Configuring SCIM provisioning for Enterprise Managed Users

In this article

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

> 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 provisioning for Enterprise Managed Users

You must configure provisioning for Enterprise Managed Users to create, manage, and deactivate user accounts for your enterprise members.

After you configure provisioning for Enterprise Managed Users, users assigned to the GitHub Enterprise Managed User application in your identity provider are provisioned as new managed user accounts on GitHub via SCIM, and the managed user accounts are added to your enterprise. If you assign a group to the application, all users within the group will be provisioned as new managed user accounts.

When you update information associated with a user's identity on your IdP, your IdP will update the user's account on GitHub.com. When you unassign the user from the GitHub Enterprise Managed User application or deactivate a user's account on your IdP, your IdP will communicate with GitHub to invalidate any sessions and disable the member's account. The disabled account's information is maintained and their username is changed to a hash of their original username with the short code appended. If you reassign a user to the GitHub Enterprise Managed User application or reactivate their account on your IdP, the managed user account on GitHub will be reactivated and username restored.

Groups in your IdP can be used to manage team membership within your enterprise's organizations, allowing you to configure repository access and permissions through your IdP. For more information, see "Managing team memberships with identity provider groups."

Prerequisites

Before you can configure provisioning for Enterprise Managed Users, you must configure SAML or OIDC single-sign on.

- For more information on configuring OIDC, see "[Configuring OIDC for Enterprise Managed Users](#)"
- For information on configuring SAML, see "[Configuring SAML single sign-on for Enterprise Managed Users](#)."

Creating a personal access token 🔗

To configure provisioning for your enterprise with managed users, you need a personal access token (classic) with the **admin:enterprise** scope that belongs to the setup user.

> **Warning:** If the token expires or a provisioned user creates the token, SCIM provisioning may unexpectedly stop working. Make sure that you create the token while signed in as the setup user and that the token expiration is set to "No expiration".

1. Sign into GitHub.com as the setup user for your new enterprise with the username **@*SHORT-CODE*_admin**.

2. In the upper-right corner of any page, click your profile photo, then click **Settings**.
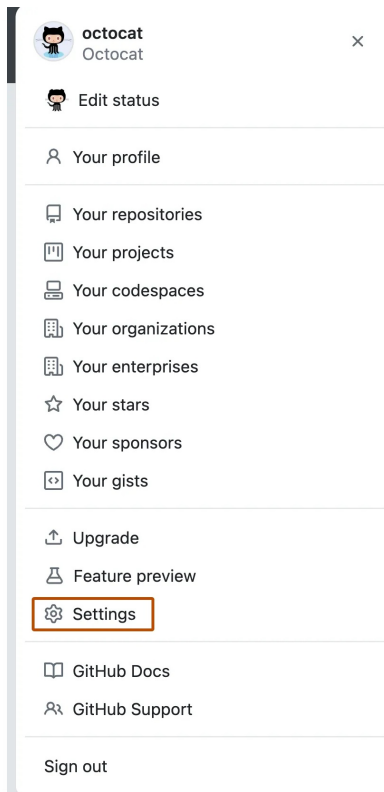
3. In the left sidebar, click <> **Developer settings**.

4. In the left sidebar, click **Personal access tokens**.

5. Click **Generate new token**.

6. Under **Note**, give your token a descriptive name.

7. Select the **Expiration** dropdown menu, then click **No expiration**.

8. Select the **admin:enterprise** scope.

☑ **admin:enterprise**	Full control of enterprises
☑ manage_runners:enterprise	Manage enterprise runners and runner groups
☑ manage_billing:enterprise	Read and write enterprise billing data
☑ read:enterprise	Read enterprise profile data

9. Click **Generate token**.

10. To copy the token to your clipboard, click ⧉.

> Make sure to copy your personal access token now. You won't be able to see it again!

✓ ghp_▮▮ ▬ ▮ ▮▮ ▬▬▬▬ ⧉   Configure SSO ▾   Delete

11. To save the token for use later, store the new token securely in a password manager.

Configuring provisioning for Enterprise Managed Users 🔗

After creating your personal access token and storing it securely, you can configure provisioning on your identity provider.

> **Note:** To avoid exceeding the rate limit on GitHub Enterprise Cloud, do not assign more than 1,000 users per hour to the IdP application. If you use groups to assign users to the IdP application, do not add more than 1,000 users to each group per hour. If you exceed these thresholds, attempts to provision users may fail with a "rate limit" error. You can review your IdP logs to confirm if attempted SCIM provisioning or push operations failed due to a rate limit error. The response to a failed provisioning attempt will depend on the IdP. For more information, see "[Troubleshooting identity and access management for your enterprise](.)."

To configure provisioning, follow the appropriate link from the table below.

Identity provider	SSO method	More information
Azure AD	OIDC	[Tutorial: Configure GitHub Enterprise Managed User (OIDC) for automatic user provisioning](.) in the Azure AD documentation
Azure AD	SAML	[Tutorial: Configure GitHub Enterprise Managed User for automatic user provisioning](.) in the Azure AD documentation
Okta	SAML	[Configuring SCIM provisioning for Enterprise Managed Users with Okta](.)
PingFederate	SAML	[Configure PingFederate for provisioning and SSO](.) and [Managing channels](.) in the PingFederate documentation

> **Note:** Azure AD does not support provisioning nested groups. For more information, see [How Application Provisioning works in Azure Active Directory](#).

Legal

[Terms](#)   [Privacy](#)   [Status](#)   [Pricing](#)   [Expert services](#)   [Blog](#)