Configuring SCIM provisioning for Enterprise Managed Users with Okta

In this article

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

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 with Okta

You can use Enterprise Managed Users with Okta as your identity provider to provision new accounts, manage enterprise membership, and manage team memberships for organizations in your enterprise. For more information about provisioning for Enterprise Managed Users, see "Configuring SCIM provisioning for Enterprise Managed Users."

Note: SCIM is required for Enterprise Managed Users, so you must use a version of Okta that includes SCIM.

Before you can configure provisioning with Okta, you must configure SAML single-sign on. For more information, see "Configuring SAML single sign-on for Enterprise Managed Users."

To configure provisioning with Okta, you must set your enterprise's name in the GitHub Enterprise Managed User application and enter your setup user's personal access token. You can then start provisioning users in Okta.

Supported features

Enterprise Managed Users supports many provisioning features in Okta.

Feature	Description
Push New Users	Users that are assigned to the GitHub Enterprise Managed User application in Okta are automatically created in the enterprise on GitHub Enterprise Cloud.

Push Profile Update	Updates made to the user's profile in Okta will be pushed to GitHub Enterprise Cloud.
Push Groups	Groups in Okta that are assigned to the GitHub Enterprise Managed User application as Push Groups are automatically created in the enterprise on GitHub Enterprise Cloud.
Push User Deactivation	Unassigning the user from the GitHub Enterprise Managed User application in Okta will disable the user on GitHub Enterprise Cloud. The user will not be able to sign in, but the user's information is maintained.
Reactivate Users	Users in Okta whose Okta accounts are reactivated and who are assigned back to the GitHub Enterprise Managed User application will be enabled.

Note: Enterprise Managed Users does not support modifications to usernames.

Setting your enterprise name

After your enterprise with managed users has been created, you can begin to configure provisioning by setting your enterprise name in Okta.

1. Navigate to your GitHub Enterprise Managed User application on Okta.
2. Click the **Sign On** tab.
3. To make changes, click **Edit**.
4. Under "Advanced Sign-on Settings", in the "Enterprise Name" text box, type your enterprise name. For example, if you access your enterprise at `https://github.com/enterprises/octoinc`, your enterprise name would be "octoinc".
5. To save your enterprise name, click **Save**.

Configuring provisioning

After setting your enterprise name, you can proceed to configure provisioning settings.

To configure provisioning, the setup user with the **@*SHORT-CODE*_admin** username will need to provide a personal access token (classic) with the **admin:enterprise** scope. For more information on creating a new token, see "Configuring SCIM provisioning for Enterprise Managed Users."

1. Navigate to your GitHub Enterprise Managed User application on Okta.
2. Click the **Provisioning** tab.
3. In the settings menu, click **Integration**.
4. To make changes, click **Edit**.
5. Select **Enable API integration**.
6. In the "API Token" field, enter the personal access token (classic) with the

admin:enterprise scope belonging to the setup user.

7. Click **Test API Credentials**. If the test is successful, a verification message will appear at the top of the screen.

8. To save the token, click **Save**.

9. In the settings menu, click **To App**.

10. To the right of "Provisioning to App", to allow changes to be made, click **Edit**.

11. Select **Enable** to the right of **Create Users**, **Update User Attributes**, and **Deactivate Users**.

12. To finish configuring provisioning, click **Save**.

Assigning users and groups

After you have configured SAML SSO and provisioning, you will be able to provision new users on GitHub.com by assigning users or groups to the GitHub Enterprise Managed User application.

> **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."

You can also automatically manage organization membership by adding groups to the "Push Groups" tab in Okta. When the group is provisioned successfully, it will be available to connect to teams in the enterprise's organizations. For more information about managing teams, see "Managing team memberships with identity provider groups."

When assigning users, you can use the "Roles" attribute in the GitHub Enterprise Managed User application to set a user's role in your enterprise on GitHub Enterprise Cloud. For more information about the roles available to assign, see "Roles in an enterprise."

> **Note:** You can only set the "Roles" attribute for an individual user, not a group. If you want to set roles for everyone in a group that's assigned to the GitHub Enterprise Managed User application, you must use the "Roles" attribute for each group member, individually.

Deprovisioning users and groups

To remove a user or group from GitHub Enterprise Cloud, remove the user or group from both the "Assignments" tab and the "Push groups" tab in Okta. For users, make sure the user is removed from all groups in the "Push Groups" tab.