

Migrating from SAML to OIDC

In this article

About migration of an enterprise with managed users from SAML to OIDC

Prerequisites

Migrating your enterprise

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.

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](#)."

Note: OpenID Connect (OIDC) and Conditional Access Policy (CAP) support for Enterprise Managed Users is only available for Azure AD.

About migration of an enterprise with managed users from SAML to OIDC

If your enterprise with managed users uses SAML SSO to authenticate with Azure Active Directory (Azure AD), you can migrate to OIDC. 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.

When you migrate from SAML to OIDC, managed user accounts and groups that were previously provisioned for SAML but are not provisioned by the GitHub Enterprise Managed User (OIDC) application will have "(SAML)" appended to their display names.

If you're new to Enterprise Managed Users and haven't yet configured authentication for your enterprise, you do not need to migrate and can set up OIDC single sign-on immediately. For more information, see "[Configuring OIDC for Enterprise Managed Users](#)."

Prerequisites

- Your enterprise on GitHub.com must currently be configured to use SAML for authentication. For more information, see "[Configuring SAML single sign-on for Enterprise Managed Users](#)."
- You'll need to access both your enterprise on GitHub.com and your tenant on Azure Active Directory (AD).
 - To configure the GitHub Enterprise Managed User (OIDC) application on Azure AD, you must sign into the Azure AD tenant as a user with the Global


Administrator role.

- To sign in as the setup user for your enterprise on GitHub.com, you must use a recovery code for the enterprise. For more information, see "[Downloading your enterprise account's single sign-on recovery codes](#)."
- Schedule a time to migrate when people aren't actively using your enterprise's resources. During the migration, users cannot access your enterprise until after you configure the new application and users as re-provisioned.


Migrating your enterprise

To migrate your enterprise from SAML to OIDC, you will disable your existing GitHub Enterprise Managed User application on Azure AD, prepare and begin the migration as the setup user for your enterprise on GitHub.com, then install and configure the new application for OIDC on Azure AD. After the migration is complete and Azure AD provisions your users, the users can authenticate to access your enterprise's resources on GitHub.com using OIDC.

Warning: Migration of your enterprise from SAML to OIDC can take up to an hour. During the migration, users cannot access your enterprise on GitHub.com.

- 1 Before you begin the migration, sign in to Azure and disable provisioning in the existing GitHub Enterprise Managed User application.
- 2 If you use [Conditional Access \(CA\) network location policies](#) in Azure AD, and you're currently using an IP allow list with your enterprise account or any of the organizations owned by the enterprise account on GitHub.com, disable the IP allow lists. For more information, see "[Enforcing policies for security settings in your enterprise](#)" and "[Managing allowed IP addresses for your organization](#)."
- 3 Sign into GitHub.com as the setup user for your enterprise with the username **@SHORT-CODE_admin**, replacing SHORT-CODE with your enterprise's short code.
- 4 In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.
- 5 In the list of enterprises, click the enterprise you want to view.
- 6 In the enterprise account sidebar, click  **Settings**.
- 7 When prompted to continue to your identity provider, click **Use a recovery code** and sign in using one of your enterprise's recovery codes.

Note: You must use a recovery code for your enterprise, not your user account. For more information, see "[Downloading your enterprise account's single sign-on recovery codes](#)."

- 8 Under  **Settings**, click **Authentication security**.
- 9 At the bottom of the page, next to "Migrate to OpenID Connect single sign-on", click **Configure with Azure**.
- 10 Read the warning, then click "I understand, begin migrating to OpenID Connect".
- 11 After GitHub Enterprise Cloud redirects you to your IdP, sign in, then follow the instructions to give consent and install the GitHub Enterprise Managed User (OIDC) application. After Azure AD asks for permissions for GitHub Enterprise Managed Users with OIDC, enable **Consent on behalf of your organization**, then click

Accept.

Warning: You must sign in to Azure AD as a user with global admin rights in order to consent to the installation of the GitHub Enterprise Managed User (OIDC) application.

- 12 After you grant consent, a new browser window will open to GitHub.com and display a new set of recovery codes for your enterprise with managed users. Download the codes, then click "Enable OIDC authentication".
- 13 Wait for the migration to complete, which can take up to an hour. To check the status of the migration, navigate to your enterprise's authentication security settings page. If "Require SAML authentication" is selected, the migration is still in progress.

Warning: Do not provision new users from the application on Azure AD during the migration.

- 14 In a new tab or window, while signed in as the setup user on GitHub.com, create a personal access token (classic) with the **admin:enterprise** scope and **no expiration** and copy it to your clipboard. For more information about creating a new token, see "[Configuring SCIM provisioning for Enterprise Managed Users](#)."
- 15 In the provisioning settings for the GitHub Enterprise Managed User (OIDC) application in Azure Portal, under "Tenant URL", type `https://api.github.com/scim/v2/enterprises/YOUR_ENTERPRISE`, replacing YOUR_ENTERPRISE with the name of your enterprise account.

For example, if your enterprise account's URL is

`https://github.com/enterprises/octo-corp`, the name of the enterprise account is `octo-corp`.

- 16 Under "Secret token", paste the personal access token (classic) with the **admin:enterprise** scope that you created earlier.
- 17 To test the configuration, click **Test Connection**.
- 18 To save your changes, at the top of the form, click **Save**.
- 19 In Azure Portal, copy the users and groups from the old GitHub Enterprise Managed User application to the new GitHub Enterprise Managed User (OIDC) application.
- 20 Test your configuration by provisioning a single new user.
- 21 If your test is successful, start provisioning for all users by clicking **Start provisioning**.

Legal