CIS Benchmarks

Center for Internet Security Configuration Assessment Tool CIS-CAT

Users Guide

v3.0.43

October 24, 2017

Table of Contents

Overview

CIS-CAT is a configuration assessment software tool available to CIS members as a benefit of membership. Written in Java, CIS-CAT:

a) reads those CIS Benchmarks that are expressed in XCCDF (XML) format;
b) reports the configuration status of a target system as compared to the technical controls defined in those CIS Benchmarks; and
c) provides a comparative score based on a conformity scale of 0-100.

CIS-CAT can operate as a command line interface (CLI) or GUI tool. CIS-CAT will assess the configuration posture of the local system only. CIS-CAT cannot currently be used to "scan" a remote target or network.

System Requirements

CIS-CAT requires a Java Runtime Environment (JRE) in order to execute. The following JRE versions are currently supported in CIS-CAT:

- JRE 6 (also referred to as v1.6),
- JRE 7 (also referred to as v1.7).
- JRE 8 (also referred to as v1.8).

The tool and the JRE can reside on the target system of evaluation or on a removable or network drive, provided it is accessible from the target of evaluation. CIS-CAT will operate on Microsoft Windows XP and greater; Sun Solaris, IBM AIX, HP-UX, and Linux platforms provided the JRE is accessible to it. It is recommended that the latest JRE version for the given platform is used, and that 64-bit JREs are utilized on 64-bit systems, where applicable.

NOTE: **CIS-CAT must be executed as root, Administrator, or an equivalently privileged principal**.

CIS-CAT Support

If you have questions, comments, or are experiencing trouble using CIS-CAT, please email support@cisecurity.org. CIS has also established a community forum designed to foster collaboration around CIS-CAT. It is recommended that this resource be reviewed when troubleshooting CIS-CAT.

Supported Benchmarks

CIS-CAT reads:

a) 86 CIS Benchmarks currently available in XCCDF;
b) XCCDF configuration files distributed by NIST for Microsoft Win XP and Vista,
c) user-modified CIS Benchmark XCCDF files,
d) XCCDF configuration files distributed by DISA (Windows 2008 version 6, Windows XP version 6, Windows 2003 version 6, Windows Vista version 6 and Windows 7 version 1), and
e) USGCB content for Windows 7 version 1.1.X.0. .
f) USGCB Tier IV SCAP 1.2 content for
    a. Microsoft Internet Explorer 7
    b. Microsoft Internet Explorer 8
    c. Microsoft Windows 7 (32 and 64-bit)
    d. Microsoft Windows Vista
    e. Microsoft Windows XP Pro Service Pack 3
    f. Red Hat Enterprise Linux 5 (32 and 64-bit)

CIS currently distributes CIS-CAT with production support for the following benchmarks. The benchmarks which utilize the OVAL language are noted in *italics*. The "Auto-Assessment" column denotes those benchmarks discoverable via the "Automatic Benchmark Inventory and Assessment" process. Further information can be found for the Graphical User Interface and the Command-line User Interface.

Benchmark	OVAL?	Auto-Assess?
CIS Amazon Linux Benchmark v2.0.0	*Y*	Y
CIS Apache Tomcat 5.5-6.0 Benchmark v1.0.0	N	Y
CIS Apple OSX 10.5 Benchmark v1.1.0	N	Y
CIS Apple OSX 10.6 Benchmark v1.0.0	N	Y
CIS Apple OSX 10.8 Benchmark v1.3.0	N	Y
CIS Apple OSX 10.9 Benchmark v1.3.0	N	Y
CIS Apple OSX 10.10 Benchmark v1.2.0	N	Y
CIS Apple OSX 10.11 Benchmark v1.1.0	N	Y
CIS Apple OSX 10.12 Benchmark v1.0.0	N	Y
CIS CentOS Linux 6 Benchmark v2.0.2	*Y*	Y
CIS CentOS Linux 7 Benchmark v2.1.1	*Y*	Y
CIS Cisco Firewall (ASA) Benchmark v4.1.0	*Y*	*N*
CIS Cisco IOS 12 Benchmark v4.0.0	*Y*	*N*
CIS Cisco IOS 15 Benchmark v4.0.0	*Y*	*N*
CIS Debian Linux 3 Benchmark v1.0.0	N	Y
CIS Debian Linux 7 Benchmark v1.0.0	*Y*	Y
CIS Debian Linux 8 Benchmark v1.0.0	*Y*	Y
CIS Google Chrome Benchmark v1.2.0	*Y*	Y
CIS HP-UX 11i Benchmark v1.4.2	N	N
CIS IBM AIX 4.3-5.1 Benchmark v1.0.1	N	N
CIS IBM AIX 5.3-6.1 Benchmark v1.1.0	N	N
CIS IBM AIX 7.1 Benchmark v1.1.0	N	N
CIS Microsoft Internet Explorer 10 Benchmark v1.1.0	*Y*	Y
CIS Microsoft Internet Explorer 11 Benchmark v1.0.0	*Y*	Y
CIS Microsoft Internet Information Server 7/7.5 Benchmark v1.8.0	*Y*	Y

Benchmark	OVAL?	Auto-Assess?
CIS Microsoft Internet Information Server 8/8.5 Benchmark v1.5.0	*Y*	Y
CIS Microsoft Office 2013 Benchmark v1.1.0	*Y*	Y
CIS Microsoft Office 2016 Benchmark v1.1.0	*Y*	Y
CIS Microsoft Office – Access 2013 Benchmark v1.0.1	*Y*	Y
CIS Microsoft Office – Access 2016 Benchmark v1.0.1	*Y*	Y
CIS Microsoft Office – Excel 2013 Benchmark v1.0.1	*Y*	Y
CIS Microsoft Office – Excel 2016 Benchmark v1.0.1	*Y*	Y
CIS Microsoft Office – Outlook 2013 Benchmark v1.1.0	*Y*	Y
CIS Microsoft Office – Outlook 2016 Benchmark v1.1.0	*Y*	Y
CIS Microsoft Office – PowerPoint 2013 Benchmark v1.0.1	*Y*	Y
CIS Microsoft Office – PowerPoint 2016 Benchmark v1.0.1	*Y*	Y
CIS Microsoft Office – Word 2013 Benchmark v1.1.0	*Y*	Y
CIS Microsoft Office – Word 2016 Benchmark v1.1.0	*Y*	Y
CIS Microsoft SQL Server 2008 R2 Database Engine Benchmark v1.3.0	*Y*	Y
CIS Microsoft SQL Server 2012 Database Engine Benchmark v1.2.0	*Y*	Y
CIS Microsoft SQL Server 2014 Database Engine Benchmark v1.1.0	*Y*	Y
CIS Microsoft Windows 7 Benchmark v3.0.1	*Y*	Y
CIS Microsoft Windows 8 Benchmark v1.0.0	*Y*	Y
CIS Microsoft Windows 8.1 Benchmark v2.2.1	*Y*	Y
CIS Microsoft Windows 10 Enterprise Release 1607 Benchmark v1.2.0	*Y*	Y
CIS Microsoft Windows Server 2003 Benchmark v3.1.0	*Y*	Y
CIS Microsoft Windows Server 2008 Benchmark v3.0.1	*Y*	Y
CIS Microsoft Windows Server 2008 R2 Benchmark v3.0.1	*Y*	Y
CIS Microsoft Windows Server 2012 Benchmark v2.0.1	*Y*	Y
CIS Microsoft Windows Server 2012 R2 Benchmark v2.2.1	*Y*	Y
CIS Microsoft Windows Server 2016 Benchmark v1.0.0	*Y*	Y
CIS Microsoft Windows XP Benchmark v3.1.0	*Y*	Y
CIS MIT Kerberos 1.10 Benchmark v1.0.0	*Y*	Y
CIS Mozilla Firefox 3 Benchmark v1.0.0	N	N
CIS Mozilla Firefox 24 ESR Benchmark v1.0.0	*Y*	Y
CIS Mozilla Firefox 38 ESR Benchmark v1.0.0	*Y*	Y
CIS Oracle Database 9i-10g Benchmark v2.0.1	N	N
CIS Oracle Database 11g Benchmark v1.0.1	N	N
CIS Oracle Database 11g R2 Benchmark v2.2.0	*Y*	N
CIS Oracle Database 12c Benchmark v2.0.0	*Y*	N
CIS Oracle Linux 6 Benchmark v1.0.0	*Y*	*Y*
CIS Oracle Linux 7 Benchmark v2.0.0	*Y*	Y
CIS Oracle MySQL Community Server 5.6 Benchmark v1.0.0	*Y*	N
CIS Oracle MySQL Community Server 5.7 Benchmark v1.0.0	*Y*	N
CIS Oracle MySQL Enterprise Edition 5.6 Benchmark v1.0.0	*Y*	N
CIS Oracle MySQL Enterprise Edition 5.7 Benchmark v1.0.0	Y	N
CIS Oracle Solaris 2.5.1-9 Benchmark v1.3.0	N	N
CIS Oracle Solaris 10 Benchmark v5.2.0	N	Y
CIS Oracle Solaris 11 Benchmark v1.1.0	N	Y
CIS Oracle Solaris 11.1 Benchmark v1.0.0	N	Y

Benchmark	OVAL?	Auto-Assess?
CIS Oracle Solaris 11.2 Benchmark v1.1.0	N	Y
CIS Red Hat Enterprise Linux 4 Benchmark v1.0.5	N	Y
CIS Red Hat Enterprise Linux 5 Benchmark v2.2.0	*Y*	Y
CIS Red Hat Enterprise Linux 6 Benchmark v2.0.2	*Y*	Y
CIS Red Hat Enterprise Linux 7 Benchmark v2.1.1	*Y*	Y
CIS Slackware Linux 10.2 Benchmark v1.1.0	N	N
CIS SUSE Linux Enterprise Server 9 Benchmark v1.0.0	N	Y
CIS SUSE Linux Enterprise Server 10 Benchmark v2.0.0	N	Y
CIS SUSE Linux Enterprise Server 11 Benchmark v2.0.0	Y	Y
CIS SUSE Linux Enterprise Server 12 Benchmark v2.0.0	Y	Y
CIS Ubuntu 12.04 LTS Server Benchmark v1.1.0	N	Y
CIS Ubuntu Linux 14.04 LTS Benchmark v2.0.0	*Y*	*Y*
CIS Ubuntu Linux 16.04 LTS Benchmark v1.0.0	*Y*	*Y*
CIS VMware ESX 3.5 Benchmark v1.2.0	N	N
CIS VMware ESX 4.1 Benchmark v1.0.0	N	N
CIS VMware ESXi 5.5 Benchmark v1.2.0	*Y*	Y

Vulnerability Assessments

CIS-CAT contains the capability to perform an assessment against vulnerability definitions constructed with the OVAL checking language against the following platforms:

- Microsoft Windows XP,
- Microsoft Windows 7,
- Microsoft Windows 8,
- Microsoft Windows 8.1,
- Microsoft Windows 10,
- Microsoft Windows Server 2003,
- Microsoft Windows Server 2008,
- Microsoft Windows Server 2008 R2,
- Microsoft Windows Server 2012,
- Microsoft Windows Server 2012 R2,
- Microsoft Windows Server 2016,
- Red Hat Enterprise Linux 4,
- Red Hat Enterprise Linux 5,
- Red Hat Enterprise Linux 6,
- Red Hat Enterprise Linux 7,
- SUSE Linux Enterprise Server 9,
- SUSE Linux Enterprise Server 10,
- SUSE Linux Enterprise Server 11, and
- SUSE Linux Enterprise Server 12

See Executing a Vulnerability Assessment (GUI) or Executing a Vulnerability Assessment (Command-Line) to learn more about executing a Vulnerability Assessment with CIS-CAT.

Obtaining CIS-CAT

CIS-CAT is distributed exclusively from the CIS member web site, https://community.cisecurity.org. CIS-CAT documentation, XCCDF benchmarks, supplemental scripts, and the scoring tool are contained in a single bundle. The structure of this bundle is detailed below:

Location	Description
/benchmarks	Contains all XCCDF Benchmarks
/custom/brand	Placeholder for member-created CSS and graphics for customized branding of HTML Reports generated by CIS-CAT.
/docs	Contains User Documentation
/misc	Contains XSDs and supplemental batch files
/misc/Windows/cis-cat-centralized.bat	A batch file that wraps CIS-CAT.jar to simplify evaluating Windows targets which lack a local instance of the JRE and CIS-CAT.
/misc/Unix-Linux/cis-cat-centralized.sh	A shell script that wraps CIS-CAT.jar to simplify evaluating Unix/Linux targets which lack a local instance of a JRE and CIS-CAT.
/lib	Contains Libraries used by CIS-CAT. A number of library executables are contained in this folder. See the "Library Functions" section of this document for more information.
/third-party-content/org.mitre.oval **/third-party-content/com.redhat.rhsa** **/third-party-content/com.novell.support**	When obtained via the `Options --> Update Vulnerability Definitions` menu, these folders contain OVAL-based vulnerability definitions files for various platforms supported by CIS-CAT.
CISCAT.jar	The CIS-CAT Java Archive
CIS-CAT.sh	A UNIX/Linux Wrapper for CIS-CAT.jar. Useful for CLI mode.

Installing CIS-CAT

To install CIS-CAT, simply unzip the archive. No further action is required provided JRE v1.6.0+ is installed on the system. If the JRE is available on removable media or via a network share, perform the following steps to get CIS-CAT running:

1. Insert or mount the removable media or network drive. For demonstration purposes, we will assume the JRE is accessible via `/mnt/jre` on Linux/Unix platforms and `\\server\jre` on Windows platforms.

2. Map the `JAVA_HOME` environment variable to the location noted above. From a command prompt or shell, execute the following to create this mapping:

```
Windows> set JAVA_HOME=\\server\jre
Unix> export JAVA_HOME=/mnt/jre
```

Once the above is complete, CIS-CAT is ready to go. To run CIS-CAT execute the following:

```
Windows> CIS-CAT.bat
Unix> ./CIS-CAT.sh
```

Note: the first time CIS-CAT is run on a Unix machine the shell script might need to be granted execute permissions. To do this run the following command:

```
chmod +x CIS-CAT.sh
```

Using CIS-CAT within a Graphical User Interface (GUI)

To execute CIS-CAT in a GUI environment, simply double click on `CIS-CAT.jar`.

Note: If the system has an archive manager associated with `.jar` files, you will need to double click on `CIS-CAT.sh` for Unix and Linux systems or `CIS-CAT.bat` for Windows systems. This will cause the following dialog to appear:

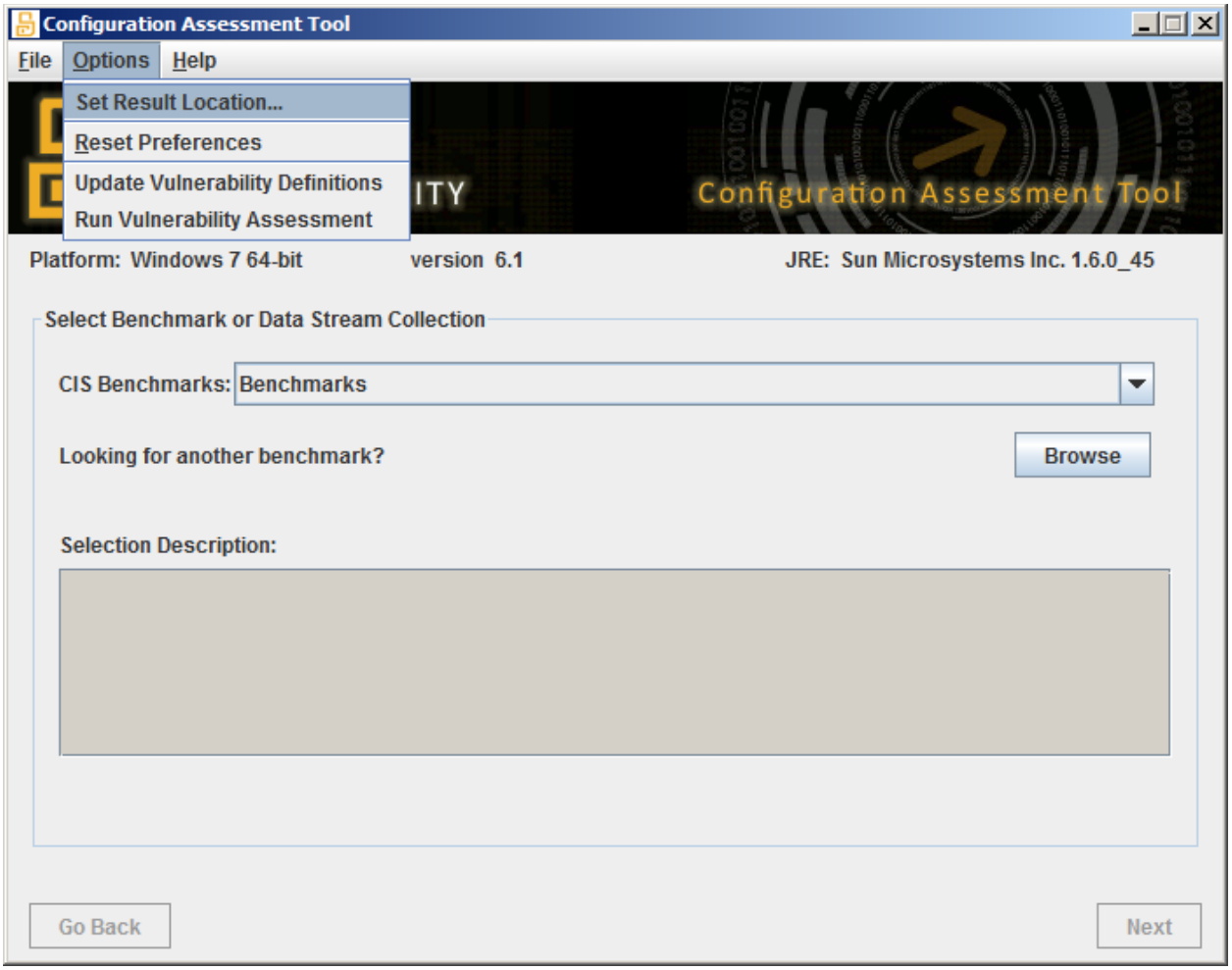
Configuring Result Location

Before evaluating a system against a CIS benchmark, it is recommended that the Result Location be specified. The default location for results is articulated below:

Platform	Location
Windows	`%HOMEDRIVE%%HOMEPATH%\My Documents\CIS-CAT Results`
Unix/Linux	`$HOME/CIS-CAT_Results`

Note: if the default location is used each assessment report(s) will be placed in a new time stamped directory under the default location.

To change the report location, click `Options -> Set Result Location` and browse to the desired directory, as seen below:



On Windows, this preference is preserved in the registry at the following location:

Component	Value
Hive	HKEY_CURRENT_USER
Key	`Software\JavaSoft\Prefs\org\cisecurity\tools\ciscat`
Value (REG_SZ)	`result-location`

On Unix/Linux platforms, this preference is persisted on the file system at:

`$HOME/.java/.userPrefs/org/cisecurity/tools/ciscat/prefs.xml`

Note: The acceptance of the CIS-CAT Terms of Use agreement is also persisted in the above locations. On Windows, the registry key Value name is `terms-of-use-accepted`.

Choosing a Benchmark and Profile

CIS-CAT has the ability to assess multiple benchmarks. Each individual benchmark and profile must be configured and added to the assessment queue. To select a benchmark, either select a CIS benchmark from the drop down or click on the `Browse` button, as seen below:

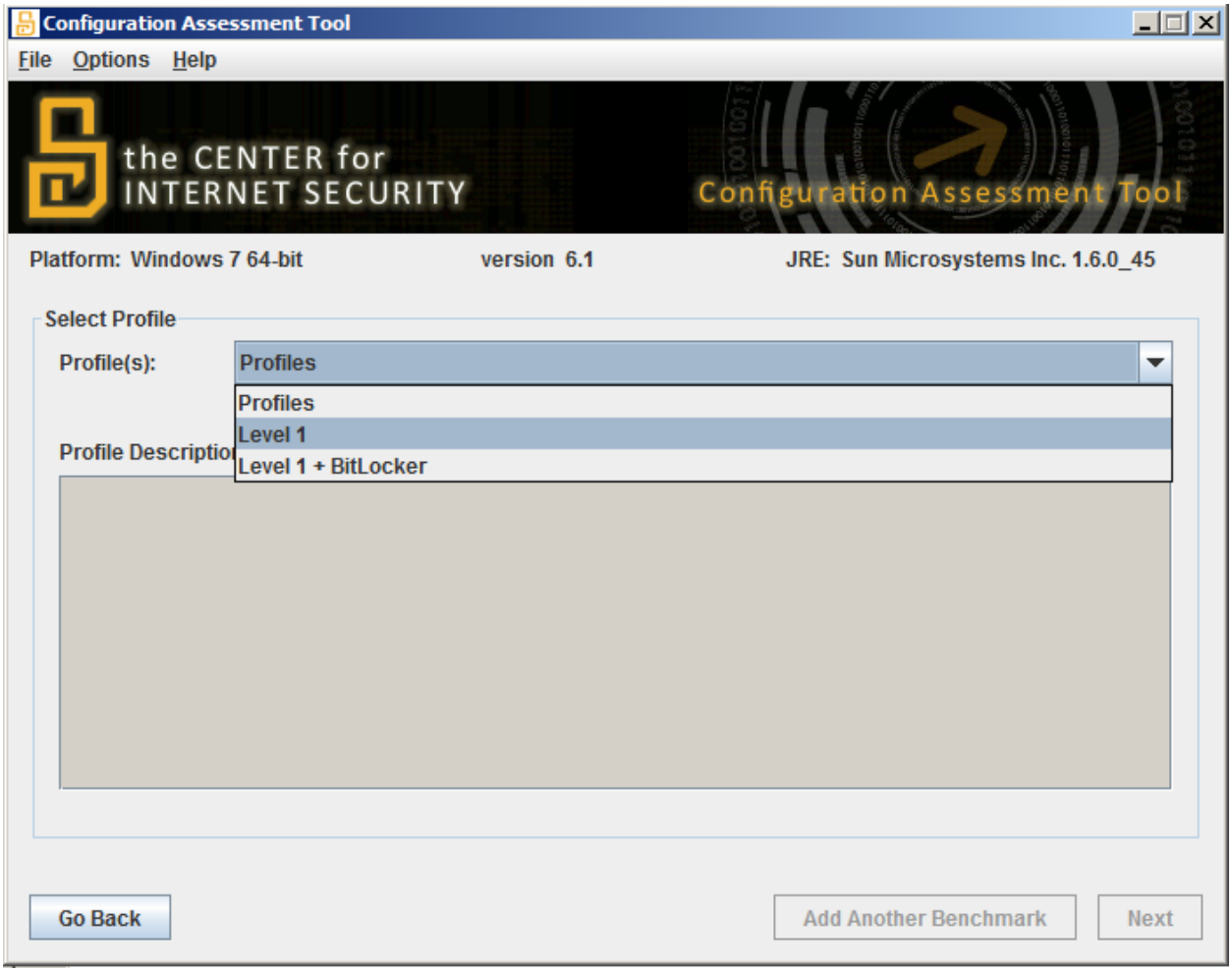
Once a benchmark is loaded, click `Next`. CIS-CAT will then determine whether the selected CIS Benchmark contains a data stream collection. If a data stream collection is discovered, the list of available data streams and checklists will be displayed:

Once a data stream is selected, the user may select either a checklist, representing the XCCDF component of the data stream, or any OVAL-based set of definitions contained within the data stream.

Loading a selected checklist first triggers the platform validation process. This process attempts to ensure that CIS-CAT is assessing against the appropriate software or operating system platform, such as attempting to assess the Windows 7 benchmark on a Windows XP machine. If CIS-CAT determines the platform is invalid for the selected benchmark, an error message is displayed.

If the user receives this message, the `Next` button will not be enabled and the user will not be allowed to continue until a valid checklist is selected. Once platform validation has succeeded, click `Next` to display the Profile selection screen.

A list of available profiles will be provided in the drop down menu. When a profile is selected, that profile's description will be displayed as seen below:



Profiles represent a logical grouping of benchmark recommendations. Profiles are commonly used to distinguish between Level-I and Level-II scoring recommendations, or target role, such as domain controllers or member servers.

Adding Multiple Benchmarks

Once a profile has been selected, users have the option of continuing to the report output options, via the "`Next`" button, or adding another benchmark to the assessment process, via the "`Add Another Benchmark`" button.

When a user clicks the "`Add Another Benchmark`" button, the currently selected benchmark and profile are added to the assessment queue, and the user is returned to the benchmark selection screen. A user can add as many benchmarks as are desired. Once all benchmarks and profiles have been selected and queued, click the "`Next`" button.

A number of different screens are possible to display:

- The "interactive parameters" screen enables users to enter information specific to the current assessment being performed, such as database connection information, or any other non-automatable values required from the user.
- The "SSH connection configuration" screen allows users to enter a hostname, user, password or private key information in order to establish SSH connections, when required.
- The "report generation option" screen allows users to select the reports to be generated following the assessment process.

Interactive Parameters

When the benchmark and profile to be assessed require interactive user parameters to be entered, such as database connection information, or Oracle Home directories, or Tomcat configuration values, the "interactive parameters" screen is presented to the user, allowing for the entry of those parameters:

Once all interactive parameters have been entered, click the "Next" button to continue.

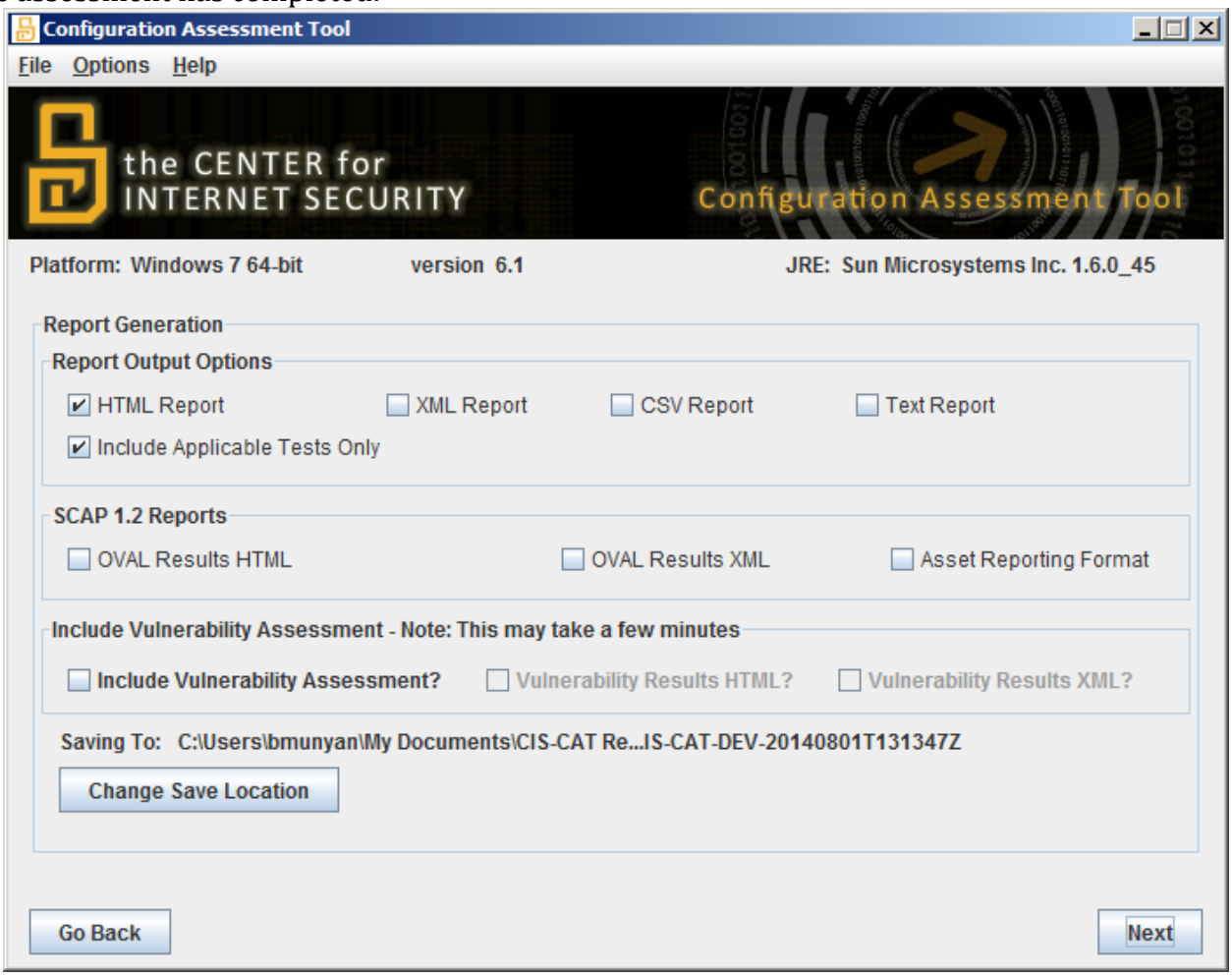
SSH Connection Parameters

When CIS-CAT recognizes a test or set of tests to be evaluated which require a SSH connection to be made, the user is presented with either a GUI screen or CLI prompts in order to enter the appropriate SSH configurations, such as the host and port, along with a username and credentials (or path to a private key file).

When performing assessments against Cisco devices, the user is also able to enter their "enable" credentials in order to execute privileged commands. Similar to database benchmark assessments, the "Test Connection" button is available for users to verify host and credential information. Once the appropriate SSH connection information has been entered, click the "Next" to continue.

Report Generation Options

Once you have selected the benchmark(s) and profile(s) to evaluate, along with any interactive parameters and/or SSH connection information, click `Next` to select the reports to be generated once assessment has completed:



By default an HTML report will be generated. The HTML report is the most "user friendly" view of the assessment results, containing prose content such as recommendation description, rationale, audit and remediation, as well as test results and evidence indicating to users the expected configuration state and actual state collected by CIS-CAT.

The other report formats available are:

Report Output Option	Description
XML Report	The XML report contains the raw XML data used in the assessment as well as the result information in its appropriate XML format.
Text Report	The Text report contains basic plain-text information, presenting the title of each rule evaluated and its evaluation result (Pass, Fail, Error, etc)
CSV Report	The CSV report contains basic report evaluation information in a comma-separated value format, which may be opened as an Excel worksheet.
OVAL Results HTML	When a data stream collection utilizes the OVAL checking language, OVAL Results may be generated. * SCAP 1.2 Data Stream Collections Only
OVAL Results XML	When a data stream collection utilizes the OVAL checking language, OVAL

	Results may be generated. These OVAL results conform to the specifications outlined in the OVAL Results XML schema. * SCAP 1.2 Data Stream Collections Only
Asset Reporting Format	The Asset Reporting Format represents an XML model expressing the relationships between the target systems being assessed and the reports generated for that target system. More information about ARF can be found here. * SCAP 1.2 Data Stream Collections Only

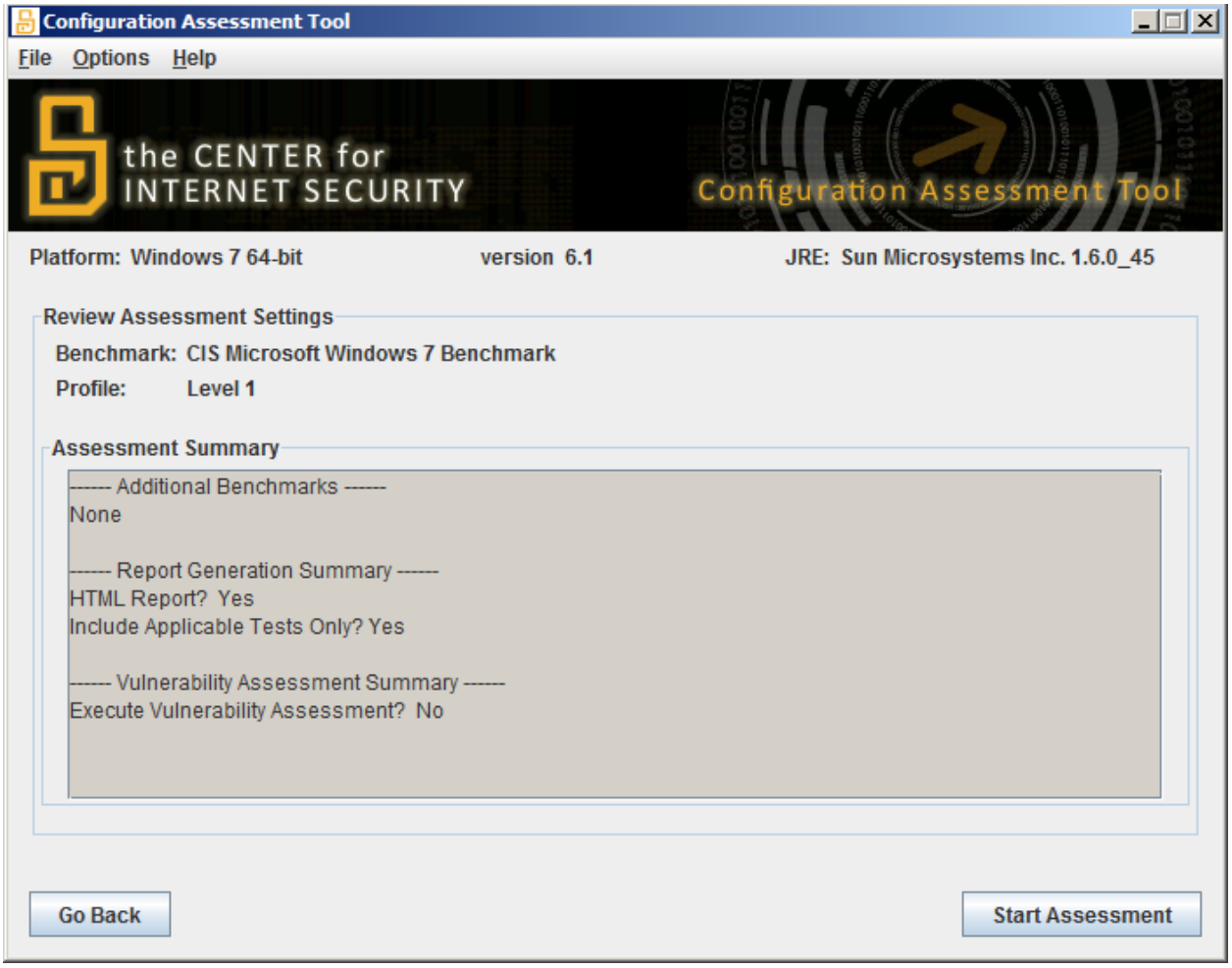
The `Include Applicable Tests Only` option when checked will only output selected tests for HTML and Text reports. If desired un-checking the `Include Applicable Tests Only` option all tests including `not selected` tests will be included in the reports. Note, for the XML report all tests will always be included. It is also possible to change the report save location if desired. Once the options are set click on `Generate Report(s)` and once the report(s) are generated you can then click on `View Report(s)`. If multiple reports were generated then the folder the reports were saved to will be opened. If only one report was generated then on Windows, this will launch your system's default program for HTML, text or xml files. On UNIX/Linux systems, CIS-CAT will try to find a browser to open up the given report. For details on how to interpret these reports, see the Interpreting Evaluation Results section.

If a vulnerability assessment is to be included with the benchmark assessment, check the `Include Vulnerability Assessment` checkbox, as well as one or both checkboxes indicating the vulnerability results reports to be generated.

NOTE:
If you plan to use the *CIS-CAT Dashboard*, you **must** export assessment results in XML format by selecting the `XML Report` checkbox.

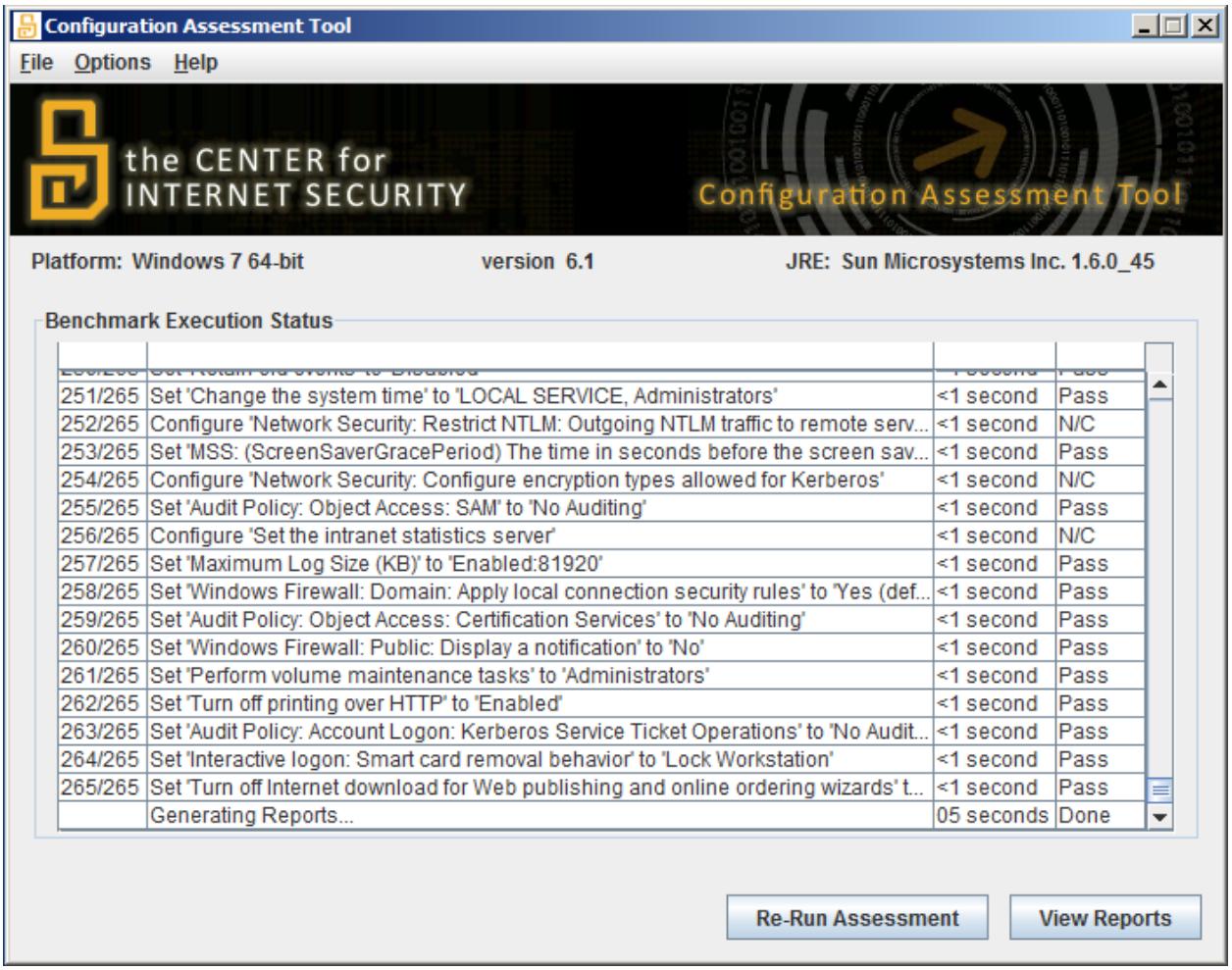
Evaluating a Benchmark

Once report generation options have been selected, click `Next` to review the assessment summary:



If all assessment settings are correct click the `Start Assessment` button.

CIS-CAT will then display the benchmark execution status screen like the one shown below:

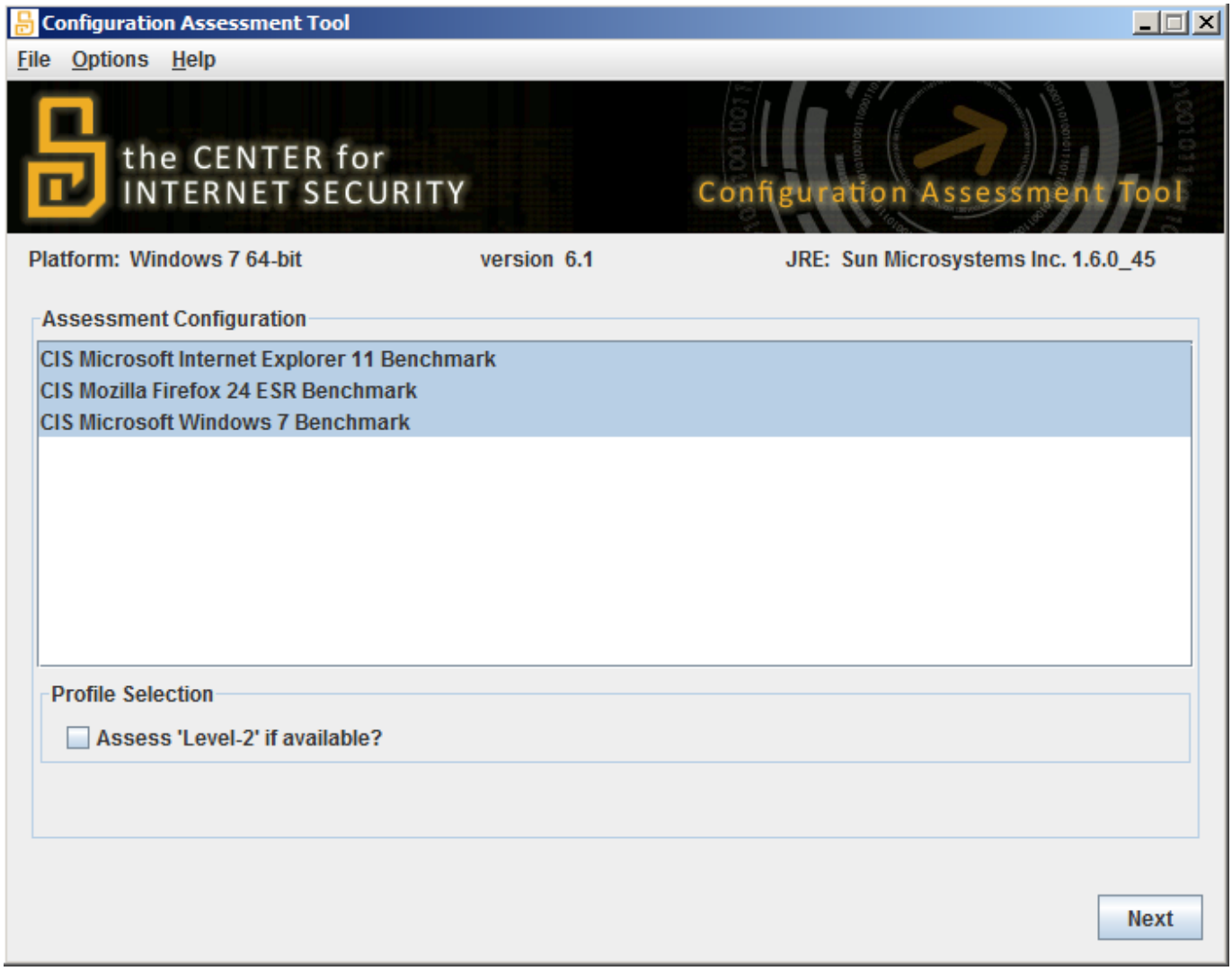


Once the benchmark evaluation is complete, if the user included a vulnerability assessment, the progress bar will indicate its status. Following the completion of all assessments, the `View Reports` button and `Re-Run Assessment` button will be enabled allowing the user to view the generated reports, or re-execute the entire selected assessment again, respectively.

Automatic Benchmark Inventory & Assessment

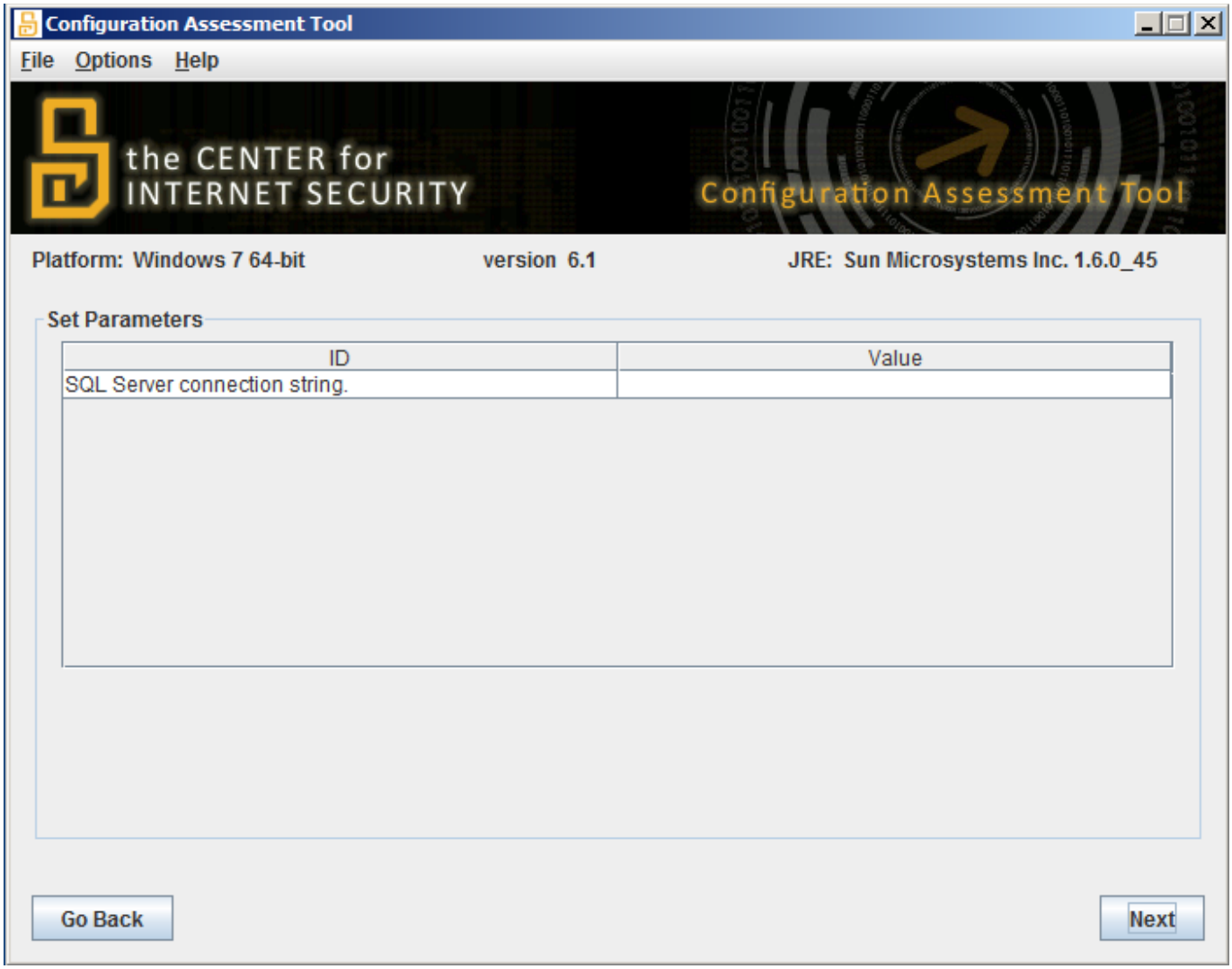
CIS-CAT's capabilities include the ability to automatically inventory which CIS benchmarks are applicable to a target system, and perform the assessment of each discovered benchmark. To initiate the inventory process, execute the CIS-CAT GUI and select the `Options -> Automatic Benchmark Inventory & Assessment` menu item.

When this menu item is selected, CIS-CAT will perform the benchmark inventory process and display the discovered benchmarks:

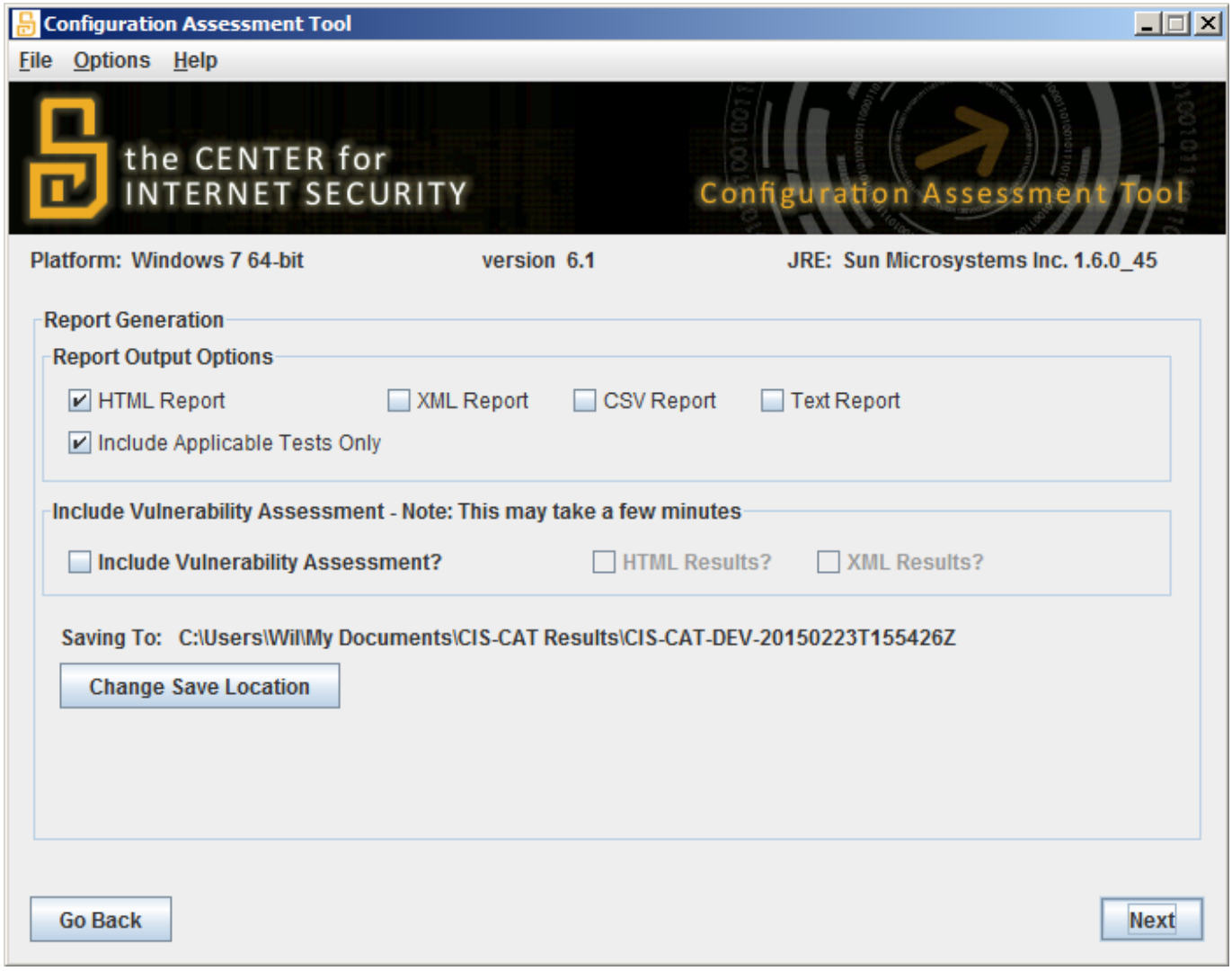


By default, all discovered benchmarks are selected for assessment, but a user can select or de-select any benchmarks. The "`Assess 'Level-2' if available`" checkbox allows users to assess any "defense in depth" profiles for the selected benchmarks, if a profile of that type is defined in the benchmark.

Once inventoried benchmarks have been selected, click "`Next`". If any interactive parameters are required by the benchmarks, such as JDBC connection strings, the interactive parameters screen will be displayed:



Once parameters have been entered, click "`Next`" to select report output options:



The report output options screen allows users to select which report formats will be generated for EACH benchmark that was inventoried. If five benchmarks were discovered and selected for assessment, five sets of output reports will be generated in the reports' "`Saving To`" location. As with a standard benchmark assessment, if a vulnerability assessment is applicable, users may select to include the vulnerability assessment along with all inventoried benchmark assessments.

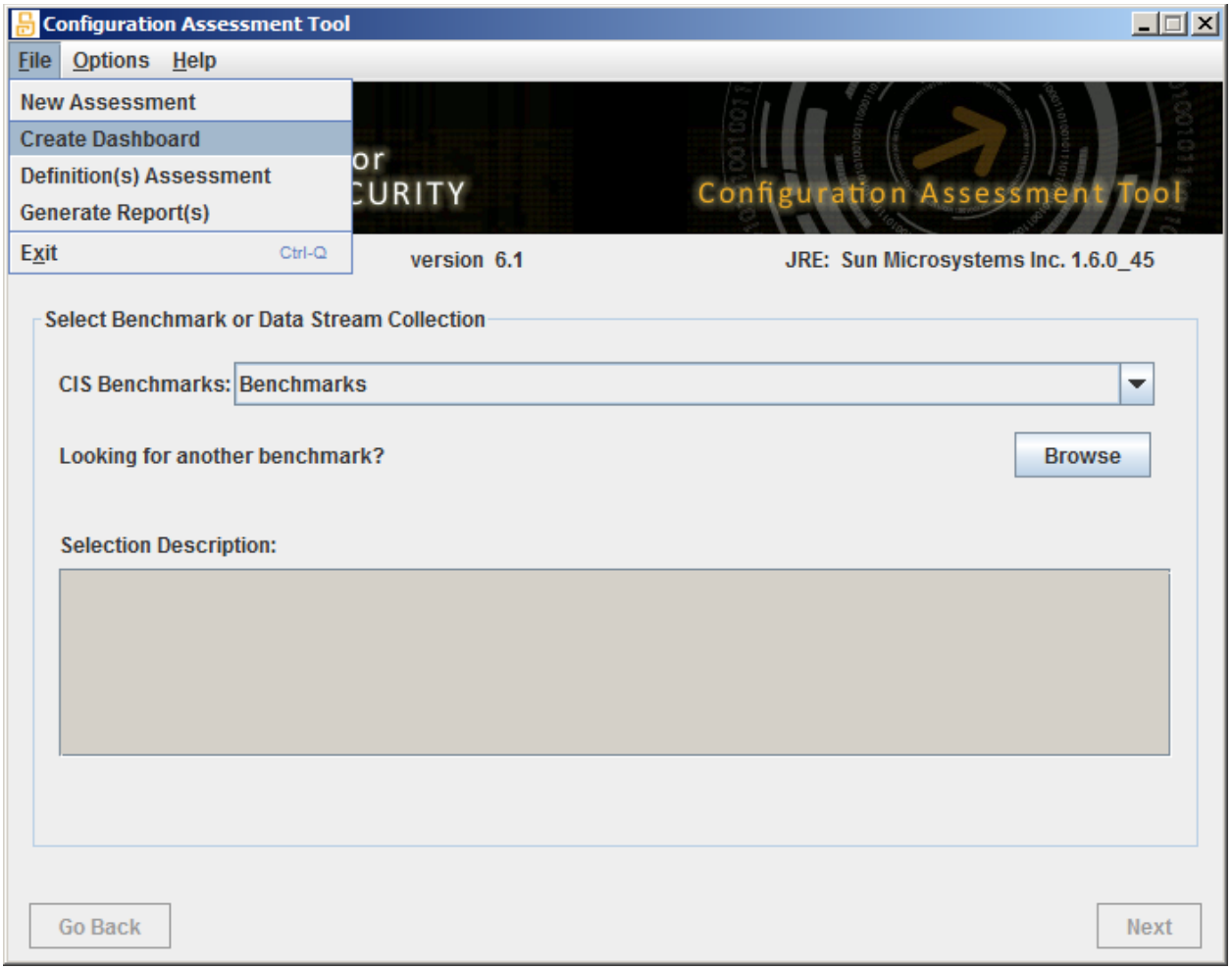
Clicking the "`Next`" button allows the user to review the inventoried benchmarks prior to executing the assessment(s):

Finally, the user can click the "`Start Assessment`" button to execute the selected benchmark assessments and generate applicable result reports.

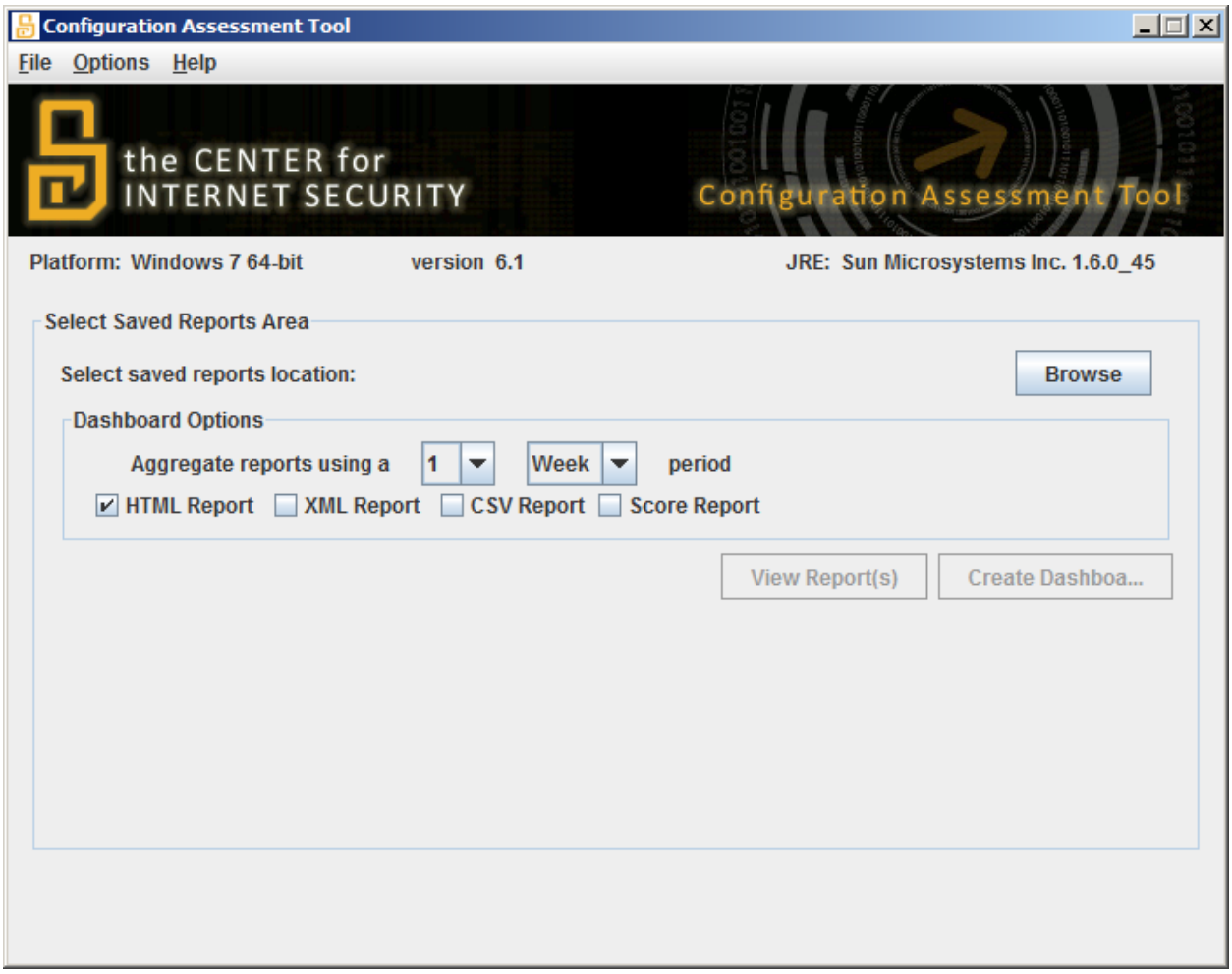
Creating a CIS-CAT Dashboard

CIS-CAT's dashboard feature consumes multiple instances of CIS-CAT XML result files and summarizes them into a single XML file. The primary goal of this feature is to provide the ability to trend configuration status over time on a per-benchmark, or device basis from different devices/computers.

To get started, move all of the CIS-CAT XML result files to be summarized into a single directory. Next, run CIS-CAT and select the `File -> Create Dashboard` menu option as shown below:

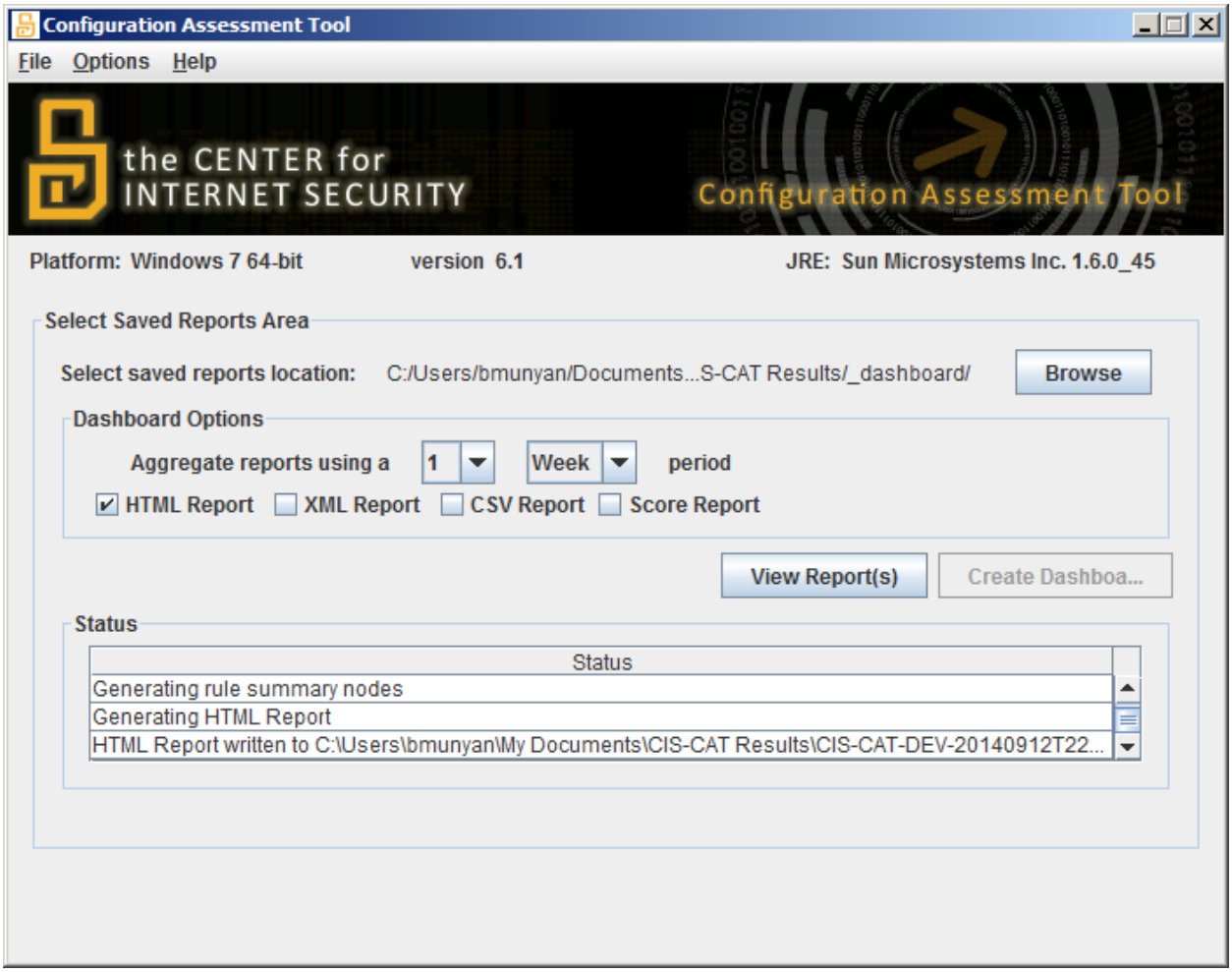

Configuration Assessment Tool
File
Options
Help
New Assessment
Create Dashboard
Definition(s) Assessment
Generate Report(s)
Exit
Ctrl-Q
Configuration Assessment Tool
version 6.1
JRE: Sun Microsystems Inc. 1.6.0_45
Select Benchmark or Data Stream Collection
CIS Benchmarks:
Benchmarks
Looking for another benchmark?
Browse
Selection Description:
Go Back
Next

Next, select the directory that contains the CIS-CAT XML results that need to be summarized.



Next, provide CIS-CAT with an aggregation period. By default, CIS-CAT will report aggregate configuration results on a weekly basis. This configuration will cause CIS-CAT to summarize all reports that occur within the same calendar week. Similarly, if the aggregation period is set to 1 month, CIS-CAT will summarize all reports that occur in the same calendar month.

Next, click `Create Dashboard` to start the aggregation process. Once the aggregation is complete, the last line in the status window will tell you the location of the aggregation file.



Configuring Dashboard Report Groups

The CIS-CAT dashboard can be configured to enable selection of hierarchical and time-trend reports for various groups. A group could be defined as a technical or management resource accountable for a set of devices, a set of benchmarks, etc. These groups may only be configured in the CIS-CAT properties file (a default "`ciscat.properties`" file is contained in the "`misc`" folder of a typical CIS-CAT installation) and must begin with the prefix "`dashboard.group`".

The following options may be included in a dashboard group:

Option	Description
name	The "name" attribute is translated into the group label when displayed in the dashboard HTML
ip	A value or regular expression identifying the set of IP addresses for devices included in the group
device	A value or regular expression identifying the set of device names included in the group
benchmark	A value or regular expression identifying the title of a benchmark or set of benchmarks included in the group
[the identifier of another group]	The property name (beginning with "dashboard.group") of a sub-group to be compiled and included in this group.

Any number of options may be included in a dashboard group, each option separated by a pipe character "|", and options are additive, meaning a group with multiple options will include assessment information for all matching items, not the intersection of items matching each option.

An example properties file, defining three dashboard report groups might look as follows:

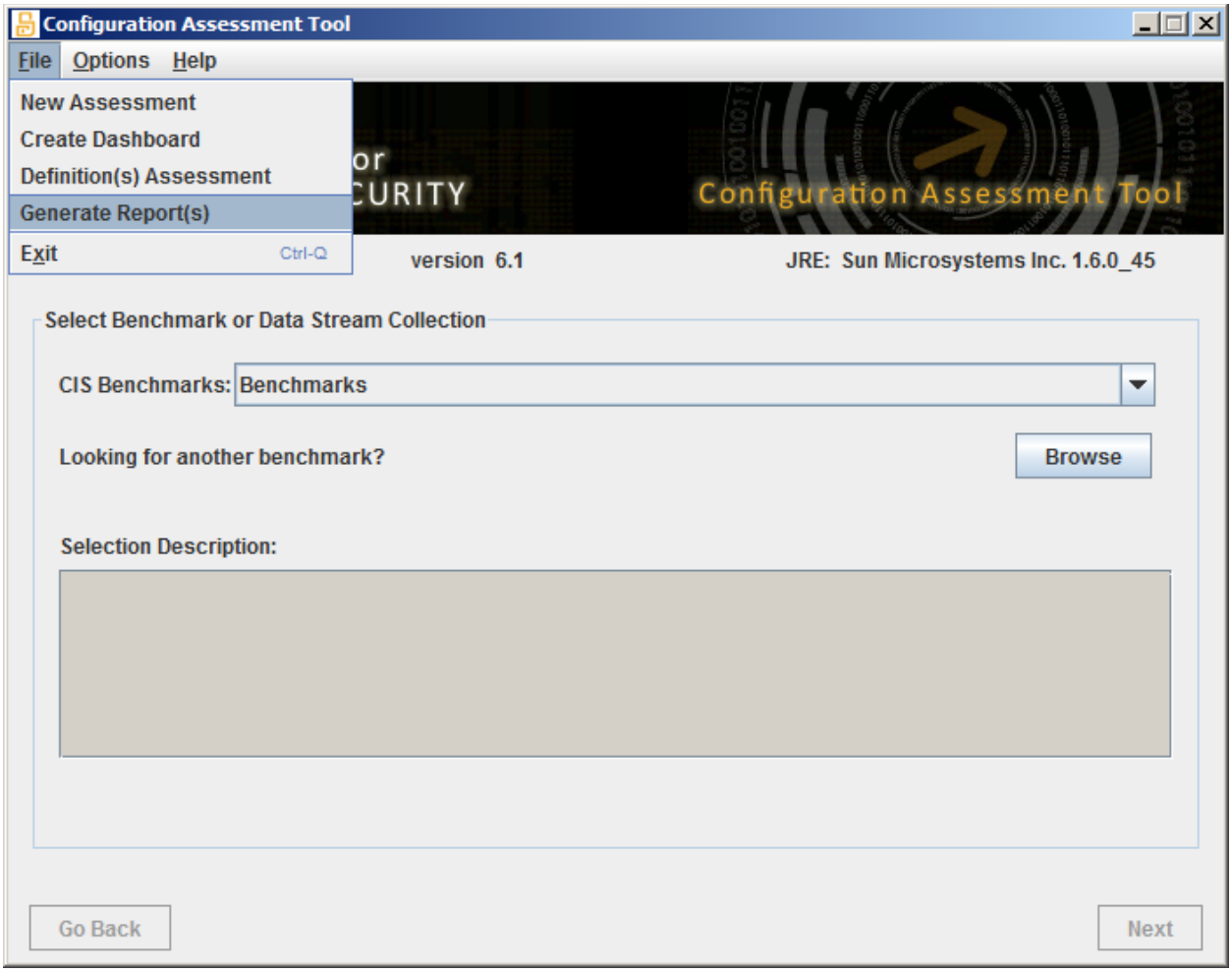
```
# Dashboard Group Specification...
dashboard.group.first=name:John Doe|ip:192.168.41.58
dashboard.group.second=name:Development Machines|device:^DEV.*
dashboard.group.third=name:All Windows Benchmarks|benchmark:^.*Windows.*$
```

The first entry defines a group collecting all reports generated from a specific IP Address.
The second entry defines a group collecting all reports from machines with a device name beginning with "DEV".
The third entry defines a group collecting all reports from machines which assessed a Windows benchmark.

Ad-Hoc Report Generation

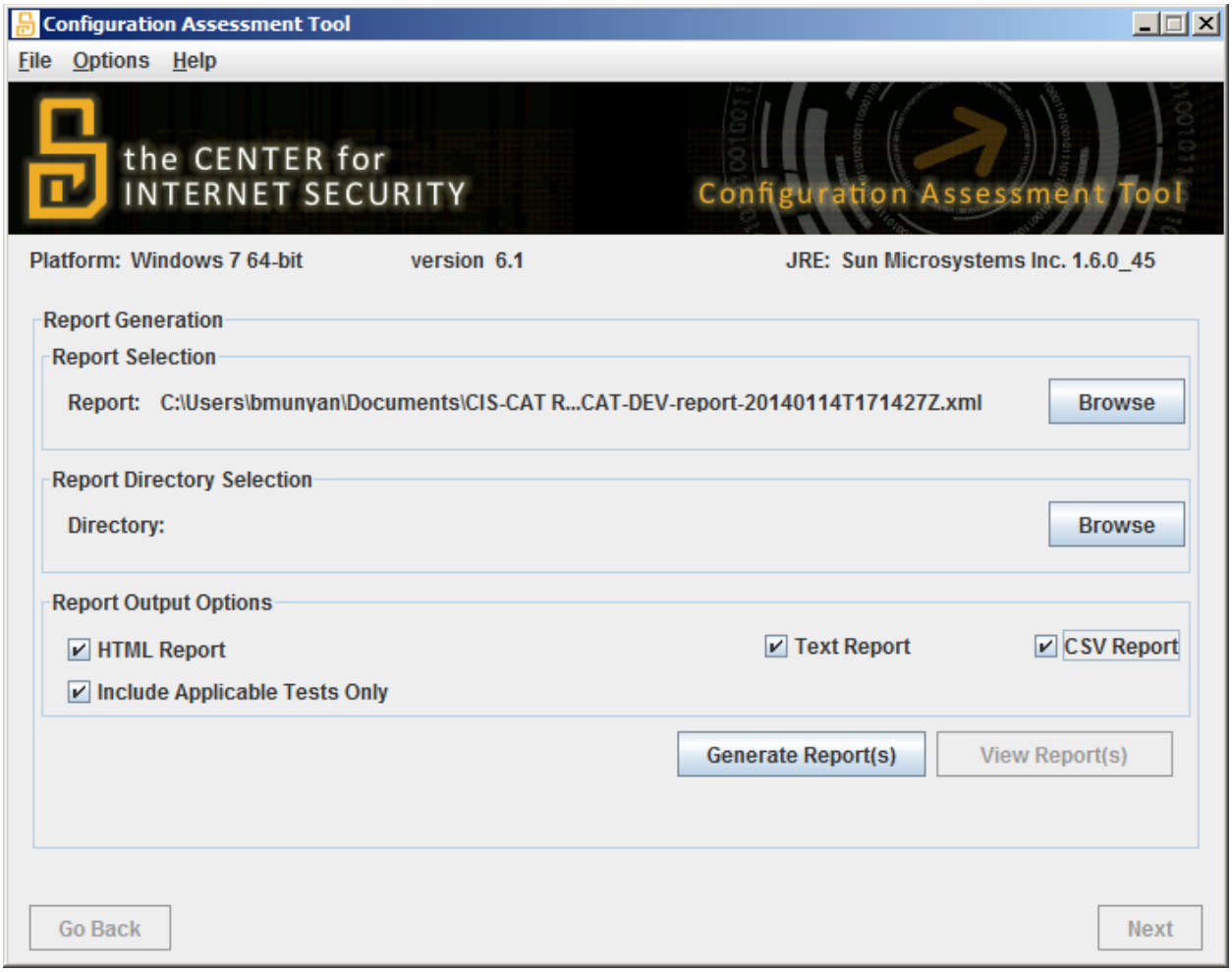
CIS-CAT can also be used to re-generate various reports using existing XML results. If a previous execution of CIS-CAT has generated an XML report, a user can, at a later time, use CIS-CAT to create the HTML, CSV, and/or Text reports using the ad-hoc report generation functionality.

From the CIS-CAT GUI, select the `File -> Generate Report(s)` menu option:



Once opened, the user has the option to either select a single XML report for generation, or select a directory from which all XML reports will be processed, generating the selected report types for each discovered XML report.

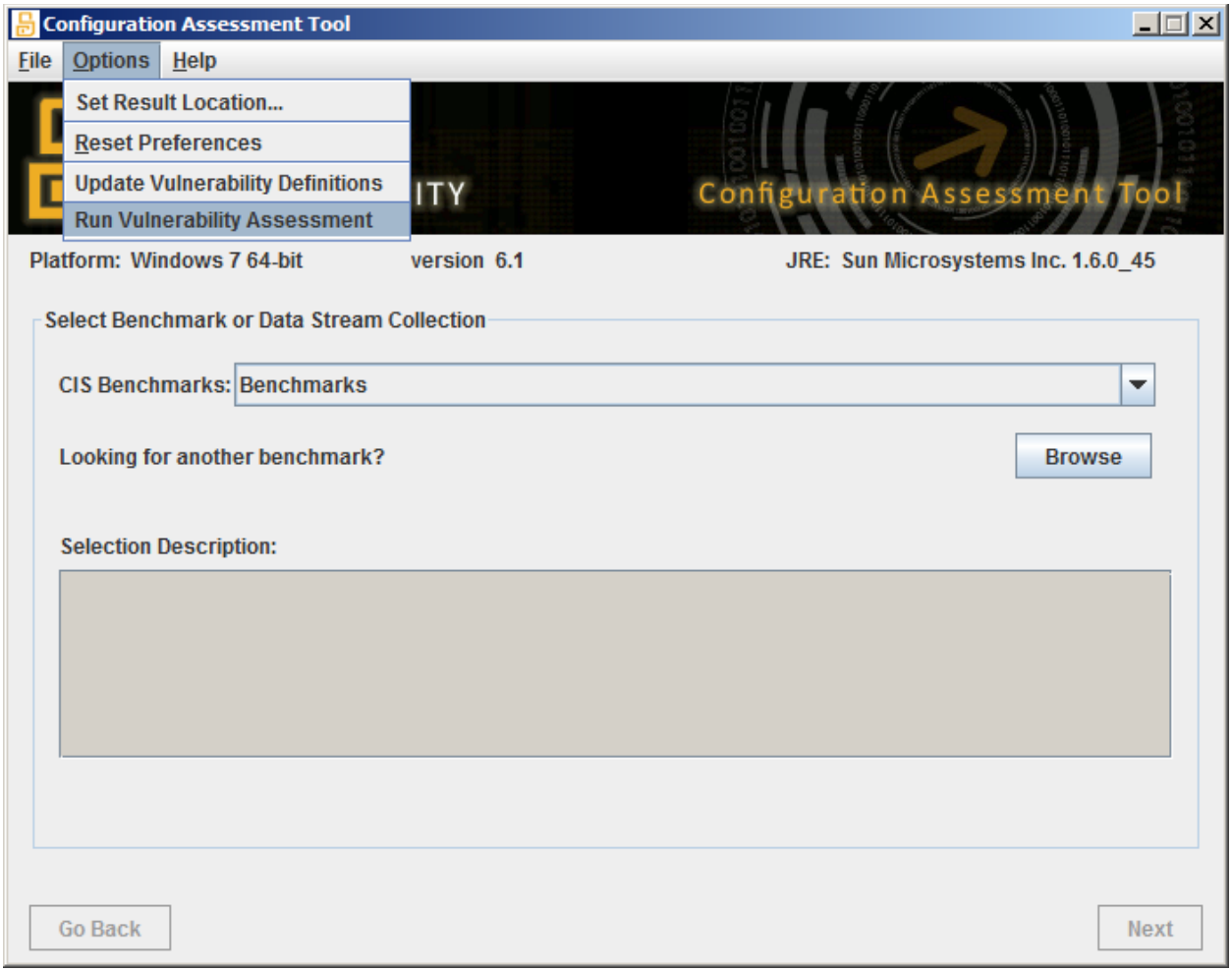
When an XML report or a directory has been selected, the user can then configure the report output options, selecting any combination of HTML, CSV, or Text reports to be generated.



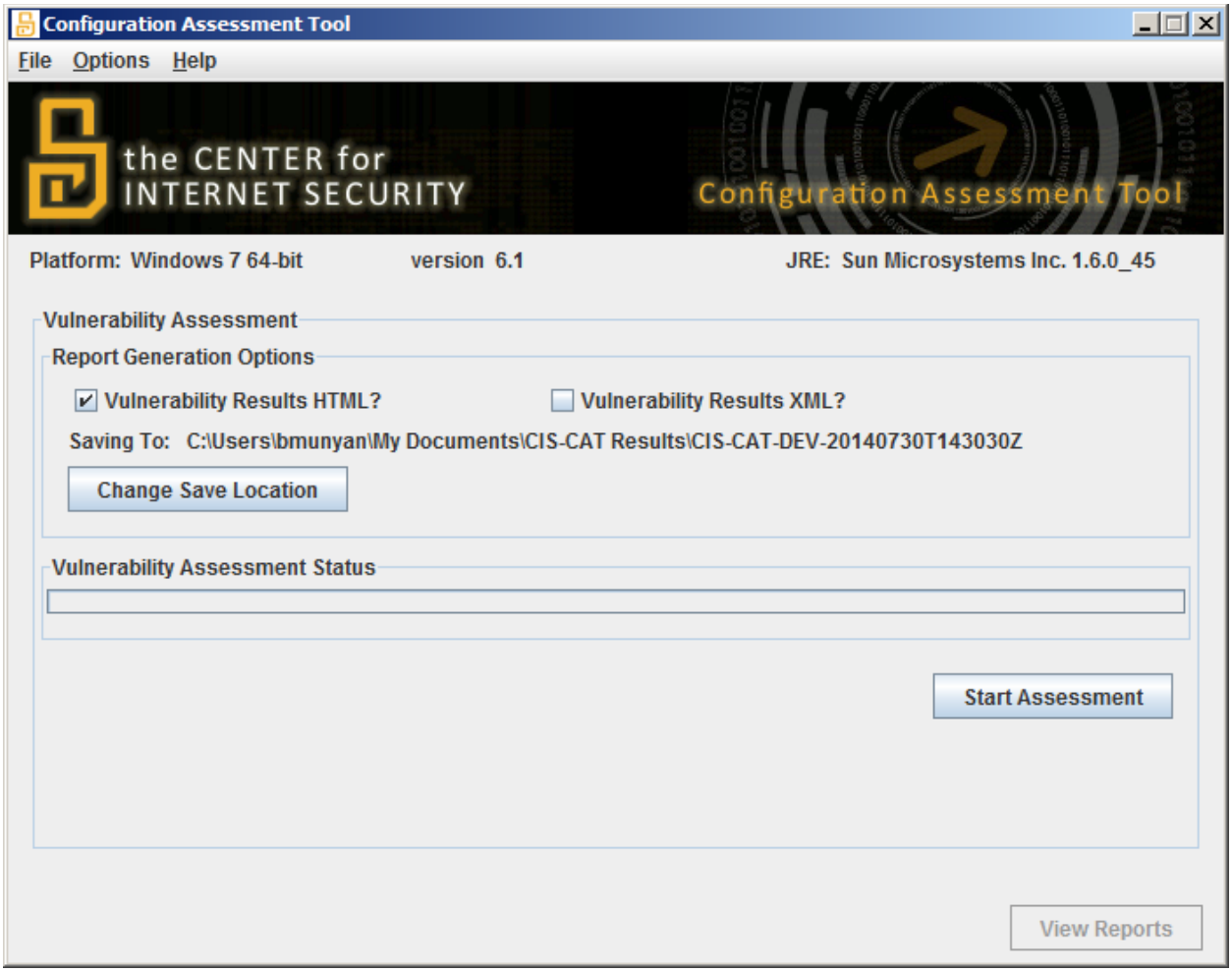
Once report output options have been selected, the user can then click the Generate Report(s) button to proceed. Following the completion of report generation, the View Report(s) button will become enabled to allow the user to select and view the newly created reports.

Executing a Vulnerability Assessment

CIS-CAT contains the capability to perform a vulnerability assessment against various platforms. To perform a vulnerability assessment separate from any other benchmark assessments, select the `Options -> Run Vulnerability Assessment` menu option:



Once the Vulnerability Assessment screen opens, verify or select a report destination and click the `Start Assessment` button:



The status of the vulnerability assessment will be displayed using the progress bar. Once the assessment has completed and reports generated, the `View Reports` button will become enabled in order to view the CIS-CAT results reports.

Vulnerability Definition Blacklist

A number of vulnerability definitions downloaded from the various repositories have been found to cause false positives, due to the definitions being written against security bulletins/patches which have since been superseded by newer ones. In order to mitigate the number of false positives, CIS has bundled a "blacklist" of OVAL vulnerability definitions which, when executing a vulnerability assessment, will not be evaluated.

The most recent version of the list is bundled with CIS-CAT, under the "`lib`" folder of a standard CIS-CAT installation, and is named "`blacklist.xml`". When a user manually updates to the latest vulnerability definitions, the latest version of the CIS blacklist will also be downloaded.

Individual organizations may create their own blacklist in order to suppress the evaluation of certain OVAL definitions.

NOTE: A user-defined blacklist *must* be named "`blacklist.xml`" and be saved to the "`custom`" folder of a CIS-CAT installation in order to be processed.

A template of a blacklist entry is as follows:

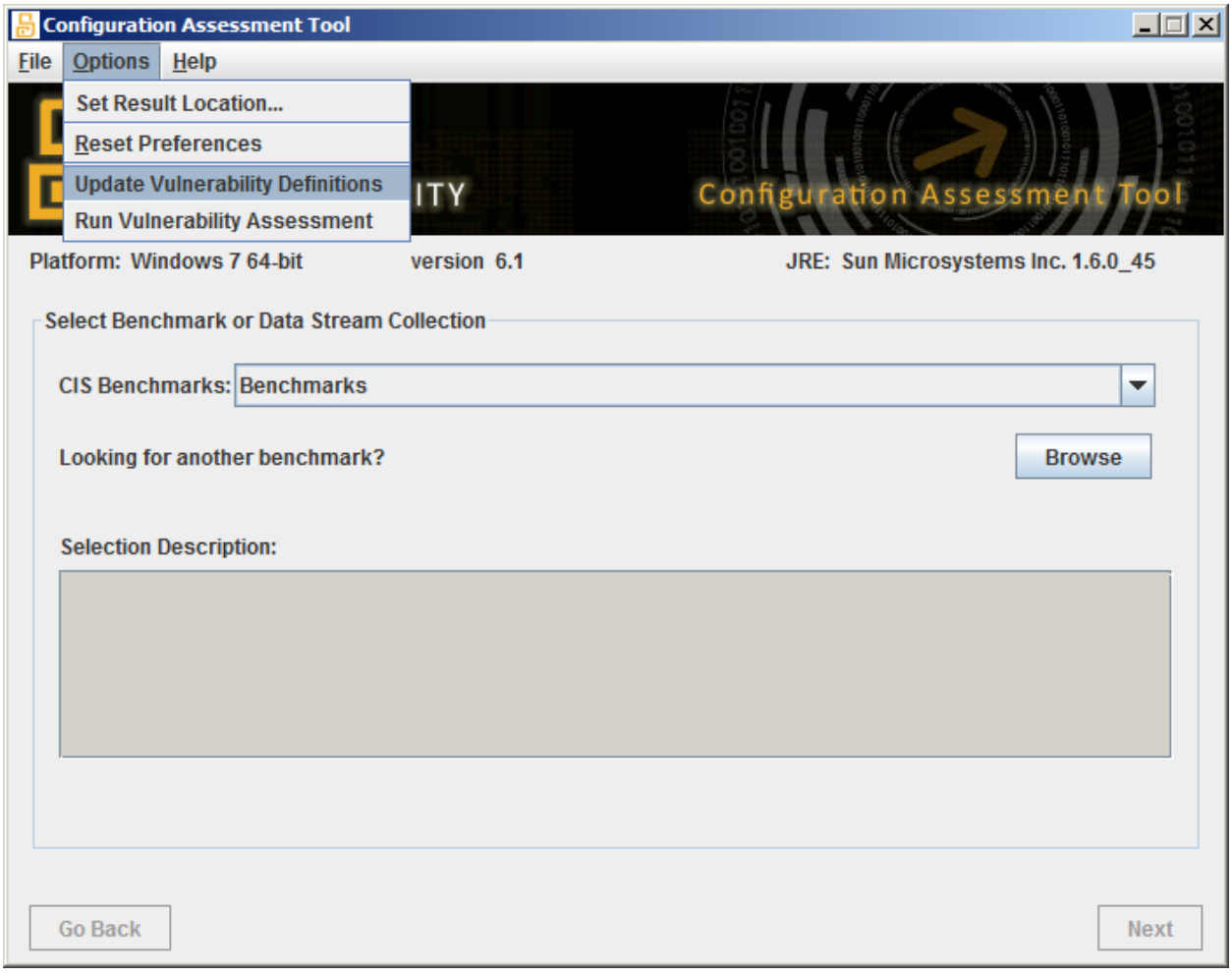
```
<?xml version="1.0" encoding="UTF-8"?>
<blacklist id="blacklist_com.your_organization_1.0.0" version="1.0.0">
      <entry id="THE_OVAL_DEFINITION_ID" type="false_positive">
            <notes>Any notes pertinent to the OVAL definition blacklist item</notes>
            <notes>More than 1 note is allowed</notes>
      </entry>
</blacklist>
```

The first highlighted item defines an id for the user-created blacklist.
Each blacklist `<entry>` contains the Definition ID of the OVAL definition to be blacklisted. The `type` attribute's allowed values are "`false_positive`", "`performance`", and "`other`", and is mandatory. An `<entry>` may have multiple `<notes>`, which are transferred to the OVAL results when processing a blacklist entry.

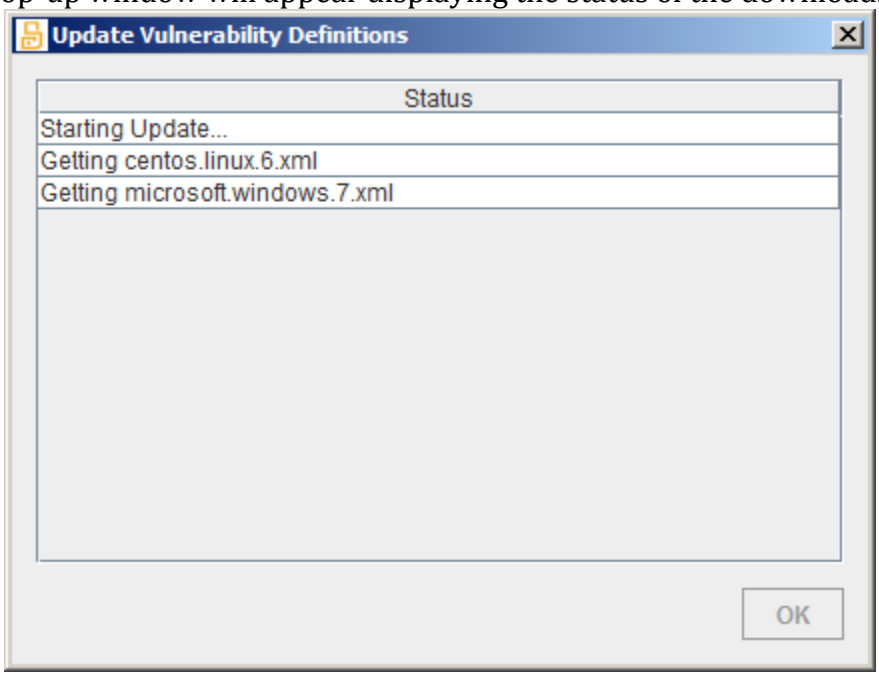
Updating Vulnerability Definitions

When executing a CIS-CAT benchmark assessment, a user is also able to enable an assessment of vulnerability definitions. These definition files are bundled with each release of CIS-CAT and are taken from the most recent set of vulnerability definitions contained in the OVAL repository for the Windows platforms supported by CIS-CAT. Red Hat Enterprise Linux vulnerability definitions are drawn from Red Hat's repository. SuSE vulnerability definitions are drawn from a repository hosted by Novell. These repositories are updated regularly, and thus CIS-CAT has the capabilities to download the latest versions of the supported OVAL definitions files.

From the CIS-CAT GUI, select `Options -> Update Vulnerability Definitions`



Once selected, a pop-up window will appear displaying the status of the download.



NOTE 1: This may take a few minutes, as many of the downloaded vulnerability definitions files are large.

Following the completion of the download, the OK button will become enabled and the user can return to the main CIS-CAT window.

NOTE 2: The "Update Vulnerability Definitions" process downloads information from the following sources:

- CIS: The OVAL repository, currently hosted by CIS (formerly hosted by MITRE), is used to download the latest vulnerability definitions for the supported Microsoft Windows platforms.
- Red Hat: Red Hat maintains an OVAL repository of vulnerability definitions for the various Red Hat Enterprise Linux platforms.
- Novell: Novell maintains an OVAL repository of vulnerability definitions for the various SUSE Linux platforms.
- CIS: Any CIS-maintained OVAL definition blacklists are downloaded from the CIS community site. When downloading the latest blacklist information, CIS-CAT will send basic usage information, such as CIS-CAT version, Operating System, and Java Runtime Environment, back to CIS.

Using CIS-CAT within a Command Line Interface (CLI)

CIS-CAT can also be executed from a CLI. To get a list of runtime options for CIS-CAT, execute the following (regardless of OS platform):

```
shell> java -jar CISCAT.jar -help

usage:

 -a,--accept-terms                Accepts terms of use w/o saving acceptance to disk

 -aa, --auto-assess               Performs automatic benchmark inventory and
                                  Assessment.

 -ap,--aggregation-period <arg>   The width of a dashboard aggregation
                                  period, ex. 1M, 13W, 20D

 -ar,--aggregate-reports <arg>    Create a CIS-CAT Dashboard by aggregating all the
                                  XML reports in the specified directory

 -arf, --report-arf               Creates an ARF report (SCAP 1.2 Data-Stream
                                  Collections Only)

 -as, --aggregation-status        Report Aggregation Status information is displayed.

 -b,--benchmark <arg>             Path to benchmark to run

 -c,--reset                       Reset preferences

 -csv,--report-csv                Creates a CSV report

 -d,--benchmark-dir <arg>         Override default location for
                                  benchmarks. Used with --list and --find.

 -db, --database <arg>            Test connectivity to a SQL database using its
                                  JDBC connection string.

 -dbs, --database-sysdba          Used with -db, this option indicates to attempt
                                  to connect to a database as SYSDBA.

 -ds, --datastream-id <arg>       Specifies a particular data-stream to select (SCAP
                                  1.2 Data-Stream Collections Only)

 -esxi, --esxi-connection <arg>   Test connectivity to an ESXi host using a
                                  connection string formatted as user/password@host.

 -f,--find                        Interactively select a benchmark

 -h,--help                        Prints help for this application

 -l,--list                        List all benchmarks in default benchmark
                                  location

 -n,--report-no-html              No HTML report will be created, by
                                  default an HTML report is created

 -od, --oval-definitions <arg>    Specifies an OVAL definitions file to process

 -or, --oval-results              Creates an OVAL Results HTML report

 -orx, --oval-results-xml         Creates an OVAL Results XML report
```

```
-ov, --oval-variables <arg>      Specifies an OVAL Variables file to process

-p, --profile <arg>              Title of benchmark profile to evaluate

-D <property=value>              Allows for a single user-specified property to be
                                 passed into CIS-CAT, configuring "interactive"
                                 benchmark values without requiring user input at
                                 runtime.

-props, --properties <arg>       Allows for a set of user-specified properties to
                                 be loaded, configuring "interactive" benchmark
                                 values without requiring user input at runtime.
                                 By default, user properties can be configured with
                                 a file named "ciscat.properties", saved to the
                                 "misc" folder of the CIS-CAT installation.

-r, --results-dir <arg>          Directory to save results in



-rg, --report-gen                The path to a previously generated XML report or a
                                 directory containing multiple XML reports; Used to
                                 generate ad-hoc HTML, Text, and CSV reports.

-rn, --report-name <arg>         The base name of the report, no
                                 extension

-s, --status                     Status information is displayed

-sr, --score                     Creates a dashboard-only score report

-t, --report-txt                 Creates a text report

-u, --report-upload <arg>        Sends a HTTP POST with the generated report(s)
                                 to the specified URL. POST parameter name is
                                 "ciscat-report"

-ui, --ignore-certificate-errors Ignores any SSL certificate errors during report
                                 upload

-up, --update                    Download the latest Vulnerability definitions from
                                 the OVAL repository

-upo, --update-platform-only     Download the latest Vulnerability definitions for
                                 only the currently running OS platform, if one
                                 exists.

-v, --version                    Display CIS-CAT version and JRE information

-va, --vulnerabilities           Execute a Vulnerability Assessment and generate
                                 a vulnerability results HTML report

-vax, --vulnerabilities-xml      When used with -va, this option will cause CIS-CAT
                                 to produce a vulnerability results XML report

-vac, --vulnerabilities-csv      When used with -va, this option will cause CIS-CAT
                                 to produce a vulnerability results CSV report

-vs,--verify-signature           Verify that the XML benchmarks have
                                 valid signatures

-x,--report-xml                  Creates an XML report
```

```
 -xc, -xccdf <arg>                Specifies a particular XCCDF benchmark within a
                                  data-stream to select (SCAP 1.2 Data-Stream
                                  Collections Only)

 -y,--report-all-tests            Causes the HTML and text reports to show
                                  all tests. Only applicable tests are
                                  displayed by default
```

The Java portions of the above command can be avoided by utilizing platform specific wrapper scripts provided within the CIS-CAT bundle, as described in the following table:

Platform	Command
Linux/Unix	`./CIS-CAT.sh [<options>] [<benchmark>] [<profile>]`
Windows	`CIS-CAT.bat [<options>] [<benchmark>] [<profile>]`

Listing Available Benchmarks

To produce a list of all benchmarks packaged with CIS-CAT, perform the following:

```
Windows> CIS-CAT.bat --list
Unix> ./CIS-CAT.sh --list

Here are the available benchmarks:
#1 Center for Internet Security AIX Benchmark version 1.0.1.1
file:/C:/cis-cat/benchmarks/aix-benchmark.xml
...
```

Choosing a Benchmark and Profile

CIS-CAT provides two mechanisms to select the desired Benchmark and Profile to evaluate; by expressing each as command line arguments and by interactively selecting each. To interactively select a Benchmark and Profile, perform the following:

```
Windows> CIS-CAT.bat --find
Unix> ./CIS-CAT.sh --find
```

When the `--find` option is used, CIS-CAT will enumerate all XCCDF documents located in the `benchmarks` directory. For each discovered benchmark, the title and version will be displayed. This is demonstrated below:

```
Here are the available benchmarks:
...
#13 Windows XP Professional Benchmark version 2.0.1.3
file:/C:/cis-cat/benchmarks/windows-xp-benchmark.xml

Which benchmark should be used? (return to exit) 13
```

Select the desired benchmark by typing the number located to the left of the benchmark title. In the above example, the *Windows XP Processional Benchmark* was selected by entering `13`. Once a benchmark has been selected, CIS-CAT will display the list of profiles defined in the benchmark. If no list is provided, the benchmark does not contain a profile. The following demonstrates the profile listing associated with the *Windows XP Processional Benchmark:*

```
Selected C:\cis-cat\benchmarks\windows-xp-benchmark.xml
This benchmark has 15 profiles.
1: SP1 Legacy (legacy-profile-sp1)
2: SP2 Legacy Standalone (legacy-profile-sp2-standalone)
```

```
3: SP2 Legacy Domain Member (legacy-profile-sp2-domain)
...
15: NIST Specialized (NIST-Specialized)
Which profile should be used? (return for none) 1
```

Once a profile is selected, CIS-CAT will evaluate the local system against that profile.

Running a specific Benchmark and Profile

If the desired benchmark and optional profile is already known, they can be provided to CIS-CAT as command line arguments. The following, which is equivalent to the example above, demonstrates this:

```
Windows> CIS-CAT.bat benchmarks\windows-xp-benchmark.xml legacy-profile-sp1
Unix> ./CIS-CAT.sh benchmarks/hpux-benchmark.xml base
```

Additionally a user can specify the benchmark through the command-line arguments `-b` and optionally a profile with `-p`. If no profile is selected the first profile in the benchmark is used. An example of this would look like:

```
Windows> CIS-CAT.bat -b benchmarks\windows-xp-benchmark.xml [-p legacy-profile-sp1]
Unix> ./CIS-CAT.sh -b benchmarks/hpux-benchmark.xml [-p base]
```

Note: The benchmark profile can be reference as either the `xccdf:profile@id` attribute of the `xccdf:title`. When using the profile title, for titles that contain spaces, you will need to use quotes as shown below:

```
Windows> CIS-CAT.bat -b benchmarks\windows-xp-benchmark.xml -p "Legacy Standalone"
Unix> ./CIS-CAT.sh -b benchmarks/hpux-benchmark.xml -p "Base Profile"
```

If benchmarks are stored in a location other than `benchmarks/`, use the `-d` option to cause CIS-CAT to list or find benchmarks in that location.

NOTICE:
If you plan to use the CIS-CAT Dashboard, you must export assessment results in XML format. See the Configuring Report Output section for additional details.

Evaluating a Data Stream Collection, Data Stream, Collection and Profile

If the desired SCAP 1.2-compliant data stream collection, data stream, checklist and profile are already known, they can be provided to CIS-CAT as command line arguments. The data stream collection filename may be specified either with or without the `-b` command-line argument:

Data Stream Collection Only

When only a data stream collection is specified, the first data stream, checklist and profile will automatically be selected for assessment.

```
Windows> CIS-CAT.bat [-b] benchmarks\scap_gov.nist_USGCB-Windows-7.xml
Unix> ./CIS-CAT.sh [-b] benchmarks/scap_gov.nist_USGCB-Windows-7.xml
```

Data Stream Collection and Data Stream

When a data stream collection and data stream are specified, the first checklist and profile will automatically be selected for assessment.

```
Windows> CIS-CAT.bat [-b] benchmarks\scap_gov.nist_USGCB-Windows-7.xml -ds
scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip

Unix> ./CIS-CAT.sh [-b] benchmarks/scap_gov.nist_USGCB-Windows-7.xml -ds
scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip
```

Data Stream Collection, Data Stream, and Checklist

When a data stream collection, data stream, and checklist are specified, the first profile will automatically be selected for assessment.

```
Windows> CIS-CAT.bat [-b] benchmarks\scap_gov.nist_USGCB-Windows-7.xml -ds
scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip -xc
xccdf_gov.nist_benchmark_USGCB-Windows-7

Unix> ./CIS-CAT.sh [-b] benchmarks/scap_gov.nist_USGCB-Windows-7.xml -ds
scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip -xc
xccdf_gov.nist_benchmark_USGCB-Windows-7
```

Data Stream Collection, Data Stream, Checklist, and Profile

When a data stream collection, data stream, checklist, and profile are specified, the selected profile will be assessed.

```
Windows> CIS-CAT.bat [-b] benchmarks\scap_gov.nist_USGCB-Windows-7.xml -ds
scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip -xc
xccdf_gov.nist_benchmark_USGCB-Windows-7 -p
xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1.2.3.
1

Unix> ./CIS-CAT.sh [-b] benchmarks/scap_gov.nist_USGCB-Windows-7.xml -ds
scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip -xc
xccdf_gov.nist_benchmark_USGCB-Windows-7 -p
xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1.2.3.
1
```

Note: When specifying a profile for evaluation, either the profile's unique ID or the profile title may be specified.

Data Stream Collection, Data Stream, and Definitions

When a data stream collection, data stream, and OVAL definitions component are specified, all available definitions referenced in that data stream component are assessed, and OVAL results are produced.

```
Windows> CIS-CAT.bat [-b] benchmarks\scap_gov.nist_USGCB-Windows-7.xml -ds
scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip -od scap_gov.nist_comp_USGCB-
Windows-7-oval.xml

Unix> ./CIS-CAT.sh [-b] benchmarks/scap_gov.nist_USGCB-Windows-7.xml -ds
scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip -od scap_gov.nist_comp_USGCB-
Windows-7-oval.xml
```

Note: When specifying an OVAL Definitions component, either the component reference ID in the data stream, or the component's unique ID may be specified.

Displaying Status Information during Evaluation

To view detailed status information while executing CIS-CAT from a command line interface, pass CIS-CAT the `-s` or `--status` flag. The following demonstrates this use case:

```
Windows> CIS-CAT.bat -s -b benchmarks\windows-2003-benchmark.xml -p "legacy profile -
domain controller"
```

```
1/169   Current Service Pack Installed                          <1 second Fail
2/169   All Critical and Important...date have been installed. <1 second  N/A
...
168/169 HKU\.Default\Software\Micr...cates\Root\ProtectedRoots <1 second Pass
169/169 HKLM \SOFTWARE\Microsoft\W...NT\CurrentVersion\SeCEdit <1 second Fail
Total Evaluation Time: 28 seconds

Results written to: CIS-CAT Results\test-result-20100126T184725Z.xml
Report written to: CIS-CAT Results\test-report-20100126T184725Z.html
```

Accepting Terms of Use

When CIS-CAT is executed for the first time on a given computer, it will prompt the user to accept the terms of use. In environments where CIS-CAT is deployed en masse, it may be beneficial to accept the terms of use via the command line to ensure the prompt does not disrupt automated invocations of CIS-CAT. To accept the terms of use via the command line, specify the `-a` option as shown below:

```
Windows> CIS-CAT.bat -b benchmarks\windows-xp-benchmark.xml -a
Unix> ./CIS-CAT.sh -b benchmarks/slackware-benchmark.xml -a
```

Reset CIS-CAT Preferences

To reset the CIS-CAT preferences, specify the `-c` option as shown below:

```
Windows> CIS-CAT.bat -c
Unix> ./CIS-CAT.sh -c
This is CIS-CAT version 2.1.4
All preferences removed
```

Configuring Result Location

Before evaluating a system against a CIS benchmark, it is recommended that the Result Location be specified. The default location for results is articulated below:

Platform	Location
Windows	`%HOMEDRIVE%%HOMEPATH%\My Documents\CIS-CAT Results`
Unix/Linux	`$HOME/CIS-CAT_Results`

To change the report location, specify the `-r` option as shown below:

```
Windows> CIS-CAT.bat -r d:\reports -b benchmarks\windows-xp-benchmark.xml
Unix> ./CIS-CAT.sh -r /cis-cat-results -b benchmarks/slackware-benchmark.xml
```

Configuring Report Name

To change the report name for all formats use the `-rn` argument. Using this will change all of the report names to be the value supplied appended with either .html, .xml or .txt depending on the specified report output type. The following command will cause CIS-CAT to save the report as `quarterlyAssessment.html` under the `reports` directory.

```
Windows> CIS-CAT.bat -r d:\reports -rn quartelyAssessment ...
Unix> ./CIS-CAT.sh -r /reports -rn quartelyAssessment ...
```

Configuring Report Output

By default CIS-CAT will output an HTML report with only applicable tests. It is possible to generate a text (`-t`), an XML (`-x`) report or CSV (`-csv`) report. When CIS-CAT is executed against a data stream collection, OVAL results (`-or`) and an Asset Reporting Format report (`-arf`) may also be generated. The following command will cause CIS-CAT to save the following four reports under the `reports` directory and the report:

1. `quarterlyAssessment.txt`
2. `quarterlyAssessment.csv`
3. `quarterlyAssessment.html`
4. `quarterlyAssessment.xml`

```
Windows> CIS-CAT.bat -r d:\reports -rn quartelyAssessment -t -x -csv ...
Unix> ./CIS-CAT.sh -r /reports -rn quartelyAssessment -t -x -csv ...
```

To have all tests included in the report, including tests that are not selected for a given profile, specify the command argument `-y`.

```
Windows> CIS-CAT.bat -r d:\reports -rn quartelyAssessment -t -x -csv -y
Unix> ./CIS-CAT.sh -r /reports -rn quartelyAssessment -t -x -csv -y
```

To generate OVAL results and an Asset Reporting Format report, specify the `-or` and `-arf` command arguments.

```
Windows> CIS-CAT.bat -r d:\reports -rn quartelyAssessment -or -arf
Unix> ./CIS-CAT.sh -r /reports -rn quartelyAssessment -or -arf
```

Configuring Interactive Values

A number of CIS benchmarks require values to be set at runtime. An example would be the various CIS database benchmarks, such as Oracle and Microsoft SQL Server. When selected for assessment, a user must interactively enter values specific to the database being assessed, such as a JDBC connection string.

Users can modify the benchmark XML in order to convert these "interactive" values, hard-coding these settings to specific values. However, this presents an issue when there is a requirement to assess multiple databases. In this case, multiple copies of the benchmark would be necessary, each with specific configurations for the database it is meant to assess.

In order to address this need, functionality has been integrated into CIS-CAT allowing for a "properties" file to be created, configuring the settings for the "interactive" values without the need to edit the XML benchmark content.

By default, CIS-CAT will always search for user configuration settings in a file named `ciscat.properties`, located in the `misc` folder of the CIS-CAT installation. In order to configure a benchmark's "interactive" values, a user may simply edit the ciscat.properties file, adding a name/value pair representing the "interactive" value's `ID` and the configured value. For example, the Oracle database benchmark requires user intervention to enter a setting for the `xccdf_org.cisecurity_value_jdbc.url` value. In the `ciscat.properties` file, a user can simply add an entry:

```
xccdf_org.cisecurity_value_jdbc.url=jdbc:oracle:thin:sys/password1@localhost:1521:CIS
DB1
```

When CIS-CAT executes, it will first check for a matching value in the user-defined properties. If no value matching the "interactive" value ID is present, the standard prompts will be displayed to the user for manual entry.

From the Command-Line User Interface, a user may also configure the location of the user-defined properties file to be used during an assessment. This allows, for example, the ability to configure a number of properties files, one for each database to be assessed. This is a significant decrease in complexity from maintaining a copy of the Oracle database benchmark for each database to be assessed. Once a user-defined properties file is configured and saved, it can be used in a CIS-CAT assessment using the `-props` command-line option:

```
> CIS-CAT.bat -b path\to\benchmark.xml -props path\to\propfile.properties
```

When a single or few interactive properties are needed, or perhaps when scripting user-supplied properties, a user can pass individual properties to the CIS-CAT command-line with the "-D" option (NOTE the capital "D"). Instead of creating an entire properties file for a single JDBC connection string, for example, a user can supply the value right on the command-line:

```
> CIS-CAT.bat -b path\to\benchmark.xml -D
xccdf_org.cisecurity_value_jdbc.url=jdbc:oracle:thin:sys/pwd@database
```

Users may pass multiple –D property=value pairs into CIS-CAT from the command-line:

```
> CIS-CAT.bat -D prop1=value1 -D prop2=value2
```

Creating a CIS-CAT Dashboard

To run report aggregation use the `-ar` parameter followed by the location of all the CIS-CAT XML results to be summarized. By default report aggregation will use a timeframe of one week for each benchmark, profile, computer combination. Meaning only one of these combinations will show up in that timeframe. It is possible to change this timeframe by using the `-ap` argument and passing in a value in the format of *<LENGTH OF TIMEFRAME>* followed by either: `m` (months), `d` (days) or `w` (weeks).

Uploading a CIS-CAT Results File

To send the results after a CIS-CAT scan is done to a URL specify the `-u` argument. CIS-CAT will attempt to upload each report format specified by the various reporting command-line options. The URL specified can be either HTTP or HTTPS. If uploading to a HTTPS URL and the SSL certificate is not valid passing in the `-ui` argument will cause CIS-CAT to not validate the SSL certificate. When the CIS-CAT results files are sent to the website they will be sent over as a POST and the report data will be associated with the parameter name `ciscat-report`. The following is an example command:

```
Windows> CIS-CAT.bat -ui -u https://www.cisecurity.org/ciscat-handler.php ...
Unix> ./CIS-CAT.sh -ui -u https://www.cisecurity.org/ciscat-handler.php ...
```

Below is an example handler that would receive the request:

```
<?php
      if(isset($_POST['ciscat-report']) && !empty($_POST['ciscat-report'])) {
            mail("yourname@example.com", "CIS-CAT Results File", $_POST['ciscat-report']);
```

```
        }
?>
```

Executing a Vulnerability Assessment

Performing a vulnerability assessment from the command-line is simply a matter of adding the "-va" option. This command-line option can be used on its own, or utilized in conjunction with a benchmark assessment.

To perform only a vulnerability assessment, execute the following from the command-line:

```
> ./CIS-CAT.sh -va
```

To include a vulnerability assessment along with a benchmark assessment, simply add the "-va" command-line option. For example, to execute the CIS CentOS 6 benchmark assessment, using the Level 1 profile, adding a vulnerability assessment:

```
> ./CIS-CAT.sh -b benchmarks/CIS_CentOS_Linux_6_Benchmark_v1.0.0.xml -p
xccdf_org.cisecurity.benchmarks_profile_Level_1 -va
```

Vulnerability Definition Blacklist

A number of vulnerability definitions downloaded from the various repositories have been found to cause false positives, due to the definitions being written against security bulletins/patches which have since been superseded by newer ones. In order to mitigate the number of false positives, CIS has bundled a "blacklist" of OVAL vulnerability definitions which, when executing a vulnerability assessment, will not be evaluated.

The most recent version of the list is bundled with CIS-CAT, under the "lib" folder of a standard CIS-CAT installation, and is named "blacklist.xml". When a user manually updates to the latest vulnerability definitions, the latest version of the CIS blacklist will also be downloaded.

Individual organizations may create their own blacklist in order to suppress the evaluation of certain OVAL definitions.

NOTE: A user-defined blacklist *must* be named "blacklist.xml" and be saved to the "custom" folder of a CIS-CAT installation in order to be processed.

A template of a blacklist entry is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<blacklist id="blacklist_com.your_organization_1.0.0" version="1.0.0">
      <entry id="THE_OVAL_DEFINITION_ID" type="false_positive">
            <notes>Any notes pertinent to the OVAL definition blacklist item</notes>
            <notes>More than 1 note is allowed</notes>
      </entry>
</blacklist>
```

The first highlighted item defines an id for the user-created blacklist.
Each blacklist <entry> contains the Definition ID of the OVAL definition to be blacklisted. The type attribute's allowed values are "false_positive", "performance", and "other", and is mandatory. An <entry> may have multiple <notes>, which are transferred to the OVAL results when processing a blacklist entry.

Updating Vulnerability Definitions

From the CIS-CAT command-line interface, a user may download the latest vulnerability definitions using the "`-up`" option.

```
>CIS-CAT.bat -up
```

NOTE 1: This may take a few minutes, as many of the downloaded vulnerability definitions files are large.

NOTE 2: The "Update Vulnerability Definitions" process downloads information from the following sources:

- The OVAL Repository: The OVAL repository, currently hosted by CIS, is used to download the latest vulnerability definitions for the supported Microsoft Windows platforms.
- Red Hat: Red Hat maintains an OVAL repository of vulnerability definitions for the various Red Hat Enterprise Linux platforms.
- CIS: Any CIS-maintained OVAL definition blacklists are downloaded from the CIS community site. When downloading the latest blacklist information, CIS-CAT will send basic usage information, such as CIS-CAT version, Operating System, and Java Runtime Environment, back to CIS.

Ad-Hoc Report Generation

Using the "`-rg`" command-line option CIS-CAT is configured to execute the ad-hoc report generation workflow. The user is required to specify either a path to an existing XML report or a path to a directory containing XML reports to be processed, along with the command-line options representing the report types to be generated. By default, the HTML report will always be regenerated.

To configure CIS-CAT to generate an HTML, CSV, and Text report,

```
>CIS-CAT.bat -rg <path_to_xml_report> -csv -t
```

In order to configure CIS-CAT to NOT generate an HTML report,

```
>CIS-CAT.bat -rg <path_to_xml_report> -n
```

In order to configure CIS-CAT to report all test results, analogous to un-checking the "Include Applicable Tests Only" checkbox,

```
>CIS-CAT.bat -rg <path_to_xml_report> -y
```

Command-Line Error Codes

When executing CIS-CAT using the command-line user interface, one of a number of error codes may result due to errors in execution, invalid benchmark selection, etc. The following listing describes the potential error codes which could be displayed to a user on the command-line:

Error Code	Error Description
ERR-CLI-0001	An unrecognized Command-Line option was entered. Use -h to list all available Command-Line options.
ERR-CLI-0002	An error occurred parsing the available Command-Line options. Please contact CIS-CAT support.
ERR-CLI-0003	An error occurred when attempting to connect to the database. (Error message is

	included)
ERR-CLI-0004	An error occurred configuring the reports directory. The directory does not exist. Either create this directory or specify a valid directory.
ERR-CLI-0005	An error occurred configuring the HTTP POST URL (url value). Please ensure this URL exists and is reachable.
ERR-CLI-0006	An error occurred configuring the dashboard report source directory. (directory name) does not exist. Specify a valid directory containing the XML reports to be aggregated.
ERR-CLI-0007	An error occurred reading the benchmark file (name of benchmark file). Ensure a valid benchmark file is selected.
ERR-CLI-0008	An error occurred parsing the benchmark file (name of benchmark file). Ensure a valid benchmark file is selected.
ERR-CLI-0009	The User chose to exit CIS-CAT
ERR-CLI-0010	An error occurred configuring the data stream selected for assessment. Ensure the data stream is valid for the selected benchmark.
ERR-CLI-0011	An error occurred configuring the checklist selected for assessment. Ensure the checklist is valid for the selected benchmark.
ERR-CLI-0012	An error occurred configuring the profile selected for assessment. Ensure the profile is valid for the selected benchmark.
ERR-CLI-0013	An error occurred loading the available benchmarks from (benchmark source directory).
ERR-CLI-0014	When the checklist option (-xc) is entered, a valid data stream selection (-ds) must also be entered.
ERR-CLI-0015	When the OVAL Variables file option (-ov) is entered, a valid OVAL Definitions file option (-od) must also be entered.
ERR-CLI-0016	An invalid Command-Line option combination has been entered. Use -h to list all available Command-Line options.
ERR-CLI-0017	An error occurred loading available OVAL Definitions from (source directory).
ERR-CLI-0018	An error occurred reading the OVAL Definitions file (filename). Ensure a valid OVAL Definitions file is selected.
ERR-CLI-0019	An error occurred reading the OVAL Variables file (filename). Ensure a valid OVAL Variables file is selected.
ERR-CLI-0020	The User did not accept the CIS-CAT Terms of Use. Use the -a option to accept the Terms of Use.
ERR-CLI-0021	An invalid selection was made. CIS-CAT will now exit.
ERR-CLI-0022	An error occurred configuring ad-hoc report generation. The file/directory (directory name) does not exist.
ERR-CLI-0024	An error occurred when attempting to connect to the ESXi host. The host may be unreachable or the user/password could be invalid.
ERR-CLI-0025	The selected benchmark does not match the target platform.
ERR-CLI-0026	An error occurred when attempting to establish an SSH session. The host may be unreachable or the user/password/port could be invalid.

Configurable Runtime Properties

CIS-CAT executes using a default set of runtime properties. These properties can control certain types of content validation, benchmark-to-platform verifications, report output, and interfaces to CIS-CAT Pro Dashboard. The runtime properties are stored in the `ciscat.properties` file, contained in the `misc` folder, and the following table describes them. Unless otherwise noted as (true/false), each property value is a string.

Property Name	Description

user.assigned.machine.name	A secondary method of identifying the assessed endpoint. Displays on HTML reports.
ignore.platform.mismatch	(true/false) Controls whether or not CIS-CAT allows assessment of benchmarks that are not applicable to the target platform.
include.csv.remediation	(true/false) Allow for the inclusion of remediation text in CSV reports. Default is false.
include.csv.headers	(true/false) Allow for the inclusion of a row of column headers in CSV reports. Default is false.
include.csv.target_ip	(true/false) Allow for the inclusion of the target IP address in CSV reports. Default is false.
include.csv.username	(true/false) Allow for the inclusion of the executing user's username in CSV reports. Default is false.
include.csv.scoring	(true/false) Allow for the inclusion of overall scoring information in CSV reports. Default is true.
system.identifier.ciscat.primary	Configuration of the "primary system identifier", used by the CIS-CAT Pro Dashboard to uniquely identify the assessed endpoint.
ciscat.post.parameter.ccpd.token	Configuration of the CIS-CAT Pro Dashboard authentication token, allowing the assessment results to be uploaded to CCPD through the "POST results to URL" functionality.
ciscat.post.parameter.report.name	Allows for the customization of the CIS-CAT POST parameter for the report name. Default is "report-name"
ciscat.post.parameter.report.body	Allows for the customization of the CIS-CAT POST parameter for the report body. Default is "ciscat-report"
ciscat.welcome.message	Allows for a custom message to be displayed when launching CIS-CAT. The default value is empty, causing the standard "This is CIS-CAT Pro Assessor, version X" to be displayed.
successful.report.upload.message	Allows for a custom message to be displayed upon a successful POST of report data to a URL.
ssh.session.host	SSH connection property indicating the hostname/IP to which CIS-CAT will connect (IOS/ASA only)
ssh.session.port	SSH connection property indicating the port to which CIS-CAT will connect (IOS/ASA only). Default port is 22.
ssh.session.username	SSH connection property indicating the username with which CIS-CAT will connect (IOS/ASA only)
ssh.session.credentials	SSH connection property indicating the credentials with which CIS-CAT will connect (IOS/ASA only). Either credentials or a private key file may be used, but not both.
ssh.session.enable	SSH connection property indicating the credentials which CIS-CAT will use to elevate the device into "enable" mode (IOS/ASA only)
ssh.session.privatekey	SSH connection property indicating the path to a private key file with which CIS-CAT will connect. Either credentials or a private key file may be used, but not both.
vulnerability.proxy.host	Manual configuration of a proxy host for use in downloading vulnerability definitions.

`vulnerability.proxy.port`	Manual configuration of a proxy port for use in downloading vulnerability definitions.

Any or all of these properties, as well as any "interactive" XCCDF value ID's, may be specified using the CIS-CAT command-line interface by using the "-D" option. When options are specified on the command-line, they are used only for that single execution of CIS-CAT and are not propagated to the `ciscat.properties` file.

For example, in order to disable platform verification when searching for a benchmark to assess, the user may utilize the following command-line:

```
> ./CIS-CAT.sh -f -D ignore.platform.mismatch=true
```

By adding the –D option, the command-line is instructing CIS-CAT to temporarily ignore any platform verification errors. Also note that many –D options are allowed on a single command-line:

```
> ./CIS-CAT.sh -f -D ignore.platform.mismatch=true -D include.csv.remediation=true -
csv
```

The above command-line allows the user to interactively select a benchmark and profile for assessment (-f), ignore any platform verification errors, include remediation information in the CSV report, and generate the CSV report (-csv).

Interpreting Evaluation Results

Once CIS-CAT has completed evaluating the target system it will store results at the location described in Configuring Report Location. Two files will be created:

File	Description
`<ComputerName>-report-<timestamp>.html`	This is the primary report that has been formatted to present evaluation results in an easily understood format. This report is intended to be viewed in a web browser.
`<ComputerName>-result-<timestamp>.xml`	This is the source XCCDF document that the report is built from. This file contains all test definitions and results. This file is not intended to be viewed outside the context of an XML editor.

Summary of Results

The summary section of the report provides a high level overview of the target system's conformance to the configuration profile defined in the selected Benchmark and Profile.

Summary

Description	Tests				Scoring		
	Pass	Fail	Error	Not Selected	Score	Max	Percent
1 Computer Configuration	**204**	**42**	**0**	**51**	**204.0**	**249.0**	**82%**
1.1 Administrative Templates	37	40	0	7	37.0	77.0	48%
1.1.1 Windows Components	21	38	0	5	21.0	59.0	36%
1.1.1.1 BitLocker Drive Encryption	2	38	0	0	2.0	40.0	5%
1.1.1.1.1 Operating System Drives	0	16	0	0	0.0	16.0	0%
1.1.1.1.2 Fixed Data Drives	1	10	0	0	1.0	11.0	9%
1.1.1.1.3 Removable Data Drives	1	11	0	0	1.0	12.0	8%
1.1.1.2 AutoPlay Policies	1	0	0	0	1.0	1.0	100%
1.1.1.3 Event Log Service	6	0	0	0	6.0	6.0	100%
1.1.1.3.1 Application	2	0	0	0	2.0	2.0	100%
1.1.1.3.2 Security	2	0	0	0	2.0	2.0	100%
1.1.1.3.3 System	2	0	0	0	2.0	2.0	100%
1.1.1.4 Windows Remote Shell	1	0	0	0	1.0	1.0	100%
1.1.1.5 Windows Explorer	1	0	0	0	1.0	1.0	100%
1.1.1.6 Windows Update	5	0	0	3	5.0	5.0	100%
1.1.1.7 Credential User Interface	1	0	0	1	1.0	1.0	100%
1.1.1.8 Remote Desktop Services	4	0	0	0	4.0	4.0	100%
1.1.1.8.1 Remote Desktop Session Host	3	0	0	0	3.0	3.0	100%
1.1.1.8.1.1 Security	2	0	0	0	2.0	2.0	100%

In the above example, there are three major sections, each with their own score. The following details the significant values in the above summary:

- Values in the `Pass` column represent the number of rules that passed in the respective section. In the above illustration, we can see that two (2) rules passed in the *BitLocker Drive Encryption* section.
- Values in the `Fail` column represent the number of rules that failed in the respective section. In the above illustration, we can see that 38 rules failed in the *BitLocker Drive Encryption* section.
- Values in the `Error` column represent the number of rules that resulted in an error. No success or failure result is derived from this column.

- Values in the `Not Selected` column represent the number of rules that are informational only. These rules do not impact the final score of the evaluation.
- Values in the `Score` column represent the rules that passed in a given section.
- Values in the `Max` column represent the maximum score for the given section.
- Values in the `Percent` column represent the percent of rules passed in the given section out of all scorable (`Max`) items. For example, the score for the *BitLocker Drive Encryption* section is 5%. This value is derived by dividing the number of rules passed, two (2), by the number of total rules, forty (40).

At the bottom of the summary area there is a `Total` row which is the aggregate of all sections.

Assessments Results

The `Assessments` section of the report details all rules defined in the benchmark, as seen in the following illustration:

Assessment Results

Display All Defined Tests

W	Benchmark Item	Result
	1 Computer Configuration	
	1.1 Administrative Templates	
	1.1.1 Windows Components	
	1.1.1.1 BitLocker Drive Encryption	
	1.1.1.1.1 Operating System Drives	
	1.1.1.1.2 Fixed Data Drives	
	1.1.1.1.3 Removable Data Drives	
	1.1.1.2 AutoPlay Policies	
1.0	1.1.1.2.1 Set 'Turn off Autoplay' to 'Enabled:All drives'	Pass
	1.1.1.3 Event Log Service	
	1.1.1.3.1 Application	
1.0	1.1.1.3.1.1 Set 'Maximum Log Size (KB)' to 'Enabled:32768'	Pass
1.0	1.1.1.3.1.2 Set 'Retain old events' to 'Disabled'	Pass
	1.1.1.3.2 Security	
1.0	1.1.1.3.2.1 Set 'Retain old events' to 'Disabled'	Pass
1.0	1.1.1.3.2.2 Set 'Maximum Log Size (KB)' to 'Enabled:81920'	Pass
	1.1.1.3.3 System	
1.0	1.1.1.3.3.1 Set 'Maximum Log Size (KB)' to 'Enabled:32768'	Pass
1.0	1.1.1.3.3.2 Set 'Retain old events' to 'Disabled'	Pass
	1.1.1.4 Windows Remote Shell	
1.0	1.1.1.4.1 Set 'Allow Remote Shell Access' to 'Enabled'	Pass
	1.1.1.5 Windows Explorer	
1.0	1.1.1.5.1 Set 'Turn off Data Execution Prevention for Explorer' to 'Disabled'	Pass
	1.1.1.6 Windows Update	
1.0	1.1.1.6.1 Set 'Configure Automatic Updates' to 'Enabled:3 - Auto download and notify for install'	Pass
1.0	1.1.1.6.2 Set 'Reschedule Automatic Updates scheduled installations' to 'Enabled:1'	Pass
1.0	1.1.1.6.3 Set 'No auto-restart with logged on users for scheduled automatic updates installations' to 'Disabled'	Pass

The following details the significant values in the above checklist:

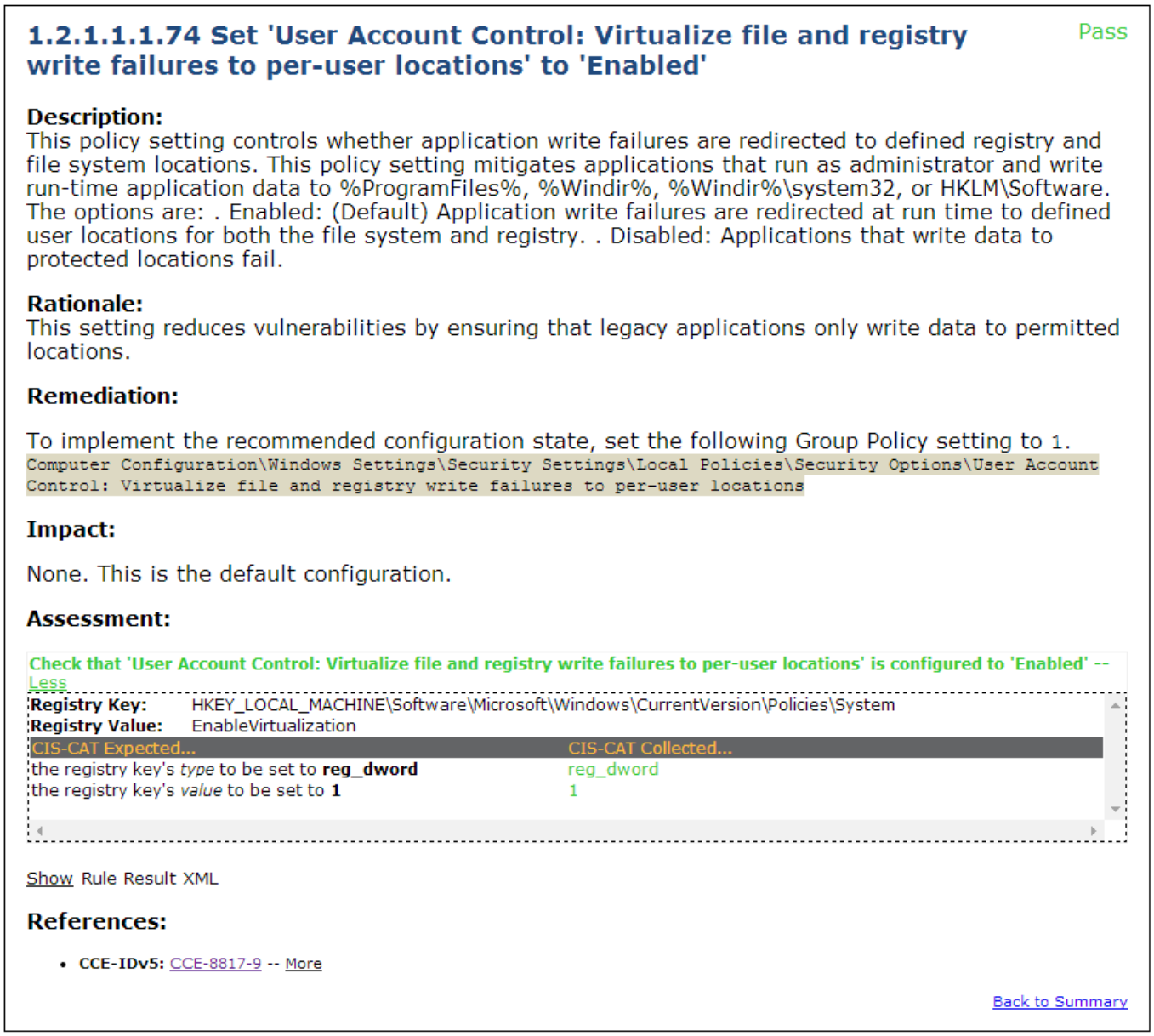
- The value in the `W` column indicates the scoring weight of the given Benchmark Item. Currently, all benchmark items are weighted equally – 1.0.
- The `Benchmark Item` column contains the title of a given Benchmark rule. Each item in this column is a link to Result Details.
- The `Result` column displays the result of a given test. Possible values are: `Fail`, `Pass`, `Error`, `Unknown` and `Not Selected`.

Assessment Details

The `Details` section of the report contains the following information for each Benchmark recommendation:

- All information in the `Checklist` section including Description, CCE (if applicable), Remediation, and Audit information for the given rule.
- The details of the assessment performed, including the applicable evidence which CIS-CAT collected and used to determine pass/fail status.

The following illustrates this:



1.2.1.1.1.74 Set 'User Account Control: Virtualize file and registry write failures to per-user locations' to 'Enabled' Pass

Description:
This policy setting controls whether application write failures are redirected to defined registry and file system locations. This policy setting mitigates applications that run as administrator and write run-time application data to %ProgramFiles%, %Windir%, %Windir%\system32, or HKLM\Software. The options are: . Enabled: (Default) Application write failures are redirected at run time to defined user locations for both the file system and registry. . Disabled: Applications that write data to protected locations fail.

Rationale:
This setting reduces vulnerabilities by ensuring that legacy applications only write data to permitted locations.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.
`Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Virtualize file and registry write failures to per-user locations`

Impact:

None. This is the default configuration.

Assessment:

Check that 'User Account Control: Virtualize file and registry write failures to per-user locations' is configured to 'Enabled' -- Less

Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
Registry Value: EnableVirtualization

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **1**	1

Show Rule Result XML

References:

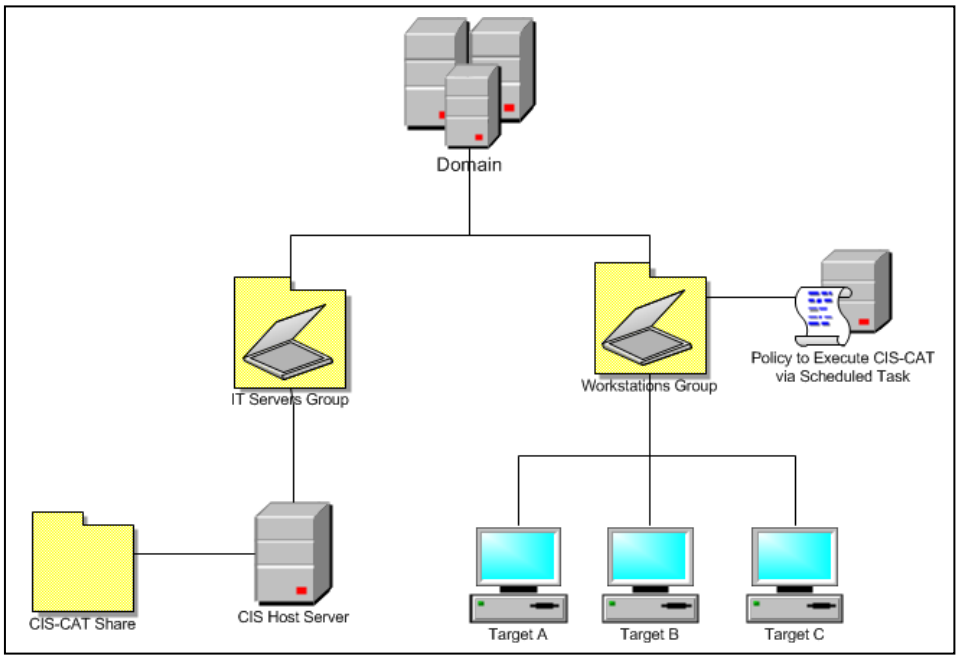
- **CCE-IDv5:** CCE-8817-9 -- More

Back to Summary

To view the XCCDF constructs, click the `Show Rule Result XML` link below the "Assessments" section. The information presented when clicking on this link is primarily for debugging purposes and will be covered in a future version of this guide.

Assessing Multiple Windows Targets

It is possible to assess a population of Microsoft Windows targets in an automated manner without installing CIS-CAT or the JRE on each target. The following diagram depicts this deployment pattern:



CIS Host Server

The *CIS Host Server* is where the CIS-CAT bundle, Java Runtime Environment, and Reports are placed. Targets within the `Workstations Group` will access these resources to perform a self-assessment using CIS-CAT.

Workstations Group

The *Workstations Group* represents a population of Microsoft Windows targets to be assessed with CIS-CAT. The Domain Administrator will create Group Policy that causes devices in this group to invoke CIS-CAT via a Scheduled Task.

Notice

Microsoft security bulletin MS14-025 notifies Windows users of a vulnerability in Group Policy Preferences which could allow elevation of privileges. Once the appropriate patch has been installed on the various systems, scheduled tasks are no longer allowed to store passwords, because the password was stored insecurely.

In order to address this patch, the "Assessing Multiple Windows Targets" workflow required modification. The scheduled task configured by this process can no longer store the credentials of the *CIS-CAT Domain User*, and in order to maintain a secure configuration of the *CIS Host Server*, authenticated users should only be allowed to execute the "cis-cat-centralized.bat" file.

Prerequisites

1. All targets must be joined to an Active Directory Domain
2. All targets must have read access to the *CIS-CAT Share* hosted off of the *CIS Host Server*

Setup

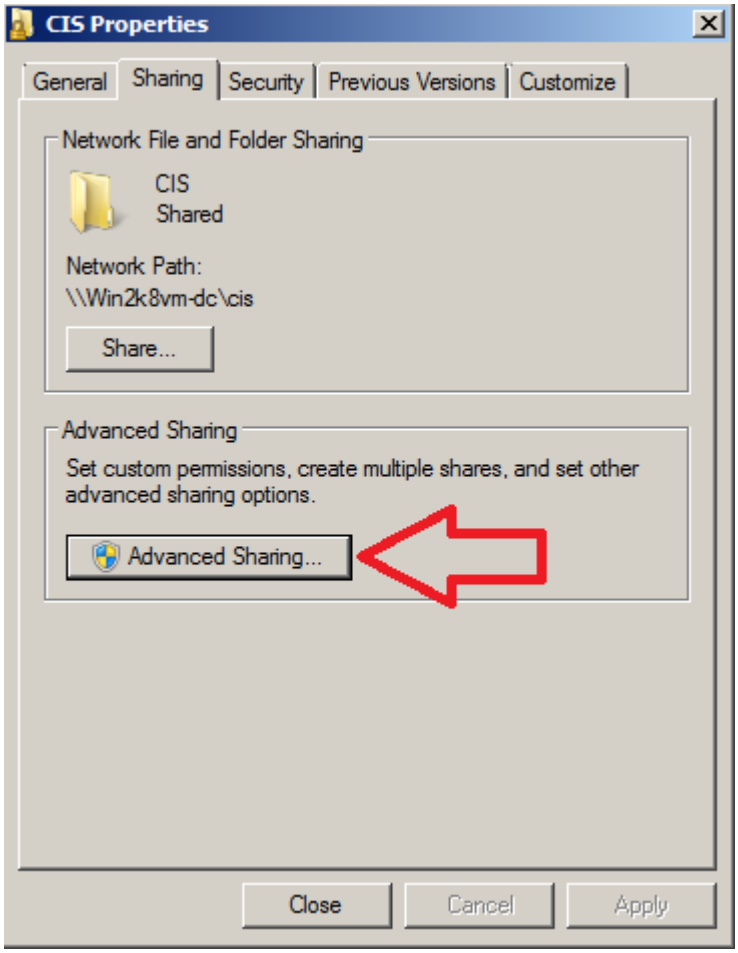
Perform the following steps to cause the *Workstations Group* to execute the CIS-CAT instance on the *CIS Host Server*.

Create CIS Share on the CIS Hosting Server

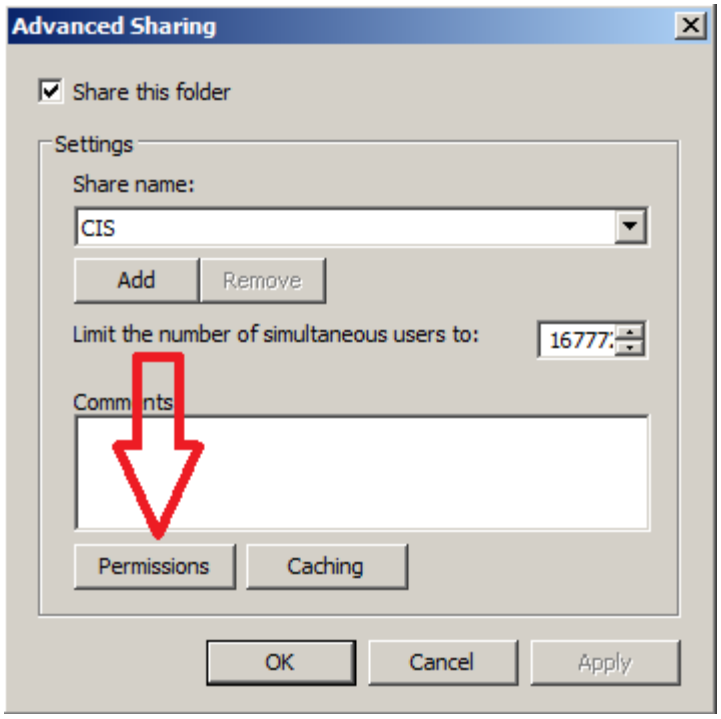
1. Create a shared folder on the *CIS Host Server* named CIS.

   Share permissions on the CIS folder should allow the `Authenticated Users` group the ability to both **Read** and **Change** information in the folder.

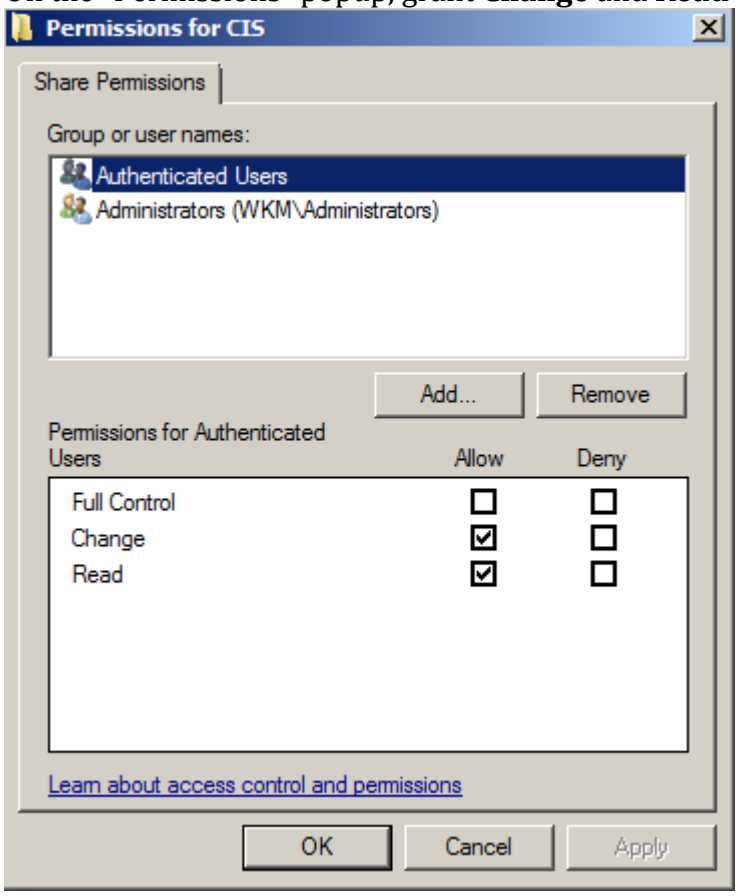
   To configure the permissions on the CIS share, right-click on the CIS folder and select "Properties". Click on the "Sharing" tab, and select "Advanced Sharing":



   From the "Advanced Sharing" popup, select "Permissions":



On the "Permissions" popup, grant **Change** and **Read** to the `Authenticated Users` group:



2. Unzip the CIS-CAT bundle within the CIS folder on the *CIS Host Server.*
3. Create the following directories beneath the CIS folder on the *CIS Host Server*:
    a. Java
    b. Java64
    c. Reports

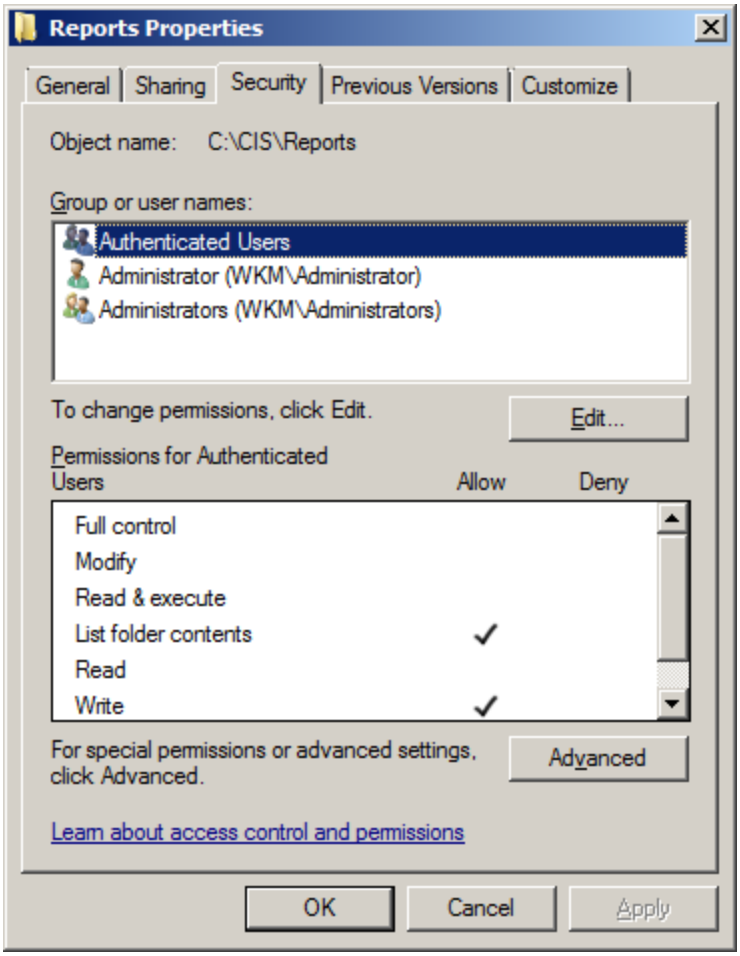
4. To copy the java runtime (JRE) to the CIS folder do the following:
    a. Browse to the location where Java is installed, by default Java is located at "%ProgramFiles%\Java".
    b. Copy the 32-bit JRE that applies to the targets you will be evaluating, such as `jre1.6.0_45`, to the `Java` folder you created in step 3.
    c. Copy the 64-bit JRE that applies to the targets you will be evaluating, such as `jre1.6.0_45`, to the `Java64` folder you created in step 3.
5. Move `CIS\cis-cat-full\misc\Windows\cis-cat-centralized.bat` to the root of the CIS folder.
6. Share the CIS folder as `CIS`.

The resulting directory structure will be as follows:

- `CIS\cis-cat-full`
- `CIS\cis-cat-full\CISCAT.jar`
- `CIS\cis-cat-full\benchmarks`
- `CIS\cis-cat-full\lib`
- `CIS\cis-cat-full\misc`
- `CIS\cis-cat-full\docs`
- `CIS\cis-cat-centralized.bat`
- `CIS\Java`
- `CIS\Java64`
- `CIS\Reports`

Security Considerations

The `CIS\Reports` folder will contain reports that detail configuration related vulnerabilities for each system evaluated by CIS-CAT. As such, "Authenticated Users" should only be granted "Write" and "List Folder Contents" access to the contents of this folder, and read access to the `CIS\Reports` folder should be restricted to only those personnel who are necessary to the appropriate functioning of the *CIS Host Server*:



Permissions which should be applied within the `CIS` folder on the *CIS Host Server*:

File or Folder	Permissions
CIS	Permissions on the shared folder
CIS\cis-cat-centralized.bat	**Execute** to "`Authenticated Users`"
CIS\cis-cat-full (folder)	**List Folder Contents**, **Read**, and **Read & Execute** to "`Authenticated Users`"
CIS\Java (folder)	**Read** and **Read & Execute** to "`Authenticated Users`"
CIS\Java64 (folder)	**Read** and **Read & Execute** to "`Authenticated Users`"
CIS\Reports (folder)	**List Folder Contents** and **Write** to "`Authenticated Users`"

Additionally, Write, Modify, Read and Execute permissions on the above resources should be limited to only those users necessary to the appropriate functioning of the CIS Host Server.

Update cis-cat-centralized.bat

Once the CIS folder is setup on the *CIS Hosting Server,* a few modifications must be made to `cis-cat-centralized.bat`:

```
SET NetworkShare=\\CisHostServer\CIS
```

Replace `CisHostServer` with the fully qualified domain name or IP address of the *CIS-CAT Host Server*.

```
SET JavaPath=Java\jre
```

```
SET JavaPath64=Java64\jre
```

Note that the 32-bit and 64-bit JRE paths are those installed in step 4 under Create CIS Share on the CIS Hosting Server.

```
SET JavaMaxMemoryMB=768
```

Indicate the maximum amount of memory CIS-CAT will allocate for execution. The default is 768 MB. When executing with 32-bit versions of the JRE, this value can be set to a maximum of 2048 MB. 64-bit JRE's may allocate as much memory as is required, limited by the available memory of machines invoking CIS-CAT.

```
SET CisCatPath=cis-cat-full
```

Set the CisCatPath value to the location, relative to the network share, of the installed version of CIS-CAT. For example, the value above indicates the path to CIS-CAT is `\\CisHostServer\CIS\cis-cat-full`.

```
SET ReportsPath=Reports
```

Set the ReportsPath value to the location, relative to the network share, of the folder to which CIS-CAT reports are written. For example, the value above indicates `\\CisHostServer\CIS\Reports` as the location to which reports are written.

```
SET CISCAT_OPTS=-x -t -csv
```

Finally, set the various reporting options to be used when launching CIS-CAT.

- `-x` indicates generation of the CIS-CAT XML report,
- `-t` indicates generation of the CIS-CAT Text report,
- `-csv` indicates generation of the CIS-CAT CSV report,
- `-n` indicates that CIS-CAT should NOT generate an HTML report.

Configuration Note: The "cis-cat-centralized.bat" script sets local environment variables denoting file system paths and folder names. CIS recommends, for simplicity, that these paths do not contain spaces, as without modification to the script, spaces in paths can cause unexpected behavior.

Near line 610 of the "cis-cat-centralized.bat" script, the following code section illustrates the configuration of the CIS-CAT command-line for execution.

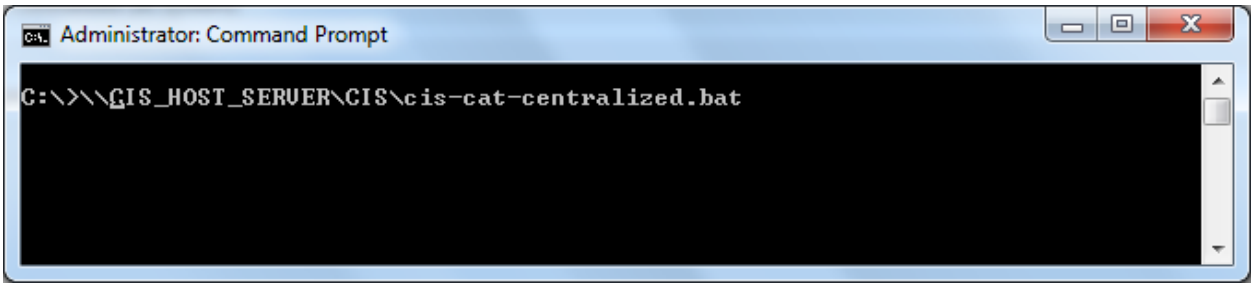
```
::
:: Put all the options together and form the CIS-CAT command-line
::
:: When using the timed version of CIS-CAT, the benchmarks are stored in the jar,
:: so the path to the benchmark needs to indicate the resource path, for example
:: /benchmarks/%Benchmark%
:: SET FULL_CISCAT_CMD=%mJavaPath%\bin\java.exe -Xmx%JavaMaxMemoryMB%M -jar
::  %mCisCatPath%\CISCAT.jar -a -s %CISCAT_OPTS% -b /benchmarks/%Benchmark%
::
IF %TIMED%==1 (
      SET FULL_CISCAT_CMD=%mJavaPath%\bin\java.exe -Xmx%JavaMaxMemoryMB%M -jar
%mCisCatPath%\CISCAT.jar -a -s %CISCAT_OPTS% -b /benchmarks/%Benchmark%
) ELSE (
      SET FULL_CISCAT_CMD=%mJavaPath%\bin\java.exe -Xmx%JavaMaxMemoryMB%M -jar
%mCisCatPath%\CISCAT.jar -a -s %CISCAT_OPTS% -b %mCisCatPath%\benchmarks\%Benchmark%
)
```

When spaces are included in any path names for environment variables, they must be surrounded with quotes to enable the full path to be discovered, for example:

```
SET FULL CISCAT CMD="%mJavaPath%\bin\java.exe" -Xmx%JavaMaxMemoryMB%M -jar
"%mCisCatPath%\CISCAT.jar" -a -s %CISCAT_OPTS% -b
"%mCisCatPath%\benchmarks\%Benchmark%"
```

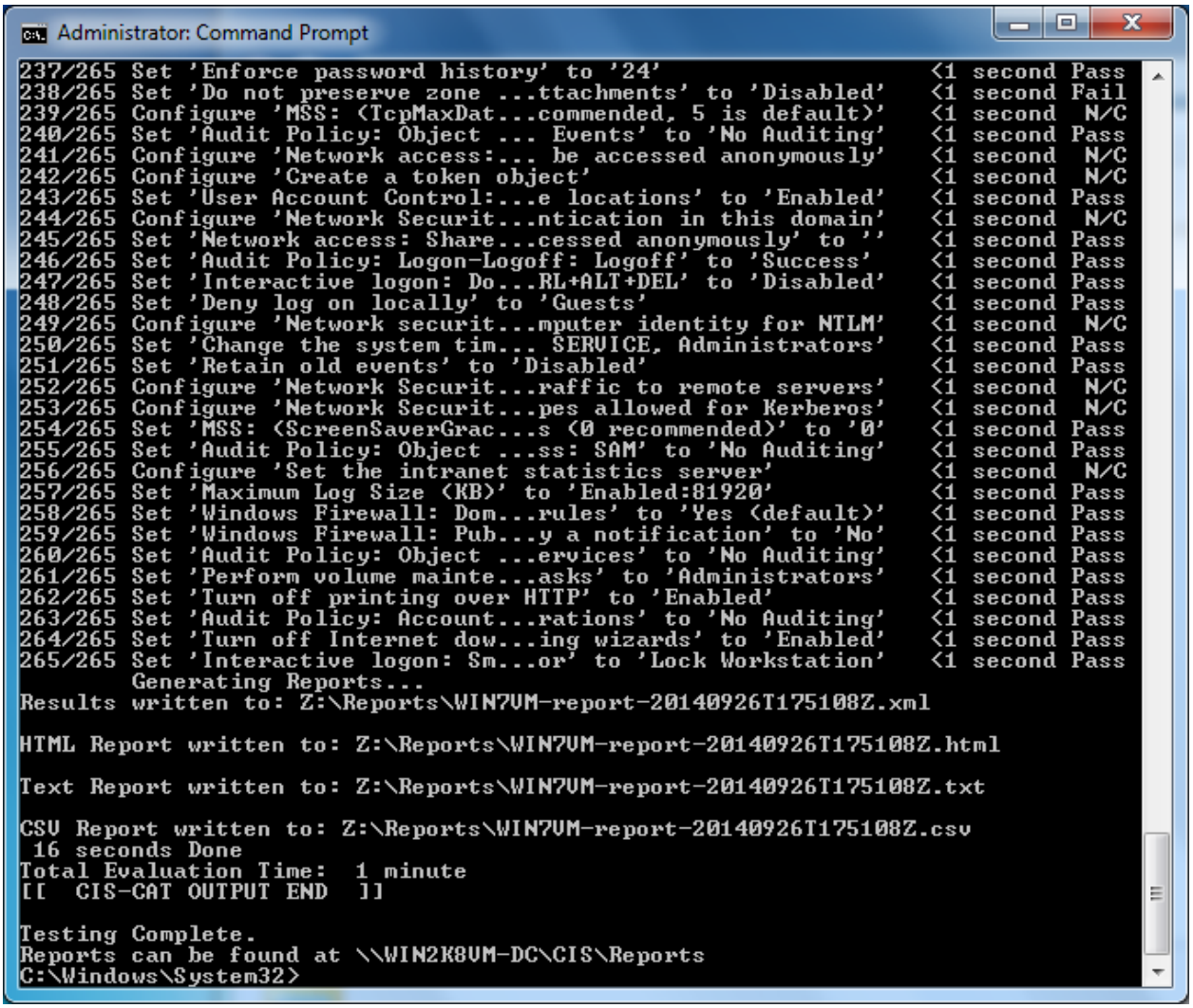
Validate the Install

To test the setup, log into one of the target systems in the *Workstation Group* as a user capable of executing commands from an elevated command prompt, such as a domain admin. Execute the following command ***from an elevated command prompt:***



Note that the "CIS_HOST_SERVER" value should be substituted with the actual name or IP of the machine configured as the *CIS Host Server*.

If successful, the above command will result in the following output:

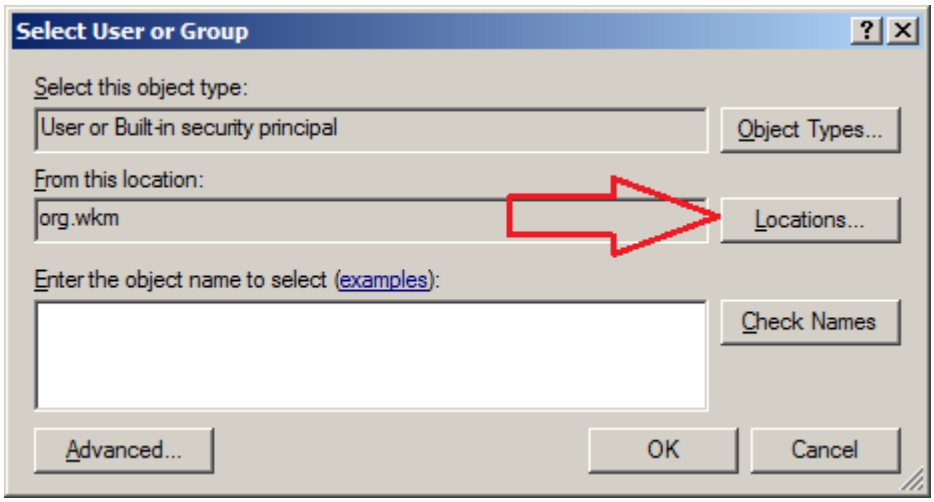


Configuring the Scheduled Task via Group Policy

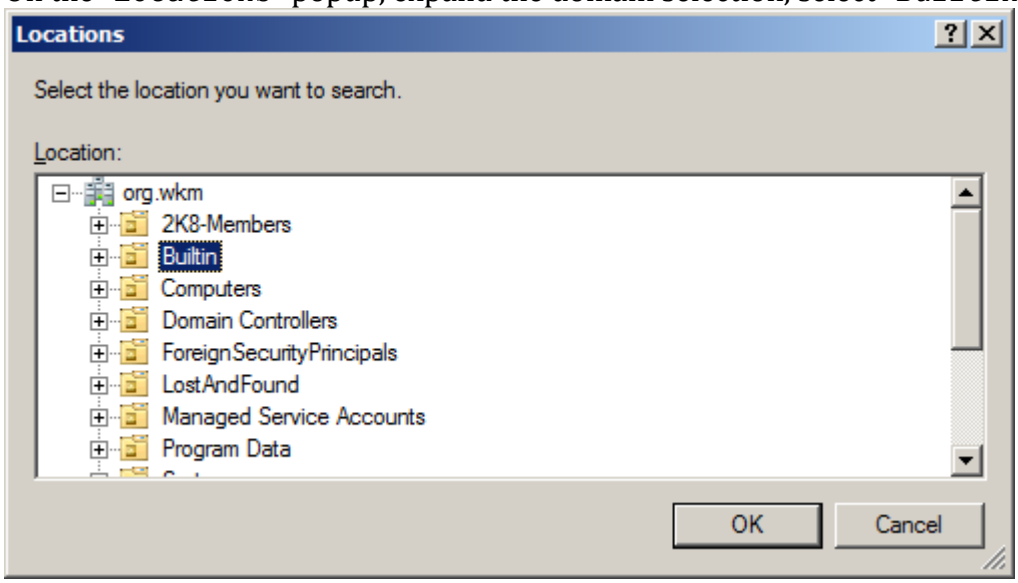
Perform the following steps to create and assign a Group Policy that will cause target systems in the *Workstation Group* to execute CIS-CAT via a Scheduled Task.

1. Run `gpmc.msc` to modify the group policy
2. Select a group policy that is already targeted towards the computers that CIS-CAT needs to scan or create a new policy.
3. Next create the scheduled task so go to `Computer Configuration -> Preferences -> Control Panel Settings -> Scheduled Tasks` once there click on `Action -> New -> Scheduled Task (Windows Vista and Later)`. Fill in the name of the task.

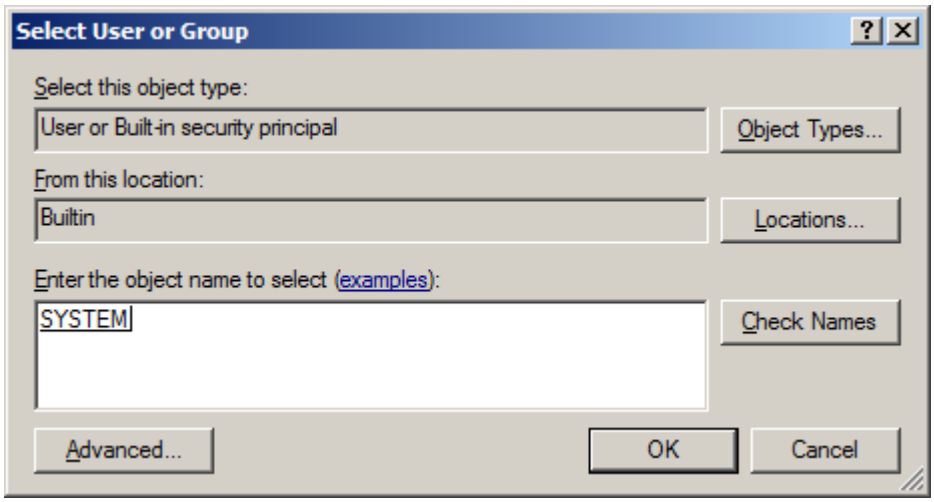
4. When setting the user who will be running the task, click the "`Change User or Group`" button, and click the "`Locations`" button on the "`Select User or Group`" popup:



5. On the "`Locations`" popup, expand the domain selection, select "`Builtin`" and click `OK`:

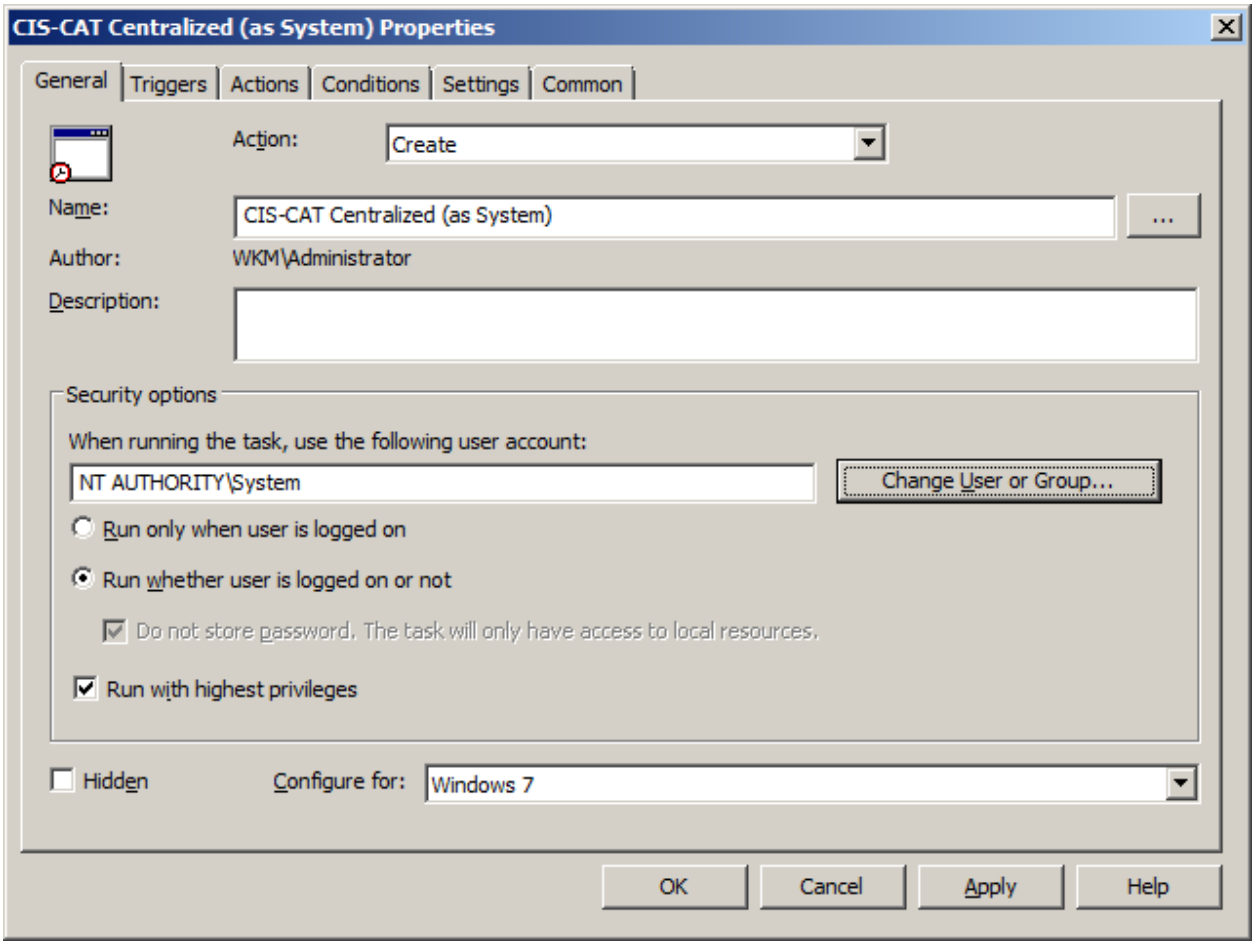


6. Returning to the "`Select User or Group`" window, enter "`SYSTEM`" in the "`Enter the object name to select`" box, and click the "`Check Names`" button. Select "`OK`" to select the `SYSTEM` user:



When returned to the scheduled task window, the "NT AUTHORITY\System" user should be indicated in the "When running the task, use the following user account" box.

7. Ensure the "Run whether user is logged on or not" radio button is selected, and make sure "Run with highest privileges" is checked. It should look similar to the below screen shot. Note that the "Do not store password. The task will only have access to local resources." checkbox will automatically be checked and disabled. The inability to store credentials in the scheduled task is the result of applying the patch for Microsoft security update MS14-025.

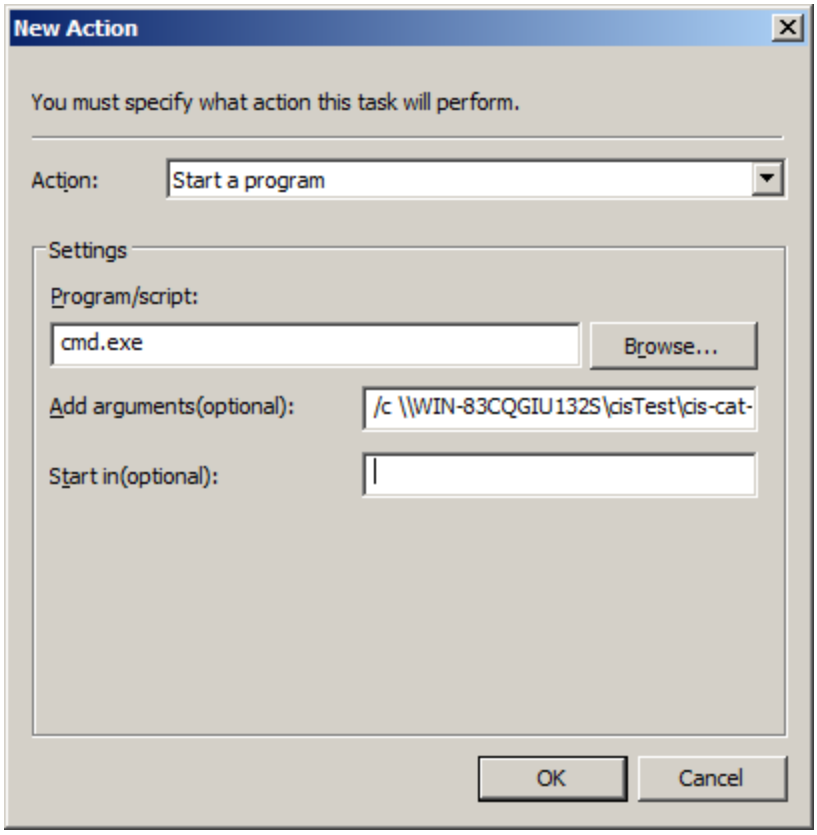


Add in whatever scheduling is needed via the Triggers tab. Then go to the Actions tab click New and specify the following settings:

- Set the Action drop down to Start a program
- Set Program/script to cmd.exe
- Set Add arguments(optional) to the following value:

```
/c \\<CisHostServer>\CIS\cis-cat-centralized.bat
```

Once these steps are implemented, the New Action Dialog will look as follows:



CIS-CAT is now scheduled to run on all computers that are associated with the group policy.

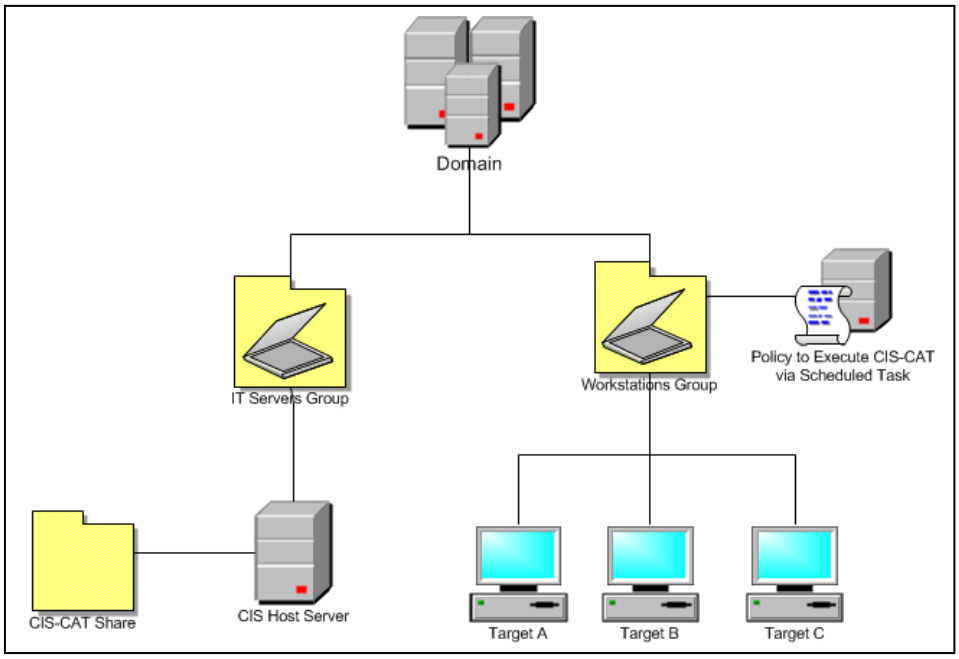
CIS-CAT reports will be stored at the folder location configured in your web server settings. Using the CIS XML Reports, it is possible to create a CIS-CAT Dashboard that provides a visual representation of your environments configuration posture over time.

Bandwidth Considerations

Through the deployment and testing of the CIS-CAT Centralized workflow, bandwidth utilization can reach approximately 300 MB of data for each machine invoking CIS-CAT. This bandwidth utilization is the cost of invoking CIS-CAT over the network.

Using the CIS-CAT Dissolvable Agent

It is possible to assess a population of Microsoft Windows targets in an automated manner by temporarily installing CIS-CAT and a compatible JRE on each target, executing the assessment, uploading the generated reports, and finally removing CIS-CAT. Using this "dissolvable agent" deployment pattern utilizes approximately 80MB of network bandwidth per target which, depending on member network bandwidth, would significantly reduce the amount of network traffic generated while running CIS-CAT. The following diagram depicts this deployment pattern, which is very similar in its architecture to the "centralized" CIS-CAT deployment in the previous section(s):



CIS Host Server

The *CIS Host Server* is where the CIS-CAT bundle (including a Java Runtime Environment), the unzipping utility, and Reports are placed. Targets within the `Workstations Group` will access these resources to perform a self-assessment using CIS-CAT.

Workstations Group

The *Workstations Group* represents a population of Microsoft Windows targets to be assessed with CIS-CAT. The Domain Administrator will create Group Policy that causes devices in this group to invoke CIS-CAT via a Scheduled Task.

Notice

Microsoft security bulletin MS14-025 notifies Windows users of a vulnerability in Group Policy Preferences which could allow elevation of privileges. Once the appropriate patch has been installed on the various systems, scheduled tasks are no longer allowed to store passwords, because the password was stored insecurely.

In order to address this patch, the "Using the CIS-CAT Dissolvable Agent" workflow required modification. The scheduled task configured by this process can no longer store the credentials of the *CIS-CAT Domain User*, and in order to maintain a secure configuration of the *CIS Host Server*, authenticated users should only be allowed to execute the "cis-cat-dissolvable.bat" file.

Prerequisites

1. All targets must be joined to an Active Directory Domain
2. All targets must have read access to the *CIS-CAT Share* hosted off of the *CIS Host Server*

Setup

Perform the following steps to cause the *Workstations Group* to execute the CIS-CAT instance on the *CIS Host Server*.

Create CIS Share on the CIS Hosting Server

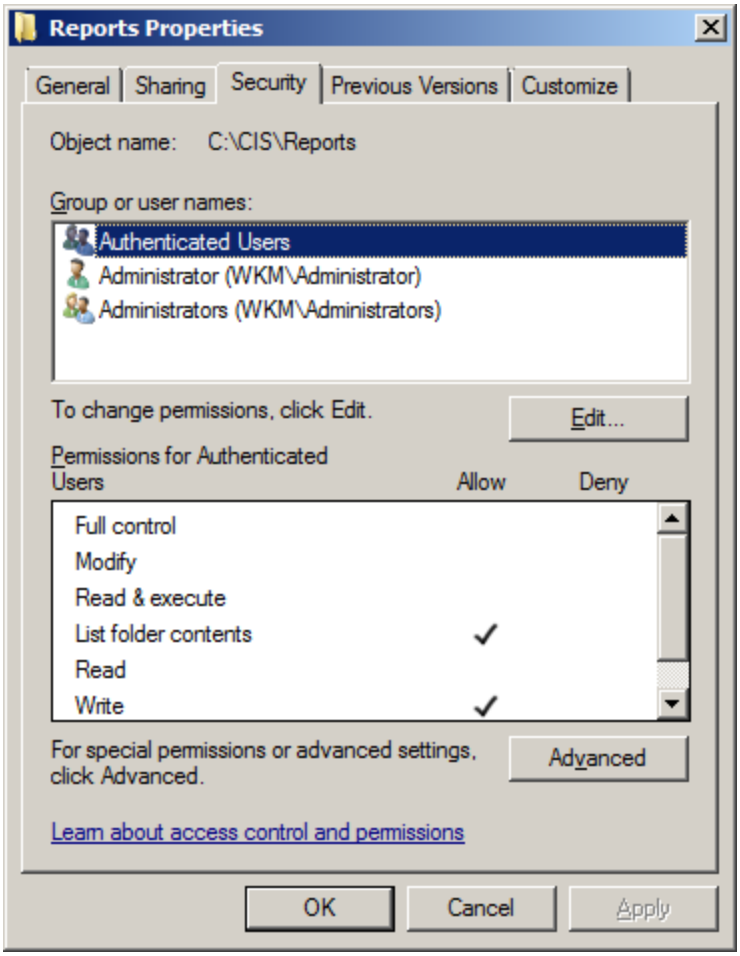
1. Create a shared folder on the *CIS Host Server* named CIS.
2. Unzip the CIS-CAT dissolvable bundle within the CIS folder on the *CIS Host Server.*
3. Create the following directory beneath the CIS folder on the *CIS Host Server*:
    a. Reports
4. Share the CIS folder as `CIS`.

The resulting directory structure will be as follows:

- `CIS\cis-cat-dissolvable.bat`
- `CIS\cis-cat-dissolvable.zip`
- `CIS\unzip.exe`
- `CIS\Reports`

Security Considerations

The `CIS\Reports` folder will contain reports that detail configuration related vulnerabilities for each system evaluated by CIS-CAT. As such, "Authenticated Users" should only be granted "Write" and "List Folder Contents" access to the contents of this folder, and read access to the `CIS\Reports` folder should be restricted to only those personnel who are necessary to the appropriate functioning of the *CIS Host Server*:



Permissions which should be applied within the `CIS` folder on the *CIS Host Server*:

File or Folder	Permissions
CIS	**List Folder Contents** to "`Authenticated Users`"
CIS\cis-cat-dissolvable.bat	**Execute** and **Read & Execute** to "`Authenticated Users`"
CIS\cis-cat-dissolvable.zip	**Read** to "`Authenticated Users`"
CIS\unzip.exe	**Execute** and **Read & Execute** to "`Authenticated Users`"
CIS\Reports (folder)	**List Folder Contents** and **Write** to "`Authenticated Users`"

Additionally, Write, Modify, Read and Execute permissions on the above resources should be limited to only those users necessary to the appropriate functioning of the *CIS Host Server*.

Update cis-cat-dissolvable.bat

Once the CIS folder is setup on the *CIS Hosting Server,* a few modifications must be made to `cis-cat-dissolvable.bat`:

```
SET RootDir=%TEMP%
```

The `RootDir` value should be set to a valid temporary directory into which the CIS-CAT files can be copied. By default this is set to the %TEMP% environment variable. Any valid directory in which the user executing the script has permissions, may be used. If the `RootDir` does not resolve to a valid directory, the script will not execute.

```
SET NetworkShare=\\CisHostServer\CIS
```

Replace `CisHostServer` with the fully qualified domain name or IP address of the *CIS-CAT Host Server*.

```
SET JavaMaxMemoryMB=768
```

Configure the maximum heap size to be allocated by the JRE, in Megabytes

```
SET CISCAT_OPTS=-x -t -csv
```

Configure CIS-CAT report generation options:

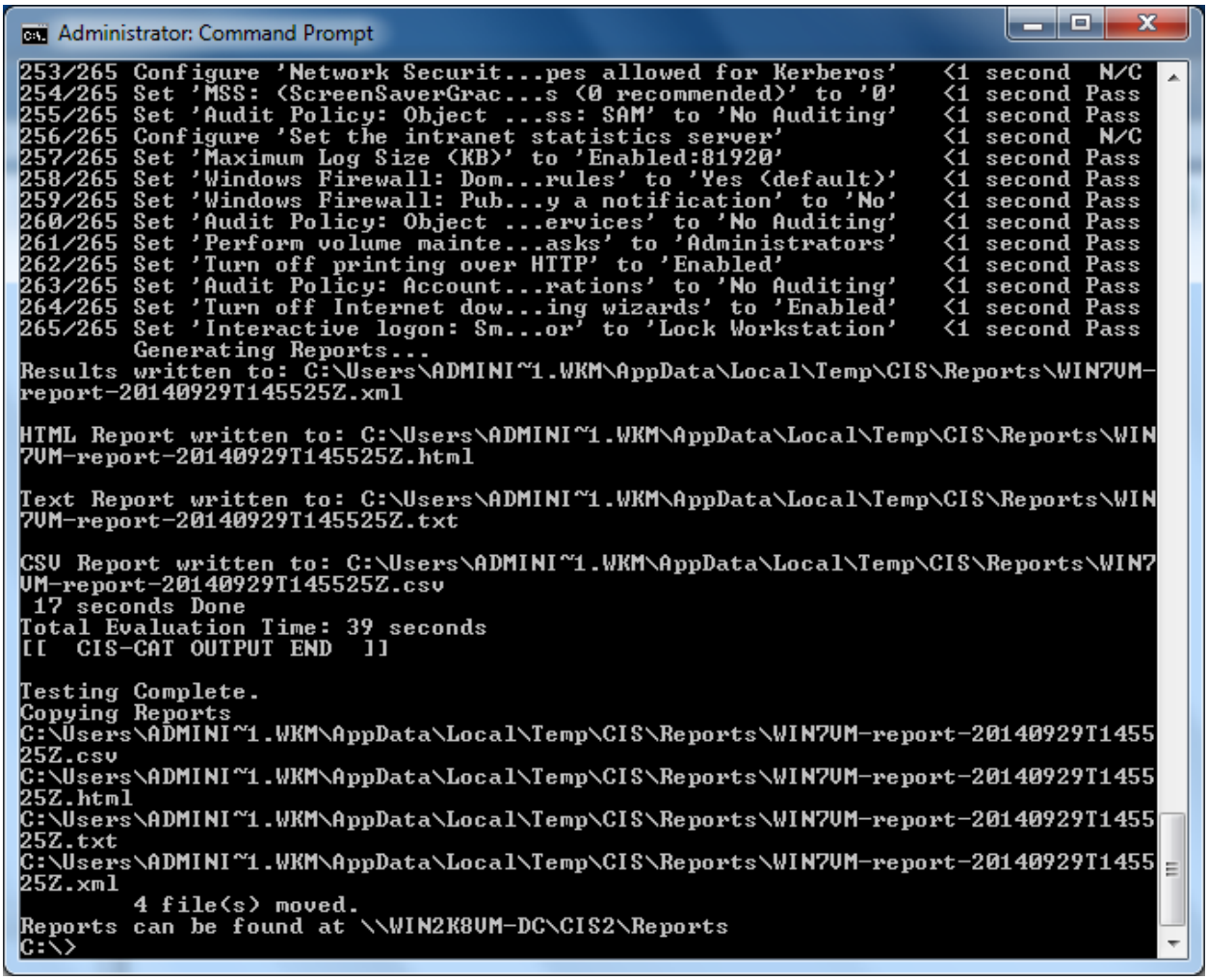
- `-x` : Generate an XML report
- `-t` : Generate a Text report
- `-csv` : Generate a CSV report
- `-y` : Causes the HTML and Text reports to display all tests (default is only applicable tests)
- `-n` : Do NOT generate an HTML report

Validate the Install

To test the setup, log into one of the target systems in the *Workstation Group* as a user capable of executing commands from an elevated command prompt, such as a domain admin. Execute the following command ***from an elevated command prompt:***

Note that the "`CIS_HOST_SERVER`" value should be substituted with the actual name or IP of the machine configured as the *CIS Host Server*.

If successful, the above command will result in the following output:



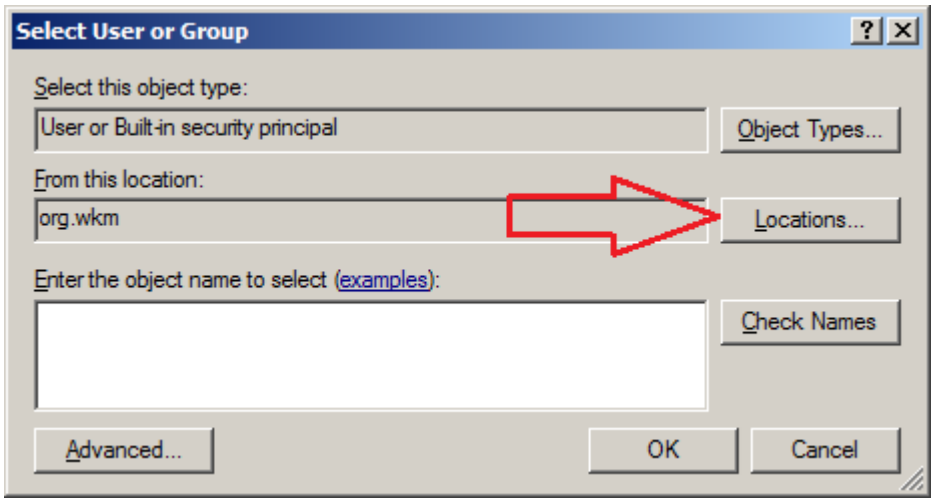
Configuring the Scheduled Task via Group Policy

Perform the following steps to create and assign a Group Policy that will cause target systems in the *Workstation Group* to execute CIS-CAT via a Scheduled Task.

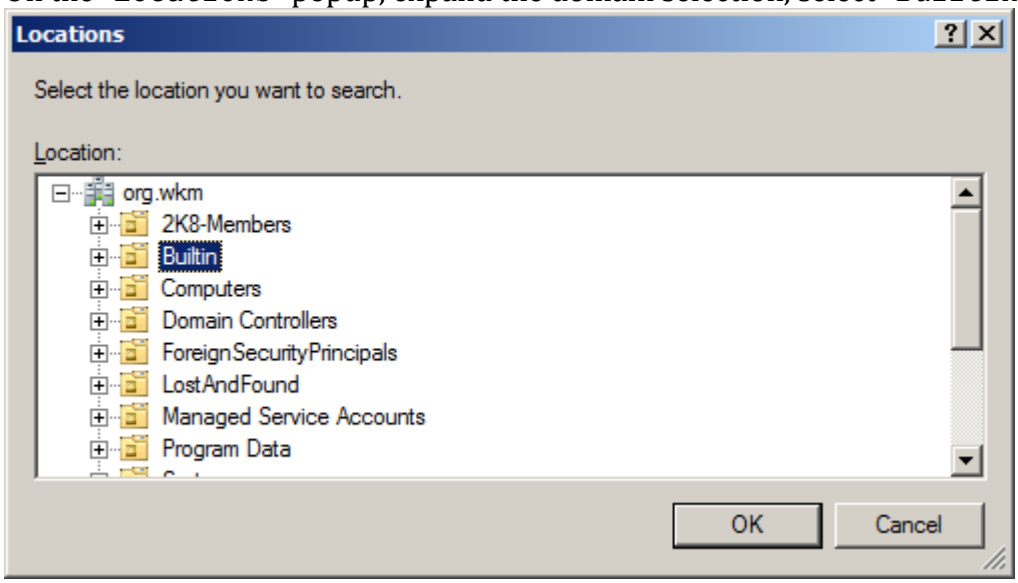
1. Run `gpmc.msc` to modify the group policy
2. Select a group policy that is already targeted towards the computers that CIS-CAT needs to scan or create a new policy.

3. Next create the scheduled task so go to `Computer Configuration -> Preferences -> Control Panel Settings -> Scheduled Tasks` once there click on `Action -> New -> Scheduled Task (Windows Vista and Later)`. Fill in the name of the task.

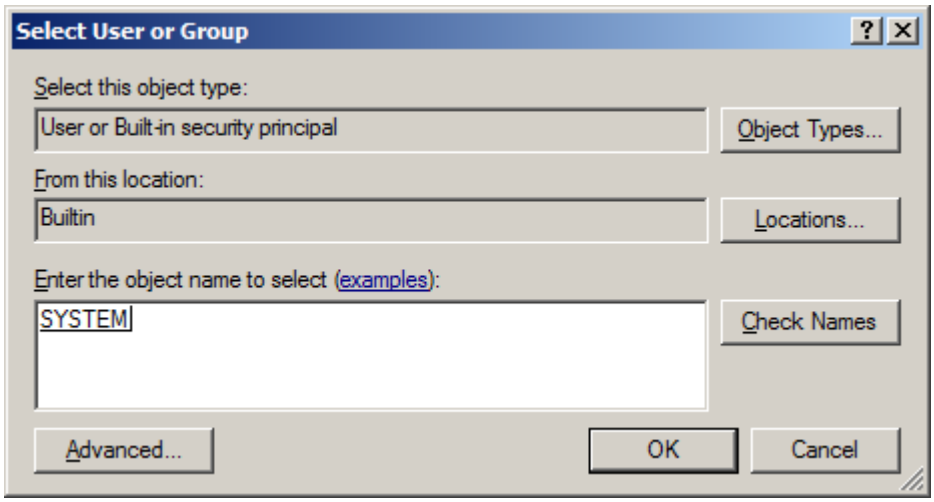
4. When setting the user who will be running the task, click the "`Change User or Group`" button, and click the "`Locations`" button on the "`Select User or Group`" popup:



5. On the "`Locations`" popup, expand the domain selection, select "`Builtin`" and click `OK`:

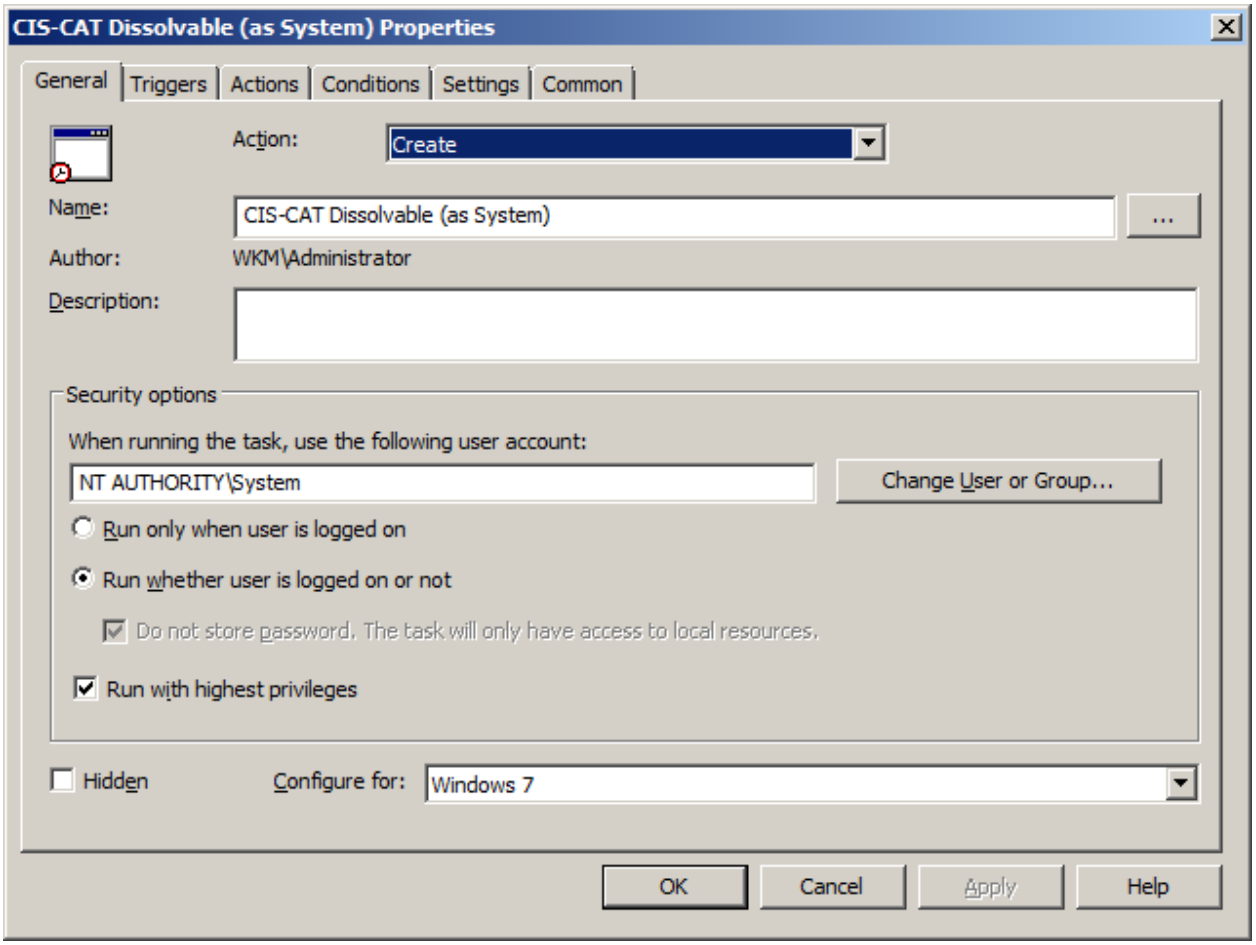


6. Returning to the "`Select User or Group`" window, enter "`SYSTEM`" in the "`Enter the object name to select`" box, and click the "`Check Names`" button. Select "`OK`" to select the `SYSTEM` user:



When returned to the scheduled task window, the "NT AUTHORITY\System" user should be indicated in the "When running the task, use the following user account" box.

7. Ensure the "Run whether user is logged on or not" radio button is selected, and make sure "Run with highest privileges" is checked. It should look similar to the below screen shot. Note that the "Do not store password. The task will only have access to local resources." checkbox will automatically be checked and disabled. The inability to store credentials in the scheduled task is the result of applying the patch for Microsoft security update MS14-025.

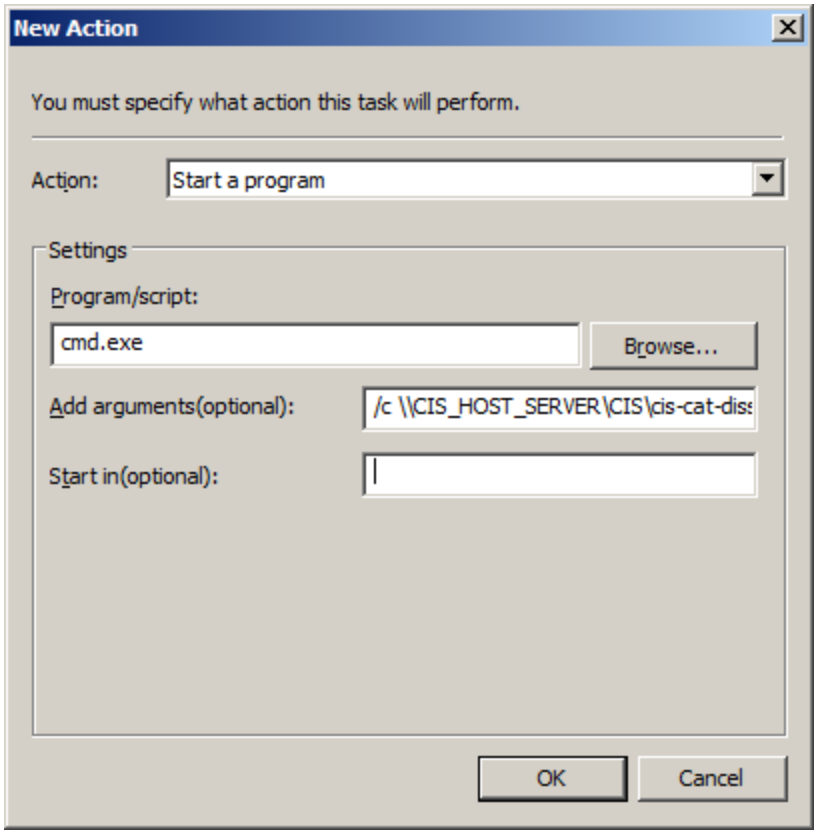


Add in whatever scheduling is needed via the Triggers tab. Then go to the Actions tab click New and specify the following settings:

- Set the Action drop down to Start a program
- Set Program/script to cmd.exe
- Set Add arguments(optional) to the following value:

```
/c \\<CisHostServer>\CIS\cis-cat-dissolvable.bat
```

Once these steps are implemented, the New Action Dialog will look as follows:



The CIS-CAT dissolvable agent is now scheduled to run on all computers that are associated with the group policy.

CIS-CAT reports will be stored `\\<CisHostServer>\CIS\Reports`. Using the CIS XML Reports, it is possible to create a CIS-CAT Dashboard that provides a visual representation of your environments configuration posture over time.

Bandwidth Considerations

Through the deployment and testing of the CIS-CAT Dissolvable workflow, bandwidth utilization can reach approximately 85-90 MB of data for each machine invoking CIS-CAT. This bandwidth is the "up-front cost" of the network traffic involved in downloading the dissolvable bundle from the CIS Host Server to each target machine.

Assessing Multiple Unix/Linux Targets

Similar to the "Assessing Multiple Windows Targets" section above, it is possible to assess multiple Unix, Linux, MacOS, Debian, Solaris, SUSE, etc targets in an automated manner without installing CIS-CAT or the JRE on each target. The `cis-cat-centralized.sh` script is intended to reside on a centralized file share that is accessible by the computers to be assessed by CIS-CAT.

CIS Host Server

The *CIS Host Server* is where the CIS-CAT bundle (including the various Java Runtime Environments), and Reports are placed. Configured target machines will access these resources to perform a self-assessment using CIS-CAT.

Using the default configuration, consider the root folder for this workflow is at `/cis`. The first setup step is to copy the required scripts to the root folder. The four scripts which are required reside in the `misc/Unix-Linux` folder of a CIS-CAT installation bundle:

1. cis-cat-centralized.sh
2. detect-os-variant.sh
3. make-jre-directories.sh
4. map-to-benchmark.sh

Once the four required scripts have been copied to the workflow's root folder, the default configuration of the folder structure should be as follows:

```
/cis

/cis/cis-cat-centralized.sh   <-- Copied from misc/Unix-Linux
/cis/detect-os-variant.sh     <-- Copied from misc/Unix-Linux
/cis/make-jre-directories.sh  <-- Copied from misc/Unix-Linux
/cis/map-to-benchmark.sh      <-- Copied from misc/Unix-Linux

/cis/cis-cat-full
/cis/cis-cat-full/CISCAT.jar
...
/cis/reports
/cis/jres
/cis/jres/AIX
/cis/jres/AIX/bin/java
...
/cis/jres/Debian
/cis/jres/HPUX
/cis/jres/Linux
/cis/jres/OSX
/cis/jres/RedHat
/cis/jres/Solaris
/cis/jres/SolarisSparc
/cis/jres/SUSE
```

Configuring the JRE sub-folders

The "cis-cat-centralized.sh" script is configured with an option to create the "jres" subfolder and all OS-specific folders underneath it:

```
/cis> ./cis-cat-centralized.sh --make-jre-directories
```

This command will create the jres/* directories, but those folders will not contain the actual JRE's appropriate for those OS'. Various URL's are contained within the script detailing locations from which appropriate JRE's may be downloaded.

Configuring Environment Variables

Once the JRE folders have been created, and applicable JRE's have been downloaded and installed in their respective /jres/* folder, three environment variables must be configured to align with the target-facing file structure.

```
CISCAT_DIR=/cis/cis-cat-full
REPORTS_DIR=/cis/reports
JRE_BASE=/cis/jres
```

Profile Configuration

The "cis-cat-centralized.sh" script can be configured to execute either the "Level 1" or "Level 2" profile (if available), based on an environment variable value. This variable is named SSLF, and may be set to either 0 or 1. Setting the value to 1 results in CIS-CAT evaluating the "Level 2" profile.

```
SSLF='1'
```

Validate the Install

In order to test the proper installation of the "cis-cat-centralized.sh" script, log into one of the target systems in the environment as either a root user or a user capable of executing commands using sudo. Execute the following command, where /path/to/cis represents a file system path to the CIS Host Server:

```
> /path/to/cis/cis-cat-centralized.sh
```

If the path is correct, and all environment variables are configured correctly, output will be displayed similar to the following:

```
Detected OS as RedHat 7.0
Using JRE located at '/path/to/cis/jres/RedHat/bin/java'
Using CISCAT located at '/path/to/cis/cis-cat-full/CISCAT.jar'
Using Benchmark '/path/to/cis/cis-cat-
full/benchmarks/CIS_Red_Hat_Enterprise_Linux_7_Benchmark_v1.0.0-xccdf.xml'
Using Profile 'Level 2'
Storing Reports at '/path/to/cis/reports'
```

This would be followed by standard status information presented to the user during the assessment.

CIS-CAT reports will be stored at `/path/to/cis/reports`. Using the CIS XML Reports, it is possible to create a CIS-CAT Dashboard that provides a visual representation of your environments configuration posture over time.

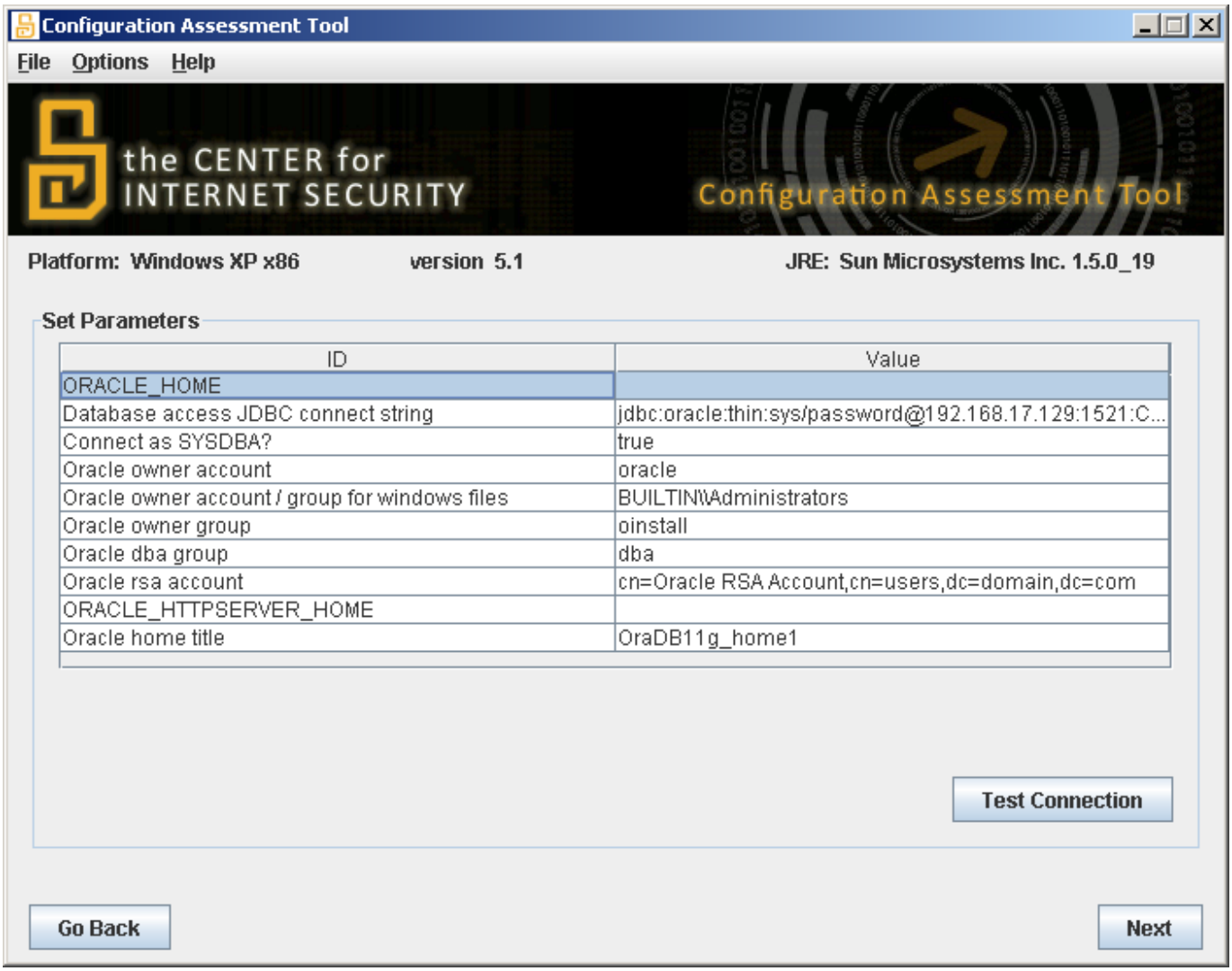
CIS-CAT users can now integrate the invocation of the "cis-cat-centralized.sh" script into a task scheduling system such as `cron`, to be executed on any schedule deemed prudent for organizational needs. Configuration of a Unix/Linux-based scheduling tool is beyond the scope of this User's Guide.

Using CIS-CAT with Database Benchmarks

Oracle Database Support

When using CIS' Oracle Database benchmarks it is recommended you connect to the database server with an account that has SYSDBA privileges. The reason for this is that some checks will require these privileges. If it is not possible to connect to the database with SYSDBA privileges the checks that do not have sufficient permissions will be marked with an `error` instead of `pass` or `fail`.

To run CIS-CAT with SYSDBA privileges in the connection string use an account SYSDBA privileges (i.e. `sys`) and then set the `Connect as SYSDBA?` parameter to `true`. It should look similar to the below screen shot.



Once the parameters are set continue running the CIS-CAT scan like normal. Below is a description of the parameters:

1. The `ORACLE_HOME` parameter corresponds with the Oracle Database server's `ORACLE_HOME` environment variable. CISCAT will attempt to populate this value from the environment. For more information on the `ORACL_HOME` variable, see

http://docs.oracle.com/cd/E11857_01/em.111/e12255/oui2_manage_oracle_homes.htm

2. The JDBC string parameter is the connection string used to connect to and authenticate to the Oracle Database service and instance that CIS-CAT will assess. The Oracle JDBC driver has the ability to connect to Oracle database instances using either the SID or Service Name.

    a. When to a database using the Oracle SID:

```
jdbc:oracle:thin:[username]/[password]@[hostname]:[port]:[SID]

For Example:
jdbc:oracle:thin:sys as sysdba/pa55w0rd!@servername:1521:ORCL
```

    b. When connecting to a database using the Oracle Service Name:

```
jdbc:oracle:thin:[username]/[password]@//[hostname]:[port]/[service_name]

For Example:
jdbc:oracle:thin:sys as sysdba/pa55w0rd!@//servername:1521/SERVICE_NAME
```

The following components of the JDBC string must be changed in order for CISCAT to successfully connect to the Oracle instance:

Property Name	Property Description
Username	A valid username who can connect to the database instance.
Password	The credentials for the user to connect to the database
Hostname	The name of the server (or its IP address) hosting the database
Port	The port number on which the database is listening. The default Oracle port number is 1521
SID	The database SID
Service Name	The database Service Name

3. The `Connect as SYSDBA` parameter determines if CISCAT will connect to the Oracle instance with the SYSDBA privilege. This is required for CISCAT to accurately assess Oracle databases. Ensure this parameter is set to true. For more information on the AS SYSDBA directive, see http://asktom.oracle.com/pls/asktom/f?p=100:11:0::::P11_QUESTION_ID:6186627748045 0.

4. The `oracle owner account` parameter refers to the Linux user that the Oracle service was installed using. This user typically owns the file system resources associated with the Oracle installation. I.e. "oracle".

5. The `oracle owner account / group for windows files` parameter refers to the Windows principal that the Oracle service was installed as. I.e. "oracle".

6. The `oracle owner group` parameter refers to the Linux group that the Oracle service was installed as. This group typically owns the file system resources associated with the Oracle installation. I.e. "oinstall".

7. The `oracle dba group` parameter refers to the Linux group that Oracle DBAs belong to. I.e "dba".

8. The `oracle rsa group` parameter refers to least privileged restricted service account (RSA) that the Oracle service executes as. This parameter is only applicable to Oracle on Windows.

9. The `ORACLE_HTTPSERVER_HOME` parameter corresponds with the Oracle Database server's `ORACLE_HTTPSERVER_HOME` environment variable. CISCAT will attempt to populate this value from the environment. For more information on the `ORACL_HOME` variable, see http://docs.oracle.com/cd/E10513_01/doc/install.310/e10496/db_install.htm

Further Database Support

Further database support is implemented in CIS-CAT using the OVAL `sql57_test`, `sql57_object`, and `sql57_state`.

The OVAL `sql57` constructs are used to check information stored in a database. Connection information is supplied via a JDBC connection string and a query is supplied to retrieve the desired information. Any valid SQL query is usable with one exception; ALL fields must be named in the SELECT portion of the query. For example, "`SELECT column1, column2 FROM table`" is valid, but "`SELECT * FROM table`" is NOT valid.

These OVAL constructs are supported in CIS-CAT content contained in XCCDF 1.2 benchmarks and SCAP 1.2 data streams. See the "Using CIS-CAT with SCAP Content" section for more information.

The most common technical issue users will face when implementing CIS-CAT assessments of database instances, is the construction of the JDBC connection string. Any valid JDBC URL supplied for a given database vendor is supported, and some common formats/examples are provided in the following sections. The following terminology and descriptions apply to the JDBC URL examples:

`<hostname>` – The hostname or IP address of the machine hosting the database instance.
`<port>` – The port number on which the database is listening.
`<instance>` – The name of the database instance being connected to.
`<username>` – The database user.
`<credential>` – The database user's credentials/password.
`<property>` – One of several properties which can be supplied in the JDBC URL
`<value>` – The assigned value of a named <property>

Microsoft SQL Server Database Support

Microsoft SQL Server database support is implemented using the jTDS open source JDBC driver. The jTDS driver provides support for SQL Server 6.5, 7, 2000, 2005, 2008, and 2012.

The format of the jTDS JDBC URL for MS SQL Server is:

```
jdbc:jtds:sqlserver://<server>[:<port>][/<database>][;<property>=<value>]
```

Properties required for the database connection can be provided as `<property>=<value>` pairs, separated by a semi-colon (;).

Consider a Microsoft SQL Server database instance with the following information:

Property Name	Property Value
Server Name	CIS-SERVER
Database Name	TestDB
Database Port	1433
Windows Domain	WIN-DOMAIN
Windows Domain User & Password	jsmith/qw3rty
SQL Server Database User & Password	db_user/db_pass
Instance Name	InstanceName

Windows Authentication Mode

Windows Authentication Mode allows a user to connect to a SQL Server instance through a Microsoft Windows user account. This mode allows domain user account information to be supplied in order to establish a connection. The following JDBC URL would be valid for establishing a connection using the above example information:

```
jdbc:jtds:sqlserver://CIS-SERVER:1433/TestDB;domain=WIN-
DOMAIN;user=jsmith;password=qw3rty;instance=InstanceName
```

Windows Authentication Mode may also be used against databases running on machines not joined to a domain (standalone servers). When authenticating with Microsoft Windows user accounts to non-domain joined servers, substitute in the computer name for the domain. For example, if the name of the standalone server is SQLSERVER, the JDBC URL would look as such:

```
jdbc:jtds:sqlserver://CIS-
SERVER:1433;DatabaseName=TestDB;domain=SQLSERVER;user=jsmith;password=qw3rty;instance
=InstanceName
```

NOTE: When connecting to a SQL Server using Windows Authentication, a common error message indicates that "the user is attempting to log in from an untrusted domain" (or similar message). In order to resolve this issue, add the `useNTLMv2=true` property/value:

```
jdbc:jtds:sqlserver://CIS-
SERVER:1433;DatabaseName=TestDB;domain=SQLSERVER;user=jsmith;password=qw3rty;instance
=InstanceName;useNTLMv2=true
```

SQL Server Authentication or Mixed Mode

SQL Server Authentication provides the ability for connections to a database instance to be made using trusted username and password information, allowing SQL Server to perform the authentication itself by checking to see if a SQL Server login account has been setup and if the password matches one previously recorded for that user. The following JDBC URLs would be valid for establishing a connection using the above example information:

```
jdbc:jtds:sqlserver://CIS-
SERVER:1433/TestDB;user=db_user;password=db_pass;instance=InstanceName
-or-
jdbc:jtds:sqlserver://CIS-
SERVER:1433;DatabaseName=TestDB;user=jsmith;password=qw3rty;instance=InstanceName
```

NOTES:

- The default port number for MS SQL Server databases is `1433`.

- The full set of connection properties supported by jTDS can be found at http://jtds.sourceforge.net/faq.html#urlFormat

Oracle MySQL Database Support

Oracle MySQL database support is implemented using the MariaDB JDBC driver. The MariaDB driver provides support for MySQL 5.6 in CIS-CAT.

The format of the MariaDB JDBC URL for MySQL is:

```
jdbc:mysql://<host>:<port>/<database>?<key1>=<value1>&<key2>=<value2>...
```

Consider a MySQL database instance with the following information:

Property Name	Property Value
Server Name	CIS-SERVER
Database Name	TestDB
Database Port	3306
Database Username	db_user
Database Credentials	db_pass

When configuring the JDBC URL information in CIS-CAT, the above connection information would be entered as:

```
jdbc:mysql://CIS-SERVER:3306/TestDB?user=db_user&password=db_pass
```

Notable optional URL parameters involve ensuring JDBC connections are made via SSL:

Property Name	Property Description
user	Database user name
password	Password of database user
useSSL	Force SSL on connection
trustServerCertificate	When using SSL, do not check server's certificate
serverSslCert	Server's certificate in DER form, or server's CA certificate. Can be used in one of 3 forms, serverSslCert=/path/to/cert.pem (full path to certificate), serverSslCert =classpath:relative/cert.pem (relative to current classpath), or as verbatim DER-encoded certificate string "------BEGING CERTIFICATE-----"

NOTES:

- The default port number for MySQL databases is `3306`.
- The full set of connection properties/optional URL parameters supported by MariaDB can be found at https://mariadb.com/kb/en/mariadb/about-the-mariadb-java-client/.

Sybase Database Support

Sybase Adaptive Server Enterprise database support is implemented using the jTDS open source JDBC driver. The jTDS driver provides support for Sybase Adaptive Server Enterprise 10, 11, 12, and 15.

The format of the jTDS JDBC URL for Sybase is:

```
jdbc:jtds:sybase://<hostname>[:<port>][/<instance>][;<property>=<value>]
```

NOTES:

- The default port number for Sybase databases is `7100`
- The full set of connection properties supported by jTDS can be found at http://jtds.sourceforge.net/faq.html#urlFormat

Using CIS-CAT with VMware Benchmarks

VMware ESXi 5.5 Support

CIS' support for assessments of VMware ESXi hosts is supported through developed interfaces with VMware PowerCLI. VMware PowerCLI contains snap-ins of cmdlets based on Microsoft PowerShell for automating ESXi and vSphere administration. It provides C# and PowerShell interfaces to VMware ESXi, which are leveraged in CIS-CAT assessments.

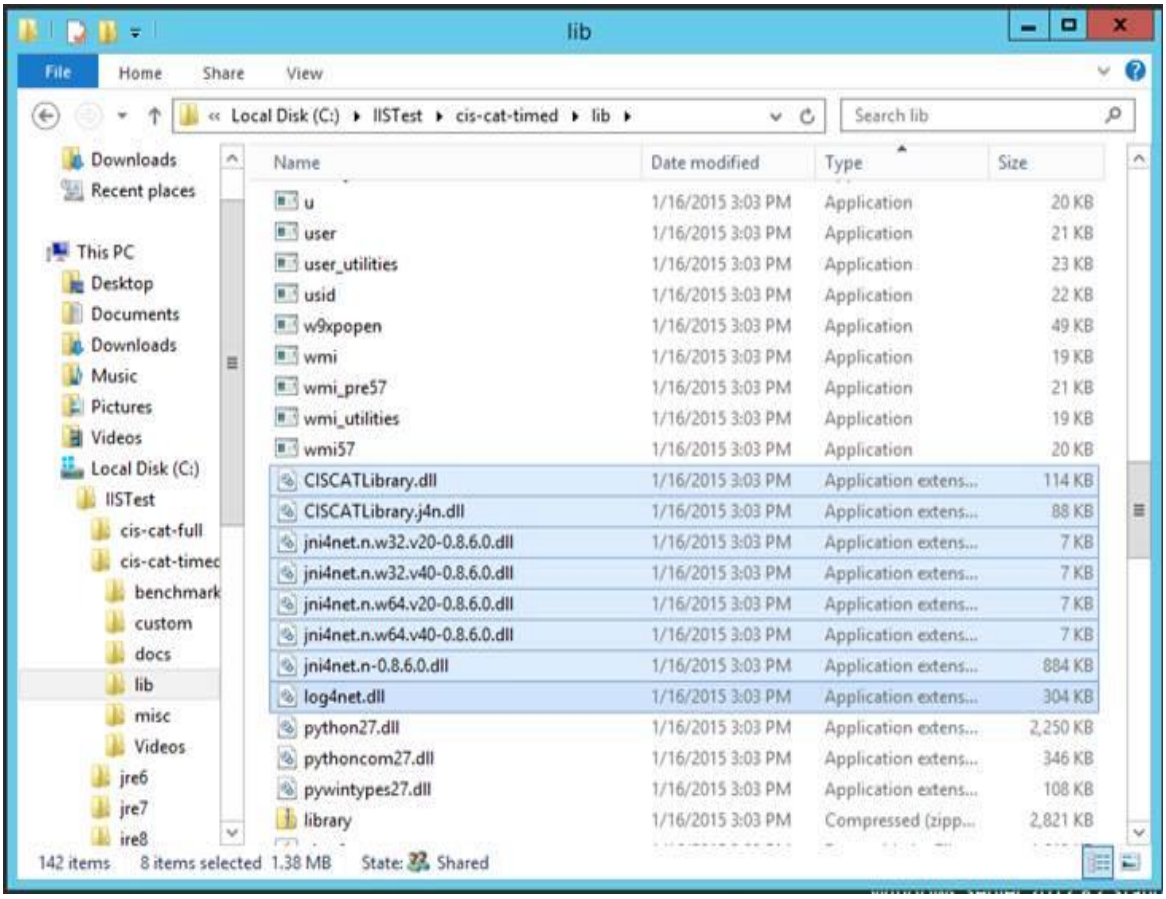
Because of CIS-CAT's usage of PowerCLI, and therefore Microsoft PowerShell, assessments can be executed against ESXi hosts which are not local to the machine executing CIS-CAT. However, **the machine being used to execute CIS-CAT must have PowerCLI installed**. PowerCLI can be downloaded here, and may only be installed on the following operating systems:

- Server
  - Windows Server 2012 R2
  - Windows Server 2008 R2 SP1
- Workstation
  - Windows 8.1
  - Windows 7 SP1

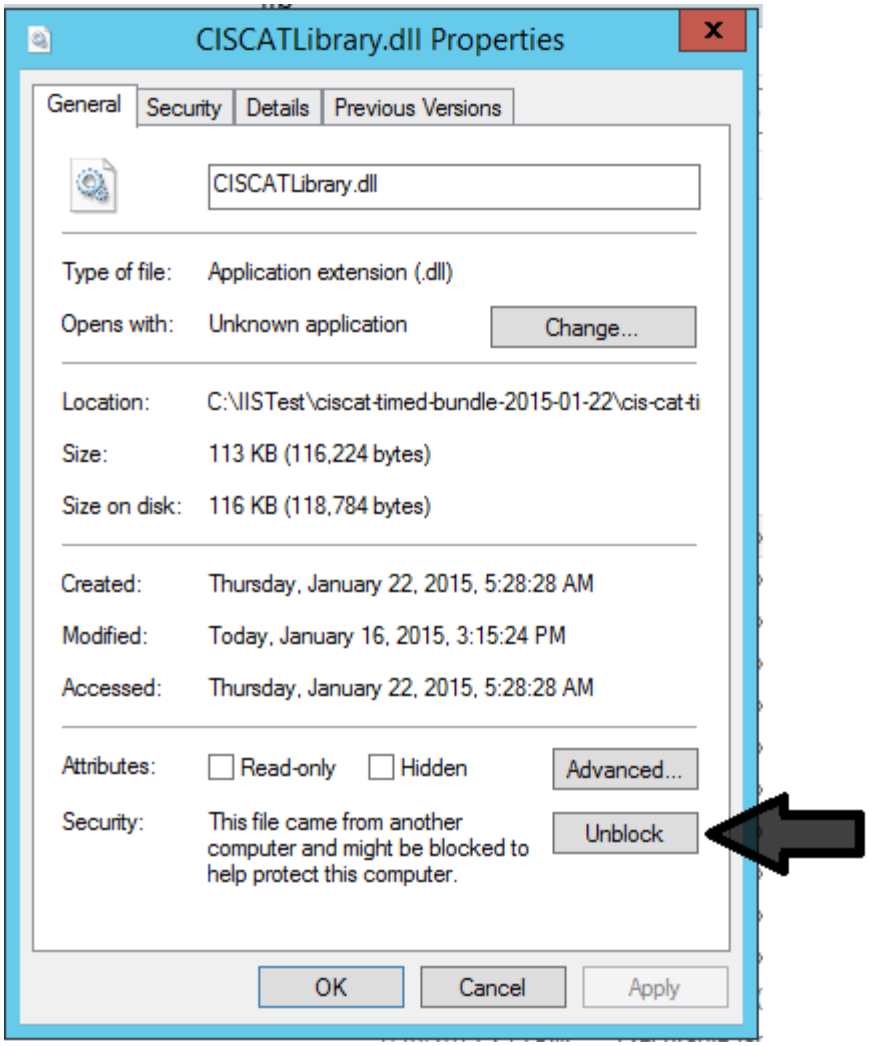
Pre-Configuration

Prior to executing CIS-CAT, ensure that the appropriate dynamic link libraries (DLL's) have been "unblocked". When assessing VMware benchmarks, CIS-CAT communicates with VMware through a connection using the PowerCLI interface. Because of the tool's use of .NET, some of the dll's are subject to .NET restrictions. These restrictions sometimes come into play when Windows believes that certain executable code is downloaded from the internet, and CIS-CAT then attempts to initialize that code. Windows marks those dll's as "unsafe".

Users can resolve this issue by "unblocking" the dll's being used by CIS-CAT. First navigate a Windows Explorer to the CIS-CAT installation folder, and enter the "lib" folder. Sort that list by Type and scroll to the `CISCATLibrary.dll`. Note the number of dll's highlighted below:



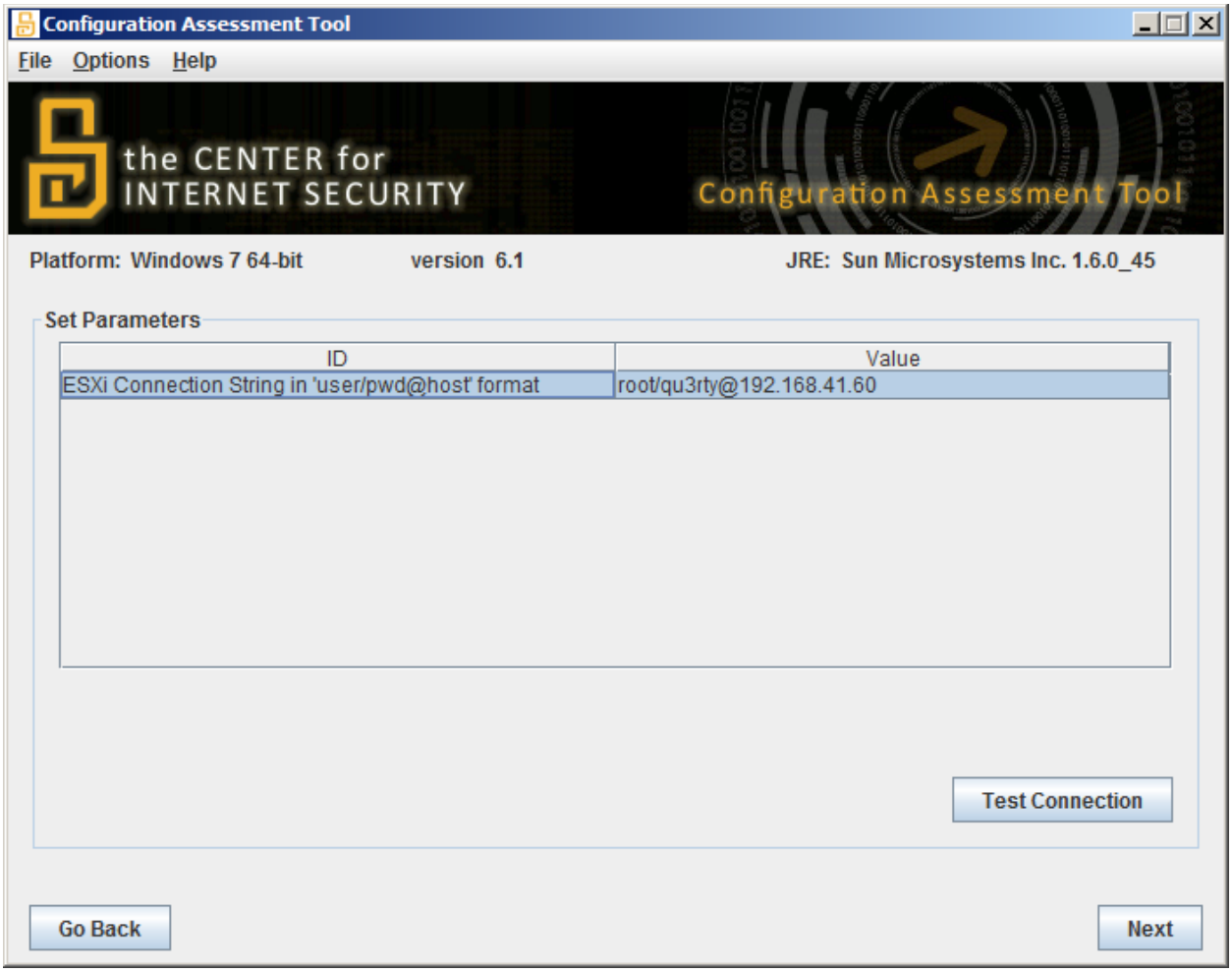
Users will have to "unblock" ***each of these dll's***. Right-Click on each of the dll's and select "Properties". On the main "Properties" screen, the user should see an "Unblock" button:



Click "Unblock", then click "OK" to close the Properties dialog. This "unblock" process ***must*** be completed for ***EVERY DLL*** highlighted above.

Connecting to VMware ESXi

Once a user has started CIS-CAT and selected an applicable VMware ESXi benchmark, he/she will be prompted to enter connection information for the ESXi host. The format of this connection string is `user/password@host`, for example `root/qu3rty@192.168.41.60`. Using the CIS-CAT graphical user interface, the connection string is entered on the parameter entry screen:



Once a connection string has been entered, the user can test its validity using the "Test Connection" button. A message box will alert the user of either a successful connection or a failed attempt.

Following the entry of connection information, and optional connection validation, CIS-CAT execution will proceed as normal, assessing the ESXi host against the appropriate benchmark recommendations.

CIS has developed a schema describing the various tests that have been implemented in support of the assessment of VMware ESXi hosts:

Test Name	Description
VMHost Account Configuration	This test is used to determine certain aspects of the user accounts on an ESXi host.
VMHost Acceptance Level Configuration	This test is used to determine if the software installed for the VMHost represents untested code.
VMHost Advanced Setting	This test is used to collect advanced configuration information from an ESXi host.
VMHost Authentication Configuration	This test is used to determine if ESXi is configured to use a directory service such as Active Directory to manage users and groups.
VMHost Core Dump Configuration	This test is used to validate the configuration of a centralized location to collect ESXi host core dumps. The VMware vSphere Network Dump Collector

	service allows for collecting diagnostic information from a host that experiences a critical fault.
VMHost Firewall Exception Configuration	This test is used to collect ESXi firewall configuration information for an ESXi host.
VMHost Bus Adapter Configuration	This test is used to collect information about ESXi host bus adapters.
VMHost iSCSI Bus Adapter Configuration	This test is used to collect information specific to iSCSI host bus adapters on an ESXi host.
VMHost Lockdown Configuration	This test is used to collect lockdown mode configuration information for an ESXi host.
VMHost Module Configuration	This test is used to determine if any ESXi host's loaded kernel modules lack valid digital signatures.
VMHost NTP Server Configuration	This test is used to collect configuration information for any NTP servers added to an ESXi host.
VMHost SNMP Configuration Test	This test is used to determine certain aspects of an ESXi host's SNMP configuration.
VMHost Web Server SSL Certificate Validation	This test is used to determine if any expired or revoked SSL certificates exist on the ESXi host.
VMHost Services Configuration	This test is used to collect service-related configuration information from an ESXi host.
VMHost vSphere Installation Bundle (VIB) Configuration	This test is used to determine if the software installed for a vSphere Installation Bundle (VIB) represents untested code. A VIB is a collection of files that are packaged into an archive. The VIB contains a signature file that is used to verify the level of trust.
VMHost vSwitch Policy Configuration	This test is used to collect information about various vSwitch policies on ESXi host vSwitches.
Virtual Machine Advanced Setting	This test is used to collect advanced configuration information from the virtual machines on an ESXi host.
Virtual Machine Device Configuration	This test is used to collect information about various virtual machine device settings on an ESXi host.
Virtual Machine Hard Disk Configuration	This test is used to collect information about virtual machine hard disk device settings on an ESXi host.
Virtual Machine Resource Configuration	This test is used to collect information about about the resource allocation between the virtual machines.
Virtual Port Group Configuration	This test is used to retrieve the available port groups of hosts, virtual machines, and virtual switches.

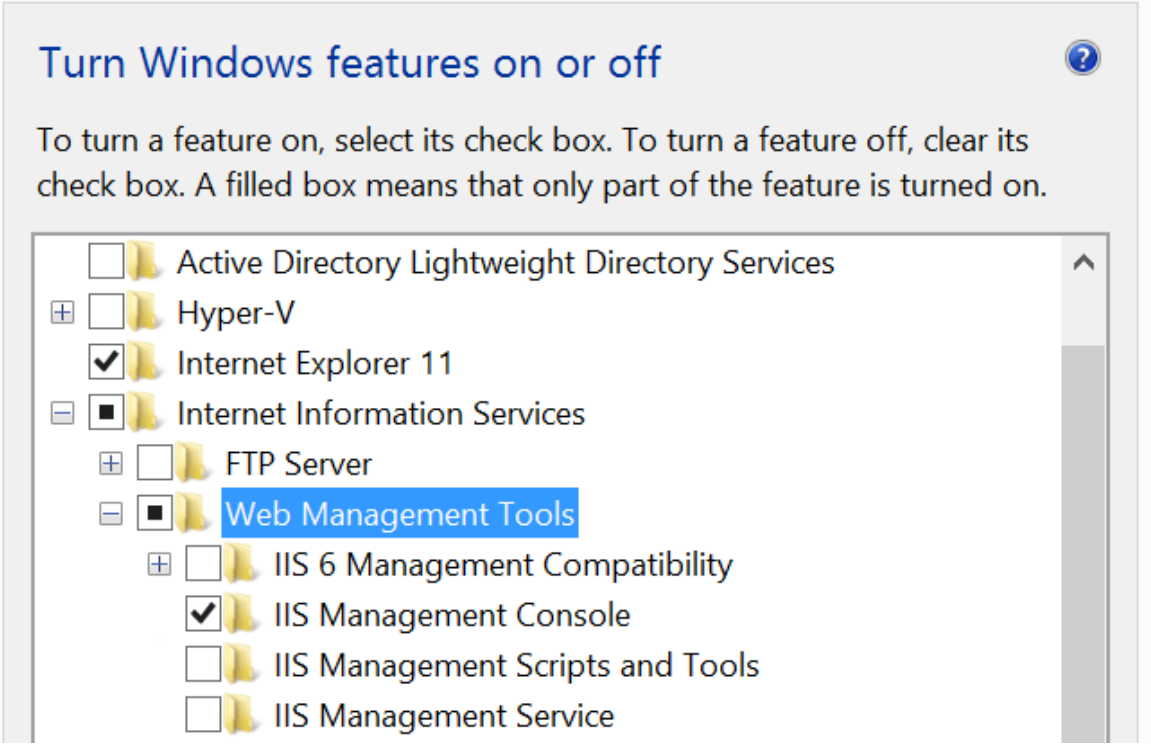
Using CIS-CAT with IIS Benchmarks

IIS 7/7.5 and IIS 8/8.5 Support

CIS' support for assessments of Microsoft IIS hosts is supported through developed interfaces with the Microsoft Web Administration libraries. These libraries provide C# interfaces to IIS servers, sites, applications and virtual directories, which are leveraged in CIS-CAT assessments.

- Microsoft IIS 7 is available as a server role on machines running Windows Server 2008,
- Microsoft IIS 7.5 is available as a server role on machines running Windows Server 2008 R2
- Microsoft IIS 8 is available as a server role on machines running Windows Server 2012,
- Microsoft IIS 8.5 is available as a server role on machines running Windows Server 2012 R2

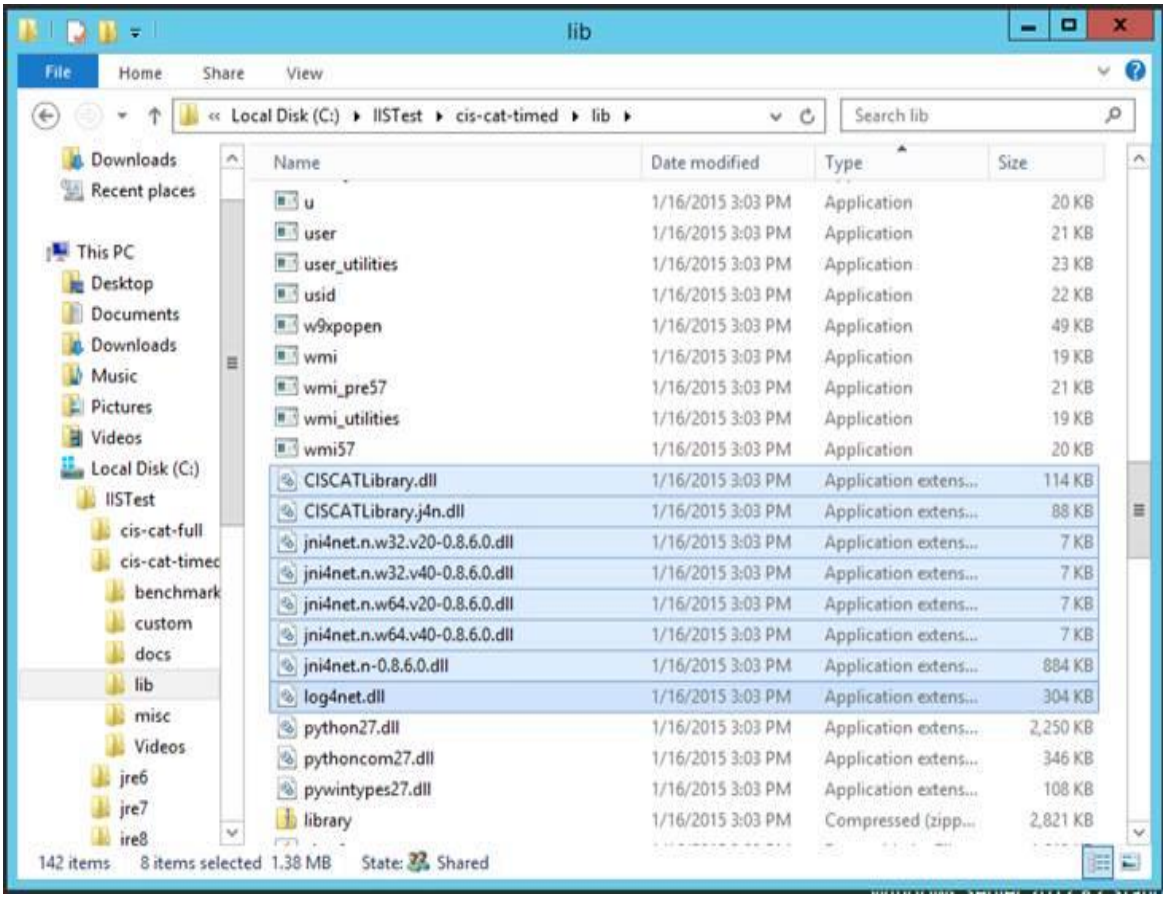
In order to install the required Microsoft Web Administration libraries, the server hosting IIS will need to configure the IIS Management Console. To enable the console, turn the feature on:



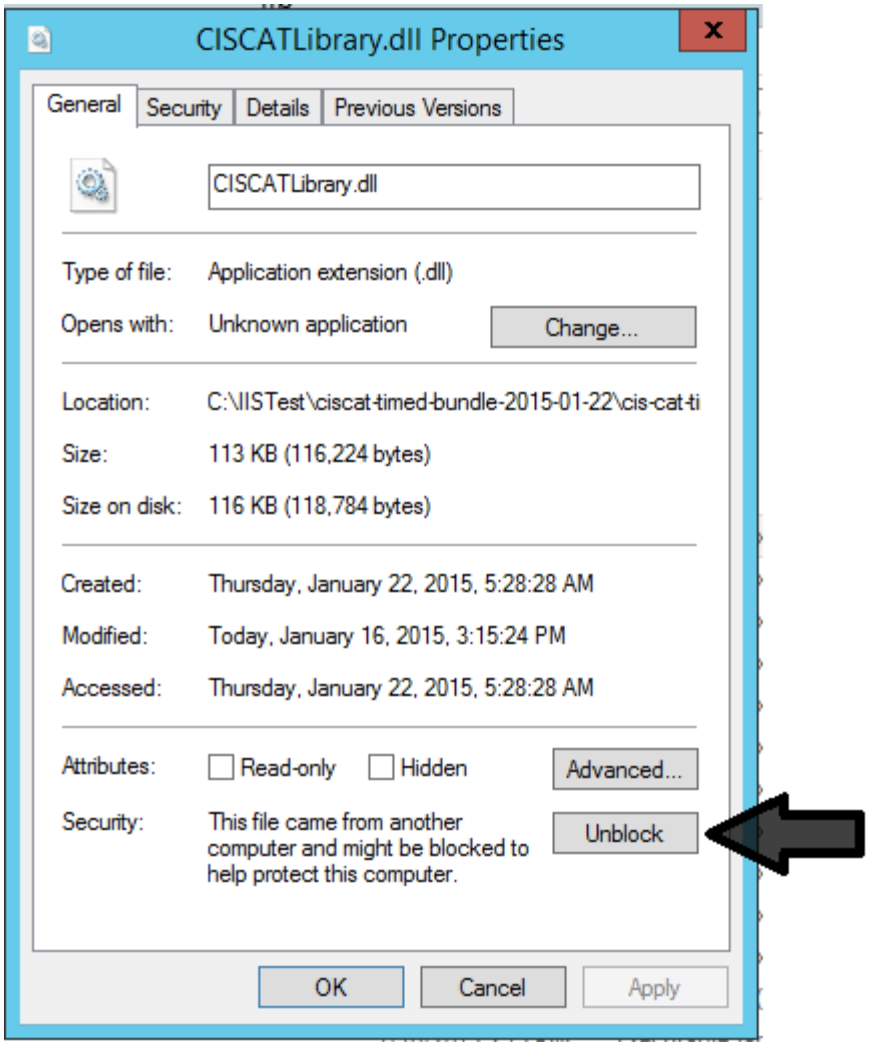
Pre-Configuration

Prior to executing CIS-CAT, ensure that the appropriate dynamic link libraries (DLL's) have been "unblocked". When assessing IIS benchmarks, CIS-CAT communicates with IIS through the Microsoft Web Administration interface. Because of the tool's use of .NET, some of the dll's are subject to .NET restrictions. These restrictions sometimes come into play when Windows believes that certain executable code is downloaded from the internet, and CIS-CAT then attempts to initialize that code. Windows marks those dll's as "unsafe".

Users can resolve this issue by "unblocking" the dll's being used by CIS-CAT. First navigate a Windows Explorer to the CIS-CAT installation folder, and enter the "lib" folder. Sort that list by Type and scroll to the `CISCATLibrary.dll`. Note the number of dll's highlighted below:



Users will have to "unblock" ***each of these dll's***. Right-Click on each of the dll's and select "Properties". On the main "Properties" screen, the user should see an "Unblock" button:



Click "Unblock", then click "OK" to close the Properties dialog. This "unblock" process ***must*** be completed for ***EVERY DLL*** highlighted above.

CIS has developed a schema describing the various tests that have been implemented in support of the assessment of Microsoft IIS 7, 7.5, 8, and 8.5:

Test Name	Description
Application Host Configuration Test	This test is used to collect IIS server level configuration information.
Application Pool Test	This test is used to collect information regarding application pool usage at the IIS server level.
Web Configuration Test	This test collects configuration information from the IIS site, application, and/or virtual directory level(s).
Bindings Test	This test is used to collect site binding and host header information from IIS managed web sites
System Web Test	This test is used to collect IIS site, application and virtual directory level configuration information stored in the systemWeb configuration section.

Using CIS-CAT with Cisco Benchmarks

Cisco IOS Support

CIS-CAT's support for assessments of Cisco IOS devices is supported through SSH connections to the applicable devices and execution of commands based on the application of OVAL-based constructs utilizing the device's running configuration.

When CIS-CAT recognizes a test or set of tests to be evaluated which require a SSH connection to be made, the user is presented with either a GUI screen or CLI prompts in order to enter the appropriate SSH configurations, such as the host and port, along with a username and credentials (or path to a private key file).

When performing assessments against Cisco devices, the user is also able to enter their "enable" credentials in order to execute privileged commands. For Cisco IOS assessments, the user used to connect to the device *must* be a privileged user, allowed to execute commands against the current running configuration. Similar to database benchmark assessments, the "Test Connection" button is available for users to verify host and credential information.

CIS-CAT has implemented the following OVAL 5.11 tests in support of assessments of Cisco IOS devices:

Test Name	Description
BGP Neighbor Test	The bgpneighbor test is used to check the bgp neighbpr properties of bgp instances instances in IOS
Global Test	The global test is used to check for the existence of a particular line in the ios config file under the global context
Interface Test	The interface test is used to check for the existence of a particular interface on the Cisco IOS device
Line Test	The line test is used to check the properties of specific output lines from a SHOW command, such as show running-config.
Router Test	The router test is used to check the properties of specific output lines from a router configurated instance in IOS
Routing Protocol Authentication Interface Test	The routing protocol authentication interface test is used to check the properties of routing protocol authentication configured under interfaces in IOS
Section Test	The section test is used to check the properties of specific output lines from a configuration section
SNMP Test	Tests if lines under the global context associated with snmp that have a specifiec access list or community name.
SNMP Community Test	The snmpcommunity test is used to check the properties of specific output lines from an SNMP configuration.
SNMP Group Test	The snmpgroup test is used to check the properties of specific output lines from an SNMP group configuration.
SNMP Host Test	The snmphost test is used to check the properties of specific output lines from an SNMP configuration.
SNMP User Test	The snmpuser test is used to check the properties of specific output lines from an SNMP user configuration.
SNMP View Test	The snmpview test is used to check the properties of specific output lines from an SNMP view configuration
Tclsh Test	The tclsh test is used to check tclsh information of the IOS operating system
Version/Version 5.5 Test	The version and version 5.5 tests are used to check the version of the IOS operating system

Cisco ASA Support

CIS-CAT's support for assessments of Cisco ASA devices is supported through SSH connections to the applicable devices and execution of commands based on the application of OVAL-based constructs utilizing the device's running configuration.

When CIS-CAT recognizes a test or set of tests to be evaluated which require a SSH connection to be made, the user is presented with either a GUI screen or CLI prompts in order to enter the appropriate SSH configurations, such as the host and port, along with a username and credentials (or path to a private key file).

When performing assessments against Cisco devices, the user is also able to enter their "enable" credentials in order to execute privileged commands. For Cisco ASA assessments, the user used to connect to the device *must* be a privileged user, allowed to execute commands against the current running configuration. Similar to database benchmark assessments, the "Test Connection" button is available for users to verify host and credential information.

As of this writing, a number of recommendations in the Cisco ASA benchmark require some organization-specific information regarding "untrusted interfaces" and "internet facing interfaces". This information is received from the user at assessment-time using "interactive" values. Using the CIS-CAT GUI, users are presented the Interactive Parameters screen, allowing for values to be entered. The CIS-CAT Command Line interface will allow users to enter values in the terminal used to execute the assessment. The following table provides information regarding the "interactive" values required for ASA:

Test Name	Description
"Untrusted" Interfaces	Untrusted interfaces are those which are not trusted, in other words those from which attacks can be generated. For example, interfaces connected to a DMZ, interfaces connected to Internet or third parties. The "untrusted" interface values used in this setting are the values of the "ifname" attribute of the interface. Examples

	could include “outside”, “mgmt”, or “inside”.
“Internet-facing” Interfaces	The “Internet-facing” interfaces are those untrusted interfaces acting as the line of demarcation between an internal network and the internet. The “internet-facing” interfaces, in the context of a CIS-CAT assessment, must be specified using the physical name of the interface, such as “GigabitEthernet0/1”, etc.

CIS-CAT has implemented the following OVAL 5.11 tests in support of assessments of Cisco ASA devices:

Test Name	Description
ACL Test	The acl test is used to check the properties of specific output lines from an ACL configuration.
Class-Map Test	Stores information about the MPF class-map configuration in ASA. That information includes the name, the type, the inspection type, the match type, the match commands, the policy-map or class-map it is used and the action in the policy-map.
Interface Test	Stores information about interfaces on a Cisco ASA device.
Line Test	Stores the configuration information associated with the evaluation of a SHOW sub-command on Cisco ASA. This includes the name of ths sub-command and the corresponding config line.
Policy-Map Test	Stores information about a policy-map configuration in ASA. That information includes the policy-map name, the inspection type, the paremeters, the match and action commands, the policy-map it is used in and the service-policy that applies it.
Service-Policy Test	Stores information about an MPF service-policy configuration in ASA. That information includes the service-policy name, where it is applied and the interface it is applied (if applicable).
SNMP Group Test	Stores information about an SNMP group configuration in ASA. That information includes the group name, the SNMP version, the IPv4 or IPv6 ACL it is applied to and the read, write and/or notify views applied to the group..
SNMP Host Test	Stores information about the SNMP host configuration in ASA. That information includes the host, the community or user strings, the SNMP version, the snmp security (if the SNMP version is SNMPv3) and the SNMP traps.
SNMP User Test	Stores information about an SNMP user configuration in ASA. That information includes the user name, the SNMP group he belongs to, the SNMP version, the IPv4 or IPv6 ACL it is applied to, the Security Level and the Authentication type that apply to the user (for SNMPv3).
TCP-Map Test	Stores information about MPF tcp-map configuration in ASA. That information includes the tcp-map name and its configured options.

Version Test	The version test is used to check the version of the ASA device being assessed

CIS-CAT Report Customization

The CIS-CAT HTML report can be customized in the following ways:

- Changing the report's cover page graphics, and
- Modifying the styling of the report

Replacing the Default Cover Page Graphics

Underneath the installation folder of the CIS-CAT bundle, there is a folder path named "custom/brand". It is into this folder that customized graphics may be stored for usage in generated HTML reports.

Logo

The default logo is the "Security Benchmarks" graphic located in the top-right-hand corner of the HTML report cover page. In order to utilize a custom image for the HTML report logo, place an image named "logo.gif" into the "custom/brand" folder of the CIS-CAT installation.

Cover Page Main Graphic

The default "cover page main graphic" is the orange colored vertical bar on the left-hand side of the first page of the HTML report. In order to utilize a custom image for the "cover page main graphic", place an image named "cover_page_background.gif" into the "custom/brand" folder of the CIS-CAT installation.

Subtitle Graphic

The default "subtitle graphic" is the dark-grey colored horizontal image containing

a. The benchmark assessed,
b. The profile assessed, and
c. The date/time of the assessment which generated the HTML report

In order to utilize a custom image for the "subtitle graphic", place an image named "cover_page_subtitle.gif" into the "custom/brand" folder of the CIS-CAT installation.

Customizing the Report Styling

It is possible to modify the styling on the HTML reports generated by CIS-CAT. In order to customize the styling, rename the "report_template.css" file to "report.css"; this file can be found under the "custom/brand" folder of the CIS-CAT installation. By default, the following styles may be changed:

- **body**: The "body" element specifies the font type and the background of the report. To change the background you would modify the rule "background-color" to either an RGB code (i.e. #FFFFFF) or specify a valid CSS color name. To modify the font type, change the "font-family" value.
- **footerBar**: The "footerBar" style specifies the look and feel of the orange-yellow bar at the end of the CIS-CAT HTML report. To change the background color of the footer, modify the "background-color" value to either an RGB code or valid CSS color name.

Valid CSS color names can be found at http://www.w3schools.com/cssref/css_colornames.asp. Another useful resource is the "color picker", located at http://www.w3schools.com/tags/ref_colorpicker.asp.

Script Check Engine (SCE)

Currently, many administrators use several of their own scripts to make sure their systems follow certain guidelines. These scripts are usually written in Bash, Windows batch files, PowerShell, etc. and are executed as they are. The administrators would like to move to SCAP to allow them to inter-operate and use tools supporting these standards. However they can't afford to make that transition abruptly, it would require them to rework all of their testing scripts at once. In order to ease the transition from scripts to standards-based assessment content, the Script Check Engine concept was developed to allow standards-based content to reference/execute scripts and report on their output. The Script Check Engine was initially developed as part of the OpenSCAP project.

Specific details on creating XCCDF Rules utilizing the Script Check Engine can be found in the accompanying CIS-CAT XML Customization Guide.

NOTE: When SCE-based Rules for Unix/Linux content exist, users ***must*** ensure that any scripts referenced by those Rules are granted execute permissions. For example, if a script exists named "world_writable_files.sh", prior to executing CIS-CAT, users must first grant execute permission:

```
# chmod +x world_writable_files.sh
```

Finally, CIS-CAT is compiled and bundled on a Windows system. Because of this, many Unix/Linux bash scripts are bundled using Windows-format CRLF line endings. This can cause unexpected behaviors when executing SCE-based Rules. In order to alleviate this undesired behavior, execute the "dos2unix" program on the target system prior to CIS-CAT assessment.

```
# dos2unix world_writable_files.sh
```

Using CIS-CAT with SCAP Content

The Center for Internet Security Configuration Assessment Tool (CIS-CAT) is built to support both the consensus security configuration benchmarks distributed by The Center for Internet Security and the configuration content distributed by NIST under the Security Content Automation Protocol (SCAP) program, a U.S. government multi-agency initiative to enable automation and standardization of technical security operations. Currently, XML provided by CIS is only available to CIS members. CIS-CAT reads system configuration guidance documents written in eXtensible Configuration Checklist Description Format (XCCDF) and Open Vulnerability and Assessment Language (OVAL), processes the contents, and outputs system compliance reports in HTML, text, and XML formats. The output XML is well-formed and valid XCCDF result documents containing SCAP compliance information suitable for submission to NIST, as well as additional detailed information useful for inspecting low-level evaluation check outcomes. The HTML output report contains a summary table listing the compliance status of each item, a numeric compliance score for each item and section, and a detailed report on each compliance item, including in most cases, the desired settings and the setting found on the system. The text report contains the benchmark item number, pass/fail results status, and the title of each item.

SCAP 1.0 Compatibility

CIS-CAT was previously a validated SCAP 1.0 FDCC Scanner, providing the capability to audit and assess a target system to determine its compliance with FDCC requirements. To exercise this capability, a user may download the "SCAP 1.0 Content…using OVAL version 5.3" resources from the NIST NVD National Checklist Program repository, or any other source of SCAP 1.0 compliant

content, and perform assessments in exactly the same manner as that user would with any other CIS benchmark.

As is required by the SCAP 1.1 specifications, CIS-CAT implements/adheres to the following language/enumeration standards:

- The eXtensible Configuration Checklist Description Format (XCCDF), version 1.1.4
- The Open Vulnerability and Assessment Language (OVAL), version 5.3
- The Common Configuration Enumeration (CCE), version 5
- The Common Platform Enumeration (CPE), version 2.2
- The Common Vulnerabilities and Exposures (CVE)
- The Common Vulnerability Scoring System (CVSS), version 2

SCAP 1.1 Compatibility

CIS-CAT provides the capability to audit and assess a target system using content conforming to the Security Content Automation Protocol, version 1.1 (SCAP 1.1). To exercise this capability, a user may download the "SCAP 1.1 Content…" resources from the NIST NVD National Checklist Program repository, or any other source of SCAP 1.1 compliant content, and perform assessments in exactly the same manner as that user would with any other CIS benchmark.

As is required by the SCAP 1.1 specifications, CIS-CAT implements/adheres to the following language/enumeration standards:

- The eXtensible Configuration Checklist Description Format (XCCDF), version 1.1.4
- The Open Vulnerability and Assessment Language (OVAL), version 5.8
- The Common Configuration Enumeration (CCE), version 5
- The Common Platform Enumeration (CPE), version 2.2
- The Common Vulnerabilities and Exposures (CVE)
- The Common Vulnerability Scoring System (CVSS), version 2

SCAP 1.2 Compatibility

CIS-CAT conforms to the specifications of the Security Content Automation Protocol, version 1.2 (SCAP 1.2), as outlined in NIST Special Publication (SP) 800-126 rev 2. As part of the SCAP 1.2 protocol, CIS-CAT's assessment capabilities have been expanded to include the consumption of source data stream collection XML files and the generation of well-formed SCAP result data streams. To exercise this capability, a user may download the "SCAP 1.2 Content…using OVAL version 5.10" resources from the NIST NVD National Checklist Program repository, or any other source of SCAP 1.2 compliant content, and perform assessments in exactly the same manner as that user would with any other CIS benchmark.

As is required by the SCAP 1.2 specifications, CIS-CAT implements/adheres to the following language/enumeration standards:

- The eXtensible Configuration Checklist Description Format (XCCDF), version 1.2
- The Open Vulnerability and Assessment Language (OVAL), version 5.10.1
- Asset Identification, version 1.1
- Asset Reporting Format (ARF), version 1.1
- The Trust Model for Security Automation Data (TMSAD), via XML digital signatures
- The Common Configuration Enumeration (CCE), version 5.
- The Common Platform Enumeration (CPE), version 2.3
- The Common Vulnerabilities and Exposures (CVE)
- The Common Vulnerability Scoring System (CVSS), version 2.0

- The Common Configuration Scoring System (CCSS), version 1.0

Platform Applicability

CIS-CAT's assessment capabilities have been validated as an Authenticated Configuration Scanner (ACS), with CVE option on the following operating system platforms:

- Microsoft Windows XP Professional with Service Pack 3
- Microsoft Windows Vista with Service Pack 2
- Microsoft Windows 7, 32-bit edition
- Microsoft Windows 7, 64-bit edition
- Red Hat Enterprise Linux 5 Desktop, 32-bit edition
- Red Hat Enterprise Linux 5 Desktop, 64-bit edition

Standards Implemented in CIS-CAT

The following standards are implemented in CIS-CAT:

XCCDF Implementation

CIS-CAT's capabilities include the ability to assess a target system based on rules defined using the eXtensible Configuration Checklist Description Format (XCCDF), versions 1.1.4 and 1.2. XCCDF is used throughout CIS-CAT as the required XML schema for benchmarks, as well as the checklist definition schema within SCAP source data streams. This ensures that outside compliance benchmarks/data streams, such as those provided by the NIST National Checklist Program, Federal Desktop Core Configuration (FDCC), or the US Government Configuration Baseline (USGCB), can be used alongside custom or CIS' benchmarks. The XCCDF format specifies the required tests for one or more profiles. At run-time, a user will be able to select any of the given profiles specified in a XCCDF, and CIS-CAT will assess the configuration rules included in the selected profile. With CIS-CAT, an evaluation check can be specified in three ways:

- In-place, contained in the rule definition using CIS' proprietary Embedded Check Language (ECL),
- Through a separate Open Vulnerability Assessment Language (OVAL) file, or
- Through a reference to OVAL definitions contained in the same SCAP data stream.

The relevant descriptions, CCE ID's and other related artifacts entered in the XCCDF will be preserved and included in the XML and HTML results produced by a CIS-CAT assessment.

OVAL Implementation

The Open Vulnerability and Assessment Language (OVAL) is used to identify vulnerabilities and issues. Common examples of the use of OVAL files are:

- the checking language referenced from a separate XCCDF file,
- the checking language referenced from a checklist component of a SCAP source data stream,
- the checking language referenced from a CPE dictionary component of SCAP source data stream

The OVAL component will contain the definitions, tests, as well as the state a target system is expected to exhibit. When CIS-CAT encounters a reference to an OVAL definition, it parses the specific OVAL components/files and uses those referenced definition identifiers to look up the appropriate tests to be executed. Each OVAL definition may be comprised of one-to-many OVAL

tests; the results of which may be logically combined to enumerate an overall definition result. The CIS-CAT evaluation engine is the controller for parsing the required tests, collecting the appropriate system characteristics, evaluating the collected information against the expected state, and recording the success, failure, or any error conditions of a given test. CIS-CAT supports components specified using versions 5.3, 5.8, 5.10.1, 5.11, 5.11.1, and 5.11.2 of the OVAL language.

CIS-CAT supports the following component schema and implements the indicated OVAL tests within each:

Component Schema	Implemented OVAL Tests
Platform Independent Definitions	• family_test • filehash_test • filehash58_test • environmentvariable_test • environmentvariable58_test • sql57_test • textfilecontent_test • textfilecontent54_test • unknown_test • variable_test • xmlfilecontent_test • shellcommand_test (extension added by CIS)
Unix Definitions	• file_test • inetd_test • password_test • process58_test • runlevel_test • shadow_test • symlink_test (included in OVAL 5.11) • sysctl_test • uname_test • xinetd_test
Linux Definitions	• inetlisteningservers_test • partition_test • rpminfo_test • selinuxboolean_test • systemdunitproperty_test (included in OVAL 5.11) • apparmorstatus_test (included in OVAL 5.11.2)
Windows Definitions	• accesstoken_test • auditeventpolicy_test • auditeventpolicysubcategories_test • cmdlet_test • file_test • fileauditedpermissions_test • fileauditedpermissions53_test • fileeffectiverights_test • fileeffectiverights53_test • group_test • group_sid_test • interface_test • lockoutpolicy_test • passwordpolicy_test • process58_test • registry_test • regkeyeffectiverights_test • regkeyeffectiverights53_test • service_test • serviceeffectiverights_test • sid_test

	• sid_sid_test • uac_test • user_test • userright_test (included in OVAL 5.11) • user_sid_test • user_sid55_test • volume_test • wmi_test • wmi57_test • wuaupdatesearcher_test
Cisco IOS Definitions	• bgpneighbor_test • global_test • interface_test • line_test • router_test • routingprotocolauthintf_test • section_test • snmp_test • snmpcommunity_test • snmpgroup_test • snmphost_test • snmpuser_test • snmpview_test • tclsh_test • version_test • version55_test
Cisco ASA Definitions	• acl_test • class_map_test • interface_test • line_test • policy_map_test • service_policy_test • snmp_group_test • snmp_host_test • snmp_user_test • tcp_map_test • version_test
Mac OS Definitions	• accountinfo_test • authorizationdb_test • gatekeeper_test • keychain_test • launchd_test • plist510_test • plist_test • pwpolicy59_test • pwpolicy_test • rlimit_test • softwareupdate_test • systemprofiler_test • systemsetup_test
VMware ESXi Definitions **CIS developed schema extension**	• vmhost_account_test • vmhost_acceptancelevel_test • vmhost_advancedsetting_test • vmhost_authentication_test • vmhost_coredump_test • vmhost_firewallexception_test • vmhost_busadapter_test • vmhost_lockdown_test • vmhost_module_test • vmhost_ntpserver_test • vmhost_snmp_test • vmhost_webserverssl_test • vmhost_services_test • vmhost_vib_test

	• vmhost_vswitch_policy_test • vm_advancedsetting_test • vm_device_test • vm_harddisk_device_test • vm_resourceconfig_test • virtual_portgroup_test
Microsoft IIS Definitions **CIS developed schema extension**	• applicationhostconfig_test • applicationpool_test • webconfig_test • bindings_test • systemweb_test

Asset Identification Implementation

CIS-CAT supports the use of the Asset Identification (AI) standard. Utilizing the AI standard, CIS-CAT is capable of reporting the necessary information to uniquely identify assets based on known identifiers and/or known information about the target systems being assessed.

Asset Reporting Format Implementation

CIS-CAT supports the use of the Asset Reporting Format (ARF) standard. ARF describes a data model for expressing information about assets and the relationships between assets and reports. When the CIS-CAT evaluation engine completes the assessment of a target system, users have the option to generate an output XML report utilizing the ARF data model. The CIS-CAT ARF report will contain component results (XCCDF, check results), information about the target asset (utilizing the Asset Identification, or AI, data model – described above), and the SCAP source data stream collection.

Trust Model for Security Automation Data

CIS-CAT supports the leveraging of the Trust Model for Security Automation Data (TMSAD) through its support of XML digital signatures on source data streams. A CIS-CAT assessment may be performed against both signed and unsigned data streams, and supports the validation of XML digital signatures through the `-vs` command-line interface option. Using the `-vs` option, source data stream content containing invalid XML digital signatures, or lacking XML digital signatures altogether, will be rejected and assessment halted. Note that this is an optional command-line option; digital signature validation will not be attempted by default.

Common Configuration Enumeration Implementation

CIS-CAT supports the use of the Common Configuration Enumeration (CCE) standard. CCE identifiers uniquely distinguish entries within a dictionary of security-related software (mis-) configuration issues. Source data stream collections and XCCDF benchmark documents may contain CCE references, and such references will be manifest in output reports with the associated benchmark item as links to the National Vulnerability Database (NVD) CCE database, providing an convenient path to detailed information regarding a CCE-identified configuration issue. CCE's are useful as a key to refer to the same configuration recommendation, regardless of its context or the tool used for processing. While minor differences may be necessary depending on the context, it is useful to keep track of the underlying configuration recommendation that is being processed by use of this common configuration identifier for comparisons across multiple systems, for reporting purposes, and for organizing security configuration guidance in a structured manner for efficient data management.

Common Platform Enumeration Implementation

CIS-CAT supports the use of the Common Platform Enumeration (CPE) standard, versions 2.2 and 2.3. CPE is a structured naming scheme for information technology systems, platforms, and applications that is similar to a URI. The advantage of using CPE is that it provides a standard naming convention for Operating Systems and other applications. CIS-CAT implements support for CPE name matching in XCCDF components of source data streams, as specified in section 4.3.1 of NIST SP800-126r2 (SCAP 1.2 Technical Specifications). The CIS-CAT evaluation engine can determine if particular XCCDF rules are applicable to the target platform, and is able to skip evaluation of rules which are not applicable; indicating a status of "Not Applicable".

Common Vulnerabilities and Exposures Implementation

CIS-CAT supports the Common Vulnerabilities and Exposures (CVE) standard. CVE allows users of CIS-CAT to identify known security vulnerabilities and exposures, such as the presence of unpatched software. CIS-CAT assumes that a CVE will be defined in the metadata section of an OVAL definition. The CVE should be defined with a reference node and a source attribute of "CVE". There can be one or multiple CVE ID's for a given OVAL definition because one software patch or issue may be associated with many vulnerabilities.

Common Vulnerability Scoring System Implementation

CIS-CAT provides support for the Common Vulnerability Scoring System (CVSS), version 2. CIS-CAT supports a number of scoring mechanisms, including the Common Vulnerability Scoring System (CVSS). CVSS is an industry standard for assessing the weight, or severity, of system security vulnerabilities relative to other vulnerabilities. It is a means by which to establish a numeric value to a security vulnerability, so that organizations can measure overall risk to its systems, and to prioritize the correction of system vulnerabilities. The score is based on a series of vulnerability attributes including: if the vulnerability can be exploited remotely; the complexity necessary for a successful attack; if authentication is first necessary for a given exploit; if the vulnerability could lead to unauthorized access to confidential data; whether or not system integrity could be damaged via a given vulnerability; and whether or not system availability could be reduced via the vulnerability. CVSS is an evolving standard.

Common Configuration Scoring System Implementation

CIS-CAT provides support for the Common Configuration Scoring System (CCSS), version 1. Whereas CVSS represents a scoring system for software flaw vulnerabilities, CCSS addresses software security configuration issue vulnerabilities[i]. Per NIST SP800-126r2, CCSS data is not directly useful in the same way as CVSS data. CCSS data needs to be considered in the context of each organization's security policies and in the context of dependencies among vulnerabilities.[ii] CIS-CAT supports CCSS scores when that score is used in the `@weight` attribute within XCCDF rules.

Creating the CSV Report for FDCC

To create the CSV report for FDCC purposes, execute the FDCC assessment, export the results as CSV, then open the file in Excel and remove all but the last two columns.

[i] http://csrc.nist.gov/publications/nistir/ir7502/nistir-7502_CCSS.pdf
[ii] http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf