

# CIS Configuration Assessment Tool CIS-CAT

## Users Guide

v2.2.39

March 31, 2014

## Table of Contents

Overview .....	3
System Requirements .....	3
Supported Benchmarks.....	3
Obtaining CIS-CAT .....	4
Installing CIS-CAT .....	5
CIS-CAT Support.....	5
Using CIS-CAT within a Graphical User Interface (GUI) .....	6
Configuring Result Location .....	6
Choosing a Benchmark and Profile.....	8
Evaluating a Benchmark .....	11
Viewing Evaluation Results .....	13
Creating a CIS-CAT Dashboard .....	15
Using CIS-CAT within a Command Line Interface (CLI) .....	18
Listing Available Benchmarks.....	19
Choosing a Benchmark and Profile.....	19
Running a specific Benchmark and Profile .....	21
Evaluating a Data Stream Collection, Data Stream, Collection and Profile.....	21
Data Stream Collection Only .....	21
Data Stream Collection and Data Stream.....	21
Data Stream Collection, Data Stream, and Checklist .....	22
Data Stream Collection, Data Stream , Checklist, and Profile.....	22
Data Stream Collection, Data Stream, and Definitions .....	22
Displaying Status Information during Evaluation.....	22
Accepting Terms of Use.....	23
Reset CIS-CAT Preferences.....	23
Configuring Result Location .....	23
Configuring Report Name.....	23
Configuring Report Output .....	24
Creating a CIS-CAT Dashboard .....	24
Uploading a CIS-CAT Results File .....	24
Interpreting Evaluation Results.....	26
Summary of Results .....	26
Assessments Results.....	27
Assessment Details.....	28
Assessing Multiple Windows Targets.....	29
Prerequisites.....	29
Setup .....	29
Create CIS Share on the CIS Hosting Server.....	29
Security Considerations.....	30
Update cis-cat-centralized.bat .....	30
Validate the Install.....	31
Configuring the Scheduled Task via Group Policy.....	31
Benchmark Considerations.....	33
Using the CIS-CAT Dissolvable Agent .....	34
Prerequisites.....	35
Setup .....	35
Create CIS Share on the CIS Hosting Server.....	35
Security Considerations.....	35
Update cis-cat-dissolvable.bat .....	36

Validate the Install.....	36
Configuring the Scheduled Task via Group Policy.....	36
Benchmark Considerations.....	39
Using CIS-CAT with Database Benchmarks.....	41
Oracle Database Support .....	41
Further Database Support.....	43
Microsoft SQL Server Database Support.....	43
Sybase Database Support .....	44
CIS-CAT Report Customization .....	44
Replacing the Default Cover Page Graphics.....	45
Logo.....	45
Cover Page Main Graphic.....	45
Subtitle Graphic .....	45
Customizing the Report Styling.....	45
Using CIS-CAT with SCAP Content .....	46
SCAP 1.0 Compatibility .....	46
SCAP 1.1 Compatibility .....	46
SCAP 1.2 Compatibility .....	47
Platform Applicability .....	47
Standards Implemented in CIS-CAT .....	47
XCCDF Implementation .....	47
OVAL Implementation.....	48
Asset Identification Implementation.....	49
Asset Reporting Format Implementation.....	49
Trust Model for Security Automation Data.....	49
Common Configuration Enumeration Implementation .....	50
Common Platform Enumeration Implementation .....	50
Common Vulnerabilities and Exposures Implementation.....	50
Common Vulnerability Scoring System Implementation .....	50
Common Configuration Scoring System Implementation.....	51
Creating the CSV Report for FDCC.....	51

## 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 JRE v1.5.0 or later. 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.

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

## Supported Benchmarks

CIS-CAT reads:

- a) 36 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

CIS currently distributes CIS-CAT with production version support for the following 37 benchmarks:

- CIS Apache Tomcat 5.5-6.0 Benchmark v1.0.0
- CIS Apple OSX 10.5 Benchmark v.1.1.0
- CIS Apple OSX 10.6 Benchmark v.1.0.0
- CIS CentOS Linux 6 Benchmark v1.0.0
- CIS Debian Linux 3 Benchmark v1.0.0
- CIS HP-UX 11i Benchmark v1.4.2
- CIS IBM AIX 4.3-5.1 Benchmark v1.0.1
- CIS IBM AIX 5.3-6.1 Benchmark v1.1.0
- CIS IBM AIX 7.1 Benchmark v1.1.0
- CIS Microsoft Internet Explorer 10 Benchmark v1.0.0\*
- CIS Microsoft SQL Server 2008 R2 Database Engine Benchmark v1.0.0\*

- CIS Microsoft SQL Server 2012 Database Engine Benchmark v1.0.0\*
- CIS Microsoft Windows 7 Benchmark v2.1.0\*
- CIS Microsoft Windows 8 Benchmark v1.0.0\*
- CIS Microsoft Windows Server 2003 Benchmark v3.1.0\*
- CIS Microsoft Windows Server 2008 Benchmark v2.1.0\*
- CIS Microsoft Windows Server 2008 R2 Benchmark v2.1.0\*
- CIS Microsoft Windows Server 2012 Benchmark v1.0.0\*
- CIS Microsoft Windows XP Benchmark v3.1.0\*
- CIS MIT Kerberos 1.10 Benchmark v1.0.0\*
- CIS Mozilla Firefox 3 Benchmark v1.0.0
- CIS Oracle Database 9i-10g Benchmark v2.0.1
- CIS Oracle Database 11g Benchmark v1.0.1
- CIS Oracle Solaris 2.5.1-9 Benchmark v1.3.0
- CIS Oracle Solaris 10 Benchmark v5.1.0
- CIS Oracle Solaris 11 Benchmark v1.1.0
- CIS Oracle Solaris 11.1 Benchmark v1.0.0
- CIS Red Hat Enterprise Linux 4 Benchmark v1.0.5
- CIS Red Hat Enterprise Linux 5 Benchmark v2.0.0
- CIS Red Hat Enterprise Linux 6 Benchmark v1.2.0
- CIS Slackware Linux 10.2 Benchmark v1.1.0
- CIS SUSE Linux Enterprise Server 9 Benchmark v1.0.0
- CIS SUSE Linux Enterprise Server 10 Benchmark v2.0.0
- CIS SUSE Linux Enterprise Server 11 Benchmark v1.0.0
- CIS Ubuntu 12.04 LTS Server Benchmark v1.0.0
- CIS VMware ESX 3.5 Benchmark v1.2.0
- CIS VMware ESX 4.1 Benchmark v1.0.0

NOTE: Those benchmarks denoted with an asterisk (\*) utilize XCCDF with the OVAL checking language. See [OVAL Implementation](#) for more information regarding OVAL.

## 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
<b>/benchmarks</b>	Contains all XCCDF Benchmarks
<b>/custom/brand</b>	Placeholder for member-created CSS and graphics for customized branding of HTML Reports generated by CIS-CAT.
<b>/docs</b>	Contains User Documentation
<b>/misc</b>	Contains XSDs and supplemental batch files
<b>/lib</b>	Contains Libraries used by CIS-CAT
<b>CISCAT.jar</b>	The CIS-CAT Java Archive
<b>CIS-CAT.sh</b>	A UNIX/Linux Wrapper for CIS-CAT.jar. Useful for CLI mode.
<b>CIS-CAT.bat</b>	A Windows Wrapper for CIS-CAT.jar. Useful for CLI mode.
<b>cis-cat-centralized.bat</b>	A Windows batch file that wraps CIS-CAT.jar to simply evaluating targets that lack a local instance of the JRE and CIS-CAT.

## Installing CIS-CAT

To install CIS-CAT, simply unzip the archive. No further action is required provided JRE v1.5.0+ 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 ran on a Unix machine the shell script might need to execute permissions to do this run the following command:

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

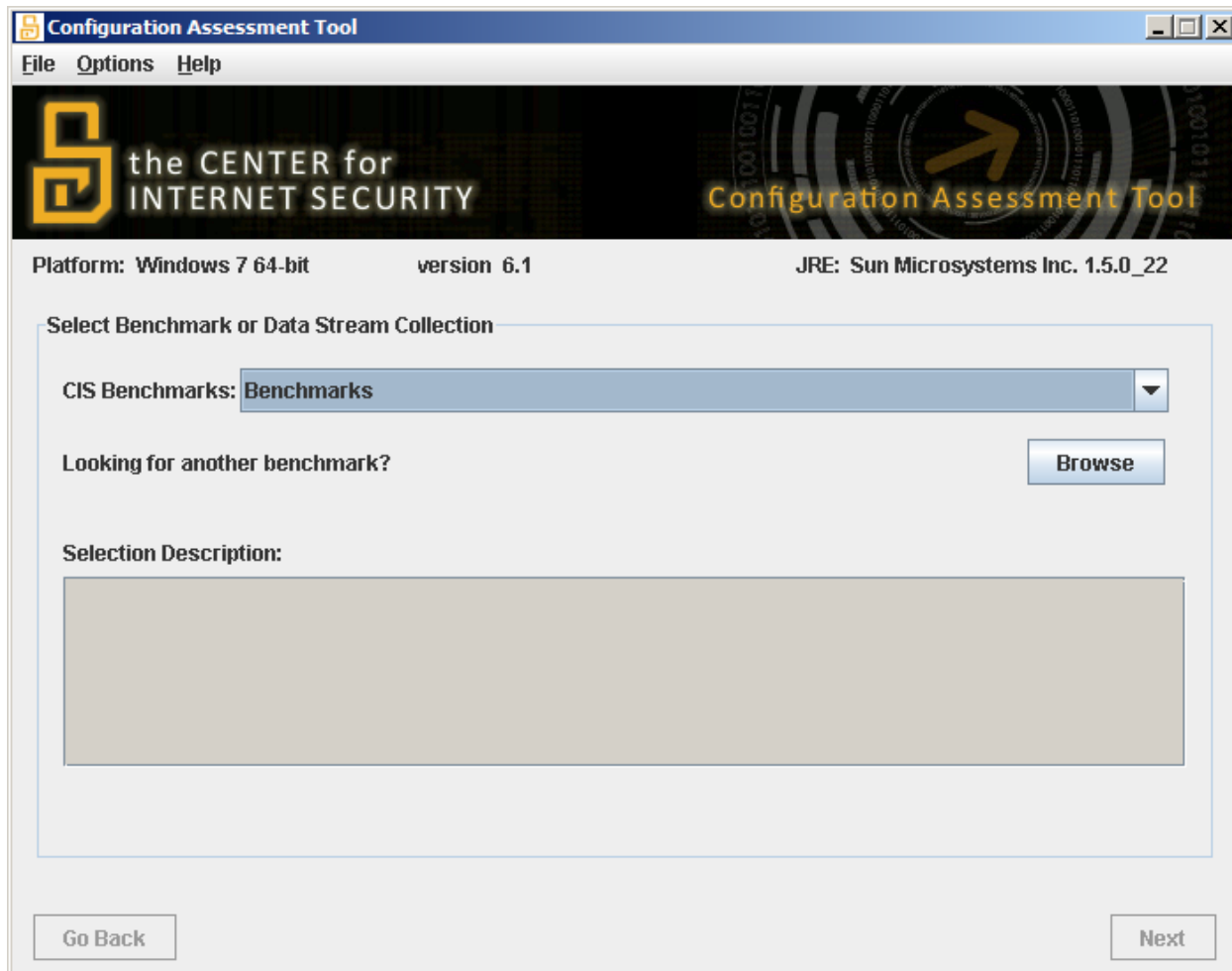
## CIS-CAT Support

If you have questions, comments, or are experiencing trouble using CIS-CAT, please email [support@cisecurity.org](mailto: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.

## 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:



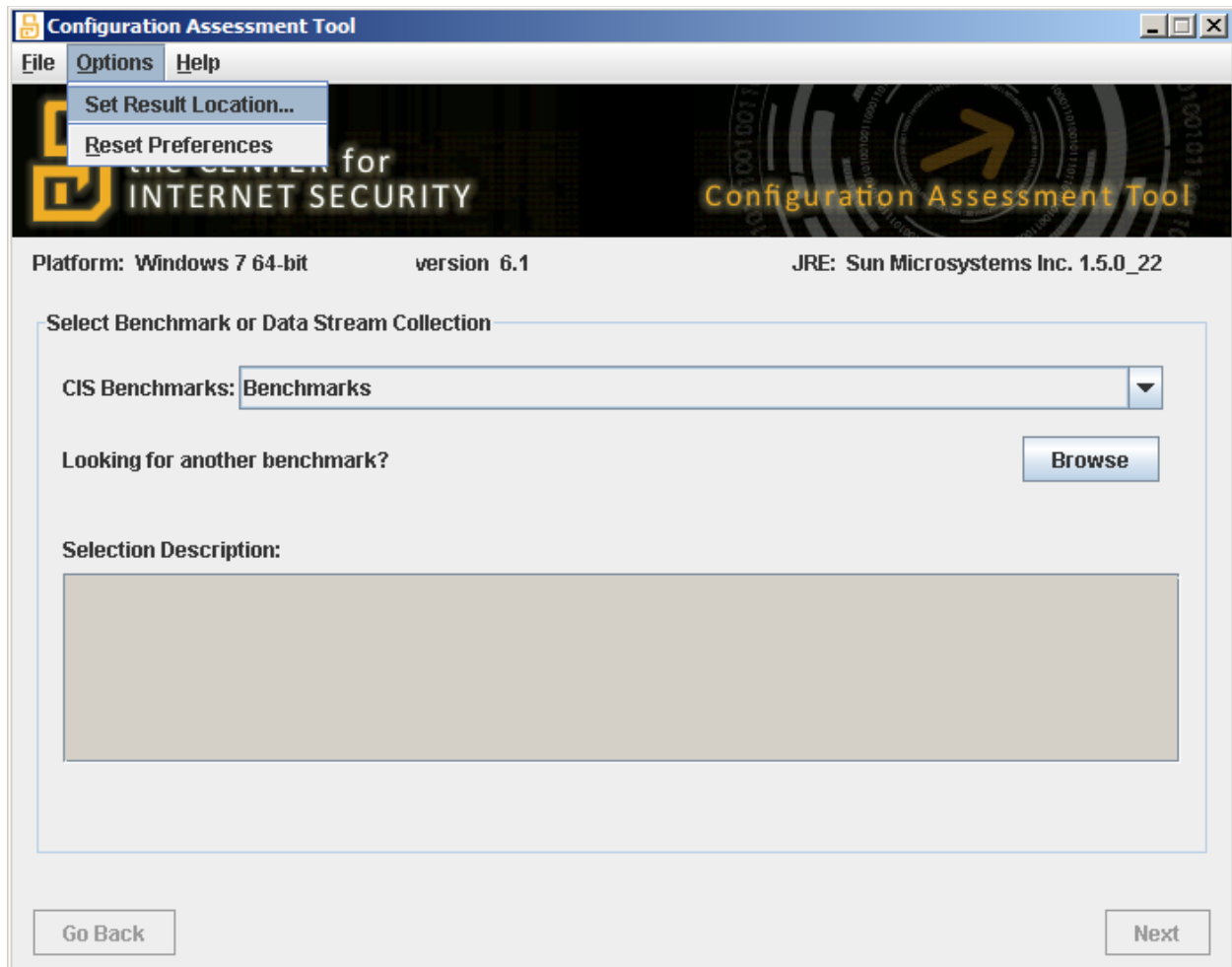
### Configuring Result Location

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
<b>Hive</b>	HKEY_CURRENT_USER
<b>Key</b>	Software\JavaSoft\Prefs\org\cisecurity\tools\cisecat
<b>Value (REG_SZ)</b>	result-location

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

`$HOME/.java/.userPrefs/org/cisecurity/tools/cisecat/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`.

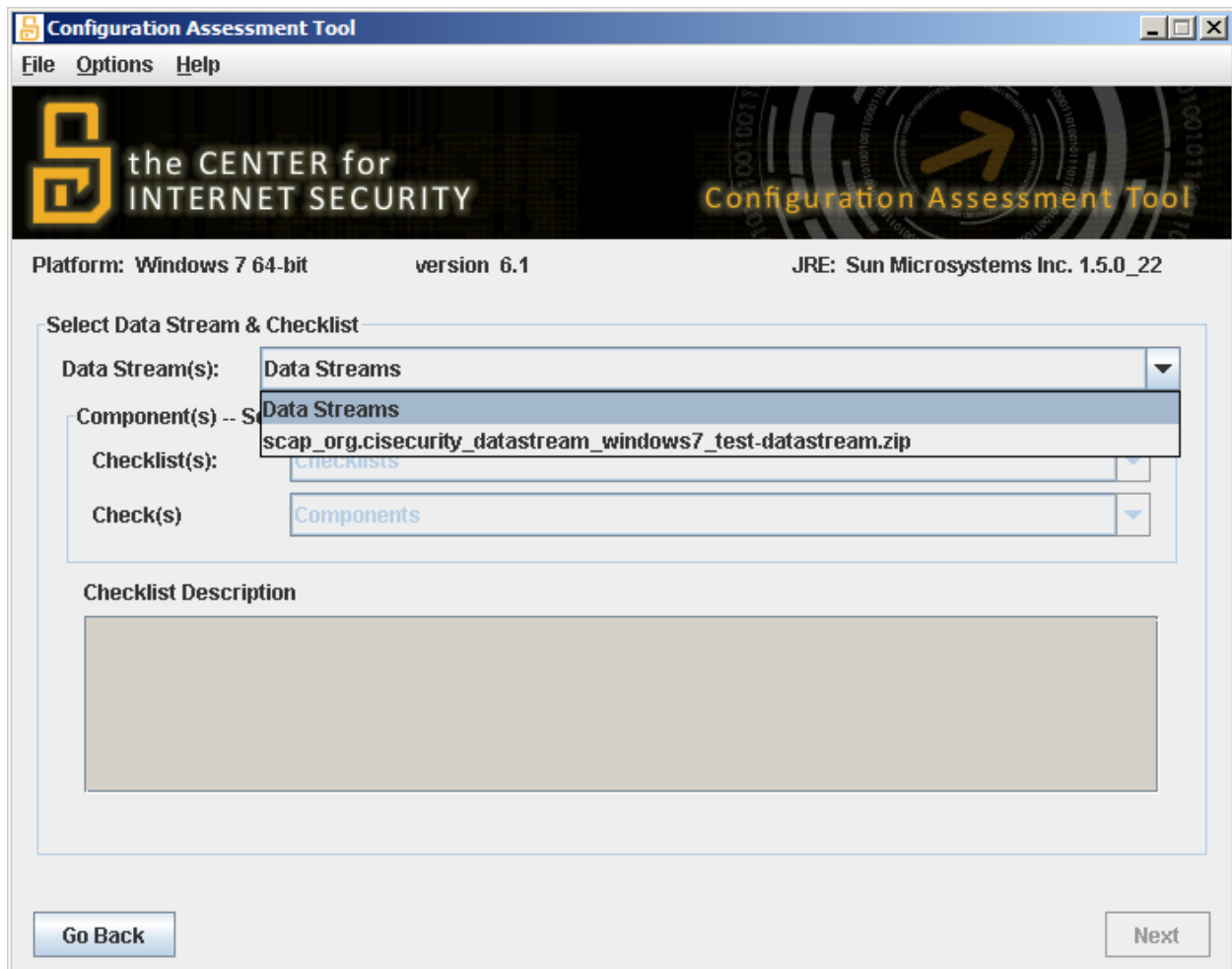


## Choosing a Benchmark and Profile

CIS-CAT will only evaluate one benchmark at a time. To select a benchmark, either select a CIS benchmark from the drop down or click on the `Browse`, 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.



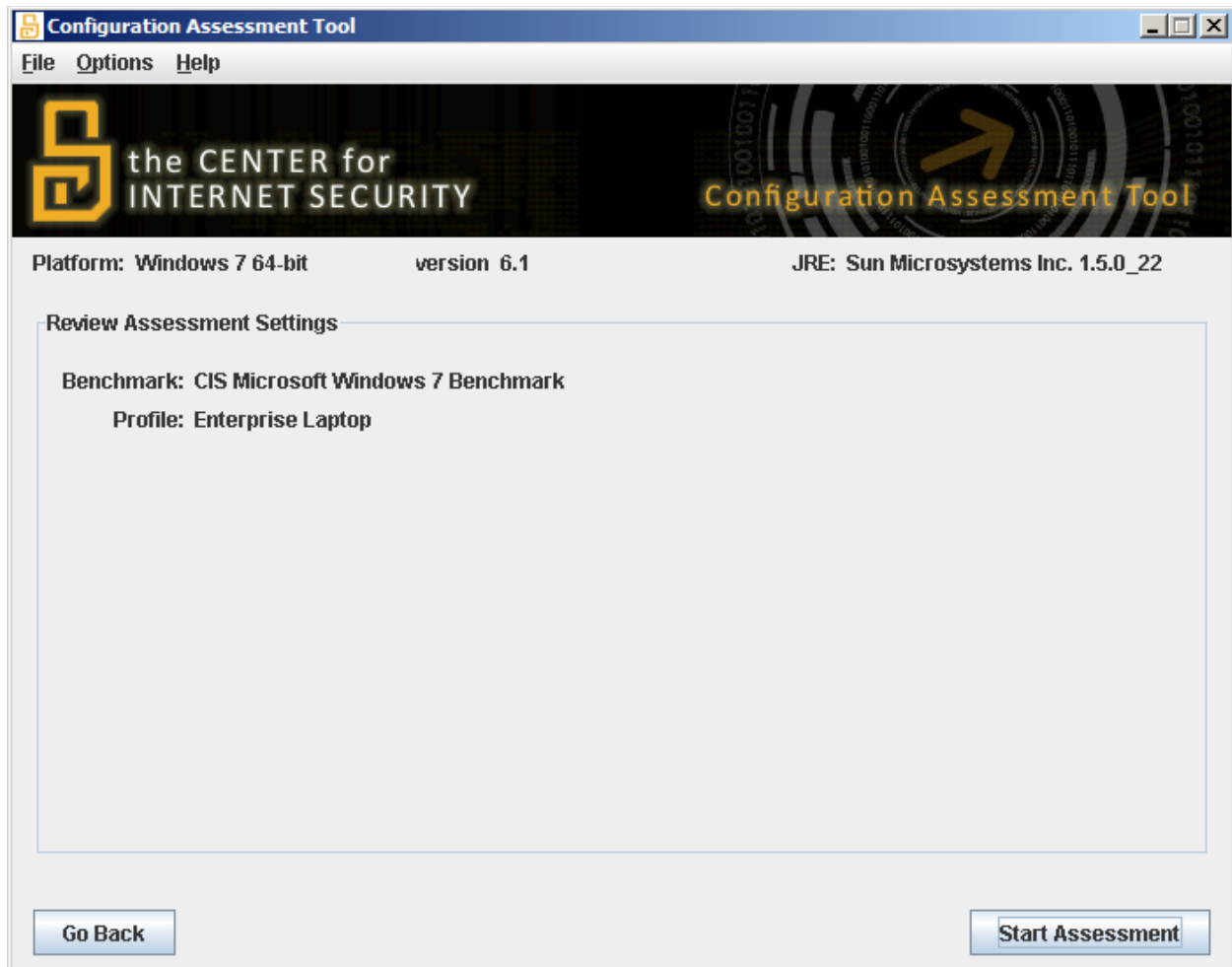
Once a checklist is loaded, click `Next`. A list of available profiles will be provided in the drop down menu. When a profile is selected, that profile's description will be displayed as seen below:



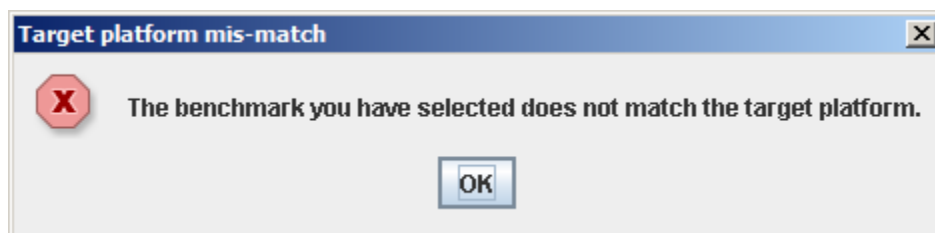
Profiles represent a logical grouping of benchmark recommendations. Profiles are commonly used to distinguish between Level I and Level II scoring recommendations, or target role, such as Enterprise Desktop, Enterprise Laptop, SSLF Desktop, and SSLF Laptop as seen above in the Windows 7 benchmark.

## Evaluating a Benchmark

Once you have selected a benchmark and profile to evaluate, click **Next** to review your choices, as seen below:



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



This message is informational. CIS-CAT will continue to assess the selected benchmark and profile. CIS-CAT will then display the benchmark execution status screen like the one shown below:

The screenshot shows the Configuration Assessment Tool window. The title bar reads "Configuration Assessment Tool". The menu bar includes "File", "Options", and "Help". The header area features the logo for "the CENTER for INTERNET SECURITY" and the text "Configuration Assessment Tool". Below the header, system information is displayed: "Platform: Windows 7 64-bit", "version 6.1", and "JRE: Sun Microsystems Inc. 1.5.0\_22".

The main content area is titled "Benchmark Execution Status" and contains a table with the following data:

Number	Title	Time	Result
3/166	Minimum password age	<1 second	Pass
4/166	Minimum password length	<1 second	Pass
5/166	Password must meet complexity requirements	<1 second	Pass
6/166	Store passwords using reversible encryption	<1 second	Pass
7/166	Account lockout duration	<1 second	Pass
8/166	Account lockout threshold	<1 second	Fail
9/166	Reset account lockout counter after	<1 second	Pass
10/166	Enforce user logon restrictions	<1 second	Fail
11/166	Maximum tolerance for computer clock synchronization	<1 second	Fail
12/166	Maximum lifetime for service ticket	<1 second	Fail
13/166	Maximum lifetime for user ticket renewal	<1 second	Fail
14/166	Maximum lifetime for user ticket	<1 second	Fail
15/166	Audit: Shut down system immediately if unable to log security audits	<1 second	Pass
16/166	Audit: Force audit policy subcategory settings (Windows Vista or later) to overrid...	<1 second	Pass
17/166	Audit Policy: System: IPsec Driver	<1 second	Pass
18/166	Audit Policy: System: Security State Change	<1 second	Pass

A "Next" button is located at the bottom right of the window.

Once the evaluation is complete, the `Next` button will be enabled allowing for the benchmark results to be generated and viewed.

## Viewing Evaluation Results

Once the evaluation is complete, click on `Next` to go to the report generation screen, as seen below:



By default an HTML report will be generated. 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	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 <a href="#">OVAL Results XML schema</a> .
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 <a href="#">here</a> .

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.

### NOTICE:

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

## Creating a CIS-CAT Dashboard

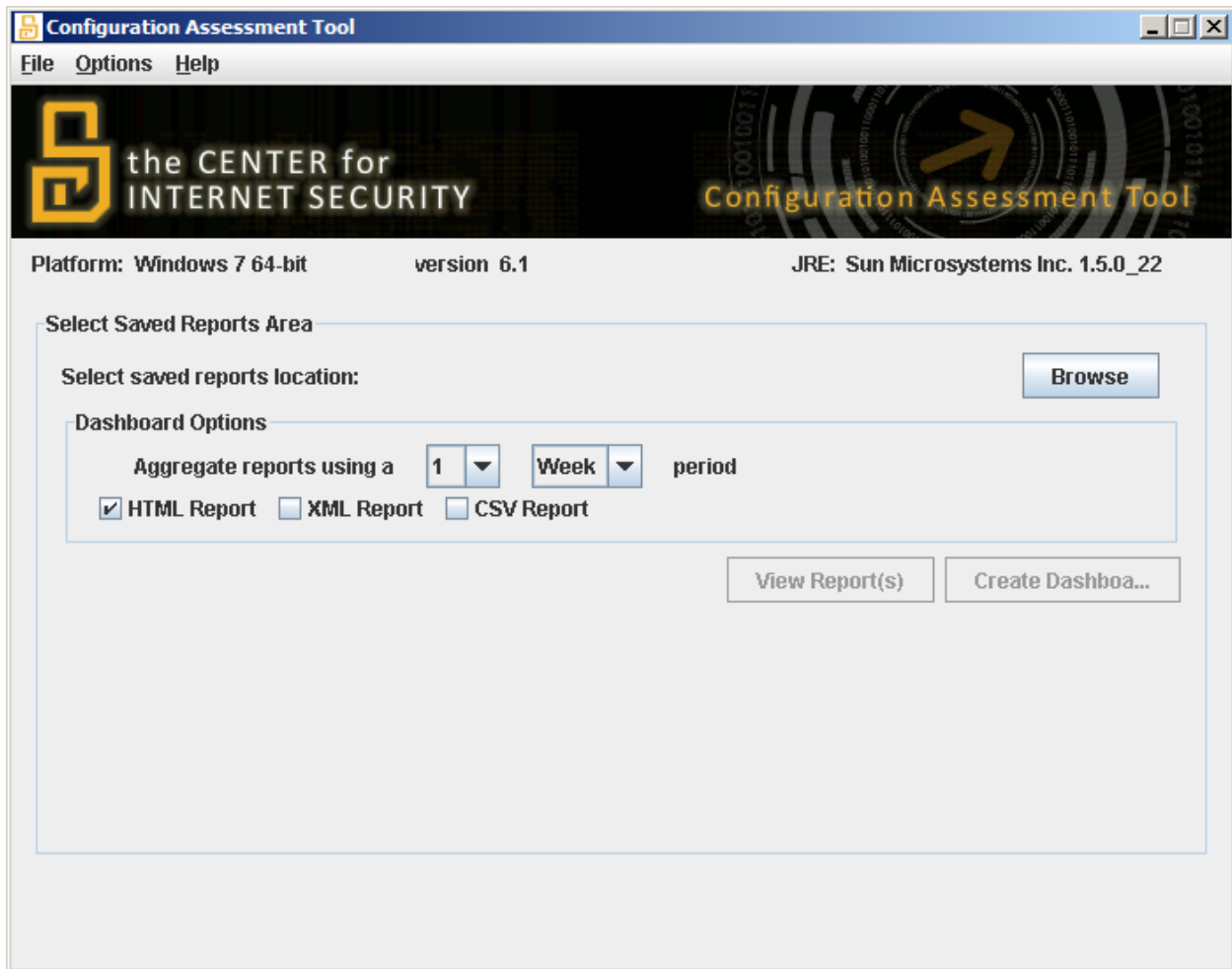
CIS-CAT's dashboard feature consumes multiple instances of CIS-CAT XML result files and summarizes them into a single XML file. The primary goal of this feature is to provide the ability to trend configuration status over time on a per benchmark, or device basis from different devices/computers.

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:





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.



## 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
-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)
-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 report
-ov, --oval-variables <arg> Specifies an OVAL Variables file to process
-p, --profile <arg>         Title of benchmark profile to evaluate
-r, --results-dir <arg>     Directory to save results in
```

<code>-rg, --report-gen</code>	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.
<code>-rn, --report-name &lt;arg&gt;</code>	The base name of the report, no extension
<code>-s, --status</code>	Status information is displayed
<code>-t, --report-txt</code>	Creates a text report
<code>-u, --report-upload &lt;arg&gt;</code>	Sends a HTTP POST with the XML report to the specified URL. POST parameter name is ciscat-report
<code>-ui, --ignore-certificate-errors</code>	Ignores any SSL certificate errors during report upload
<code>-v, --version</code>	Display CIS-CAT version and JRE information
<code>-vs, --verify-signature</code>	Verify that the XML benchmarks have valid signatures
<code>-x, --report-xml</code>	Creates an XML report
<code>-xc, -xccdf &lt;arg&gt;</code>	Specifies a particular XCCDF benchmark within a data-stream to select (SCAP 1.2 Data-Stream Collections Only)
<code>-y, --report-all-tests</code>	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
<b>Linux/Unix</b>	<code>./CIS-CAT.sh [&lt;options&gt;] [&lt;benchmark&gt;] [&lt;profile&gt;]</code>
<b>Windows</b>	<code>CIS-CAT.bat [&lt;options&gt;] [&lt;benchmark&gt;] [&lt;profile&gt;]</code>

## 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 Professional 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 Professional 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-spl
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-spl]
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
<b>Windows</b>	%HOMEDRIVE%%HOMEPATH%\My Documents\CIS-CAT Results
<b>Unix/Linux</b>	\$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 quarterlyAssessment ...
Unix> ./CIS-CAT.sh -r /reports -rn quarterlyAssessment ...

```



## 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
```

## 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 XML results after a CIS-CAT scan is done to a URL specify the -u argument. 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 XML results file is sent to the website it will be sent over as a POST and the XML result 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']);
    }
}
```



# 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
<b>1 Computer Configuration</b>	<b>204</b>	<b>42</b>	<b>0</b>	<b>51</b>	<b>204.0</b>	<b>249.0</b>	<b>82%</b>
1.1 <a href="#">Administrative Templates</a>	37	40	0	7	37.0	77.0	48%
1.1.1 <a href="#">Windows Components</a>	21	38	0	5	21.0	59.0	36%
1.1.1.1 <a href="#">BitLocker Drive Encryption</a>	2	38	0	0	2.0	40.0	5%
1.1.1.1.1 <a href="#">Operating System Drives</a>	0	16	0	0	0.0	16.0	0%
1.1.1.1.2 <a href="#">Fixed Data Drives</a>	1	10	0	0	1.0	11.0	9%
1.1.1.1.3 <a href="#">Removable Data Drives</a>	1	11	0	0	1.0	12.0	8%
1.1.1.2 <a href="#">AutoPlay Policies</a>	1	0	0	0	1.0	1.0	100%
1.1.1.3 <a href="#">Event Log Service</a>	6	0	0	0	6.0	6.0	100%
1.1.1.3.1 <a href="#">Application</a>	2	0	0	0	2.0	2.0	100%
1.1.1.3.2 <a href="#">Security</a>	2	0	0	0	2.0	2.0	100%
1.1.1.3.3 <a href="#">System</a>	2	0	0	0	2.0	2.0	100%
1.1.1.4 <a href="#">Windows Remote Shell</a>	1	0	0	0	1.0	1.0	100%
1.1.1.5 <a href="#">Windows Explorer</a>	1	0	0	0	1.0	1.0	100%
1.1.1.6 <a href="#">Windows Update</a>	5	0	0	3	5.0	5.0	100%
1.1.1.7 <a href="#">Credential User Interface</a>	1	0	0	1	1.0	1.0	100%
1.1.1.8 <a href="#">Remote Desktop Services</a>	4	0	0	0	4.0	4.0	100%
1.1.1.8.1 <a href="#">Remote Desktop Session Host</a>	3	0	0	0	3.0	3.0	100%
1.1.1.8.1.1 <a href="#">Security</a>	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](#)

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

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.

[Show Rule XML](#)

**Test(s)**  
This item has a scoring weight of 1.000.  
«Check that '&#39;User Account Control: Virtualize file and registry write failures to per-user locations&#39; is configured to '&#39;Enabled&#39;»

[Show Rule Result XML](#)

**References:**

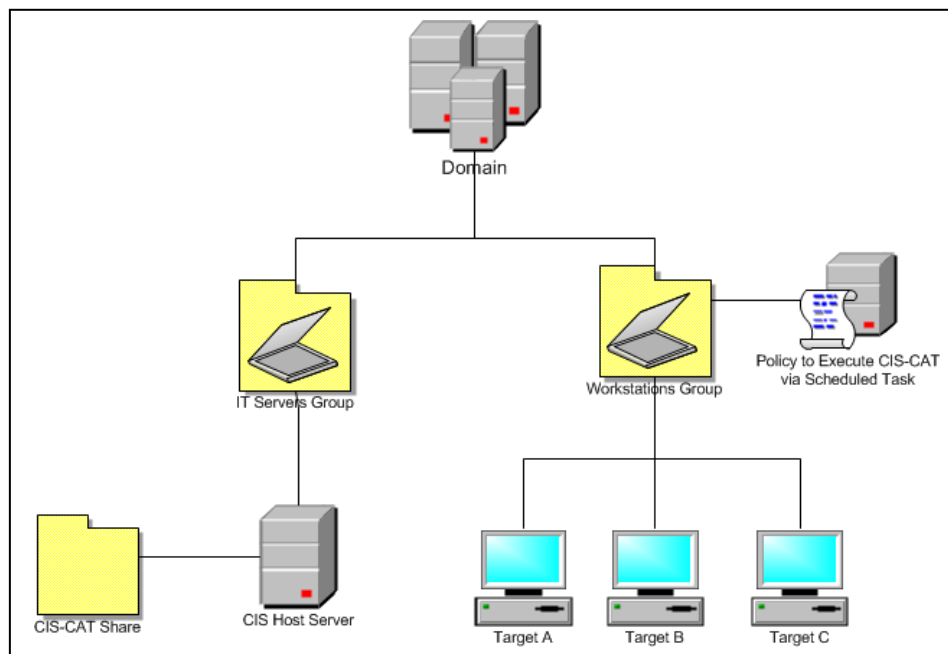
- CCE-IDs: [CCE-8817-9](#) -- [More](#)

[Back to Summary](#)

To view the XCCDF constructs, click the `Show Rule Result XML` link below the `Tests` dialog box. 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.

## Prerequisites

1. All targets must be joined to an Active Directory Domain
2. All targets must have read and write 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 bundle within the CIS folder on the *CIS Host Server*.
3. Create the following two directories beneath the CIS folder on the *CIS Host Server*:
  - a. Reports

- b. Java
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 JRE that applies to the targets you will be evaluating, such as jre1.5.0\_19, to the Java folder you created in step 3.
5. Move CIS\cis-cat-full\misc\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\Reports

### *Security Considerations*

The CIS\Reports folder will contain reports that detail configuration related vulnerabilities for each system evaluated by CIS-CAT. As such, Read, List folder Contents, Modify, and Write access to the contents of this folder should be restricted. One way to accomplish this is to create a domain user, *CIS-CAT Domain User*, that resides in the local administrators group on each target system. Execute CIS-CAT under the context of this user. Restrict access to the CIS\Reports directory such that only this new domain user, and appropriate personnel, can write to or read from this folder.

Write and Modify permissions to following the resources should also be limited to domain administrators and security personnel:

- CIS\cis-cat-centralized.bat
- CIS\cis-cat-full
- CIS\Java

Anyone with the ability to write to the above resources will be able to execute arbitrary commands on target systems under the context of the *CIS-CAT Domain User* (local Administrator). Additionally, Write, Modify, Read and Execute permissions on the above resources should be limited to the *CIS-CAT Domain User*.

### *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
SET JavaPath=Java\jre1.5.0_19
SET JavaPath64=Java64\jre1.5.0_19
```

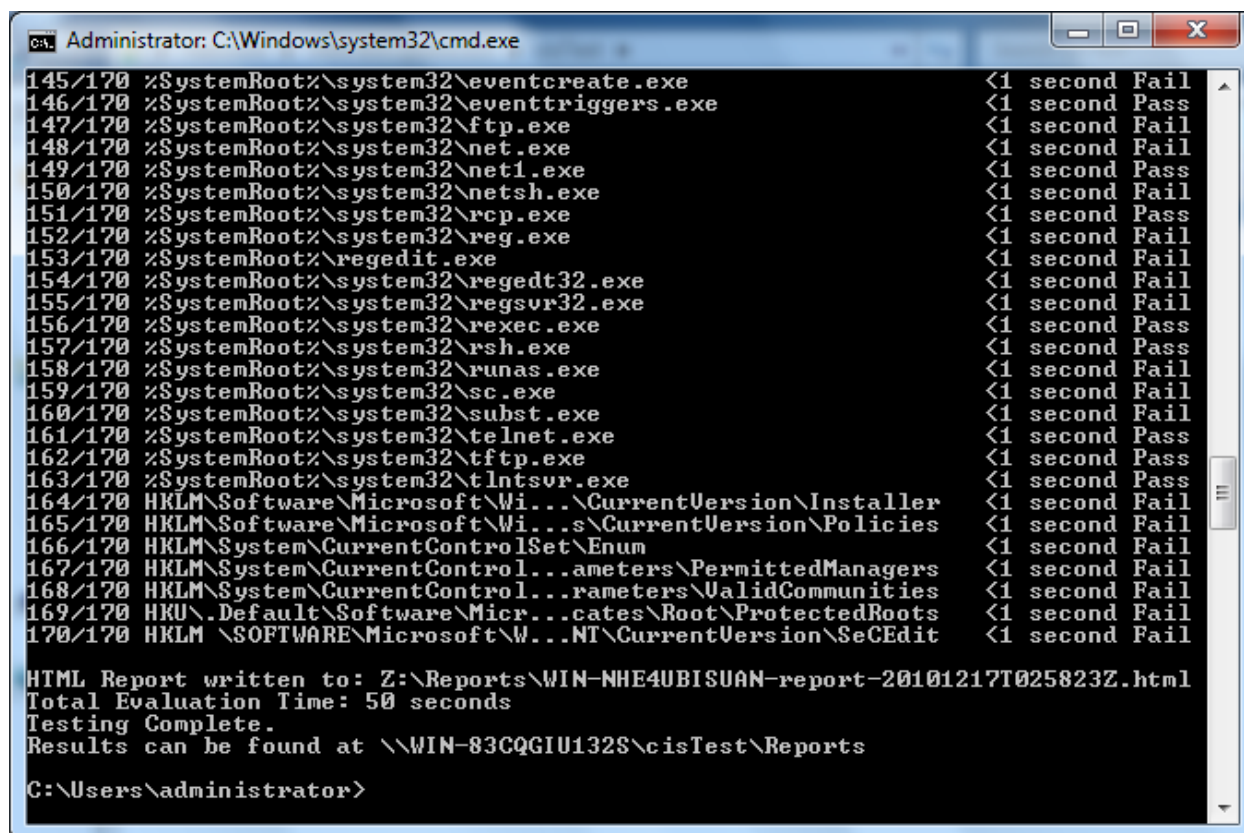
Replace `CisHostServer` with the fully qualified domain name or IP address of the *CIS-CAT Host Server*. Replace `jre_1.5.0_19` with version of Java installed in Step 4 under [Create CIS Share on the CIS Hosting Server](#).

### Validate the Install

To test the setup, execute the following command *from an elevated command prompt* on one of the target systems in the *Workstation Group*:

```
cmd.exe /c \\<CiSHostServer>\CIS\cis-cat-centralized.bat
```

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



```
Administrator: C:\Windows\system32\cmd.exe
145/170 %SystemRoot%\system32\eventcreate.exe <1 second Fail
146/170 %SystemRoot%\system32\eventtriggers.exe <1 second Pass
147/170 %SystemRoot%\system32\ftp.exe <1 second Fail
148/170 %SystemRoot%\system32\net.exe <1 second Fail
149/170 %SystemRoot%\system32\net1.exe <1 second Pass
150/170 %SystemRoot%\system32\netsh.exe <1 second Fail
151/170 %SystemRoot%\system32\rcp.exe <1 second Pass
152/170 %SystemRoot%\system32\reg.exe <1 second Fail
153/170 %SystemRoot%\regedit.exe <1 second Fail
154/170 %SystemRoot%\system32\regedt32.exe <1 second Fail
155/170 %SystemRoot%\system32\regsvr32.exe <1 second Fail
156/170 %SystemRoot%\system32\rexc.exe <1 second Pass
157/170 %SystemRoot%\system32\rsh.exe <1 second Pass
158/170 %SystemRoot%\system32\runas.exe <1 second Fail
159/170 %SystemRoot%\system32\sc.exe <1 second Fail
160/170 %SystemRoot%\system32\subst.exe <1 second Fail
161/170 %SystemRoot%\system32\telnet.exe <1 second Pass
162/170 %SystemRoot%\system32\tftp.exe <1 second Pass
163/170 %SystemRoot%\system32\tlntsvr.exe <1 second Pass
164/170 HKLM\Software\Microsoft\Wi...CurrentVersion\Installer <1 second Fail
165/170 HKLM\Software\Microsoft\Wi...s\CurrentVersion\Policies <1 second Fail
166/170 HKLM\System\CurrentControlSet\Enum <1 second Fail
167/170 HKLM\System\CurrentControl...ameters\PermittedManagers <1 second Fail
168/170 HKLM\System\CurrentControl...rameters\ValidCommunities <1 second Fail
169/170 HKU\.Default\Software\Micr...cates\Root\ProtectedRoots <1 second Fail
170/170 HKLM \SOFTWARE\Microsoft\W...NT\CurrentVersion\SeCEdit <1 second Fail

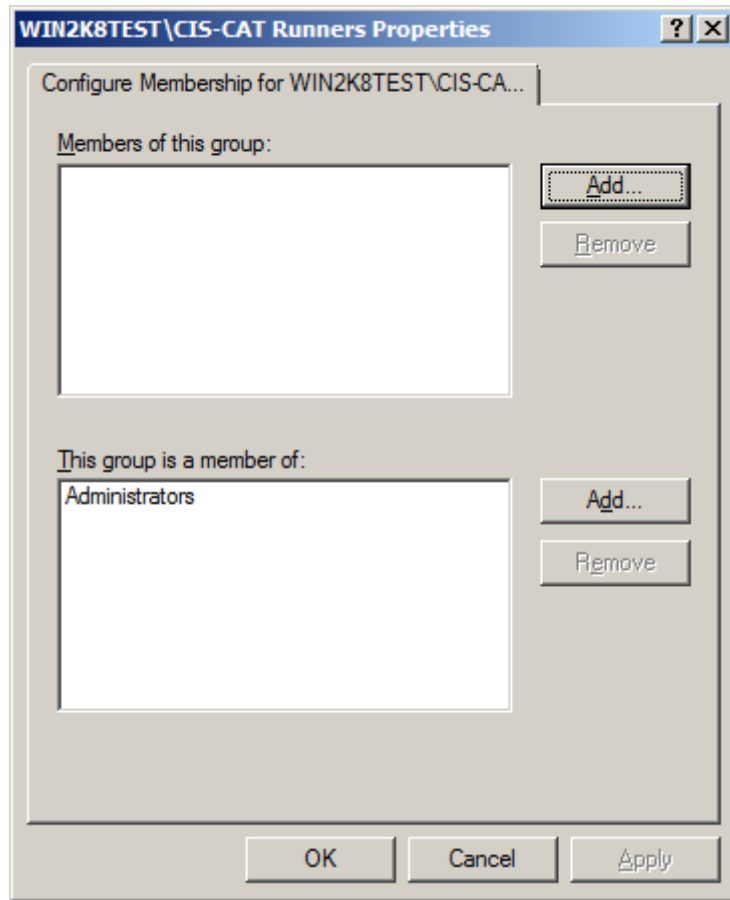
HTML Report written to: Z:\Reports\WIN-NHE4UBISUAN-report-20101217T025823Z.html
Total Evaluation Time: 50 seconds
Testing Complete.
Results can be found at \\WIN-83CQGIU132S\cisTest\Reports
C:\Users\administrator>
```

### Configuring the Scheduled Task via Group Policy

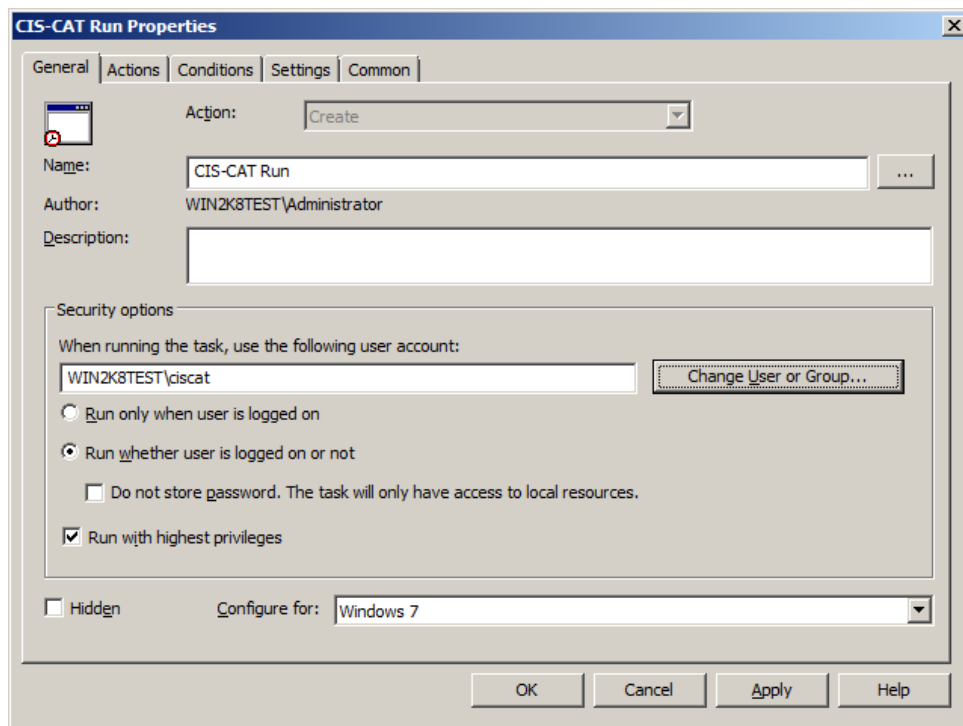
Perform the following steps to create and assign a Group Policy that will cause target systems in the *Workstation Group* to execute CIS-CAT via a Scheduled Task.

1. Run `gpmmc.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. Right click and edit the policy then go to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Restricted Groups then right click and select Add Group. Select the group that has the user(s) that need to run CIS-CAT and then specify "administrators" as the group the CIS-CAT group should be a member of. Like the screen shot below:





- 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 set the user who will be running the task and make sure “Run with highest privileges” is checked.** It should look similar to the below screen shot.

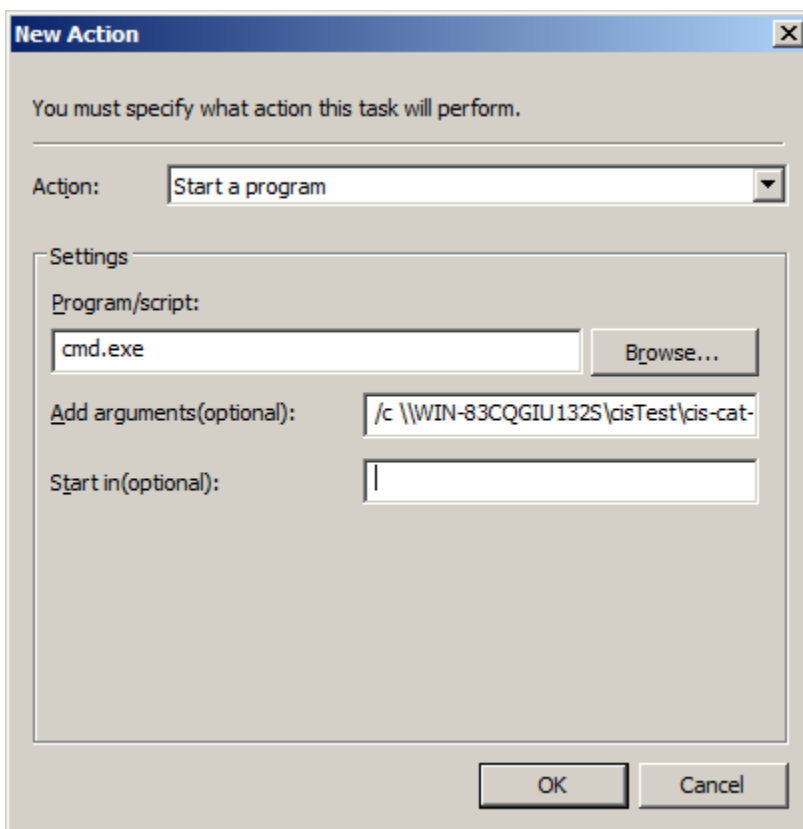


Add in whatever scheduling is needed via the Triggers tab. Then go to the Actions tab click New and specify the following settings:

- 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 be 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 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.

### *Benchmark Considerations*

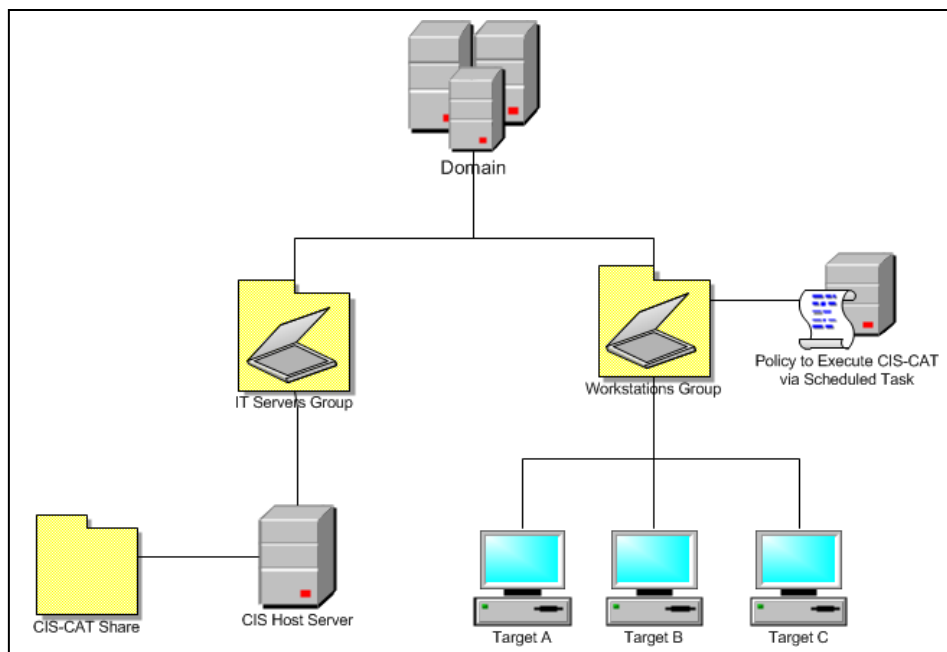
In order to successfully execute this workflow, the scheduled task created via Group Policy must be allowed to store the credentials of the *CIS-CAT Domain User* created in previous steps. If any target

system is configured using CIS benchmarks, certain rules will need to be relaxed in order for these credentials to be stored:

Benchmark	Configuration Item
Windows XP	3.2.1.41: Network Access: Do not allow storage of credentials or .NET passports for network authentication
Windows 8	1.1.3.10.11: Configure 'Network access: Do not allow storage of passwords and credentials for network authentication'
Windows Server 2003	3.2.1.42: Network Access: Do not allow storage of credentials or .NET passports for network authentication
Windows Server 2008	1.9.39: Network Access: Do not allow storage of credentials or .NET Passports for network authentication
Windows Server 2012	1.1.3.11.1: Configure 'Network access: Do not allow storage of passwords and credentials for network authentication'

## 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 60MB 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.

## Prerequisites

1. All targets must be joined to an Active Directory Domain
2. All targets must have read and write 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 full CIS-CAT 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, Read, List folder Contents, Modify, and Write access to the contents of this folder should be restricted. One way to accomplish this is to create a domain user, *CIS-CAT Domain User*, that resides in the local administrators group on each target system. Execute CIS-CAT under the context of this user. Restrict access to the CIS\Reports directory such that only this new domain user, and appropriate personnel, can write to or read from this folder.

Write and Modify permissions to following the resource should also be limited to domain administrators and security personnel:

- CIS\cis-cat-dissolvable.bat

Anyone with the ability to write to the above resources will be able to execute arbitrary commands on target systems under the context of the *CIS-CAT Domain User* (local Administrator). Additionally, Write, Modify, Read and Execute permissions on the above resources should be limited to the *CIS-CAT Domain User*.

## 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%
SET NetworkShare=\\CisHostServer\CIS
```

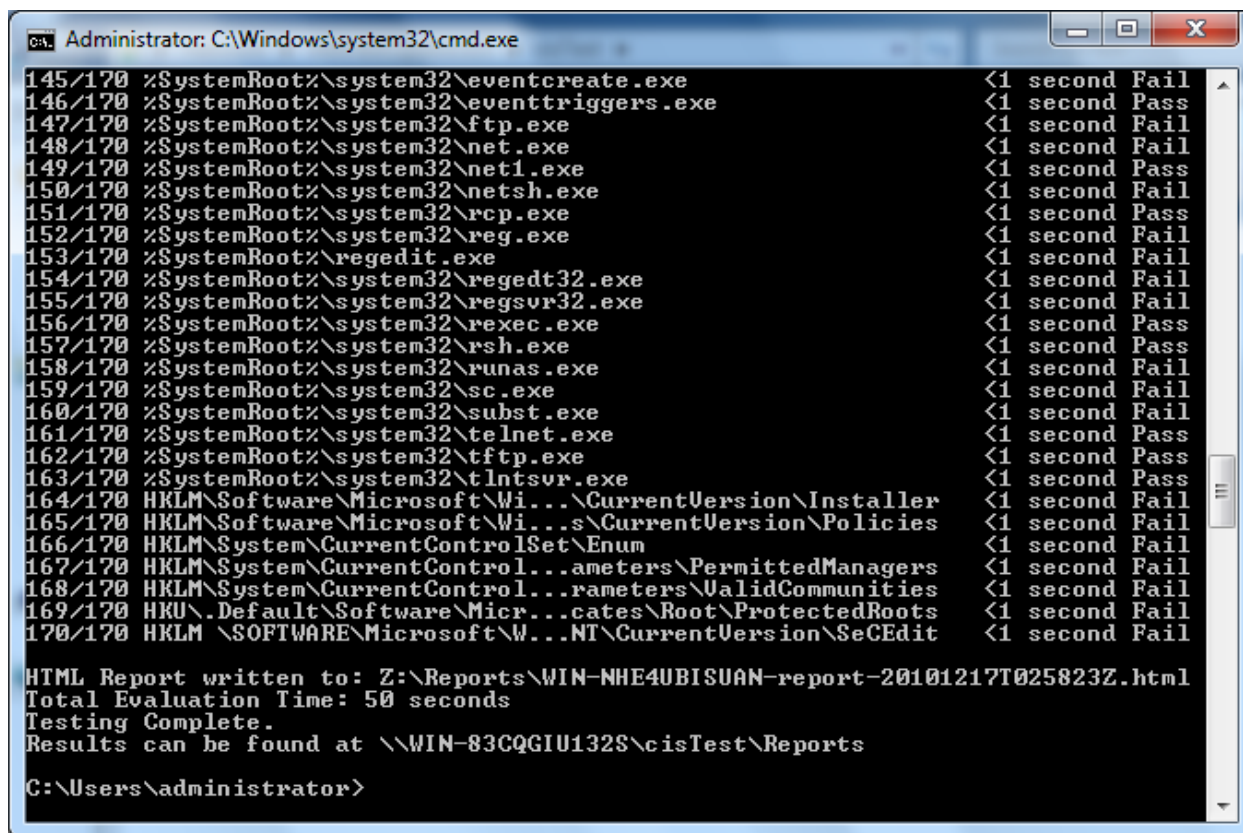
The `RootDir` value should be set to a valid temporary directory into which the CIS-CAT files can be copied. By default this is set to the `%TEMP%` environment variable. Any valid directory in which the user executing the script has permissions, may be used. If the `RootDir` does not resolve to a valid directory, the script will not execute. Replace `CisHostServer` with the fully qualified domain name or IP address of the *CIS-CAT Host Server*.

## Validate the Install

To test the setup, execute the following command from one of the target systems in the *Workstation Group*:

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

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



```
Administrator: C:\Windows\system32\cmd.exe
145/170 %SystemRoot%\system32\eventcreate.exe <1 second Fail
146/170 %SystemRoot%\system32\eventtriggers.exe <1 second Pass
147/170 %SystemRoot%\system32\ftp.exe <1 second Fail
148/170 %SystemRoot%\system32\net.exe <1 second Fail
149/170 %SystemRoot%\system32\net1.exe <1 second Pass
150/170 %SystemRoot%\system32\netsh.exe <1 second Fail
151/170 %SystemRoot%\system32\rcp.exe <1 second Pass
152/170 %SystemRoot%\system32\reg.exe <1 second Fail
153/170 %SystemRoot%\regedit.exe <1 second Fail
154/170 %SystemRoot%\system32\regedt32.exe <1 second Fail
155/170 %SystemRoot%\system32\regsvr32.exe <1 second Fail
156/170 %SystemRoot%\system32\rexec.exe <1 second Pass
157/170 %SystemRoot%\system32\rsh.exe <1 second Pass
158/170 %SystemRoot%\system32\runas.exe <1 second Fail
159/170 %SystemRoot%\system32\sc.exe <1 second Fail
160/170 %SystemRoot%\system32\subst.exe <1 second Fail
161/170 %SystemRoot%\system32\telnet.exe <1 second Pass
162/170 %SystemRoot%\system32\tftp.exe <1 second Pass
163/170 %SystemRoot%\system32\tlntsvr.exe <1 second Pass
164/170 HKLM\Software\Microsoft\Windows\CurrentVersion\Installer <1 second Fail
165/170 HKLM\Software\Microsoft\Windows\CurrentVersion\Policies <1 second Fail
166/170 HKLM\System\CurrentControlSet\Enum <1 second Fail
167/170 HKLM\System\CurrentControlSet\Parameters\PermittedManagers <1 second Fail
168/170 HKLM\System\CurrentControlSet\Parameters\ValidCommunities <1 second Fail
169/170 HKU\.\Default\Software\Microsoft\Windows\CurrentVersion\ProtectedRoots <1 second Fail
170/170 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SeCEdit <1 second Fail

HTML Report written to: Z:\Reports\WIN-NHE4UBISUAN-report-20101217T025823Z.html
Total Evaluation Time: 50 seconds
Testing Complete.
Results can be found at \\WIN-83CQGIU132S\cisTest\Reports

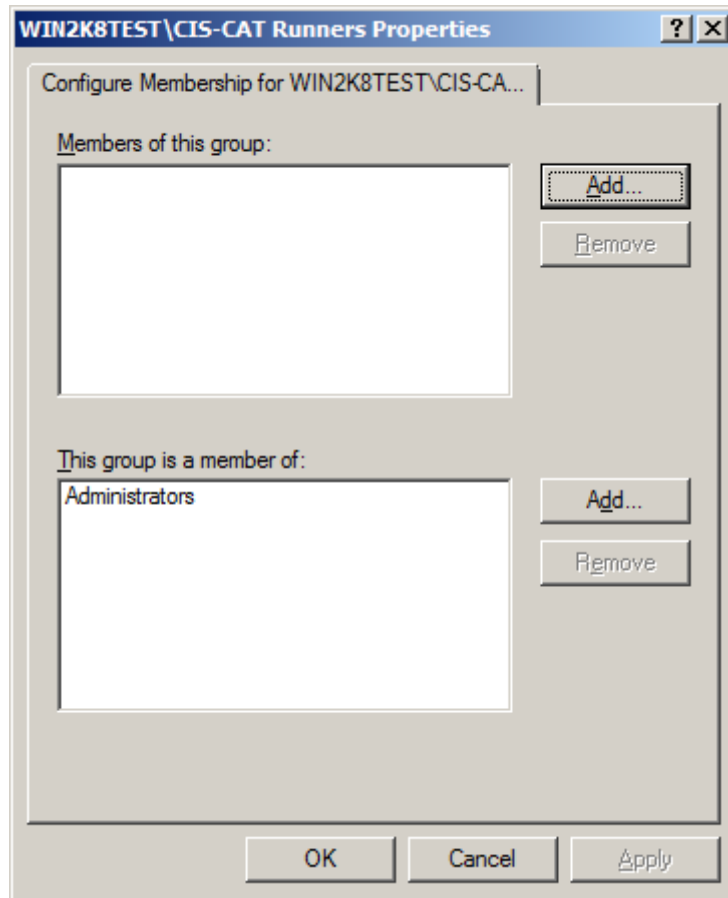
C:\Users\administrator>
```

## Configuring the Scheduled Task via Group Policy

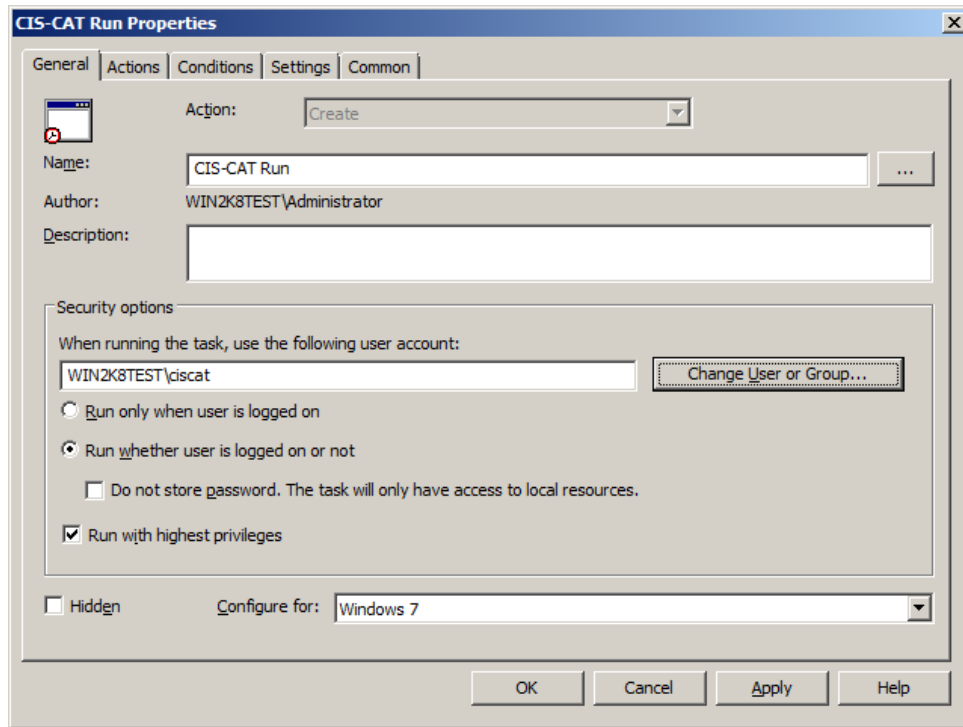
Perform the following steps to create and assign a Group Policy that will cause target systems in the *Workstation Group* to execute CIS-CAT via a Scheduled Task.

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. Right click and edit the policy then go to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Restricted Groups then right click and select Add Group. Select the group that has the user(s) that need to run CIS-CAT and then specify "administrators" as the group the CIS-CAT group should be a member of. Like the screen shot below:



4. 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 set the user who will be running the task and make sure "Run with highest privileges" is checked. It should look similar to the below screen shot.

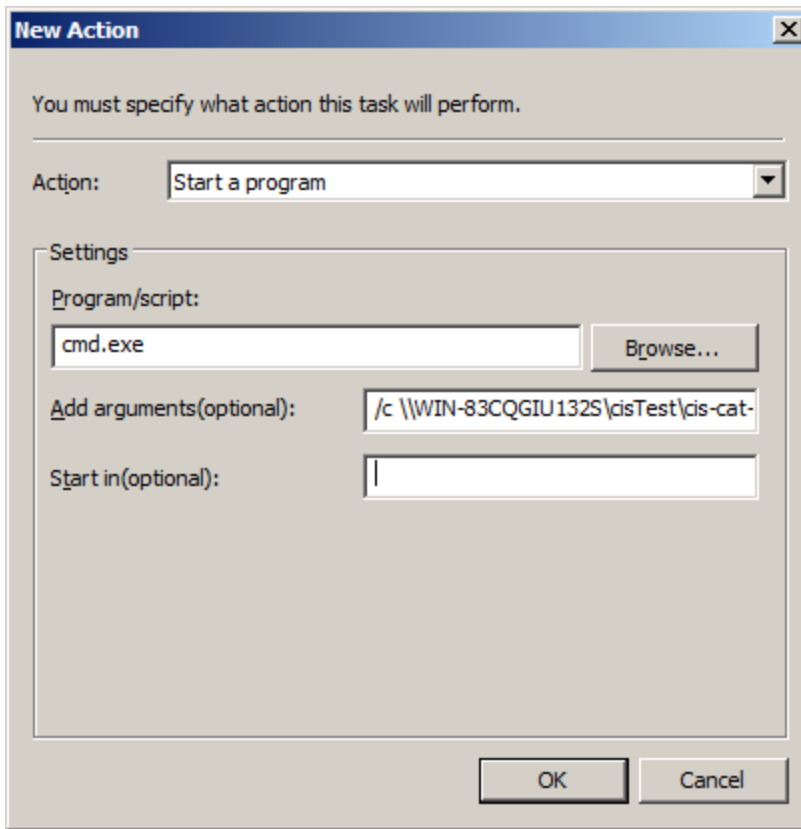


Add in whatever scheduling is needed via the Triggers tab. Then go to the Actions tab click New and specify the following settings:

- 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:



CIS-CAT 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 80 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.

### *Benchmark Considerations*

In order to successfully execute this workflow, the scheduled task created via Group Policy must be allowed to store the credentials of the *CIS-CAT Domain User* created in previous steps. If any target system is configured using CIS benchmarks, certain rules will need to be relaxed in order for these credentials to be stored:

Benchmark	Configuration Item
Windows XP	3.2.1.41: Network Access: Do not allow storage of credentials or .NET passports for network authentication
Windows 8	1.1.3.10.11: Configure ‘Network access: Do not allow storage of passwords and credentials for network authentication’
Windows Server 2003	3.2.1.42: Network Access: Do not allow storage of credentials or .NET passports for network authentication
Windows Server 2008	1.9.39: Network Access: Do not allow storage of credentials or .NET Passports for network authentication



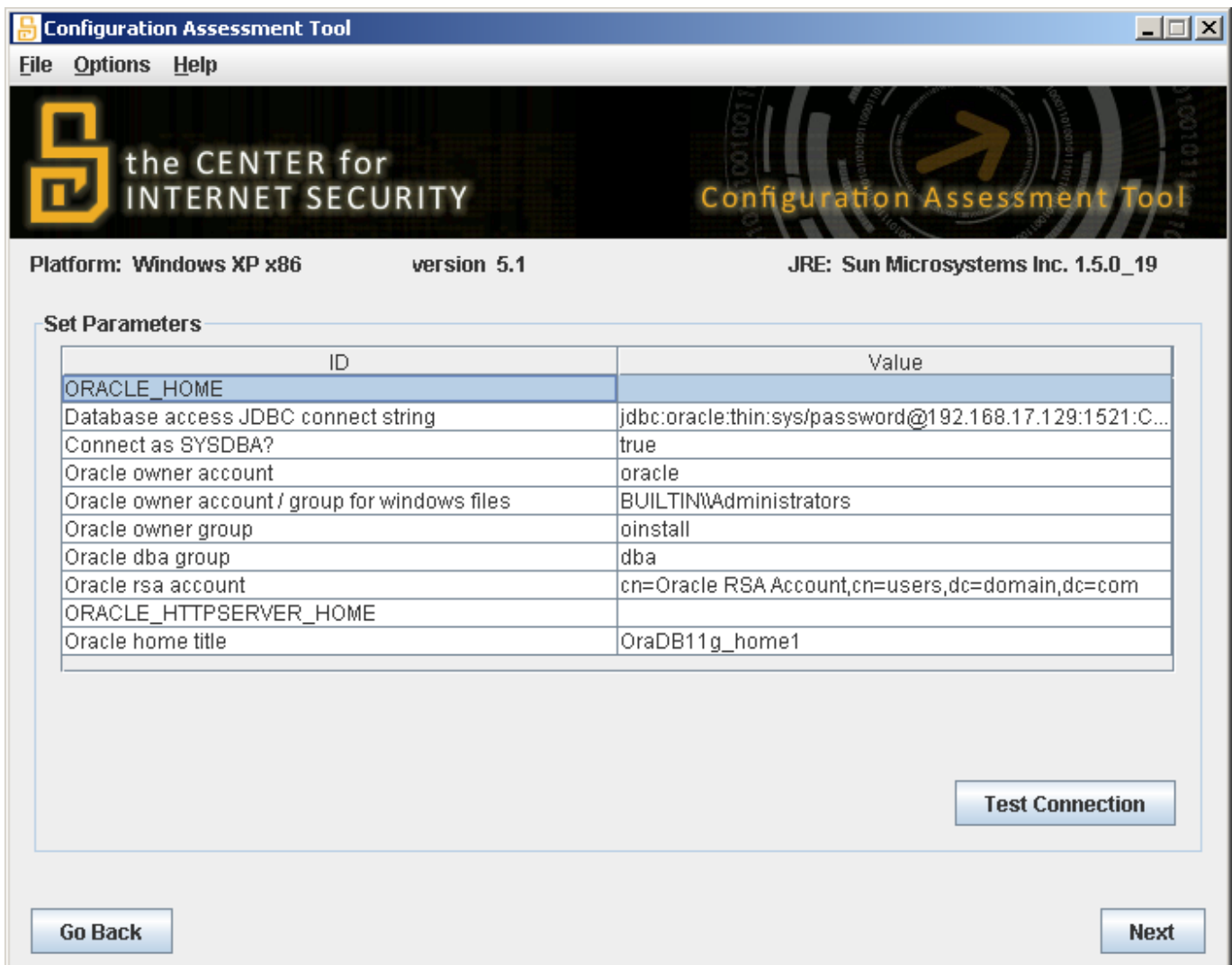


# Using CIS-CAT with Database Benchmarks

## 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 `ORACLE_HOME` variable, see

[http://docs.oracle.com/cd/E11857\\_01/em.111/e12255/oui2\\_manage\\_oracle\\_homes.htm](http://docs.oracle.com/cd/E11857_01/em.111/e12255/oui2_manage_oracle_homes.htm)

- a. 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 following components of the JDBC string must be changed in order for CIS-CAT to successfully connect to the Oracle instance:
  - b. Credentials - "sys/password" must be replaced by a valid username and password.
  - c. IP Address - the IP address must be updated to the IP address the Oracle server is bound to.
  - d. TCP Port - Oracle is typically bound to port 1521/TCP. Confirm the Oracle server you intend to assess is bound to this port. If not, update the JDBC string accordingly.
  - e. Database SID - Replace "CIS" with the SID of the Oracle database instance you intend to assess with CIS-CAT. For more information on SIDs, please see [http://asktom.oracle.com/pls/asktom/f?p=100:11:0:::P11\\_QUESTION\\_ID:318216852435](http://asktom.oracle.com/pls/asktom/f?p=100:11:0:::P11_QUESTION_ID:318216852435)
2. The `Connect as SYSDBA` parameter determines if CIS-CAT will connect to the Oracle instance with the SYSDBA privilege. This is required for CIS-CAT 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:61866277480450](http://asktom.oracle.com/pls/asktom/f?p=100:11:0:::P11_QUESTION_ID:61866277480450).
3. 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".
4. The `oracle owner account / group for windows files` parameter refers to the Windows principal that the Oracle service was installed as. I.e. "oracle".
5. 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".
6. The `oracle dba group` parameter refers to the Linux group that Oracle DBAs belong to. I.e "dba".
7. 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.
8. The `ORACLE_HTTPSERVER_HOME` parameter corresponds with the Oracle Database server's `ORACLE_HTTPSERVER_HOME` environment variable. CIS-CAT 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](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://<hostname>[:<port>][/<instance>][;<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
<b>Server Name</b>	CIS-SERVER
<b>Database Name</b>	TestDB
<b>Database Port</b>	1433
<b>Windows Domain</b>	WIN-DOMAIN
<b>Windows Domain User &amp; Password</b>	jsmith/qw3rty

## SQL Server Database User & Password

db\_user/db\_pass

### *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;DatabaseName=TestDB;domain=WIN-DOMAIN;user=jsmith;password=qw3rty
```

### *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  
-or-  
jdbc:jtds:sqlserver://CIS-SERVER:1433;DatabaseName=TestDB;user=jsmith;password=qw3rty
```

#### 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>

## 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>

## 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](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](http://www.w3schools.com/tags/ref_colorpicker.asp).

## 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, and 5.10.1 of the OVAL language.

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

Component Schema	Implemented OVAL Tests
<b>Platform Independent Definitions</b>	<ul style="list-style-type: none"> <li>• family_test</li> <li>• filehash_test</li> <li>• filehash58_test</li> <li>• environmentvariable_test</li> <li>• environmentvariable58_test</li> <li>• sql57_test</li> <li>• textfilecontent_test</li> <li>• textfilecontent54_test</li> <li>• unknown_test</li> <li>• variable_test</li> <li>• xmlfilecontent_test</li> </ul>
<b>Unix Definitions</b>	<ul style="list-style-type: none"> <li>• file_test</li> <li>• inetd_test</li> <li>• password_test</li> <li>• process58_test</li> <li>• runlevel_test</li> <li>• shadow_test</li> <li>• uname_test</li> <li>• xinetd_test</li> </ul>

<b>Linux Definitions</b>	<ul style="list-style-type: none"> <li>• partition_test</li> <li>• rpminfo_test</li> <li>• selinuxboolean_test</li> </ul>
<b>Windows Definitions</b>	<ul style="list-style-type: none"> <li>• accesstoken_test</li> <li>• auditeventpolicy_test</li> <li>• auditeventpolicysubcategories_test</li> <li>• cmdlet_test</li> <li>• file_test</li> <li>• fileauditedpermissions_test</li> <li>• fileauditedpermissions53_test</li> <li>• fileeffectiverights_test</li> <li>• fileeffectiverights53_test</li> <li>• group_test</li> <li>• group_sid_test</li> <li>• interface_test</li> <li>• lockoutpolicy_test</li> <li>• passwordpolicy_test</li> <li>• process58_test</li> <li>• registry_test</li> <li>• regkeyeffectiverights_test</li> <li>• regkeyeffectiverights53_test</li> <li>• service_test</li> <li>• serviceeffectiverights_test</li> <li>• sid_test</li> <li>• sid_sid_test</li> <li>• uac_test</li> <li>• user_test</li> <li>• user_sid_test</li> <li>• user_sid55_test</li> <li>• volume_test</li> <li>• wmi_test</li> <li>• wmi57_test</li> <li>• wuaupdatesearcher_test</li> </ul>

### *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<sup>i</sup>. 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.<sup>ii</sup> 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.

---

<sup>i</sup> [http://csrc.nist.gov/publications/nistir/ir7502/nistir-7502\\_CCSS.pdf](http://csrc.nist.gov/publications/nistir/ir7502/nistir-7502_CCSS.pdf)

<sup>ii</sup> <http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf>