Configuring SAML single sign-on for your enterprise using Okta

In this article

You can use Security Assertion Markup Language (SAML) single sign-on (SSO) with Okta to automatically manage access to your enterprise account 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 with Okta

You can control access to your enterprise account in GitHub Enterprise Cloud and other web applications from one central interface by configuring the enterprise account to use SAML SSO with Okta, an Identity Provider (IdP).

SAML SSO controls and secures access to enterprise account resources like organizations, repositories, issues, and pull requests. For more information, see "Configuring SAML single sign-on for 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."

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."

Alternatively, you can also configure SAML SSO using Okta for an organization that uses GitHub Enterprise Cloud. For more information, see "Configuring SAML single sign-on and SCIM using Okta."

Adding the GitHub Enterprise Cloud application in Okta

1. Sign into your Okta account.

2. Navigate to the GitHub Enterprise Cloud - Enterprise Accounts application in the Okta Integration Network and click **Add Integration**.

3. In the left sidebar, use the **Applications** dropdown and click **Applications**.

4. Optionally, to the right of "Application label", type a descriptive name for the application.

5. To the right of "GitHub Enterprises", type the name of your enterprise account. For example, if your enterprise account's URL is `https://github.com/enterprises/octo-corp`, type `octo-corp`.

6. Click **Done**.

Enabling and testing SAML SSO

1. Sign into your Okta account.

2. In the left sidebar, use the **Applications** dropdown and click **Applications**.

3. Click the label for the application you created for your enterprise account.

4. Assign the application to your user in Okta. For more information, see Assign applications to users in the Okta documentation.

5. Under the name of the application, click **Sign on**.

6. To the right of Settings, click **Edit**.

7. Under "Configured SAML Attributes", to the right of "groups", use the drop-down menu and select **Matches regex**.

8. To the right of the drop-down menu, type `.*.*`.

9. Click **Save**.

10. Under "SIGN ON METHODS", click **View Setup Instructions**.

11. Enable SAML for your enterprise account using the information in the setup instructions. For more information, see "Configuring SAML single sign-on for your enterprise."