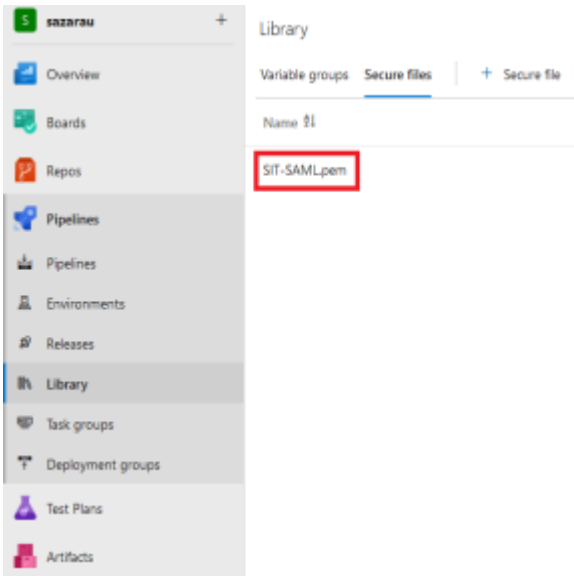


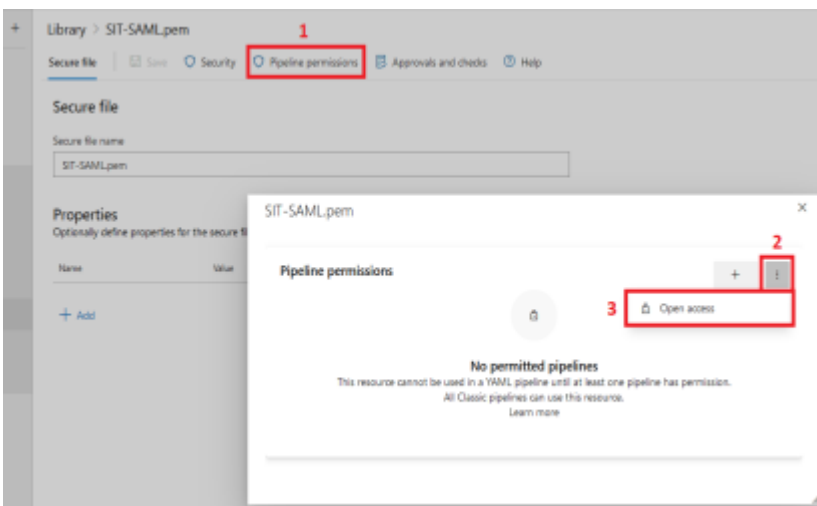
Configure File Permissions for a Pipeline

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

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

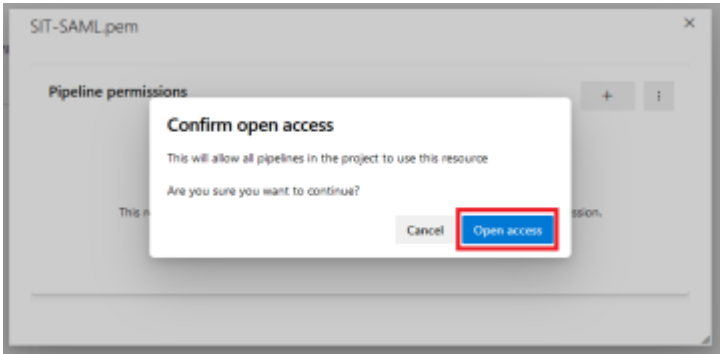


2. Click the **Pipeline permissions** Tab, the **ellipses** button, and select **Open access** from the menu.

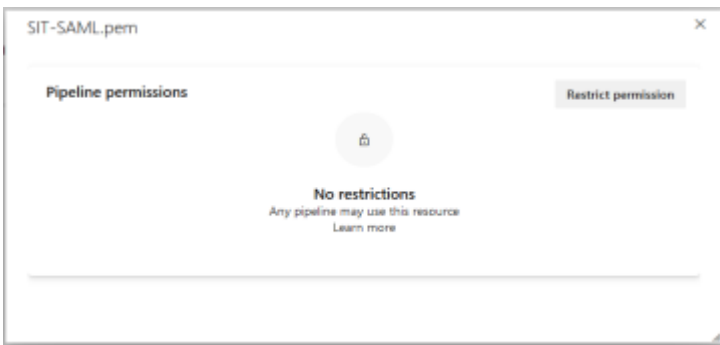


3. Click the **Open access** button to allow Pipelines to download the file.



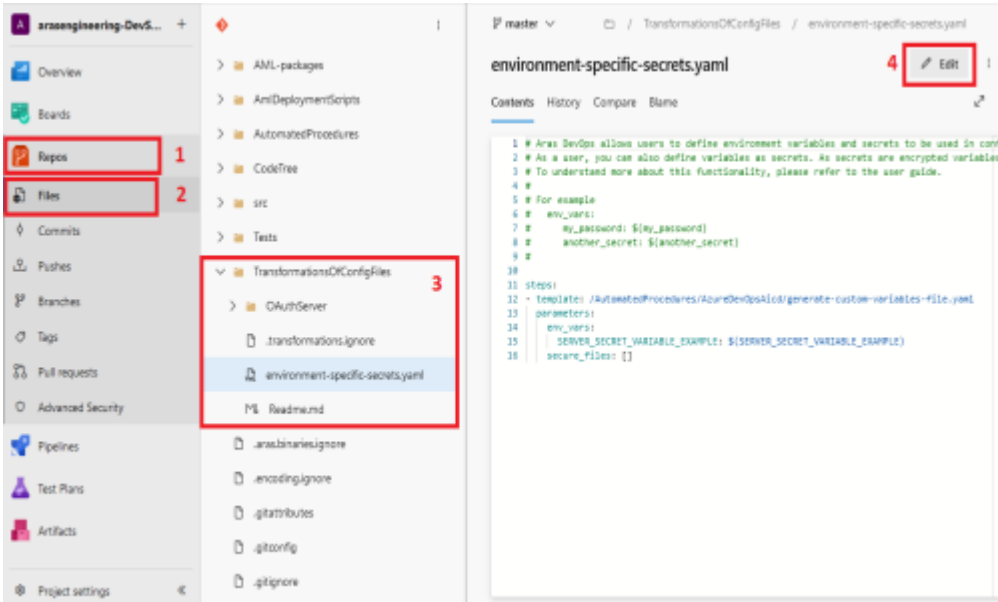


Once the permission has configured successfully, close the window.



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.

```

1 # Aras DevOps allows users to define environment variables and secrets to be used in
2 # As a user, you can also define variables as secrets. As secrets are encrypted vari
3 # To understand more about this functionality, please refer to the user guide.
4 #
5 # For example
6 #   env_vars:
7 #     my_password: $(my_password)
8 #     another_secret: $(another_secret)
9 #
10
11 steps:
12 - template: /AutomatedProcedures/AzureDevOpsA1cd/generate-custom-variables-file.yaml
13   parameters:
14     env_vars:
15       SERVER_SECRET_VARIABLE_EXAMPLE: $(SERVER_SECRET_VARIABLE_EXAMPLE)
16   secure_files:
17     - SIT-SAML.pem
18     - SIT-SAML-123.pem
19     - UAT-SAML.pem
20

```

7. Click the **Commit** button.



```
1 # Aras DevOps allows users to define environment variables and secrets to be used in config transformations.
2 # As a user, you can also define variables as secrets. As secrets are encrypted variables with higher protection
3 # To understand more about this functionality, please refer to the user guide.
4 #
5 # For example
6 # env_vars:
7 #   my_password: $(my_password)
8 #   another_secret: $(another_secret)
9 #
10
11 steps:
12 - template: /AutomatedProcedures/AzureDevOpsAics/generate-custom-variables-file.yaml
13   parameters:
14     env_vars:
15       SERVER_SECRET_VARIABLE_EXAMPLE: $(SERVER_SECRET_VARIABLE_EXAMPLE)
16     secure_files:
17       - SIT-SAM.pem
18
```

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

Azure DevOps interface showing the 'Commit' dialog box. The dialog contains a 'Comment' field with the text 'Updated environment-specific-secrets.gem' (labeled 1), a 'Branch name' field with 'master', and a 'Work items to link' section. The 'Commit' button at the bottom right is highlighted with a red box and labeled 2.

