Enforcing policies for personal access tokens in your enterprise

In this article

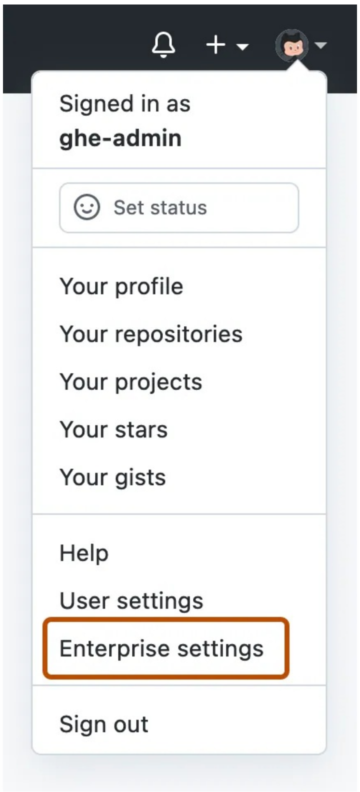
Enterprise owners can control whether to allow fine-grained personal access tokens and personal access tokens (classic), and can require approval for fine-grained personal access tokens.

> **Note**: Fine-grained personal access token are currently in beta and subject to change. To leave feedback, see [the feedback discussion].
>
> During the beta, enterprises must opt in to fine-grained personal access tokens. If your enterprise has not already opted-in, then you will be prompted to opt-in and set policies when you follow the steps below.
>
> Even if an enterprise has not opted in to fine-grained personal access tokens, organizations owned by the enterprise can still opt in. All users, including Enterprise Managed Users, can create fine-grained personal access tokens that can access resources owned by the user (such as repositories created under their account) even if the enterprise has not opted in to fine-grained personal access tokens.

Restricting access by fine-grained personal access tokens

Enterprise owners can prevent fine-grained personal access tokens from accessing private and internal resources owned by the enterprise. Fine-grained personal access tokens will still be able to access public resources within the organizations. 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.

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 **Personal access tokens**.

4. Under **Restrict access via fine-grained personal access tokens**, select the option that meets your needs:

    - **Allow organizations to configure access requirements**: Each organization owned by the enterprise can decide whether to restrict access by fine-grained personal access tokens.
    - **Restrict access via fine-grained personal access tokens**: Fine-grained personal access tokens cannot access organizations owned by the enterprise. SSH keys created by fine-grained personal access tokens will continue to work. Organizations cannot override this setting.
    - **Allow access via fine-grained personal access tokens**: Fine-grained personal access tokens can access organizations owned by the enterprise. Organizations cannot override this setting.

5. Click **Save**.

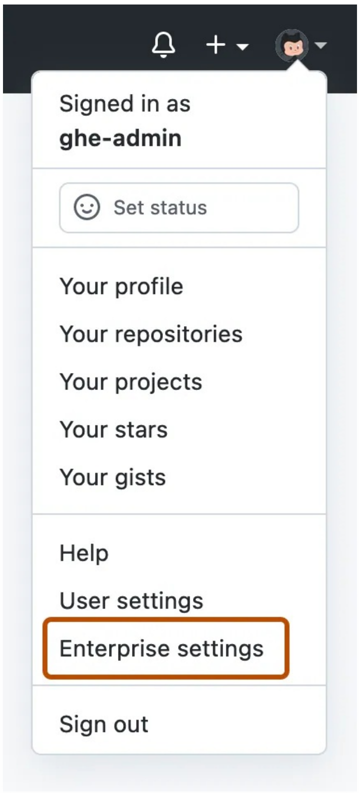
Enforcing an approval policy for fine-grained personal access tokens

Enterprise owners can require that all organizations owned by the enterprise must approve 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. Conversely, enterprise owners can allow fine-grained personal access tokens to access organizations in the enterprise without prior approval. Enterprise owners can also let each organization in the enterprise choose their own approval settings.

> **Note**: Only fine-grained personal access tokens, not personal access tokens (classic), are subject to approval. Unless the organization or enterprise has restricted access by personal access

tokens (classic), any personal access token (classic) can access organization resources without prior approval. For more information about restricting personal access tokens (classic), see "Restricting access by personal access tokens (classic)" on this page and "Setting a personal access token policy for your organization."

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 **Personal access tokens**.

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

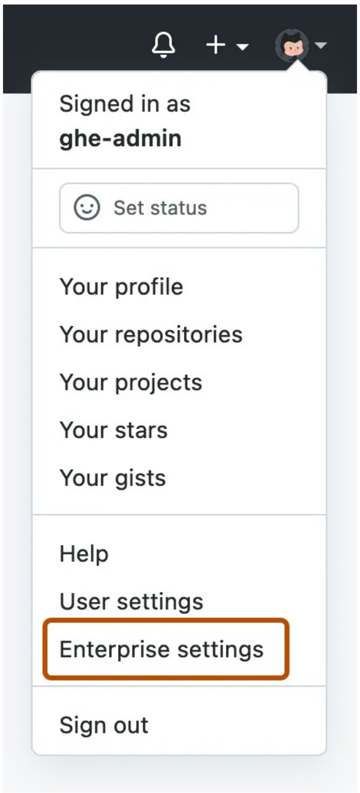
   - **Allow organizations to configure approval requirements**: Each organization owned by the enterprise can decide whether to require approval of fine-grained personal access token that can access the organization.
   - **Require organizations to use the approval flow**: All organizations owned by the enterprise 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. Organizations cannot override this setting.
   - **Disable the approval flow in all organizations**: Fine-grained personal access tokens created by organization members can access organizations owned by the enterprise without prior approval. Organizations cannot override this setting.

5. Click **Save**.

Restricting access by personal access tokens (classic)

Enterprise owners can prevent personal access tokens (classic) from accessing the enterprise and organizations owned by the enterprise. Personal access tokens (classic) will still be able to access 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.

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 **Personal access tokens**.
4. Under **Restrict personal access tokens (classic) from accessing your organizations**, select the option that meets your needs:
   - **Allow organizations to configure personal access tokens (classic) access requirements**: Each organization owned by the enterprise can decide whether to restrict access by personal access tokens (classic).
   - **Restrict access via personal access tokens (classic)**: Personal access tokens (classic) cannot access the enterprise or organizations owned by the enterprise. SSH keys created by personal access tokens (classic) will continue to work. Organizations cannot override this setting.
   - **Allow access via personal access tokens (classic)**: Personal access tokens (classic) can access the enterprise and organizations owned by the enterprise. Organizations cannot override this setting.
5. Click **Save**.