Enabling private mode

In private mode, GitHub Enterprise Server requires every user to sign in to access the installation.

You must enable private mode if your GitHub Enterprise Server instance is publicly accessible over the Internet. In private mode, users cannot anonymously clone repositories over `git://`. If built-in authentication is also enabled, an administrator must invite new users to create an account on the instance. For more information, see "[Configuring built-in authentication](#)."

> **Warning:** If you add an image attachment to a pull request or issue comment, anyone can view the anonymized image URL without authentication, even if the pull request is in a private repository, or if private mode is enabled. To prevent unauthorized access to the images, ensure that you restrict network access to the systems that serve the images, including your GitHub Enterprise Server instance.

With private mode enabled, you can allow unauthenticated Git operations (and anyone with network access to your GitHub Enterprise Server instance) to read a public repository's code on your instance with anonymous Git read access enabled. For more information, see "[Enforcing repository management policies in your enterprise](#)."

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 **Privacy**.

5. Select **Private mode**.

6. Under the "Settings" sidebar, click **Save settings**.

   > **Note:** Saving settings in the Management Console restarts system services, which could result in user-visible downtime.

7. Wait for the configuration run to complete.