Managing secrets for your repository and organization for GitHub Codespaces

In this article

Secrets allow you to store sensitive information in your organization or repository for use with GitHub Codespaces.

> **Who can use this feature**
> To manage secrets for GitHub Codespaces for an organization, you must be an organization owner.

Secrets are available in all public repositories, in private repositories owned by personal accounts, and in private repositories owned by organizations on GitHub Team or GitHub Enterprise plans. For more information, see "GitHub’s plans."

About secrets

Secrets are encrypted environment variables that you create in the GitHub Codespaces settings for an organization, a repository, or a personal account. For information on creating user-specific secrets, see "Managing secrets for your codespaces."

The secrets that you create are available to use in GitHub Codespaces. GitHub uses a libsodium sealed box to encrypt secrets before they reach GitHub and only decrypts them when you use them in a codespace.

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.

Once you have created a secret, it will be available when you create a new codespace or restart the codespace. If you've created a secret on GitHub.com and you want to use it in a currently running codespace, stop the codespace and then restart it. For information about stopping the codespace, see "Using the Visual Studio Code Command Palette in GitHub Codespaces."

Naming secrets

The following rules apply to secret names:

- Secret names can only contain alphanumeric characters (`[a-z]`, `[A-Z]`, `[0-9]`) or underscores (`_`). Spaces are not allowed.

- Secret names must not start with the `GITHUB_` prefix.
- Secret names must not start with a number.
- Secret names are not case-sensitive.
- Secret names must be unique at the level they are created at. For example, a secret created at the repository level must have a unique name in that repository, and a secret created at the organization level must have a unique name at that level.

  If a secret with the same name exists at multiple levels, the secret at the lowest level takes precedence. For example, if an organization-level secret has the same name as a repository-level secret, then the repository-level secret takes precedence.

Limits for secrets

You can store up to 100 secrets per organization and 100 secrets per repository.

Secrets are limited to 48 KB in size.

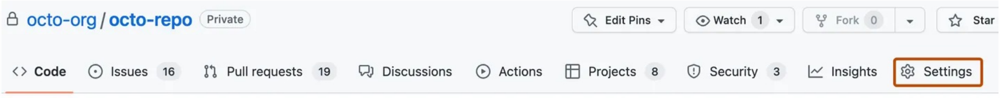
Recommended secrets for a repository

Your project may require specific user secrets. For example, to run the application in a codespace, the user may need to supply a personal API key. If this is the case, you can specify recommended secrets in the dev container configuration. The user will then be prompted to supply values for these secrets, if they haven't already created these personal secrets, when they use the advanced options page to create a codespace. If the user supplies a secret value for use in the codespace, this secret is added to their personal settings for Codespaces. They will not have to enter a value for this secret when they create a codespace for this repository in future. For more information, see "Specifying recommended secrets for a repository."

Adding secrets for a repository

To create secrets for an organization repository, you must have administrator access.

1. On GitHub.com, navigate to the main page of the repository.
2. Under your repository name, click ⚙ **Settings**. If you cannot see the "Settings" tab, select the ··· dropdown menu, then click **Settings**.



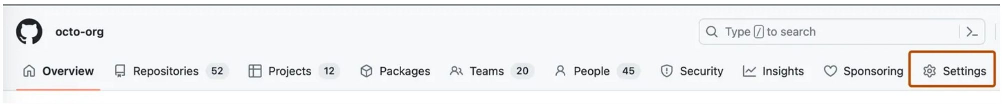
3. In the "Security" section of the sidebar, select ⊛ **Secrets and variables**, then click **Codespaces**.
4. At the top of the page, click **New repository secret**.
5. Type a name for your secret in the **Name** input box.
6. Enter the value for your secret.
7. Click **Add secret**.

Adding secrets for an organization

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.

1. On GitHub.com, navigate to the main page of the organization.
2. Under your organization name, click ⚙ **Settings**. If you cannot see the "Settings" tab, select the ··· dropdown menu, then click **Settings**.

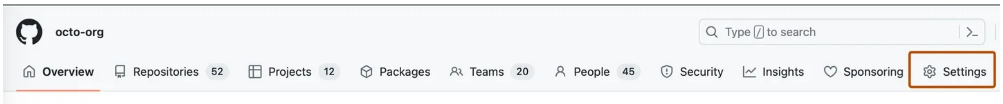


3. In the "Security" section of the sidebar, select ⊛ **Secrets and variables**, then click **Codespaces**.
4. At the top of the page, click **New organization secret**.
5. Type a name for your secret in the **Name** input box.
6. Enter the **Value** for your secret.
7. From the **Repository access** dropdown list, choose an access policy.
8. Click **Add secret**.

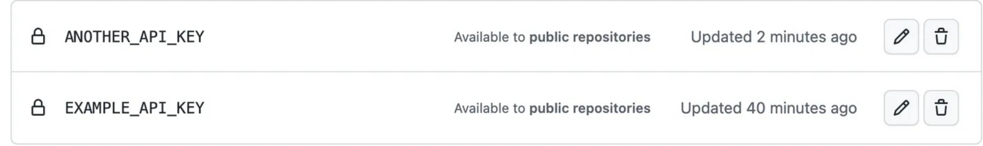
Reviewing access to organization-level secrets

You can check which access policies are applied to a secret in your organization.

1. On GitHub.com, navigate to the main page of the organization.
2. Under your organization name, click ⚙ **Settings**. If you cannot see the "Settings" tab, select the ··· dropdown menu, then click **Settings**.



3. In the "Security" section of the sidebar, select ⊛ **Secrets and variables**, then click **Codespaces**.
4. The list of secrets includes any configured permissions and policies. For example:



ANOTHER_API_KEY	Available to **public repositories**	Updated 2 minutes ago
EXAMPLE_API_KEY	Available to **public repositories**	Updated 40 minutes ago

5. For more details on the configured permissions for each secret, click **Update**.

Further reading

- "Managing secrets for your codespaces"