



TENABLE

Network Security®

xTool SCAP Assessments

January 11, 2012

(Revision 9)

Copyright © 2002-2012 Tenable Network Security, Inc. Tenable Network Security, Nessus and ProfessionalFeed are registered trademarks of Tenable Network Security, Inc. Tenable, the Tenable logo, the Nessus logo, and/or other Tenable products referenced herein are trademarks of Tenable Network Security, Inc., and may be registered in certain jurisdictions. All other product names, company names, marks, logos, and symbols may be the trademarks of their respective owners.

Table of Contents

Overview.....	3
Standards and Conventions	3
Abbreviations	3
Simple Audit Procedure	4
xTool 1.4 vs. xTool 1.6 Functionality and Content	4
XCCDF Certified vs. Lower-Tier Content.....	5
Using the xTool.....	5
Operation.....	6
Downloading FDCC XCCDF Content	6
Loading XML Content into the xTool	6
<i>XCCDF to .audit</i>	6
Generating an Audit Policy	8
<i>Selecting a Profile</i>	8
<i>Save a .audit File</i>	9
<i>OVAL to .audit</i>	9
<i>File Options</i>	10
Working with SecurityCenter	11
Loading the Audit Policy.....	11
Adding the Audit File to a Vulnerability Scan	11
Analyzing Scan Results	12
Technical Issues	13
Creating FDCC XML Reports	13
Concept	13
Downloading Scan Results	14
Converting .nessus to XCCDF Output.....	14
Filling Out Non-Compliance Override Issues.....	16
Saving and Reusing Failure Override Data	17
Completing and Producing the FDCC Report.....	17
View Options.....	18
Converting .nessus to OVAL Output	18
<i>Validate an XML File</i>	20
<i>Transform an XML File</i>	20
Transform Nessus to Other Format (LASR/ARF) with Style Sheet	21
About Tenable Network Security	26

OVERVIEW

This document describes how to use Tenable's xTool to generate SCAP-certified content audits as well as SCAP OVAL, XCCDF, ASR, and ARF reports from the scan results. The xTool is only available to SecurityCenter customers and can be downloaded from the [Tenable Support Portal](#).

STANDARDS AND CONVENTIONS

Throughout the documentation, filenames, daemons, and executables are indicated with a **courier bold** font such as **gunzip**, **httpd**, and **/etc/passwd**.

Command line options and keywords are also indicated with the **courier bold** font. Command line options may or may not include the command line prompt and output text from the results of the command. Often, the command being run will be **boldfaced** to indicate what the user typed. Below is an example running of the Unix **pwd** command:

```
# pwd
/opt/sc4/daemons
#
```



Important notes and considerations are highlighted with this symbol and grey text boxes.



Tips, examples, and best practices are highlighted with this symbol and white on blue text.

ABBREVIATIONS

The following abbreviations are used throughout this documentation:

ARF	Assessment Results Format
ASR	Assessment Summary Results
CCE	Common Configuration Enumeration
CPE	Common Platform Enumeration
CVE	Common Vulnerability Enumeration
FDCC	Federal Desktop Core Configuration
LASR	Lightweight Asset Summary Results Schema
NIST	National Institute of Standards and Technology
OVAL	Open Vulnerability and Assessment Language
SC	SecurityCenter
SCAP	Security Content Automation Protocol
XCCDF	Extensible Configuration Checklist Description Format

SIMPLE AUDIT PROCEDURE



Tenable requires that all file types for XCCDF, OVAL, and `.nessus` files be kept in the xTool “resource” directory (XTool_<version>\data\resource). The xTool references configuration files from this location and will generate errors or create incomplete reports if the reference files cannot be found or are an incorrect version.

To perform a certified SCAP audit, follow these high-level steps:

1. Download and extract the latest xTool from the Tenable Support Portal to a Windows system (XP or greater). There is no installer and the xTool will run from the location it is extracted to.
2. Download the certified [NIST SCAP content](#) to the same Windows system.
3. Using the xTool, load the SCAP content and generate a Nessus audit file based on user selected settings.
4. Load the audit file into SecurityCenter.
5. Associate the audit file with a properly configured scan policy that is targeting the desired asset(s).
6. Perform a vulnerability scan based on the selected policy.
7. When the scan is completed, load the results (`.nessus` file) into the xTool for conversion to the desired reporting format (XCCDF for [NIST reporting](#)). In addition, OVAL reports can be generated locally and viewed to ascertain NIST compliance status.



The `.nessus` file must be saved in the same location where the SCAP FDCC files from NIST were saved.

Each of these steps is documented in detail later in this document.

xTOOL 1.4 VS. xTOOL 1.6 FUNCTIONALITY AND CONTENT



Any `.audit` files created with xTool version 1.4 are not compatible with xTool version 1.6 and vice-versa.

The xTool version 1.6 differs from 1.4 in functionality and output in a number of important ways. Some of these changes reflect functional enhancements implemented to improve the xTool’s usability. Others address changes to NIST OVAL requirements for certification purposes.

The primary change is in the format of `.audit` files and the subsequent check format as reported from the SecurityCenter post-scan. NIST requires that checks be performed individually rather than grouped by rule. For example, the `.audit` in v1.6 includes an audit check for each OVAL test referenced by the XCCDF document instead of encompassing the entire audit check with the associated groupings for a given XCCDF rule in the `.audit`. The grouping is later performed by the xTool to determine if a system is compliant. Therefore, a fail result for an OVAL test in the SecurityCenter 4 report does not necessarily mean the system is not compliant.

System compliance is determined by performing a `.nessus` to OVAL or `.nessus` to XCCDF report conversion and submitting the results to NIST. A good way to preliminarily gauge compliance is by viewing the human readable report for each host, which is available under the "humanReadable" directory. A HTML report could also be created to review the system compliance by clicking on the "Transform an XML file" button while performing `.nessus` to OVAL conversion, and uploading the relevant input/output files. Note that audits created by xTool 1.6 only include CCE and OVAL test IDs, omitting other references.

The xTool version 1.6 now supports working directly with OVAL content, where xTool 1.4 only supports XCCDF content. This allows users to develop their own custom content based on localized requirements and not a "one-size-fits-all" approach.

Additional changes and functionality are described throughout this document.

XCCDF CERTIFIED VS. LOWER-TIER CONTENT

Tenable designed the xTool to work with the official [XCCDF Tier IV content](#) used in the FDCC program. Beta quality XCCDF-compliant content (Tier 3 and below) is also available from NIST. A few commercial vendors provide content that is not guaranteed to work in SCAP-validated tools, but may work with Tenable's xTool. Tier definitions are listed below:

- > IV – Will work in any SCAP validated tool
- > III – May work in any SCAP validated tool
- > II – Non-SCAP automation content
- > I – Non-automated prose content



Effective Feb 28, 2011, Tier IV RHEL 5 content is available in the NIST SCAP content repository. This content is listed as a beta-candidate and was released after the most recent xTool SCAP certification. While not currently compatible with the xTool, it will work in an upcoming release.

USING THE XTOOL

The xTool is distributed as a ZIP file. It does not have an installer and runs as a stand-alone executable. To use the xTool, follow these steps:

1. Download the xTool ZIP file from the [Tenable Support Portal](#).
2. Transfer the ZIP file to the Windows system that will be used to generate audit policies.
3. Extract the ZIP file, which contains the following:
 - > `xTool.exe`
 - > supporting `.dll` and other executable files
 - > a data directory where reports, logs, and additional support files are stored
4. Run the `xTool.exe` program to parse NIST or other XML content.

OPERATION

DOWNLOADING FDCC XCCDF CONTENT

SecurityCenter users can obtain the various SCAP bundles at http://nvd.nist.gov/fdcc/download_fdcc.cfm under the "SCAP Content" section of the page. Bundles can be downloaded collectively as a single .zip archive, or separately based on SCAP bundle types (IE 7, Vista, Windows XP, Vista Firewall, XP Firewall) at this link: http://nvd.nist.gov/fdcc/download_file_fdcc.cfm.



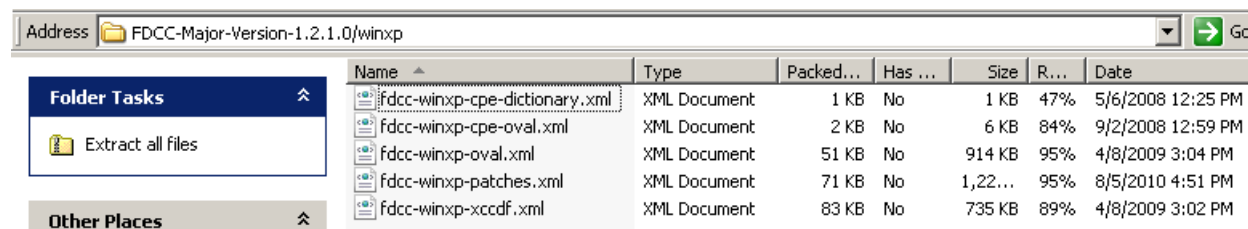
Tenable requires that all working files for XCCDF, OVAL and .nessus be kept in the xTool "resource" directory (XTool_<version>\data\resource). The xTool references files from this location and will generate errors or create incomplete reports if the reference files cannot be found or are an incorrect version.

As of August 2010, FDCC content uses the following archive file naming convention:

FDCC-Major-Version-<version number>-mmddyyyy-xxxx.zip

Download the file for OVAL version 5.3. For example, if the file version is w.x.y.z, then download w.x.1.z where 1 indicates OVAL version 5.3. As of March 2011, the latest OVAL 5.3 content available for download was version 1.2.1.0.

When this file is unzipped, folders that contain various platform categories are extracted. Within each folder, the actual SCAP content is available as displayed below:



Name	Type	Packed...	Has ...	Size	R...	Date
fdcc-winxp-cpe-dictionary.xml	XML Document	1 KB	No	1 KB	47%	5/6/2008 12:25 PM
fdcc-winxp-cpe-oval.xml	XML Document	2 KB	No	6 KB	84%	9/2/2008 12:59 PM
fdcc-winxp-oval.xml	XML Document	51 KB	No	914 KB	95%	4/8/2009 3:04 PM
fdcc-winxp-patches.xml	XML Document	71 KB	No	1,22...	95%	8/5/2010 4:51 PM
fdcc-winxp-xccdf.xml	XML Document	83 KB	No	735 KB	89%	4/8/2009 3:02 PM

SCAP Content Supporting Files

The following sections describe how to load these files into the xTool and generate audit policies that can be loaded into SecurityCenter.

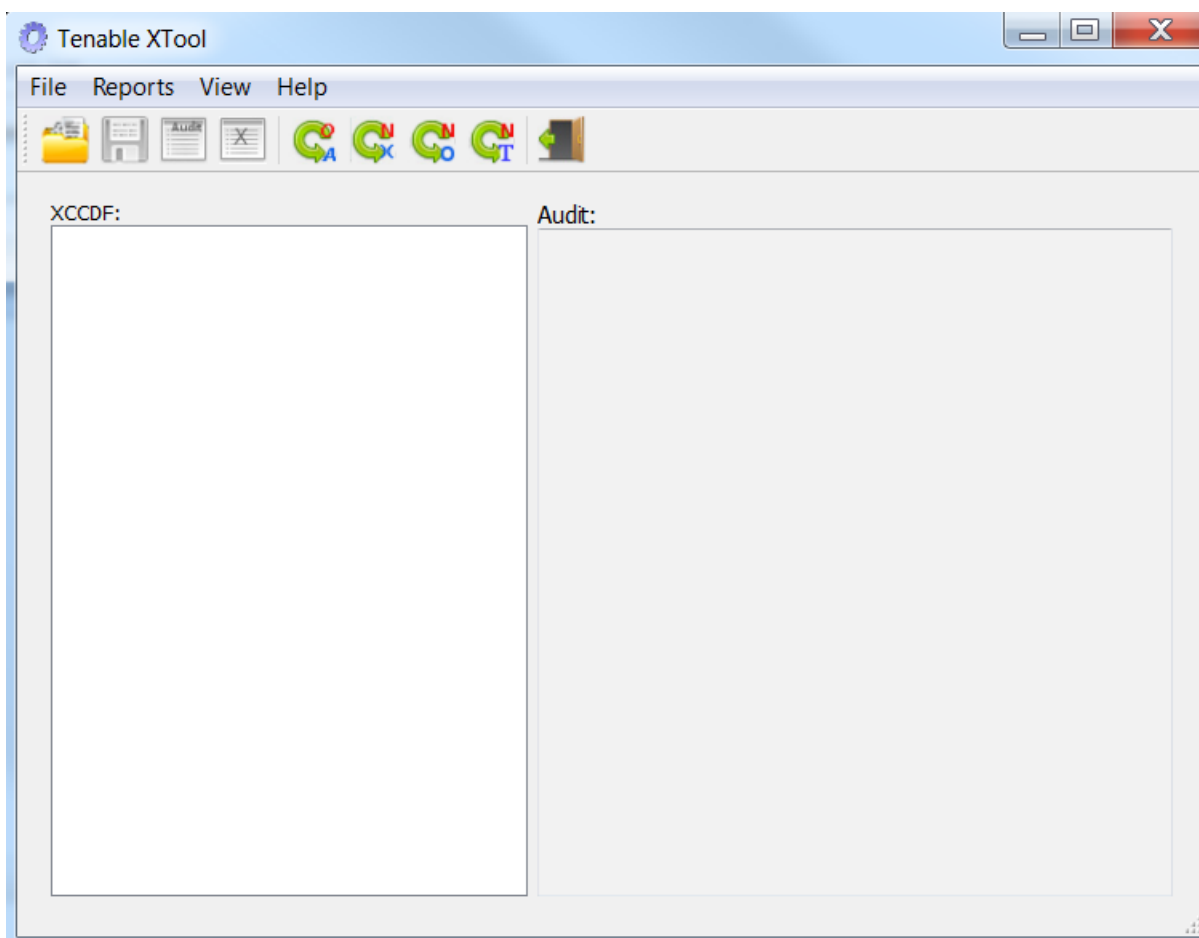
LOADING XML CONTENT INTO THE XTOOL

XCCDF to .audit



Click on the xTool user interface and then hover over the icons at the top of the interface to view item description tooltips.

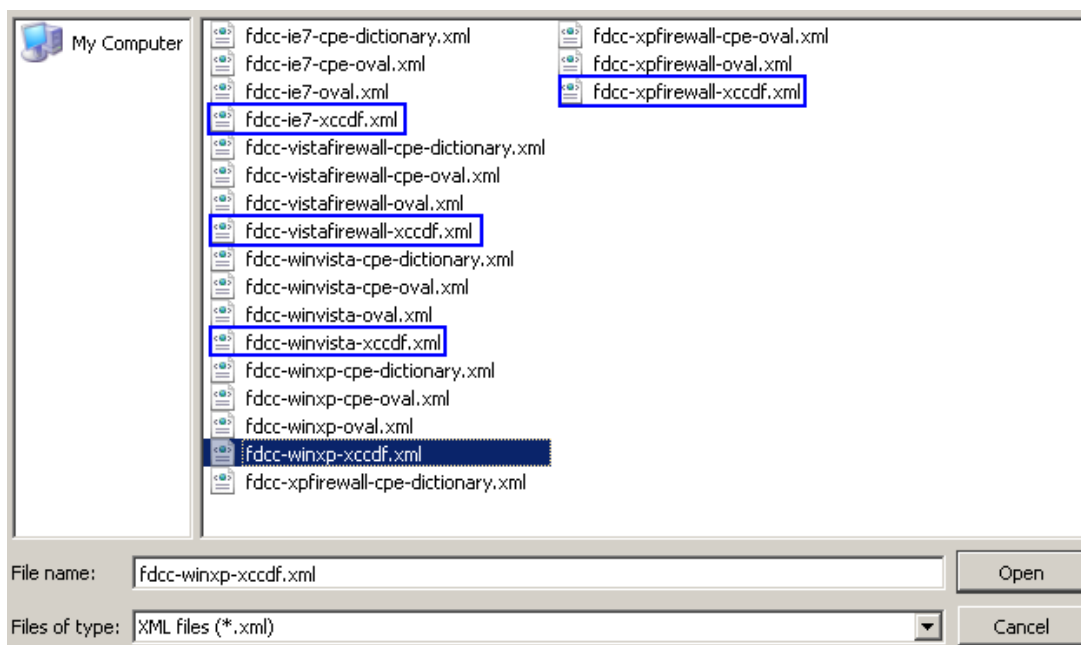
Running the xTool for the first time produces a blank output screen similar to the following:



The xTool Interface

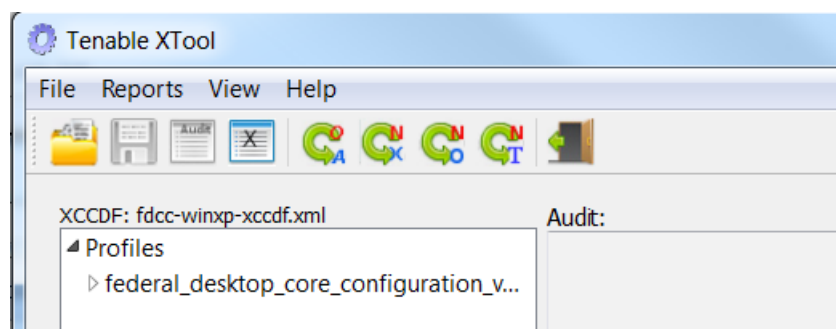
To load XCCDF content, click on the yellow browse icon in the upper left-hand corner, browse to and select the desired XCCDF XML file.

Many XML files are distributed in the FDCC content. These files define the checks (in OVAL) and the target platforms (CPE). The xTool expects a file with an "xccdf" string in the filename to be loaded as the reference file. A list of some of the valid XCCDF files distributed with the FDCC content is shown below:



Scap Content Profiles

After loading the content, the xTool window displays the available profile(s):



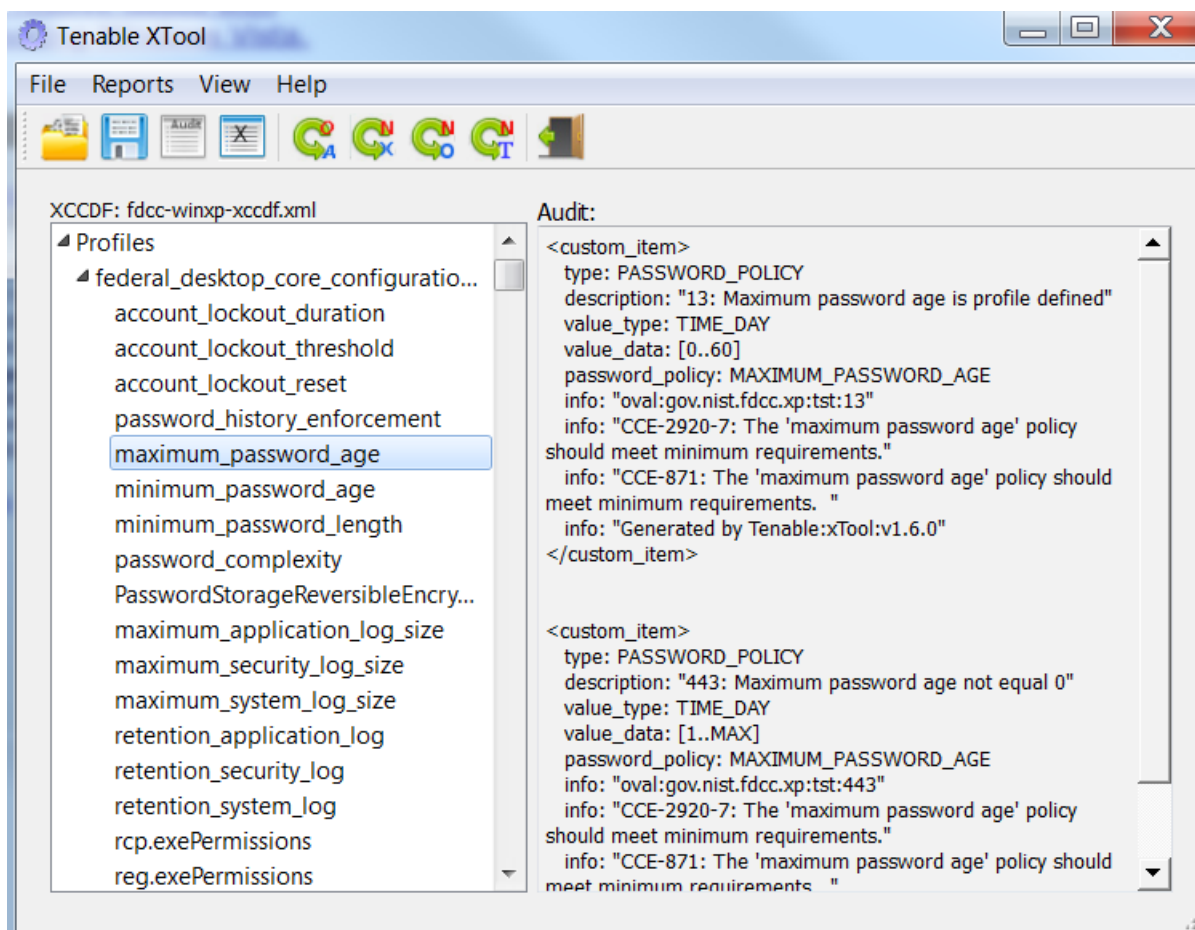
Available Profiles

If multiple profiles are available, the xTool will display them in the left-hand window. In the above screen capture, only one profile ("federal_desktop_core_configuration") is available.

GENERATING AN AUDIT POLICY

Selecting a Profile

Clicking on a profile name causes the xTool to expand this selection into a tree view. Each name of the audit specified in this profile is shown and in the bottom right window the relevant Nessus audit logic is also displayed, as shown in the following example:



Profile Items

Profile item names that start with a tilde (~) indicate a test for which no OVAL check is available or perhaps an OVAL definition containing an error.

Save a .audit File

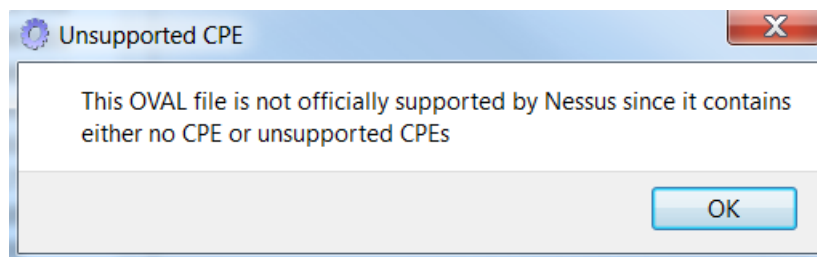


To save an audit file for a profile, highlight the profile and click on the **Save** icon. This opens a file save dialogue box to save the file (with a **.audit** extension) to a location of your choosing. After saving the **.audit** file, upload it to SecurityCenter for addition to the desired scan policy. The steps to perform this action are detailed in the "**Working with SecurityCenter**" section below.

OVAL to .audit

In the steps above, we used the xTool and XCCDF content to generate an audit policy. The user can also use the OVAL content to generate audit policies (and subsequent **.audit** files). This option is typically for advanced users who write their own OVAL content for use with Nessus/SecurityCenter. Audit files created with this method may work, but are not officially supported.

Click on the OVAL to `.audit` option and then follow the same steps provided for XCCDF to `.audit` policy generation. Before saving the `.audit` file, an "Unsupported CPE" warning dialog must be acknowledged.




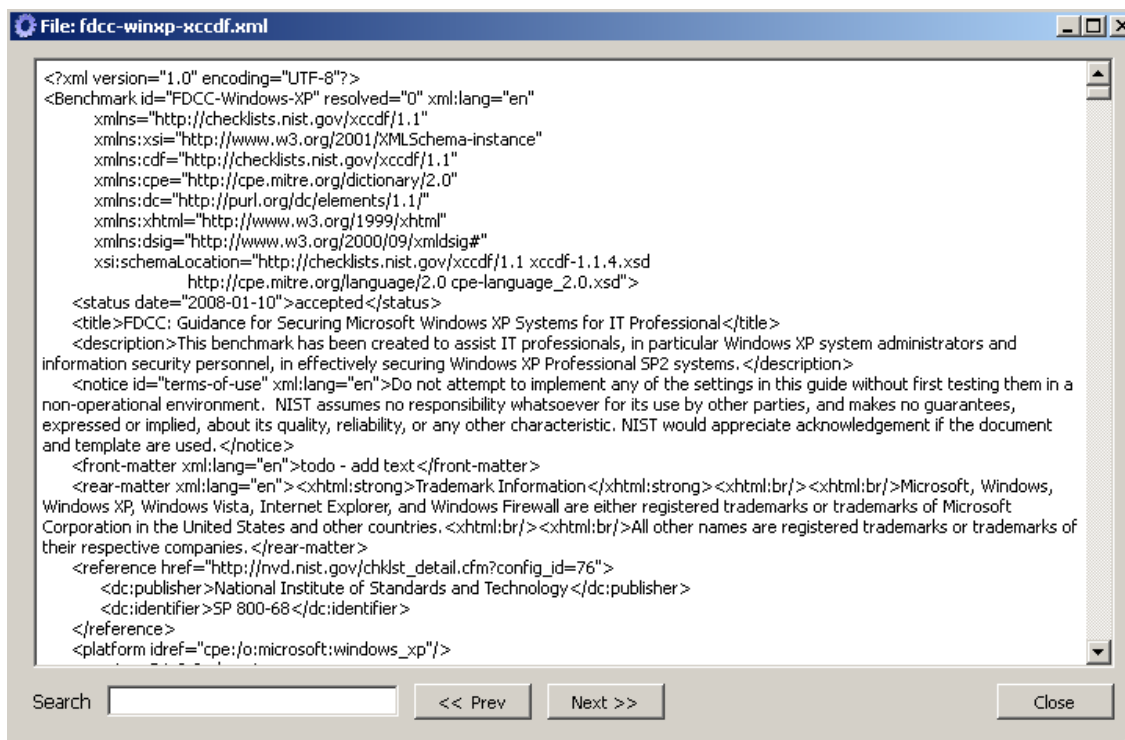
Standard OVAL to Audit Message

After acknowledging the warning, the `.audit` file is then loaded into SecurityCenter or Nessus as detailed in the "[Working with SecurityCenter](#)" section of this document.

File Options

The xTool comes with four options for viewing and searching generated data:

- **View XCCDF File** – This option, available by clicking on this icon:  or through the "File" dialog, displays the XCCDF XML content that was parsed by the xTool. An example screenshot generated from the Windows XP SCAP content is displayed below:



XCCDF Source

- > **View OVAL File** – When using the OVAL to `.audit` option, the user can click on the “View OVAL File” option to view the source `.oval` file.
- > **View Audit File** – Once an audit file has been generated from the OVAL/XCCDF content, the “View Audit File” option may be used to display the actual audit file to be used by SecurityCenter or Nessus for system auditing.
- > **View Nessus File** – This option allows the user to view the currently loaded `.nessus` file.

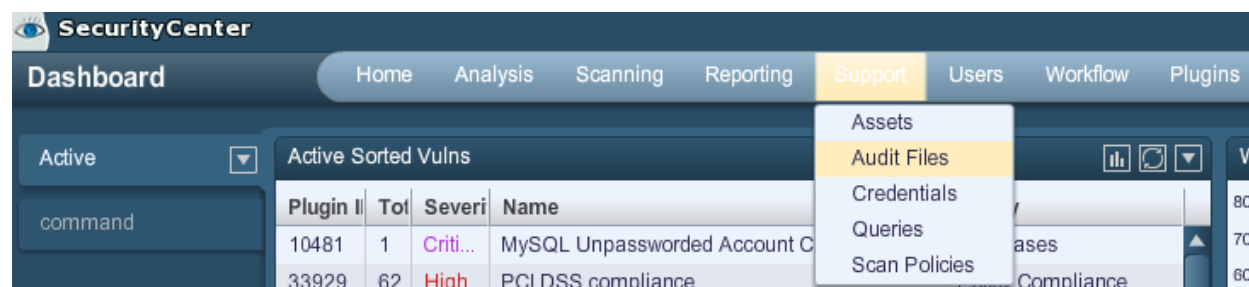
WORKING WITH SECURITYCENTER

LOADING THE AUDIT POLICY



Only users with the “Create Audit Files” permission can upload `.audit` files to SecurityCenter. The Organization Head and Administrator users always have this permission. Audit files uploaded by the administrator are available to any organization, while those uploaded by the Organization Head are available to their respective organization only.

The “**Audit Files**” window is available under the “**Support**” tab as shown below:



Loading the Audit File

This presents the user with a file upload option where a single audit file can be added to SecurityCenter.

ADDING THE AUDIT FILE TO A VULNERABILITY SCAN

Once the audit file is loaded to SecurityCenter, it can be used in a scan policy. One or more audit files can be specified in a scan policy. They do not all need to be based on FDCC or SCAP content. Vulnerability policy definition and usage is covered in SecurityCenter documentation.



The following blogs cover configuring the remote Windows XP and Vista host settings for SCAP certification testing:

<http://blog.tenablesecurity.com/2008/02/testing-windows.html> (Vista)

<http://blog.tenablesecurity.com/2007/09/using-nessus-co.html> (XP)

At a minimum, the policies must include the following:



The vulnerability scan credentials are added to the scan itself, and not through the scan policy creation dialog.

- > The specific audit policies to be used.
- > The selection of the "Policy Compliance" plugin family.
- > Port scanning options. If no vulnerability audits are being performed, consider disabling port scanning to speed up scanning.

ANALYZING SCAN RESULTS

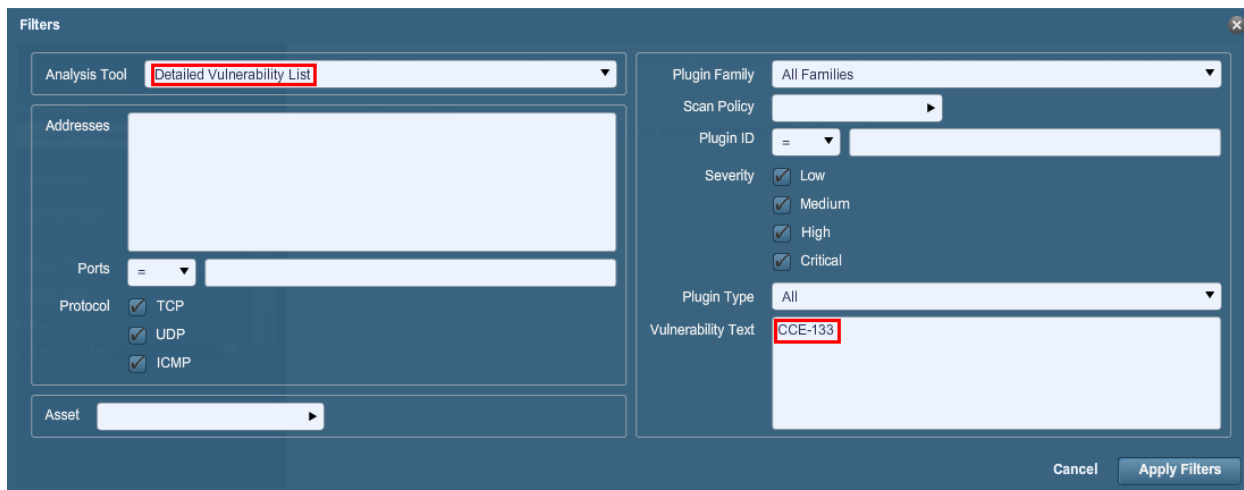
When scans complete, the results will be available in the **"Scan Results"** interface.

Important SCAP data references are available for querying from the Scan Results interface via the query and filter tools. A simple listing of configuration items found during an audit of an XP Professional host is shown below:

Scan Results						
Home Analysis Scanning Reporting Support Users Workflow Plugins						
All New Mitigated Source: FDCC_XP [2010-11-01] 649 results / 28 pages						
<div> <div>Vulnerability Summary</div> <div>Detailed Vulnerability List</div> <div>Vulnerability Summary</div> </div> <div> <div>Analysis Tool</div> <div>Vulnerability Summary</div> <div>Load Query</div> <div>Save as Query</div> <div>Show Filters</div> <div>Reset View</div> <div>Active Filters</div> </div>						
Plugin ID	Total	Severity	Name	Fan		
1000786	1	Low	133: Registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCom...	N...		
1000797	1	Low	143: Registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCom...	N...		
1000796	1	Low	142: Registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCom...	N...		
1000795	1	Low	141: Registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCom...	N...		
1000794	1	Low	140: Registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCom...	N...		
1000793	1	Low	139: Registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCom...	N...		
1000792	1	High	138: Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=537395248	N...		
1000791	1	Low	137: Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec has type REG...	N...		
1000790	1	High	136: Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=537395248	N...		
1000789	1	Low	135: Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec has type REG...	N...		
1000788	1	High	131: Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=2	N...		
1000787	1	Low	134: Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=1	N...		
1000798	1	Low	144: Registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLo...	N...		
1000785	1	High	130: Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=5	N...		
1000784	1	Low	129: Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel has type REG_DWO...	N...		
1000783	1	High	128: Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=1	N...		
1000782	1	Low	127: Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash has type REG_DWORD	N...		
1000781	1	Low	126: Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest=0	N...		
1000780	1	Low	125: Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest has type REG_DWORD	N...		
1000779	1	Low	339: Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShare...	N...		
1000778	1	Low	338: Machine registry key only has specific values System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\...	N...		
1000777	1	Low	337: Machine registry key has value System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration	N...		
1000776	1	Low	336: Machine registry key has value System\CurrentControlSet\Control\Terminal Server\UserConfig	N...		
1000775	1	Low	335: Machine registry key has value System\CurrentControlSet\Control\Terminal Server	N...		
First Prev 4 Next Last						

SecurityCenter Scan Results

Use the "Detailed Vulnerability List" filters **"Vulnerability Text"** field as shown below to locate SCAP relevant entries, such as CCE, CVE, CPE, or CVSS references.



SecurityCenter Filters

For more information on working with SecurityCenter, please refer to the SecurityCenter documentation located at: <https://support.tenable.com/support-center/>.

TECHNICAL ISSUES

There are several technical issues to be aware of when analyzing the test results:

- The Compliance Check Test Error will show as "ERROR" (medium severity) if an audit cannot be performed. It will report as a pass if there was an error at one point, but now scans have proceeded without issue.
- Tenable engineered the logic generated by the xTool to perform a "CPE Platform Check". This check ensures that the host you are scanning for is the correct OS. For example, if you scanned a Windows 2003 platform with an XP Professional policy, you would get a single result indicating a failure of this check. If this error is reported on a system that has the correct CPE, make sure the remote registry service is running before re-running the scan or use the option "SMB Registry : Start the Registry Service during the scan".
- The Xccdf_Scan_Check is also a check derived from the XCCDF content that identifies a variety of the parameters used.

CREATING FDCC XML REPORTS

CONCEPT

For FDCC reporting, NIST requires that you submit a sample of your non-compliant hosts. Although SecurityCenter has the ability to export **all** compliance data as a Nessus XML report that can be loaded into the xTool, this can sometimes be impractical.

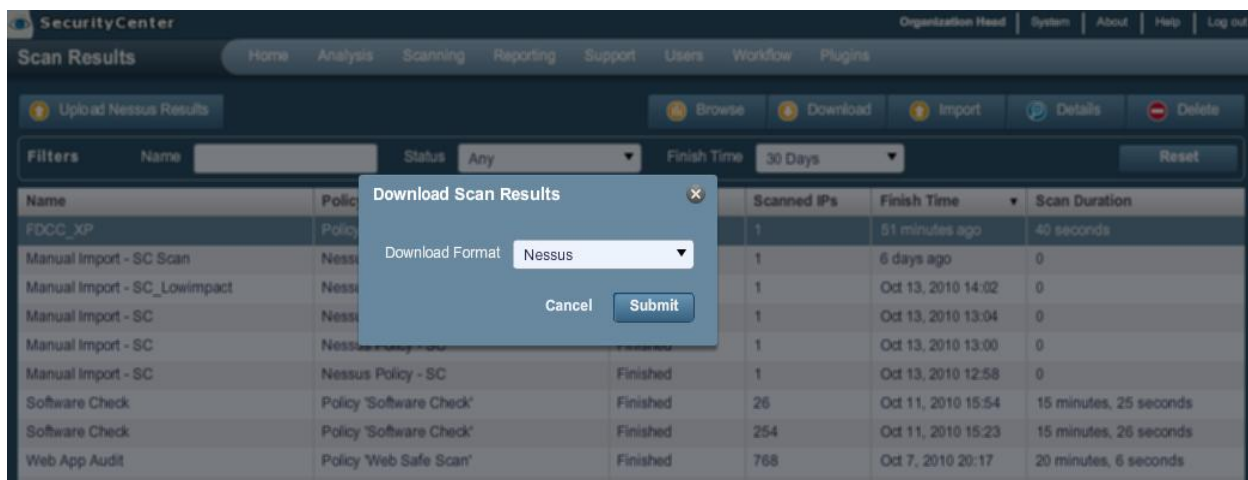
Instead, Tenable recommends that SecurityCenter be used to identify profiles of likely non-compliant hosts. Your organization may have made exceptions to the FDCC standard in several different ways. Using the various asset summary and reporting tools within SecurityCenter, you can identify which assets or hosts are likely in compliance or are not in compliance with FDCC and the exceptions.

Once these exceptions are identified, perform a full audit of each of them. If you wish to create a single scan job to perform this task, you can use a list of IPs or create an asset list to scan them.

Tenable also recommends that this scan be performed with as detailed an audit file as possible. The minimum settings for the audit policy to work include the CCE naming, the name of the audit policy used, and the date the audit was created.

DOWNLOADING SCAN RESULTS

To download your scan results for importing into the xTool, choose the **“.nessus”** download format. This provides a zipped version of the report results. The name of the file will be in the format **<scanid>.zip** where the scan ID is the actual scan ID used in SecurityCenter. A screen capture of the download process is shown below:



Downloading Nessus Scan Results

CONVERTING .NESSUS TO XCCDF OUTPUT

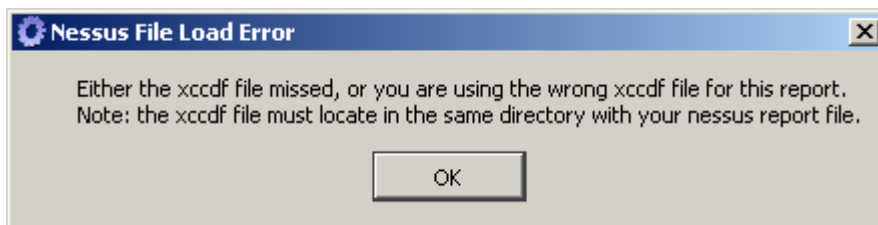


Only **“.nessus”** v1 formatted output as produced by Tenable’s SecurityCenter is supported by the xTool.

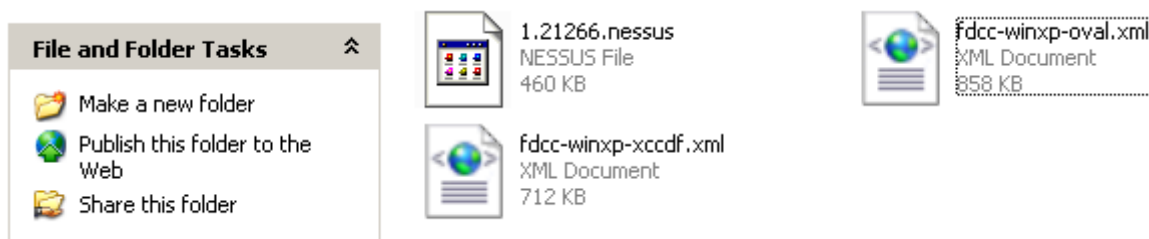


The corresponding XCCDF and OVAL reference files must be located in the same folder as the **“.nessus”** file for the import to occur.

1. First, copy the corresponding XCCDF and OVAL reference files to the folder where the **“.nessus”** file is located. If both of these files are not present in the same directory, an error similar to the one below is displayed:



In the example below, the `fdcc-winxp-xccdf.xml` and `fdcc-winxp-oval.xml` files are copied into the same directory as the `.nessus` file. Use the corresponding XML files based on the NIST bundle that your scan is based on.

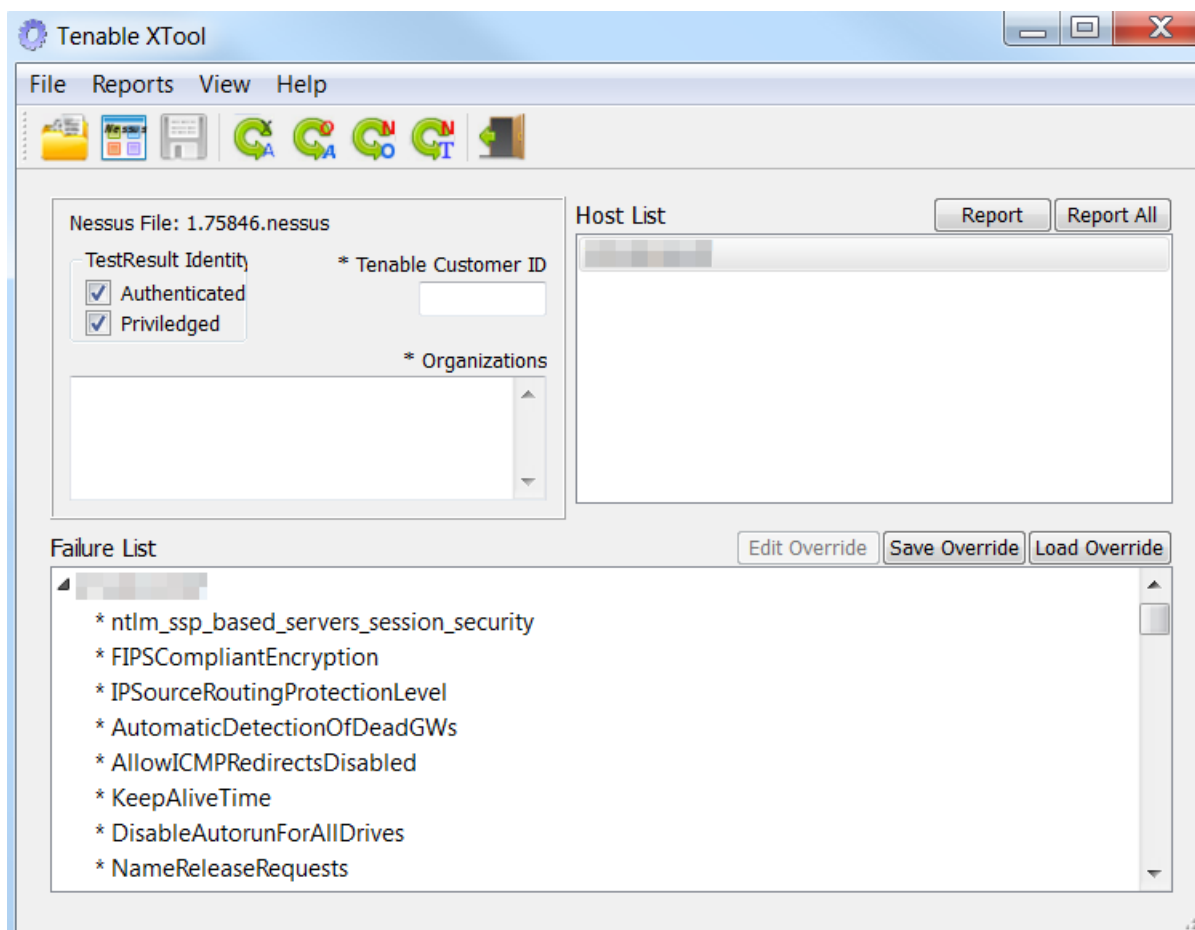


Nessus to OVAL/XCCDF Correlation

To load the Nessus report containing the non-compliant results from the SecurityCenter scan, click on the "Nessus to XCCDF" icon at the top of the interface and then click on the folder "Load" icon to browse for your `.nessus` file.



On loading, the xTool displays a list of IP addresses for which compliance data was found and also allows users to navigate through which CCE entries had compliant and non-compliant audit results. A screen capture is shown below:

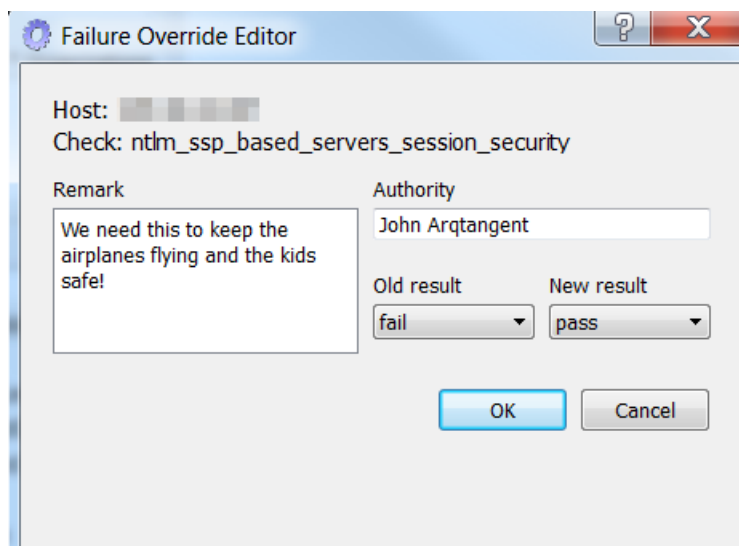


Nessus to XCCDF Interface

- Highlight the desired IP address(es) and then enter in your Tenable Customer ID and Organizations in the fields to the left of the host list. Perform any overrides as described in the section below and then click on the **"Report"** or **"Report All"** command buttons to generate the XCCDF report file. The resulting XCCDF report is saved as an XML file into the resource directory. This file can be submitted to NIST for processing.

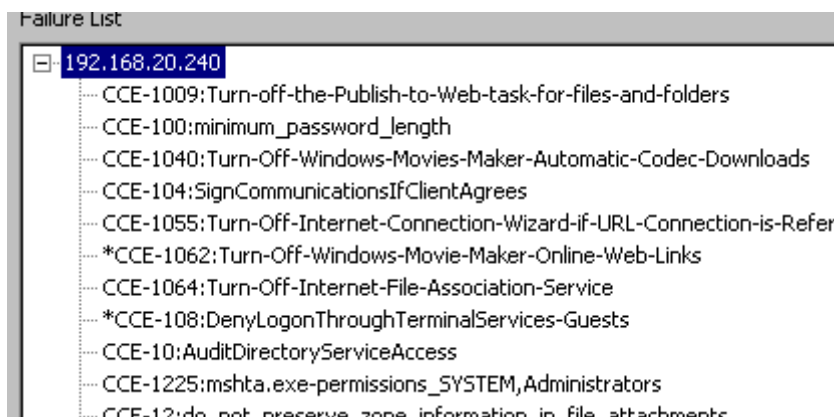
FILLING OUT NON-COMPLIANCE OVERRIDE ISSUES

The xTool allows tracking and editing of non-compliant issues. Clicking on a given discrepancy (failed audit) displays a dialog box that permits users to enter a remark. A screen capture is shown below:



Override Handling

CCE entries that have failure override data in them are indicated with an asterisk:



Overridden and Non-overridden Results

SAVING AND REUSING FAILURE OVERRIDE DATA

Since the process of filling out and tracking failure overrides and exceptions can be tedious, this data can be saved independently of the scan results.

After filling out the failure overrides, this data can be saved into a file with a **.fov** extension by choosing **Save Override**. This data can later be re-used by loading a scan and then choosing **Load Override**.

COMPLETING AND PRODUCING THE FDCC REPORT

Before any report can be saved, your Tenable Customer Support ID must be entered in the **"Tenable Customer ID"** field so that NIST can independently verify that you are using a certified FDCC solution. It is also required that you include information that describes your organization in the **"Organizations"** field. NIST uses this information to track FDCC compliance status.

There are two reporting options to produce the XML report: "Report" or "Report All". The IP addresses listed in the upper right "**Host List**" window can be toggled to specify which IP addresses to report on. Choosing either "**Report**" or "**Report All**" from the command options saves the results in an FDCC compliance XML report format. This file can be sent to NIST for analysis of FDCC compliance. For more information on FDCC compliance reporting, visit the NIST FDCC compliance reporting [FAQ](#).

VIEW OPTIONS

Other options are available from the "File" menu after the `.nessus` file has been loaded. The options are listed below:

1. **View Nessus File** – Displays the XML text from the loaded `.nessus` file.
2. **View XCCDF Report** – Displays the XML text from the generated report file.

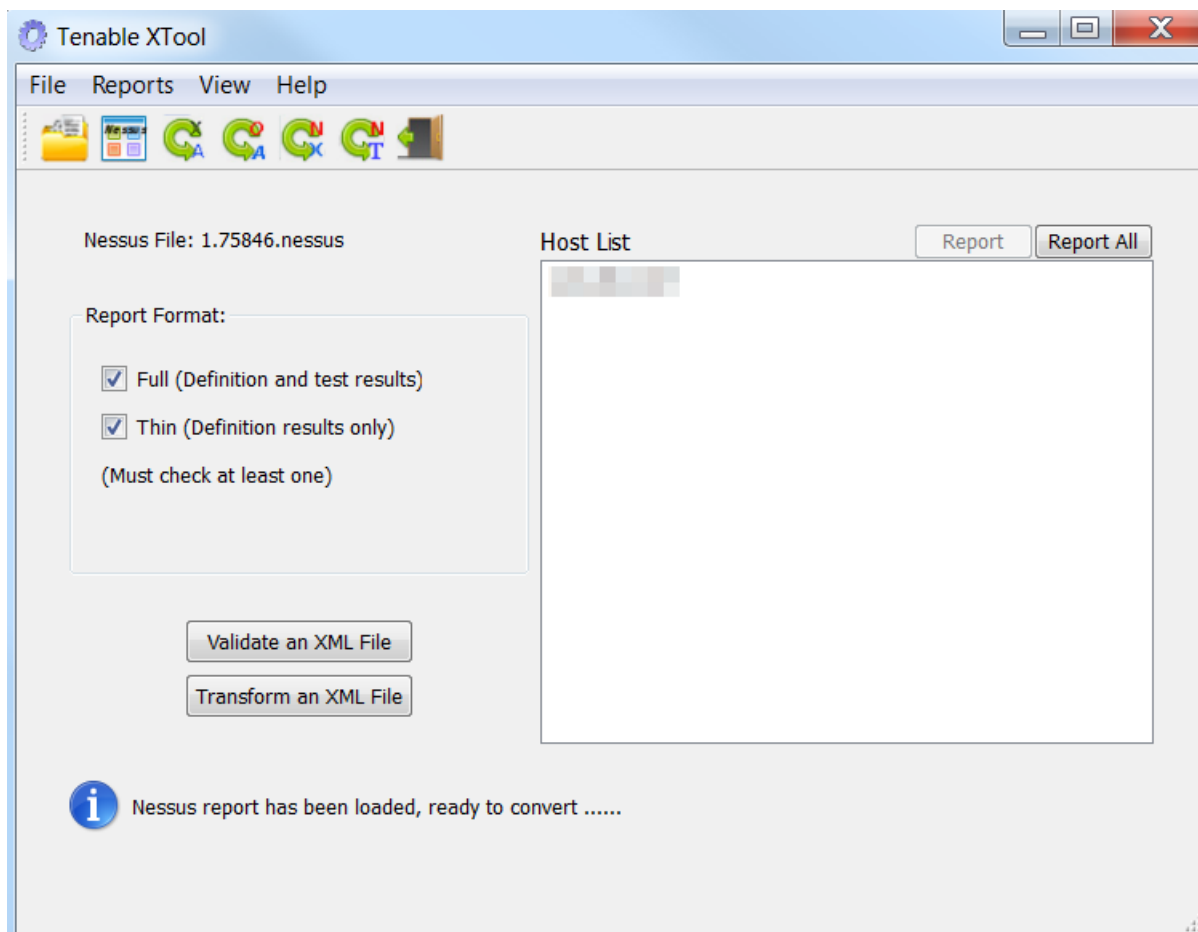
CONVERTING .NESSUS TO OVAL OUTPUT



Only `.nessus` v1 formatted output as produced by Tenable's SecurityCenter is supported by the xTool.

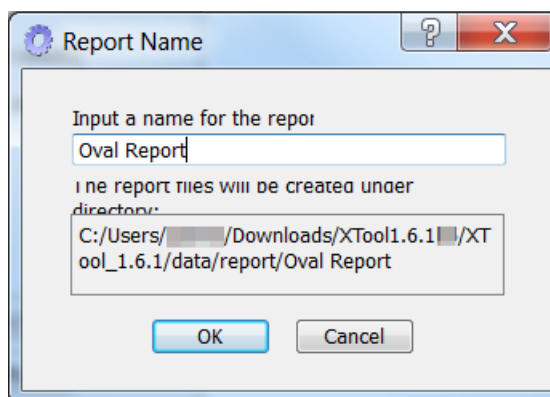


The xTool will only supports the OVAL/XCCDF content provided by the xTool for the `.nessus` to OVAL conversion process. This is the content that comes preloaded in the "resource" directory. Newer versions of content will appear periodically on the NIST web site and are updated in newer releases of the xTool during the SCAP recertification process.



Nessus to OVAL Transform Interface

The OVAL output format is an alternate viewing output. The screen capture above shows a host that has been loaded from an exported SC .nessus file and is ready for OVAL reporting. To complete the process, highlight the desired host(s) and click on "**Report**" (for a single host), or "**Report All**" (where many hosts exist). When prompted, enter the desired output location and click on "**OK**".



OVAL Report Designation

In the example above, the report is placed in the “report” folder with the name specified. This path is not configurable.

Validate an XML File

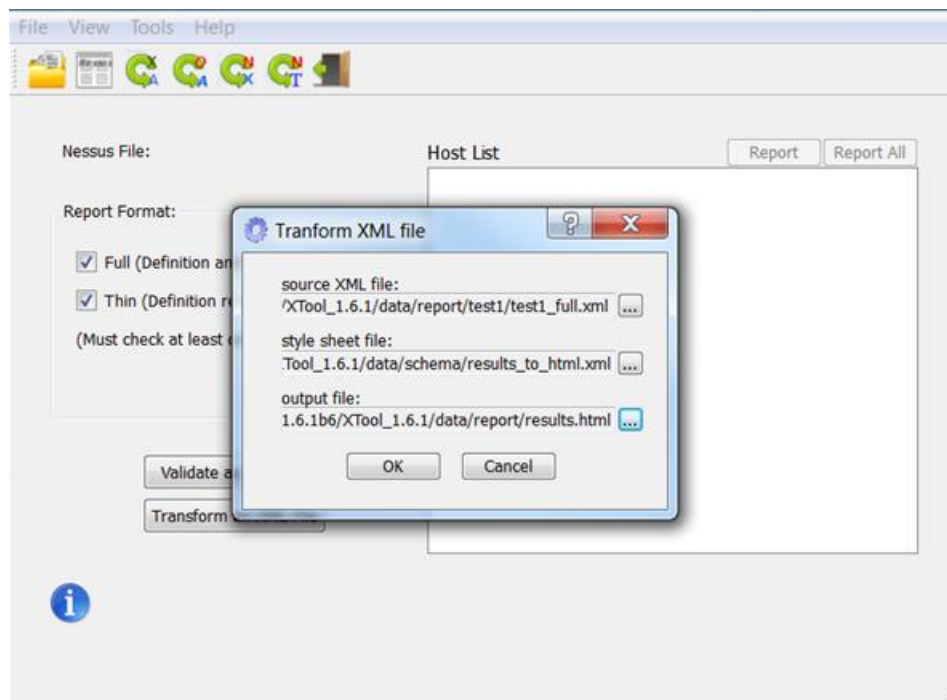
This command button validates the syntax of the provided XML file matches the NIST submission requirements.

Transform an XML File



The HTML file created by this transformation is not used for submission to NIST, but provides a better gauge of pass/fail than the OVAL or FDCC reports, which are intended primarily to be machine readable.

The “Transform an XML File” command button allows users to convert the OVAL output XML to a human-readable HTML file using the NIST-provided `results_to_html.xml` stylesheet. See the screen capture below for the transform dialog:



Transformation Completion

In the example above, `test1_full.xml` is the generated OVAL file content and `results_to_html.xml` is the stylesheet provided in the “/data/schema” folder of the xTool. The `results.html` file is the name we gave to our output file for viewing in a web browser. See the screen capture below for a sample results HTML file:



In the HTML output, the color scheme provided by NIST can be confusing. Orange cell coloring means the test passed, green means the test failed and gray or white means the check was not evaluated, not applicable or unknown.

OVAL Results Generator Information					OVAL Definition Generator Information				
Schema Version	Product Name	Product Version	Date	Time	Schema Version	Product Name	Product Version	Date	Time
5.3	Tenable SecurityCenter	4.0.3	2011-01-11	15:16:45	5.3	National Institute of Standards and Technology		2009-04-08	15:04:22

System Information	
Host Name	...
Operating System	
Operating System Version	
Architecture	
Interfaces	

OVAL System Characteristics Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.3	Tenable SecurityCenter	4.0.3	2011-01-11	10:09:15

Oval Definition Results				
<input type="checkbox"/> True	<input type="checkbox"/> False	<input type="checkbox"/> Error	<input type="checkbox"/> Unknown	<input type="checkbox"/> Not Applicable
<input type="checkbox"/> Not Evaluated				
OVAL ID	Result	Class	Reference ID	Title
oval.gov.nist.fidcc.xp.def.23	true	compliance	CCE-2929-0CCE-980	Account Lockout Duration
oval.gov.nist.fidcc.xp.def.25	true	compliance	CCE-2456-1CCE-733	Account Lockout Reset
oval.gov.nist.fidcc.xp.def.17	true	compliance	CCE-2920-7CCE-871	Maximum Password Age
oval.gov.nist.fidcc.xp.def.22	true	compliance	CCE-2889-4CCE-479	Passwords Stored Using Reversible Encryption
oval.gov.nist.fidcc.xp.def.203	true	compliance	CCE-3014-8CCE-265	Application Log Retention Method
oval.gov.nist.fidcc.xp.def.204	true	compliance	CCE-2336-6CCE-523	Security Log Retention Method
oval.gov.nist.fidcc.xp.def.205	true	compliance	CCE-2777-1CCE-864	System Log Retention Method
oval.gov.nist.fidcc.xp.def.27	true	compliance	CCE-3867-0CCE-3008-0CCE-2626CCE-2543	Account Logon Audit
oval.gov.nist.fidcc.xp.def.29	true	compliance	CCE-2905-6CCE-2902-5CCE-2000CCE-1645	Account Management Audit
oval.gov.nist.fidcc.xp.def.32	true	compliance	CCE-2100-6CCE-2243-2CCE-1686CCE-1744	Logon Audit
oval.gov.nist.fidcc.xp.def.40	true	compliance	CCE-2816-7CCE-2939-7CCE-2529CCE-2617	Audit Process Tracking
oval.gov.nist.fidcc.xp.def.243	true	compliance	CCE-3040-3CCE-332	Guest Account Status
oval.gov.nist.fidcc.xp.def.42	true	compliance	CCE-2344-0CCE-533	Local Account Use of Blank Passwords Limited to Console Logon Only
oval.gov.nist.fidcc.xp.def.45	true	compliance	CCE-3162-5CCE-2	Access Audit for Global System Objects Disabled
oval.gov.nist.fidcc.xp.def.52	true	compliance	CCE-2955-3CCE-905	Audit Backup and Restore Privilege Disabled
oval.gov.nist.fidcc.xp.def.6027	true	compliance	CCE-2851-4CCE-92	Audit: Shut down system immediately if unable to log security audits
oval.gov.nist.fidcc.xp.def.6029	true	compliance	CCE-3111-2CCE-919	Devices: Allowed to format and eject removable media
oval.gov.nist.fidcc.xp.def.56	true	compliance	CCE-2789-6CCE-402	Users Prevented from Installing Printer Drivers
oval.gov.nist.fidcc.xp.def.58	true	compliance	CCE-2974-4CCE-585	CD-ROM Access Restricted to Locally Logged-on User Only
oval.gov.nist.fidcc.xp.def.59	true	compliance	CCE-2873-8CCE-463	Floppy Access Restricted to Locally Logged-on User Only
oval.gov.nist.fidcc.xp.def.61	true	compliance	CCE-3087-3CCE-549	Secure Channel Data Always Digitally Encrypted or Signed

Nessus Transform HTML Report

TRANSFORM NESSUS TO OTHER FORMAT (LASR/ARF) WITH STYLE SHEET

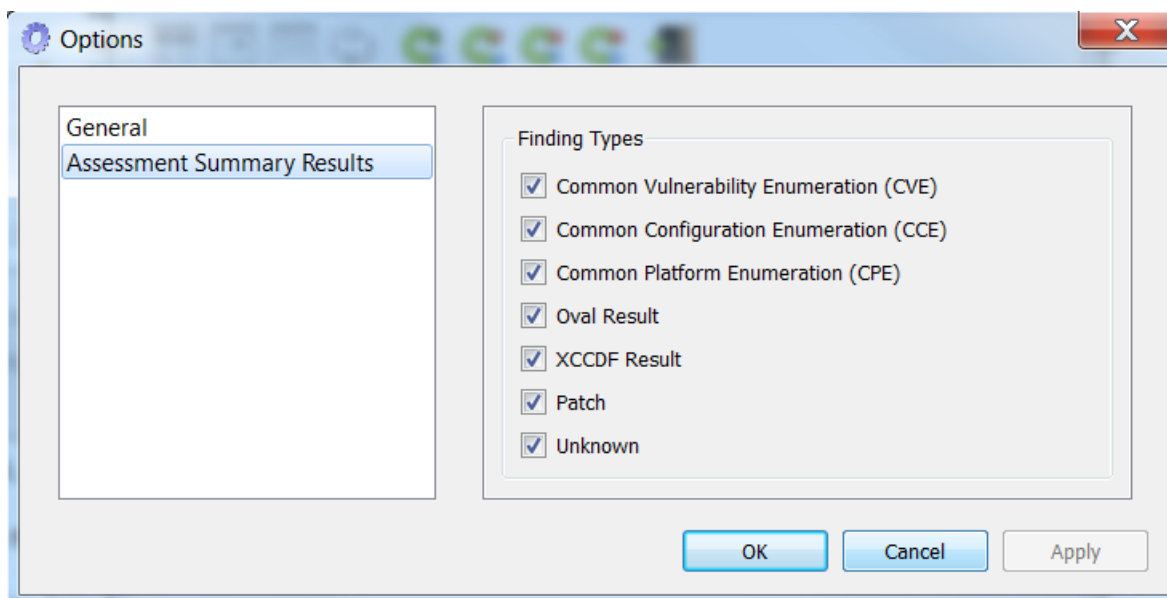
This tool allows the individual to convert existing .nessus files to either the LASR (Lightweight Asset Summary Results) or ARF (Asset Reporting Format) formats.



LASR and ARF are specialized formats for [CyberScope](#), an application developed by the Department of Homeland Security in conjunction with the Department of Justice to handle manual and automated inputs of agency data for FISMA reporting. The formats are not currently required for the SCAP certification process.

The ARF standard describes an eXtensible Markup Language (XML) schema for sharing per-device assessment results of devices on IP routed networks. The language is comprised of top-level and supporting schemas. The ARF language is a communication vehicle for sharing information grouped by individual findings per device.


There are seven LASR/ARF conversion output options available through the "File" -> "Options" -> "Assessment Summary Results" dialog as shown in the screen capture below:

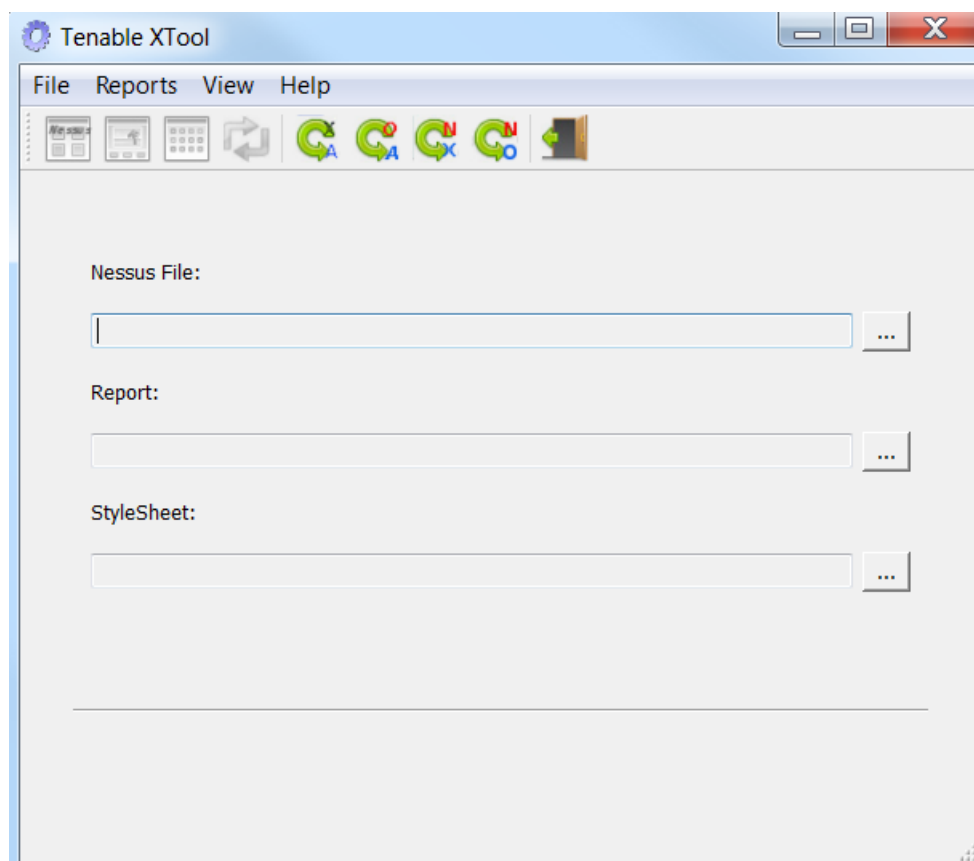


ASR Conversion Options

Each of these adds additional information to the audit file output to make it easier to track. As options are enabled or disabled, the audit window in the bottom right section is dynamically updated to show how new content and reporting options are displayed. You can toggle each of these items and inspect your changes in real-time. Each of the tags performs the following logic:

- > **Common Vulnerability Enumeration (CVE)** – In SecurityCenter, the "description" field becomes the unique name of the audit. Putting the CVE entry in this field makes all entries start with a common nomenclature. This makes sorting, reporting and reading the items within SecurityCenter easy and uniform.
- > **Common Configuration Enumeration (CCE)** – The CCE can optionally be included as additional information about the configuration audit. It will be displayed as part of the raw detail within SecurityCenter.
- > **Common Platform Enumeration (CPE)** – Typical XCCDF content includes free-form references to a wide variety of government standards. Enabling this feature includes this information as part of an audit. This data can be very detailed and Tenable recommends that audit files for large networks not make use of this data.
- > **OVAL Result** – Optionally include OVAL result data in the generated content. Enabling this option also includes this information in the audit policy.
- > **XCCDF Result** – This field enables tracking of multiple parameters such as the name of the SCAP policy, the date it was produced, its current accepted status and the date the audit file was generated.
- > **Patch** – If applicable, include host patch data in the result findings.
- > **Unknown** – Include data not belonging to any of the above categories in the result findings.

After selecting the desired output options, click on the transform icon  at the top of the interface or choose "Reports" -> "Nessus Transform". A screen similar to the one below is displayed:



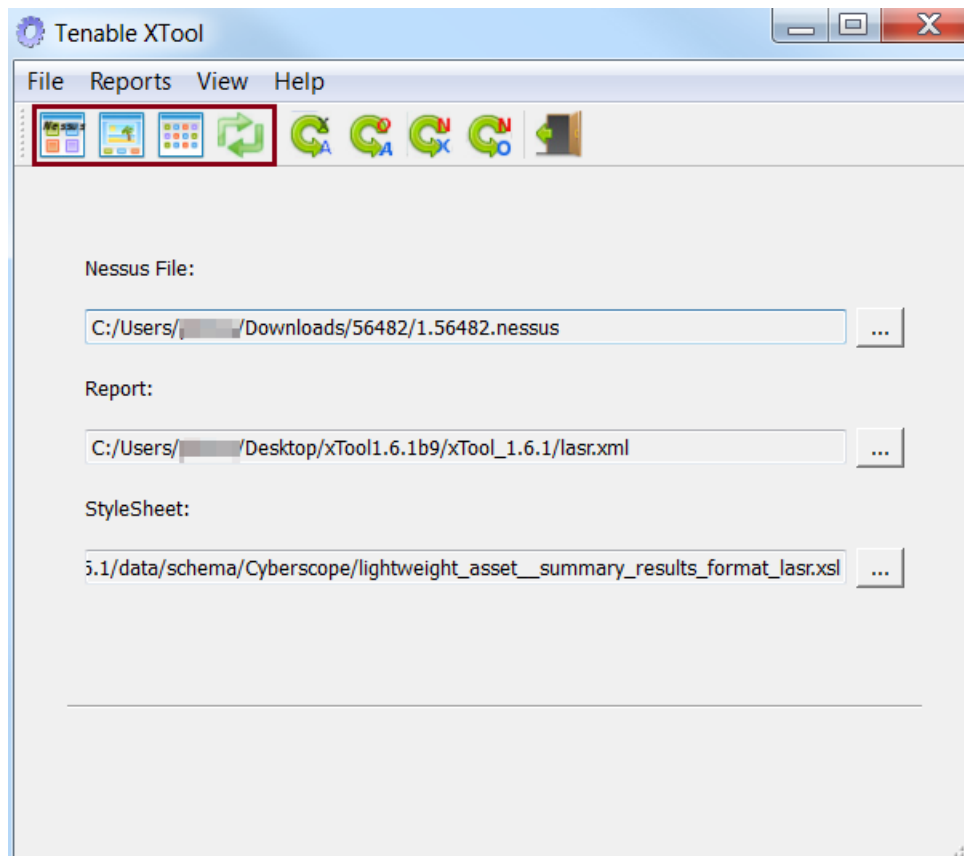
LASR Conversion Interface

Use the browse dialog to locate the `.nessus` file to report on. Click on the "Report" browse dialog to determine the name of the report to be generated. Finally, browse for the desired stylesheet.



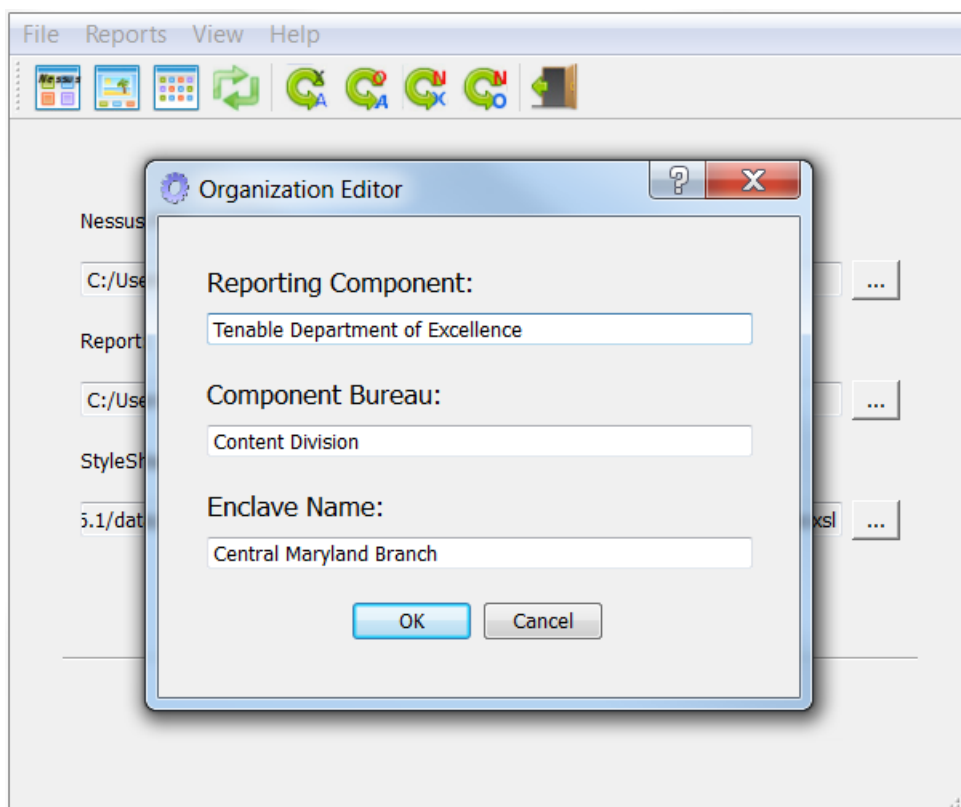
For the CyberScope data feed, you must use the `lightweight_asset_summary_results_format_lasr.xsl` stylesheet located in the "Cyberscope" folder to format the report into a manner suitable for submission.

After selecting the required fields, select the desired icon at the top portion of the interface:



LASR View Options

First, use the icon on the far right with the arrows to generate the desired report. After clicking on this icon, a screen similar to the one below is displayed:



LASR Organization Editor

The following items must be entered. These are used to identify agency and enclave information associated with the data feed:

- > **Reporting Component** – refers to a CyberScope value referencing a reporting component. For example, values such as “Department of Justice”, “Department of Transportation” or “National Institute of Standards and Technology” would be valid example entries for the first value.
- > **Component Bureau** – refers to a component-bureau, an individual FISMA reporting entity under a component. For example, under Department of Justice one might see values such as “Justice Management Division” or “Federal Bureau of Investigation”.
- > **Enclave Name** – refers to enclaves located within CyberScope associated with a specific component or bureau. Agency administrators and agency points of contact (“POCs”) are responsible for creating enclaves within CyberScope.

After completing these values and clicking on “**OK**”, click on the top middle icon to view the generated XML report. The icons on each side are for viewing the source `.nessus` file (on the left) and viewing the associated stylesheet (on the right). The XML report is now ready for submission via the CyberScope application. Please refer to the NIST CyberScope site for more information: <http://scap.nist.gov/use-case/cyberscope/index.html>.

ABOUT TENABLE NETWORK SECURITY

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit <http://www.tenable.com/>.

Tenable Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410.872.0555
www.tenable.com