Connecting your identity provider to your organization

In this article

About connection of your IdP to your organization

SAML metadata

To use SAML single sign-on and SCIM, you must connect your identity provider (IdP) to your organization on GitHub Enterprise Cloud.

About connection of your IdP to your organization 🔗

When you enable SAML SSO for your GitHub Enterprise Cloud organization, you connect your identity provider (IdP) to your organization. For more information, see "Enabling and testing SAML single sign-on for your organization."

> **Note:** To use SAML single sign-on, your organization must use GitHub Enterprise Cloud. For more information about how you can try GitHub Enterprise Cloud for free, see "Setting up a trial of GitHub Enterprise Cloud."

You can find the SAML and SCIM implementation details for your IdP in the IdP's documentation.

- Active Directory Federation Services (AD FS) SAML
- Azure Active Directory (Azure AD) SAML and SCIM
- Okta SAML and SCIM
- OneLogin SAML and SCIM
- PingOne SAML
- Shibboleth SAML

> **Note:** GitHub Enterprise Cloud supported identity providers for SCIM are Azure AD, Okta, and OneLogin. For more information about SCIM, see "About SCIM for organizations."
>
> You cannot use this implementation of SCIM with an enterprise account or with an organization with managed users. If your enterprise is enabled for Enterprise Managed Users, you must use a different implementation of SCIM. Otherwise, SCIM is not available at the enterprise level. For more information, see "Configuring SCIM provisioning for Enterprise Managed Users."

SAML metadata 🔗

For more information about SAML metadata for your organization, see "SAML configuration reference."

Legal