

**This version of GitHub Enterprise was discontinued on 2023-03-15.** No patch releases will be made, even for critical security issues. For better performance, improved security, and new features, [upgrade to the latest version of GitHub Enterprise](#). For help with the upgrade, [contact GitHub Enterprise support](#).

# Managing your personal access tokens

## In this article

About personal access tokens

Creating a personal access token

Deleting a personal access token

Using a personal access token on the command line

Further reading

You can use a personal access token in place of a password when authenticating to GitHub in the command line or with the API.

**Warning:** Treat your access tokens like passwords. For more information, see "[Keeping your personal access tokens secure](#)."

## About personal access tokens


Personal access tokens are an alternative to using passwords for authentication to GitHub Enterprise Server when using the [GitHub API](#) or the [command line](#).

Personal access tokens are intended to access GitHub resources on behalf of yourself. To access resources on behalf of an organization, or for long-lived integrations, you should use a GitHub App. For more information, see "[About creating GitHub Apps](#)."

## Creating a personal access token

- 1 In the upper-right corner of any page, click your profile photo, then click **Settings**.



- 2 In the left sidebar, click **Developer settings**.
- 3 In the left sidebar, click **Personal access tokens**.
- 4 Click **Generate new token**.
- 5 In the "Note" field, give your token a descriptive name.
- 6 To give your token an expiration, select **Expiration**, then choose a default option or click **Custom** to enter a date.
- 7 Select the scopes you'd like to grant this token. To use your token to access repositories from the command line, select **repo**. A token with no assigned scopes can only access public information. For more information, see "[Scopes for OAuth apps](#)".
- 8 Click **Generate token**.
- 9 Optionally, to copy the new token to your clipboard, click .

## Deleting a personal access token

- 1 In the upper-right corner of any page, click your profile photo, then click **Settings**.



- 2 In the left sidebar, click **Developer settings**.
- 3 In the left sidebar, click **Personal access tokens**.
- 4 To the right of the personal access token you want to delete, click **Delete**.

## Using a personal access token on the command line



Once you have a personal access token, you can enter it instead of your password when performing Git operations over HTTPS.

For example, to clone a repository on the command line you would enter the following `git clone` command. You would then be prompted to enter your username and password. When prompted for your password, enter your personal access token instead of a password.

```
$ git clone https://HOSTNAME/USERNAME/REPO.git
Username: YOUR_USERNAME
Password: YOUR_PERSONAL_ACCESS_TOKEN
```

Personal access tokens can only be used for HTTPS Git operations. If your repository uses an SSH remote URL, you will need to [switch the remote from SSH to HTTPS](#).

If you are not prompted for your username and password, your credentials may be cached on your computer. You can [update your credentials in the Keychain](#) to replace your old password with the token.

Instead of manually entering your personal access token for every HTTPS Git operation, you can cache your personal access token with a Git client. Git will temporarily store your credentials in memory until an expiry interval has passed. You can also store the token in a plain text file that Git can read before every request. For more information, see "[Caching your GitHub credentials in Git](#)."

## Further reading

---

- "[About authentication to GitHub](#)"
- "[Token expiration and revocation](#)"

### Legal

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