About authentication with SAML single sign-on

In this article

About authentication with SAML SSO

Linked SAML identities

Authorizing personal access tokens and SSH keys with SAML SSO

About OAuth apps, GitHub Apps, and SAML SSO

Further reading

You can access an organization that uses SAML single sign-on (SSO) by authenticating through an identity provider (IdP).

About authentication with SAML SSO

SAML single sign-on (SSO) gives organization owners and enterprise owners using GitHub Enterprise Cloud a way to control and secure access to organization resources like repositories, issues, and pull requests. Organization owners can invite your personal account on GitHub to join their organization that uses SAML SSO, which allows you to contribute to the organization and retain your existing identity and contributions on GitHub.

If you're a member of an enterprise with managed users, you will instead use a new account that is provisioned for you and controlled by your enterprise. For more information, see "Types of GitHub accounts."

When you attempt to access most resources within an organization that uses SAML SSO, GitHub will redirect you to the organization's SAML IdP to authenticate. After you successfully authenticate with your account on the IdP, the IdP redirects you back to GitHub, where you can access the organization's resources.

IdP authentication is not required for accessing public repositories in certain ways:

- Viewing the repository's overview page and file contents on GitHub
- Forking the repository
- Performing read operations via Git, such as cloning the repository

Authentication is required for other access to public repositories, such as viewing issues, pull requests, projects, and releases.

Note: SAML authentication is not required for outside collaborators. For more information about outside collaborators, see "Roles in an organization."

If you have recently authenticated with your organization's SAML IdP in your browser, you are automatically authorized when you access a GitHub organization that uses SAML SSO. If you haven't recently authenticated with your organization's SAML IdP in your browser, you must authenticate at the SAML IdP before you can access the organization.

You must periodically authenticate with your SAML IdP to authenticate and gain access

to the organization's resources on GitHub.com. The duration of this login period is specified by your IdP and is generally 24 hours. This periodic login requirement limits the length of access and requires you to re-identify yourself to continue. You can view and manage your active SAML sessions in your security settings. For more information, see "Viewing and managing your active SAML sessions."

Linked SAML identities

When you authenticate with your IdP account and return to GitHub, GitHub will record a link in the organization or enterprise between your GitHub personal account and the SAML identity you signed into. This linked identity is used to validate your membership in that organization, and depending on your organization or enterprise setup, is also used to determine which organizations and teams you're a member of as well. Each GitHub account can be linked to exactly one SAML identity per organization. Likewise, each SAML identity can be linked to exactly one GitHub account in an organization.

If you sign in with a SAML identity that is already linked to another GitHub account, you will receive an error message indicating that you cannot sign in with that SAML identity. This situation can occur if you are attempting to use a new GitHub account to work inside of your organization. If you didn't intend to use that SAML identity with that GitHub account, then you'll need to sign out of that SAML identity and then repeat the SAML login. If you do want to use that SAML identity with your GitHub account, you'll need to ask your admin to unlink your SAML identity from your old account, so that you can link it to your new account. Depending on the setup of your organization or enterprise, your admin may also need to reassign your identity within your SAML provider. For more information, see "Viewing and managing a member's SAML access to your organization."

If the SAML identity you sign in with does not match the SAML identity that is currently linked to your GitHub account, you'll receive a warning that you are about to relink your account. Because your SAML identity is used to govern access and team membership, continuing with the new SAML identity can cause you to lose access to teams and organizations inside of GitHub. Only continue if you know that you're supposed to use that new SAML identity for authentication in the future.

Authorizing personal access tokens and SSH keys with SAML SSO

To use the API or Git on the command line to access protected content in an organization that uses SAML SSO, you will need to use an authorized personal access token over HTTPS or an authorized SSH key.

If you don't have a personal access token or an SSH key, you can create a personal access token for the command line or generate a new SSH key. For more information, see "Managing your personal access tokens" or "Generating a new SSH key and adding it to the ssh-agent."

To use a new or existing personal access token or SSH key with an organization that uses or enforces SAML SSO, you will need to authorize the token or authorize the SSH key for use with a SAML SSO organization. For more information, see "Authorizing a personal access token for use with SAML single sign-on" or "Authorizing an SSH key for use with SAML single sign-on."

About OAuth apps, GitHub Apps, and SAML SSO

You must have an active SAML session each time you authorize an OAuth app or GitHub App to access an organization that uses or enforces SAML SSO. You can create an active SAML session by navigating to `https://github.com/orgs/ORGANIZATION-NAME/sso` in your

browser.

After an enterprise or organization owner enables or enforces SAML SSO for an organization, and after you authenticate via SAML for the first time, you must reauthorize any OAuth apps or GitHub Apps that you previously authorized to access the organization.

To see the OAuth apps you've authorized, visit your OAuth apps page. To see the GitHub Apps you've authorized, visit your GitHub Apps page.

For more information, see "SAML and GitHub Apps."

Further reading

- "About identity and access management with SAML single sign-on"