Evaluate STIG

Setup Evaluate-STIG Output to STIG-Manager

- Setup Evaluate-STIG Output to STIG-Manager
  - PREAMBLE
  - Create Keycloak Client
  - Configure the Keycloak Client
    - Service Account Roles
    - Client Scopes
    - Credentials
    - Keys
  - Evaluate-STIG Output
    - OpenSSL setup
    - Extract Certificate & Key
    - Pre-register Keycloak Client in STIG-Manager
    - Preferences.xml
      - Note about paths in Preferences.xml
  - Running Evaluate-STIG
  - Credits

PREAMBLE

- This guide's purpose is to assist with properly configuring **Keycloak** when using the **STIGManager** output option in **Evaluate-STIG**.
- This guide assumes that **Keycloak** and **STIG-Manager** are already deployed and configured.
- This guide was written utilizing the following software versions:

Software	Version
Keycloak	24.0.3
Evaluate-STIG	1.2401.3
STIG-Manager	1.4.6

Create Keycloak Client

- Login to **Keycloak** as an administrator.
- Change the **Realm** drop-down to the **STIG Manager realm**.
- From the realm management pane on the left, select **Clients**.
- Click the **Create client** button.
- Set the **Client type** to **OpenID Connect**.
- Set the **Client ID** to **evaluatestig** *(or whatever you would like)*.
- Click **Next**.
- **Enable** the **Client Authentication** switch.
- Leave the **Authorization** switch **disabled**.
- **Uncheck** all authentication flows.
- **Check** the box for Service account roles.
- Click **Next**.
- Leave **Root URL** and **Home URL** empty.
- Click **Save**.

Configure the Keycloak Client

Service Account Roles

- From the **evaluatestig Client details** window, select the **Service account roles** tab.
- Click the **Assign Role** button.
- Check the box for the **user** role.
- Click the **Assign** button.

Client Scopes

- Next, from the **Client scopes** tab, click the button **Add client scope**.
- Add the following client scopes:

Client Scope	Type	Notes
stig-manager:collection	Default	Created during STIG-Manager initial deployment. See here
stig-manager:stig:read	Default	Created during STIG-Manager initial deployment.
stig-manager:user	Default	Created during STIG-Manager initial deployment.

Credentials

- Select the **Credentials** tab.
- For **Client Authenticator** select **Signed JWT**.
- For **Signature algorithm** select **Any algorithm**.
- Click **Save**.
- A prompt may appear confirming **Change to client-jwt?** Select **Yes**.

Keys

- Select the **Keys** tab.
- Leave the **Use JWKS URL** switch set to **disabled**.
- Click the **Generate new keys** button.
- Select **PKCS12** for the **Archive format**.
- Set **Key alias** to **evaluatestig**.
- Set **Key password**. *This password will be required in a later step.*
- Set **Store password**. *This password will be required in a later step.*
- From **Import file**, click the **Browse...** button.
- Click the **Generate** button.
- **Save** the **keystore.p12** file.

Evaluate-STIG Output

OpenSSL setup

- **OpenSSL** is required to extract the **key** and **certificates** from the previously downloaded **keystore.p12** file.
- For **Linux**, just install OpenSSL from distribution's package manager *(i.e., Debian/Ubuntu = **apt**, RHEL/CentOS/Rocky/Oracle Linux = **dnf**)*.
- For **Windows**, the easiest way is to download the portable version of Git for Windows.
  - Launch **git-bash.exe**, navigate to **usr/bin** and run **openssl.exe** from there.
    - It is highly recommended to copy the **keystore.p12** to the same directory where **OpenSSL** is located. This will ease the extraction process.

Extract Certificate & Key

- Run the following command to extract the certificates into a PEM file.

```
openssl pkcs12 -nokeys -in <PATH_TO_keystore.p12> -out cert.pem -legacy
```

- Run the following command to extract the private key into an encrypted PEM file.

```
openssl pkcs12 -nocerts -in <PATH_TO_keystore.p12> -out key.pem -legacy
```

- Now move the **keystore.p12**, **cert.pem** and **key.pem** files to the **Evaluate-STIG\Prerequisites\Certificates** directory.

Pre-register Keycloak Client in STIG-Manager

- Sign-in to **STIG-Manager** as an administrator.
- From the navigation pane on the left, expand **Application Management** then select **User Grants**.
- On the **User Grants** window, click the **Pre-register User** button.
- In the **Username** field enter the **Client ID** created in Keycloak previously.
- Now click the **New Grant** button.
- Set the **Collection** drop-down to the collection that you would like Evaluate-STIG to output results to.
- Set the **Access Level** drop-down to **Manage**.
- Click the **Save** button.

Preferences.xml

Note about paths in Preferences.xml

- The Evaluate-STIG instructions state that the certificate/key file(s) should be located in the **./Evaluate-STIG/Prerequisites/Certificates** directory and you should only need to specify the **filename** for said files in the **Preferences.xml** file. However, I have only had success with specifying the **absolute path** of the certificate and key files in the **Preferences.xml**. If you receive an error stating *file not found* for the certificate, specify the **absolute path** to the files in the **Preferences.xml**.

- The **Preferences.xml** file can contain multiple **SMImport_COLLECTION** sections. So long, as the required settings are provided *(See section **3.6** of the Evaluate-STIG user guide)*. You will specify which collection to output to when running **Evaluate-STIG**. See below example.

```
<STIGManager>
  <SMImport_API_BASE>https://my.stig.manager.mil/api</SMImport_API_BASE>
  <SMImport_AUTHORITY>https://my.stig.manager.mil/kc/realms/stigman</SMImport_AUTHORITY>
  <SMImport_COLLECTION Name="Collection_1">
    <SMImport_CLIENT_ID>evaluatestig</SMImport_CLIENT_ID>
    <SMImport_CLIENT_CERT>cert.pem</SMImport_CLIENT_CERT>
    <SMImport_CLIENT_CERT_KEY>key.pem</SMImport_CLIENT_CERT_KEY>
    <SMImport_COLLECTION_ID>1</SMImport_COLLECTION_ID>
  </SMImport_COLLECTION>
  <SMImport_COLLECTION Name="Collection_2">
    <SMImport_CLIENT_ID>evaluatestig</SMImport_CLIENT_ID>
    <SMImport_CLIENT_CERT>cert.pem</SMImport_CLIENT_CERT>
    <SMImport_CLIENT_CERT_KEY>key.pem</SMImport_CLIENT_CERT_KEY>
    <SMImport_COLLECTION_ID>2</SMImport_COLLECTION_ID>
  </SMImport_COLLECTION>
  <SMImport_COLLECTION Name="Collection_3">
    <SMImport_CLIENT_ID>evaluatestig</SMImport_CLIENT_ID>
    <SMImport_CLIENT_CERT>cert.pem</SMImport_CLIENT_CERT>
    <SMImport_CLIENT_CERT_KEY>key.pem</SMImport_CLIENT_CERT_KEY>
    <SMImport_COLLECTION_ID>3</SMImport_COLLECTION_ID>
  </SMImport_COLLECTION>
</STIGManager>
```

- Edit the **./Evaluate-STIG/Preferences.xml** file and specify the following settings:
  - *These instructions can also be found in section **3.6** of the Evaluate-STIG user guide.*

Key	Setting
SMImport_API_Base	**STIG-MANAGER URL**/api
SMImport_Authority	**Keycloak URL**/realms/**STIG-Manager Realm ID** (e.g., /realms/stigman)
SMImport_Collection	Name of the STIG-Manager collection to output results to.
SMImport_CLIENT_ID	Name of the Keycloak client ID for Evaluate-STIG that was set.
SMImport_CLIENT_CERT	Location of the **cert.pem** file
SMImport_CLIENT_CERT_KEY	Specify the location of the **key.pem** file
SMImport_COLLECTION_ID	This ID is obtained from STIG-Manager by clicking the gear icon to the right of the collection name. This will bring up the settings for the collection. Look for a number in parentheses next to **Manage Collection**. That number is the Collection ID

Running Evaluate-STIG

- Reference section **3.9** of the **Evaluate-STIG user guide** for more information on running Evaluate-STIG with output to STIG-Manager.
- A simple example of running **Evaluate-STIG** and outputting the results to **STIG-Manager** would look like this:

```
Evaluate-STIG.ps1 -Output STIGManager -SMCollection Collection_1 -SMPassphrase (private key passphrase)
```

Credits

- Author: Chris Roberts, ISSE, 39th IOS/DOS
- All of the developers @ NSWC Crane Division that created and maintain Evaluate-STIG.
- All of the developers @ NUWC Newport Division that created and maintain STIG-Manager.