About identity and access management with SAML single sign-on

In this article

If you centrally manage your users' identities and applications with an identity provider (IdP), you can configure Security Assertion Markup Language (SAML) single sign-on (SSO) to protect your organization's resources on GitHub.

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."

About SAML SSO

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.

If you configure SAML SSO, members of your organization will continue to sign into their personal accounts on GitHub.com. When a member accesses most resources within your organization, GitHub redirects the member to your IdP to authenticate. After successful authentication, your IdP redirects the member back to GitHub. For more information, see "About authentication with SAML single sign-on."

Note: SAML SSO does not replace the normal sign-in process for GitHub. Unless you use Enterprise Managed Users, members will continue to sign into their personal accounts on GitHub.com, and each personal account will be linked to an external identity in your IdP.

IdP authentication is not required for accessing public repositories in certain ways:

- Viewing the repository's overview page and file contents on GitHub
- Forking the repository
- Performing read operations via Git, such as cloning the repository

Authentication is required for other access to public repositories, such as viewing issues, pull requests, projects, and releases.

Note: SAML authentication is not required for outside collaborators. For more information about outside collaborators, see "Roles in an organization."

Organization owners can enforce SAML SSO for an individual organization, or enterprise owners can enforce SAML SSO for all organizations in an enterprise account. For more information, see "About authentication for your enterprise" and "Configuring SAML single sign-on for your enterprise."

Before enabling SAML SSO for your organization, you'll need to connect your IdP to your organization. For more information, see "Connecting your identity provider to your organization."

For an organization, SAML SSO can be disabled, enabled but not enforced, or enabled and enforced. After you enable SAML SSO for your organization and your organization's members successfully authenticate with your IdP, you can enforce the SAML SSO configuration. For more information about enforcing SAML SSO for your GitHub organization, see "Enforcing SAML single sign-on for your organization."

Members must periodically authenticate with your IdP to authenticate and gain access to your organization's resources. The duration of this login period is specified by your IdP and is generally 24 hours. This periodic login requirement limits the length of access and requires users to re-identify themselves to continue.

To access the organization's protected resources using the API and Git on the command line, members must authorize and authenticate with a personal access token or SSH key. 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."

The first time a member uses SAML SSO to access your organization, GitHub automatically creates a record that links your organization, the member's account on GitHub.com, and the member's account on your IdP. You can view and revoke the linked SAML identity, active sessions, and authorized credentials for members of your organization or enterprise account. For more information, see "Viewing and managing a member's SAML access to your organization" and "Viewing and managing a user's SAML access to your enterprise."

If members are signed in with a SAML SSO session when they create a new repository, the default visibility of that repository is private. Otherwise, the default visibility is public. For more information on repository visibility, see "About repositories."

Organization members must also have an active SAML session to authorize an OAuth app. You can opt out of this requirement by contacting us through the GitHub Support portal. GitHub Enterprise Cloud does not recommend opting out of this requirement, which will expose your organization to a higher risk of account takeovers and potential data loss.

GitHub Enterprise Cloud does not support SAML Single Logout. To terminate an active SAML session, users should log out directly on your SAML IdP.

Supported SAML services

GitHub Enterprise Cloud supports SAML SSO with IdPs that implement the SAML 2.0 standard. For more information, see the SAML Wiki on the OASIS website.

GitHub officially supports and internally tests the following IdPs.

- Active Directory Federation Services (AD FS)
- Azure Active Directory (Azure AD)
- Okta
- OneLogin
- PingOne
- Shibboleth

Some IdPs support provisioning access to a GitHub organization via SCIM. For more

information, see "About SCIM for organizations."

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."

Adding members to an organization using SAML SSO

After you enable SAML SSO, there are multiple ways you can add new members to your organization. Organization owners can invite new members manually on GitHub Enterprise Cloud or using the API. For more information, see "Inviting users to join your organization" and "Organizations."

To provision new users without an invitation from an organization owner, you can use the URL `https://github.com/orgs/ORGANIZATION/sso/sign_up`, replacing ORGANIZATION with the name of your organization. For example, you can configure your IdP so that anyone with access to the IdP can click a link on the IdP's dashboard to join your GitHub organization.

> **Note:** Provisioning new users via `https://github.com/orgs/ORGANIZATION/sso/sign_up` is only supported when SAML SSO is configured at the organization level, not when SAML SSO is configured at the enterprise account level. For more information about SAML SSO for enterprise accounts, see "About SAML for enterprise IAM."

If your IdP supports SCIM, GitHub can automatically invite members to join your organization when you grant access on your IdP. If you remove a member's access to your GitHub organization on your SAML IdP, the member will be automatically removed from the GitHub organization. For more information, see "About SCIM for organizations."

You can use team synchronization to automatically add and remove organization members to teams through an identity provider. For more information, see "Synchronizing a team with an identity provider group."

Further reading

- "SAML configuration reference"
- "About two-factor authentication and SAML single sign-on"
- "About authentication with SAML single sign-on"