Enabling and testing SAML single sign-on for your organization

In this article

Organization owners and admins can enable SAML single sign-on to add an extra layer of security to their organization.

About SAML single sign-on

You can enable SAML SSO in your organization without requiring all members to use it. Enabling but not enforcing SAML SSO in your organization can help smooth your organization's SAML SSO adoption. Once a majority of your organization's members use SAML SSO, you can enforce it within your 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."

If you enable but don't enforce SAML SSO, organization members who choose not to use SAML SSO can still be members of the organization. For more information on enforcing SAML SSO, see "Enforcing SAML single sign-on for your organization."

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

When SAML SSO is disabled, all linked external identities are removed from GitHub Enterprise Cloud.

After you enable SAML SSO, OAuth app and GitHub App authorizations may need to be revoked and reauthorized before they can access the organization. For more information, see "Authorizing OAuth apps."

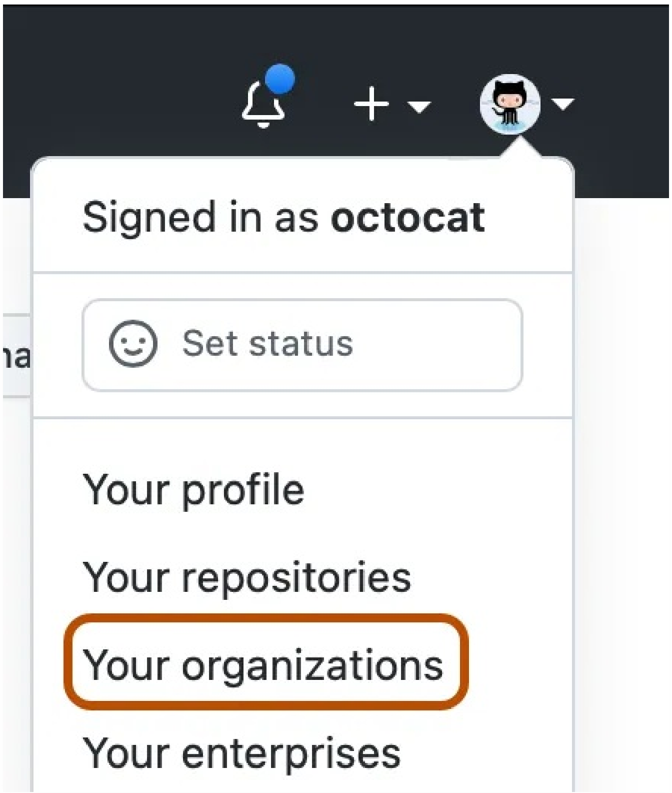
Enabling and testing SAML single sign-on for your organization

Before your enforce SAML SSO in your organization, ensure that you've prepared the organization. For more information, see "Preparing to enforce SAML single sign-on in your organization."

For more information about the identity providers (IdPs) that GitHub supports for SAML SSO, see "Connecting your identity provider 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 "SAML single sign-on", select **Enable SAML authentication**.

   > **Note:** After enabling SAML SSO, you can download your single sign-on recovery codes so that you can access your organization even if your IdP is unavailable. For more information, see "Downloading your organization's SAML single sign-on recovery codes."

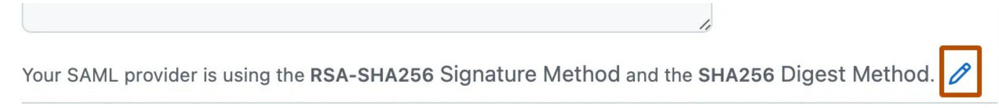
5. In the "Sign on URL" field, type the HTTPS endpoint of your IdP for single sign-on requests. This value is available in your IdP configuration.

6. Optionally, in the "Issuer" field, type your SAML issuer's name. This verifies the authenticity of sent messages.

   > **Note:** If you want to enable team synchronization for your organization, the "Issuer" field is a required. For more information, see "Managing team synchronization for your organization."

7. Under "Public Certificate," paste a certificate to verify SAML responses.

8. Under your public certificate, to the right of the current signature and digest methods, click ✎.



Your SAML provider is using the **RSA-SHA256** Signature Method and the **SHA256** Digest Method.

9. Select the **Signature Method** and **Digest Method** dropdown menus, then click the hashing algorithm used by your SAML issuer.

10. Before enabling SAML SSO for your organization, to ensure that the information you've entered is correct, click **Test SAML configuration**. This test uses Service Provider initiated (SP-initiated) authentication and must be successful before you can save the SAML settings.

    > **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.

11. To enforce SAML SSO and remove all organization members who haven't authenticated via your IdP, select **Require SAML SSO authentication for all members of the *organization name* organization**. For more information on enforcing SAML SSO, see "Enforcing SAML single sign-on for your organization."

12. Click **Save**.

Further reading

- "About identity and access management with SAML single sign-on"
- "SAML configuration reference"

Legal

Terms Privacy Status Pricing Expert services Blog