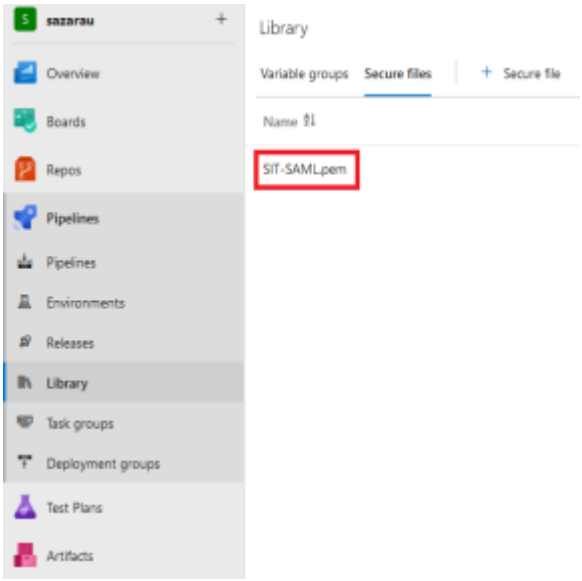
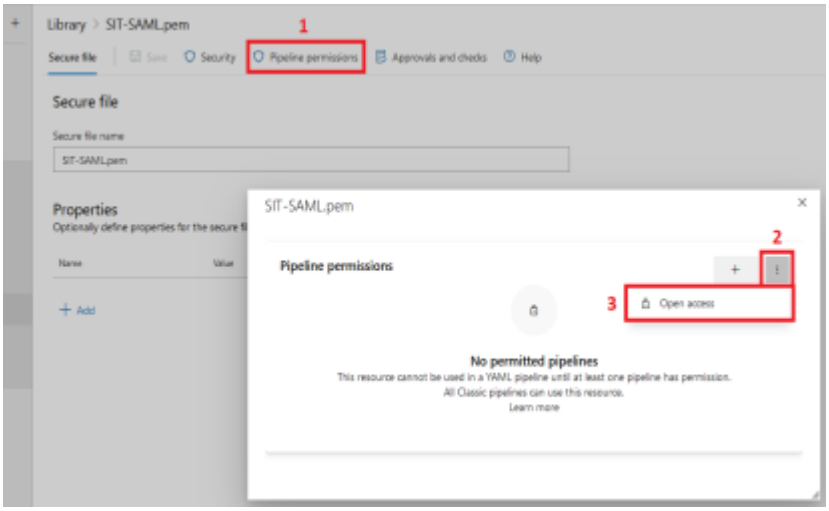
Configure File Permissions for a Pipeline

The following steps outline the process of configuring file permissions for a Pipeline:

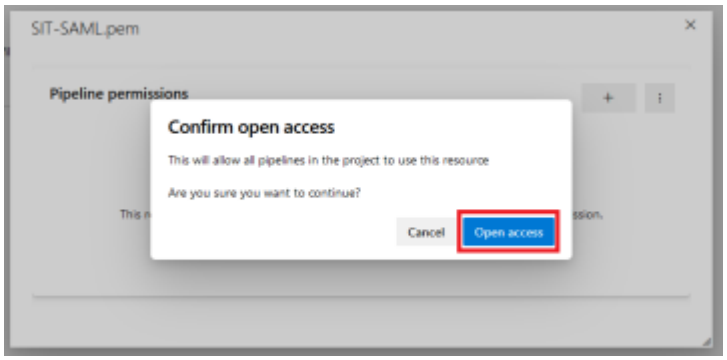
1. Click on the file name to open file properties.



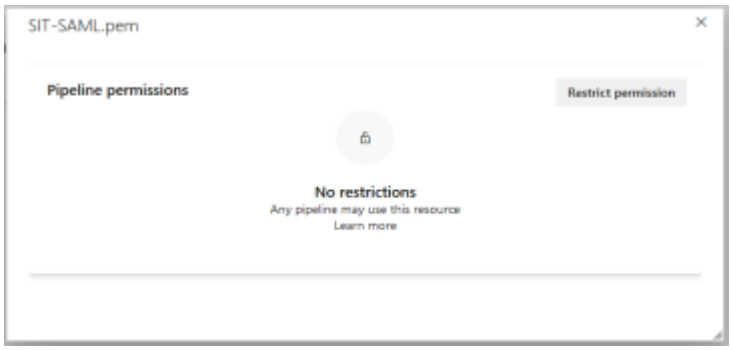
2. Click the **Pipeline permissions** Tab, the **ellipses** button, and select **Open access** from the menu.



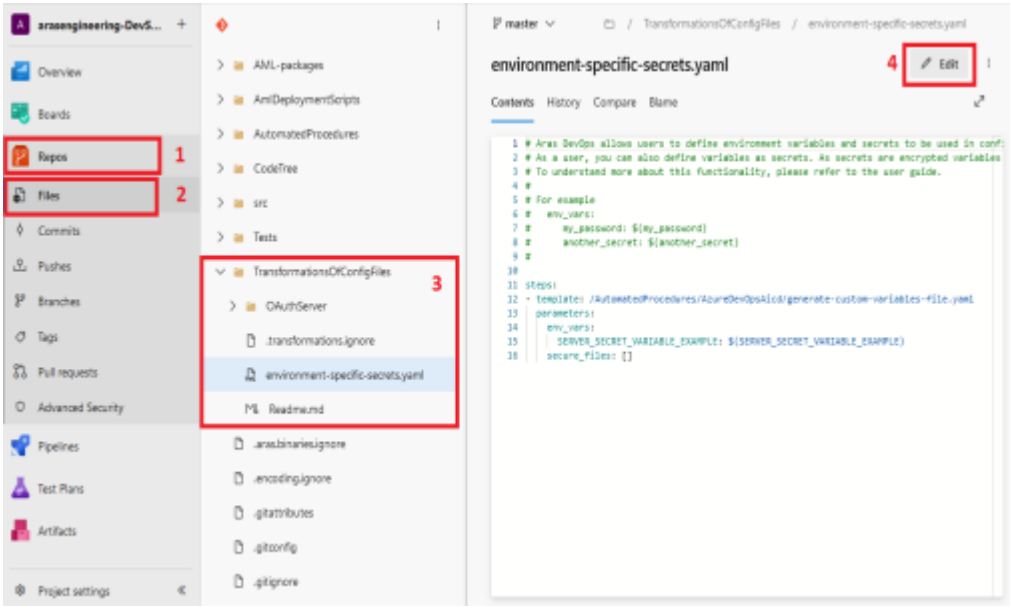
3. Click the **Open access** button to allow Pipelines to download the file.



Once the permission has configured successfully, close the window.



4. Add the certificate file name to a configuration file. This allows the file to be used in Pipelines. Click **Repos** and open the TransformationsOfConfigFiles/environment-specific-secrets.yaml file.
5. Click the **Edit** button.



6. If the secure_files section is missing, add the file name to it. To have a valid YAML file, all indents should be the same as in the screenshots below.

```yaml
# Aras DevOps allows users to define environment variables and secrets to be used in
# As a user, you can also define variables as secrets. As secrets are encrypted varia
# To understand more about this functionality, please refer to the user guide.
#
# For example
#   env_vars:
#     my_password: $(my_password)
#     another_secret: $(another_secret)
#

steps:
- template: /AutomatedProcedures/AzureDevOpsAicd/generate-custom-variables-file.yaml
  parameters:
    env_vars:
      SERVER_SECRET_VARIABLE_EXAMPLE: $(SERVER_SECRET_VARIABLE_EXAMPLE)
    secure_files:
    - SIT-SAML.pem
    - SIT-SAML-123.pem
    - UAT-SAML.pem
```

7. Click the **Commit** button.

8. Set the Comment to **Commit** (use the default **Commit** Message) and click the **Commit** button.