Configuring SAML single sign-on for your enterprise

In this article

You can control and secure access to resources like repositories, issues, and pull requests within your enterprise's organizations by enforcing SAML single sign-on (SSO) through your identity provider (IdP).

> **Who can use this feature**
> Enterprise owners can configure SAML SSO for an enterprise on GitHub Enterprise Cloud.

Note: If your enterprise uses Enterprise Managed Users, you must follow a different process to configure SAML single sign-on. For more information, see "Configuring SAML single sign-on for Enterprise Managed Users."

About 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.

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.

For more information, see "About identity and access management with SAML single sign-on."

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.

To access each organization's resources on GitHub Enterprise Cloud, the member must have an active SAML session in their browser. To access each organization's protected resources using the API and Git, the member must use a personal access token or SSH key that the member has authorized for use with the organization. Enterprise owners can view and revoke a member's linked identity, active sessions, or authorized credentials at any time. For more information, see "Viewing and managing a user's SAML access to your enterprise."

> **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."

When SAML SSO is disabled, all linked external identities are removed from GitHub Enterprise Cloud.

After you enable SAML SSO, OAuth app and GitHub App authorizations may need to be revoked and reauthorized before they can access the organization. For more information, see "Authorizing OAuth apps."

Supported identity providers

GitHub Enterprise Cloud 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.

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

For more information about connecting Azure AD to your enterprise, see Tutorial: Azure Active Directory SSO integration with GitHub Enterprise Cloud - Enterprise Account in Microsoft Docs.

Enforcing SAML single-sign on for organizations in your enterprise account

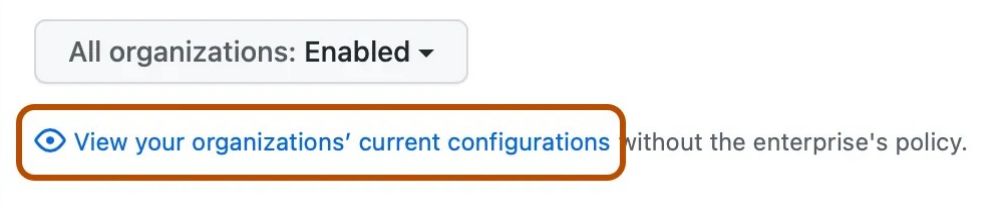
When you enforce SAML SSO for your enterprise, the enterprise configuration will override any existing organization-level SAML configurations. There are special considerations when enabling SAML SSO for your enterprise account if any of the organizations owned by the enterprise account are already configured to use SAML SSO. For more information, see "Switching your SAML configuration from an organization to an enterprise account."

When you enforce SAML SSO for an organization, GitHub removes any members of the organization that have not authenticated successfully with your SAML IdP. When you require SAML SSO for your enterprise, GitHub does not remove members of the enterprise that have not authenticated successfully with your SAML IdP. The next time a member accesses the enterprise's resources, the member must authenticate with your SAML IdP.

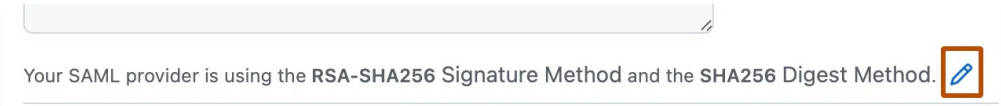
For more detailed information about how to enable SAML using Okta, see "Configuring

SAML single sign-on for your enterprise using Okta."

1. In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.
2. In the list of enterprises, click the enterprise you want to view.
3. In the enterprise account sidebar, click **Settings**.
4. Under **Settings**, click **Authentication security**.
5. Optionally, to view the current configuration for all organizations in the enterprise account before you change the setting, click **View your organizations' current configurations**.



6. Under "SAML single sign-on", select **Require SAML authentication**.
7. In the **Sign on URL** field, type the HTTPS endpoint of your IdP for single sign-on requests. This value is available in your IdP configuration.
8. Optionally, in the **Issuer** field, type your SAML issuer URL to verify the authenticity of sent messages.
9. Under **Public Certificate**, paste a certificate to verify SAML responses.
10. Under your public certificate, to the right of the current signature and digest methods, click .



11. Select the **Signature Method** and **Digest Method** dropdown menus, then click the hashing algorithm used by your SAML issuer.
12. Before enabling SAML SSO for your enterprise, to ensure that the information you've entered is correct, click **Test SAML configuration** . This test uses Service Provider initiated (SP-initiated) authentication and must be successful before you can save the SAML settings.
13. Click **Save**.
14. To ensure you can still access your enterprise in the event that your identity provider is ever unavailable in the future, click **Download**, **Print**, or **Copy** to save your recovery codes. For more information, see "Downloading your enterprise account's single sign-on recovery codes."

Further reading

- "Managing SAML single sign-on for your organization"