Preparing to enforce SAML single sign-on in your organization

Before you enforce SAML single sign-on in your organization, you should verify your organization's membership and configure the connection settings to your identity provider.

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."

When you enforce SAML SSO, all members of the organization must authenticate through your IdP to access the organization's resources. Before enforcing SAML SSO in your organization, you should review organization membership, enable SAML SSO, and review organization members' SAML access. For more information, see the following.

Task	More information
Add or remove members from your organization	• "Inviting users to join your organization" • "Removing a member from your organization"
Connect your IdP to your organization by enabling SAML SSO	• "Connecting your identity provider to your organization" • "Enabling and testing SAML single sign-on for your organization"
Ensure that your organization members have signed in and linked their accounts with the IdP	• "Viewing and managing a member's SAML access to your organization"

After you finish these tasks, you can enforce SAML SSO for your organization. For more information, see "Enforcing SAML single sign-on for your organization."

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