The attached DRAFT document (provided here for HISTORICAL purposes) has been superseded by the following publication:

Publication Number: **NIST Interagency Report 7511, Revision 3**

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

Publication Date: **02/05/2013**

- Final Publication: http://dx.doi.org/10.6028/NIST.IR.7511
- Related Information on CSRC: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7511
- Information on other NIST Computer Security Division publications and programs can be found at: http://csrc.nist.gov/

The following information was posted with the attached DRAFT document:

Final Approval of NIST Interagency Report (IR) 7511 Revision 3 is now available
February 5, 2013

NIST announces the release of NIST Interagency Report (NISTIR) 7511 Revision 3, Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements. NISTIR 7511 defines the requirements that must be met by products to achieve SCAP 1.2 Validation. 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. NISTIR 7511 Revision 3 has been written primarily for accredited laboratories and for vendors interested in producing SCAP validated products.

NIST Interagency Report 7511 **Revision 3**
(Draft)

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

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

John Banghart
Stephen Quinn
David Waltermire
Andrew Bove

NIST Interagency Report 7511
Revision 3 (Draft)

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

John Banghart
Stephen Quinn
David Waltermire
Andrew Bove

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

November 2011

U.S. Department of Commerce

Rebecca M. Blank Acting Secretary

National Institute of Standards and Technology

Dr. Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

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 analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Interagency Report discusses ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report 7511 Revision 3 (Draft)
34 pages **(November 2011)**

Acknowledgements

The authors, John Banghart, Stephen Quinn, and David Waltermire of the National Institute of Standards and Technology (NIST), and Andrew Bove of Secure Acuity, would like to thank the many people that reviewed and contributed to this document. In particular, the following individuals provided invaluable input and feedback: Lon Kight, Melanie Cook, and Matt Kerr of G2 Inc.

Abstract

This report defines the requirements and associated test procedures necessary for products 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).

Audience

The intended audience for SCAP Validation Program test requirements includes laboratories that are accredited to conduct SCAP product testing for the program, vendors that are interested in receiving SCAP validation for their products, and organizations seeking to deploy SCAP products in their environments. Accredited laboratories use the information in this report to guide their testing and ensure that 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 what features their products must have to be eligible to receive an SCAP validation. Government agencies and integrators use the information to gain insight into the criteria that products being considered for procurement must meet to be validated. The secondary audience for this publication is end users, which can review the test requirements to determine what a validated product had to do to be awarded a validation, as well as to better understand what SCAP validation means.

Comments

Comments on this report are welcome. Please direct them to NIST (IR7511comments@nist.gov).

Table of Contents

List of Tables

1. Introduction to SCAP and the SCAP Validation Program

The Security Content Automation Protocol (SCAP) is a suite of specifications[1] 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, an XML specification for exchanging technical details on how to check systems for security-related software flaws, configuration issues, and 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 [OCIL]
- 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
- Asset Identification (AI) 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.
- 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.
- 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 defines what SCAP's components are and how they relate to each other within the context of SCAP. However, the SCAP specification does not define the SCAP components themselves; each component has its own standalone specification 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).

[1] See NIST SP 800-126R2, The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2

NIST provides SCAP content, such as vulnerability and product enumeration identifiers, through a repository supplied by the National Vulnerability Database (NVD). All of the content in NVD, as well as the high-level SCAP specification, is freely available from NIST. SCAP content is also created and made available by non-U.S. government organizations through the National Checklist Program (NCP)[2]. More information on SCAP can be found at http://scap.nist.gov.

1.1 Purpose and Scope of the Program

The NIST SCAP Validation Program is designed to test the ability of products to use the features and functionality available through SCAP and its components. An information technology (IT) product 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 product capability[3]. At this time, validations are not being awarded based on the individual component specifications through this program. NIST may create new validation programs that address some or all of the individual specifications in the future as needed.

Under the SCAP Validation Program, independent laboratories are accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP) (http://ts.nist.gov/standards/accreditation/index.cfm). Accreditation requirements are defined in NIST Handbook 150, NVLAP Procedures and General Requirements and NIST Handbook 150-17, NVLAP Cryptographic and Security Testing. Independent laboratories conduct the tests contained 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 products are publicly posted on the NIST SCAP Validated Products web page (http://nvd.nist.gov/scapproducts.cfm).[4]

Validated products will be listed on the SCAP Validated Products web page to include, but not limited to the following corresponding information:

- Product vendor or manufacture name
- Product name
- Product version (full identifier at the time of testing)
- SCAP Validation Capabilities
- Validation Date
- Expiration Date

1.2 Superseded Compatibility 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 and the Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements Update released in January 2011.

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

[3] The SCAP Validation Program defines capability as "a specific function or functions of a product". Further information can be found in Section 2.4.

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

2. Versions and Definitions

2.1 Versions

For all test requirements that reference particular specifications, the versions indicated in the following section should be used and are derived primarily from the NIST SP 800-126.

Definition: SCAP is a specification for expressing and manipulating security data in standardized ways. SCAP uses several individual specifications in concert to automate continuous monitoring, vulnerability management, and security policy compliance evaluation reporting. The SCAP version allows the versions of the SCAP components to be referred to collectively.

Version: 1.2

Specification: NIST SP 800-126R2

SCAP 1.2 includes:

- XCCDF 1.2 - Extensible Configuration Checklist Description Format (XCCDF) 1.2, a language for authoring security checklists/benchmarks and for reporting results of checklist evaluation
- OVAL 5.10 - a language for representing system configuration information, assessing machine state, and reporting assessment results
- OVAL Power Shell Extension - a method for examining the configuration of Microsoft products.
- 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
- CCE 5 - a nomenclature and dictionary of software security configurations
- CPE 2.3 - a nomenclature and dictionary of hardware, operating systems, and applications
- CVE[5] - a nomenclature and dictionary of security-related software flaws
- CVSS 2.0 - a specification for measuring the relative severity of software flaw vulnerabilities
- CCSS 1.0 - a specification for measuring the relative severity of system security configuration issues
- AI 1.1 - a specification for asset identification
- ARF 1.1 - a data model for asset reporting
- TMSAD 1.0 - a specification for using digital signatures in a common trust model applied to other security automation specifications

2.1.1 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.

[5] CVE does not have a version number

Version: 1.2

Specification: Draft NIST IR 7275 Revision 4

Schema Location: http://csrc.nist.gov/publications/nistir/ir7275-rev4/NISTIR-7275r4.pdf

2.1.2 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.

Version: 5.10

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

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

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

2.1.3 Open Checklist Interactive Language (OCIL)

Definition: The Open Checklist Interactive Language (OCIL) defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions.

Version: 2.0

Specification: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7692

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

2.1.4 Common Configuration Enumeration (CCE)

Definition: CCE[6] is a format to describe system configuration issues to facilitate correlation of configuration data across multiple information sources and tools.

Version: 5

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

Schema Location: http://cce.mitre.org/

2.1.5 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.

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

2.1.5.1 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

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

2.1.5.2 CPE.Name Matching

Definition: The Name Matching specification defines the procedures for comparing WFNs to each other so as to determine 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

2.1.5.3 CPE.Dictionary[7]

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

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

2.1.5.4 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

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

[7] http://nvd.nist.gov/cpe.cfm

2.1.6 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/

2.1.7 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

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

2.1.8 Common Configuration Scoring System (CCSS)

Definition: The Common Configuration Scoring System (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

2.1.9 Asset Identification (AI)

Definition: This 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

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

2.1.10 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

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

2.1.11 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

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

2.2 Document Conventions

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 Request for Comment (RFC) 2119[8].

2.3 Internet Connectivity

An Internet connection, wireless or wired, during the evaluation of each test requirement is permitted for all tests. However, the product's validation record will indicate whether or not Internet connectivity is required for the product to function as expected. Every effort has been made in the test requirements to avoid mandating that the capability to run in the presence or absence of Internet connectivity be supported by a product. Access to a local area network (LAN) shall be allowed in all tests to support client-server based implementations.

2.4 Common Definitions

The following definitions represent key terms used in this document.

Authenticated Scanner: A product that runs with 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 2.1.

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 2.1.

[8] For more information, please refer to Internet Engineering Task Force (IETF) RFC 2119, Key words for use in RFCs to Indicate Requirement Levels. S. Bradner. March 1997, http://www.ietf.org/rfc/rfc2119.txt?number=2119.

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 2.1.

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 product. During this process, the vendor process may optionally translate this file into a proprietary format.

Machine-Readable: Tool 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 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 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 enables 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 2.1.

Product: A software application 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.

Reference Product: A product provided to accredited laboratory testers by NIST for use as a baseline for testing requirements. The product exhibits the behavior that is deemed to be correct.

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.
- Authenticated Vulnerability and Patch Scanner: the capability to scan a target system to locate and identify the presence of known vulnerabilities and evaluate the software patch status to determine compliance with a defined patch policy using target system logon privileges

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

SCAP Source Data Stream: A bundle of SCAP components along with the mappings of references between SCAP components.

SCAP Result Data Stream: A bundle of SCAP components along with the mappings of references between SCAP components.

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.

Software Flaw: See Vulnerability.

Target Platform: Is 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: Are checklists in the National Checklist Repository that are prose-based, such as narrative descriptions of how a person can manually alter a product's configuration.

Tier II Checklist: Are checklists in the National Checklist Repository that document 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: Are checklists in the National Checklist Repository that use 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 tools should be able to process Tier III checklists though this capability is not tested by the accredited independent testing laboratory.

Tier IV Checklist: Are checklists in the National Checklist Repository that are considered production-ready and have 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.

3. Derived Test Requirements

This section contains the Derived Test Requirements (DTR) for SCAP and its components Version information and download location, listed in Section 2.1, should be referenced to ensure that the correct version is being used prior to testing.

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.
- 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 SCAP and its components
2. Input Processing – Those requirements that govern the processing of SCAP source data streams and its major permutations
3. Correctness – Those requirements that define how products will be assessed for their ability to correctly process specific classes of SCAP content
4. Results Production – Those requirements that define how products will be assessed for their ability to produce valid SCAP results.

3.1 SCAP Assertions

This section addresses the assertions that vendors must make about the products seeking validations relative to the SCAP and its component specifications as specified in Section 2.1.

SCAP.R.10: 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.

Required Vendor Information

SCAP.V.10: 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.10.1: 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.20: The vendor must assert that the product implements the 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.

Required Vendor Information

SCAP.V.20: The vendor shall provide a separate, 150 to 2500 word plain text document written in the English language to the lab asserting that the product implements the SCAP and its component specifications for the capabilities claimed in Table 6-1. This document shall include a high-level summary of the implementation approach and list any special considerations. This content will be used on NIST web pages to explain details about each validated product and thus must contain only information that is to be publicly released.

Required Test Procedures

SCAP.T.20.1: The tester shall inspect the provided documentation to verify that the documentation asserts that the product implements the SCAP and its component specifications and provides a high-level summary of the implementation approach. This test does not judge the quality or accuracy of the documentation, nor does it test how thoroughly the product implements SCAP.

SCAP.T.20.2: The tester shall verify that the provided documentation is an English language document consisting of 150 to 500 words.

SCAP.R.30: 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.

Required Vendor Information

SCAP.V.30.1: The vendor shall indicate which one or more of the defined SCAP capabilities their product is being tested for.

Required Test Procedures

SCAP.T.30.1: The tester shall ensure that all tests associated with the asserted SCAP capabilities of the product are conducted.

SCAP.T.30.2: 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, Authenticated Vulnerability Scanner).

3.2 SCAP Source Data Stream Processing

This section addresses the SCAP source data stream processing requirements. The SCAP Data streams that SCAP Validated Products need to support are enumerated in the following table:

Check System	Profile	Benchmark	Data Stream
OVAL	NONE	XCCDF Benchmark	SCAP Data Stream
OVAL	One	XCCDF Benchmarks	Scap Data Stream Collection
OCIL	NONE	XCCDF Benchmarks	SCAP Data Stream
OCIL	One	XCCDF Benchmark	Scap Data Stream Collection
Unsupported	Multiple	XCCDF Benchmark	SCAP Data Stream
Unsupported	NONE	XCCDF Benchmarks	Scap Data Stream Collection
Patches-Up-To-Date	Multiple	XCCDF Benchmarks	Scap Data Stream Collection
Patches-Up-To-Date	One	XCCDF Benchmark	SCAP Data Stream
OVAL and Patches-Up-To-Date	NONE	XCCDF Benchmark	Scap Data Stream Collection
OVAL and Patches-Up-To-Date	One	XCCDF Benchmarks	SCAP Data Stream
OVAL and OCIL	Multiple	XCCDF Benchmark	Scap Data Stream Collection
OVAL and OCIL	NONE	XCCDF Benchmarks	SCAP Data Stream
OVAL and OCIL and Patches-Up-To-Date	Multiple	XCCDF Benchmarks	SCAP Data Stream
OVAL and OCIL and Patches-Up-To-Date	NONE	XCCDF Benchmark	Scap Data Stream Collection
OVAL and OCIL and Unsupported	One	XCCDF Benchmark	SCAP Data Stream
OVAL and OCIL and Unsupported	Multiple	XCCDF Benchmarks	Scap Data Stream Collection
OVAL and OCIL and Patches-Up-To-Date and Unsupported	One	XCCDF Benchmarks	Scap Data Stream Collection
OVAL and OCIL and Patches-Up-To-Date and Unsupported	Multiple	XCCDF Benchmark	SCAP Data Stream
OVAL	Multiple	XCCDF Benchmark	Scap Data Stream Collection
OCIL	Multiple	XCCDF Benchmarks	SCAP Data Stream
Unsupported	One	XCCDF Benchmark	~CAP Data Stream
Patches-Up-To-Date	NONE	XCCDF Benchmark	Scap Data Stream Collection
OVAL and Patches-Up-To-Date	Multiple	XCCDF Benchmarks	SCAP Data Stream
OVAL and OCIL	One	XCCDF Benchmarks	Scap Data Stream Collection
OVAL and OCIL and Patches-Up-To-Date	One	XCCDF Benchmark	SCAP Data Stream
OVAL and OCIL and Unsupported	NONE	XCCDF Benchmarks	SCAP Data Stream
OVAL and OCIL and Patches-Up-To-Date and Unsupported	NONE	XCCDF Benchmark	Scap Data Stream Collection

SCAP.R.100: The product shall be able to import an SCAP source data stream for the target platform and correctly load the included Rules and their associated Check System Definitions on a target system rejecting any invalid content.

Required Vendor Information

SCAP.V.100: The vendor shall provide documentation and instruction on how to import an SCAP source data stream for the target platform.

Required Test Procedures

SCAP.T.100.1: The tester shall import valid SCAP source data streams for the target platform into the vendor product and execute them on a target system. Results of the scan shall be visually compared to the results from the NIST reference implementation to validate that the results match.

SCAP.R.101: The product shall be able to select a specific SCAP source data stream when processing a SCAP data stream collection.

Required Vendor Information

SCAP.V.101: The vendor shall provide documentation and instruction on how to select a specific data stream (by ID) when running a SCAP data stream collection.

Required Test Procedures

SCAP.T.101.1: The tester shall validate the vendor product can selectively choose and apply a specific valid SCAP data stream.

SCAP.R.102: 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.

Required Vendor Information

SCAP.V.102: The vendor shall provide documentation and instruction on how to select a specific XCCDF benchmark (by ID) when processing a SCAP data stream or data stream collection.

Required Test Procedures

SCAP.T.102.1: The tester shall validate the vendor product can selectively choose and apply a specific valid XCCDF benchmark.

SCAP.R.103: 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.

Required Vendor Information

SCAP.V.103: The vendor shall provide documentation and instruction on how to select a specific XCCDF profile (by ID) when processing a SCAP data stream or data stream collection.

Required Test Procedures

SCAP.T.103.1: The tester shall validate the vendor product can selectively choose and apply a specific valid XCCDF profile (by ID).

SCAP.R.104: The product shall enable the user to import (signed and unsigned) SCAP source data streams

Required Vendor Information

SCAP.V.104: 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.104.1: The tester shall verify that the product documentation includes instructions on how the end user can import an SCAP source data stream.

SCAP.T.104.2: The tester shall import a valid SCAP source data stream into the vendor product and ensure that the imported content is available for execution.

SCAP.R.105: The product shall recognize and reject SCAP source data streams that have invalid signatures.

Required Vendor Information

SCAP.V.105: 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.105.1: The tester shall verify that the product documentation includes instructions on how the end user can import an SCAP source data stream.

SCAP.T.105.2: The tester shall validate the vendor product can correctly process a data stream with a valid signature.

SCAP.T.105.3: The tester shall validate that the vendor product correctly identifies and reports an error when processing a data stream with an invalid signature.

SCAP.R.106: The product shall recognize and reject SCAP source data streams that have signatures based on invalid certificates.

Required Vendor Information

SCAP.V.106: 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.106.1: The tester shall verify that the product documentation includes instructions on how the end user can import an SCAP source data stream.

SCAP.T.106.2: The tester shall validate that the vendor product correctly identifies and reports an error when processing a data stream with a signature based on an invalid certificate.

SCAP.T.106.3: 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.107: The product SHALL be able to correctly import all earlier versions of SCAP content.

Required Vendor Information

SCAP.V.107: The vendor shall provide documentation explaining how earlier versions of SCAP content can be imported into the product.

Required Test Procedures

SCAP.T.107.1: Using the vendor product, the tester shall execute a valid SCAP source data stream with CCE compliance mapping information and view the resultant output to ensure that the CCE compliance mappings are correct.

SCAP.R.108: The product shall be able to determine the validity of imported SCAP source data stream by evaluating the associated OVAL definition for the CPE Name on an XCCDF <Benchmark>, <Group>, or <Rule> and verifying that the associated XCCDF content applies to the target system.

Required Vendor Information

SCAP.V.108: The vendor shall provide instructions on how the product indicates the validity 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 valid for a target platform. This requirement is testing the use of the OVAL check associated with a CPE name via the CPE dictionary to determine applicability of the data stream.

Required Test Procedures

SCAP.T.108.1: The tester shall import an SCAP source data stream into the tool that contains a CPE Name 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.R.109: The product shall report and optionally reject OVAL content that is part of an SCAP source data stream that is invalid according to the OVAL XML schemas and schematron stylesheets[9].

Required Vendor Information

SCAP.V.109: The vendor shall provide instructions on how validation of OVAL content that is part of a SCAP data stream is performed and where errors from validation will be displayed within the product output.

Required Test Procedures

SCAP.T.109.1: The tester shall attempt to import known invalid OVAL Definition content that is part of a SCAP data stream into the vendor product and examine the product output to validate that the product reports and optionally rejects the content as invalid according to the OVAL Definition schema and schematron stylesheets.

SCAP.R.110: The product shall report and optionally reject OCIL content that is invalid according to the OCIL XML schema.

Required Vendor Information

SCAP.V.110: 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

[9] This does not imply that the product being tested MUST use schematron; the product need only produce the same results as the schematron implementation.

SCAP.T.110.1: 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 and optionally rejects the content as invalid according to the OCIL XML schema.

3.3 SCAP Correctness Requirements

This section addresses those requirements that will assess products ability to correctly process SCAP content.

SCAP.R.1000: The product shall be able to correctly assess the target systems using the Tier IV source data streams as input.

Required Vendor Information

SCAP.V.1000: The vendor shall provide instructions on how to execute the previously imported valid Tier IV SCAP source data streams.

Required Test Procedures

Per vendor instruction in SCAP.V.1000, the lab will 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.

The following Tier IV source data streams will be used for each of the following tests:

- Windows Family
  - Windows XP
  - Windows XP Firewall
  - Windows Vista
  - Windows Vista Firewall
  - Internet Explorer 7
  - Windows 7
  - Windows 7 Firewall
  - Internet Explorer 8
- Red Hat Family
  - Red Hat Enterprise Linux (RHEL) 5 Desktop

These source data streams are found in the official National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

SCAP.T.1000.1: 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 results produced by the reference implementation to ensure that they match.

SCAP.R.1100: If the vendor product requires a specific configuration of the target platform that is not in compliance with the Tier IV content, the vendor shall provide documentation indicating which settings must be changed and a rationale for each changed setting. Products should only require changes to the target platform so that it can function correctly.

NOTE: ***Pursuant to OMB Memorandum 07-18:[10] "The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC)." Products undergoing SCAP validation are also required by OMB to make this self-assertion and that listing their non-complaint settings for FDCC.R.3 in no way negates the OMB M-07-18 requirement.***

Required Vendor Information

SCAP.V.1100: The vendor shall provide an English language document to the lab that indicates which settings must be changed 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 must contain only information that is to be publicly released.

Required Test Procedures

SCAP.T.1100.1: The tester shall review the provided documentation to ensure that each indicated setting includes an associated rationale.

SCAP**.R.1200: The product shall be able to process the content that is representative of content published at the Tier III and the OVAL repository which is associated with the platform family for which validation is being sought.**

Required Vendor Information

SCAP.V.1200: The vendor shall provide instructions on how to execute a previously imported valid representative data stream for a platform family.

Required Test Procedures

Per vendor instruction in SCAP.V.1000, the lab will establish the environment on a target platform.

SCAP.T.1200.1: The tester shall evaluate a Tier IV compliant target platforms, validate results produced with SCAPVAL, and compare results against those produced by the reference implementation.

SCAP.R.1200: The product shall be able to determine the validity of imported SCAP source data stream by evaluating the associated OVAL definition and/or OCIL questionnaire for the CPE Name on an XCCDF <Benchmark>, <Group>, or <Rule> and verifying that the associated XCCDF content applies to the target system.

Required Vendor Information

SCAP.V.1200: The vendor shall provide instructions on how the product indicates the validity of the imported SCAP source data stream to a target platform. Instructions should also describe how

[10] http://www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf

the imported data stream is indicated to not be valid for a target platform. This requirement is testing the use of the OVAL check associated and OCIL questionnaire with a CPE name via the CPE dictionary 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 tool that contains a CPE Name and related OVAL definition and OCIL questionnaire not applicable for the target system. The tester shall verify that the product declines to execute the non-applicable tests.

SCAP.R.1300: The product shall be able to correctly evaluate a valid OVAL Definition file, where the contents of the OVAL definition file are consistent with the normative guidance[11] 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 expressed as Single Machine Without System Characteristics, Single Machine With System Characteristics, or Single Machine With Thin Results

Required Vendor Information

SCAP.V.1300: The vendor shall provide instructions on how a valid OVAL Definitions 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.

For SCAP.T.1300.5, the vendor shall indicate how two or more values can be specified for a variable used by one OVAL Definition.

Required Test Procedure

SCAP.T.1300.1: The tester shall run the tool using valid OVAL Definitions files against the target systems of the target platform type. The results shall compare against results from NIST reference implementation and they MUST produce the same true/false result for each OVAL definition and criteria contained within the definition.

SCAP.T.1300.2: The tester shall validate the resulting OVAL XML Full Results by importing the result set into the SCAPVAL utility and check for any validation errors.

SCAP.T.1300.3: The tester shall validate that the resulting OVAL XML Full Results are available for viewing by the user.

SCAP.T.1300.4: The tester shall capture the successful results of the import and comparison for the final validation

SCAP.T.5.1300.1: 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.

SCAP.R.1350: The product shall be able to correctly evaluate a valid OVAL Definition file that is part of a SCAP data stream, where the contents of the OVAL definition file are consistent with the normative guidance[12] 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 expressed as

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

Single Machine Without System Characteristics, Single Machine With System Characteristics, or Single Machine With Thin Results

Required Vendor Information

SCAP.V.1350: 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.

For SCAP.T.1350.5, the vendor shall indicate how two or more values can be specified for a variable used by one OVAL Definition.

Required Test Procedure

SCAP.T.1350.1: The tester shall run the tool using valid SCAP data stream against the target systems of the target platform type. The results shall compare against results from NIST reference implementation and they MUST produce the same true/false result for each OVAL definition and criteria contained within the definition.

SCAP.T.1350.2: The tester shall validate the resulting SCAP data stream by importing them into the SCAPVAL any validation errors.

SCAP.T.1350.3: The tester shall validate that the resulting SCAP data stream are available for viewing by the user.

SCAP.T.1350.4: The tester shall capture the successful results of the import and comparison for the final validation

SCAP.T.1350.4.1: 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.

SCAP.R.1400: The product shall be able to correctly evaluate a valid OCIL Questionnaire file 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. If the product does not implement OCIL it MUST produce results that indicate the test was not checked

Required Vendor Information

SCAP.V.1400: 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

OCIL.T.1400.1: The tester shall run the tool using valid OCIL Definitions files against the target systems of the target platform type. The results shall be compared against results from NIST reference implementation and they must produce the same true/false result for each OCIL definition and criteria contained within the definition.

OCIL.T.1400.2: The tester shall validate the resulting OCIL Output file by importing into SCAPVAL without any errors.

OCIL.T.1400.3: The tester shall validate that the resulting OCIL Output file is available for viewing by the user.

SCAP.R.1450: The product shall be able to correctly evaluate a valid OCIL Questionnaire file that is part of a 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. If the product does not implement OCIL it MUST produce results that indicate the test was not checked

Required Vendor Information

SCAP.V.1450: The vendor shall provide instructions on how a valid OCIL Questionnaire file that is part of a 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

OCIL.T.1450.1: The tester shall run the tool using valid SCAP data stream files against the target systems of the target platform type. The results shall be compared against results from NIST reference implementation and they must produce the same true/false result for each OCIL definition and criteria contained within the definition.

OCIL.T.1450.2: The tester shall validate the resulting SCAP data stream by importing into SCAPVAL without any errors.

OCIL.T.1450.3: The tester shall validate that the resulting SCAP data stream is available for viewing by the user.

SCAP.R.1500: 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).

Required Vendor Information

SCAP.V.1500: None.

Required Test Procedures

SCAP.T.1500.1: Using the product output from SCAP.R.2700, 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 or equal to 10 and less than or equal to 30 of the total configuration issue items with CCE IDs,. The tester does not need to rigorously prove that the vendor's configuration issue description matches the official CCE description, but merely needs to identify that the two appear to be same. This test ensures that the product correctly maps to CCE, but does not test for completeness of the mapping.

SCAP.R.1600: 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).

Required Vendor Information

SCAP.V.1600: None.

Required Test Procedures

SCAP.T.1600.1: Using the list of configuration issue items produced in SCAP.R.2700, 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.1700: 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.

Required Vendor Information

CPE.V.1700.1: 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 2.1.

CPE.V.1700.2: 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

CPE.T.1700.1: The tester shall compare the vendor-provided list of CPE Names for comparison against the official CPE Dictionary[13]. The tester shall verify that all exceptions found match the list of exceptions provided by the vendor.

SCAP.R.1710: 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 Section 4.3.1 of NIST SP800-126R2

Required Vendor Information

SCAP.V.1710**:** The vendor shall provide instructions import an SCAP source data stream that contains references to CPEs in an <xccdf:platform> element directly or by a <cpe2:fact-ref>

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

contained within a referenced <cpe2:platform-specification> element and have it applied against a known platform. The vendor shall also provide instructions how to view the results of the application of the content against the platform.

Required Test Procedures

SCAP.T.1710.1: The tester shall import the known content into the tool and apply it against a known platform.

SCAP.T.1710.2. The tester shall import the results of the content into SCAPVAL without any errors.

SCAP.T.1710.3. The tester shall compare the results against those produced by the NIST reference implementation to ensure the same results were produced.

SCAP.R.1800: The product shall indicate the correct CVE ID 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).

Required Vendor Information

SCAP.V.1800: None

Required Test Procedures

SCAP.T.1800.1: Using the product output from SCAP.R.2950 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.

SCAP.R.1810: 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).

Required Vendor Information

SCAP.V.1810: None.

Required Test Procedures

SCAP.T.1810.1: Using the list of software flaws and/or patch definitions produced in SCAP.R.2950, 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.

3.4 SCAP Result(s) Data Stream

This section addresses those requirements that assess a products ability to produce validate SCAP results.

SCAP.R.2000: SCAP result data streams shall be produced by the product in compliance with the SCAP result data streams as specified in NIST SP800-126R2.

Required Vendor Information

SCAP.V.2000: The vendor shall provide instruction on where the corresponding XCCDF and OVAL results files can be located for inspection.

Required Test Procedures

SCAP.T.2000.1: The tester shall visually inspect XCCDF and OVAL results to verify that they are valid according to the associated specification for each. The output MUST be processed by SCAPVAL with errors and/or warnings. The output is also compared to the results from the NIST reference implementation to verify completeness and accuracy of SCAP results.

SCAP.R.2100: The product shall be able to process XCCDF components that are part of an SCAP source data stream and generate XCCDF component results within a SCAP result data stream in accordance with the XCCDF specification for the target platform.

Required Vendor Information

SCAP.V.2100: 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.2100.1: The tester shall import a known valid XCCDF component content that is part of SCAP data streams for the target platform into the vendor tool and execute it according to the product operation instructions provided by the vendor. The tester will inspect the product output to validate that it includes the same checks and uses the same check parameters as that produced by the NIST reference implementation.

SCAP.T.2100.2: The tester shall validate the resulting XCCDF component results with in a SCAP result data stream output using the SCAPVAL. This validation must not produce any validation errors.

SCAP.T.2100.3: The tester shall compare the product results to those produced by the NIST reference implementation to ensure that the pass/fail results match for each Rule.

SCAP.R.2200: 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.

Required Vendor Information

SCAP.V.2000: 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.2200: The tester shall visually inspect a non-vendor-directed sample of 10% of the XCCDF Rules, up to a total 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.2300: The product output shall enable users to view the XML OCIL Questionnaires being consumed by the tool (e.g., within the product user interface or through an XML dump of the OCIL questionnaires to a file).

Required Vendor Information

SCAP.V.2300: 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.2300.1: 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.2400: The product shall be able to produce NOT-CHECKED results for unsupported Check Systems

Required Vendor Information

SCAP.V.2400: The vendor shall provide instructions on how to import SCAP source data streams containing XCCDF component content for execution and provide instructions on where the SCAP result data streams with 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.2400.1 The tester shall import a known valid SCAP source data streams containing XCCDF component content for the target platform into the vendor tool and execute it according to the product operation instructions provided by the vendor. The tester will inspect the product output to validate that it includes the same checks and uses the same check parameters as that produced by the NIST reference implementation.

SCAP.T.2400.2: The tester shall validate the SCAP result data streams containing XCCDF component content output using SCAPVAL. This validation MUST not produce any validation errors.

SCAP.T.2400.3: The tester shall compare the product results to those produced by the NIST reference implementation to ensure that the pass/fail results match for each Rule.

SCAP.R.2500: The product output shall enable users to view the XML OVAL Definitions being consumed by the tool (e.g., within the product user interface or through an XML dump of the OVAL definitions to a file).

Required Vendor Information

SCAP.V.2500: 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.2500.1: 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.2600: 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

Required Vendor Information

SCAP.V.2600: 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.2600.1: The tester shall visually inspect the product output for the dates of all static or bundled SCAP data included with the vendor product.

SCAP.R.2700: The product shall display the associated CCE ID for each configuration issue definition in the product output (i.e., the product displays CCE IDs).

Required Vendor Information

SCAP.V.2700: The vendor shall provide instructions on how product output can be generated that contains a listing of all security configuration issue items both with and without CCE IDs. 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.2700.1: 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.2750: The product shall provide a means to view the CCE Description for each displayed CCE ID within the product output.

Required Vendor Information

SCAP.V.2750: The vendor shall provide instructions noting where the CCE ID can be located within the product output. The vendor shall provide procedures and a test environment (if necessary) so that the product will output configuration issues with associated CCE IDs.

Required Test Procedures

SCAP.T.2750.1: The tester shall inspect the CCE IDs from the product output and verify that the official CCE Description[14] is available and correct. The vendor may provide additional CCE descriptions and information and should not be penalized for doing so. The tester shall perform this using a non-vendor-directed set of 10% of the total CCE IDs available in the product output, up to a maximum of 30.

SCAP.R.2775: A product's machine-readable output must provide the CPE naming data using CPE names.

Required Vendor Information

SCAP.V.2775: 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.2775.1: 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 up to 30 vendor and product names in the product output that are also included in the official CPE Dictionary.

SCAP.R.2800: The product shall allow users to locate configuration issue items using CCE IDs.

Required Vendor Information

SCAP.V.2800: The vendor shall provide documentation (printed or electronic) indicating how security configuration issue items can be located using CCE IDs.

Required Test Procedures

SCAP.T.2800.1: The tester shall verify that security configuration issue items can be located 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.2850: The product SHALL be able to correctly produce the Asset Identification Fields as specified in NIST SP800-126R2 when assessing a target.

Required Vendor Information

SCAP.V.2850 The vendor shall provide documentation on how to import a SCAP data stream and how to apply it to a target system.

[14] The official CCE descriptions are found at http://cce.mitre.org/lists/cce_list.html.

Required Test Procedures

SCAP.T.2850.1: The tester shall import the SCAP source data stream and apply it to a known target producing a SCAP result data stream

SCAP.T.2850.2: The tester shall validate the results produced using SCAPVAL, the validation MUST not produce any errors

SCAP.T.2850: The tester shall visually inspect the results to ensure that the Asset Identification Fields are what is expected.

SCAP.R.2875: The product SHALL be able to correctly produce an ARF report object for each XCCDF, OVAL, and OCIL component.

Required Vendor Information

SCAP.V.2875.1: The vendor shall supply documentation how to import an SCAP data stream, apply it against a target and produce a SCAP result data stream

Required Test Procedures

SCAP.T.2875.1: The tester shall import the SCAP source data stream and apply it to a known target producing a SCAP result data stream

SCAP.T.2875.2: The tester shall validate the results produced using SCAPVAL, the validation MUST not produce any errors

SCAP.T.2875.3: The tester shall compare the results against those produced by the NIST reference implementation to ensure they are equivalent.

SCAP.R.2890: The product shall provide a means to view the CVE Description and CVE references for each displayed CVE ID[15] within the product output.

Required Vendor Information

SCAP.V.2890: The vendor shall provide instructions on the 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.

Required Test Procedures

SCAP.T.2890.1: The tester shall select a non-vendor-directed sampling of CVE IDs from within the available forms of the product output. The tester shall determine that the product output enables the user to view, at minimum, the official CVE description and references.[16] The vendor may provide additional CVE descriptions and information and should not be penalized for doing

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

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

so. The tester shall perform this using a non-vendor-directed sample comprised of greater or equal to 10 and less than or equal to 30of the total CVE IDs available in the product output.

SCAP.R.2900: 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.

Required Vendor Information

SCAP.V.2900: 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.2900.1: 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.2950: 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. [17]

Required Vendor Information

SCAP.V.2950: 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 both with and without CVE IDs. 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.2950.1: The tester shall visually inspect, within the product output, a non-vendor-selected sample comprised of greater 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.2975: If the product uses CVE, it shall include NVD CVSS base scores and vector strings for each CVE ID referenced in the product.

Required Vendor Information

SCAP.V.2975: The vendor shall provide documentation explaining where the NVD CVSS base scores and vector strings can be located with the corresponding CVE ID.[18] The vendor may optionally provide the tester information on how the product can be updated with new NVD CVSS base scores and vector strings prior to testing.

Required Test Procedure

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

[18] A link to the information on the NVD web site is sufficient for this test.

SCAP.T.2975.1: 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.2990: When processing SCAP source data streams that contain compliance mappings to included CCEs, the product shall output the compliance mappings.

Required Vendor Information

SCAP.V.2990: The vendor shall provide documentation explaining where CCE compliance mappings can be viewed within the product output.

Required Test Procedures

SCAP.T.2990.1: Using the vendor product, the tester shall execute a valid SCAP source data stream with CCE compliance mapping information and view the resultant output to ensure that the CCE compliance mappings are correct.

4. Derived Test Requirements for Specific Capabilities

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

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

The following chart summarizes the required *SCAP* components for each SCAP capability together with the specific requirements necessary to achieve SCAP validation.

Table 6-1. Required SCAP Components for Each SCAP Capability

Requirement ID	Authenticated Configuration Scanner	Authenticated Vulnerability and Patch Scanner
SCAP.R.10	X	X
SCAP.R.20	X	X
SCAP.R.30	X	X
SCAP.R.100	X	X
SCAP.R.101	X	X
SCAP.R.102	X	X
SCAP.R.103	X	X
SCAP.R.104	X	X
SCAP.R.105	X	X
SCAP.R.106	X	X
SCAP.R.107	X	X
SCAP.R.108	X	X
SCAP.R.109	X	X
SCAP.R.110	X	X
SCAP.R.1000	X	
SCAP.R.1100	X	
SCAP.R.1200	X	X
SCAP.R.1300	X	X
SCAP.R.1350	X	X
SCAP.R.1400	X	X
SCAP.R.1450	X	X

Requirement ID	Authenticated Configuration Scanner	Authenticated Vulnerability and Patch Scanner
SCAP.R.1500	X	X
SCAP.R.1600	X	
SCAP.R.1700	X	X
SCAP.R.1710	X	X
SCAP.R.1800	X	X
SCAP.R.1810	X	X
SCAP.R.2000	X	X
SCAP.R.2100	X	X
SCAP.R.2200	X	
SCAP.R.2300	X	X
SCAP.R.2400	X	X
SCAP.R.2500	X	X
SCAP.R.2600	X	X
SCAP.R.2700	X	
SCAP.R.2750	X	
SCAP.R.2775	X	
SCAP.R.2800	X	
SCAP.R.2850	X	X
SCAP.R.2875	X	X
SCAP.R.2890	X	X
SCAP.R.2900	X	X
SCAP.R.2950	X	X
SCAP.R.2975	X	X
SCAP.R.2990	X	

5. Appendix A—Acronyms and Abbreviations

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

AI	Asset Identification
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 Requirements
FDCC	Federal Desktop Core Configuration
FIRST	Forum of Incident Response and Security Teams
ID	Identifier
IETF	Internet Engineering Task Force
IR	Interagency Report
IT	Information Technology
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NCP	National Checklist Program
NVD	National Vulnerability Database
NVLAP	National Voluntary Laboratory Accreditation Program
OCIL	Open Checklist Interactive Language
OMB	Office of Management and Budget
OS	Operating System
OVAL	Open Vulnerability and Assessment Language
PDF	Portable Document Format
RHEL	Red Hat Enterprise Linux
RFC	Request for Comment
SCAP	Security Content Automation Protocol
SCAPVAL	SCAP Validation tool
TMSAD	Trust Model for Security Automation Data
U.S.	United States
USGCB	United States Government Configuration Baseline
XCCDF	Extensible Configuration Checklist Document Format
XML	Extensible Markup Language