###### Evaluate-STIG Frequently Asked Questions and Issues

**Issue:**  
When trying to run Evaluate STIG, it will immediately fail and give ***Cannot index into a null array***

**Resolution:**  
Could be that one or more files have the blocked attribute set. Run [Test-Prerequisites.bat](#_Windows) to check if any files are blocked.

**Issue:**  
When trying to a remote scan using [-ComputerName](#_-ComputerName_<String>), file compression fails with ***Exception calling ".ctor" with "1" argument(s): "Stream was not readable."***

**Resolution:**  
This is typically antivirus interfering with the compression process.

**Issue:**  
No CKL files are produced.

**Resolution:**  
Ensure you are specifying what output you want Evaluate-STIG to produce with the [-Output](file:///C:\Users\daniel.ireland\OneDrive%20-%20US%20Navy-flankspeed\Documents\Evaluate-STIG\_Documentation\CKL#_-Output_<) parameter.

**Issue:**  
Remote scan fails to connect or does not return results

**Resolution:**  
Ensure WinRM is enabled that connections are not being blocked by a firewall. Test connectivity with the Enter-PSSession command. If connection with Enter-PSSession fails, this must be resolved before Evaluate-STIG can perform a remote scan.

**Resolution:**  
Execution policy and/or code signing certificate issues on remote host. Verify prerequisites are met on remotes.

**Resolution:**  
Check [remote logs](#_Remote_Scan) for clues.

**Issue:**  
PostgreSQL scan fails with ***Local trust authentication method must be set in <path>\pg\_hba.conf***

**Resolution:**  
A "host" or "local" configuration line must exist in pg\_hba.conf and be set to "trust" authentication. This configuration allows Evaluate-STIG to connect to the database without password prompting. After scanning the configuration line can be disabled (#) or removed.

#An example of local scanning:

local all all trust

host all all 127.0.0.1/32 trust

#To allow remote scanning:

host all all [ip-of-evaluate-stig-system] trust

host all all 192.168.0.123/32 trust

###### eMASSter Frequently Asked Questions and Issues

**Issue:**  
I cannot open eMASSter.

**Resolution:**  
ensure Microsoft office and .Net is installed on the machine. eMASSter only works on Windows-based Operating systems. If running from a DoD-based machine, be sure to run it from a share drive or OneDrive.

**Issue:**  
“File Processor Not Found” Error message.

**Resolution:**  
One or more of the files uploaded are either corrupt, or not formatted correctly. This often happens when user’s manipulate the defined templates/schemas. Be sure to only use the raw-exported files from eMASS, and do not alter the XML or JSON of test files manually.

**Issue:**  
The severity values in the poam for Nessus-based-entries does not match what is in the Nessus reports.

**Resolution:**  
eMASSter uses the STIG Severity value by default for Nessus entries. To use the default values, make sure to select the “ignore STIG Severity” checkbox in the Nessus Options panel.

**Question:**  
Where can I get the latest version of eMASSter?

**Answer:**  
The eMASSter Spork page will be the first place to access the latest version of eMASSter. Other sources are usually a week or two behind at most.

[https://spork.navsea.navy.mil/RMF-Automation/emasster](https://usg01.safelinks.protection.office365.us/?url=https%3A%2F%2Fspork.navsea.navy.mil%2FRMF-Automation%2Femasster&data=05%7C02%7Cdaniel.r.jermyn.civ%40us.navy.mil%7C6eed9177c24b4ce9affa08dc2c9f89b4%7Ce3333e00c8774b87b6ad45e942de1750%7C0%7C0%7C638434310928341146%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=sX5LFsGApl8Rkrd22J8kl%2Fvzh%2BLjgs0LigknNeDrrdw%3D&reserved=0)

**Question:**  
Where can I send bug reports and feature requests?

**Answer:**  
The “issues” section of eMASSter Spork page. Please be sure to upload all files used to the issue itself to assist the development team.

[https://spork.navsea.navy.mil/RMF-Automation/emasster](https://usg01.safelinks.protection.office365.us/?url=https%3A%2F%2Fspork.navsea.navy.mil%2FRMF-Automation%2Femasster&data=05%7C02%7Cdaniel.r.jermyn.civ%40us.navy.mil%7C6eed9177c24b4ce9affa08dc2c9f89b4%7Ce3333e00c8774b87b6ad45e942de1750%7C0%7C0%7C638434310928341146%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=sX5LFsGApl8Rkrd22J8kl%2Fvzh%2BLjgs0LigknNeDrrdw%3D&reserved=0)

**Additional eMASSter information:**   
eMASSter was developed by Daniel Jermyn at NSWC Panama City Division in 2020 as part of the NAVSEA RMF Automation efforts. He is still the current lead developer and project lead as of 28-MAY-2024. eMASSter has continuous funding, and is officially supported by NSWC HQ.

###### STIG Manager Frequently Asked Questions and Issues

**What is STIG Manager OSS?**

STIG Manager OSS is an Open Source API and Web client for managing the assessment of Information Systems for compliance with DISA STIGs or SRGs published in the XCCDF format.

STIG Manager helps users understand and collaborate on thousands of individual checklists by providing a centralized Web Application and API for managing Collections of Assets, their STIGs, and Reviews. Collections can be populated by importing checklist result files (.ckl/b, XCCDF) in bulk, Reviews edited and analyzed in the application, and then exported back out as checklist files for use in other tools. [Please see our User Guides and Documentation for more information on STIG Manager OSS features](https://stig-manager.readthedocs.io/).

STIG Manager OSS is being actively developed entirely in the open. All project materials are available publicly in the GitHub repository or linked to from there: <https://github.com/NUWCDIVNPT/stig-manager>

**How do I deploy STIG Manager OSS?**

STIG Manager is offered as a containerized NodeJS application that conforms with the Open Container Initiative (OCI) specification, though it can also be run from source code or binaries. [Deployment guidance is available in our Documentation.](https://stig-manager.readthedocs.io/en/latest/installation-and-setup/installation-and-setup.html)

STIG Manager requires a deployer-provisioned and maintained MySQL database, OIDC Provider, and in many cases a proxy to satisfy HTTPS requirements.

A sample docker-compose orchestration is offered on Docker Hub: <https://hub.docker.com/r/nuwcdivnpt/stig-manager>

A more complex STIG Manager orchestration demonstrating the use of a proxy and CAC login is available here: <https://github.com/NUWCDIVNPT/stigman-orchestration>

**How do I get started with STIG Manager OSS?**

The video guides and documentation below provide a good starting point for getting familiar with STIG Manager OSS:

* [STIG Manager YouTube Channel](https://www.youtube.com/@stig-manager)
* [STIG Manager Documentation](https://stig-manager.readthedocs.io/)

**How do I build a Collection with .ckl/b or XCCDF Files in STIG Manager OSS?**

Create your Collection (with the +Create Collection... node of the Nav Tree) and go to its Collection Management workspace by clicking the "gear" icon on the node for your Collection. You can also Manage your Collection by opening the main Collection Dashboard and clicking the "Manage" button in the Inventory block. From the Collection Management Workspace, select the "Import CKL/B or XCCDF..." button in the Asset Panel, then check out the [Collection Builder](https://stig-manager.readthedocs.io/en/latest/user-guide/user-guide.html#collection-builder) portion of our User Guide for more info.

**How do I Review a STIG on an Asset?**

Many STIGs do not have automated evaluations, and even after automated results are imported, many Rules may still require additional manual Evaluation. The Asset Review Workspace in STIG Manager provides a comprehensive environment for Users to complete Evaluations of a specific STIG on an Asset, and set statuses that can be used to gauge progress.

Use the [Asset Review Workspace](https://stig-manager.readthedocs.io/en/latest/user-guide/user-guide.html#asset-review-workspace) to manually review individual STIG Rules, import results from .ckl or XCCDF files, compare Reviews to other Assets in the Collection, and to see a History of Reviews for that Asset.

**How do I Review an entire Collection at once?**

Many Collections will contain Assets that are assigned the same STIG. The Collection Review Workspace allows Evaluators and Validators to step through each Rule in the STIG and view each Asset's Review and Status in one place. Restricted Users will only see the Assets they have been assigned, while Users with higher grants to the Collection will see every Asset. Comments, Evaluations, and Statuses can all be edited via this interface, which also offers bulk actions for Submitting and Accepting Reviews. This interface also provides an export option that will produce a .zip archive of .ckls representing the state of every Asset in the Collection that has this STIG.

See the User Guide's section on the [Collection Review Workspace](https://stig-manager.readthedocs.io/en/latest/user-guide/user-guide.html#collection-review-workspace) for more information.

**How do I update the DISA Reference STIGs in STIG Manager OSS?**

STIG Manager bases all calculations and checklist data (except Reviews) using the Reference STIGs published by DISA. These STIGs must be updated in cadence with DISA to ensure that the most recent security requirements are being applied to your Assets. Most STIG updates only change a small fraction of the Rules therein. STIG Manager tracks reviews using the Rule Version and Rule Check Content, so in most cases a completely reviewed Asset with a new STIG will still have most of the Reviews already populated and in the same state they were in before the update.

Download the new STIGs from DISA, and upload the STIGs you want to update using the [STIGS Import interface.](https://stig-manager.readthedocs.io/en/latest/admin-guide/admin-quickstart.html#stig-updates)

**I have other questions about using STIG Manager OSS!**

Check out the [Common Tasks](https://stig-manager.readthedocs.io/en/latest/features/common-tasks.html) section of our User Guide for more information on how to use STIG Manager OSS.

**How do I report a bug or request new features for STIG Manager OSS?**

Bugs Reports and Feature Requests should be submitted by creating an issue in the project repository on GitHub: <https://github.com/NUWCDIVNPT/stig-manager/issues>