STIG Viewer 3.x User Guide

Version 1, Release 5

11 February 2025

Developed by DISA for the DOD

Table of Contents

Page

1. INTRODUCTION 1

1.1 About DOD/DISA STIG Viewer 1
1.2 About the SRG/STIG Applicability Guide 1

2. INSTALLING AND RUNNING STIG VIEWER 3.X 3

2.1 Installing Standalone STIG Viewer 3
2.2 Installing the STIG Viewer Windows MSI Package 4
2.3 Verifying Integrity of STIG Viewer Packages 5
2.4 Unblocking on Windows 5
2.5 Linux File Access Policy 5
2.6 Digital Signatures 6
2.7 STIG Viewer Help 6

3. USING STIG VIEWER 3.X 7

3.1 Opening STIG Viewer 7

4. STIG EXPLORER 9

4.1 Open STIGs 9
4.1.1 To Open STIGs from the Home Screen 9
4.1.2 To Open STIGs from the STIG Viewer Icon 10
4.2 Adding STIGs to the Library 13
4.3 Viewing STIGs 15
4.3.1 View Multiple STIGs – Filtered 18
4.3.2 View Multiple STIGs – Unfiltered 24
4.3.3 Viewing More STIGs 27
4.4 Remove STIGs from Recent STIGs and STIG Library 29
4.5 Keyword Search 30
4.6 Comparing STIGs 32

5. CHECKLIST 35

5.1 Create Checklist from Home Page or Top Navigation Bar 35
5.2 Create Another Checklist 46
5.3 Opening an Existing Checklist 48
5.4 Updating Checklists 49
5.4.1 Changing the Status of Rules 49
5.4.2 Override Severity Status 51
5.4.3 Filtering a Checklist 52
5.4.4 Populating Target Data 53
5.4.5 Adding Comments and Finding Details to a Single Rule 54
5.4.6 Adding Comments and Finding Details to Multiple Rules 55

5.5 Saving a Checklist 56
5.6 Importing XCCDF Results into a Checklist 60
5.7 Importing Checklist Data 63
5.8 Exporting Checklist Data 65
5.9 Resizing the Checklist Pane 67

6. SRG/STIG APPLICABILITY GUIDE 68

6.1 Accessing Applicability Guide from STIG Viewer 3 Dashboard 68
6.2 Menu 68
6.2.1 File Menu 69
6.2.2 App Menu 69
6.3 Navigation Bar Menu 70
6.3.1 Overview 70
6.3.2 Merge Button 70
6.3.3 Save Button 70
6.3.4 Export Button 71
6.3.5 Right-Click Menu 71
6.4 Asset Tree 72
6.4.1 Overview 72
6.4.2 Creating a Collection 73
6.4.3 Adding Assets (Standard Mode) 74
6.4.4 Adding Assets (Guide Mode) 76
6.4.5 Adding Parent Assets 78
6.4.6 Adding Parent Assets (Guide Mode) 80
6.4.7 Editing Assets 83
6.4.8 Removing Assets 84
6.5 Save, Open, and Merge 85
6.5.1 Overview 85
6.5.2 Save Collection 85
6.5.3 Open Collection 86
6.5.4 Merge Collection 87
6.6 Drag and Drop 88
6.6.1 Overview 88
6.6.2 Drag and Drop Assets 88
6.7 Exports 88
6.7.1 Overview 88
6.7.2 Preview 89
6.7.3 Exporting 89
6.7.4 Scenario 90

1. INTRODUCTION

STIG Viewer Version 3.x is a replacement for the previous DISA tools STIG Viewer 2.x and STIG-SRG Applicability Guide. The intent of this User Guide is to assist in navigating version 3.x and describe 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 (Extensible Configuration Checklist Description Format) 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 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.

STIG Viewer supports additional functionality using the following features:

- Allows multiple STIGs to be imported and used when creating checklists.
- Individually loads one or more XCCDF STIG files.
- Extracts XCCDF STIG files from zipped STIG packages, including nested ZIP files.
- Maintains an internal library of loaded STIGs.
- Sorts the list of STIG requirements by Group ID, Rule ID, and STIG ID.
- Searches or filters all loaded STIG files based on one or more keywords. Searches all fields or individual fields and returns a filtered list of STIG requirements/vulnerabilities.
    - Searches may also be restricted to Content (Discussion, Check, and Fix), Rule Title, Severity, STIG ID, Group ID, Rule ID, CCI, or Legacy ID.
- Displays CCI data if the CCI reference is contained in the STIG requirements.
- Prints or exports (HTML and CSV file formats) selected STIG data for use with other programs.
    - Bases the printed/exported data on the list of requirements displayed in the pane of the viewer and formats the output as a table containing each requirement.
- Imports automated review SCAP (Security Content Automation Protocol) or XCCDF Results 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.
- Exports the checklist as a CSV file.
- Displays PDF documents bundled with STIG packages.

1.2 About the SRG/STIG Applicability Guide

The SRG/STIG Applicability Guide allows the user to build a collection of assets pertaining to an environment, such as an information system. Using the collection of assets built by the user, the tool will determine the SRGs, STIGs, and other policy documents the user needs to harden or assess their environment. The tool allows the user to preview and export the policy documents as well as import and export the collection.

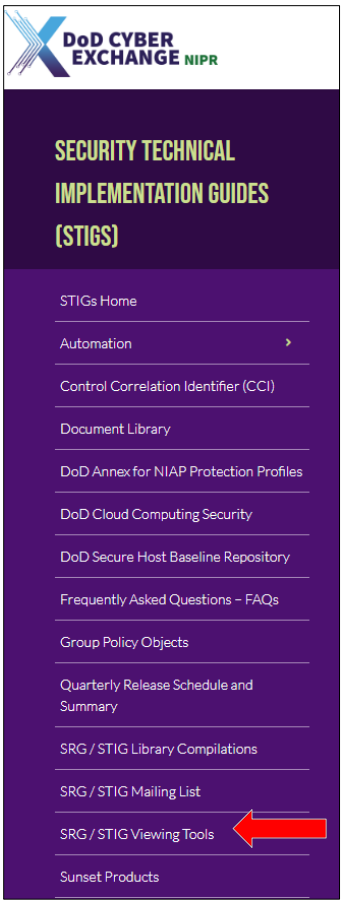
Applicability Guide functions include the following:

- Select from two modes of asset addition for different levels of familiarity.
- Drag and drop assets in the asset tree.
- Import and export asset collections.
- Export policy documents.

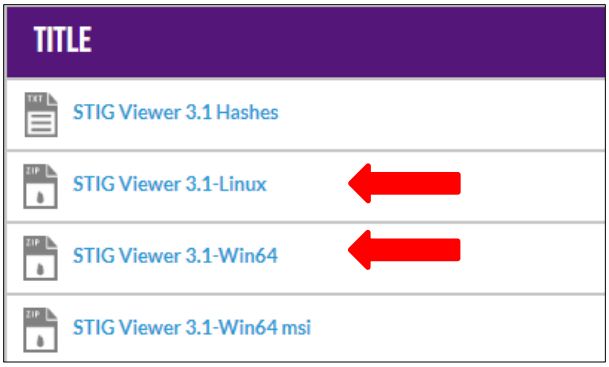
2. INSTALLING AND RUNNING STIG VIEWER 3.X

2.1 Installing Standalone STIG Viewer

1. Download the STIG Viewer 3.x standalone ZIP file from the Cyber Exchange website. Go to SRGs/STIGs >> SRG/STIG Viewing Tools.



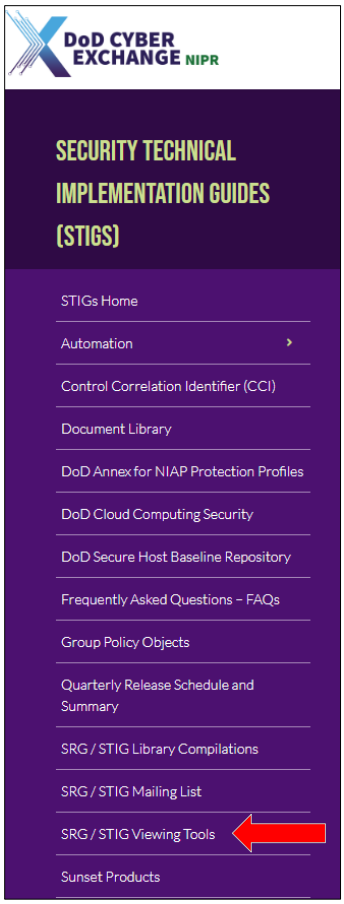
2. Click **STIG Viewer 3.x-Win64** or **STIG Viewer 3.x-Linux**.



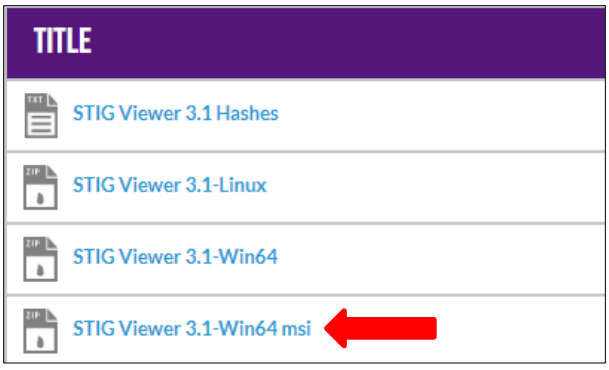
3. Click **Save** to save as U_STIGViewer-win32_x64-3-x-x.zip or U_STIGViewer-linux_x64-3-x-x.zip. Extract all contents of the ZIP file to the local hard disk; the standalone application does not run from within the ZIP file.

2.2 Installing the STIG Viewer Windows MSI Package

1. Download the STIG Viewer 3.x Windows MSI ZIP file from the Cyber Exchange website. Go to SRGs/STIGs >> SRG/STIG Viewing Tools.



2. Click **STIG Viewer Version 3.x-Win64_msi**.



3. Click **Save** to save as U_STIGViewer-win32_x64-3-x-x_msi.zip.
4. Open the downloaded ZIP file. Open the enclosed .msi file to begin the installation process. Administrative rights are required for installation.

2.3 Verifying Integrity of STIG Viewer Packages

A file containing secure hash values for the STIG Viewer ZIP packages is published on cyber.mil. These hash values can be used to verify the integrity of STIG Viewer packages. Values are provided for the SHA256, SHA384, and SHA512 algorithms. To verify, compute the hash value on the STIG Viewer package under inspection using tools such as the Get-FileHash cmdlet (available in Windows PowerShell) or the sha256sum, sha384sum, and sha512sum programs (available on Linux). To verify the integrity of the file, compare the hash value from the published file to the computed value for the file under inspection for the same algorithm.

2.4 Unblocking on Windows

When STIG Viewer is downloaded on Windows, the file may be marked to indicate it was downloaded from the internet, which may prevent running the application. This can also apply to the contents of a ZIP file when extracted. Consult with the local system administrator for guidance. If approved, a verified file can be unblocked. Using **File Explorer**, select **Properties** for the file. In the **Properties** dialog, navigate to the **General** tab and the **Security** section. Unblock the file by checking the **Unblock** checkbox and selecting **OK**. Alternatively, in Windows PowerShell, the Unblock-File cmdlet can be used.

2.5 Linux File Access Policy

Linux systems using the File Access Policy Daemon (fapolicyd) may block the execution of STIG Viewer and present an "Operation Not Permitted" or "cannot open shared object file" message when attempting to launch STIG Viewer. The following procedure can be used to trust a common installation of STIG Viewer:

1. Make the directory for the shared STIG Viewer installation.

   ```
   $ sudo mkdir /opt/stigviewer
   ```

2. Unzip the STIG Viewer package into the shared directory.

   ```
   $ sudo unzip U_STIGViewer-linux_x64-3-x-x.zip -d /opt
   $ sudo mv /opt/stig_viewer_3-linux-x64 /opt/stigviewer
   ```

3. Add the STIG Viewer library and binaries to the fapolicyd trust database.

   ```
   $ sudo fapolicyd-cli --file add /opt/stigviewer
   ```

4. Notify fapolicyd that the database has been updated.

   ```
   $ sudo fapolicyd-cli --update
   ```

5. Run STIG Viewer from the shared directory.

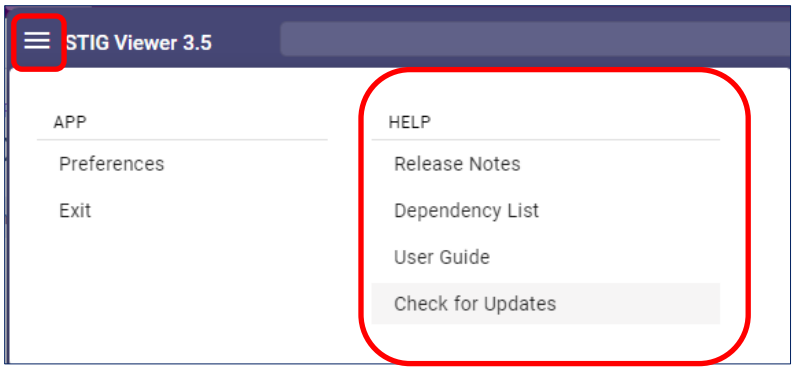
   ```
   $ /opt/stigviewer/STIG\ Viewer\ 3
   ```

2.6 Digital Signatures

Beginning with STIG Viewer version 2.15, the Windows EXE and MSI files are digitally signed with a DOD code signing certificate. Information on installing DOD trust anchors is available at https://public.cyber.mil/pki-pke/. To view the signatures, open the file's properties in Windows Explorer and select the **Digital Signatures** tab.

2.7 STIG Viewer Help

The STIG Viewer Help section can be found under the hamburger menu. This section provides links to the Release Notes, Dependency List, User Guide, and Check for Updates, which is a link to Cyber Exchange to verify the latest version available.



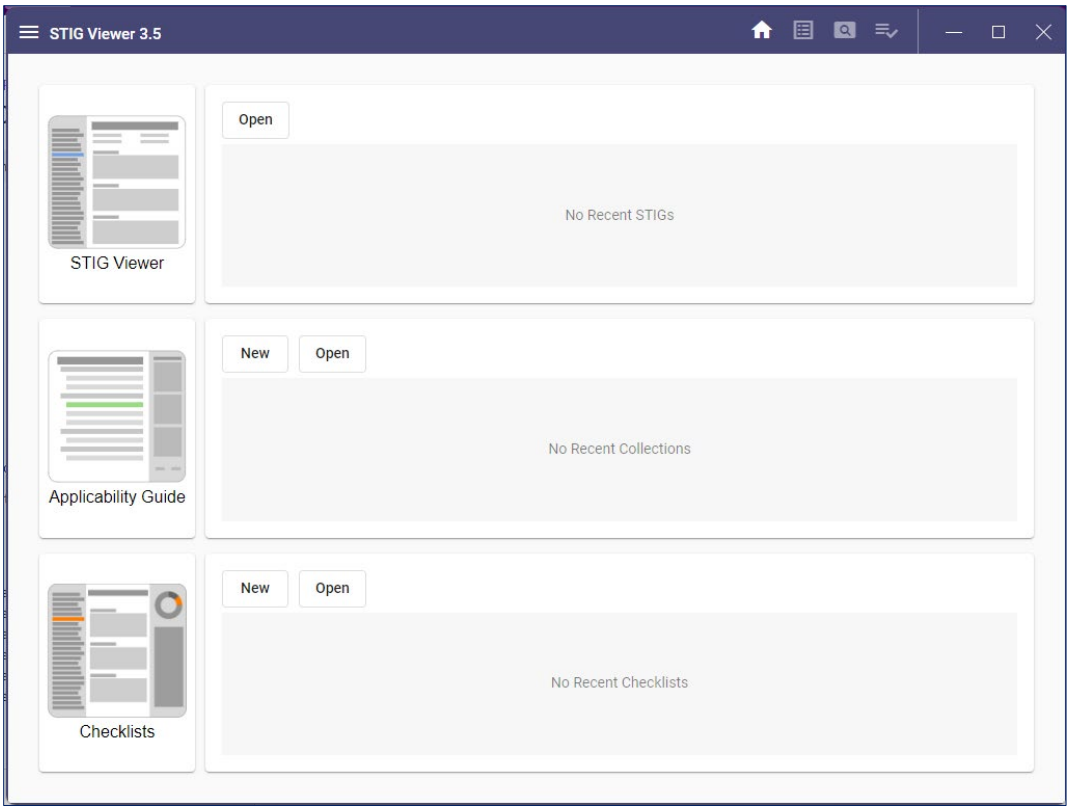
3. USING STIG VIEWER 3.X

STIG Viewer 3.x has combined the STIG Applicability Guide, STIG Explorer (Viewer), and STIG Checklists into one application.

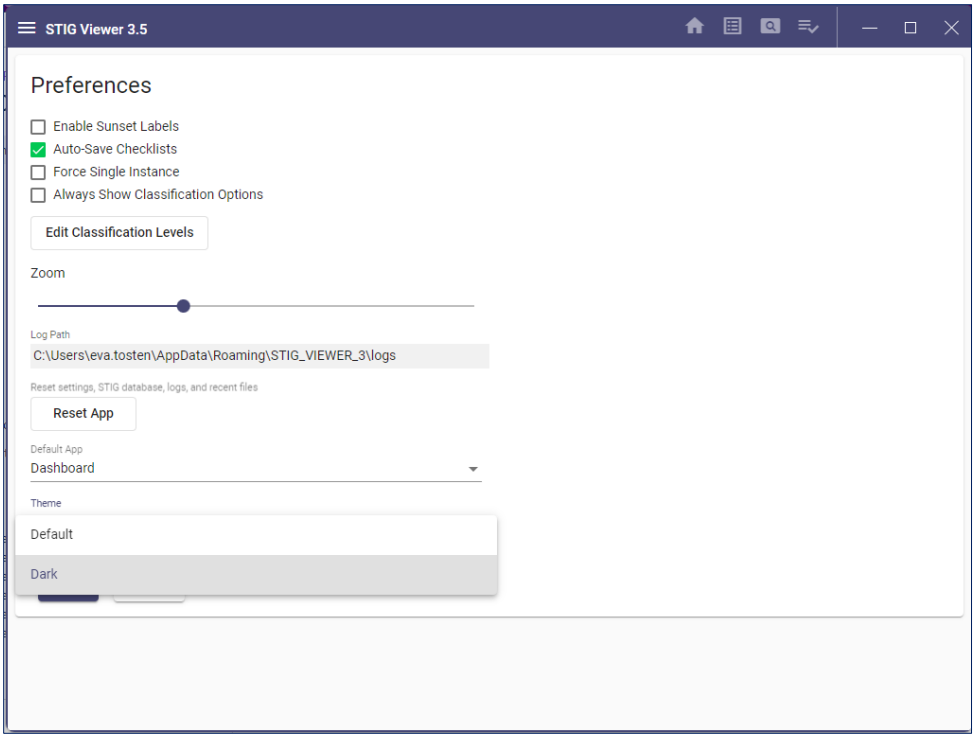
Note: If there is a long path in any of the sections, the user can either adjust the pane to see the entire path or go to the bottom of the section and use the scroll bar to view.

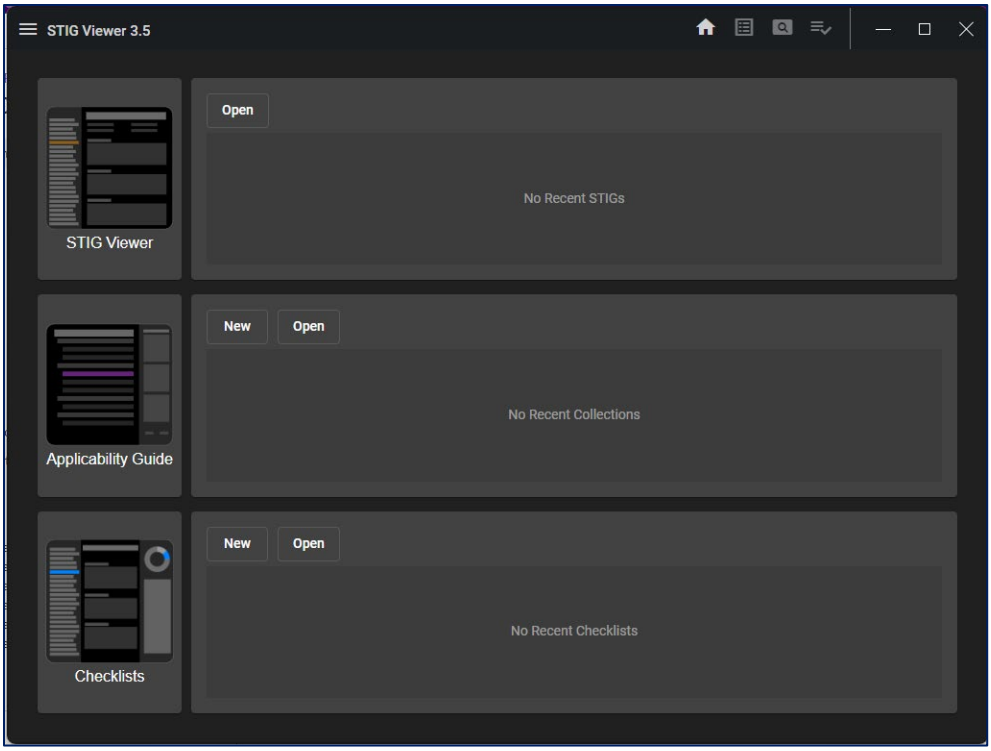
3.1 Opening STIG Viewer

1. The procedure for opening STIG Viewer depends on the release package used.
   a. Windows standalone package:
      i. Start STIG Viewer by opening the **STIG Viewer 3.exe** file.
   b. Windows MSI package:
      i. Start STIG Viewer by opening the **STIG Viewer 3** item from the Start Menu.
   c. Linux standalone package:
      i. Start the standalone STIG Viewer executable from the command line (**STIG Viewer 3**).
   d. Other considerations:
      i. Consult local system administrators for assistance in running standalone versions of STIG Viewer with any application firewalls.
2. At startup, the application will open to the **Home** page and look like this:



3. To change the appearance from Default to Dark mode, select the hamburger menu in the top-left corner of the screen and then select **Preferences**. Under **Theme**, change to **Dark**, and then click **Save**.





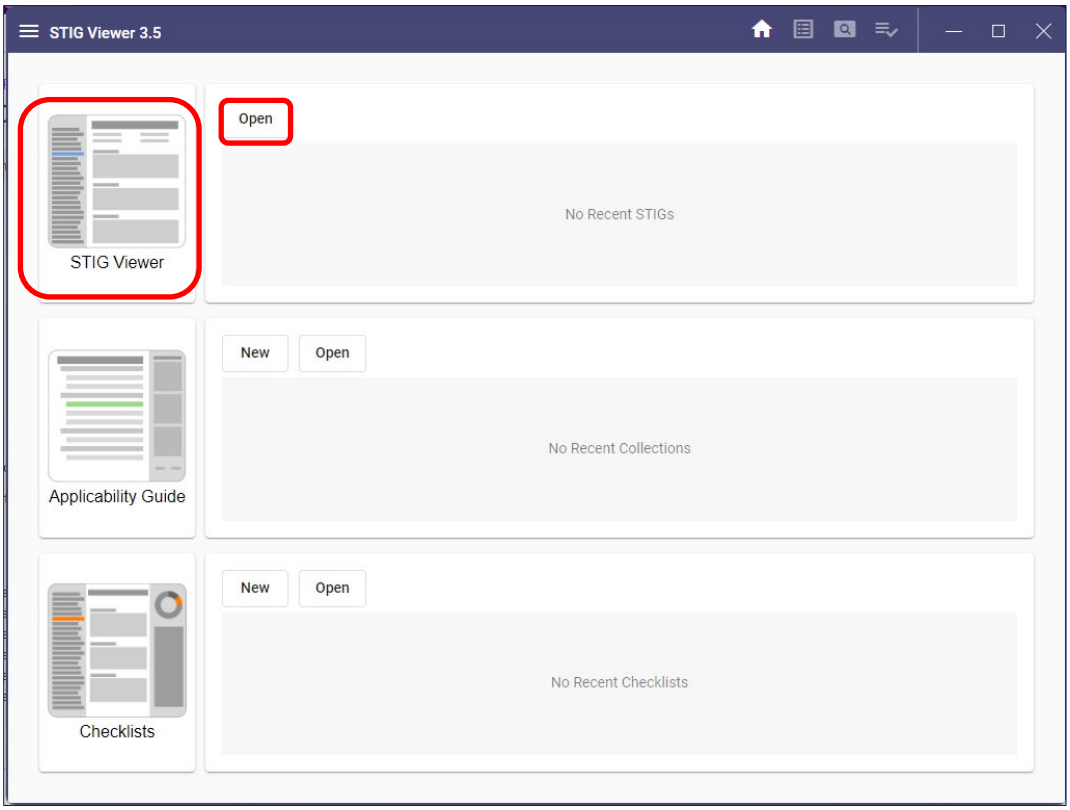
4. STIG EXPLORER

4.1 Open STIGs

Open STIGs from the **Home** screen or by selecting the **STIG Viewer** icon on the left side of the screen.

4.1.1 To Open STIGs from the Home Screen

1. Click **Open** in the upper portion of the STIG Viewer section of the screen.

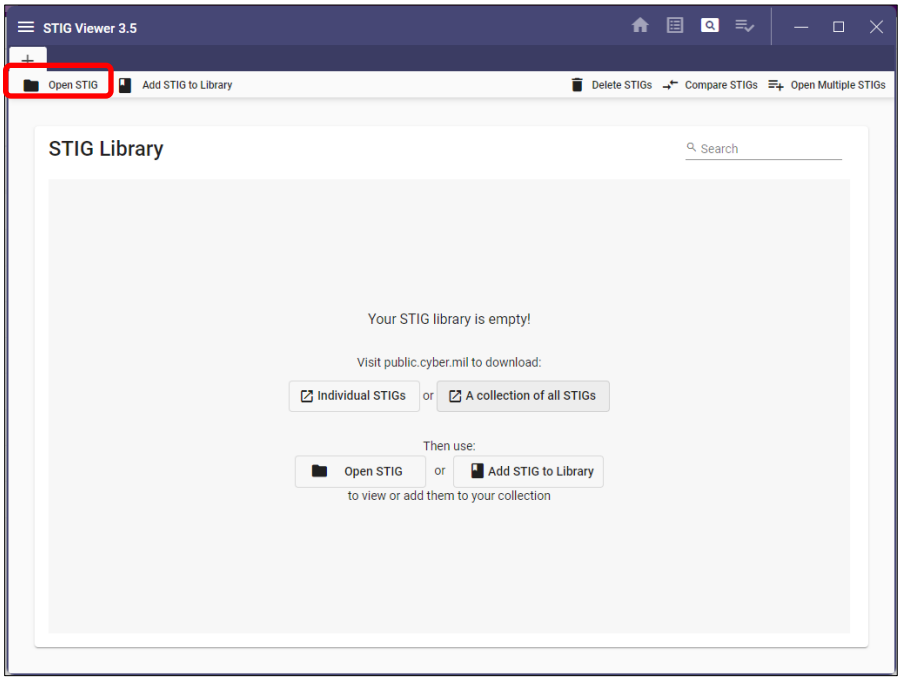


2. Navigate to the location of the STIG and double-click or select the STIG and then click **Load**.

Note: The user can import either .ZIP/.zip or .XML/.xml formats.

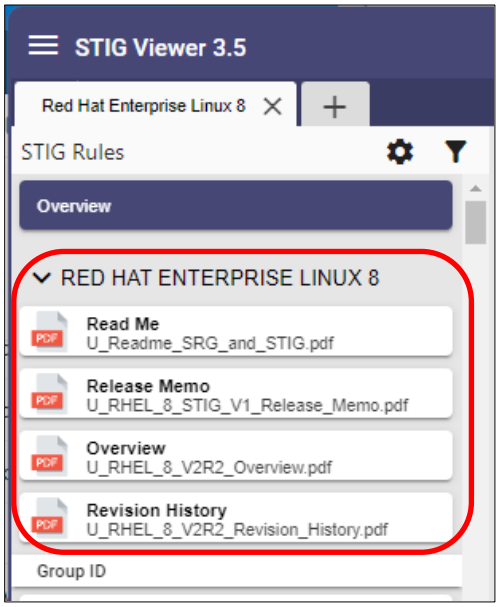
4.1.2 To Open STIGs from the STIG Viewer Icon

1. Click the **STIG Viewer** icon on the **Home** page.
2. Click the **Open STIG** icon in the upper portion of the screen.



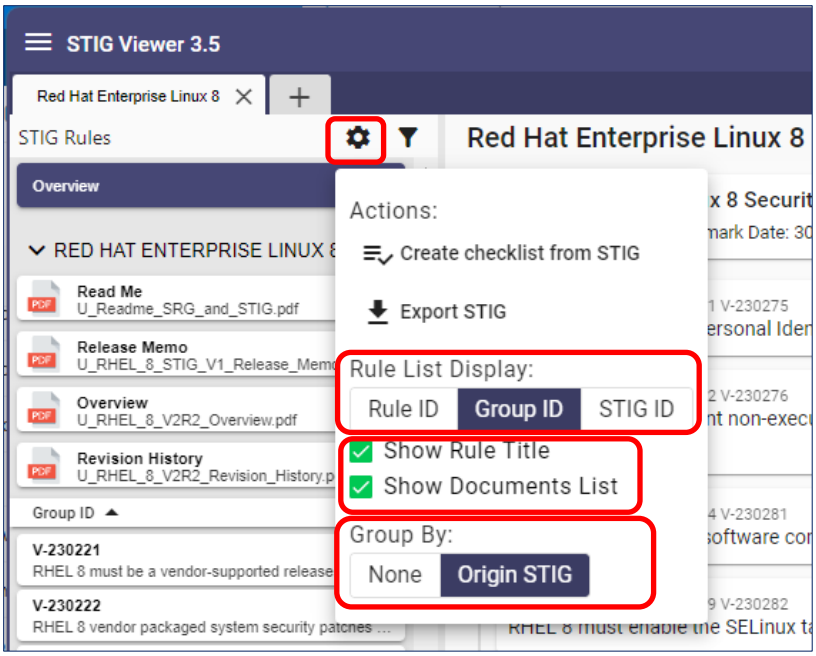
Note: Once a STIG is opened, there are three main sections to the screen as shown below.

SECTION 1: STIG Overview shows the STIG's associated documents, such as Read Me, Release Memo, Overview, Revision History, etc. The user can choose to show or hide these documents via the checkbox found in the **Gear** icon.

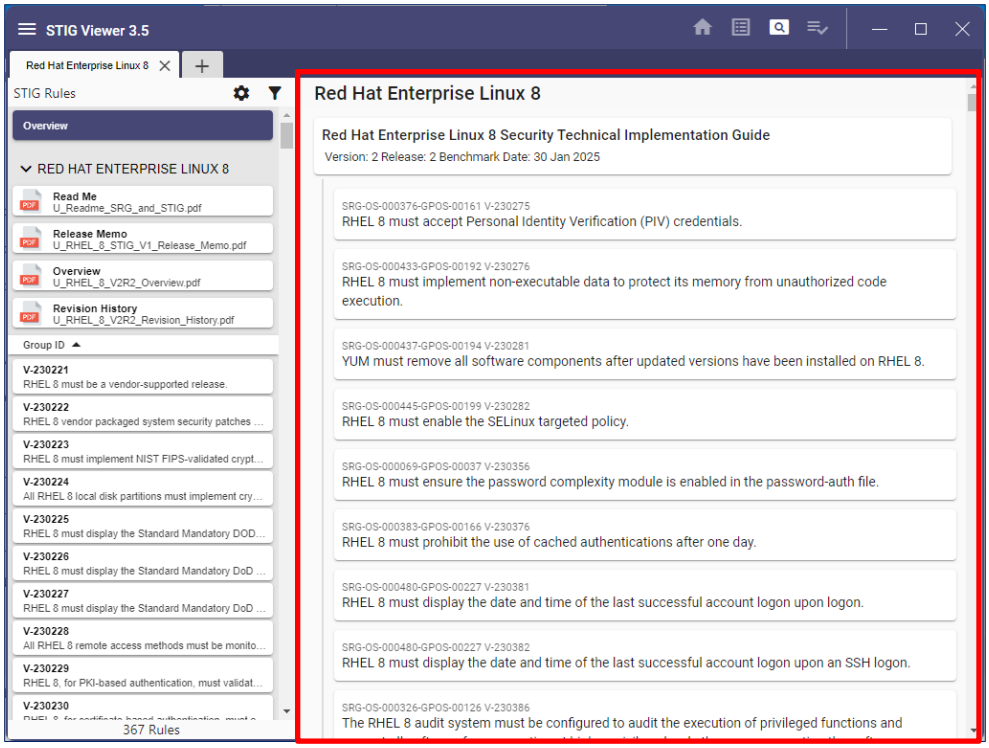


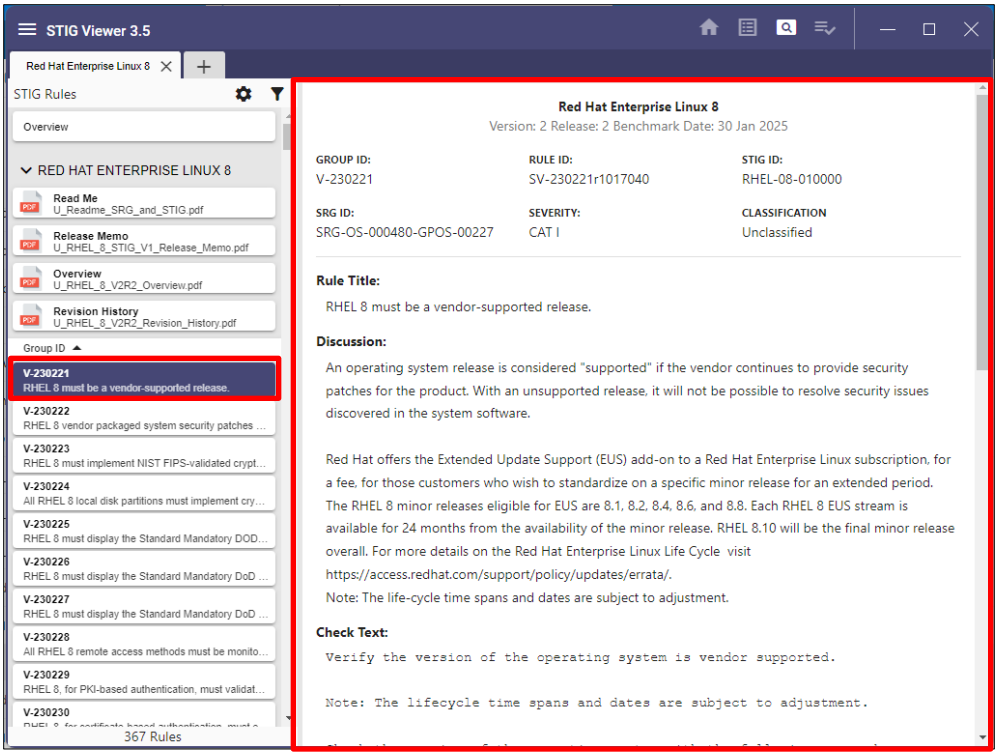
Note: The Read Me, Release Memo, Overview, and Revision History files will only appear if the ZIP file has been opened.

SECTION 2: Rules shows the **Group ID**. Also, a user can add **Rule ID** and/or **STIG ID**, or any combination of the three, by selecting the **gear** icon in the navigation bar. The default is **Group ID** for the **Origin STIG**. The user can also choose to show or hide the **Rule Title** via the checkbox.



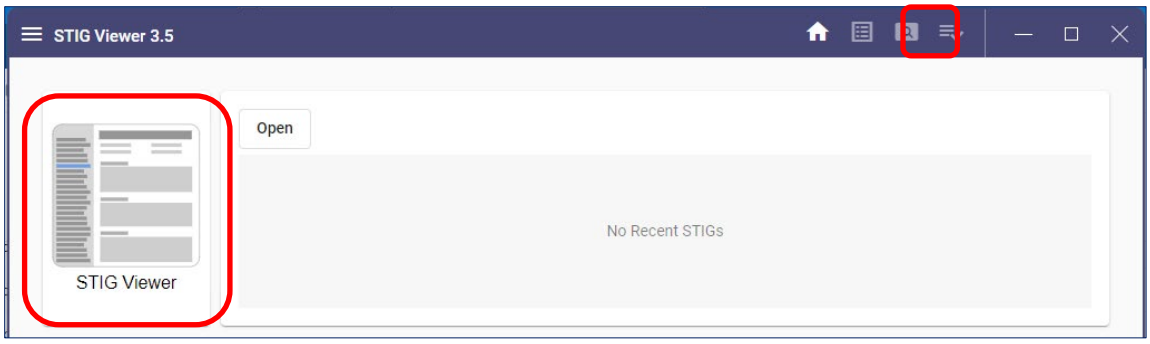
SECTION 3: Vulnerability detail shows more details about each vulnerability in the selected STIG or more detailed information about a selected rule/requirement.





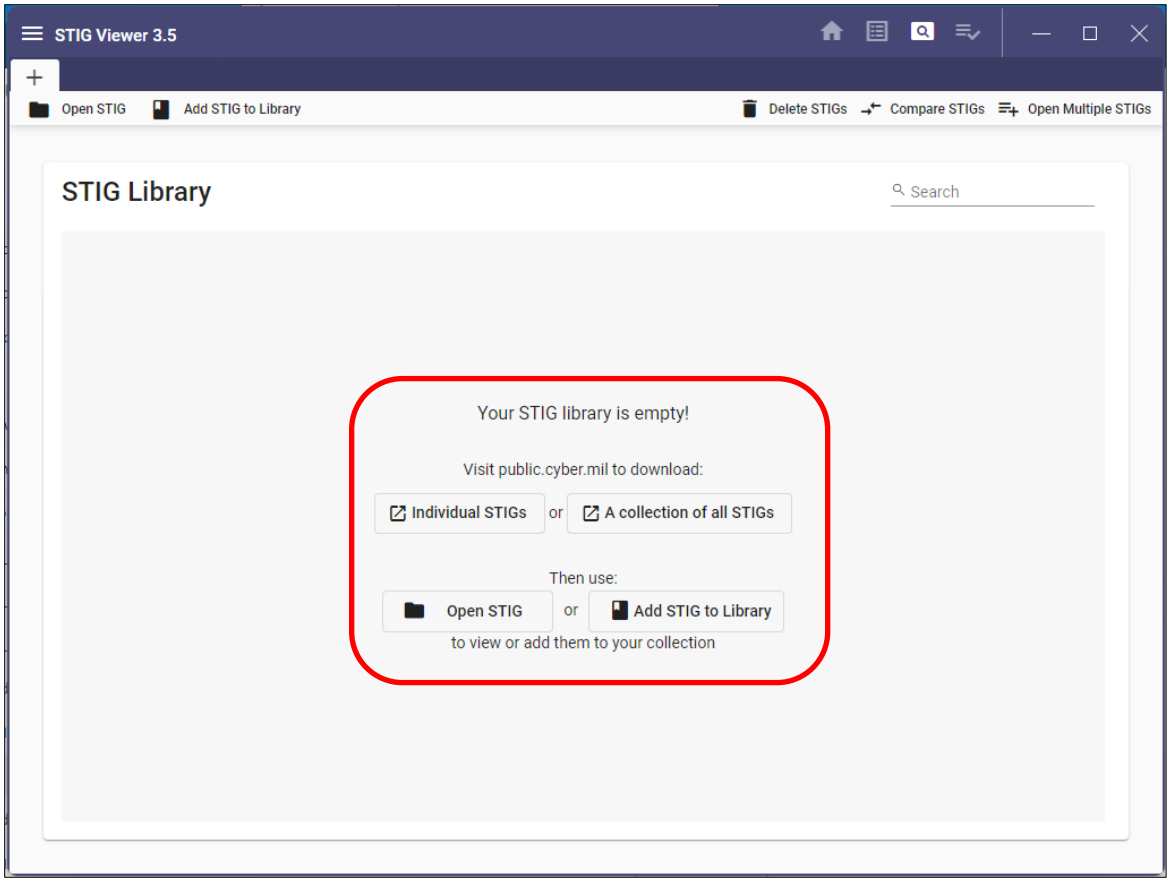
4.2 Adding STIGs to the Library

1. Click the **STIG Viewer** icon on the **Home** page or the magnifying glass icon in the upper-right portion of screen.



2. Click the **Add STIG to Library** icon in the upper portion of the screen.

   Note: If no STIGs are loaded into the library, the screen will display the following message: "Your STIG library is empty! Visit public.cyber.mil to download: Individual STIGs or A Collection of all STIGs Then use: Open STIG or Add STIG to Library to view or add them to your collection".

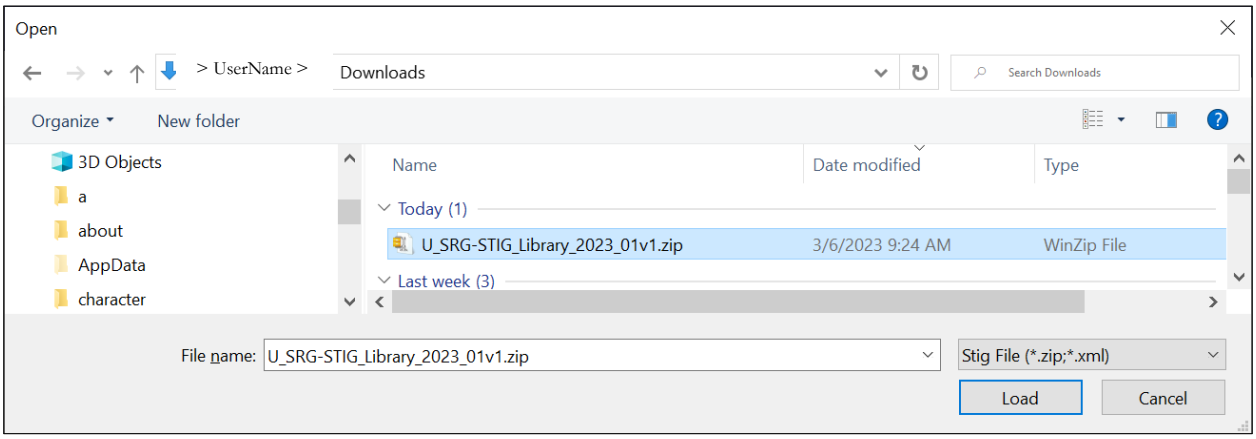


Note: The links on the screen will take the user to the public version of Cyber Exchange.

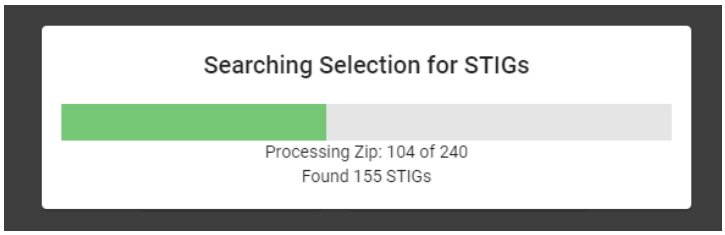
3. Download the desired STIGs.
4. Click **Add STIG to Library** and navigate to the location of the STIGs to be imported.

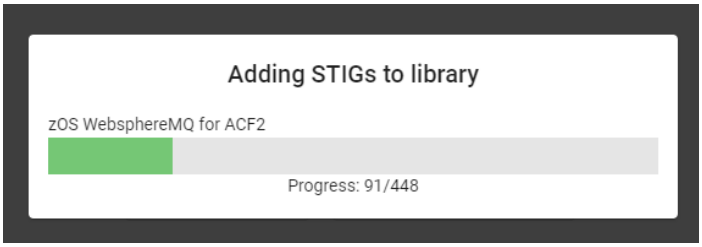
   Note: The user can select .ZIP/.zip or .XML/.xml file formats.

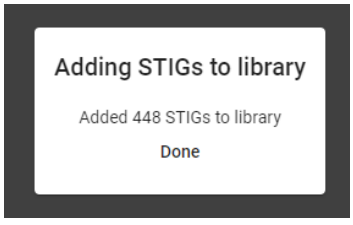
5. Select the file(s) and click **Load.**



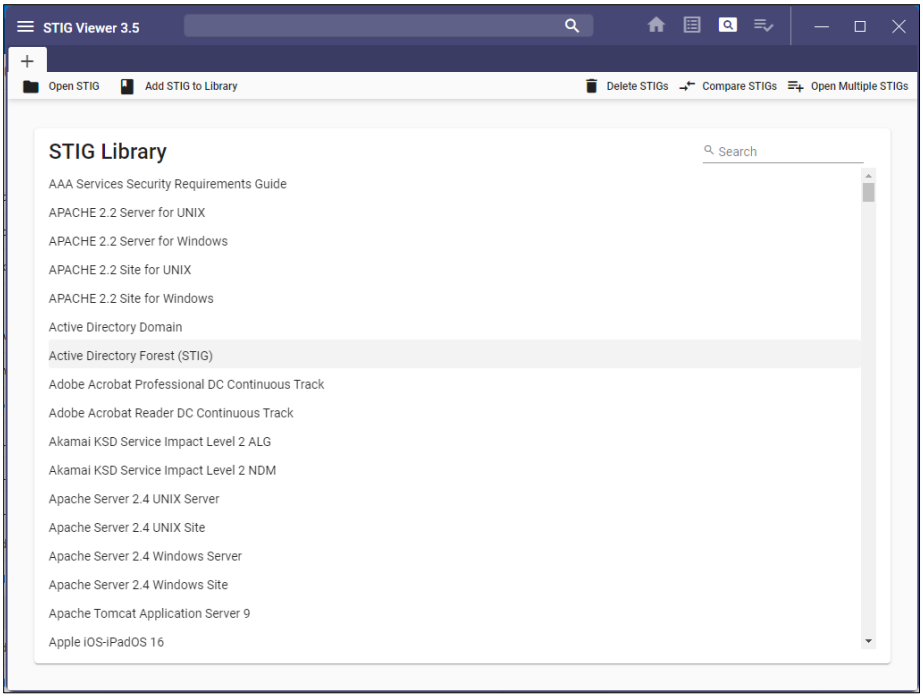
Note: The user can import the **Compilation** file to load all the STIGs. A counter will display the import progress.





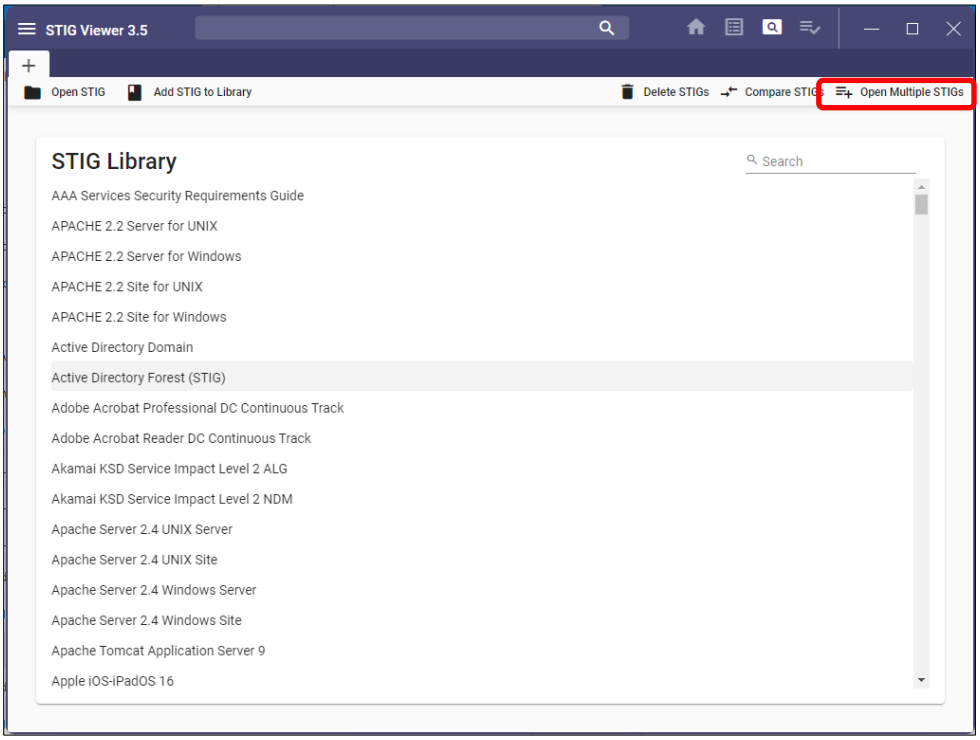


6. Once the desired STIGs are loaded into STIG Viewer 3, the screen will look like this:



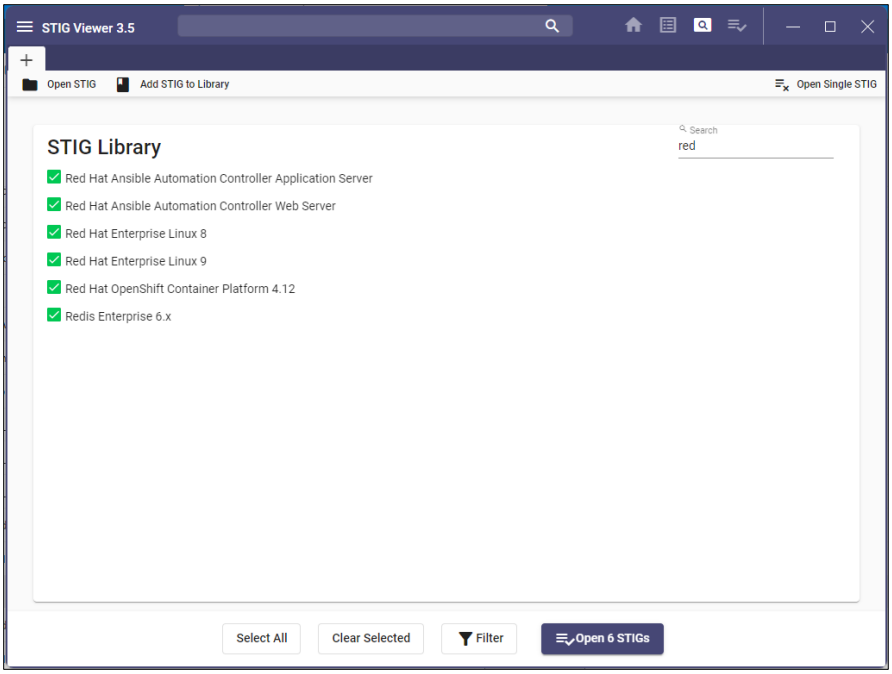
4.3 Viewing STIGs

1. To view a single STIG, click the name of the STIG.
2. To view multiple STIGs, click **Open Multiple STIGs** in the upper-right portion of the screen.

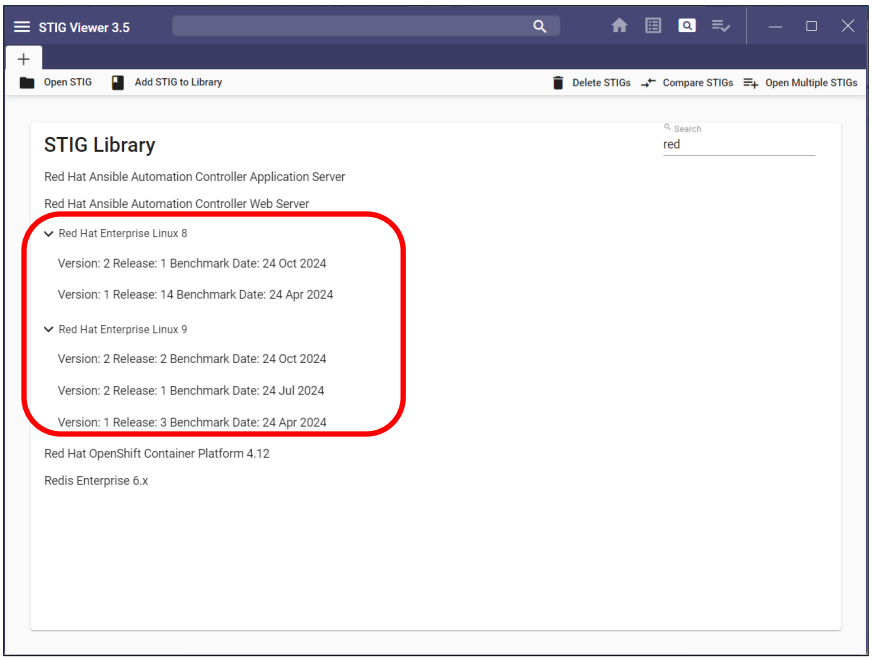


3. Checkboxes will appear beside the STIGs in the Library, which are used to select STIGs to view.

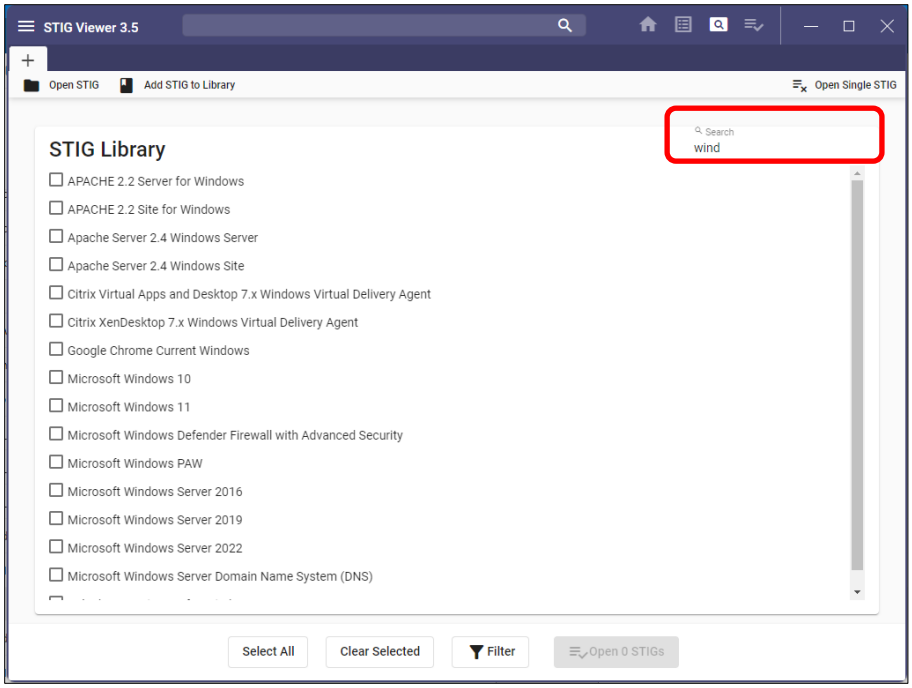
   Note: To select all listed STIGs, click **Select All**. To unselect all checked STIGs, click **Clear Selected**.



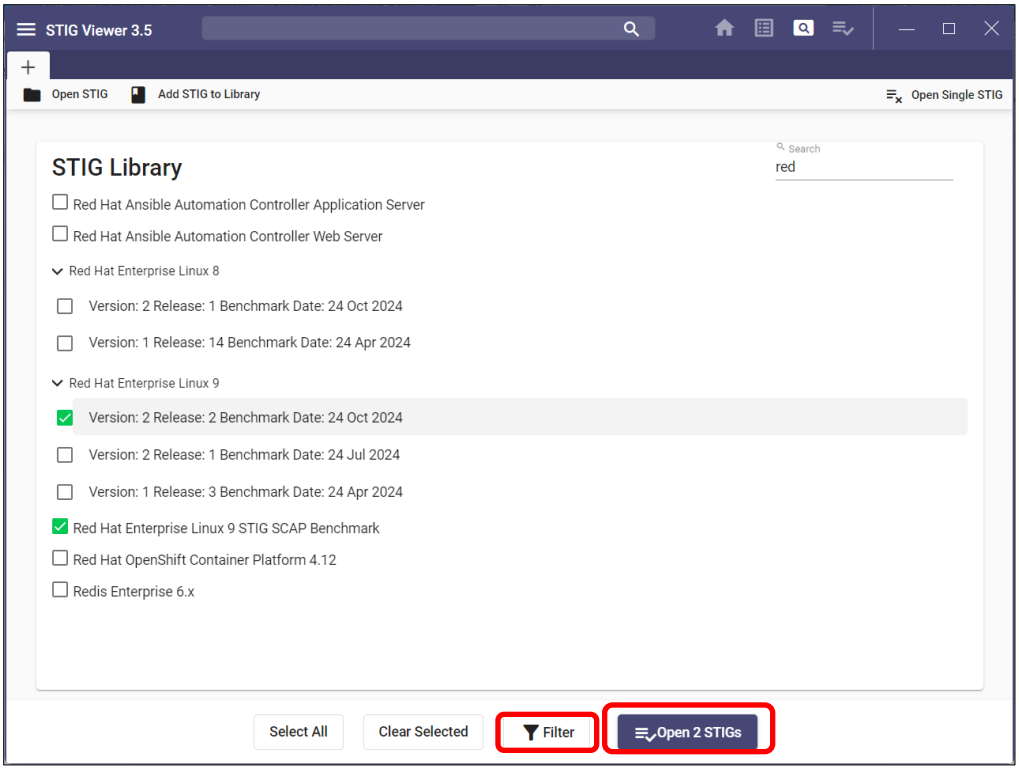
Note: If there is more than one version of a STIG, an expansion arrow will appear beside the STIG name. Once expanded, the user can select one or multiple versions of the STIG to add to the view.



4. Search for STIGs that contain a common word (e.g., STIGs that contain Windows in their title) by entering the search word in the search field located in the list of STIGs.

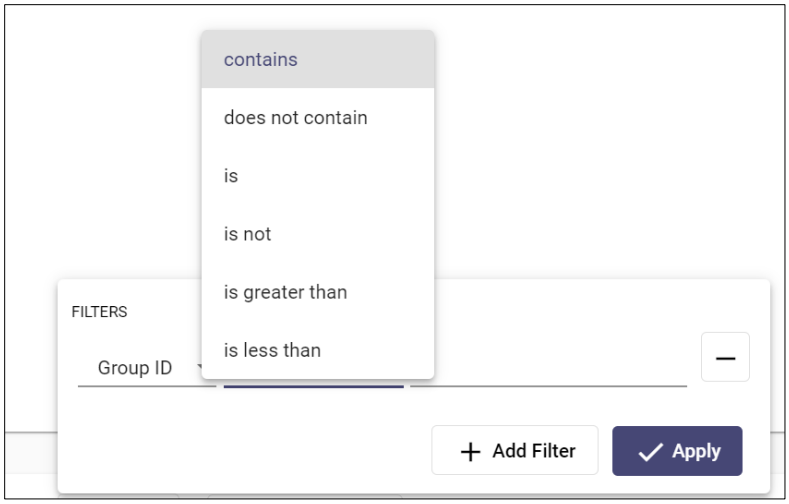


5. Once all STIGs have been selected, at the bottom of the page click the **Filter** icon or **Open X STIG(s)**, where **X** represents the number of STIGs selected.

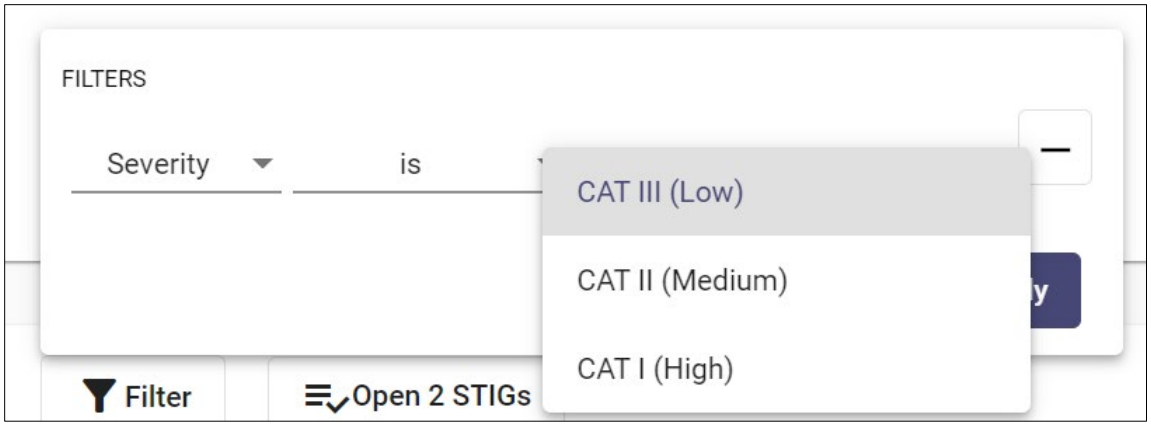


4.3.1 View Multiple STIGs – Filtered

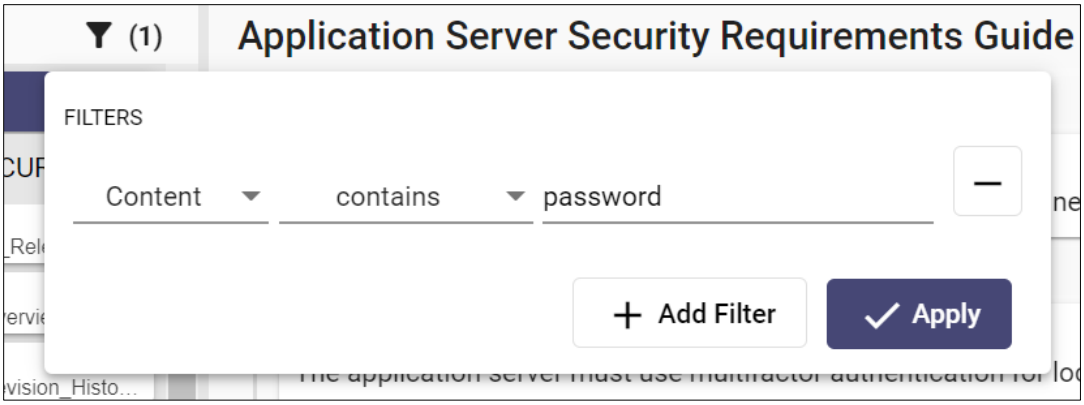
1. Click the **Filter** icon to filter requirements for review. Requirements can be filtered on Content, Title, Severity, STIG ID, Group ID, Rule ID, CCI ID, and Legacy ID. Options available depend on the subject being filtered and can be any combination of the following:
   a. contains
   b. does not contain
   c. is
   d. is not
   e. is greater than
   f. is less than

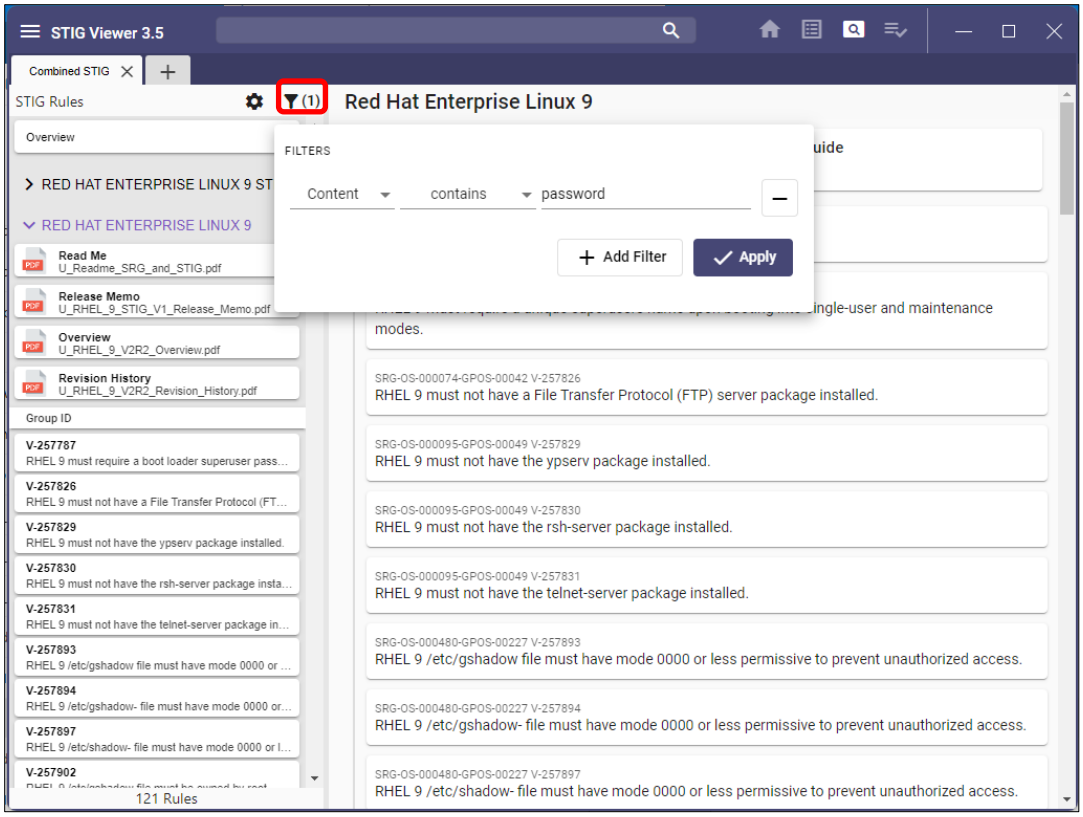


Note: Not all options will be available for each category. For example, **Severity** provides three choices in the drop-down menu.

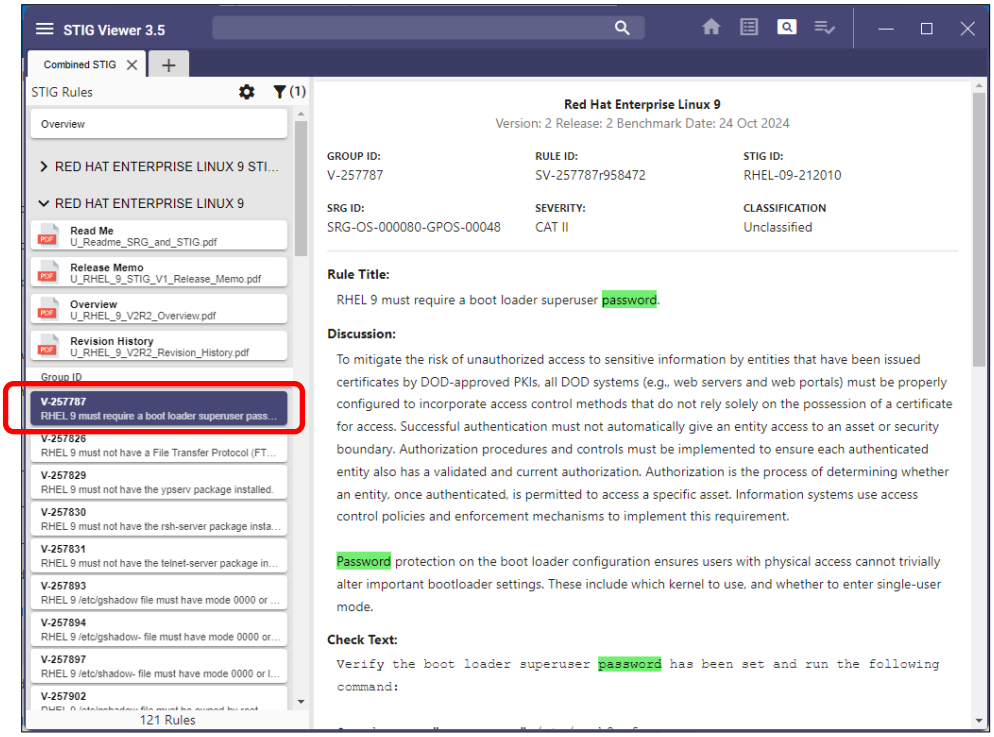


2. Click **Open X STIGs**, where **X** equals the number of STIGs selected. The screenshot below shows a combination of two STIGs that have been filtered for **Content contains password**. The funnel icon at the top left indicates the number of filters that have been applied. To view the filter, click the **funnel** icon.

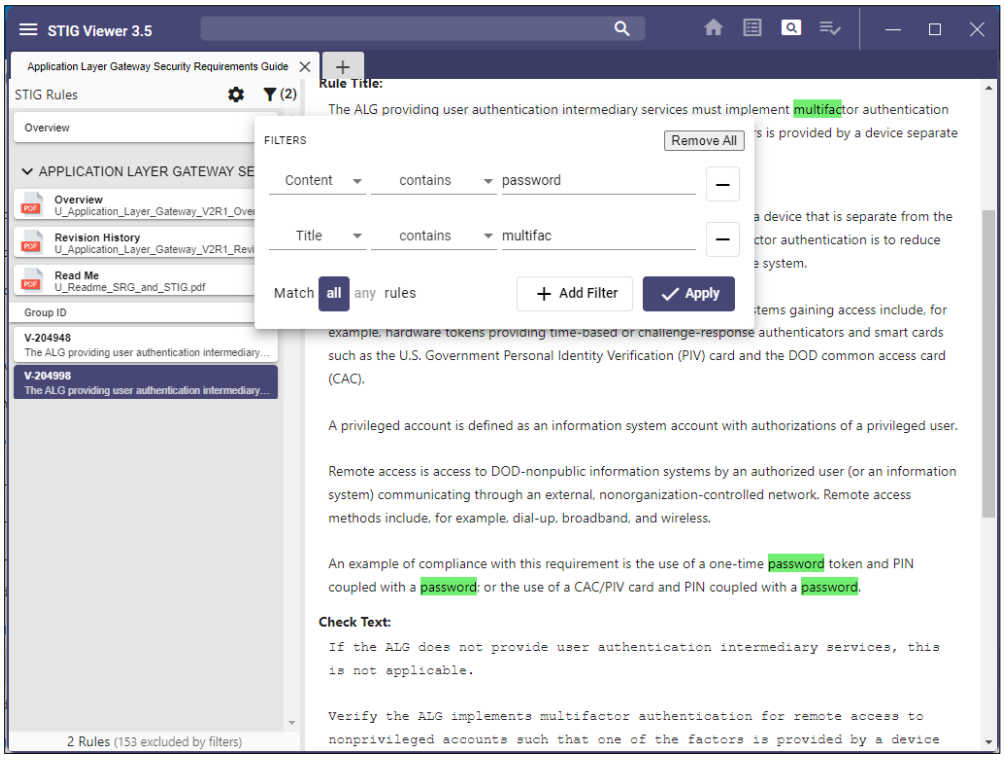




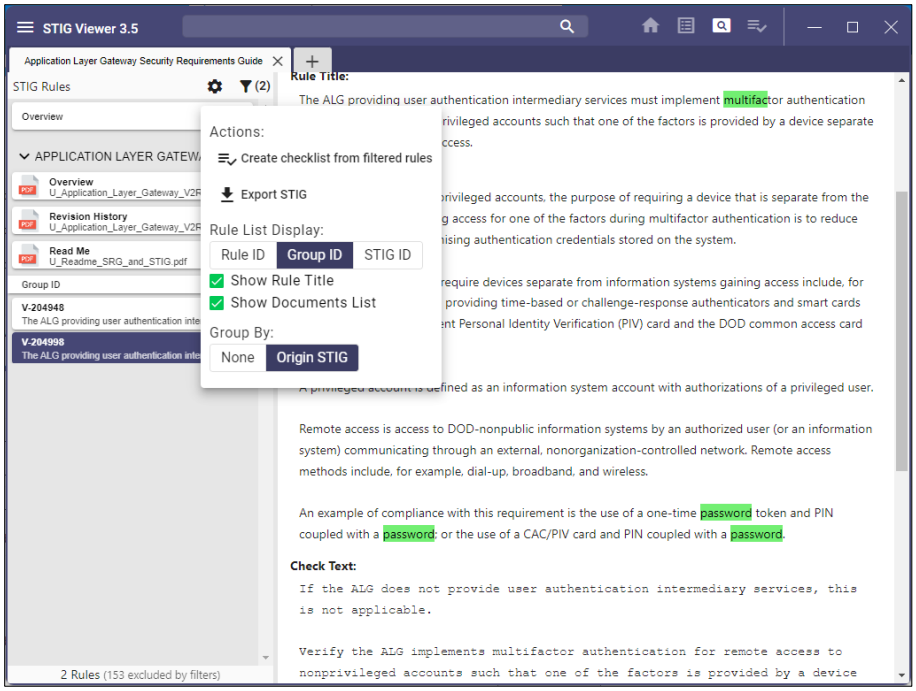
3. To view a specific rule/requirement, click it and the details will appear in the main pane. The rule/requirement selected will be highlighted on the left.

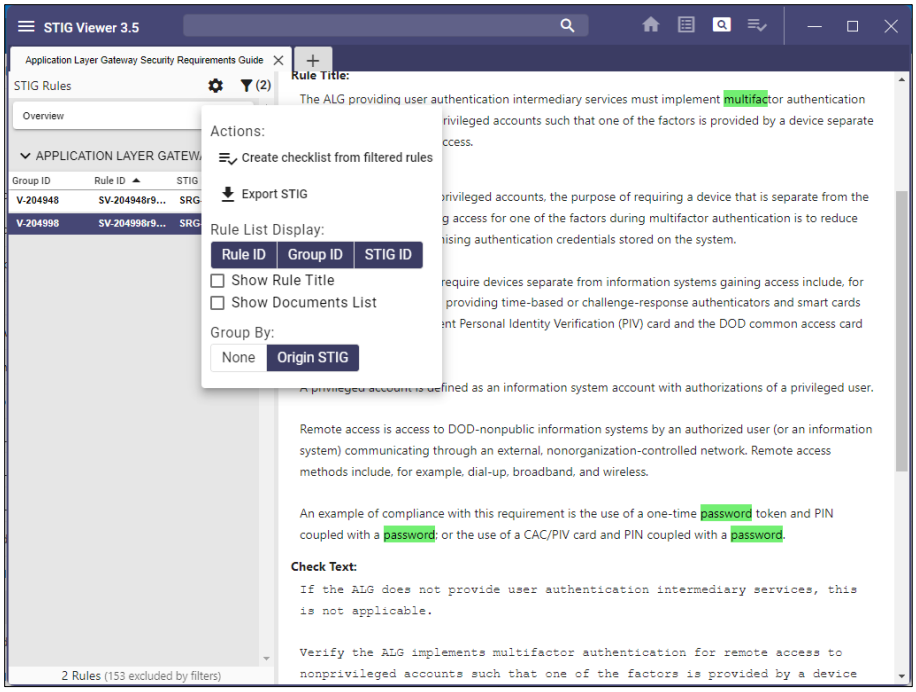


Note: The filter applied at STIG selection is carried over to this view. To further filter these requirements, click the **funnel** icon at the top of the left column and add filters.



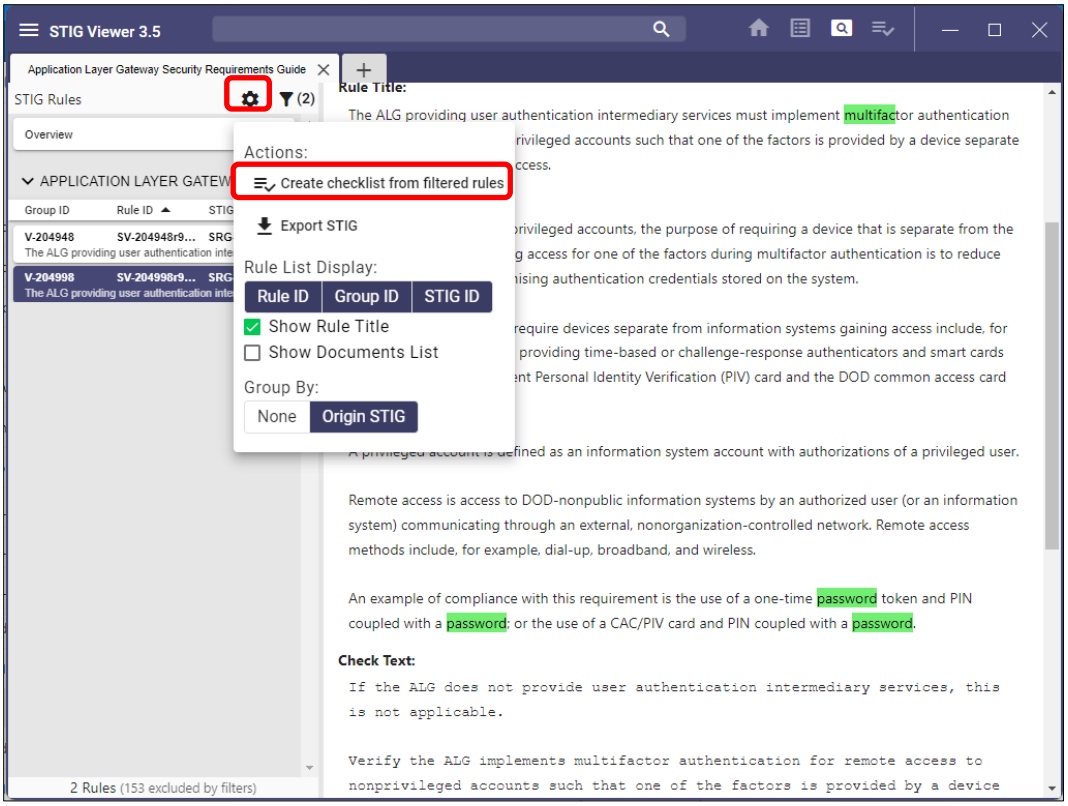
4. To change the data displayed in the left column, click the **gear** icon at the top of the left column. The default **Rule List Display:** is set to show **Group ID**. To add **Rule ID** and/or **STIG ID** and change the order of the headers, unselect them all and click them in the order the headers should appear on the screen. **Group By:** can be changed from the default of **Origin STIG** to **None.** The **Rule Title** can be removed by unchecking the checkbox for **Show Rule Title**.





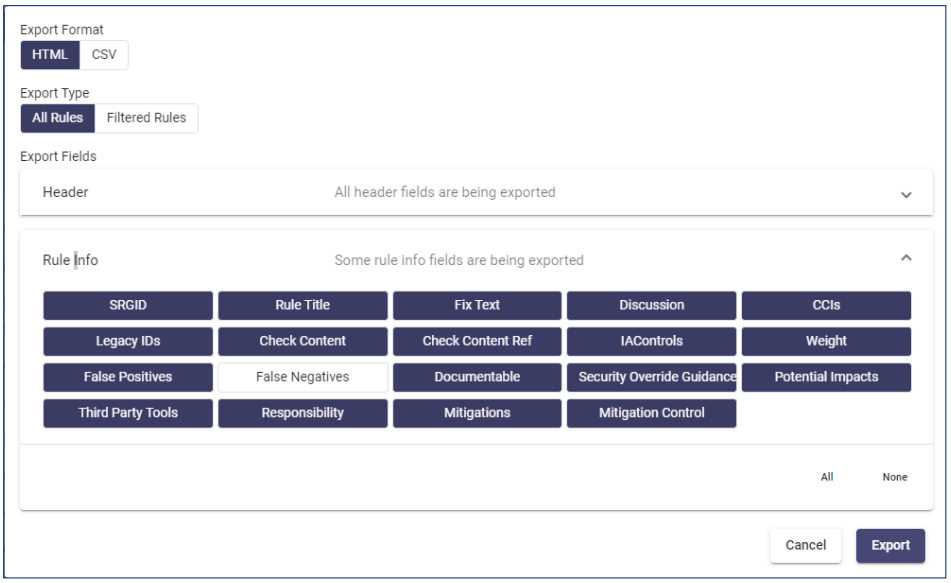
5. Sort in ascending or descending order for each of the selected IDs by clicking its header.

6. Create a checklist from these requirements by clicking the **gear** icon and then selecting **Create checklist from filtered rules.** Refer to the Checklist section for more information.



7. Export STIGs to HTML and CSV formats by clicking **Export STIGs** and selecting the format and the fields to export.

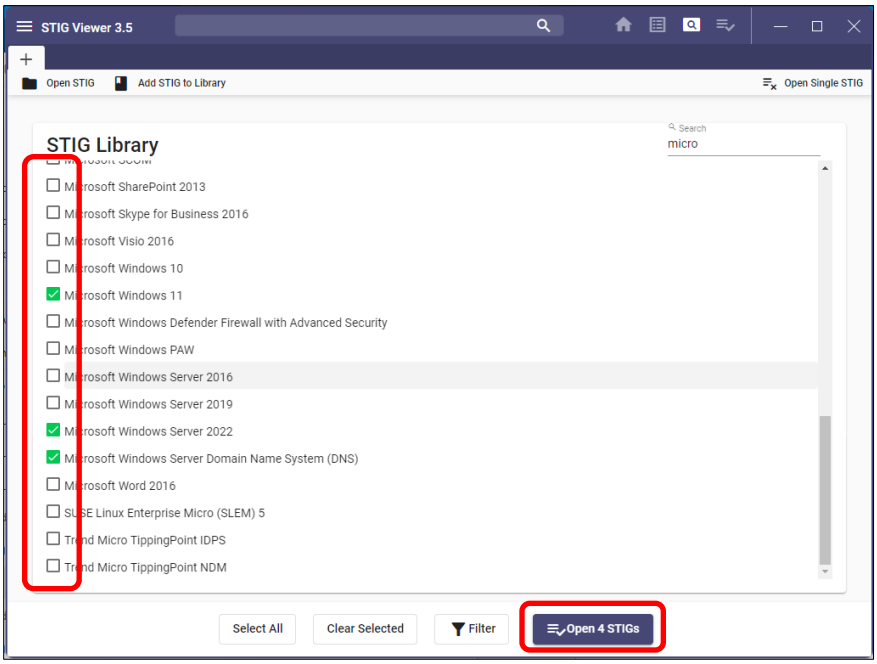
8. All fields will be exported unless the user deselects fields by clicking the file name to unhighlight it. The fields are divided into two sections: **Header** and **Rule Info**.

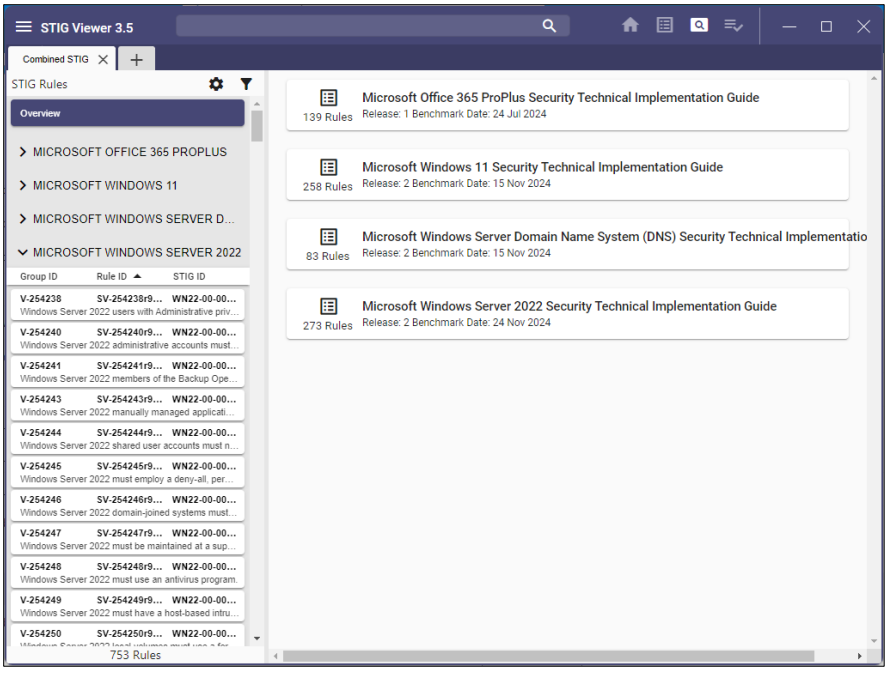


9. After all fields have been selected for export, click **Export.**
10. In the navigation window that opens, select where to export the STIG.

4.3.2 View Multiple STIGs – Unfiltered

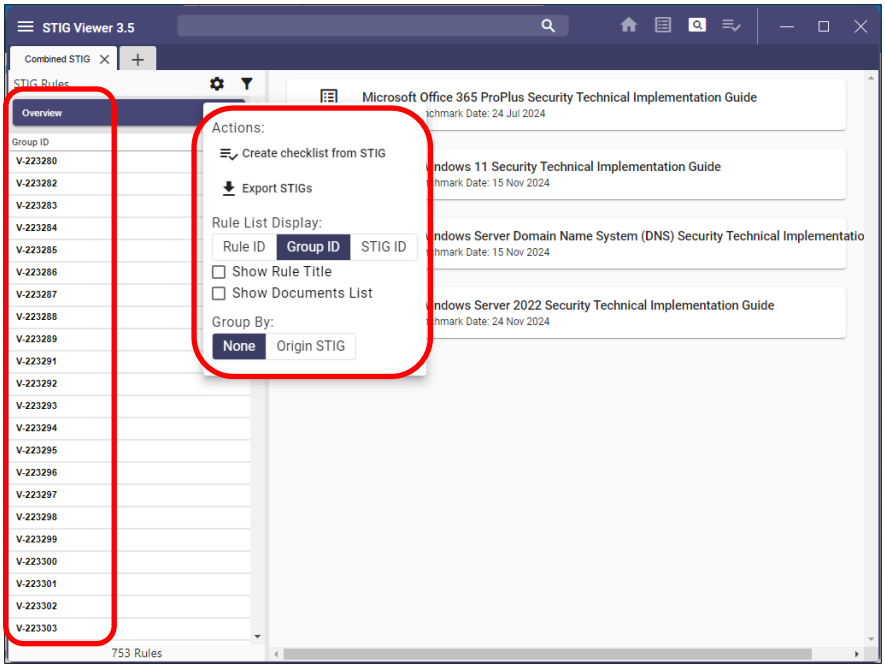
1. Select **Add STIG to Library** and navigate to the STIG's location. Select the STIGs to bring into STIG Viewer. The user can also bring in the entire Compilation file and choose STIGs from the list. Click **Open Multiple STIGs** in the top-right corner and select the checkbox beside the STIGs to be brought in together. At the bottom of the screen, click **Open X STIG**, where **X** represent the number of STIGs selected.



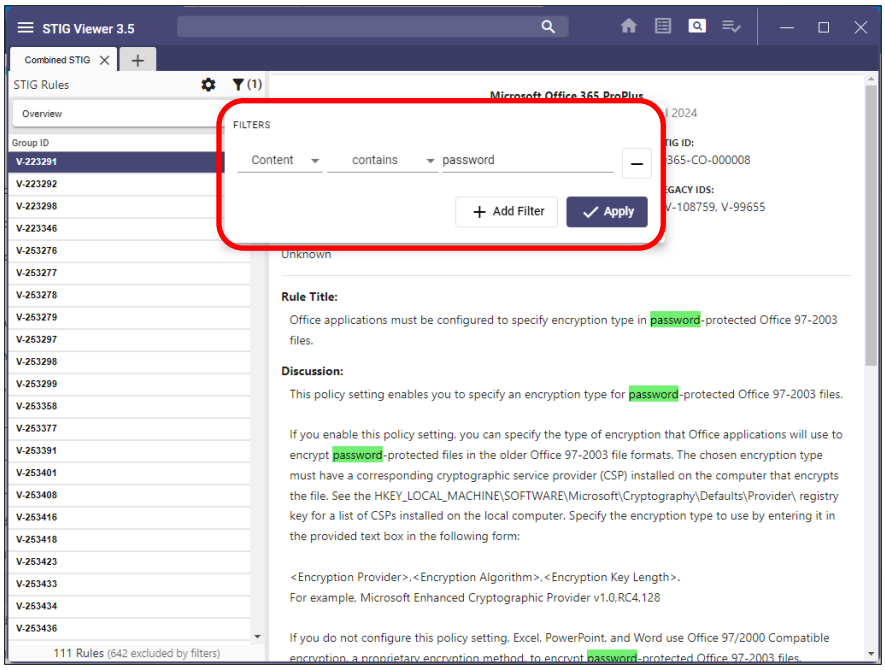


2. Each STIG will be listed on the left pane, with its respective documents listed first. To view all the requirements together, select the **gear** icon to change the view and then select **None**.

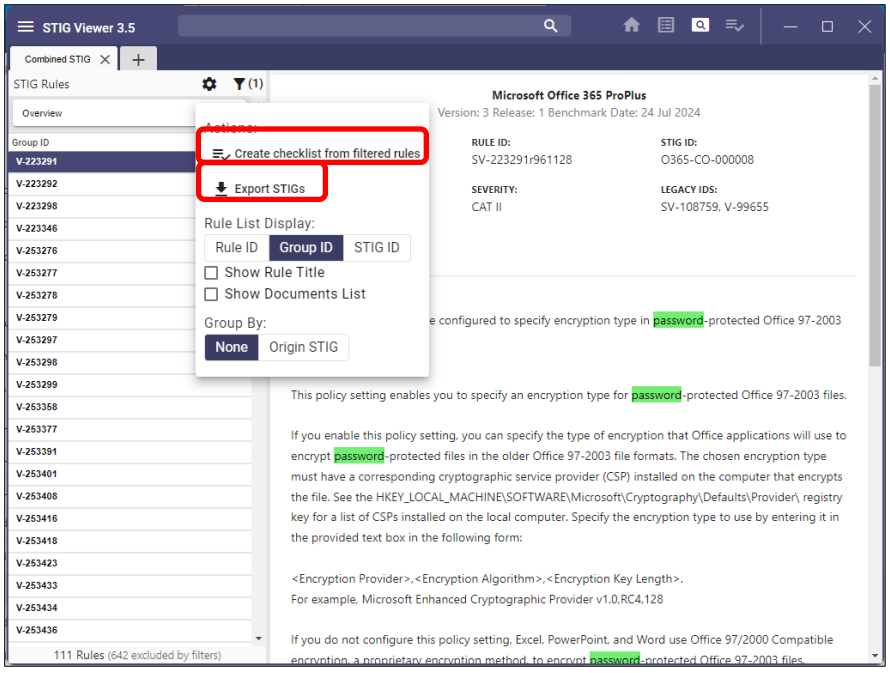
Note: In the screenshot below, **None** was selected, and **Show Rule Title** was unchecked. Now, all the requirements are listed in Group ID in ascending or descending order.



3. Add a filter to narrow down the requirements. The requirements that do not meet the filter are listed below the filtered requirements.

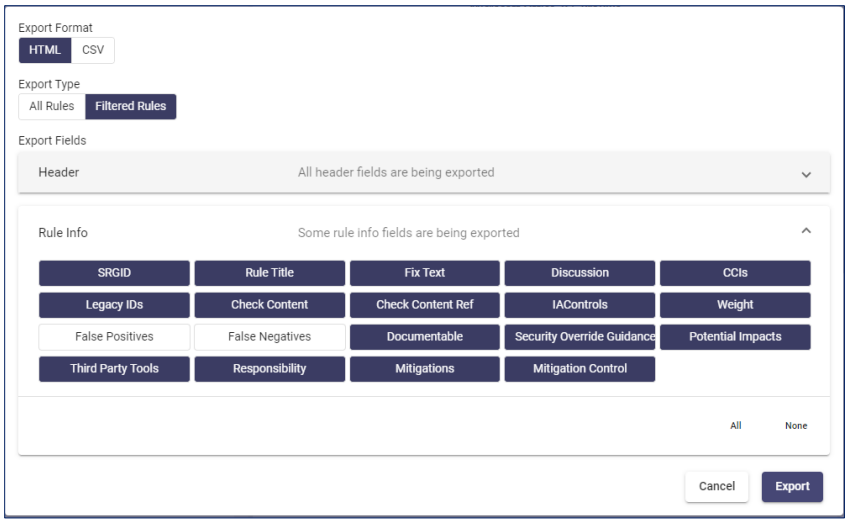


4. Create a checklist of the filtered requirements by clicking the **gear** icon and selecting **Create checklist from filtered rules.** Refer to the Checklist section for more information.



5. Export STIGs to HTML and CSV formats by clicking **Export STIGs** and selecting a format and the fields to export.

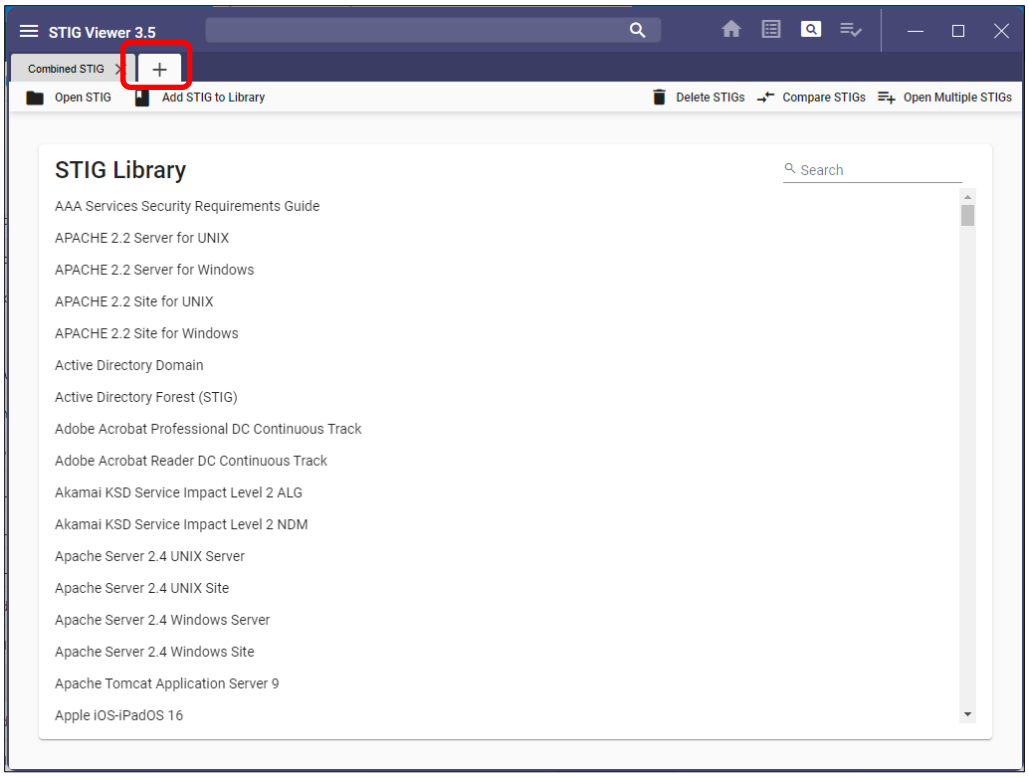
Note: All fields will be exported unless the user deselects them. To deselect, click the field name. The fields are divided into two sections: **Header** and **Rule Info**. Because this example is a selection of filtered items, the **Filtered Rules** selections have been made in the **Export Type** area.



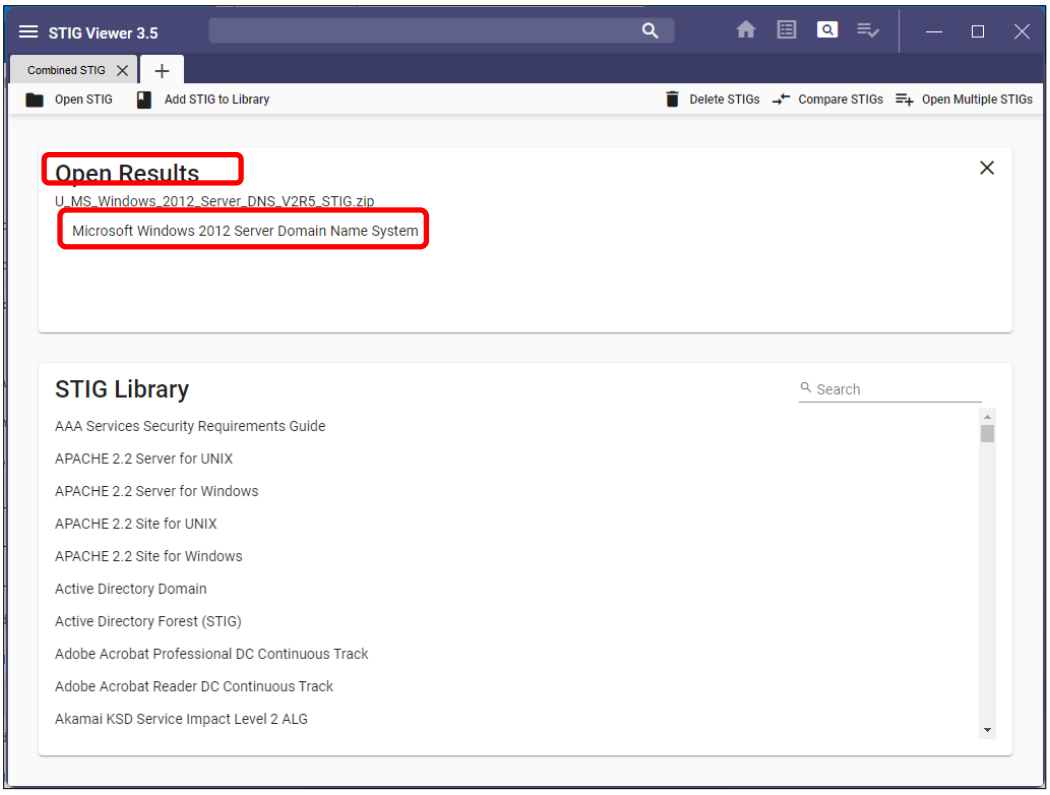
6. Once all desired fields have been selected, click **Export.**
7. In the navigation window that opens, select where to export the STIG.

4.3.3 Viewing More STIGs

View another STIG or combined STIGs by selecting the **+** (plus icon) tab in the upper portion of the screen. This opens the STIG Viewer explorer main page, where the user can add more STIGs for selection or open STIGs already in the list. The **Recent STIGs** section shows a list of recently opened STIGs. To open a recently opened STIG, click the STIG, and the details screen will open. To create another view of combined STIGs, follow the directions above.

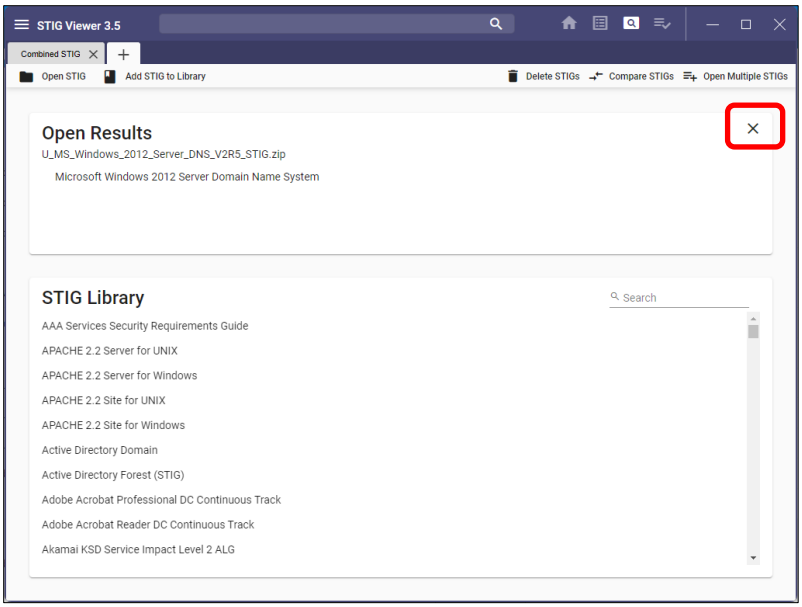


Note: If a STIG was opened and not saved to the library, it will be displayed as shown below. To view a STIG, click the STIG name in the **Open Results** section.

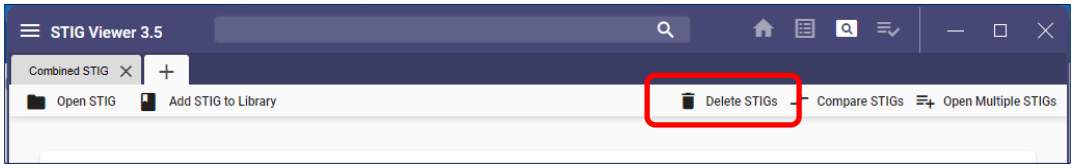


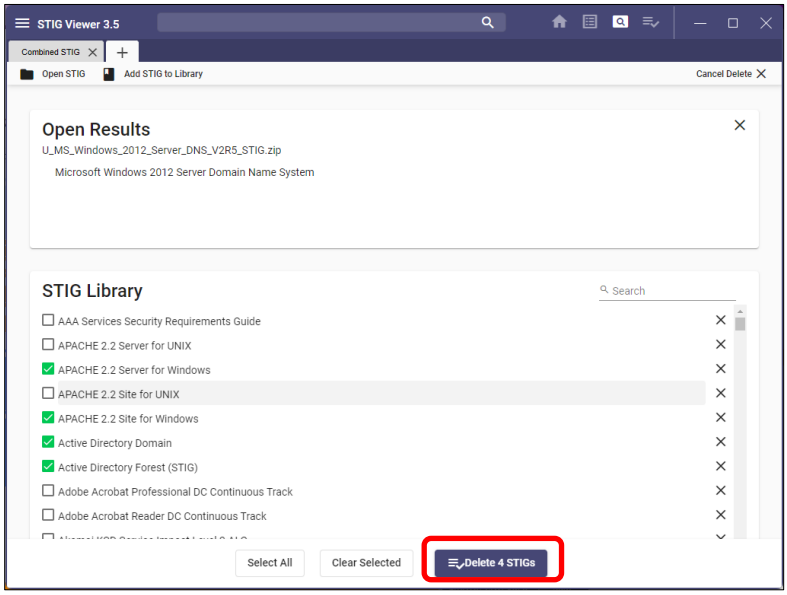
4.4 Remove STIGs from Recent STIGs and STIG Library

To remove a STIG not loaded in the Library, click the **X** to the right of the STIG name to be removed.



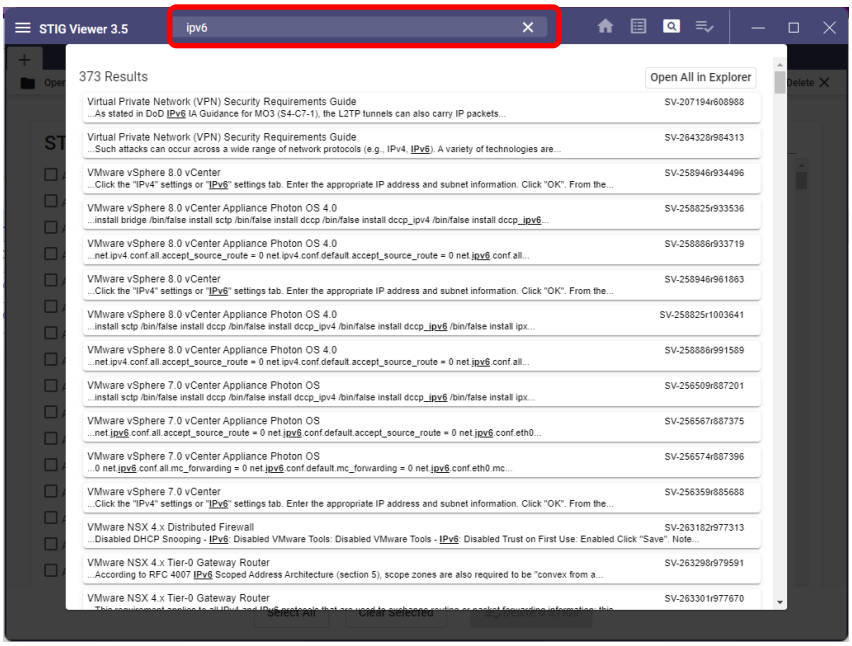
To remove STIGs loaded in the Library, click **Delete STIGs** and then check the box beside the STIGs to be removed and click **Delete X STIGs**, where X represents the number of STIGs selected. Users can **Select All** STIGs to select all the STIGs in their library and **Clear Selected** STIGs to clear all the selected STIGs**.**



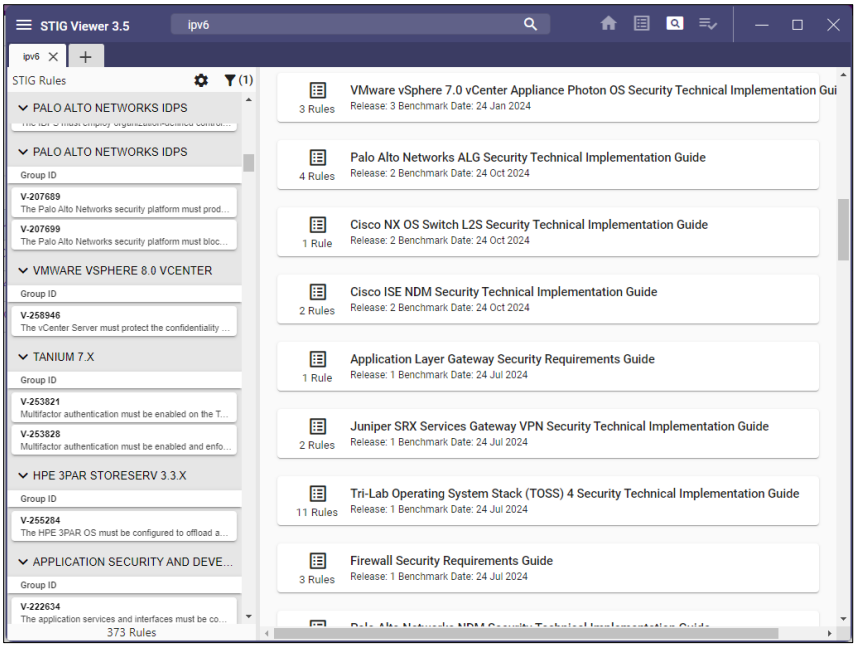


4.5 Keyword Search

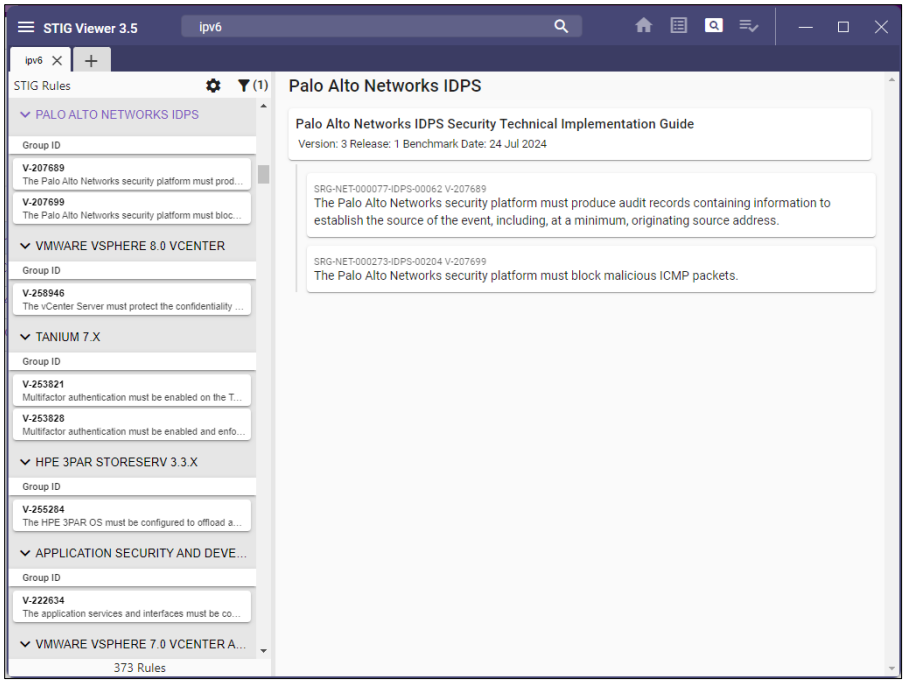
1. To search all STIGs listed in the user's library that contain a certain word (e.g., IPv6), enter the word in the search box at the top of the screen.



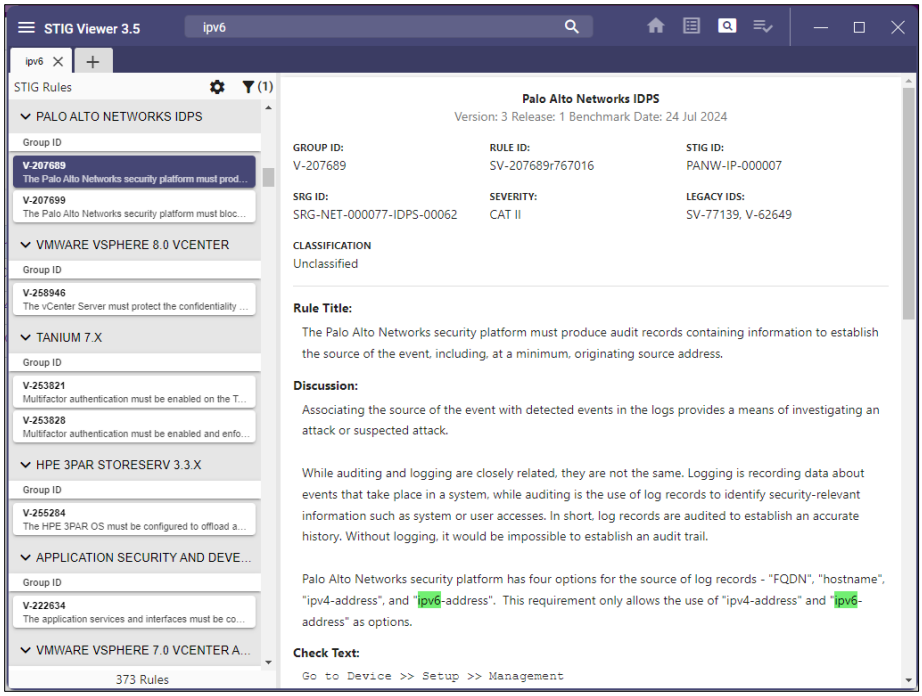
2. A list of all the Rules that contain the search word will appear. Click **Open All in Explorer** in the upper-right corner. This opens the STIG Explorer details screen to show all the STIGs that contain the search term in the main section of the screen and all the individual Rules in the left pane.



3. Scroll through the listed STIGs and click on a STIG to view all the Rules for that STIG that contain the search term.



4. To view the Rule details, click the Rule in the main pane.

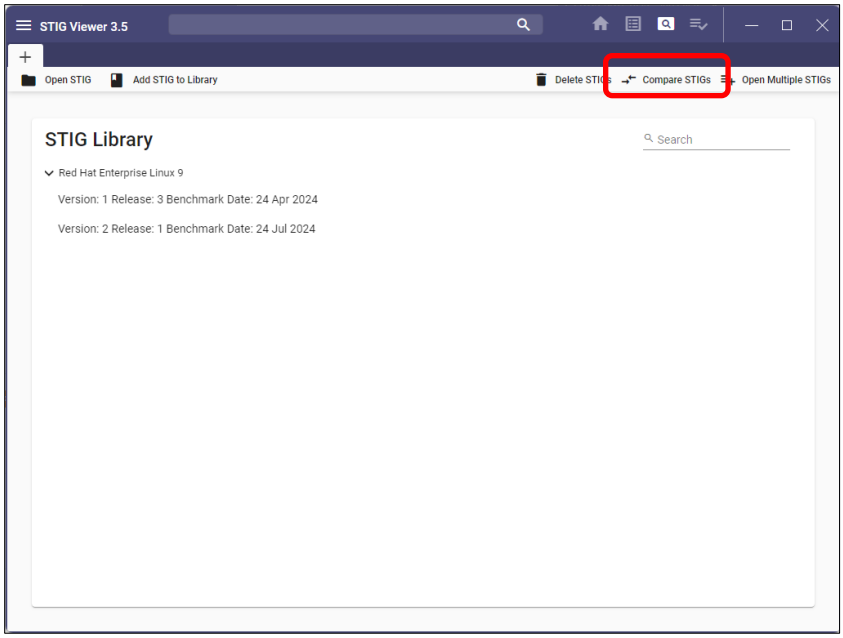


4.6 Comparing STIGs

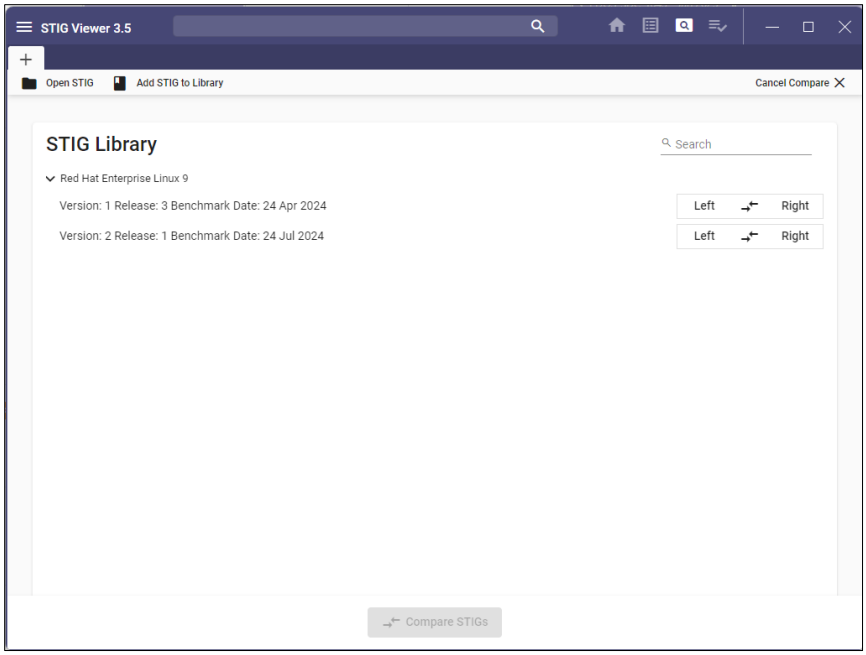
The user can compare differences between two versions of a STIG.

Note: For this option to work properly, it is important to load the STIGs that you want to compare in the correct order. The older STIG must be loaded into the Library first, followed by the newer STIG.

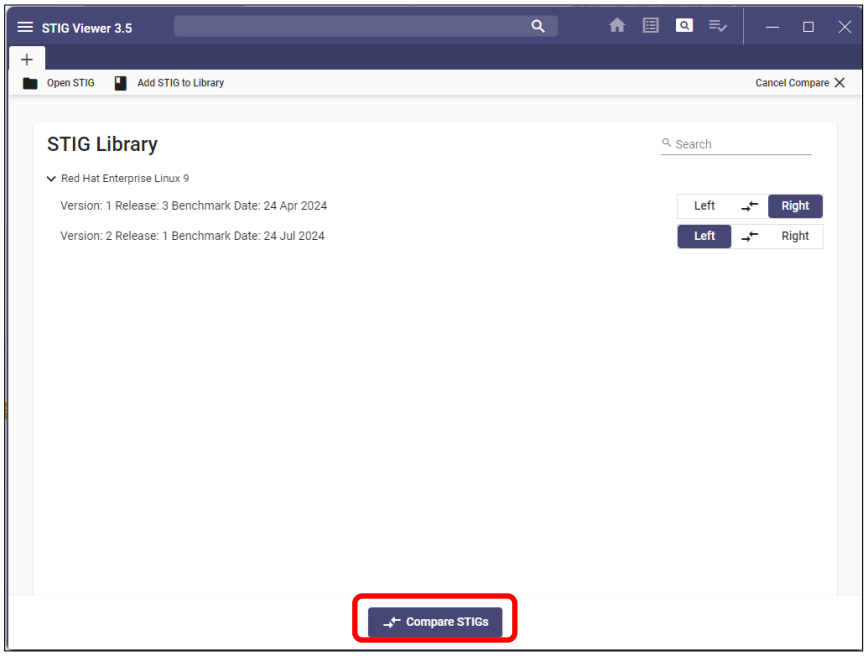
1. Ensure both versions are listed in the STIG Library and then click **Compare STIGs** located in the upper-right portion of the screen.



The screen should look like the following:

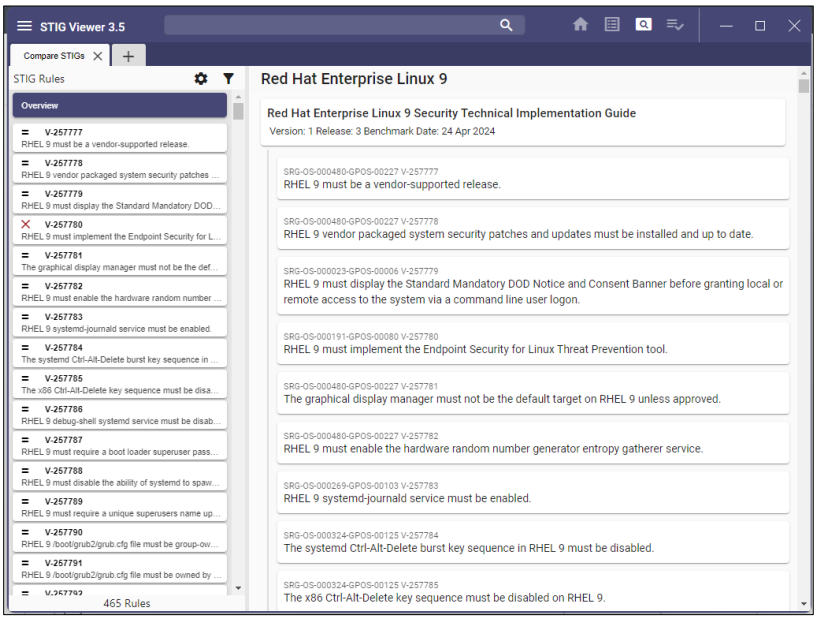


2. Select the **older** version for the **Right** and the **newer** version of the STIG for the **Left**, and then click the **Compare STIGs** button located at the bottom of the page.

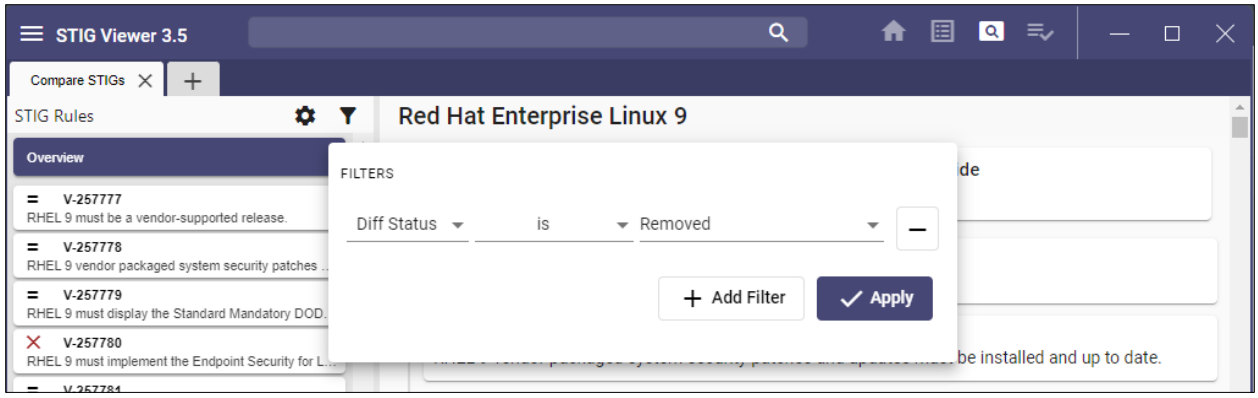


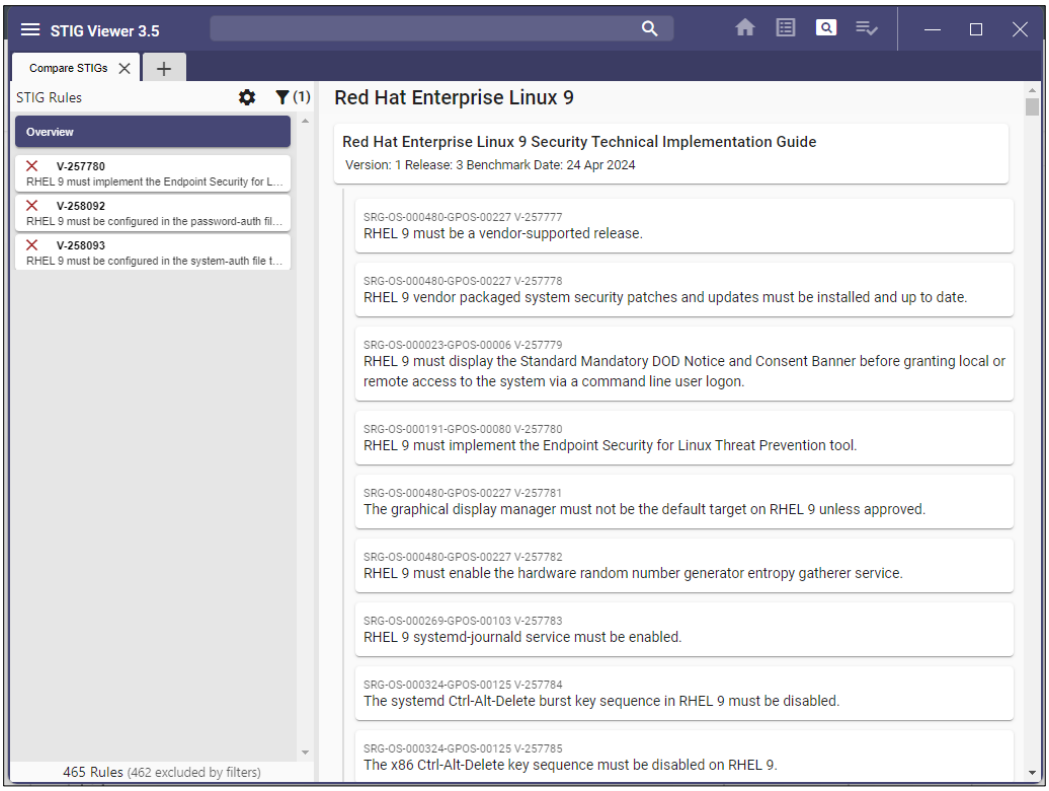
Note: The Benchmark Dates should be used to determine the older and newer version of a STIG because when a major release of a STIG occurs, the release number will be reset back to "1," as shown in the case above.

Note: The development team is working to make this more user friendly.



3. Users can scroll through the rules and look for **Changed** rules (denoted with an orange-colored asterisk), **Added** rules (denoted with a green-colored plus sign), and **Removed** rules (denoted by a red-colored X), or they can apply a **Diff Status** filter to view only **Unchanged** rules, **Changed** rules, **Added** rules, or **Removed** rules by clicking on the funnel icon.

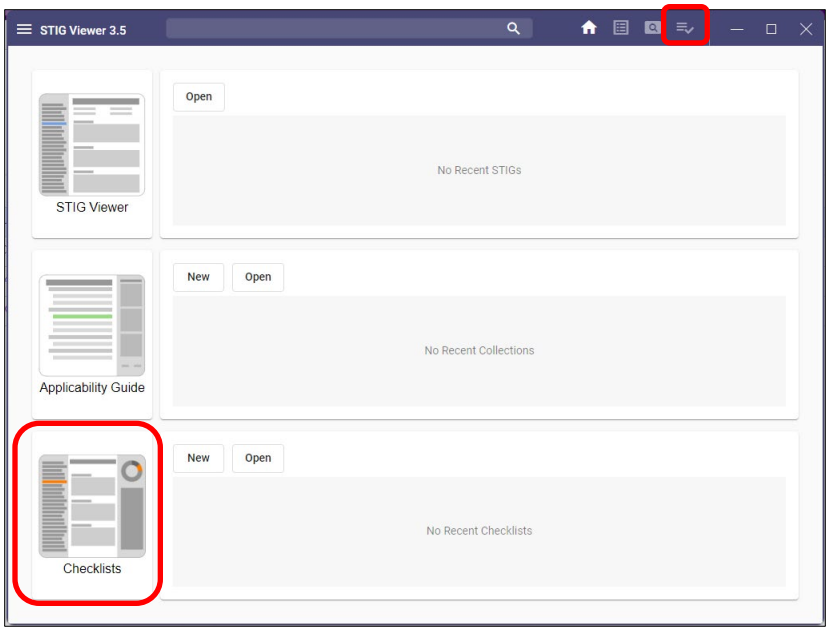




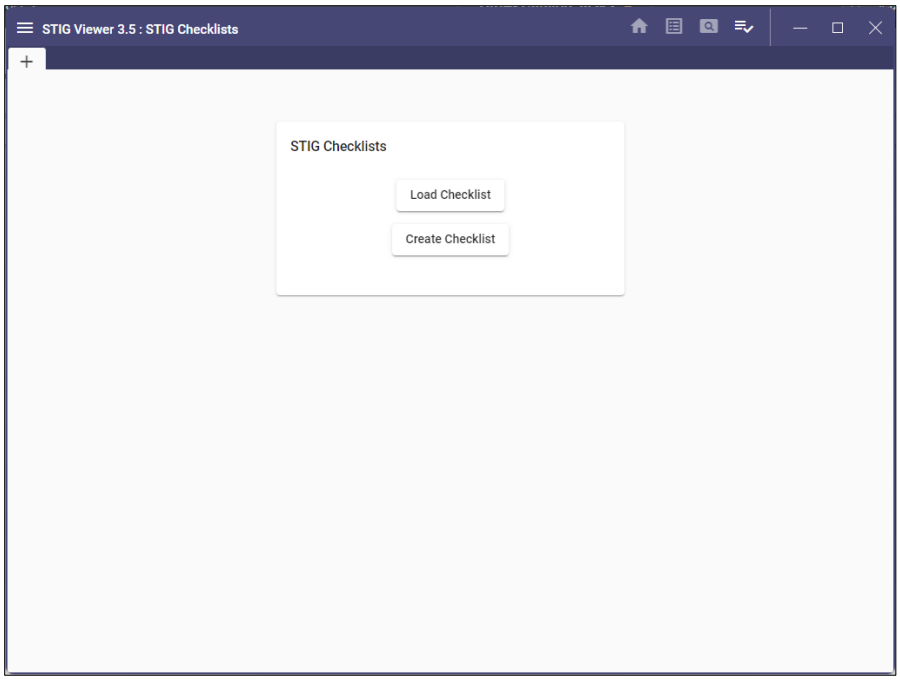
5. CHECKLIST

5.1 Create Checklist from Home Page or Top Navigation Bar

1. If STIGs are loaded into the library, checklists can be created by clicking the **checklist** icon (represented by three lines and a checkmark at the top of the screen) or clicking the **Checklists** section at the bottom of the **Home** page.

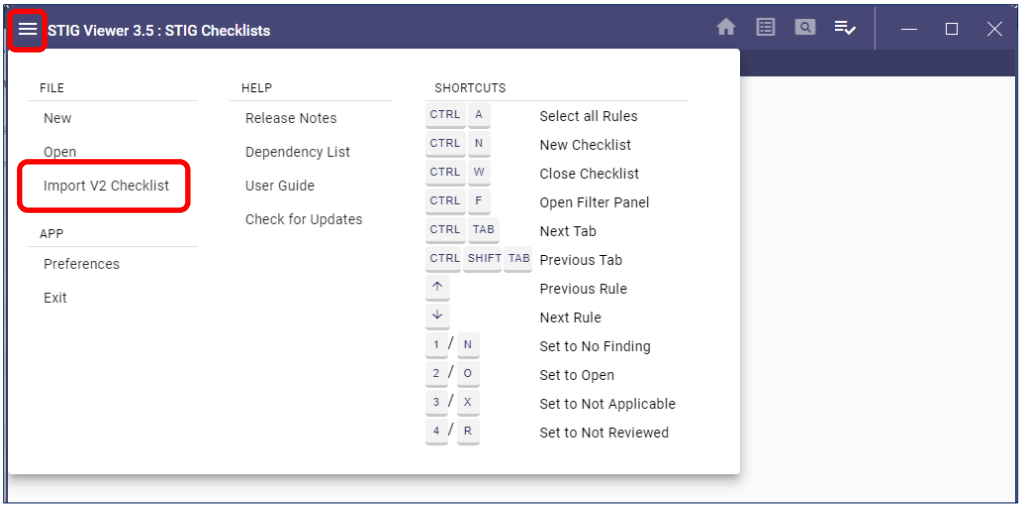


2. When either of these selections are made, the screen will look like this:

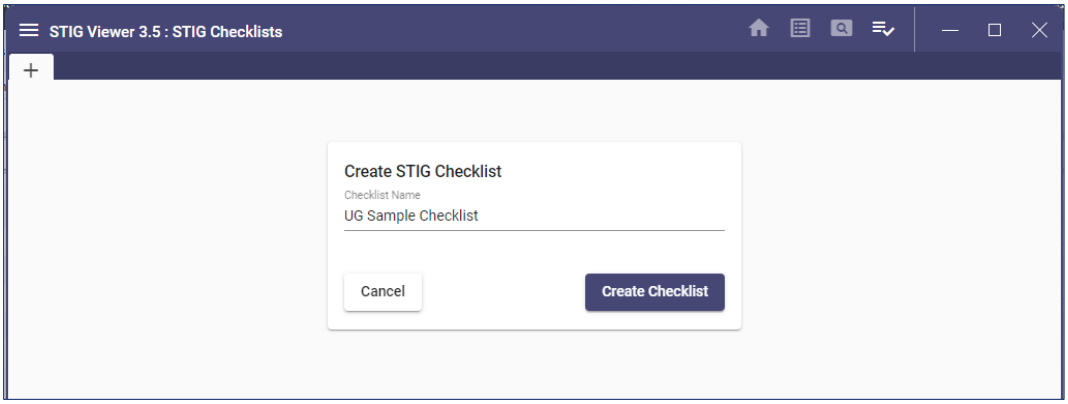


3. Click **Create Checklist** to create a new checklist or **Load Checklist** to open an existing V3 checklist.

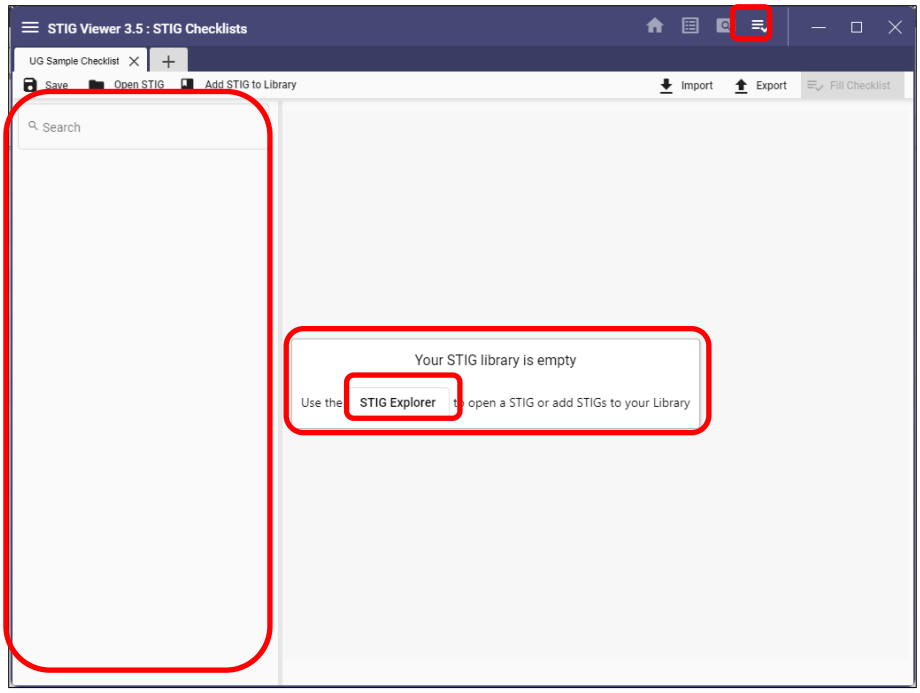
   Note: Checklists created in STIG Viewer 2.x can be imported to STIG Viewer 3.x by clicking the hamburger menu and selecting **Import V2 Checklist.** Users can import multiple STIG Viewer 2.x checklists into STIG Viewer 3.x by navigating to a central location and selecting the desired checklists to import.



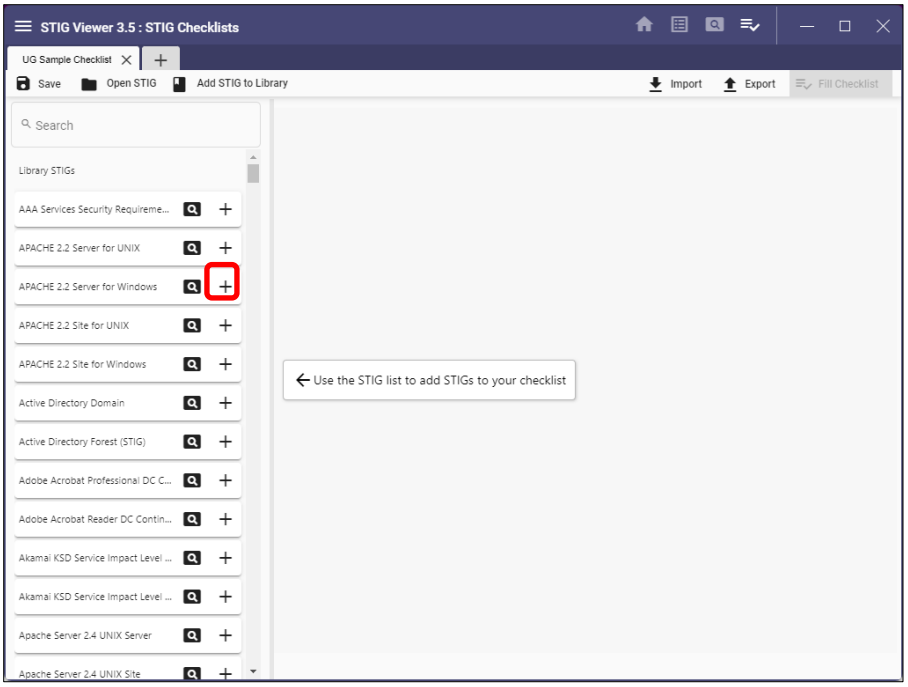
4. After clicking **Create Checklist**, a prompt to name the checklist appears. After entering a name, click **Create Checklist**.



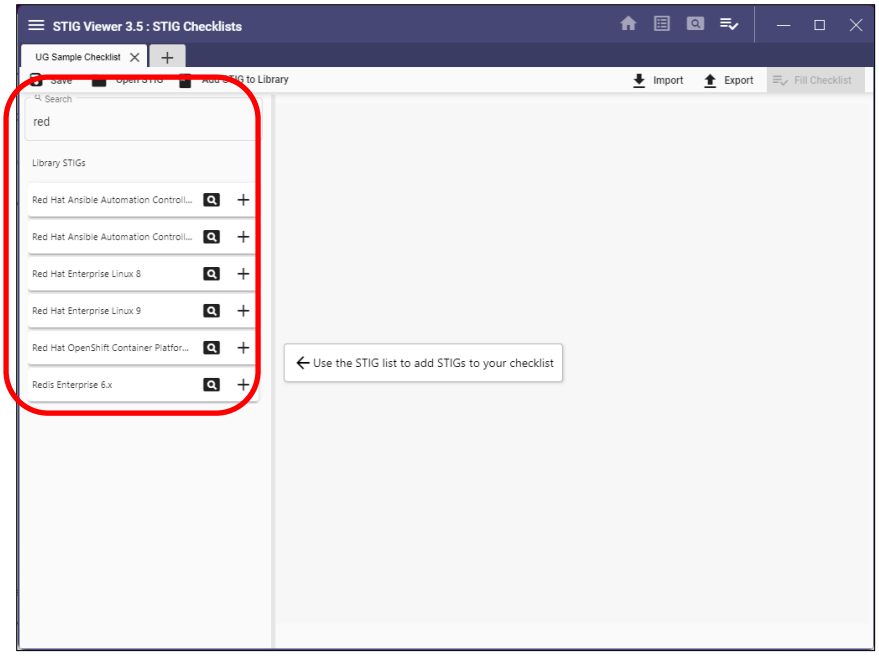
5. The user will be prompted to select from the STIGs listed in the left pane. If no STIGs are loaded in the library, use the STIG **Explorer** button to add STIGs.



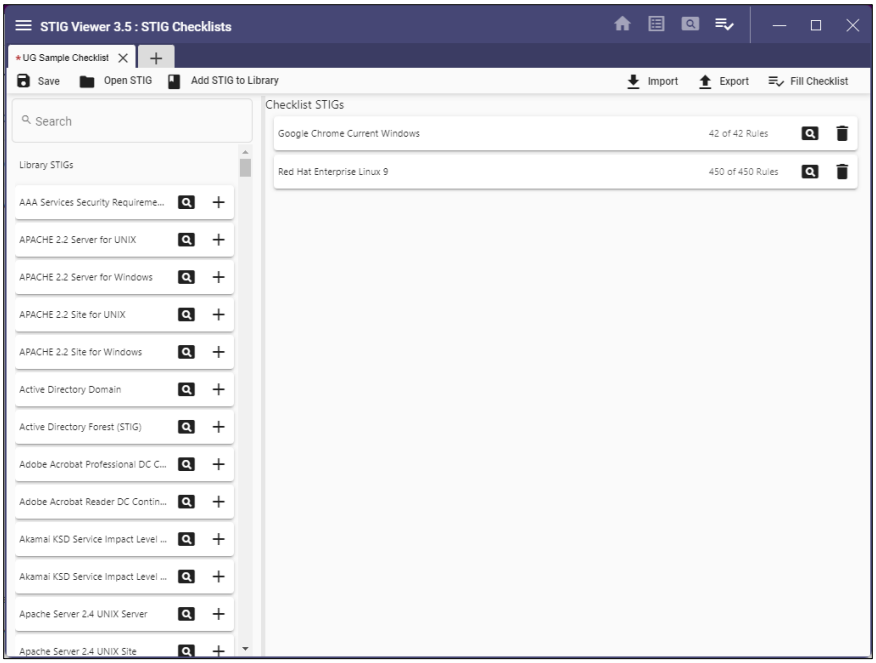
6. If STIGs are loaded into the library, select STIGs to be included in the checklist by clicking the **+** beside the STIG name.



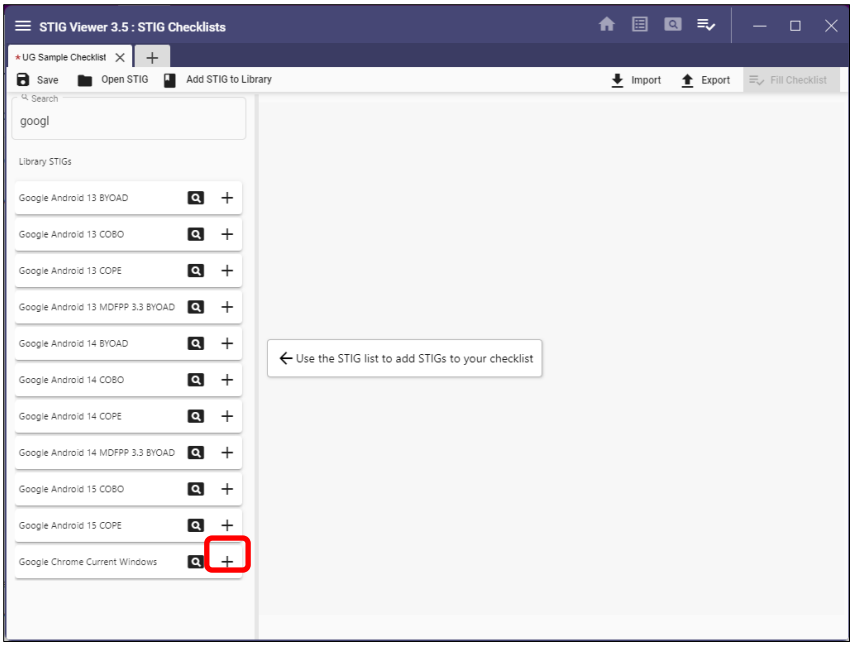
Note: Use the **Search** field to find STIGs to be added.

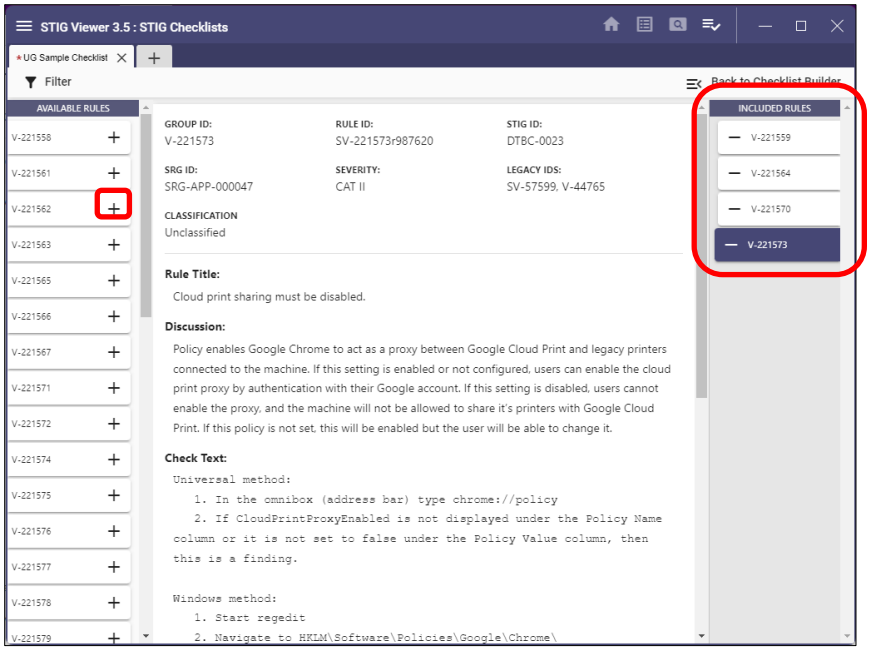


7. Clicking the **+** beside the STIG name adds all rules to the main pane for inclusion in the checklist.

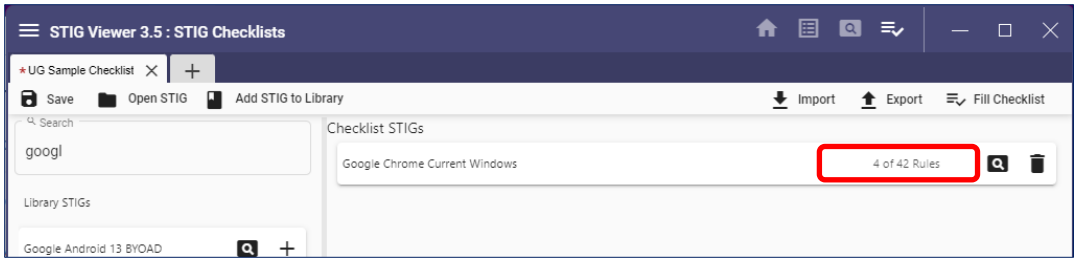


Note: To select individual rules to include in the checklist, click the magnifying glass beside the STIG name and click the **+** beside the desired rules. The selected rules will be listed in the far-right pane.

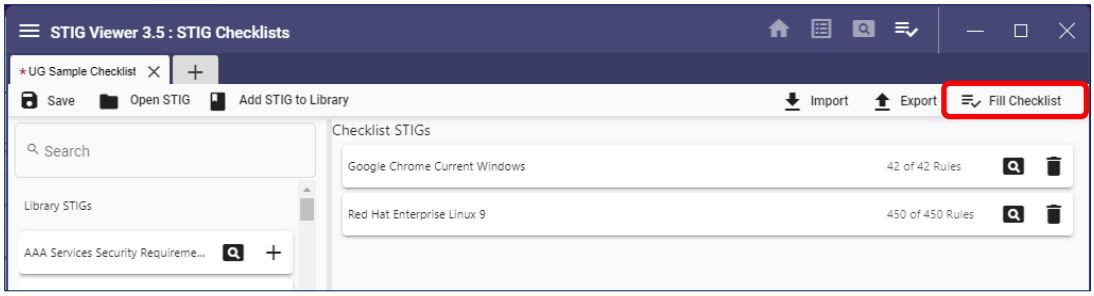




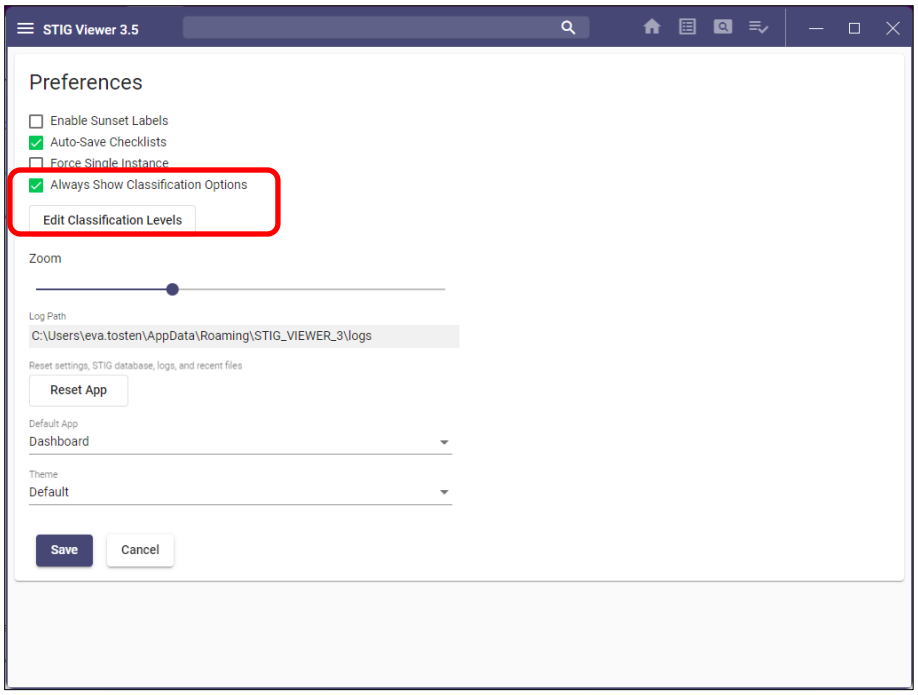
8. Click the **Back to Checklist Builder** in the upper-right corner to return to the STIG selection pane. The count of included rules for a STIG will be listed beside the STIG name.



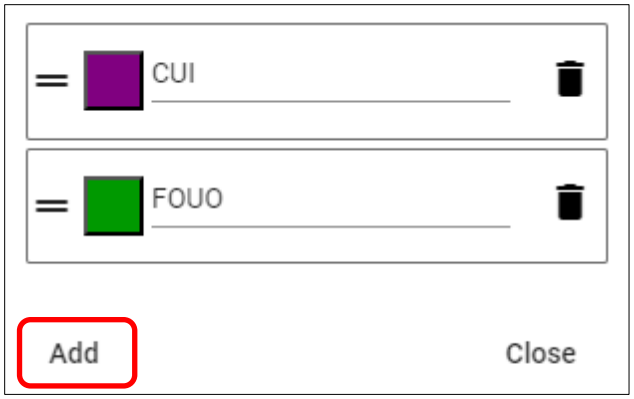
9. After all desired STIGs are listed in the main pane, click **Fill Checklist** in the upper-right corner to begin processing the checklist.



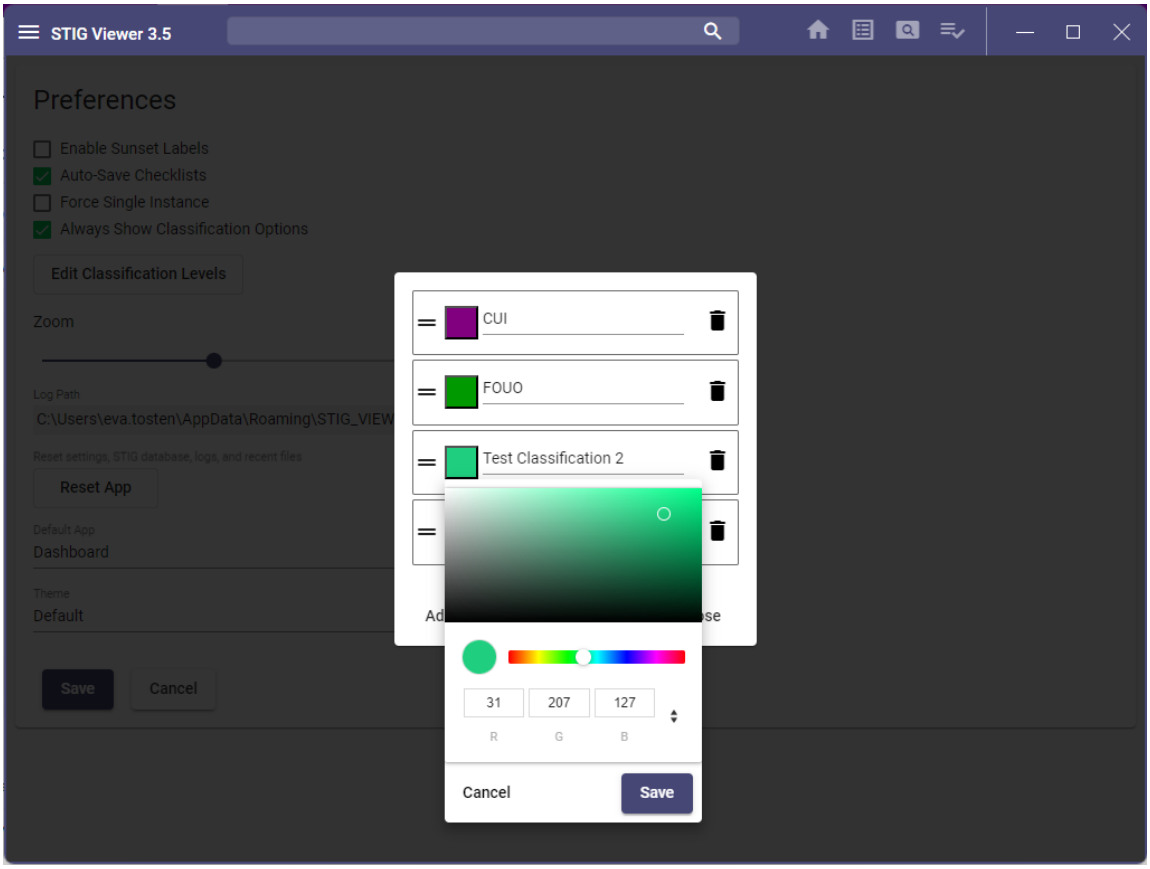
Note: Users can add classification to user-controlled pieces of the checklist (i.e., Comments, Finding Details, and Target Data) by opting to in their **Preferences**. Select the **Always Show Classification Options** and then click **Edit Classification Levels**.



Users can add different classification values.

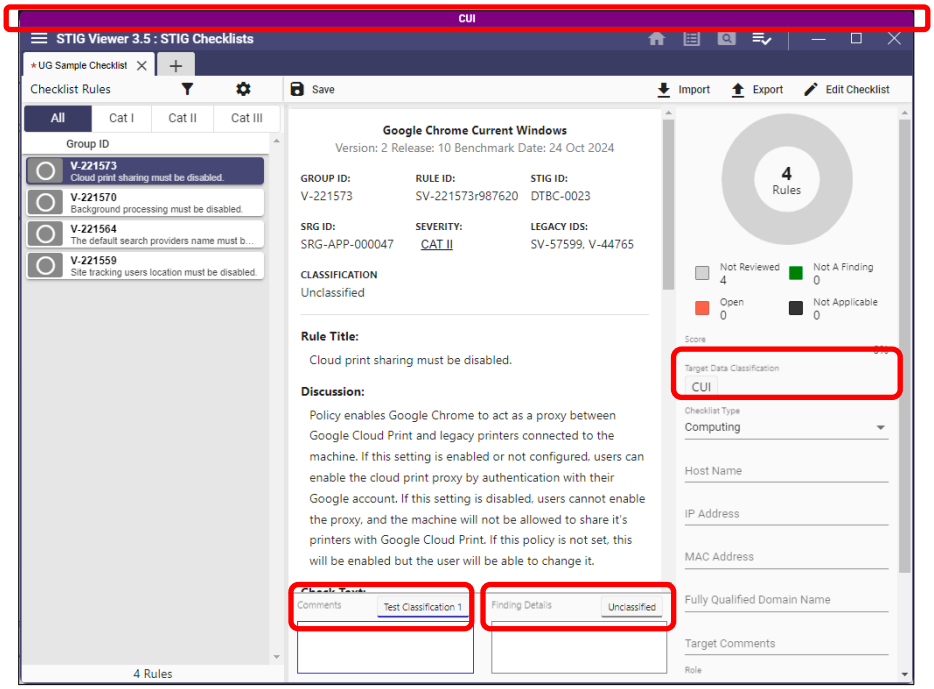


Select a banner color. Classification options can be arranged by clicking and dragging the equals sign to the left of the color picker.



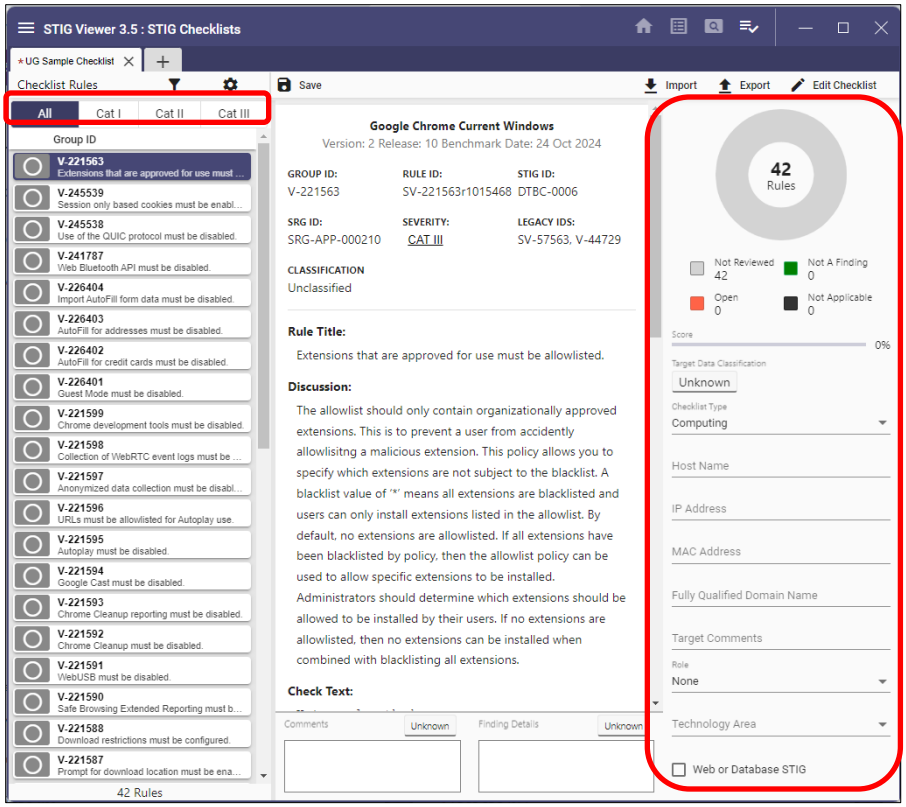
Higher classification levels in the list take priority. If a document has both CUI and FOUO items, CUI will be displayed on the banner.

Note: Some of the screenshot images contained in this document are labeled as CUI for instructional purposes but do not contain any CUI data.

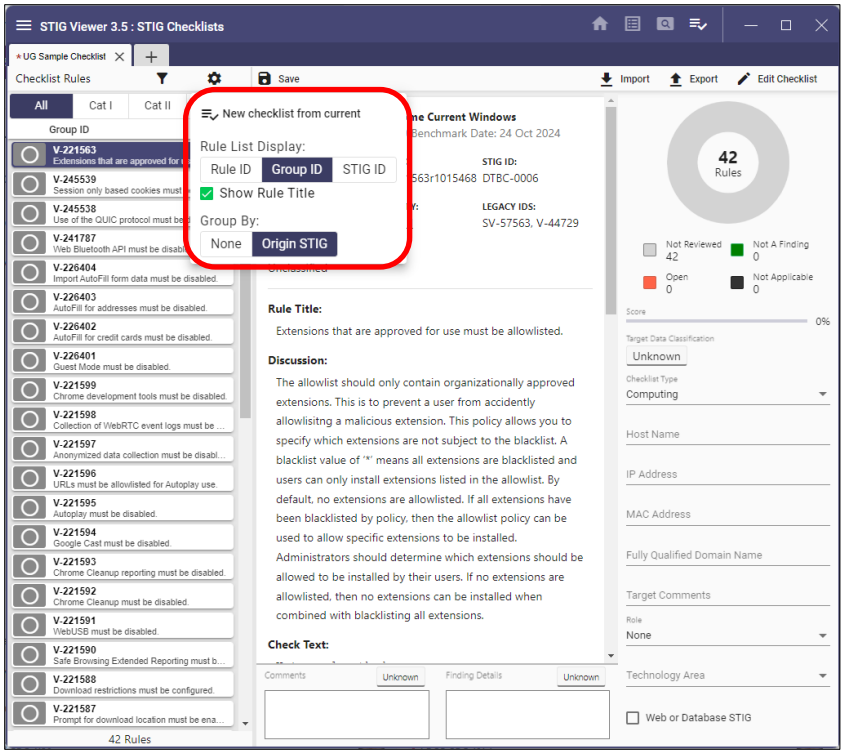


10. The STIG details will be displayed. There is a tab for the combined severities and individual tabs for each severity. The Target Data is on the right portion of the screen along with a graph of Rule Statuses and their respective counts.

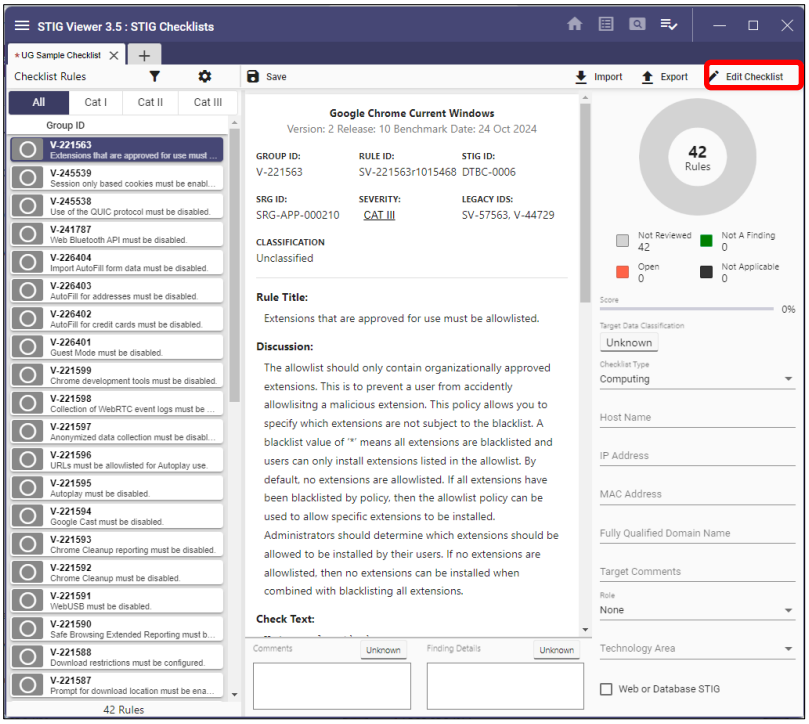
    Note: As the user updates the status of rules, the **Score** will be updated accordingly. This uses rule status and weight to determine the checklist score.



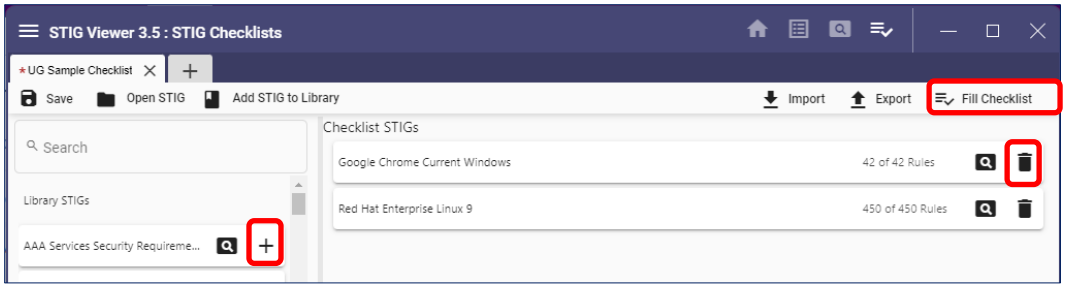
11. To change the **Rule List Display:**, add **Rule ID** and **STIG ID** to the left pane, sort on any of them in ascending or descending order by clicking the gear icon, and click the desired header to add. Also, **Group By:** can be changed from the default of **Origin STIG** to **None**.



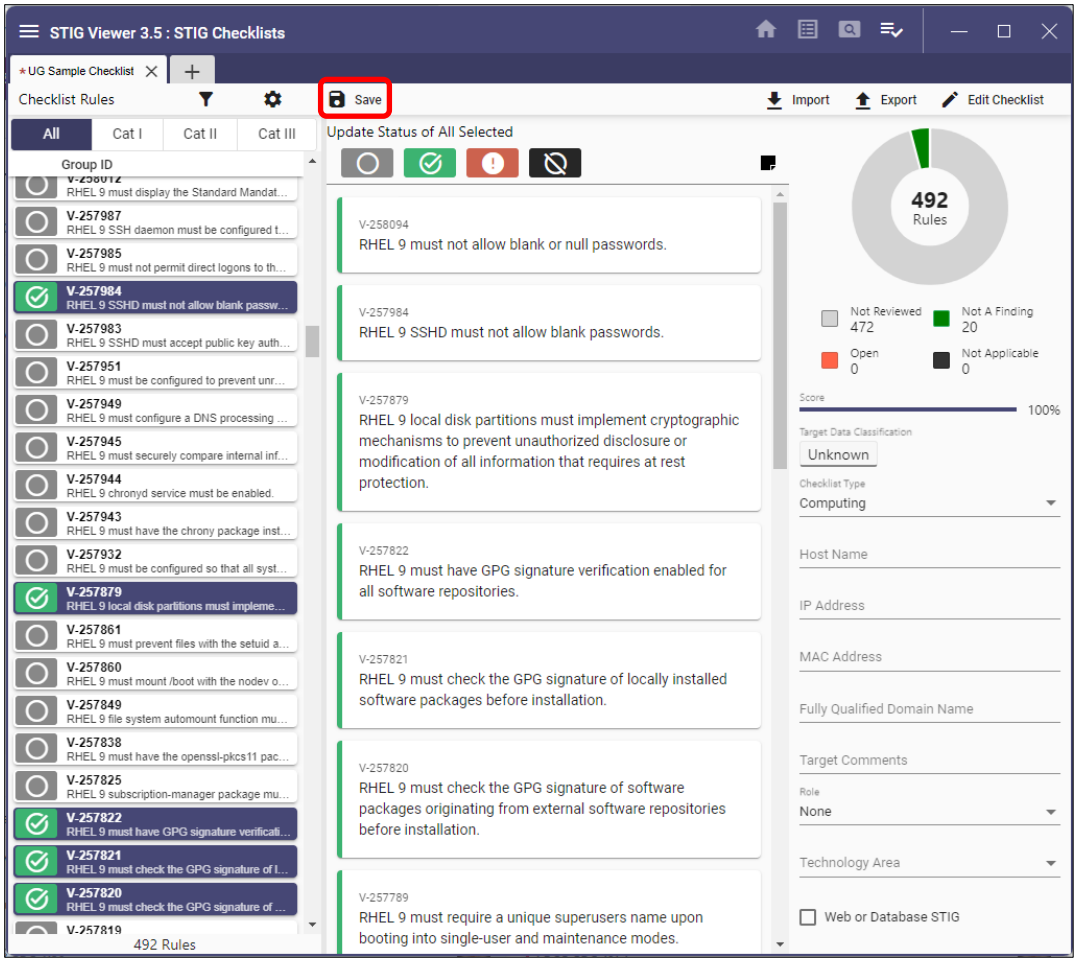
12. To add a STIG to or remove a STIG from the checklist, click **Edit Checklist** in the upper-right corner.



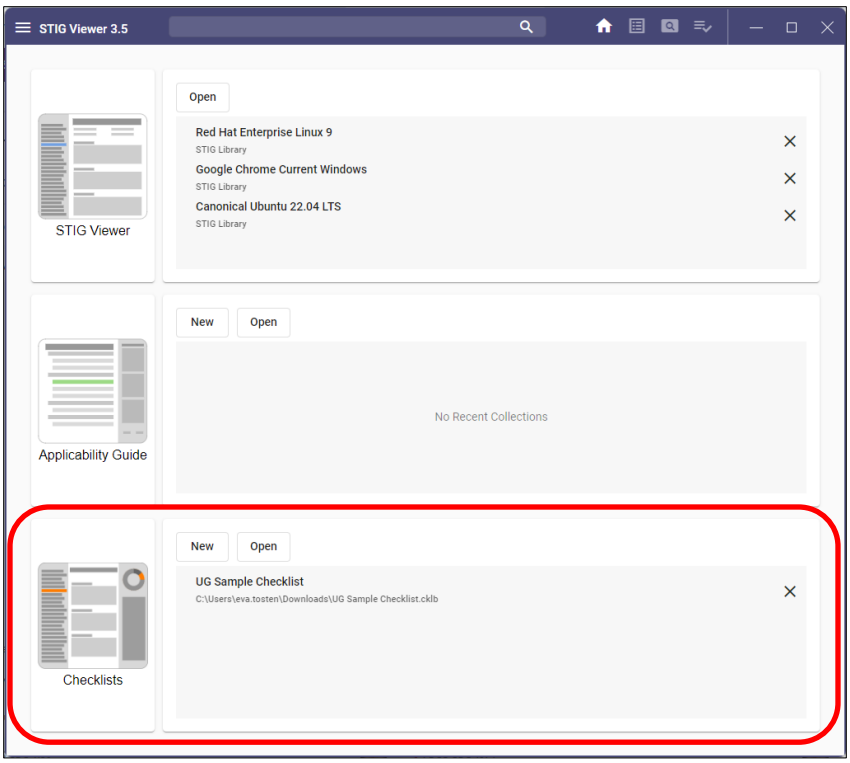
13. To remove a STIG, click the trash can icon beside the STIG name in the main pane. To add a STIG, click the **+** beside the name in the left pane. To go back to editing the checklist, click **Fill Checklist** in the upper-right corner.



14. After all edits have been made to the checklist, click **Save** to finish creating the checklist.

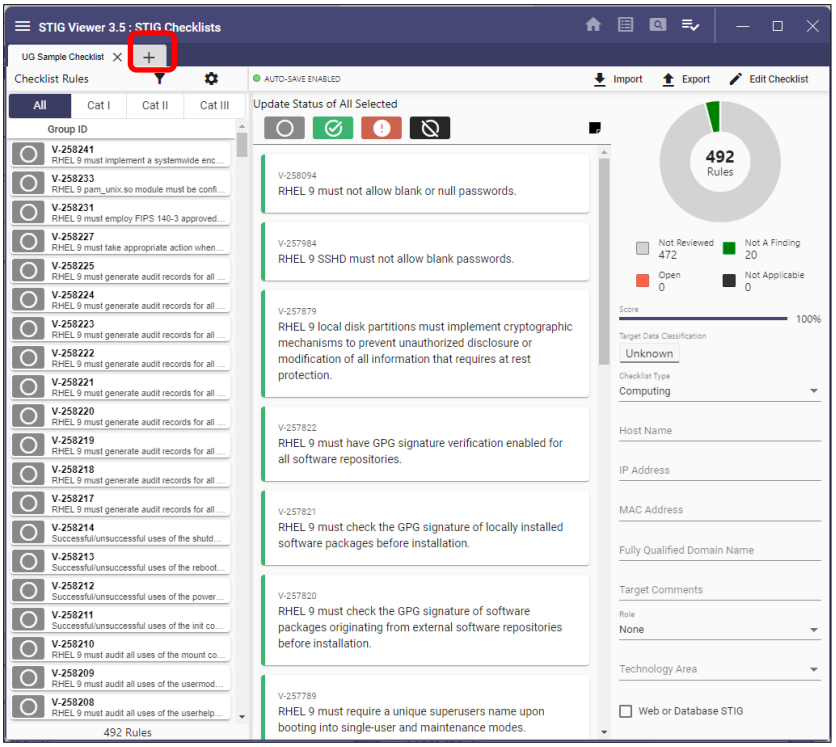


15. The saved checklist will now appear on the homepage under the **Checklists** section.

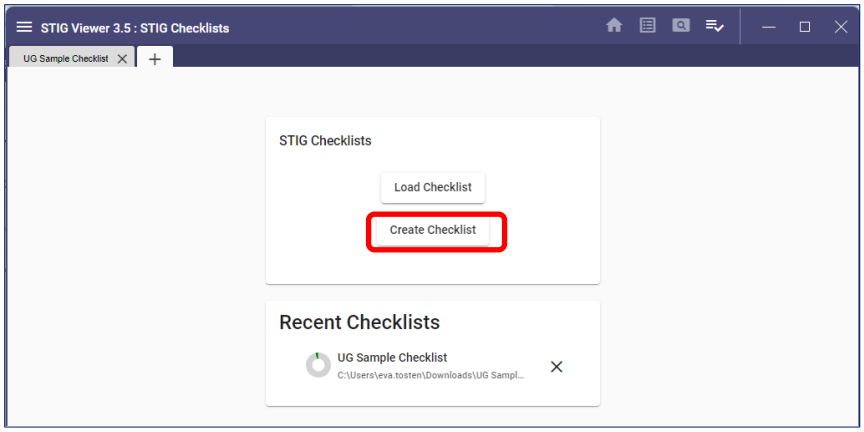


5.2 Create Another Checklist

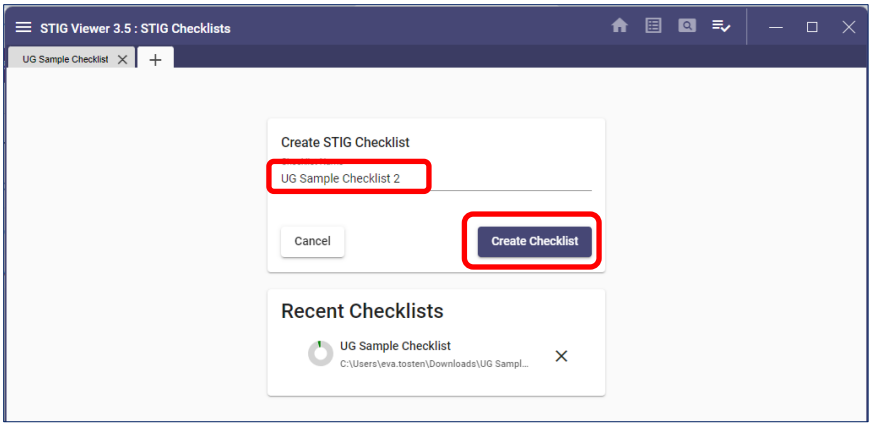
1. To add a checklist from the STIG Checklists page, click the **Add (+)** tab.



2. Select **Create Checklist**.

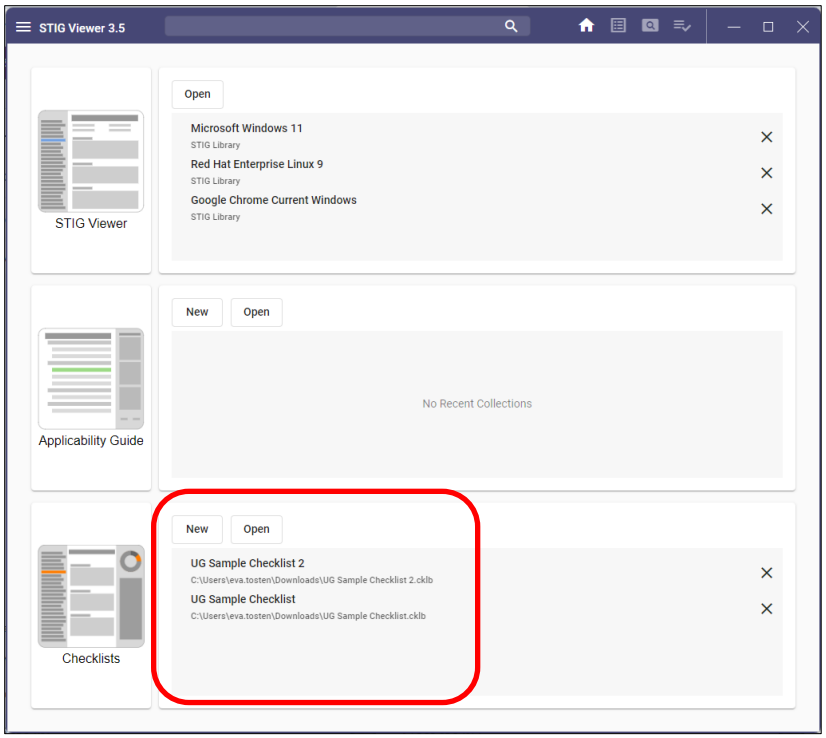


3. Enter a name for the checklist and then click **Create Checklist**.

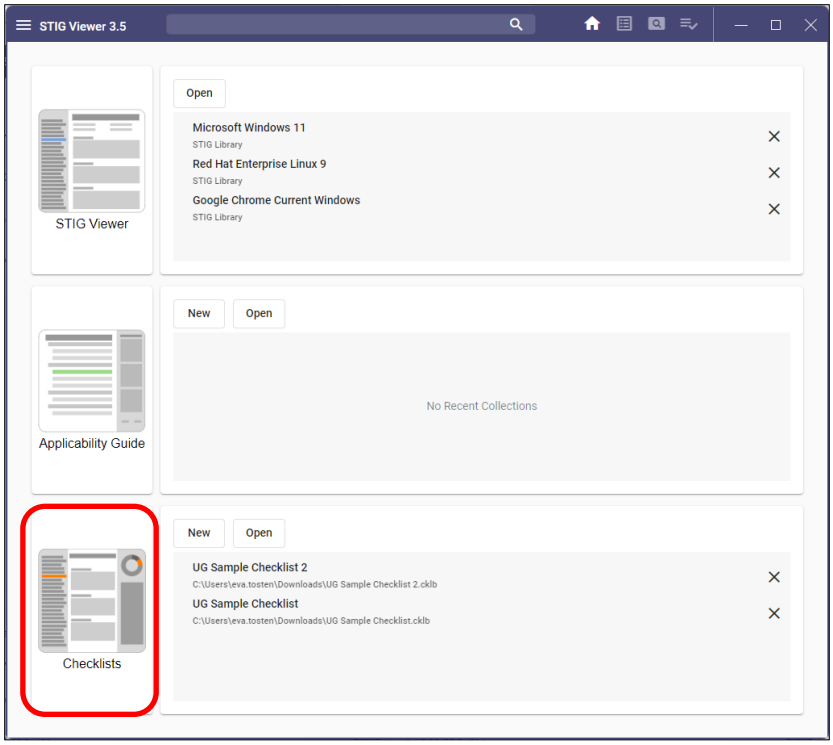


5.3 Opening an Existing Checklist

To open an existing checklist, navigate to the **Home** page and select one of the checklists listed or click **Open** and navigate to the location of the checklist.

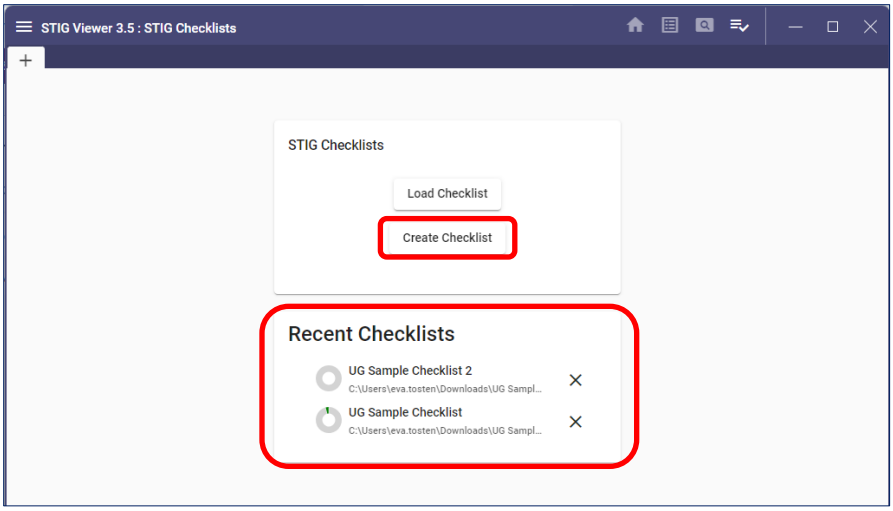


Another option is to click the **Checklists** icon on the left.



Select one of the **Recent Checklists** or click **Load Checklist** and navigate to the checklist to be loaded.

Note: If a checklist is already open, the user will need to click the **Add (+)** tab to open a new screen.



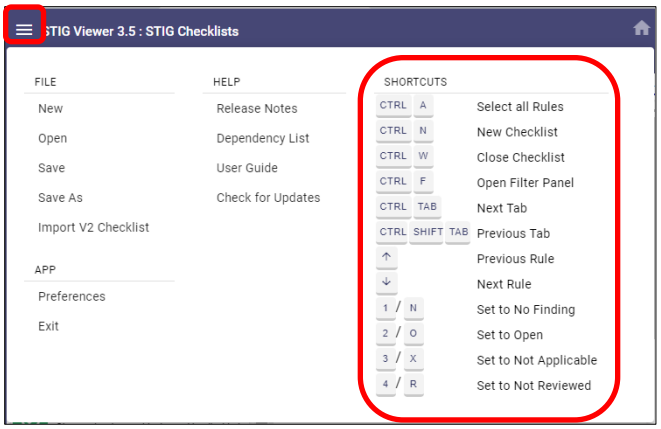
5.4 Updating Checklists

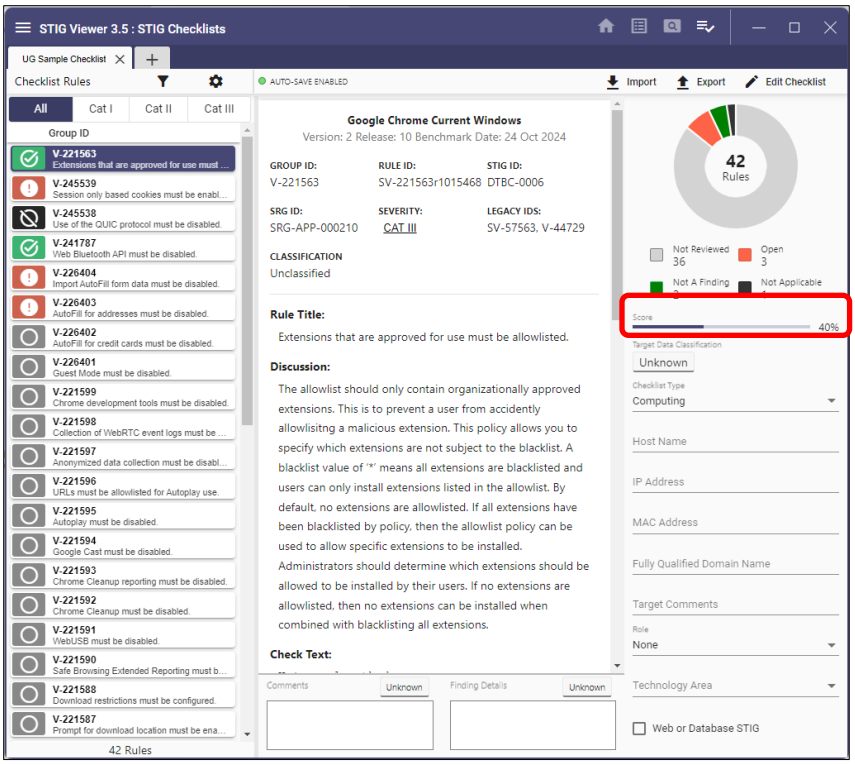
5.4.1 Changing the Status of Rules

1. To mark requirements as **Open, Not A Finding, Not Reviewed**, or **Not Applicable**, click the circle beside the Rule. Click once to set the status to **Not a Finding** (green checkmark), twice to set the status to **Open** (red exclamation mark), three times to set the status to **Not Applicable** (black circle with slash), and four times to set the status back to **Not Reviewed** (gray blank circle)**.**

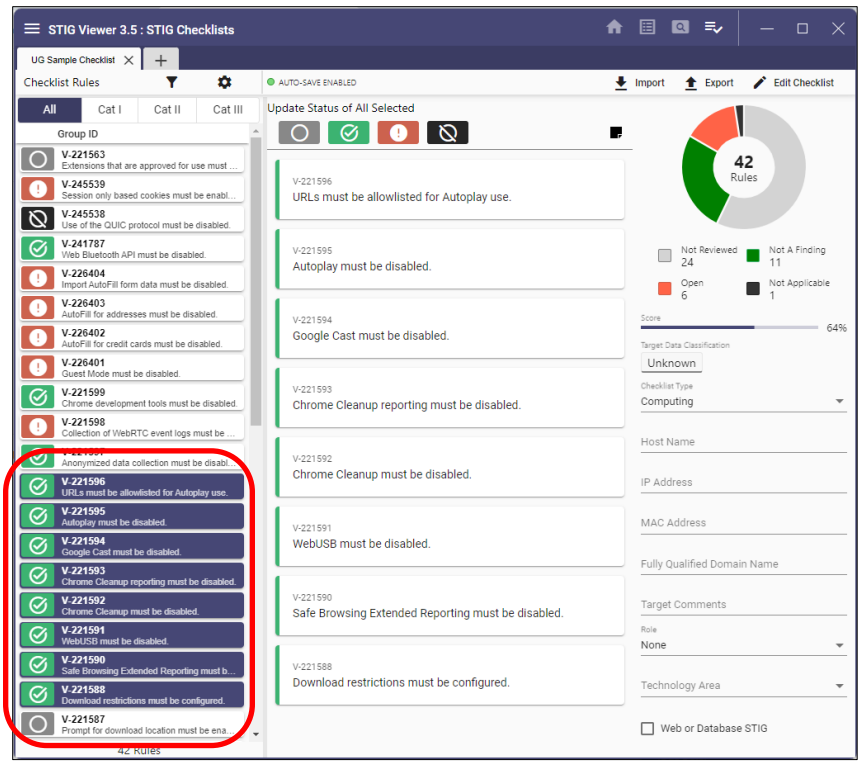
   Note: As the user updates the status of rules, the **Score** will be updated accordingly. This uses rule status and weight to determine the checklist score.

   Note: To view the shortcut keys, click the hamburger menu.





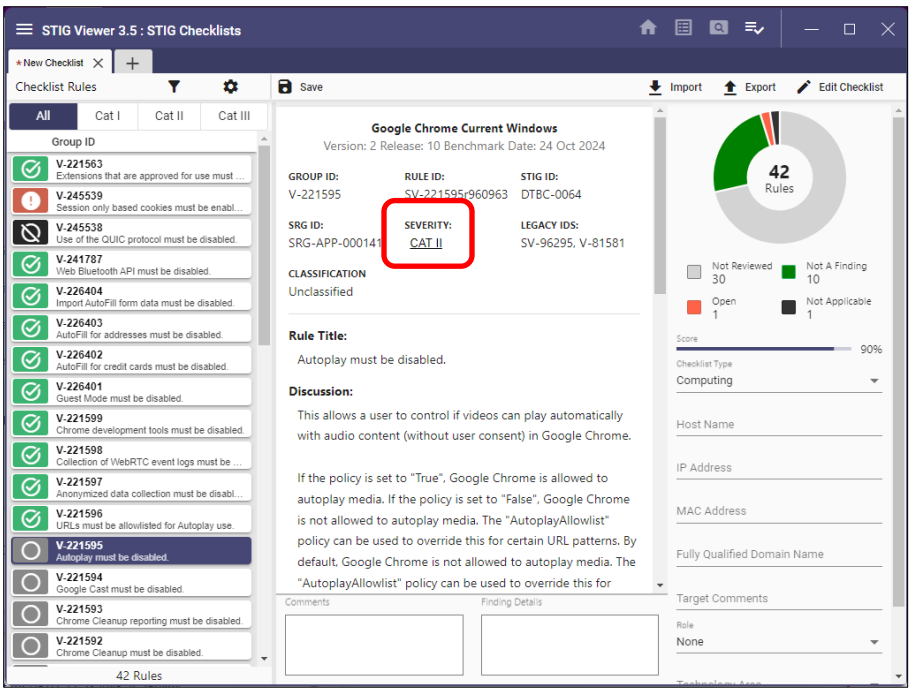
2. To update multiple rules, select the rules to be updated by clicking the ID and either using SHIFT and clicking another ID to include all IDs in between, or using CTRL and clicking the rules to be updated. At the top of the center pane, the possible statuses appear. Clicking any of these will set all selected rules to the selected status.



Note: When a new status is assigned, the chart on the right side updates to reflect progress, the circle beside the ID reflects the assigned status, and the Score is updated.

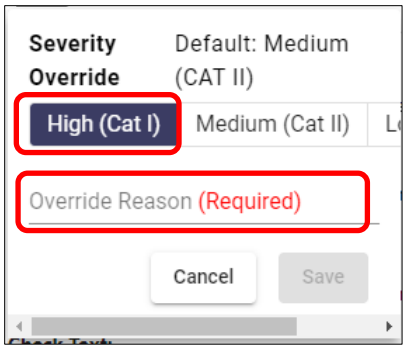
5.4.2 Override Severity Status

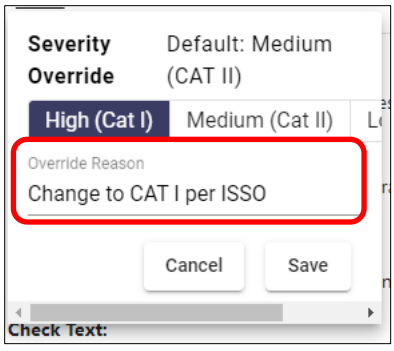
Users can override a severity status by clicking on the severity and then changing the severity to a different value.



User must select the new severity, which will trigger the requirement of an **Override Reason**.

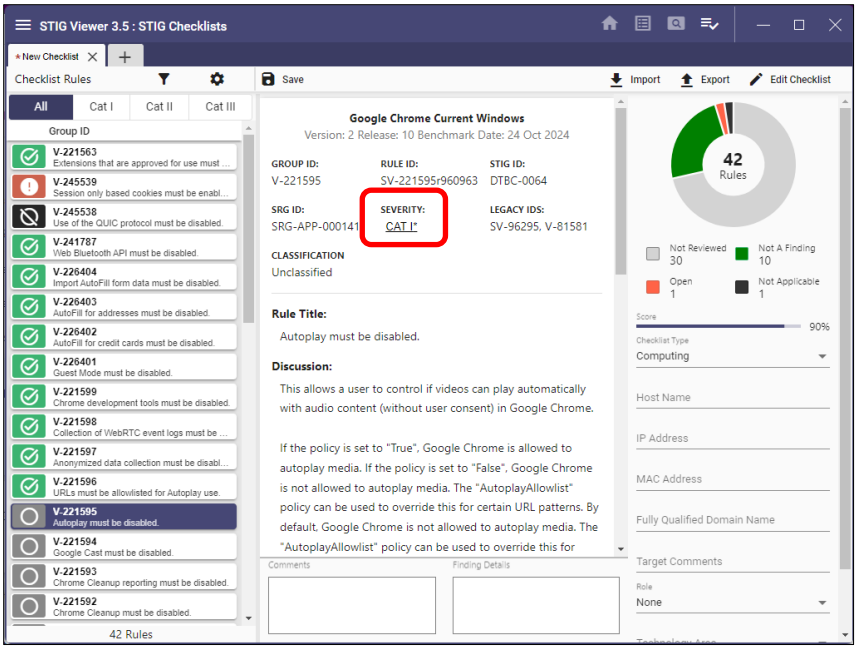
Note: Users must provide an override reason for the severity to change.





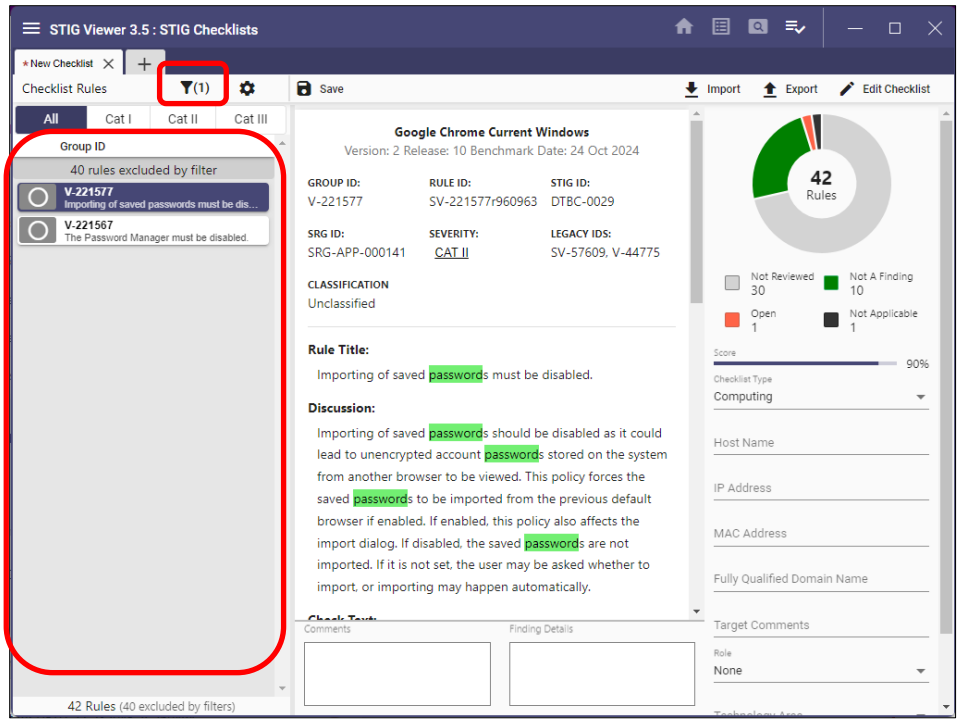
Click **Save** to save the severity change.

An asterisk will appear beside the Severity showing that it has been overridden.



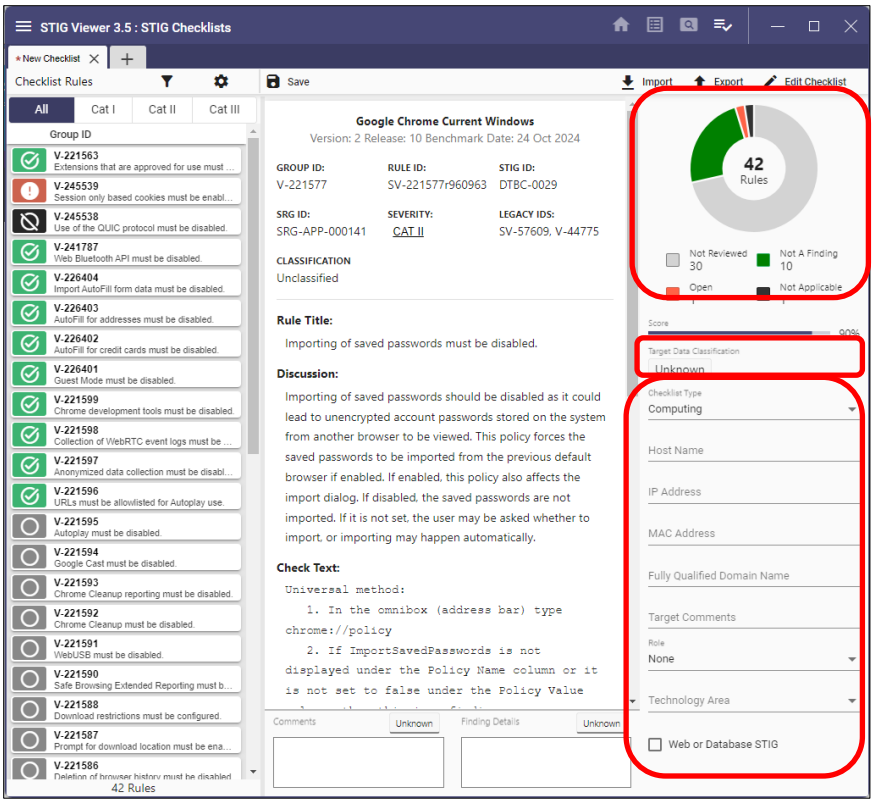
5.4.3 Filtering a Checklist

Filter the rules by clicking the **funnel** icon and applying filters. The number of filters applied will be shown beside the funnel icon. Rules matching the filter will be listed. Change from Group ID to Rule ID or STIG ID in the left column by selecting the **gear** icon.



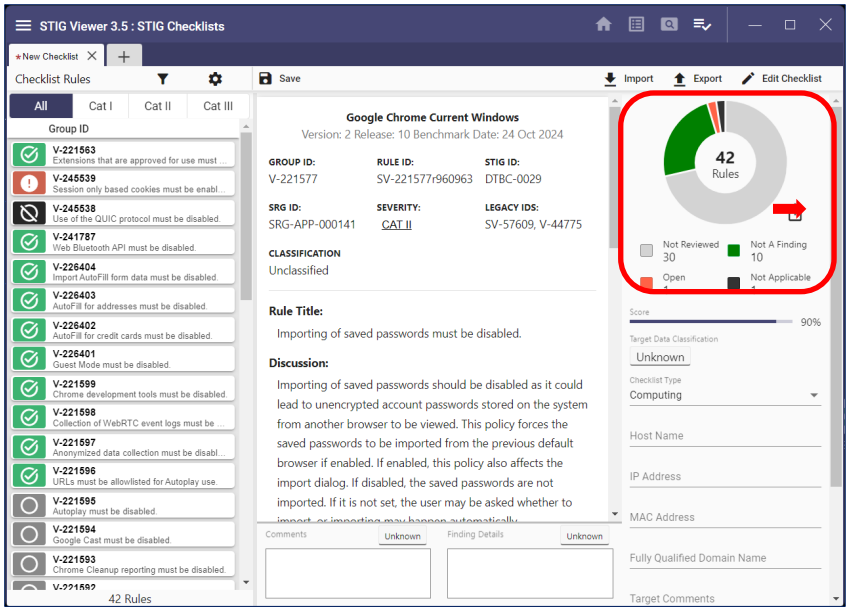
5.4.4 Populating Target Data

Target data can be populated on the far-right side of the screen. This area also displays a graphic showing the number of rules in the STIGs included in the checklist, the progress of status changes, and the Score.



If the target data has a classification already set, or if "Always Show Classification Options" is enabled in the preferences menu, the classification level of the target data can be set using the classification editor button at the top of the target data section. (In the preview above, the classification is set to "Unknown.")

Note: Hovering over the graphic displays a download symbol to obtain a copy of the graphic to be used in presentations.

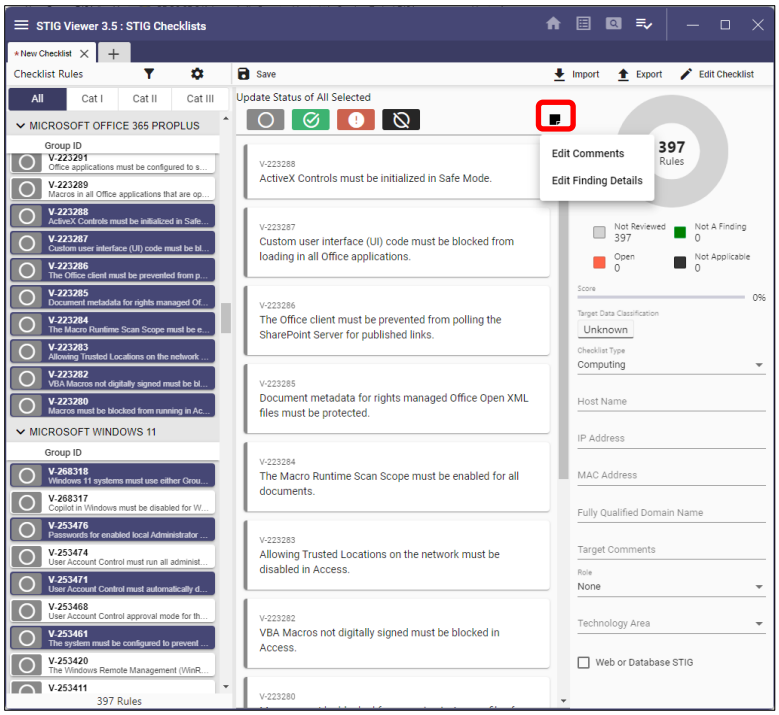


5.4.5 Adding Comments and Finding Details to a Single Rule

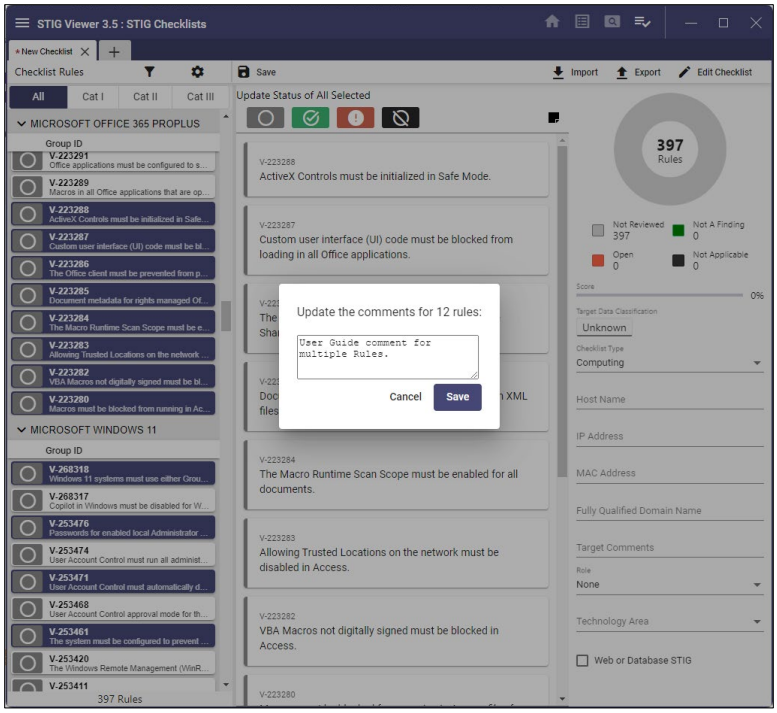
Add **Comments** and **Finding Details** to an individual rule by typing directly into the **Comments** and **Finding Details** boxes or copying and pasting from another document into the boxes.

5.4.6 Adding Comments and Finding Details to Multiple Rules

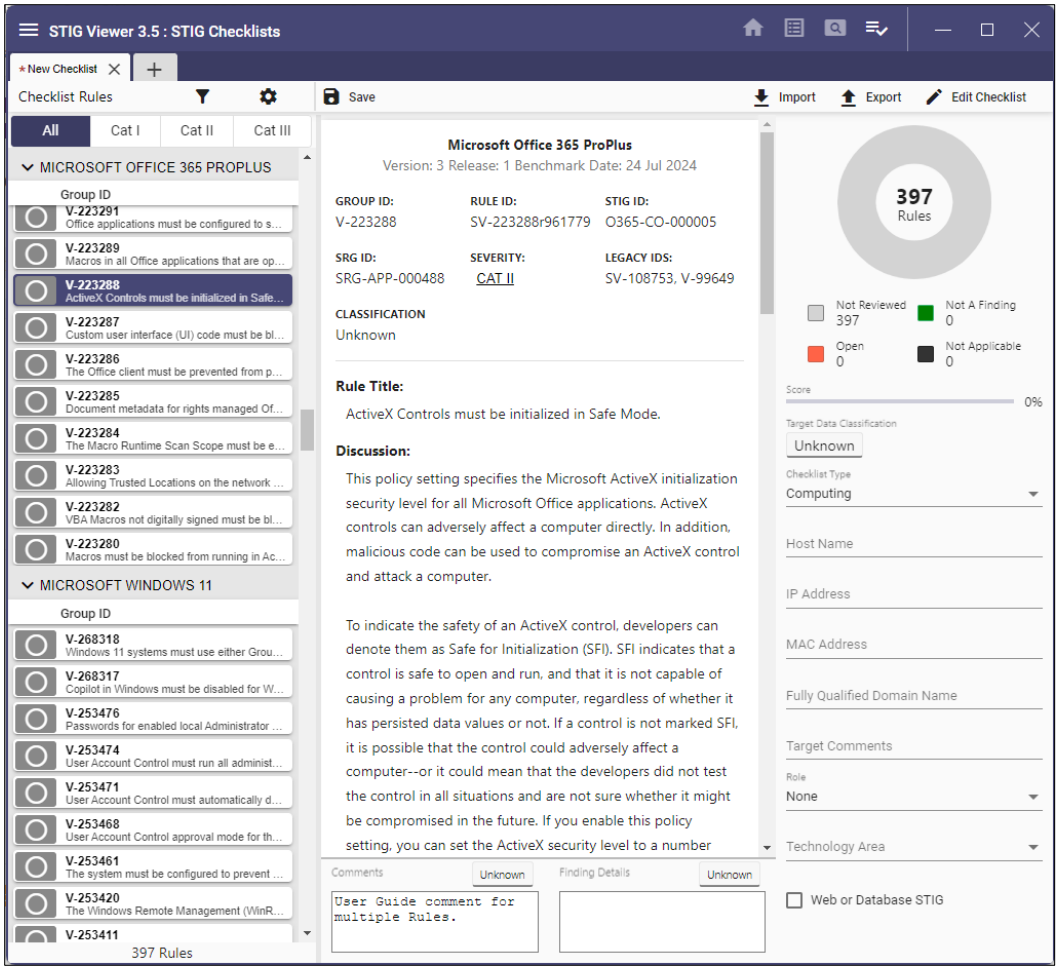
1. Multiple rules can be updated at one time. After selecting all rules for updating, click the square in the upper-right portion of the screen. From the pop-up menu, select **Edit Comments** or **Edit Finding Details**.



2. After a selection has been made, either type or copy and paste in the box.



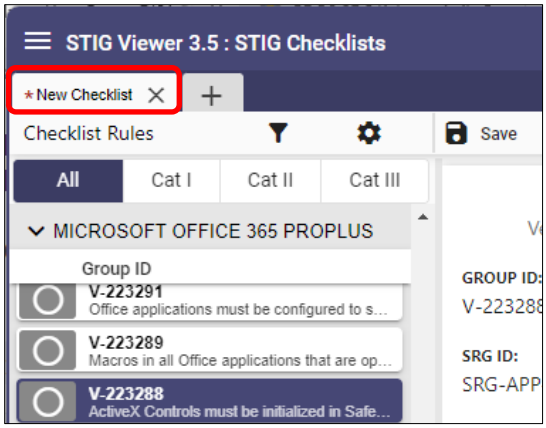
3. Click **Save** to add the text to the selected rules.



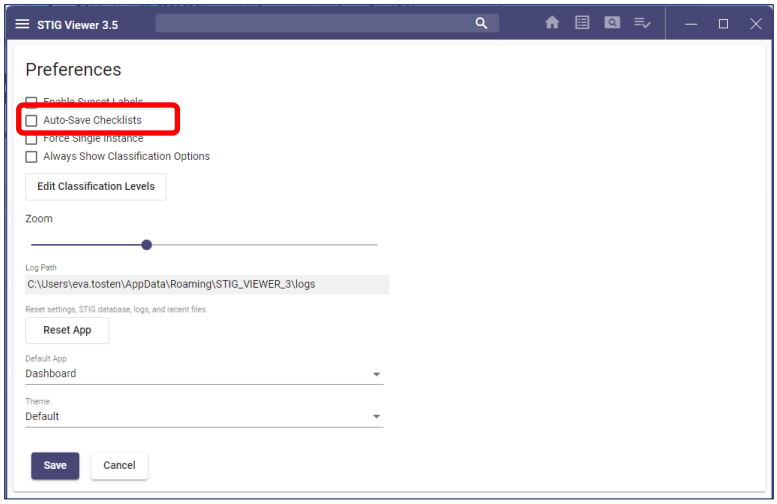
4. All Rules selected will have the same **Comment** or **Finding Details** text.

5.5 Saving a Checklist

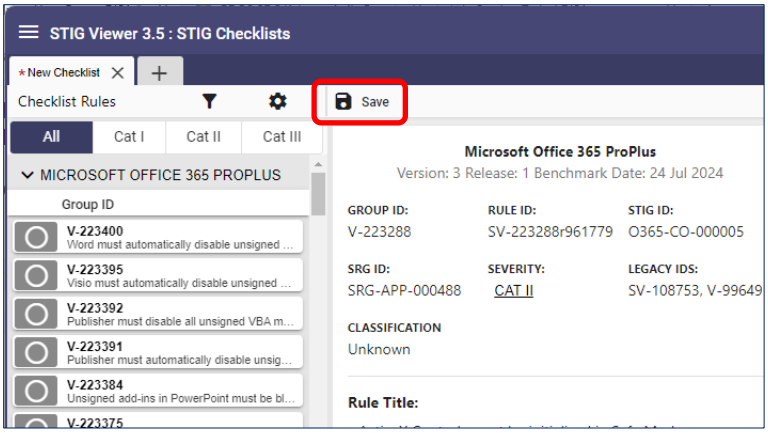
1. An unsaved checklist will have an asterisk beside the checklist name. The example below is a new checklist that has not been named (created from the STIG Explorer tab).

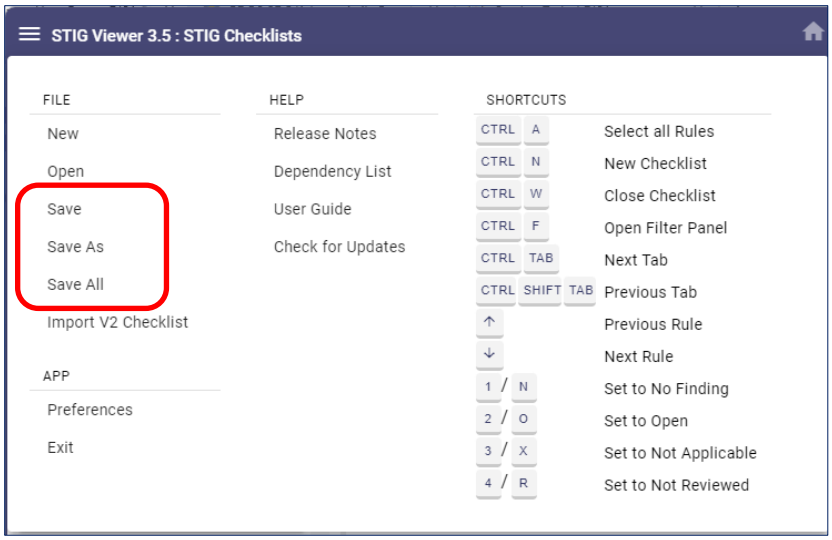


2. In the **Preferences** section, the default is **Auto-Save Checklists**. Uncheck the selection to save the checklist manually.

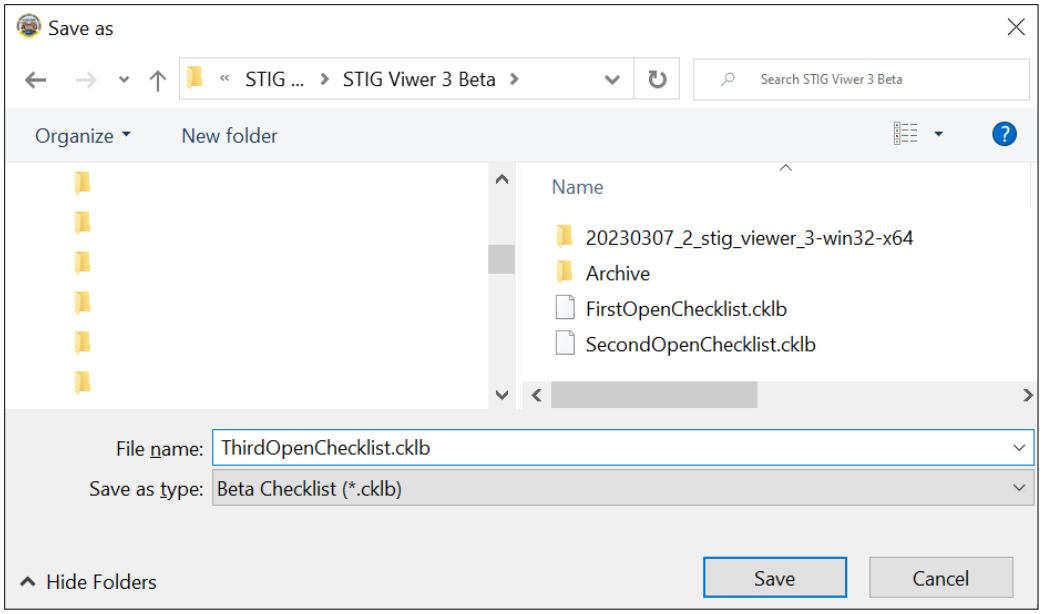


3. To save a checklist, click **Save** in the upper part of the screen or click the **hamburger** menu.

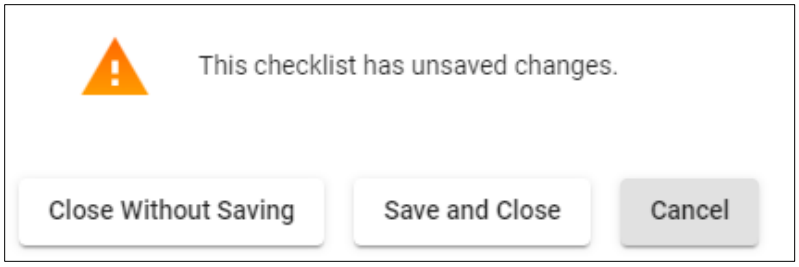




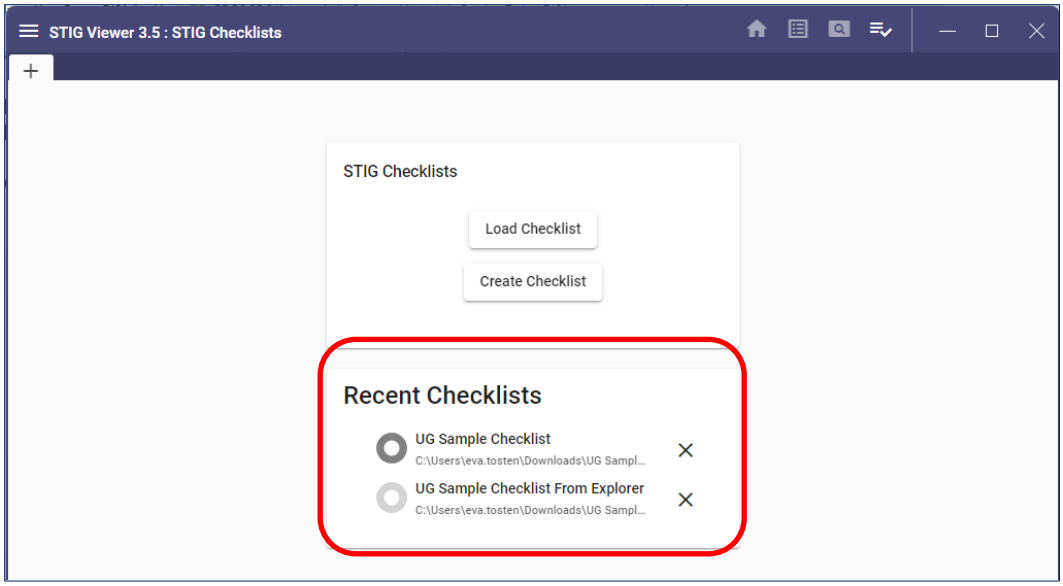
4. The hamburger menu provides the options to **Save**, **Save As**, or **Save All open checklists** (only shows if more than one checklist is open and unsaved), which will prompt the user to save each open checklist separately. Navigate to the desired location and save each open checklist. The application will open the navigation window to the last location accessed.

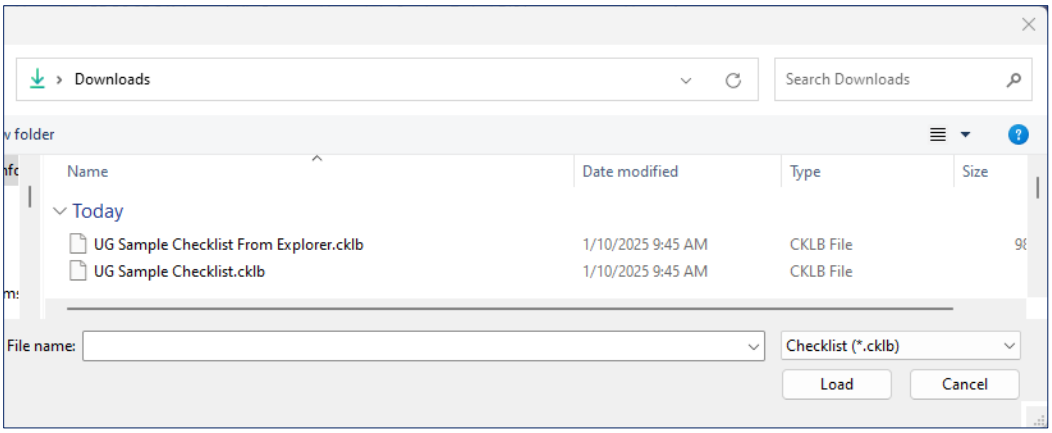


5. If the user tries to exit a checklist that has not been updated (no asterisk beside name), the application will close with no prompts. If updates have been made to the checklist (asterisk beside name), the user will be prompted to **Close without Saving**, **Save and Close**, or **Cancel. Cancel** is the default.



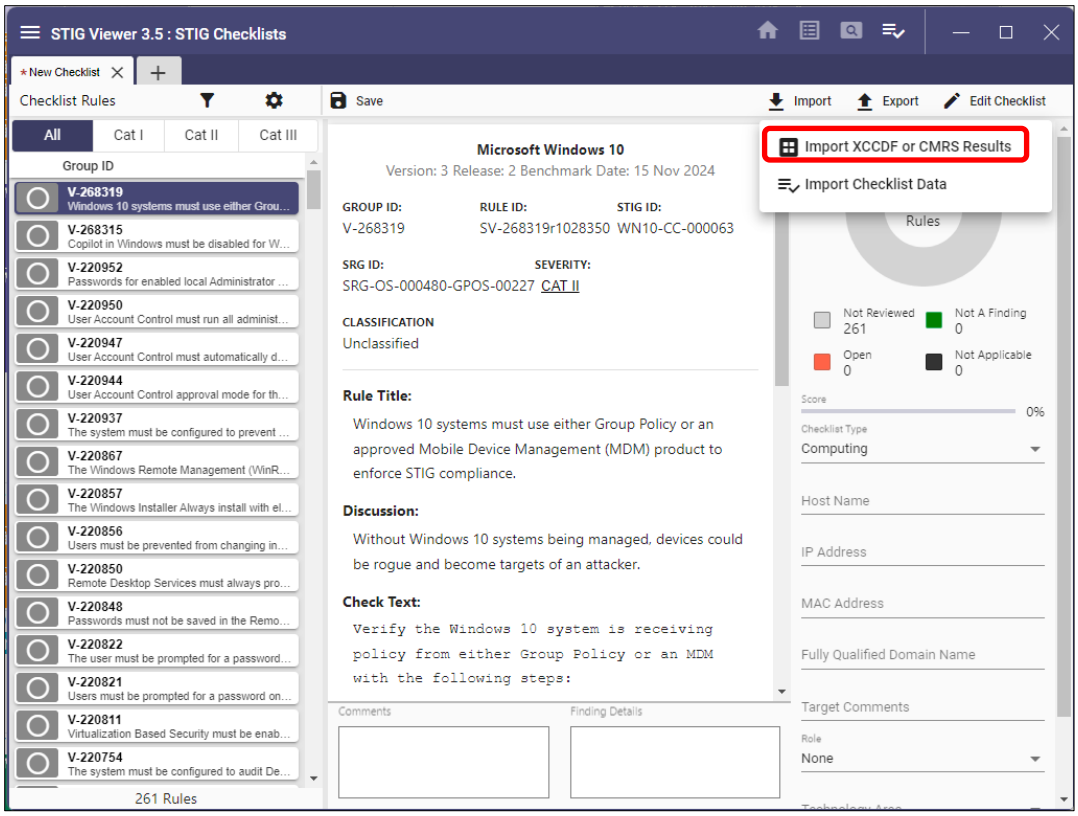
6. After a checklist has been saved, it can be reopened by either clicking the name of the checklist in the **Recent Checklists** section or by clicking **Load Checklist**, navigating to the saved location, and clicking **Load**.





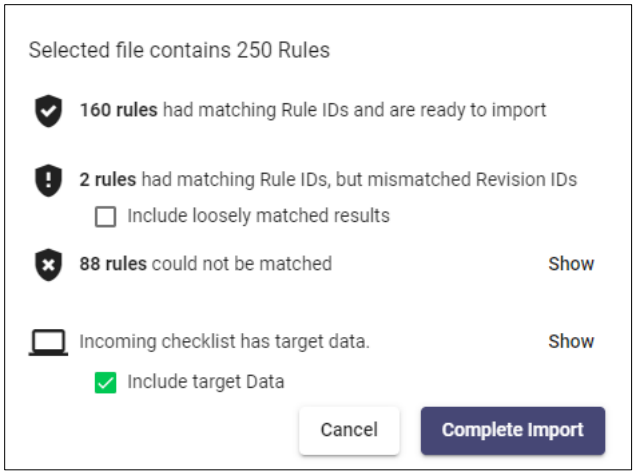
5.6 Importing XCCDF Results into a Checklist

1. To import XCCDF results into a checklist, click the **Import** icon and select **Import XCCDF or CMRS Results.**

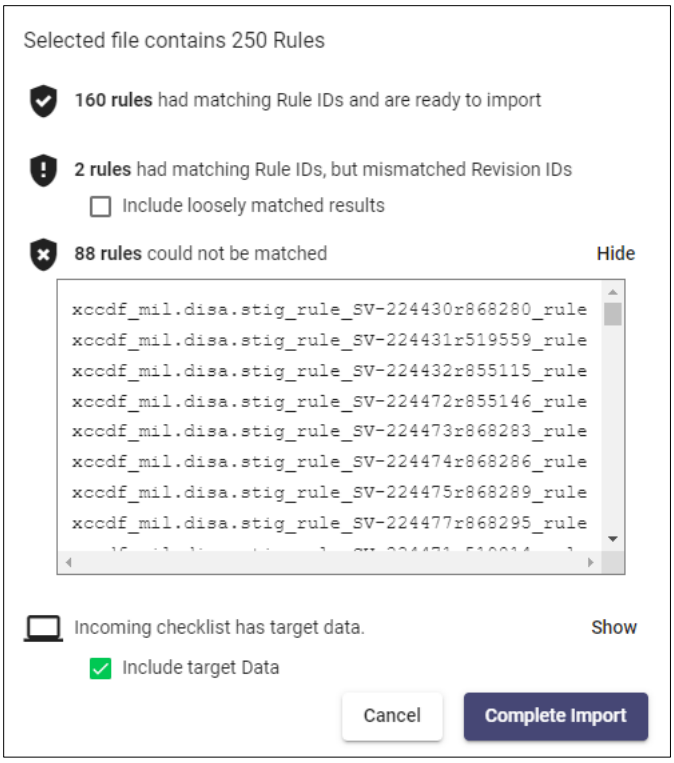


2. Navigate to the results file to import and click **Load**.
3. A pop-up window will display the following:
   - The number of results with matching Rule IDs and revision numbers that are ready to import.
   - The number of results having matching Rule IDs but that did NOT match on revision number.
   - Any results that did NOT match a Rule ID.
   - Incoming checklist has target data.
     Note: This wording only shows if the checklist being imported contains target data.

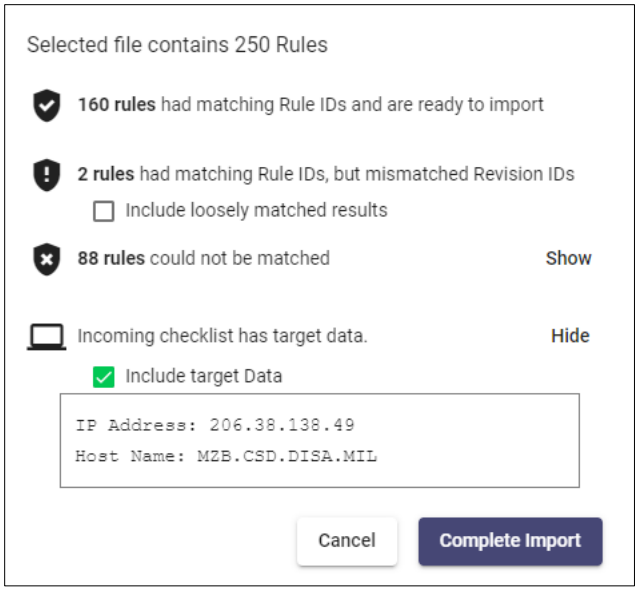
4. Complete the import with only the Rule IDs having matching revision numbers by clicking **Complete Import.** To bring in all results regardless of revision matches, click the checkbox beside **Include loosely matched results** and then click **Complete Import**.



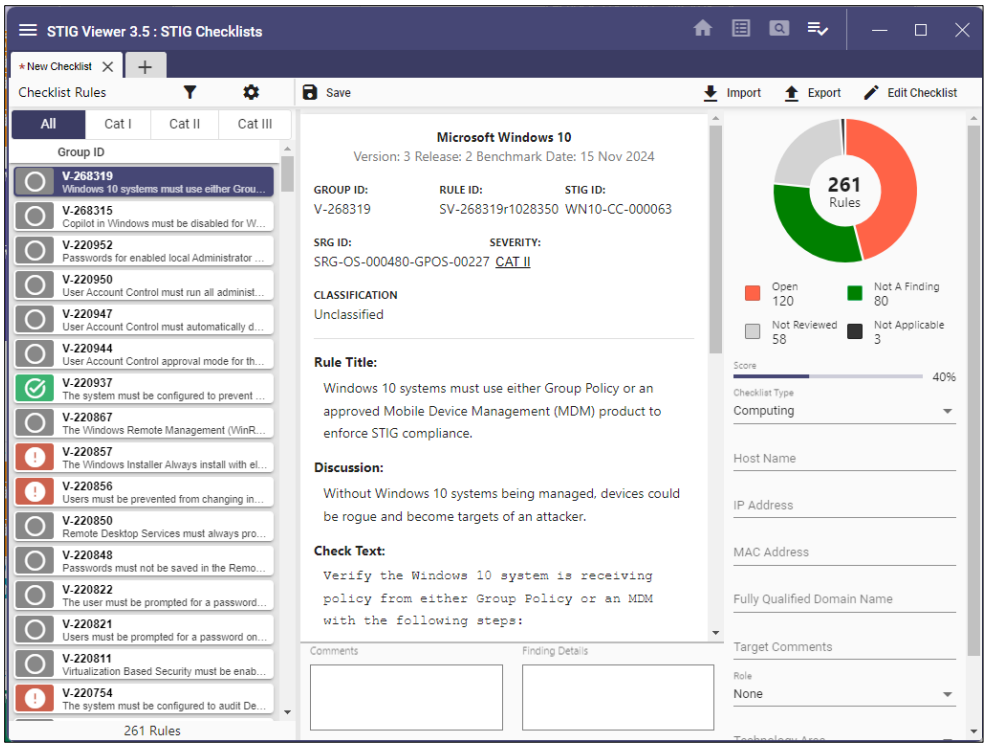
5. If any rules did not match, click **Show**, and the rule(s) that could not be matched will be displayed.



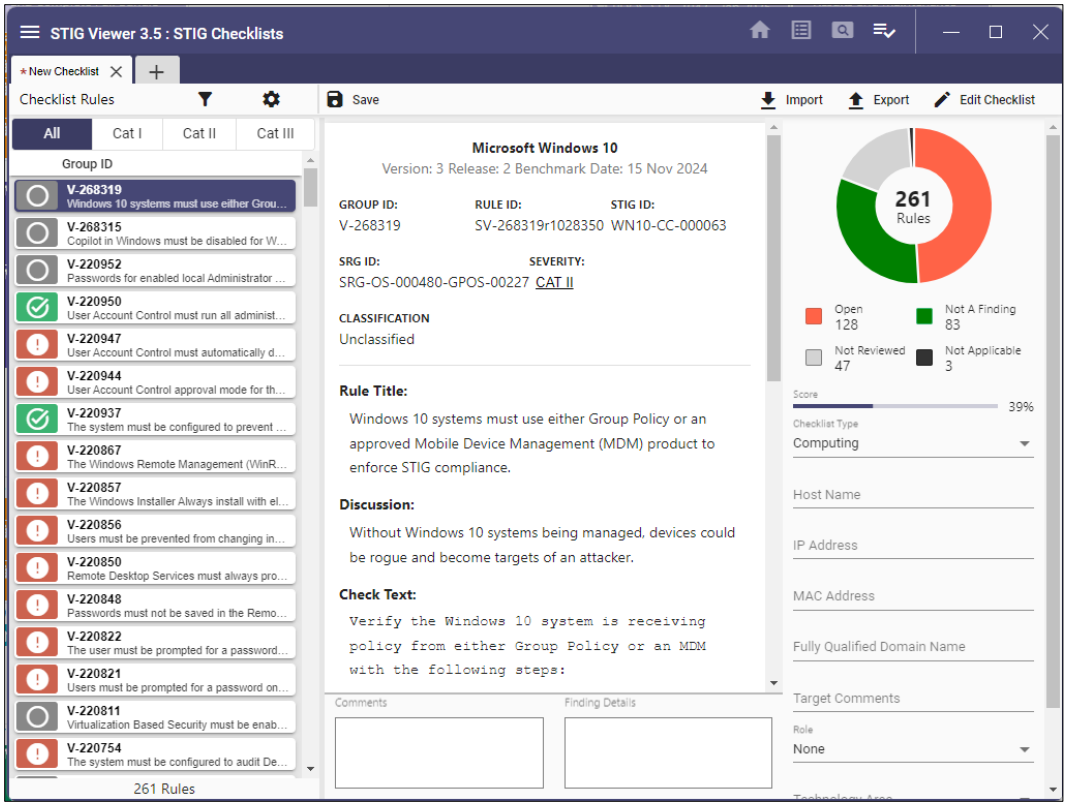
If the file being imported contains target data, the pop-up will give the user the option to include the target data or exclude it from the import. It will also allow the user to view the target data being imported.



6. The imported results will show in the checklist. The example below was completed using the **Import XCCDF or CMRS Results** without checking the box to **Include loosely matched results**.



The example below was completed using the **Import XCCDF or CMRS Results** and checking the box to **Include loosely matched results**.



5.7 Importing Checklist Data

To import STIG Viewer 3.x checklist data into another checklist, click **Import** and then select **Import Checklist Data**. This will bring in **Status**, **Comments**, **Finding Details**, and **Target Data** from the checklist being imported.

1. Navigate to the checklist file to import and click **Load**.
2. A pop-up window will display the following:
   - The number of results with matching Rule IDs and revision numbers that are ready to import.
   - The number of results having matching Rule IDs but that did NOT match on revision number.

     Note: To include these rules, the user must check the checkbox to include the loosely matched results.

     Note: This wording shows only if the checklist being imported contains Rule IDs that did not match on revision number.
   - Any results that did NOT match a Rule ID.

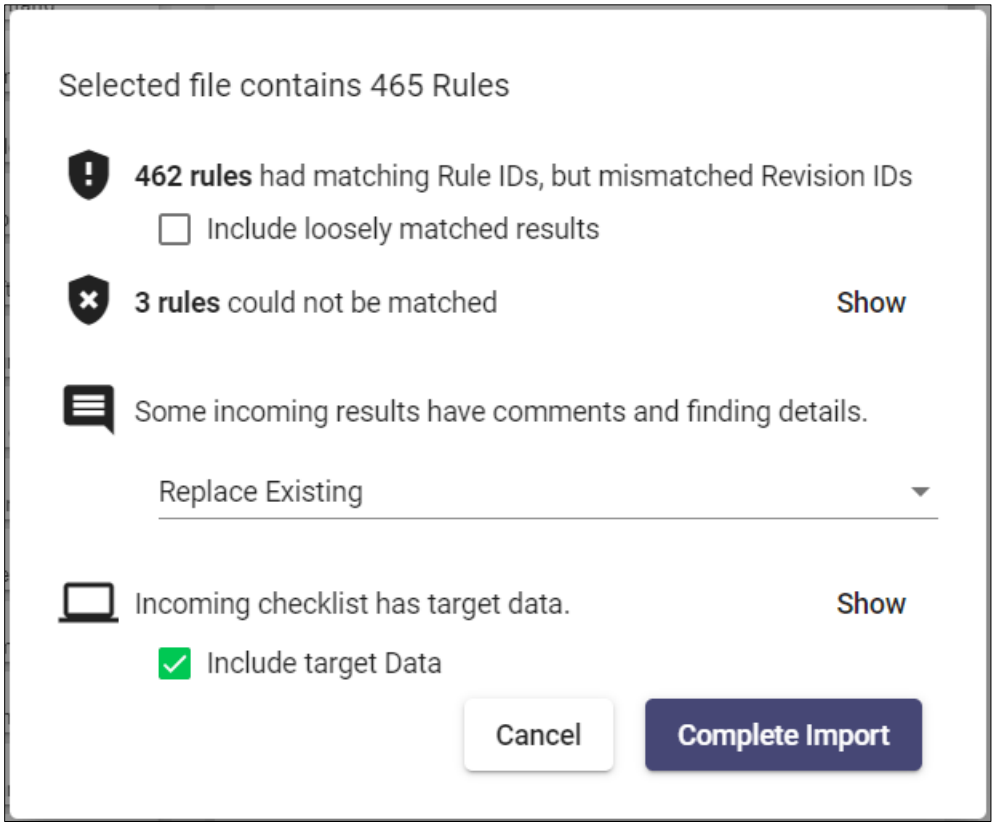
     Note: This wording shows only if the checklist being imported contains Rule IDs that did not match on Rule ID.
   - If some of the incoming Rules have Comments or Finding Details, this allow the user to select what to do with those Comments and Finding Details.

Note: This wording shows only if the checklist being imported contains Comments or Finding Details.

- Options are:
  - Replace existing.
  - Append to existing.
  - Ignore incoming.

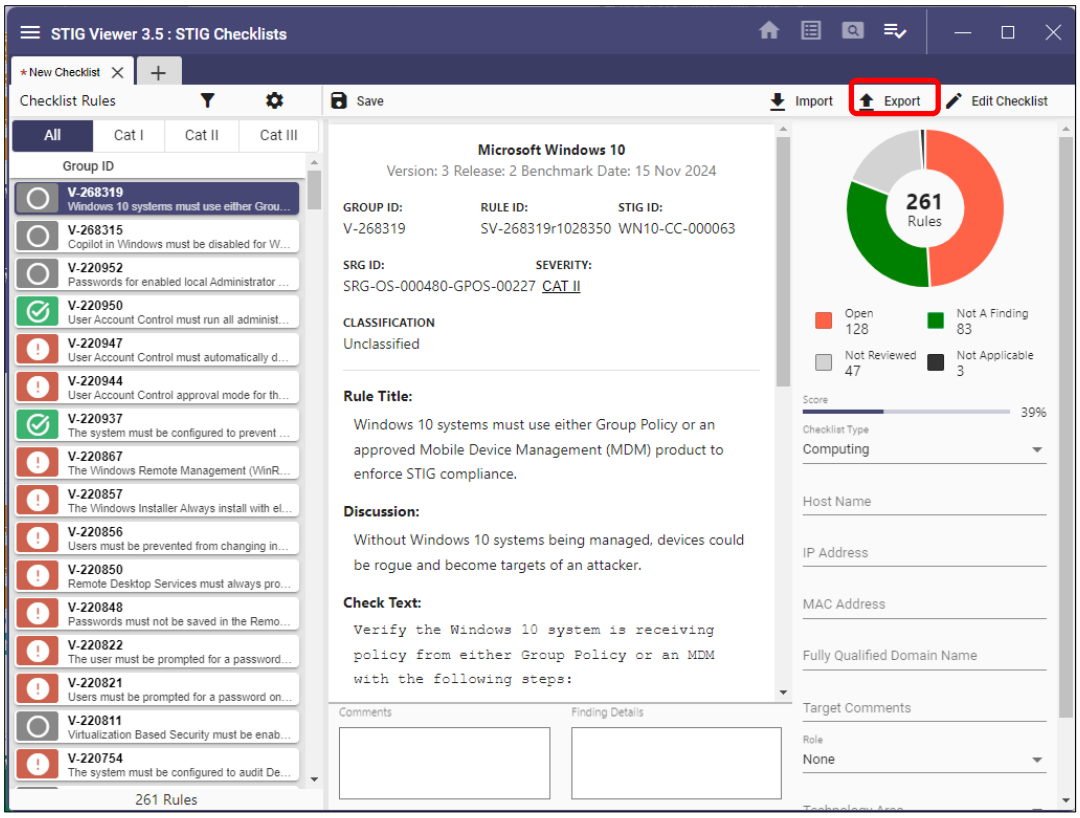
- Incoming checklist has target data.

  Note: This wording shows only if the checklist being imported contains target data.



5.8 Exporting Checklist Data

1. Click the **Export** icon to export the checklist data.

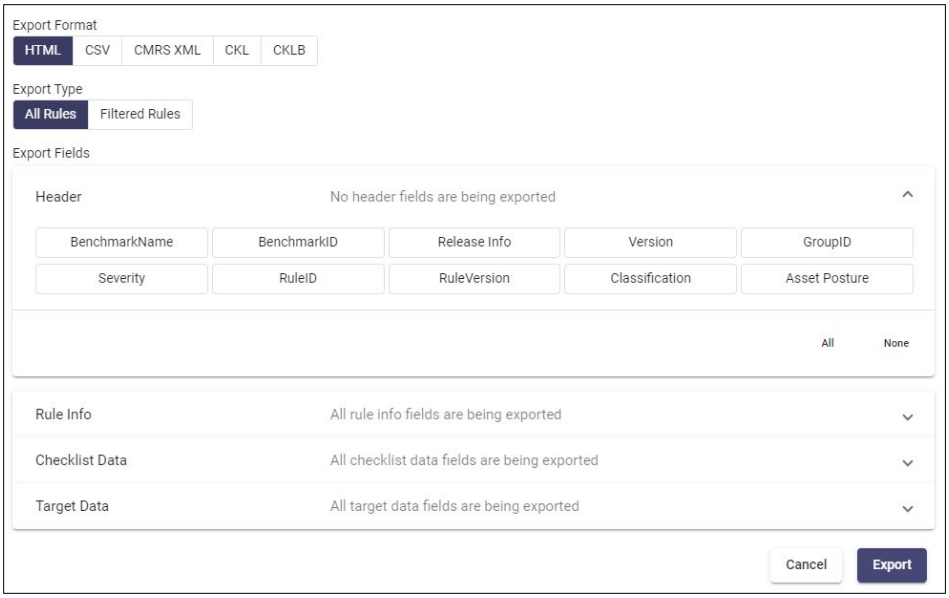


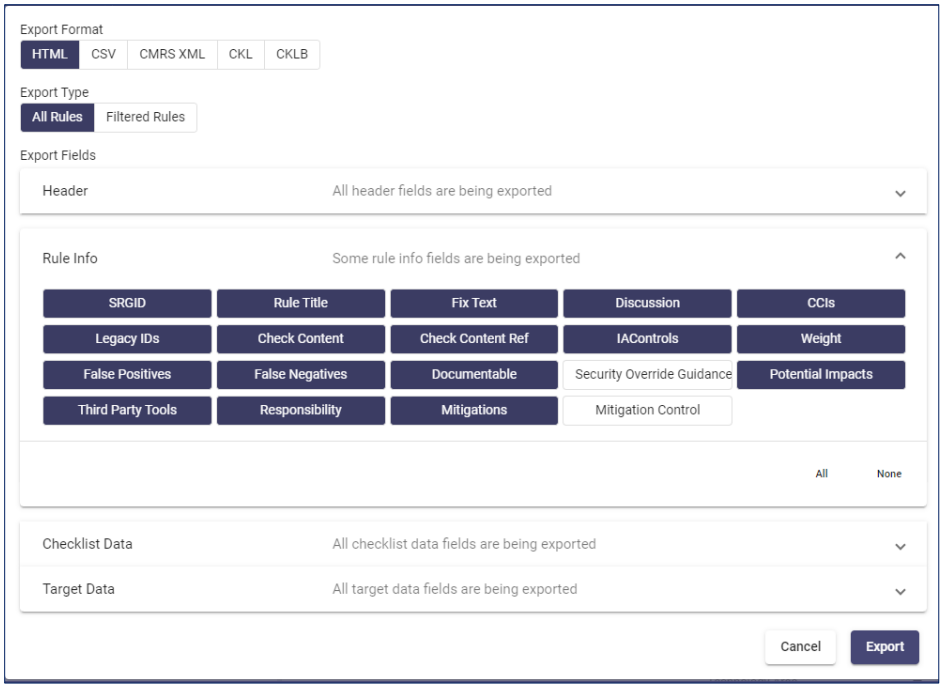
2. This displays a pop-up window, which shows a choice of export format and which fields to include.

The defaults are **HTML** format and **All fields**. Users can change the export format by clicking the desired format. Possible formats are **HTML, CSV, CMRS XML, CKL** (SV v2 format), and **CKLB**.

Note: CKLB format can now be imported into eMASS.

Users can exclude fields from each section by clicking the caret to display fields for each section and clicking **None** to exclude all the fields or clicking a field to exclude it.





Note: Any fields not highlighted will be excluded from the export.

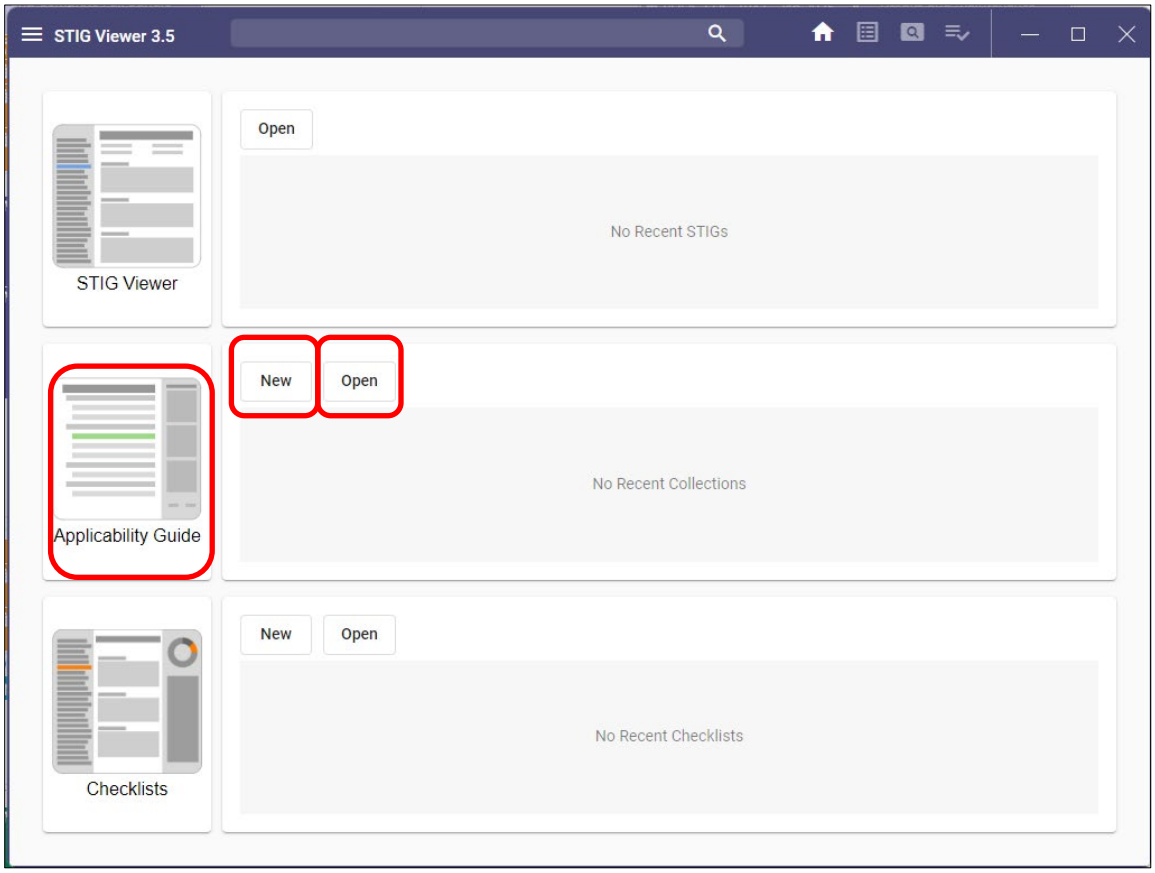
5.9 Resizing the Checklist Pane

1. To resize the checklist pane vertically, click the bar between the rule list and the rule details and drag left or right.
2. To resize the checklist pane horizontally, click the bar between the rule details and the **Comments** and **Finding Details** and drag up or down.

6. SRG/STIG APPLICABILITY GUIDE

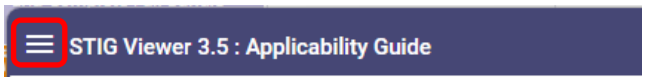
6.1 Accessing Applicability Guide from STIG Viewer 3 Dashboard

1. To access existing Applicability Guides, select the **Open** icon and navigate to the existing location.
2. To create a new collection, select the **New** icon or click the **Applicability Guide** icon.



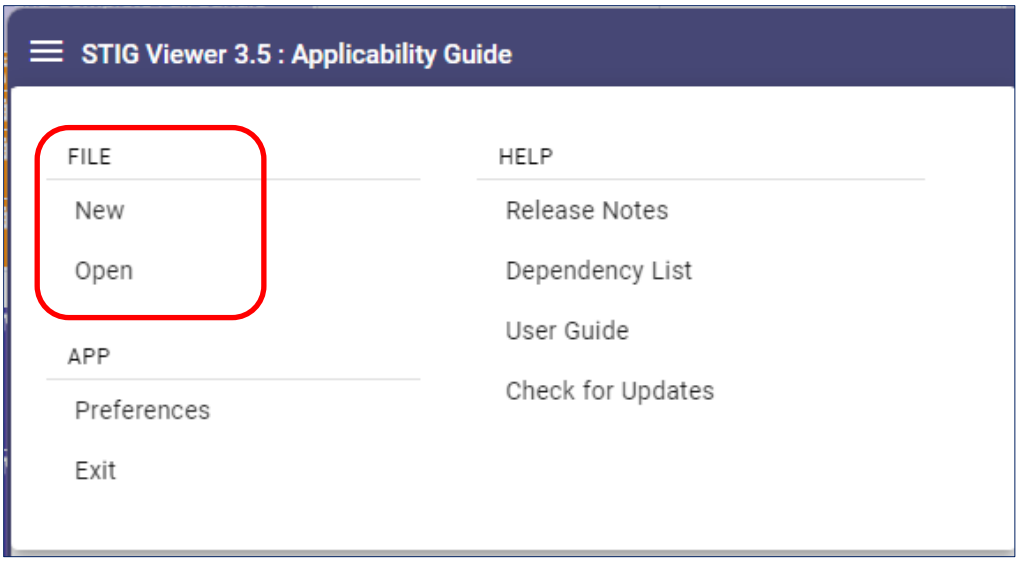
6.2 Menu

The hamburger menu is in the upper-left corner. This menu is divided into three sections: **FILE, APP,** and **HELP**. It also contains the **Exit** option.



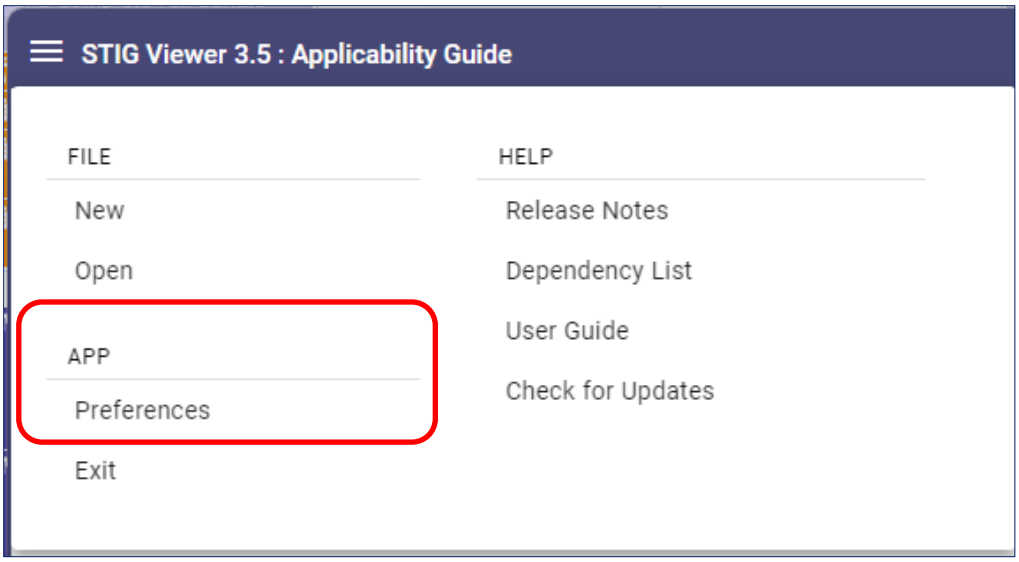
6.2.1 File Menu

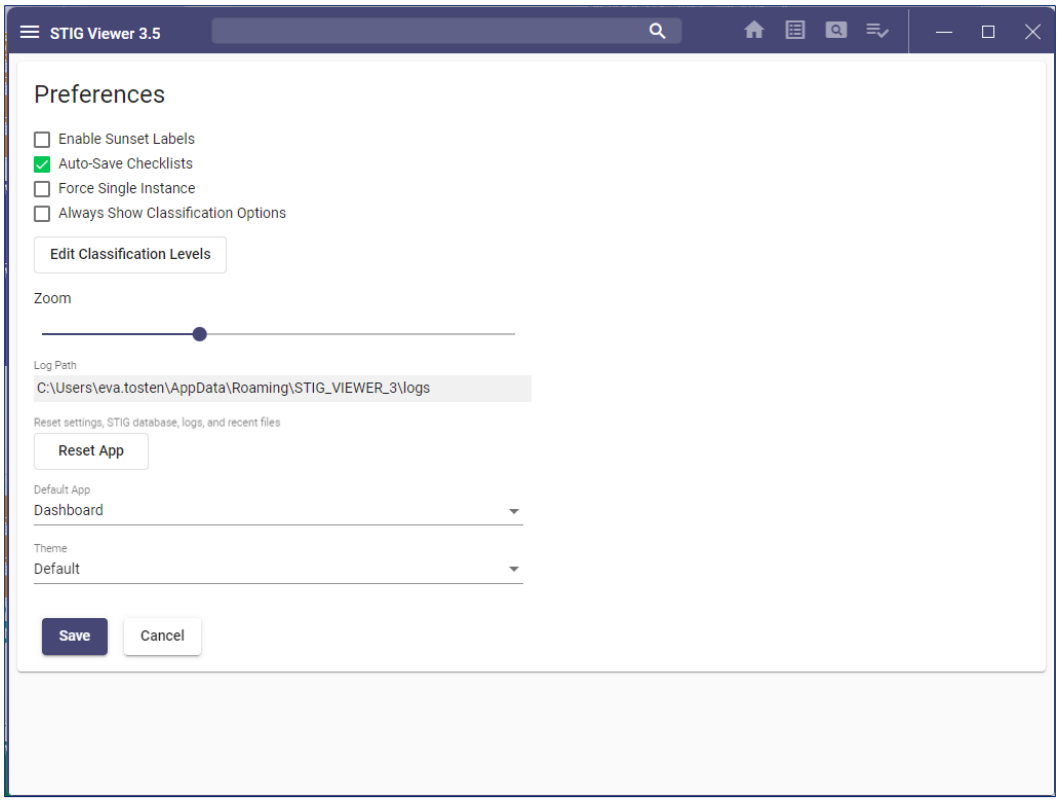
The **FILE** section allows the user to create a new asset collection or open an existing one.



6.2.2 App Menu

This section contains the Preferences menu, which allows the user to set preferences in the application such as enable sunset labels, change the font size, access application logs, change the theme, set the **Default App** for which application to open when accessing STIG Viewer, and reset the application back to the default settings.

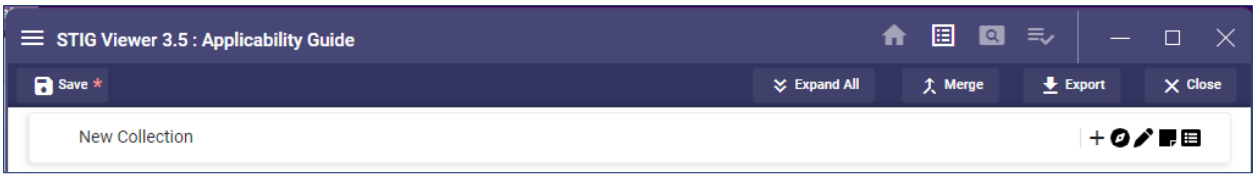




6.3 Navigation Bar Menu

6.3.1 Overview

The navigation bar (Navbar) will display a list of options to interact with the application and the created collection. When viewing a collection, buttons will appear such as Save, Merge, etc.



6.3.2 Merge Button

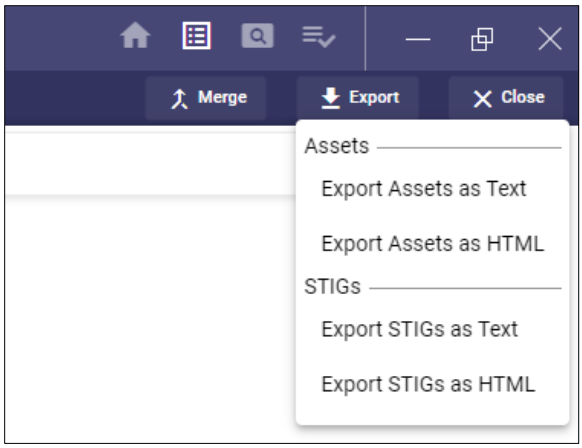
Click this button to open a file dialog and select a collection file to merge into the open collection. This is explained below in more detail.

6.3.3 Save Button

Click this button to open a file dialog, name the collection file, and save it to disk. This is explained below in more detail.

6.3.4 Export Button

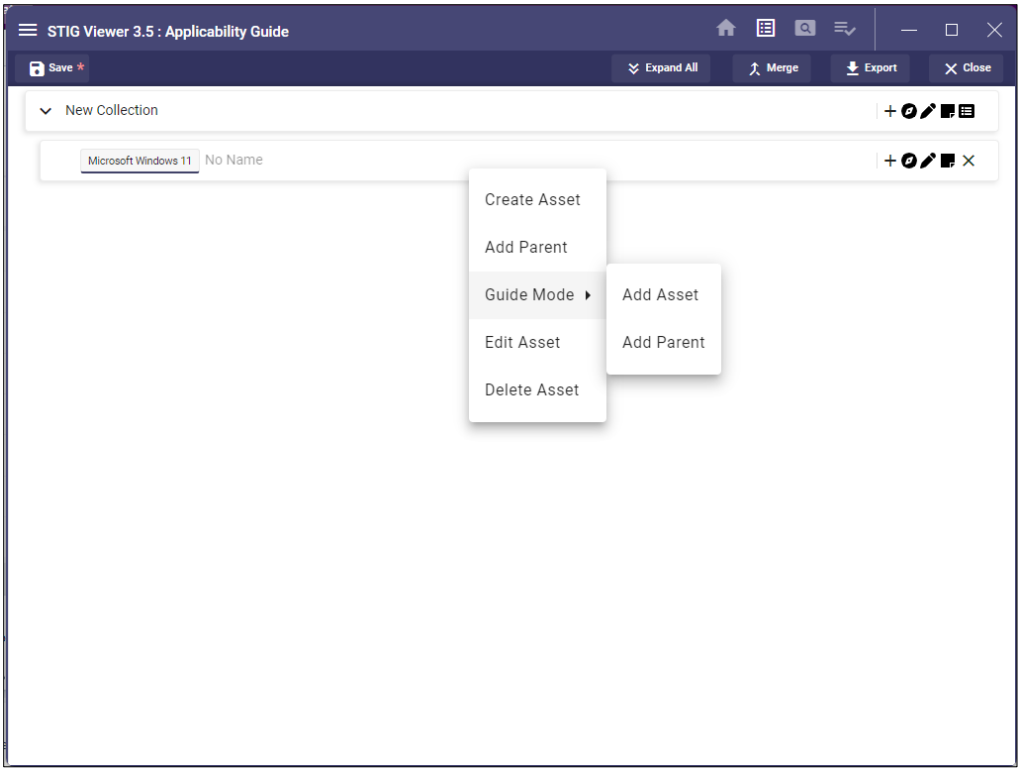
Click this button to expand the export button into four options. These are explained below in more detail.



6.3.5 Right-Click Menu

6.3.5.1 Menu

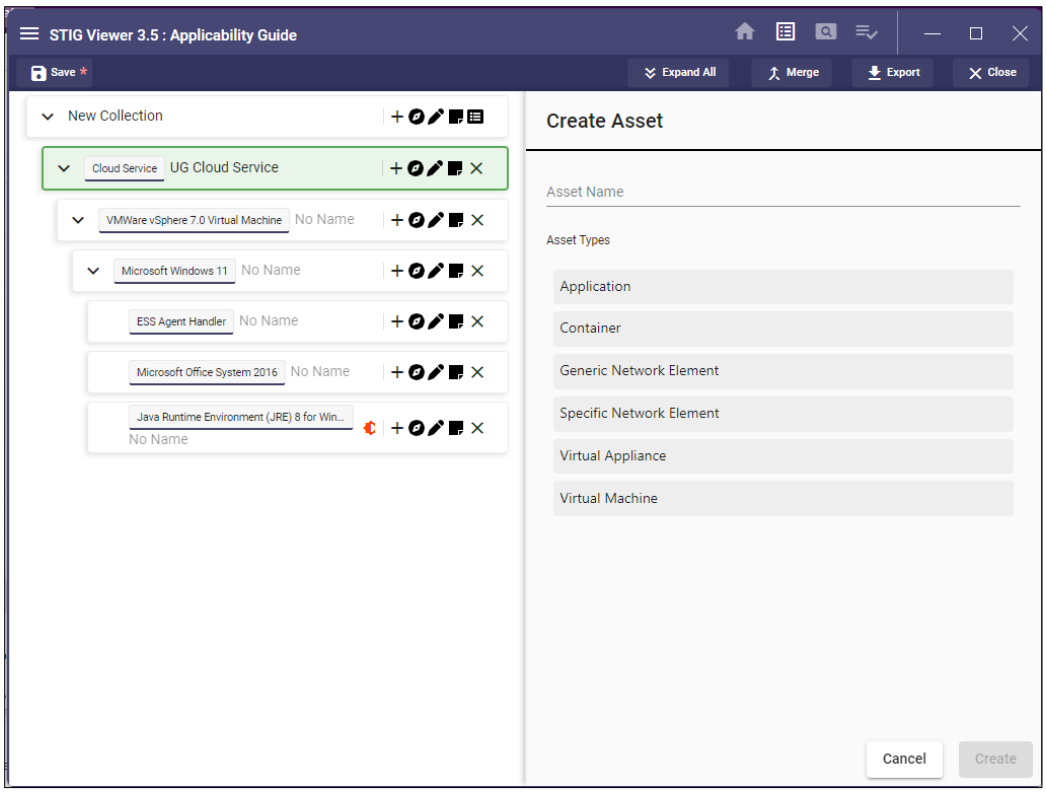
Right clicking an asset will provide a menu. This menu has shortcuts to add an asset, edit the asset, remove the asset, and enter Guide Mode. The right-click menu also includes two features that are not available elsewhere: **Add Parent** and **Add Parent** using **Guide Mode**. Note that these two features are only available if the selected asset and its current parent have matching assets.



6.4 Asset Tree

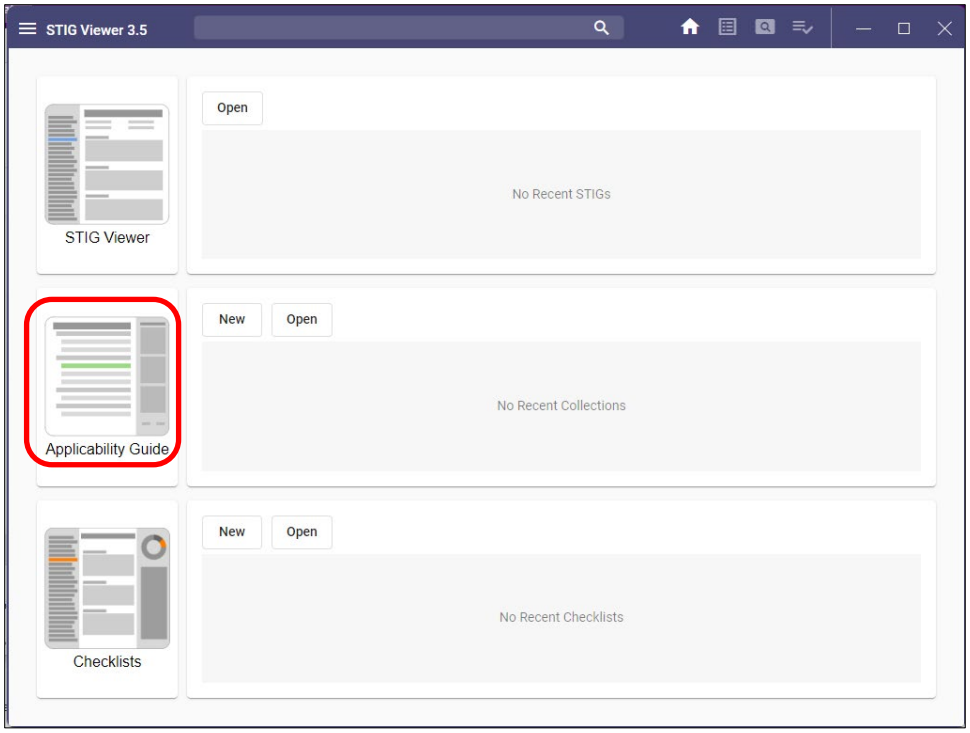
6.4.1 Overview

The main view under the File menu is the Asset Tree. This allows the user to view their current collection and add, edit, or remove assets. Based on the selections, a pane to the right can appear to display or collect additional information about the selection. The Asset the user is working with will be highlighted in green.

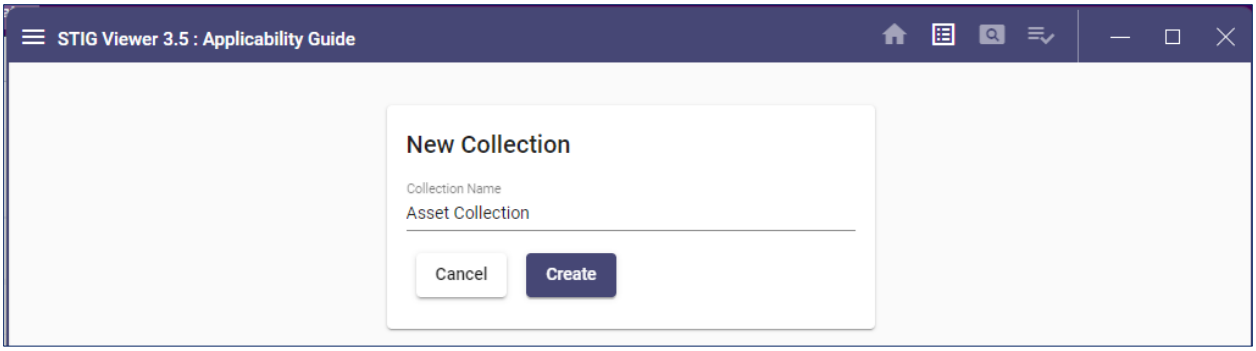


6.4.2 Creating a Collection

1. To create an asset collection and begin adding assets, click the **Applicability Guide** icon on the home page or click the icon in the navigation bar at the top.



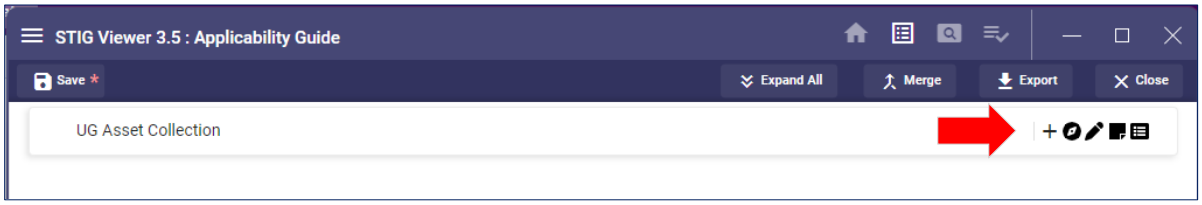
2. Enter a **name** for the collection, and then click **Create**.

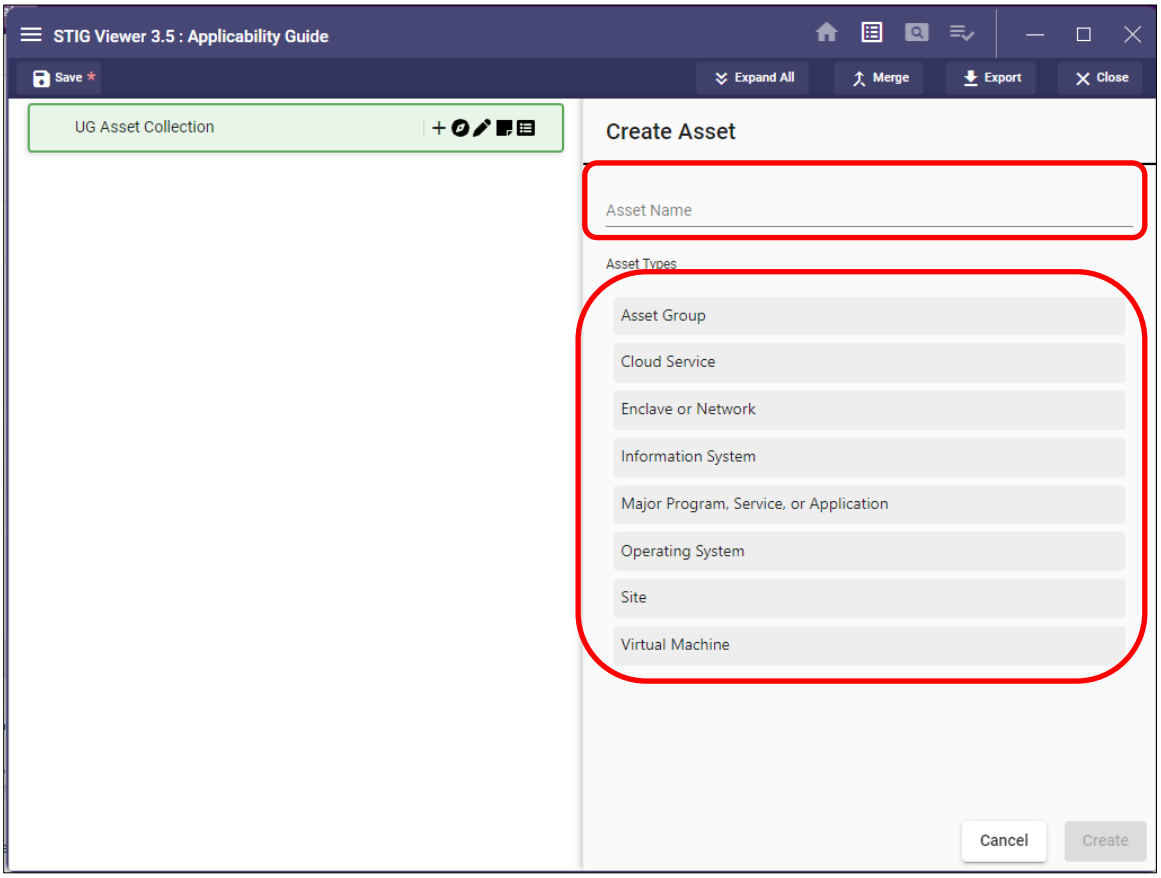


Note: To go straight to a collection without naming it, click **New** in the **Applicability Guide** section of the home page.

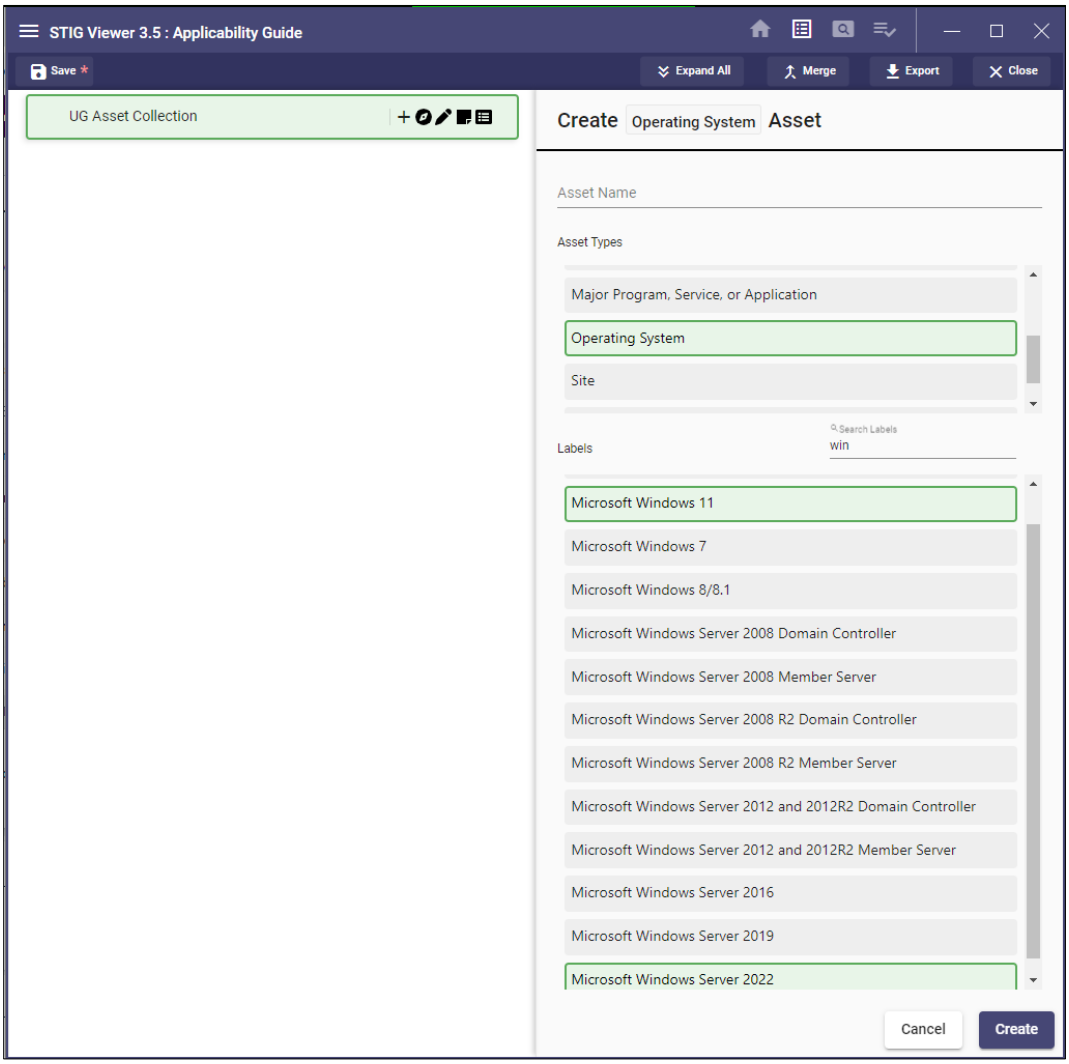
6.4.3 Adding Assets (Standard Mode)

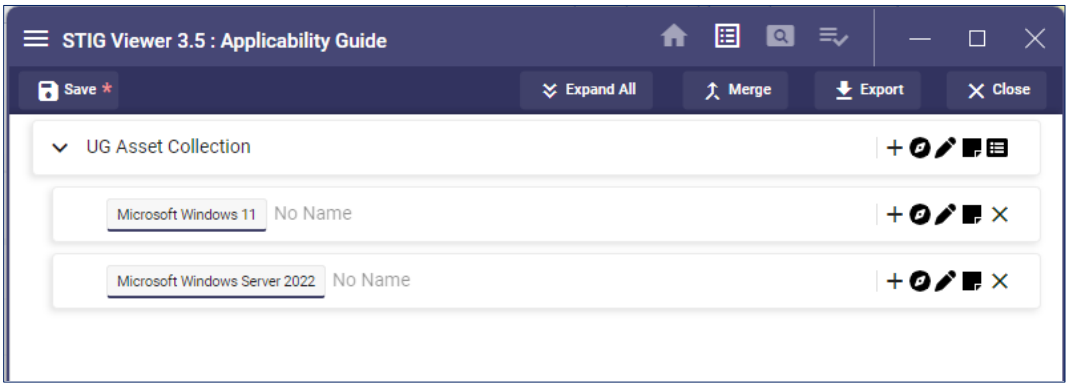
1. Click the "**+**" button to add the first Asset.
2. A selection pane will appear to the right, and the selected asset will be highlighted in green. Enter the **Asset Name** and select the **Asset Type** that applies to this asset.





3. After the **Asset Type** is selected, applicable labels[1] for the asset can be selected. Select **zero** or more labels that apply to the asset, and then click **Create** to create entries in the asset tree representing that item. Use the search input to find desired labels quickly.



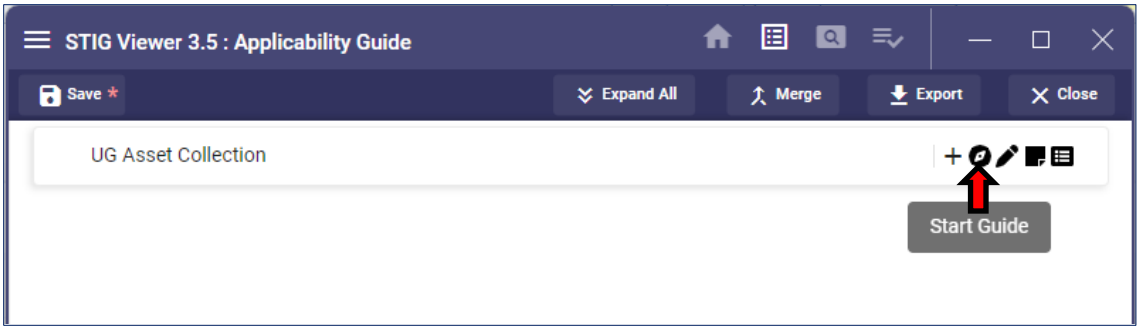


Note: The user can replace **No Name** by using **Edit Asset** described later in this document.

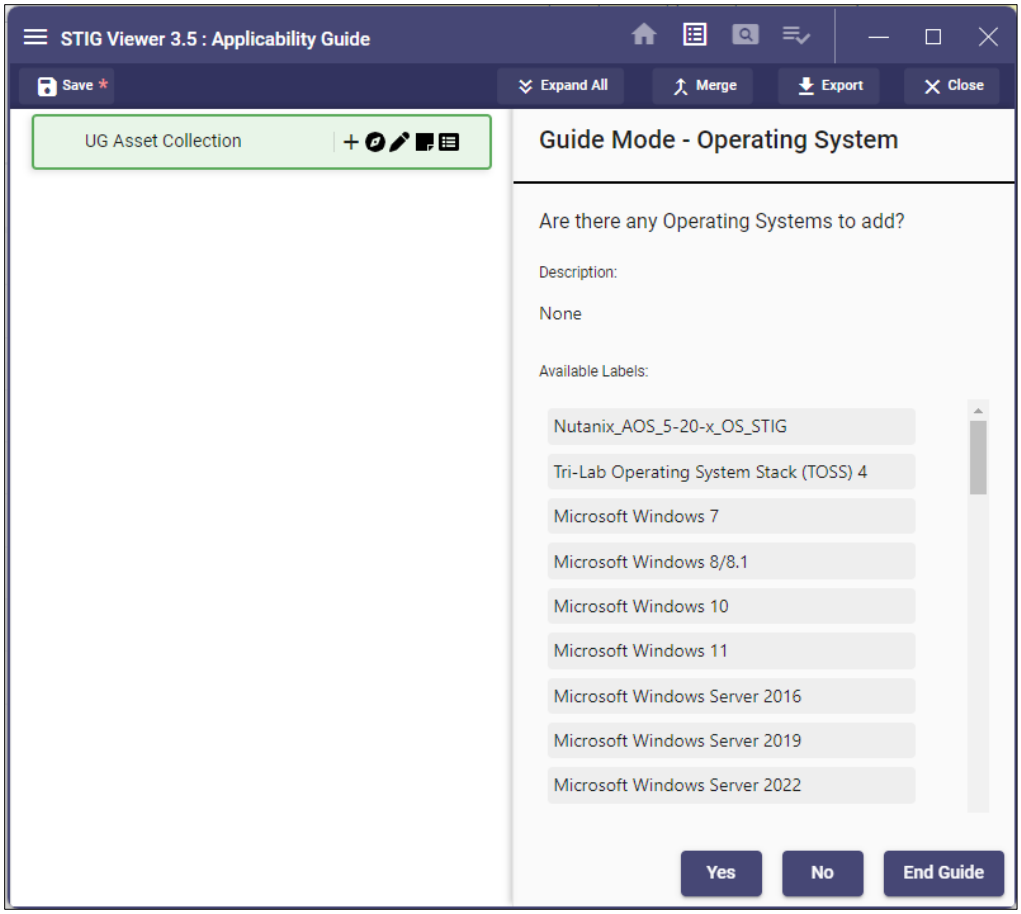
[1] Asset Label: A descriptive tag that applies to an asset type.

6.4.4 Adding Assets (Guide Mode)

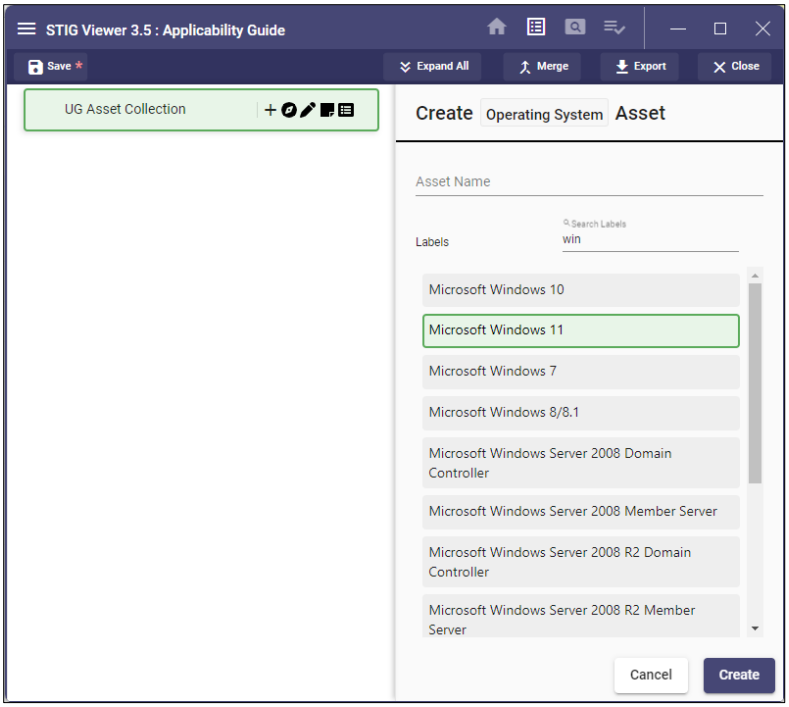
1. Click the **compass icon** (circle with a diamond) next to the "**+**" button to begin Guide Mode.



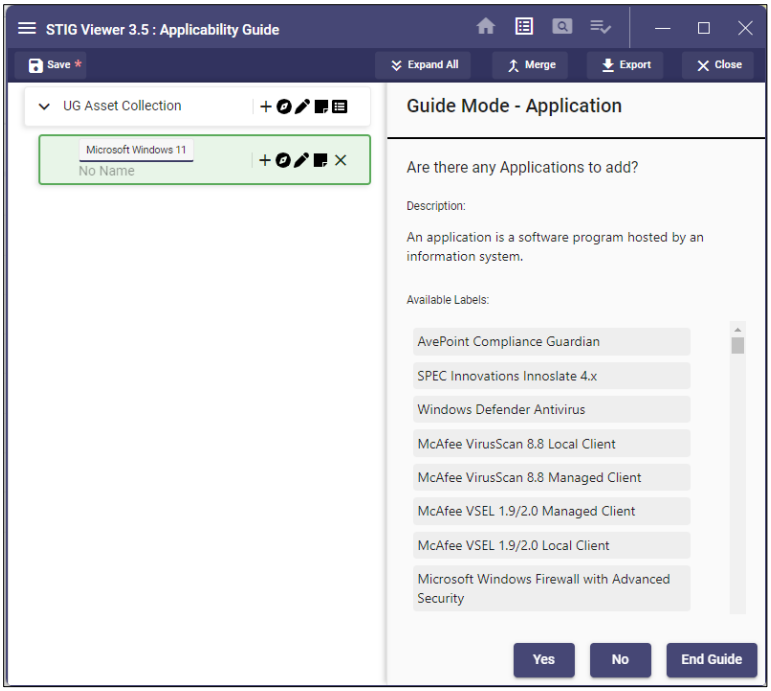
2. After clicking **Guide Mode**, a pane will appear to the right prompting the user to add an asset by asking a series of questions. Answer **Yes** or **No** to each appropriate question and select **End Guide** when finished.



3. Select **No** to move to the next asset in the list. Select **Yes** to move to the label pane where name and the asset type label can be selected (if available).



4. After adding and creating an asset, the wizard will descend into its children. The next prompt will be the first child of the asset just added. After a decision is made to add each child, the wizard will return to the top level, and other assets can be added. This process continues until every asset type available has been addressed.



Notes:

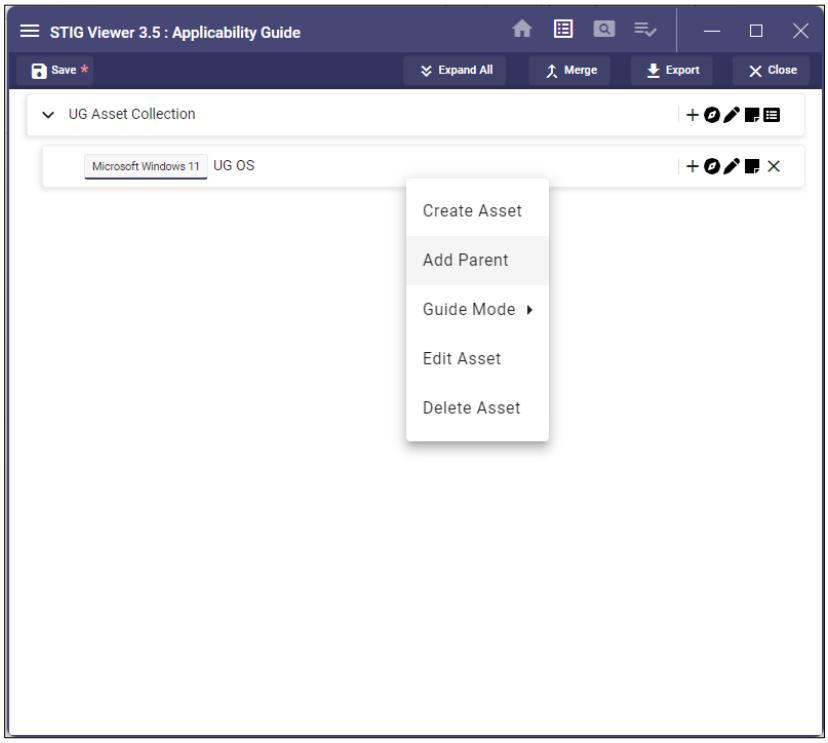
- Select multiple labels to create multiple tree items with the different labels selected.
- To leave Guide Mode, click **End Guide**.

6.4.5 Adding Parent Assets

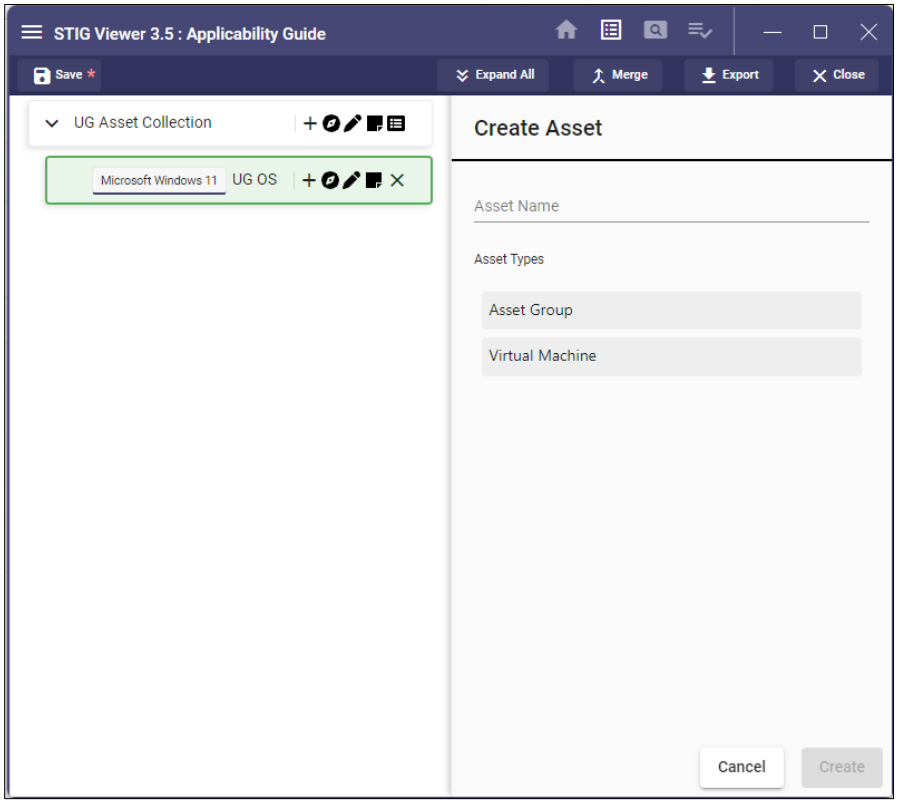
After an asset has been created, a new parent can be added by using the **Add Parent** feature.

Note: The **Add Parent** feature will only be available if an asset type is available that allows relationships between the selected asset and its current parent.

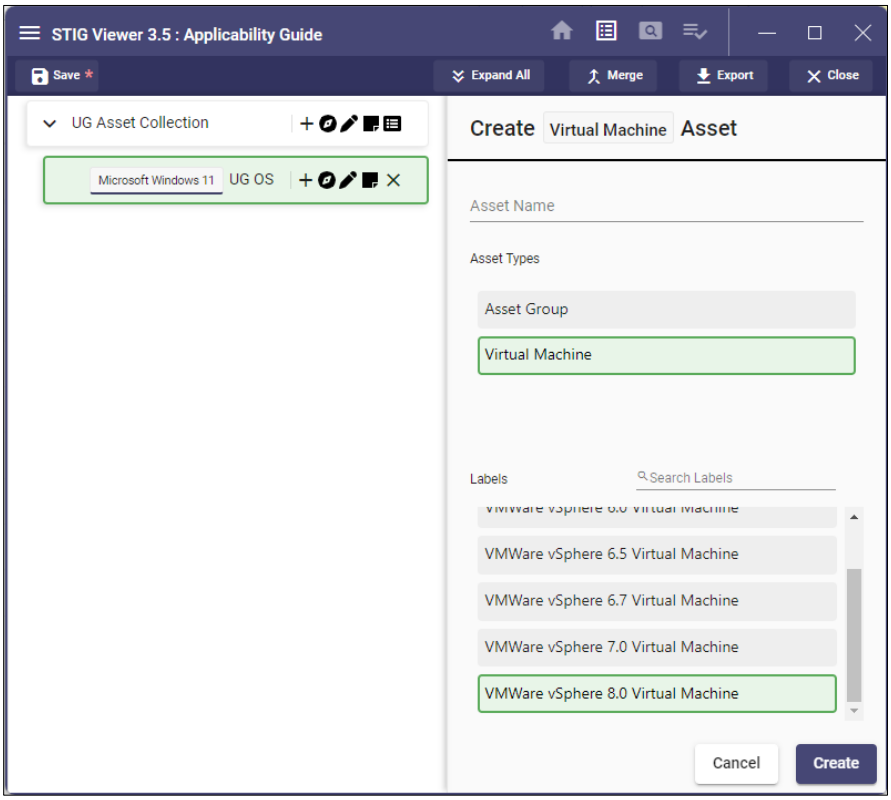
1. Right-click the asset to which the parent will be added and select **Add Parent**.



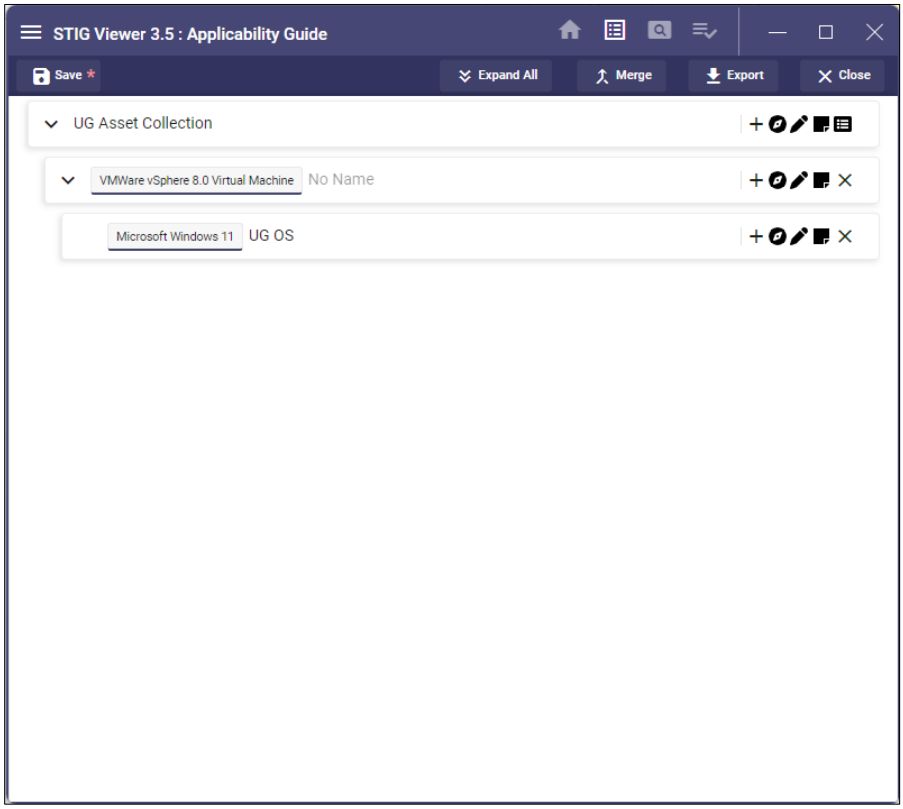
2. Select the asset to add and click **Create**.



Note: Listed on the right are assets available based on the asset selected and its current parent.



3. The new parent will be added to the asset.

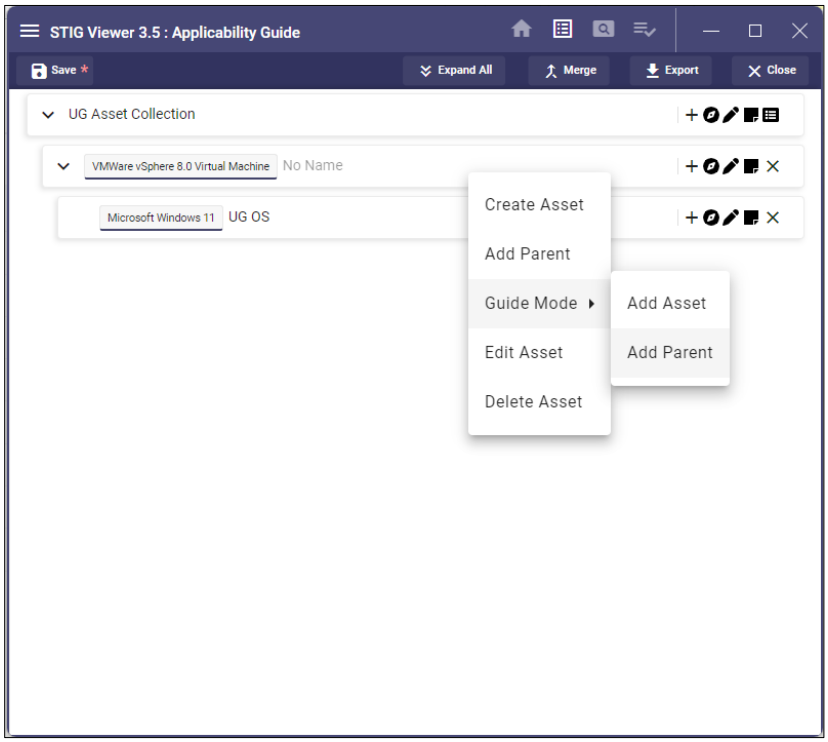


6.4.6 Adding Parent Assets (Guide Mode)

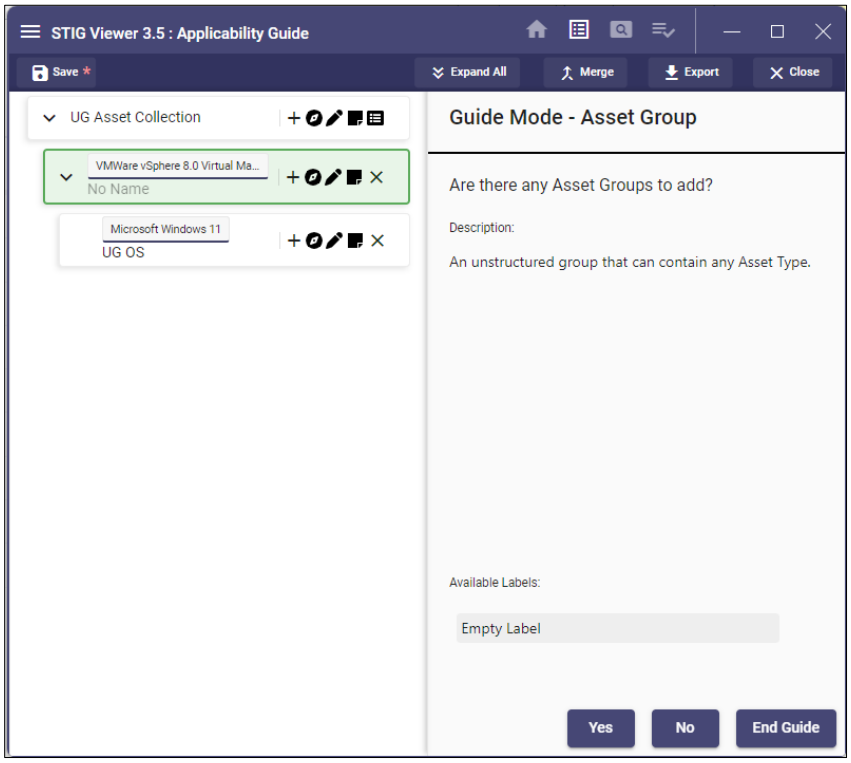
If an asset has been created but reverse order is desired, a parent can be added using the Guide Mode by clicking the **Add Parent** option when selecting Guide Mode.

Note: The **Add Parent** feature will only be available if an asset type is available that allows relationships between the selected asset and its current parent.

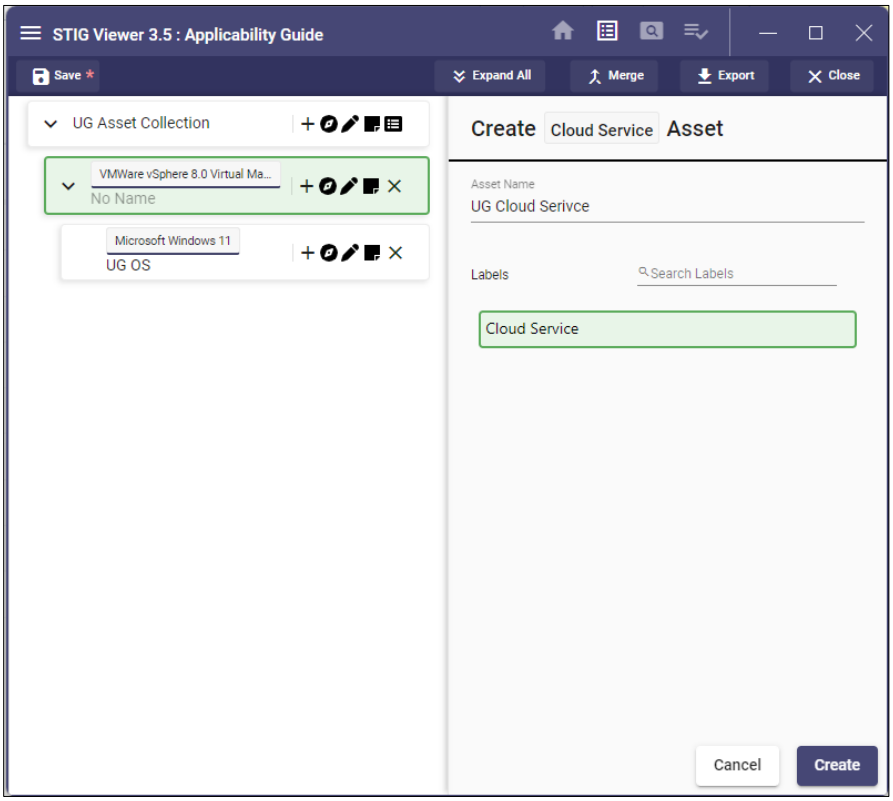
1. Right-click the asset to which the parent will be added and select Guide Mode >> Add Parent.



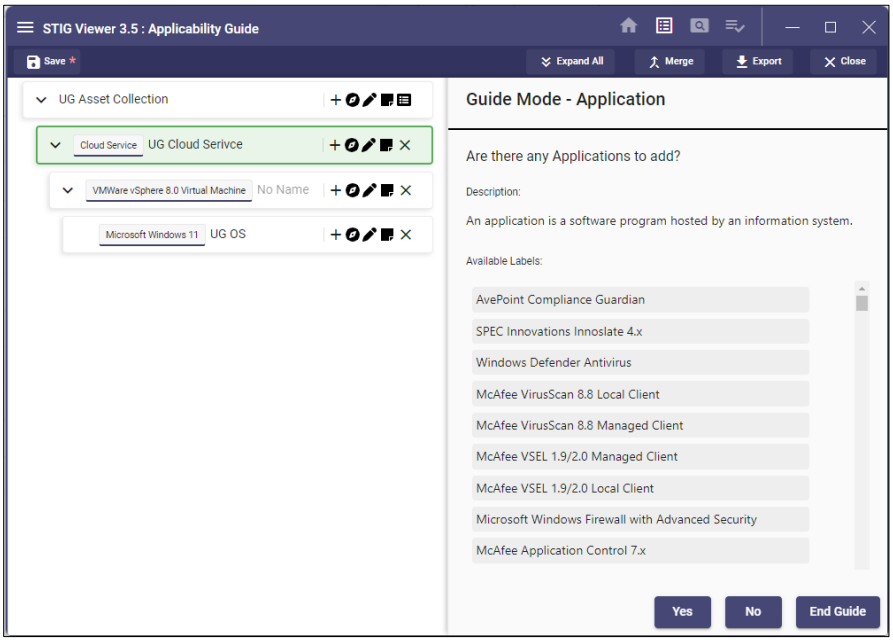
2. On the right, select **Guide Mode** to view available asset labels based on the asset selected and its current parent.



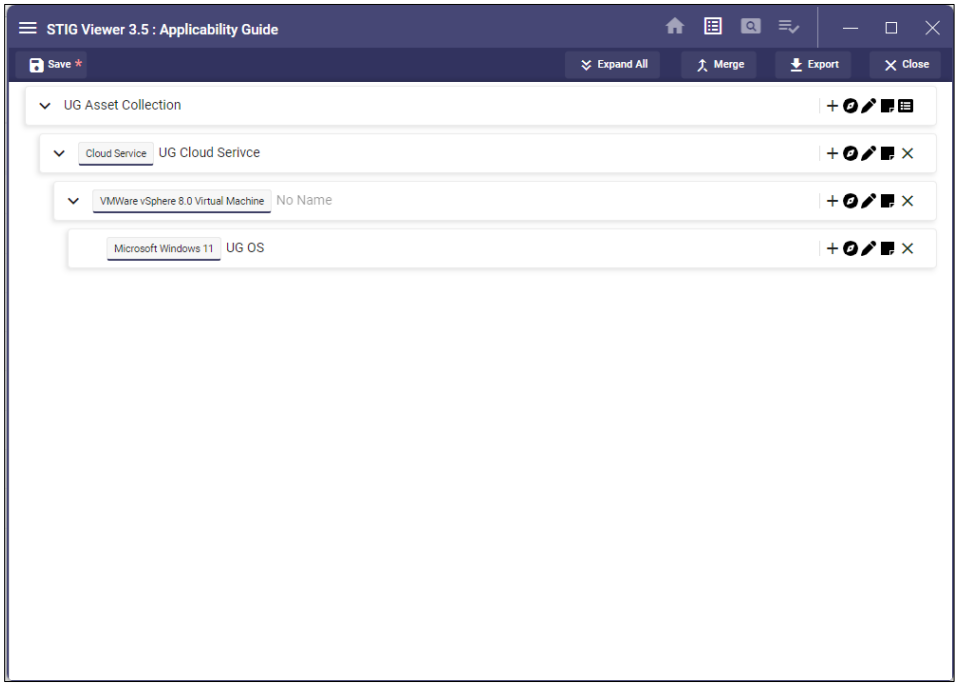
3. Select **Yes** on the **Asset Type**, name it, select the label to add, and then click **Create**.



4. The new parent will be added to the asset.

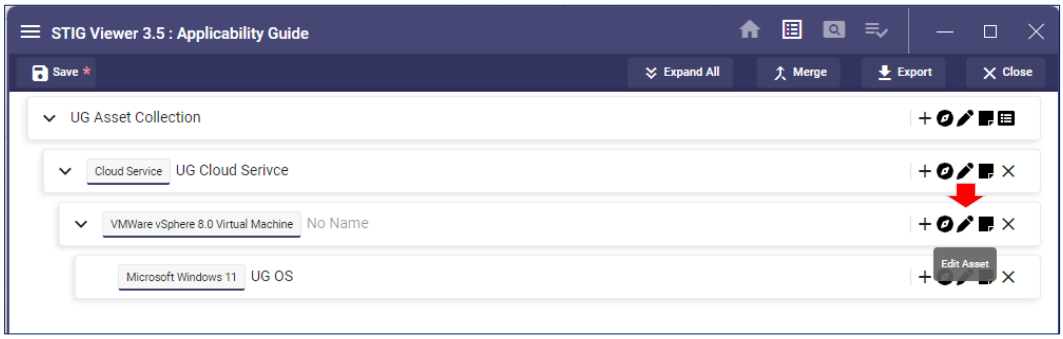


5. Click **End Guide**.

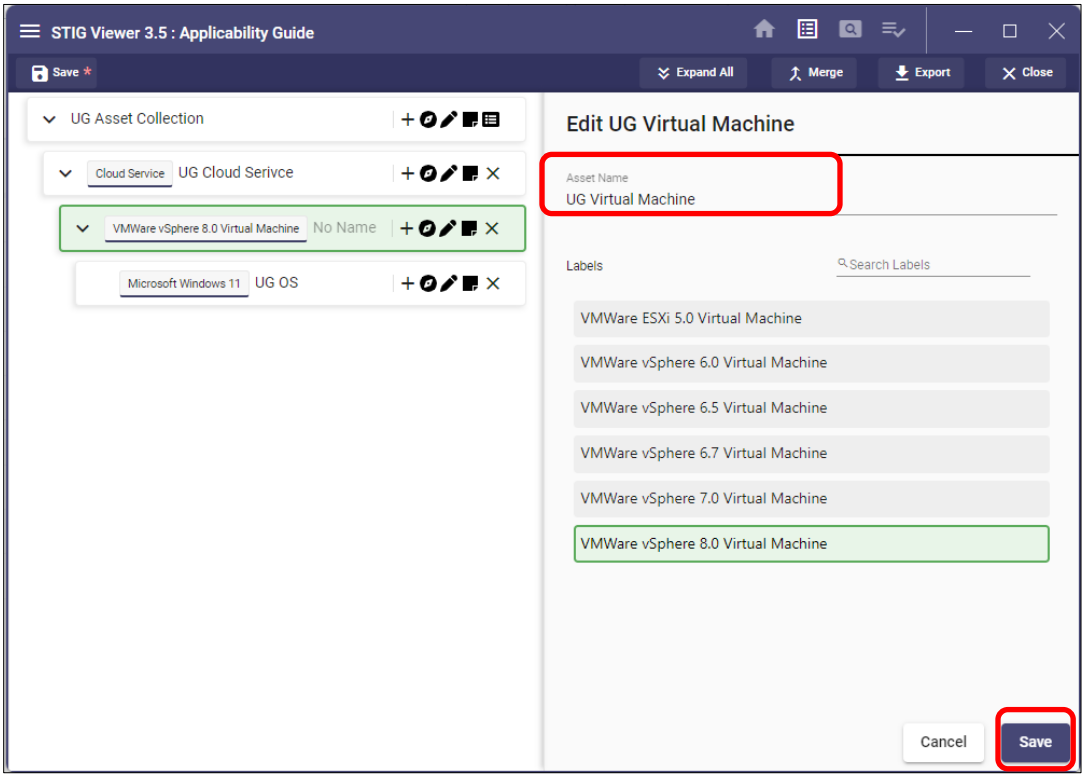


6.4.7 Editing Assets

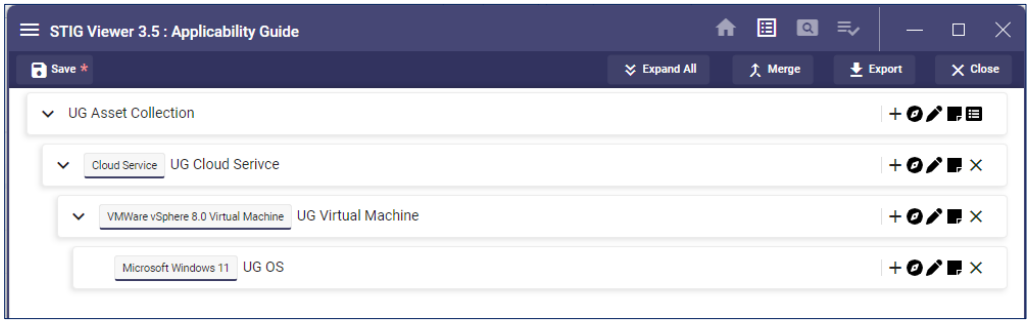
1. After creating an asset, click the **pencil icon** to begin editing an asset. A pane will appear on the right side with the current asset information.



2. Change the name of the asset and the label (if available) as needed and click **Save**.

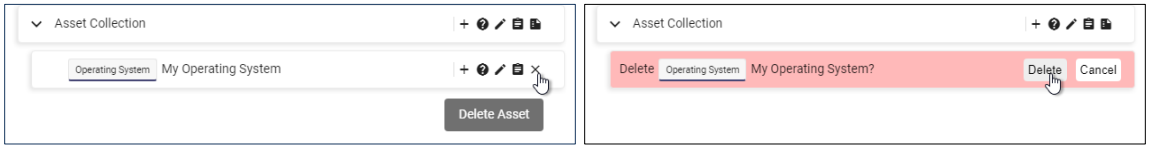


3. The changes will be reflected on the tree to the left.



6.4.8 Removing Assets

To remove an asset, click **X** next to the tree item and click **Delete**.



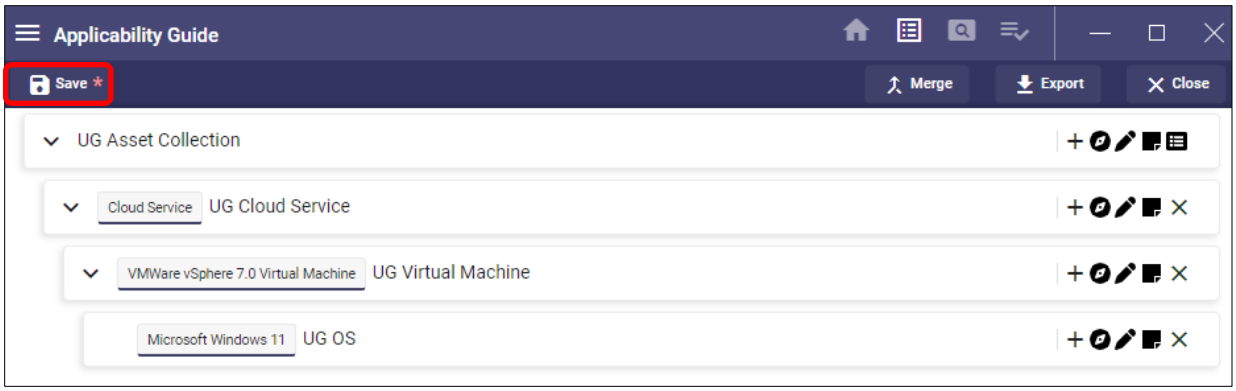
6.5 Save, Open, and Merge

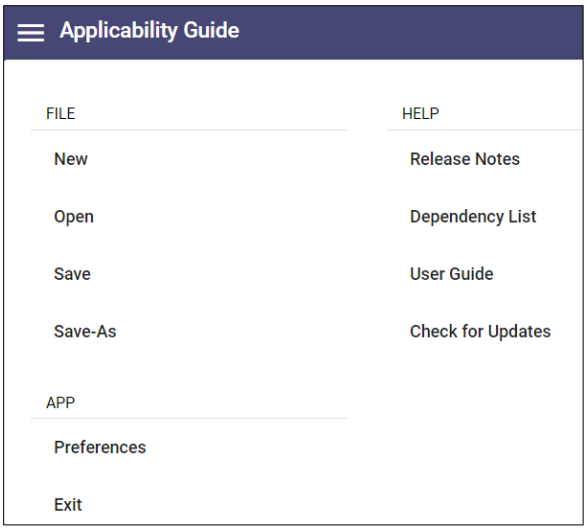
6.5.1 Overview

When an asset posture is built, the application allows the user to save the collection as a JSON document for import later. These options can be found under the **File** menu located under the hamburger menu or by using the **Save** icon at the top of the page.

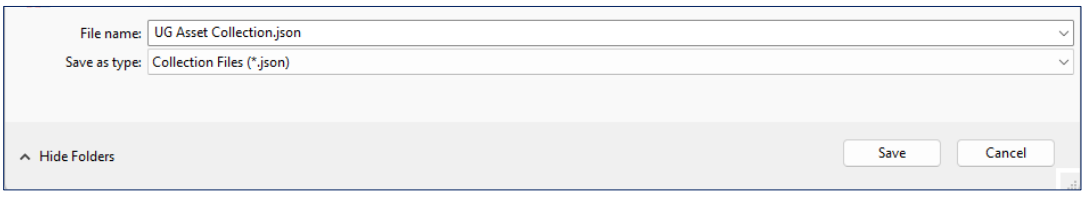
6.5.2 Save Collection

1. To save a collection, select the **Save** icon in the navigation bar or open the hamburger menu and select File >> Save.





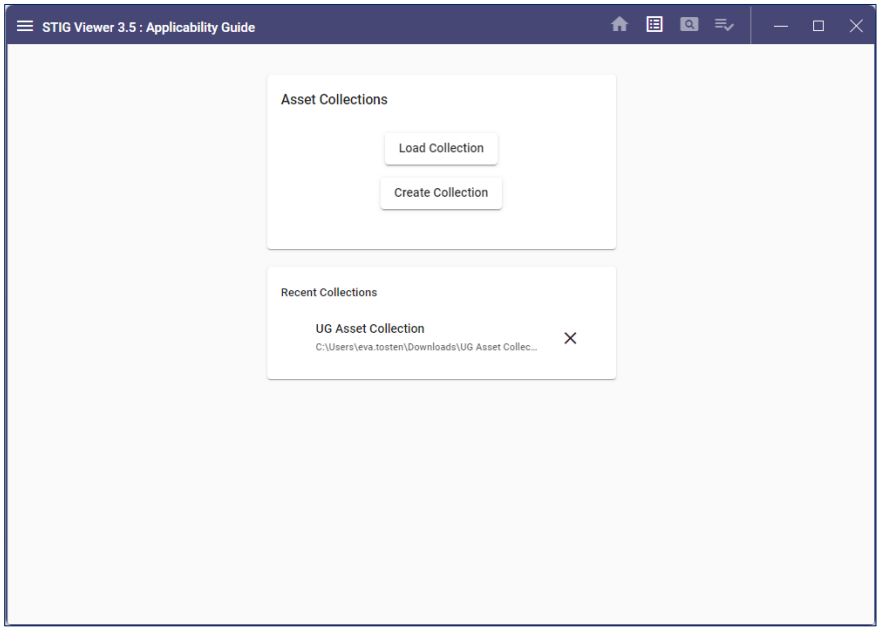
2. A window will pop up with the option to choose a save location and a file name if this is a new collection. Click **Save** to save the collection.



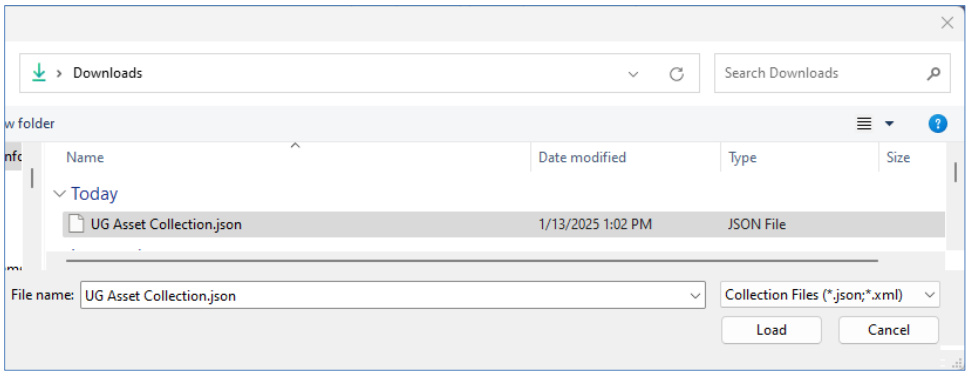
6.5.3 Open Collection

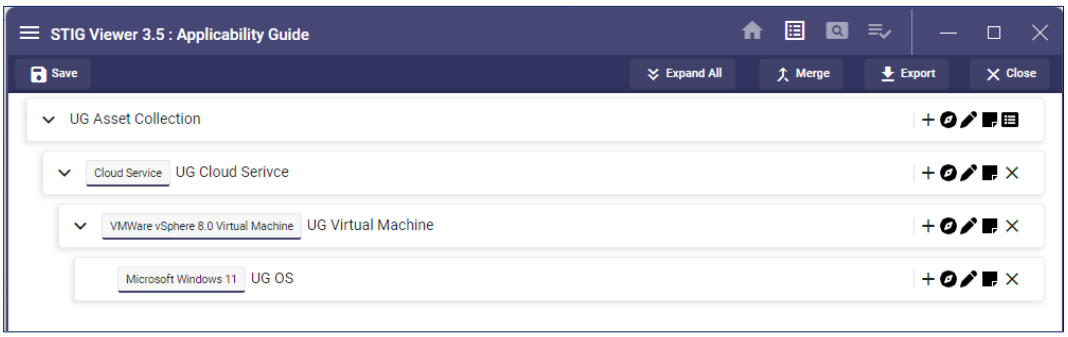
1. To open an Asset Collection (either JSON or XML), click **Load Collection** to load an existing collection or select from the **Recent Collections** section of the main page.

   Note: Alternatively, click the hamburger menu and select File >> Open to open files.

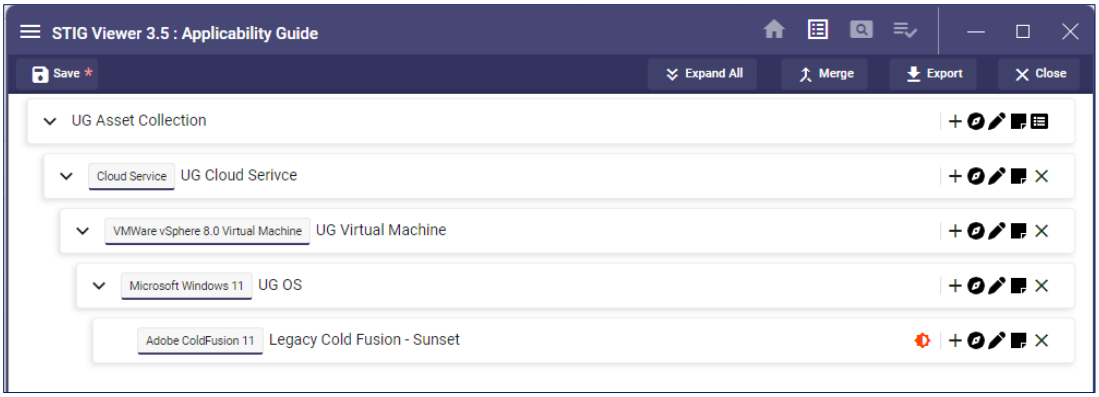


2. Navigate to the location of the saved Asset Collection document, select it, and click **Load**.





Note: If an imported asset has been sunset or deprecated, an indicator will be displayed next to the asset. A red sun indicator signifies that it is sunset. To view the names of sunset assets, select File >> Preferences and check **Enable Sunset Labels** to enable the **Sunset Labels** option.



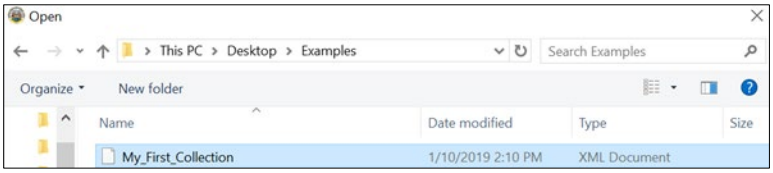
6.5.4 Merge Collection

Merging an asset collection allows the user to import assets from an asset collection file into the currently open collection. When the merge operation is successful, the assets of the merged collection will be appended to the end of the current collection.

6.5.4.1 Merge an Asset Collection

1. In the Navbar, click the **Merge** icon.

2. Navigate to the location of the saved Asset Collection document, select it, and click **Load**.



6.5.4.2 Merge Collections (with tree not empty)

6.6 Drag and Drop

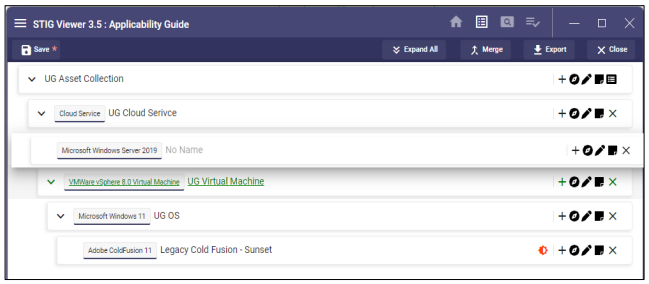
6.6.1 Overview

The SRG/STIG Applicability Guide is drag-and-drop enabled, meaning the user can drag and drop a compatible asset into another asset.

6.6.2 Drag and Drop Assets

To drag and drop an asset, left-click and hold with the left mouse button and then drag it to the intended asset. When the dragged asset encounters a compatible asset, the compatible asset will turn green, signaling a valid drop location. If the asset is not compatible, the asset will not be moved, and a message will be displayed.

Compatible Item Dragged

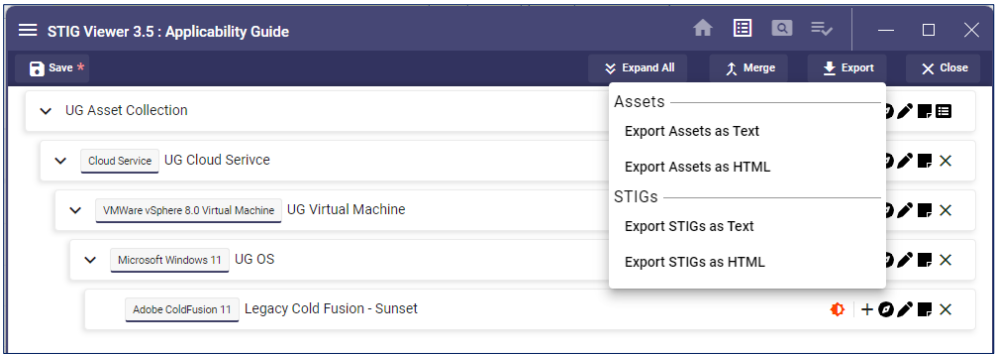


Incompatible Item Dragged

6.7 Exports

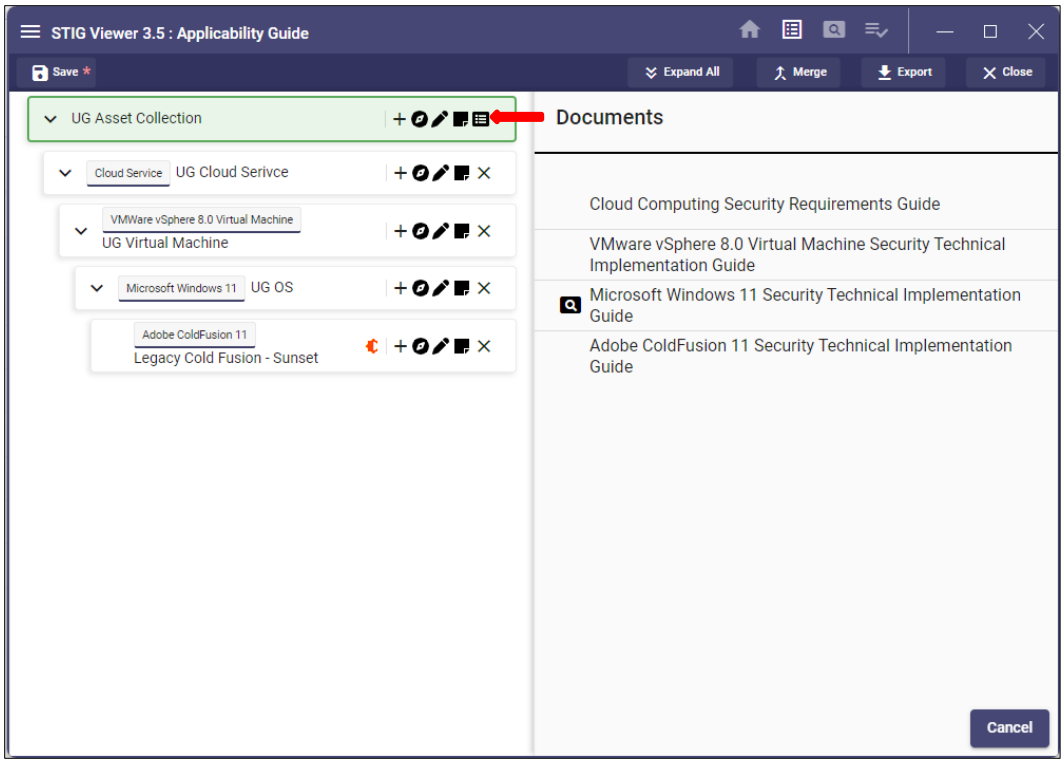
6.7.1 Overview

After building an asset collection, the user can export the requirements/policy documents using options in the Navbar menu. Exports come in two file types, HTML and text, and in two varieties, normal/flat and asset-based list. The flat list contains only the policy documents and their information, whereas the asset-based list also contains the asset that it applies to and the path to get to that asset.



6.7.2 Preview

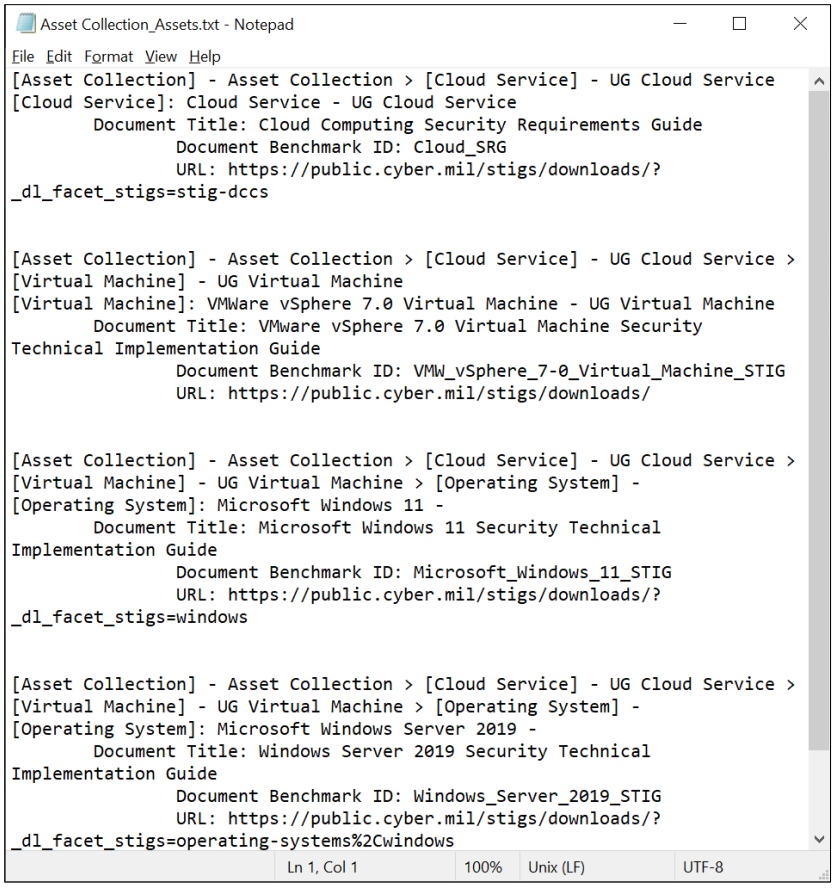
To access a preview of the current collection, select **Documents** from the asset tree. The window on the right will show a list of the Requirements/Policy Documents that apply to the current asset posture.



6.7.3 Exporting

1. To export assets, select **Export Assets as Text (or as HTML)** in the Navbar.
2. In the pop-up menu, choose the location and name of the export file and click **Save**.

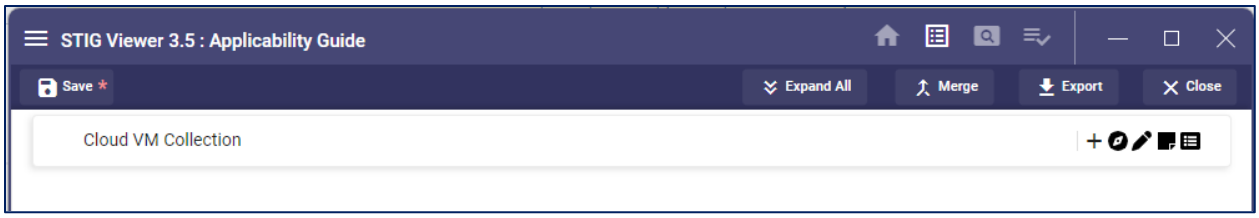
Examples:



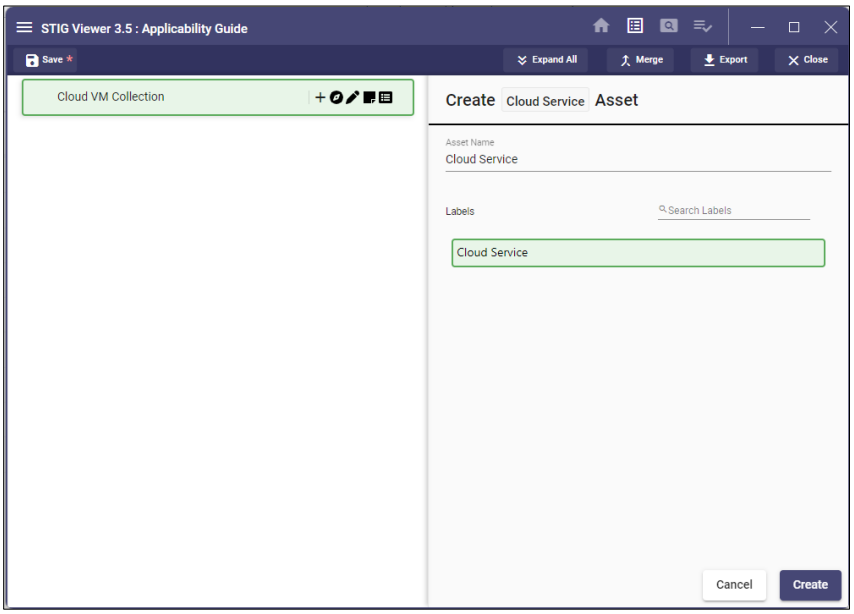
6.7.4 Scenario

A task is required to secure a system on a VMware-based cloud environment. The VM is running Windows 11 and has several applications installed, including JRE 8, Microsoft Office 2016, and .Net Framework 4.0. Securing this system requires knowing what policy documents to follow. Therefore, the SRG/STIG Applicability Guide is used to fill this need easily and quickly.

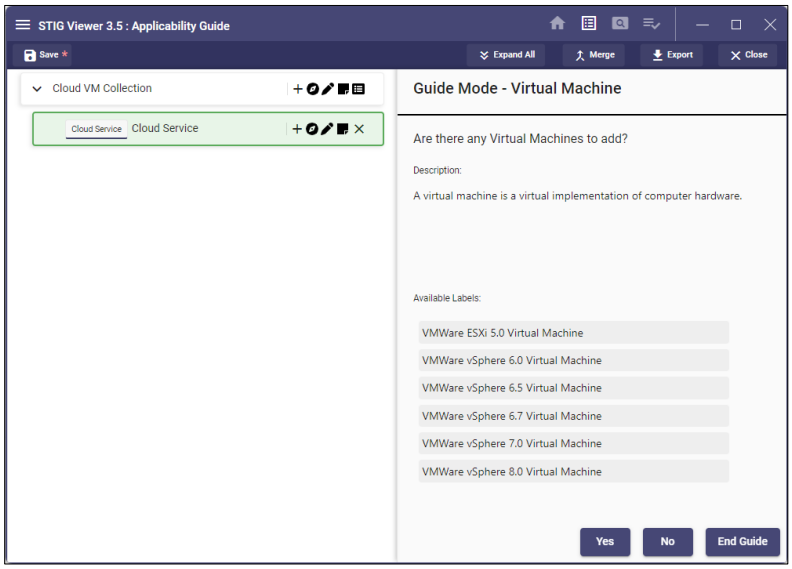
1. Add a new collection and name it accordingly.



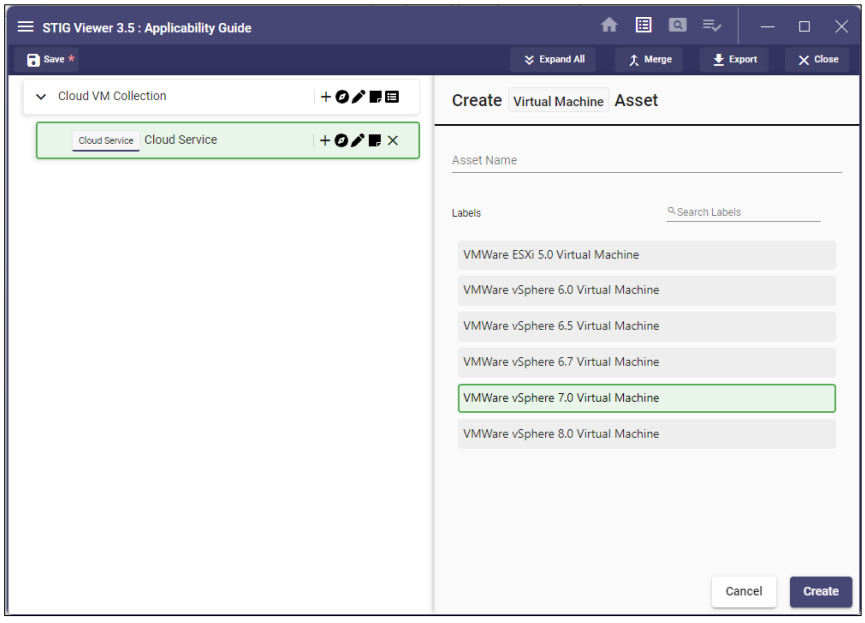
2. Add a cloud service asset. (For this scenario, use Guide Mode.)
   a. Click **No** on **Guide Mode – Asset Group**.
   b. Click **Yes** on **Guide Mode – Cloud Service**.
   c. Name the Asset and select **Cloud Service** under the **Label**.
   d. Click **Create**.



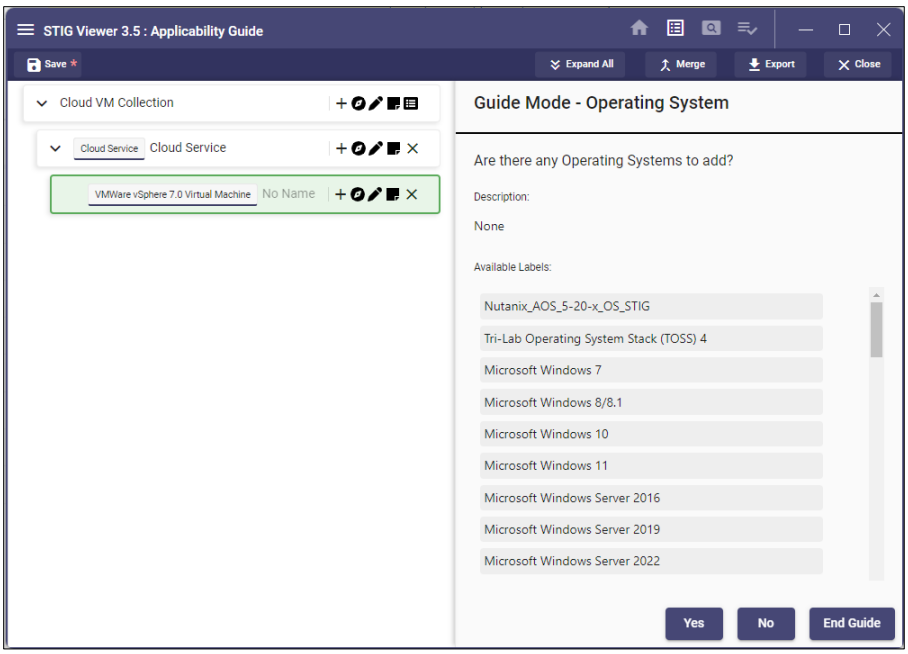
3. Add a VM.
   a. Click **No** on **Guide Mode – Application**.
   b. Click **No** on **Guide Mode – Container**.
   c. Click **No** on **Guide Mode – Generic Network Element**.
   d. Click **No** on **Guide Mode – Specific Network Element**.
   e. Click **No** on **Guide Mode – Virtual Appliance**.
   f. Click **Yes** on **Guide Mode – Virtual Machine**.



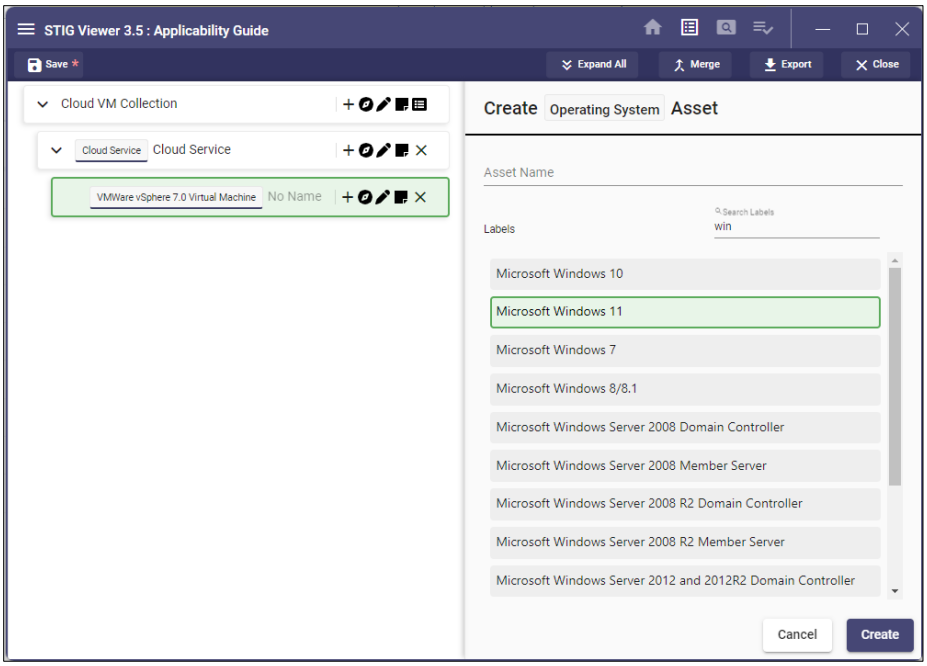
   g. Select VMWare vSphere 7.0 Virtual Machine.



h. Click **Create.**

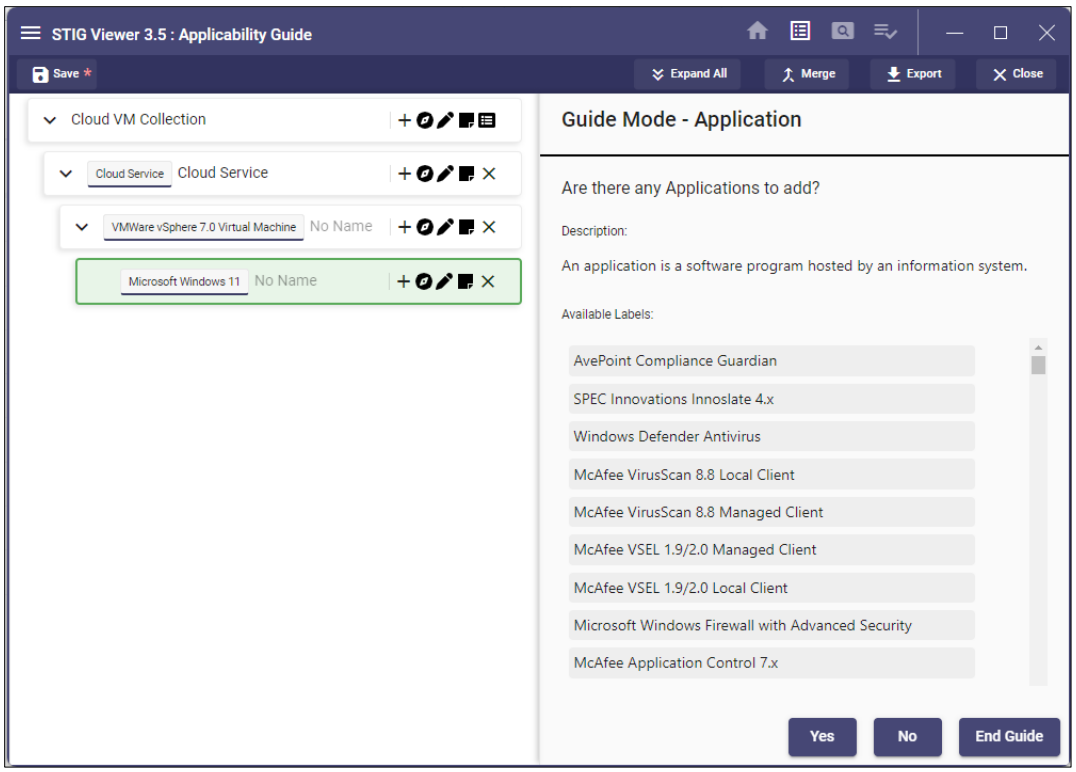


4. Add the Windows 11 operating system.
   a. Click **Yes** on **Guide Mode – Operating System**.
   b. Enter **win** in the search section.



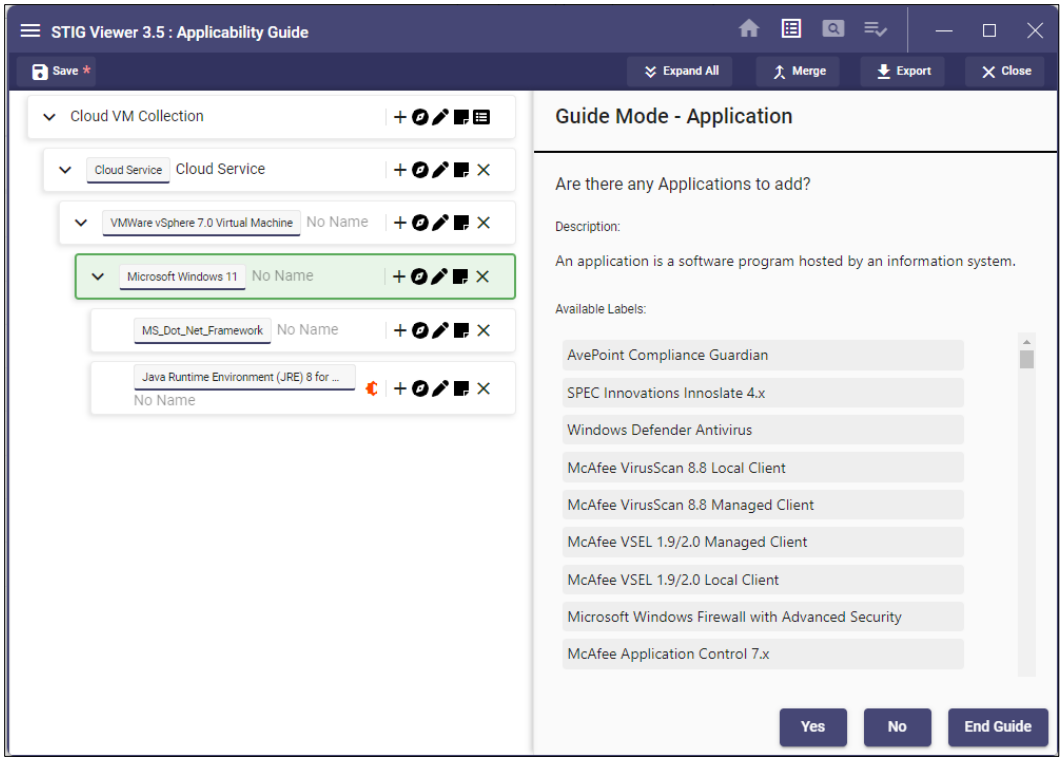
   c. Select **Windows 11**.

d. Click **Create**.

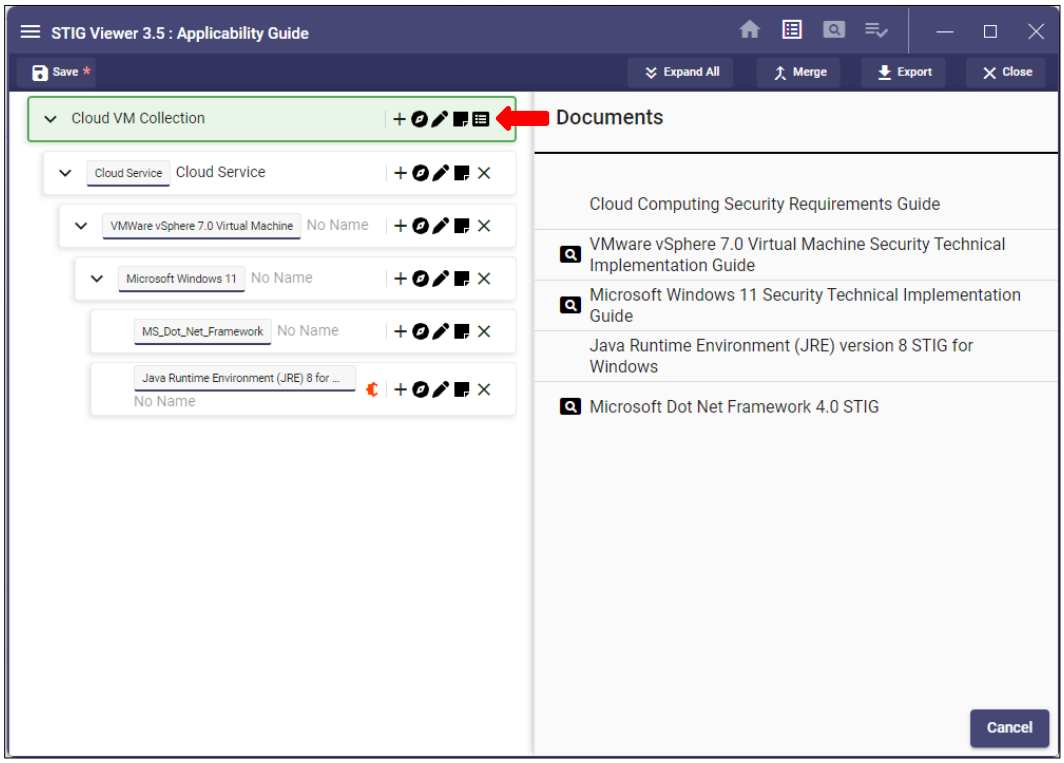


e. Click **Yes** on **Guide Mode – Application**.

f. Add the necessary applications (JRE 8, Microsoft Office 2016, .Net Framework 4.0). Select each one individually. After each one is selected, it will return to the Guide Mode Application screen. After selecting all the desired applications, click **End Guide**.

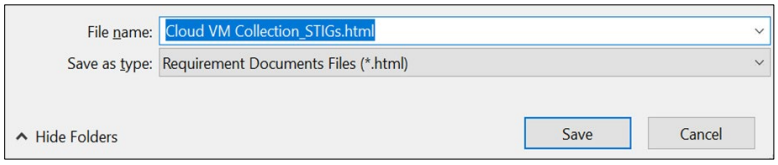


5. Now that the collection is built, policy documents can be previewed by selecting the document icon at the top level (last one on right).

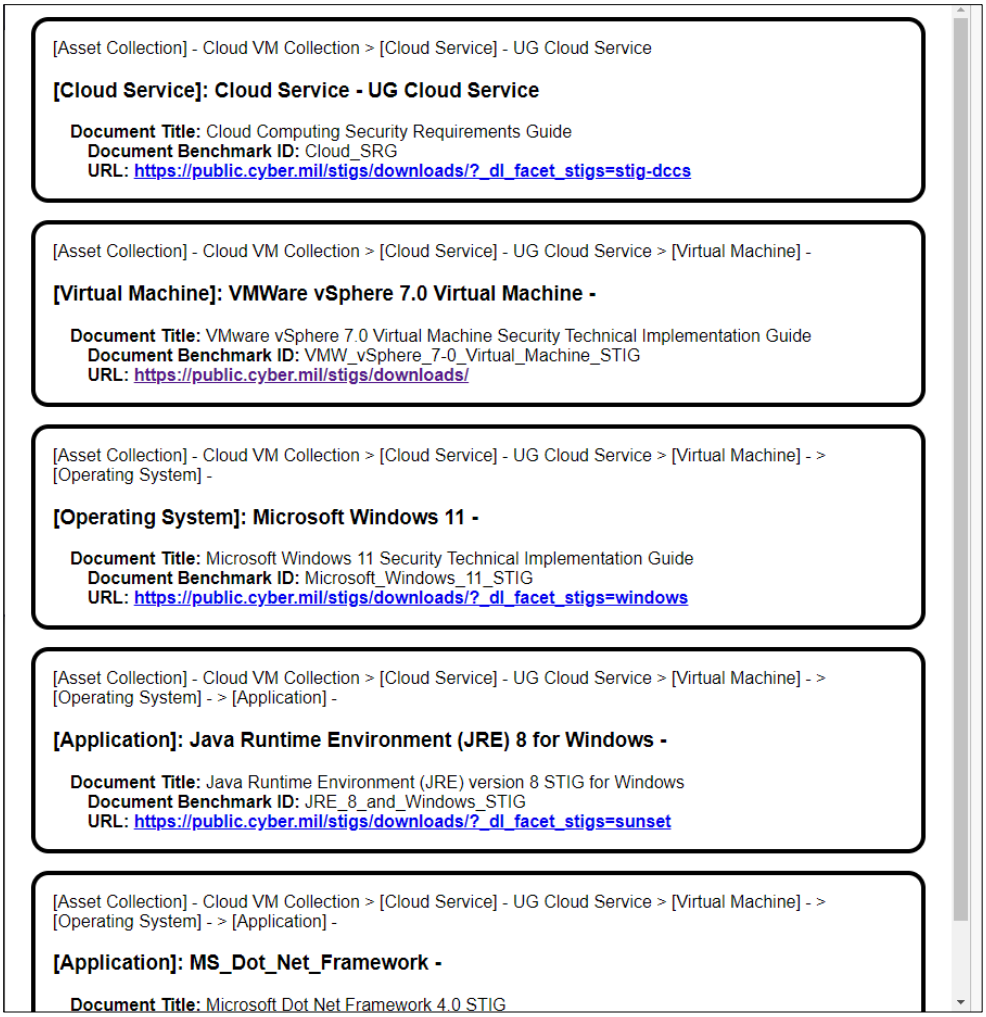


6. To save the collection, click **Save** on the Navbar.

7. On the Navbar, select Export >> STIGs as HTML. Choose an appropriate name and location and then click **Save**.



The exported document should look like this:



[Asset Collection] - Cloud VM Collection > [Cloud Service] - UG Cloud Service

[Cloud Service]: Cloud Service - UG Cloud Service

Document Title: Cloud Computing Security Requirements Guide
Document Benchmark ID: Cloud_SRG
URL: https://public.cyber.mil/stigs/downloads/?_dl_facet_stigs=stig-dccs

[Asset Collection] - Cloud VM Collection > [Cloud Service] - UG Cloud Service > [Virtual Machine] -

[Virtual Machine]: VMWare vSphere 7.0 Virtual Machine -

Document Title: VMware vSphere 7.0 Virtual Machine Security Technical Implementation Guide
Document Benchmark ID: VMW_vSphere_7-0_Virtual_Machine_STIG
URL: https://public.cyber.mil/stigs/downloads/

[Asset Collection] - Cloud VM Collection > [Cloud Service] - UG Cloud Service > [Virtual Machine] - > [Operating System] -

[Operating System]: Microsoft Windows 11 -

Document Title: Microsoft Windows 11 Security Technical Implementation Guide
Document Benchmark ID: Microsoft_Windows_11_STIG
URL: https://public.cyber.mil/stigs/downloads/?_dl_facet_stigs=windows

[Asset Collection] - Cloud VM Collection > [Cloud Service] - UG Cloud Service > [Virtual Machine] - > [Operating System] - > [Application] -

[Application]: Java Runtime Environment (JRE) 8 for Windows -

Document Title: Java Runtime Environment (JRE) version 8 STIG for Windows
Document Benchmark ID: JRE_8_and_Windows_STIG
URL: https://public.cyber.mil/stigs/downloads/?_dl_facet_stigs=sunset

[Asset Collection] - Cloud VM Collection > [Cloud Service] - UG Cloud Service > [Virtual Machine] - > [Operating System] - > [Application] -

[Application]: MS_Dot_Net_Framework -

Document Title: Microsoft Dot Net Framework 4.0 STIG