

Sudo mode

In this article

About sudo mode

Confirming access for sudo mode

Confirming access using a passkey

To confirm access to your account before you perform a potentially sensitive action, GitHub.com prompts for authentication.

About sudo mode

To maintain the security of your account when you perform a potentially sensitive action on GitHub.com, you must authenticate even though you're already signed in. For example, GitHub considers the following actions sensitive because each action could allow a new person or system to access your account.

- Modification of an associated email address
- Authorization of a third-party application
- Addition of a new SSH key
- Creation of a PAT or application

After you authenticate to perform a sensitive action, your session is temporarily in "sudo mode." In sudo mode, you can perform sensitive actions without authentication. GitHub Enterprise Cloud has a two-hour session timeout period before prompting you for authentication again. During this time, any sensitive action that you perform will reset the timer.

Note: If your enterprise uses Enterprise Managed Users, only the setup user will receive prompts to enter sudo mode, as managed user accounts don't have credentials stored on GitHub Enterprise Cloud.

"sudo" is a reference to a program on Unix systems, where the name is short for "superuser **do**." For more information, see [sudo](#) on Wikipedia.

Confirming access for sudo mode

To confirm access for sudo mode, you can authenticate with your password. Optionally, you can use a different authentication method, like a passkey, a security key, GitHub Mobile, or a 2FA code.

- [Confirming access using a passkey key](#)
- [Confirming access using a security key](#)
- [Confirming access using GitHub Mobile](#)
- [Confirming access using a 2FA code](#)
- [Confirming access using your password](#)

Confirming access using a passkey

You must have a passkey registered to your account to confirm access to your account for sudo mode using a passkey. For more information, see "[About passkeys](#)" and "[Managing your passkeys](#)."

Confirming access using a security key

You must configure two-factor authentication (2FA) for your account using a security key to confirm access to your account for sudo mode using the security key. For more information, see "[Configuring two-factor authentication](#)."

When prompted to authenticate for sudo mode, click **Use security key**, then follow the prompts.

Confirming access using GitHub Mobile

You must install and sign into GitHub Mobile to confirm access to your account for sudo mode using the app. For more information, see "[GitHub Mobile](#)."

- 1 When prompted to authenticate for sudo mode, click **Use GitHub Mobile**.
- 2 Open GitHub Mobile. GitHub will display numbers that you must enter in GitHub Mobile to approve the request.
- 3 In GitHub Mobile, type the numbers displayed.

Confirming access using a 2FA code

You must configure 2FA using a TOTP mobile app to confirm access to your account for sudo mode using a 2FA code. For more information, see "[Configuring two-factor authentication](#)."

When prompted to authenticate for sudo mode, type the authentication code from your TOTP mobile app, then click **Verify**.

Text messages are not supported for use on the sudo prompt. If you have registered SMS as the only 2FA method on your account, you'll be asked for your password to enter sudo mode.

Confirming access using your password

When prompted to authenticate for sudo mode, type your password, then click **Confirm**.

Legal

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