

About SAML for enterprise IAM

In this article

About SAML SSO for your enterprise on GitHub.com

Supported IdPs

Further reading

You can use SAML single sign-on (SSO) to centrally manage access to organizations owned by your enterprise on GitHub.com.

About SAML SSO for your enterprise on GitHub.com



If your enterprise members manage their own user accounts on GitHub.com, you can configure SAML authentication as an additional access restriction for your enterprise or organization. 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.

If you configure SAML SSO, members of your organization will continue to sign into their personal accounts on GitHub.com. When a member accesses most resources within your organization, GitHub redirects the member to your IdP to authenticate. After successful authentication, your IdP redirects the member back to GitHub. For more information, see "[About authentication with SAML single sign-on](#)."

Note: SAML SSO does not replace the normal sign-in process for GitHub. Unless you use Enterprise Managed Users, members will continue to sign into their personal accounts on GitHub.com, and each personal account will be linked to an external identity in your IdP.

Enterprise owners can enable SAML SSO and centralized authentication through a SAML IdP across all organizations owned by an enterprise account. After you enable SAML SSO for your enterprise account, SAML SSO is enforced for all organizations owned by your enterprise account. All members will be required to authenticate using SAML SSO to gain access to the organizations where they are a member, and enterprise owners will be required to authenticate using SAML SSO when accessing an enterprise account. For more information, see "[About authentication for your enterprise](#)" and "[Configuring SAML single sign-on for your enterprise](#)."

Alternatively, you can provision and manage the accounts of your enterprise members with Enterprise Managed Users. To help you determine whether SAML SSO or Enterprise Managed Users is better for your enterprise, see "[Identifying the best authentication method for your enterprise](#)."

If a SAML configuration error or an issue with your identity provider (IdP) prevents you from using SAML SSO, you can use a recovery code to access your enterprise. For more information, see "[Managing recovery codes for your enterprise](#)."

After you enable SAML SSO, depending on the IdP you use, you may be able to enable

additional identity and access management features.

Note: You cannot configure SCIM for your enterprise account unless your account was created for Enterprise Managed Users. For more information, see "[About Enterprise Managed Users](#)."

If you do not use Enterprise Managed Users, and you want to use SCIM provisioning, you must configure SAML SSO at the organization level, not the enterprise level. For more information, see "[About identity and access management with SAML single sign-on](#)."

If you use Azure AD as your IdP, you can use team synchronization to manage team membership within each organization. If team sync is enabled for your organization or enterprise account, you can synchronize a GitHub team with an IdP group. When you synchronize a GitHub team with an IdP group, membership changes to the IdP group are reflected on GitHub Enterprise Cloud automatically, reducing the need for manual updates and custom scripts. For more information, see "[Managing team synchronization for organizations in your enterprise](#)."

There are special considerations when enabling SAML SSO for your enterprise account if any of the organizations owned by the enterprise account are already configured to use SAML SSO. For more information, see "[Switching your SAML configuration from an organization to an enterprise account](#)."

For more information about the configuration of SAML SSO on GitHub Enterprise Cloud, see "[Configuring SAML single sign-on for your enterprise](#)." To learn how to configure both authentication and provisioning for GitHub.com with your specific IdP, see the articles for individual IdPs in "[Using SAML for enterprise IAM](#)."

Supported IdPs

We test and officially support the following IdPs. For SAML SSO, we offer limited support for all identity providers that implement the SAML 2.0 standard. For more information, see the [SAML Wiki](#) on the OASIS website.

IdP	SAML	Team synchronization
Active Directory Federation Services (AD FS)	✓	✗
Azure Active Directory (Azure AD)	✓	✓
Okta	✓	✗
OneLogin	✓	✗
PingOne	✓	✗
Shibboleth	✓	✗

Further reading

- [SAML Wiki](#) on the OASIS website

Legal