Setting a personal access token policy for your organization

In this article

Restricting access by fine-grained personal access tokens

Enforcing an approval policy for fine-grained personal access tokens

Restricting access by personal access tokens (classic)

Organization owners can control whether to allow fine-grained personal access tokens and personal access tokens (classic), and can require approval for fine-grained personal access tokens.

> **Note**: Fine-grained personal access token are currently in beta and subject to change. To leave feedback, see [the feedback discussion](#).
>
> During the beta, organizations must opt in to fine-grained personal access tokens. If your organization is owned by an enterprise, and the enterprise has opted in to fine-grained personal access tokens, then your organization is opted in by default. If your organization has not already opted-in, then you will be prompted to opt-in and set policies when you follow the steps below.

Restricting access by fine-grained personal access tokens 🔗

Organization owners can prevent fine-grained personal access tokens from accessing resources owned by the organization. Fine-grained personal access tokens will still be able to read public resources within the organization. This setting only controls access by fine-grained personal access tokens, not personal access tokens (classic). For more information about restricting access by personal access tokens (classic), see "[Restricting access by personal access tokens (classic)](#)" on this page.

If your organization is owned by an enterprise, and your enterprise owner has restricted access by fine-grained personal access tokens, then you cannot override the policy in your organization. For more information, see "[Enforcing policies for personal access tokens in your enterprise](#)."

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

2 Next to the organization, click **Settings**.

3 In the left sidebar, under 🔑 **Personal access tokens**, click **Settings**.

4 Under **Fine-grained personal access tokens**, select the option that meets your needs:

- **Allow access via fine-grained personal access tokens**: Fine-grained personal access tokens can access resources owned by the organization.
- **Restrict access via fine-grained personal access tokens**: Fine-grained personal access tokens cannot access resources owned by the organization. SSH keys created by fine-grained personal access tokens will continue to work.
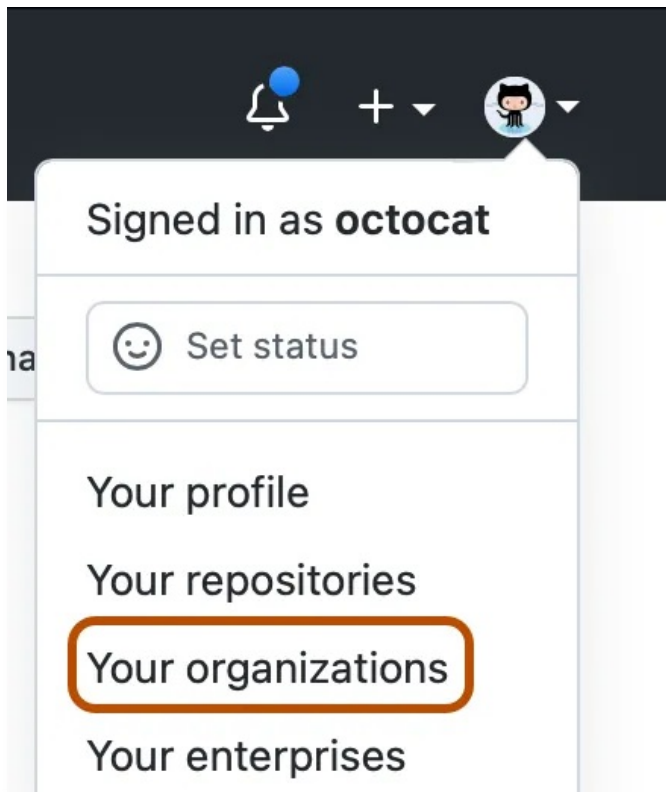
5 Click **Save**.

Enforcing an approval policy for fine-grained personal access tokens 🔗

Organization owners can require approval for each fine-grained personal access token that can access the organization. Fine-grained personal access tokens will still be able to read public resources within the organization without approval. Fine-grained personal access tokens created by organization owners will not need approval.

If your organization is owned by an enterprise, and your enterprise owner has set an approval policy for fine-grained personal access tokens, then you cannot override the policy in your organization. For more information, see "Enforcing policies for personal access tokens in your enterprise."

> **Note**: Only fine-grained personal access tokens, not personal access tokens (classic), are subject to approval. Unless the organization has restricted access by personal access tokens (classic), any personal access token (classic) can access organization resources without prior approval. For more information, see "Restricting access by personal access tokens (classic)" on this page.

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

2. Next to the organization, click **Settings**.

3. In the left sidebar, under 🔑 **Personal access tokens**, click **Settings**.

4. Under **Require approval of fine-grained personal access tokens**, select the option that meets your needs:

   - **Require administrator approval**: An organization owner must approve each fine-grained personal access token that can access the organization. Fine-grained personal access tokens created by organization owners will not need approval.
   - **Do not require administrator approval**: Fine-grained personal access tokens created by organization members can access resources in the organization without prior approval.

5. Click **Save**.

Restricting access by personal access tokens (classic) 🔗

Organization owners can prevent personal access tokens (classic) from accessing resources owned by the organization. Personal access tokens (classic) will still be able to read public resources within the organization. This setting only controls access by personal access tokens (classic), not fine-grained personal access tokens. For more information about restricting access by fine-grained personal access tokens, see "Restricting access by fine-grained personal access tokens" on this page.

If your organization is owned by an enterprise, and your enterprise owner has restricted access by personal access tokens (classic), then you cannot override the policy in your organization. For more information, see "Enforcing policies for personal access tokens in

1. In the top right corner of GitHub Enterprise Server, click your profile photo, then click **Your organizations**.
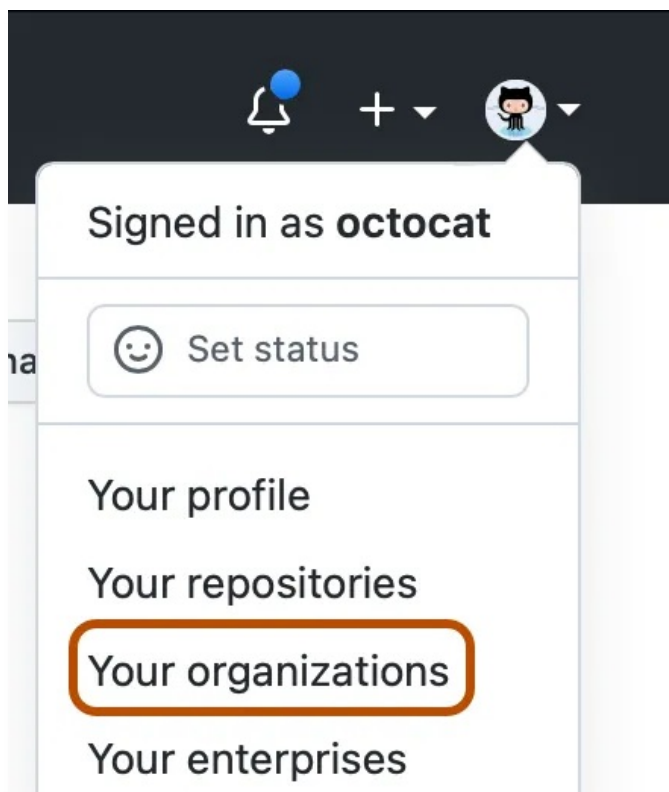
2. Next to the organization, click **Settings**.

3. In the left sidebar, under 🔑 **Personal access tokens**, click **Settings**.

4. Under **Personal access token (classic)**, select the option that meets your needs:

   - **Allow access via personal access tokens (classic)**: Personal access tokens (classic) can access resources owned by the organization.
   - **Restrict access via personal access tokens (classic)**: Personal access tokens (classic) cannot access resources owned by the organization. SSH keys created by personal access tokens (classic) will continue to work.

5. Click **Save**.

Legal