Managing requests for personal access tokens in your organization

In this article

Organization owners can approve or deny fine-grained personal access tokens that request access to their organization.

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 fine-grained personal access token requests

When organization members create a fine-grained personal access token to access resources owned by the organization, if the organization requires approval for fine-grained personal access tokens, then an organization owner must approve the token before it can be used to access any resources that are not public. For more information, see "Setting a personal access token policy for your organization."

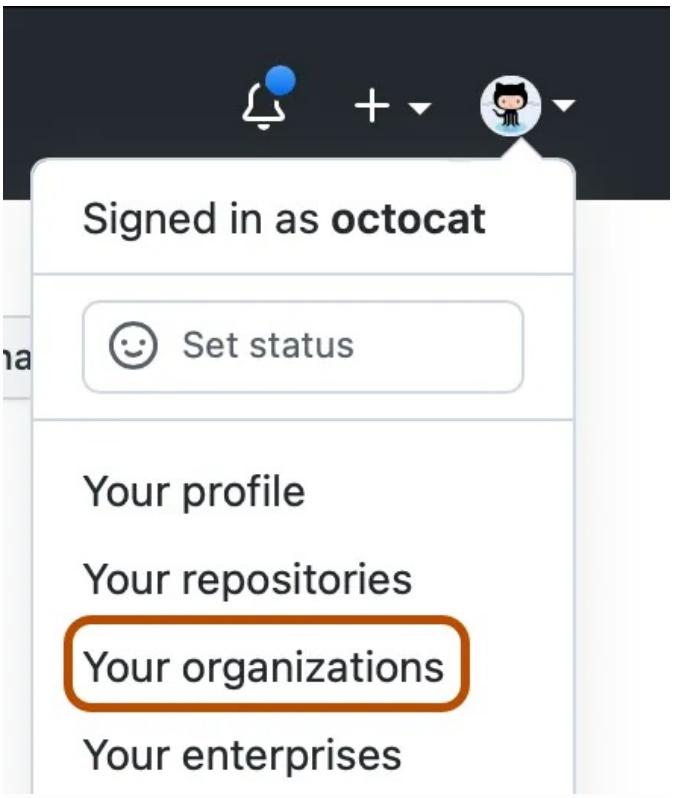
GitHub will notify organization owners with a daily email about all fine-grained personal access tokens that are awaiting approval. When a token is denied or approved, the user who created the token will receive an email notification.

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 "Setting a personal access token policy for your organization."

Organization owners can also use the REST API to review and manage fine-grained personal access token requests. 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."

Managing fine-grained personal access token requests

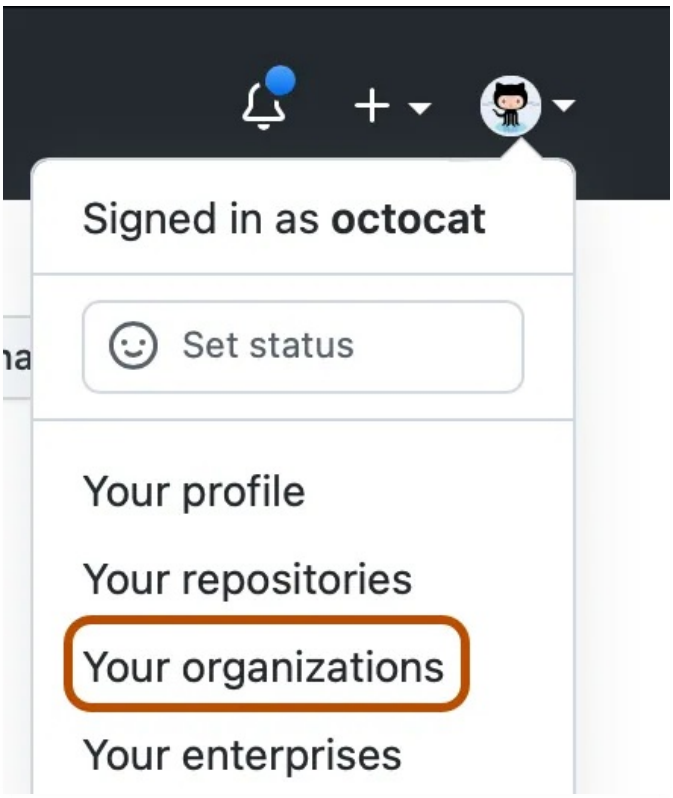
1. In the top right corner of GitHub.com, click your profile photo, then click **Your organizations**.



2. Next to the organization, click **Settings**.
3. In the left sidebar, under **Personal access tokens**, click **Pending requests**. If any tokens are pending approval for your organization, they will be displayed.
4. Click the name of the token that you want to approve or deny.
5. Review the access and permissions that the token is requesting.
6. To grant the token access to the organization, click **Approve**. To deny the token access to the organization, click **Deny**.
7. If you denied the request, in the confirmation box, optionally enter the reason that you denied the token. This reason will be shared in the notification that is sent to the token owner. Then, click **Deny**.

Alternatively, you can approve or deny multiple tokens at once:

1. In the top right corner of GitHub.com, 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 **Pending requests**. If any tokens are pending approval for your organization, they 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 approve or reject.
6. Select the **request selected...** dropdown menu and click **Approve...** or **Deny...**.