Caching your GitHub credentials in Git - GitHub Docs

2-2 minutes

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

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).

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