



STIG Viewer 2.x User Guide

Version 1, Release 2

March 2016

Developed by DISA for the DoD

This page is intentionally blank.

TABLE OF CONTENTS

	Page
1. INTRODUCTION	1
1.1 About DoD/DISA STIG Viewer	1
2. INSTALLING STIG VIEWER 2.X	3
2.1.1 Opening STIG Viewer	4
2.1.2 STIG Explorer tab - Menu Selections	5
3. LOAD STIGS	6
3.1.1 Create Checklist from STIG	8
3.1.2 Checklist tab - Menu Selections	11
4. CHECKLIST SECTIONS	12
4.1.1 Checklist – Target Data Section	12
4.1.2 Checklist – Totals Section	13
4.1.3 Checklist – STIGs Section	14
4.1.4 Checklist – Technology Area Section	15
4.1.5 Checklist – Filter Options Section	16
4.1.6 Checklist – General Information Section	17
4.1.7 Checklist – Vuln Information Section	18
4.1.8 Checklist – Finding Details Section and Comments Section	20

This page is intentionally blank.

1. INTRODUCTION

STIG Viewer 2.x is a replacement for previous DISA tool (STIG Viewer 1.2). The intent of this User Guide is to assist in navigating 2.x and describing functionalities from a user perspective.

1.1 About DoD/DISA STIG Viewer

The DoD/DISA STIG Viewer tool provides the capability to view one or more XCCDF.xml formatted STIGs in an easy to navigate human readable format. It is compatible with STIGs developed and published by DISA for the DoD. The purpose of the STIG Viewer is to provide an intuitive graphical user interface that allows ease of access to the STIG content along with additional search and sort functionality unavailable with the current method of viewing the STIGs using a style sheet in a web browser. STIG Viewer also supports additional functionality. STIG Viewer features:

- STIG Viewer allows multiple STIGs to be imported and utilized when creating checklists (NOTE: the current version of STIG Viewer allows only a single checklist to be open at a time.)
- One or more XCCDF STIG files can be individually loaded.
- XCCDF STIG files can be extracted from zipped STIG packages.
- A 'Local Save-point' can be created on a system to store user configuration data and the current set of imported STIGs. This permits the last set of loaded STIGs to be reloaded each time the STIG Viewer is started. The 'Local Save-point' can be deleted from the Viewer's options menu. Only one 'Local Save-point' can be created at a time.
- Multiple XCCDF STIG files can be simultaneously unzipped and loaded from a .zip file containing one or more folders which contain the zipped STIG packages. STIG Viewer will drill down to find all XCCDF files and load them. A 'Local Save-point' is required for this operation as all XCCDF files are extracted to its local folder.
- The list of STIG requirements/vulnerabilities can be sorted by STIG ID, Vulnerability ID, or Rule ID.
- All loaded STIG files can be searched or filtered based on one or more keywords. All fields or individual fields can be searched. A filtered list of STIG requirements/vulnerabilities is returned.
- CCI data can be displayed if the CCI reference is contained in the STIG requirements/vulnerabilities.

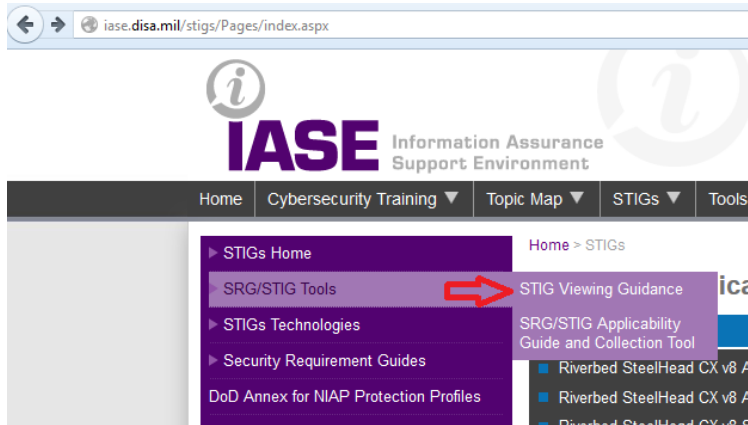
- Loaded and filtered STIG data can be printed or exported to HTML and RTF file formats for use with other programs (i.e. web browsers and Microsoft Word). The printed/exported data is based on the list of requirements displayed in the center pane of the viewer. The output is formatted as a table containing each requirement.
- A manual review checklist can be generated from the currently loaded STIG (or STIGs) or a filtered list. The checklist is generated from all requirements showing in the center pane. This checklist can be used to manually enter review results and notes. The manual review checklist can be saved and reloaded.
- The manual review checklist can be formatted as a short form paper checklist for recording review results. This format can be exported to a file or printed.
- Automated review SCAP XCCDF Results files can be imported into the checklist, populating the checklist with the automated results. The manual portion of the review can be completed and added to the automated results.
- The checklist can be exported as a .CSV file.

NOTES:

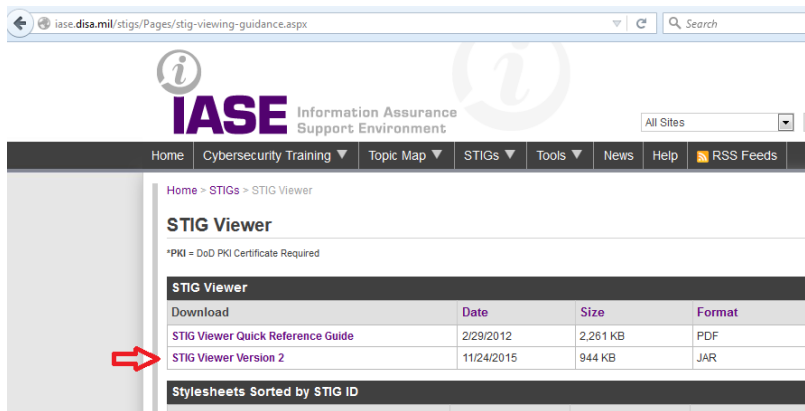
1. This project is produced in Java, and delivered as a single JAR file. It requires the Java Runtime Environment (JRE) be installed on the user's machine to run. This allows the program to be run on any operating system for which the JRE is produced. This also limits the program to running at the permission level of the currently logged in user.
2. The STIG Viewer does not open or make use of any network connections.
3. 'Local Save-points' are created in the logged in user's "local directory" as defined by JAVA. This is a different location in each operating system. Under Windows 7 this is in the %USERPROFILE%\AppData\Local\STIGV_AppData directory. This folder is deleted when the 'Local Save-point' is deleted.
4. The input to the STIG Viewer is an XCCDF XML file, other file types are rejected. STIG Viewer is optimized to XCCDF Formatted STIGs produced by DISA for DoD.

2. INSTALLING STIG VIEWER 2.X

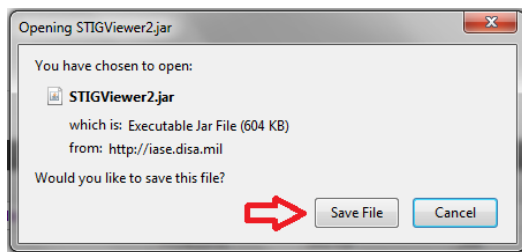
STIG Viewer 2.x can be downloaded from the IASE website. Go to SRG/STIG Tools - STIG Viewing Guidance...



...and click on STIG Viewer Version 2.

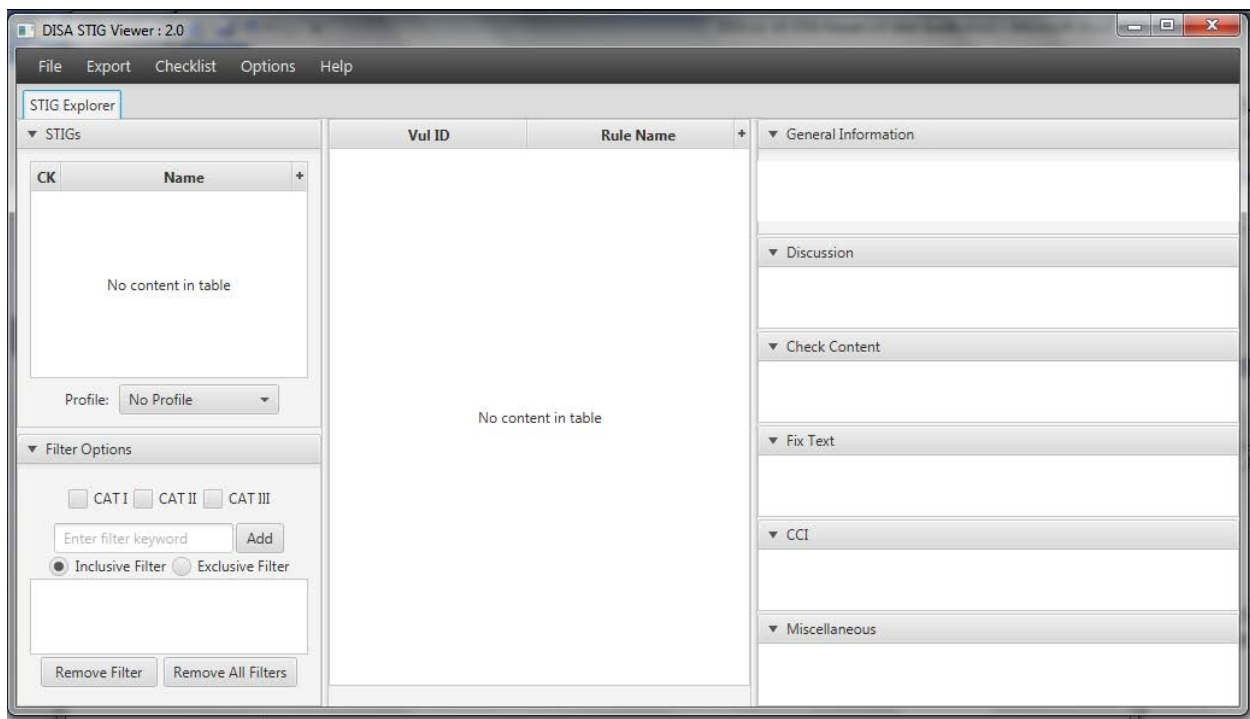


Click on Save File, and save to your computer as STIGViewer2.jar file.



2.1.1 Opening STIG Viewer

1. Invoke/Open STIG Viewer (STIGViewer2.jar). Empty STIG Viewer looks like this:



2. There are three main columns to the Viewer.

Left column - will contain STIG names and Filters.

Center column - will contain Vulnerability ID information.

Right column - will contain Vulnerability detail information.

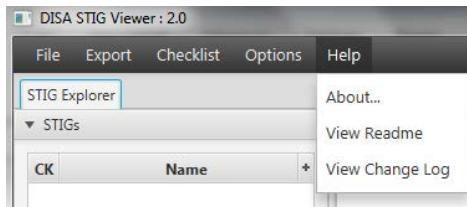
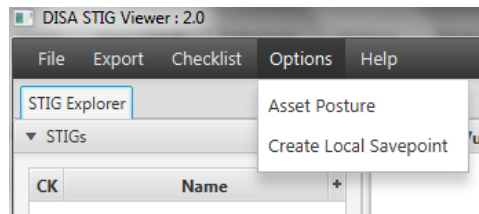
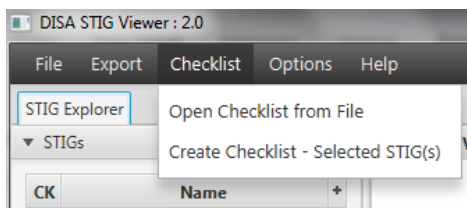
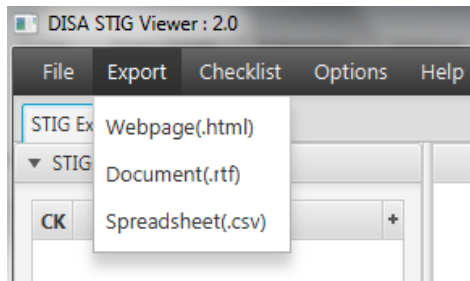
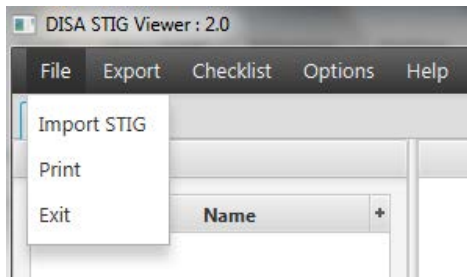
3. The Left and Right columns have collapsible sections in each. Clicking on small arrowheads to left of each section label will toggle section to either expand or collapse. (You cannot vertically slide the divider between sections to adjust their size. The more sections you collapse, the wider each other section will open.

Left column labels - STIGS, Filter Options

Right column labels - General Information, Discussion, Check Content, Fix Text, CCI, Miscellaneous

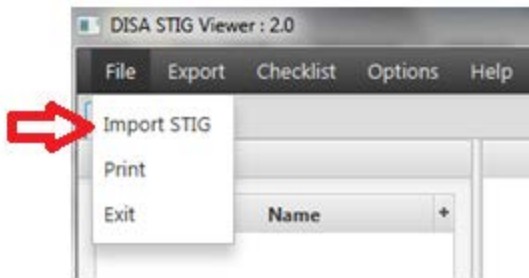
2.1.2 STIG Explorer tab - Menu Selections

1. STIG Explorer tab has 5 Menu drop-down selections (File, Export, Checklist, Options, Help). Choices within each selection are shown below:

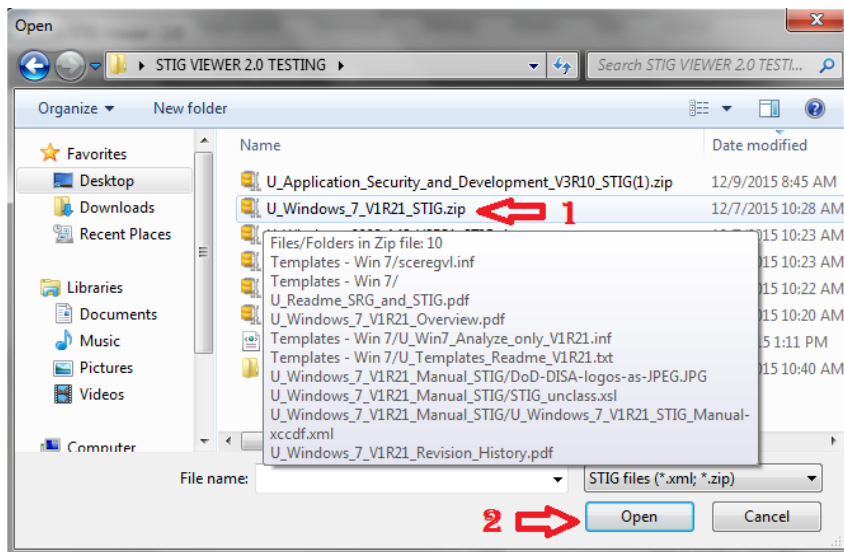


3. Load STIGS

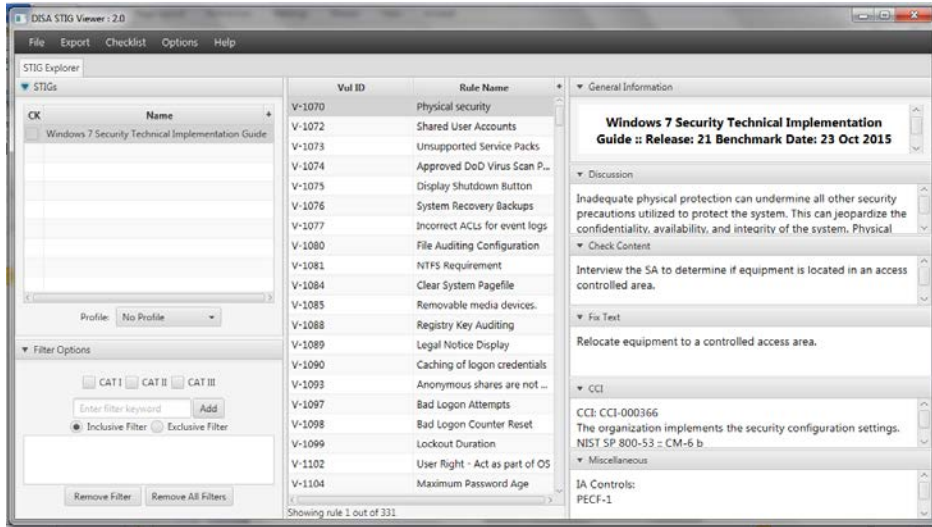
1. STIGs can be downloaded from the IASE website. They are provided as .zip files, to be loaded into STIG Viewer. All STIGs are handled the same by the Viewer, so this guide provides generic instructions, suitable for all technologies. From the STIG Explorer tab, select Menu item FILE – Import STIG.



2. Select STIG .zip file you wish to load and click Open button. This example shows a Windows 7 STIG.

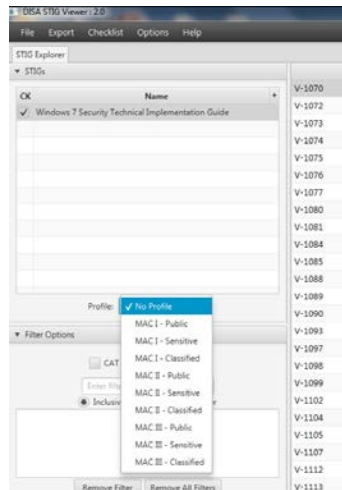


3. STIG Viewer will show STIG has been loaded.

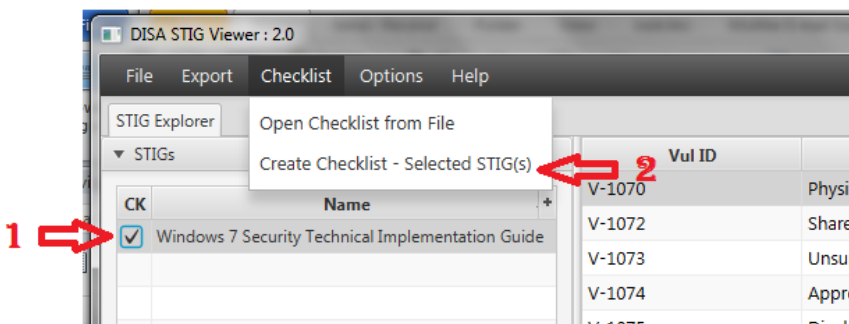


3.1.1 Create Checklist from STIG

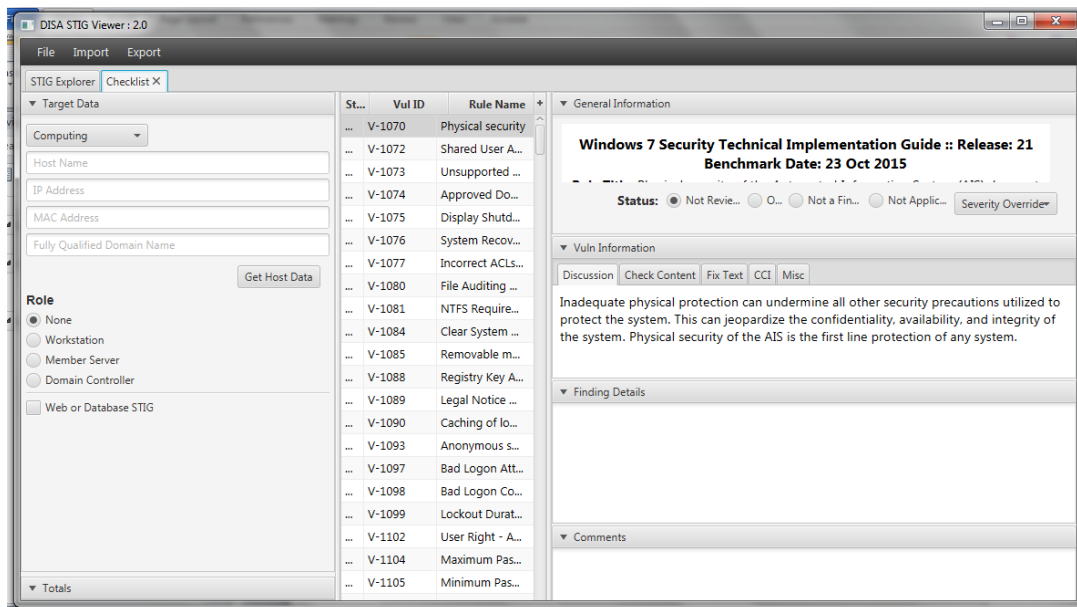
1. Click Profile drop-down and select MAC/Classification Level for checklist being created, for asset being reviewed.



2. Check CK box next to STIG in STIG Explorer, then click Menu item Checklist – Create Checklist – Selected STIG(s).



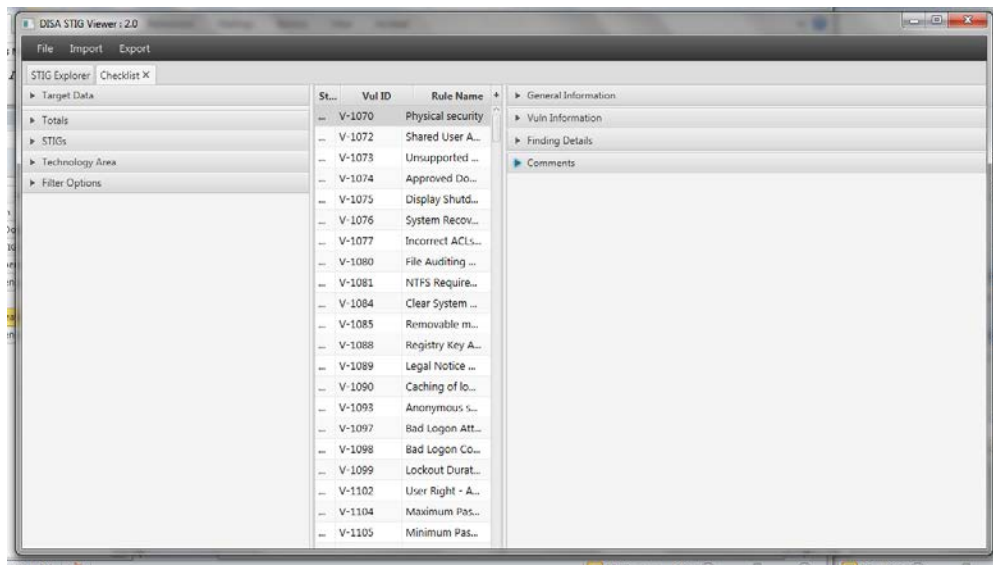
3. A Checklist tab will open, with checklist information for STIG selected.



4. The Checklist tab columns are different from the STIG Explorer tab columns.

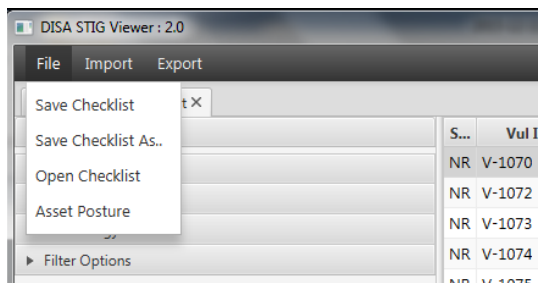
- Left column - will contain Target Data, Totals, STIGs, Technology Area, Filter Options.
- Center column - will contain Vulnerabilities in checklist.
- Right column - will contain General Information, Vuln Information, Finding Details, Comments.

5. To see all sections, you may have to collapse some of them. Here is a view with all sections collapsed.



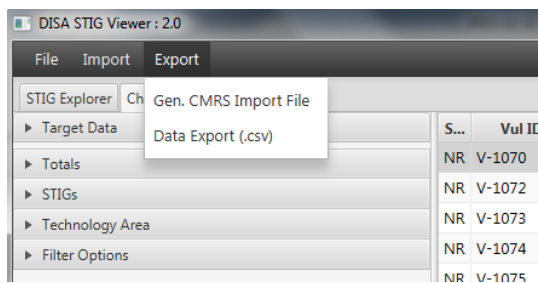
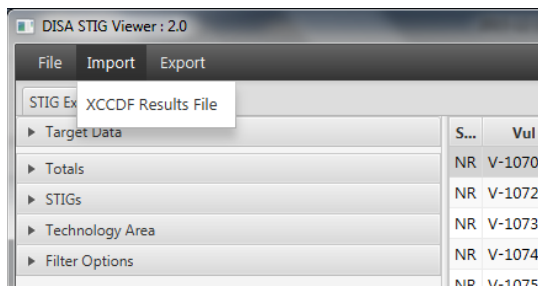
3.1.2 Checklist tab - Menu Selections

1. Checklist tab has 3 Menu drop-down selections (File, Import, Export). Choices within each selection are shown below:



File – Save Checklist As:

Be sure to save checklist to a .ckl file before Exporting .csv file.

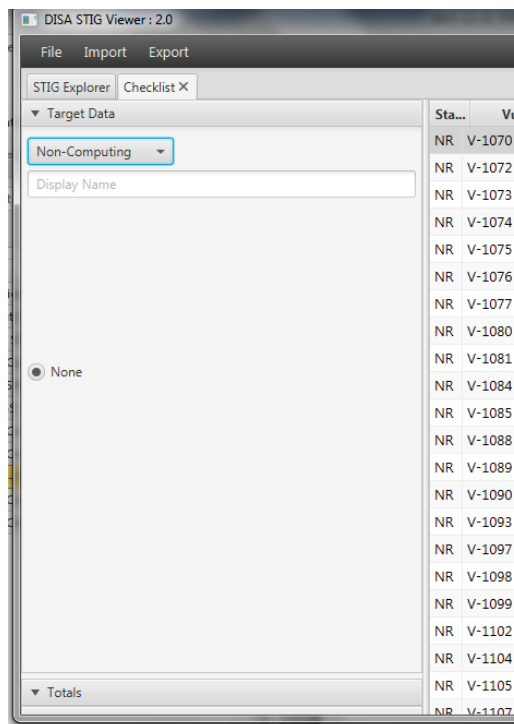
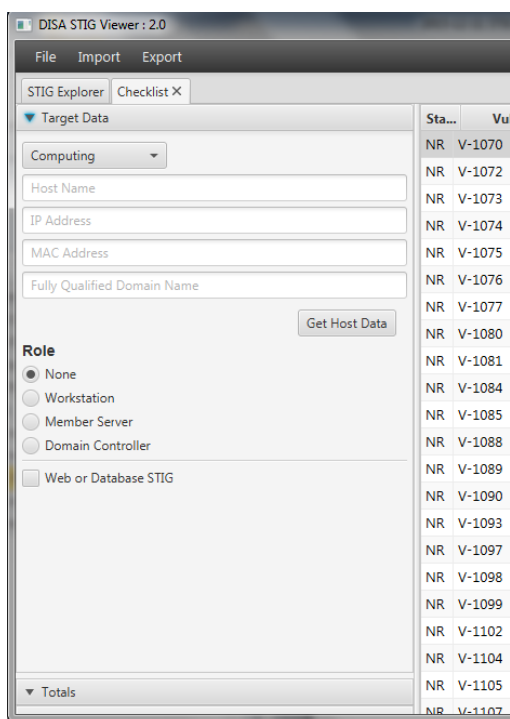


4. Checklist Sections

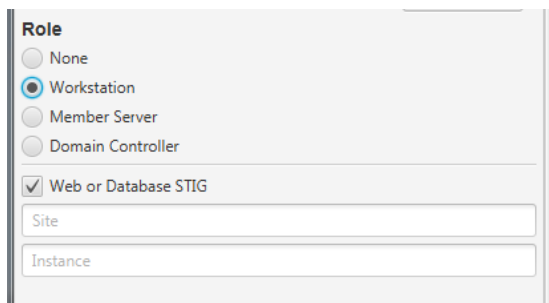
4.1.1 Checklist – Target Data Section

1. The Checklist Target Data section is where the STIG asset is identified. The drop-down button at the top can toggle between Computing and Non-Computing. For Computing asset, enter Host Name, IP Address, and MAC Address of asset being reviewed. For Non-Computing asset, enter the name of asset only.

NOTE: Do NOT click the Get Host Data button. That will only populate the Computing fields with information from computer for which you are running STIG Viewer.

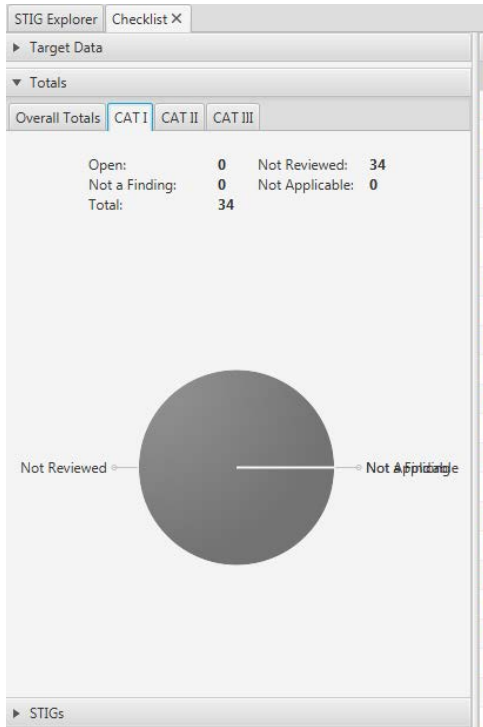


2. Select Role radio button for server type. Clicking the Web or Database STIG box, will provide fields for Site and Instance names.



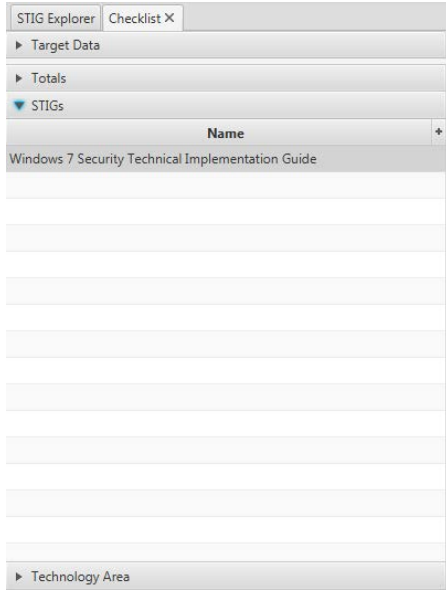
4.1.2 Checklist – Totals Section

1. The Checklist Totals section contains tabs for individual CAT I, II, or III total counts of each vulnerability status, as well as Overall Totals.



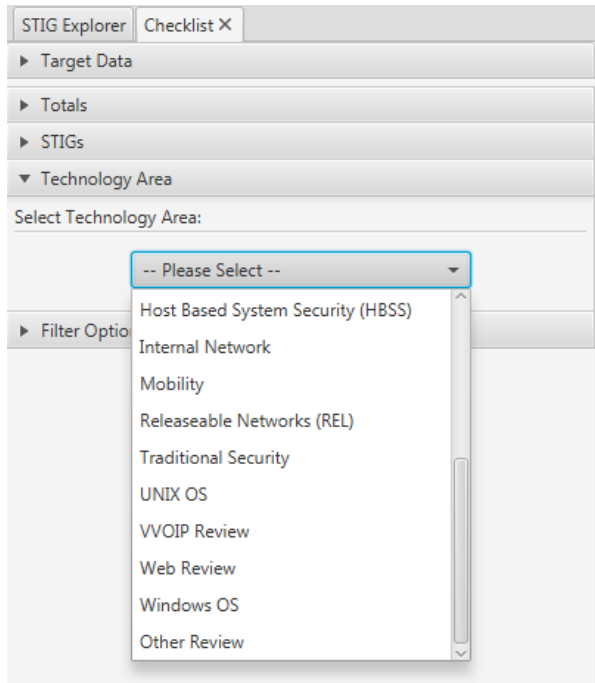
4.1.3 Checklist – STIGs Section

1. The STIGs section contains type of STIGs contained within this Checklist. A single Checklist tab may contain multiple STIGs.



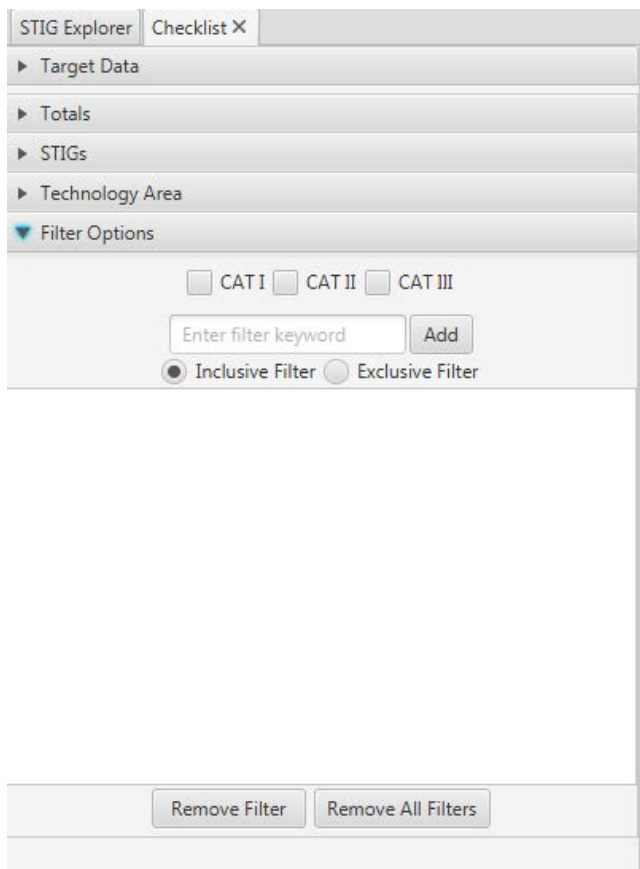
4.1.4 Checklist – Technology Area Section

1. The Technology Area section contains a drop-down list of technologies, to select specific technology for asset being reviewed.



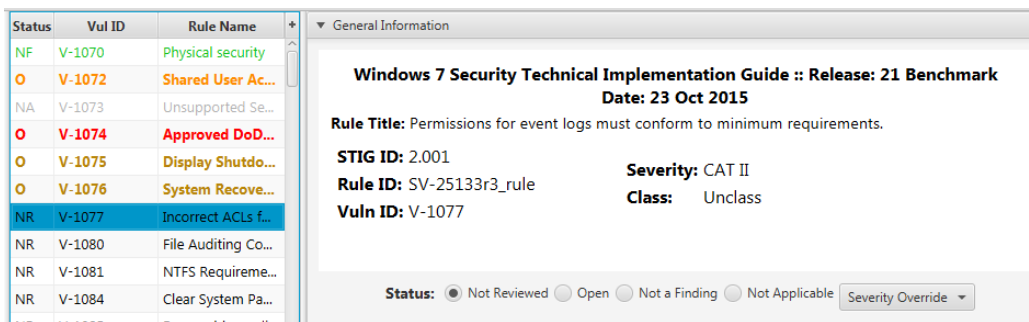
4.1.5 Checklist – Filter Options Section

1. The Filter Options section allows you to filter the vulnerabilities by severity (CAT I, II, or III) or by entering a keyword. Select either Inclusive or Exclusive Filter radio button.
2. To clear the filter, select either Remove Filter or Remove All Filters button.

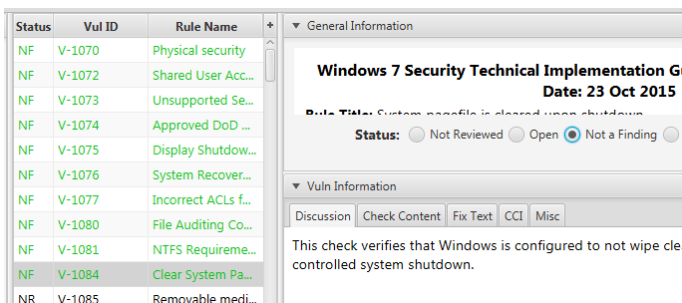
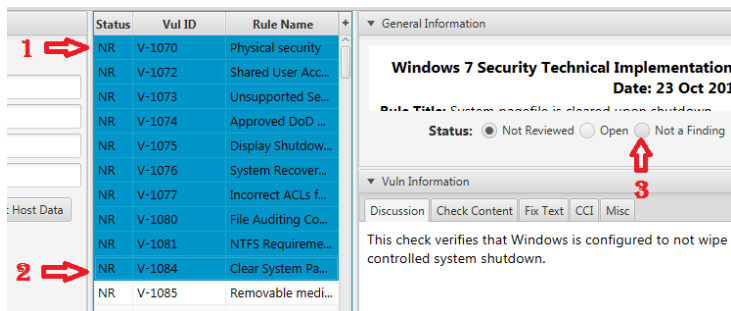


4.1.6 Checklist – General Information Section

1. The General Information section displays in the right column, for Vulnerability selected in the center column.
2. Select status radio button to identify Vulnerability as Open (O), Not a Finding (NF), or Not Applicable (NA). The Vulnerability text color will also change to reflect status.
3. Click Severity Override drop-down when necessary to down-grade or up-grade status. Pop-up box will display to enter required justification text for override.

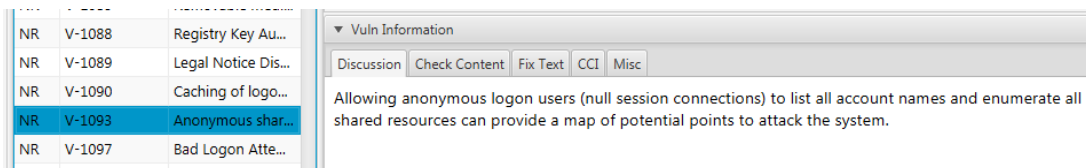


4. To select multiple vulnerability checks, click on first one to be selected (1), then hold Shift-Key down and click on last one to be selected (2). Next, select Status radio button you wish to set all selected checks (3).

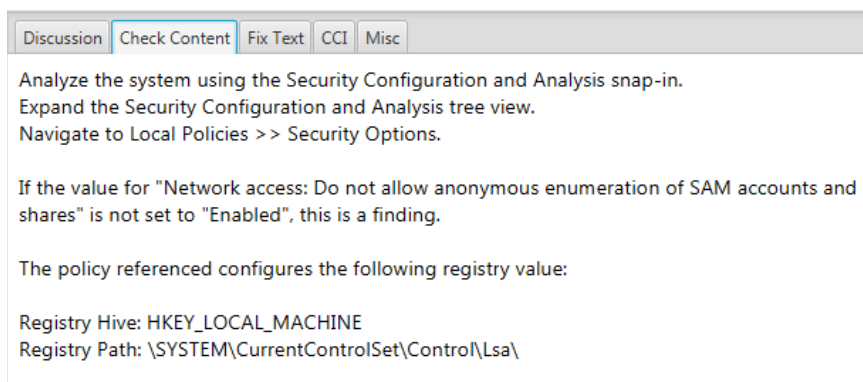


4.1.7 Checklist – Vuln Information Section

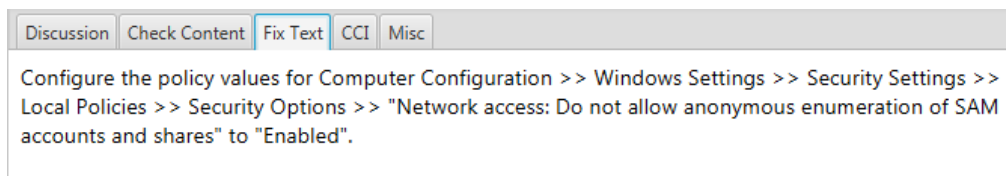
1. The Vuln Information section contains 5 tabs relating to Vulnerability selected in center column.
2. Discussion tab – A brief description of the check.



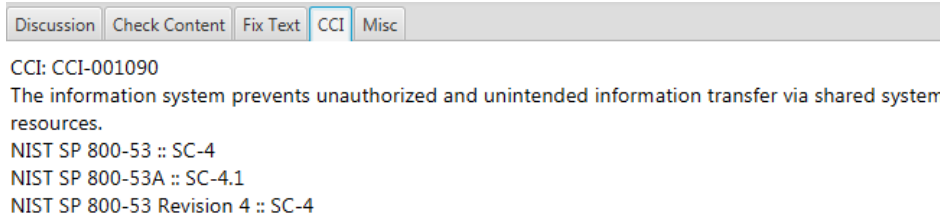
3. Check Content tab – Describes how to conduct the check for review.



4. Fix Text tab – Describes how to fix an Open finding for check.

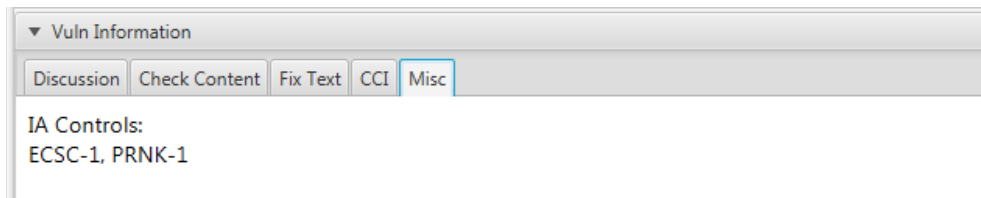


5. CCI tab – Describes CCI information about check.



The screenshot shows a horizontal tabbed interface with five tabs: Discussion, Check Content, Fix Text, CCI, and Misc. The CCI tab is selected and highlighted. Below the tabs, the text reads: CCI: CCI-001090. The information system prevents unauthorized and unintended information transfer via shared system resources. NIST SP 800-53 :: SC-4. NIST SP 800-53A :: SC-4.1. NIST SP 800-53 Revision 4 :: SC-4.

6. Misc tab – Describes IA Controls about check.



The screenshot shows a window titled 'Vuln Information' with a dropdown arrow. Below the title is a horizontal tabbed interface with five tabs: Discussion, Check Content, Fix Text, CCI, and Misc. The Misc tab is selected and highlighted. Below the tabs, the text reads: IA Controls: ECSC-1, PRNK-1.

4.1.8 Checklist – Finding Details Section and Comments Section

1. The Finding Details section and Comments section are used to record details and comments from reviewer.

