Securing enterprise resources with single sign-on

Learn how to set up secure sign-on for organizations in your enterprise.

This article applies to enterprises that use **personal accounts**. If you use personal accounts, enabling SSO is an optional step you can take to secure your enterprise's resources.

If your enterprise uses **managed users**, SSO is mandatory, and all managed user accounts must authenticate through your identity provider (IdP) to sign in to GitHub. See Configuring SAML single sign-on for Enterprise Managed Users.

Single sign-on (SSO) gives organization owners and enterprise owners a way to control and secure access to organization resources like repositories, issues, and pull requests. See About SAML for enterprise IAM.

You can configure SAML for your enterprise account to apply the same settings to all organizations, or you can configure settings for individual organizations. See Deciding whether to configure SAML for your enterprise or your organizations.

You can enable SAML SSO and centralized authentication through a SAML IdP across all organizations owned by your enterprise account. See Configuring SAML single sign-on for your enterprise.

Supported identity providers

GitHub supports SAML SSO with IdPs that implement the SAML 2.0 standard. For more information, see the SAML Wiki on the OASIS website.

GitHub officially supports and internally tests the following IdPs for SAML.

- Microsoft Active Directory Federation Services (AD FS)
- Microsoft Entra ID (previously known as Azure AD)
- Okta
- OneLogin
- PingOne
- Shibboleth

For more information about connecting Microsoft Entra ID (previously known as Azure AD) to your enterprise, see Tutorial: Microsoft Entra SSO integration with GitHub Enterprise Cloud - Enterprise Account in Microsoft Docs.

Next steps

Next, learn how to set up an organization in your enterprise. See Setting up an organization.