Securing your enterprise with Managed Users

Learn about Enterprise Managed Users.

In this article

Get started with managed users

Next steps

With Enterprise Managed Users, you manage the lifecycle and authentication of your users on GitHub.com or GHE.com from an external identity management system, or IdP:

- Your IdP **provisions new user accounts** on GitHub, with access to your enterprise.
- Users must **authenticate on your IdP** to access your enterprise's resources on GitHub.
- You control **usernames, profile data, organization membership, and repository access** from your IdP.
- If your enterprise uses OIDC SSO, GitHub will validate access to your enterprise and its resources using your IdP's **Conditional Access Policy (CAP)**. See [About support for your IdP's Conditional Access Policy](#).
- Managed user accounts **cannot create public content** or collaborate outside your enterprise. See [Abilities and restrictions of managed user accounts](#).

See [About Enterprise Managed Users](#).

Get started with managed users

To use Enterprise Managed Users, you will:

- Configure authentication using SAML or OIDC

- Configure SCIM provisioning
- Provision users to your enterprise

To get started, see [Getting started with Enterprise Managed Users](#).

Next steps

Next, learn how to set up an organization in your enterprise. See [Setting up an organization](#).

Legal

© 2025 GitHub, Inc.   [Terms](#)   [Privacy](#)   [Status](#)   [Pricing](#)   [Expert services](#)   [Blog](#)