

Security Content Automation Protocol (SCAP)

SCAP Vendor Assertions Document

March 12, 2021

By



6220 America Center Drive
San Jose, CA 95002, USA

Product Version:

This SCAP Vendor Assertion Document is for McAfee® Policy Auditor Version 6.5.0.263¹.

Assertion:

McAfee LLC asserts that McAfee Policy Auditor version 6.5.0.263 meets or exceeds the Derived Test Requirements (DTR) for SCAP Version 1.3 as described in NIST IR 7511 Revision 5 for the following SCAP capabilities and supported platform family:

- Capabilities:**
- Authenticated Configuration Scanner
 - CVE
 - OCIL

Platforms:

- Microsoft Windows Vista SP
- Microsoft Windows 7 SP_ 32-bit
- Microsoft Windows 7 SP_ 64-bit
- Microsoft Windows 8.1 SP_ 32-bit
- Microsoft Windows 8.1 SP_ 64-bit
- Microsoft Windows 10 SP_ 32-bit
- Microsoft Windows 10 SP_ 64-bit
- Microsoft Windows Server 2012 R2 SP_ 64-bit

- Red Hat Enterprise Linux 6 Desktop 32 bit
- Red Hat Enterprise Linux 6 Desktop 64 bit
- Red Hat Enterprise Linux 7 Desktop 64 bit

- Apple Mac OS 10.11 (OS X El Capitan)

SCAP Component Technologies:

The following table provides a brief summary of the individual SCAP Component Standards supported by McAfee Policy Auditor.

Supported	Component	Version	Description
<input checked="" type="checkbox"/>	AI	1.1	Asset Identification (AI) is a specification for identifying assets
<input checked="" type="checkbox"/>	ARF	1.1	The Asset Reporting Format (ARF) is a specification describing a data model for asset reporting
<input checked="" type="checkbox"/>	CCE	5	The Common Configuration Enumeration™ (CCE) is a nomenclature and dictionary of software security configurations
<input checked="" type="checkbox"/>	CCSS	1.0	The Common Configuration Scoring System (CCSS) is a specification for measuring the relative severity of system security configuration issues
<input checked="" type="checkbox"/>	CPE	2.3	The Common Platform Enumeration (CPE) is a specification measuring the relative severity of system security configuration issues

¹ Versioning numbering for the product uses a construct of major.minor.update-build HFnn (where nn is a number)

<input checked="" type="checkbox"/>	CVE	n/a	The Common Vulnerability Enumeration® (CVE) is a specification describing a nomenclature and dictionary of security-related software flaws
<input checked="" type="checkbox"/>	CVSS	3.0	The Common Vulnerability Scoring System is a language for representing system configuration information, assessing machine state, and reporting assessment results
<input type="checkbox"/>	OCIL	2.0	The Open Checklist Interactive Language (OCIL) is a language for representing checks that collect information from people or from existing data stores made by other data collection efforts
<input checked="" type="checkbox"/>	OVAL	5.11.2	The Open Vulnerability and Assessment Language is a language for representing system configuration information, assessing machine state, and reporting assessment results
<input checked="" type="checkbox"/>	SCAP	1.1, 1.2 and 1.3	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
<input checked="" type="checkbox"/>	SWID	2015 revision	The Software Identification (SWID) Tags 2015 revision is a format for representing software identifiers and associated metadata
<input checked="" type="checkbox"/>	TMSAD	1.0	The trust Model for Security Automation Data (TMSAD) describes a common trust model that can be applied to specifications within the security automation domain
<input checked="" type="checkbox"/>	XCCDF	1.2	Extensible Configuration Checklist Description Format (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents

SCAP Implementation Statement(s):

The Security Content Automation Protocol (SCAP) is a collection of open standards developed jointly by various United States government organizations and the private sector. Security content conforming to the SCAP standard can be used by any product that supports the standard and the results can be shared among these products.

Policy Auditor allows users to import and export benchmarks and checks that use SCAP. Users can tailor or edit benchmarks within the McAfee Benchmark Editor interface and activate them for use in audits. Benchmarks determine whether a system complies with the benchmark rules. Benchmarks also return results that can be converted to a human-readable format.

Benchmarks and checks incorporate the following reference protocols to ensure that all rules are processed accurately and appropriately, and that the results appear properly in reports and export files:

- Common Vulnerabilities and Exposures (CVE)
- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
- Common Vulnerability Scoring System (CVSS)
- Common Configuration Scoring System (CCSS)
- Trust Model for Security Automation Data (TMSAD)
- Extensible Configuration Checklist Description Format (XCCDF)
- Open Vulnerability and Assessment Language (OVAL)
- Asset Identification (AI)
- Asset Reporting Format (ARF)
- Software Identification (SWID)

McAfee Policy Auditor 6.5 provides the ability to detect and assess thousands of systems from a Policy Auditor Server. This standardization allows regulatory authorities and security administrators to construct definitive security guidance and to compare results reliably and repeatedly.

Policy Auditor is designed exclusively around SCAP and manages all aspects of analyzing systems for compliance. It has authenticated configuration scanning capability but does not use the OCIL option. It uses XCCDF and OVAL to determine what items to check and how to check them. It uses the CPE, CCE, CVSS, and CVE reference protocols to ensure that all rules are accurately and appropriately evaluated during system audits. The SCAP standard references are visible in the interface, reports, and export files.

SCAP Backwards Compatibility:

Policy Auditor supports the older SCAP 1.0, 1.1 and 1.2 specifications

Disclaimer:

Copyright © 2021 McAfee, LLC

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

This document may be freely reproduced and distributed whole and intact including this copyright notice.