

Preventing unauthorized access

You may be alerted to a security incident in the media, such as the discovery of the [Heartbleed bug](#), or your computer could be stolen while you're signed in to your GitHub Enterprise Server instance. In such cases, changing your password prevents any unintended future access to your account and projects.

GitHub Enterprise Server requires a password to perform sensitive actions, such as adding new SSH keys, authorizing applications, or modifying team members.

After changing your password, you should perform these actions to make sure that your account is secure:

- Enable two-factor authentication on your account so that access requires more than just a password. For more information, see "[About two-factor authentication](#)."
- Review your SSH keys, deploy keys, and authorized integrations and revoke unauthorized or unfamiliar access in your SSH and Applications settings. For more information, see "[Reviewing your SSH keys](#)," "[Reviewing your deploy keys](#)," and "[Reviewing and revoking authorization of GitHub Apps](#)."
- Review your account's security log. This provides an overview on various configurations made to your repositories. For example, you can ensure that no private repositories were turned public, or that no repositories were transferred. For more information, see "[Reviewing your security log](#)."
- Review the webhooks on your repositories. Webhooks could allow an attacker to intercept pushes made to your repository. For more information, see "[About webhooks](#)."
- Make sure that no new deploy keys were created. This could enable outside servers access to your projects. For more information, see "[Managing deploy keys](#)."
- Review recent commits made to your repositories.
- Review the list of collaborators for each repository.

Legal