Enhanced SCAP Editor (eSCAPe) User's Guide

eSCAPe User's Guide
Revision: 11292012

Contents

Introduction

The Enhanced SCAP Editor (eSCAPe) software package enables creation of Security Content Automation Protocol (SCAP) content in response to time sensitive security alerts.

SCAP content consists of system tests written in the Open Vulnerability Assessment Language (OVAL) and Open Checklist Interactive Language (OCIL) and enumerated in Extensible Configuration Checklist Description Format (XCCDF). It allows security operators to specify in a standard language what attributes and properties are to be inspected on IT systems. OVAL tests can address questions regarding the security posture, software vulnerabilities, and presence of malware on a system. OCIL questionnaires provide a way to pose a variety of questions to a human respondent. The introduction of eSCAPe expedites and reduces the amount of human error in SCAP content creation.

When SCAP content generated with eSCAPe is run on a NIST-validated SCAP compliant tool such as McAfee Policy Auditor (HBSS) or the SPAWAR SCAP Compliance Checker (SCC), what results is a transparent and scalable methodology for the detection of software vulnerabilities, configuration settings or malware and the foundation for a vulnerability and configuration management strategy. eSCAPe-developed SCAP content is frequently used to enable security operators to rapidly "spot check" an enterprise for the presence of malicious software or un-patched vulnerabilities.

eSCAPe has been used extensively in the generation of SCAP content to address Threat Information Product, Threat Activity Report, and Customer Response Form alerts from the Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE).

eSCAPe Features

- Full OVAL file creation
    - Creation of definitions, tests, objects, states and variables
    - Support for OVAL versions 5.3 - 5.10
- Full OVAL file editing
    - Support for OVAL versions 5.3 - 5.10
- Searching inside OVAL documents
- Full XCCDF file creation and editing
- Automated XCCDF generation from OVAL and OCIL documents
- Rapid OVAL and XCCDF creation with wizards
- CPE OVAL and CPE Dictionary viewing and creation
- Regular Expression Editor Tool and Validator Tool
- OVAL document merging
- Schema validation of OVAL and XCCDF documents
- Support for SCAP 1.2 (NIST Special Publication 800-126r2)
- SCAP Content use case Style Guidance

Installation & Getting Started

System Requirements

- A Java Runtime Environment (JRE) of version 1.6 or later must be installed. The Java JRE can be downloaded here: http://java.sun.com/javase/downloads/index.jsp
- The system should have at least 1GB of memory.
- Supported operating systems: Windows 2000/XP and later, Ubuntu Linux 9.10 and later

Installing with Source Files

Extract the eSCAPe archive files to a new directory. It is suggested that a folder be created in C:\Program Files named ‘eSCAPe’ and that the extracted files be placed there.

In the directory where the installation archive was extracted locate startEditor.bat and startEditor.sh. If you are using a Microsoft Windows system, double-click startEditor.bat to launch the eSCAPe Editor. On UNIX/Linux systems the startEditor.sh file can be used to launch eSCAPe.

These scripts will call Java with the appropriate arguments. These can be edited if you need to give JAVA more memory or set some other system property. Editing these files is only recommended for advanced users.

Navigating the Interface

Modes: Wizard and Standard

The eSCAPe Editor includes two interfaces for creating SCAP documents. The first is termed the ‘standard’ interface. Through this interface all features of the editor can be accessed by simply using the menu bar items. The ‘wizard’ interface will take the user directly into the flow of SCAP content creation through a more stream-lined process, but provides a more limited set of features. The wizard is a quick way to create SCAP content for simple tasks like checking for malware. Of course, the user is able to switch to Wizard Mode at any time by merely selecting it from the File menu.

When eSCAPe first launches, a mode selection window appears allowing for the selection of either the ‘Wizard-Driven’ or the ‘standard’ mode interfaces. If ‘Wizard-Driven’ is selected then the wizard selection window opens and eSCAPe enters wizard mode.

While in wizard mode the standard features of eSCAPe, including opening and editing of SCAP documents, are disabled. The disabled standard options appear grayed out in the menu. For a list of disabled standard mode operations while in wizard mode please see the table below. To return to Standard-mode, close the wizard windows.

Disabled Menu Options in Wizard Mode
'New' > 'OVAL' > 'Blank'
'New' > 'XCCDF' > 'Blank'
'New' > 'XCCDF' > 'From OCIL'
'New' > 'XCCDF' > 'From OVAL'
'Open' > 'CPE Dictionary'
'Open' > 'OVAL'
'Open' > 'XCCDF'

Table 1. List of disabled eSCAPe menu options while in Wizard Mode

See the figure below for an image of the interface selection window.

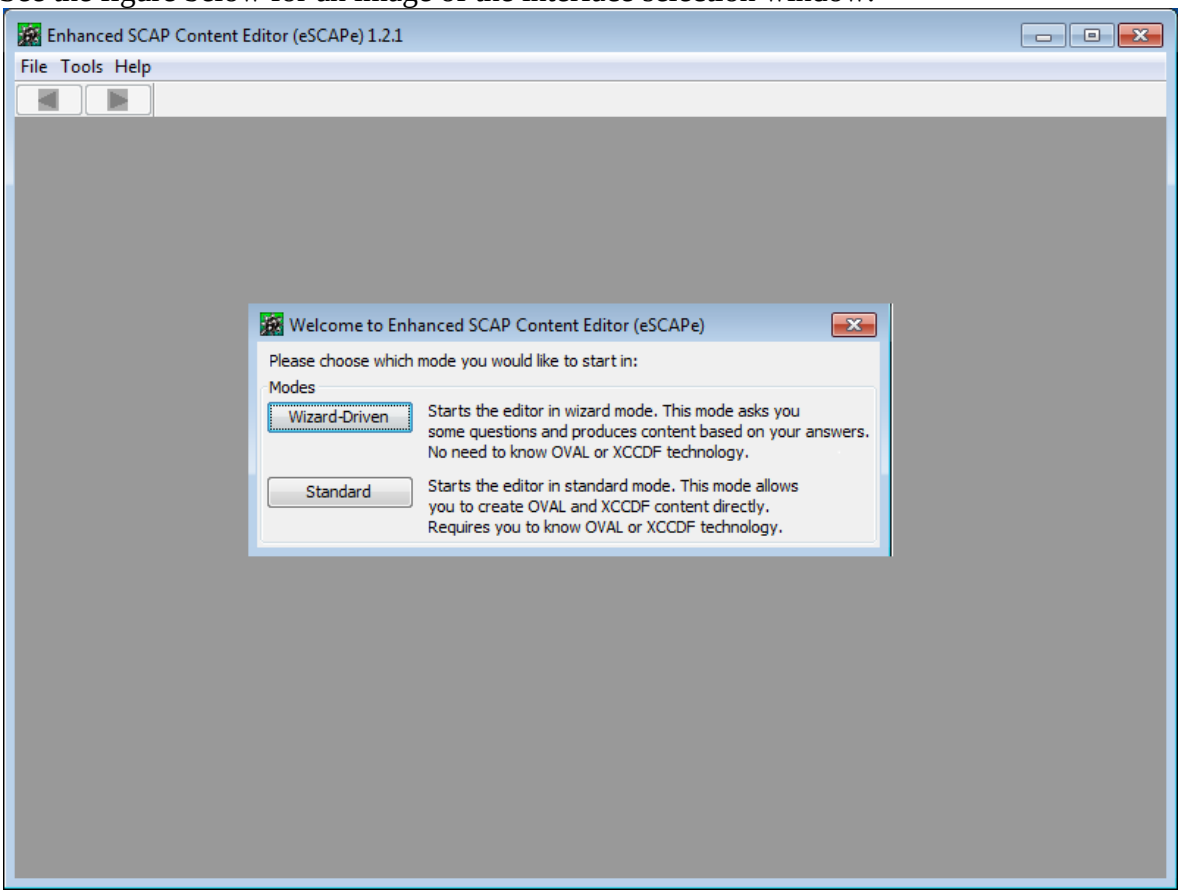

Figure 1. eSCAPe start screen displaying interface selection window

For more information on the Wizards please see the *eSCAPe Wizards* section below. For a step by step guide to using the eSCAPe wizards please see the use case example *Creating Malware SCAP Content with the Wizard*. When in standard mode the

application can be switched to wizard mode by selecting 'File' > 'Wizard Mode' from the File menu. See Figure 2 below for the Wizard Mode file menu item location.

The Menu Items

There are three application menus in eSCAPe:

1) File
2) Tools
3) Help

Under the File menu there are options for creating new files and opening existing files. Under the New menu, there are options to create a new CPE Dictionary, OVAL or XCCDF file. Under the Open menu there are options for opening CPE Dictionary, OVAL and XCCDF files, and an SCAP Data Stream. A list of recently opened files can be accessed with the Recent menu item. The 'Wizard Mode' menu option under the File menu, switches the interface to the Wizard Mode. See Figure 2 below to view the File menu layout.

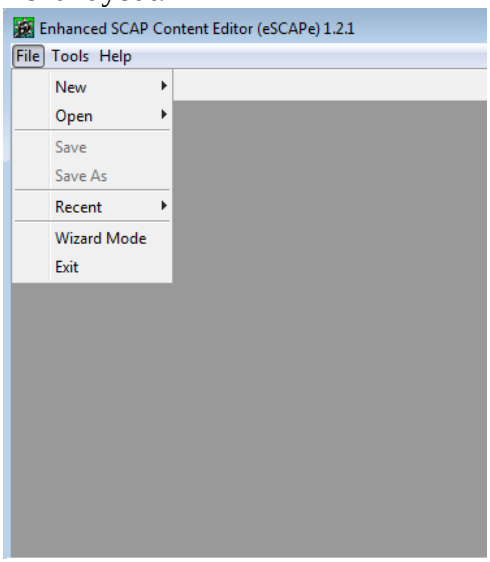

Figure 2. eSCAPe with File menu selected

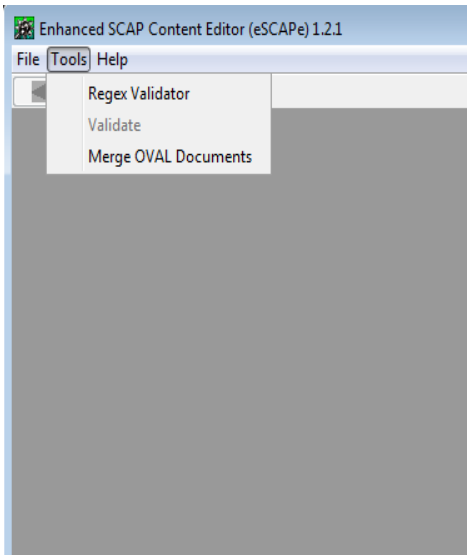

Figure 3. eSCAPe with Tools menu selected

Under the tools menu there are three tools available to users. The Regex Validator tool provides a graphical interface for constructing and testing regular expressions. Regular expressions are supported throughout eSCAPe in accordance with support for OVAL 5.3 and above. Regular expressions allow users to apply powerful pattern matching to system elements like file names and registry keys. The Regex Validator tool allows users to check that their expressions are working as expected. The Validate tool can be used to perform schema validation on open OVAL and XCCDF documents. This validation will alert the developer if the OVAL or XCCDF document does not conform to the proper structure dictated in the XML schema(s). Validation of SCAP content is considered a

best-practice step final step in the content creation process. See Figure 3 above to view the Tools menu layout.

The Breadcrumb Toolbar

The eSCAPe Editor includes a breadcrumb toolbar that can aid in navigating an OVAL document. While in standard mode with an OVAL document open and a test selected, if an object or state is double-clicked, the Editor will jump to that object or state and create a breadcrumb for the parent test in the toolbar. Later the breadcrumb can be clicked and the interface will return the user to the test. See the figure below for a view of an open OVAL document displaying the breadcrumbs toolbar in operation.

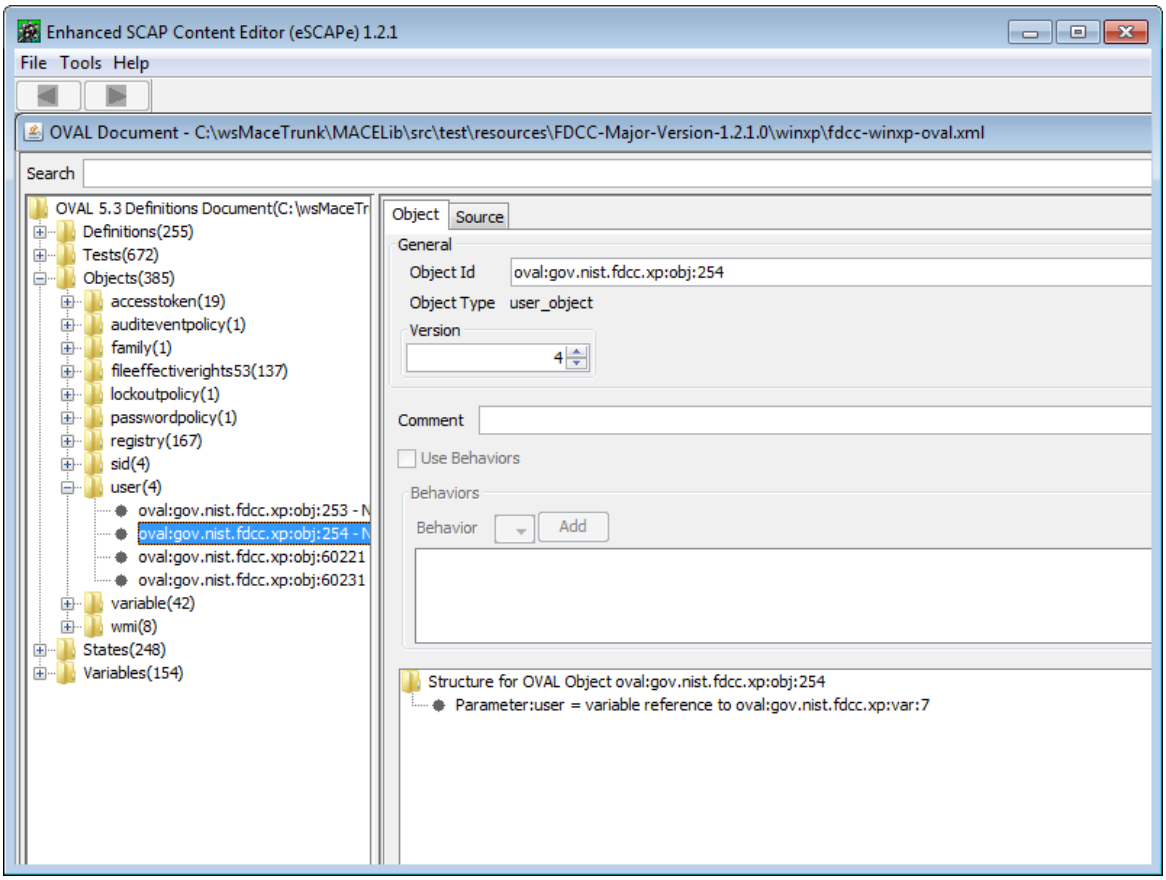

Figure 4. eSCAPe with open OVAL file displaying document tree, breadcrumb navigation toolbar, information area and search bar.

The Document Tree

In opened OVAL and XCCDF documents, an expandable and collapsible document tree allows for navigation of the SCAP document by structural groupings. For an OVAL file, the highest branching of the tree is the Definition level. This branches into Tests, Objects, States and Variables. In an XCCDF document the first branching is between Profiles and Groups. Expansion of profile elements reveal selected rules and expansion of Groups reveal groupings and then Rules. At the bottom of the document tree there are options for

'Expand All' and 'Collapse All'. These buttons provide a quick way to expand or collapse the entire document tree.

The Information Area

To the right of the document tree is the information area. Information on the currently selected item in the document tree is displayed in this area. In Figure 4 above, information on the currently selected User Test is being displayed in a 'Test' tab in the information area to the right. The test information can also be edited by adjusting settings, for example the test comment, in this area. For lists of

The Search Bar

The eSCAPe SCAP Editor includes a search bar for searching within open OVAL documents. Searches can be conducted using object comments and object IDs. Please see the top of Figure 4 above, for an image showing the search bar location.

Editors

There are three editor's provided with eSCAPe. The first editor allows for full editing and creation of OVAL documents. The second editor allows for partial editing and creation of XCCDF documents. The third editor allows for full editing and viewing of CPE OVAL and CPE Dictionary documents. The combination of OVAL, OCIL, XCCDF, CPE OVAL and CPE Dictionary documents is termed an "SCAP Data Stream." For more information on what defines an SCAP Data Stream please see NIST Special Publication 800-126r2 here: http://csrc.nist.gov/publications/PubsSPs.html.

OVAL Editor

The OVAL Editor allows for viewing and editing of opened OVAL files. This is the standard editor and provides full editing of OVAL documents version 5.3 - 5.10. To see an OVAL document in eSCAPe opened with the OVAL Editor view Figure 4 above.

OVAL Viewing and Editing

The OVAL Editor provides a range of features for editing OVAL and CPE OVAL documents. For a full list of the OVAL viewing and editing features, displayed in the eSCAPe information area, that are available to users, please see the table below.

Editor	Tree Node	Tabs	Information
OVAL	Definition	General	Displays an overview of the definition including Class, ID, Title and Version. A summary of the references is also displayed.
		Metadata	Displays metadata including Affected Platforms/Products. Title and description can be edited here.
		Criteria	Displays the criteria logic block. Tests and definition references can be added/removed and operators changed here.
		Source	Displays the XML Source of the

			selected definition.
	Test	Test	Contains 2 panes: General and Test Detail. Under the first pane the Test ID, Test Type and other attributes are displayed and can be edited. The second pane contains the object and state settings.
		Source	Displays the XML Source of the selected test.
	Object	Object	Displays and allows for editing of Object ID, type, version, comment, behaviors and parameters.
		Source	Displays the XML Source of the selected object.
	State	State	Displays and allows for editing of State ID, type, version, comment, behaviors and parameters.
		Source	Displays the XML Source of the selected state.
	Variable	Variable	Displays Variable type and allows for editing of Variable ID, version, data type, comment, possible_value and possible_restrictions.
		Source	Displays the XML Source of the selected variable.

Table 2. eSCAPe OVAL Editor Tree view elements and information area options and settings

XCCDF Editor

The XCCDF Editor allows for viewing and editing of opened XCCDF files. As different elements of the document are selected in document tree, their corresponding properties and settings appear on the right in the information area.

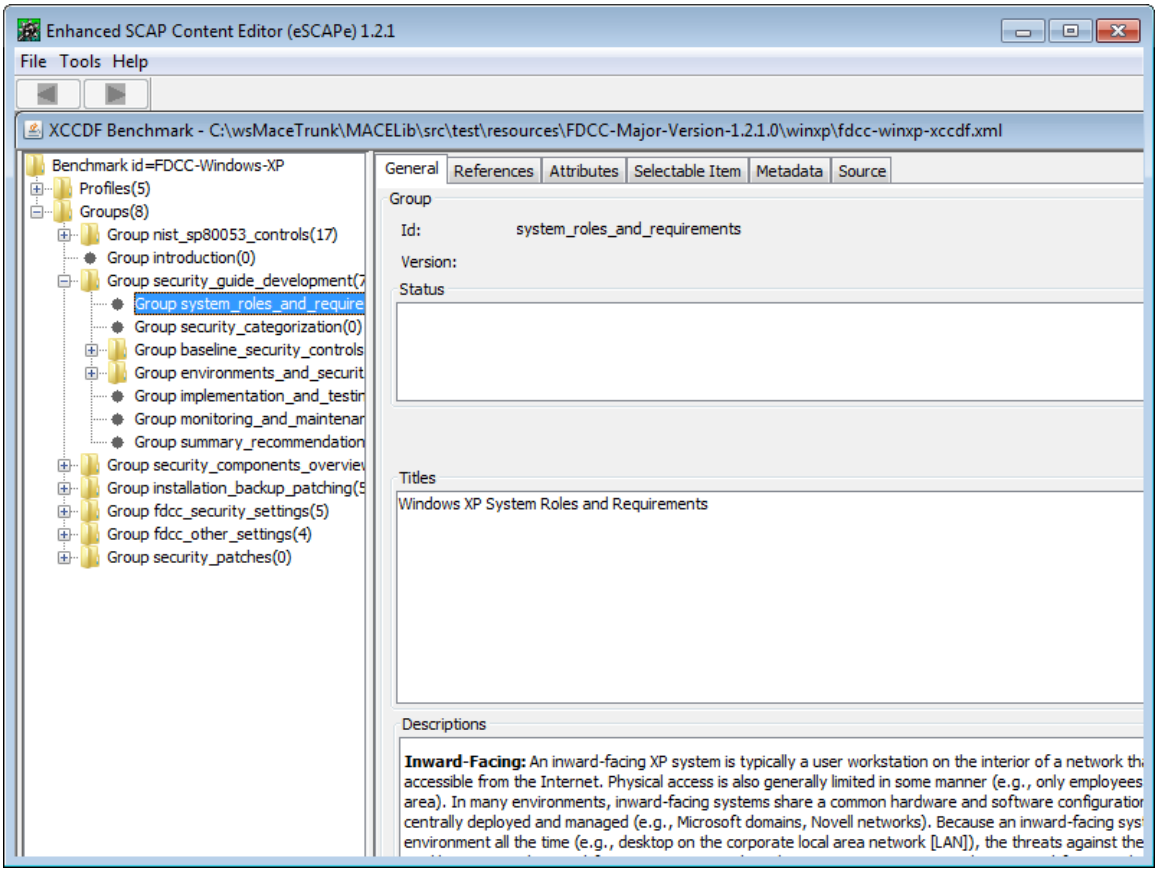

Figure 5. eSCAPe with an open XCCDF file - XCCDF Editor

XCCDF Viewing and Editing

The XCCDF Editor provides a range of features for editing XCCDF documents. For a full list of the XCCDF viewing and editing features, displayed in the eSCAPe information area, that are available to users, please see the table below.

Editor	Tree Node	Tabs	Information
XCCDF	Benchmark	General	Displays and allows for editing of benchmark ID, version, status, titles and descriptions.
		References	Editing of references and notices.
		Matter	Editing of front and rear matter metadata.
		Models	Editing/Viewing of associated benchmark scoring models.
		Platforms	Editing/Viewing of associated platforms.
		Attributes	Editing of associated style elements and the resolved attribute.
	Profile	General	Displays and allows for editing of profile ID, version, status, titles and descriptions.
		Attributes	Editing of note-tag, extends, abstract and

			prohibit changes attributes.
		Children	Lists all allows for editing of all selected and rule elements.
		Source	Displays the XML Source of the selected profile.
	Group	General	Displays and allows for editing of group ID, version, status, titles and descriptions.
		References	Editing of references, warnings and questions.
		Attributes	Editing of cluster-id, extends, abstract, hidden and prohibit changes attributes.
		Selectable Item	Editing/Viewing of Platforms, Requires, Conflicts, Rationales, weight and selected.
		Source	Displays the XML Source of the selected group.
	Rule	General	Displays and allows for editing of rule ID, version, status, titles and descriptions.
		References	Editing of references, warnings and questions.
		Attributes	Editing of cluster-id, extends, abstract, hidden and prohibit changes attributes.
		Selectable Item	Editing/Viewing of Platforms, Requires, Conflicts, Rationales, weight and selected.
		Role/Severity	Setting of multiple option, and selection of Role and Severity attributes.
		Checks	Editing/Viewing of selected Check Content Refs and Check Exports.
		Source	Displays the XML Source of the selected rule.
	Value	General	Displays and allows for editing of value ID, version, status, titles and descriptions.
		References	Editing of references, warnings and questions.
		Attributes	Editing of cluster-id, extends, abstract, hidden and prohibit changes attributes.
		Values	Editing/Viewing of type, operator and set values.
		Source	Displays the XML Source of the selected value.

Table 3. eSCAPe XCCDF Editor Tree view elements and information area options and settings

CPE Dictionary Editor

The CPE Dictionary Editor allows for viewing and editing of opened CPE Dictionary files. See the figure below for an image of the CPE Dictionary Editor with an open CPE dictionary file.

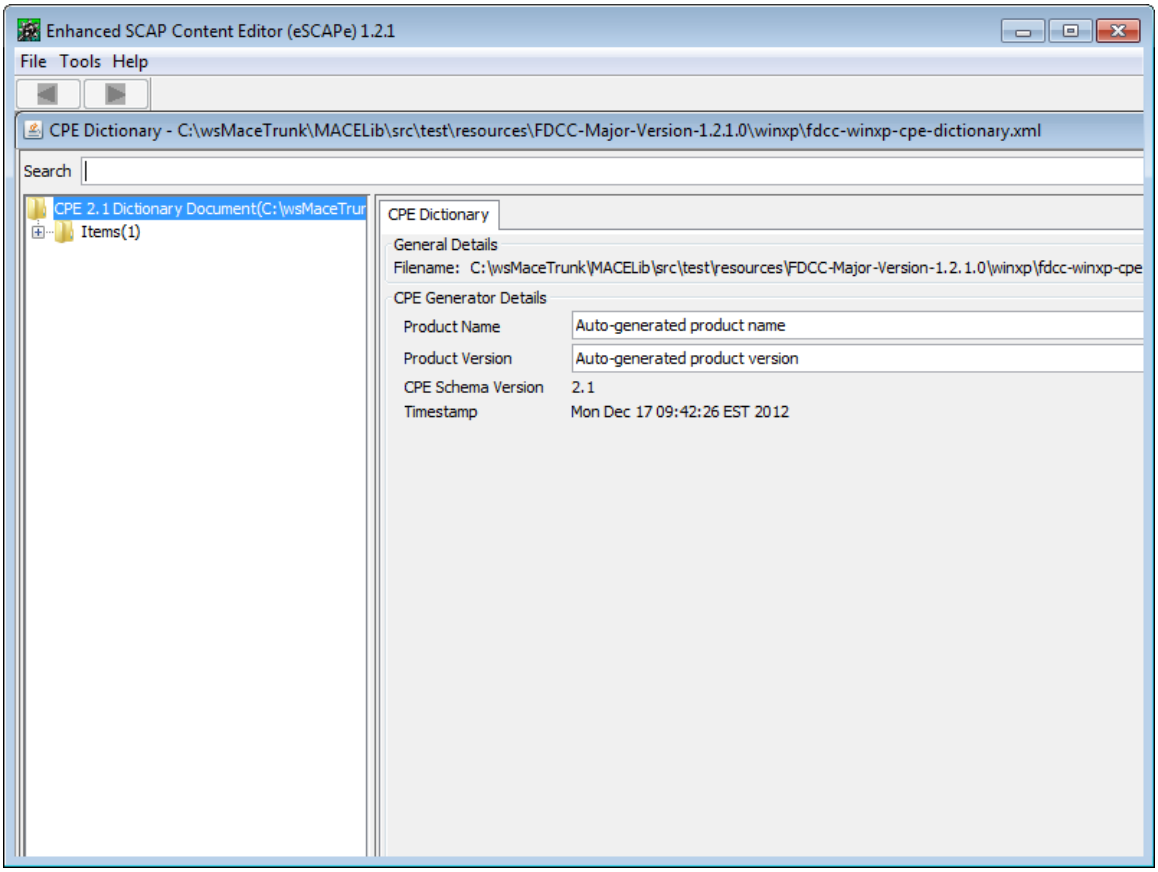

Figure 6. eSCAPe with an open CPE Dictionary file - CPE Dictionary Editor

CPE Dictionary Viewing and Editing

The CPE Dictionary Editor provides a range of features for editing CPE Dictionary documents. For a full list of the CPE Dictionary viewing and editing features, displayed in the eSCAPe information area, that are available to users, please see the table below.

Editor	Tree Node	Tabs	Information
CPE Dictionary	CPE Dictionary	CPE Dictionary	Displays CPE file details and allows for editing of generator Product Name and Product version.
	CPE Item	General	Displays and allows for editing of CPE ID, version, status, titles and descriptions.
		Titles	Editing/Viewing of associated titles.
		Notes	Editing/Viewing of associated notes and notes containers.
		Reference	Editing of associated references.

		Checks	Editing/Viewing of associated Check Refs.
		Source	Displays the XML Source of the selected CPE Dictionary.

Table 4. eSCAPe CPE Dictionary Editor Tree view elements and information area options and settings

The eSCAPe Wizards

The eSCAPe Wizards are designed for rapid creation of SCAP content. The wizards completely abstract the creation of the underlying SCAP documents and therefore present the user with the lowest requirement of understanding regarding SCAP protocols. Each wizard requires only 2 steps to create content and produces both an OVAL test file and an accompanying XCCDF checklist. The wizards are only capable of creating one test at a time. However the OVAL Merger utility included with eSCAPe can be used to group many OVAL tests created with the wizard into a single file for distribution. See the section *Using the Merge OVAL Documents tool* under *Additional Tools* for information on how to use the OVAL Merger tool. There are currently three wizards available for the rapid creation of SCAP content.

Available Wizards:

1. Windows File Test Wizard
2. UNIX File Test Wizard
3. Windows Registry Test Wizard

As described in the *Creating Malware SCAP Content with the Wizards* section, the eSCAPe wizards are particularly well suited for the generation of malware detection content.

Common Tasks

Opening and Navigating Files

OVAL

To open an existing OVAL document in eSCAPe follow the menu sequence File > Open > OVAL and then navigate to and select the OVAL file to open. An OVAL editor window will appear with the OVAL file that was chosen.

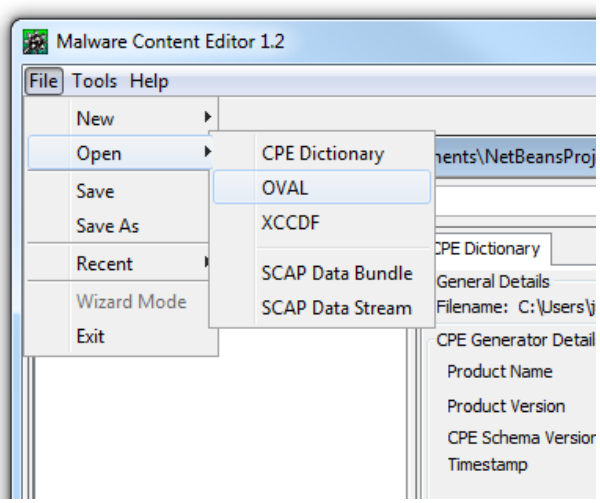

Figure 7. eSCAPe w/ menu Open OVAL

XCCDF

To open an existing XCCDF benchmark in eSCAPe follow the menu sequence 'File' > 'Open' > 'XCCDF' and then navigate to and select the XCCDF file to open. An XCCDF editor window will appear with the XCCDF file chosen. See Figure 7 above for an image of the XCCDF Editor with an open benchmark file.

CPE Dictionary

To open an existing CPE Dictionary file in eSCAPe follow the menu sequence 'File' > 'Open' > 'CPE Dictionary' and then navigate to and select the CPE Dictionary file to open. A CPE Dictionary editor window will appear with the CPE Dictionary file chosen. See Figure 6 above for an image of the CPE Dictionary Editor with an open CPE Dictionary file.

SCAP Data Stream

To open an existing SCAP Data Stream in eSCAPe follow the menu sequence 'File' > 'Open' > 'SCAP Data Stream' and then navigate to and select either a Data Stream archive (Zip) file or an XCCDF file that is part of an SCAP Data Stream. An SCAP Data Stream window will appear with the chosen CPE Dictionary files displayed in a window. See the figure below for an image of the SCAP Data Stream window with an open data stream.

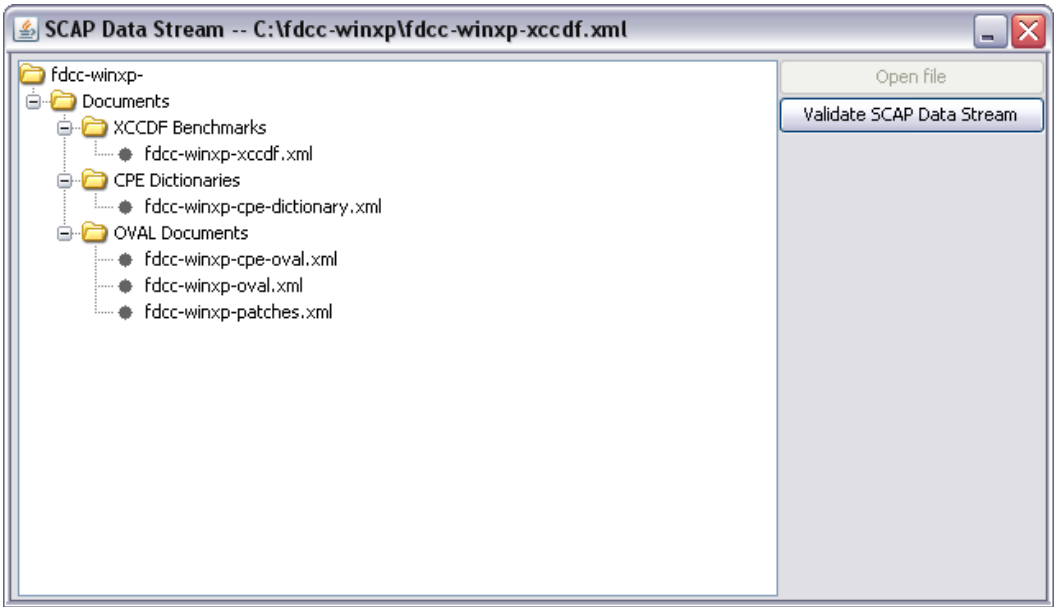

Figure 8. SCAP Data Stream window displaying stream files

Creating a New OVAL document

To begin creation of a new OVAL document, launch eSCAPe and from the menu select 'File' > 'New' > 'OVAL'.

Choosing Document Settings

In the first tab of the window that opens, select the OVAL version. For maximum compatibility choose OVAL version 5.3, for maximum functionality choose OVAL version 5.10. For information on available tests and features between OVAL versions see http://oval.mitre.org/oval/archive/.

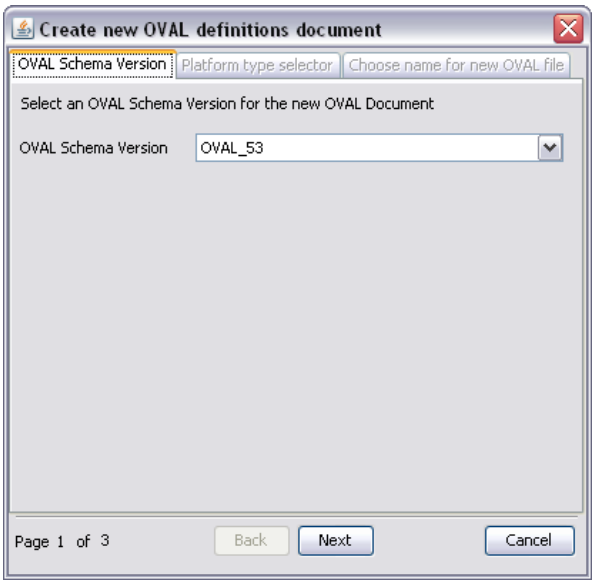

Figure 9. eSCAPe New OVAL window tab 1

In the next tab, select the target operating system platform from the available list. This should be the computing platform that the content is intended to run on.

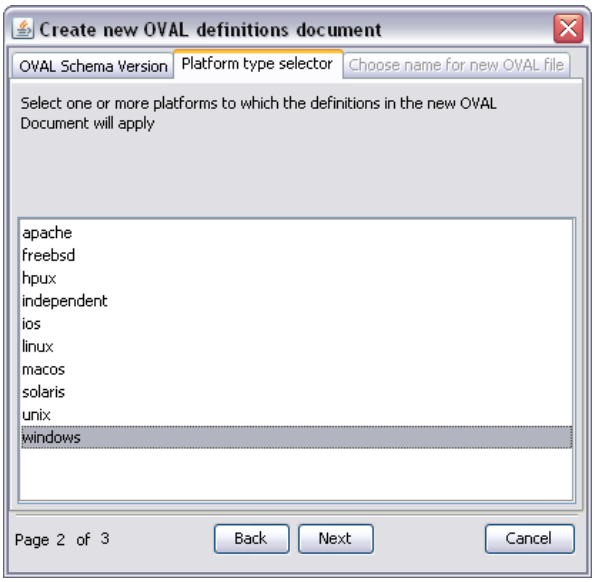

Figure 10. eSCAPe New OVAL window tab 2

Click 'Next' and then 'Browse' to navigate to a save directory and choose a destination file name for the new OVAL document. To complete this step click 'Finish'.

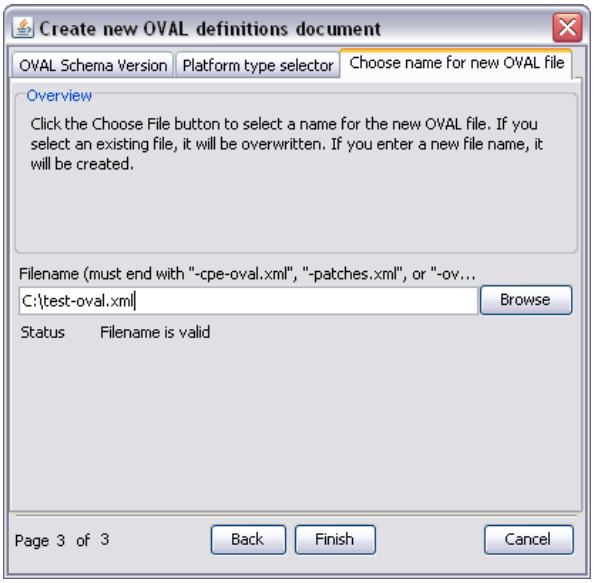

Figure 11. eSCAPe New OVAL window tab 3

Adding a Definition and Choosing Namespace

In the new opened OVAL file right click on the base node and select 'Add a Definition'.

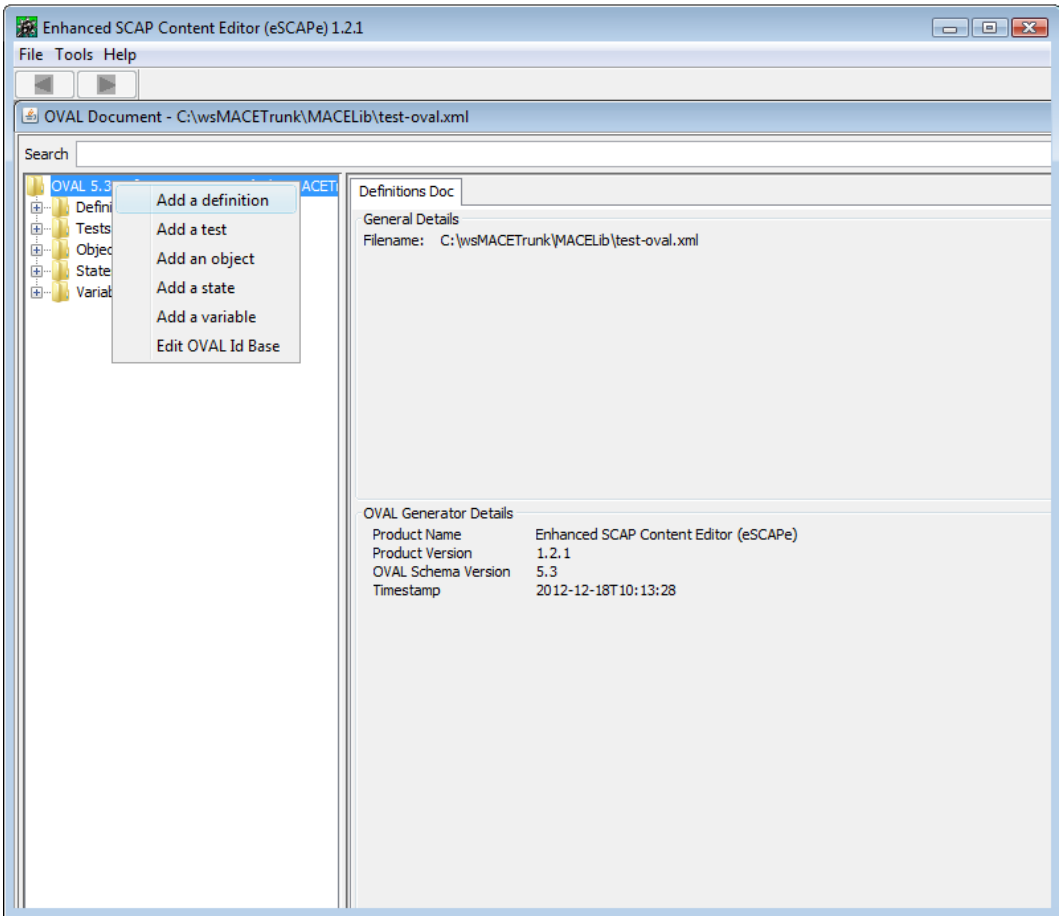

Figure 12. eSCAPe New OVAL – OVAL Editor with root node and context menu

In the window that opens select and enter an OVAL base identifier. This can be any string, but is generally used to indicate the source of the document.

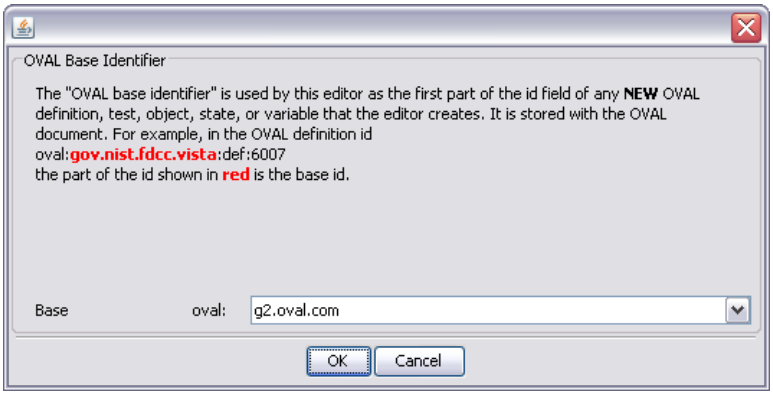

Figure 13. eSCAPe New OVAL – Setting base identifier

Next, the 'Create new OVAL definition' window opens and will ask for the definition class, title and description. The options for class are Vulnerability, Compliance, Patch, Inventory, and Miscellaneous. The choice of definition class will not affect the availability of tests later but may change the behavior and scoring results inside vendor tools. For this reason the choice of class should best match the issue the content is intended to address.

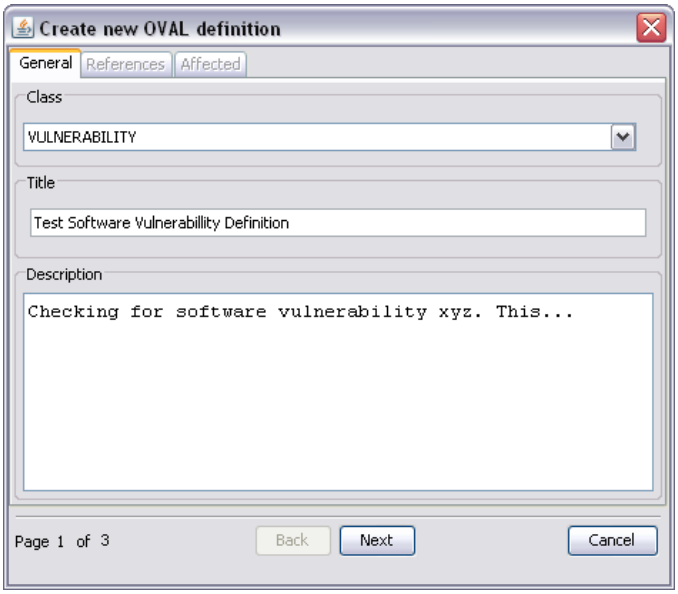

Figure 14. eSCAPe New OVAL – General information

After clicking 'Next' the reference tab is displayed, allowing for entry of definition references. Assigning references to a definition is optional but recommended. See Table 5 below for the recommended references per definition type. To add a definition click 'Add' and either choose a source from the drop-down box or enter one not listed. Next enter a Reference ID and last a URL if available. See Figure 15 below for an example of how a CVE reference for a vulnerability definition can be entered. There is also support on this tab for editing and removing references using the 'Edit' and 'Remove' buttons on the right side of the window.

Definition Type	**Recommended reference**
Vulnerability	CVE
Inventory	CPE
Compliance	CCE
Patch	CVE

Table 5. Recommended references per OVAL definitions type

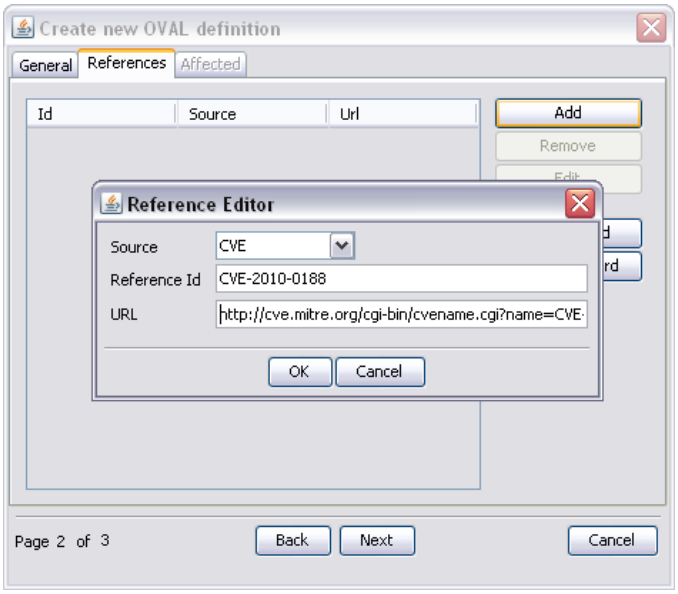

Figure 15. eSCAPe New OVAL – Adding references

After entering references click 'Next' to add affected platforms and elements. This step is required and you will not be able to click 'Finish' until a family and platform or product has been added. To add an affected platform, right-click on the 'Affected elements' node and click 'Add affected elements'. In the window that opens select a family from the drop down list. The available families are 'catos', 'ios', 'macos', 'pixos', 'undefined', 'windows' and 'unix'. See Figure 16 for how to add an affected element, and Figure 16 for how to add an affected platform.

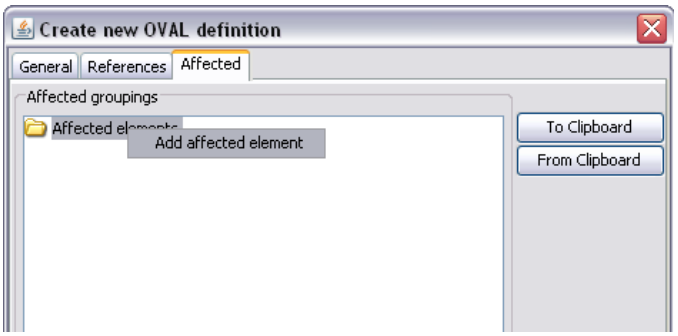

Figure 16. eSCAPe New OVAL – Context menu on affected elements root node

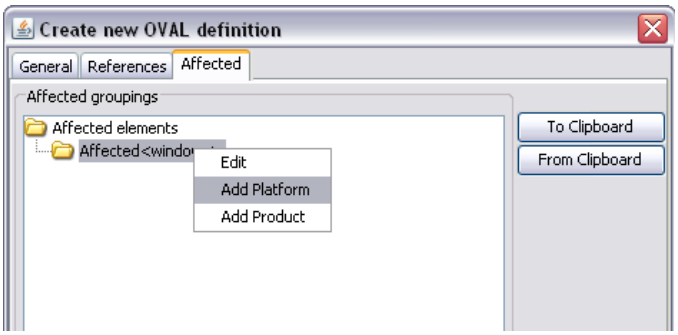

Figure 17. eSCAPe New OVAL – Context menu on affected element - adding affected platform

The affected platforms can be added by right-clicking on the affected element node and clicking ‘Add Platform’ or ‘Add Product’ (see Figure 17 above). In the window that opens you may add any String, but for general Windows platforms the recommended strings are listed in the table below.

Recommended Platform Strings
Microsoft Windows 2000
Microsoft Windows XP
Microsoft Windows Vista
Microsoft Windows 7
Microsoft Windows Server 2003
Microsoft Windows Server 2008

Table 6. Recommended platform strings

After at least one platform or product has been added, click ‘Finish’ to complete the creation of the OVAL definition.

Adding an Object

To add an object to an OVAL definition right-click on the root node and select ‘Add an object’ from the context menu that appears. For the next several sections, through *Adding a Test*, we will be constructing an OVAL filehash_test to check for the malicious file in the table below.

Path	Filename	MD5
C:\WINDOWS\temp	34564.exe	31125f0cef9b543911b0e68589c3acf5

Table 7. Example malicious file and attributes

In the screen that appears after clicking ‘Add an object’, a platform must be selected. For this example select ‘independent’ from the drop down box and click ‘Next.’ See the figure below for the full list of available object platforms.

Figure 18. Adding an object – Tab 1

In the next tab select ‘filehash_object’ and then click ‘Next’. The objects listed in this drop down box are all the object types available under the independent platform schema.

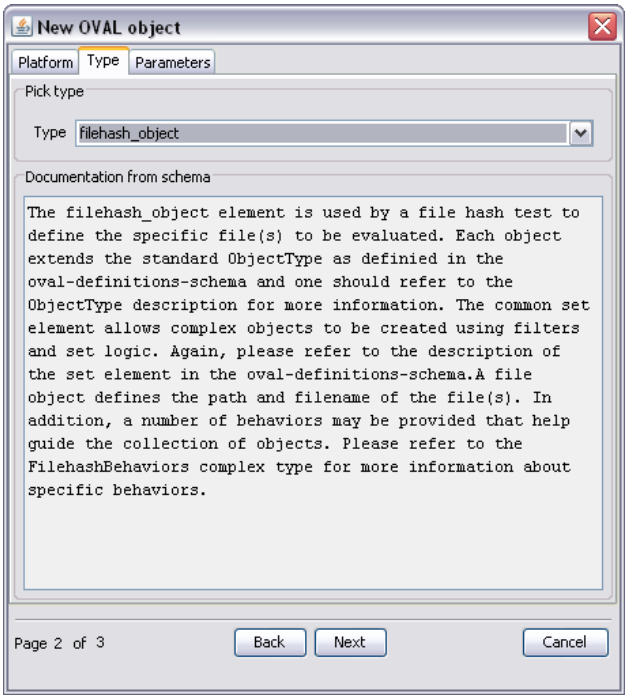

Figure 19. Adding an object – Tab 2 w/ filehash_object selected

In the final step we need to enter the object parameters. First the object comment should be updated to best indicate what the object is referring to. Something that resembles “File hash object for ‘34564.exe’” is recommended. Second, parameters for path and filename need to be provided. To add parameters right click on the object root node in the table and click ‘Add parameters.’ Select both ‘path’ and ‘filename’ from the window that appears and click ok. For an image of the context menu that appears, see Figure 20 below.

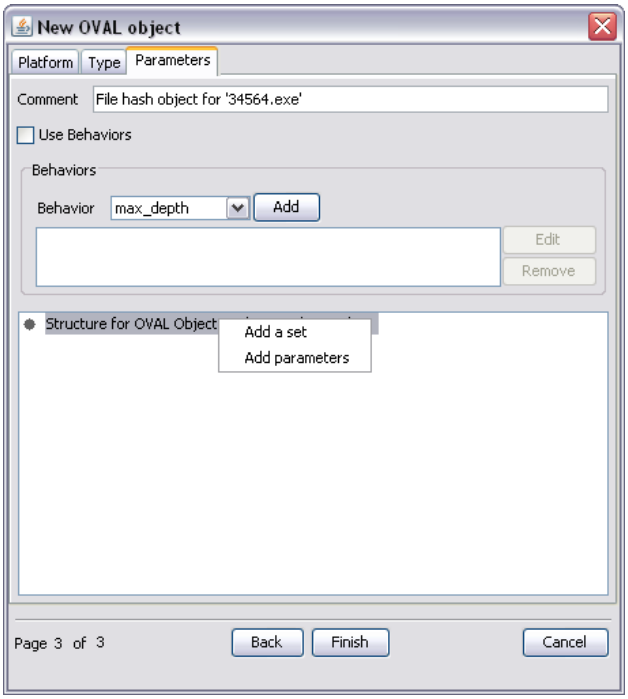

Figure 20. Adding an object – Tab 3 w/ new comment and context menu

There should now be two entries in the bottom window, one for path and the other for filename. Notice the option to apply behaviors to the object on this screen. Selecting 'Use behaviors' at this step will enable behaviors to be applied to the file_hash test. If selected the max_depth and/or recurse_direction behaviors should be added and set. Now right click on the parameter node for path and click 'Edit'.

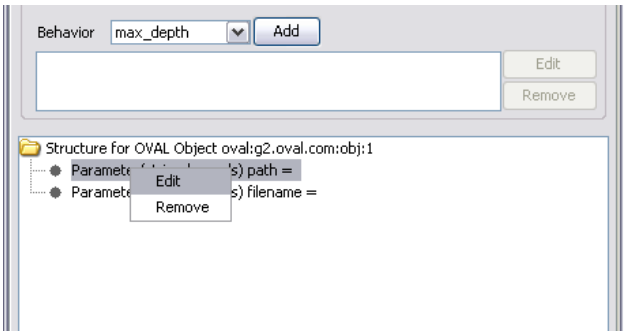

Figure 21. Adding an object – adding parameters

In the window that opens, under 'Data defined here' click 'Edit' and in the window that opens enter the file path (C:\WINDOWS\temp for this example), click 'Ok' and then click 'Ok' again in the previous open window.

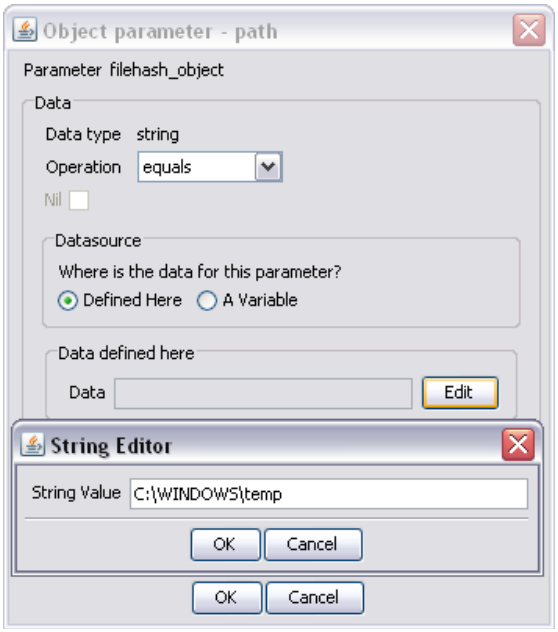

Figure 22. Adding an object - Editing object parameters

Use the same operations to enter the filename (34564.exe) and then click 'Finish' to complete the creation of the OVAL object.

Adding a State

To add a state to an OVAL definition right-click on the root node and from the context menu that appears select 'Add a state'. In the window that opens a state platform must be selected. For this example, select 'independent' from the drop down box and click 'Next.' See Figure 18 above for a view of what this window will look like and the full list of available platforms.

In the next tab select the filehash_state object type from the drop down box and click 'Next. See Figure 23 below for an image of the second tab in the New OVAL state window.

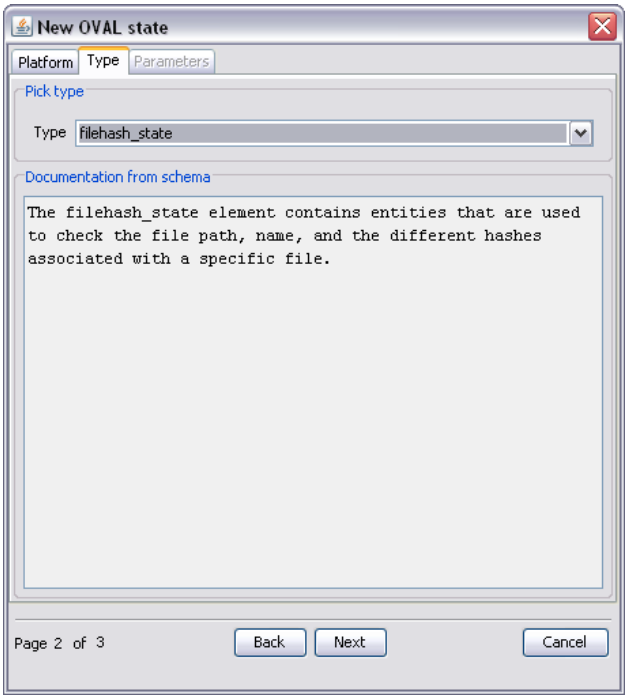

Figure 23. Adding a state - Selecting state type

In the Parameters tab the state comment should be updated to best indicate what the state is referring to. Something that resembles "File hash state for '34564.exe'" is recommended. Next, in the drop down box under 'Possible parameters', select md5 and click 'Add'. The md5 parameter should now appear in the Added parameters table at the bottom of the window.

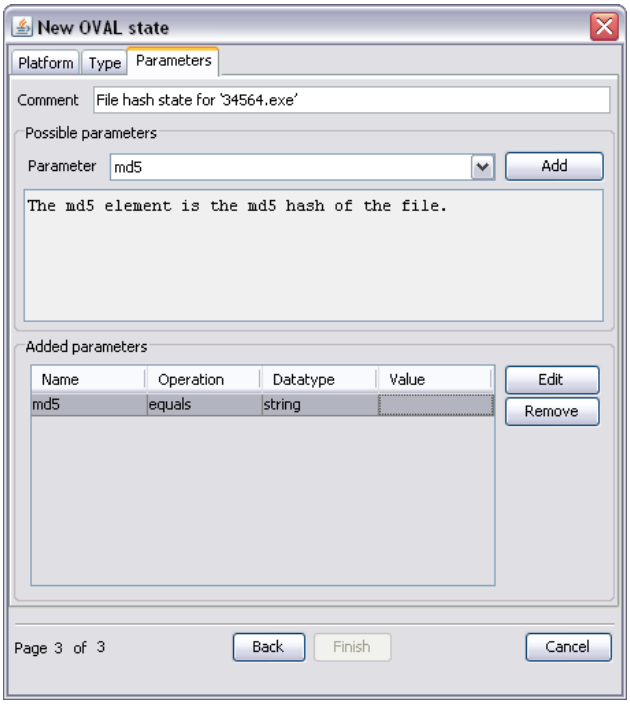

Figure 24. Adding a state - adding a parameter

Next select the md5 parameter in the ‘Added parameters’ table and click the ‘Edit’ button the right. In the window that opens, under ‘Data defined here’ click ‘Edit’ and in the window that opens enter the file hash (31125f0cef9b543911b0e68589c3acf5 for this example), click ‘Ok’ and then click ‘Ok’ again in the previous open window.

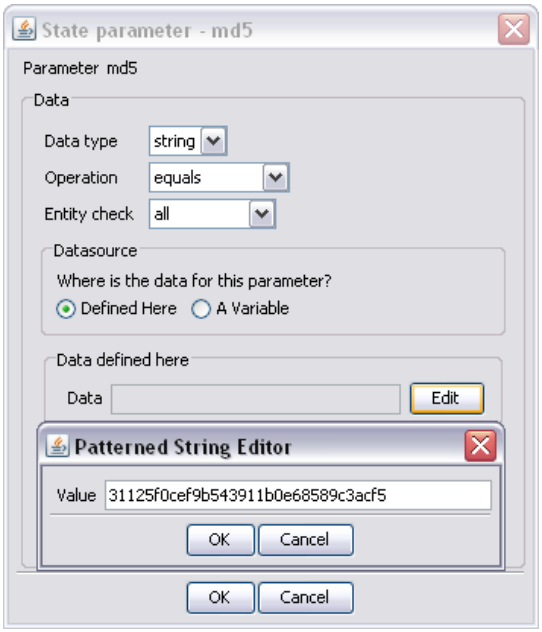

Figure 25. Adding state parameter

Click ‘Finish’ to complete the creation of the OVAL state.

Adding a Test

This section will describe how to create an OVAL test using eSCAPe in standard mode. In the 2 sections above, a filehash_object and filehash_state were created. In this section, instructions will be provided to put those objects and states together to create a test that checks for the malicious file described in Table 4 above. If the above sections were followed then a filehash_object and filehash_state should now appear in the OVAL document tree in eSCAPe. To add a test to the OVAL file, start by right clicking on the root node and select ‘Add a test’ from the context menu that appears.

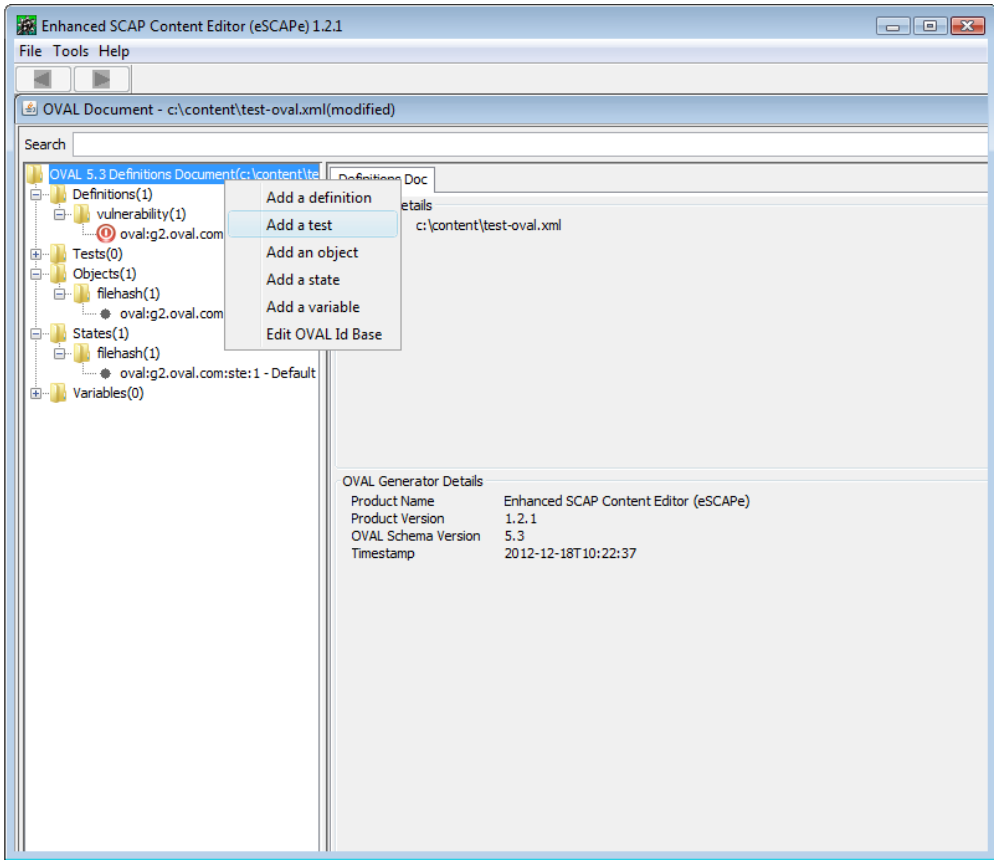

Figure 26. eSCAPe with OVAL document root node context menu

In the ‘New OVAL test’ window that opens, select a test platform group. For this example we are creating a file_hash test that will reference the filehash_object and filehash_state created in the last sections. This test is defined under the OVAL independent platform schema so select ‘independent’ from the drop down list.

Figure 27. New OVAL Test – platform selection

With the test platform selected, click 'Next' to move on to the 'Type' tab and select 'file_hash test' from the list of tests. Click 'Next' to move to the 'Object and State' tab.

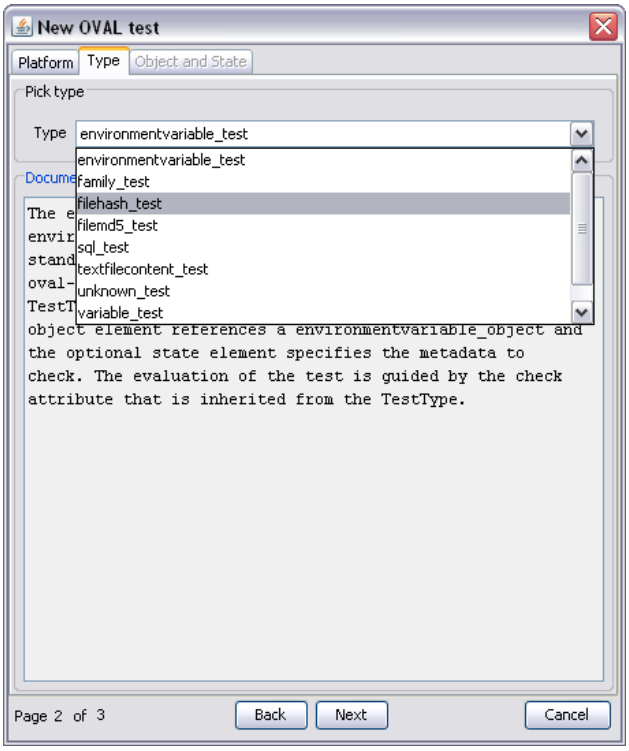

Figure 28. New OVAL Test – test type selection

On the object and state tab shown in Figure 29 below, an object and a state (multiple states in OVAL 5.6) can be associated with the new test. The test comment should be adjusted to something descriptive like “File hash test for malicious file '34564.exe'”. For this example the other fields can be left as defaults. To associate an object with this new test, click the ‘Choose Object’ button. See Figure 29 below for the object and state tab of the new OVAL test window with a new comment entered.

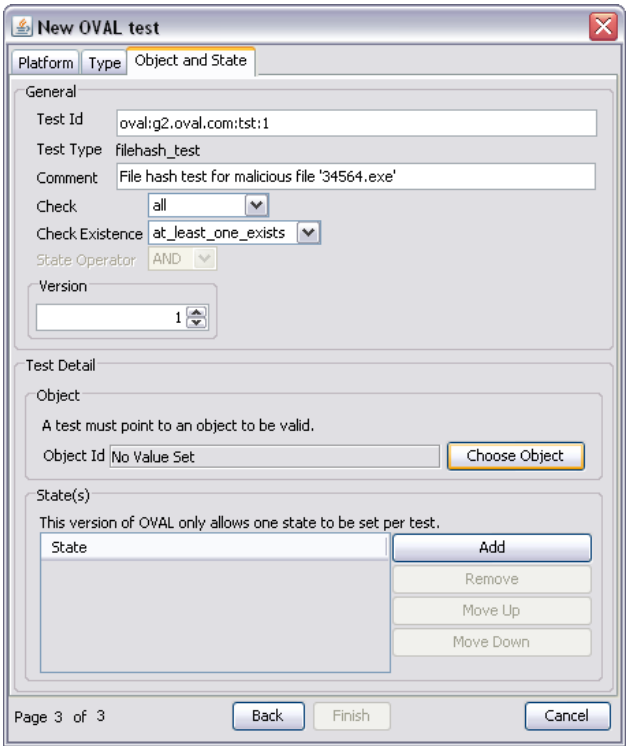

Figure 29. New OVAL Test – object selection

A ‘Choose Object’ window will appear with all available objects for the test type listed. Select object 1 and click Ok. To associate a state with this new test, click the ‘Choose State’ button. The ‘Choose State window will appear with all available states for the test type listed. Select state 1 and click Ok. See Figures 30 and 31 below for the choose object and state windows.

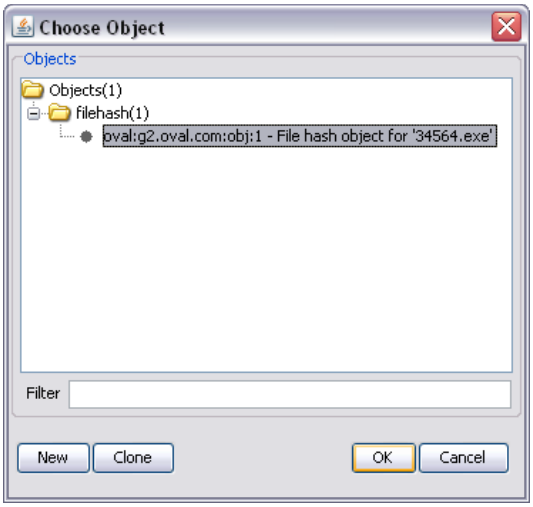

Figure 30. OVAL Test – Choose Object window

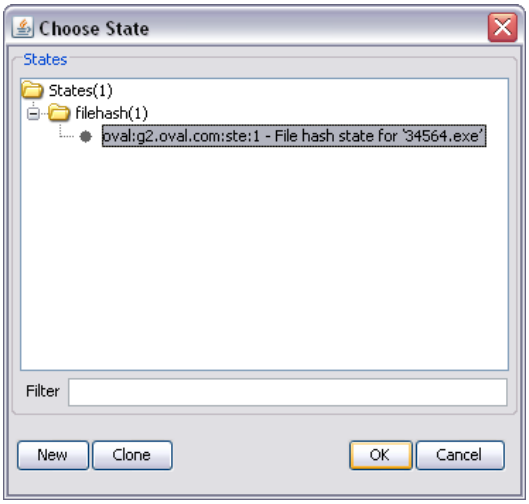

Figure 31. OVAL Test – Choose State window

With the test object and state now associated click 'Finish' to complete the creation of the OVAL test.

Adding Test Criterion to a Definition

After each OVAL test is created it should then be added as a criterion under the proper definition. The *Adding a Definition and Choosing Namespace* section above described how to add a definition. Now that a test has been created we can go back and add a criteria element for it. To start, select the definition in the document tree and then click on the 'Criteria' tab in the information area.

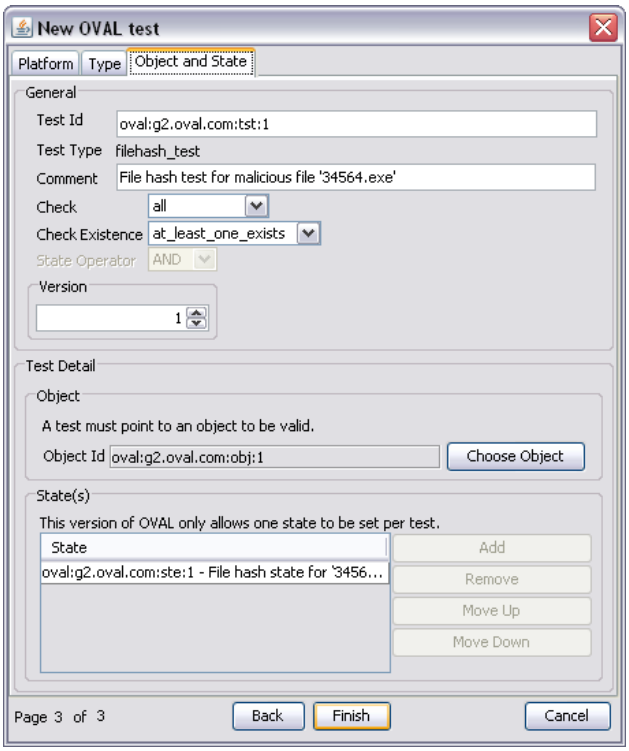

Figure 32. New OVAL Test with selected object and state

To add a criteria block, right click on the root node and click ‘Add criteria’.

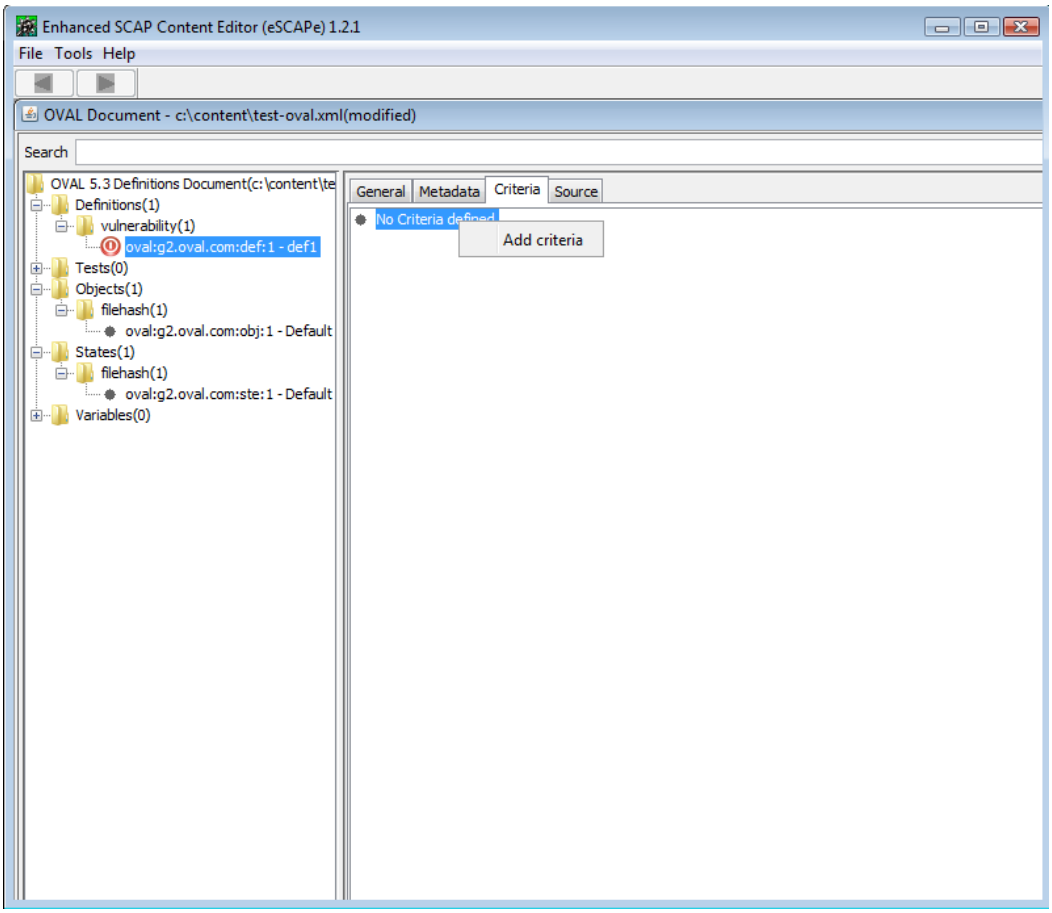

Figure 33. eSCAPe w/ definition selected and criteria tab open

In the window that opens there are options for operator, negate and comment. For this example leave the operator set to ‘AND’, and negate set to ‘false’. When two or more criteria are entered, the operator selection here will determine how the results of the test criterion are meant to be interpreted. Selecting ‘OR’ indicates that any or the individual tests may indicated a problem, while a selection of ‘AND’ indicates that all the tests in the criteria block must pass or fail to signify a problem. The comment is optional and can be left blank at this time. Click ‘Ok’ to save the criteria block.

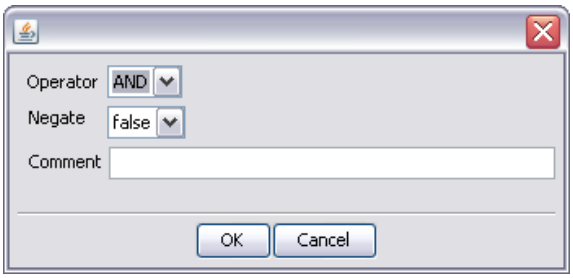

Figure 34. Add criteria window

Now, right click on the root node and choose ‘Add criterion’.

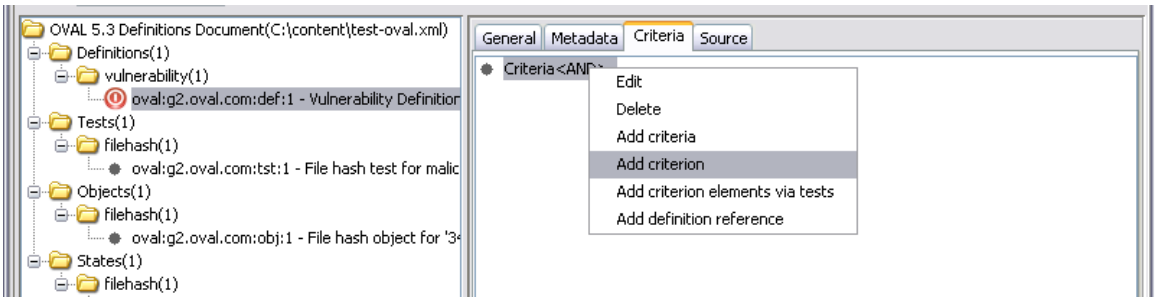

Figure 35. Root criteria node context menu

In the window that opens click ‘Choose Test’. In the next window that opens a list appears of all tests in the OVAL document, grouped by type. Select from this list the desired OVAL Test. If desired, a comment can be added to the criterion element using the comment field.

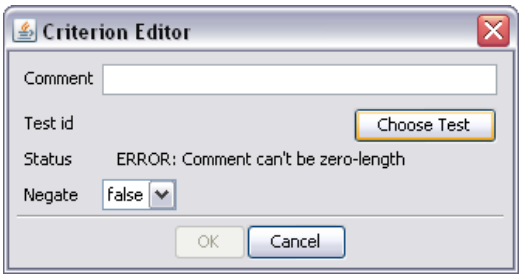

Figure 36. Criterion Editor

Click ‘Ok’, and then click ‘Ok’ again. The test should now appear as a node under the root criteria block. Calls to this definition will now be directed to execute the listed test.

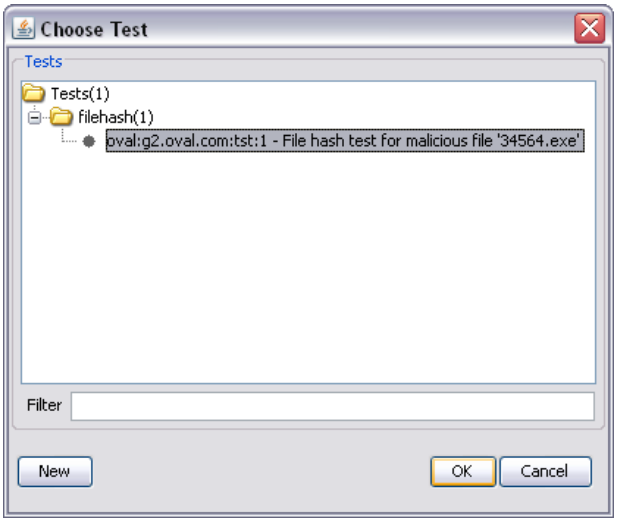

Figure 37. Criterion Editor – Choose Test window

Creating an XCCDF Document from an OVAL Document

eSCAPe includes support for creating a simple XCCDF document given a source OVAL document. To generate an XCCDF document from an OVAL document, in the File menu go to ‘File’ > ‘New’ > ‘XCCDF’ > ‘From OVAL’. If an OVAL document is open it will be used as the source file. If an OVAL document is not open a navigation window will appear allowing for browsing and selection of the source OVAL file. Next, the generator window will appear and ask for XCCDF profile and group titles to be provided. See the figure below for a view of the XCCDF from OVAL generator window.

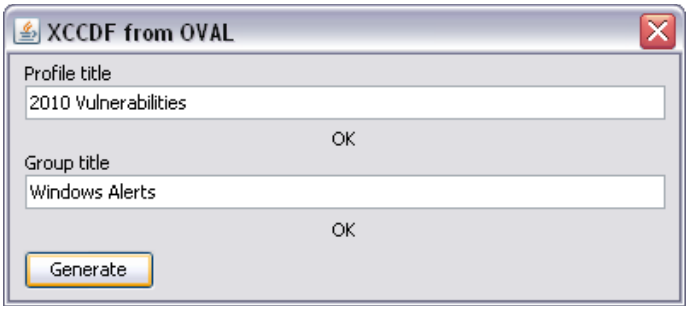

Figure 38. XCCDF From OVAL

It is recommended to change the profile and group titles from their default values, but they can be left for quick testing. After entering a desired profile and group title click ‘Generate’. A file save window will appear allowing for the selection of a destination path and file name. A filename suggestion with the same file name as the OVAL file with an ‘-xccdf’ suffix will be pre-entered. Once the file name and path are decided, click ‘Save’ to create the document. Last, the newly created XCCDF document will open inside eSCAPe.

Creating an XCCDF Document from an OCIL Document

eSCAPe also includes support for creating a simple XCCDF document given a source OCIL document. To generate an XCCDF document from an OVAL document, in the File menu go to ‘File’ > ‘New’ > ‘XCCDF’ > ‘From OCIL’. A navigation window will appear allowing for browsing and selection of the source OVAL file. Next, the generator window will appear and ask for XCCDF profile and group titles to be selected. Once the profile and group titles have been provided and the ‘Generate’ button clicked, an XCCDF document will be generated.

Use Case Examples

Creating Malware SCAP Content with the Wizards

The eSCAPe wizards are particularly well suited for the generation of malware detection content. Often the presence of malware on a system can be detected by checking for malware artifacts such as files or registry keys. These artifacts can be detected with certain OVAL tests. The below examples demonstrate the steps necessary to create an

OVAL Test and accompanying XCCDF document to check systems for malware registry or file artifacts.

Creating Content - Registry Test Example

Start eSCAPe and enter the Wizard Mode. There are two ways to enter Wizard mode. Either click the "Wizard-Driven" button in the window that opens when eSCAPe starts (see figure below), or select 'File' > 'Wizard Mode' from the menu.

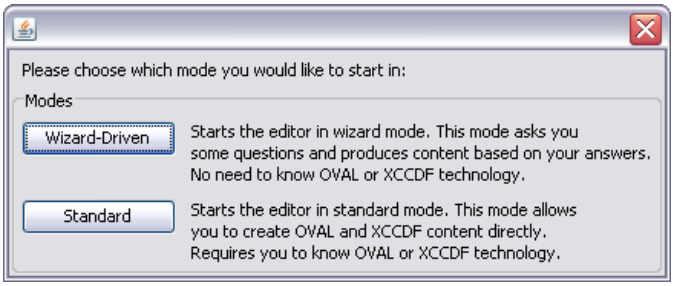

Figure 40. eSCAPe interface selection window

Next, adjust the Target OVAL version and set the OVAL namespace identifier. The choice of OVAL version will be most constrained by the OVAL version supported by the vendor tool the content will be run in. If the tool provides full support for OVAL 5.6 then you may select that. At the time of the publication of this document, many vendors still only fully supported OVAL 5.3.

Last, from the list of available wizards select 'Registry' and click 'Go.'

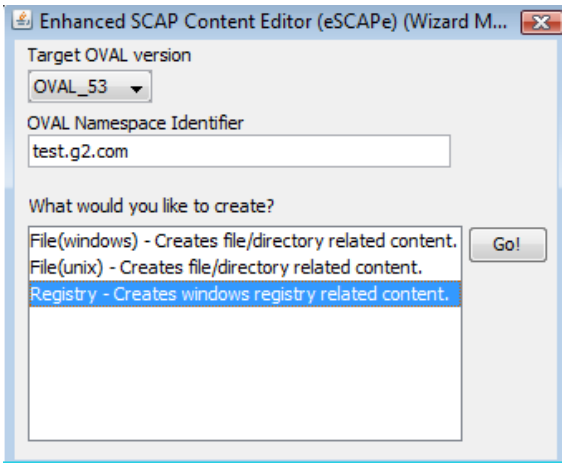

Figure 41. Wizard selection window

In this example we will be checking for the presence of the following malicious registry key entry:

"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Goodprogram = C:\WINDOWS\Temp\Badprogram.exe"

In the window that opens there are fields for entering the title and the registry key information. The use of a descriptive title will easily identify what the OVAL definition is checking for. A suggested registry test title might resemble:

"Registry Check for malicious key - 'Badprogram.exe'"

Since we are checking for both the existence of a registry key and its value, make sure that under 'What is to be tested', "Value of hive\key\name" is selected. Next, from the drop-down Registry Hive menu select 'HKEY_LOCAL_MACHINE'. See the figure below for the layout of this window and the list of registry hives available.

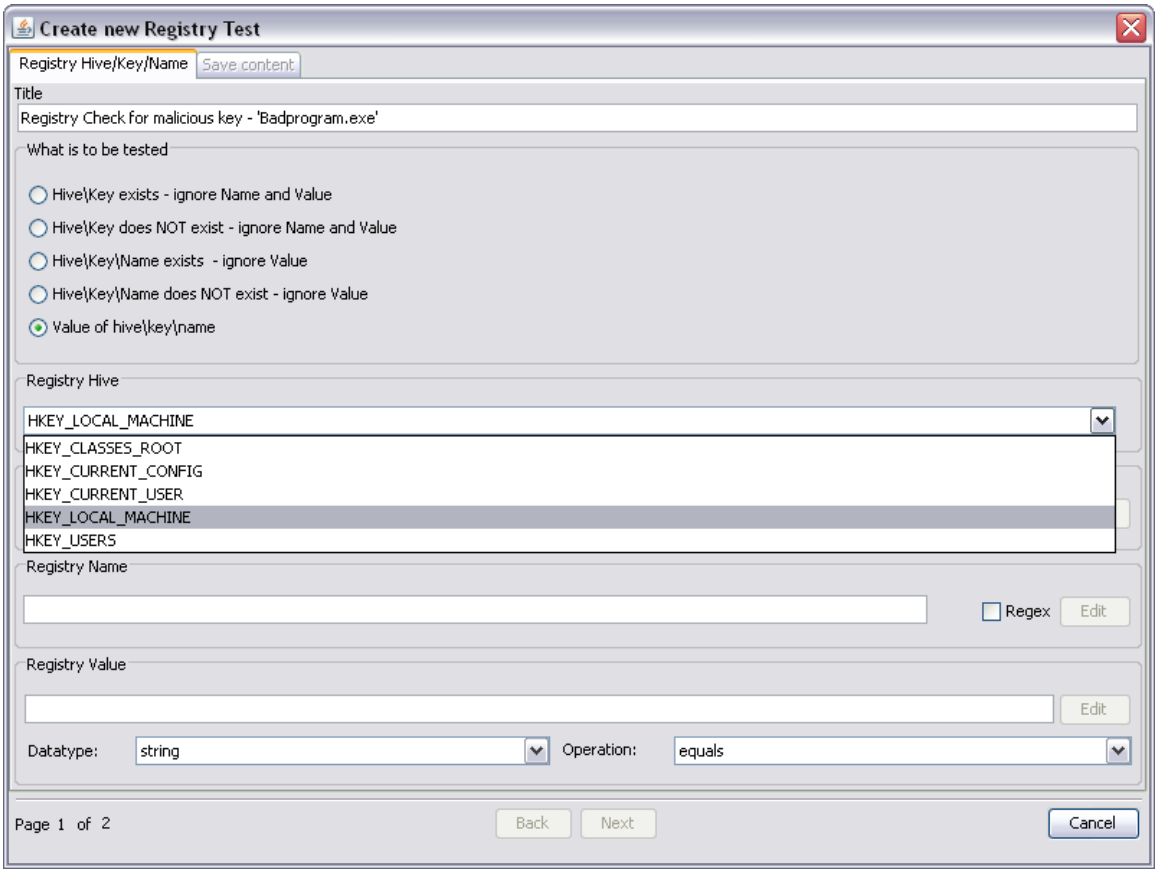

Figure 42. Registry Test Wizard window Tab 1 - with Title and Hive selected

Next, the key, name and value must to be entered. For this example, the *key* consists of "SOFTWARE\Microsoft\Windows\CurrentVersion\Run", the key *name* is "Goodprogram" and the registry *value* is "C:\WINDOWS\Temp\Badprogram.exe". The data type can be left as 'string' and the operation as 'equals'.

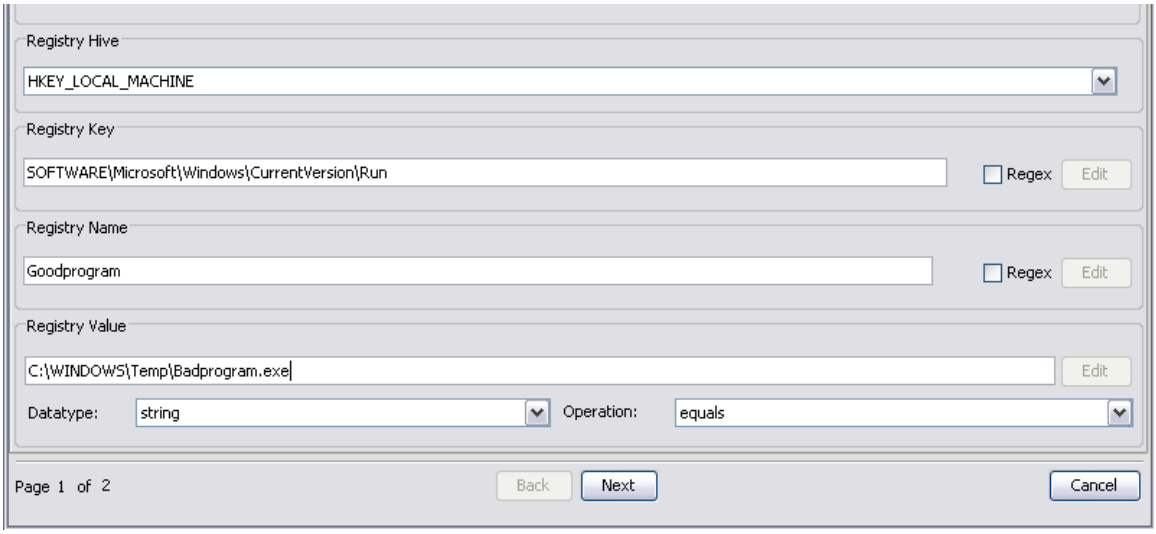

Figure 43. Bottom half of Registry Test Wizard window Tab 1 - Hive, Key, Name & Value entered

Now click 'Next' to move to the last step and save the content. On this screen click the 'Browse' button, navigate to where you want to save the file, enter a destination filename and then click 'Save'.

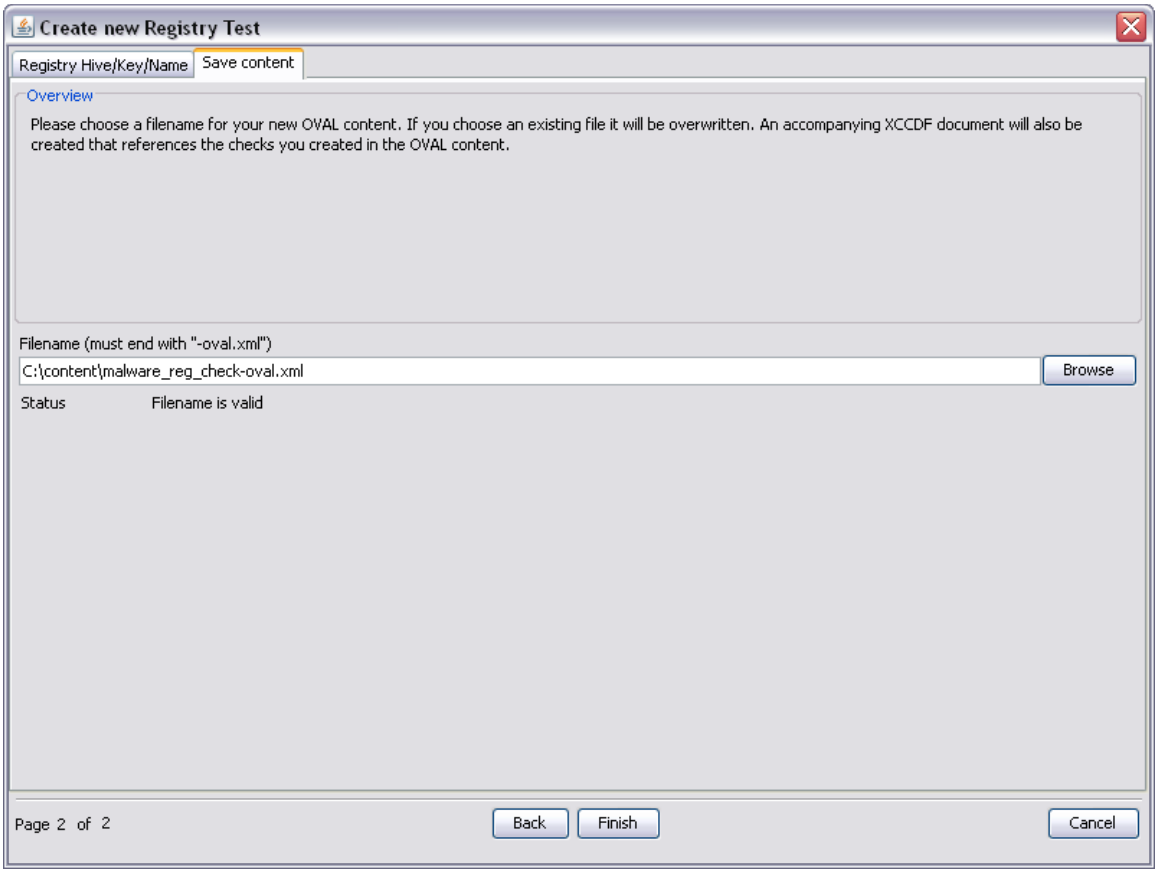

Figure 44. Registry Test Wizard window Tab 2 - with path and filename entered

It is convention to save OVAL files with '-oval' at the end and to save XCCDF files with a trailing '-xccdf'. At this last step in the wizard, the application requires that the

destination filename match those formats. If an OVAL filename is entered without the appropriate suffix, a red error message will appear above the field. See the figure below for an example of the error that will appear if an incorrectly formatted filename is entered. To complete this step and create the SCAP files click 'Finish.'

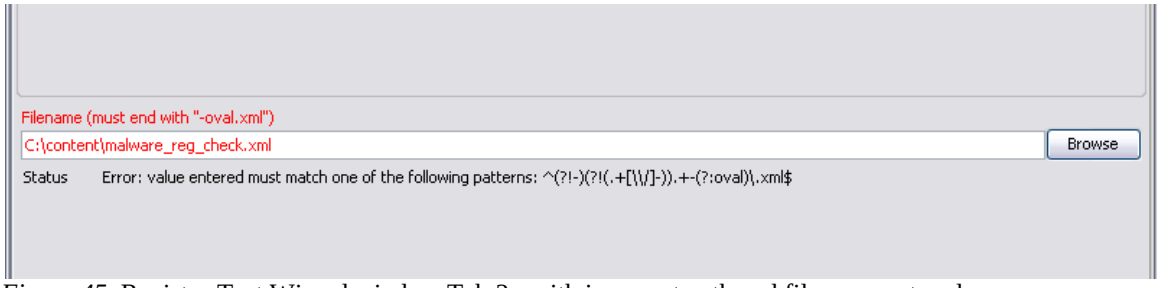

Figure 45. Registry Test Wizard window Tab 2 - with incorrect path and filename entered

Last, locate and view the 2 files that have been created:

1. malware_reg_check-oval.xml
2. malware_reg_check-xccdf.xml

The OVAL file contains the body of the checks for the malicious registry entry and the XCCDF file references those checks. These files are ready to be handed off to a NIST validated SCAP scanner.

Creating Content - File Test Example

This example will demonstrate how to create SCAP content to check for the presence of a malicious file on a system. In this example we will be checking for the presence of the malicious file in the table below.

Path	Filename	Size (KB)	MD5
C:\WINDOW\temp	34564.exe	89,829	31125f0cef9b543911b0e68589c3acf5

Table 9. Example malicious file

Start eSCAPe and enter the Wizard Mode. Select the OVAL file version, namespace identifier and then choose the File(windows) wizard and click 'Go!'

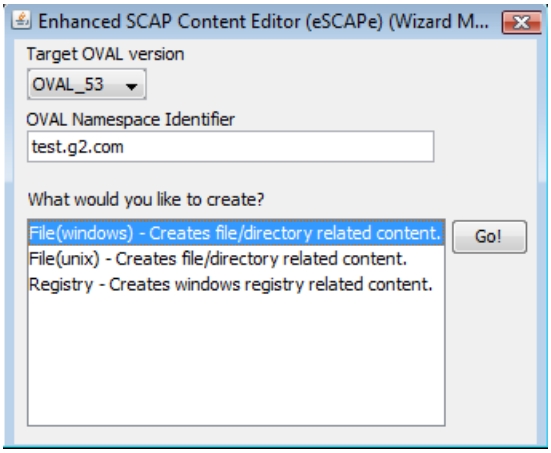

Figure 46. Wizard selection window

The window that opens contains all the settings for creating the Windows file test. First, enter a title into the *title* field. A suggested title would resemble:

"File test for malicious file – '34564.exe'"

In the *path* field there are two ways to specify a path. The first way is to enter the specified path into the *path* field. For this example we are given the file path so we will enter that into the field as shown in the figure below.

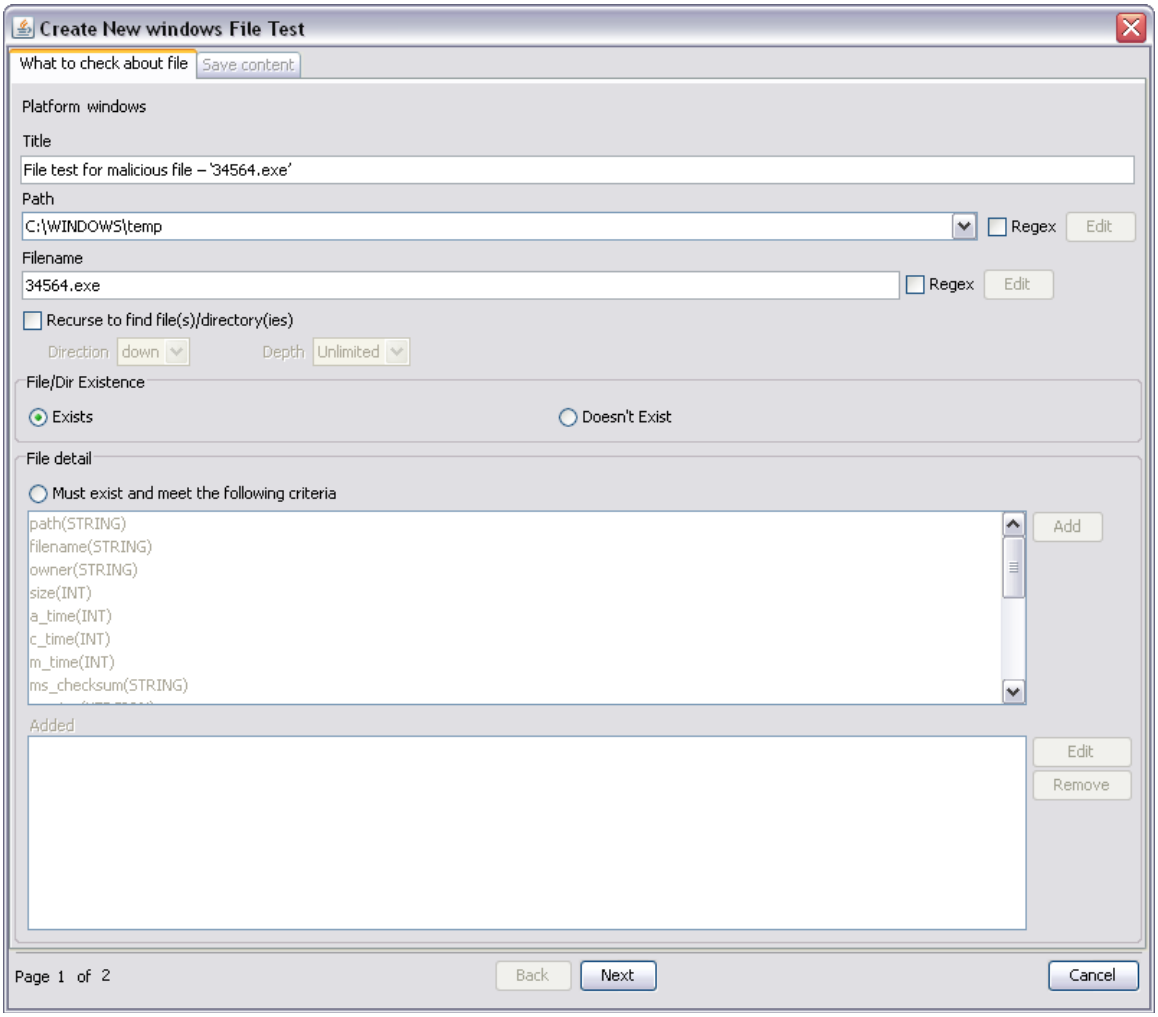

Figure 47. File Test Wizard window with Title, Path and Filename entered

The second way to specify a path is to use one of the predefined path shortcuts available (see Figure 48). Using one of these shortcuts will result in the creation of an OVAL test capable of determining the actual path on the destination system. In certain circumstances this is preferred to hard-coding a path that might not be the same on all installations. For example it is possible to set the systemroot which is generally C:\WINDOWS to a non-standard path like C:\temp\WINDOWS. Such a choice would mean that content which assumes that systemroot is set to C:\WINDOWS might not effectively perform the test. The currently supported path shortcuts and examples of how they might be expanded are displayed in Table 10 below.

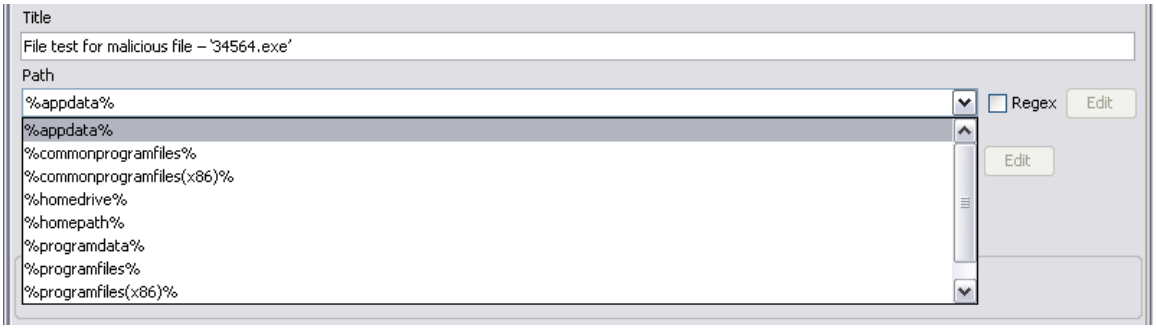

Figure 48. Available path shortcuts from the Path field

Path Shortcut	**Possible value on target system**
%appdata%	C:\Documents and Settings\user\Application Data
%commonprogramfiles%	C:\Program Files\Common Files
%commonprogramfiles(x86)%	C:\Program Files\Common Files (x86)
%homedrive%	C:\
%homepath%	C:\Documents and Settings\user
%programdata%	C:\Documents and Settings\All Users\Application Data
%programfiles%	C:\Program Files
%programfiles(x86)%	C:\Program Files (x86)
%systemroot%	C:\WINDOWS

Table 10. eSCAPe File Wizard path shortcuts and general values

Selecting 'Recurse to find file(s)/directory(ies)' at this step will apply behaviors to the file test directing it to continue through the directory tree until it finds the file or directory. For example, if the file path is not known, the root directory (generally C:\) can be specified and the content will direct the scanner to start at the root level and search down the directory tree. The default recurse direction is down and depth unlimited, however other options may be selected. Direction may be adjusted to 'up' or 'none' and depth may be adjusted to 'Unlimited', '1', '2', '3', '4', '5', '10', '20', or '100'. See the figure below for sample recursion settings.

Figure 49. File Test Wizard window with recursion options

Next, we will add file details to check for properties of the file. In the section of the window titled 'File detail' make sure the radio button 'Must exist and meet the following criteria' is selected. Then in that selection box click 'size(INT)' and then click the 'Add' button to the right of the field. In the window that opens for 'Operation' choose 'equals' and then enter the file size in bytes in the 'Data' field and click 'Ok.' Upon clicking Ok, "size(INT) equals 89829" appears now in the window under 'Added'. For each file detail

attribute check that is added, a line item appears in the Added window. See Figure 47 below for an image of the detail entry window and entered file size. Next click on md5(STRING) in the list of file details, and in the window that opens for 'Operation' choose equals and then enter the MD5 hash in the 'Data' field and click 'Ok.' See Figure 48 for an image of the md5 hash detail entry window and the entered hash. If a string of the wrong length is entered for the md5 hash, the field will appear in red and 'Ok' will be disabled until a valid md5 hash string is entered.

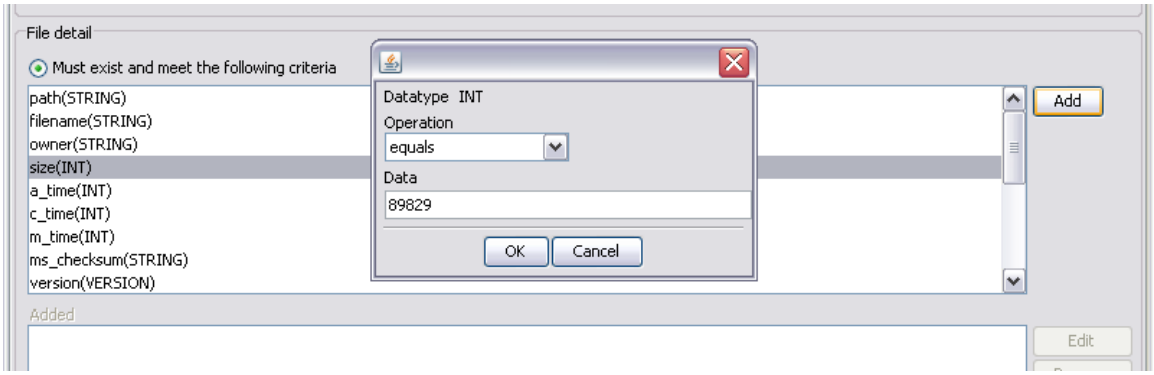

Figure 50. File Test Wizard window with file size being entered

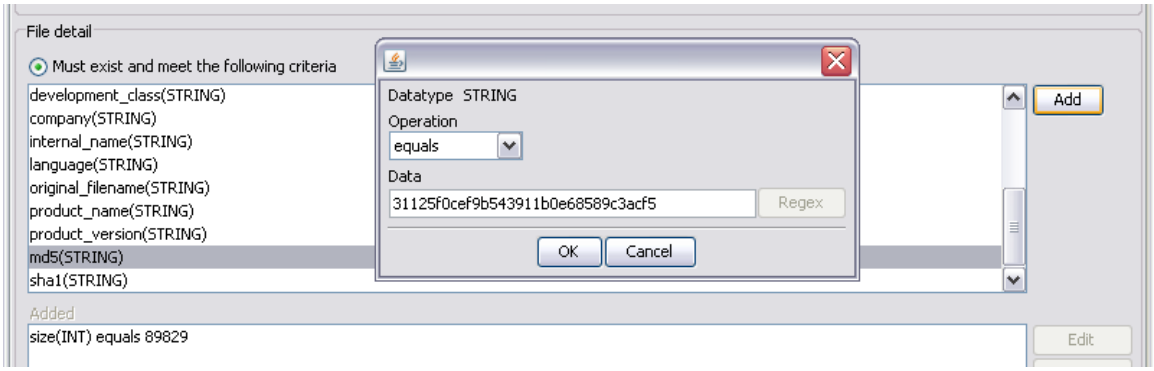

Figure 51. File Test Wizard window with file hash being entered

Now that file information and details have been entered click 'Next' to move on to save the file. On the screen that appears click the 'Browse' button, navigate to where you want to save the file, enter a destination filename and then click 'Save'. See Figure 49 below for the final step to save the file.

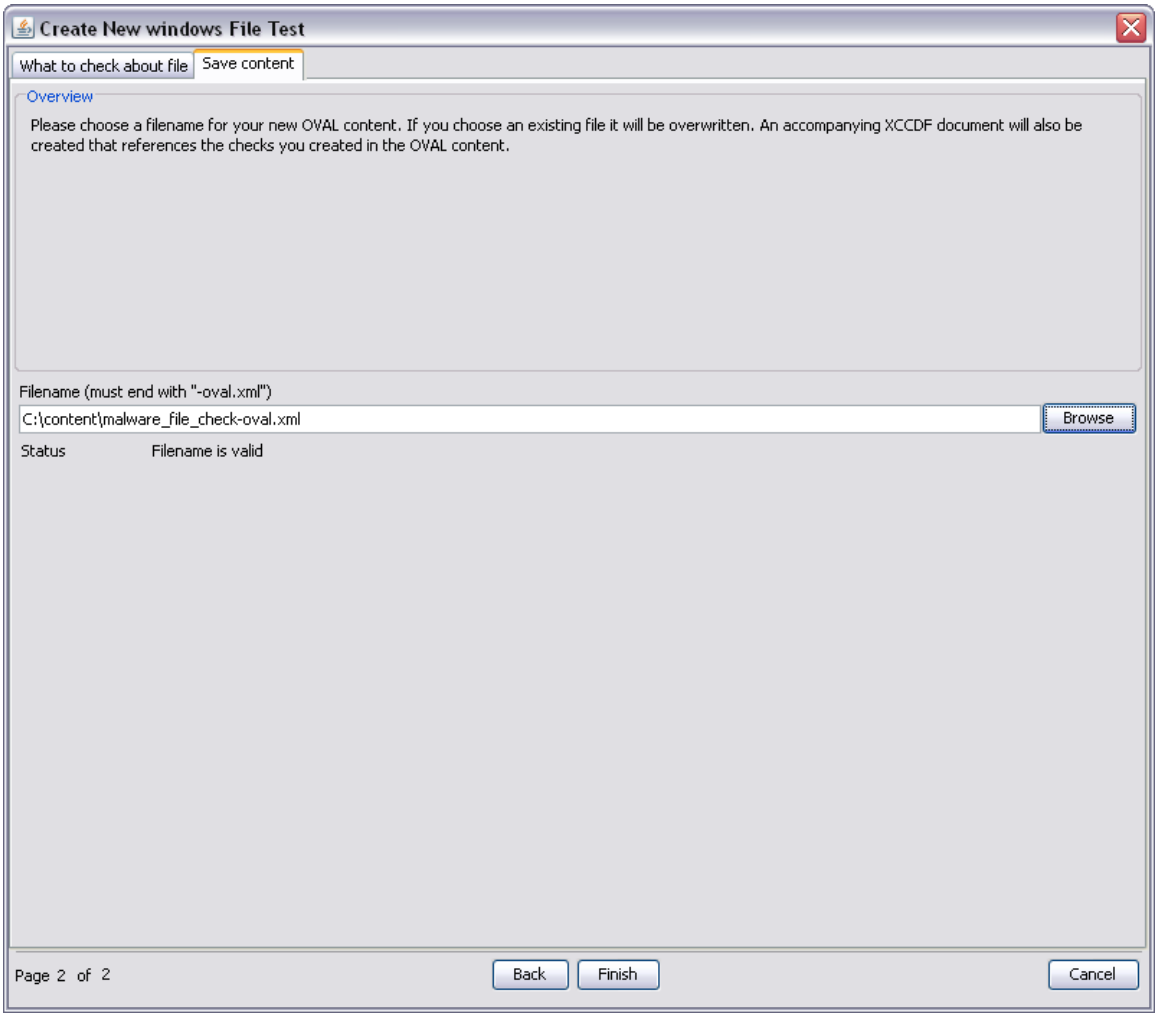

Figure 52. File Test Wizard window Tab 2 - with path and filename entered

Last, locate the 2 files that have been created:

1. malware_file_check-oval.xml
2. malware_file_check-xccdf.xml

The OVAL file contains the body of the malware check for the malicious file and the XCCDF file references those checks. These files are ready to be handed off to a NIST validated SCAP scanner.

Additional Tools

Using the Regex Validator tool

eSCAPe includes support for regular expressions throughout OVAL and for convenience includes a regular expression (REGEX) validator tool. This tool can be used to compose and test regular expressions before saving them in an OVAL document. To access the Regex Validator tool from the menu navigate to ‘Tools’ > ‘Regex Validator’.

To test a regular expression, enter it into the 'Pattern' field, then enter in the 'Text to match' field a sample sting that the regular expression should match. Last, click 'Match' and if the regular expression is working then the sample string will be listed after 'Matched text.' In the figure below a regular expression written to match 'Service Pack [2-4]' is entered. Notice that the string 'Service Pack 3' proved to be a match and this demonstrates the desired behavior of the regular expression.

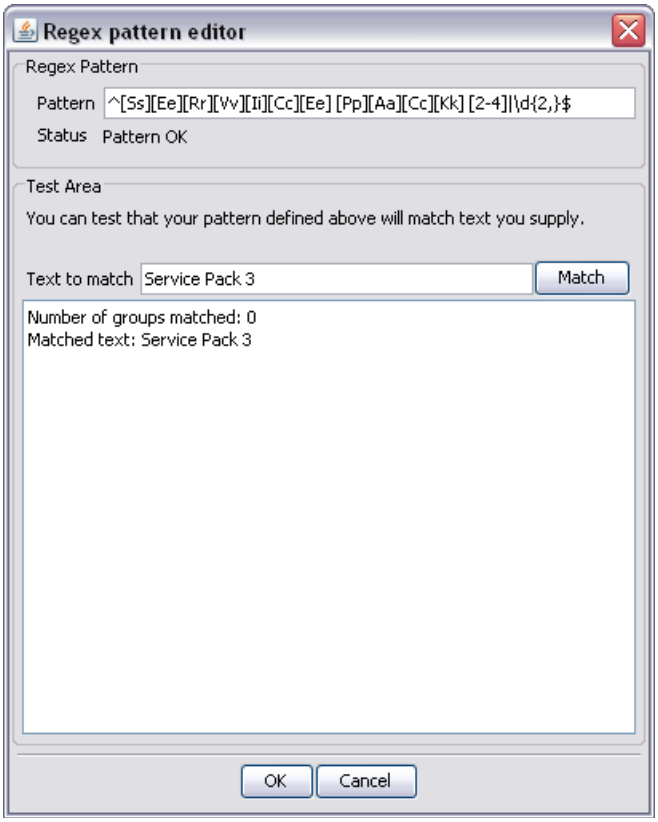

Figure 53. eSCAPe Regex validator tool

Using the Validate Documents tool

While an SCAP data file is open, the file can be validated using the Validate tool. To validate an open SCAP document from the menu click 'Tools' > 'Validate'. Results from the validation will be displayed in a new window. Please see Figures 54 and 55 below for a sample of the validation successful (Figure 54) and validation error (Figure 55) windows.

Figure 54. Successful eSCAPe validation results window

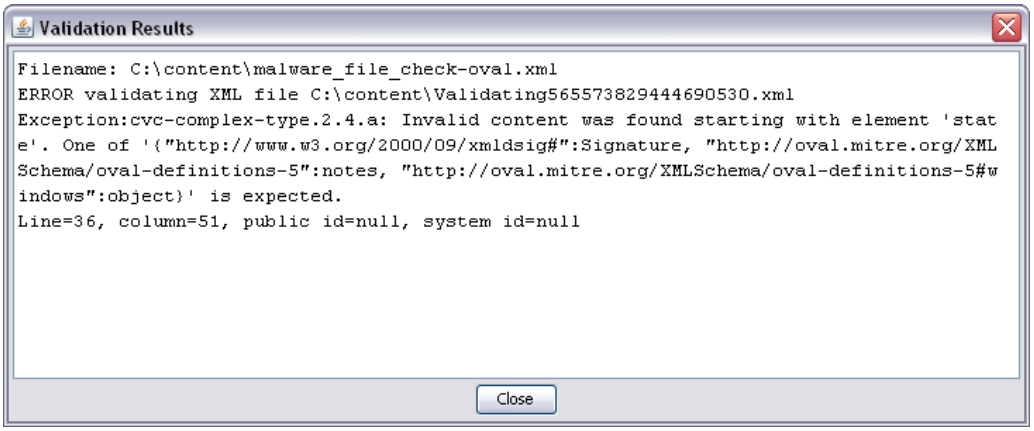

Figure 55. Error eSCAPe validation results window

Using the Merge OVAL Documents tool

Included with eSCAPe is a utility for merging OVAL files. To access this tool navigate in the menu to ‘Tools’ > ‘Merge OVAL Documents’.

If several OVAL files were made with the wizards, which only allow for the creation of a single test for each generated definition OVAL file, then it may often make sense to merge those files together if they all pertain to the same security issue. The OVAL Merger tool features two merge styles, simple and with wrapper definition. The simple merge style combines all the definitions, tests, objects, states and variables together into a single file. The ‘With Wrapper Definition’ option adds a definition at the top of the OVAL file that references all the combined tests. This utility also addresses any possible object ID collisions.

To use the tool first click the ‘Add’ button in the upper right corner and select the files you would like to merge. Files can also be dragged and dropped into this window. Once the files to be merged are listed in the tool window a merger style must be selected. The default style is ‘simple’ which just merges all the files together. The ‘With Wrapper Definition’ option adds a definition at the top of the OVAL file that references all the combined tests. When the ‘With Wrapper Definition’ option is selected a definition namespace must be chosen. The definition class should be adjusted as is necessary and it is recommended to select a definition title. Next, click ‘Browse’ and enter a choose a path and filename for the merged definition file. Last, click ‘Merge’ to merge the OVAL files.

For a view of the tool in use please see the figure below.

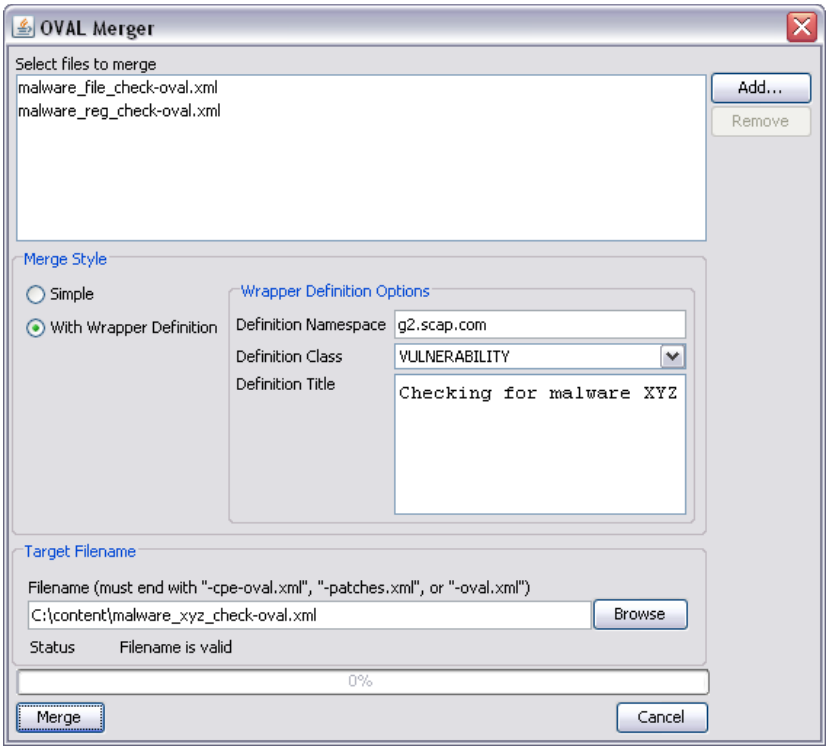

Figure 56. OVAL Merger window with 2 OVAL files being merged

Validating an SCAP Data Stream

When an SCAP Data Stream is open inside eSCAPe there is a utility provided for validating the data stream files. This validation performs a variety of checks including schema validation of the files, schematron validation and verification of all references between the documents.

Clicking 'Validate SCAP Data Stream' on the SCAP Data Stream window, opens a dialog box. Under the Choose Use Case panel, the validation use case may be selected. Each use case corresponds to an SCAP use case defined in Special Publication 800-126. The currently supported use cases in eSCAPe include CONFIGURATION, VULNERABILITY_XCCDF_OVAL, VULNERABILITY_OVAL and SYSTEM_INVENTORY.

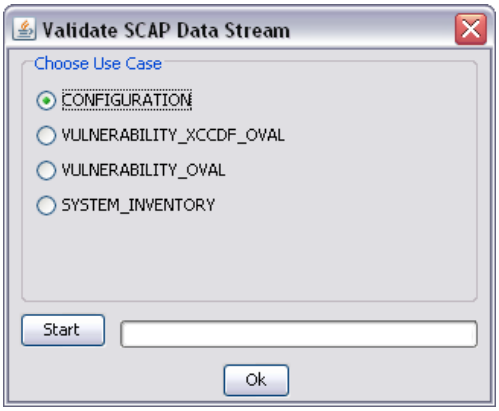

Figure 57. Data Stream Validation Use case selector

Once a use case is selected from the 'Choose Use Case' panel, click the 'Start' button to validate. Once the validation process is complete, eSCAPe will display the Validation Results dialog which shows the results returned from the SCAP Content Validation Tool. The 'Ok' button closes the Validate SCAP Document Bundle dialog without performing validation. See the figure below for a view of some sample validation results.

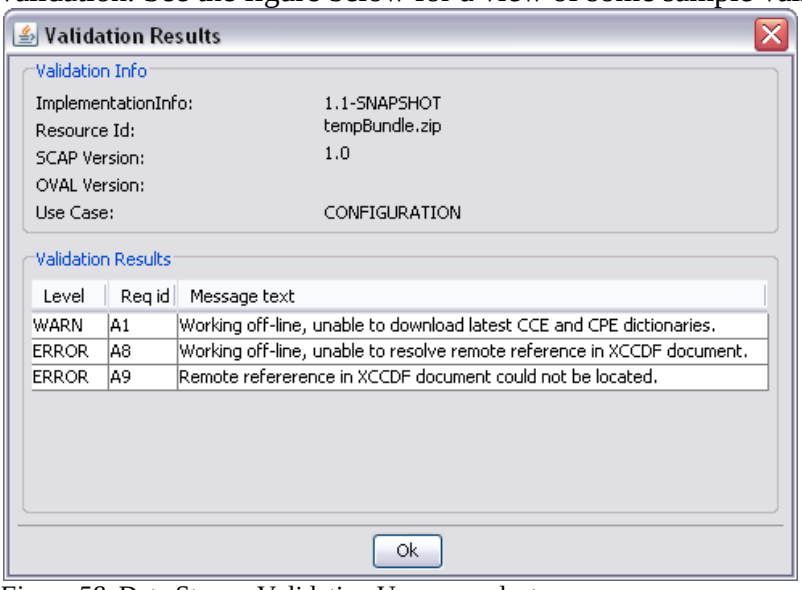

Figure 58. Data Stream Validation Use case selector

Reference

Key Terms

Term	Definition
OCIL	Open Checklist Interactive Language. OCIL is an XML based language for expressing questions to be answered by people.
OVAL	Open Vulnerability Assessment Language. OVAL is an XML based language for expressing the necessary logic to check for vulnerabilities, compliance, installed software, and patches.
SCAP	Security Content Automation Protocol. SCAP represents a suite of XML document specifications and other standards used in trying to develop a common way to assess compliance and vulnerability issues. Specifications like XCCDF, OVAL, OCIL, AI, CCE, CPE, CVE, and CVSS used in concert allow policy makers and sysadmins alike to assess their systems for compliance and vulnerability in a standard, non-proprietary way.
XCCDF	eXtensible Configuration Checklist Description Format. An XCCDF benchmark defines a number of rules who generally reference definitions in an OVAL document. Rules can be grouped together in a number of different ways and are usually selected by a profile under the benchmark.

Table 11. eSCAPe key terms reference table