Vendor Provided Validation Details - McAfee Policy Auditor 6.2

The following text was provided by the vendor during testing to describe how the product implements the specific capabilities.

Statement of FDCC Compliance

McAfee asserts that McAfee Policy Auditor 6.2 does not alter or conflict with the Federal Desktop Core Configuration (FDCC) settings on Microsoft Windows XP and Vista systems.

Statement of USGCB Compliance

McAfee asserts that McAfee Policy Auditor 6.2 does not alter or conflict with the United States Government Configuration Baseline (USGCB) settings on Microsoft's Windows 7, Windows 7 Firewall, Windows Vista, Windows Vista Firewall, Windows XP, Windows XP Firewall, Internet Explorer 7, Internet Explorer 8, and Red Hat Enterprise Linux 5. USGCB is a further clarification of the FDCC; specifically, the USGCB initiative falls within FDCC and comprises the configuration settings component of FDCC. In the SCAP 1.2 Validation Program, products must correctly import and process all Tier IV data streams. The USGCB content is Tier IV; therefore, the USGCB data streams are used in the validation program to test if products are capable of correctly processing Tier IV content.

The relevant platforms supported by the Policy Auditor 6.2 agent are

- Windows XP SP3
- Windows Vista Business Edition SP2
- Windows 7, 64 bit, with Internet Explorer 8
- Windows 7, 32 bit, with Internet Explorer 8
- RedHat Enterprise 5, 32 bit
- RedHat Enterprise 5, 64 bit

The product also supports SCAP version 1.0 and 1.1

Statement of SCAP Compliance

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)

McAfee Policy Auditor 6.2 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 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 product supports the SCAP 1.2 Authentication Configuration Scanner (ACS) with CVE option capabilities. The OCIL option capability is not supported by the product. The SCAP standard references are visible in the interface, reports, and export files.

Statement of CVE Compliance

McAfee Policy Auditor 6.2 fully implements and supports the Common Vulnerabilities and Exposures (CVE) standard vulnerability dictionary. CVE provides unique, standardized identifiers for security vulnerabilities. CVE address vulnerability and exposure issues, not compliance items.

Policy Auditor implements and supports CVE enumeration, which provides standardized references to known vulnerabilities. CVE uses a named list of information security weaknesses, providing standardized identifiers to facilitate a universal naming convention. Each CVE identifier consists of:

- A CVE identifier number, such as CVE-2008-0042.
- An indication of whether the CVE has a status of "entry" or "candidate."

- A description of the vulnerability.
- A list of any references, such as advisories or OVAL identification.

Policy Auditor patch and vulnerability definitions are updated periodically when new content is available. The audit results can be viewed from the Audits, Reports, or Dashboard user interfaces.

CVE information is accessible from the Checks interface, which displays details of Common Vulnerabilities. Users have the ability to view even more detailed CVE information from the Check Details page, which displays the Source, ID, and URL. For example, the URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2122 refers the user to the Mitre site to view details about CVE-2005-2122. The security content provided by McAfee refers to CVE identifiers when addressing vulnerabilities and whether a vendor's patch has been applied to address the vulnerability.

Previous versions of Policy Auditor have been certified by Mitre as CVE-Compatible.

Statement of CPE Implementation

McAfee Policy Auditor 6.2 implements version 2.3 of the Common Platform Enumeration (CPE) standard. CPE provides a standard reference and notation method for information technology systems, platforms, and packages.

Policy Auditor contains the CPE data dictionary in the database with some of it in aggregated format to promote ease of use. Information from this dictionary drives various aspects of the Policy Auditor interface. Policy Auditor associates OVAL definitions with CPE Names and allows users to specify CPE names at the benchmark, group, profile, or rule level. Policy Auditor users can create audits with SCAP content that cover a number of common operating systems and platforms.

When CPE platforms are specified, Policy Auditor uses this information to determine whether it should evaluate compliance with a rule or group of rules. For example, an audit can cover both Windows XP and Windows Vista operating systems but not the Windows 2000 operating system. CPE allows Policy Auditor to use the correct content on the correct systems.

Previous versions of Policy Auditor have been certified by Mitre as CPE-Compatible.

Statement of CVSS Compliance

McAfee Policy Auditor 6.2 incorporates version 2.0 of the Common Vulnerability Scoring System (CVSS). CVSS is a standardized open framework for measuring the impact of vulnerabilities.

Each CVE includes an associated CVSS vector to determine the relative severity of vulnerabilities.

CVSS is built on a quantitative model that ensures repeatable measurements on systems, valid comparisons between systems, and that allows users to view the underlying vulnerability characteristics. Using CVSS scores help an organization to determine and prioritize responses to detected vulnerabilities.

Policy Auditor supports all four standard SCAP scoring models:

- Flat
- Unweighted
- Absolute
- Default

The default setting for Policy Auditor is a flat unweighted scoring model normalized to a maximum possible score of 100. The scoring model can be changed for comparison purposes.

Previous versions of Policy Auditor have been certified by Mitre as CVSS-Compatible.

Statement of CCSS Compliance

McAfee Policy Auditor 6.2 incorporates version 1.0 of the Common Configuration Scoring System (CCSS). CCSS is a standardized open framework for measuring the impact of configuration vulnerabilities.

Each CCE includes an associated CCSS vector to determine the relative severity of configuration vulnerabilities.

CCSS is built on a quantitative model that ensures repeatable measurements on systems, valid comparisons between systems, and that allows users to view the underlying configuration vulnerability characteristics. Using CCSS scores help an organization to determine and prioritize responses to detected configuration vulnerabilities.

Policy Auditor supports all four standard SCAP scoring models:

- Flat
- Unweighted
- Absolute
- Default

The default setting for Policy Auditor is a flat unweighted scoring model normalized to a maximum possible score of 100. The scoring model can be changed for comparison purposes.

Statement of TMSAD compliance

TMSAD specifies the trust model that can be applied to the processing of XML documents since XML is primarily used for security automation domain information exchange. It recommends the specifications around the representation of signatures in an XML document.

Policy Auditor 6.2 can validate the structure but does not process the signature.

Statement of CCE Implementation

CCE provides a standard system for identifying and referencing system configuration settings. CCE identifies the configuration itself, not the means by which that configuration was reached. CCE encourages interoperability, improves the correlation of test results, and simplifies gathering metrics.

Policy Auditor includes CCE references in the checks content. The Checks tab lists all the checks available to users. Clicking on a check with CCE content lists CCE references that identify the CCE system configuration settings.

McAfee Policy Auditor 6.2 incorporates and supports version 5.0 of the Common Configuration Enumeration (CCE) standard. Previous versions of Policy Auditor have been certified by Mitre as CCE-Compatible.

Statement of XCCDF Implementation

The Extensible Configuration Checklist Description Format (XCCDF) is an XML specification language that supports the exchange of information, generation of results, tailoring, automated compliance testing, and compliance scoring. It also provides a data model and format for storing results of benchmark compliance testing.

XCCDF provides a uniform standard for the expression of benchmarks and other configuration guidance to encourage good security practices. Policy Auditor uses benchmarks from McAfee or third-party sources to construct audits. Users can select the benchmark profile, if any, to use for the audit. After a system is audited, the audit results are returned to Policy Auditor, which analyzes and reports on the configuration and vulnerability data. The user can specify how long audit data is retained so that they or auditors can review any changes in the state of a system over time.

McAfee Policy Auditor 6.2 implements version 1.2 of XCCDF. Previous versions of Policy Auditor have been certified by Mitre as XCCDF-Compatible.

Statement of OVAL Implementation

The Open Vulnerability and Assessment Language (OVAL) describes the ideal configuration of systems, compares systems to the ideal configuration, and reports the test results. It provides a structured model for network and system administrators to detect vulnerabilities and configuration issues on systems. Policy Auditor uses the Checks interface to import and export OVAL definitions and other formats supported by XCCDF. These checks can be filtered based on OVAL IDs, platforms, or any other criteria set by the user. The Check Details interface displays a hyperlink to specific OVAL IDs, which will display OVAL in XML format.

When a system is audited, the OVAL content is processed according to the information in the XCCDF benchmarks contained in the audit. The OVAL content captures the state of the system at the particular point in time that the audit is run. The results are returned to Policy Auditor for analysis and reporting.

The user specifies how long audit data is to be retained so that they or auditors can review any changes in the state of a system over time.

Policy Auditor 6.2 provides fully integrated support for version 5.10 of the OVAL. Previous versions of Policy Auditor have been certified by Mitre as OVAL-Compatible.

Statement of AI and ARF implementation

The Asset Identification (AI) specification is used to enable tools to represent asset identification information for purposes of external consumption by other tools or reports. The Asset Reporting Format (ARF) specification facilitates the sharing of asset information. It also helps with the correlation of different views on asset to enable a more complete view of the asset. This specification also defines the format of the way in which tools can receive and consume reports about assets.

In Policy Auditor 6.2, the server has the ability to export Audit results in the minimum ARF format and agent has the capability to save the audit result in the complete ARF format. The Audit catalog page provides the functionality to export the minimum ARF report in the zip format for the user selected audits. For storing the audit result in the complete ARF format, the “Generate result data stream on target system” setting has to be enabled for the audit. The ARF report represents the asset information in the AI format.