This version of GitHub Enterprise was discontinued on 2023-03-15. No patch releases will be made, even for critical security issues. For better performance, improved security, and new features, upgrade to the latest version of GitHub Enterprise. For help with the upgrade, contact GitHub Enterprise support.

Managing access to self-hosted runners using groups

In this article

You can use policies to limit access to self-hosted runners that have been added to an organization or enterprise.

> **Who can use this feature**
> Enterprise accounts, organizations owned by enterprise accounts, and organizations using GitHub Team can create and manage additional runner groups.

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.

About runner groups

To control access to runners at the organization and/or enterprise levels, enterprise administrators can use runner groups.Enterprise administrators can configure access policies that control which organizations in an enterprise have access to the runner group.

When you grant access access to a runner group, you can see the runner group listed in the organization's runner settings. Optionally, you can assign additional granular repository access policies to the runner group.

When new runners are created, they are automatically assigned to the default group. Runners can only be in one group at a time. You can move runners from the default group to another group. For more information, see "Moving a runner to a group."

Creating a self-hosted runner group for an organization

Warning: We recommend that you only use self-hosted runners with private repositories. This is because forks of your public repository can potentially run dangerous code on your self-hosted runner machine by creating a pull request that executes the code in a workflow.

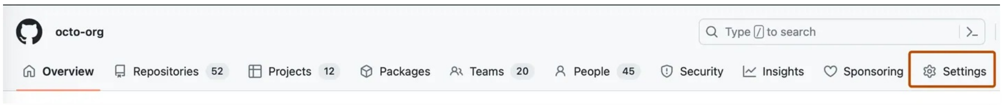
For more information, see "About self-hosted runners."

All organizations have a single default runner group. Organizations within an enterprise account can create additional groups. Organization admins can allow individual repositories access to a runner group. For information about how to create a runner group with the REST API, see "Actions."

Runners are automatically assigned to the default group when created, and can only be members of one group at a time. You can move a runner from the default group to any group you create.

When creating a group, you must choose a policy that defines which repositories have access to the runner group.

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 **Actions**.
4. In the left sidebar, under "Actions", click **Runner groups**.
5. In the "Runner groups" section, click **New runner group**.
6. Enter a name for your runner group.
7. Assign a policy for repository access.

   You can configure a runner group to be accessible to a specific list of repositories, or to all repositories in the organization. By default, only private repositories can access runners in a runner group, but you can override this. This setting can't be overridden if configuring an organization's runner group that was shared by an enterprise.
8. Click **Create group** to create the group and apply the policy.

Creating a self-hosted runner group for an enterprise

Warning: We recommend that you only use self-hosted runners with private repositories. This is because forks of your public repository can potentially run dangerous code on your self-hosted runner machine by creating a pull request that executes the code in a workflow.

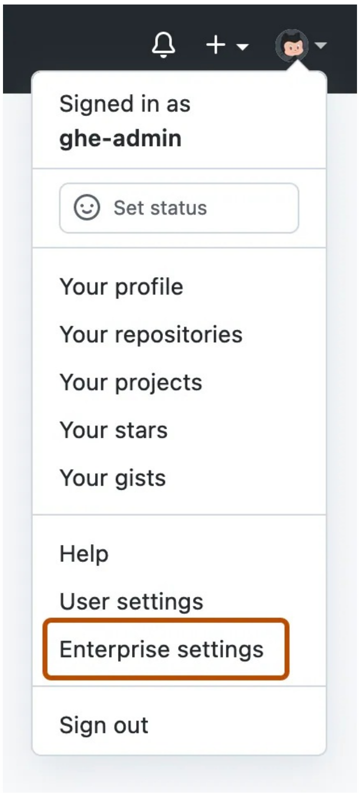
For more information, see "About self-hosted runners."

Enterprises can add their runners to groups for access management. Enterprises can create groups of runners that are accessible to specific organizations in the enterprise account. Organization owners can then assign additional granular repository access policies to the enterprise runner groups. For information about how to create a runner group with the REST API, see the enterprise endpoints in the GitHub Actions REST API.

Runners are automatically assigned to the default group when created, and can only be members of one group at a time. You can assign the runner to a specific group during the registration process, or you can later move the runner from the default group to a custom group.

When creating a group, you must choose a policy that defines which organizations have access to the runner group.

1. In the top-right corner of GitHub Enterprise Server, click your profile photo, then click **Enterprise settings**.



2. In the enterprise account sidebar, click ⚖ **Policies**.
3. Under "⚖ Policies", click **Actions**.
4. Click the **Runner groups** tab.
5. Click **New runner group**.
6. Under "Group name", type a name for your runner group.
7. To choose a policy for organization access, select the **Organization access** dropdown menu and click a policy. You can configure a runner group to be accessible to a specific list of organizations, or all organizations in the enterprise. By default, only private repositories can access runners in a runner group, but you can override this.
8. Click **Save group** to create the group and apply the policy.

Changing the access policy of a self-hosted runner group

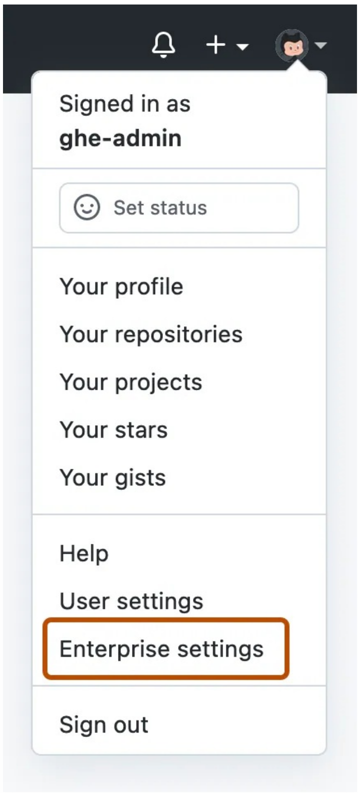
Warning: We recommend that you only use self-hosted runners with private repositories. This is because forks of your public repository can potentially run dangerous code on your self-hosted runner machine by creating a pull request that executes the code in a workflow.

For more information, see "About self-hosted runners."

For runner groups in an enterprise, you can change what organizations in the enterprise can access a runner group. For runner groups in an organization, you can change what repositories in the organization can access a runner group.

Changing what organizations or repositories can access a runner group

1. Navigate to where your runner groups are located:
   - **In an organization**:
     a. Navigate to the main page and click ⚙ **Settings**.
   - **If using an enterprise-level group**:
     a. In the top-right corner of GitHub Enterprise Server, click your profile photo, then click **Enterprise settings**.



Signed in as
ghe-admin

2. Navigate to the "Runner groups" settings:
   - **In an organization**:
     a. In the left sidebar, click **Actions**.
     b. In the left sidebar, under "Actions", click **Runner groups**.
   - **If using an enterprise-level group**:

a. In the enterprise account sidebar, click ⚖ **Policies**.

b. Under "⚖ Policies", click **Actions**.

c. Click the **Runner groups** tab.

3. In the list of groups, click the runner group you'd like to configure.

4. For runner groups in an organization, under "Repository access," use the dropdown menu to click **Selected organizations**.

   a. To the right of the dropdown menu, click ⚙.

   b. In the popup, use the checkboxes to select repositories that can access this runner group.

5. For runner groups in an enterprise, under "Organization access," use the dropdown menu to click **Selected organizations**.

   a. To the right of the dropdown menu, click ⚙.

   b. In the popup, use the checkboxes to select organizations that can use this runner group.

6. Click **Save group**.

> **Warning**
>
> We recommend that you only use self-hosted runners with private repositories. This is because forks of your public repository can potentially run dangerous code on your self-hosted runner machine by creating a pull request that executes the code in a workflow.
>
> For more information, see "About self-hosted runners."

Changing the name of a runner group

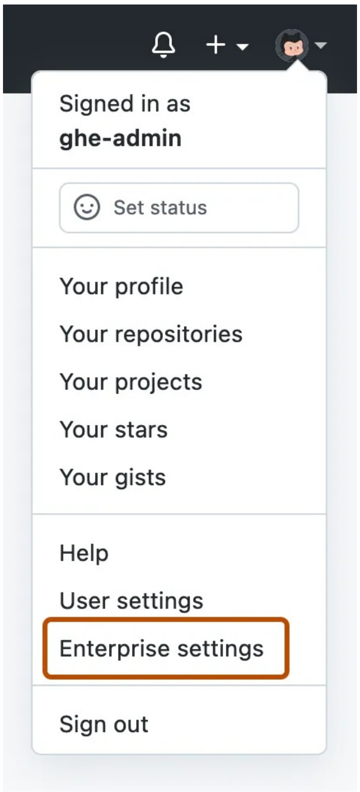
1. Navigate to where your runner groups are located:

   - **In an organization**:

     a. Navigate to the main page and click ⚙ **Settings**.

   - **If using an enterprise-level group**:

     a. In the top-right corner of GitHub Enterprise Server, click your profile photo, then click **Enterprise settings**.



2. Navigate to the "Runner groups" settings:
   - **In an organization**:
     a. In the left sidebar, click **Actions**.
     b. In the left sidebar, under "Actions", click **Runner groups**.
   - **If using an enterprise-level group**:
     a. In the enterprise account sidebar, click ⚖ **Policies**.
     b. Under "⚖ Policies", click **Actions**.
     c. Click the **Runner groups** tab.
3. In the list of groups, click the runner group you'd like to configure.
4. Enter the new runner group name in the text field under "Group name."
5. Click **Save**.

Automatically adding a self-hosted runner to a group

You can use the configuration script to automatically add a new runner to a group. For example, this command registers a new runner and uses the `--runnergroup` parameter to add it to a group named `rg-runnergroup`.

```
./config.sh --url $org_or_enterprise_url --token $token --runnergroup rg-runnergrou
```

The command will fail if the runner group doesn't exist:

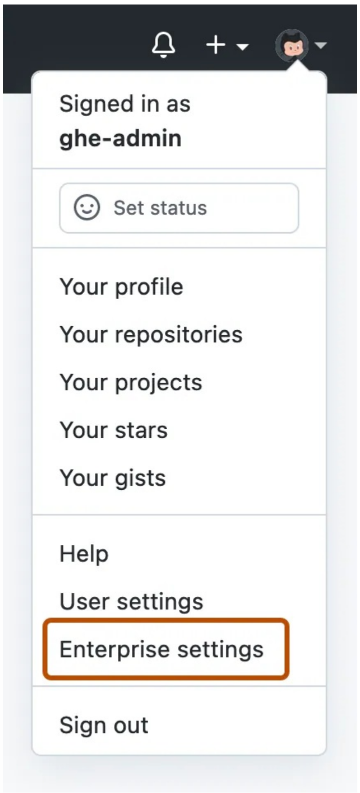
```
Could not find any self-hosted runner group named "rg-runnergroup".
```

Moving a self-hosted runner to a group

If you don't specify a runner group during the registration process, your new runners are automatically assigned to the default group, and can then be moved to another group.

1. Navigate to where your runner is registered:
   - **In an organization**: navigate to the main page and click ⚙ **Settings**.
   - **If using an enterprise-level runner**:

     a. In the top-right corner of GitHub Enterprise Server, click your profile photo, then click **Enterprise settings**.



2. Navigate to the GitHub Actions settings:
   - **In an organization**:

     a. In the left sidebar, click **Actions**.

     b. In the left sidebar, under "Actions", click **Runners**.

   - **If using an enterprise-level runner**:

     a. In the enterprise account sidebar, click ⚖ **Policies**.

     b. Under "⚖ Policies", click **Actions**.

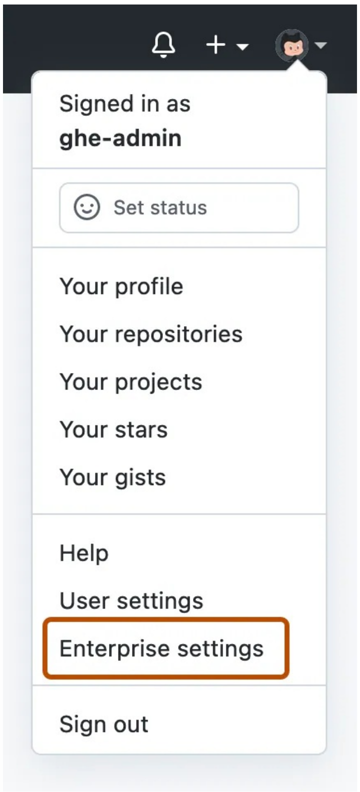
     c. Click the **Runners** tab.

3. In the "Runners" list, click the runner that you want to configure.
4. Select the **Runner group** drop-down.
5. In "Move runner to group", choose a destination group for the runner.

Removing a self-hosted runner group

Runners are automatically returned to the default group when their group is removed.

1. Navigate to where your runner groups are located:
   - **In an organization**:
     a. Navigate to the main page and click ⚙ **Settings**.
   - **If using an enterprise-level group**:
     a. In the top-right corner of GitHub Enterprise Server, click your profile photo, then click **Enterprise settings**.



2. Navigate to the "Runner groups" settings:
   - **In an organization**:
     a. In the left sidebar, click **Actions**.
     b. In the left sidebar, under "Actions", click **Runner groups**.
   - **If using an enterprise-level group**:

   a. In the enterprise account sidebar, click ⚖ **Policies**.

   b. Under "⚖ Policies", click **Actions**.

   c. Click the **Runner groups** tab.

3. In the list of groups, to the right of the group you want to delete, click •••.
4. To remove the group, click **Remove group**.
5. Review the confirmation prompts, and click **Remove this runner group**. Any runners still in this group will be automatically moved to the default group, where they will inherit the access permissions assigned to that group.