Configuring SAML single sign-on for Enterprise Managed Users

In this article

You can automatically manage access to your enterprise account on GitHub by configuring Security Assertion Markup Language (SAML) single sign-on (SSO).

To manage users in your enterprise with your identity provider, your enterprise must be enabled for Enterprise Managed Users, which is available with GitHub Enterprise Cloud. For more information, see "About Enterprise Managed Users."

About SAML single sign-on for Enterprise Managed Users

With Enterprise Managed Users, your enterprise uses your corporate identity provider to authenticate all members. Instead of signing in to GitHub with a GitHub username and password, members of your enterprise will sign in through your IdP.

Enterprise Managed Users supports the following IdPs:

- Azure Active Directory (Azure AD)
- Okta
- PingFederate

After you configure SAML SSO, we recommend storing your recovery codes so you can recover access to your enterprise in the event that your identity provider is unavailable.

If you currently use SAML SSO for authentication and would prefer to use OIDC and benefit from CAP support, you can follow a migration path. For more information, see "Migrating from SAML to OIDC."

Note: When SAML SSO is enabled, the only setting you can update on GitHub for your existing SAML configuration is the SAML certificate. If you need to update the Sign on URL or Issuer, you must first disable SAML SSO and then reconfigure SAML SSO with the new settings.

Configuring SAML single sign-on for Enterprise Managed Users

To configure SAML SSO for your enterprise with managed users, you must configure an application on your IdP and then configure your enterprise on GitHub.com. After you configure SAML SSO, you can configure user provisioning.

To install and configure the GitHub Enterprise Managed User application on your IdP, you must have a tenant and administrative access on a supported IdP.

> If you need to reset the password for your setup user, contact GitHub Support through the GitHub Support portal.

1. Configuring your identity provider
2. Configuring your enterprise
3. Enabling provisioning

Configuring your identity provider

To configure your IdP, follow the instructions they provide for configuring the GitHub Enterprise Managed User application on your IdP.

1. To install the GitHub Enterprise Managed User application, click the link for your IdP below:
    - GitHub Enterprise Managed User application on Azure Active Directory
    - GitHub Enterprise Managed User application on Okta
    - GitHub Enterprise Managed User connector on PingFederate

      To download the PingFederate connector, navigate to the **Add-ons** tab and select **GitHub EMU Connector 1.0**.

2. To configure the GitHub Enterprise Managed User application and your IdP, click the link below and follow the instructions provided by your IdP:
    - Azure Active Directory tutorial for Enterprise Managed Users
    - Okta documentation for Enterprise Managed Users
    - PingFederate documentation for Enterprise Managed Users

3. So you can test and configure your enterprise, assign yourself or the user that will be configuring SAML SSO on GitHub to the GitHub Enterprise Managed User application on your IdP.

4. To enable you to continue configuring your enterprise on GitHub, locate and note the following information from the application you installed on your IdP.

Value	Other names	Description
IdP Sign-On URL	Login URL, IdP URL	Application's URL on your IdP
IdP Identifier URL	Issuer	IdP's identifier to service providers for SAML authentication
Signing certificate, Base64-encoded	Public certificate	Public certificate that IdP uses to sign authentication requests

Configuring your enterprise

After you install and configure the GitHub Enterprise Managed User application on your identity provider, you can configure your enterprise.

1. Sign into GitHub.com as the setup user for your enterprise with the username **@SHORT-CODE_admin**, replacing SHORT-CODE with your enterprise's short code.

2. In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.

3. In the list of enterprises, click the enterprise you want to view.

4. In the enterprise account sidebar, click ⚙ **Settings**.

5. Under ⚙ **Settings**, click **Authentication security**.

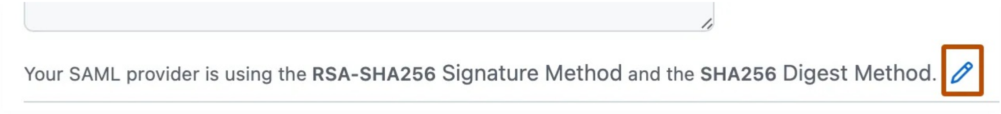
6. Under "SAML single sign-on", select **Require SAML authentication**.

7. Under **Sign on URL**, type the HTTPS endpoint of your IdP for single sign-on requests that you noted while configuring your IdP.

8. Under **Issuer**, type your SAML issuer URL that you noted while configuring your IdP, to verify the authenticity of sent messages.

9. Under **Public Certificate**, paste the certificate that you noted while configuring your IdP, to verify SAML responses.

10. Under your public certificate, to the right of the current signature and digest methods, click ✎.



Your SAML provider is using the **RSA-SHA256** Signature Method and the **SHA256** Digest Method.

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**.

> **Note:** When you require SAML SSO for your enterprise, the setup user will no longer have access to the enterprise but will remain signed in to GitHub. Only managed user accounts provisioned by your IdP will have access to the enterprise.

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."

Enabling provisioning

After you enable SAML SSO, enable provisioning. For more information, see "Configuring SCIM provisioning for Enterprise Managed Users."