Using Enterprise Managed Users for IAM

You can manage identity and access with your identity provider and provision accounts that can only contribute to your enterprise.

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 Enterprise Managed Users

You can centrally manage identity and access for your enterprise members on GitHub from your identity provider.

Configuring SAML single sign-on for Enterprise Managed Users

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

Configuring OIDC for Enterprise Managed Users

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).

Configuring SCIM provisioning for Enterprise Managed Users

You can configure your identity provider to provision new users and manage their membership in your enterprise and teams.

Configuring SCIM provisioning for Enterprise Managed Users with Okta

You can provision new users and manage their membership of your enterprise and teams using Okta as your identity provider.

Managing team memberships with identity provider groups

You can manage team and organization membership on GitHub Enterprise Cloud through your identity provider (IdP) by connecting IdP groups with teams within your enterprise with managed users.

Troubleshooting team membership with identity provider groups

If you manage team membership using groups on your identity provider (IdP), but team

membership is not in sync, you can troubleshoot the problem.

About support for your IdP's Conditional Access Policy

When your enterprise uses OIDC SSO, GitHub can validate access to your enterprise and its resources using your IdP's Conditional Access Policy (CAP).

Migrating from SAML to OIDC

If you're using SAML to authenticate members in your enterprise with managed users, you can migrate to OpenID Connect (OIDC) and benefit from support for your IdP's Conditional Access Policy.

Migrating from OIDC to SAML

If you're using OpenID Connect (OIDC) to authenticate members in your enterprise with managed users, you can migrate to SAML SSO.

Migrating your enterprise to a new identity provider or tenant

You can migrate your enterprise to a different identity provider (IdP) or Azure AD tenant.

Disabling authentication for Enterprise Managed Users

You can disable SAML single sign-on (SSO) or OIDC for Enterprise Managed Users by using a recovery code to sign in as the setup user.

Legal

© 2023 GitHub, Inc. Terms Privacy Status Pricing Expert services Blog