

Managing team synchronization for your organization

In this article

About team synchronization

Enabling team synchronization

Managing whether team sync can re-invite non-members to your organization

Disabling team synchronization

You can enable and disable team synchronization between your identity provider (IdP) and your organization on GitHub Enterprise Cloud.

Who can use this feature

Organization owners can manage team synchronization for an organization.

Note: If your enterprise uses Enterprise Managed Users, you do not need to use team synchronization. Instead, you can manage team membership via the SCIM configuration you created while setting up your enterprise. For more information, see "[Managing team memberships with identity provider groups](#)."

About team synchronization

You can enable team synchronization between your IdP and GitHub Enterprise Cloud to allow organization owners and team maintainers to connect teams in your organization with IdP groups.

If team sync is enabled for your organization or enterprise account, you can synchronize a GitHub team with an IdP group. When you synchronize a GitHub team with an IdP group, membership changes to the IdP group are reflected on GitHub Enterprise Cloud automatically, reducing the need for manual updates and custom scripts.

To connect a team on GitHub Enterprise Cloud to an IdP group, the team must already exist in your organization. Even if you have configured SCIM provisioning, creating a group in your IdP does not automatically create a team on GitHub Enterprise Cloud.

Note: To use SAML single sign-on, your organization must use GitHub Enterprise Cloud. For more information about how you can try GitHub Enterprise Cloud for free, see "[Setting up a trial of GitHub Enterprise Cloud](#)."

You can use team synchronization with supported IdPs.

- Azure AD commercial tenants (Gov Cloud is not supported)
- Okta

Team synchronization is not a user provisioning service and does not invite non-members to join organizations in most cases. This means a user will only be successfully added to a team if they are already an organization member. However, you can

optionally allow team synchronization to re-invite users who were previously organization members and have since been removed.

After you enable team synchronization, team maintainers and organization owners can connect a team to an IdP group on GitHub or through the API. For more information, see "[Synchronizing a team with an identity provider group](#)" and "[Teams](#)."

You can also enable team synchronization for all organizations owned by an enterprise account. If SAML is configured at the enterprise level, you cannot enable team synchronization on an individual organization. Instead, you must configure team synchronization for the entire enterprise. For more information, see "[Managing team synchronization for organizations in your enterprise](#)."

If your organization is owned by an enterprise account, enabling team synchronization for the enterprise account will override your organization-level team synchronization settings. For more information, see "[Managing team synchronization for organizations in your enterprise](#)."

Usage limits

There are usage limits for the team synchronization feature. Exceeding these limits will lead to a degradation in performance and may cause synchronization failures.

- Maximum number of members in a GitHub team: 5,000
- Maximum number of members in a GitHub organization: 10,000
- Maximum number of teams in a GitHub organization: 1,500

Enabling team synchronization

The steps to enable team synchronization depend on the IdP you want to use. There are prerequisites to enable team synchronization that apply to every IdP. Each individual IdP has additional prerequisites.

Prerequisites

To enable team synchronization with any IdP, you must obtain administrative access to your IdP or work with your IdP administrator to configure the IdP integration and groups. The person who configures your IdP integration and groups must have one of the required permissions.

IdP	Required permissions
Azure AD	<ul style="list-style-type: none">• Global administrator• Privileged Role administrator
Okta	<ul style="list-style-type: none">• Service user with read-only administrator permissions

You must enable SAML single sign-on for your organization and your supported IdP. For more information, see "[Enforcing SAML single sign-on for your organization](#)."


You must have a linked SAML identity. To create a linked identity, you must authenticate to your organization using SAML SSO and the supported IdP at least once. For more information, see "[Authenticating with SAML single sign-on](#)."

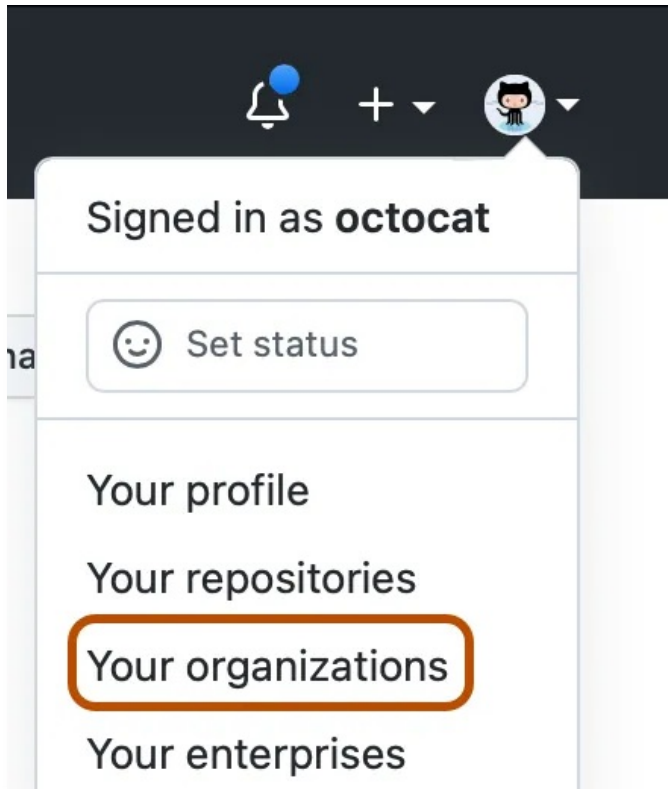
Note: For team synchronization to work, your SAML settings must contain a valid IdP URL for the "Issuer" field. For more information, see "[Enabling and testing SAML single sign-on for your organization](#)."


Enabling team synchronization for Azure AD [🔗](#)

To enable team synchronization for Azure AD, your Azure AD installation needs the following permissions.

- Read all users' full profiles
- Sign in and read user profile
- Read directory data

- 1 In the top right corner of GitHub.com, click your profile photo, then click  **Your organizations**.



- 2 Next to the organization, click **Settings**.
- 3 In the "Security" section of the sidebar, click  **Authentication security**.
- 4 Confirm that SAML SSO is enabled for your enterprise.
- 5 Under "Team synchronization", click **Enable for Azure AD**.
- 6 Confirm team synchronization.
 - If you have IdP access, click **Enable team synchronization**. You'll be redirected to your identity provider's SAML SSO page and asked to select your account and review the requested permissions.
 - If you don't have IdP access, copy the IdP redirect link and share it with your IdP administrator to continue enabling team synchronization.
- 7 Review the identity provider tenant information you want to connect to your organization, then click **Approve**.

Enabling team synchronization for Okta [🔗](#)

Okta team synchronization requires that SAML and SCIM with Okta have already been set

up for your organization.


To avoid potential team synchronization errors with Okta, we recommend that you confirm that SCIM linked identities are correctly set up for all organization members who are members of your chosen Okta groups, before enabling team synchronization on GitHub.

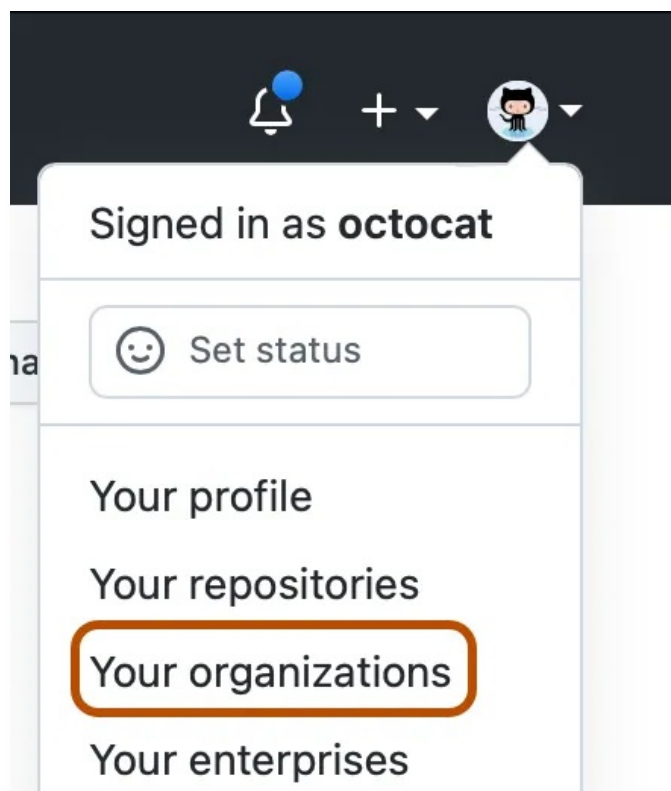
If an organization member does not have a linked SCIM identity, then team synchronization will not work as expected and the user may not be added or removed from teams as expected. If any of these users are missing a SCIM linked identity, you will need to re-provision them.


For help on provisioning users that have missing a missing SCIM linked identity, see "[Troubleshooting identity and access management for your organization](#)."

Before you enable team synchronization for Okta, you or your IdP administrator must:

- Configure the SAML, SSO, and SCIM integration for your organization using Okta. For more information, see "[Configuring SAML single sign-on and SCIM using Okta](#)."
- Provide the tenant URL for your Okta instance.
- Generate a valid SSWS token with read-only admin permissions for your Okta installation as a service user. For more information, see [Create the token](#) and [Service users](#) in Okta's documentation.


- 1 In the top right corner of GitHub.com, click your profile photo, then click  **Your organizations**.

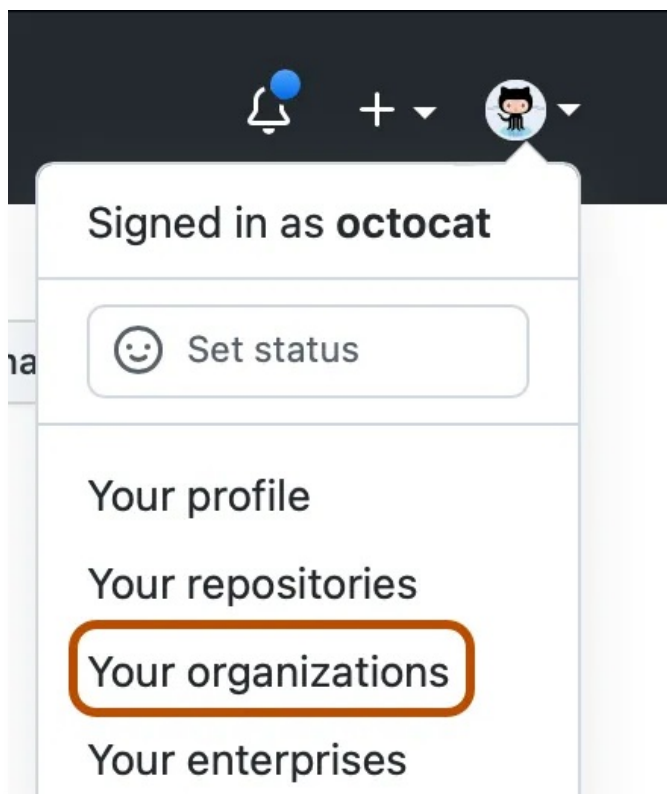



- 2 Next to the organization, click **Settings**.
- 3 In the "Security" section of the sidebar, click  **Authentication security**.
- 4 Confirm that SAML SSO is enabled for your enterprise.
- 5 We recommend you confirm that your users have SAML enabled and have a linked SCIM identity to avoid potential provisioning errors. For more information, see "[Troubleshooting identity and access management for your organization](#)."

- 6 Consider enforcing SAML in your organization to ensure that organization members link their SAML and SCIM identities. For more information, see "[Enforcing SAML single sign-on for your organization](#)."
- 7 Under "Team synchronization", click **Enable for Okta**.
- 8 Under your organization's name, in the "SSWS Token" field, type a valid SSWS token.
- 9 In the "URL" field, type the URL for your Okta instance.
- 10 Review the identity provider tenant information you want to connect to your organization, then click **Create**.

Managing whether team sync can re-invite non-members to your organization [↗](#)

- 1 In the top right corner of GitHub.com, click your profile photo, then click  **Your organizations**.




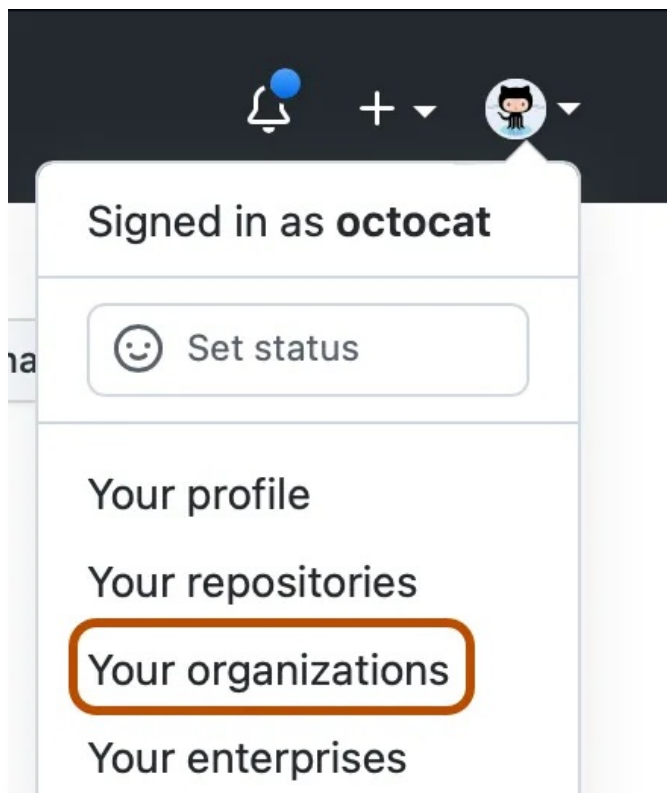
- 2 Next to the organization, click **Settings**.
- 3 In the "Security" section of the sidebar, click  **Authentication security**.
- 4 Under "Team synchronization", select or deselect **Do not allow Team Sync to re-invite past members to this organization that were removed by an organization owner**.


Disabling team synchronization [↗](#)

Warning: When you disable team synchronization, any team members that were assigned to a GitHub team through the IdP group are removed from the team and may lose access to

repositories.

- 1 In the top right corner of GitHub.com, click your profile photo, then click  **Your organizations**.



- 2 Next to the organization, click **Settings**.
- 3 In the "Security" section of the sidebar, click  **Authentication security**.
- 4 Under "Team synchronization", click **Disable team synchronization**.

Legal

© 2023 GitHub, Inc. [Terms](#) [Privacy](#) [Status](#) [Pricing](#) [Expert services](#) [Blog](#)