

Enforcing SAML single sign-on for your organization

In this article

About enforcement of SAML SSO for your organization

Enforcing SAML SSO for your organization

Further reading

Organization owners and admins can enforce SAML SSO so that all organization members must authenticate via an identity provider (IdP).

About enforcement of SAML SSO for your organization

When you enable SAML SSO, GitHub will prompt members who visit the organization's resources on GitHub.com to authenticate on your IdP, which links the member's personal account to an identity on the IdP. Members can still access the organization's resources before authentication with your IdP.

You can also enforce SAML SSO for your organization. When you enforce SAML SSO, all members of the organization must authenticate through your IdP to access the organization's resources. Enforcement removes any members and administrators who have not authenticated via your IdP from the organization. GitHub sends an email notification to each removed user.

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](#)."


Any users removed due to SAML SSO enforcement can rejoin your organization by authenticating via SAML single sign-on. If a user rejoins the organization within three months, the user's access privileges and settings will be restored. For more information, see "[Reinstating a former member of your organization](#)."

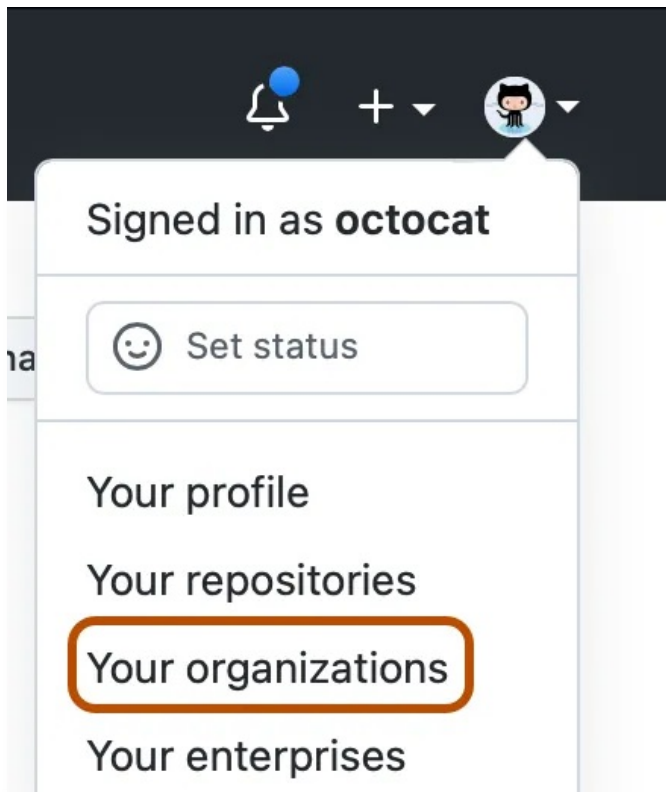
Bots and service accounts that do not have external identities set up in your organization's IdP will also be removed when you enforce SAML SSO. For more information about bots and service accounts, see "[Managing bots and service accounts with SAML single sign-on](#)."


If your organization is owned by an enterprise account, requiring SAML for the enterprise account will override your organization-level SAML configuration and enforce SAML SSO for every organization in the enterprise. For more information, see "[Configuring SAML single sign-on for your enterprise](#)."

Tip: When setting up SAML SSO in your organization, you can test your implementation without affecting your organization members by leaving **Require SAML SSO authentication for all members of the organization name organization** unchecked.

Enforcing SAML SSO for your organization [🔗](#)

- 1 Enable and test SAML SSO for your organization, then authenticate with your IdP at least once. For more information, see "[Enabling and testing SAML single sign-on for your organization](#)."
- 2 Prepare to enforce SAML SSO for your organization. For more information, see "[Preparing to enforce SAML single sign-on in your organization](#)."
- 3 In the top right corner of GitHub.com, click your profile photo, then click  **Your organizations**.



- 4 Next to the organization, click **Settings**.
- 5 In the "Security" section of the sidebar, click  **Authentication security**.
- 6 Under "SAML single sign-on", select **Require SAML SSO authentication for all members of the ORGANIZATION organization**.
- 7 If any organization members have not authenticated via your IdP, GitHub displays the members. If you enforce SAML SSO, GitHub will remove the members from the organization.

Review the warning and click **Remove members and require SAML single sign-on**.
- 8 Under "Single sign-on recovery codes", review your recovery codes. Store the recovery codes in a safe location like a password manager.

Further reading [🔗](#)

- "[Viewing and managing a member's SAML access to your organization](#)"

Legal