Authorizing a personal access token for use with SAML single sign-on

To use a personal access token (classic) with an organization that uses SAML single sign-on (SSO), you must first authorize the token.

You must authorize your personal access token (classic) after creation before the token can access an organization that uses SAML single sign-on (SSO). For more information about creating a new personal access token (classic), see "Managing your personal access tokens." Fine-grained personal access tokens are authorized during token creation, before access to the organization is granted.

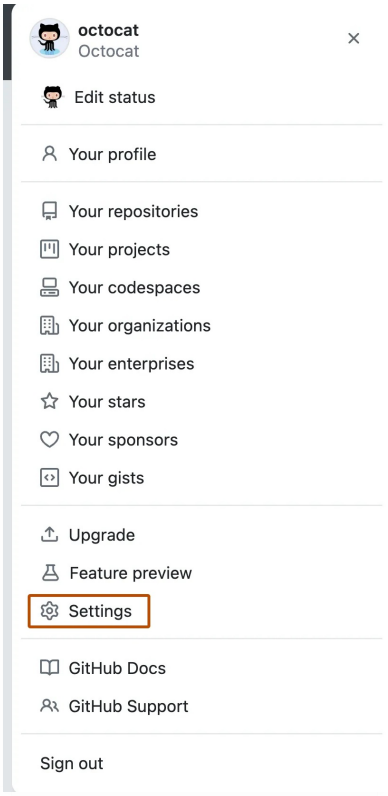
> **Note:** If you have a linked identity for an organization, you can only use authorized personal access tokens and SSH keys with that organization, even if SAML is not enforced. You have a linked identity for an organization if you've ever authenticated via SAML SSO for that organization, unless an organization or enterprise owner later revoked the linked identity. For more information about revoking linked identities, see "Viewing and managing a member's SAML access to your organization" and "Viewing and managing a user's SAML access to your enterprise."

Before you can authorize a personal access token or SSH key, you must have a linked SAML identity. If you're a member of an organization where SAML SSO is enabled, you can create a linked identity by authenticating to your organization with your IdP at least once. For more information, see "About authentication with SAML single sign-on."

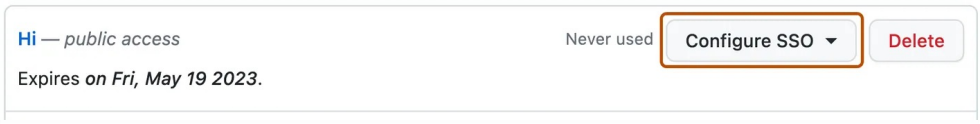
After you authorize a personal access token or SSH key, the token or key will stay authorized until revoked in one of the following ways.

- An organization or enterprise owner revokes the authorization.
- You are removed from the organization.
- The scopes in a personal access token are edited, or the token is regenerated.
- The personal access token expired as defined during creation.

1. In the upper-right corner of any page, click your profile photo, then click **Settings**.



2. In the left sidebar, click <> **Developer settings**.
3. In the left sidebar, click **Personal access tokens**.
4. Next to the token you'd like to authorize, click **Configure SSO**. If you don't see **Configure SSO**, ensure that you have authenticated at least once through your SAML IdP to access resources on GitHub.com. For more information, see "About authentication with SAML single sign-on."



5. In the dropdown menu, to the right of the organization you'd like to authorize the token for, click **Authorize**.

Further reading

- "Managing your personal access tokens"
- "About authentication with SAML single sign-on"