Publication Number: **NIST Internal Report (NISTIR) 7511 Revision 4**

Title: **Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements**

Publication Date: **1/28/2016**

- Final Publication: http://dx.doi.org/10.6028/NIST.IR.7511r4 (which links to http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7511r4.pdf).
- Related Information on CSRC:
  http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7511-Rev.%204
  and
  http://scap.nist.gov/validation/
- Information on other NIST cybersecurity publications and programs can be found at: http://csrc.nist.gov/

The following information was posted with the attached DRAFT document:

Sep. 18, 2015

NIST IR 7511 Rev. 4

DRAFT Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements

NIST requests comments on a revision of Interagency Report (IR) 7511 Revision 4, *Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements*. This document defines the test requirements that products must satisfy in order to be awarded SCAP 1.2 validation. A list of changes is provided in the Summary of Changes section of the document. Please send comments to ir7511comments @nist.gov by **October 15, 2015** with "Comments on IR 7511 Rev 4" in the subject line.

DRAFT NISTIR 7511
Revision 4

Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements

Melanie Cook
Stephen Quinn
David Waltermire
Dragos Prisaca

http://dx.doi.org/10.6028/NIST.IR.xxxx

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

DRAFT NISTIR 7511
Revision 4

Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements

Melanie Cook
Stephen Quinn
David Waltermire
Computer Security Division
Information Technology Laboratory

Dragos Prisaca
G2, Inc.

http://dx.doi.org/10.6028/NIST.IR.xxxx

September 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Internal Report 7511 Revision 4
45 pages (September 2015)

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.XXXX

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: *September 18, 2015* through *October 15 2015*

All comments are subject to release under the Freedom of Information Act (FOIA).

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930), Gaithersburg, MD 20899-8930
Electronic mail: ir7511comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

This report defines the requirements and associated test procedures necessary for products or modules to achieve one or more Security Content Automation Protocol (SCAP) validations. Validation is awarded based on a defined set of SCAP capabilities by independent laboratories that have been accredited for SCAP testing by the NIST National Voluntary Laboratory Accreditation Program (NVLAP).

Keywords

Security Content Automation Protocol (SCAP); SCAP derived test requirements (DTR); SCAP validated tools; SCAP validated products; SCAP validated modules; SCAP validation

Acknowledgements

The authors, Melanie Cook, Stephen Quinn, and David Waltermire of the National Institute of Standards and Technology (NIST), and Dragos Prisaca of G2, Inc. would like to thank the many people who reviewed and contributed to this document, in particular, John Banghart of Microsoft who was the original author and pioneered the first SCAP Validation Program. The authors thank Matt Kerr, Danny Haynes of the MITRE Corporation, Andrew Bove of Secure Acuity, and Lon Kight for their insightful technical contribution to the design of the SCAP 1.2 Validation Program and creation of validation test content. We also thank our document reviewers, Michael Cooper of NIST and Karen Scarfone of Scarfone Cybersecurity for their invaluable input.

Audience

This publication is intended for NVLAP accredited laboratories conducting SCAP product and module testing for the program, vendors interested in receiving SCAP validation for their products or modules, and organizations deploying SCAP products in their environments. Accredited laboratories use the information in this report to guide their testing and ensure all necessary requirements are met by a product before recommending to NIST that the product be awarded the requested validation. Vendors may use the information in this report to understand the features that products and modules need in order to be eligible for an SCAP validation. Government agencies and integrators use the information to gain insight into the criteria required for SCAP validated products. The secondary audience for this publication includes end users, who can review the test requirements in order to understand the capabilities of SCAP validated products and gain knowledge about SCAP validation.

Trademark Information

OVAL and CVE are registered trademarks, and CCE, CPE, and OCIL are trademarks, of The MITRE Corporation.

Red Hat is a registered trademark of Red Hat, Inc.

Windows operating system is registered trademark of Microsoft Corporation.

All other registered trademarks or trademarks belong to their respective organizations.

Summary of Changes

The following table details the changes between NISTIR 7511 Revision 3 and NISTIR 7511 Revision 4, which are incorporated in the present document.

Date	Type	Change	Page Number
6/26/2015	Editorial	Changed the revision from “3” to “4”	cover page, i, ii
	Editorial	Added new author: “Dragos Prisaca”	cover page, i
	Editorial	Changed secretary name to “Penny Pritzker, Secretary”	i
	Editorial	Changed the date of the document	i
	Substantive	Changed abstract from “This report defines the requirements and associated test procedures necessary for products to achieve one or more Security Content Automation Protocol (SCAP) validations.” to ‘This report defines the requirements and associated test procedures necessary for products or modules to achieve one or more Security Content Automation Protocol (SCAP) validations.”	iii
	Editorial	Added keywords “SCAP validated products; SCAP validated modules”	iii
	Editorial	Updated the Acknowledgements section	iv
	Substantive	Changed “SCAP Product” to “SCAP product and module” in the Audience section	iv
	Substantive	Changed the Trademark Information section from “Windows XP, Windows Vista, and Windows 7 are registered trademarks of Microsoft Corporation.” to “Windows® operating system is registered trademark of Microsoft Corporation.”	iv
	Substantive	Changed “3.3 Tools” to “3.3 Validation Tools” in the Table of Contents	viii
	Substantive	Changed “3.3.1 SCAP Validation Tool” to “3.3.1 SCAP Validation Tool (SCAPVal)” in the Table of Contents	viii
	Substantive	Added “7. Appendix C— Use of SCAP 1.2 Logo and phrases” to the Table of Contents	viii
	Substantive	Added SCAP Product and Module definitions in the Introduction section	1
	Substantive	Added information about the XML conventions to the section 1.3 Document Conventions	2
	Substantive	Added IR7511 revisions 1, 2, and 3 to the section 1.4 Superseded Validation Programs	4
	Substantive	Added new URL “http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61713” for the XCCDF 1.2 specification in the section 2.1 Extensible Configuration Checklist Document Format (XCCDF)	6
	Substantive	Replaced “Vendor products may seek validation for SCAP 1.2 capabilities for Windows and/or Red Hat platforms. One core SCAP 1.2 capability and two optional capabilities are offered.” with “Vendor of products may seek validation for one core and two	10

Date	Type	Change	Page Number
		optional SCAP 1.2 capabilities on one or more platform such as those listed below.” in section 3.1 SCAP 1.2 Capabilities and Validations	
	Substantive	Added table with supported platforms in section 3.1 SCAP 1.2 Capabilities and Validations, SCAP Module minor versions are validated	10
	Substantive	Removed the old platforms listed in section 3.1 SCAP 1.2 Capabilities and Validations.	9
	Substantive	Added clarification about supporting new platforms “The SCAP Validation Program may add support for new platforms which will be listed on the SCAP Validation Program web page. For the most current list of available platforms, please refer to http://scap.nist.gov/validation.” to section 3.1 SCAP 1.2 Capabilities and Validations	11
	Editorial	Replaced “Product” with “Product/Module” in section 3.1 SCAP 1.2 Capabilities and Validations	11
	Editorial	Changed the example used in section 3.2 Demarcation and Validation Expirations to use future dates.	11
	Editorial	Replaced section name “3.3 Tools” with “3.3Validation Tools”	12
	Editorial	Replaced section name “3.3.1 SCAP Validation Tool” with “3.3.1 SCAP Validation Tool (SCAPVal)”	12
	Substantive	Added “Use of reference implementation tools is not required by the SCAP Validation Program.” to section 3.3.2 Reference Implementation Tools	12
	Substantive	Added the <Profile> element to the list XCCDF elements referenced in SCAP.R.1200	18
	Editorial	Replaced “tool” with “product” in SCAP.T.1200.1 and SCAP.T.1200.2	18
	Substantive	Replaced “the Tier IV” with “USGCB” in SCAP.R.1500	19
	Substantive	Added footnote 14 for SCAP.R.1500	19
	Substantive	Replaced “SCAP.V.1500.1: The vendor SHALL provide instructions on how to execute the previously imported valid Tier IV SCAP source data streams.” with “SCAP.V.1500.1: The vendor SHALL provide instructions on how to import and execute valid SCAPUSGCB source data streams.”	20
	Editorial	Corrected typo in footnote 12	17
	Substantive	Added SCAP.V.1500.2	20
	Substantive	Changed the instructions for the section Required Test Procedures of SCAP.R.1500	20
	Substantive	Added “All the applicable USGCB source data streams published in the official National Checklist Program Repository should be used for testing this requirement: http://checklists.nist.gov.” in section “Required Test Procedures” of SCAP.R.1500.	20
	Substantive	Removed Tier IV source data streams listed in the section Required Test Procedures of SCAP.R.1500	20

Date	Type	Change	Page Number
	Substantive	Changed "SCAP.T.1500.1: The tester SHALL evaluate the compliant target platforms, in a domain connected configuration for Windows and standalone configuration for Red Hat, and compare the pass/fail results from the product to the expected results, ensuring the actual results match the expected results." to "SCAP.T.1500.1: The lab or the vendor SHALL evaluate the compliant target platforms, in a domain connected configuration for Windows and standalone configuration for other platforms (i.e., RHEL, Mac OS X, Unix, etc.), and compare the pass/fail results from the product to the expected results, ensuring the actual results match the expected results. If the testing is performed by the vendor, the source data streams, the scan results, and their hashes will be submitted to the lab for verification."	20
	Substantive	Added footnote 15: "The hashes SHALL comply with Annex A: Approved Security Functions of FIPS 140-2 publication."	20
	Substantive	Added SCAP.T.1500.2	20
	Substantive	Added new requirement SCAP.R.1510	20
	Substantive	Changed "Tier IV content" to "USGCB checklist" for SCAP.R.1600	21
	Substantive	Replaced "SCAP.R.1700: The product SHALL be able to process the content that is representative of content published at Tier III and the OVAL repository which is associated with the platforms for which validation is being sought." with "SCAP.R.1700: The product SHALL be able to correctly process the content that is representative of content published at Tier III, Tier IV, and the OVAL repository16 which is associated with the platforms for which validation is being sought."	21
	Substantive	Added footnote 17: "The OVAL repository is hosted by MITRE Corporation: https://oval.mitre.org/repository/"	21
	Substantive	Changed "XCCDF <Benchmark>, <Group>, or <Rule>" to "XCCDF <Benchmark>, <Profile>, <Group>, or <Rule>" in SCAP.R.1800.	22
	Editorial	Changed "tool" to "product" in SCAP.T.1800.1.	22
	Substantive	Changed "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 specified in NIST SP 800-126 Revision 1, against target systems of the target platform type and produce a result file for each definition using the OVAL XML Full Results expressed as Single Machine Without System Characteristics, Single Machine With System Characteristics, or Single Machine With Thin Results." to "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 specified in NIST SP 800-126 Revision 1, against target systems of the target platform type and produce a result file for each definition using the OVAL XML Full Results expressed as Single Machine Without System	22

Date	Type	Change	Page Number
		Characteristics, Single Machine With System Characteristics, and Single Machine With Thin Results.” in SCAP.R.1900.	
	Editorial	Changed “tool” to “product” in SCAP.T.1900.1.	22
	Substantive	Changed “SCAP.R.2000: The product SHALL be able to correctly evaluate a valid OVAL Definition file that is part of an SCAP data stream, where the contents of the OVAL definition file are consistent with the normative guidance specified in NIST SP 800-126 Revision 2, against target systems of the target platform type and produce a result file for each definition using the OVAL XML Full Results expressed as Single Machine Without System Characteristics, Single Machine With System Characteristics, or Single Machine With Thin Results. ” to “SCAP.R.2000: The product SHALL be able to correctly evaluate a valid OVAL Definition file that is part of an SCAP data stream, where the contents of the OVAL definition file are consistent with the normative guidance specified in NIST SP 800-126 Revision 2, against target systems of the target platform type and produce a result file 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.” In SCAP.R.2000.	23
	Substantive	Removed “For SCAP.T.2000.5, the vendor SHALL indicate how two or more values can be specified for a variable used by one OVAL Definition.” from section Required Vendor Information - SCAP.V.2000.1.	23
	Editorial	Changed “tool” to “product” in SCAP.T.2000.1.	23
	Substantive	Removed “SCAP.T.2000.5: When an OVAL Definition has been evaluated more than once on a single target system, each time with different values for the variables, the tester SHALL validate that the OVAL XML Full Results file includes unique variable instance values for each individual case.”	23
	Editorial	Changed “tool” to “product” in SCAP.T.2100.1.	24
	Editorial	Changed “tool” to “product” in SCAP.T.2200.1.	24
	Substantive	Changed “SCAP.R.3600” to “SCAP.R.2930” in SCAP.T.2300.1.	24
	Substantive	Changed “SCAP.R.3600” to “SCAP.R.2930” in SCAP.T.2400.1.	24
	Editorial	Changed “tool” to “product” in SCAP.T.2600.1.	26
	Substantive	Changed “SCAP.R.4400” to “SCAP.R.2920” in SCAP.T.2700.1.	26
	Substantive	Removed “and/or patch definitions” and changed “SCAP.R.4400” to “SCAP.R.2920” in SCAP.T.2800.1.	27
	Substantive	Added new requirement SCAP.R.2910	27
	Substantive	Added new requirement SCAP.R.2920	28
	Substantive	Added new requirement SCAP.R.2930	28
	Substantive	Added new requirement SCAP.R.2940	28
	Editorial	Changed “tool” to “product” in SCAP.T.3000.1.	29
	Substantive	Added new requirement SCAP.R.3005	28

Date	Type	Change	Page Number
	Substantive	Added new requirement SCAP.R.3010	29
	Editorial	Changed “tool” to “product” in SCAP.T.3200	30
	Editorial	Changed “tool” to “product” in SCAP.T.3300.1.	31
	Editorial	Changed “tool” to “product” in SCAP.T.3400	31
	Editorial	Changed “tool” to “product” in section 5. Derived Test Requirements for Specific Capabilities	36
		Added the following entries to Table 5-1. Required SCAP Components for Each SCAP Capability: SCAP.R.1510, SCAP.R.2910, SCAP.R.2920, SCAP.R.2930, SCAP.R.2940, and SCAP.R.3010	36/37
	Substantive	Changed “Table 5-2 lists the OVAL tests used for testing the ACS SCAP 1.2 capability.” to “The list of OVAL tests used for testing the ACS SCAP 1.2 capability is published on the SCAP Validation Program web page http://scap.nist.gov/validation.” in section 5. Derived Test Requirements for Specific Capabilities	38
	Editorial	Removed Table 5.2 OVAL Tests	38
	Editorial	Changed “tool” to “product” in Appendix A.	39
	Editorial	Added SCAP Module definition in Appendix A.	40
	Editorial	Removed definition for Reference Product in Appendix A.	40
	Editorial	Added Appendix C	43

157

Table of Contents

1. Introduction 1

1.1 Purpose and Scope 2
1.2 Document Structure 2
1.3 Document Conventions 2
1.4 Superseded Validation Programs 3

2. SCAP 1.2 Component Specification Versions 4

2.1 Extensible Configuration Checklist Document Format (XCCDF) 5
2.2 Open Vulnerability and Assessment Language (OVAL) 5
2.3 Open Checklist Interactive Language (OCIL) 5
2.4 Common Configuration Enumeration (CCE) 5
2.5 Common Platform Enumeration (CPE) 6
2.5.1 CPE.Naming 6
2.5.2 CPE.Name Matching 6
2.5.3 CPE.Dictionary 6
2.5.4 CPE.Applicability Language 7
2.6 Common Vulnerabilities and Exposures (CVE) 7
2.7 Common Vulnerability Scoring System (CVSS) 7
2.8 Common Configuration Scoring System (CCSS) 7
2.9 Asset Identification 7
2.10 Asset Reporting Format (ARF) 8
2.11 Trust Model for Security Automation Data (TMSAD) 8

3. Validation Process 9

3.1 SCAP 1.2 Capabilities and Validations 9
3.2 Demarcation and Validation Expirations 10
3.3 Validation Tools 11
3.3.1 SCAP Validation Tool 11
3.3.2 Reference Implementation Tools 11

4. Derived Test Requirements 13

4.1 SCAP Assertions 14
4.2 SCAP Source Data Stream Processing and Correctness 15
4.3 SCAP Result(s) Data Stream 26

5. Derived Test Requirements for Specific Capabilities 36

Appendix A—Terms and Definitions 39

Appendix B—Acronyms 42

Appendix C—Use of SCAP 1.2 Logo and phrases 43

Appendix D—References 44

1. Introduction

The National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP) Validation Program tests the ability of products and modules to use the features and functionality available through SCAP and its components. SCAP 1.2 consists of a suite of specifications for standardizing the format and nomenclature by which security software communicates information about software flaws and security configurations. The standardization of security information facilitates interoperability and enables predictable results among disparate SCAP enabled security software. The SCAP Validation Program provides vendors an opportunity to have independent verification that security software correctly processes SCAP expressed security information and provides standardized output. Industry and government end users benefit from the SCAP Validation Program by having assurance that SCAP validated products have undergone independent testing and met all requirements defined in this document.

The validation program supports the U.S. Office of Management and Budget (OMB) Memorandum M-08-22 to Federal CIOs [OMB M-08-22]. This memorandum states, "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. Agencies will use SCAP tools to scan for both FDCC configurations and configuration deviations approved by department or agency accrediting authority. Agencies must also use these tools when monitoring use of these configurations as part of FISMA continuous monitoring."[1] The checklist portion of the FDCC mandate is now referred to as the United States Government Configuration Baseline (USGCB), and the FDCC Scanner capability has evolved and is now referred to as the Authenticated Configuration Scanner (ACS) capability.[2]

Under the SCAP Validation Program, independent laboratories are accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP). Accreditation requirements are defined in NIST Handbook 150, *National Voluntary Laboratory Accreditation Program: Procedures and General Requirements* [NIST HB 150] and NIST Handbook 150-17, *NVLAP Cryptographic and Security Testing* [NIST HB 150-17]. More information about NVLAP can be found at http://www.nist.gov/nvlap/.

Independent laboratories conduct the tests defined in this document on products and deliver the results to NIST. Based on the independent laboratory test report, the SCAP Validation Program then validates the product under test. The validation certificates awarded to vendor's products are publicly posted on the NIST SCAP Validated Products web page (http://nvd.nist.gov/scapproducts.cfm).[3] An information technology (IT) vendor can obtain one or more validations for a product. These validations are based on the test requirements defined in this document. Products are validated in the context of a particular SCAP capability.[4]

An SCAP product is defined as a software application that has one or more capabilities and an SCAP module is defined as an embedded software component of a product or application, or a complete product in-and-of-itself that has one or more capabilities. Unless otherwise stated herein, the term "product" refers to either a "product" or "module" under test.

[1] [OMB M-08-22, p.2]

[2] http://usgcb.nist.gov

[3] The SCAP Validation Program does not provide physical certificates to the participating vendors.

[4] The SCAP Validation Program defines SCAP capability as "a specific function or functions of a product or module". Further information can be found in Section 3.

1.1 Purpose and Scope

The purpose of this report is to define the SCAP 1.2 Validation Program Derived Test Requirements. This report gives an introduction to the SCAP 1.2 Validation Program and documents the requirements for SCAP 1.2 product and module validations. Future versions of the SCAP Validation Program will be defined in revisions of this report, each clearly labeled with a revision number and the appropriate SCAP version number.

1.2 Document Structure

The remainder of this document is organized into the following major sections:

- Section 2 describes SCAP and its component specification versions referenced in the SCAP 1.2 validation program,
- Section 3 describes the validation process,
- Section 4 defines the derived test requirements,
- Section 5 maps the derived test requirements to SCAP capabilities,
- Appendix A—Terms and Definitions lists terms and definitions,
- Appendix B—Acronyms lists acronyms,
- Appendix C—Use of SCAP 1.2 Logo and phrases discusses the use of the SCAP 1.2 logo and phrases, and
- Appendix D—References includes a list of references.

1.3 Document Conventions

Throughout this document, the key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 2119 [RFC 2119].

Some of the requirements and conventions used in this document reference Extensible Markup Language (XML) content [XMLS]. These references come in two forms, inline and indented. An example of an inline reference is: a `<cpe2_dict:cpe-item>` may contain `<cpe2_dict:check>` elements that reference OVAL Definitions.

In this example the notation `<cpe2_dict:cpe-item>` can be replaced by the more verbose equivalent “the XML element whose qualified name is `cpe2_dict:cpe-item`”.

An example of an indented reference is:

> References to OVAL Definitions are expressed using the following format:
>
> `<cpe2_dict:check system=`
> `"http://oval.mitre.org/XMLSchema/oval-definitions-5"`
> `href="`*Oval_URL*`">[`*Oval_inventory_definition_id*`]`
> `</cpe2_dict:check>`.

The general convention used when describing XML attributes within this document is to reference the attribute as well as its associated element including the namespace alias, employing the general form *`"@attributeName`* for the *`<prefix:localName>"`*.

Indented references are intended to represent the form of actual XML content. Indented references represent literal content by the use of a `fixed-length font`, and parametric (freely replaceable) content by the use of an *italic font*. Square brackets '[]' are used to designate optional content. Thus "[*Oval_inventory_definition_id*]" designates optional parametric content.

Both inline and indented forms use qualified names to refer to specific XML elements. A qualified name associates a named element with a namespace. The namespace identifies the XML model, and the XML schema is a definition and implementation of that model. A qualified name declares this schema to element association using the format '*prefix*:*element-name*'. The association of prefix to namespace is defined in the metadata of an XML document and varies from document to document. In this specification, the conventional mappings listed in Table 1-1.-1 are used.

Table 1-1. Conventional XML Mappings[5]

Prefix	Namespace	Schema
cpe2	http://cpe.mitre.org/language/2.0	Embedded CPE references
cpe2-dict	http://cpe.mitre.org/dictionary/2.0	CPE dictionaries
xccdf	http://checklists.nist.gov/xccdf/1.2	XCCDF policy documents
xml	http://www.w3.org/XML/1998/namespace	Common XML attributes

1.4 Superseded Validation Programs

This publication supersedes the draft *Security Content Automation Protocol (SCAP) Validation Program Test Requirements Version 1.0* released in August 2008, the *Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements* released in April 2009, the *Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements* released in September 2010, the *Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements Update* released in January 2011, and the *Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements* revisions 1, 2, and 3.

[5] For a complete list of mappings, please refer to [NIST SP 800-126 R2].

2. SCAP 1.2 Component Specification Versions

For all test requirements that reference particular specifications, the versions indicated in this section SHOULD be used and are derived primarily from the SCAP 1.2 as defined in NIST Special Publication (SP) 800-126 Revision 2 [NIST SP 800-126 R2].

SCAP is a suite of specifications established by NIST for expressing and manipulating security data in standardized ways. Adoption of SCAP facilitates an organization's automation of continuous monitoring, vulnerability management, and security policy compliance evaluation reporting.

The component specifications that comprise SCAP 1.2 are as follows:

- Extensible Configuration Checklist Description Format (XCCDF) 1.2, an Extensible Markup Language (XML) specification for structured collections of security configuration rules used by operating system (OS) and application platforms;
- Open Vulnerability and Assessment Language (OVAL) 5.10.1, an XML specification for exchanging technical details on how to check systems for security-related software flaws, configuration issues, and software patches;
- Open Checklist Interactive Language (OCIL) 2.0, a language for representing checks that collect information from people or from existing data stores made by other data collection efforts;
- Common Configuration Enumeration (CCE) 5, a dictionary of names for software security configuration issues (e.g., access control settings, password policy settings);
- Common Platform Enumeration (CPE) 2.3, a naming convention for hardware, OS, and application products;
- Common Vulnerabilities and Exposures (CVE), a dictionary of names for publicly known security-related software flaws;
- Common Vulnerability Scoring System (CVSS) 2.0, a method for classifying characteristics of software flaws and assigning severity scores based on these characteristics;
- Common Configuration Scoring System (CCSS) 1.0, a system for measuring the relative severity of system security configuration issues;
- Asset Identification 1.1, a format for uniquely identifying assets based on known identifiers and/or known information about the assets;
- Asset Reporting Format (ARF) 1.1, a format for expressing the transport format of information about assets and the relationships between assets and reports; and
- Trust Model for Security Automation Data (TMSAD) 1.0, a specification for using digital signatures in a common trust model applied to other security automation specifications.

The SCAP specification describes the SCAP components at a high level and how the components relate to each other within the context of SCAP. The SCAP specification does not define the SCAP components in detail; each component has its own standalone specification document or reference. The SCAP components were created and are maintained by several entities, including NIST, the MITRE Corporation, the National Security Agency (NSA), and the Forum of Incident Response and Security Teams (FIRST).

NIST provides SCAP content, such as vulnerability and product enumeration identifiers, through a repository supplied by the National Vulnerability Database (NVD).[6] All of the content in NVD and the SCAP specification are freely available from NIST. SCAP content is also created and made available by non-U.S. government organizations through the National Checklist Program (NCP).[7] More information about SCAP can be found at http://scap.nist.gov/.

2.1 Extensible Configuration Checklist Document Format (XCCDF)

Definition: XCCDF is an XML-based language for representing security checklists, benchmarks, and related documents in a machine-readable form. An XCCDF document represents a structured collection of security configuration rules for one or more applications and/or systems. The XCCDF specification also defines a data model and format for storing the results of benchmark compliance testing.

Version: 1.2

Specification: http://csrc.nist.gov/publications/nistir/ir7275-rev4/NISTIR-7275r4.pdf [NISTIR 7275 R4]
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61713

Schema Location: http://scap.nist.gov/schema/xccdf/1.2/xccdf_1.2.xsd

2.2 Open Vulnerability and Assessment Language (OVAL)

Definition: OVAL is an XML-based language used for communicating the details of vulnerabilities, patches, security configuration settings, and other machine states in a machine-readable form. There is also the OVAL Power Shell Extension, a method for examining the configuration of Microsoft products.

Version: 5.10.1

Specification: http://oval.mitre.org/

Schema Location: http://oval.mitre.org/language/download/schema/version5.10/index.html

2.3 Open Checklist Interactive Language (OCIL)

Definition: OCIL defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions.

Version: 2.0

Specification: http://csrc.nist.gov/publications/nistir/ir7692/nistir-7692.pdf [NISTIR 7692]

Schema Location: http://scap.nist.gov/schema/ocil/2.0/ocil-2.0.xsd

2.4 Common Configuration Enumeration (CCE)

Definition: CCE is a format for describing system configuration issues to facilitate correlation of configuration data across multiple information sources and tools.

Version: 5

[6] http://nvd.nist.gov

[7] http://checklists.nist.gov

Specification: http://cce.mitre.org/

Dictionary: http://cce.mitre.org/lists/cce_list.html

2.5 Common Platform Enumeration (CPE)

Definition: CPE is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets. CPE 2.3 is defined through a set of specifications in a stack-based model.

2.5.1 CPE.Naming

Definition: The Naming specification defines the logical structure of Well-Formed Names (WFNs).

Version: 2.3

Specification: http://csrc.nist.gov/publications/nistir/ir7695/NISTIR-7695-CPE-Naming.pdf [NISTIR 7695]

Schema Location: http://scap.nist.gov/schema/cpe/2.3/cpe-naming_2.3.xsd

2.5.2 CPE.Name Matching

Definition: The Name Matching specification defines the procedures for comparing WFNs to each other with the purpose of determining whether they refer to some or all of the same products.

Version: 2.3

Specification: http://csrc.nist.gov/publications/nistir/ir7696/NISTIR-7696-CPE-Matching.pdf [NISTIR 7696]

2.5.3 CPE.Dictionary

Definition: The Dictionary specification defines the concept of a CPE dictionary, which is a repository of CPE names and metadata, with each name identifying a single class of IT product. The Dictionary specification defines processes for using the dictionary, such as how to search for a particular CPE name or look for dictionary entries that belong to a broader product class. Also, the Dictionary specification outlines all the rules that dictionary maintainers MUST follow when creating new dictionary entries and updating existing entries.

Version: 2.3

Specification: http://csrc.nist.gov/publications/nistir/ir7697/NISTIR-7697-CPE-Dictionary.pdf [NISTIR 7697]

Schema Locations: http://scap.nist.gov/schema/cpe/2.3/cpe-dictionary_2.3.xsd
http://scap.nist.gov/schema/cpe/2.3/cpe-dictionary-extension_2.3.xsd

2.5.4 CPE.Applicability Language

Definition: The Applicability Language specification defines a standardized structure for forming complex logical expressions out of WFNs. These expressions, also known as applicability statements, are used to tag checklists, policies, guidance, and other documents with information about the product(s) to which the documents apply.

Version: 2.3

Specification: http://csrc.nist.gov/publications/nistir/ir7698/NISTIR-7698-CPE-Language.pdf [NISTIR 7698]

Schema Location: http://scap.nist.gov/schema/cpe/2.3/cpe-language_2.3.xsd

2.6 Common Vulnerabilities and Exposures (CVE)

Definition: CVE is a format to describe publicly known information security vulnerabilities and exposures. Using this format, new CVE IDs will be created, assigned, and referenced in content on an as-needed basis without a version change.

Version: N/A

Specification: http://cve.mitre.org/

Dictionary: http://nvd.nist.gov/

2.7 Common Vulnerability Scoring System (CVSS)

Definition: CVSS is a scoring system that provides an open framework for determining the relative severity of software flaw vulnerabilities and a standardized format for communicating vulnerability characteristics.

Version: 2.0

Specification: http://csrc.nist.gov/publications/nistir/ir7435/NISTIR-7435.pdf [NISTIR 7435]

CVSS Base Scores: http://nvd.nist.gov/

2.8 Common Configuration Scoring System (CCSS)

Definition: CCSS is a set of measures of the severity of software security configuration issues.

Version: 1.0

Specification: http://csrc.nist.gov/publications/nistir/ir7502/nistir-7502_CCSS.pdf [NISTIR 7502]

2.9 Asset Identification

Definition: The Asset Identification specification provides the necessary constructs to uniquely identify assets based on known identifiers and/or known information about the assets. This specification describes the purpose of asset identification, a data model for identifying assets, methods for identifying assets, and guidance on how to use asset identification. It also identifies a number of known use cases for asset identification.

Version: 1.1

Specification: http://csrc.nist.gov/publications/nistir/ir7693/NISTIR-7693.pdf [NISTIR 7693]

Schema Location: http://scap.nist.gov/schema/asset-identification/1.1/asset-identification_1.1.0.xsd

2.10 Asset Reporting Format (ARF)

Definition: ARF is a data model to express the transport format of information about assets, and the relationships between assets and reports. The standardized data model facilitates the reporting, correlating, and fusing of asset information throughout and between organizations.

Version: 1.1

Specification: http://csrc.nist.gov/publications/nistir/ir7694/NISTIR-7694.pdf [NISTIR 7694]

Schema Location: http://scap.nist.gov/schema/asset-reporting-format/1.1/asset-reporting-format_1.1.0-rc1.xsd

2.11 Trust Model for Security Automation Data (TMSAD)

Definition: TMSAD is a data model for establishing trust for security automation data.

Version: 1.0

Specification: http://csrc.nist.gov/publications/nistir/ir7802/NISTIR-7802.pdf [NISTIR 7802]

Schema Location: http://scap.nist.gov/schema/tmsad/1.0/tmsad_1.0.xsd

3. Validation Process

With the SCAP Validation Program, SCAP accredited laboratories conduct the tests defined in this document on products and deliver the test report to NIST. NIST reviews the test report and determines whether the product has successfully fulfilled all requirements for SCAP validation. Upon successful completion of all requirements, the SCAP Validation Program then validates the product based on the independent laboratory test report. SCAP validated products and modules are publicly posted on the NIST SCAP Validated Products web page at http://nvd.nist.gov/scapproducts.cfm.

This section of the document covers the validation process. Section 3.1 discusses SCAP 1.2 capabilities and validations. Section 3.2 addresses demarcation and validation expirations. Finally, Section 3.3 discusses reference implementation tools.

3.1 SCAP 1.2 Capabilities and Validations

Vendor products may seek validation for one core and two optional SCAP 1.2 capabilities on one or more platform such as those listed below.

SCAP Capabilities

- Authenticated Configuration Scanner (ACS) core SCAP 1.2 capability
    - CVE option (optional CVE support may be combined with ACS)
    - OCIL option (optional OCIL support may be combined with ACS)

NOTE: The ACS capability includes the FDCC Scanner functionality that is mentioned in Office of Management and Budget (OMB) memorandum M-08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)* [OMB M-08-22] and the USGCB Scanner previously offered in the SCAP 1.0 validation program.

Platforms

Microsoft Windows
Microsoft Windows XP Professional with Service Pack 3
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
Red Hat Enterprise Linux
Red Hat Enterprise Linux 5, 32-bit edition
Red Hat Enterprise Linux 5, 64-bit edition
Red Hat Enterprise Linux 6, 32-bit edition
Red Hat Enterprise Linux 6, 64-bit edition

The SCAP Validation Program is not inherently limited to the platforms listed above and NIST reserves the right to add or remove platforms in future updates to the SCAP 1.2 Validation Program. The SCAP Validation Program may add support for new platforms which will be listed on the SCAP Validation Program web page. For the most current list of available platforms, please refer to http://scap.nist.gov/validation.

Validations will be awarded to major product versions for SCAP capabilities and platforms supported. Vendors must provide a description of their product versioning method in order to define how major releases are numbered for the product entering the validation process. In general, validations will be awarded to major releases of products; however, if a minor release modifies the SCAP component of the product, then the vendor should enter validation for the minor release.

Validations will be awarded to SCAP module minor version number. Vendors must provide a versioning statement that describes how module versions are assigned. As with products, any modification of the SCAP component requires revalidation. Validated products will be listed on the SCAP Validated Products web page to include, but not limited to the following corresponding information:

- Product/module vendor or manufacturer name
- Product/module name
- Product/module major version validated
- Product/module version tested (full identifier at the time of testing)
- Platforms tested
- SCAP Capabilities
- Validation number
- Validation date
- Validation test suite version used for testing

3.2 Demarcation and Validation Expirations

The SCAP Validation Program recognizes the need for a clear demarcation point for end users, product vendors, the standards body and NVLAP accredited labs in order to develop, test, and deploy efficiently. The SCAP Validation Program also recognizes that SCAP component specifications, standards, and products typically change over time and employ a variety of versioning schemes for identifying different releases.

The final release date of NIST IR 7511 for the next version of SCAP[8] determines the end of the SCAP 1.2 Validation Program and the expiration date for SCAP 1.2 product validations. The SCAP 1.2 Validation Program will end 15 months after the final release of NIST IR 7511 for the next SCAP version. SCAP 1.2 product validations will expire 12 months after the SCAP 1.2 Validation Program ends. For example, if NIST IR 7511 for SCAP 1.3[9] is finalized on January 1, 2017, the SCAP 1.2 Validation Program would end on March 31, 2018. All SCAP 1.2 validated products would expire on March 31, 2019. The new SCAP 1.3 Validation Program would begin April 1, 2017.[10]

This document identifies a specific set of SCAP component specifications as described in Section 2 and the associated Derived Test Requirements (DTRs) as described in Section 4. Minor updates to SCAP

[8] The current version of SCAP is 1.2.

[9] This statement explains the revision cycle. The next release of SCAP may or may not be numbered 1.3, and the release date in this example is hypothetical.

[10] See http://scap.nist.gov/timeline.html for more information about the SCAP release cycle.

component specifications and products do not invalidate currently validated products. Major changes in functionality, including support for new SCAP technologies, may require product revalidation.

3.3 Validation Tools

The SCAP Validation Program uses several reference implementation tools that aid in the development and testing of SCAP products. The SCAP Validation (SCAPVal) Tool may be used for checking the correctness of SCAP data streams; SCAPVal is required during formal SCAP validation testing. Reference implementation tools may be used to process SCAP content; these tools are not required during formal SCAP validation testing. The SCAP Validation Tool and reference implementation tools are discussed in more detail below.

3.3.1 SCAP Validation Tool

The SCAP Validation Tool (SCAPVal) validates the correctness of an SCAP data stream for a particular use case according to what is defined in SP 800-126. The SCAPVal output provides information about whether an SCAP data stream (.zip file) conforms to conventions and recommendations outlined in NIST SP 800-126 Revision 2 [NIST SP 800-126 R2].

SCAPVal provides the following functions:

- Validates the data stream according to one of the use cases for an SCAP-validated product listed in Section 5 of [NIST SP 800-126 R2], namely Compliance Checking, Vulnerability Scanning, or Inventory Scanning.
- Checks components and data streams against appropriate schemas.
- Uses Schematron to perform additional checks within and across component data streams.
- Produces validation results that convey all error and warning conditions detected; results are output in both XML and HTML formats.

For a listing of the SCAP requirements, refer to the SCAP Version 1.0 Requirements Matrix, SCAP Version 1.1 Requirements Matrix, and SCAP Version 1.2 Requirements Matrix included with the tool. SCAPVal may be downloaded from http://scap.nist.gov/revision/index.html.

3.3.2 Reference Implementation Tools

Reference implementation tools or interpreters are open source tools that process SCAP data streams. Several interpreters are available with varying degrees of support across platforms. Each interpreter is command line and all have readme files providing usage guidance. Use of reference implementation tools is not required by the SCAP Validation Program.

The SCAP interpreter is an open source Java application that scans a system based on the requirements defined in [NIST SP 800-126 R2]. This application uses the XCCDF interpreter, the OVAL interpreter, and the OCIL interpreter when processing SCAP data streams. SCAP versions 1.0, 1.1, and 1.2 are supported. The SCAP interpreter is available on SourceForge at http://sourceforge.net/projects/scapexec/.

The XCCDF interpreter is an open source application for performing system analysis and report generation using the XCCDF format. This application will process XCCDF and OVAL files. The application is available on SourceForge at http://sourceforge.net/projects/xccdfexec/.

The OVAL interpreter (OVAL DI) is an open source application that demonstrates the evaluation of OVAL definitions. This reference implementation collects system information, evaluates it, and generates a detailed OVAL Results file. The OVAL interpreter is available on SourceForge at http://sourceforge.net/projects/ovaldi/.

The OCIL interpreter (OCIL QI) is an open source Java GUI application that demonstrates how an OCIL document can be evaluated. It guides the end user in completing questionnaires, viewing, and computing results. This application is available on SourceForge at http://sourceforge.net/projects/interactive/.

4. Derived Test Requirements

This section contains the test requirements for each of the SCAP components for the purpose of allowing individual validation of each SCAP component within a product. Version information and download location, listed in Section 2, SHOULD be referenced to ensure that the correct version is being used prior to testing. SCAP-specific requirements are found in Section 5.

Each DTR includes the following information:

- The DTR name: comprised of the acronym followed by ".R" to denote it is a requirement, and then the requirement number.
- SCAP Capability (summarized in Table 5-1) where
  - ACS = Authenticated Configuration Scanner
    - CVE = Optional CVE Support when combined with ACS
    - OCIL = Optional OCIL Support when combined with ACS
- Required vendor information: states required information vendors MUST provide to the testing lab for the test to be conducted.
- Required test procedure(s): defines one or more tests that the testing laboratory will conduct to determine the product's ability to meet the stated requirement.

The derived requirements are organized into the following major categories:

1. Assertions – Statements made by the products (in its documentation) that indicate what the product does (or does not) do relative to SCAP and its components (see Section 4.1)
2. Input Processing and Correctness – Those requirements that define the processing of SCAP source data streams and their major permutations (e.g., various source data stream tests such as source data streams with multiple benchmarks, legacy data streams, and signed data streams) (see Section 4.2)
3. Results Production – Those requirements that define how products will be assessed for their ability to produce valid SCAP results (see Section 4.3)

4.1 SCAP Assertions

This section addresses the assertions that vendors MUST make about the products seeking validations relative to SCAP and its component specifications as defined in Section 2.

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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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 a static electronic document (e.g., a PDF or help file).

Required Test Procedures:

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.

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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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. This document SHALL include a high-level summary of the implementation approach and an assertion of backwards compatibility with SCAP 1.0 and SCAP 1.1. 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.

Required Test Procedures:

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 1.0 and SCAP 1.1. 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.

SCAP.T.200.2: The tester SHALL verify that the provided documentation is an English language document consisting of 150 to 2500 words.

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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

SCAP.V.300.1: The vendor SHALL indicate the defined SCAP capabilities (one or more) for which their product is being tested.

Required Test Procedures:

SCAP.T.300.1: The tester SHALL ensure that all tests associated with the asserted SCAP capabilities of the product are conducted.

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).

4.2 SCAP Source Data Stream Processing and Correctness

This section addresses the ability of a product to correctly process SCAP source data streams.

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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

SCAP.V.400.1: The vendor SHALL provide documentation and instruction on how to import SCAP source data streams for the target platform.

Required Test Procedures:

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.

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.

SCAP.R.500: The product SHALL be able to select a specific SCAP source data stream when processing an SCAP data stream collection.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

SCAP.T.500.1: The tester SHALL validate the vendor product can selectively choose and apply a specific valid SCAP data stream.

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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

SCAP.T.600.1: The tester SHALL validate the vendor product can selectively choose and apply a specific valid XCCDF benchmark.

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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

SCAP.T.700.1: The tester SHALL validate the vendor product can selectively choose and apply a specific valid XCCDF profile.

SCAP.R.800: The product SHALL enable the user to import (signed and unsigned) SCAP source data streams.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

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.

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.

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.

SCAP.R.900: The product SHALL recognize and reject SCAP source data streams that have invalid signatures.

This requirement has been deferred.

SCAP.R.1000: The product SHALL recognize and reject SCAP source data streams that have signatures based on invalid certificates.

This requirement has been deferred.

SCAP.R.1100: The product SHALL be able to correctly import all earlier versions of SCAP content.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

SCAP.T.1100.1: Using the vendor product, the tester SHALL execute a valid SCAP source data stream based on SCAP 1.0 and SCAP 1.1 content.

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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

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.

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.

SCAP.R.1300: The product SHALL report and MAY reject OVAL content that is part of an SCAP source data stream and that is invalid according to the OVAL XML schemas and Schematron style sheets.[11]

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

SCAP.V.1300.1: The vendor SHALL provide instructions on how validation of OVAL content that is part of an SCAP data stream is performed and where errors from validation will be displayed within the product output.

Required Test Procedures:

SCAP.T.1300.1: The tester SHALL attempt to import known invalid OVAL content that is part of an SCAP 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 style sheets.

SCAP.R.1400: The product SHALL report and MAY reject OCIL content that is invalid according to the OCIL XML schema.

SCAP Capability: ☐ ACS ☐ CVE ☑ OCIL

Required Vendor Information:

SCAP.V.1400.1: The vendor SHALL provide instructions on how validation of OCIL content is performed and where errors from validation will be displayed within the product output.

Required Test Procedures:

SCAP.T.1400.1: The tester SHALL attempt to import known invalid OCIL 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.

SCAP.R.1500: The product SHALL be able to correctly assess the target systems using USGCB source data streams as input.[12]

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

[11] 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.

[12] In the case where the Tier IV repository does not contain a source data stream for the tested platform, the tester SHALL use a source data stream from Tier III. In case there is no content applicable to the tested platform, this requirement does not apply.

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. The tested systems SHALL be configured as Exact Compliance Configuration (the configuration settings are equal to the discrete settings defined in the baseline).

Required Test Procedures:

Per vendor instruction in SCAP.V.1500.1, the lab or the vendor will configure the test systems, make the necessary configuration changes to the target platform, and document what has been changed. The pass/fail comparison of these changes SHALL NOT impact the Pass or Fail result of the test.

All the applicable USGCB source data streams published in the official National Checklist Program Repository should be used for testing this requirement: http://checklists.nist.gov.

SCAP.T.1500.1: The lab or the vendor SHALL evaluate the compliant target platforms, in a domain connected configuration for Windows and standalone configuration for other platforms (i.e., RHEL, Mac OS X, Unix, etc.), and compare the pass/fail results from the product to the expected results, ensuring the actual results match the expected results. If the testing is performed by the vendor, the source data streams, the scan results, and their hashes[13] will be submitted to the lab for verification.

SCAP.T.1500.2: The tester SHALL review the scan results to ensure the files have not been altered, the actual results match expected results, and pass the SCAPVal validation without any errors.

SCAP.R.1510: The product SHALL be able to correctly evaluate a patches up-to-date rule which references an OVAL source data stream component consistent with the normative guidance specified in [NIST SP 800-126 R2], against target systems of the target platform type and produce the expected results.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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 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 rule(s), 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), in a domain connected configuration for Windows and standalone configuration for other platforms, validate results

[13] The hashes SHALL comply with *Annex A: Approved Security Functions* of [FIPS 140-2].

produced with SCAPVal, and compare the scan results produced by the product to the expected results, ensuring the actual results match the expected results.

SCAP.R.1600: If the vendor 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." [OMB M-08-22] 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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

SCAP.T.1600.1**:** The tester SHALL review the provided documentation to ensure that each indicated setting includes an associated rationale.

SCAP.R.1700: The product SHALL be able to correctly process the content that is representative of content published at Tier III, Tier IV, and the OVAL repository[14] which is associated with the platforms for which validation is being sought.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

SCAP.V.1700.1: The vendor SHALL provide instructions on how to execute a previously imported valid data stream for platforms supported.

Required Test Procedures:

SCAP.T.1700.1**:** Per vendor instruction in SCAP.V.1700, the tester SHALL evaluate a target platform using test content representative of Tier III content, validate results produced with SCAPVal, and ensure actual results match expected results.

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.

[14] The OVAL repository is hosted by MITRE Corporation: https://oval.mitre.org/repository/.

SCAP Capability: ☐ ACS ☐ CVE ☑ OCIL

Required Vendor Information:

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.

Required Test Procedures:

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.

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[15] specified in [NIST SP 800-126 R1], against target systems of the target platform type and produce a result file 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.[16]

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedure

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.

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.

SCAP.T.1900.3: The tester SHALL validate that the resulting OVAL XML Full Results are available for viewing by the user.

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.

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

[16] The use case for OVAL-Only Scanning is described in Section 5.4 of [NIST SP 800-126 R1].

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.

SCAP.R.2000: The product SHALL be able to correctly evaluate a valid OVAL Definition file that is part of an SCAP data stream, where the contents of the OVAL definition file are consistent with the normative guidance[17] specified in [NIST SP 800-126 R2], against target systems of the target platform type and produce a result file 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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedure:

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.

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.

SCAP.T.2000.3: The tester SHALL validate that the resulting SCAP data stream is available for viewing by the user.

SCAP.T.2000.4: The tester SHALL capture the successful results of the import and verify the correctness of the results.

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.

SCAP Capability: ☐ ACS ☐ CVE ☑ OCIL

Required Vendor Information:

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.

Required Test Procedure:

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

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.

SCAP.T.2100.2: The tester SHALL validate the resulting OCIL Output file with the SCAPVal utility and check for any validation errors.

SCAP.T.2100.3: The tester SHALL validate that the resulting OCIL Output file is available for viewing by the user.

SCAP.R.2200: The product SHALL be able to correctly evaluate a valid OCIL Questionnaire file that is part of an SCAP source data stream against target 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.

SCAP Capability: ☐ ACS ☐ CVE ☑ OCIL

Required Vendor Information:

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.

Required Test Procedure:

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.

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.

SCAP.T.2200.3: The tester SHALL validate that the resulting SCAP data stream is available for viewing by the user.

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).

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

SCAP.V.2300.1: None.

Required Test Procedures:

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.

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).

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

SCAP.V.2400.1: None.

Required Test Procedures:

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.

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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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 2.5.

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.

Required Test Procedures:

SCAP.T.2500.1: The tester SHALL compare the vendor-provided list of CPE Names against the official CPE Dictionary.[18] The tester SHALL verify that all exceptions found match the list of exceptions provided by the vendor.

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 [NIST SP 800-126 R2].

[18] http://static.nvd.nist.gov/feeds/xml/cpe/dictionary/official-cpe-dictionary_v2.2.xml

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

SCAP.T.2600.1: The tester SHALL import the known content into the product and apply it against a known platform.

SCAP.T.2600.2: The tester SHALL import the results of the content into the SCAPVal utility and check for any validation errors.

SCAP.T.2600.3: The tester SHALL ensure the actual results match the expected results.

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).

SCAP Capability: ☐ ACS ☑ CVE ☐ OCIL

Required Vendor Information:

SCAP.V.2700.1: None

Required Test Procedures:

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 URLs that link to the NVD website. For example, http://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2011-1377. It is not sufficient to provide a URL to http://web.nvd.nist.gov.

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).

SCAP Capability: ☐ ACS ☑ CVE ☐ OCIL

Required Vendor Information:

SCAP.V.2800.1: None.

Required Test Procedures:

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.

4.3 SCAP Result(s) Data Stream

This section addresses those requirements that assess a product's ability to produce validated SCAP results.

SCAP.R.2900: SCAP result data streams SHALL be produced by the product in compliance with the SCAP result data streams as specified in [NIST SP 800-126 R2].

SCAP Capability: ☑ ACS □ CVE □ OCIL

Required Vendor Information:

SCAP.V.2900.1: The vendor SHALL provide instruction on where the corresponding XCCDF and OVAL results files can be located for inspection.

Required Test Procedures:

SCAP.T.2900.1: The tester SHALL visually inspect SCAP results to verify that they are valid according to the associated specification for each. The SCAP output MUST be processed by the SCAPVal utility without any errors.

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 NIST [NIST SP 800-126 R2], against target systems of the target platform type and produce the expected results.

SCAP Capability: ☑ ACS □ CVE □ OCIL

Required Vendor Information:

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.

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 [NIST SP 800-126 R2].

SCAP Capability: ☑ ACS ☑ CVE □ OCIL

Required Vendor Information:

SCAP.V.2920.1: The vendor SHALL provide instruction on where the SCAP Result Data Stream files can be located for inspection.

Required Test Procedures:

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.

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 [NIST SP 800-126 R2].

SCAP Capability: ☑ ACS □ CVE □ OCIL

Required Vendor Information:

SCAP.V.2930.1: The vendor SHALL provide instruction on where the SCAP Result Data Stream files can be located for inspection.

Required Test Procedures:

SCAP.T.2930.1: The tester SHALL visually inspect the results to 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.

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 [NIST SP 800-126 R2].

SCAP Capability: ☑ ACS □ CVE □ OCIL

Required Vendor Information:

SCAP.V.2940.1: The vendor SHALL provide instruction on where the SCAP Result Data Stream files can be located for inspection.

Required Test Procedures:

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.

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.[19]

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

NOTE: "XCCDF components" refer to the elements such as benchmark, profile, group, rule, value, and test result.

Required Vendor Information:

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” result for a given rule.

Required Test Procedures:

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.

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.

SCAP.T.3000.3: The tester SHALL compare the product results to the expected results ensuring that the “pass”/ “fail” results match for each Rule.

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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

[19] XCCDF Specification in [NISTIR 7275 R4].

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.

Required Test Procedures:

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.

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.

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.

SCAP.T.3005.4: The tester SHALL compare the product results to the expected results ensuring that all the results match the expected results.

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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

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.

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.

SCAP.T.3010.3: The tester SHALL compare the product results to the expected results ensuring that all the results match the expected results.

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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

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.

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).

SCAP Capability: ☐ ACS ☐ CVE ☑ OCIL

Required Vendor Information:

SCAP.V.3200.1: The vendor SHALL provide instructions on how the user can view the XML OCIL Questionnaires being consumed by the product.

Required Test Procedure:

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.

SCAP.R.3300: The product SHALL be able to produce “notchecked” results for unsupported Check Systems. [20]

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

SCAP.V.3300.1: The vendor SHALL provide instructions indicating how content for unsupported check systems is processed.

Required Test Procedures:

[20] XCCDF Specification in [NISTIR 7275 R4].

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 check system.

SCAP.R.3400: The product output SHALL enable users to view the XML OVAL Definitions being consumed by the product (e.g., within the product user interface or through an XML dump of the OVAL definitions to a file).

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

SCAP.V.3400.1: The vendor SHALL provide instructions on how the user can view the XML OVAL Definitions being consumed by the product.

Required Test Procedure:

SCAP.T.3400.1: The tester SHALL follow the provided vendor instructions to view the XML OVAL Definitions being consumed by the product and verify that access is provided as stated.

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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

SCAP.T.3500.1: The tester SHALL visually inspect the product output for the dates of all SCAP source data streams processed by the vendor product.

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).

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

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.

SCAP.R.3700 has been removed.

SCAP.R.3800: A product's machine-readable output MUST provide the CPE naming data using CPE names.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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).

Required Test Procedures:

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.

SCAP.R.3900: The product SHALL allow users to locate configuration issue items using CCE IDs.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

SCAP.V.3900.1: The vendor SHALL provide documentation (printed or electronic) indicating how configuration issue items can be located using CCE IDs.

Required Test Procedures:

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.

SCAP.R.4000: The product SHALL be able to correctly produce the Asset Identification Fields as specified in [NIST SP 800-126 R2] when assessing a target.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

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.

SCAP.T.4000.2: The tester SHALL validate the results produced using SCAPVal; the validation MUST NOT produce any errors.

SCAP.T.4000.3: The tester SHALL visually inspect the results to ensure the Asset Identification Fields are as expected.

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.

SCAP Capability: ☑ ACS ☐ CVE ☑ OCIL

Required Vendor Information:

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.

Required Test Procedures:

SCAP.T.4100.1: The tester SHALL import the SCAP 1.2 source data stream, apply it to a known target, and produce an SCAP result data stream conforming to the ARF specification.

SCAP.T.4100.2: The tester SHALL validate the results produced using SCAPVal; the validation MUST NOT produce any errors.

SCAP.T.4100.3: The tester SHALL compare the actual results to the expected results ensuring the results match.

SCAP.R.4200: The product SHALL provide a means to view the CVE Description and CVE references for each displayed CVE ID[21] within the product output.

SCAP Capability: ☐ ACS ☑ CVE ☐ OCIL

Required Vendor Information:

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 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.

Required Test Procedures:

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

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

output enables the user to view, at minimum, the official CVE description and references.[22] 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.

SCAP.R.4300: For all static or product -bundled CCE data, 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.

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

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.

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.[23]

SCAP Capability: ☐ ACS ☑ CVE ☐ OCIL

Required Vendor Information:

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.

Required Test Procedures:

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.

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.

SCAP Capability: ☐ ACS ☑ CVE ☐ OCIL

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

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

Required Vendor Information:

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.[24] The vendor MAY provide information about how the product can be updated with new NVD CVSS base scores and vector strings prior to testing.

Required Test Procedure:

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.

SCAP.R.4600: When processing SCAP source data streams that contain compliance mappings to CCEs, the product SHALL output the compliance mappings.[25]

SCAP Capability: ☑ ACS ☐ CVE ☐ OCIL

Required Vendor Information:

SCAP.V.4600.1: The vendor SHALL provide documentation explaining where CCE to NIST SP 800-53 compliance mappings can be viewed within the product output.

Required Test Procedures:

SCAP.T.4600.1: Using the vendor product, the tester SHALL execute a valid SCAP source data stream with CCE to NIST SP 800-53 compliance mapping information and view the resultant output to ensure that the CCE compliance mappings are correct.

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

[25] The USGCB data streams have associated machine readable CCE to 800-53 mappings available at https://usgcb.nist.gov .

5. Derived Test Requirements for Specific Capabilities

This section contains Derived Test Requirements for each of the defined SCAP capabilities. When a product is submitted for validation, the submitting organization will provide a list of SCAP capabilities the product possesses. The information regarding capabilities will be provided by the vendor as part of their submission package. To determine the correct test requirements for that product, the tester creates the union of all these capabilities using the chart below.

The matrix currently contains a total of three SCAP capabilities. As additional capabilities are available for validation, this list will be updated. Vendors seeking validation for an SCAP capability not listed should contact NIST at scap@nist.gov.

The following chart summarizes the requirements for each SCAP 1.2 capability.

Table 5-1. Required SCAP Components for Each SCAP Capability

Requirement ID	Authenticated Configuration Scanner (ACS)	CVE option	OCIL option
SCAP.R.100	X		
SCAP.R.200	X		
SCAP.R.300	X		
SCAP.R.400	X		
SCAP.R.500	X		
SCAP.R.600	X		
SCAP.R.700	X		
SCAP.R.800	X		
SCAP.R.1100	X		
SCAP.R.1200	X		
SCAP.R.1300	X		
SCAP.R.1400			X
SCAP.R.1500	X		
SCAP.R.1510	X		
SCAP.R.1600	X		
SCAP.R.1700	X		
SCAP.R.1800			X
SCAP.R.1900	X		
SCAP.R.2000	X		
SCAP.R.2100			X
SCAP.R.2200			X

Requirement ID	Authenticated Configuration Scanner (ACS)	CVE option	OCIL option
SCAP.R.2300	X		
SCAP.R.2400	X		
SCAP.R.2500	X		
SCAP.R.2600	X		
SCAP.R.2700		X	
SCAP.R.2800		X	
SCAP.R.2900	X		
SCAP.R.2910	X		
SCAP.R.2920	X	X	
SCAP.R.2930	X		
SCAP.R.2940	X		
SCAP.R.3000	X		
SCAP.R.3005	X		
SCAP.R.3010	X		
SCAP.R.3100	X		
SCAP.R.3200			X
SCAP.R.3300	X		
SCAP.R.3400	X		
SCAP.R.3500	X		
SCAP.R.3600	X		
SCAP.R.3800	X		
SCAP.R.3900	X		
SCAP.R.4000	X		
SCAP.R.4100	X		X
SCAP.R.4200		X	
SCAP.R.4300	X		
SCAP.R.4400		X	
SCAP.R.4500		X	
SCAP.R.4600	X		

CVE and OCIL are optional SCAP component specifications that may be combined with ACS in SCAP 1.2 product validations. Product vendors may elect adding CVE, OCIL, or both options to the core ACS product validation. If the CVE option is chosen, the product must pass all CVE requirements marked in the CVE column in Table 5-1. If the OCIL option is chosen, the product must pass all OCIL requirements marked in the OCIL column in Table 5-1. Products may not be validated against the CVE or OCIL requirements alone. These optional validations must be combined with the core ACS product validation.

NOTE: The ACS capability encompasses the functionality covered by FDCC Scanner and USGCB Scanner capabilities that were included in the SCAP 1.0 Validation Program.

The list of OVAL tests used for testing the ACS SCAP 1.2 capability is published on the SCAP Validation Program web page http://scap.nist.gov/validation.[26]

[26] Support of deprecated OVAL tests is required for the Authenticated Configuration Scanner (ACS) capability. Backward compatibility is required for SCAP 1.2 validated products.

Appendix A—Terms and Definitions

This appendix lists definitions of key terms used in this document.

Authenticated Configuration Scanner: A product that runs with administrative or root privileges on a target system to conduct its assessment.

CCE ID: An identifier for a specific configuration defined within the official CCE Dictionary and that conforms to the CCE specification. For more information please see the CCE specification reference in Section 2.

Compliance Mapping: The process of correlating CCE settings defined in a source data stream with the security control identifiers defined in NIST SP 800-53.

CPE Name: An identifier for a unique uniform resource identifier (URI) assigned to a specific platform type that conforms to the CPE specification. For more information please see the CPE specification reference in Section 2.

CVE ID: An identifier for a specific software flaw defined within the official CVE Dictionary and that conforms to the CVE specification. For more information please see the CVE specification reference in Section 2.

Derived Test Requirement/Test Requirement: A statement of requirement, needed information, and associated test procedures necessary to test a specific SCAP feature.

Import: A process available to end users by which an SCAP source data stream can be loaded into the vendor's product. During this process, the vendor process may optionally translate this file into a proprietary format.

Machine-Readable: Product output that is in a structured format, typically XML, which can be consumed by another program using consistent processing logic.

Major Revision: Any increase in the version of an SCAP component's specification or SCAP related data set that involves substantive changes that will break backwards compatibility with previous releases. See also SCAP revision.

Minor Revision: Any increase in the version of an SCAP component's specification or SCAP related data set that may involve adding additional functionality, but that preserves backwards compatibility with previous releases. See also SCAP revision.

Misconfiguration: A setting within a computer program that violates a configuration policy or that permits or causes unintended behavior that impacts the security posture of a system. CCE can be used for enumerating misconfigurations.

> **NOTE:** NIST generally defines vulnerability as including both software flaws and configuration issues [misconfigurations]. For the purposes of the validation program and dependent procurement language, the SCAP Validation program is defining vulnerability and misconfiguration as two separate entities, with "vulnerability" referring strictly to software flaws.)

National Checklist Program Repository (NCP): A NIST maintained repository, which is a publicly available resource that contains information on a variety of security configuration checklists for specific IT products or categories of IT products.

National Vulnerability Database (NVD): The U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data informs automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Non-vendor-directed: This term is used to indicate that any sample chosen for testing is selected by the testing laboratory without the input or knowledge of the product vendor.

OVAL ID: An identifier for a specific OVAL definition that conforms to the format for OVAL IDs. For more information please see the OVAL specification reference in Section 2.

Product: A software application that has one or more capabilities.

Module (SCAP Module): it is an embedded software component of a product or application, or a complete product in-and-of-itself that has one or more capabilities.

Product Output: Information produced by a product. This includes the product user interface, human-readable reports, and machine-readable reports. Unless otherwise indicated by a specific requirement, there are no constraints on the format. When this output is evaluated in a test procedure, either all or specific forms of output will be sampled as indicated by the test procedure.

SCAP Capability: A specific function or functions of a product as defined below:

- Authenticated Configuration Scanner: the capability to audit and assess a target system to determine its compliance with a defined set of configuration requirements using target system logon privileges.
- Common Vulnerabilities and Exposures (CVE) Option: the capability to process and present CVEs correctly and completely
- Open Checklist Interactive Language (OCIL) Option: the capability to process and present OCIL correctly and completely

SCAP Component: One of the eleven specifications that comprise SCAP: Asset Identification, ARF, CCE, CCSS, CPE, CVE, CVSS, OCIL, OVAL, TMSAD, and XCCDF.

SCAP Result Data Stream: A bundle of SCAP components, along with the mappings of references between SCAP components, that holds output (result) content.

SCAP Revision: A version of the SCAP specification designated by a revision number in the format nn.nn.nn, where the first nn is the major revision number, the second nn number is the minor revision number, and the final nn number is the refinement number. A specific SCAP revision will populate all three fields, even if that means using zeros to show no minor revision or refinement number has been used to date. A leading zero will be used to pad single-digit revision or refinement numbers.

SCAP Source Data Stream: A bundle of SCAP components, along with the mappings of references between SCAP components, that holds input (source) content. See also Compliance Mapping.

Software Flaw: See Vulnerability.

Target Platform: The target operating system or application on which a vendor product will be evaluated using a platform-specific validation lab test suite. These platform-specific test suites consist of specialized SCAP content used to perform the test procedures defined in this document.

Tier I Checklist: A checklist in the National Checklist Repository that is prose-based, such as narrative descriptions of how a person can manually alter a product's configuration.

Tier II Checklist: A checklist in the National Checklist Repository that documents the recommended security settings in a machine-readable but non-standard format, such as a proprietary format or a product-specific configuration script.

Tier III Checklist: A checklist in the National Checklist Repository that uses SCAP to document the recommended security settings in machine-readable standardized SCAP formats that meet the definition of "SCAP Expressed" specified in NIST SP 800-126. SCAP Validated products should be able to process Tier III checklists.

Tier IV Checklist: A checklist in the National Checklist Repository that is considered production-ready and has been validated by NIST or a NIST-recognized authoritative entity to ensure, to the maximum extent possible, interoperability with SCAP-validated products. Tier IV checklists also demonstrate the ability to map low-level security settings (for example, standardized identifiers for individual security configuration issues) to high-level security requirements as represented in various security frameworks (e.g., SP 800-53 controls for FISMA), and the mappings have been vetted with the appropriate authority.

Vulnerability: An error, flaw, or mistake in computer software that permits or causes an unintended behavior to occur. CVE is a common means of enumerating vulnerabilities.

XCCDF Content: A file conforming to the XCCDF schema. For more information please see the XCCDF specification reference in Section 2.

Appendix B—Acronyms

This appendix contains selected acronyms and abbreviations used in the publication.

ACS	Authenticated Configuration Scanner
ARF	Asset Reporting Format
CCE	Common Configuration Enumeration
CCSS	Common Configuration Scoring System
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DTR	Derived Test Requirement
FDCC	Federal Desktop Core Configuration
FIRST	Forum of Incident Response and Security Teams
FISMA	Federal Information Security Management Act
GUI	Graphical User Interface
HTML	Hypertext Markup Language
ID	Identifier
IETF	Internet Engineering Task Force
IR	Interagency Report
IT	Information Technology
ITL	Information Technology Laboratory
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
NVLAP	National Voluntary Laboratory Accreditation Program
OCIL	Open Checklist Interactive Language
OCIL QI	Open Checklist Interactive Language Questionnaire Interpreter
OMB	Office of Management and Budget
OS	Operating System
OVAL	Open Vulnerability and Assessment Language
OVAL DI	Open Vulnerability and Assessment Language Definition Interpreter
PDF	Portable Document Format
RFC	Request for Comment
RHEL	Red Hat Enterprise Linux
SCAP	Security Content Automation Protocol
SCAPVal	SCAP Validation tool
SP	Special Publication
TMSAD	Trust Model for Security Automation Data
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
U.S.	United States
USGCB	United States Government Configuration Baseline
WFN	Well-Formed Name
XCCDF	Extensible Configuration Checklist Document Format
XML	Extensible Markup Language

Appendix C—Use of SCAP 1.2 Logo and phrases

This appendix contains information regarding the use of SCAP 1.2 Logo and phrases

The phrases SCAP 1.2 Validated and SCAP 1.2 Logo are intended for use in association with SCAP 1.2 products or modules validated by the National Institute of Standards and Technology (NIST) as complying with Security Content Automation Protocol (SCAP) Version 1.2 Requirements for Products/Modules.

Vendors of validated SCAP products and/or modules or vendors of products that embed validated SCAP modules are encouraged to use the phrases and logo provided that they agree to the following and returning the signed SCAP 1.2 Logo Form:

1. The phrases SCAP 1.2 Validated and the SCAP 1.2 Logo are Certification Marks of NIST, which retains exclusive rights to their use.

2. NIST reserves the right to control the quality of the use of the phrase SCAP 1.2 Validated and the logo itself.

3. Permission for advertising SCAP 1.2 validation and use of the logo is conditional on and limited to those SCAP products/modules validated by NIST as complying with the requirements for Security Content Automation Protocol (SCAP) Version 1.2.

4. An SCAP module may either be a component of a product, or a standalone product. Use of the SCAP 1.2 Logo on product reports, letterhead, brochures, marketing material, and product packaging shall be accompanied by the following: ‘TM: A Certification Mark of NIST, which does not imply product endorsement by NIST or the U.S. Government’. If the SCAP module is a component of a product, the phrase “SCAP 1.2 Inside” shall accompany the logo.

5. Permission for the use of the phrase SCAP 1.2 Validated and the logo may be revoked at the discretion of NIST.

6. Permission to use the phrase SCAP 1.2 Validated and the SCAP 1.2 Logo in no way constitutes or implies product endorsement by NIST.

Appendix D—References

The following references are cited in the document above.

[FIPS 140-2] Federal Information Process Standards Publication (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, May 2001 (with Change Notices through December 3, 2002). http://csrc.nist.gov/publications/PubsFIPS.html#140-2.

[NIST HB 150] NIST Handbook 150 (2006 Edition), *National Voluntary Laboratory Accreditation Program: Procedures and General Requirements*, February 2006. http://www.nist.gov/nvlap/upload/nist-handbook-150.pdf.

[NIST HB 150-17] NIST Handbook 150-17, *NVLAP Cryptographic and Security Testing*, May 2013. http://dx.doi.org/10.6028/NIST.HB.150-17.

[NISTIR 7275 R4] NIST Interagency Report (NISTIR) 7275 Revision 4, *Specification for the Extensible Configuration Checklist Description Format (SCCDF) Version 2.1*, September 2011 (updated March 2012). http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7275-Rev.%204.

[NISTIR 7435] NIST Interagency Report (NISTIR) 7435, *The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems*, August 2007. http://csrc.nist.gov/publications/nistir/ir7435/NISTIR-7435.pdf.

[NISTIR 7502] NIST Interagency Report (NISTIR) 7502, *The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities*, December 2010. http://csrc.nist.gov/publications/nistir/ir7502/nistir-7502_CCSS.pdf.

[NISTIR 7511 R3] NIST Interagency Report (NISTIR) 7511 Revision 3, *Security Content Automation Protocol (SCAP) Version 2.1 Validation Program Test Requirements*, January 2013 (updated July 11, 2013). http://dx.doi.org/10.6028/NIST.IR.7511.

[NISTIR 7692] NIST Interagency Report (NISTIR) 7692, *Specification for the Open Checklist Interactive Language (OCIL) Version 2.0*, April 2011. http://csrc.nist.gov/publications/nistir/ir7692/nistir-7692.pdf.

[NISTIR 7693] NIST Interagency Report (NISTIR) 7693, *Specification for Asset Identification 1.1*, June 2011. http://csrc.nist.gov/publications/nistir/ir7693/NISTIR-7693.pdf.

[NISTIR 7694] NIST Interagency Report (NISTIR) 7694, *Specification for the Asset Reporting Format 1.1*, June 2011. http://csrc.nist.gov/publications/nistir/ir7694/NISTIR-7694.pdf.

[NISTIR 7695] NIST Interagency Report (NISTIR) 7695, *Common Platform Enumeration: Naming Specification Version 2.3*, August 2011. http://csrc.nist.gov/publications/nistir/ir7695/NISTIR-7695-CPE-Naming.pdf.

[NISTIR 7696] NIST Interagency Report (NISTIR) 7696, *Common Platform Enumeration: Name Matching Specification Version 2.3*, August 2011. http://csrc.nist.gov/publications/nistir/ir7696/NISTIR-7696-CPE-Matching.pdf.

[NISTIR 7697] NIST Interagency Report (NISTIR) 7697, *Common Platform Enumeration: Dictionary Specification Version 2.3*, August 2011. http://csrc.nist.gov/publications/nistir/ir7696/NISTIR-7696-CPE-Matching.pdf.

[NISTIR 7698] NIST Interagency Report (NISTIR) 7698, *Common Platform Enumeration: Applicability Language Specification Version 2.3*, August 2011. http://csrc.nist.gov/publications/nistir/ir7698/NISTIR-7698-CPE-Language.pdf.

[NISTIR 7802] NIST Interagency Report (NISTIR) 7802, *Trust Model for Security Automation Data 1.0 (TMSAD)*, September 2011. http://csrc.nist.gov/publications/nistir/ir7802/NISTIR-7802.pdf.

[NIST SP 800-53 R4] NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated January 22, 2015). http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[NIST SP 800-126 R1] NIST Special Publication (SP) 800-126 Revision 1, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1*, February 2011. http://csrc.nist.gov/publications/nistpubs/800-126-rev1/SP800-126r1.pdf.

[NIST SP 800-126 R2] NIST Special Publication (SP) 800-126 Revision 2, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*, September 2011. http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf.

[OMB M-08-22] Office of Management and Budget (OMB) Memorandum M-08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)*, August 11, 2008. http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-22.pdf

[RFC 2119] Internet Engineering Task Force (IETF) Request for Comment (RFC) 2119, *Key words for use in RFCs to Indicate Requirement Levels*, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

[XMLS] World Wide Web Consortium (W3C) Recommendation, *XML Schema* [XML Schema 1.1], October 28, 2004. http://www.w3.org/XML/Schema.html.