Using CAS

In this article

If you use Central Authentication Service (CAS) to centralize access to multiple web applications, you can integrate GitHub Enterprise Server by configuring CAS authentication for your instance.

About CAS authentication for GitHub Enterprise Server

CAS is a single sign-on (SSO) protocol that centralizes authentication to multiple web applications. For more information, see "Central Authentication Service" on Wikipedia.

After you configure CAS, people who use your GitHub Enterprise Server instance must use a personal access token to authenticate API or Git requests over HTTP(S). CAS credentials cannot be used to authenticate these requests. For more information, see "Managing your personal access tokens."

If you configure CAS, people with accounts on your identity provider (IdP) do not consume a user license until the person signs into your GitHub Enterprise Server instance.

If you want to allow authentication for some people who don't have an account on your external authentication provider, you can allow fallback authentication to local accounts on your GitHub Enterprise Server instance. For more information, see "Allowing built-in authentication for users outside your provider."

Username considerations with CAS

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."

CAS attributes

The `username` attribute is required and should be set to the GitHub Enterprise Server username.

No other attributes are available.

Configuring CAS

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 **CAS**.

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. In the **Server URL** field, type the full URL of your CAS server. If your CAS server uses a certificate that can't be validated by GitHub Enterprise Server, you can use the `ghe-ssl-ca-certificate-install` command to install it as a trusted certificate. For more information, see "Command-line utilities."