

Configuring SAML single sign-on for your enterprise

In this article

About SAML SSO

Supported identity providers

Username considerations with SAML

Configuring SAML SSO

Further reading

You can control and secure access to your GitHub Enterprise Server instance by configuring SAML single sign-on (SSO) through your identity provider (IdP).

Who can use this feature

Site administrators can configure SAML SSO for a GitHub Enterprise Server instance.

About SAML SSO

SAML SSO allows you to centrally control and secure access to your GitHub Enterprise Server instance from your SAML IdP. When an unauthenticated user visits your GitHub Enterprise Server instance in a browser, GitHub Enterprise Server will redirect the user to your SAML IdP to authenticate. After the user successfully authenticates with an account on the IdP, the IdP redirects the user back to your GitHub Enterprise Server instance. GitHub Enterprise Server validates the response from your IdP, then grants access to the user.

After a user successfully authenticates on your IdP, the user's SAML session for your GitHub Enterprise Server instance is active in the browser for 24 hours. After 24 hours, the user must authenticate again with your IdP.

With JIT provisioning, if you remove a user from your IdP, you must also manually suspend the user's account on your GitHub Enterprise Server instance. Otherwise, the account's owner can continue to authenticate using access tokens or SSH keys. For more information, see "[Suspending and unsuspending users](#)".

Supported identity providers

GitHub Enterprise Server 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

For more information about connecting Azure AD to your enterprise, see [Tutorial: Azure Active Directory SSO integration with GitHub Enterprise Cloud - Enterprise Account](#) in Microsoft Docs.



Username considerations with SAML

GitHub Enterprise Server normalizes a value from your external authentication provider to determine the username for each new personal account on your GitHub Enterprise Server instance. For more information, see "[Username considerations for external authentication](#)."

Configuring SAML SSO

You can enable or disable SAML authentication for your GitHub Enterprise Server instance, or you can edit an existing configuration. You can view and edit authentication settings for GitHub Enterprise Server in the Management Console. For more information, see "[Administering your instance from the web UI](#)."

Note: GitHub strongly recommends that you verify any new configuration for authentication in a staging environment. An incorrect configuration could result in downtime for your GitHub Enterprise Server instance. For more information, see "[Setting up a staging instance](#)."

- 1 From an administrative account on GitHub Enterprise Server, in the upper-right corner of any page, click .
- 2 If you're not already on the "Site admin" page, in the upper-left corner, click **Site admin**.
- 3 In the " Site admin" sidebar, click **Management Console**.
- 4 In the "Settings" sidebar, click **Authentication**.
- 5 Under "Authentication", select **SAML**.
- 6 Optionally, to allow people without an account on your external authentication system to sign in with built-in authentication, select **Allow built-in authentication**. For more information, see "[Allowing built-in authentication for users outside your provider](#)."
- 7 Optionally, to enable unsolicited response SSO, select **IdP initiated SSO**. By default, GitHub Enterprise Server will reply to an unsolicited Identity Provider (IdP) initiated request with an `AuthnRequest` back to the IdP.

Note: We recommend keeping this value **unselected**. You should enable this feature **only** in the rare instance that your SAML implementation does not support service provider initiated SSO, and when advised by GitHub Enterprise Support.

- 8 Optionally, if you do not want your SAML provider to determine administrator rights for users on your GitHub Enterprise Server instance, select **Disable administrator demotion/promotion**.
- 9 Optionally, to allow your GitHub Enterprise Server instance to receive encrypted assertions from your SAML IdP, select **Require encrypted assertions**.

You must ensure that your IdP supports encrypted assertions and that the encryption and key transport methods in the management console match the values configured on your IdP. You must also provide your GitHub Enterprise Server instance's public certificate to your IdP. For more information, see "[Enabling encrypted assertions](#)."

- 10 Under "Single sign-on URL," type the HTTP or HTTPS endpoint on your IdP for single sign-on requests. This value is provided by your IdP configuration. If the host is only available from your internal network, you may need to [configure your GitHub Enterprise Server instance to use internal nameservers](#).
- 11 Optionally, in the **Issuer** field, type your SAML issuer's name. This verifies the authenticity of messages sent to your GitHub Enterprise Server instance.
- 12 Select the **Signature Method** and **Digest Method** dropdown menus, then click the hashing algorithm used by your SAML issuer to verify the integrity of the requests from your GitHub Enterprise Server instance.
- 13 Select the **Name Identifier Format** dropdown menu, then click a format.
- 14 Under "Verification certificate," click **Choose File**, then choose a certificate to validate SAML responses from the IdP.
- 15 Under "User attributes", modify the SAML attribute names to match your IdP if needed, or accept the default names.

Further reading

- "[Promoting or demoting a site administrator](#)"

Legal

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