Sharing workflows, secrets, and runners with your organization

In this article

Learn how you can use organization features to collaborate with your team, by sharing starter workflows, secrets, and self-hosted runners.

> **Note:** GitHub-hosted runners are not currently supported on GitHub Enterprise Server. You can see more information about planned future support on the GitHub public roadmap.

Overview 🔗

If you need to share workflows and other GitHub Actions features with your team, then consider collaborating within a GitHub organization. An organization allows you to centrally store and manage secrets, artifacts, and self-hosted runners. You can also create starter workflows in the `.github` repository and share them with other users in your organization.

Sharing workflows 🔗

Your organization can share workflows by reusing the workflows exactly or by creating starter workflows that provide templates for new workflows.

Reusing workflows 🔗

You can share workflows with your organization, publicly or privately, by calling one workflow from within another workflow. This allows you to reuse workflows, avoiding duplication and making your workflows easier to maintain. For more information, see "Reusing workflows."

Using starter workflows 🔗

Starter workflows allow everyone in your organization who has permission to create

workflows to do so more quickly and easily. When you create a new workflow, you can choose a starter workflow and some or all of the work of writing the workflow will be done for you. You can use starter workflows as a starting place to build your custom workflow or use them as-is. This not only saves time, it promotes consistency and best practice across your organization. For more information, see "[Creating starter workflows for your organization](#)."

Sharing secrets within an organization 🔗

You can centrally manage your secrets within an organization, and then make them available to selected repositories. This also means that you can update a secret in one location, and have the change apply to all repository workflows that use it.

When creating a secret in an organization, you can use a policy to limit which repositories can access it. 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 your GitHub Enterprise Server instance, 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**.
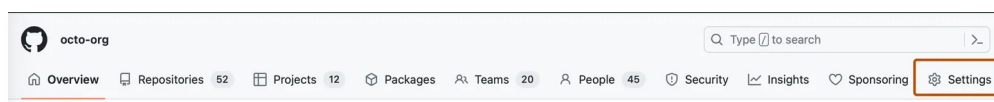
3 In the left sidebar, click **Secrets**.

4 Click **New 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**.

Share self-hosted runners within an organization 🔗

Organization admins can add their self-hosted runners to groups, and then create policies that control which repositories can access the group.

For more information, see "[Managing access to self-hosted runners using groups](#)."

Next steps 🔗

To continue learning about GitHub Actions, see "[Creating starter workflows for your organization](#)."