STIG Viewer 2.x User Guide

Version 1, Release 13

August 2022

Developed by DISA for the DoD

Table of Contents

Page

INTRODUCTION

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

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 the STIG Viewer is to provide an intuitive graphical user interface that allows ease of access to the STIG content, along with additional search and sort functionality unavailable with the current method of viewing the STIGs (using a style sheet in a web browser). STIG Viewer also supports additional functionality 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.
- Creates a Local Data Cache on a system to store user configuration data and the current set of imported STIGs. This permits the reloading of the last set of loaded STIGs each time the STIG Viewer starts.
- Deletes the Local Data Cache from the Viewer's options menu. STIG Viewer can only create one Local Data Cache at a time.
- Multiple XCCDF STIG files can be simultaneously unzipped and loaded from a .zip file containing one or more folders with zipped STIG packages. STIG Viewer will drill down to find all XCCDF files and load them. It then extracts all XCCDF files to its local folder since a Local Data Cache is required for this operation.
- Sorts the list of STIG requirements/vulnerabilities by Vulnerability ID, STIG ID, Rule ID, CCI, or Group/Rule Name.
- Searches or filters all loaded STIG files based on one or more keywords. Searches all fields or individual fields and then returns a filtered list of STIG requirements/vulnerabilities.
    - Searches may also be restricted to Rule Title, STIG ID, Vulnerability ID, Rule ID, Severity, or CCI.
- Displays CCI data if the CCI reference is contained in the STIG requirements.
- Prints or exports (HTML and RTF file formats) selected STIG data for use with other programs (i.e., web browsers and Microsoft Word).
    - Bases the printed/exported data on the list of requirements displayed in the center 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.

NOTE: DISA initially developed STIG Viewer in Java and delivered it as a single JAR file for use with the Oracle Java 8 Java Runtime Environment (JRE). With changes in Java licensing and distribution accompanying the release of Java 11, DISA now provides a standalone STIG Viewer application in a ZIP file that does not require the Oracle JRE. This allows the application to run on 64-bit X86 systems running Windows and Linux with minimal disruption to existing workflows. This limits the program to running at the permission level of the currently logged-in user.

- STIG Viewer does not open or use any network connections.
- Java creates Local Data Caches in the logged-in user's local directory. This is a different location in each operating system.
    - Under Windows 10, this is in the following directory:

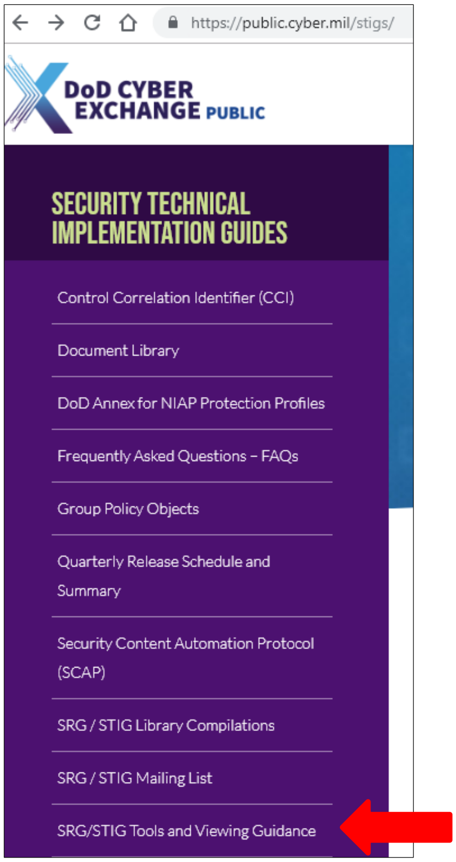
      %USERPROFILE%\AppData\Local\STIGV_AppData

      (When clearing the Local Data Cache, Java deletes the folder and the Local Data Cache simultaneously.)
- The input to the STIG Viewer is XCCDF contained in an XML file. STIG viewer rejects other file types. STIG Viewer is optimized for XCCDF-formatted STIGs produced by DISA for DoD.

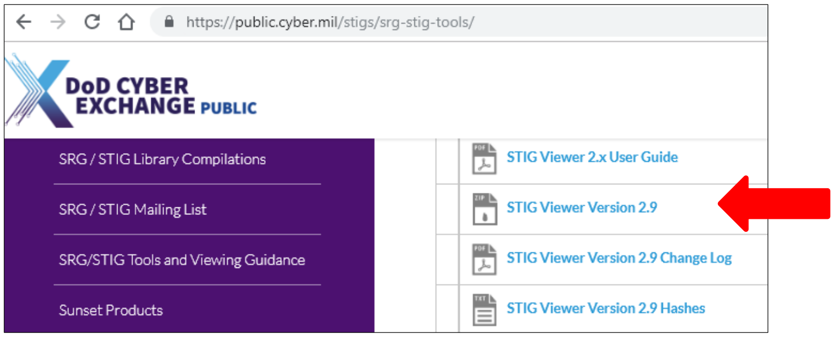
1. INSTALLING AND RUNNING STIG VIEWER 2.X

1.1 Installing Java JAR STIG Viewer

1. Download the STIG Viewer 2.x ZIP file from the Cyber Exchange website. Go to SRGs/STIGs >> SRG/STIG Tools and Viewing Guidance:


https://public.cyber.mil/stigs/
DoD CYBER EXCHANGE PUBLIC
SECURITY TECHNICAL IMPLEMENTATION GUIDES
Control Correlation Identifier (CCI)
Document Library
DoD Annex for NIAP Protection Profiles
Frequently Asked Questions – FAQs
Group Policy Objects
Quarterly Release Schedule and Summary
Security Content Automation Protocol (SCAP)
SRG / STIG Library Compilations
SRG / STIG Mailing List
SRG/STIG Tools and Viewing Guidance

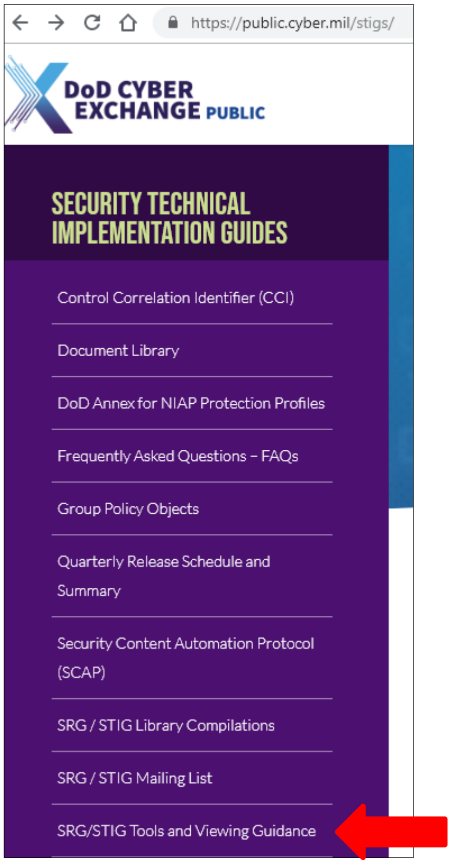
2. Right-click on STIG Viewer Version 2.x.


https://public.cyber.mil/stigs/srg-stig-tools/
DoD CYBER EXCHANGE PUBLIC
SRG / STIG Library Compilations
SRG / STIG Mailing List
SRG/STIG Tools and Viewing Guidance
Sunset Products
STIG Viewer 2.x User Guide
STIG Viewer Version 2.9
STIG Viewer Version 2.9 Change Log
STIG Viewer Version 2.9 Hashes

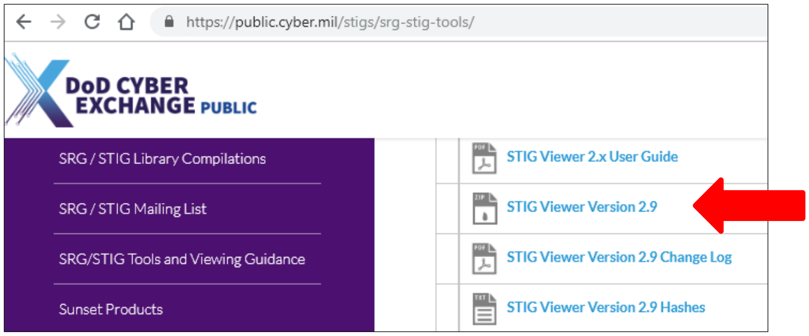
3. Click **Save File** to save to your computer as STIGViewer2.x.zip. Run the JAR file directly from the ZIP file or extract it to any location for subsequent execution.

1.2 Installing Standalone STIG Viewer

1. Download the STIG Viewer 2.x standalone ZIP file from the Cyber Exchange website. Go to SRGs/STIGs >> SRG/STIG Tools and Viewing Guidance.


https://public.cyber.mil/stigs/
DoD CYBER EXCHANGE PUBLIC
SECURITY TECHNICAL IMPLEMENTATION GUIDES
Control Correlation Identifier (CCI)
Document Library
DoD Annex for NIAP Protection Profiles
Frequently Asked Questions – FAQs
Group Policy Objects
Quarterly Release Schedule and Summary
Security Content Automation Protocol (SCAP)
SRG / STIG Library Compilations
SRG / STIG Mailing List
SRG/STIG Tools and Viewing Guidance

2. Right-click STIG Viewer 2.x-Win64 or STIG Viewer 2.x-Linux.

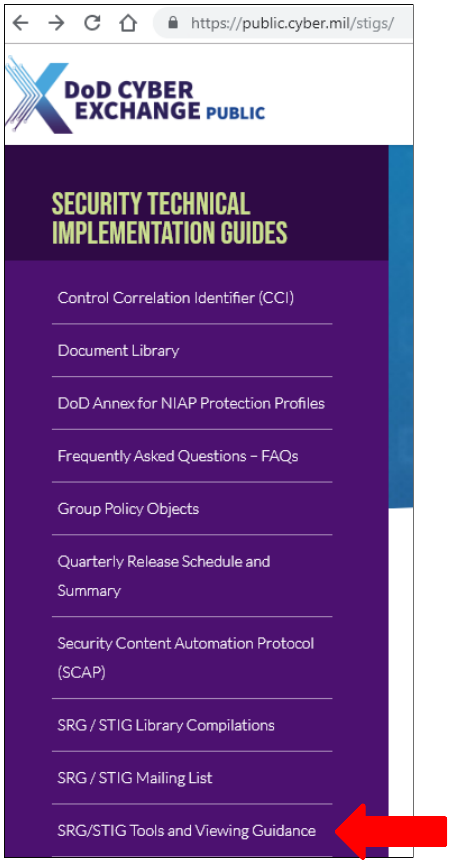

https://public.cyber.mil/stigs/srg-stig-tools/
DoD CYBER EXCHANGE PUBLIC
SRG / STIG Library Compilations
SRG / STIG Mailing List
SRG/STIG Tools and Viewing Guidance
Sunset Products
STIG Viewer 2.x User Guide
STIG Viewer Version 2.9
STIG Viewer Version 2.9 Change Log
STIG Viewer Version 2.9 Hashes

3. Click **Save File** to save to your computer as STIGViewer2.x-Win64.zip or STIGViewer2.x-Linux.zip. Extract all contents of the ZIP file to the local hard disk; the standalone application does not run from within the ZIP file.

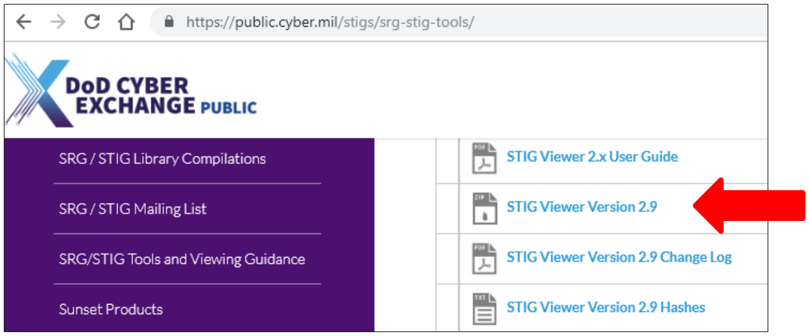
   NOTE: The Linux standalone STIG Viewer requires GLIBC 2.14 or later to run; this means that the application will not run on RHEL 6.

1.3 Installing the STIG Viewer Windows MSI Package

1. Download the STIG Viewer 2.x Windows MSI ZIP file from the Cyber Exchange website. Go to SRGs/STIGs >> SRG/STIG Tools and Viewing Guidance.


https://public.cyber.mil/stigs/
DoD CYBER EXCHANGE PUBLIC
SECURITY TECHNICAL IMPLEMENTATION GUIDES
Control Correlation Identifier (CCI)
Document Library
DoD Annex for NIAP Protection Profiles
Frequently Asked Questions – FAQs
Group Policy Objects
Quarterly Release Schedule and Summary
Security Content Automation Protocol (SCAP)
SRG / STIG Library Compilations
SRG / STIG Mailing List
SRG/STIG Tools and Viewing Guidance

2. Right-click STIG Viewer Version 2.x-Win64_msi.


https://public.cyber.mil/stigs/srg-stig-tools/
DoD CYBER EXCHANGE PUBLIC
SRG / STIG Library Compilations
SRG / STIG Mailing List
SRG/STIG Tools and Viewing Guidance
Sunset Products
STIG Viewer 2.x User Guide
STIG Viewer Version 2.9
STIG Viewer Version 2.9 Change Log
STIG Viewer Version 2.9 Hashes

3. Click **Save File** to save to your computer as STIGViewer2.x-Win64_msi.zip.

4. Open the downloaded ZIP file. Open the enclosed .msi file to begin the installation process. Administrative rights are required for installation.

1.4 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.

1.5 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 your 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.

1.6 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_2-XX_Linux.zip -d /opt/stigviewer
   ```

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

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

4. Notify fapolicyd that the database has been updated.

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

5. Run STIG Viewer from the shared directory.

   ```
   $ /opt/stigviewer/STIGViewer
   ```

1.7 Digital Signatures

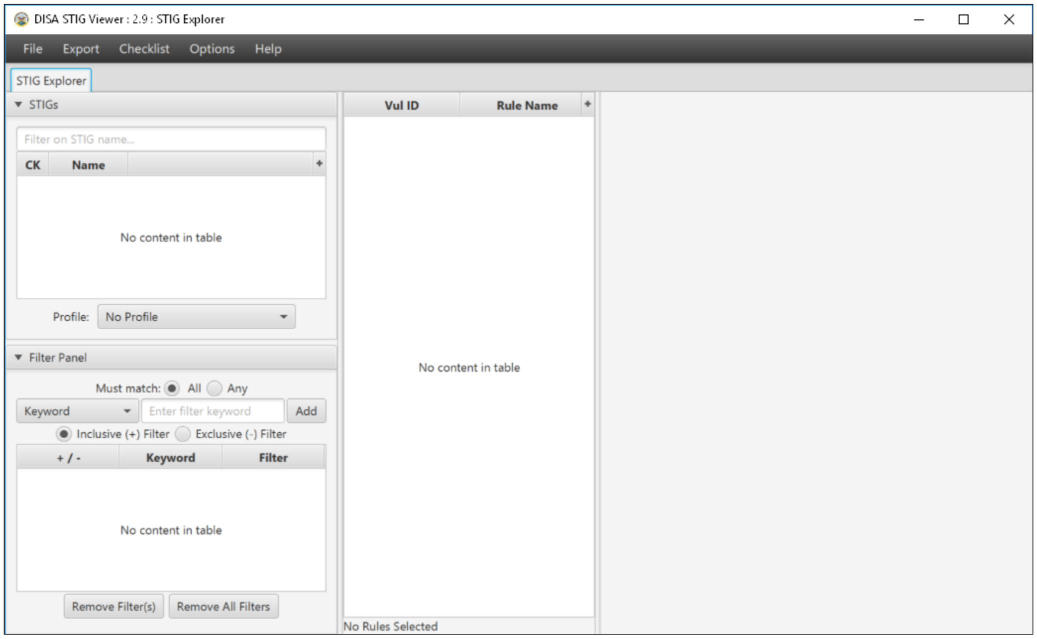
Beginning with version 2.15, the Windows EXE and MSI files are digitally signed with a DoD code signing certificate. Information on installing DoD trust anchors is available at https://public.cyber.mil/pki-pke/. To view the signatures, open the file's properties in Windows Explorer and select the **Digital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

2. USING STIG VIEWER 2.X

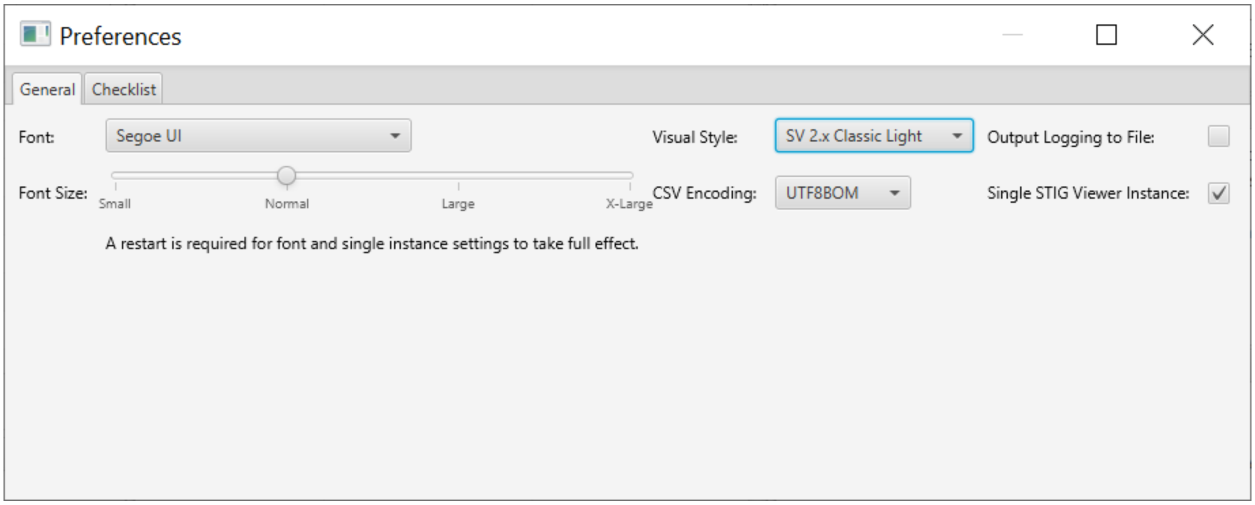
2.1 Opening STIG Viewer

1. The procedure for opening STIG Viewer depends on the release package used.
   a. **STIG Viewer Java Archive (JAR) package.**
      i. This package requires version 8 of the Oracle Java Runtime Environment to be installed.
      ii. Start STIG Viewer by opening the STIGViewer2.x.jar file.
   b. **Windows standalone package.**
      i. Start STIG Viewer by opening the “STIG Viewer.exe” file.
   c. **Windows MSI package.**
      i. Start STIG Viewer by opening the “STIG Viewer” item from the Start Menu.
   d. **Linux standalone package.**
      i. Start the standalone STIG Viewer from the command line with the bundled STIG Viewer shell script file (“STIGViewer”).
   e. **Other considerations.**
      i. Consult local system administrators for assistance in running standalone versions of STIG Viewer with any application firewalls.

2. At startup, an empty STIG Viewer looks like this:



3. When STIGs are loaded into STIG Viewer, preferences will determine their appearance. To change the appearance, select **Options** >> **Preferences** from the top navigation bar and then select the desired appearance from the **Visual Style** drop-down box.



Font: Segoe UI

Font Size: Normal

Visual Style: SV 2.x Classic Light

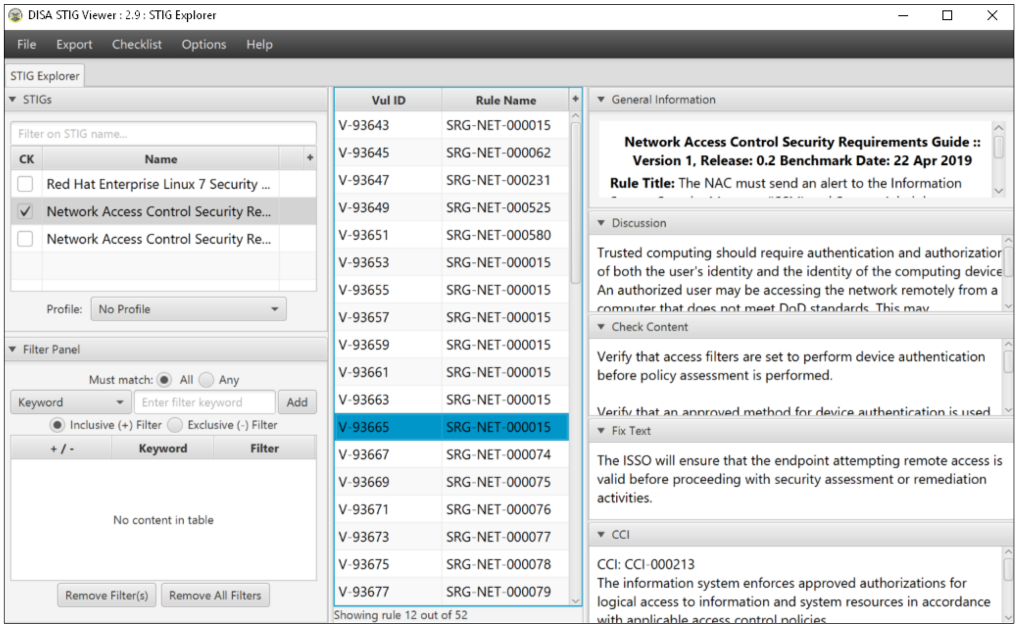
Output Logging to File: ☐

CSV Encoding: UTF8BOM

Single STIG Viewer Instance: ☑

A restart is required for font and single instance settings to take full effect.

a. SV 2.x Classic light:



DISA STIG Viewer : 2.9 : STIG Explorer

CK	Name
☐	Red Hat Enterprise Linux 7 Security ...
☑	Network Access Control Security Re...
☐	Network Access Control Security Re...

Profile: No Profile

Must match: ● All ○ Any

Keyword

● Inclusive (+) Filter ○ Exclusive (-) Filter

+ / -	Keyword	Filter

No content in table

Vul ID	Rule Name
V-93643	SRG-NET-000015
V-93645	SRG-NET-000062
V-93647	SRG-NET-000231
V-93649	SRG-NET-000525
V-93651	SRG-NET-000580
V-93653	SRG-NET-000015
V-93655	SRG-NET-000015
V-93657	SRG-NET-000015
V-93659	SRG-NET-000015
V-93661	SRG-NET-000015
V-93663	SRG-NET-000015
V-93665	SRG-NET-000015
V-93667	SRG-NET-000074
V-93669	SRG-NET-000075
V-93671	SRG-NET-000076
V-93673	SRG-NET-000077
V-93675	SRG-NET-000078
V-93677	SRG-NET-000079

Showing rule 12 out of 52

Network Access Control Security Requirements Guide :: Version 1, Release: 0.2 Benchmark Date: 22 Apr 2019

Rule Title: The NAC must send an alert to the Information

Trusted computing should require authentication and authorizatior of both the user's identity and the identity of the computing device An authorized user may be accessing the network remotely from a computer that does not meet DoD standards. This may

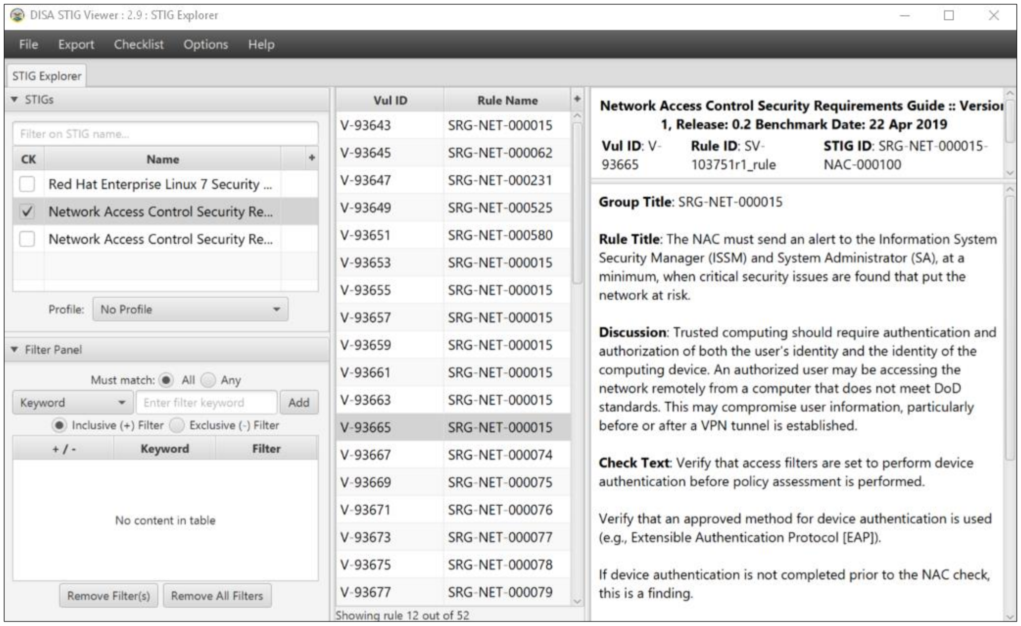
Verify that access filters are set to perform device authentication before policy assessment is performed.

Verify that an approved method for device authentication is used

The ISSO will ensure that the endpoint attempting remote access is valid before proceeding with security assessment or remediation activities.

CCI: CCI-000213
The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

b. Light theme:



CK	Name
□	Red Hat Enterprise Linux 7 Security ...
☑	Network Access Control Security Re...
□	Network Access Control Security Re...

+ / -	Keyword	Filter
No content in table		

Vul ID	Rule Name
V-93643	SRG-NET-000015
V-93645	SRG-NET-000062
V-93647	SRG-NET-000231
V-93649	SRG-NET-000525
V-93651	SRG-NET-000580
V-93653	SRG-NET-000015
V-93655	SRG-NET-000015
V-93657	SRG-NET-000015
V-93659	SRG-NET-000015
V-93661	SRG-NET-000015
V-93663	SRG-NET-000015
V-93665	SRG-NET-000015
V-93667	SRG-NET-000074
V-93669	SRG-NET-000075
V-93671	SRG-NET-000076
V-93673	SRG-NET-000077
V-93675	SRG-NET-000078
V-93677	SRG-NET-000079

Showing rule 12 out of 52

Network Access Control Security Requirements Guide :: Versio
1, Release: 0.2 Benchmark Date: 22 Apr 2019

Vul ID: V-93665 **Rule ID**: SV-103751r1_rule **STIG ID**: SRG-NET-000015-NAC-000100

Group Title: SRG-NET-000015

Rule Title: The NAC must send an alert to the Information System Security Manager (ISSM) and System Administrator (SA), at a minimum, when critical security issues are found that put the network at risk.

Discussion: Trusted computing should require authentication and authorization of both the user's identity and the identity of the computing device. An authorized user may be accessing the network remotely from a computer that does not meet DoD standards. This may compromise user information, particularly before or after a VPN tunnel is established.

Check Text: Verify that access filters are set to perform device authentication before policy assessment is performed.

Verify that an approved method for device authentication is used (e.g., Extensible Authentication Protocol [EAP]).

If device authentication is not completed prior to the NAC check, this is a finding.

4. There are three main columns to the Viewer:
   - Left column: STIGs, which shows the STIG names and Filter Panel.
   - Center column: Vulnerability ID information.
   - Right column: General Information, which shows the Vulnerability detail information.

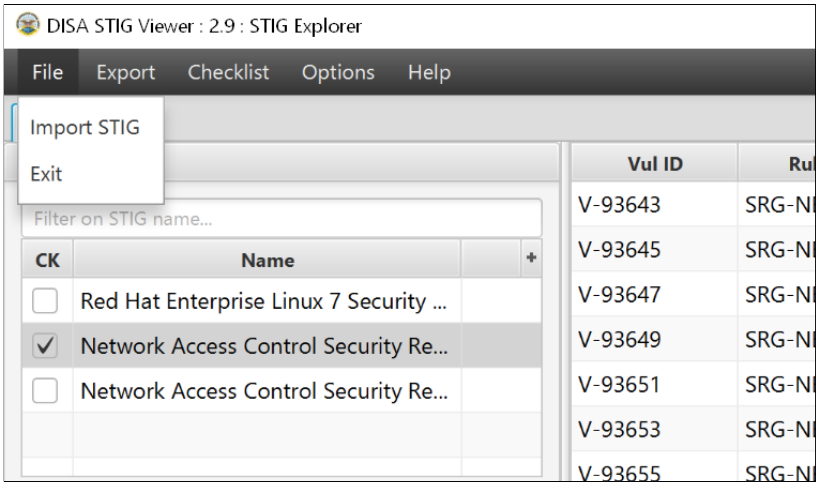
5. In the Classic themes, the left and right columns each have collapsible sections. Clicking on the small arrowheads to the left of each section label will toggle the section to either expand or collapse. The more sections you collapse, the higher each of the other sections will open. The vertical dividers between columns slide to adjust their sizes.
   - Left column labels: **STIGs**, **Filter Panel.**
   - Right column labels: **General Information**, **Discussion**, **Check Content**, **Fix Text**, **CCI**, **Misc** (when applicable).

6. In the non-Classic themes, the various sections of the right column merge into two.

7. In addition to the **Light** themes presented above, there are also equivalent **Dark** themes.

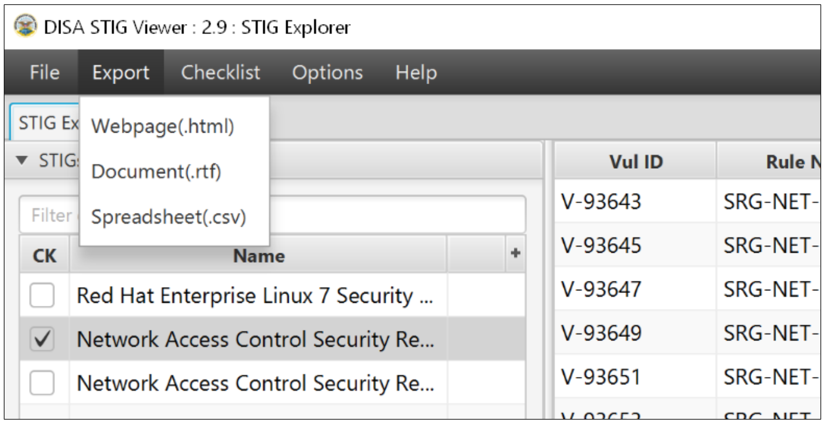
2.2 STIG Viewer Menu Bar

1. The STIG Viewer Menu bar has five menu drop-down selections: **File**, **Export**, **Checklist**, **Options**, and **Help**. Choices within each selection are shown below:



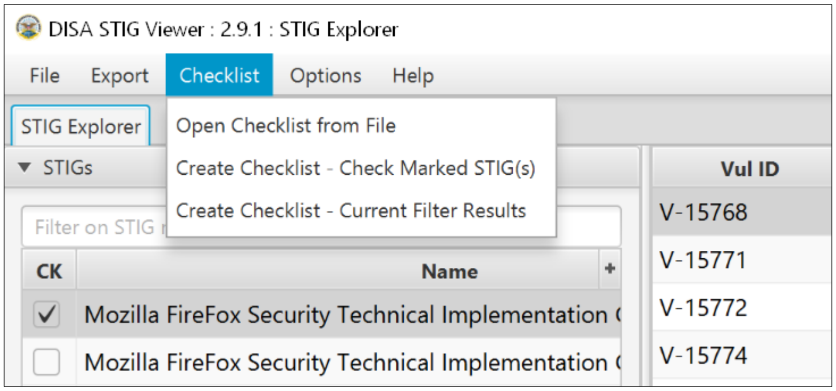
CK	Name
□	Red Hat Enterprise Linux 7 Security ...
☑	Network Access Control Security Re...
□	Network Access Control Security Re...

Vul ID	Rul
V-93643	SRG-NI
V-93645	SRG-NI
V-93647	SRG-NI
V-93649	SRG-NI
V-93651	SRG-NI
V-93653	SRG-NI
V-93655	SRG-NI



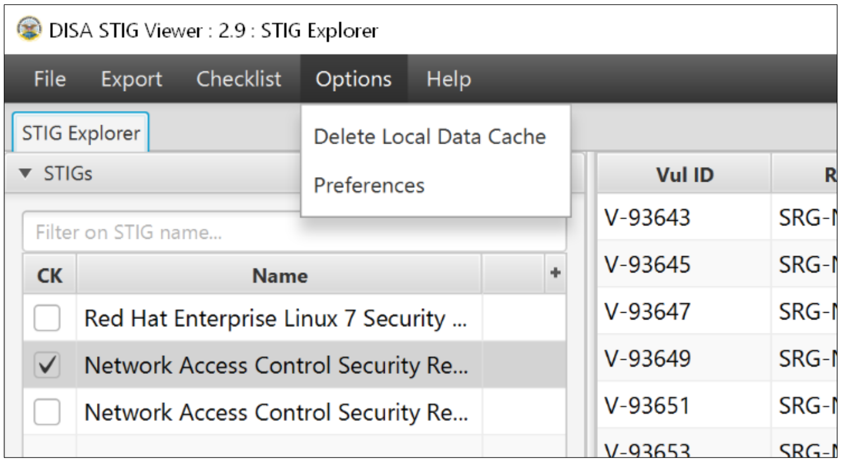
CK	Name
□	Red Hat Enterprise Linux 7 Security ...
☑	Network Access Control Security Re...
□	Network Access Control Security Re...

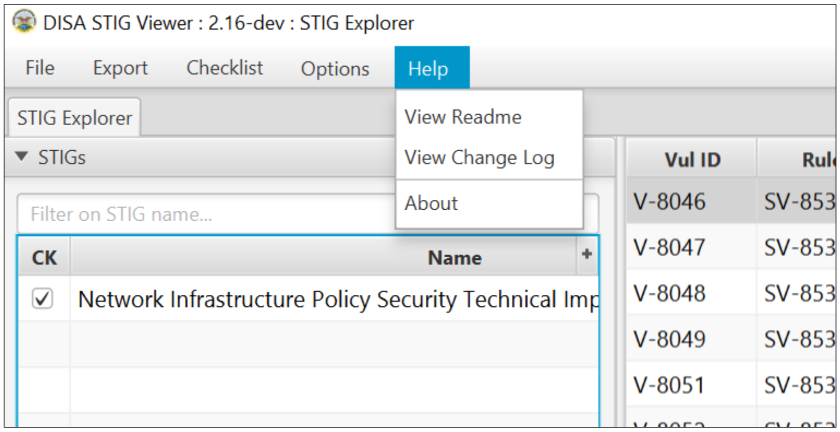
Vul ID	Rule N
V-93643	SRG-NET-
V-93645	SRG-NET-
V-93647	SRG-NET-
V-93649	SRG-NET-
V-93651	SRG-NET-


DISA STIG Viewer : 2.9.1 : STIG Explorer
File
Export
Checklist
Options
Help
STIG Explorer
STIGs
Filter on STIG
Open Checklist from File
Create Checklist - Check Marked STIG(s)
Create Checklist - Current Filter Results

CK	Name
☑	Mozilla FireFox Security Technical Implementation (
□	Mozilla FireFox Security Technical Implementation (

Vul ID
V-15768
V-15771
V-15772
V-15774

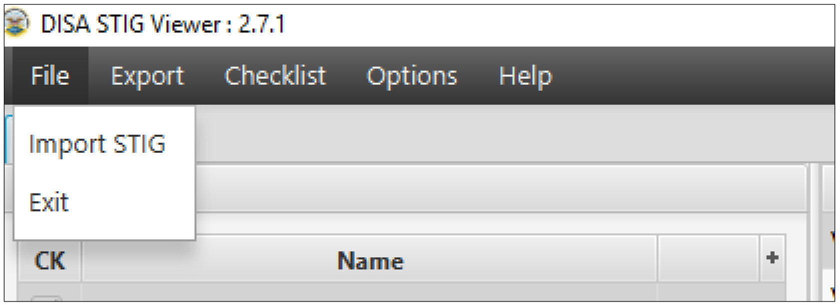




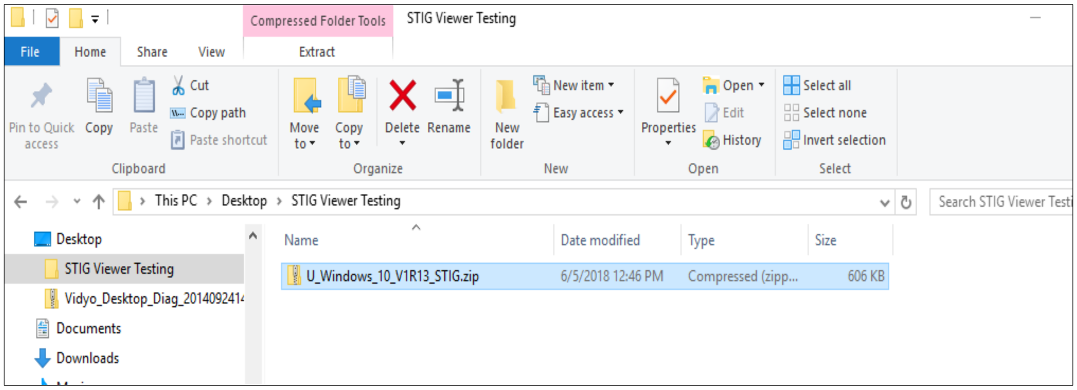
2.3 Loading STIGS

STIGs downloaded from the Cyber Exchange website are in .zip format, which is loaded into the STIG Viewer. STIG Viewer handles all STIGs in the same manner; this guide provides generic instructions suitable for all technologies.

1. From the STIG Viewer Menu bar, select **File** >> **Import STIG**.

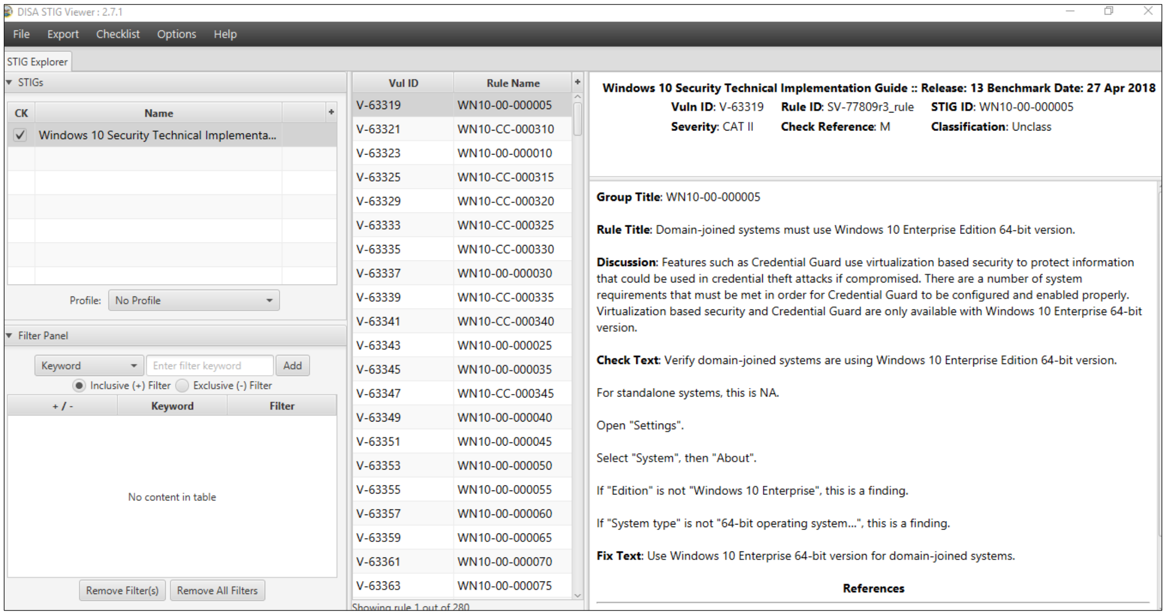


2. Select the STIG .zip file you want to load and click the Open button. This example shows a Windows 10 STIG.



Name	Date modified	Type	Size
U_Windows_10_V1R13_STIG.zip	6/5/2018 12:46 PM	Compressed (zipp...	606 KB

3. STIG Viewer will show the STIG has been loaded.



CK	Name
☑	Windows 10 Security Technical Implementa...

+ / -	Keyword	Filter

Vul ID	Rule Name
V-63319	WN10-00-000005
V-63321	WN10-CC-000310
V-63323	WN10-00-000010
V-63325	WN10-CC-000315
V-63329	WN10-CC-000320
V-63333	WN10-CC-000325
V-63335	WN10-CC-000330
V-63337	WN10-00-000030
V-63339	WN10-CC-000335
V-63341	WN10-CC-000340
V-63343	WN10-00-000025
V-63345	WN10-00-000035
V-63347	WN10-CC-000345
V-63349	WN10-00-000040
V-63351	WN10-00-000045
V-63353	WN10-00-000050
V-63355	WN10-00-000055
V-63357	WN10-00-000060
V-63359	WN10-00-000065
V-63361	WN10-00-000070
V-63363	WN10-00-000075

Showing rule 1 out of 280

Windows 10 Security Technical Implementation Guide :: Release: 13 Benchmark Date: 27 Apr 2018

Vuln ID: V-63319 **Rule ID**: SV-77809r3_rule **STIG ID**: WN10-00-000005
Severity: CAT II **Check Reference**: M **Classification**: Unclass

Group Title: WN10-00-000005

Rule Title: Domain-joined systems must use Windows 10 Enterprise Edition 64-bit version.

Discussion: Features such as Credential Guard use virtualization based security to protect information that could be used in credential theft attacks if compromised. There are a number of system requirements that must be met in order for Credential Guard to be configured and enabled properly. Virtualization based security and Credential Guard are only available with Windows 10 Enterprise 64-bit version.

Check Text: Verify domain-joined systems are using Windows 10 Enterprise Edition 64-bit version.

For standalone systems, this is NA.

Open "Settings".

Select "System", then "About".

If "Edition" is not "Windows 10 Enterprise", this is a finding.

If "System type" is not "64-bit operating system...", this is a finding.

Fix Text: Use Windows 10 Enterprise 64-bit version for domain-joined systems.

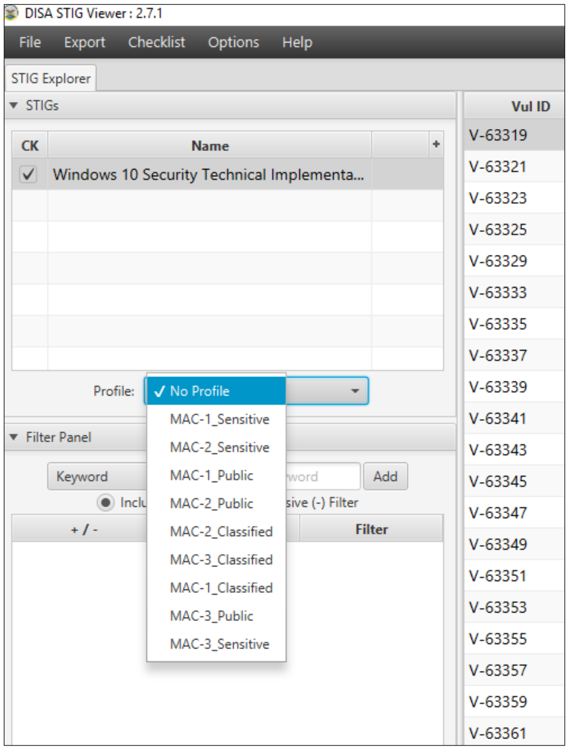
References

When there is more than one STIG loaded, you can right-click in the STIGs list to bring up the **Check All** option. This option is useful when doing a keyword search. Additionally, using the shortcut Ctrl+A highlights all the STIGs in the list.

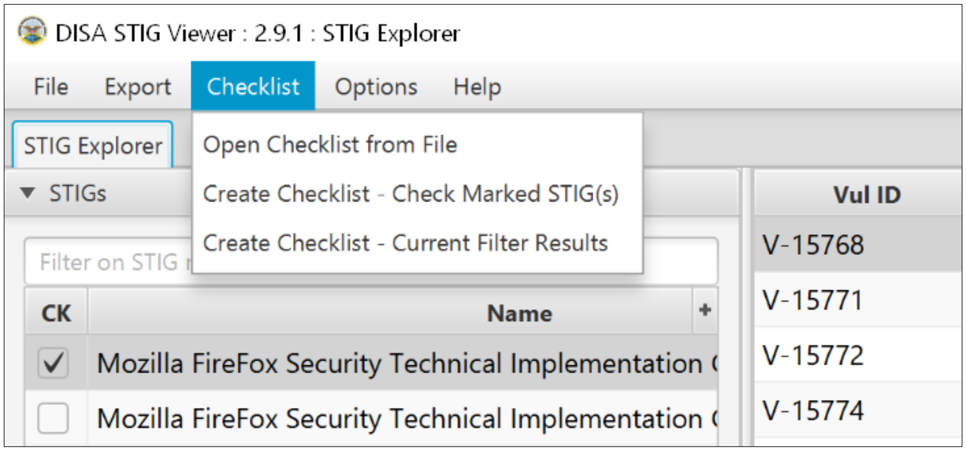
2.4 Create Checklist from STIG

1. Check the box next to the desired STIG(s).

2. Click the **Profile** drop-down menu and select MAC/Classification Level for the checklist and the asset under review.

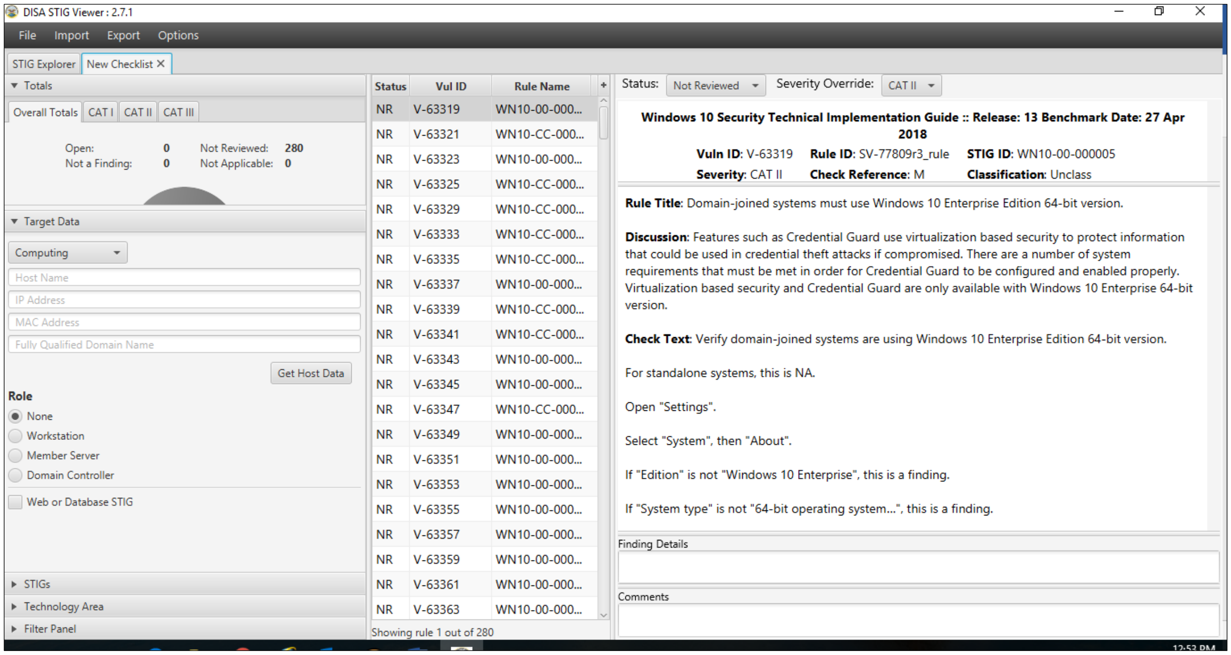


3. Click the menu item **Checklist** >> **Create Checklist – Check Marked STIG(s)**.


DISA STIG Viewer : 2.9.1 : STIG Explorer
File
Export
Checklist
Options
Help
STIG Explorer
Open Checklist from File
Create Checklist - Check Marked STIG(s)
Create Checklist - Current Filter Results
STIGs
Filter on STIG
CK
Name
☑ Mozilla FireFox Security Technical Implementation
□ Mozilla FireFox Security Technical Implementation
Vul ID
V-15768
V-15771
V-15772
V-15774

4. -OR- Create a checklist from filtered results by selecting **Checklist** >> **Create Checklist – Current Filter Results**.

5. A **Checklist** tab will open, with checklist information for the STIG selected.



Open: 0 Not Reviewed: 280
Not a Finding: 0 Not Applicable: 0

Status	Vul ID	Rule Name
NR	V-63319	WN10-00-000...
NR	V-63321	WN10-CC-000...
NR	V-63323	WN10-00-000...
NR	V-63325	WN10-CC-000...
NR	V-63329	WN10-CC-000...
NR	V-63333	WN10-CC-000...
NR	V-63335	WN10-CC-000...
NR	V-63337	WN10-00-000...
NR	V-63339	WN10-CC-000...
NR	V-63341	WN10-CC-000...
NR	V-63343	WN10-00-000...
NR	V-63345	WN10-00-000...
NR	V-63347	WN10-CC-000...
NR	V-63349	WN10-00-000...
NR	V-63351	WN10-00-000...
NR	V-63353	WN10-00-000...
NR	V-63355	WN10-00-000...
NR	V-63357	WN10-00-000...
NR	V-63359	WN10-00-000...
NR	V-63361	WN10-00-000...
NR	V-63363	WN10-00-000...

Showing rule 1 out of 280

Windows 10 Security Technical Implementation Guide :: Release: 13 Benchmark Date: 27 Apr 2018

Vuln ID: V-63319 **Rule ID**: SV-77809r3_rule **STIG ID**: WN10-00-000005
Severity: CAT II **Check Reference**: M **Classification**: Unclass

Rule Title: Domain-joined systems must use Windows 10 Enterprise Edition 64-bit version.

Discussion: Features such as Credential Guard use virtualization based security to protect information that could be used in credential theft attacks if compromised. There are a number of system requirements that must be met in order for Credential Guard to be configured and enabled properly. Virtualization based security and Credential Guard are only available with Windows 10 Enterprise 64-bit version.

Check Text: Verify domain-joined systems are using Windows 10 Enterprise Edition 64-bit version.

For standalone systems, this is NA.

Open "Settings".

Select "System", then "About".

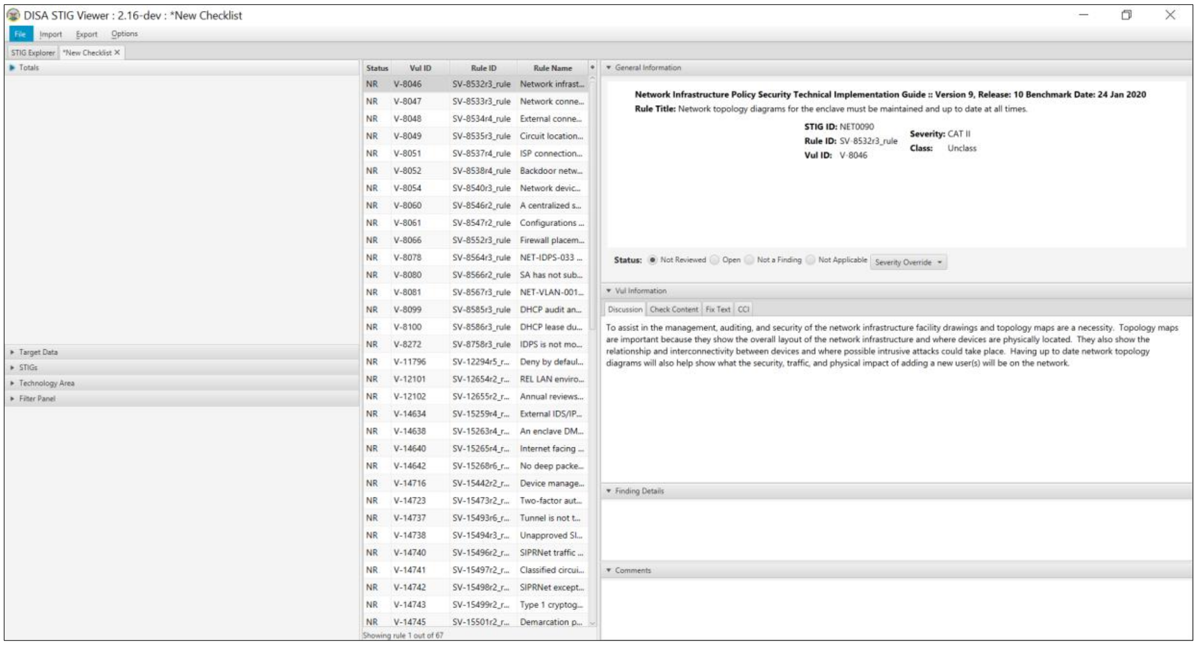
If "Edition" is not "Windows 10 Enterprise", this is a finding.

If "System type" is not "64-bit operating system...", this is a finding.

6. The **Checklist** tab columns are different from the **STIG** tab columns:

- Left column: Totals, Target Data, STIGs, Technology Area, and Filter Panel.
- Center column: Vulnerabilities in the checklist.
- Right column: General Information, Vuln Information, Finding Details, and Comments.

NOTE: These are tabs in the SV 2.x Classic Light visual style option under **Options** >> **Preferences** menu. To collapse the right column sections, change to the **Light theme** prior to creating the checklist. To view all sections, collapse some of them. The following shows a view with all sections collapsed:



Status	Vul ID	Rule ID	Rule Name
NR	V-8046	SV-8532r3_rule	Network infrast...
NR	V-8047	SV-8533r3_rule	Network conne...
NR	V-8048	SV-8534r4_rule	External conne...
NR	V-8049	SV-8535r3_rule	Circuit location...
NR	V-8051	SV-8537r4_rule	ISP connection...
NR	V-8052	SV-8538r4_rule	Backdoor netw...
NR	V-8054	SV-8540r3_rule	Network devic...
NR	V-8060	SV-8546r2_rule	A centralized s...
NR	V-8061	SV-8547r2_rule	Configurations ...
NR	V-8066	SV-8552r3_rule	Firewall placem...
NR	V-8078	SV-8564r3_rule	NET-IDPS-033 ...
NR	V-8080	SV-8566r2_rule	SA has not sub...
NR	V-8081	SV-8567r3_rule	NET-VLAN-001...
NR	V-8099	SV-8585r3_rule	DHCP audit an...
NR	V-8100	SV-8586r3_rule	DHCP lease du...
NR	V-8272	SV-8758r3_rule	IDPS is not mo...
NR	V-11796	SV-12294r5_r...	Deny by defaul...
NR	V-12101	SV-12654r2_r...	REL LAN enviro...
NR	V-12102	SV-12655r2_r...	Annual reviews...
NR	V-14634	SV-15259r4_r...	External IDS/IP...
NR	V-14638	SV-15263r4_r...	An enclave DM...
NR	V-14640	SV-15265r4_r...	Internet facing ...
NR	V-14642	SV-15268r6_r...	No deep packe...
NR	V-14716	SV-15442r2_r...	Device manage...
NR	V-14723	SV-15473r2_r...	Two-factor aut...
NR	V-14737	SV-15493r6_r...	Tunnel is not t...
NR	V-14738	SV-15494r3_r...	Unapproved SI...
NR	V-14740	SV-15496r2_r...	SIPRNet traffic ...
NR	V-14741	SV-15497r2_r...	Classified circui...
NR	V-14742	SV-15498r2_r...	SIPRNet except...
NR	V-14743	SV-15499r2_r...	Type 1 cryptog...
NR	V-14745	SV-15501r2_r...	Demarcation p...

Showing rule 1 out of 67

Network Infrastructure Policy Security Technical Implementation Guide :: Version 9, Release: 10 Benchmark Date: 24 Jan 2020
Rule Title: Network topology diagrams for the enclave must be maintained and up to date at all times.

STIG ID: NET0090
Rule ID: SV-8532r3_rule
Vul ID: V-8046
Severity: CAT II
Class: Unclass

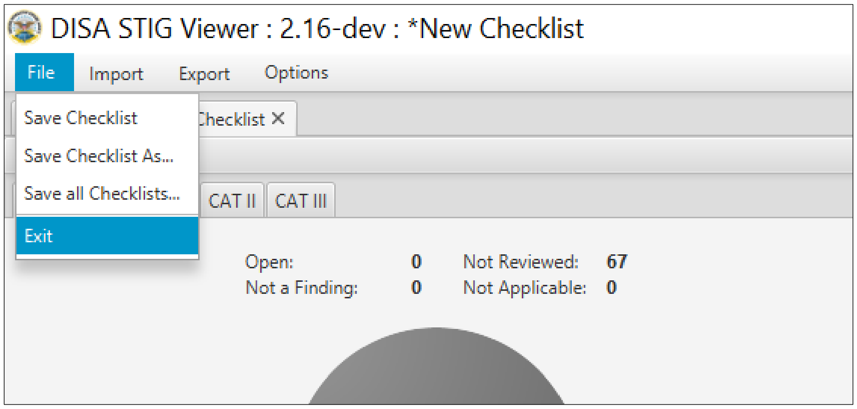
Status: ● Not Reviewed ○ Open ○ Not a Finding ○ Not Applicable Severity Override

To assist in the management, auditing, and security of the network infrastructure facility drawings and topology maps are a necessity. Topology maps are important because they show the overall layout of the network infrastructure and where devices are physically located. They also show the relationship and interconnectivity between devices and where possible intrusive attacks could take place. Having up to date network topology diagrams will also help show what the security, traffic, and physical impact of adding a new user(s) will be on the network.

2.5 Checklist Tab – Menu Selections

2.5.1 File Menu

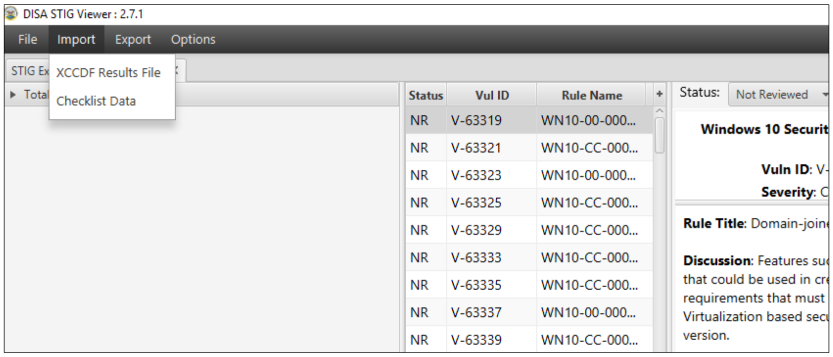
The **File** menu allows you to save the checklist, save the checklist with a new filename/location, or save all the checklists that are open.



Open: 0
Not a Finding: 0
Not Reviewed: 67
Not Applicable: 0

2.5.2 Import Menu

In the **Import** menu, the options allow you to import an **XCCDF Results file** or **Checklist Data**. The XCCDF Results file is a file with the extension of .xml that contains the results of a scan using a SCAP-compliant tool, such as the SCC tool (https://cyber.mil/stigs/scap/).



Status	Vul ID	Rule Name
NR	V-63319	WN10-00-000...
NR	V-63321	WN10-CC-000...
NR	V-63323	WN10-00-000...
NR	V-63325	WN10-CC-000...
NR	V-63329	WN10-CC-000...
NR	V-63333	WN10-CC-000...
NR	V-63335	WN10-CC-000...
NR	V-63337	WN10-00-000...
NR	V-63339	WN10-CC-000...

The **Import** menu includes the capability to import previously saved STIG Viewer Checklist files (.ckl). Results for recently updated rules will not be imported because their Rule IDs will have changed. **Preferences** allow for different rule matching behaviors.

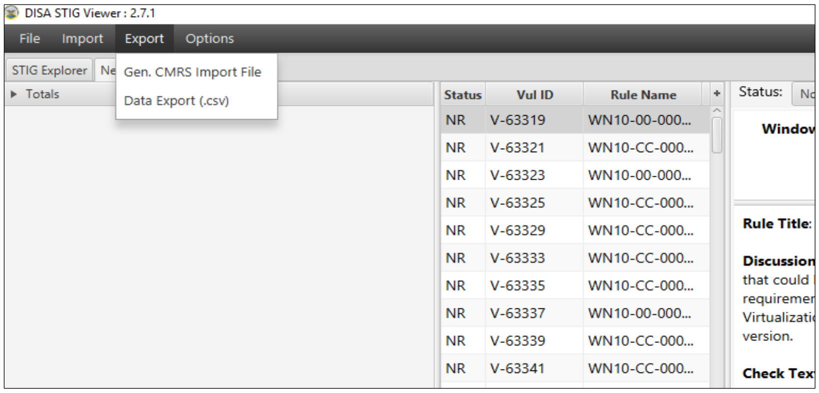
Once the import is complete, address the remaining Not Reviewed (NR) rules that are Manual checks. Be sure to set all items with **NR** status to their appropriate status to complete the Checklist.

2.5.2.1 Limitations

- Technology Area selections are **not** imported.
- Severity Overrides from STIG Viewer version 1.2 checklist files are **not** imported.

2.5.3 Export Menu

The **Export** menu provides the capability to export the checklist data to a general CMRS Import file for reporting. You can also export the checklist data to an Excel spreadsheet (.csv).



Status	Vul ID	Rule Name
NR	V-63319	WN10-00-000...
NR	V-63321	WN10-CC-000...
NR	V-63323	WN10-00-000...
NR	V-63325	WN10-CC-000...
NR	V-63329	WN10-CC-000...
NR	V-63333	WN10-CC-000...
NR	V-63335	WN10-CC-000...
NR	V-63337	WN10-00-000...
NR	V-63339	WN10-CC-000...
NR	V-63341	WN10-CC-000...

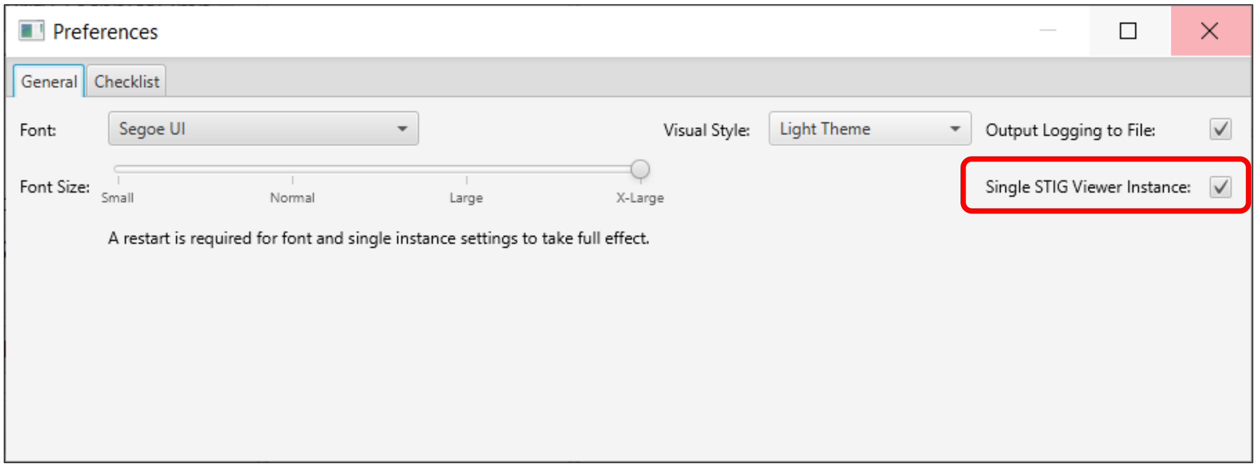
2.5.4 Options

The **Options** menu provides preferences for changing the font size, visual style, and checklist text colors. The visual style options include both Light and Dark themes, as well as the appearance of some sections for both the STIG and checklist.

2.5.4.1 General Preferences

2.5.4.1.1 Single STIG Viewer Instance

When enabled, STIG Viewer will only run a single instance per user. To run multiple instances of STIG Viewer, disable this setting.



Font: Segoe UI

Visual Style: Light Theme

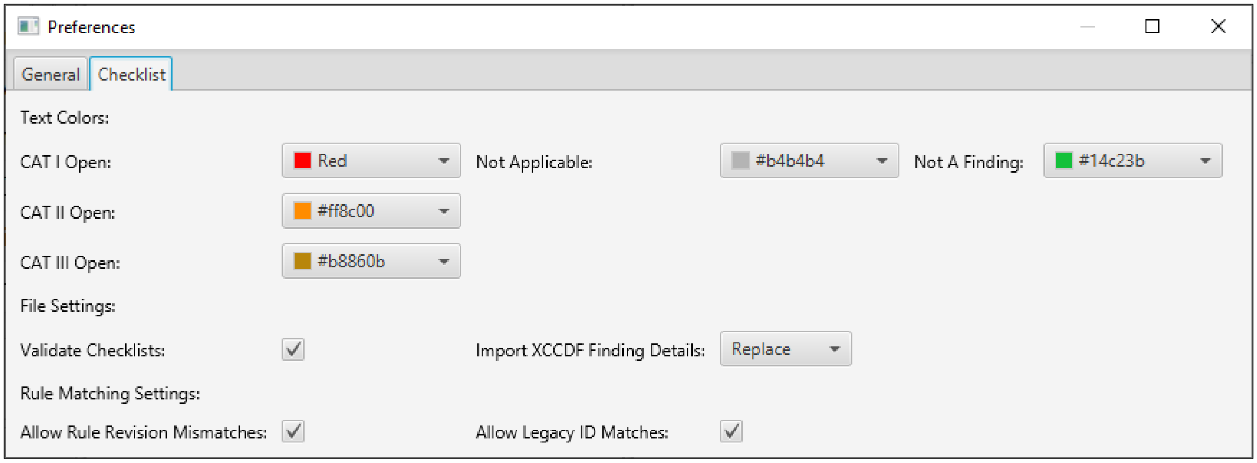
Output Logging to File: ☑

Font Size: X-Large

Single STIG Viewer Instance: ☑

A restart is required for font and single instance settings to take full effect.

2.5.4.2 Checklist Preferences



Text Colors:

CAT I Open: 🟥 Red

Not Applicable: #b4b4b4

Not A Finding: 🟩 #14c23b

CAT II Open: 🟧 #ff8c00

CAT III Open: #b8860b

File Settings:

Validate Checklists: ☑

Import XCCDF Finding Details: Replace

Rule Matching Settings:

Allow Rule Revision Mismatches: ☑

Allow Legacy ID Matches: ☑

2.5.4.2.1 Rule Matching Settings

The Rule Matching Settings change the behavior of rule matching performed during the import of XCCDF Results Files and Checklist Data.

2.5.4.2.2 Allow Rule Revision Mismatches

This setting ignores the revision component of Rule IDs. For example:

	Rule ID
STIG Document V2R1	SV-923456r100007_rule
STIG Document V2R2	SV-923456r113112_rule

With this setting enabled, these two Rule IDs will match on import.

For documents generated from DPMS 3.x, which released in October 2020, the revision number changes for each document release. This option allows for importing results from previous revisions against new revisions of the same document.

Caution: This option will match rules *even if the content of those rules has changed*. Consult the document's revision history to determine which rules have changed and may require reevaluation.

2.5.4.2.3 Allow Legacy ID Matches

This setting will match the imported Rule ID to the Legacy Rule ID in the Checklist.

Documents generated from DPMS 3.x, which was released in October 2020, have different Rule IDs than earlier versions of the same document. To allow mapping between old and new versions, Legacy IDs are published in the newer versions. This setting allows for matching against the Legacy Rule ID.

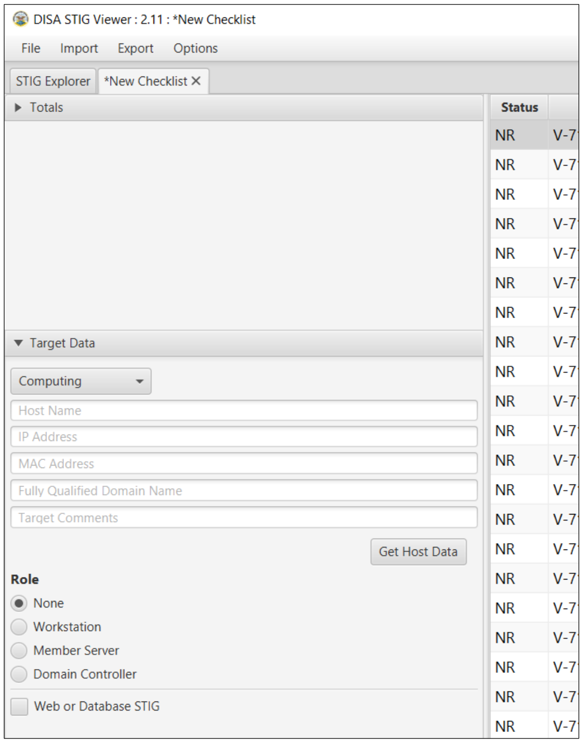
Caution: Legacy IDs do not map to specific revisions. This option will match rules *even if the content of those rules has changed*. Consult the document's revision history to determine which rules have changed and may require reevaluation.

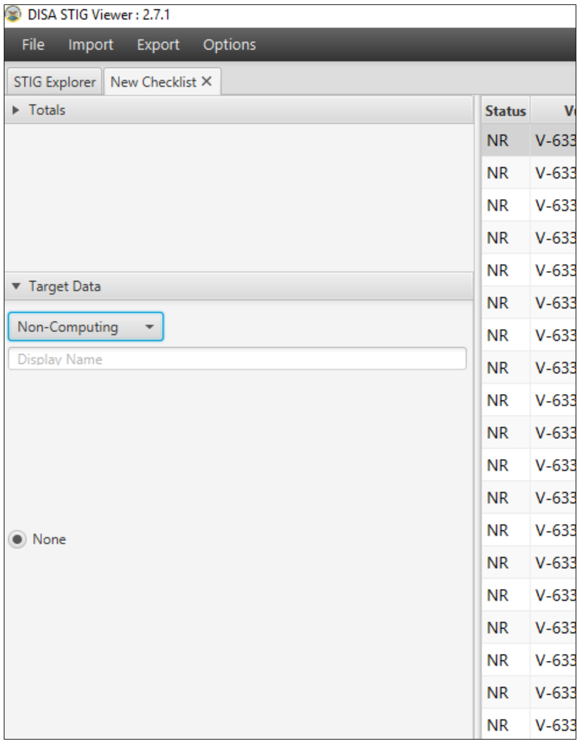
3. CHECKLIST SECTIONS

3.1 Checklist – Target Data Section

1. The Checklist **Target Data** section identifies the STIG asset. The drop-down button at the top can toggle between computing and non-computing. For computing asset, enter the Host Name, IP Address, and MAC Address of the asset under review. Comments can also be added for all assets under Target **Comments**. For non-computing asset, enter the name of asset only.

   NOTE: Do NOT click the Get Host Data button. That will only populate the Computing fields with information from the computer you are using.



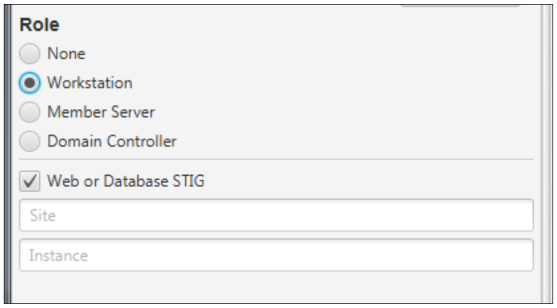


Non-Computing

● None

Status	V
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633
NR	V-633

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



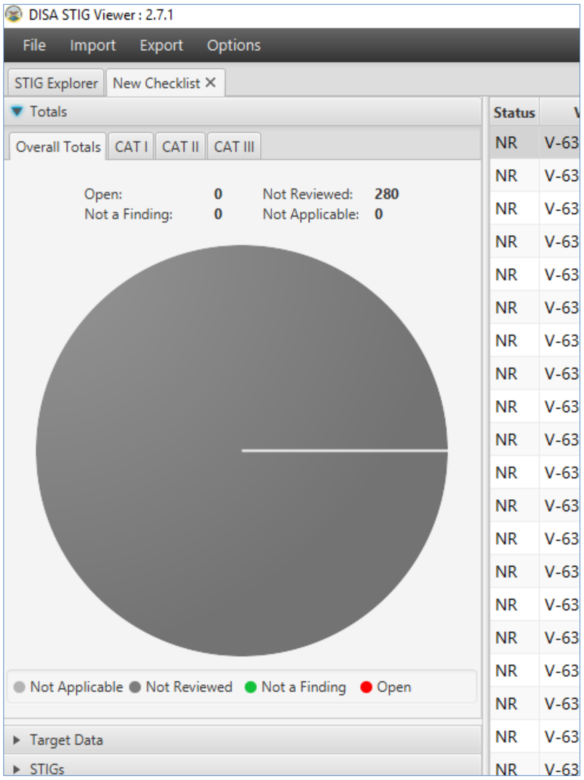
Role

○ None
● Workstation
○ Member Server
○ Domain Controller

☑ Web or Database STIG

3.2 Checklist – Totals Section

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

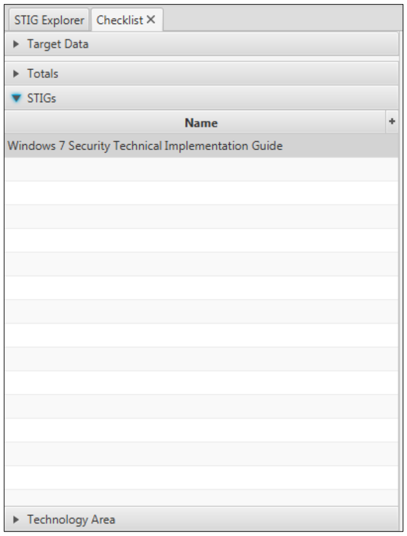


Open: 0 Not Reviewed: 280
Not a Finding: 0 Not Applicable: 0

Status	V
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63
NR	V-63

3.3 Checklist – STIGs Section

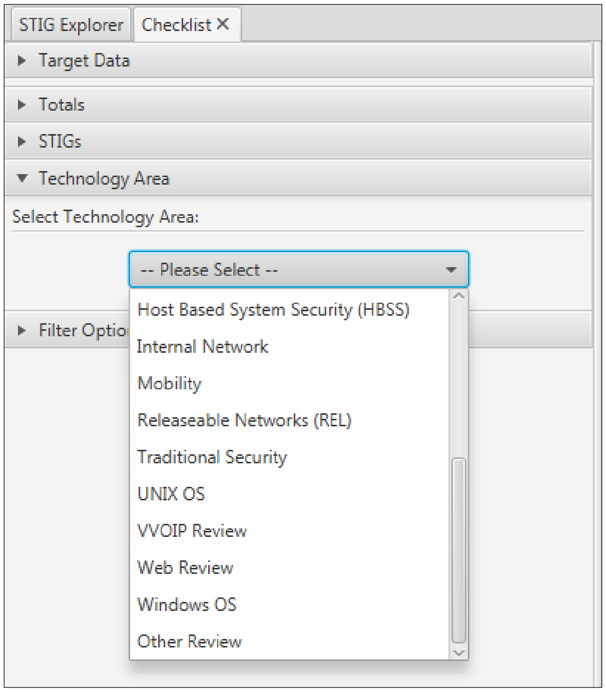
The **STIGs** section contains type of STIGs within this Checklist. A single Checklist tab may contain multiple STIGs.



Name
Windows 7 Security Technical Implementation Guide

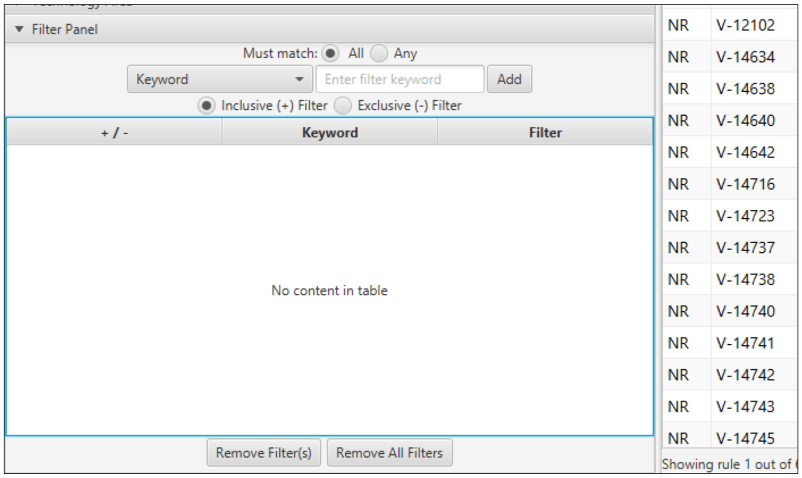
3.4 Checklist – Technology Area Section

The **Technology Area** section contains a drop-down list of technologies to select a specific technology for the asset under review.



3.5 Checklist – Filter Panel Section

The **Filter Panel** section allows you to filter the vulnerabilities by Keyword, Rule Title, STIG ID, Vulnerability ID, Rule ID, Severity, CCI, Legacy, or Status. Select the **Inclusive (+) Filter** or **Exclusive (-) Filter** radio button to find vulnerabilities that either meet or do not meet the criterion. Combine multiple filters by using the **Must match: All** or **Any** selection so that either all filters must match or any filters may match, respectively. To clear the filter, select either the **Remove Filter(s)** or **Remove All Filters** button.



Must match: ● All ○ Any

● Inclusive (+) Filter ○ Exclusive (-) Filter

+ / -	Keyword	Filter

No content in table

NR	V-12102
NR	V-14634
NR	V-14638
NR	V-14640
NR	V-14642
NR	V-14716
NR	V-14723
NR	V-14737
NR	V-14738
NR	V-14740
NR	V-14741
NR	V-14742
NR	V-14743
NR	V-14745

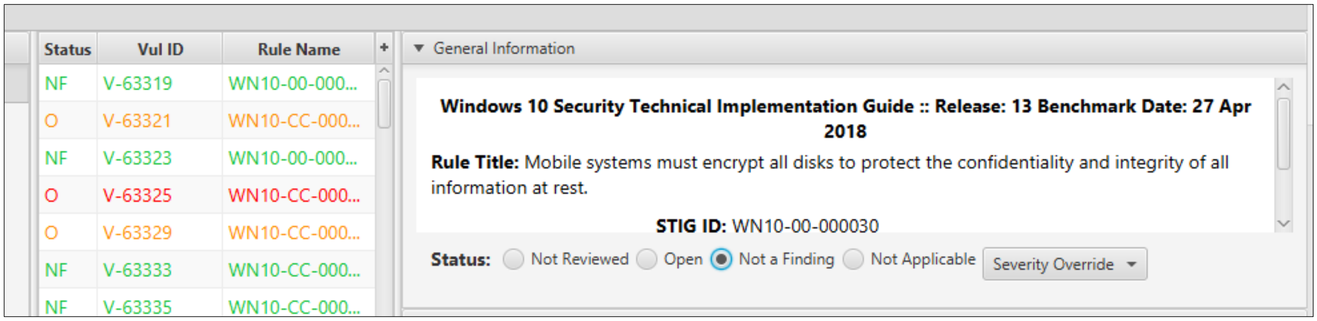
Showing rule 1 out of

3.6 Checklist – General Information Section

1. The **General Information** section displays in the right column for the Vulnerability selected in the center column.

2. Select the **Status** radio button to identify Vulnerability as **Open (O)**, **Not a Finding (NF)**, or **Not Applicable (NA)**. The Vulnerability text color will also change to reflect status.

3. Click the **Severity Override** drop-down menu when necessary to downgrade or upgrade status. A pop-up box will display to enter required justification text for override.



Status	Vul ID	Rule Name
NF	V-63319	WN10-00-000...
O	V-63321	WN10-CC-000...
NF	V-63323	WN10-00-000...
O	V-63325	WN10-CC-000...
O	V-63329	WN10-CC-000...
NF	V-63333	WN10-CC-000...
NF	V-63335	WN10-CC-000...

General Information

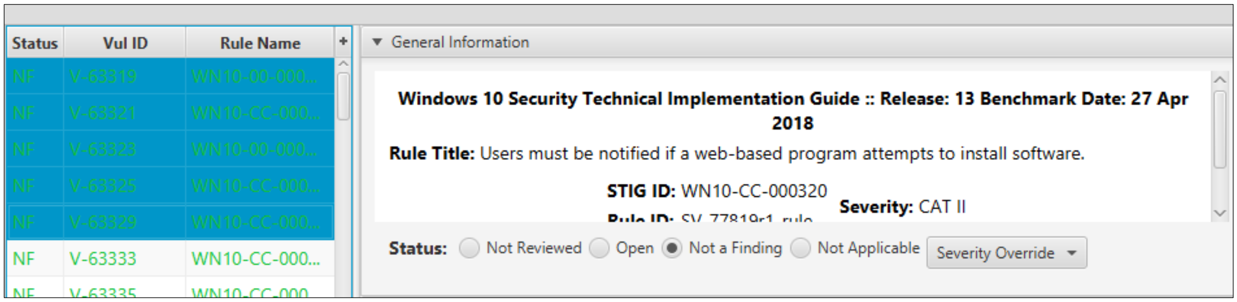
Windows 10 Security Technical Implementation Guide :: Release: 13 Benchmark Date: 27 Apr 2018

Rule Title: Mobile systems must encrypt all disks to protect the confidentiality and integrity of all information at rest.

STIG ID: WN10-00-000030

Status: ○ Not Reviewed ○ Open ● Not a Finding ○ Not Applicable Severity Override

4. To select multiple vulnerability checks, click on first selection and then shift-click on subsequent selections. Select all vulnerabilities using Ctrl+A or right-clicking and then selecting **Select All**.



Status	Vul ID	Rule Name
NF	V-63319	WN10-00-000...
NF	V-63321	WN10-CC-000...
NF	V-63323	WN10-00-000...
NF	V-63325	WN10-CC-000...
NF	V-63329	WN10-CC-000...
NF	V-63333	WN10-CC-000...
NF	V-63335	WN10-CC-000...

General Information

Windows 10 Security Technical Implementation Guide :: Release: 13 Benchmark Date: 27 Apr 2018

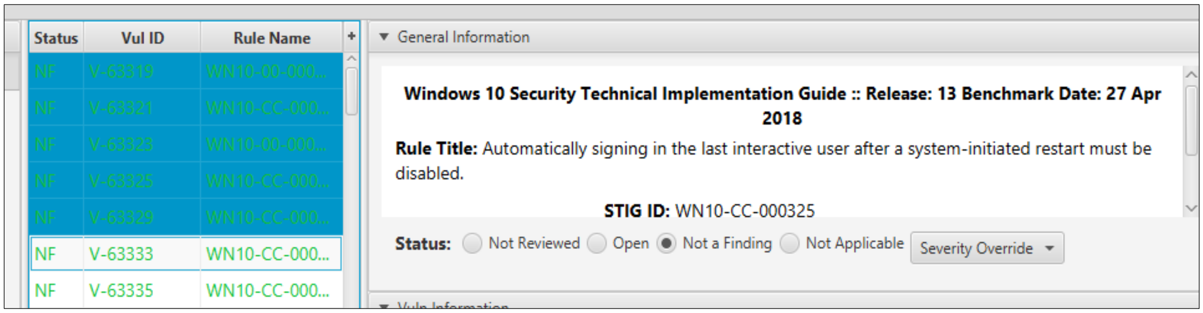
Rule Title: Users must be notified if a web-based program attempts to install software.

STIG ID: WN10-CC-000320 **Severity:** CAT II

Rule ID: SV-77819r1_rule

Status: ○ Not Reviewed ○ Open ● Not a Finding ○ Not Applicable Severity Override

5. Select the **Status** radio button or drop-down menu option you want to set for all selected checks.



Status	Vul ID	Rule Name
NF	V-63319	WN10-00-000...
NF	V-63321	WN10-CC-000...
NF	V-63323	WN10-00-000...
NF	V-63325	WN10-CC-000...
NF	V-63329	WN10-CC-000...
NF	V-63333	WN10-CC-000...
NF	V-63335	WN10-CC-000...

General Information

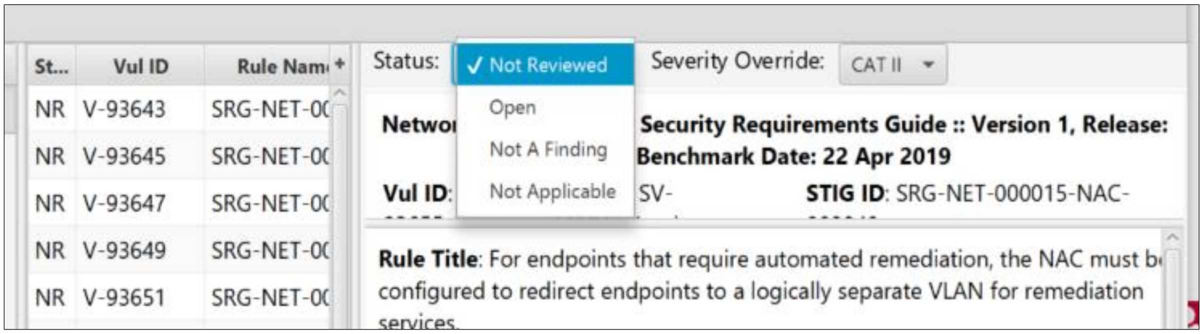
Windows 10 Security Technical Implementation Guide :: Release: 13 Benchmark Date: 27 Apr 2018

Rule Title: Automatically signing in the last interactive user after a system-initiated restart must be disabled.

STIG ID: WN10-CC-000325

Status: ○ Not Reviewed ○ Open ● Not a Finding ○ Not Applicable Severity Override

Vuln Information



St...	Vul ID	Rule Name
NR	V-93643	SRG-NET-0C
NR	V-93645	SRG-NET-0C
NR	V-93647	SRG-NET-0C
NR	V-93649	SRG-NET-0C
NR	V-93651	SRG-NET-0C

Status: ✓ Not Reviewed

Severity Override: CAT II

Netwo Security Requirements Guide :: Version 1, Release: Benchmark Date: 22 Apr 2019

Vul ID: SV- STIG ID: SRG-NET-000015-NAC-

Rule Title: For endpoints that require automated remediation, the NAC must be configured to redirect endpoints to a logically separate VLAN for remediation services.

6. In addition to the **Status** radio buttons (in SV 2.x Classic Light appearance) or **Status:** drop-down menu options (in Light Theme) for status selections for one or more checks, there are shortcut keys for each of the four statuses:

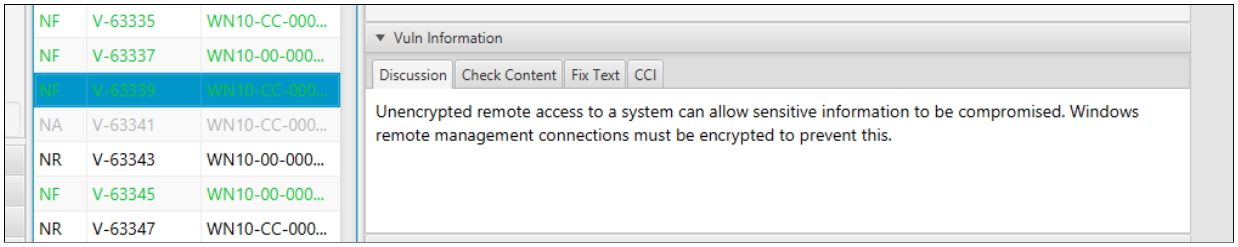
   - “R” or “r” marks the selected check(s) as “Not Reviewed”.
   - “O” or “o” marks the selected check(s) as “Open”.
   - “N” or “n” marks the selected check(s) as “Not a Finding”.
   - “X” or “x” marks the selected check(s) as “Not Applicable”.

3.7 Checklist – Vuln Information Section

The SV 2.x Classic styles’ **Vul Information** section contains five tabs relating to the Vulnerability selected in the center column (the Light and Dark theme styles do not contain these tabs). The style may be selected in **Options** >> **Preferences** (refer to section 2.5.4 Options).

The SV 2.x Classic tabs are:

- **Discussion** tab – A brief description of the check.

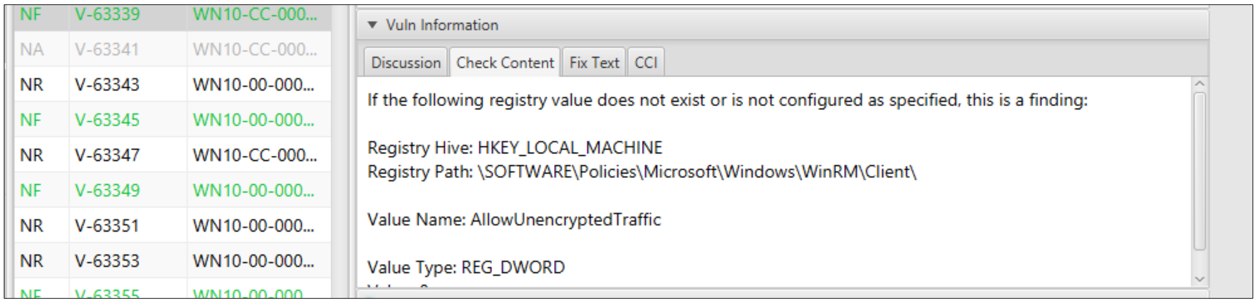


NF	V-63335	WN10-CC-000...
NF	V-63337	WN10-00-000...
NF	V-63339	WN10-CC-000...
NA	V-63341	WN10-CC-000...
NR	V-63343	WN10-00-000...
NF	V-63345	WN10-00-000...
NR	V-63347	WN10-CC-000...

▼ Vuln Information

Unencrypted remote access to a system can allow sensitive information to be compromised. Windows remote management connections must be encrypted to prevent this.

- **Check Content** tab – Describes how to conduct the check for review (automated benchmarks will not include this tab or any manual check instructions).



NF	V-63339	WN10-CC-000...
NA	V-63341	WN10-CC-000...
NR	V-63343	WN10-00-000...
NF	V-63345	WN10-00-000...
NR	V-63347	WN10-CC-000...
NF	V-63349	WN10-00-000...
NR	V-63351	WN10-00-000...
NR	V-63353	WN10-00-000...

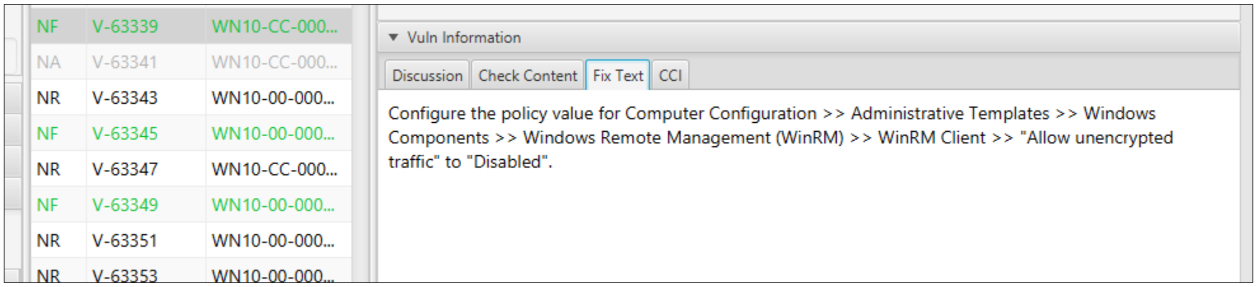
If the following registry value does not exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\WinRM\Client\

Value Name: AllowUnencryptedTraffic

Value Type: REG_DWORD

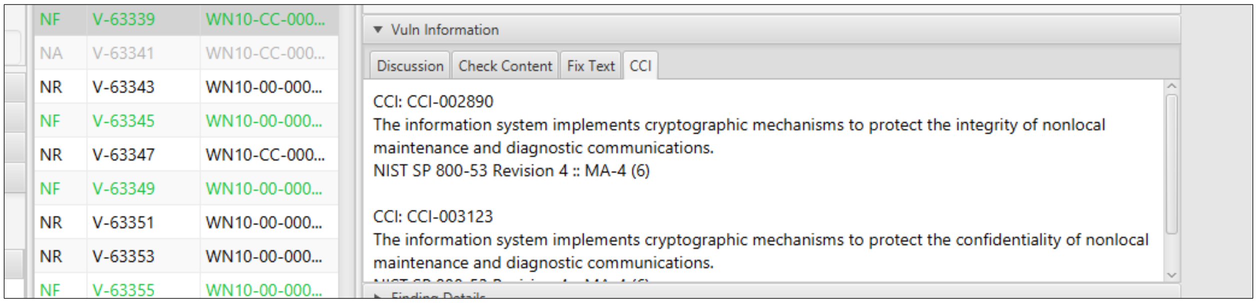
- **Fix Text** tab – Describes how to fix an Open finding for check.



NF	V-63339	WN10-CC-000...
NA	V-63341	WN10-CC-000...
NR	V-63343	WN10-00-000...
NF	V-63345	WN10-00-000...
NR	V-63347	WN10-CC-000...
NF	V-63349	WN10-00-000...
NR	V-63351	WN10-00-000...
NR	V-63353	WN10-00-000...

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Client >> "Allow unencrypted traffic" to "Disabled".

- **CCI** tab – Provides CCI information about check and the NIST SP 800-53 reference.

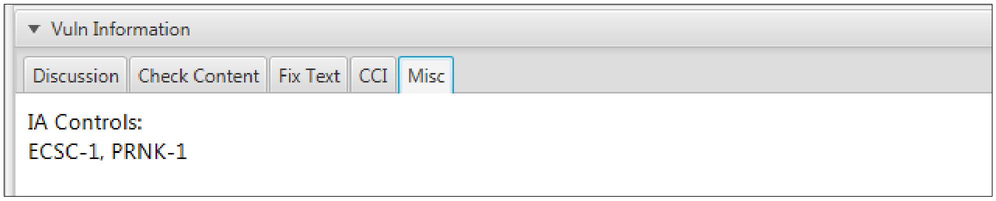


NF	V-63339	WN10-CC-000...
NA	V-63341	WN10-CC-000...
NR	V-63343	WN10-00-000...
NF	V-63345	WN10-00-000...
NR	V-63347	WN10-CC-000...
NF	V-63349	WN10-00-000...
NR	V-63351	WN10-00-000...
NR	V-63353	WN10-00-000...
NF	V-63355	WN10-00-000...

CCI: CCI-002890
The information system implements cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.
NIST SP 800-53 Revision 4 :: MA-4 (6)

CCI: CCI-003123
The information system implements cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.

- **Misc** tab – Provides IA Controls for the check (only appears if applicable).

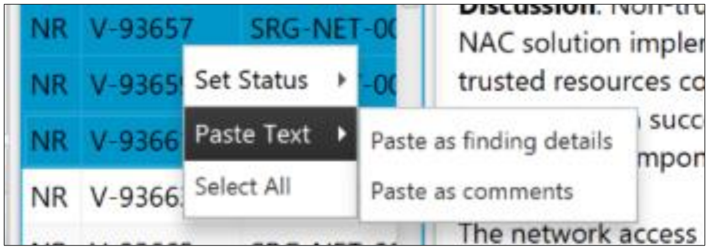


IA Controls:
ECSC-1, PRNK-1

3.8 Checklist – Finding Details Section and Comments Section

Use the **Finding Details** section and **Comments** section to record details and comments from the reviewer.

Paste **Finding Details** or **Comments** in bulk by right-clicking in the middle section and selecting **Paste Text** then select where to paste, either finding details or comments.


NR V-93657 SRG-NET-0(
NR V-9365
NR V-9366
NR V-9366.
Set Status
Paste Text
Select All
Paste as finding details
Paste as comments
NAC solution impler
trusted resources co
The network access