Managing Secrets for CI/CD

Secrets are encrypted environment variables that you create.

These variables can be managed in multiple ways.

a. As Organization Secrets
b. As Repository Secrets
c. As Env Variable declared in the configuration file.
d. Secrets Managed in AKV

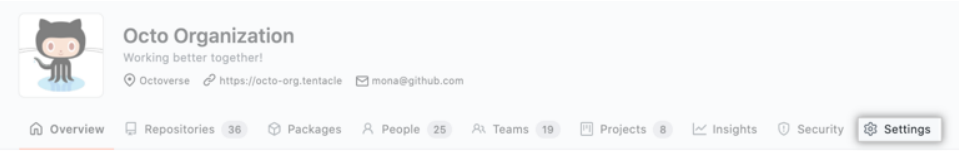
a. Organization Secrets:

Organization-level secrets let you share secrets between multiple repositories, which reduces the need to create duplicate secrets. You can use access policies to control which repositories can use organization secrets.

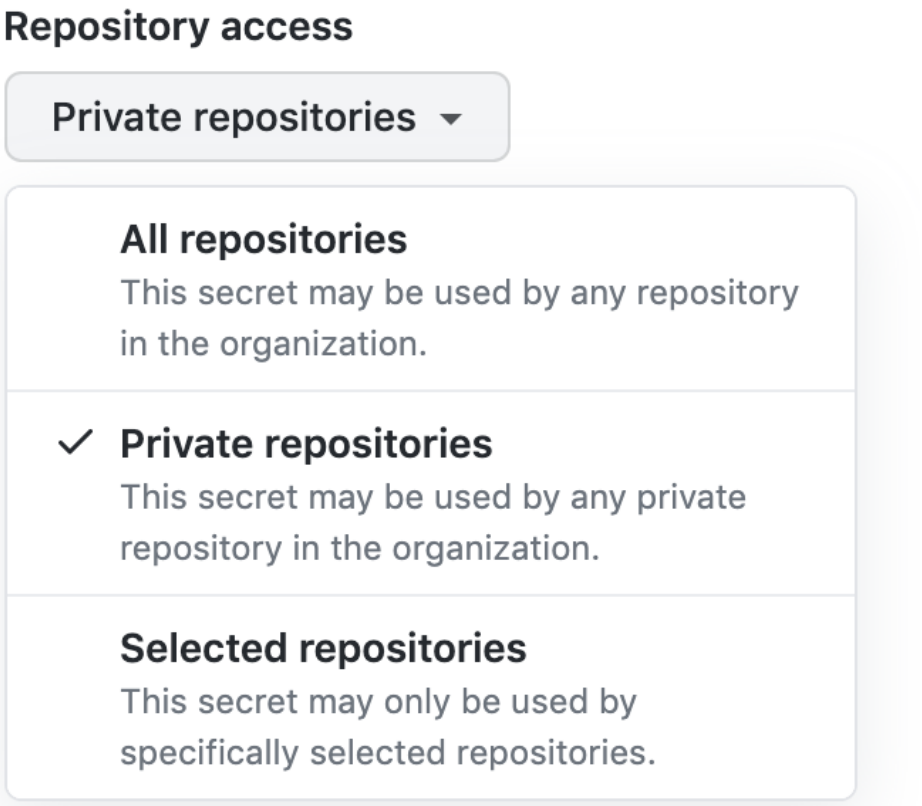
When creating a secret in an organization, you can use a policy to limit which repositories can access that secret. For example, you can grant access to all repositories, or limit access to only private repositories or a specified list of repositories.

To create secrets at the organization level, you must have admin access.

- On GitHub.com, navigate to the main page of the organization.
- Under your organization name, click Settings.



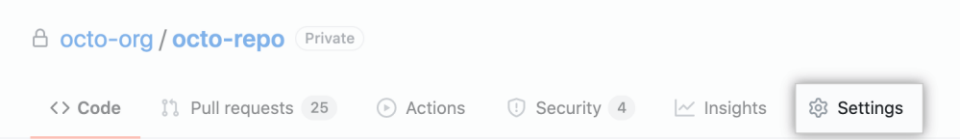
- In the "Security" section of the sidebar, select Secrets then click Codespaces.
- At the top of the page, click new organization secret.
- Type a name for your secret in the Name input box.
- Enter the Value for your secret.
- From the Repository access dropdown list, choose an access policy.



- Click Add secret.

b. Repository Secrets:

Adding secrets for a repository



- To create secrets for an organization repository, you must have administrator access.
- On GitHub.com, navigate to the main page of the repository.
- Under your repository name, click Settings.
- In the "Security" section of the sidebar, select Secrets then click Codespaces.
- At the top of the page, click new repository secret.
- Type a name for your secret in the Name input box.
- Enter the value for your secret.
- Click Add secret.

c. Env Variable declaration in the config file:

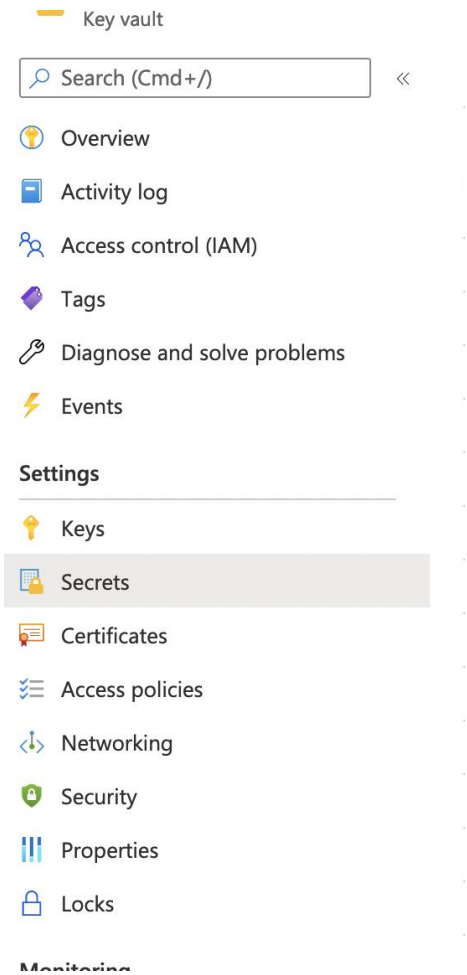
Environment variables should not include credentials. It can be for example a project name.

d. Secrets Managed using AKV:

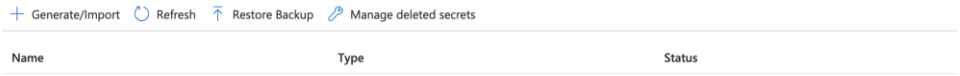
In Azure Key Vault we can manage keys and secrets.

Steps to save secrets on AKV:

- Navigate to your new key vault in the Azure portal
- On the Key Vault settings pages, select Secrets.



- Click on Generate/Import.



- On the “Create a secret” screen choose the following values:
    - Upload options: Manual.
    - Name: Type a name for the secret. The secret name must be unique within a Key Vault.
    - Value: Type a value for the secret. Key Vault APIs accepts and return secret values as strings.
    - Leave the other values to their defaults. Click Create.