About SCIM for organizations

In this article

With System for Cross-domain Identity Management (SCIM), administrators can automate the exchange of user identity information between systems.

About SCIM for organizations

If your organization uses SAML SSO, you can implement SCIM to add, manage, and remove organization members' access to GitHub Enterprise Cloud. For example, an administrator can deprovision an organization member using SCIM and automatically remove the member from the organization.

> **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 cannot use this implementation of SCIM with an enterprise account or with an organization with managed users. If your enterprise is enabled for Enterprise Managed Users, you must use a different implementation of SCIM. Otherwise, SCIM is not available at the enterprise level. For more information, see "Configuring SCIM provisioning for Enterprise Managed Users."

If you use SAML SSO without implementing SCIM, you won't have automatic deprovisioning. When organization members' sessions expire after their access is removed from the IdP, they aren't automatically removed from the organization. Authorized tokens grant access to the organization even after their sessions expire. If SCIM is not used, to fully remove a member's access, an organization owner must remove the member's access in the IdP and manually remove the member from the organization on GitHub.

If SCIM provisioning is implemented for your organization, any changes to a user's organization membership should be triggered from the identity provider. If a user is invited to an organization manually instead of by an existing SCIM integration, their user account may not get properly linked to their SCIM identity. This can prevent the user account from being deprovisioned via SCIM in the future. If a user is removed manually instead of by an existing SCIM integration, a stale linked identity will remain, which can lead to issues if the user needs to re-join the organization.

Supported identity providers

These identity providers (IdPs) are compatible with the GitHub Enterprise Cloud SCIM API for organizations. For more information, see SCIM in the GitHub API documentation.

- Azure AD
- Okta
- OneLogin

About SCIM configuration for organizations

To use SCIM with your organization, you must use a third-party-owned OAuth app. The OAuth app must be authorized by, and subsequently acts on behalf of, a specific GitHub user. If the user who last authorized this OAuth app leaves or is removed from the organization, SCIM will stop working. To avoid this issue, we recommend creating a dedicated user account to configure SCIM. This user account must be an organization owner and will consume a license.

Before you authorize the OAuth app, you must have an active SAML session. For more information, see "About authentication with SAML single sign-on."

> **Note:** The SAML IdP and the SCIM client must use matching `NameID` and `userName` values for each user. This allows a user authenticating through SAML to be linked to their provisioned SCIM identity.

Further reading

- "Viewing and managing a member's SAML access to your organization"