Easily Create SCAP Content with the MACE Wizard Tool

Tina Ackerman
DoD
September 27, 2010

Definitions

- **SCAP (S-CAP)** – “Security Content Automation Protocol” is a standard way of documenting server configurations and descriptions of malware in a machine readable form. A suite of XML document specifications and other standards used to develop a common way to assess compliance and vulnerability issues.

- **XML**- eXtensible Markup Language

- **OVAL** – Open Vulnerability and Assessment Language: Standard XML based language for expressing the necessary logic to check for vulnerabilities, compliance, installed software and patches.

Definitions cont.

- **XCCDF**- Extensible Configuration Checklist Description Format. It is XML for specifying checklists and for reporting results of checklist evaluation. An XCCDF benchmark defines a number of rules who generally reference definitions in an OVAL.xml document.

- **CPE- Dictionary.xml**- A dictionary consisting of two files, a CPE-Dictionary.xml and CPE OVAL.xml. CPE-Dictionary.xml contains targeted platforms and references the file containing the platform inventory definitions/checks.

- **CPE- OVAL.xml**- Is an accompanying file of the CPE Dictionary.xml file. It includes the platform OVAL check(s) for determining applicability of the benchmark definitions.

Malware Content Editor (MACE) 1.0

- **Wizard Mode-** designed for automated SCAP content generation of XCCDF wrapped OVAL SCAP content without requiring users to fully understand XML, XCCDF, or OVAL. This mode provides a limited set of features.

- **Standard Mode-** considered an advanced feature, for example, editing OVAL and XCCDF documents/files.

Malware Content Editor (MACE) 1.0

- **Purpose:**

  To provide step-by-step instruction on how to create an SCAP data stream (OVAL, XCCDF, CPE – Dictionary.xml, and CPE- OVAL.xml) to search for and discover artifacts on an operating system.

Malware Content Editor (MACE) 1.0

- **Per National Institute of Standards and Technology (NIST) 800-126**

- **SCAP Data Stream**
  1. OVAL.xml
  2. XCCDF.xml
  3. CPE- Dictionary.xml
  4. CPE- OVAL.xml

Content Creation

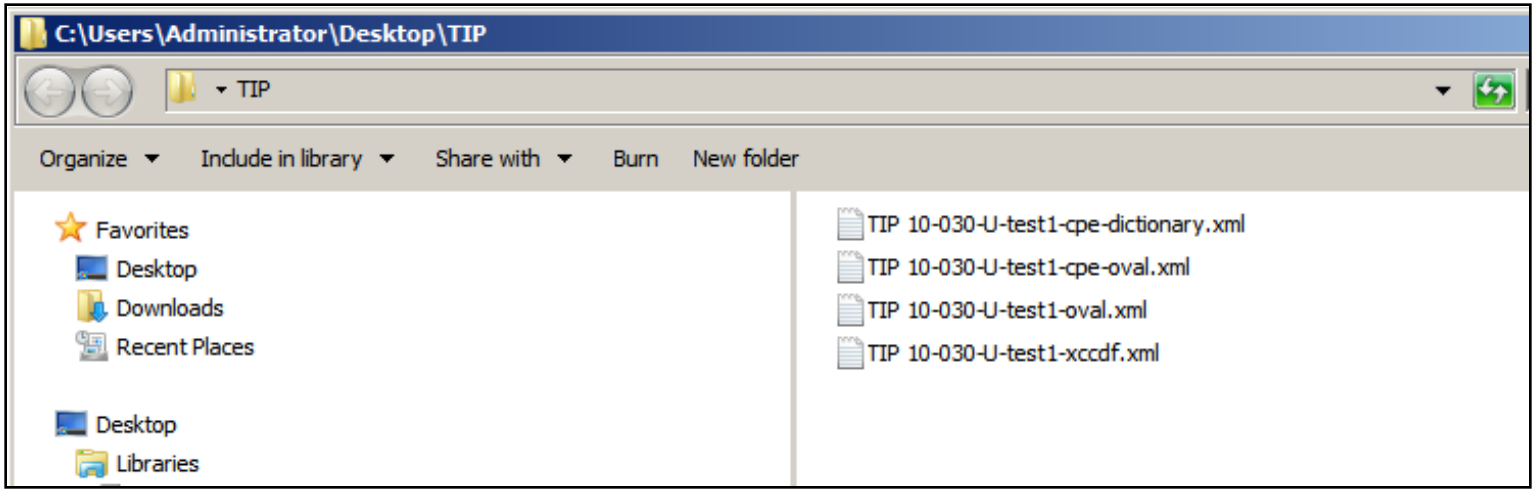
- **PART 1 -** Create SCAP Data Stream for a Single OVAL file.

- **PART 2 -** Create SCAP Data Stream for Multiple OVAL files.

PART 1

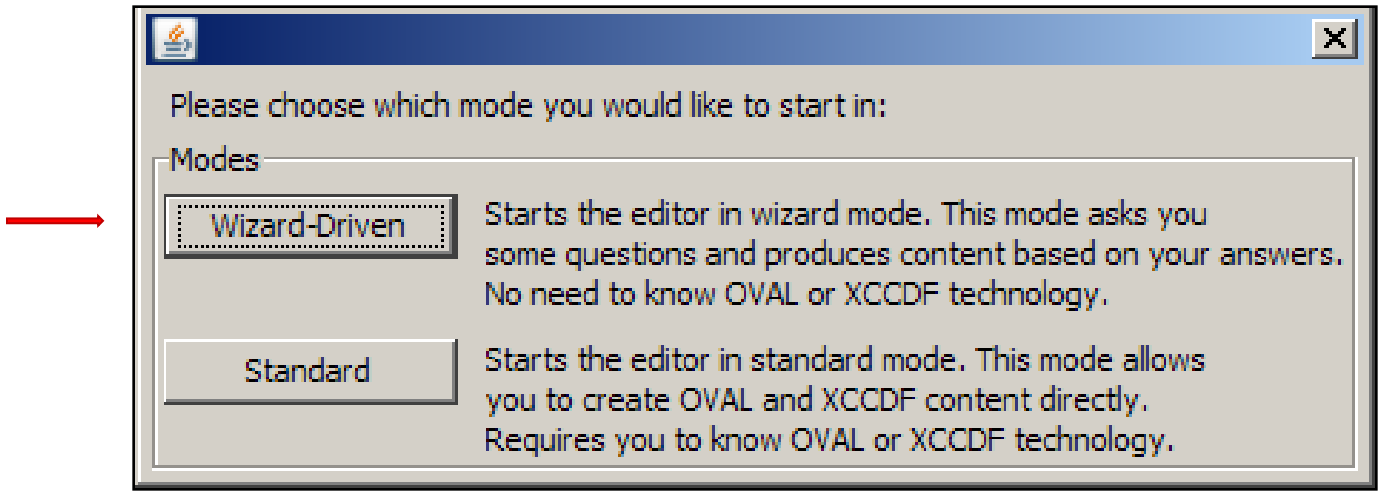
OVAL Creation for a File

OVAL Creation (for a file)

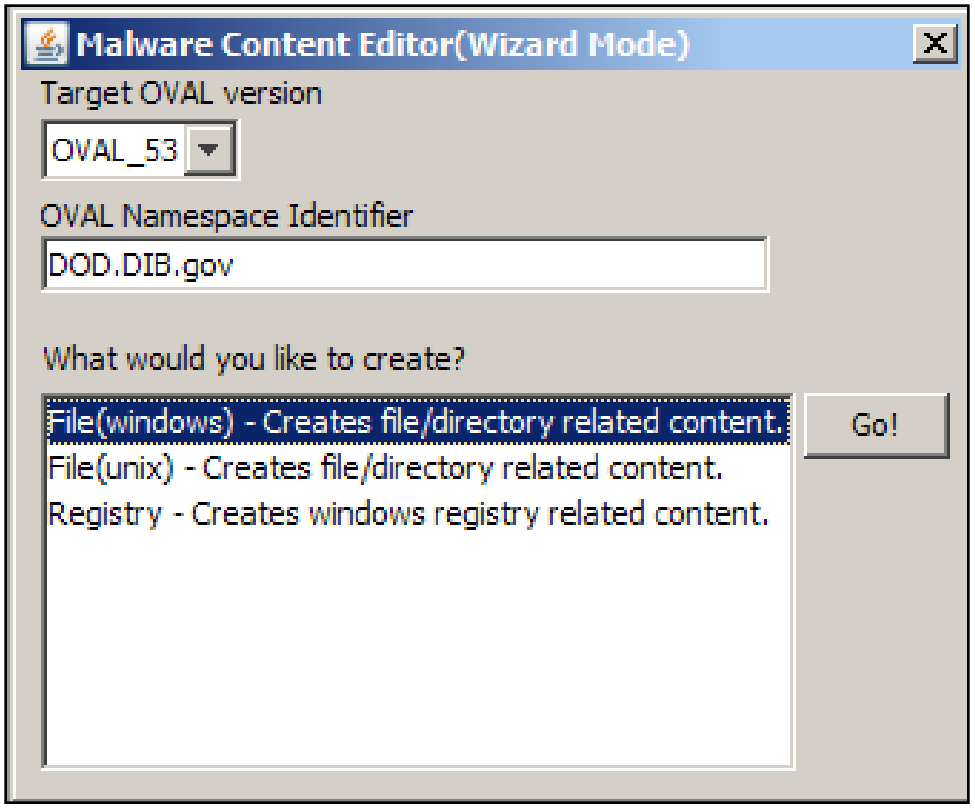


Create SCAP Data Stream for a Single OVAL check

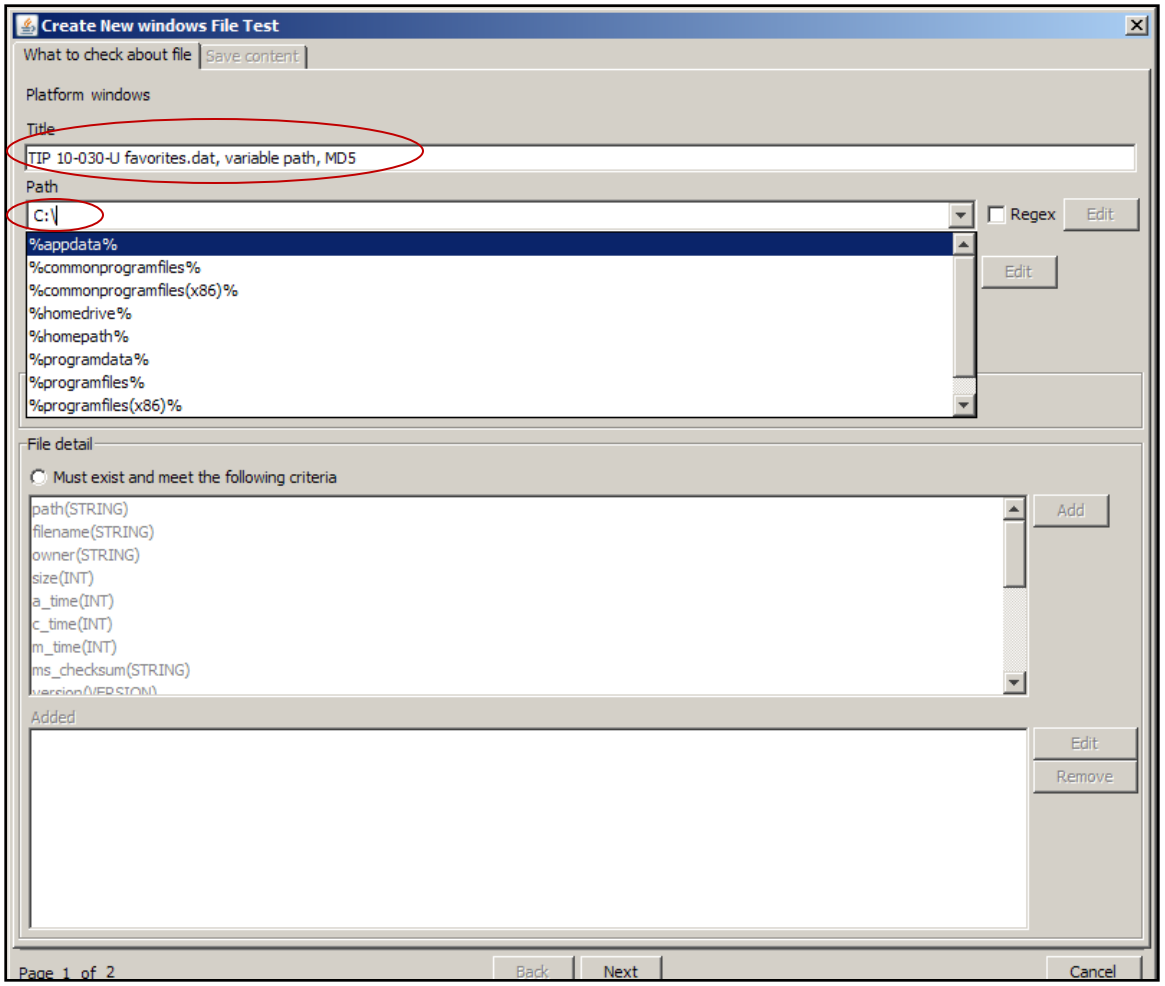
OVAL Creation (for a file)



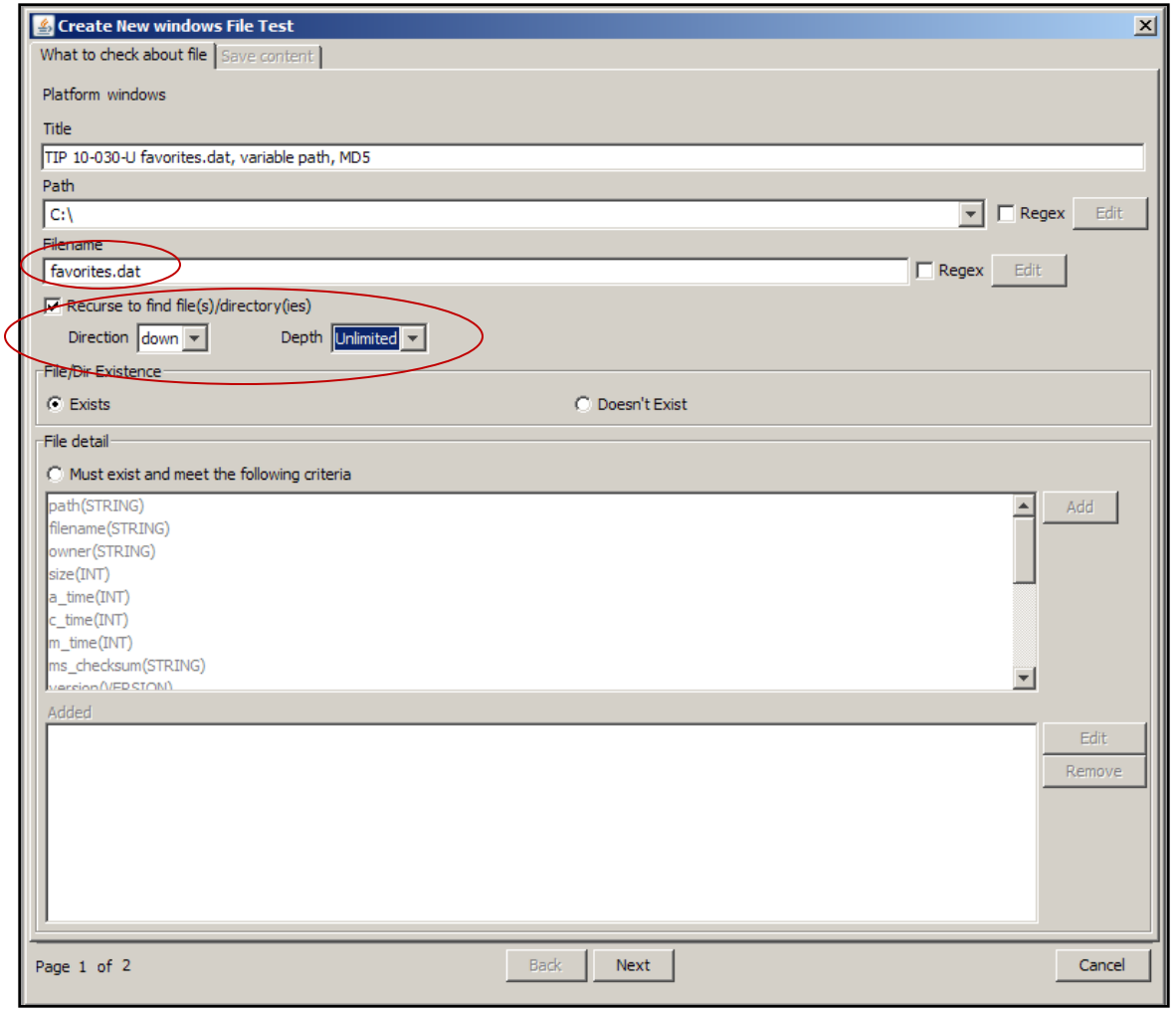
OVAL Creation (for a file)



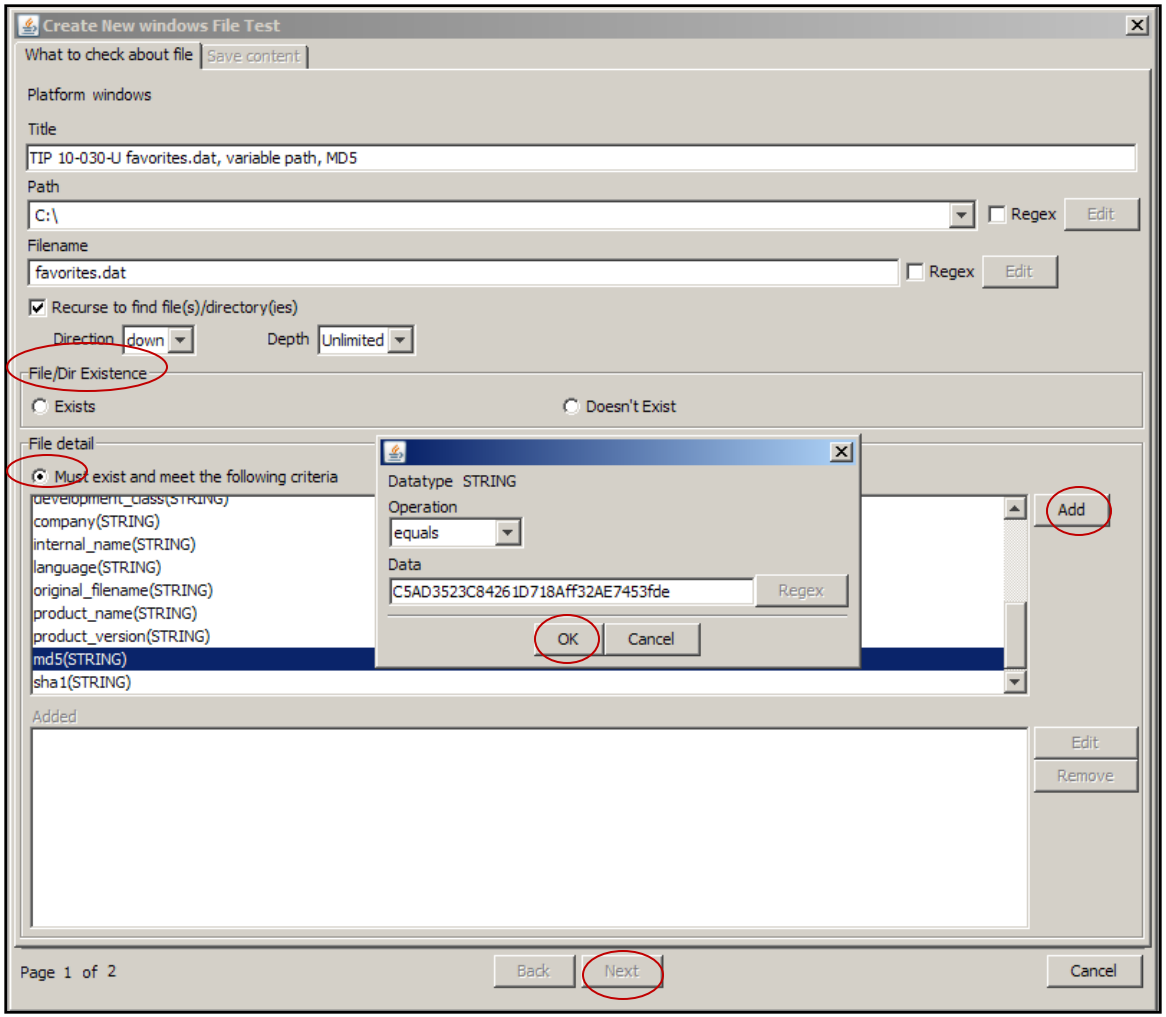
OVAL Creation (for a file)



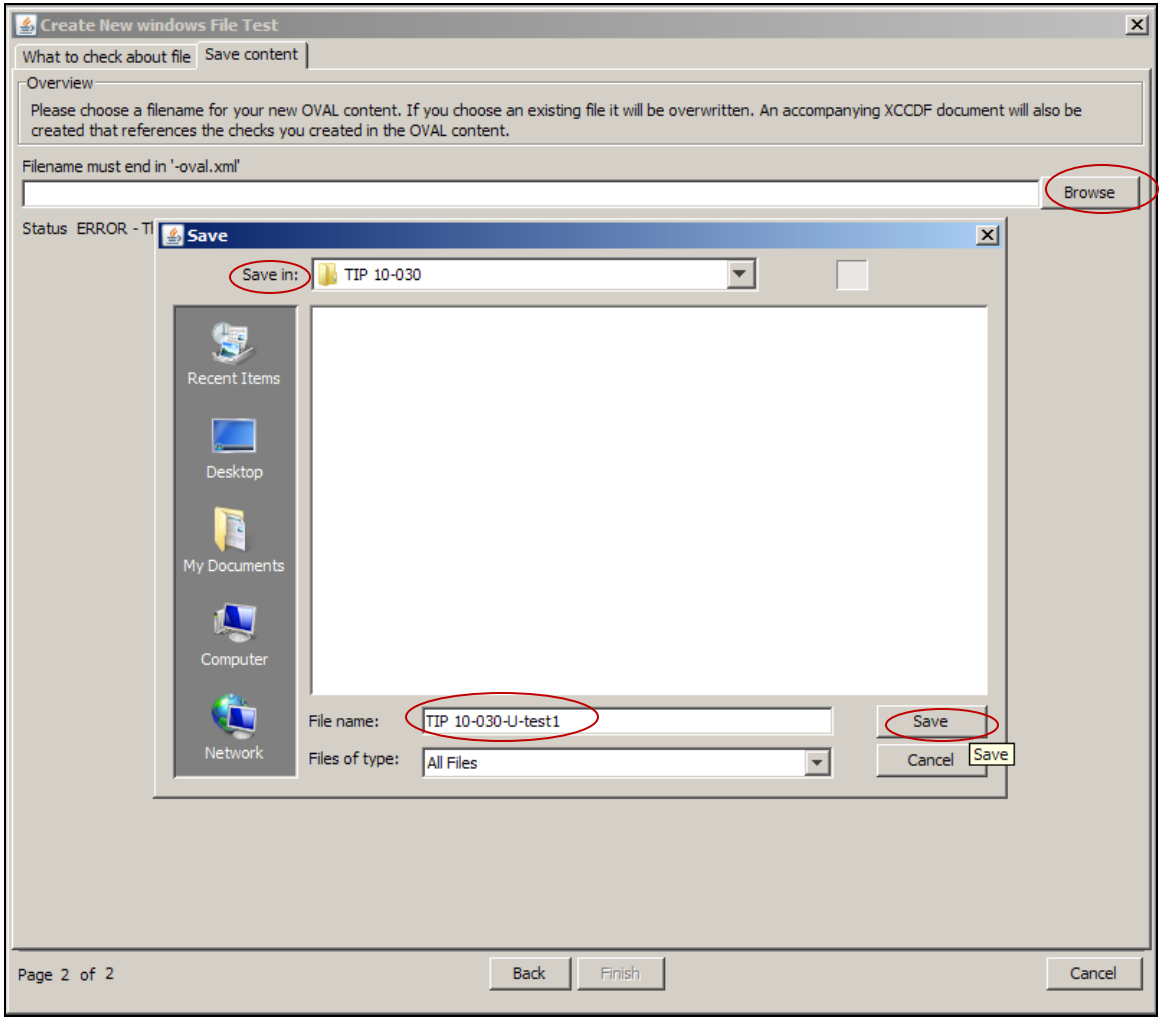
OVAL Creation (for a file)



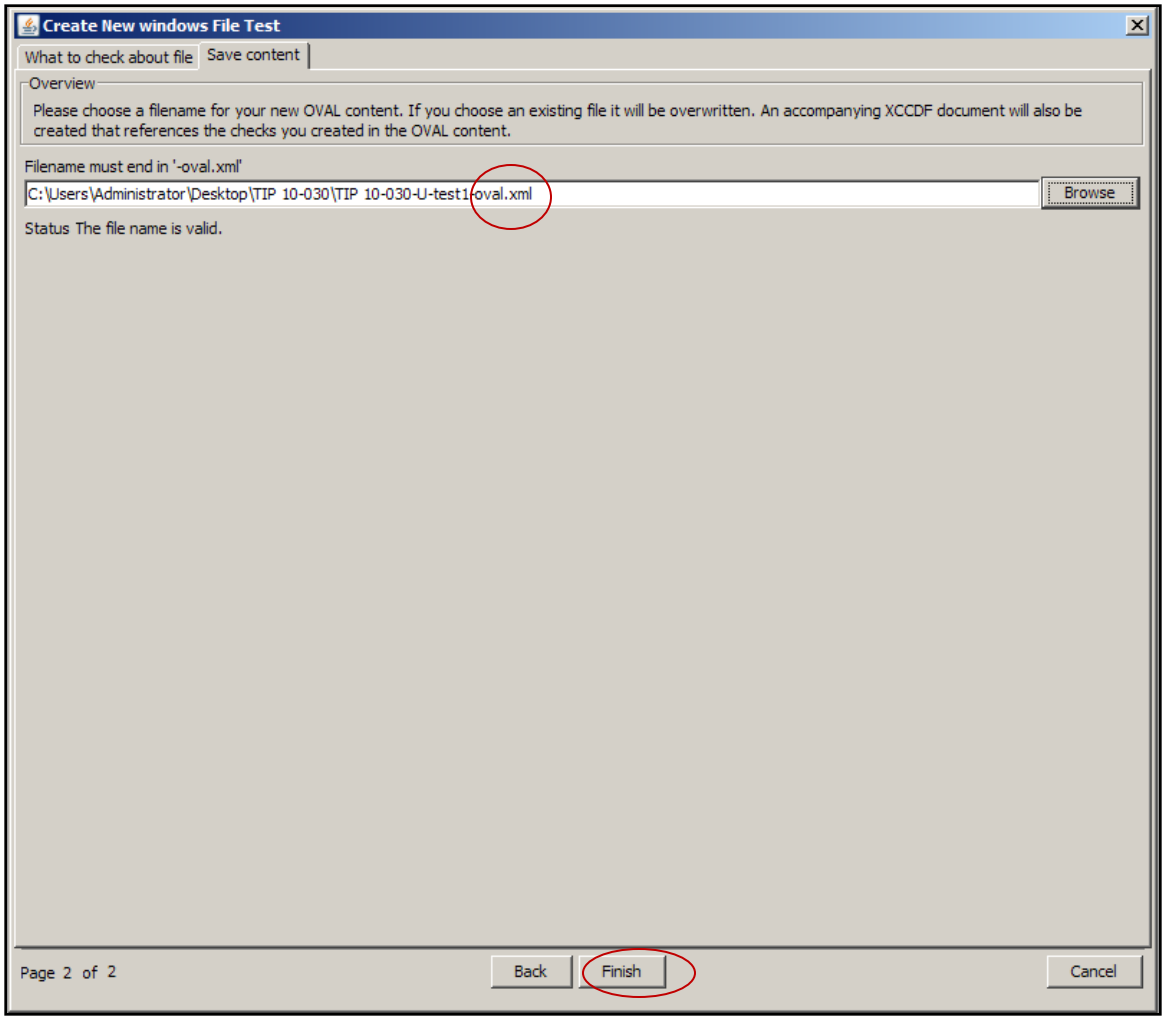
OVAL Creation (for a file)



OVAL Creation (for a file)

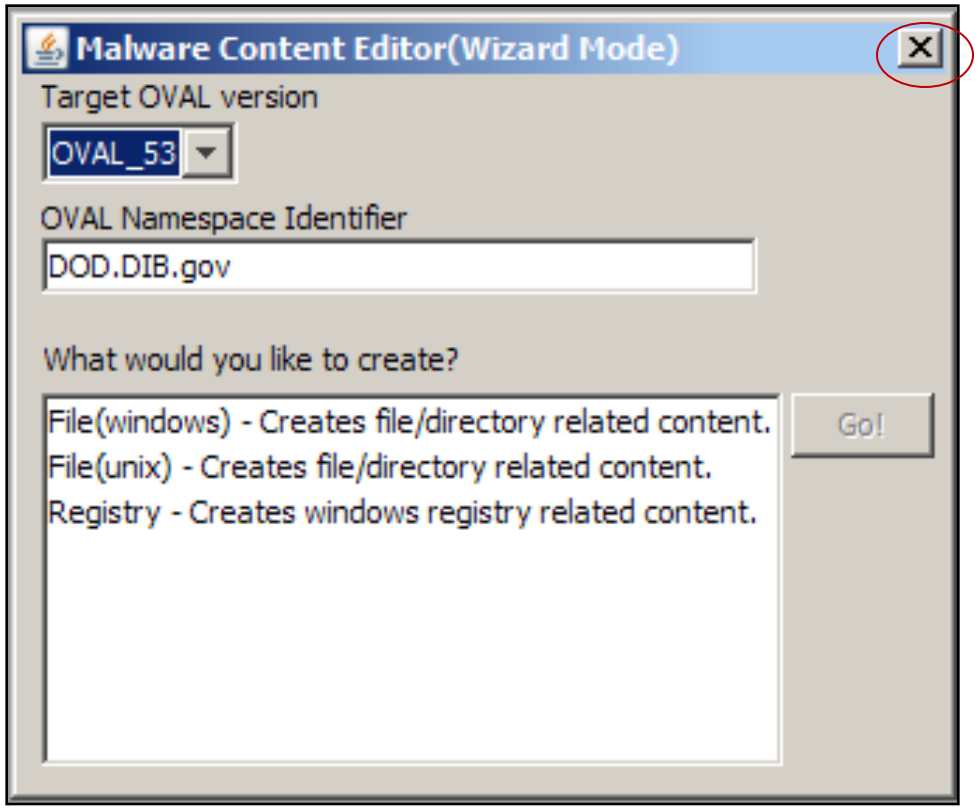


OVAL Creation (for a file)



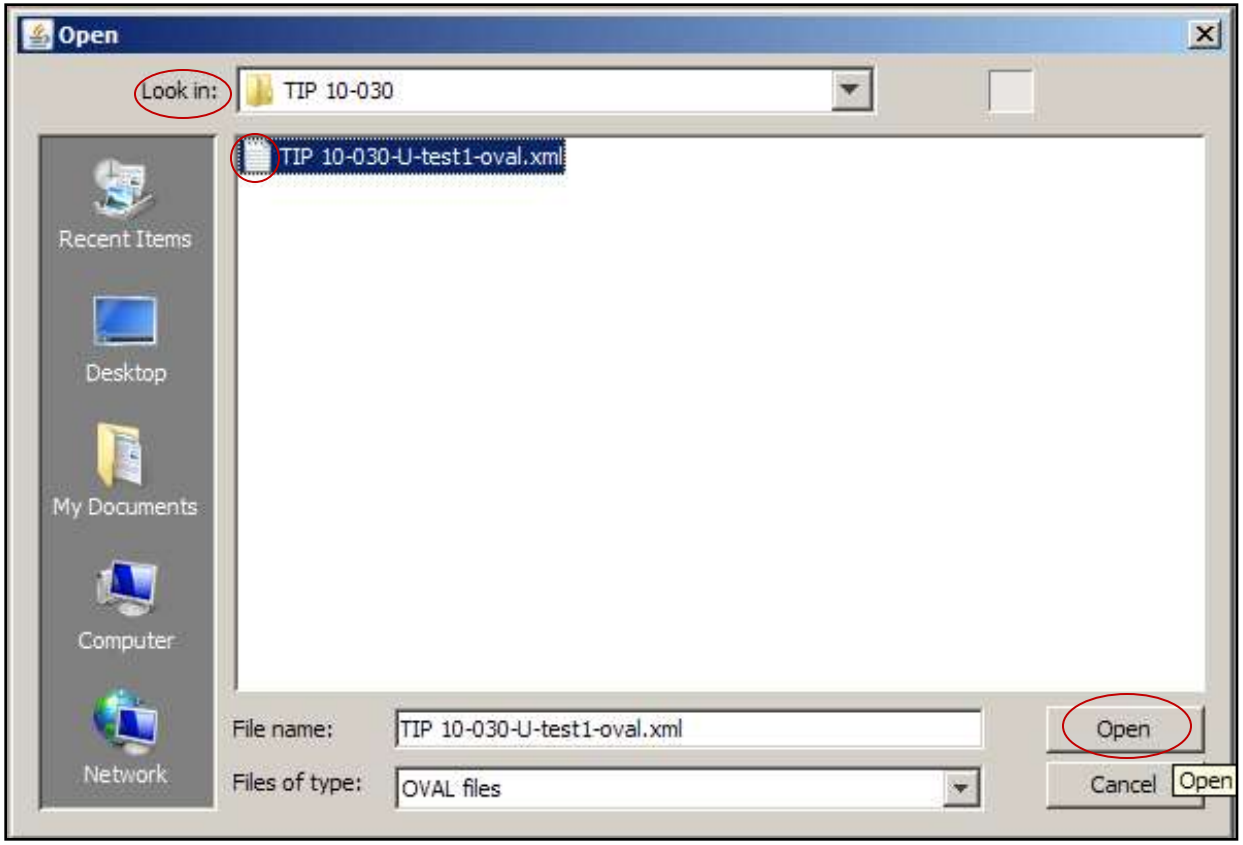
Xccdf automatically generated

OVAL Creation (for a file)



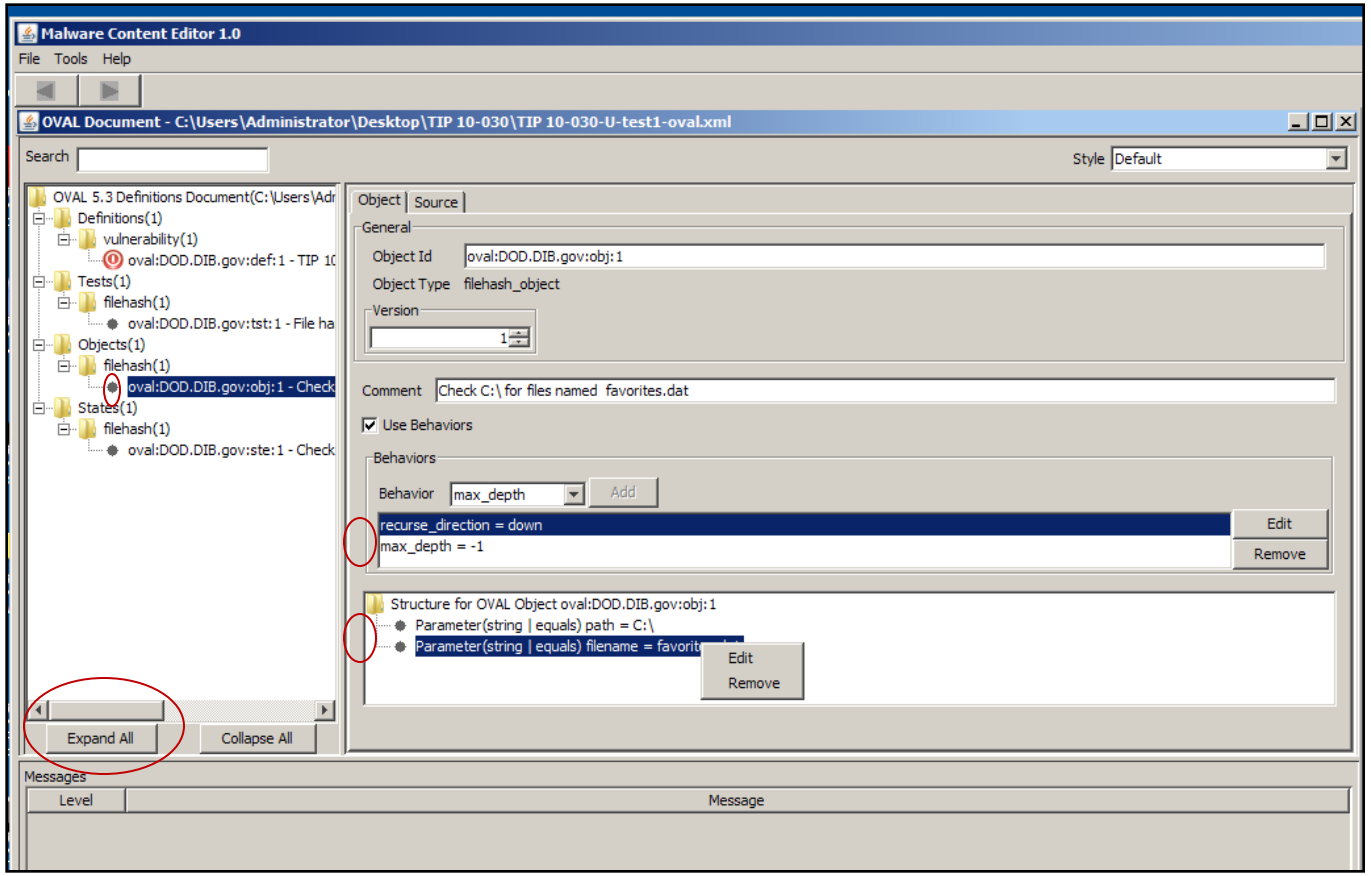
OVAL Content Verification

OVAL Content Verification



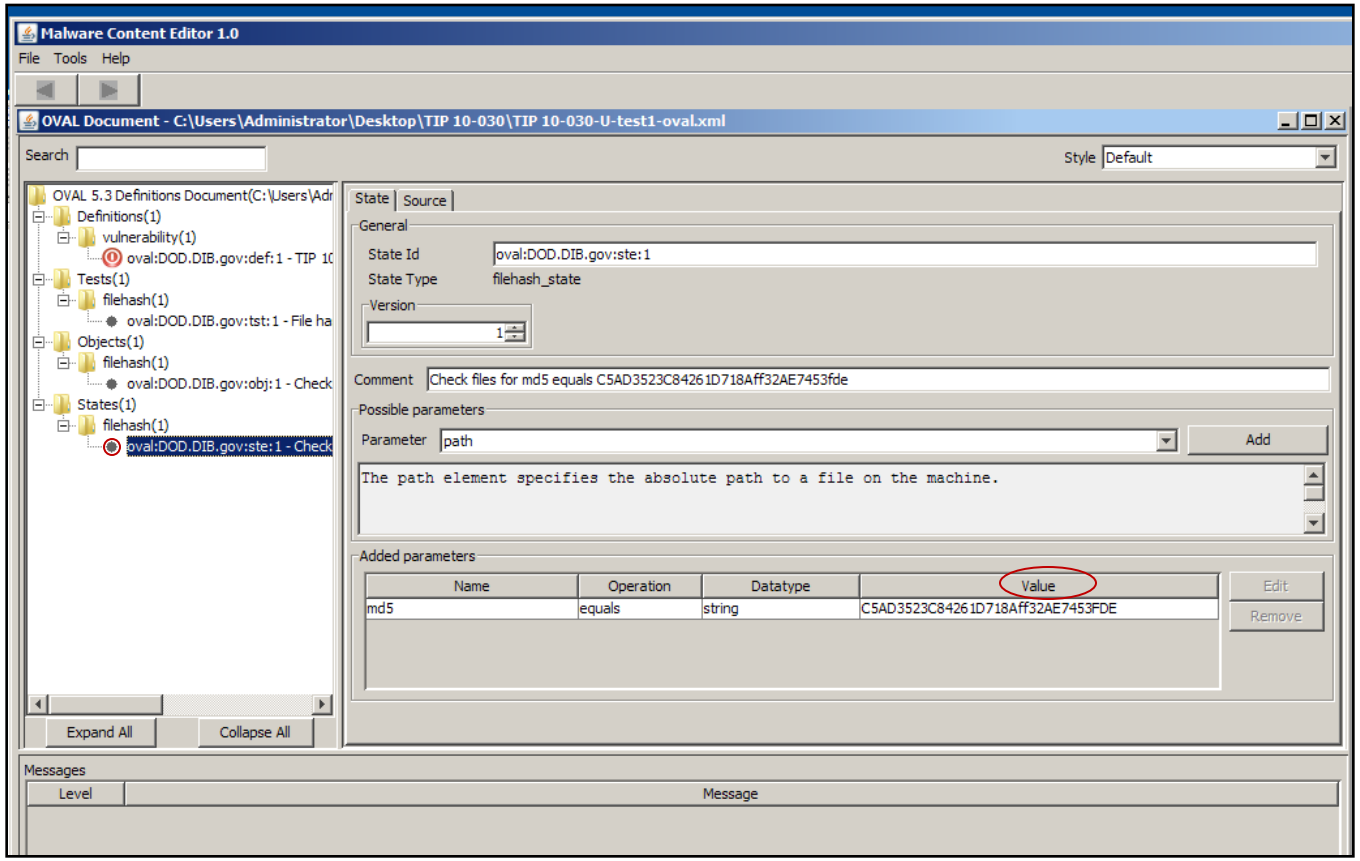
In Standard Mode

OVAL Content Verification



1

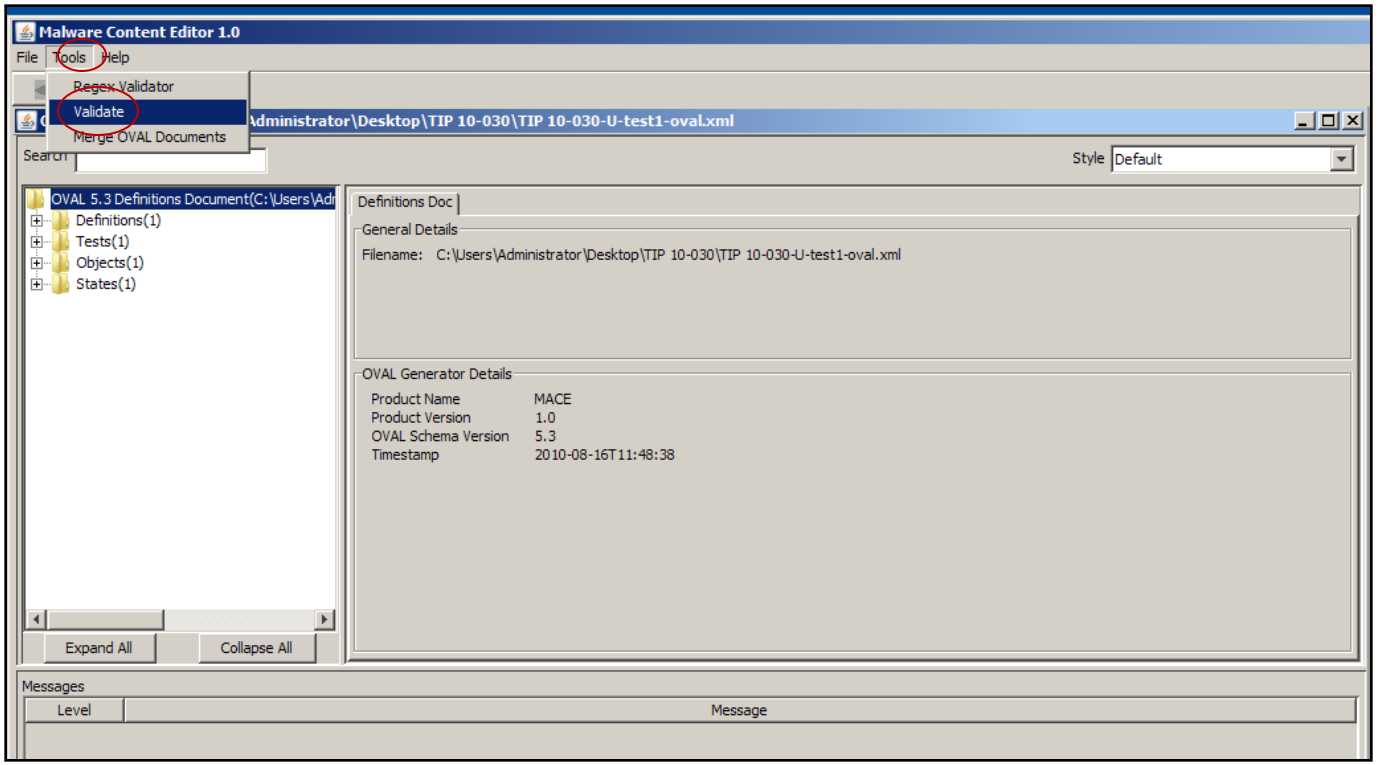
OVAL Content Verification



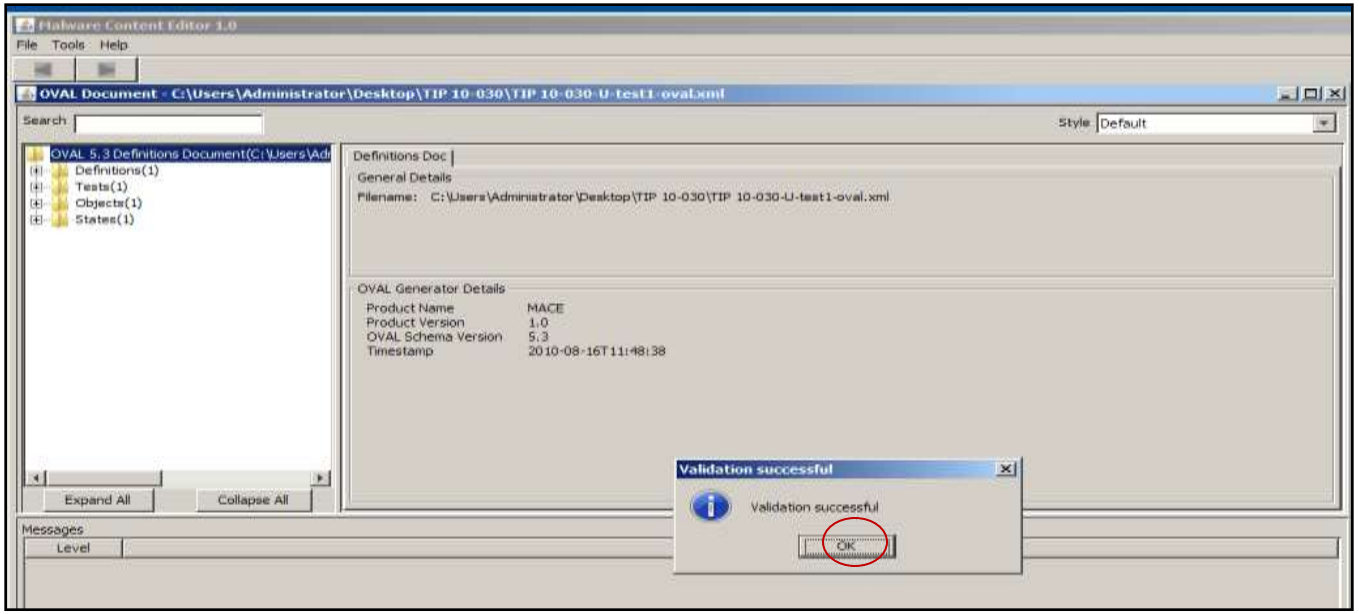
File > Save for any changes

OVAL Validation

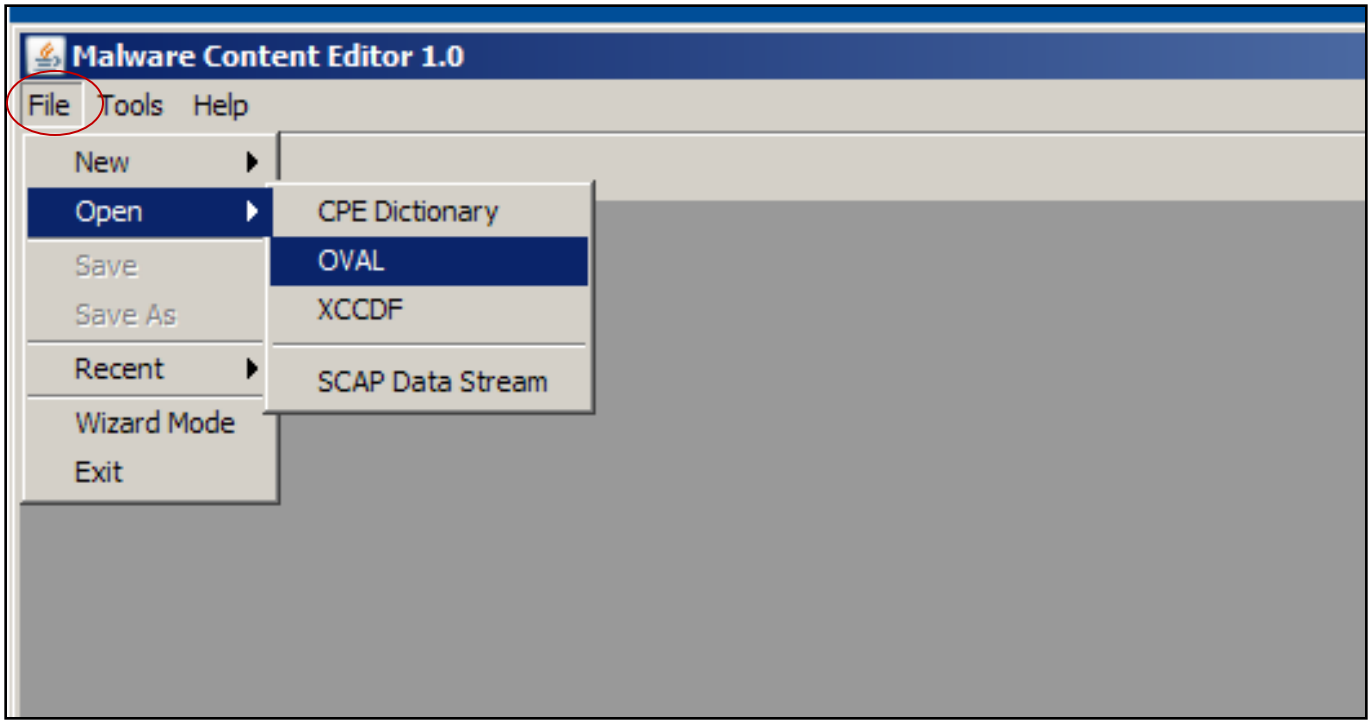
OVAL Validation



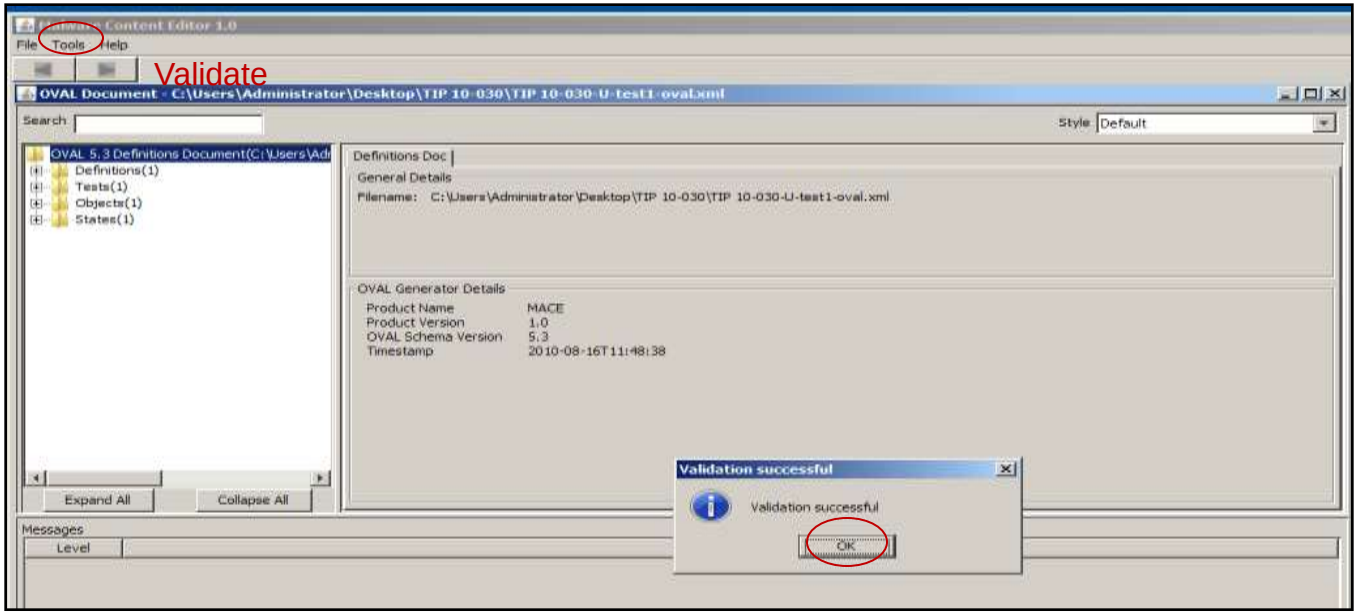
OVAL Validation



OVAL Validation

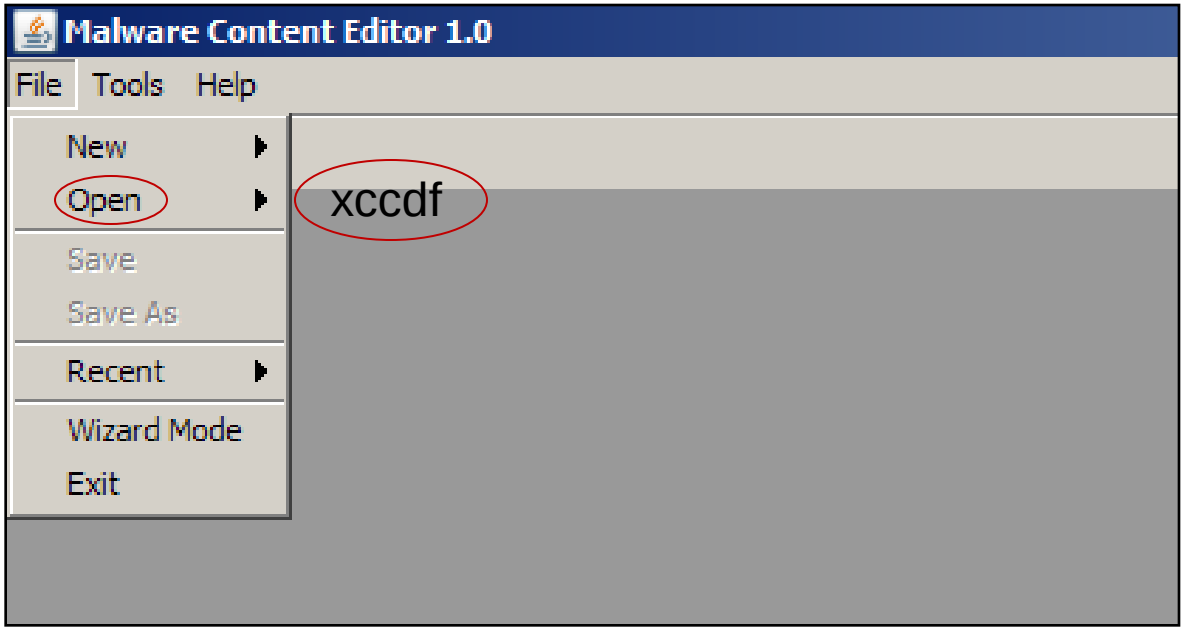


OVAL Validation

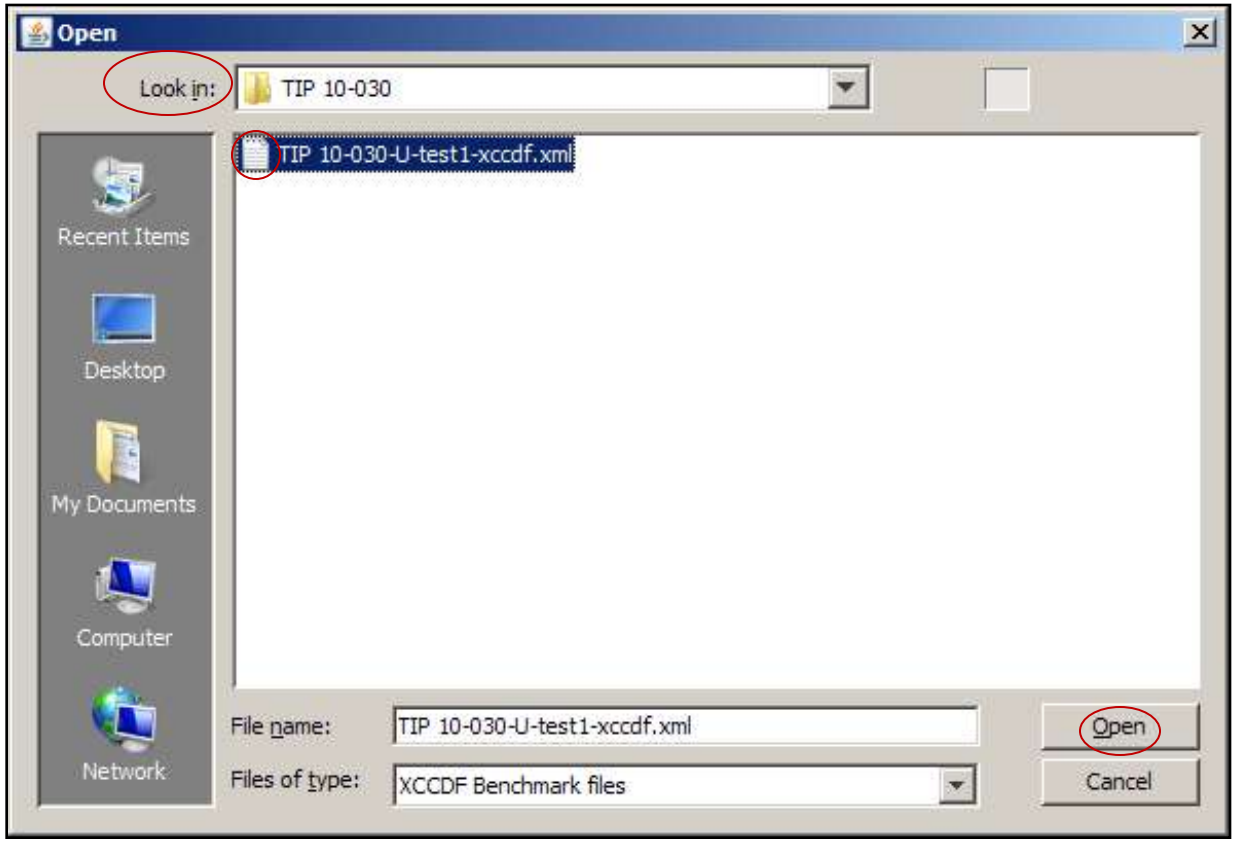


Validate the Automatically Generated XCCDF

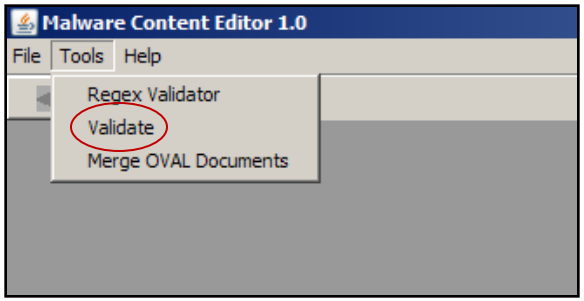
XCCDF Validation



XCCDF Validation

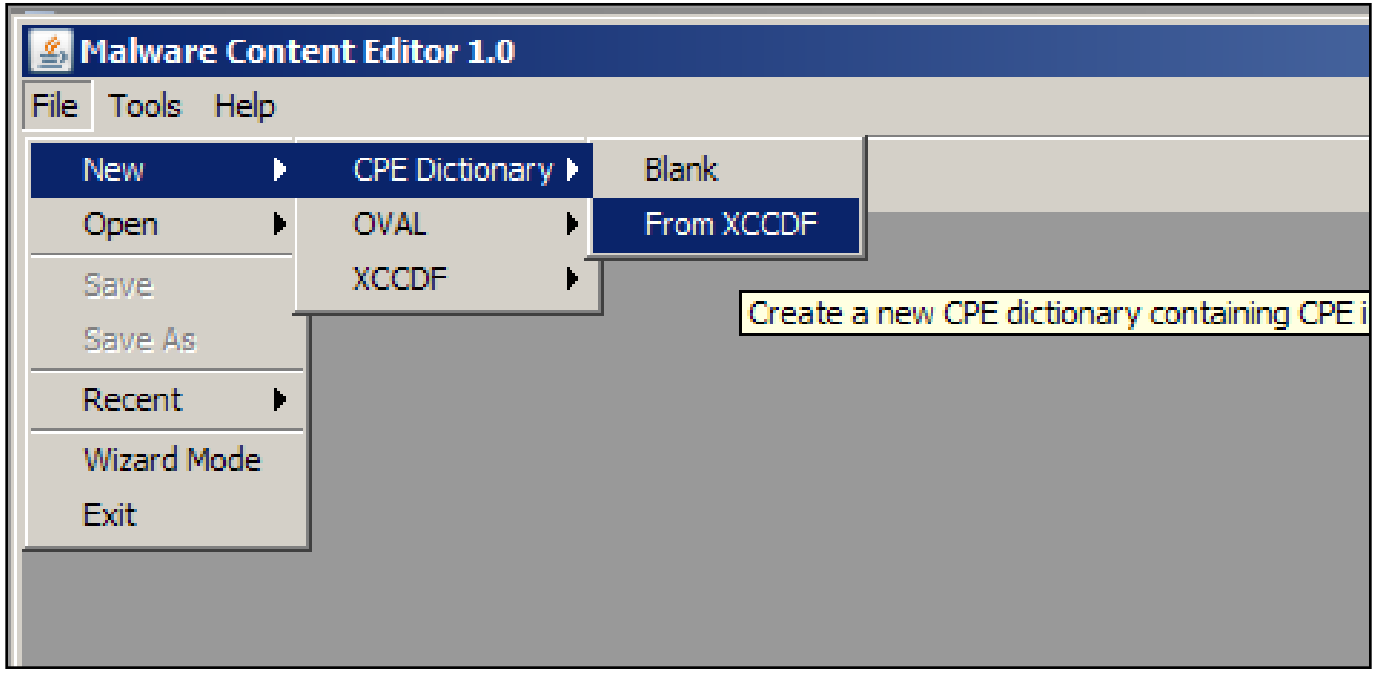


XCCDF Validation

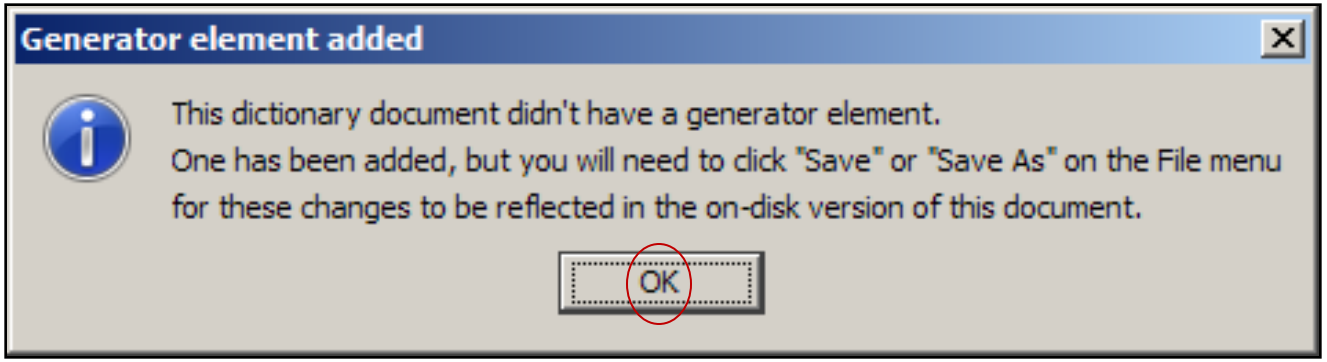


Create Additional SCAP Data Stream files (from the XCCDF)

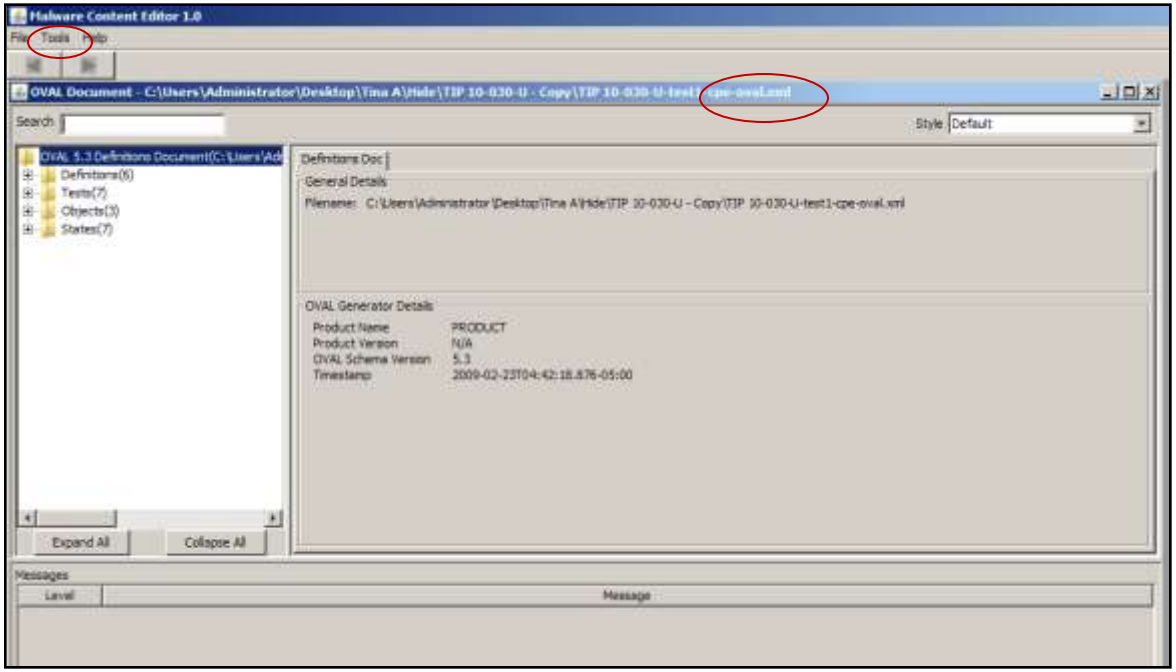
Create the SCAP data stream files



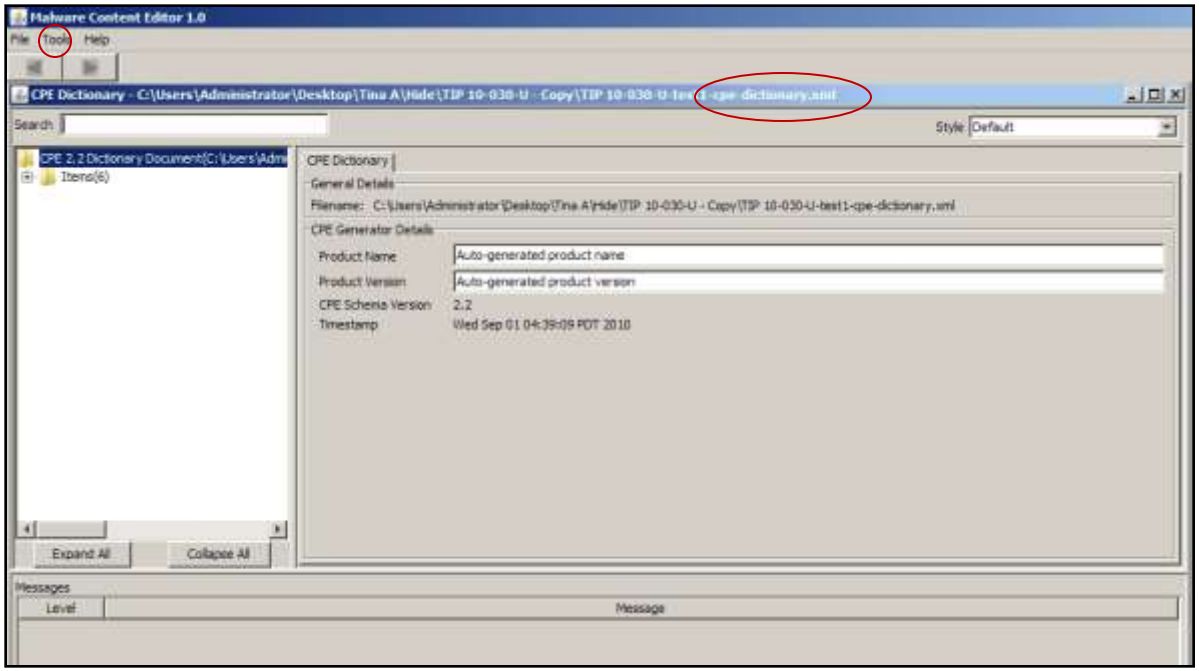
Create the SCAP data stream files



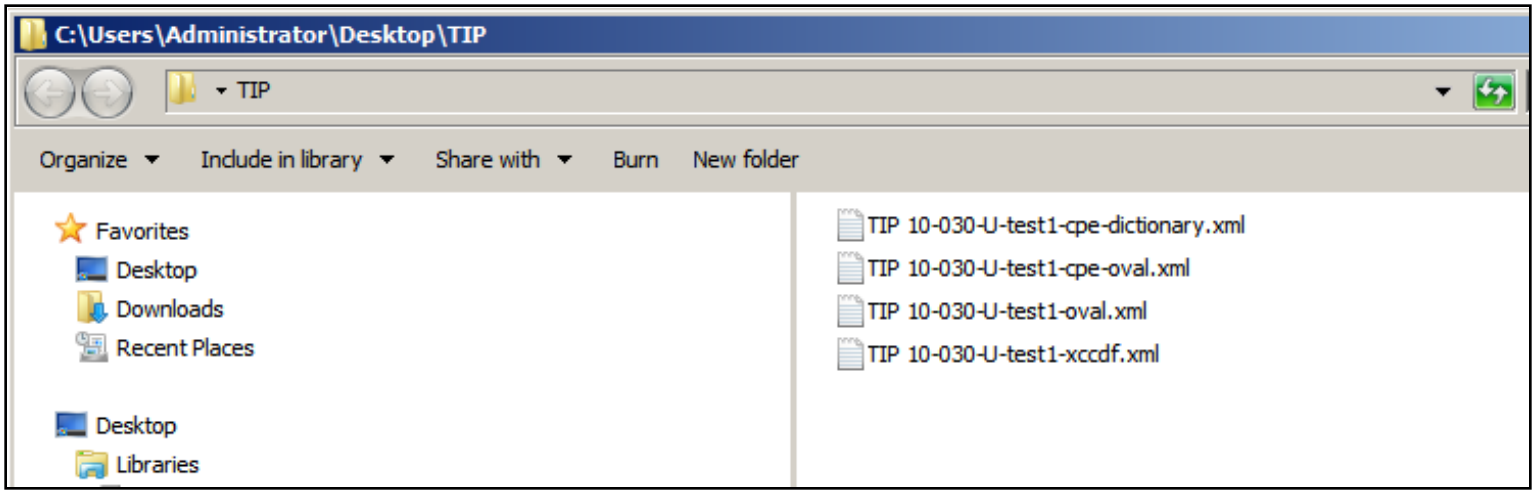
Create the SCAP data stream files



Create the SCAP data stream files

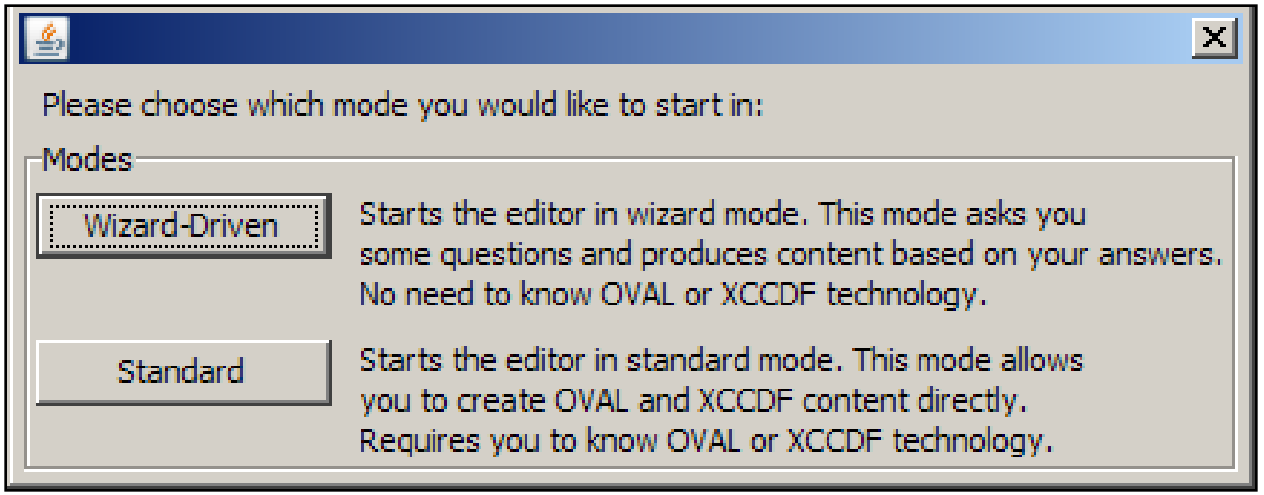


Create the SCAP data stream files

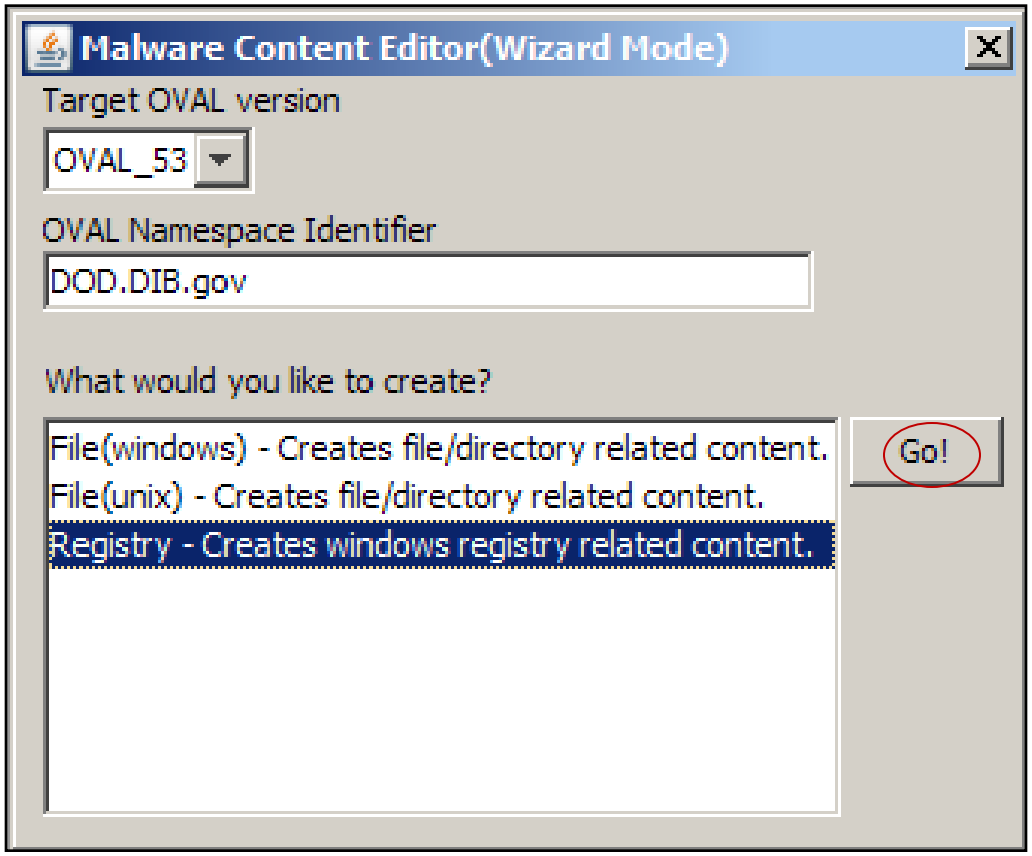


PART 2

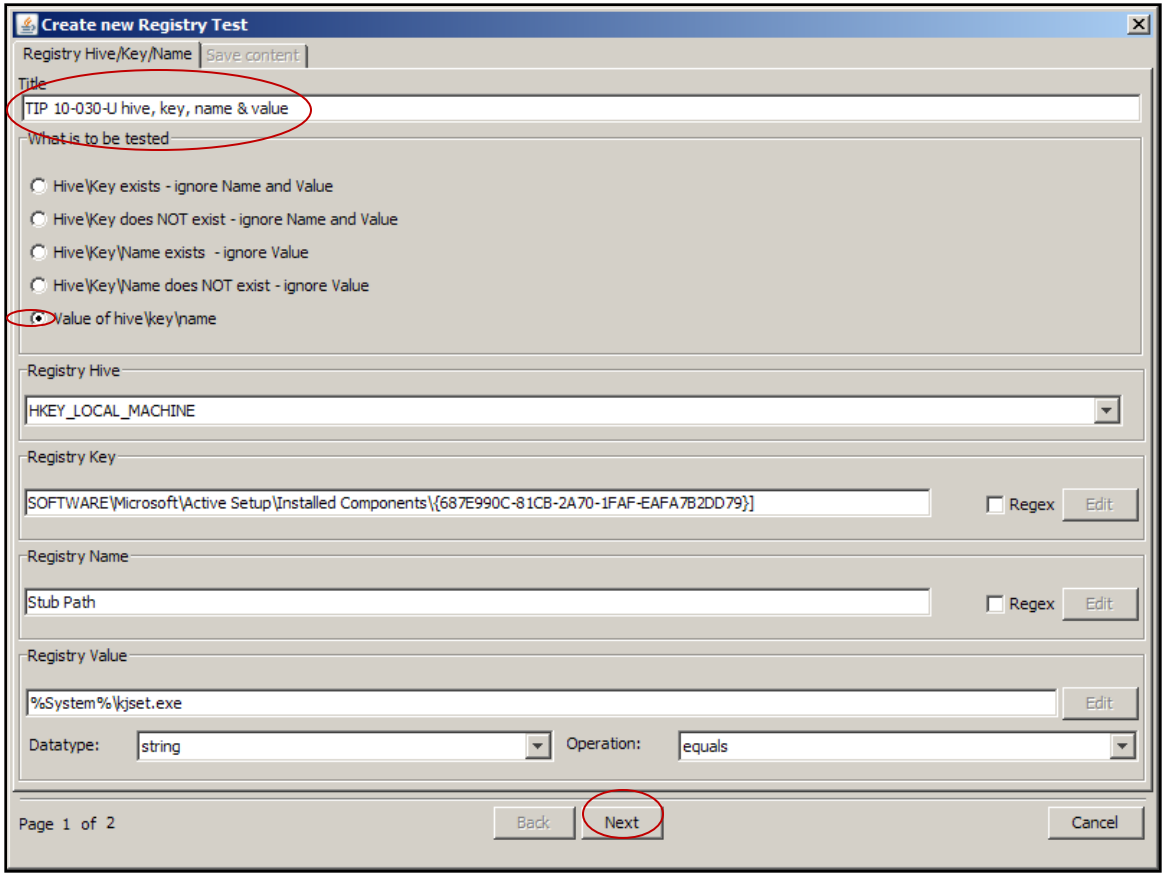
OVAL Creation (for a registry entry)



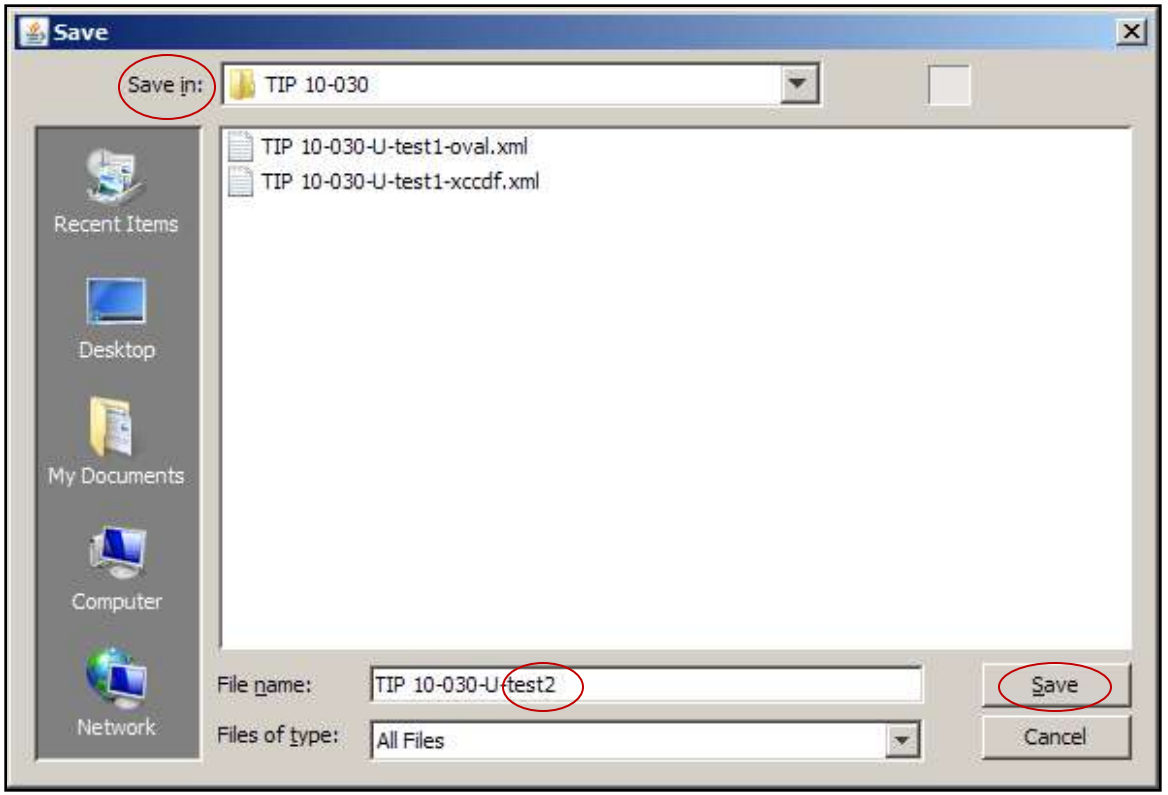
OVAL Creation (for a registry key)



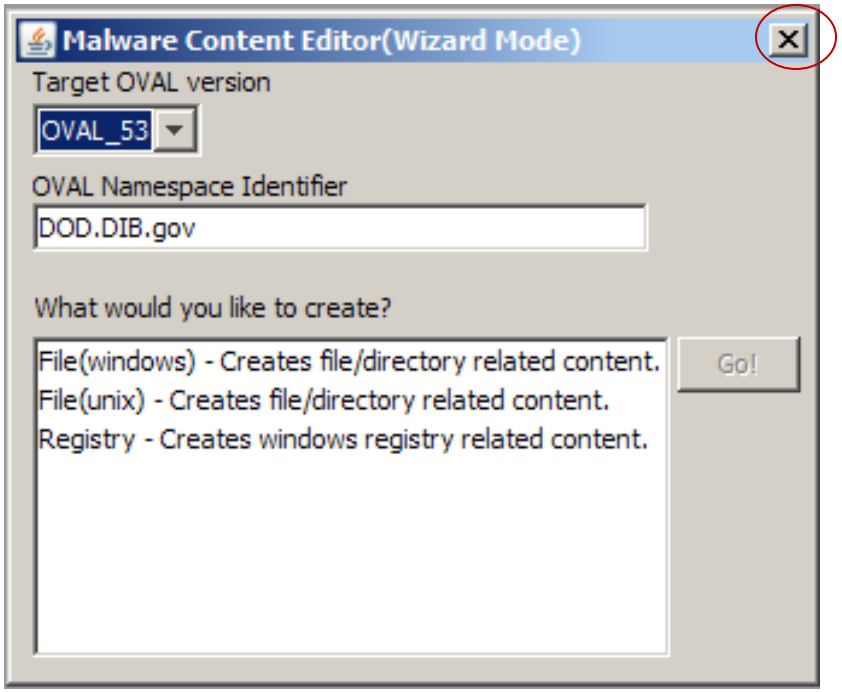
OVAL Creation (for a registry key)



OVAL Creation (for a registry key)

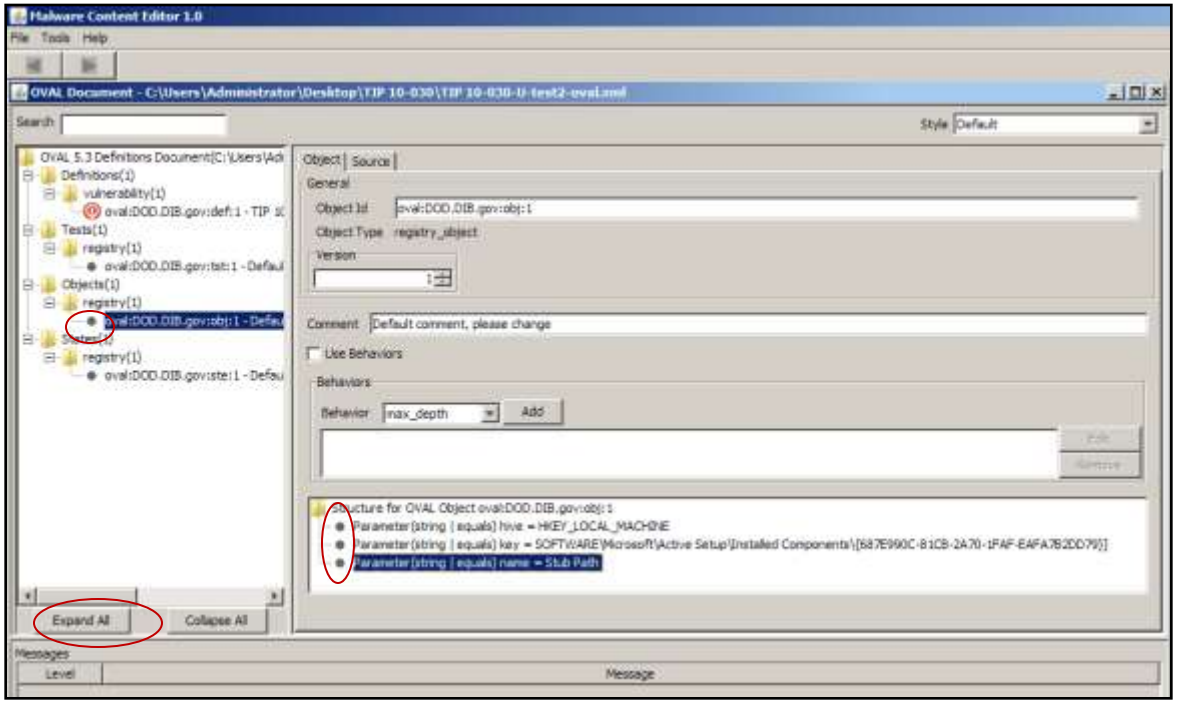


OVAL Creation (for a registry key)

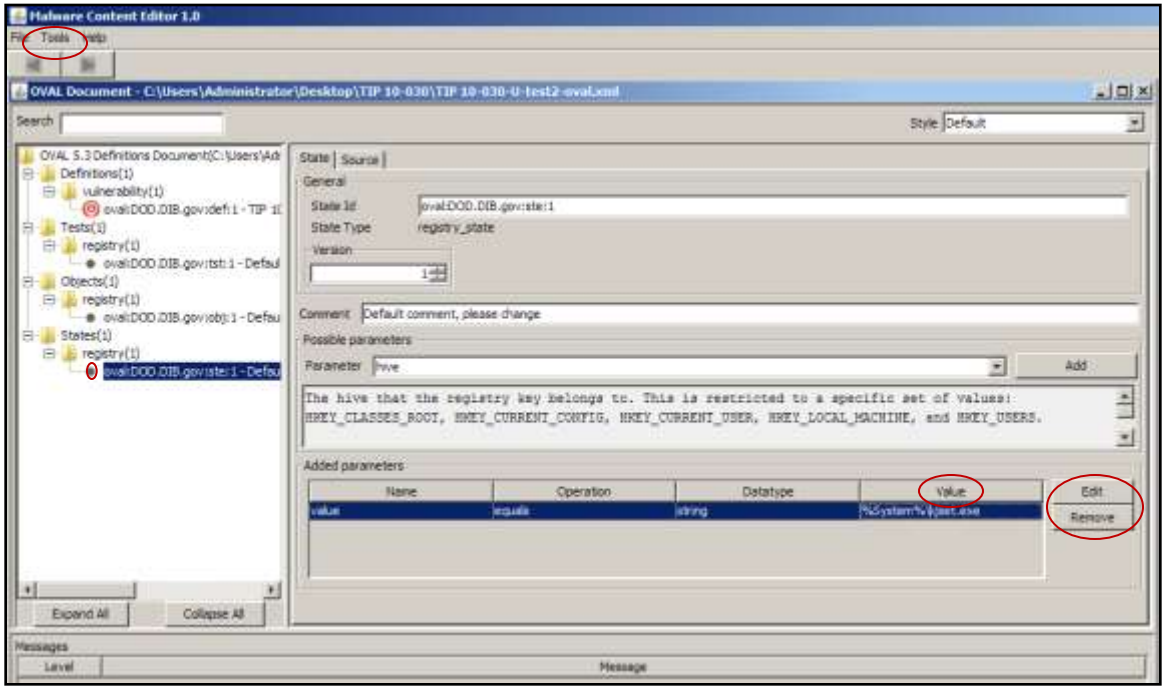


OVAL Content Verification – Registry

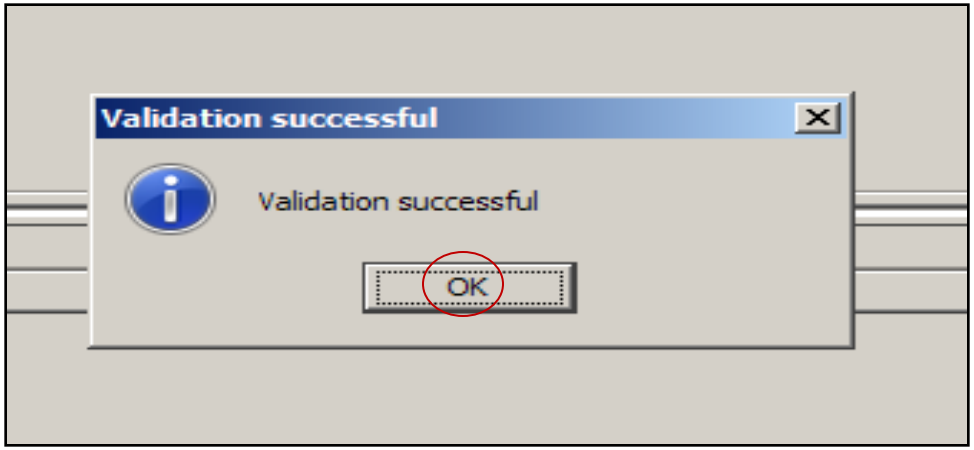
OVAL Content Verification – Registry



OVAL Content Verification – Registry

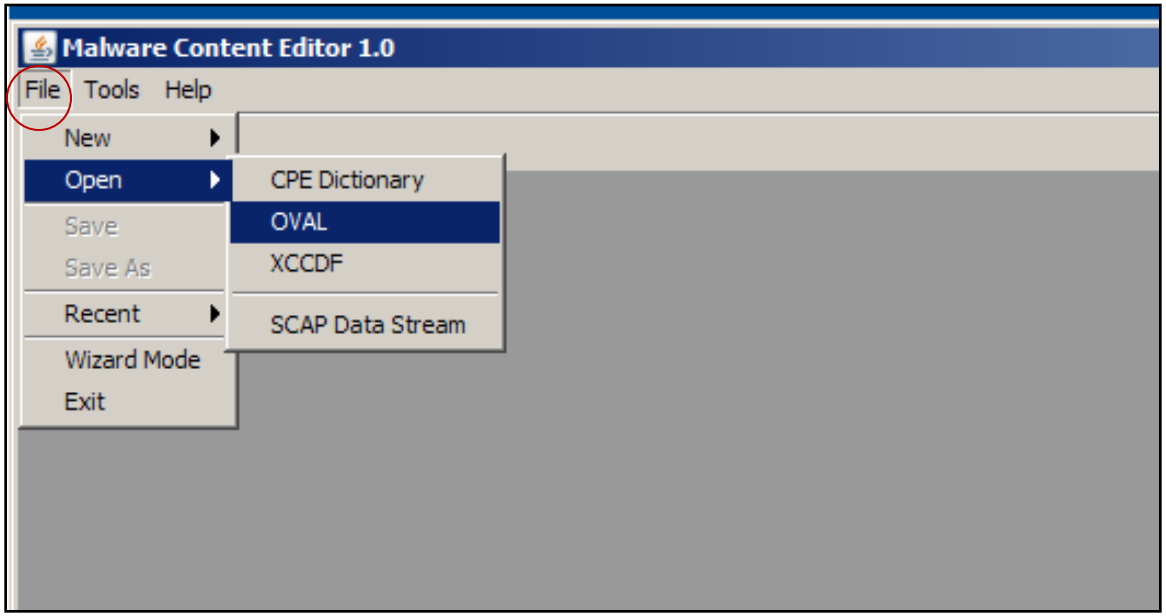


OVAL Content Verification – Registry

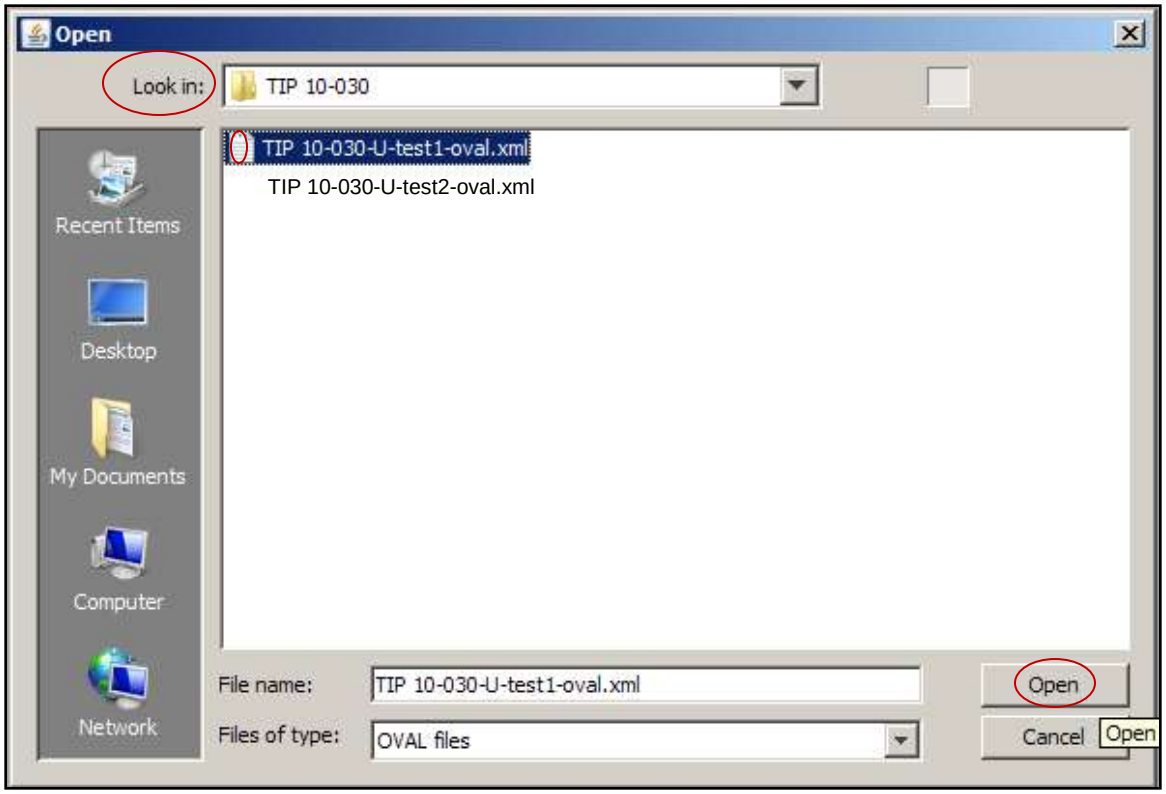


Validate OVAL File

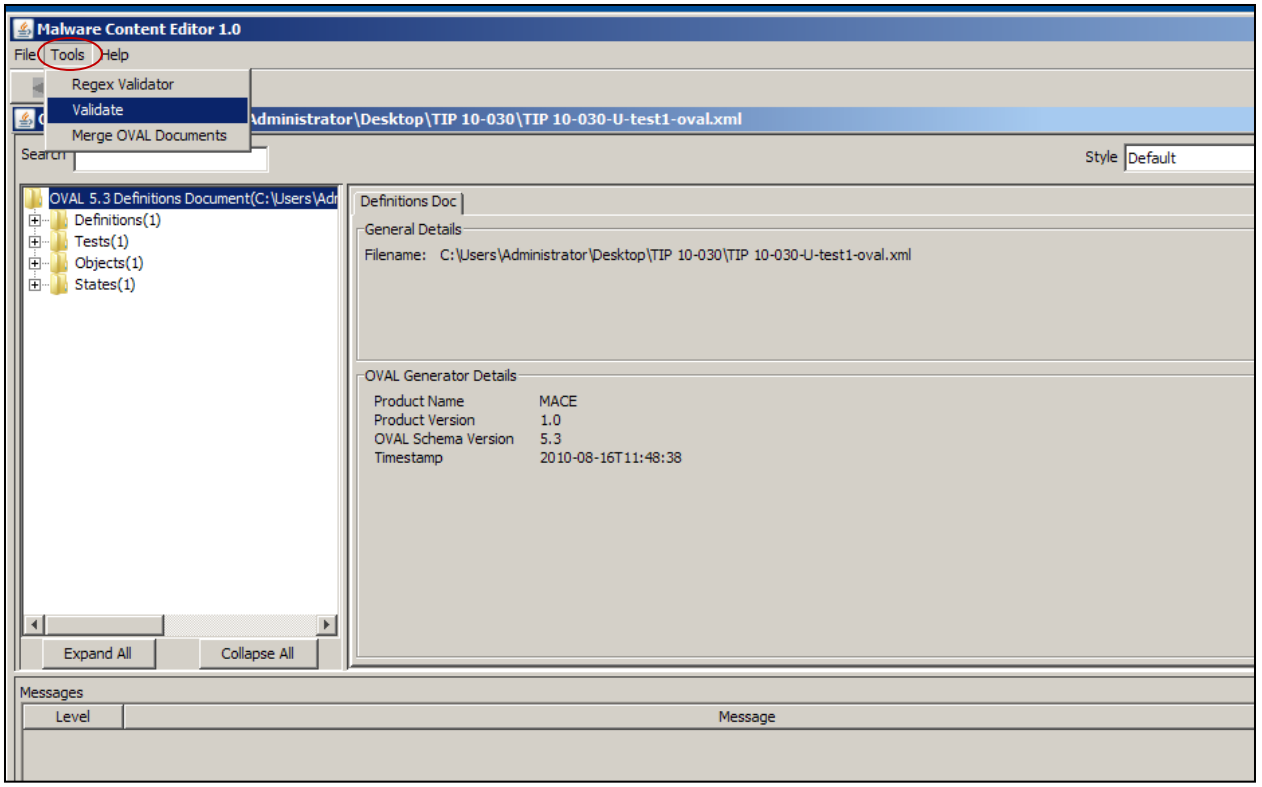
Validate OVAL File



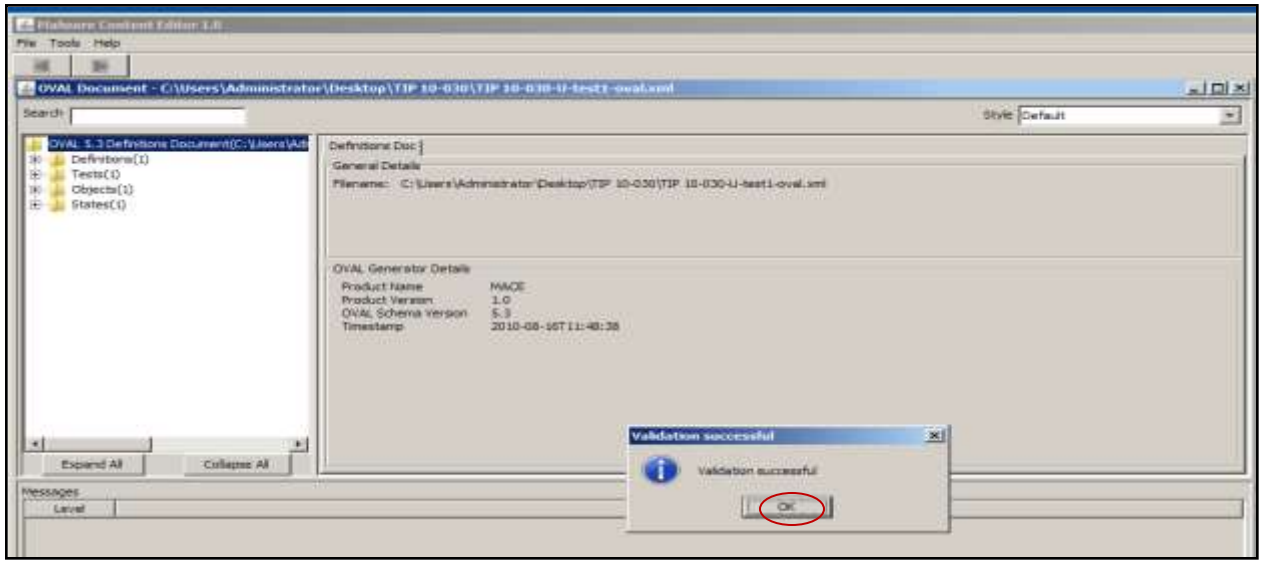
Validate OVAL File



Validate OVAL File



Validate OVAL File



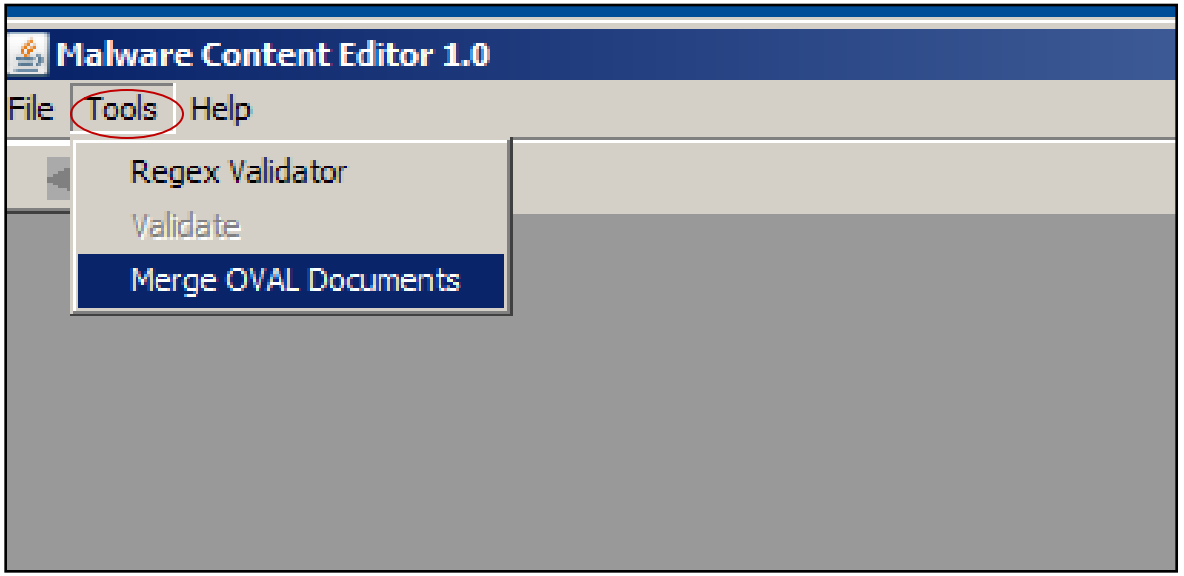
OVAL Creation

***If you have additional registry checks then you will repeat these steps for all additional registry checks.

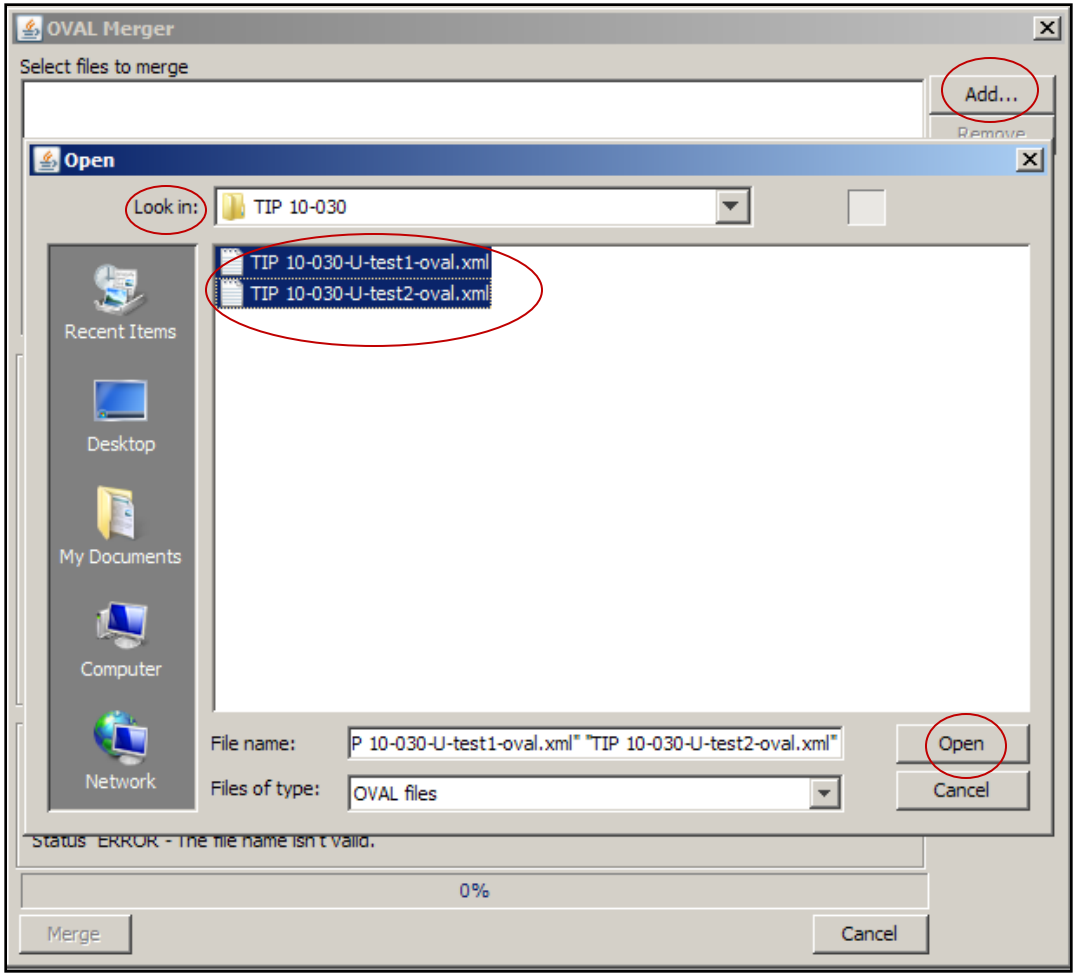
***If you have additional OVAL Checks for files follow the steps in the previous section to generate, verify and validate each OVAL. Repeat these steps for any additional OVAL checks for files. The remaining slides will indicate how to merge all OVAL files and produce the FINAL OVAL.xml, FINAL-XCCDF.xml , FINAL-CPE-Dictionary.xml, and FINAL-CPE-OVAL.xml files

Create FINAL-OVAL.xml by Merging Multiple OVAL files

Create FINAL-OVAL.xml by Merging Multiple OVAL files

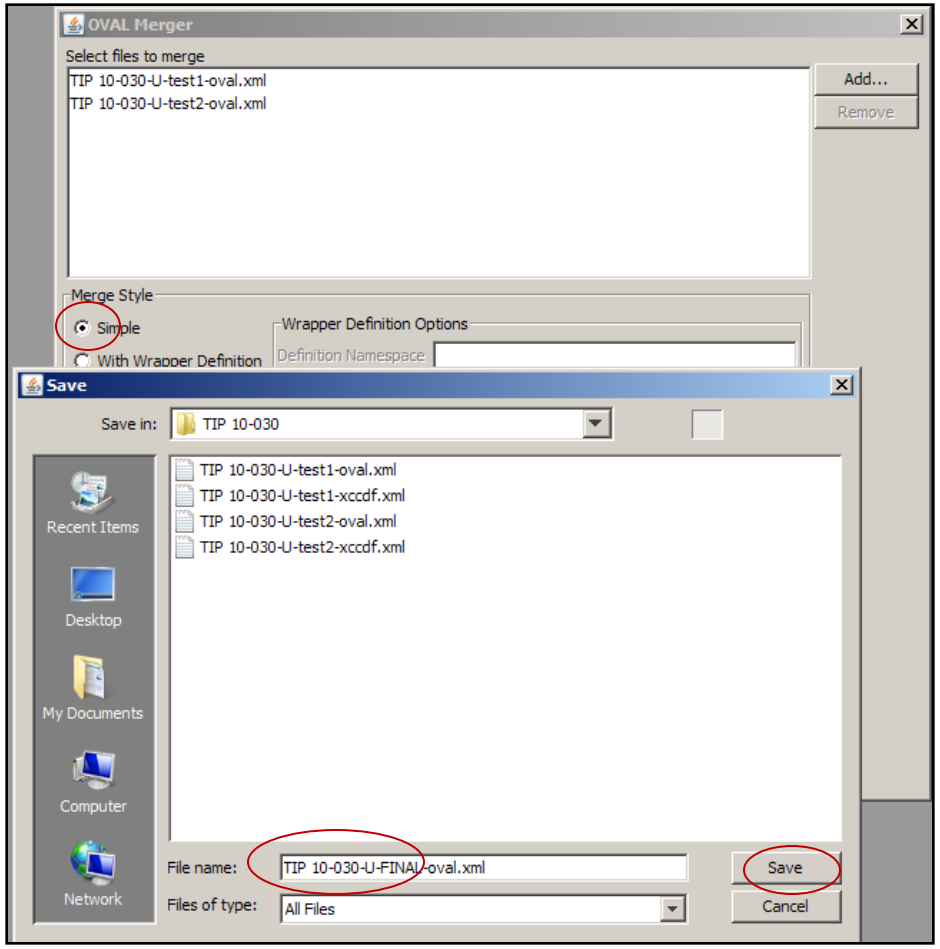


Create FINAL-OVAL.xml by Merging Multiple OVAL files

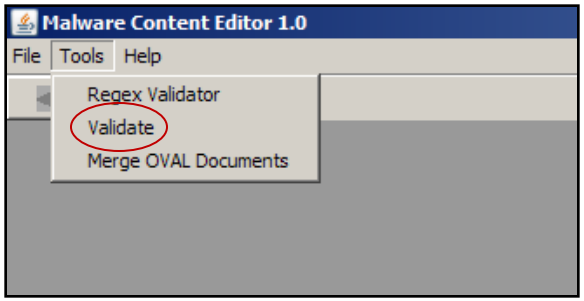


Create FINAL-OVAL.xml by Merging Multiple OVAL files

Select Browse & name FINAL

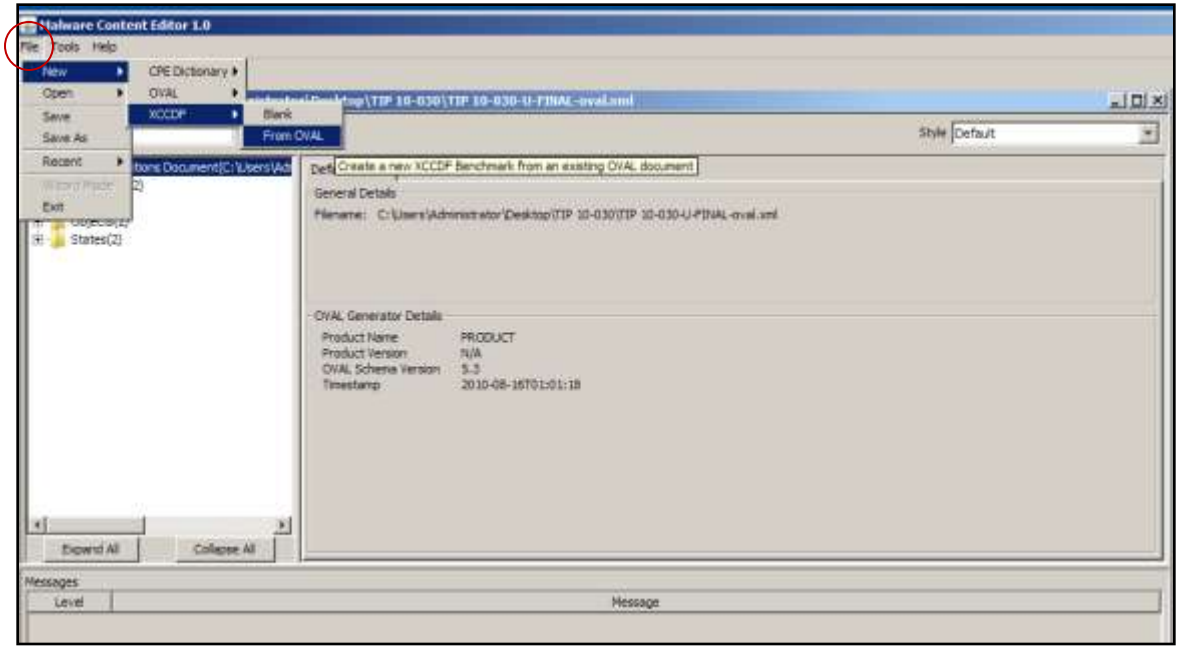


Merged OVAL Validation

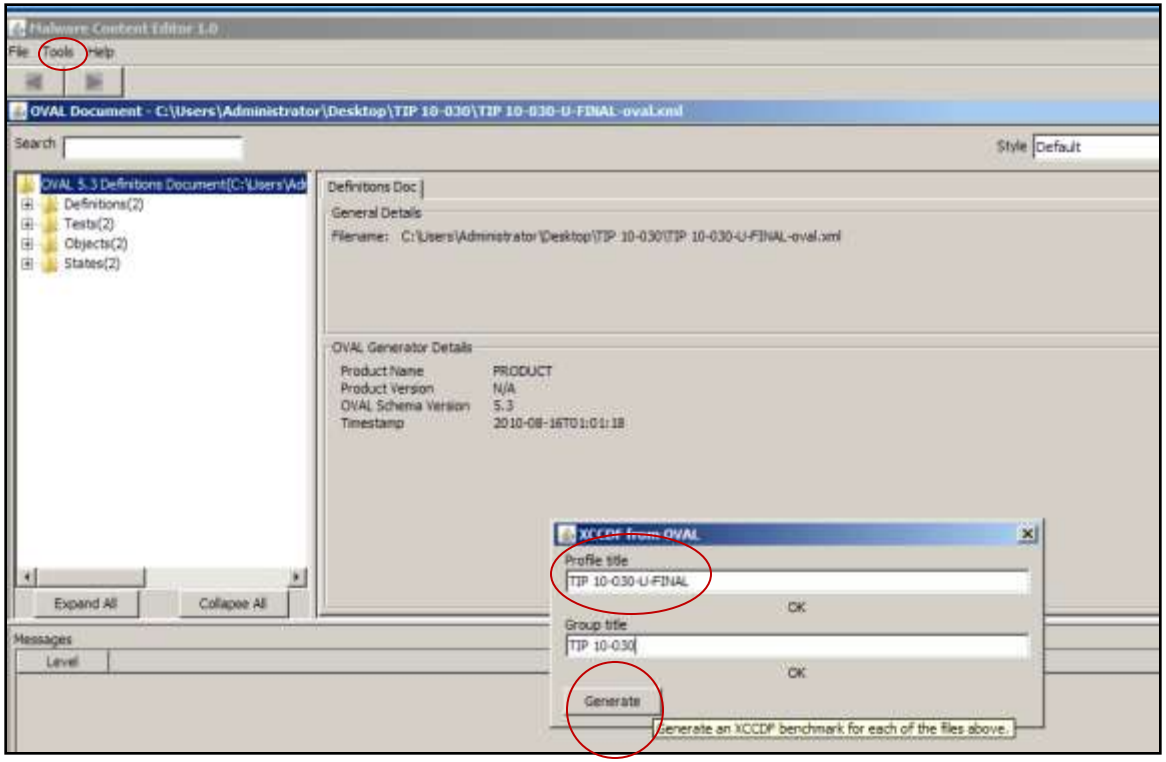


Create the FINAL XCCDF.xml from the FINAL OVAL.xml

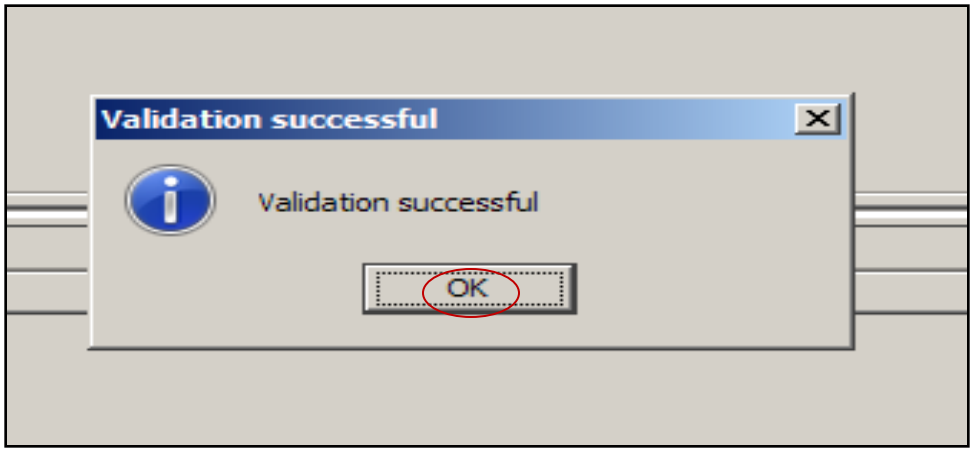
Create the FINAL XCCDF.xml from the FINAL OVAL.xml



Create the FINAL XCCDF.xml from the FINAL OVAL.xml

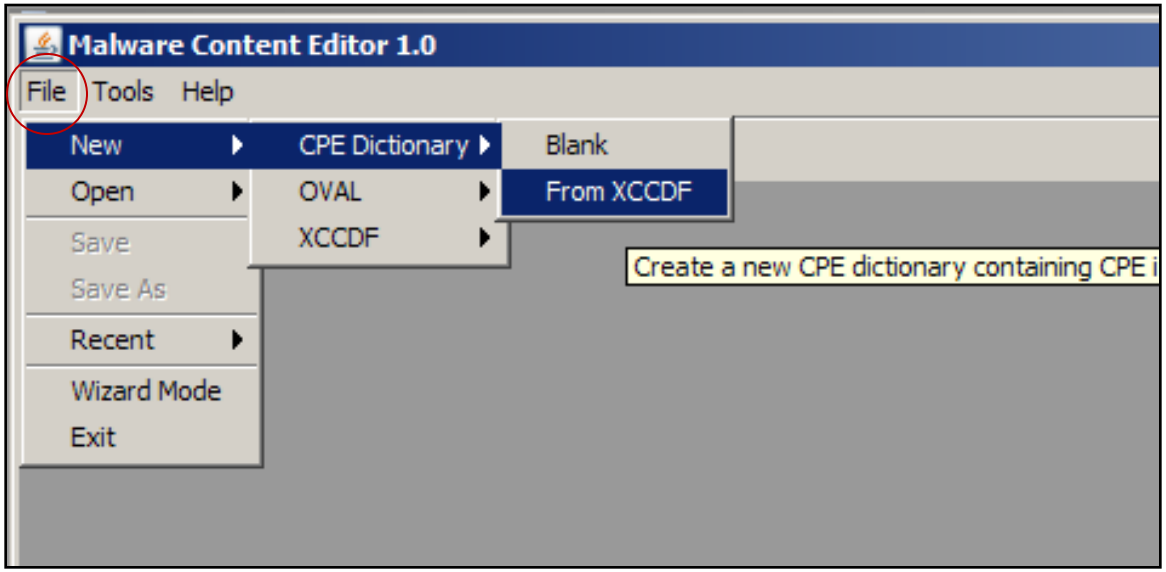


Create the FINAL XCCDF.xml from the FINAL OVAL.xml

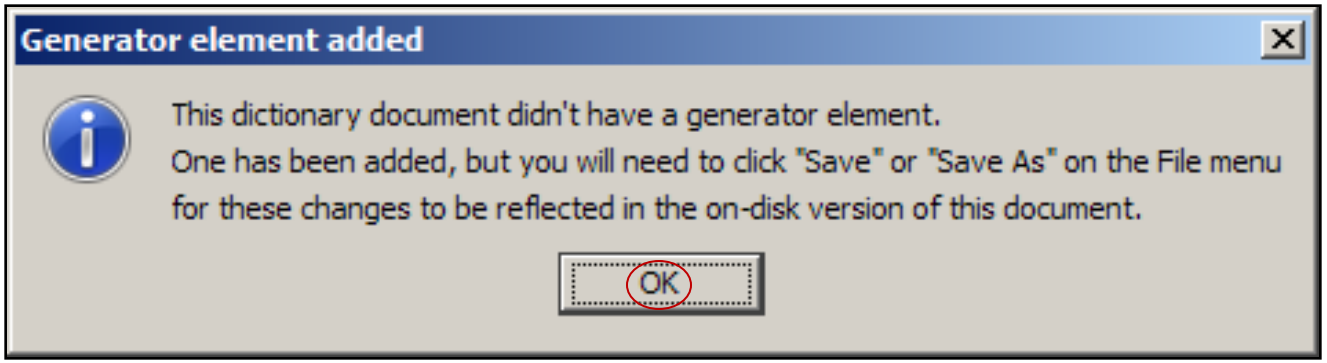


Create the additional SCAP data stream files from the FINAL-XCCDF.xml

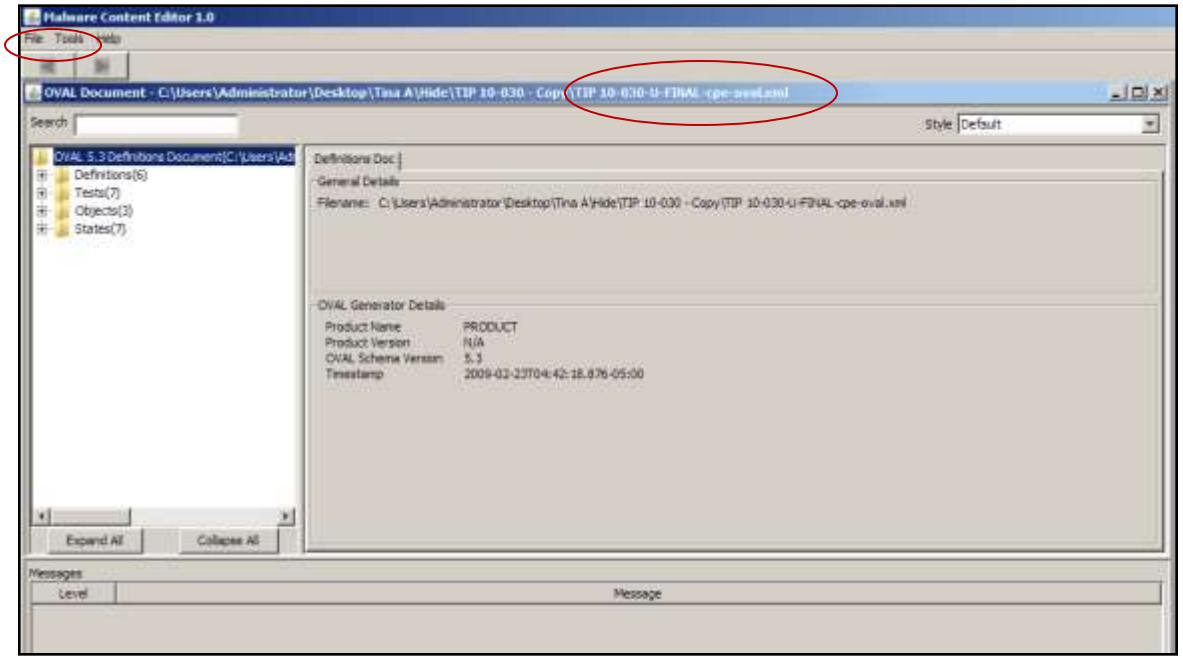
Create SCAP data stream files from the FINAL-XCCDF.xml



Create SCAP data stream files from the FINAL-XCCDF.xml

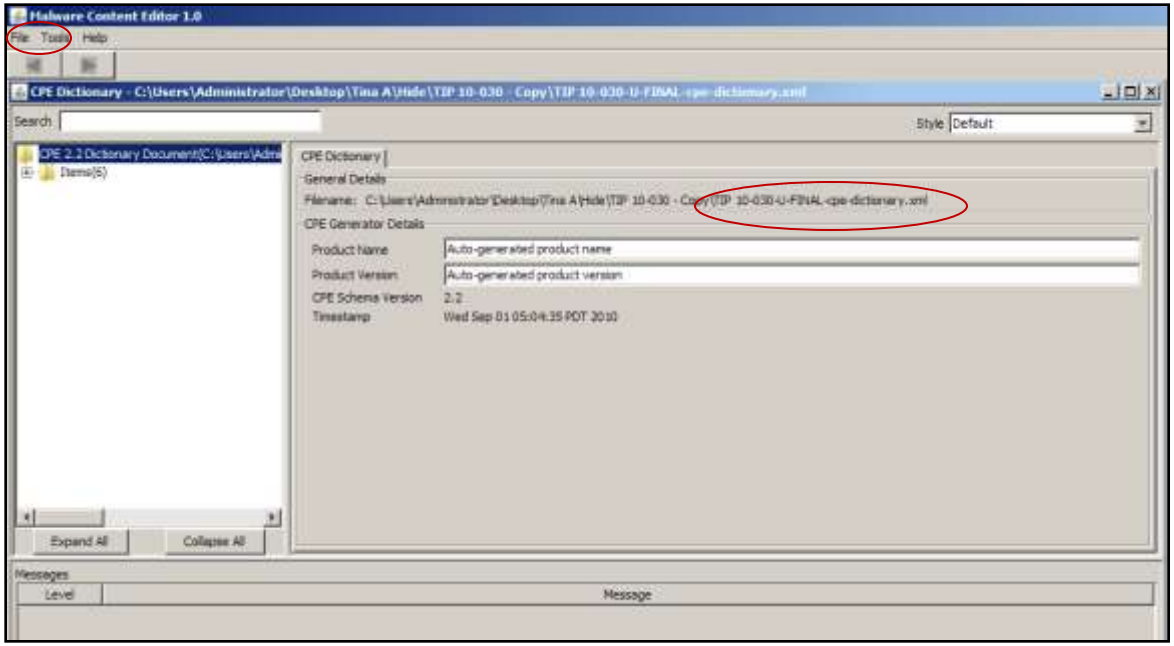


Create SCAP data stream files from the FINAL-XCCDF.xml



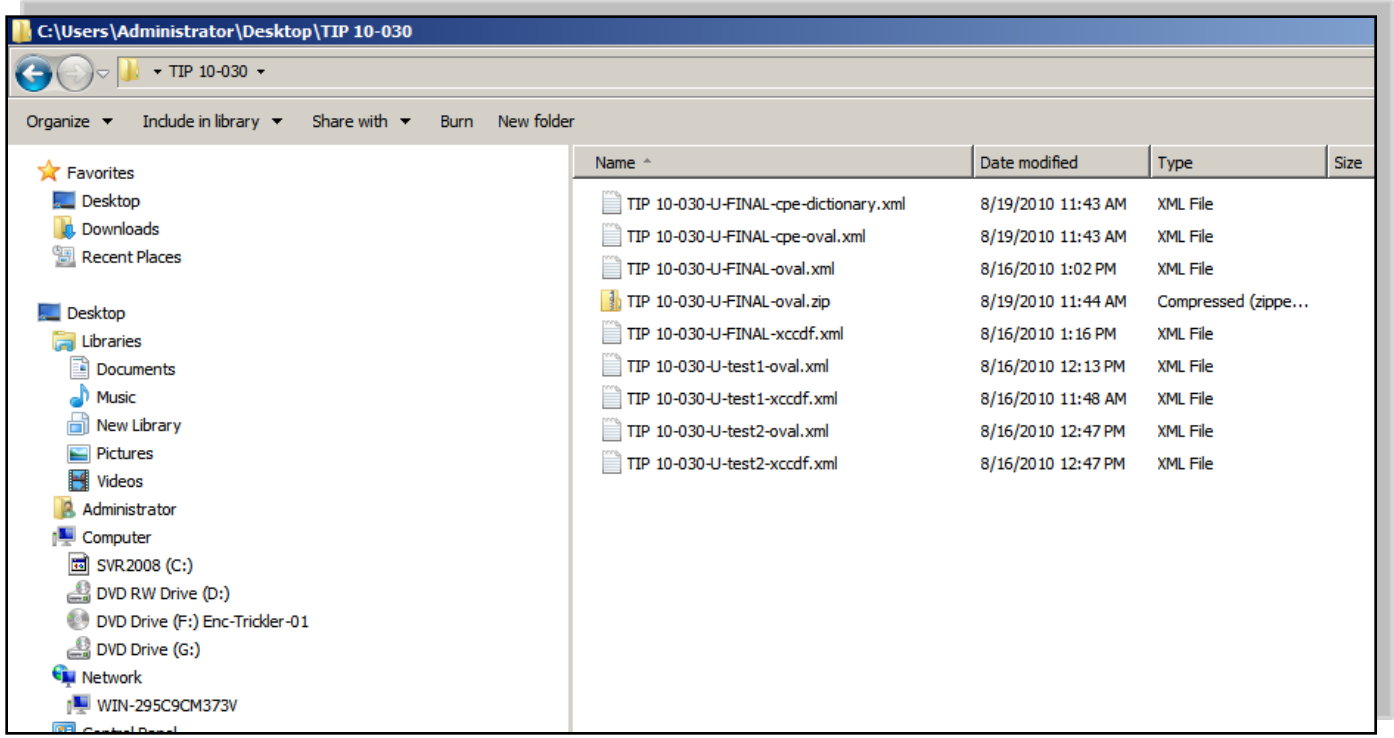
File > Save > Tools > Validate > Close xml

Create SCAP data stream files from the FINAL-XCCDF.xml



File > Save > Tools > Validate > Close xml

Create SCAP data stream files from the FINAL-XCCDF.xml



View Folder


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
CENTRAL SECURITY SERVICE
UNITED STATES OF AMERICA


IAD

?????'s

POC's

- **Tina Ackerman, DoD**
  410-854-0692

- **Mike Kinney, DoD**
  m.kinne@radium.ncsc.mil

- **Shane Shaffer, G2**
  shane.shaffer@g2-inc.com
  s.shaffe@radium.ncsc.mil

THE DECISIVE ADVANTAGE