematron schemas.**[6]	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.1300.1	The vendor SHALL provide instructions on how validation of SCAP source data stream collection content is performed and where errors from validation will be displayed within the product output.	
	SCAP.T.1300.1	The tester SHALL attempt to import known-invalid SCAP source data stream collection content into the vendor product and examine the product output to validate that the product reports the invalid SCAP source data stream collection content. The product MAY reject the content as invalid according to the SCAP source data stream collection schema and Schematron schemas.	

[6] This does not imply that the product being tested MUST use Schematron; the product needs only to produce the same results as the Schematron implementation.

	Guidance	This requirement requires an unsigned data stream applied to the product under test. The tester SHALL use the following content to test this requirement: r400.2.1-datastream.xml, and r400.2.3-datastream.xml. This requirement is intended to identify, communicate, and prevent software failure due to errors that MAY exist in content. The test report SHALL include evidence of the error(s).	
		Source Data Stream(s): r400.2.1-datastream.xml, and r400.2.3-datastream.xml Expected Scan Results: N/A Artifact(s): - Evidence that the product reports the error(s). - One report for each platform family.	
	SCAP.T.1300.2	The tester SHALL attempt to import known invalid XCCDF component content into the vendor product and examine the product output to validate that the product reports the invalid XCCDF content. The product MAY reject the content as invalid according to the XCCDF XML schema and Schematron schema.	
	Guidance	The tester SHALL use the following unsigned content to test this requirement: r1300.2.1-datastream.xml, and r1300.2.2-datastream.xml. This requirement is intended to identify, communicate, and prevent software failure due to errors that MAY exist in content. The test report SHALL include evidence of the error.	
		Source Data Stream(s): r1300.2.1-datastream.xml, and r1300.2.2-datastream.xml Artifact(s): - Evidence that the product reports the error(s). - One report for each platform family.	
	SCAP.T.1300.3	The tester SHALL attempt to import known invalid OVAL component content that is part of an SCAP source data stream into the vendor product and examine the product output to validate that the product reports the invalid OVAL content. The product MAY reject the content as invalid according to the OVAL Definition schema and Schematron schemas.	

	Guidance	The tester SHALL use the following unsigned content to test this requirement: r1300.3.1-datastream.xml, r1300.3.2-datastream.xml, and r1300.3.3-datastream.xml. This requirement is intended to identify, communicate, and prevent software failure due to errors that MAY exist in content. The test report SHALL include evidence of the error.	
		Source Data Stream(s): r1300.3.1-datastream.xml, r1300.3.2-datastream.xml, and r1300.3.3-datastream.xml. Artifact(s): - Evidence that the product reports the error(s). - One report for each platform family.	
	SCAP.T.1300.4	The tester SHALL attempt to import known invalid CPE dictionary component content into the vendor product and examine the product output to validate that the product reports the invalid CPE dictionary content. The product MAY reject the content as invalid according to the CPE dictionary XML schema.	
	Guidance	The tester SHALL use the following unsigned content to test this requirement: r1300.4.1-datastream.xml. This requirement is intended to identify, communicate, and prevent software failure due to errors that MAY exist in content. The test report SHALL include evidence of the error.	
		Source Data Stream(s): r1300.4.1-datastream.xml. Artifact(s): - Evidence that the product reports the error(s). - One report for each platform family.	
13.	**SCAP.R.1400**	**The product SHALL report and MAY reject SCAP source data stream collection content that includes an OCIL component that is invalid according to the OCIL XML schema.**	
	Capability	☐ ACS ☐ CVE ☑ OCIL	
	SCAP.V.1400.1	The vendor SHALL provide instructions on how validation of SCAP source data stream collection that includes an invalid OCIL component is performed and where errors from validation will be displayed within the	

		product output.	
	SCAP.T.1400.1	The tester SHALL attempt to import a SCAP source data stream collection that includes an invalid OCIL component content into the vendor product and examine the product output to validate that the product reports the invalid OCIL content. The product MAY reject the content as invalid according to the OCIL XML schema.	
	Guidance	This is an OCIL only use case. This requirement is intended to identify, communicate, and prevent software failure due to errors that MAY exist in content. This requirement SHALL be validated using the r1400-ocil.xml content. Ensure the product reports and MAY reject the OCIL content that is invalid.	
		Source OCIL content: r1400-ocil.xml. Artifact(s): One ARF report for each platform family.	
14.	**SCAP.R.1500**	**The product SHALL be able to correctly process USGCB source data streams as input and produce valid results. If there are no USGCB source data streams for the platform(s) being tested, then this requirement is not applicable.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.1500.1	The vendor SHALL provide instructions on how to import and execute valid USGCB source data streams.	
	SCAP.V.1500.2	The lab or the vendor SHALL provide the scan results for each tested platform using USGCB content associated with the platforms for which validation is being sought.	
	SCAP.T.1500.1	The lab or the vendor SHALL evaluate the target platforms, in a managed configuration for Windows and standalone configuration for other platforms (i.e., RHEL, Mac OS, Unix, etc.), and produce results. If the testing is performed by the vendor, the source data streams, the scan results, and their hashes[7] will be submitted to the lab for verification.	
	Guidance	This requirement is intended to identify platforms supported by the product. All platforms for which the	

[7] The hashes SHALL comply with *Annex A: Approved Security Functions* of [Error! Reference source not found.].

Deleted: FIPS 140-2

		vendor intends to claim support on the Validated Products List MUST be tested. This requirement SHALL be tested using the all USGCB source data streams available on https://usgcb.nist.gov which are applicable to the tested platforms. The test report SHALL indicate the name of the data streams applied to the target system. The data stream that was executed and the scan results SHALL be included in the submission. The tester SHALL also include the hashes for source data streams and the scan results if the testing is performed by the vendor. Note: This requirement becomes not applicable if the USGCB repository does not contain a checklist for the platform(s) being tested.	
		Source Data Stream(s): Win7-Firewall-1.3.0.1.zip WinVista-Firewall-2.1.0.1.zip IE8-1.3.3.1.zip Win7-2.0.5.1.zip WinVista-3.0.5.1.zip Artifact(s): One ARF report for each platform being tested.	
	SCAP.T.1500.2	The tester SHALL review the scan results to ensure the files have not been altered, and pass the SCAPVal validation without any errors.	
	Guidance	If the testing was performed by the vendor, the Lab's tester SHALL verify the followings: - the hash of each result files and ensure it matches the value specified by the vendor; - visually inspect the scan results and look for anomalies like multiple errors, notapplicable, unknown, or notchecked results. Alternately, the tester MAY use a catalog file and compare.py to automate results comparison; - run the SCAPVal and verify if the results pass the validation without any errors. The following artifacts SHALL be included in the test package submitted to NIST: - a copy of the source data streams executed - a copy of scan results - the hashes of the scan results - the output of the SCAPVal	

15.	**SCAP.R.1510**	**The product SHALL be able to correctly evaluate a patches up-to-date XCCDF rule which references an OVAL source data stream component consistent with the normative guidance specified in [Error! Reference source not found.], against target systems of the target platform type and produce the expected results.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.1510.1	The vendor SHALL provide instructions on how to import and execute a valid SCAP source data stream with a patches up-to-date XCCDF rule. The vendor SHALL also provide instructions on where the resultant ARF XML Result output can be viewed by the tester.	
		Required Test Procedures: Per vendor instruction in SCAP.V.1510, the tester SHALL evaluate the target platform(s) using test content with patches up-to-date XCCDF rule implemented via numerous and single OVAL patch class definitions, validate results produced with SCAPVal, and compare actual results to expected results, ensuring actual results match expected results.	
	SCAP.T.1510.1	The tester SHALL evaluate the target platform(s) using a source data stream with an XCCDF patches up-to-date rule implemented via numerous OVAL patch class definitions in a domain connected configuration for Windows and standalone configuration for other platforms, validate results produced with SCAPVal, and compare the scan results produced by the product to the expected results, ensuring the actual results match the expected results.	
	Guidance	At least one platform per platform family for which the vendor intends to claim support on the Validated Products List MUST be tested. The scan results produced by the product SHALL match the expected results. The test report SHALL provide evidence of the comparison between actual results and expected results using the compare.py tool. The SCAPVal result output SHALL be included with the submission.	

Deleted: NIST SP 800-126 R3

		Source Data Stream(s): r1510.1-datastream.xml Artifact(s): - Scan results: one ARF report for each platform family. - SCAPVal output (xml and html) - Compare.py output.	
	SCAP.T.1510.2	The tester SHALL evaluate the target platform(s) using a source data stream with an XCCDF patches up-to-date rule implemented via a single OVAL patch class definition, in a domain connected configuration for Windows and standalone configuration for other platforms, validate results produced with SCAPVal, and compare the scan results produced by the product to the expected results, ensuring the actual results match the expected results	
	Guidance	Please follow the guidance for SCAP.T.1510.1.	
		Source Data Stream(s): r1510.2-datastream.xml Artifact(s): - Scan results: one ARF report for each platform family. - SCAPVal output (xml and html) - Compare.py output.	
16.	**SCAP.R.1600**	**If the product requires a specific configuration of the target platform that is not in compliance with the USGCB checklist, the vendor SHALL provide documentation indicating which settings require modification and a rationale for each changed setting. Products SHOULD only require changes to the target platform if needed for product functionality.**	
		NOTE: Pursuant to the U.S. Office of Management and Budget (OMB) Memorandum M-08-22 to Federal CIOs: "Both industry and government information technology providers must use SCAP validated tools with FDCC Scanner capability to certify their products operate correctly with FDCC configurations and do not alter FDCC settings." [**Error! Reference source not found.**] Products undergoing SCAP validations are required by OMB to make this self-assertion. Listing non-complaint settings in no way negates the OMB M-08-22 requirement.	
	Capability	☑ ACS ☐ CVE ☐ OCIL	

Deleted: OMB M-08-22

	SCAP.V.1600.1	The vendor SHALL provide an English language document to the lab that indicates which settings require modification and a rationale for each changed setting. This content will be used on NIST web pages to explain details about each validated product and thus SHOULD contain only information that is to be publicly released.	
	SCAP.T.1600.1	The tester SHALL review the provided documentation to ensure that each indicated setting includes an associated rationale.	
	Guidance	The test report SHOULD identify the document. This MAY be a document title, filename, URL, menu path, actual excerpt, or screenshot.	
17.	**SCAP.R.1700**	**The product SHALL be able to correctly process the test content that is representative of SCAP expressed content published at NIST National Checklist Program Repository, and the OVAL repository[8] which is associated with the platforms for which validation is being sought.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.1700.1	The vendor SHALL provide instructions on how to execute a previously imported valid data stream for platforms supported.	
	SCAP.T.1700.1	Per vendor instruction in SCAP.V.1700, the tester SHALL evaluate a target platform using test content representative of NIST NCP and OVAL repository, validate results produced with SCAPVal tool, and ensure actual results match expected results.	
	Guidance	These tests SHALL be executed using the OVAL Test Data (also referred to as the validation test suite) in the consolidated format. The configuration settings spreadsheets for these data streams are located in the "documents" folder. All platforms for which the vendor intends to claim support on the Validated Products List MUST be tested. The tester SHALL validate the ARF results with SCAPVal tool and include the results in the report. The test	

[8] The OVAL repository is hosted by Center for Internet Security: https://oval.cisecurity.org/repository.

		report SHALL provide evidence of the comparison between actual results and expected results using the compare.py tool. Any exceptions need to be justified. Source Data Stream(s): Windows-datastream.xml, RHEL-datastream.xml, and MacOS-datastream.xml Artifact(s): - Scan results: one ARF report for each tested platform. If the target machine is a Windows Server 2012 R2, the tests must be executed on a domain controller as well as on the Server 2012 member(s). - SCAPVal output (xml and html) - Compare.py output.	
18.	**SCAP.R.1800**	**The product SHALL be able to determine the applicability of an imported SCAP source data stream by evaluating the associated OCIL questionnaire for the CPE Name and platform id on an XCCDF <Benchmark>, <Profile>, <Group>, or <Rule> and verifying that the associated XCCDF content applies to the target system.**	
	Capability	☐ ACS ☐ CVE ☑ OCIL	
	SCAP.V.1800.1	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.	
	SCAP.T.1800.1	The tester SHALL import an SCAP source data stream into the product that contains a CPE Name and related OCIL questionnaire not applicable for the target system. The tester SHALL verify that the product declines to execute the non-applicable tests.	
	Guidance	For products being tested for the OCIL capability, this requirement SHALL be tested using r1800-ocil-datastream.xml data stream located in the requirements\r1800-ocil directory. The test report SHOULD indicate which XCCDF component (<Benchmark>, <Profile>, <Group>, or <Rule>) was correctly selected and executed based on the evaluation of the applicability tests, providing	

		evidence that the product declined to execute the non-applicable tests. Source Data Stream(s): r1800-datastream.xml Artifact(s): Expected Scan Results: ARF reports for each platform family. 1. ARF reports for test cases (1.a, 1.b) or (1.c, 1.d) 2. ARF reports for test cases 2.a, and 2.b. 3. ARF reports for test cases 3.a, and 3.b - SCAPVal output (xml and html) - Compare.py output.	
19.	**SCAP.R.1900**	**The product SHALL be able to correctly evaluate a valid OVAL Definition file and external variable file, where the contents of the OVAL Definition file are consistent with the normative guidance[9] specified in [Error! Reference source not found.], against target systems of the target platform type and produce a result for each definition using the OVAL XML Full Results expressed as Single Machine Without System Characteristics, Single Machine With System Characteristics, and Single Machine With Thin Results.[10]**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.1900.1	The vendor SHALL provide instructions on how a valid OVAL Definitions file and external variable file can be imported into the product for interpretation. The vendor SHALL also provide instructions on where the resultant OVAL XML Results output can be viewed by the tester.	
	SCAP.T.1900.1	The tester SHALL run the product using valid OVAL Definitions files and an external variable file against the test system of the target platform type. The actual results SHALL match the expected results.	
	Guidance	This is an OVAL only use case. The R1900 content SHALL be used when testing this requirement.	

Deleted: NIST SP 800-126 R1

[9] The supported OVAL tests are published at https://scap.nist.gov/validation/index.html.

[10] The use case for OVAL-Only Scanning is described in Section 5.4 of [Error! Reference source not found.].

Deleted: NIST SP 800-126 R1

		Source OVAL file: macos-R1900-ext-var-oval.xml macos-R1900-ext-var-variables.xml macos-R1900-oval.xml rhel-R1900-ext-var-oval.xml rhel-R1900-ext-var-variables.xml rhel-R1900-oval.xml win-R1900-ext-var-oval.xml win-R1900-ext-var-variables.xml win-R1900-oval.xml Artifact(s): Expected Scan Results: OVAL XML full results expressed as Single Machine Without System Characteristics, Single Machine With System Characteristics, and Single Machine With Thin Results for each platform family.	
	SCAP.T.1900.2	The tester SHALL validate the resulting OVAL XML Full Results by importing the result set into the SCAPVal utility and checking for validation errors.	
	Guidance	The test report SHALL indicate the SCAPVal results. The SCAPVal result output SHALL be included with the submission.	
		Artifact(s): - SCAPVal output (xml and html)	
	SCAP.T.1900.3	The tester SHALL validate that the resulting OVAL XML Full Results are available for viewing by the user.	
	Guidance	The test report SHALL provide evidence that the output is available for viewing. Providing evidence of the actual output as opposed to just its availability is preferred though either is acceptable.	
		Artifact(s): - Location of the output folder where the scan results can be checked.	
	SCAP.T.1900.4	After the test system is assessed using the OVAL file, the tester SHALL capture the	

		successful results of the scan and verify the correctness of the results.	
	Guidance	The test report SHALL indicate the location of the product output. The output produced by the product SHALL be included in the submission. The tester SHALL compare the scan results with the expected results from the Excel spreadsheet.	
		Artifact(s): - OVAL scan results - Comparison results with the expected results - SCAPVal output	
	SCAP.T.1900.5	When the OVAL Definition file has been evaluated with the external variable file that defines different values for the variables, the tester SHALL validate that the OVAL XML Full Results file includes unique variable values as defined in the external variables file.	
	Guidance	A variable (in the context of OVAL) is analogous to a DEFINE or CONSTANT statement in several programming languages. A variable is nothing more than a static value that has been named one or more times within the xml content. The "requirements\r1900 content SHALL be used when testing this requirement. This content includes the external variable file. The test report SHALL indicate the name and values of the variable that were reported by the product under test.	
		Source OVAL file: macos-R1900-ext-var-oval.xml macos-R1900-ext-var-variables.xm rhel-R1900-ext-var-oval.xml rhel-R1900-ext-var-variables.xml win-R1900-ext-var-oval.xml win-R1900-ext-var-variables.xml Artifact(s): Expected Scan Results: OVAL XML full results expressed as Single Machine Without System Characteristics, Single Machine With System Characteristics, and Single Machine With Thin Results for each platform family. - Comparison results with the expected results - SCAPVal output	

20.	**SCAP.R.2000**	**The product SHALL be able to correctly evaluate a valid OVAL Definition component that is part of an SCAP source data stream, where the contents of the OVAL definition file are consistent with the normative guidance[11] specified in [Error! Reference source not found.] and [Error! Reference source not found.], against target systems of the target platform type and produce a result for each definition using the OVAL XML Full Results expressed as Single Machine Without System Characteristics, Single Machine With System Characteristics, and Single Machine With Thin Results.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.2000.1	The vendor SHALL provide instructions on how a valid SCAP data stream file can be imported into the product for interpretation. The vendor SHALL also provide instructions on where the resultant SCAP Results output can be viewed by the tester.	
	SCAP.T.2000.1	The tester SHALL run the product using a valid SCAP data stream against the target systems of the target platform type. The actual results SHALL match the expected results.	
	Guidance	This is use case demonstrates the ability to process an OVAL component that is part of an SCAP source data stream that is referred by an XCCDF component. The data stream import and compliance scan from SCAP.T.1700.1 SHALL be used to address this requirement. The test report SHALL provide evidence of the comparison between actual results and expected results. Any exceptions SHALL be justified.	
		Source Data Stream(s): Windows-datastream.xml; RHEL-datastream.xml; or MacOS-datastream.xml Artifact(s): - Expected Scan Results: One ARF report for each platform family with OVAL XML Full Results component expressed as Single Machine Without System Characteristics, Single Machine With System Characteristics, and Single Machine With Thin Results from Configuration 1. - Comparison results with the expected results - SCAPVal output	

Deleted: NIST SP 800-126 R3

Deleted: NIST SP 800-126A

[11] The supported OVAL tests are published at https://scap.nist.gov/validation/index.html.

	SCAP.T.2000.2	The tester SHALL validate the resulting SCAP data stream by importing it into the SCAPVal utility and checking for any validation errors.	
	Guidance	The test report SHALL indicate the SCAPVal analysis result and location. The SCAPVal analysis output SHALL be included with the submission.	
		Source Data Stream(s): Windows-datastream.xml; RHEL-datastream.xml; or MacOS-datastream.xml Artifact(s): - Expected Scan Results: One ARF report for each platform family with OVAL XML Full Results component expressed as Single Machine Without System Characteristics, Single Machine With System Characteristics, and Single Machine With Thin Results from Configuration 1. - SCAPVal output	
	SCAP.T.2000.3	The tester SHALL validate that the resulting SCAP data stream is available for viewing by the user.	
	Guidance	The test report SHALL provide evidence that the output is available for viewing.	
	SCAP.T.2000.4	The tester SHALL capture the successful results of the import and verify the correctness of the results.	
	Guidance	The test report SHALL indicate the location of the product output. The output produced by the compare.py tool SHALL be included in the submission.	
		Source Data Stream(s): Windows-datastream.xml; RHEL-datastream.xml; or MacOS-datastream.xml Artifact(s): - Expected Scan Results: One ARF report for each platform family with OVAL XML Full Results component expressed as Single Machine Without System Characteristics, Single Machine With System Characteristics, and Single Machine With Thin Results from Configuration 1. - Comparison results with the expected results	

21.	**SCAP.R.2100**	**The product SHALL be able to correctly evaluate a valid OCIL Questionnaire file against test systems of the target platform type, and produce a valid OCIL Output file (i.e., file that includes both the original content and the evaluation results) using the format defined by the OCIL XML schema.**	
	Capability	☐ ACS ☐ CVE ☑ OCIL	
	SCAP.V.2100.1	The vendor SHALL provide instructions on how a valid OCIL Questionnaire file can be imported into the product for interpretation. The vendor SHALL also provide instructions on where the resultant OCIL Output file can be viewed by the tester.	
	SCAP.T.2100.1	The tester SHALL run the product using valid OCIL document files against the test systems of the target platform type. The results SHALL be verified by the tester, ensuring each OCIL definition and criteria contained within the definition produces the correct response.	
	Guidance	This is an OCIL only use case that demonstrates the ability to process OCIL questionnaires. Content that is not executed as a result of an OCIL evaluation SHOULD report "Not-Checked". This requirement SHALL be validated using requirements\R2100-ocil.xml. The test report SHOULD indicate the name of the data stream. The data stream that was executed SHOULD be included in the submission. The test report SHALL provide evidence of the comparison between actual results and expected results. This MAY be a screenshot or some indicator of the differences if any. Any exceptions need to be justified.	
		Source OCIL file: r2100-ocil.xml Artifact(s): - Expected Scan Results: OCIL XML results file for each platform family. - Comparison results.	

	SCAP.T.2100.2	The tester SHALL validate the resulting OCIL Output file with the SCAPVal utility and check for any validation errors.	
	Guidance	The test report SHALL indicate the SCAPVal analysis result and location. The SCAPVal analysis output SHALL be included with the submission.	
		Source OCIL file: r2100-ocil.xml Artifact(s): - Expected Scan Results: OCIL XML results file for each platform family. - SCAPVal output.	
	SCAP.T.2100.3	The tester SHALL validate that the resulting OCIL Output file is available for viewing by the user.	
	Guidance	The test report SHALL provide evidence that the output is available for viewing.	
		Artifact(s): - Location of the output folder where the scan results can be checked.	
22.	**SCAP.R.2200**	**The product SHALL be able to correctly evaluate a valid OCIL Questionnaire component that is part of an SCAP source data stream against target systems of the target platform type, and produce a valid OCIL results component (i.e., component that includes both the original content and the evaluation results) using the format defined by the OCIL XML schema.**	
	Capability	☐ ACS ☐ CVE ☑ OCIL	
	SCAP.V.2200.1	The vendor SHALL provide instructions on how a valid OCIL Questionnaire file that is part of an SCAP source data stream can be imported into the product for interpretation. The vendor SHALL also provide instructions on where the resultant SCAP data stream can be viewed by the tester.	
	SCAP.T.2200.1	The tester SHALL run the product using valid SCAP data stream files against the target systems of the target platform type. The actual	

		results SHALL match the expected results.	
	Guidance	This requirement is testing an OCIL component that is part of a SCAP source data stream. This requirement SHALL be validated using the r2200-datastream.xml data stream located in the R2200 folder. The data stream that was executed and the scan results SHALL be included in the submission. The test report SHALL provide evidence of the comparison between actual results and expected results. This MAY be a screenshot or some indicator of the differences if any. Any exceptions need to be justified.	
		Source Data Stream(s): r2200-datastream.xml Artifact(s): - Expected Scan Results: One ARF report for each platform family. - Comparison results with the expected results	
	SCAP.T.2200.2	The tester SHALL validate the resulting SCAP data stream by importing it into the SCAPVal utility and checking for any validation errors.	
	Guidance	The test report SHALL indicate the SCAPVal result and location. The SCAPVal output SHALL be included with the submission.	
		Source Data Stream(s): r2200-datastream.xml Artifact(s): - Expected Scan Results: One ARF report for each platform family. - SCAPVal output	
	SCAP.T.2200.3	The tester SHALL validate that the resulting SCAP data stream is available for viewing by the user.	
	Guidance	The test report SHALL provide evidence that the output is available for viewing.	
		Artifact(s): - Location of the output folder where the scan results can be checked.	

23.	**SCAP.R.2300**	**The product SHALL indicate the correct CCE ID for each configuration issue referenced within the product that has an associated CCE ID (i.e., the product's CCE mapping MUST be correct).**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.2300.1	None.	
	SCAP.T.2300.1	Using the product output from SCAP.R.2930, the tester SHALL compare the vendor data against the official CCE description. The tester SHALL perform the comparison using a non-vendor-directed sample comprised of greater than or equal to 10 and less than or equal to 30 of the total configuration issue items with CCE IDs. The tester SHOULD prove that the vendor's CCE ID correctly maps to the configuration issue. This test ensures that the product correctly maps to CCE IDs, but does not test for completeness of the mapping.	
	Guidance	The test report SHALL provide evidence indicating the existence of the sampled CCE IDs within the product output. This SHALL be the entire random sample selected by the lab. This does not need to include the information used for comparison from the official CCE ID list. If applicable, a list of mis-matches found during testing SHALL be reported.	
		Source Data Stream(s): r2930-win-datastream.xml, r2930-rhel-datastream.xml, and r2930-macos-datastream.xml Artifact(s): - Scan results: one ARF report for each platform family. - List of sampled CCE IDs from the ARF report	
24.	**SCAP.R.2400**	**The product SHALL associate an existing CCE ID to each configuration issue referenced within the product for which a CCE ID exists (i.e., the product's CCE mapping MUST be complete).**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.2400.1	None.	
	SCAP.T.2400.1	Using the list of configuration issue items produced in SCAP.R.2930, the tester SHALL examine the descriptions and search the CCE dictionary for all corresponding CCE IDs. The tester SHALL perform this using a non-vendor-directed sample comprised of 10% of the total	

		configuration issue items with no CCE IDs, up to a maximum of 30. The tester does not need to rigorously prove that no CCE ID exists, only that there does not appear to be a match. This test ensures that the product has a complete mapping to CCE, but does not test the correctness of the mapped data.	
	Guidance	The test report SHALL provide evidence indicating the existence of the sampled CCE IDs and their associated description within the product output. This SHALL be the entire random sample selected by the lab. If applicable, a list of mis-matches found during testing SHALL be reported. Source Data Stream(s): r2930-win-datastream.xml, r2930-rhel-datastream.xml, and r2930-macos-datastream.xml Artifact(s): - Scan results: one ARF report for each platform family. - List of sampled CCE IDs from the ARF report	
25.	**SCAP.R.2500**	**If the product natively contains a product dictionary (as opposed to dynamically importing content containing CPE names), the product MUST contain CPE naming data from the current official CPE Dictionary.** **NOTE:** This requirement does not apply if the product is using the official dynamic CPE Dictionary as provided on the NVD web site or as part of an SCAP source data stream.	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.2500.1	The vendor SHALL provide a list of all CPE names included in the product using the standard CPE Dictionary XML schema as provided in the CPE Specification version cited in Section 2.	
	SCAP.V.2500.2	If the vendor product includes CPE names that are not in the official CPE Dictionary, a listing of exceptions MUST be provided.	
	SCAP.T.2500.1	The tester SHALL compare the vendor-provided list of CPE Names against the official CPE Dictionary.[12] The tester SHALL verify that all exceptions found match the list of exceptions	

[12] Official Common Platform Enumeration (CPE) Dictionary is available at https://nvd.nist.gov/products/cpe

		provided by the vendor.	
	Guidance	This requirement does not apply if the product is using the official dynamic CPE Dictionary as provided on the NVD web site or as part of an SCAP source data stream. The test report SHOULD provide the vendor provided list of all CPE Names included in the product, and list of exceptions if any.	
26.	**SCAP.R.2600**	**Products MUST process CPEs referenced in an** *<xccdf:platform>* **element directly or by a** *<cpe2:fact-ref>* **contained within a referenced** *<cpe2:platform-specification>* **element as specified in [**Error! Reference source not found.**].**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.2600.1	The vendor SHALL provide instructions describing how to import an SCAP source data stream that contains references to CPEs in an *<xccdf:platform>* element directly or by a *<cpe2:fact-ref>* contained within a referenced *<cpe2:platform-specification>* element and have it applied against a known platform. The vendor SHALL also provide instructions on how to view the results of the application of the content against the platform.	
	SCAP.T.2600.1	The tester SHALL import the known content into the product and apply it against a known platform.	
	Guidance	This use case demonstrates the ability to process content based on the CPE referenced in the content. This requirement MAY be validated using the R1200 data stream located in the OVAL Test Data (R1200\r1200-datastream.xml). The test report SHALL indicate the name of the data stream. The data stream that was imported SHOULD be included in the submission.	
		Source Data Stream(s): r1200-datastream.xml Expected Scan Results: 1. ARF reports for test cases (1.a, 1.b, 1.c, 1.d, and 1.e) or (1.f, 1.g, 1.h, 1.i, and 1.j) 2. ARF reports for test cases 2.a, 2.b, and 2.c 3. ARF reports for test cases 3.a, and 3.b Expected Scan Results: ARF reports for each platform	

Deleted: NIST SP 800-126 R3

		family.	
	SCAP.T.2600.2	The tester SHALL import the results of the content into the SCAPVal utility and check for any validation errors.	
	Guidance	The test report SHALL indicate the SCAPVal analysis result and location. The SCAPVal analysis output SHALL be included with the submission.	
		Source Data Stream(s): r1200-datastream.xml Expected Scan Results: 1. ARF reports for test cases (1.a, 1.b, 1.c, 1.d, and 1.e) or (1.f, 1.g, 1.h, 1.i, and 1.j) 2. ARF reports for test cases 2.a, 2.b, and 2.c 3. ARF reports for test cases 3.a, and 3.b Artifact(s) - Expected Scan Results: ARF reports for each platform family. - SCAPVal output (xml and html)	
	SCAP.T.2600.3	The tester SHALL ensure the actual results match the expected results.	
	Guidance	The test report SHALL provide evidence of the comparison between actual results and expected results.	
		Source Data Stream(s): r1200-datastream.xml Expected Scan Results: 1. ARF reports for test cases (1.a, 1.b, 1.c, 1.d, and 1.e) or (1.f, 1.g, 1.h, 1.i, and 1.j) 2. ARF reports for test cases 2.a, 2.b, and 2.c 3. ARF reports for test cases 3.a, and 3.b Artifact(s) - Expected Scan Results: ARF reports for each platform family. - compare.py output	
27.	**SCAP.R.2700**	**The product SHALL indicate the correct CVE ID or metadata for each software flaw and/or patch**	

		definition referenced within the product that has an associated CVE ID (i.e., the product's CVE mapping MUST be correct).	
	Capability	☐ ACS ☑ CVE ☐ OCIL	
	SCAP.V.2700.1	None	
	SCAP.T.2700.1	Using the product output from SCAP.R.2920, the tester SHALL compare the vendor data against the official NVD CVE ID description and references. The tester SHALL perform this test using a non-vendor-directed sample comprised of 10% of the total software flaws and/or patches with CVE IDs, up to a maximum of 30. The tester does not need to rigorously prove that the vendor's software flaw and/or patch description matches the NVD CVE description, but merely needs to identify that the two descriptions appear to pertain to the same vulnerability. This test ensures that the product correctly maps to CVE, but does not test for completeness of the mapping. It is sufficient to provide specific URLs that link to the NVD website. For example, https://nvd.nist.gov/vuln/detail/CVE-2017-7269. It is not sufficient to provide a generic URL to https://nvd.nist.gov/vuln.	
	Guidance	The test report SHALL provide evidence indicating the existence of the sampled CVE IDs within the product output. This SHALL be the entire random sample selected by the lab. This SHOULD include the information used for comparison at the NVD web site.	
		Source Data Stream(s): r2920-datastream.xml Artifact(s) - Expected Scan Results: ARF reports for each platform family. - list of CVE IDs used by the tester for comparison.	
28.	**SCAP.R.2800**	**The product SHALL associate an existing CVE ID to each software flaw and/or patch referenced within the product for which a CVE ID exists (i.e., the product's CVE mapping MUST be complete).**	
	Capability	☐ ACS ☑ CVE ☐ OCIL	
	SCAP.V.2800.1	None.	
	SCAP.T.2800.1	Using the list of software flaws produced in SCAP.R.2920, the tester SHALL examine the descriptions and search the NVD for any	

		corresponding CVE IDs. The tester SHALL perform this using a non-vendor-directed sample comprised of 10% of the total software flaws and/or patches with no CVE IDs, up to a maximum of 30. The tester does not need to rigorously prove that no CVE ID exists, only that there does not appear to be a match. This test ensures that the product has a complete mapping to CVE, but does not test the correctness of the mapped data.	
	Guidance	The test report SHALL provide evidence indicating the existence of the sampled software flaws and/or patches within the product output. This SHALL be the entire random sample selected by the lab. This does not need to include the information used for comparison at the NVD web site. It is sufficient to provide URLs that link to the NVD, MITRE and/or vendor vulnerability database website. For example, https://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2011-1377 or https://access.redhat.com/security/cve/CVE-2013-0151. The URL SHALL be specific and it is not sufficient to provide a generic URL such as: https://web.nvd.nist.gov or https://access.redhat.com/security/updates/ .	
		Source Data Stream(s): r2920-datastream.xml Artifact(s) - Expected Scan Results: ARF reports for each platform family. - list of CVE IDs used by the tester for comparison.	
29.	**SCAP.R.2850**	**The product SHALL be able to identify SWID tags installed on a target asset using OVAL class inventory class definitions that are part of an SCAP source data stream. The product SHALL use the methods described in [Error! Reference source not found.][13].**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.2850.1	The vendor SHALL provide instructions on how the product identifies SWID tags using OVAL	

Deleted: NIST SP 800-126 R3

[13] See Section 3.6 Software Identification (SWID) Tags of the [NIST SP 800-126 R3]

		inventory class definitions that are part of an SCAP source data stream.	
	SCAP.T.2850.1	The tester SHALL import the SCAP 1.3 source data stream, apply it to a known target, and produce an SCAP result data stream conforming to the ARF specification.	
	Guidance	Per vendor instruction in SCAP.V.2850, the tester SHALL evaluate the target platform(s) using the test content, validate results produced with SCAPVal, and compare actual results to expected results, ensuring actual results match expected results. The test report SHALL provide evidence indicating the existence of the sampled SWID tags within the product output (ARF report).	
		Source Data Stream(s): r2850-win-datastream.xml, r2850-rhel-datastream.xml, and r2850-macos-datastream.xml Artifact(s): - Scan results: one ARF report for each platform family. - List of SWID tags identified by the product that are included in the ARF report	
	SCAP.T.2850.2	The tester SHALL validate the results produced using SCAPVal; the validation MUST NOT produce any errors.	
	Guidance	The tester SHALL validate results produced with SCAPVal and make sure there are no errors.	
		Source Data Stream(s): r2850-win-datastream.xml, r2850-rhel-datastream.xml, and r2850-macos-datastream.xml Artifact(s): - Scan results: one ARF report for each platform family. - SCAPVal output	
	SCAP.T.2850.3	The tester SHALL compare the actual results to the expected results ensuring the results match.	
	Guidance	The test report SHALL provide evidence of the comparison between actual results and expected results using the compare.py tool.	
		Source Data Stream(s): r2850-win-datastream.xml, r2850-rhel-datastream.xml, and r2850-macos-datastream.xml	

		Artifact(s): – Scan results: one ARF report for each platform family. – compare.py output	
30.	**SCAP.R.2860**	**The product SHALL be able to identify SWID tags installed on a target asset using OVAL inventory class definitions that are part of a standalone OVAL Definition file. The product SHALL use the methods described in [**Error! Reference source not found.**][14].**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	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.	
	SCAP.T.2860.1	The tester SHALL import OVAL inventory class definitions that are part of a standalone OVAL Definition file, apply it to a known target, and produce an OVAL results file conforming to the OVAL specification.	
	Guidance	Per vendor instruction in SCAP.V.2860, the tester SHALL evaluate the target platform(s) using the test content, validate results produced with SCAPVal, and compare actual results to expected results, ensuring actual results match expected results. The test report SHALL provide evidence indicating the existence of the sampled SWID tags within the product output (OVAL results file). The tester SHAL validate results produced with SCAPVal and make sure there are no errors.	
		Source OVAL files: r2860-win-oval.xml, r2860-rhel-oval.xml, and r2860-macos-oval.xml Artifact(s): – Scan results: one OVAL Full Results with System Characteristics for each platform family. – List of SWID tags identified by the product that are included in the OVAL results file.	
	SCAP.T.2860.2	The tester SHALL validate the results produced using SCAPVal; the validation MUST NOT produce any errors.	

Deleted: NIST SP 800-126 R3

[14] *Ibid.*

	Guidance	The tester SHAL validate results produced with SCAPVal and make sure there are no errors.
		Source Data Stream(s): r2860-win-oval.xml, r2860-rhel-oval.xml, and r2860-macos-oval.xml Artifact(s): - Scan results: one OVAL Full Results with System Characteristics for each platform family. - SCAPVal output
	SCAP.T.2860.3	The tester SHALL compare the actual results to the expected results ensuring the results match.
	Guidance	The test report SHALL provide evidence of the comparison between actual results and expected results using the compare.py tool.
		Source Data Stream(s): r2860-win-oval.xml, r2860-rhel-oval.xml, and r2860-macos-oval.xml Artifact(s): - Scan results: one OVAL Full Results with System Characteristics for each platform family. - compare.py output
31.	**SCAP.R.2900**	**SCAP result data streams SHALL be produced by the product in compliance with the SCAP result data streams as specified in [Error! Reference source not found.] and [Error! Reference source not found.].**
	Capability	☑ ACS ☐ CVE ☐ OCIL
	SCAP.V.2900.1	The vendor SHALL provide instruction on where the corresponding SCAP result data stream file(s) can be located for inspection.
	SCAP.T.2900.1	The tester SHALL visually inspect SCAP results to verify that the ARF report contains a report object for each XCCDF, OVAL, and OCIL component executed when a source data stream is evaluated against a target. Each

Deleted: NIST SP 800-126 R3

Deleted: NIST SP 800-126A

		component result SHALL be captured as a separate <arf:report> element[15] in the <arf:asset-report-collection> element.
	Guidance	The vendors are not required to produce signed ARF reports. The test report SHALL provide the resulting output from the candidate product. The tester SHALL verify that the ARF report contains a report object for each XCCDF, OVAL, and OCIL component executed. The test report SHALL indicate the SCAPVal result and location. The SCAPVal output SHALL be included with the submission.
		Source Data Stream(s): Windows-datastream.xml, RHEL-datastream.xml, and MacOS-datastream.xml Artifact(s) - Expected Scan Results: One ARF report for each platform family. - verify that each the ARF report contains three <arf:report> elements: 1xXCCDF, 1xOVAL Inventory, and 1xOVAL compliance results.
	SCAP.T.2900.2	The tester SHALL validate the SCAP result data stream files with SCAPVal and pass without any errors.
	Guidance	The tester SHALL validate results produced with SCAPVal and make sure there are no errors.
		Source Data Stream(s): Windows-datastream.xml, RHEL-datastream.xml, and MacOS-datastream.xml Artifact(s) - Expected Scan Results: One ARF report for each platform family. - SCAPVal output.
32.	SCAP.R.2910	**The product SHALL be able to correctly import and evaluate SCAP source data streams which reference external content consistent with the normative guidance specified in [Error! Reference source not found.], against target systems of the target platform type and produce the expected results.**
	Capability	☑ ACS ☐ CVE ☐ OCIL

Deleted: NIST SP 800-126 R3

[15] For instance, if a source data stream which includes four components (XCCDF, OVAL, CPE-Dictionary, and CPE-OVAL) is evaluated, then the ARF report SHALL include three component results (XCCDF results, OVAL results, CPE-OVAL results).

	SCAP.V.2910.1	The vendor SHALL provide instructions on how to import and execute a valid SCAP source data stream with references to external content. The vendor SHALL also provide instructions on where the resultant ARF XML Result output can be viewed by the tester.	
		Required Test Procedures: Per vendor instruction in SCAP.V.2910, the tester SHALL evaluate the target platform(s) using test content with references to external content, validate results produced with SCAPVal, and compare actual results to expected results, ensuring actual results match expected results.	
	SCAP.T.2910.1	The tester SHALL evaluate the target platform(s), in a domain connected configuration for Windows and standalone configuration for other platforms, validate results produced with SCAPVal, and compare the scan results produced by the product to the expected results, ensuring the actual results match the expected results.	
	Guidance	All platforms families for which the vendor intends to claim support on the Validated Products List MUST be tested. This requirement SHALL be tested using the SCAP 1.3 data stream r2910-datastream.xml located in the R2910 folder. The scan results produced by the product SHALL match the expected results. The test report SHALL indicate the SCAPVal results. The SCAPVal result output SHALL be included with the submission. The test report SHOULD indicate the name of the data streams applied to the target system. The data stream that was executed SHOULD be included in the submission. The test report SHALL provide evidence of the comparison between actual results and expected results using the compare.py tool. Any exceptions need to be justified.	
		Source Data Stream(s): r2910-datastream.xml Artifact(s) - Expected Scan Results: One ARF report for each platform family. - SCAPVal output.	

		- compare.py output	
33.	**SCAP.R.2920**	**The product SHALL be able to assign CVE identifiers to rule results in compliance with the SCAP result data streams as specified in** Error! Reference source not found.**.**	
	Capability	☑ ACS ☑ CVE ☐ OCIL	
	SCAP.V.2920.1	The vendor SHALL provide instruction on where the SCAP Result Data Stream files can be located for inspection.	
	SCAP.T.2920.1	The tester SHALL visually inspect the results to verify that the CVE identifiers are included within the <xccdf:rule-result> element. The SCAP Result Data Streams MUST be processed by the SCAPVal utility without any errors.	
	Guidance	The tester SHALL use the requirements\r2920-datastream.xml content for testing this requirement. The test report SHALL include the resulting SCAP result data streams from vendor's product. The test report SHALL indicate the SCAPVal result and location. The SCAPVal output SHALL be included with the submission.	
		Source Data Stream(s): r2920-datastream.xml Artifact(s) - Expected Scan Results: One ARF report for each platform family. - SCAPVal output. - compare.py output	
34.	**SCAP.R.2930**	**The product SHALL be able to assign CCE identifiers to rule results in compliance with the SCAP result data streams as specified in [**Error! Reference source not found.**].**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.2930.1	The vendor SHALL provide instruction on where the SCAP Result Data Stream files can be located for inspection.	
	SCAP.T.2930.1	The tester SHALL visually inspect the results to	

Deleted: NIST SP 800-126 R3

Deleted: NIST SP 800-126 R3

		verify that the CCE identifiers are included within the <xccdf:rule-result> element. The SCAP Result Data Streams MUST be processed by the SCAPVal utility without any errors.	
	Guidance	The tester SHALL use the requirements\r2930-win-datastream.xml, r2930-rhel-datastream.xml, and r2930-macos-datastream.xml for testing this requirement. The test report SHALL include the resulting SCAP result data streams from vendor's product. The test report SHALL indicate the SCAPVal result and location. The SCAPVal output SHALL be included with the submission.	
		Source Data Stream(s): r2930-win-datastream.xml, r2930-rhel-datastream.xml, and r2930-macos-datastream.xml Artifact(s) - Expected Scan Results: One ARF report for each platform family. - SCAPVal output. - compare.py output	
35.	**SCAP.R.2940**	**The product SHALL be able to assign CPE identifiers to rule results in compliance with the SCAP result data streams as specified in [**Error! Reference source not found.**].**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.2940.1	The vendor SHALL provide instruction on where the SCAP Result Data Stream files can be located for inspection.	
	SCAP.T.2940.1	The tester SHALL visually inspect the results to verify that the CPE identifiers are included within the <xccdf:rule-result> element. The SCAP Result Data Streams MUST be processed by the SCAPVal utility without any errors.	
	Guidance	The tester SHALL use the r2940-datastream.xml for testing this requirement. The test report SHALL include the resulting SCAP result data streams from vendor's product. The test report SHALL indicate the SCAPVal result and	

Deleted: NIST SP 800-126 R3

		location. The SCAPVal output SHALL be included with the submission.	
		Source Data Stream(s): r2940-datastream.xml Artifact(s) - Expected Scan Results: One ARF report for each platform family. - SCAPVal output. - compare.py output	
36.	**SCAP.R.3000**	**The product SHALL be able to process XCCDF components that are part of an SCAP source data stream and generate XCCDF component results within an SCAP result data stream in accordance with the XCCDF specification for the target platform.**[16]	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.3000.1	The vendor SHALL provide instructions on how to import XCCDF component content that is part of SCAP source data streams for execution and provide instructions on where the XCCDF component results can be located for visual inspection. The purpose of this requirement is to ensure that the product produces valid XCCDF Results and a matching "pass", "fail", "error", "unknown", "notapplicable", "notchecked", "notselected", "informational", or "fixed" result for a given rule.	
	SCAP.T.3000.1	The tester SHALL import a known valid XCCDF component content that is part of SCAP data streams for the target platform into the vendor product and execute it according to the product operation instructions provided by the vendor. The tester will inspect the product output ensuring XCCDF components are compliant with the XCCDF specification.	
	Guidance	The product results SHALL be compliant with the XCCDF specification. For example, the **<xccdf:result>** MUST match the results defined in the specification (i.e., "pass", "fail", "error", "unknown", "notapplicable", "notchecked", "notselected", "informational", or "fixed"). Variations are not acceptable. The data stream import and compliance scan from	

[16] XCCDF Specification in [Error! Reference source not found.].

Deleted: NISTIR 7275 R4

		SCAP.T.800.3 MAY be used to validate that the product output includes the checks and check parameters as expected. The test report SHALL indicate the OVAL definitions inspected by the tester for a single platform. The test report SHALL indicate the platform validated. The test report SHOULD indicate the location of the data stream. The data stream that was imported SHOULD be included in the submission. The test report SHALL provide evidence of the comparison between actual results and expected results using the compre.py tool. Any exceptions need to be justified.	
		Source Data Stream(s): r800-win-datastream.xml; r800-rhel-datastream.xml; and r800-macos-datastream.xml Artifact(s): - Expected Scan Results: One ARF report for each platform family.	
	SCAP.T.3000.2	The tester SHALL validate the resulting XCCDF component results within an SCAP result data stream output using the SCAPVal utility. This validation MUST NOT produce any validation errors.	
	Guidance	Using the result from SCAP.T.3000.1, the test report SHALL indicate the SCAPVal result and location. The SCAPVal output SHALL be included with the submission.	
		Source Data Stream(s): r800-win-datastream.xml; r800-rhel-datastream.xml; and r800-macos-datastream.xml Artifact(s): - Expected Scan Results: One ARF report for each platform family. - SCAPVal output (html and XML)	
	SCAP.T.3000.3	The tester SHALL compare the product results to the expected results ensuring that the “pass”, “fail”, “error”, “unknown”, “notapplicable”, “notchecked”, “notselected”, “informational”, or “fixed” results match for each <xccdf:Rule>.	
	Guidance	Using the result from SCAP.T.3000.1, the test report	

		SHOULD indicate the name of the data stream. The data stream that was imported SHOULD be included in the submission. The test report SHALL provide evidence of the comparison between actual results and expected results using the compare.py tool. Any exceptions need to be justified. Source Data Stream(s): r800-win-datastream.xml; r800-rhel-datastream.xml; and r800-macos-datastream.xml Artifact(s): - Expected Scan Results: One ARF report for each platform family. - compare.py output	
37.	**SCAP.R.3005**	**The product SHALL be able to process XCCDF Tailoring component (<xccdf:Tailoring>) that is part of an SCAP source data stream as well as XCCDF Tailoring component that is external to the source datastream and generate XCCDF component results within an SCAP result data stream in accordance with the XCCDF specification for the target platform.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.3005.1	The vendor SHALL provide instructions on how to import XCCDF Tailoring component content that is part of or external to the SCAP source data streams for execution and provide instructions on where the XCCDF component results can be located for visual inspection. The purpose of this requirement is to ensure that the product produces valid XCCDF Results and the results match the expected results for all given rules.	
	SCAP.T.3005.1	The tester SHALL import a known valid XCCDF Tailoring component content that is part of SCAP source data streams for the target platform into the vendor product and execute it according to the product operation instructions provided by the vendor. The tester will inspect the product output ensuring XCCDF components are compliant with the XCCDF specification.	
	Guidance	The tester SHALL use the requirements\R3005\r3005-datastream-01.xml and r3005-datastream-02.xml data streams.	

		The test report SHOULD indicate the location of the data streams. The data streams that were imported SHOULD be included in the submission. The test report SHALL provide evidence from the product output that the selected data stream was in fact executed. The ARF reports SHALL be included in the submission.	
		Source Data Stream(s): r3005-datastream-01.xml; and r3005-datastream-02.xml. Artifact(s): - Expected Scan Results: One ARF report for each platform family for the following selected profiles "xccdf_gov.nist.validation_profile_r3005_01", "xccdf_gov.nist.validation_profile_r3005_tailoring_01", and "xccdf_gov.nist.validation_profile_r3005_tailoring_02".	
	SCAP.T.3005.2	The tester SHALL import a known valid XCCDF Tailoring component content that is external to the SCAP source data streams for the target platform into the vendor product and execute it according to the product operation instructions provided by the vendor. The tester will inspect the product output ensuring XCCDF components are compliant with the XCCDF specification.	
	Guidance	The tester SHALL use the requirements\R3005\ r3005-datastream-03.xml data stream. The test report SHOULD indicate the location of the data streams. The data streams that were imported SHOULD be included in the submission. The test report SHALL provide evidence from the product output that the selected data stream was in fact executed. The ARF reports SHALL be included in the submission.	
		Source Data Stream(s): r3005-datastream-03.xml. Artifact(s): - Expected Scan Results: One ARF report for each platform family for the following selected profile: "xccdf_gov.nist.validation_profile_r3005_tailoring_03".	

	SCAP.T.3005.3	The tester SHALL validate the resulting XCCDF component results within an SCAP result data stream output using the SCAPVal utility. This validation MUST NOT produce any validation errors.	
	Guidance	Using the results from SCAP.T.3005.1 and SCAP.T.3005.2, the test report SHALL indicate the SCAPVal result and location. The SCAPVal output SHALL be included with the submission.	
		Source Data Stream(s): r3005-datastream-01.xml; r3005-datastream-02.xml; and r3005-datastream-03.xml Artifact(s): - Expected Scan Results: One ARF report for each platform family for the following selected profiles "xccdf_gov.nist.validation_profile_r3005_01", "xccdf_gov.nist.validation_profile_r3005_tailoring_01", "xccdf_gov.nist.validation_profile_r3005_tailoring_02", and "xccdf_gov.nist.validation_profile_r3005_tailoring_03". - SCAPVal output (html and XML).	
	SCAP.T.3005.4	The tester SHALL compare the product results to the expected results ensuring that all the results match the expected results.	
	Guidance	Using the results from SCAP.T.3005.1 and SCAP.T.3005.2, the test report SHALL provide evidence of the comparison between actual results and expected results using the compare.py tool. Any exceptions SHALL be justified.	
		Source Data Stream(s): r3005-datastream-01.xml; r3005-datastream-02.xml; and r3005-datastream-03.xml Artifact(s): - Expected Scan Results: One ARF report for each platform family for the following selected profiles "xccdf_gov.nist.validation_profile_r3005_01", "xccdf_gov.nist.validation_profile_r3005_tailoring_01", "xccdf_gov.nist.validation_profile_r3005_tailoring_02", and "xccdf_gov.nist.validation_profile_r3005_tailoring_03". - compare.py output.	

38.	**SCAP.R.3010**	**The product SHALL be able to select and process XCCDF Benchmark components, which do not include <xccdf:Profile> elements, that are part of an SCAP source data stream and generate XCCDF component results within an SCAP result data stream in accordance with the XCCDF specification for the target platform.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.3010.1	The vendor SHALL provide instructions on how to import XCCDF component content without <xccdf:Profile> elements that is part of SCAP source data streams for execution and provide instructions on where the XCCDF component results can be located for visual inspection. The purpose of this requirement is to ensure that the product produces valid XCCDF Results and the results match the expected results for all given rules.	
	SCAP.T.3010.1	The tester SHALL import a known valid XCCDF component content without <xccdf:Profile> elements that is part of SCAP data streams for the target platform into the vendor product and execute it according to the product operation instructions provided by the vendor. The tester will inspect the product output ensuring XCCDF components are compliant with the XCCDF specification.	
	Guidance	The tester SHALL use the following R3010 source data stream: R3010\r3010-datastream.xml. The test report SHOULD indicate the results inspected by the tester and the platform(s) validated. The test report SHOULD indicate the location of the data stream. The data stream that was imported SHOULD be included in the submission. The test report SHALL provide evidence of the comparison between actual results and expected results using the compare.py tool. Any exceptions SHALL be justified.	
		Source Data Stream(s): r3010-datastream.xml. Artifact(s): - Expected Scan Results: One ARF report for each platform family.	

	SCAP.T.3010.2	The tester SHALL validate the resulting XCCDF component results within an SCAP result data stream output using the SCAPVal utility. This validation MUST NOT produce any validation errors.	
	Guidance	Using the result from SCAP.T.3010.1, the test report SHALL indicate the SCAPVal result and location. The SCAPVal output SHALL be included with the submission.	
		Source Data Stream(s): r3010-datastream.xml. Artifact(s): - Expected Scan Results: One ARF report for each platform family. - SCAPVal output (html and XML).	
	SCAP.T.3010.3	The tester SHALL compare the product results to the expected results ensuring that all the results match the expected results.	
	Guidance	Using the result from SCAP.T.3010.1, the test report SHOULD indicate the name of the data stream. The data stream that was imported SHOULD be included in the submission. The test report SHALL provide evidence of the comparison between actual results and expected results using the compare.py tool. Any exceptions SHALL be justified.	
		Source Data Stream(s): r3010-datastream.xml. Artifact(s): - Expected Scan Results: One ARF report for each platform family. - compare.py output.	
39.	**SCAP.R.3100**	**For all CCE IDs in the SCAP source data stream, the product SHALL correctly display the CCE ID with its associated XCCDF Rule in the product output.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.3100.1	The vendor SHALL provide instructions on where the XCCDF Rules and their associated CCE IDs can be visually inspected within the product output.	

	SCAP.T.3100.1	The tester SHALL visually inspect a non-vendor-directed sample of 10% of the XCCDF Rules, up to a maximum of 30, within the product output and reports to validate that the CCE IDs for each inspected XCCDF Rule match those found in the XCCDF source file.	
	Guidance	Using the scan results produced in SCAP.R.2930, the tester SHALL inspect the sample within the product output to validate that the CCE IDs for each inspected XCCDF Rule match those found in the XCCDF source file. The test report SHOULD provide the list of non-vendor directed sample of XCCDF Rules and associated CCE IDs. If applicable, a list of mis-matches found during testing SHOULD also be reported.	
		Source Data Stream(s): r2930-win-datastream.xml, r2930-rhel-datastream.xml, and r2930-macos-datastream.xml Artifact(s): - Scan results: one ARF report for each platform family. - List of sampled CCE IDs from the ARF report	
40.	**SCAP.R.3200**	**The product output SHALL enable users to view the XML OCIL Questionnaires being consumed by the product (e.g., within the product user interface or through an XML dump of the OCIL questionnaires to a file).**	
	Capability	☐ ACS ☐ CVE ☑ OCIL	
	SCAP.V.3200.1	The vendor SHALL provide instructions on how the user can view the XML OCIL Questionnaires being consumed by the product.	
	SCAP.T.3200.1	The tester SHALL follow the provided vendor instructions to view the XML OCIL Questionnaires being consumed by the product and verify that access is provided as stated.	
	Guidance	This requirement SHALL be validated using the requirements\r2200-datastream.xml content. The test report SHALL provide evidence of the OCIL Questionnaires processed by the product under test.	
		Source Data Stream(s): r2200-datastream.xml Artifact(s): - Expected Scan Results: One ARF report for each platform family.	

		– the arf report request SHALL include the source data stream.
41.	**SCAP.R.3300**	**The product SHALL be able to produce "notchecked" results for unsupported checking systems.** [17]
	Capability	☑ ACS ☐ CVE ☐ OCIL
	SCAP.V.3300.1	The vendor SHALL provide instructions indicating how content for unsupported checking systems is processed.
	SCAP.T.3300.1	The tester SHALL import a valid SCAP source data stream containing a check system unsupported by the vendor product for the target platform into the product and execute the data stream according to the product operation instructions provided by the vendor. The tester SHALL inspect the product output to validate that it includes "notchecked" results for the unsupported checking system.
	Guidance	The r3300-datastream.xml content SHALL be used to validate a check system unsupported by the vendor product for the target platform. This use case demonstrates the ability to successfully process content containing a check system (perhaps OCIL) that MAY not be supported. Rules that are not supported MUST result in "notchecked". The test report SHOULD indicate the name of the data stream. The data stream that was imported SHOULD be included in the submission. The test report SHALL provide evidence of the comparison between actual results and expected results using the compare.py tool. Any exceptions SHALL be justified.
		Source Data Stream(s): r3300-datastream.xml Artifact(s): – Expected Scan Results: One ARF report for each platform family. – SCAPVal output (html and XML). – compare.py output.
42.	**SCAP.R.3400**	**The product output in ARF format SHALL enable**

[17] XCCDF Specification in [Error! Reference source not found.].

Deleted: NISTIR 7275 R4

		users to view the SCAP source data stream collection that was used to generate the results against the target.	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.3400.1	The vendor SHALL provide instructions on how the user can view the ARF report produced by the product which includes the source content consumed by the product.	
	SCAP.T.3400.1	The tester SHALL follow the provided vendor instructions to view the ARF report and verify that the source data stream collection that was used to generate the results was included in the report as an <arf:report-request>.	
	Guidance	The data stream import and compliance scan from SCAP.T.1700.1 and SCAP.T.2910.1 SHALL be used to address this requirement. The test report SHALL indicate the <arf:report-request> element inspected by the tester for a the tested platforms.	
		Source Data Stream(s): Windows-datastream.xml; RHEL-datastream.xml; MacOS-datastream.xml; and r2910-datastream.xml. Artifact(s): - Expected Scan Results: One ARF report for each platform family. - Evidence of the <arf:report-request> element included in the ARF report(s).	
	SCAP.T.3400.2	The tester SHALL import a valid SCAP source data stream with an <xccdf:Tailoring> component and execute the data stream according to the product operation instructions provided by the vendor. The tester SHALL inspect the product output to make sure the tailoring component was included in the ARF report as an <arf:report-request>.	
	Guidance	The tester SHALL use the r3005-datastream-01.xml, r3005-datastream-02.xml, and r3005-datastream-03.xml data streams to validate this requirement. The test report SHALL provide evidence from the product output that the <xccdf:Tailoring> component was included in the ARF report. The ARF reports SHALL be included in the submission.	
		Source Data Stream(s): r3005-datastream-01.xml; r3005-datastream-02.xml; and r3005-datastream-	

		03.xml. Artifact(s): - Expected Scan Results: One ARF report for each platform family. - Evidence of the <arf:report-request> element included in the ARF report(s).	
43.	**SCAP.R.3500**	**For all SCAP source data streams, the product SHALL indicate the date the data was last generated and updated. The generated date is when the data was originally created/officially published. The updated date is the date the product obtained its copy of the data.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.3500.1	The vendor SHALL provide instructions on where the dates for all imported SCAP source data streams can be inspected in the product output.	
	SCAP.T.3500.1	The tester SHALL visually inspect the product output for correctly recorded dates of all SCAP source data streams processed by the vendor product.	
	Guidance	The test report SHALL provide evidence indicating the dates of content processed.	
		Source Data Stream(s): Windows-datastream.xml; RHEL-datastream.xml; MacOS-datastream.xml; and r2910-datastream.xml. Artifact(s): - Expected Scan Results: One ARF report for a platform family. - Evidence of the date the data was last generated and updated from the ARF report(s).	
44.	**SCAP.R.3600**	**The product SHALL display the associated CCE ID for each configuration issue definition in the product output (i.e., the product displays CCE IDs).**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.3600.1	The vendor SHALL provide instructions on how product output can be generated that contains	

		a listing of all security configuration issue items, with associated CCE IDs when available. Instructions SHALL include where the CCE IDs and the associated vendor supplied and/or official CCE descriptions can be located within the product output.	
	SCAP.T.3600.1	The tester SHALL visually inspect, within the product output, a non-vendor-directed set of 30 security configuration issue items, to ensure that the CCE IDs are displayed. This test is not intended to determine whether the product correctly maps to CCE or whether it provides a complete mapping.	
	Guidance	The data stream import and compliance scan from SCAP.T.2930 SHALL be used to visually inspect the 30 security configuration issues within the product output are displayed. The test report SHALL provide evidence indicating the existence of the CCE IDs within the product output. A sample SHALL be provided.	
		Source Data Stream(s): r2930-win-datastream.xml, r2930-rhel-datastream.xml, and r2930-macos-datastream.xml Artifact(s) - Expected Scan Results: One ARF report for each platform family. - Evidence of the CCE IDs included in the ARF report(s).	
45.	**SCAP.R.3800**	**A product's machine-readable output MUST provide the CPE naming data using CPE names.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.3800.1	The vendor SHALL provide procedures and/or a test environment where machine-readable output containing the CPE naming data can be produced and inspected. The vendor SHALL provide a translation tool to create human-readable data for inspection if the provided output is not in a human-readable format (e.g., binary data, encrypted text).	
	SCAP.T.3800.1	The tester SHALL manually inspect the vendor-identified machine-readable output and ensure that CPE naming data is correct according to the CPE specification. The tester will do this by	

		choosing a minimum of 30 vendor and product names in the product output that are also included in the official CPE Dictionary.	
	Guidance	The tester SHALL inspect the vendor-identified machine-readable output from SCAP.T.2940.1 and ensure that CPE naming data is correct. The test report SHALL provide evidence indicating the machine-readable output produced by the vendor product. List of 30 non-vendor directed sample entries reviewed during testing. If applicable, a list of mis-matches found during testing SHALL be reported.	
		Source Data Stream(s): r2940-datastream.xml Artifact(s) - Expected Scan Results: One ARF report for each platform family. - Evidence of the CCE IDs included in the ARF report(s).	
46.	**SCAP.R.3900**	**The product SHALL allow users to locate configuration issue items using CCE IDs.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.3900.1	The vendor SHALL provide documentation (printed or electronic) indicating how configuration issue items can be located using CCE IDs.	
	SCAP.T.3900.1	The tester SHALL verify that configuration issue items can be identified using CCE IDs. The tester SHALL perform this using a non-vendor-directed sample comprised of 10% of the total configuration issue items, up to a maximum of 30.	
	Guidance	The data stream import and compliance scan from SCAP.T.2930.1 SHALL be used to verify the security configuration issue items can be identified using CCE IDs. The test report SHALL indicate existence of the sampled CCE IDs and their associated description within the product output. This SHALL be the entire random sample selected by the lab.	
		Source Data Stream(s): r2930-win-datastream.xml, r2930-rhel-datastream.xml, and r2930-macos-datastream.xml Artifact(s):	

		– Scan results: one ARF report for each platform family. – List of sampled CCE IDs from the ARF report	
47.	**SCAP.R.4000**	**The product SHALL be able to correctly produce the Asset Identification Fields as specified in [Error! Reference source not found.] when assessing a target.**	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.4000.1	The vendor SHALL provide documentation on how to import an SCAP data stream and how to apply it to a target system.	
	SCAP.T.4000.1	The tester SHALL import the SCAP source data stream and apply it to a known target, producing an SCAP result data stream.	
	Guidance	The data stream import and compliance scan from SCAP.T.1700.1 SHALL be used to verify Asset Identification Fields. The test report SHOULD indicate the name of the data stream. The data stream that was imported SHOULD be included in the submission.	
		Source Data Stream(s): Windows-datastream.xml; RHEL-datastream.xml; and MacOS-datastream.xml. Artifact(s): – Expected Scan Results: One ARF report for each platform family. – Evidence of the AI fields included in the ARF report(s).	
	SCAP.T.4000.2	The tester SHALL validate the results produced using SCAPVal; the validation MUST NOT produce any errors.	
	Guidance	The test report SHALL indicate the SCAPVal result and location. The SCAPVal output SHALL be included with the submission.	
		Source Data Stream(s): Windows-datastream.xml; RHEL-datastream.xml; and MacOS-datastream.xml. Artifact(s): – SCAPVal output (html and XML)	

Deleted: NIST SP 800-126 R3

	SCAP.T.4000.3	The tester SHALL visually inspect the results to ensure the Asset Identification Fields are as expected	
	Guidance	The test report SHALL provide evidence indicating the Asset Identification fields are correct. For example, the ai:computing-device hostname property SHOULD match the hostname of the test system.	
		Source Data Stream(s): Windows-datastream.xml; RHEL-datastream.xml; and MacOS-datastream.xml. Artifact(s): - Expected Scan Results: One ARF report for each platform family. - Evidence of the correct AI fields included in the ARF report(s).	
48.	**SCAP.R.4100**	**The product SHALL be able to correctly produce an SCAP result data stream conforming to the ARF specification for each XCCDF, OVAL, and OCIL component.**	
	Capability	☑ ACS ☐ CVE ☑ OCIL	
	SCAP.V.4100.1	The vendor SHALL supply documentation on how to import an SCAP data stream, apply it against a target, and produce an SCAP result data stream conforming to the ARF specification.	
	SCAP.T.4100.1	The tester SHALL import the SCAP 1.3 source data stream, apply it to a known target, and produce an SCAP result data stream conforming to the ARF specification.	
	Guidance	Any SCAP 1.3 Windows,RHEL, and Mac OS data streams such as the consolidated data streams SHALL be used when testing this requirement. The test report SHOULD indicate the name of the data stream. The data stream that was imported SHOULD be included in the submission.	
		Source Data Stream(s): Windows-datastream.xml; RHEL-datastream.xml; and MacOS-datastream.xml. Artifact(s): - Expected Scan Results: One ARF report for each platform family.	

	SCAP.T.4100.2	The tester SHALL validate the results produced using SCAPVal; the validation MUST NOT produce any errors.	
	Guidance	The test report SHALL indicate the SCAPVal result and location. The SCAPVal output SHALL be included with the submission.	
		Source Data Stream(s): Windows-datastream.xml; RHEL-datastream.xml; and MacOS-datastream.xml. Artifact(s): - Expected Scan Results: One ARF report for each platform family. - SCAPVal output (html and XML).	
	SCAP.T.4100.3	The tester SHALL compare the actual results to the expected results ensuring the results match.	
	Guidance	The test report SHALL provide evidence of the comparison between actual results and expected results using the compare.py tool. Any exceptions SHOULD be justified.	
		Source Data Stream(s): Windows-datastream.xml; RHEL-datastream.xml; and MacOS-datastream.xml. Artifact(s): - Expected Scan Results: One ARF report for each platform family. - compare.py output.	
49.	**SCAP.R.4200**	**The product SHALL provide a means to view the CVE Description and CVE references for each displayed CVE ID[18] within the product output.**	
	Capability	☐ ACS ☑ CVE ☐ OCIL	
	SCAP.V.4200.1	The vendor SHALL provide instructions on where the CVE IDs can be located within the product output. The vendor SHALL provide procedures and a test environment (if necessary) so that the product will output vulnerabilities with associated CVE IDs. Instructions SHALL include where the CVE IDs and the associated vendor-supplied and	

[18] This requirement can be met by providing a URL to the NVD CVE or MITRE CVE vulnerability summaries for the CVE IDs in question.

		official CVE descriptions can be located within the product output. It is acceptable to have CVEs in the form of a specific link for each CVE to the NVD.	
	SCAP.T.4200.1	The tester SHALL select a non-vendor-directed sampling of CVE IDs from within the available forms of the product output. The tester SHALL determine that the product output enables the user to view, at minimum, the official CVE description and references.[19] The vendor MAY provide additional CVE descriptions and information. The tester SHALL perform this using a non-vendor-directed sample comprised of greater than or equal to 10 and less than or equal to 30 of the total CVE IDs available in the product output.	
	Guidance	The data stream import and compliance scan from SCAP.T.2920.1 SHALL be used to verify CVE IDs. The test report SHALL provide evidence indicating the existence of the sample CVE IDs within the product output. It is sufficient to provide URLs that link to the NVD, MITRE and/or vendor vulnerability database website. For example, https://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2011-1377 or https://access.redhat.com/security/cve/CVE-2013-0151. The URL SHALL be specific and it is not sufficient to provide a generic URL such as https://web.nvd.nist.gov or https://access.redhat.com/security/updates. This SHALL be the entire random sample selected by the lab.	
		Source Data Stream(s): r2920-datastream.xml Artifact(s) - Expected Scan Results: One ARF report for each platform family. - Evidence of the CVE IDs included in the ARF report(s).	
50.	**SCAP.R.4300**	**For all static or product -bundled CCE data, the product SHALL indicate the date the data was last**	

[19] The official CVE description and references are found at https://nvd.nist.gov/.

		generated and updated. The generated date is when the data was originally created/officially published. The updated date is the date the product obtained its copy of the data.	
	Capability	☑ ACS ☐ CVE ☐ OCIL	
	SCAP.V.4300.1	The vendor SHALL provide instructions on where the dates for all offline CCE data can be inspected in the product output.	
	SCAP.T.4300.1	The tester SHALL visually inspect the product output for the dates of all static or bundled CCE data included with the vendor product.	
	Guidance	The test report SHALL provide evidence indicating the date.	
51.	**SCAP.R.4400**	**The product SHALL include the CVE ID(s) associated with each software flaw and/or patch definition in the product output (i.e., the product displays CVE IDs) where appropriate.[20]**	
	Capability	☐ ACS ☑ CVE ☐ OCIL	
	SCAP.V.4400.1	The vendor SHALL provide instructions, and a test environment (if necessary), indicating how product output can be generated that contains a listing of all software flaws and patches with associated CVE IDs when available. CVE IDs SHOULD be used wherever possible. Instructions SHALL include where the CVE IDs and the associated vendor-supplied and/or official CVE descriptions can be located within the product output.	
	SCAP.T.4400.1	The tester SHALL visually inspect, within the product output, a non-vendor-selected sample comprised of greater than or equal to 10 and less than or equal to 30 of the total CVE IDs available in the product output to ensure that the CVE IDs are displayed. This test is not intended to determine whether the product correctly maps to CVE or whether it provides a complete mapping.	
	Guidance	The data stream import and compliance scan from SCAP.R.2920 SHALL be used to verify CVE IDs.	

[20] In the case where the content being processed only requires results that do not contain CVE references this requirement does not apply.

		The test report SHALL provide evidence indicating the existence of the non-vendor directed sample of CVE IDs within the product output. This SHALL be the entire random sample selected by the lab.	
		Source Data Stream(s): r2920-datastream.xml Artifact(s) - Expected Scan Results: One ARF report for each platform family. - Evidence of the CVE IDs included in the ARF report(s).	
52.	**SCAP.R.4500**	**If the product uses CVE, it SHALL include NVD CVSS base scores and vector strings for each CVE ID referenced in the product.**	
	Capability	☐ ACS ☑ CVE ☐ OCIL	
	SCAP.V.4500.1	The vendor SHALL provide documentation explaining where the NVD CVSS base scores and vector strings can be located with the corresponding CVE ID.[21] The vendor MAY provide information about how the product can be updated with new NVD CVSS base scores and vector strings prior to testing.	
	SCAP.T.4500.1	The tester SHALL update the product's NVD base scores and vectors (using the vendor-provided update capability if it exists) and validate that the product displays the NVD CVSS base scores and vectors for 15 non-vendor-directed CVE IDs referenced in the product. The CVEs chosen MUST have an NVD vulnerability summary "last revision" date that is at least 30 days old. A link to the information on the NVD web site is sufficient for this test.	
	Guidance	Screenshot or other representation of product output explaining where NVD CVSS base scores and vectors can be viewed within the product output MAY be used to verify compliance, but the output from SCAP.T.2920.1 is the preferred test method to be used for this test.	
		Source Data Stream(s): r2920-datastream.xml Artifact(s) - Expected Scan Results: One ARF report for each platform family. - Evidence of the CVE IDs included in the ARF report(s).	

[21] A link to the specific CVE entry on the NVD web site is sufficient for this test.
