**Test Ingest Repository (TIR) Privileged User Guide**

# Purpose

The purpose of this document is to provide a guide for Administrative functions for Test Ingest Repository (TIR). TIR is a MITRE Security Assessment Framework (SAF) tool that is used to support boundary and software compliance and continuous monitoring.

TIR Administrators only have access to certain features in the software. Administrators can configure TIR, and change permissions on Companies and Boundaries. Administrators cannot edit boundary details. This helps maintain required separation of roles and responsibilities within the TIR.

# Account Permissions

TIR has two types of users, Administrators and Users. Administrators have access to the **Administration,** **Libraries**, and **Boundary** tabs. Users only have access to Libraries and Boundary tabs. TIR is setup as a hierarchical system with Companies and Boundaries. Users can be granted permissions to be Owners, Reviewers, and Editors for Companies and Boundaries. A summary of permissions is show in Table 1, below.

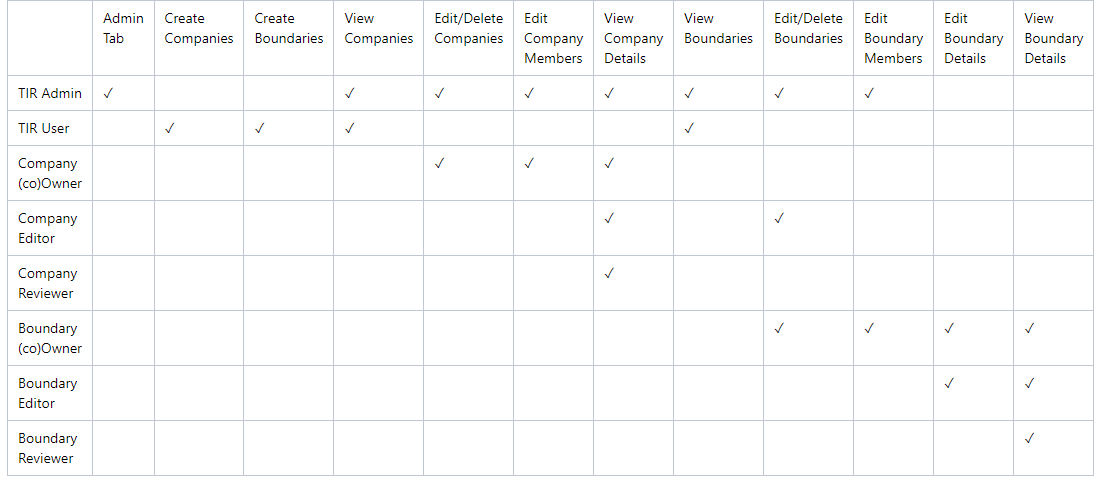


Table 1: Access Control – User Permissions

# Configuration

## Administrator Login

The default Local Administrator Username is admin@tir.local. The initial password will be provided. Enter your admin@tir.local and the initial **Password**, then review the **IS User Agreement** and acknowledge that you have read it by clicking the check box. Then, click **Sign in**.

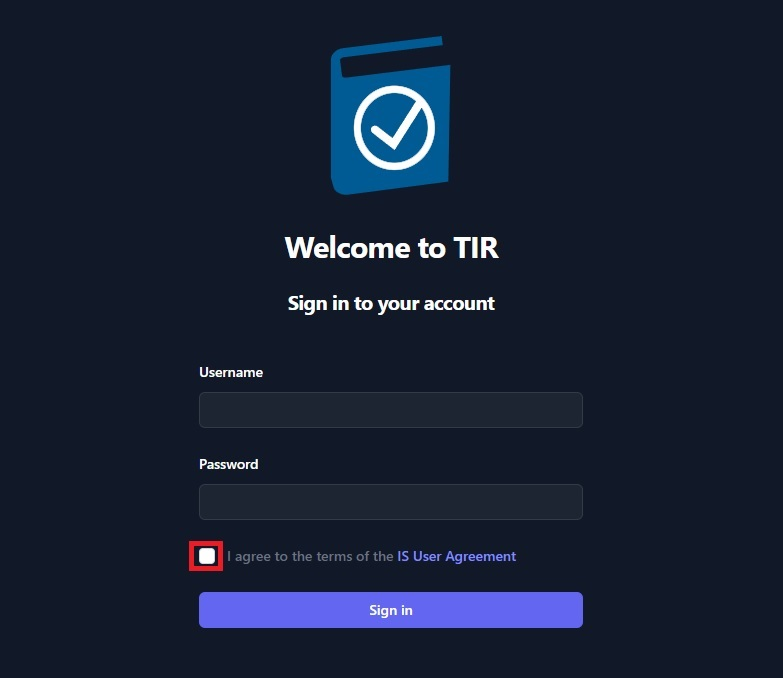


Figure 1: Login Page

* After successfully logging in for the first time, please change the TIR Admin password by completing the following:
* Click the Profile Icon in the upper right corner of the welcome screen.

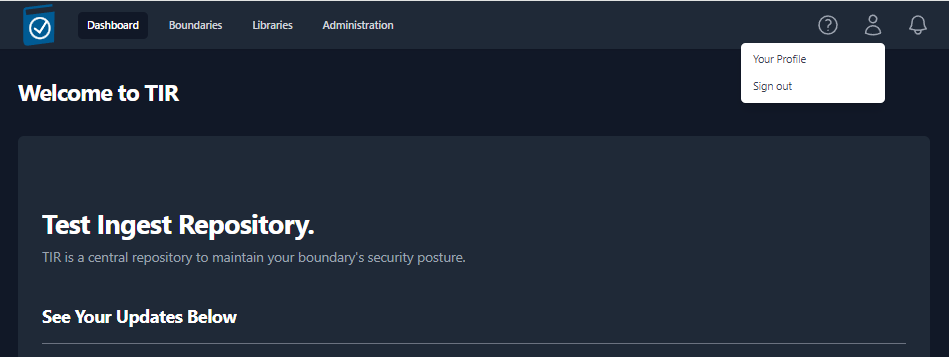


Figure 2: Selecting Your Profile

* Click Your **Profile** to bring up the TIR Admin profile.

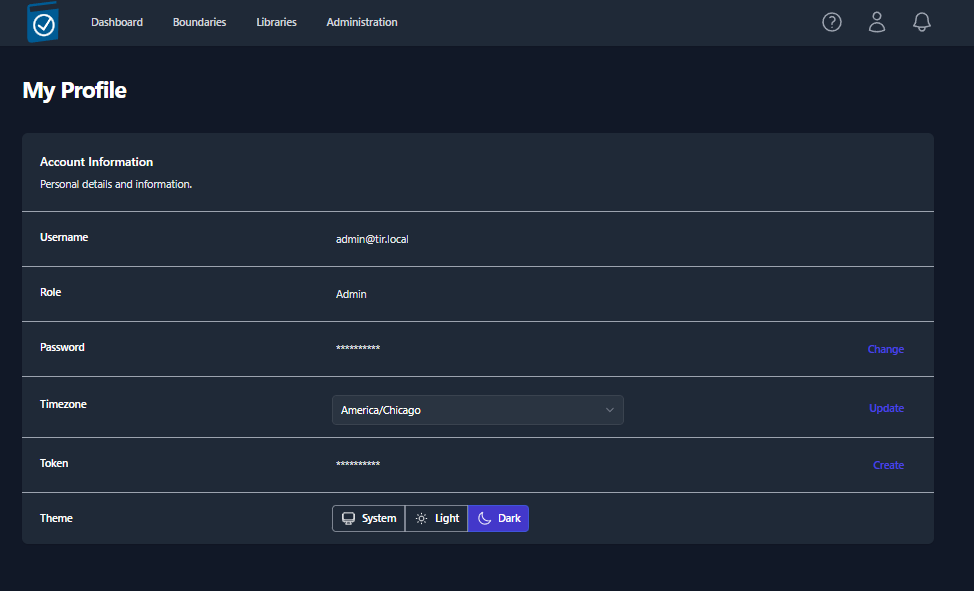


Figure 3 Changing The Local Admin Password

* In the **Password** row select **Change**

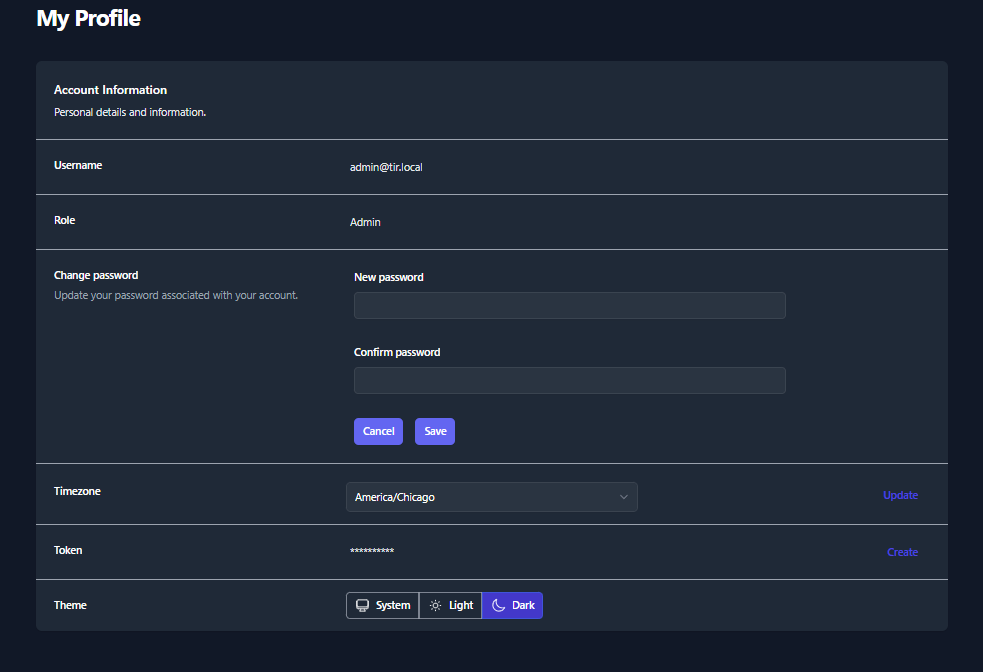


Figure 4: Changing the Local Admin Password

* Enter **New password**
* Enter **Confirm password**
* Select Save

## Administrative Functions

The TIR Local Administrator account is allowed to perform a number of configuration tasks, like creating local accounts, setting up LDAP, uploading certificates, and configurating centralized Logging. These functions are executed in the **Administration** Tab.

* + 1. **The Administration Tab**

The **Administration** tab is only available through Administrators. You access the **Administration** tab by selecting **Administration** at the top center of the web interface.

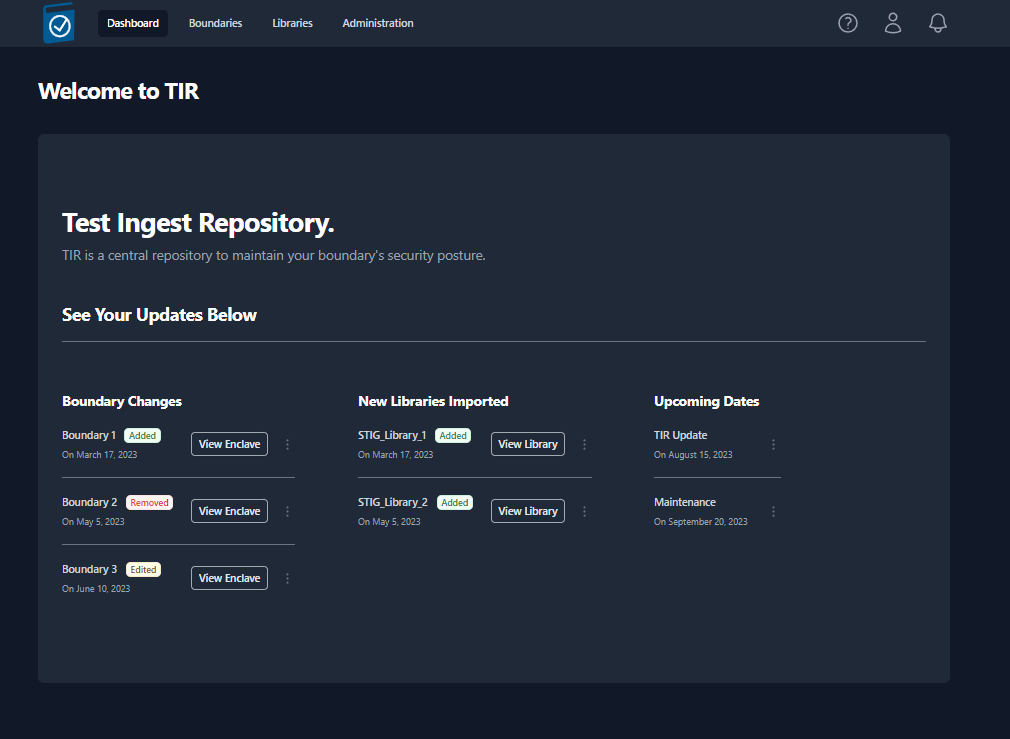


Figure 5: Location of the Administration Tab

The four major **Administration** tab functions are configuration, Notifications, Users, and Logs.

A view of the **Administration** tab is below:

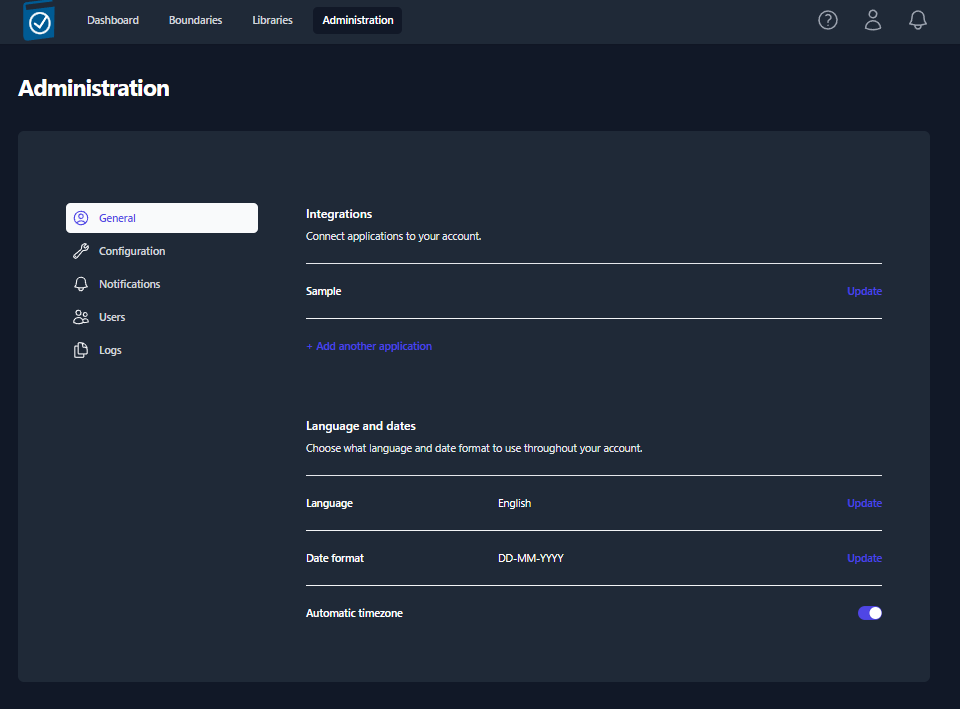


Figure 6: Administration Tab

#### Configuring LDAP

LDAP is configured during TIR deployment. Please see the TIR Deployment Guide for LDAP configuration procedures.

#### Configuration

Within the **Configuration** section an Administrator can change standard **Terminology** and import a **CA Certificate.**

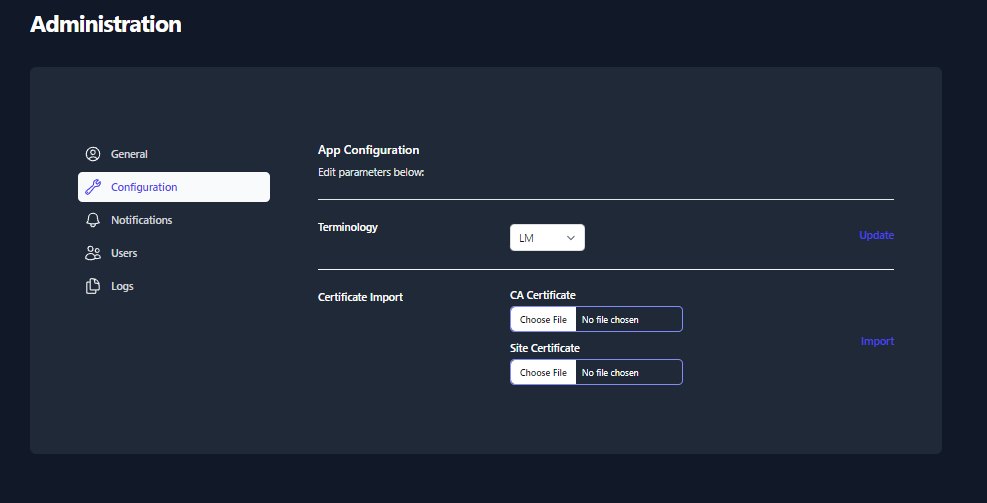


Figure 7: Configuration Functions

##### Certificate Import and Verification

* Click on the **CA Certificate** **Choose File** box to open a File dialog window and choose your signed x509 formatted .crt file and hit **Open** - the name of the file will appear in the **CA Certificate** Text Box

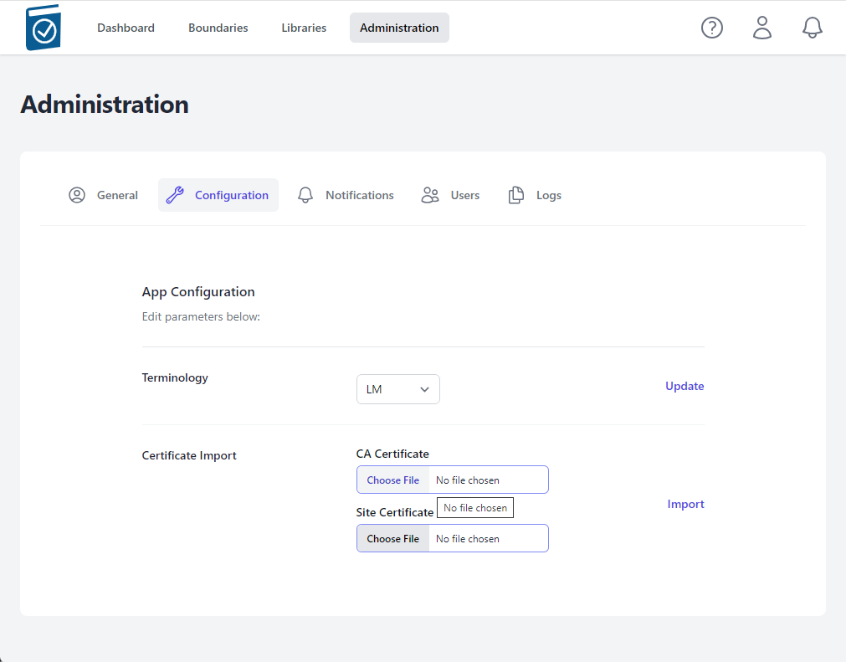


Figure 8: Import Certificates

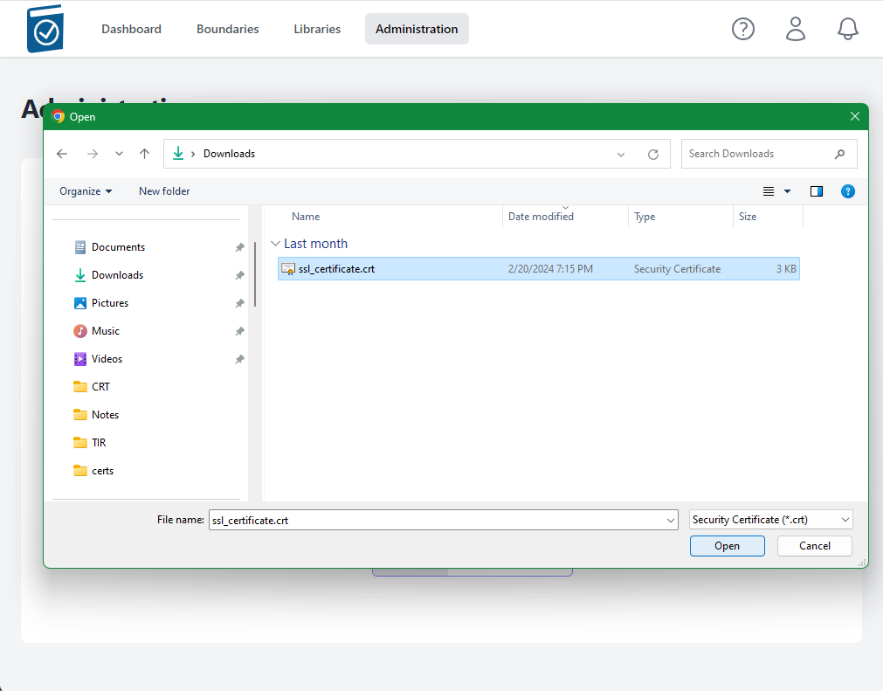


Figure 9: Choosing Certificate

* Note name of .crt file shows up in text field.

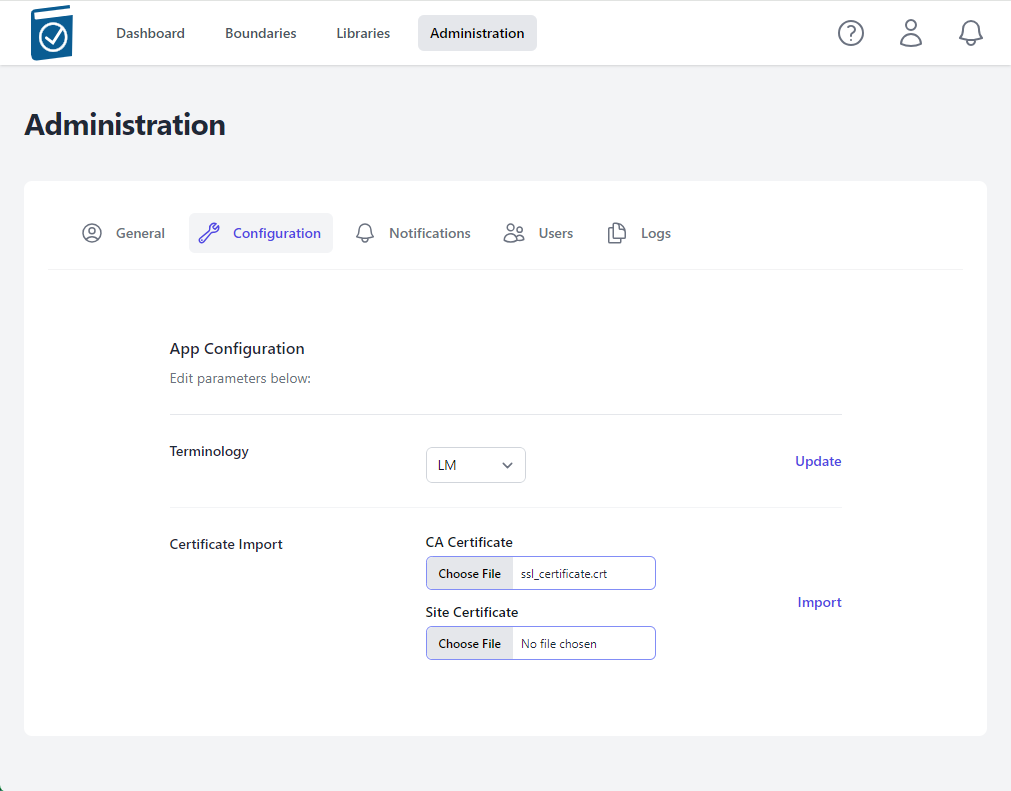


Figure 10: CA Certificate Updated

* Click on the **Site Certificate** Choose File box to open a File dialog window and choose your .pem formatted site key and hit Open - the name of the file will appear in the Site Certificate Text Box

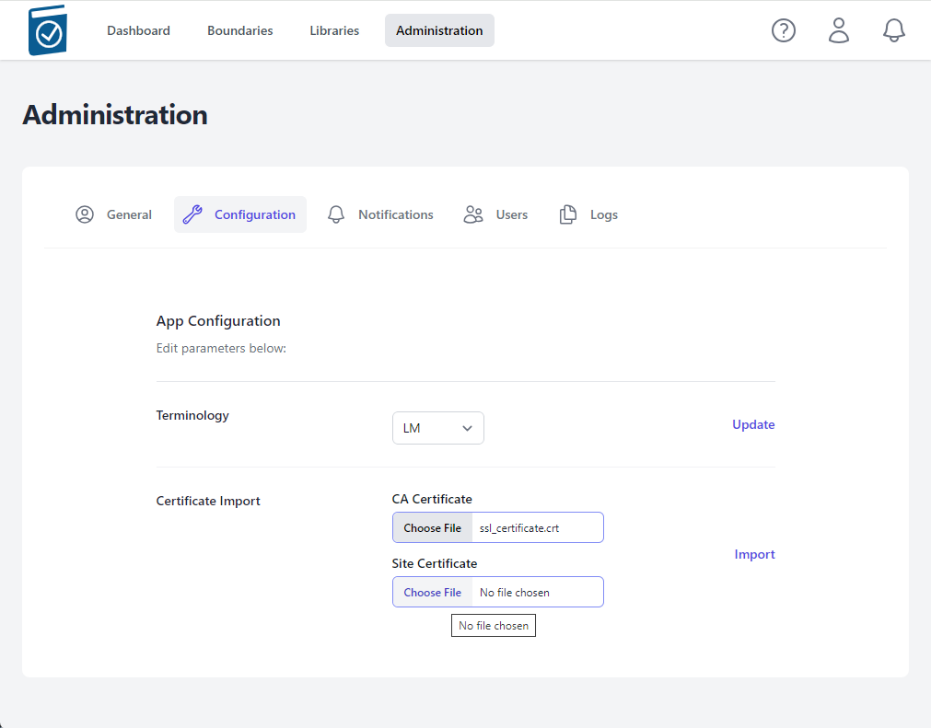


Figure 11: Choose Site Certificate

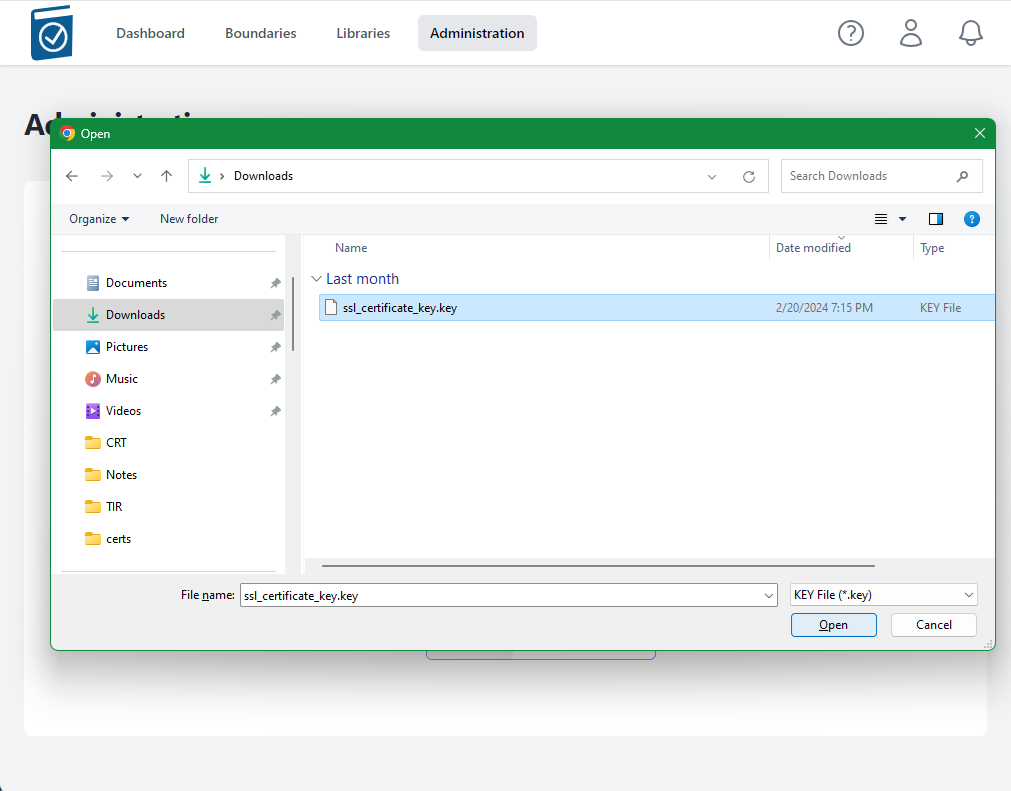


Figure 12: Select Site Certificate File

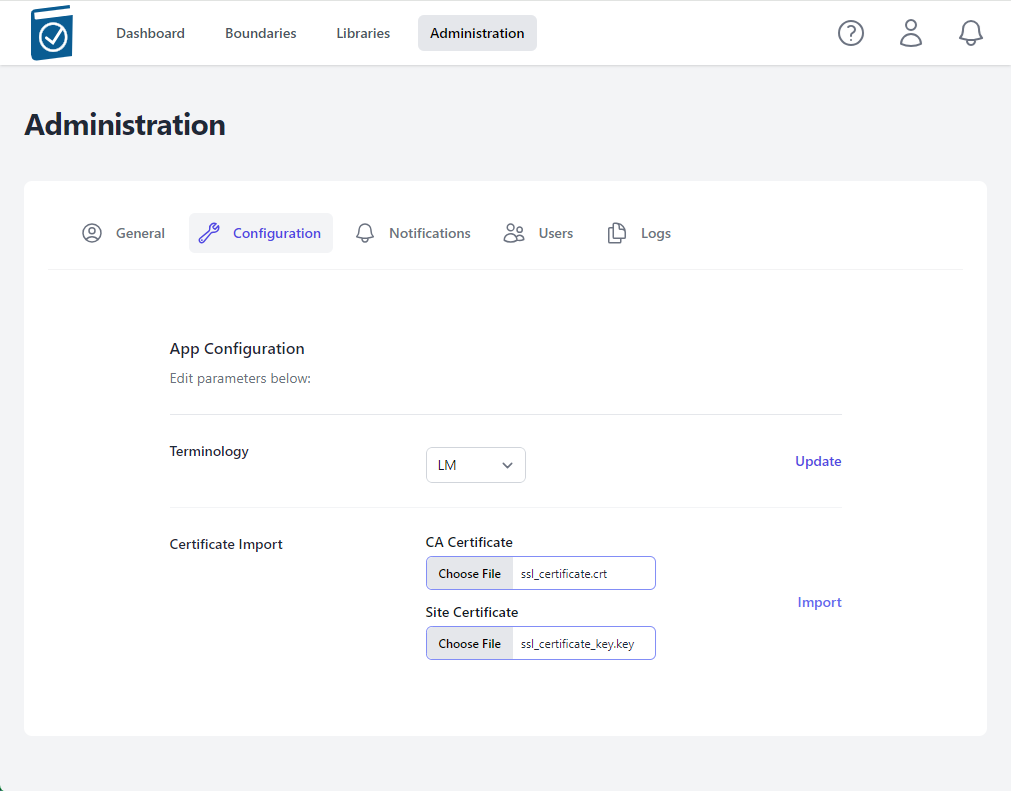


Figure 13: Site Certificate Updated

* Select **Import**

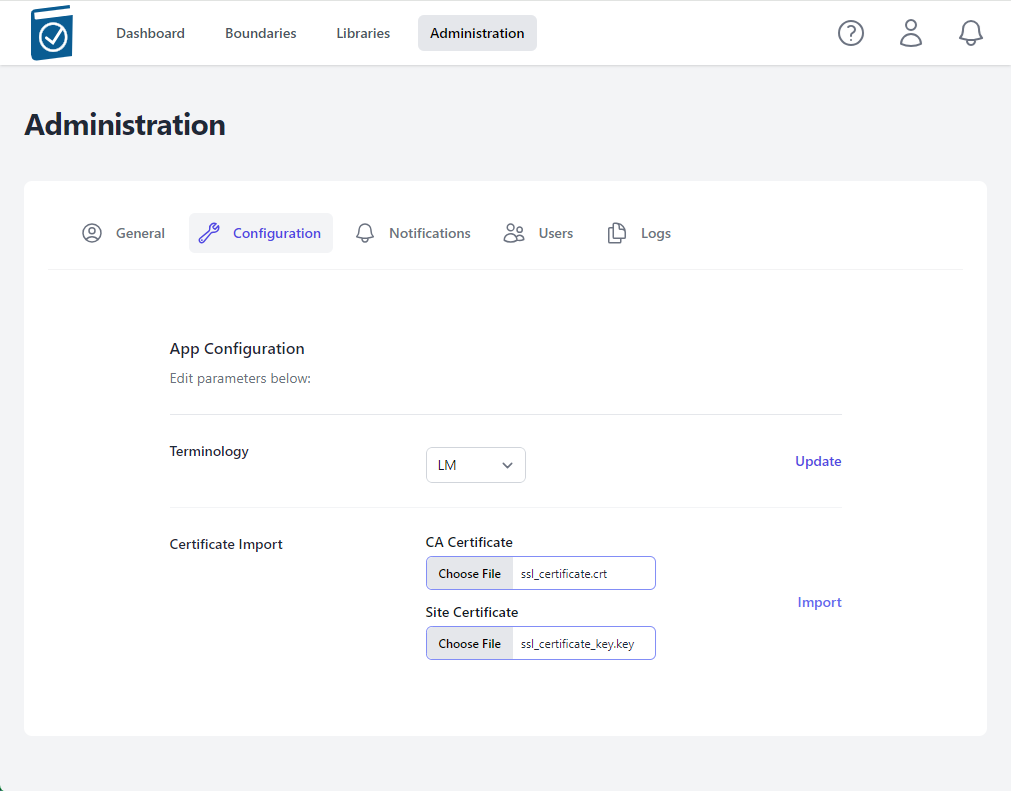


Figure 14: Import Certificates

* A modal window saying "Checking Certificates Please Wait... Circle" will appear while the files are being loaded.

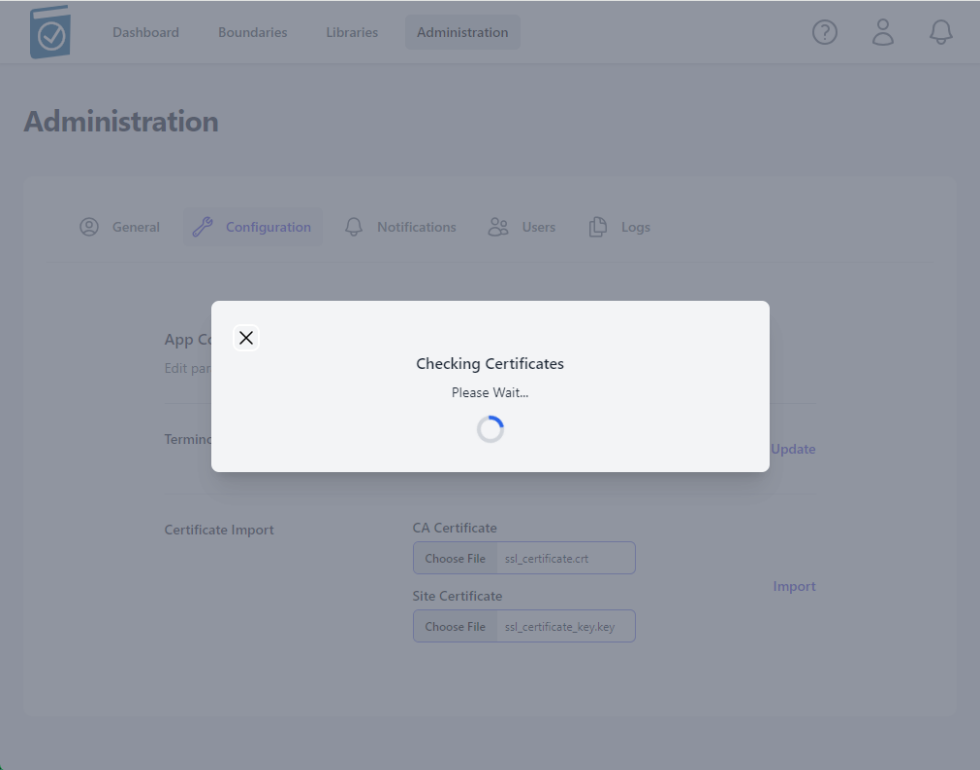


Figure 15: Certificate Import Process

* A message underneath the Certificate Import form Text Fields will appear saying "Certificate Import Successful!" if the certs are accepted.

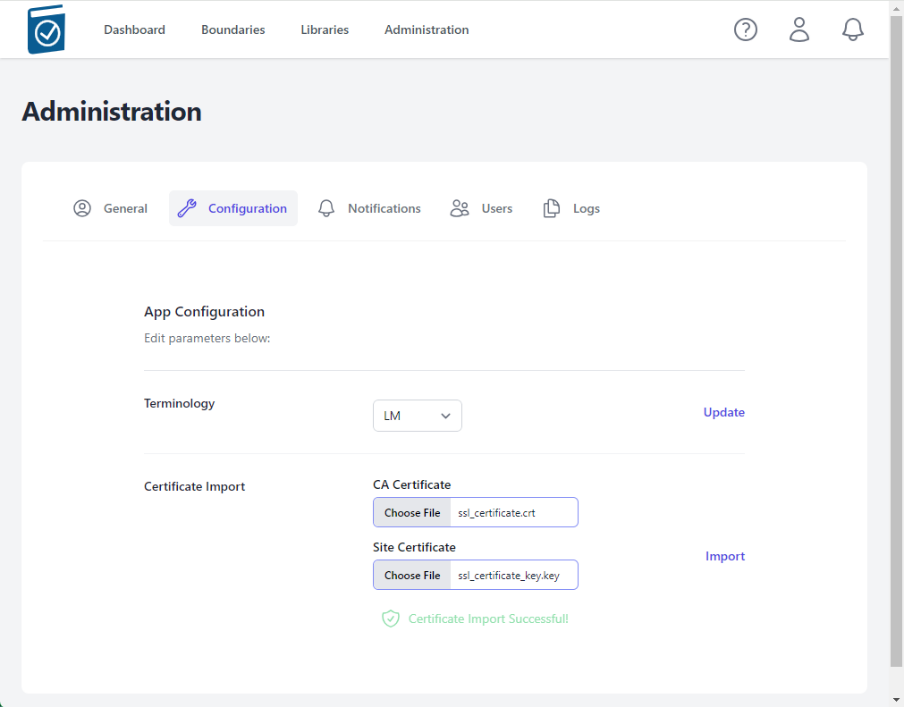


Figure 16: Successful Certificate Import Notification

Notes:

* The NGINX listener checks imported certificates for:
  + A .pem formatted key file
  + A x509 formatted .crt file
  + Cert files matching modulus
  + CRT Common Name matching NGINX\_HOST variable value
* If invalid certificate files are loaded, an error will appear saying **Error in Cert Response** in the top right of the window

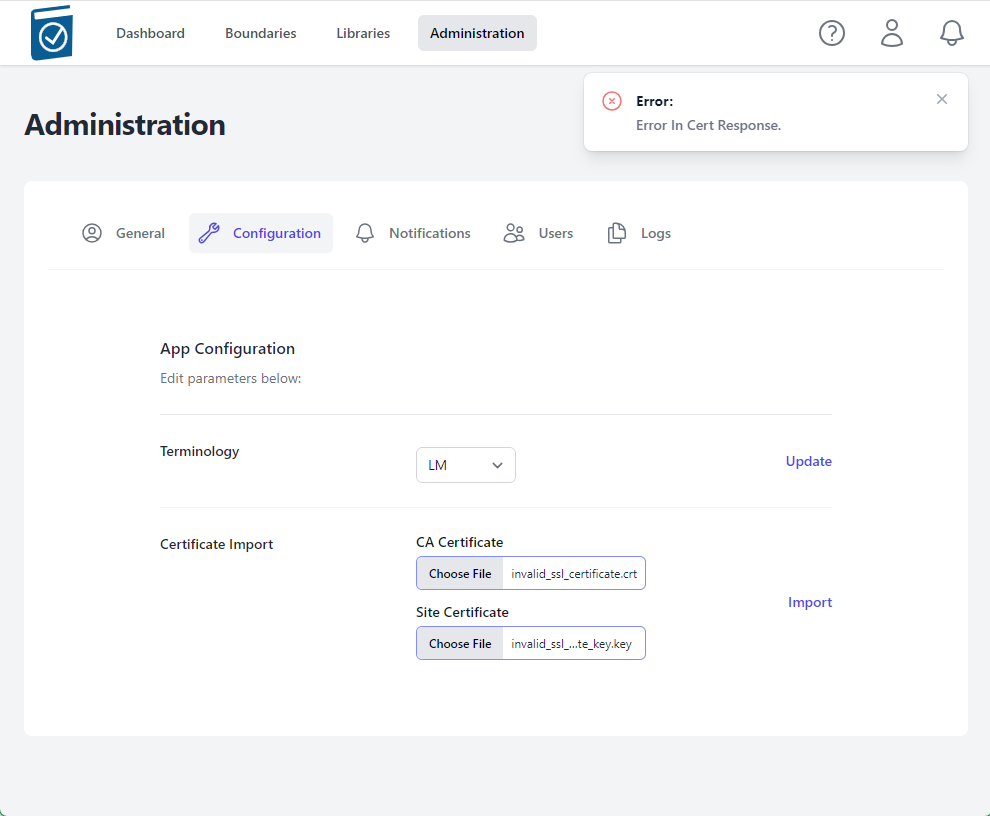


Figure 17: Invalid Certificate Notification

#### Notifications

Notifications are automatically generated at login for the following:

* New STIG Library is available for applicable boundaries
* POA&M Completion Dates coming due or overdue
* Milestone Dates coming due or overdue

#### Users

The **User** functions allow an administrator to add local User or Administrator accounts and change passwords.

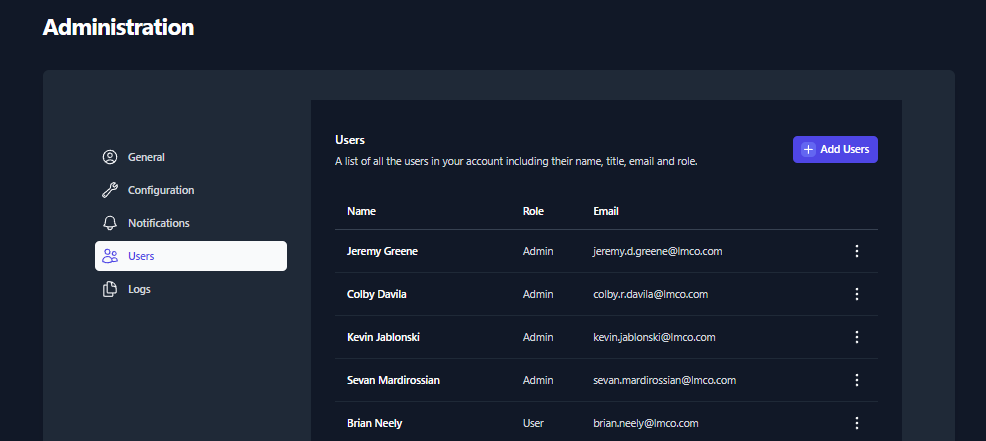


Figure 18 Administration - Users Functions

##### Adding a local Account

To add a local account, select **Add Users**

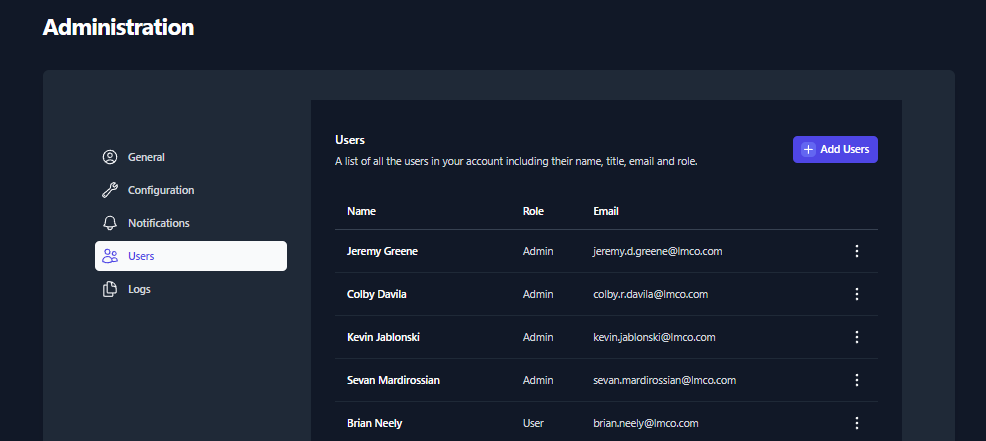


Figure 19: Add Users

This will bring up the **Add User** dialog Box. Complete the relevant data, to include **First Name**, **Last Name**, **Email Address** (username), set a unique password, and change the time zone.

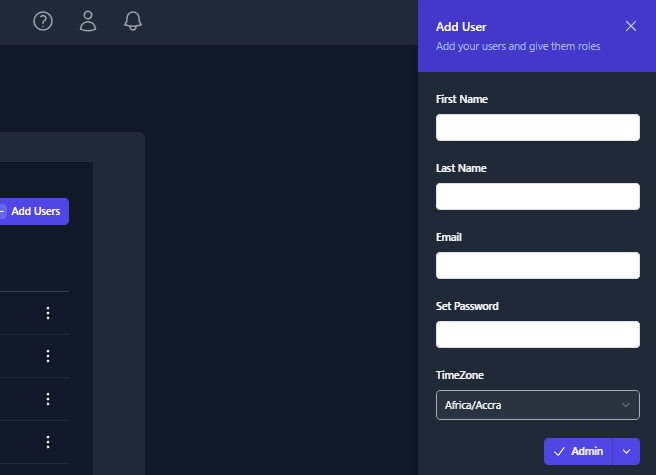


Figure 20: Add User Dialog Box

##### Change User Password

To change a user’s password. Select the 3 buttons to the far right of the user account and select Edit.

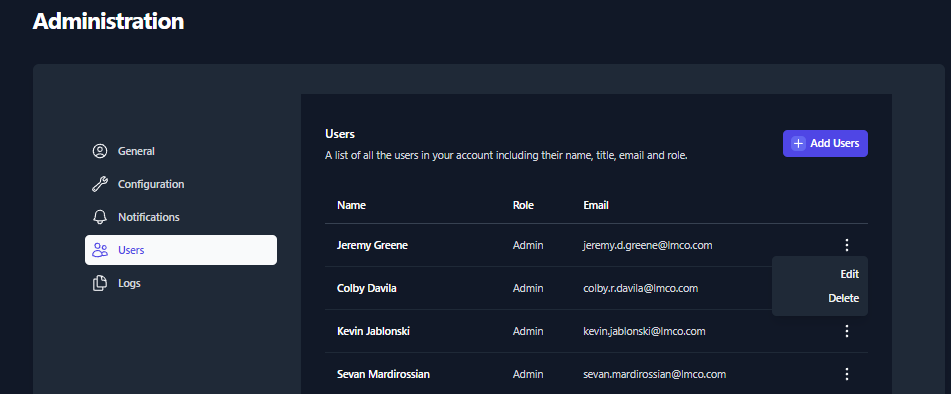


Figure 21: Change User Password – Edit Account

The **Edit User** dialog box will appear on the right side of the screen. Enter a value for **New Password** and **Confirm Password** and click **Save**.

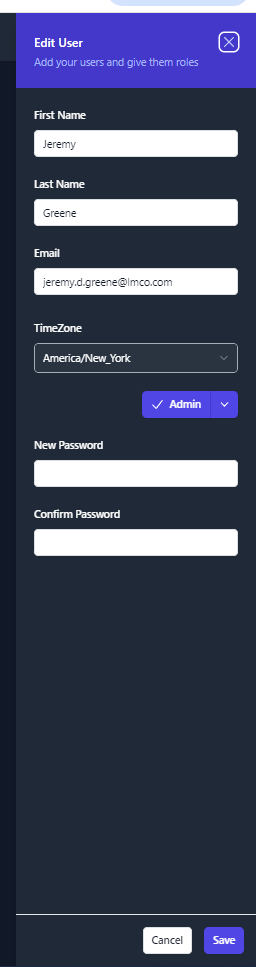


Figure 22: Change Password – Edit User Dialog Box

##### Unlock Account

Unlock account feature is not currently available.

#### Logs

Centralized logging can be configured from the **Logs** function within the Administration tab.

To setup logging, select **Logs** from the **Administration** tab menu.

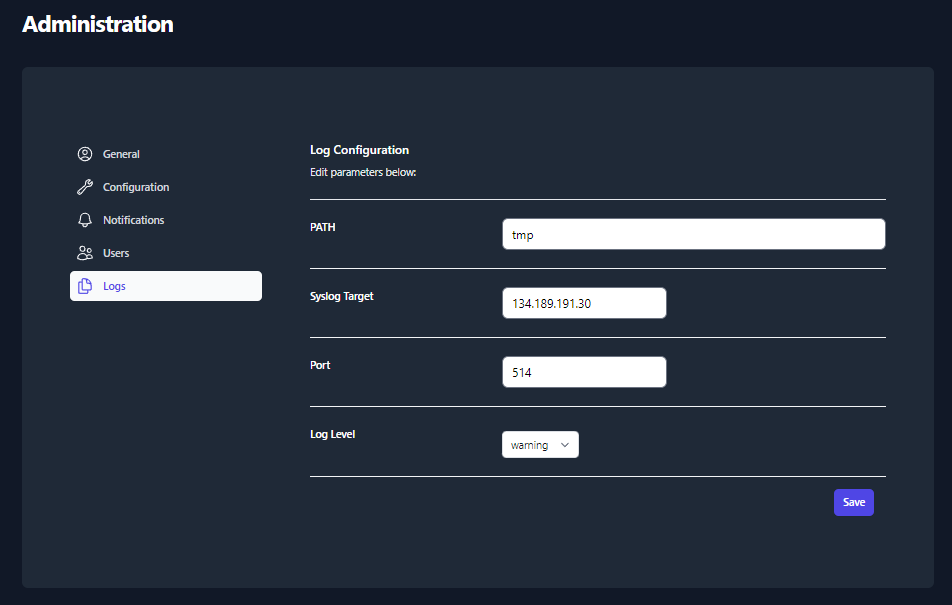




Figure 23: Log Configuration

* **PATH** is the local logging path.
* **Syslog Target** is the centralized log server, like Splunk.
* **Port** is the port being used to forward logs
* **Log Level** determines which logs will be forwarded to the centralized log server. The default setting of **Warning** should meet all required logging for SP 800-53 based authorizations.
* Once properly configured select **Save**

## Libraries

The **Libraries** tab provides the ability to import new STIG libraries and updated Control Correlation Identifiers (CCI) mappings for different NIST SP 800-53 revisions.

* + 1. **STIG Libraries**

The Department of Defense (DoD) releases quarterly updates to the STIG benchmarks. These quarterly updates are released as .zip files. Once downloaded, the .zip files can be uploaded to TIR and made available to all users.

#### View STIG Libraries

Please navigate to the **Libraries** tab by clicking the **Libraries** button at the top on the page.

Note: The **Libraries** tab will display all of the STIG libraries that have been uploaded to your TIR instance.

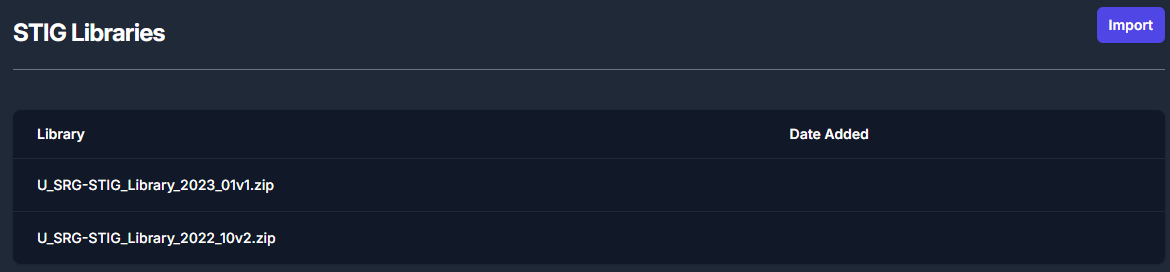


Figure 24: STIG Libraries

Once imported, the STIG libraries will follow a standardized naming convention. The naming convention will follow this template: **U\_SRG-STIG\_Library\_{year}\_{month}{revision}.zip**.

Please refer to the table below for more examples.

|  |  |  |  |
| --- | --- | --- | --- |
| **Year** | **Release Quarter/ Month** | **Revision** | **Naming Convention** |
| 2022 | Q1 / January (01) | v1 | U\_SRG-STIG\_Library\_2022\_01v1.zip |
| 2022 | Q2 / April (04) | v2 | U\_SRG-STIG\_Library\_2022\_04v2.zip |
| 2023 | Q3 / July (07) | v1 | U\_SRG-STIG\_Library\_2023\_07v1.zip |
| 2023 | Q4 / October (10) | v2 | U\_SRG-STIG\_Library\_2023\_10v2.zip |

Table 2: STIG Naming Convention

* + 1. **Import STIG Libraries**

To import a new STIG library, please navigate to the **Libraries** page and click the **Import** button inside the **STIG Libraries** section, as seen in Figure 14. For reference, this button can be found in the top right of *Figur*e 14: STIG Libraries.

The **Import** button will open a file navigation window. Please navigate to the .zip file containing the STIG Library and click **Open**.

* + 1. **CCI Matrix**

CCI mappings are provided by NIST and updated as necessary. CCI mappings different between SP 800-53 Rev 4 and Rev 5. Keeping this updated ensure more granular mapping of STIGs to applicable CCIs.

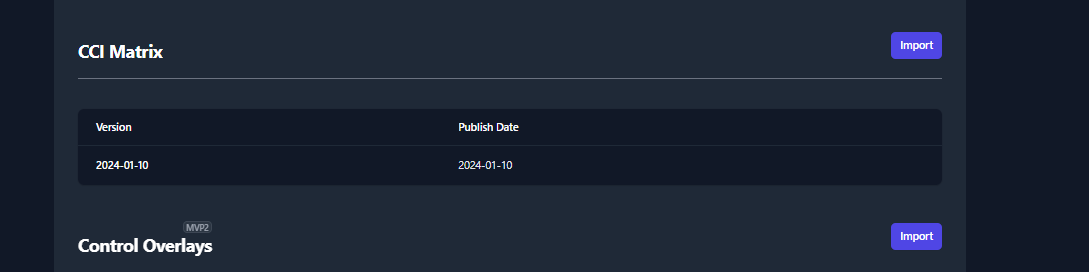


Figure 25: CCI Matrix

#### Import CCI Matrix Updates

To import a new CCI Matrix, please navigate to the Libraries page and click the **Import** button inside the CCI Matrix section. For reference, this button can be found in the top right of Figure 6: CCI Matrix.

* 1. **Changing Boundary and/or Company Permissions**
     1. **Modify Company Permissions**

To modify Company permissions select the 3 buttons to the far right of the Company and select Manage Users.

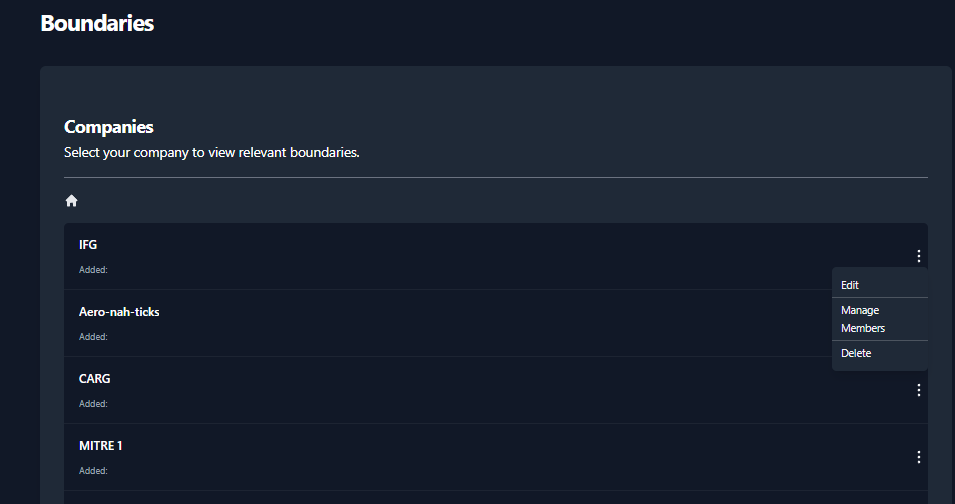


Figure 26: Modify Company Permissions

* Then the Members dialog box comes up, enter the username in the **Search Users** box.

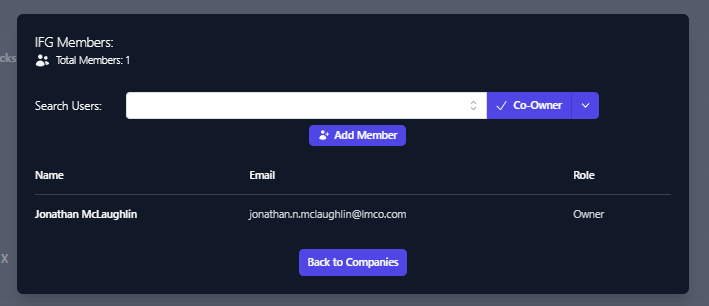


Figure 27: Adding Members – Search Users

* The Search Users box should provide a list of similar usernames. Select the user account you wish to add.
* Once selected click the down arrow next to Co-Owner and select the level of permission you wish to grant.

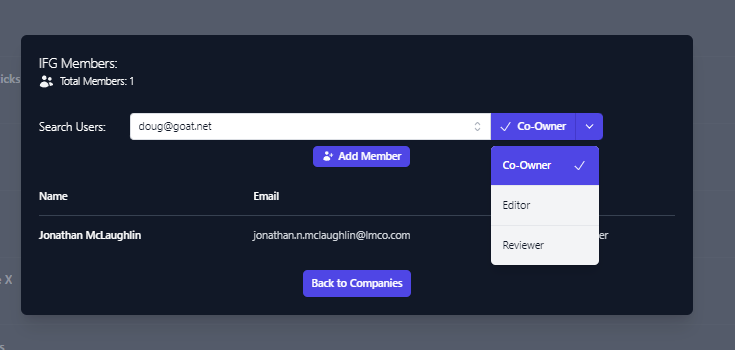


Figure 28: Manage Members – Choose level of Access

* Once the level of access you wish to grant is selected, Click **Add Member**
* You will see the account added to the user permissions list for the applicable company.

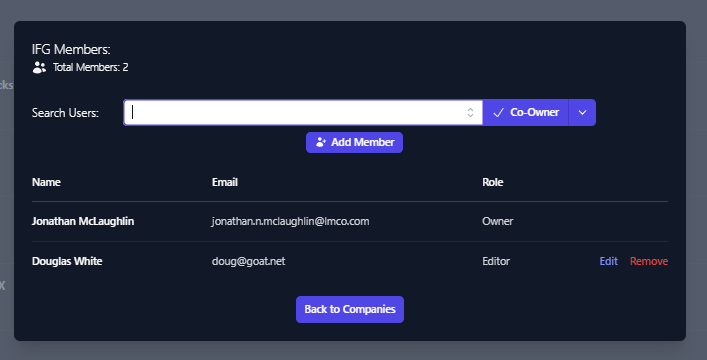


Figure 29: Member Access – User Added with Editor Role.

Member access can be edited or removed from this view as well.

* + 1. **Modify Boundary Permissions**

To modify Boundary permissions select the 3 buttons to the far right of the Company and select Manage Users.

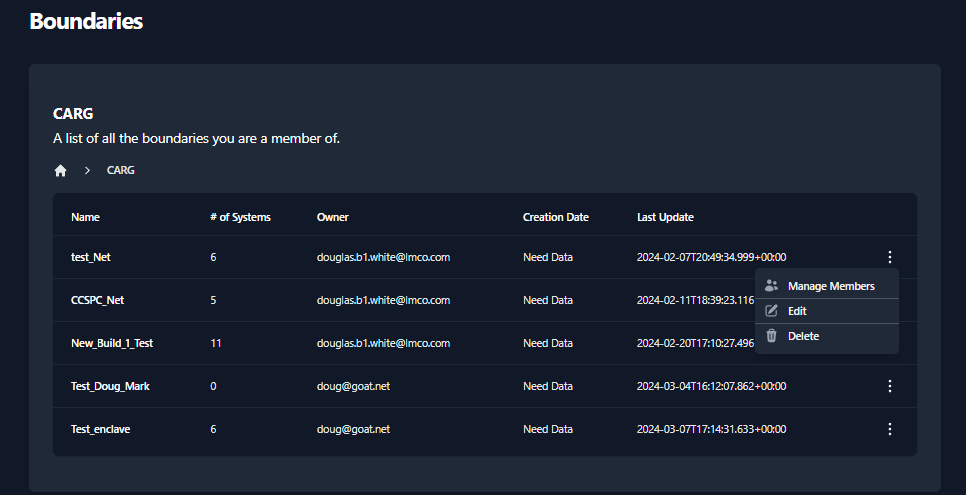


Figure 30: Modify Company Permissions

* Then the Members dialog box comes up, enter the username in the **Search Users** box.

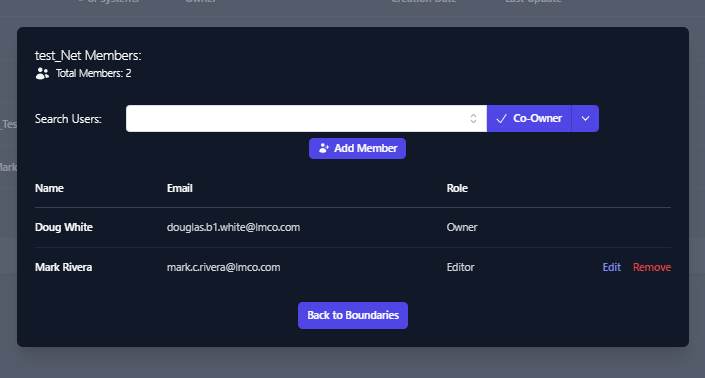


Figure 31: Adding Members – Search Users

* The Search Users box should provide a list of similar usernames. Select the user account you wish to add.
* Once selected click the down arrow next to Co-Owner and select the level of permission you wish to grant.

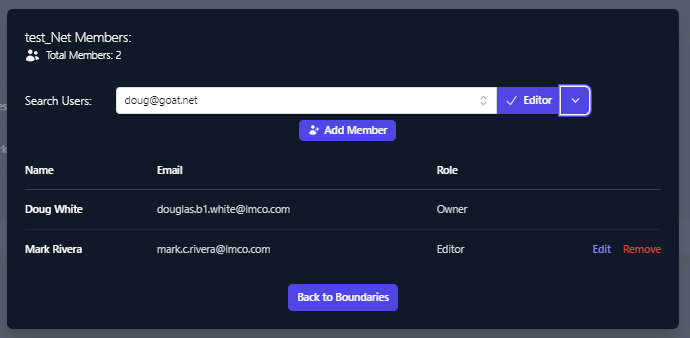


Figure 32: Manage Members – Choose level of Access

Once the level of access you wish to grant is selected, Click **Add Member**

You will see the account added to the user permissions list for the applicable company.

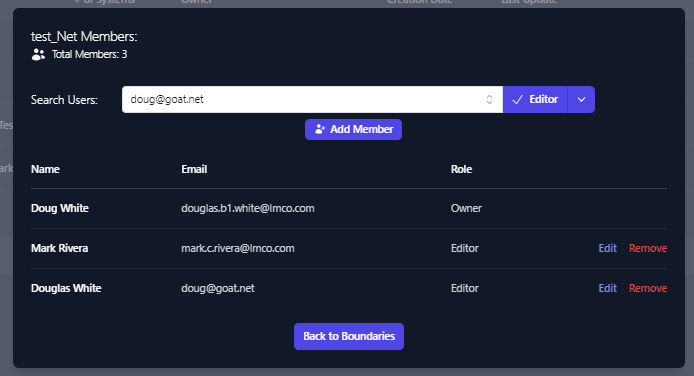


Figure 33: Member Access – User Added with Editor Role.

Member access can be edited or removed from this view as well.