Configuring OIDC for Enterprise Managed Users

In this article

You can automatically manage access to your enterprise account on GitHub by configuring OpenID Connect (OIDC) single sign-on (SSO) and enable support for your IdP's Conditional Access Policy (CAP).

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."

Note: OpenID Connect (OIDC) and Conditional Access Policy (CAP) support for Enterprise Managed Users is only available for Azure AD.

About OIDC for Enterprise Managed Users

With Enterprise Managed Users, your enterprise uses your identity provider (IdP) to authenticate all members. You can use OpenID Connect (OIDC) to manage authentication for your enterprise with managed users. Enabling OIDC SSO is a one-click setup process with certificates managed by GitHub and your IdP.

When your enterprise uses OIDC SSO, GitHub will automatically use your IdP's conditional access policy (CAP) IP conditions to validate user interactions with GitHub, when members change IP addresses, and each time a personal access token or SSH key is used. For more information, see "About support for your IdP's Conditional Access Policy."

You can adjust the lifetime of a session, and how often a managed user account needs to reauthenticate with your IdP, by changing the lifetime policy property of the ID tokens issued for GitHub from your IdP. The default lifetime is one hour. For more information, see "Configure token lifetime policies" in the Azure AD documentation.

Note: If you need assistance configuring the OIDC session lifetime, contact Microsoft Support.

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."

> **Warning:** If you use GitHub Enterprise Importer to migrate an organization from your GitHub Enterprise Server instance, make sure to use a service account that is exempt from Azure AD's CAP otherwise your migration may be blocked.

Identity provider support

Support for OIDC is available for customers using Azure Active Directory (Azure AD).

Each Azure AD tenant can support only one OIDC integration with Enterprise Managed Users. If you want to connect Azure AD to more than one enterprise on GitHub, use SAML instead. For more information, see "Configuring SAML single sign-on for Enterprise Managed Users."

OIDC does not support IdP-initiated authentication.

Configuring OIDC for Enterprise Managed Users

1. Sign into GitHub.com as the setup user for your new enterprise with the username **@*SHORT-CODE*_admin**.
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 "OpenID Connect single sign-on", select **Require OIDC single sign-on**.
7. To continue setup and be redirected to Azure AD, click **Save**.
8. After GitHub Enterprise Cloud redirects you to your IdP, sign in, then follow the instructions to give consent and install the GitHub Enterprise Managed User (OIDC) application. After Azure AD asks for permissions for GitHub Enterprise Managed Users with OIDC, enable **Consent on behalf of your organization**, then click **Accept**.

   > **Warning:** You must sign in to Azure AD as a user with global admin rights in order to consent to the installation of the GitHub Enterprise Managed User (OIDC) application.

9. 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."
10. Click **Enable OIDC Authentication**.

Enabling provisioning

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

Legal