Authorizing an SSH key for use with SAML single sign-on

In this article

To use an SSH key with an organization that uses SAML single sign-on (SSO), you must first authorize the key.

About authorization of SSH keys

You can authorize an existing SSH key, or create a new SSH key and then authorize it. For more information about creating a new SSH key, see "Generating a new SSH key and adding it to the ssh-agent."

> **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.

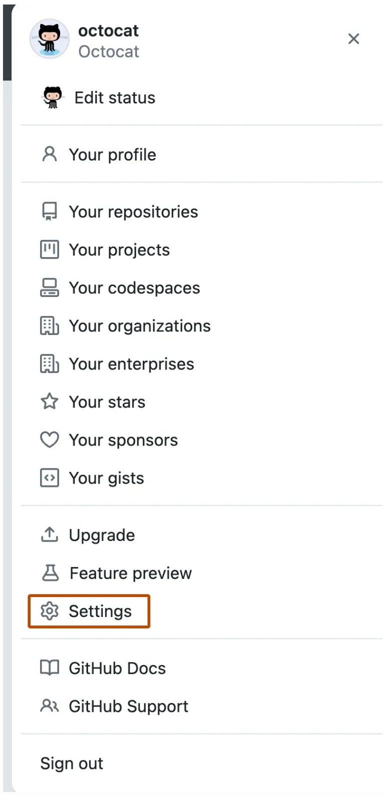
- An organization or enterprise owner revokes the authorization.
- You are removed from the organization.
- The scopes in a personal access token are edited, or the token is regenerated.
- The personal access token expired as defined during creation.

> **Note:** If your SSH key authorization is revoked by an organization, you will not be able to reauthorize the same key. You will need to create a new SSH key and authorize it. For more information about creating a new SSH key, see "Generating a new SSH key and adding it to the ssh-agent."

You do not need to authorize SSH certificates signed by your organization's SSH certificate authority (CA).

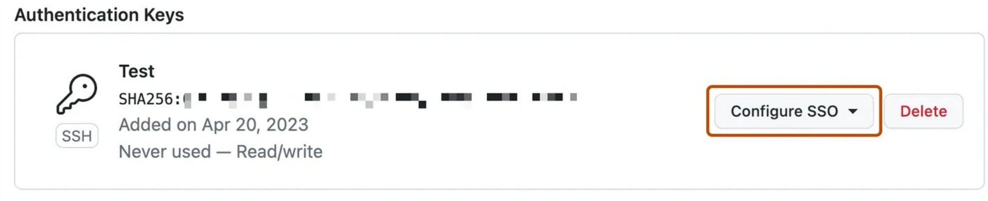
Authorizing an SSH key

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



2. In the "Access" section of the sidebar, click 🔑 **SSH and GPG keys**.

3. To the right of the SSH key 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."



Authentication Keys

Test
SHA256:[redacted]
Added on Apr 20, 2023
Never used — Read/write

4. In the dropdown menu, to the right of the organization you'd like to authorize the SSH key for, click **Authorize**.

Further reading

- "Checking for existing SSH keys"
- "About authentication with SAML single sign-on"

Legal

Terms Privacy Status Pricing Expert services Blog