Accessing GitHub using two-factor authentication

In this article

With 2FA enabled, you'll be asked to provide your 2FA authentication code, as well as your password, when you sign in to GitHub.

With two-factor authentication (2FA) enabled, you'll need to use a second factor when accessing GitHub through your browser. When you first configure 2FA, your account will enter a check up period for 28 days to ensure your account's 2FA methods are setup correctly. You can exit the check up period by successfully performing 2FA within 28 days. If you don't authenticate within 28 days, you'll be asked to perform 2FA inside one of your existing GitHub.com sessions. If you cannot perform 2FA to pass the 28th day checkup, use the provided shortcut to reconfigure your 2FA settings and retain access to GitHub.com. For more information, see "Configuring two-factor authentication."

If you access GitHub using other methods, such as the API or the command line, you'll authenticate using a token, application, or SSH key. For more information, see "About authentication to GitHub."

Performing 2FA when signing in to the website

After you sign in to GitHub using your password, you'll need to provide an authentication code, tap a notification in GitHub Mobile, or use a security key to perform 2FA.

GitHub will only ask you to provide your 2FA authentication code again if you've logged out, are using a new device, are performing a sensitive action, or your session expires. For more information on 2FA for sensitive actions, see "Sudo mode."

Generating a code through a TOTP application

If you chose to set up two-factor authentication using a TOTP application, you can generate an authentication code for GitHub at any time. In most cases, just launching the application will generate a new code. You should refer to your application's documentation for specific instructions.

If you delete your authenticator application after configuring two-factor authentication, you'll need to provide your recovery code to get access to your account. Many TOTP apps support the secure backup of your authentication codes in the cloud and can be restored if you lose access to your device. For more information, see "Recovering your account if you lose your 2FA credentials."

Using a security key

If you've set up a security key on your account, and your browser supports security keys, you can use it to complete your sign in.

1. Using your username and password, sign in to GitHub through your browser.
2. If you use a physical security key, ensure it's connected to your device.
3. To trigger the security key prompt from your operating system, select "Use security key".
4. Select the appropriate option in the prompt. Depending on your security key configuration, you may type a PIN, complete a biometric prompt, or use a physical security key.

Using a passkey

If you have enabled 2FA, and you have added a passkey to your account, you can use the passkey to sign in. Since passkeys satisfy both password and 2FA requirements, you can complete your sign in with a single step. For more information, see "About passkeys" and "Signing in with a passkey."

Receiving a text message

If you set up two-factor authentication via text messages, GitHub will send you a text message with your authentication code.

Verifying with GitHub Mobile

If you have installed and signed in to GitHub Mobile, you may choose to authenticate with GitHub Mobile for two-factor authentication.

1. Sign in to GitHub with your browser, using your username and password.
2. GitHub will send you a push notification to verify your sign in attempt. Opening the push notification or opening the GitHub Mobile app will display a prompt, asking you to approve or reject this sign in attempt.

   > **Note**: This prompt may require you to enter a two-digit number displayed within the browser you are signing in to.

   - Upon approving the login attempt using GitHub Mobile, your browser will complete the sign in attempt automatically.
   - Rejecting the sign in attempt will prevent the authentication from finishing. For more information, see "Keeping your account and data secure."

Using two-factor authentication with the command line

Enabling 2FA may affect authentication to GitHub through the command line. To find out if your authentication method is affected, see the following sections.

Authenticating on the command line using Git Credential Manager

Git Credential Manager is a secure Git credential helper that runs on Windows, macOS, and Linux. For more information about Git credential helpers, see Avoiding repetition in the Pro Git book.

Setup instructions vary based on your computer's operating system. For more information, see Download and install in the GitCredentialManager/git-credential-manager repository.

Authenticating on the command line using HTTPS

You must create a personal access token to use as a password when authenticating to GitHub on the command line using HTTPS URLs.

When prompted for a username and password on the command line, use your GitHub username and personal access token. The command line prompt won't specify that you should enter your personal access token when it asks for your password.

For more information, see "Managing your personal access tokens."

Authenticating on the command line using SSH

Enabling 2FA doesn't change how you authenticate to GitHub on the command line using SSH URLs. For more information about setting up and using an SSH key, see "Connecting to GitHub with SSH."

Using two-factor authentication to access a repository using Subversion

> **Note**: Subversion support will be removed from GitHub on January 8, 2024. A future release of GitHub Enterprise Server after January 8, 2024 will also remove Subversion support. To read more about this, see the GitHub blog.

When you access a repository via Subversion, you must provide a personal access token instead of entering your password. For more information, see "Managing your personal access tokens."

Troubleshooting

If you lose access to your two-factor authentication credentials, you can use your recovery codes or another recovery method (if you've set one up) to regain access to your account. For more information, see "Recovering your account if you lose your 2FA credentials."

> **Note:** If you cannot use any recovery methods, you have permanently lost access to your account. However, you can unlink an email address tied to the locked account. The unlinked email address can then be linked to a new or existing account. For more information, see "Unlinking your email address from a locked account."

If your authentication fails several times, you may wish to synchronize your phone's clock with your mobile provider. Often, this involves checking the "Set automatically" option on your phone's clock, rather than providing your own time zone.

Further reading

- "About two-factor authentication"
- "Configuring two-factor authentication"
- "Configuring two-factor authentication recovery methods"
- "Recovering your account if you lose your 2FA credentials"