Tivoli Endpoint Manager for Configuration Management SCAP User's Guide

IBM

Contents

Configuration Management SCAP User's Guide

Tivoli Endpoint Manager Configuration Management is a portfolio of content in the form of checklists that allow organizations to assess and manage the configurations of desktops, laptops, and servers. Tivoli Endpoint Manager Configuration Management is one of the few products to have achieved Security Content Automation Protocol (SCAP) through the National Institute of Standards and Technology (NIST) for both misconfiguration assessment and remediation. By offering a comprehensive library of technical controls, Configuration Management detects and enforces security configuration policies using industry best practices.

Checklists

Configuration Management checklists assess and manage the configurations of desktops, laptops, and servers. Security teams use the Configuration Management checklists to define and assess security parameters and configurations that are required by organizational policy. IT managers use the Configuration Management checklists to enforce security policy and document the current state of compliance with documented policy. Auditors use them to determine the current state of compliance for any given set of systems within the entire organization.

For detailed information about how to configure Windows or UNIX checklists, see the *Configuration Management Checklists Guide*.

Custom sites

You can control your security status by customizing Configuration Management and excluding specific computers from an analysis. You can also create custom sites and repurpose the Configuration Management checklists to fine-tune your deployment.

Creating a custom site

To create a custom checklist based on one or more subscribed external checklists, use the *Create Custom Checklist* wizard located in the “Checklist Tools” folder in the console Security Configuration domain. For more information about using this wizard, see the *Configuration Management Checklists Guide*.

Subscribing clients to the custom site

After creating your custom site, you must subscribe computers to it. The correct collection of compliance data depends on targeting the content to the appropriate computers. You can subscribe computers to your site by specific computers or by computer properties. For detailed information about how to create and manage custom sites, see the Configuration Management *User's Guide*.

About SCAP

The ability to automate technical configurations on devices across enterprise infrastructures has been a historical challenge. Organizations such as the National Institute of Standards and Technology (NIST), National Security Agency (NSA), the Center for Internet Security (CIS), and the Defense Information Systems Agency (DISA) have attempted to provide guidance through documentation, standards, and guidelines. But technology has limited the ability for full automation of these technical configurations, especially at scale across globally distributed environments.

The Security Content Automation Protocol (SCAP) has been adopted to meet this challenge. As part of the Configuration Management product, SCAP is a method for automating the definition, consumption, and assessment of system configurations on desktop systems throughout an organization's infrastructure. IBM Tivoli Endpoint Manager provides real-time visibility and control over system configurations through a single infrastructure, single agent, and single console, and enables continuous assessment and enforcement of SCAP configuration baselines for on- and off-network systems. With Tivoli Endpoint Manager, federal agencies can easily identify systems that are not compliant to a SCAP data stream, remediate settings found to be non-compliant, and report on the configuration status of one or more systems in real-time.

Information Security Automation Program

The Information Security Automation Program (ISAP) automates and standardizes technical security operations. Primarily focused on government, ISAP offers security checking, remediation, and automation of technical compliance activities to such regulations as FISMA and the FDCC.

ISAP objectives include enabling standards-based communication of vulnerability data, customizing and managing configuration baselines for various IT products, assessing information systems and reporting compliance status, using standard metrics to weight and aggregate potential vulnerability impact, and remediating identified vulnerabilities.

SCAP overview

ISAP technical specifications are contained in the related Security Content Automation Protocol (SCAP). SCAP consists of a suite of standards that enable automated vulnerability management, measurement, and policy compliance evaluation, for example, FISMA compliance.

Specifically, SCAP standards address the following objectives:

- Enumerate software flaws, security-related configuration issues, and product names
- Measure systems to determine the presence of vulnerabilities
- Provide mechanisms to rank the results of these measurements to evaluate the impact of the discovered security issues

SCAP defines how these standards are combined. The U.S. National Institute of Standards and Technology (NIST) maintains the National Checklist Program (NCP) and provides a repository of data feeds that use the SCAP standards. It is also the repository for official SCAP standards data.

NIST defines and maintains the protocol and the data feeds of content in the SCAP standards. Thus, NIST defines how to use the open standards within the SCAP context and defines the mappings between the SCAP enumeration standards.

SCAP standards

SCAP is comprised of the following standards:

Common Vulnerabilities and Exposures (CVE)

The SCAP CVE standard is a dictionary of publicly known information security vulnerabilities that enable data exchanges between security products and provide a baseline index point for evaluating coverage of tools and services.

Tivoli Endpoint Manager has actively supported CVE for several versions of the product and maintains a mature product integration with CVE content. Any security patch or vulnerability that has an associated CVE ID and is available as either a SCAP data stream or available through other Tivoli Endpoint Manager developed processes will display the relevant CVE ID within the Tivoli Endpoint Manager console.

You can find this ID associated with a given security patch or vulnerability by opening the Tivoli Endpoint Manager console and navigating to a patch or vulnerability Fixlet site, double-clicking a relevant Fixlet, selecting the Details tab and viewing the CVE ID. The CVE ID is also accessible from other views and can be used as part of the reporting criteria for detailed and summary reports on individual end-point systems or for a large group of systems reported on in the aggregate.

Common Configuration Enumeration (CCE™)

The SCAP CCE standard provides unique identifiers to system configuration issues to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. For example, CCE Identifiers can associate checks in configuration assessment tools with statements in configuration best practice documents. The Tivoli Endpoint Manager platform includes the ability to assess workstations, laptops, servers, and mobile computing devices against common configuration settings to identify misconfiguration states in a diverse computing environment. Tivoli Endpoint Manager fully supports CCE and displays the CCE ID for each misconfiguration for which there is a CCE ID within the Tivoli Endpoint Manager console. In the case where a misconfiguration is associated with multiple CCE IDs, all IDs are cross-referenced and displayed.

To find the CCE ID associated with a configuration setting, open the Tivoli Endpoint Manager console and navigate to a configuration setting used by a SCAP data stream. Click on a Fixlet that represents a configuration setting and view the Source ID column. The Source ID displays the CCE ID. The CCE ID is also accessible from other views and can be used as part of the reporting criteria for detailed reports and summary reports on individual end-point systems or for a large group of systems reported on in the aggregate.

Common Platform Enumeration (CPE™)

The SCAP CPE standard is a structured naming scheme for information technology systems, platforms, and packages. Based on the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name. Tivoli Endpoint Manager uses CPE to ensure that configuration settings are assessed on the correct system. Regardless of the operating system, the CPE ID can identify a platform and ensure that an assessment is performed.

You can assess and remediate system configurations by targeting systems by platform in addition to other targeting mechanisms. By targeting a particular platform, you can ensure that system scans are done properly and are weighed against applicable configuration checks. Checks are assessed in real-time based on the platform and policies can be enforced, giving administrators current visibility and control over platforms in a distributed or non-distributed computing environment.

Common Vulnerability Scoring System (CVSS)

The SCAP CVSS standard provides an open framework for communicating the characteristics of IT vulnerabilities. Its quantitative model ensures repeatable, accurate measurement while displaying vulnerability characteristics used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and agencies that need accurate and consistent vulnerability impact scores.

Tivoli Endpoint Manager assesses and reports on vulnerabilities and quantifies the impact for multiple computing platforms. Tivoli Endpoint Manager fully supports the CVSS standard and displays both the CVSS base score for each applicable vulnerability and the CVSS Base Score Vector used to produce the score.

Tivoli Endpoint Manager administrators can access the CVSS score and the associated vector string from within the Tivoli Endpoint Manager console. For additional details, administrators can navigate to the a vulnerability definition from within the Fixlets. Tivoli Endpoint Manager provides a link for administrators to connect to the CVSS definition located on the NVD website. Tivoli Endpoint Manager enhances the value of CVSS by displaying this common metric for detailed reports on individual end-point systems and for large groups of systems reported on in the aggregate.

Extensible Configuration Checklist Description Format (XCCDF)

The SCAP XCCDF standard is a specification language for writing security checklists, benchmarks, and related documents. An XCCDF document represents a structured collection of security configuration rules for some sets of target systems and is the core element of the SCAP data stream. The specification also defines a data model and format for storing results of checklist compliance testing.

SCAP data streams use the XCCDF format to translate underlying configuration checks that are defined in Tivoli Endpoint Manager Fixlets. When created, these SCAP-based configuration Fixlets allow administrators to assess their computing assets against the SCAP-defined configuration rules in real-time and on a global scale.

When the SCAP configuration rules are imported into Tivoli Endpoint Manager, any system can immediately assess against the defined configuration rules. The results of those configuration checks are relayed to the Tivoli Endpoint Manager console, where administrators can view results and generate detailed reports on an individual system or on large groups of systems.

Tivoli Endpoint Manager also exports the results of the configuration checks into the defined XCCDF report format so that the organization can store, send, or import those reports into another tool.

Open Vulnerability and Assessment Language (OVAL™)

The SCAP OVAL standard is an international, information security community standard that promotes security content and standardizes the transfer of this information across an entire spectrum of security tools and services. The OVAL language is a collection of XML schema for representing system information, expressing specific machine states, and reporting the results of an assessment.

Through a repository of vulnerability assessment policies, Tivoli Endpoint Manager assesses managed computers against OVAL vulnerability definitions using real-time data tracking based on the data elements of each definition. These policies are automatically retrieved by the Tivoli Endpoint Manager product within an organization's network. When validated for authenticity, the policies are made available to the Tivoli Endpoint Manager client installed on each managed computer and added to their local library of configuration policies. The agent continuously evaluates the state of the machine against each policy so that any instance of non-compliance can be reported to the Tivoli Endpoint Manager Server for administrator review. If pre-authorized by an administrator, the appropriate corrective action is applied to the computer immediately upon misconfiguration detection, even to remote or mobile users not connected to the organization's network.

Content Availability Options

SCAP is comprised of SCAP Fixlet checklists and SCAP generation wizards, which Tivoli Endpoint Manager administrators can use to manage and maintain SCAP-based checklist content and compliance results.

SCAP Fixlet Checklists

Tivoli Endpoint Manager distributes Fixlets through subscription and sites. Tivoli Endpoint Manager has taken the SCAP checklist XML, generated Tivoli Endpoint Manager content from it, and made it available through subscription. Customers load the external site mastheads for each of the available SCAP checklists in the Tivoli Endpoint Manager console, and the Tivoli Endpoint Manager server downloads the content and makes it available to the Tivoli Endpoint Manager administrator to begin evaluating on systems.

Tivoli Endpoint Manager currently provides out-of-the-box content for the Federal Desktop Core Configuration (FDCC) SCAP checklists. As new checklists are made available by NIST, Tivoli Endpoint Manager might include those sites as part of the subscription service.

In addition to the Fixlet sites, Tivoli Endpoint Manager includes a reporting dashboard that provides visibility into the results of the system evaluations and a reporting dashboard for generating Tivoli Endpoint Manager content from an SCAP checklist. These dashboards are found in the *Configuration Management Reporting* site.

The following out-of-the-box SCAP checklists are currently available as part of this product:

- *FDCC on Windows XP*

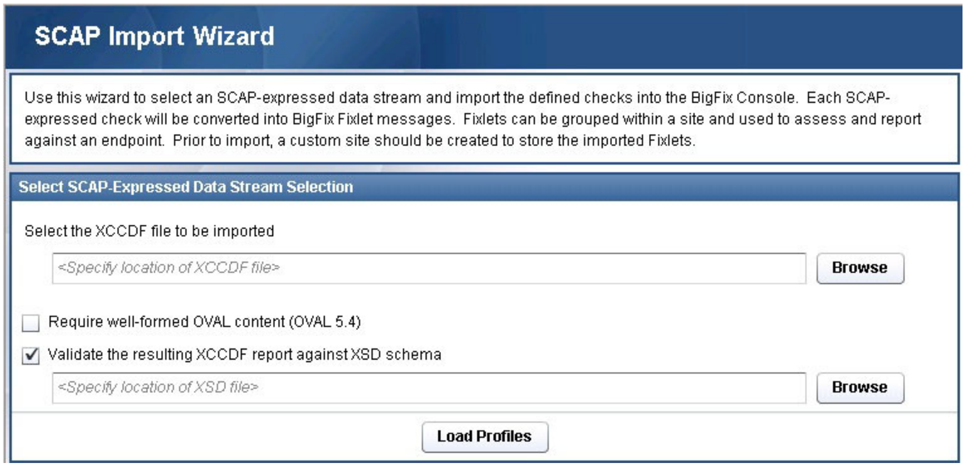
- *FDCC on Windows XP Firewall*
- *FDCC on Windows Vista*
- *FDCC on Windows Vista Firewall*
- *FDCC on Internet Explorer 7*
- *USGCB on Windows 7 Firewall*
- *USGCB on Windows 7 Energy*
- *USGCB on Internet Explorer 8*
- *USGCB on Windows 7*

SCAP Generation Wizards

You can customize SCAP checklists to generate your own configuration checklists rather than using subscription-based content. To facilitate this, Tivoli Endpoint Manager provides tools that allow you to use a SCAP checklist and generate Fixlets to assess one or more endpoints.

The following tools are included:

1. **SCAP Import Wizard** – This wizard generates Tivoli Endpoint Manager content from a SCAP checklist. The content is then imported into a custom site that you create for this purpose. It includes a Fixlet for each check in the SCAP checklist.



SCAP Import Wizard

Use this wizard to select an SCAP-expressed data stream and import the defined checks into the BigFix Console. Each SCAP-expressed check will be converted into BigFix Fixlet messages. Fixlets can be grouped within a site and used to assess and report against an endpoint. Prior to import, a custom site should be created to store the imported Fixlets.

Select SCAP-Expressed Data Stream Selection

Select the XCCDF file to be imported

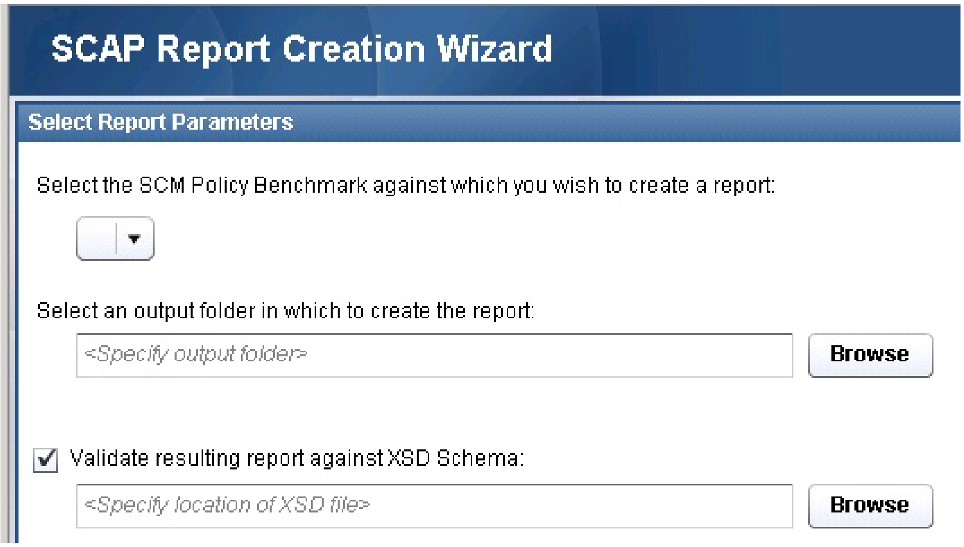
<Specify location of XCCDF file>

☐ Require well-formed OVAL content (OVAL 5.4)

☑ Validate the resulting XCCDF report against XSD schema

<Specify location of XSD file>

2. **SCAP Report Creation Wizard** – This Wizard is used to create an XCCDF results file for each managed endpoint.



SCAP Report Creation Wizard

Select Report Parameters

Select the SCM Policy Benchmark against which you wish to create a report:

Select an output folder in which to create the report:

<Specify output folder>

☑ Validate resulting report against XSD Schema:

<Specify location of XSD file>

Using SCAP

Tivoli Endpoint Manager provides periodic updates in the FDCC content. However, you can also use SCAP tools to generate content from other SCAP checklists.

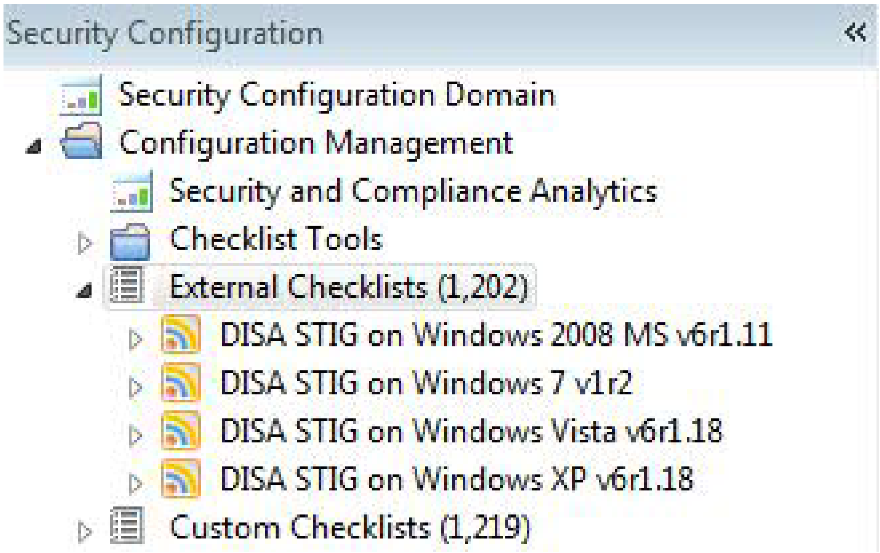
Subscribing to SCAP content

The Tivoli Endpoint Manager Configuration Management solution consists of several external Fixlets that can be imported into the Tivoli Endpoint Manager console to evaluate one or more systems. Each Fixlet provides a specific set of content based on the translation of an individual SCAP data stream into a set of Fixlets. Each Fixlet represents a single configuration check as described in the SCAP data stream.

After the SCAP site is loaded into the console, content is updated and continuously evaluates endpoints for compliance with the configuration standard.

The process for site subscription depends on your version of the Tivoli Endpoint Manager console. For specific site subscription directions, see the Tivoli Endpoint Manager Knowledge Base article **here**.

After the SCAP site is loaded into the console, the Tivoli Endpoint Manager server gathers the content and displays it in the Configuration Management navigation tree.



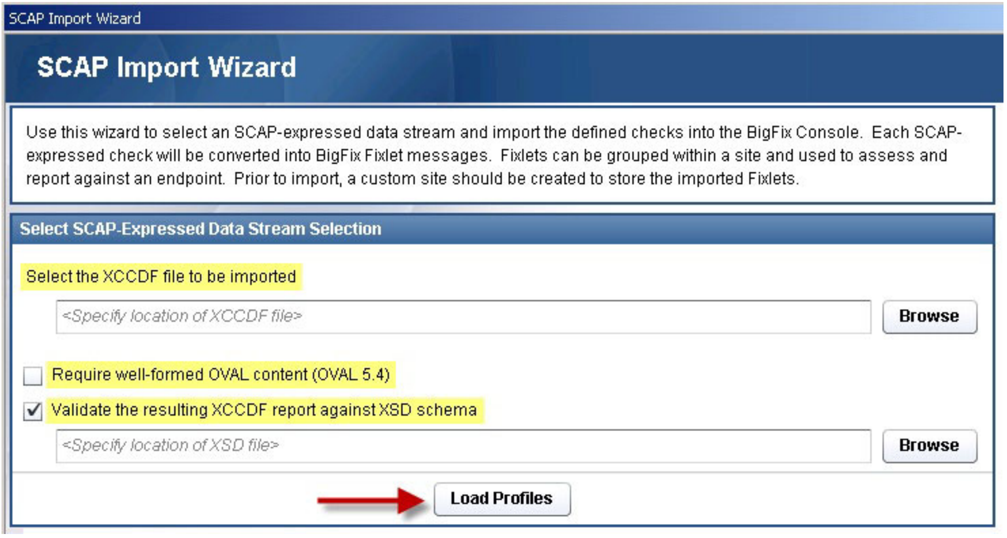
Security Configuration
Security Configuration Domain
Configuration Management
Security and Compliance Analytics
Checklist Tools
External Checklists (1,202)
DISA STIG on Windows 2008 MS v6r1.11
DISA STIG on Windows 7 v1r2
DISA STIG on Windows Vista v6r1.18
DISA STIG on Windows XP v6r1.18
Custom Checklists (1,219)

Note: When Tivoli Endpoint Manager generates Fixlets from a SCAP data stream, the CPE strings associated with the SCAP data stream determine what types of systems must evaluate against the content. When subscribed, systems evaluate the content, if the content matches the defined CPE string. This behavior can be altered. For more information, see the Tivoli Endpoint Manager Support website.

Using the SCAP Import Wizard

Use this wizard to generate Tivoli Endpoint Manager content from a set of SCAP XML input files. The content that is generated includes a Fixlet for each check found in the SCAP checklist. Before using the wizard, you must create a custom site that will contain the resulting checklist. For more information about using custom checklists, see the Configuration Management User's Guide.

SCAP checklists can be found **here**. The SCAP Import Wizard has been validated for checklists at Tier IV in this repository. To use the import wizard, perform the following steps:



SCAP Import Wizard

SCAP Import Wizard

Use this wizard to select an SCAP-expressed data stream and import the defined checks into the BigFix Console. Each SCAP-expressed check will be converted into BigFix Fixlet messages. Fixlets can be grouped within a site and used to assess and report against an endpoint. Prior to import, a custom site should be created to store the imported Fixlets.

Select SCAP-Expressed Data Stream Selection

Select the XCCDF file to be imported

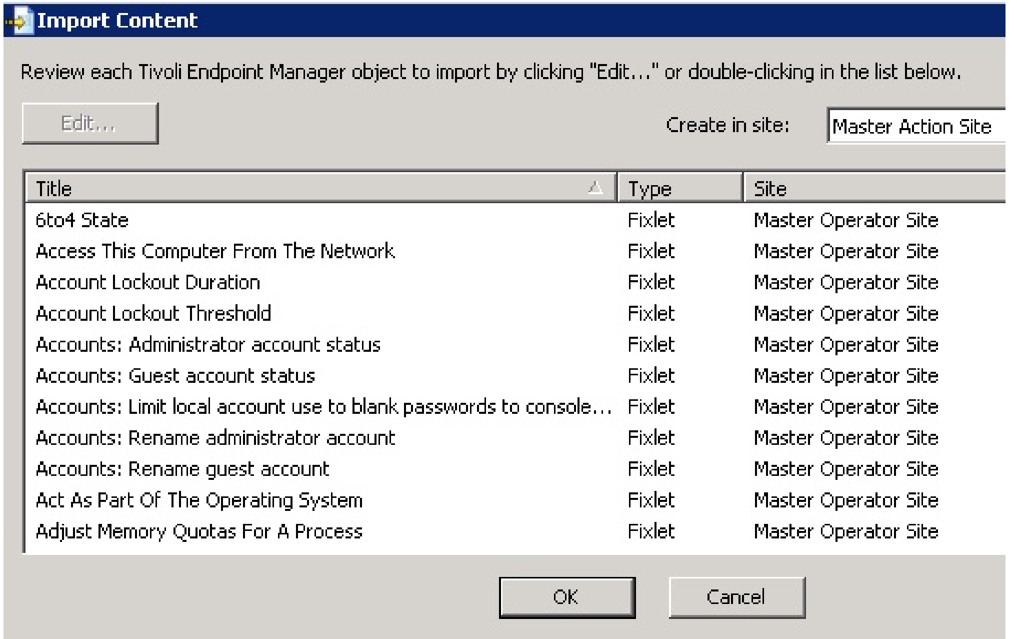
<Specify location of XCCDF file> Browse

□ Require well-formed OVAL content (OVAL 5.4)

☑ Validate the resulting XCCDF report against XSD schema

<Specify location of XSD file> Browse

1. Click *Browse* and select the XCCDF file to be imported.
2. Optional: Check the OVAL content requirements box.
3. Optional: Specify an XCCDF XSD schema file that will be used to validate the XML input.
4. Click *Load Profiles*. The window for selecting the XCCDF profiles is displayed. This process might take from 1 to 2 minutes.
5. Select an XCCDF profile from the menu.
6. Click *Import*. The *Import Content* window is displayed. Select the custom site from the menu and click *OK*.



Review each Tivoli Endpoint Manager object to import by clicking "Edit..." or double-clicking in the list below.

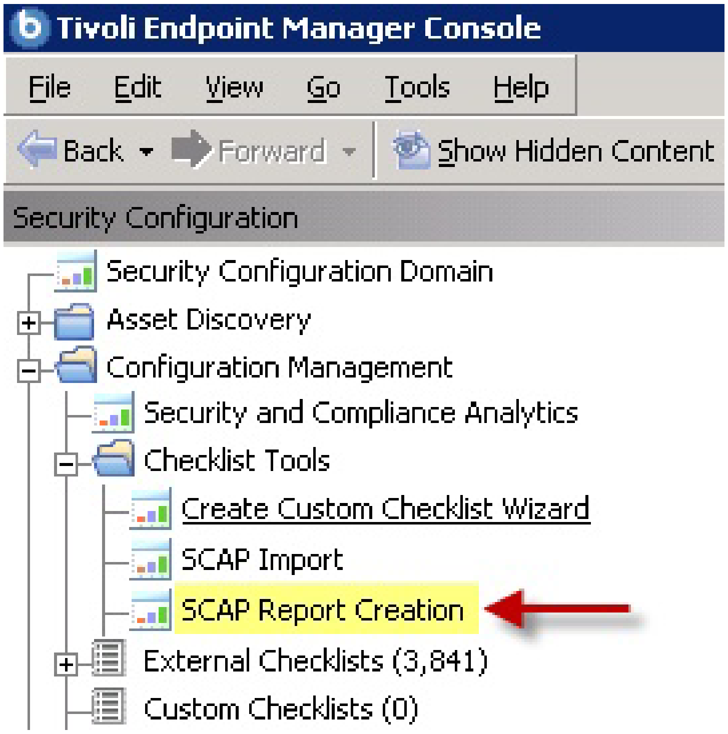
Create in site: Master Action Site

Title	Type	Site
6to4 State	Fixlet	Master Operator Site
Access This Computer From The Network	Fixlet	Master Operator Site
Account Lockout Duration	Fixlet	Master Operator Site
Account Lockout Threshold	Fixlet	Master Operator Site
Accounts: Administrator account status	Fixlet	Master Operator Site
Accounts: Guest account status	Fixlet	Master Operator Site
Accounts: Limit local account use to blank passwords to console...	Fixlet	Master Operator Site
Accounts: Rename administrator account	Fixlet	Master Operator Site
Accounts: Rename guest account	Fixlet	Master Operator Site
Act As Part Of The Operating System	Fixlet	Master Operator Site
Adjust Memory Quotas For A Process	Fixlet	Master Operator Site

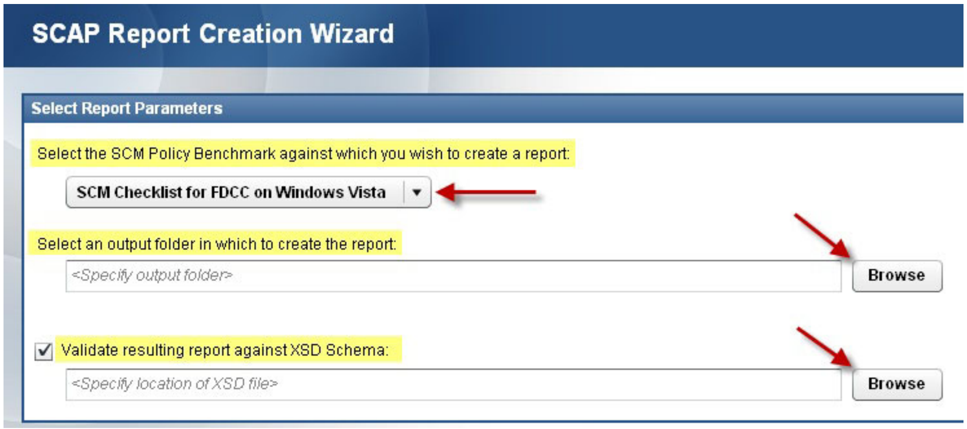
Using the SCAP Report Creation Wizard

To generate an XCCDF results file for each endpoint using the SCAP Report Creation Wizard, perform the following steps:

1. Click SCAP Report Creation.



2. Select report parameters.



SCAP Report Creation Wizard

Select Report Parameters

Select the SCM Policy Benchmark against which you wish to create a report:

SCM Checklist for FDCC on Windows Vista ▾

Select an output folder in which to create the report:

<Specify output folder> Browse

☑ Validate resulting report against XSD Schema:

<Specify location of XSD file> Browse

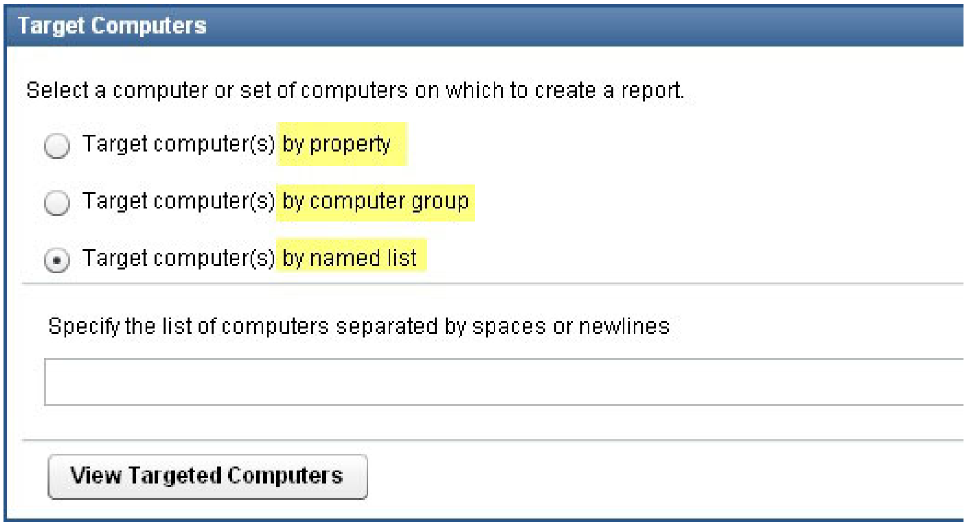
a. Specify a SCAP checklist from the menu.

b. To specify an output folder, click the top *Browse* button.

c. Optional: To specify an XCCDF schema to validate the results file, click the lower *Browse* button.

3. Target computers.

You can target computers by name, property, or computer group. You can also manually enter a list of computers in the designated field. Click the *View Targeted Computers* button to check your selection.



Target Computers

Select a computer or set of computers on which to create a report.

○ Target computer(s) by property

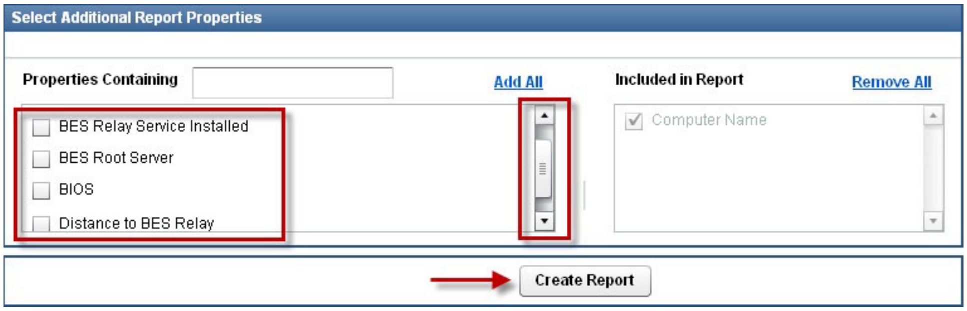
○ Target computer(s) by computer group

● Target computer(s) by named list

Specify the list of computers separated by spaces or newlines

4. Select Additional Report Properties.

   Use the scroll bar to view a list of available report properties. Check any applicable boxes and view each selection in the corresponding *Included in Report* box on the right.



Select Additional Report Properties

Properties Containing

□ BES Relay Service Installed

□ BES Root Server

□ BIOS

□ Distance to BES Relay

Included in Report

☑ Computer Name

5. Click *Create Report*.

   Allocate adequate time for the creation of these reports. The amount of time to generate a report depends on the size of your deployment. For example, creating a report for a deployment of 5000 computers can take 15 minutes on a properly-sized console computer.

Resources

Frequently asked questions

Are there compliance evaluation reports or mechanisms that compare a laptop or server against FISMA/NIST/DISA standards?

Tivoli Endpoint Manager Configuration Management assesses servers, laptops, and desktops against a predefined set of configuration standards such as DISA STIG (Standard Technical Implementation Guides) and FDCC (Federal Desktop Core Configuration). Tivoli Endpoint Manager can also support configuration standards from NIST, NSA, and other standards organizations. Regulatory compliance regulations such as FISMA, PCI, and others can be supported by using the standard configuration controls provided through the Tivoli Endpoint Manager across Windows and UNIX environments.

What are some of the things I cannot do using this content?

The Tivoli Endpoint Manager Confirmation Management solution is designed to be flexible. However, the remediation functionality on both Windows and UNIX is limited to specific configuration settings. In some cases, there are controls that cannot be remediated. The parameter functionality on both Windows and UNIX is also limited to specific configuration settings. Similar to remediation, not everything can and should be parameterized.

What happens if I subscribe sites incorrectly to a system?

If possible, use the site subscription function when deploying Configuration Management to ensure that the dashboard and reports calculate compliance results accurately. Configuration Management controls evaluate on any endpoint that is subscribed, including systems that should not be evaluating content. Using the subscriptions appropriately ensures that only designated systems are evaluating content. When installing the out-of-the-box Confirmation Management sites, immediately modify the subscription. When creating custom checklists, make sure to subscribe the appropriate systems. Failure to subscribe systems appropriately causes the Configuration Management reports to calculate compliance incorrectly.

Example:

If you load the mastheads for Windows XP, the default behavior is to measure the content on all systems, including Windows XP, Windows Vista, and UNIX systems. This behavior causes each non-Windows XP system to return a Not Relevant result. This translates into Compliant when running reports. By setting the site subscription to include only Windows XP systems, only Windows XP systems are evaluated. This ensures that compliance reports generate the most accurate results.

Should the "Source Release Date" in the FDCC content be the date that NIST released or the date the content was generated?

Any data consumed from a SCAP data feed includes the following dates of reference:

1. **Source Release Date –** This date represents the date that Tivoli Endpoint Manager generated the out-of-the-box configuration Fixlets from a SCAP data stream or when a user generates content using the SCAPEval.exe tool. This date is displayed in the *Source Release Date* column of each Fixlet found in the Tivoli Endpoint Manager console.
2. **Published Status and Date –** Within the SCAP data stream, each checklist object includes a status element that indicates a revision or standardization status for a checklist. This element must display once in a checklist object and can display once in any item. If an item does not have its own status element, the parent element is assumed. This element includes a status (accepted, deprecated, draft, interim, or incomplete) along with a date that indicates when the checklist entered the given status. When the Fixlets are created, the appropriate status is added to the *Description of Checklist Information* section of the Fixlet:
   - Accepted Date: YYYY-MM-DD
   - Deprecated Date: YYYY-MM-DD
   - Draft Date: YYYY-MM-DD
   - Interim Date: YYYY-MM-DD
   - Incomplete Date: YYYY-MM-DD

Glossary

SCAP Content
Consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations.

SCAP Checklists
SCAP checklists are configuration checklists written in a machine readable language (XCCDF). SCAP checklists, also referred to as "checklists" or "baselines", have been submitted to and accepted by the NIST National Checklist Program. They also conform to a SCAP template to ensure compatibility with SCAP products and services. The SCAP template discusses requirements for including SCAP enumerations and mappings within the checklist.

SCAP Test Procedures
SCAP checklists reference "SCAP test procedures" for machine readable information on performing low level checks of machine state (OVAL). SCAP test procedures are used in conjunction with SCAP checklists.

SCAP Enumerations
Include a list of all known security related software flaws (CVE), a list of known software configuration issues (CCE), and a list of standard vendor and product names (CPE).

SCAP Mappings
Interrelate the enumerations and provide standards-based impact measurements for software flaws and configuration issues. Thus, for any given software flaw (CVE), one can determine the affected standard product names (CPE). For any given standard product name (CPE), one can determine the configuration issues that affect that product (CCE). For any given software flaw (CVE) or configuration issue (CCE), one can determine the standard impact score (CVSS).

SCAP Check
A specific configuration check within a SCAP checklist. Checks are written in XCCDF and are required to include SCAP enumerations and mappings per the SCAP template.

SCAP Reports
SCAP reports are required to include SCAP enumerations and mappings per the SCAP template.

Abbreviations

CCE	Common Configuration Enumeration
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
DOE	Department of Energy
FDCC	Federal Desktop Core Configuration

FISMA	Federal Information Security Management Act
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
OMB	Office of Management and Budget
OVAL	Open Vulnerability and Assessment Language
SCAP	Security Content Automation Protocol
STIG	Standard Technical Implementation Guide
CONFIGURATION MANAGEMENT	Security Configuration Management
XCCDF	eXtensible Configuration Checklist Description Format

Technical support

The Tivoli Endpoint Manager technical support site offers a number of specialized support options to help you learn, understand, and optimize your use of this product:

- Tivoli Endpoint Manager Info Center
- Support Site
- Documentation
- Knowledge Base
- Forums and Communities

Notices

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this

document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such

provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

2Z4A/101

11400 Burnet Road

Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their

published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

TRADEMARKS:

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also

be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.