Switching your SAML configuration from an organization to an enterprise account

Learn special considerations and best practices for replacing an organization-level SAML configuration with an enterprise-level SAML configuration.

> **Who can use this feature**
> Enterprise owners can configure SAML single sign-on for an enterprise account.

About SAML single sign-on for enterprise accounts

SAML single sign-on (SSO) gives organization owners and enterprise owners using GitHub Enterprise Cloud a way to control and secure access to organization resources like repositories, issues, and pull requests. Enterprise owners can enable SAML SSO and centralized authentication through a SAML IdP across all organizations owned by an enterprise account. After you enable SAML SSO for your enterprise account, SAML SSO is enforced for all organizations owned by your enterprise account. All members will be required to authenticate using SAML SSO to gain access to the organizations where they are a member, and enterprise owners will be required to authenticate using SAML SSO when accessing an enterprise account.

There are special considerations when enabling SAML SSO for your enterprise account if any of the organizations owned by the enterprise account are already configured to use SAML SSO.

When you configure SAML SSO at the organization level, each organization must be configured with a unique SSO tenant in your IdP, which means that your members will be associated with a unique SAML identity record for each organization they have successfully authenticated with. If you configure SAML SSO for your enterprise account instead, each enterprise member will have one SAML identity that is used for all organizations owned by the enterprise account.

After you configure SAML SSO for your enterprise account, the new configuration will override any existing SAML SSO configurations for organizations owned by the enterprise account.

Enterprise members will not be notified when an enterprise owner enables SAML for the enterprise account. If SAML SSO was previously enforced at the organization level, members should not see a major difference when navigating directly to organization resources. The members will continue to be prompted to authenticate via SAML. If members navigate to organization resources via their IdP dashboard, they will need to click the new tile for the enterprise-level app, instead of the old tile for the organization-level app. The members will then be able to choose the organization to navigate to.

Any personal access tokens, SSH keys, OAuth apps, and GitHub Apps that were previously authorized for the organization will continue to be authorized for the organization. However, members will need to authorize any PATs, SSH keys, OAuth apps, and GitHub Apps that were never authorized for use with SAML SSO for the organization.

SCIM provisioning is not currently supported when SAML SSO is configured for an enterprise account. If you are currently using SCIM for an organization owned by your enterprise account, you will lose this functionality when switching to an enterprise-level configuration.

You are not required to remove any organization-level SAML configurations before configuring SAML SSO for your enterprise account, but you may want to consider doing so. If SAML is ever disabled for the enterprise account in the future, any remaining organization-level SAML configurations will take effect. Removing the organization-level configurations can prevent unexpected issues in the future.

For more information about the decision to implement SAML SSO at the organization or enterprise level, see "About authentication for your enterprise."

Switching your SAML configuration from an organization to an enterprise account

1. Enforce SAML SSO for your enterprise account, making sure all organization members are assigned or given access to the IdP app being used for the enterprise account. For more information, see "Configuring SAML single sign-on for your enterprise."

2. Optionally, remove any existing SAML configuration for organizations owned by the enterprise account. To help you decide whether to remove the configurations, see "About SAML single sign-on for enterprise accounts."

3. If you kept any organization-level SAML configurations in place, to prevent confusion, consider hiding the tile for the organization-level apps in your IdP.

4. Advise your enterprise members about the change.

    - Members will no longer be able to access their organizations by clicking the SAML app for the organization in the IdP dashboard. They will need to use the new app configured for the enterprise account.
    - Members will need to authorize any PATs or SSH keys that were not previously authorized for use with SAML SSO for their organization. For more information, see "Authorizing a personal access token for use with SAML single sign-on" and "Authorizing an SSH key for use with SAML single sign-on."
    - Members may need to reauthorize OAuth apps that were previously authorized for the organization. For more information, see "About authentication with SAML single sign-on."