

Allowing built-in authentication for users outside your provider

In this article

About built-in authentication for users outside your provider

Configuring built-in authentication for users outside your provider

Inviting users outside your provider to authenticate to your instance

Further reading

You can configure fallback authentication to allow built-in authentication for people who don't have an account on your CAS, LDAP, or SAML authentication provider.

About built-in authentication for users outside your provider



By default, when you enable external authentication for GitHub Enterprise Server, built-in authentication is disabled for your instance. For more information, see "[About authentication for your enterprise](#)."

If you're unable to add specific accounts to your external authentication provider, such as accounts for contractors or machine users, you can configure fallback authentication. Fallback authentication allows built-in authentication for outside users and to access a fallback account if your authentication provider is unavailable.

If you configure built-in authentication and a person successfully authenticates with SAML or CAS, the person will no longer have the option to authenticate with a username and password. If a user successfully authenticates with LDAP, the credentials are no longer considered internal.

Warning: If you disable built-in authentication, you must individually suspend any users that should no longer have access to the instance. For more information, see "[Suspending and unsuspending users](#)."

Configuring built-in authentication for users outside your provider

- 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 your authentication method.
- 6 Select **Allow creation of accounts with built-in authentication**.
- 7 Read the warning, then click **Ok**.

Two-factor authentication

When using LDAP or built-in authentication, two-factor authentication is supported. Organization owners can require members to have two-factor authentication enabled.

Inviting users outside your provider to authenticate to your instance

When a user accepts the invitation, they can use their username and password to sign in rather than signing in through the IdP.

- 1 Sign in to your GitHub Enterprise Server instance at `http(s)://HOSTNAME/login`.
- 2 From an administrative account on GitHub Enterprise Server, in the upper-right corner of any page, click .
- 3 If you're not already on the "Site admin" page, in the upper-left corner, click **Site admin**.
- 4 In the left sidebar, click **Invite user**.
- 5 Type the username and email address for each of the user accounts that you'd like to create, then click **Generate a password reset link**.

Further reading

- ["Using CAS for enterprise IAM"](#)
- ["Using LDAP for enterprise IAM"](#)
- ["Using SAML for enterprise IAM"](#)

Legal

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