Migrating your enterprise to a new identity provider or tenant

In this article

You can migrate your enterprise to a different identity provider (IdP) or Azure AD tenant.

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 migrations between IdPs and tenants

While using Enterprise Managed Users, you may need to migrate your enterprise to a new IdP or Azure AD tenant. For example, you might be ready to migrate from a test environment to your production environment.

Warning: Migrating to a new identity provider or tenant can cause disruption to integrations and automated flows in your enterprise. When your current SAML identity provider is disabled, personal access tokens and SSH keys associated with managed user accounts will be deleted. You should plan for a migration window after configuring your new identity provider, during which you can create and deploy new keys to your integrations where necessary.

Before you migrate your enterprise with managed users to a new IdP or tenant, determine whether the values of the normalized SCIM `userName` attribute will remain the same for your managed user accounts in the new environment. For more information about username normalization, see "Username considerations for external authentication."

If the normalized SCIM `userName` values will remain the same after the migration, you can complete the migration by yourself. For instructions, see "Migrating when the normalized SCIM `userName` values will remain the same."

If the normalized SCIM `userName` values will change after the migration, GitHub will need to help with your migration. For more information, see "Migrating when the normalized SCIM `userName` values will change."

Migrating when the normalized SCIM `userName` values will remain the same

To migrate to a new IdP or tenant, you cannot edit your existing SAML configuration. Instead, you must completely deactivate SAML for your enterprise account, then create new SAML and SCIM configurations for the new IdP or tenant.

Warning: Do not remove any users or groups from the application for Enterprise Managed Users in your original IdP or tenant until after your migration is complete.

1. If you don't already have single sign-on recovery codes for your enterprise, download the codes now. For more information, see "Downloading your enterprise account's single sign-on recovery codes."

2. In your current IdP, deactivate provisioning in the application for Enterprise Managed Users.

   - If you use Azure AD, navigate to the "Provisioning" tab of the application, and then click **Stop provisioning**.
   - If you use Okta, navigate to the "Provisioning" tab of the application, click the **Integration** tab, and then click **Edit**. Deselect **Enable API integration**.
   - If you use PingFederate, navigate to the channel settings in the application. From the **Activation & Summary** tab, click **Active** or **Inactive** to toggle the provisioning status, and then click **Save**. For more information about managing provisioning, see "Reviewing channel settings" and "Managing channels" in the Ping Federate documentation.

3. Use a recovery code to sign into GitHub.com as the setup user, whose username is your enterprise's shortcode suffixed with `_admin`. For more information about the setup user, see "About Enterprise Managed Users."

4. Deactivate SAML for the enterprise with managed users. For more information, see "Disabling authentication for Enterprise Managed Users."

5. Wait for all users in the enterprise to show as suspended.

6. While still signed in as the setup user, configure SAML and SCIM for the new IdP or tenant with a new Enterprise Managed Users application.

   After you configure provisioning for the new application, the managed user accounts will be unsuspended, and your developers will be able to sign into their existing accounts again.

   By default, this process can take up to 40 minutes for Azure AD. To expedite the process for an individual user, click the **Provision on Demand** button in the "Provisioning" tab of the application for Enterprise Managed Users.

Migrating when the normalized SCIM `userName` values will change

If the normalized SCIM `userName` values will change, GitHub must provision a new enterprise account for your migration. Contact our sales team for help.