NIST Special Publication 800
NIST SP 800-126Ar4

SCAP 1.4 Component Specification Version Updates

An Annex to NIST SP 800-126r4

Dragos Prisaca
Stephen Quinn

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-126Ar4

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 800
NIST SP 800-126Ar4

SCAP 1.4 Component Specification Version Updates

An Annex to NIST SP 800-126r4

Dragos Prisaca
Stephen Quinn
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-126Ar4

June 2026

U.S. Department of Commerce
Howard Lutnick, Secretary of Commerce

National Institute of Standards and Technology
Arvind Raman, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified 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. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority
This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2026-04-23

How to Cite this NIST Technical Series Publication
Prisaca D, Quinn SD (2026) SCAP 1.4 Component Specification Version Updates: An Annex to NIST SP 800-126r4. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-126Ar4. https://doi.org/10.6028/NIST.SP.800-126Ar4

Author ORCID iDs
Dragos Prisaca: 0009-0007-7361-8433
Stephen Quinn: 0000-0003-1436-684X

Contact Information
scap@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/126/a/r4/final, including related content, potential updates, and document history.

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

Abstract

The Security Content Automation Protocol (SCAP) is a multi-purpose framework of component specifications that support automated configuration, vulnerability, patch checking, security measurement, and technical control compliance activities. The SCAP version 1.4 specification is defined by the combination of NIST SP 800-126r4, a set of schemas, and this document. This document allows the use of specific minor version updates to SCAP 1.4 component specifications and particular Open Vulnerability and Assessment Language (OVAL) schema versions to provide additional functionality for SCAP 1.4 without causing any loss of existing functionality.

Keywords

eXtensible Configuration Checklist Description Format (XCCDF); Open Vulnerability and Assessment Language (OVAL); security automation; security configuration; Security Content Automation Protocol (SCAP).

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. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Tables

1. Introduction

Specification versioning is the process of denoting a revision to a specification by changing its version number. For example, the Security Content Automation Protocol (SCAP) specification documents are occasionally updated, and these updates trigger an increase in the SCAP version number (e.g., 1.2, 1.3, 1.4). This specification versioning is challenging because there is no standard convention or terminology for it; each specification imparts different meanings into its version numbers. For example, moving from version 3.4 to version 3.5 might break backward compatibility for one specification, add new functionality for another specification, and simply correct an error in a third specification.

This document defines two key terms for SCAP 1.4 component specification versioning: major and minor version updates. A *major version update* is a revision of a specification that breaks backward compatibility with the previous revision of the specification in numerous significant ways. A *minor version update* is a revision of a specification that may add or enhance functionality, fix bugs, and make other changes from the previous revision, but the changes have minimal impact, if any, on backward compatibility.

1.1. Purpose and Scope

The purpose of this document is to extend the contents of NIST Special Publication (SP) 800-126r4 (Revision 4) so that SCAP 1.4 is defined by the combination of the two documents and the set of schemas. Readers should be familiar with SP 800-126r4 before reading this document.

This document can be used to make approved version updates - both minor and major - to component specifications that are already included in SCAP 1.4 by SP 800-126r4. Approved major-version updates SHALL be limited to those explicitly listed in sect. 2.2 of this document; all other major-version changes, and any new component specifications that are not included in SP 800-126r4, SHALL be deferred to a future version of SCAP as documented in a future revision of SP 800-126.

Each SCAP 1.4 extension specified in this document takes one of two forms. First, it may allow the use of particular version updates to SCAP 1.4 component specifications - including minor version updates, explicitly approved major-version updates, or particular Open Vulnerability and Assessment Language (OVAL) versions included in SCAP 1.4. Second, it may specify one or more requirements for using these updates or OVAL schemas in an SCAP 1.4-conformant manner.

This document specifies exactly which component specification version updates and OVAL platform schema versions may be used as part of SCAP 1.4 for several reasons, including:

- To support the interoperability of SCAP 1.4 tools and content
- To provide a basis for testing tools to ensure that they comply with SCAP 1.4

- To reduce the burden on SCAP 1.4 tool and content developers by clearly defining all SCAP 1.4 extensions in a single place

While organizations are free to use SCAP 1.4 with any schema or specification that they choose in any manner they choose, such usage is not considered to be SCAP 1.4-conformant unless defined as such in this document or in SP 800-126r4.

The scope of this document is versioning for SCAP 1.4 component specifications only.

1.2. Document Structure

The rest of this document consists of the following sections and appendices:

- Section 2 presents all minor version updates in SCAP 1.4 component specifications that have been approved for inclusion in SCAP 1.4 along with any corresponding requirements to be added to SCAP 1.4. This section also lists the criteria used to evaluate a minor version update for potential inclusion in SCAP 1.4.
- Section 3 describes the management processes for the document.
- Appendix A lists the acronyms and abbreviations used in the document.
- Appendix B provides a glossary of selected terms in this document.
- Appendix C lists key changes made in this revision.

2. Minor Version Updates in SCAP 1.4-Component Specifications

This section defines the criteria used to evaluate minor version updates in SCAP 1.4 component specifications for potential inclusion in SCAP 1.4 and lists all such updates that have been approved for inclusion in SCAP 1.4 along with any additional corresponding requirements. It also provides the current XML schema (XSD) and Schematron schema locations that correspond to all SCAP 1.4 component specifications.

2.1. Criteria for Potential Inclusion

The following defines the criteria that a minor version update to an SCAP 1.4 component specification and associated requirements must meet before being considered for potential inclusion in this document:

1. One or more of the following must be true:
    a. The component specification is being revised strictly for bug fixes or errata purposes. In other words, the update does not add new functionality or enhance existing functionality.
    b. The new minor version of the component specification is already being used by tools and/or content.
    c. The platform schema revision or component specification revision provides significant benefits, such as a solution for an important use case that previously had no solution.
2. The minor version update and associated requirements must not conflict with any existing SCAP 1.4 requirements, including minimizing any negative impact on backward compatibility.

2.2. Approved Component Specification Version Updates and SCAP 1.4 Requirements

The following SCAP 1.4 component specification version updates have been approved for inclusion in SCAP 1.4:

- OVAL 5.12.x - minor version update to the OVAL component schema. See sect 2.3 for schema location.
- CVSS v3.1 and v4.0 - version policy update to the CVSS scoring component. SCAP 1.4 supersedes the prior "CVSS v3" requirement (which was ambiguous between v3.0 and v3.1) by pinning the v3 floor to CVSS v3.1 [CVSS-3.1] and additionally authorizing CVSS v4.0 [CVSS-4.0]. CVSS v3.0 [CVSS-3.0] and CVSS v2.0 [CVSS-2.0] are retained as legacy versions for pre-existing vulnerability data only, scoped to NVD's version-cut off dates of 10 September 2019 (v3.0) and 13 July 2022 (v2.0). The full version-precedence rule and the legacy-data scope are normative in sect. 3.8 of SP 800-126r4 and are not duplicated here. CVSS does not have an XML schema location and therefore does not appear in sect. 2.3.

2.3. XML Schema and Schematron Schema Locations

For all other component specifications, the versions listed in SP 800-126r4 are the approved versions. As of this writing, the requirements added to SCAP 1.4 to support the approved component specification version updates are limited to those described above and to the normative text in sect. 3.8 of SP 800-126r4 (CVSS version precedence) and sect. 3.x of SP 800-126r4 (OVAL 5.12.x adoption).

Table 1 lists the XML schema (XSD) locations (and Schematron schema locations, when applicable) for the SCAP component specifications.

Table 1. SCAP XML schema and Schematron schema locations

Prefix	XML Schema Location	Schematron Schema Location (if applicable)[1]
AI	https://csrc.nist.gov/schema/asset-identification/1.1/asset-identification_1.1.0.xsd	
ARF	https://csrc.nist.gov/schema/asset-reporting-format/1.1/asset-reporting-format_1.1.0.xsd	Embedded in the schema
CPE Applicability Language	https://csrc.nist.gov/schema/cpe/2.3/cpe-language_2.3.xsd	
CPE Dictionary	https://csrc.nist.gov/schema/cpe/2.3/cpe-dictionary_2.3.xsd	
CPE Dictionary Extension	https://csrc.nist.gov/schema/cpe/2.3/cpe-dictionary-extension_2.3.xsd	
CPE Naming	https://csrc.nist.gov/schema/cpe/2.3/cpe-naming_2.3.xsd	
OCIL	https://csrc.nist.gov/schema/ocil/2.0/ocil-2.0.xsd	Embedded in the schema
OVAL 5.12.3 Schemas	https://github.com/OVAL-Community/OVAL/releases/tag/v5.12.3	Embedded in the schema
SCAP constructs	https://scap.nist.gov/schema/scap/1.4/scap-constructs_1.4.xsd	
SCAP source data stream	https://csrc.nist.gov/schema/scap/1.4/scap-source-data-stream_1.4.xsd	https://csrc.nist.gov/projects/security-content-automation-protocol/scap-releases/scap-1-4/scap-1-4-schematron-rules
TMSAD	https://csrc.nist.gov/schema/tmsad/1.0/tmsad_1.0.xsd	https://csrc.nist.gov/schema/tmsad/1.0/tmsad_1.0.sch
XCCDF	https://csrc.nist.gov/schema/xccdf/1.2/xccdf_1.2.xsd (XSD 1.0, where xsd:import statements use absolute URLs), https://csrc.nist.gov/schema/xccdf/1.2/xccdf_1.2.zip (complete schema bundle, where xsd:import statements use relative URLs)	https://csrc.nist.gov/schema/xccdf/1.2/xccdf_1.2.sch

[1] A complete bundle of Schematron schemas for SCAP 1.4 can be found on the SCAP website at https://csrc.nist.gov/projects/security-content-automation-protocol/scap-releases/scap-1-4/scap-1-4-schematron-rules.

3. Document Management

3.1. Composition

As stated in Sec. 1, the SCAP 1.4 specification comprises (a) SP 800-126r4 (i.e., the core specification), (b) this annex (i.e., the extensions document), and (c) the normative component schemas referenced by these documents.

3.2. Rationale

Maintaining this extensions document separate from the core specification enables extensions to be published or revised without republishing SP 800-126r4 and provides a single, consolidated catalogue of extensions for tool developers and content authors.

3.3. Update Cadence

The SCAP community's adoption of extensions will be driven by community needs, feedback, major platform changes, and related trends. The extensions document MAY be updated more frequently than SP 800-126r4, but the overall update cadence for both documents is expected to be infrequent.

3.4. Conformance and Assessment

NIST no longer operates the SCAP Validation Program. The National Voluntary Laboratory Accreditation Program (NVLAP) has terminated SCAP testing accreditation effective September 2, 2025. Accordingly, this specification does not anticipate revisions to NIST Interagency Report (IR) 7511 for SCAP 1.4. Organizations that develop independent conformance or interoperability assessments that are derived from this specification SHOULD cite the specific versions of SP 800-126r4, this extensions document, and the referenced component schemas from which their test requirements are derived.

Appendix A. List of Symbols, Abbreviations, and Acronyms

Selected acronyms and abbreviations used in this document are defined below.

DTR
Derived Test Requirements

FOIA
Freedom of Information Act

IETF
Internet Engineering Task Force

IR
Interagency Report

ITL
Information Technology Laboratory

NIST
National Institute of Standards and Technology

OVAL
Open Vulnerability and Assessment Language

SCAP
Security Content Automation Protocol

SP
Special Publication

Appendix B. Glossary

Selected terms used in this document are defined below. See the glossary in SP 800-126r4 for additional definitions.

major version update
A revision of a specification that breaks backward compatibility with the previous revision of the specification in numerous significant ways.

minor version update
A revision of a specification that may add or enhance functionality, fix bugs, and make other changes from the previous revision, but the changes have minimal impact, if any, on backward compatibility.

specification versioning
The process of denoting a revision to a specification by changing its version number.

Appendix C. Change Log

Revision 4 Release 1 – TBD

- Updated all references of SCAP 1.3 to SCAP 1.4
- Updated OVAL version to 5.12.3
- Removed OVAL ‘core’ and ‘platform’ schema version information
- Removed SWID requirements