ITL BULLETIN FOR APRIL 2013

SECURITY CONTENT AUTOMATION PROTOCOL (SCAP) VERSION 1.2
VALIDATION PROGRAM TEST REQUIREMENTS

NIST's Information Technology Laboratory has developed validation program test requirements for SCAP version 1.2. The SCAP Validation Program tests the ability of products to use the features and functionality available through SCAP and its components. SCAP 1.2 consists of a suite of specifications for standardizing the format and nomenclature by which security software communicates information about software flaws and security configurations. The standardization of security information facilitates tool interoperability and enables predictable results among disparate SCAP-enabled security software. The SCAP Validation Program provides vendors with an opportunity to have independent verification that security software correctly processes SCAP-expressed security information and provides standardized output. Industry and government end users benefit from the SCAP Validation Program by having assurance that SCAP-validated tools have undergone independent testing and meet all requirements defined in the SCAP Validation Program Test Requirements document.

The validation program supports the U.S. Office of Management and Budget (OMB) Memorandum 08-22 to Federal CIOs. This memorandum states, "Both industry and government information technology providers must use SCAP-validated tools with FDCC Scanner capability to certify their products operate correctly with FDCC configurations and do not alter FDCC settings. Agencies will use SCAP tools to scan for both FDCC configurations and configuration deviations approved by department or agency accrediting authority. Agencies must also use these tools when monitoring use of these configurations as part of FISMA continuous monitoring." The checklist portion of the FDCC mandate is now referred to as the United States Government Configuration Baseline (USGCB), and the FDCC Scanner capability has evolved and is now referred to as the Authenticated Configuration Scanner (ACS) capability.

Under the SCAP Validation Program, independent laboratories are accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP). These laboratories conduct the tests defined in this document on products and deliver the results to NIST. Based on the independent laboratory test report, the SCAP Validation Program then validates the product under test. The validation certificates awarded to vendor products are publicly posted on the NIST SCAP Validated Products web page. 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 the new document.

The requirements are contained in a new report, NISTIR 7511, Revision 3, *Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements*. Written by John Banghart, Melanie Cook, Stephen Quinn, and David Waltermire of NIST and Andrew Bove of Secure Acuity, the report introduces the SCAP 1.2 Validation Program and defines the requirements and associated test procedures for SCAP 1.2 product validation. For more information, see the SCAP website.

ITL Bulletin Publisher:
Elizabeth Lennon, Writer/Editor
Information Technology Laboratory
National Institute of Standards and Technology
Email elizabeth.lennon@nist.gov

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.