About Enterprise Managed Users

In this article

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

About Enterprise Managed Users

With Enterprise Managed Users, you can control the user accounts of your enterprise members through your identity provider (IdP). Users assigned to the GitHub Enterprise Managed User application in your IdP are provisioned as new user accounts on GitHub and added to your enterprise. You control usernames, profile data, team membership, and repository access for the user accounts from your IdP.

In your IdP, you can give each managed user account the role of user, enterprise owner, or billing manager. Managed user accounts can own organizations within your enterprise and can add other managed user accounts to the organizations and teams within. For more information, see "Roles in an enterprise" and "About organizations."

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 grant managed user accounts access to and the ability to contribute to repositories within your enterprise, but managed user accounts cannot create public content or collaborate with other users, organizations, and enterprises on the rest of GitHub. For more information, see "Abilities and restrictions of managed user accounts."

The usernames of your enterprise's managed user accounts and their profile information, such as display names and email addresses, are set by through your IdP and cannot be changed by the users themselves. For more information, see "Usernames and profile information."

Enterprise owners can audit all of the managed user accounts' actions on GitHub. For more information, see "Audit log events for your enterprise."

To use Enterprise Managed Users, you need a separate type of enterprise account with Enterprise Managed Users enabled. For more information about creating this account, see "Getting started with Enterprise Managed Users."

Note: There are multiple options for identity and access management with GitHub Enterprise Cloud, and Enterprise Managed Users is not the best solution for every customer. For more information about whether Enterprise Managed Users is right for your enterprise, see "Identifying the best authentication method for your enterprise."

About organization membership management

Organization memberships can be managed manually, or you can update memberships automatically using IdP groups. To manage organization memberships through your IdP, the members must be added to an IdP group, and the IdP group must be connected to a team within the organization. For more information about managing organization and team memberships automatically, see "Managing team memberships with identity provider groups."

The way a member is added to an organization owned by your enterprise (through IdP groups or manually) determines how they must be removed from an organization.

- If a member was added to an organization manually, you must remove them manually. Unassigning them from the GitHub Enterprise Managed User application on your IdP will suspend the user but not remove them from the organization.
- If a user became a member of an organization because they were added to IdP groups mapped to one or more teams in the organization, removing them from *all* of the mapped IdP groups associated with the organization will remove them from the organization.

To discover how a member was added to an organization, you can filter the member list by type. For more information, see "Viewing people in your enterprise."

Identity provider support

Identity provider	SAML	OIDC
Azure Active Directory	✓	✓
Okta	✓	×
PingFederate	✓	×

Note: Enterprise Managed Users requires the use of one IdP for both SAML and SCIM. Confirm that you've purchased a version of your IdP that includes SCIM.

Abilities and restrictions of managed user accounts

Managed user accounts can only contribute to private and internal repositories within their enterprise and private repositories owned by their user account. Managed user accounts have read-only access to the wider GitHub community. These visibility and access restrictions for users and content apply to all requests, including API requests.

- Managed user accounts authenticate using only your identity provider, and have no password or two-factor authentication methods stored on GitHub. As a result, they do not see the sudo prompt when taking sensitive actions. For more information, see "Sudo mode."
- Managed user accounts cannot be invited to organizations or repositories outside of

the enterprise, nor can the managed user accounts be invited to other enterprises.

- Managed user accounts and the content they create is only visible to other members of the enterprise.
- Other GitHub users cannot see, mention, or invite a managed user account to collaborate.
- Managed user accounts can view all public repositories on GitHub.com, but cannot interact with repositories outside of the enterprise in any of the following ways:
  - Push code to the repository
  - Create issues or pull requests within the repository
  - Create or comment on discussions within the repository
  - Comment on issues or pull requests, or add reactions to comments
  - Star, watch, or fork the repository
- Managed user accounts cannot create gists or comment on gists.
- Managed user accounts cannot follow users outside of the enterprise.
- Managed user accounts cannot create starter workflows for GitHub Actions.
- Managed user accounts cannot install GitHub Apps on their user accounts.
- Managed user accounts can install GitHub App on a repository if the app does not request organization permissions and if the managed user account has admin access to the repositories that they are granting the app access to.
- Managed user accounts can install GitHub App on an organization if the managed user account is an organization owner.
- You can choose whether managed user accounts are able to create repositories owned by their user accounts. For more information, see "Enforcing repository management policies in your enterprise."
- If you allow managed user accounts to create repositories owned by their user accounts, they can only own private repositories and can only invite other enterprise members to collaborate on their user-owned repositories.
- Managed user accounts cannot fork repositories from outside of the enterprise. Managed user accounts can fork private or internal repositories owned by organizations in the enterprise into their user account namespace or other organizations owned by the enterprise, as specified by enterprise policy.
- Only private and internal repositories can be created in organizations owned by an enterprise with managed users, depending on organization and enterprise repository visibility settings.
- Outside collaborators are not supported by Enterprise Managed Users.
- Managed user accounts are limited in their use of GitHub Pages. For more information, see "About GitHub Pages."
- Managed user accounts can only create and use codespaces that are owned and paid for by their organization or enterprise. This means that managed user accounts:
  - Can create codespaces for repositories owned by their organization, or forks of these repositories, provided that the organization can pay for GitHub Codespaces. For more information, see "Choosing who owns and pays for codespaces in your organization."
  - Cannot create codespaces for their personal repositories, other than forks of repositories owned by their organization; for any other repositories outside their organization; or from GitHub's public templates for GitHub Codespaces.

  - Cannot publish a codespace created from a template to a new repository.

- Entitlement minutes for GitHub-hosted runners are not available for managed user accounts. Enterprise Managed Users who would like to contribute to repositories in organizations they are not a member of can fork the organization repo, then open a pull request targeting the organization repository. This runs the workflows on the organization's GitHub-hosted runners.
- Managed user accounts can create GitHub Apps and OAuth apps.

  > **Note:** Even an OAuth app created by a managed user account or organization with managed users can be accessed by users outside the enterprise.

Getting started with Enterprise Managed Users

Before your developers can use GitHub Enterprise Cloud with Enterprise Managed Users, you must follow a series of configuration steps.

1. To use Enterprise Managed Users, you need a separate type of enterprise account with Enterprise Managed Users enabled. To try out Enterprise Managed Users or to discuss options for migrating from your existing enterprise, please contact GitHub's Sales team.

   Your contact on the GitHub Sales team will work with you to create your new enterprise with managed users. You'll need to provide the email address for the user who will set up your enterprise and a short code that will be used as the suffix for your enterprise members' usernames. The short code must be unique to your enterprise, a three-to-eight character alphanumeric string, and contain no special characters. For more information, see "Usernames and profile information."

2. After we create your enterprise, you will receive an email from GitHub inviting you to choose a password for your enterprise's setup user, which will be the first owner in the enterprise. Use an incognito or private browsing window when setting the password and saving the recovery codes for the user. The setup user is only used to configure single sign-on and SCIM provisioning integration for the enterprise. It will no longer be allowed to access enterprise or organization settings once SSO is configured, unless an SSO recovery code is used.

   The setup user's username is your enterprise's shortcode suffixed with `_admin`, for example `fabrikam_admin`. If you need to sign in as the setup user later, you can enter the username and password at any login page. A link to the login page is also provided on the SSO page, for convenience.

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

3. After you log in as the setup user, we recommend enabling two-factor authentication. The setup user's password and two-factor credentials can also be used to enter sudo mode, which is required to take sensitive actions. For more information, see "Configuring two-factor authentication" and "Sudo mode."

4. To get started, configure how your members will authenticate. If you are using Azure Active Directory as your identity provider, you can choose between OpenID Connect (OIDC) and Security Assertion Markup Language (SAML). We recommend OIDC, which includes support for Conditional Access Policies (CAP). If you require multiple enterprises with managed user accounts provisioned from one tenant, you must use SAML for each enterprise after the first. If you are using another identity

provider, like Okta or PingFederate, you can use SAML to authenticate your members.

To get started, read the guide for your chosen authentication method.

- "Configuring OIDC for Enterprise Managed Users."
- "Configuring SAML single sign-on for Enterprise Managed Users."

5. Once you have configured SSO, you can configure SCIM provisioning. SCIM is how your identity provider will create managed user accounts on GitHub.com. For more information on configuring SCIM provisioning, see "Configuring SCIM provisioning for Enterprise Managed Users."
6. Once authentication and provisioning are configured, you can start managing organization membership for your managed user accounts by synchronizing IdP groups with teams. For more information, see "Managing team memberships with identity provider groups."

If members of your enterprise must use one workstation to contribute to repositories on GitHub.com from both a managed user account and a personal account, you can provide support. For more information, see "Supporting developers with multiple user accounts on GitHub.com."

Authenticating as a managed user account

Managed user accounts must authenticate through their identity provider. To authenticate, a managed user account can visit their IdP application portal or use the login page on GitHub.com.

By default, when an unauthenticated user attempts to access an enterprise that uses Enterprise Managed Users, GitHub displays a 404 error. An enterprise owner can optionally enable automatic redirects to single sign-on (SSO) instead of the 404. For more information, see "Enforcing policies for security settings in your enterprise."

If a SAML configuration error or an issue with your identity provider (IdP) prevents you from using SAML SSO, you can use a recovery code to access your enterprise. For more information, see "Managing recovery codes for your enterprise."

Authenticating as a managed user account via GitHub.com

1. Navigate to https://github.com/login.
2. In the "Username or email address" text box, enter your username including the underscore and short code. When the form recognizes your username, the form will update. You do not need to enter your password on this form.
3. To continue to your identity provider, click **Sign in with your identity provider**.

Usernames and profile information

GitHub Enterprise Cloud automatically creates a username for each person by normalizing an identifier provided by your IdP. For more information, see "Username considerations for external authentication."

A conflict may occur when provisioning users if the unique parts of the identifier provided by your IdP are removed during normalization. If you're unable to provision a user due to a username conflict, you should modify the username provided by your IdP. For more

information, see "Username considerations for external authentication."

> **Note:** Because GitHub adds an underscore and short code to the normalized identifier provided by your IdP when creating each username, conflicts can only occur within each enterprise with managed users. Managed user accounts can share IdP identifiers or email addresses with other user accounts on GitHub.com that are outside the enterprise.

The profile name and email address of a managed user account is also provided by the IdP. Managed user accounts cannot change their profile name or email address on GitHub, and the IdP can only provide a single email address.

Supporting developers with multiple user accounts on GitHub.com

People on your team may need to contribute to resources on GitHub.com that are outside of your enterprise with managed users. For example, you may wish to maintain a separate enterprise for your company's open source projects. Because a managed user account cannot contribute to public resources, users will need to maintain a separate, personal account for this work.

People who must contribute from two user accounts on GitHub.com using one workstation can configure Git to simplify the process. For more information, see "Managing multiple accounts."