Reviewing and revoking personal access tokens in your organization

In this article

Organization owners can review the fine-grained personal access tokens that can access their organization. They can also revoke access of specific 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.

About reviewing and revoking fine-grained personal access tokens

Organization owners can view all fine-grained personal access tokens that can access resources owned by the organization. Organization owners can also revoke access by fine-grained personal access tokens. When a fine-grained personal access token is revoked, SSH keys created by the token will continue to work and the token will still be able to read public resources within the organization.

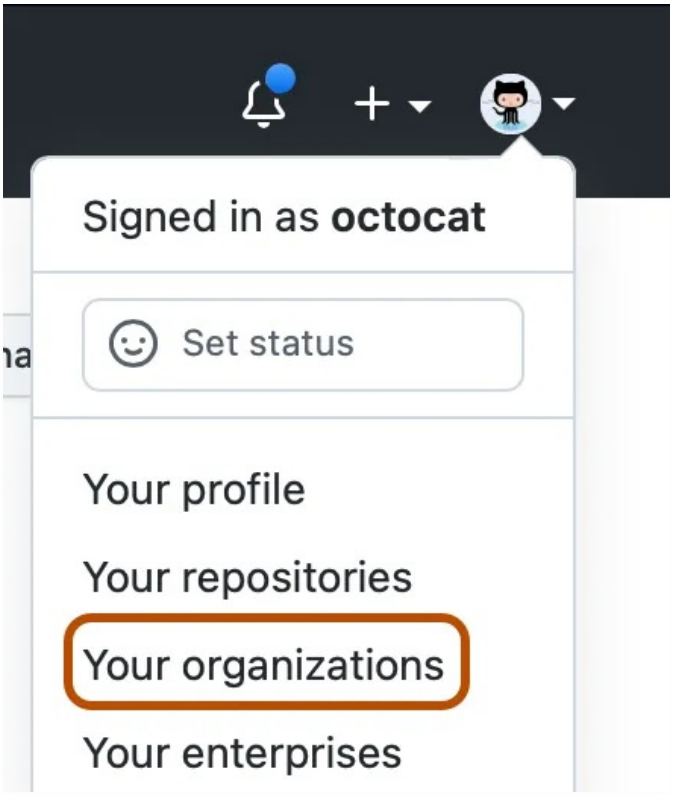
When a token is revoked, the user who created the token will receive an email notification.

Organization owners can only view and revoke fine-grained personal access tokens, not personal access tokens (classic). Unless the organization or enterprise has restricted access by personal access tokens (classic), any personal access token (classic) can access organization resources until the token expires. For more information about restricting access by personal access tokens (classic), see "Setting a personal access token policy for your organization" and "Enforcing policies for personal access tokens in your enterprise".

Organization owners can also use the REST API to review and revoke fine-grained personal access tokens. These endpoints can only be called by GitHub Apps, and cannot be called with personal access tokens or OAuth apps. For more information, see "Organizations."

Reviewing and revoking fine-grained personal access tokens

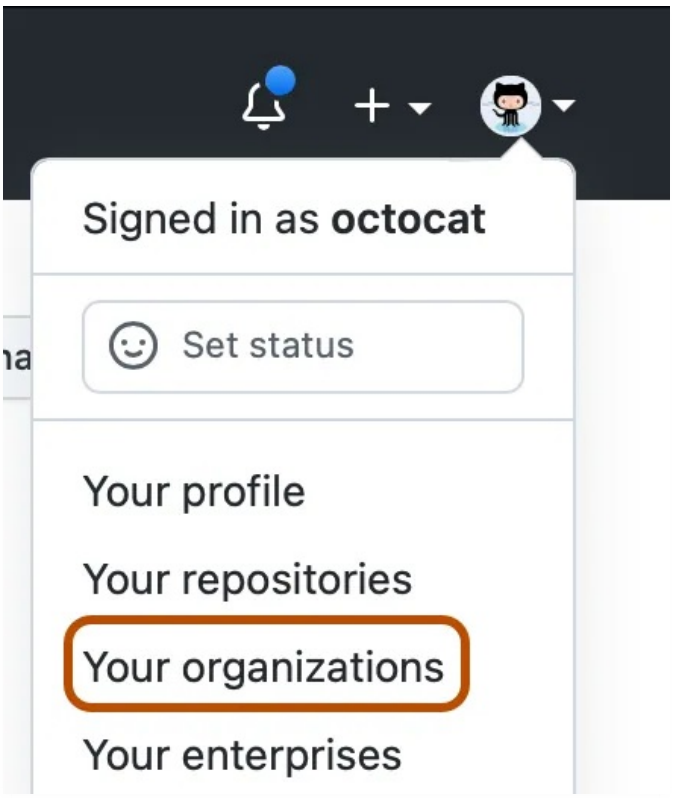
1. In the top right corner of GitHub Enterprise Server, click your profile photo, then click **Your organizations**.



2. Next to the organization, click **Settings**.
3. In the left sidebar, under **Personal access tokens**, click **Active tokens**. Any fine-grained personal access tokens that can access your organization will be displayed.
4. Click the name of the token that you want review or revoke.
5. Review the access and permissions that the token has.
6. To revoke access by the token to the organization, click **Revoke**.

Alternatively, you can revoke multiple tokens at once:

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 **Active tokens**. Any fine-grained personal access tokens that can access your organization will be displayed.
4. Optionally, use filters to only display certain tokens.
    - Use the **Owner** dropdown to filter the tokens by the member who created the token.
    - Use the **Repository** dropdown to filter the tokens by repository access.
    - Use the **Permissions** dropdown to filter the tokens by permission.
5. Select each token that you want to revoke.
6. Select the **tokens selected...** dropdown menu and click **Revoke...**.