This article is also available in Simplified Chinese.   ✕

GitHub Docs | Version: Free, Pro, & Team   ▾   🔍   ⋯

☰   Get started / Getting started with Git / Caching credentials

Caching your GitHub credentials in Git

If you're cloning GitHub repositories using HTTPS, we recommend you use GitHub CLI or Git Credential Manager (GCM) to remember your credentials.

Mac   Windows   Linux

In this article

GitHub CLI

Git Credential Manager

> **Tip:** If you clone GitHub repositories using SSH, then you can authenticate using an SSH key instead of using other credentials. For information about setting up an SSH connection, see "Connecting to GitHub with SSH."

GitHub CLI

GitHub CLI will automatically store your Git credentials for you when you choose `HTTPS` as your preferred protocol for Git operations and answer "yes" to the prompt asking if you would like to authenticate to Git with your GitHub credentials.

1   Install GitHub CLI on macOS, Windows, or Linux.

2   In the command line, enter `gh auth login`, then follow the prompts.
    ○   When prompted for your preferred protocol for Git operations, select `HTTPS`.

- ○ When asked if you would like to authenticate to Git with your GitHub credentials, enter `Y`.

For more information about authenticating with GitHub CLI, see `gh auth login`.

Git Credential Manager

Git Credential Manager (GCM) is another way to store your credentials securely and connect to GitHub over HTTPS. With GCM, you don't have to manually create and store a personal access token, as GCM manages authentication on your behalf, including 2FA (two-factor authentication).

1. Install Git using Homebrew:

   ```
   brew install git
   ```

2. Install GCM using Homebrew:

   ```
   brew install --cask git-credential-manager
   ```

For macOS, you don't need to run `git config` because GCM automatically configures Git for you.

The next time you clone an HTTPS URL that requires authentication, Git will prompt you to log in using a browser window. You may first be asked to authorize an OAuth app. If your account or organization requires two-factor auth, you'll also need to complete the 2FA challenge.

Once you've authenticated successfully, your credentials are stored in the macOS keychain and will be used every time you clone an HTTPS URL. Git will not require you to type your credentials in the command line again unless you change your credentials.

For more information or to report issues with GCM, see the official GCM docs at "Git Credential Manager."

Legal

© 2024 GitHub, Inc.   Terms   Privacy   Status   Pricing   Expert services   Blog