

Configuring two-factor authentication

In this article

Configuring two-factor authentication using a TOTP app

Configuring two-factor authentication using text messages

Configuring two-factor authentication using a passkey

Configuring two-factor authentication using a security key

Configuring two-factor authentication using GitHub Mobile

Further reading

You can choose among multiple options to add a second source of authentication to your account.

Note: Starting in March 2023 and through the end of 2023, GitHub will gradually begin to require all users who contribute code on GitHub.com to enable one or more forms of two-factor authentication (2FA). If you are in an eligible group, you will receive a notification email when that group is selected for enrollment, marking the beginning of a 45-day 2FA enrollment period, and you will see banners asking you to enroll in 2FA on GitHub.com. If you don't receive a notification, then you are not part of a group required to enable 2FA, though we strongly recommend it.

For more information about the 2FA enrollment rollout, see [this blog post](#).

You can configure two-factor authentication (2FA) using a TOTP app on mobile or desktop or via text message. After you have configured 2FA using a TOTP app or via text message, you can then also add security keys as alternate 2FA methods.

We strongly recommend using a time-based one-time password (TOTP) application to configure 2FA, and security keys as backup methods instead of SMS. TOTP applications are more reliable than SMS, especially for locations outside the United States. 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.

After you configure 2FA, your account will enter a 28-day check up period. You can leave the check up period by successfully performing 2FA in those 28 days. Otherwise, you will be prompted to perform 2FA in an existing GitHub.com session on the 28th day. If you cannot perform 2FA to pass the checkup, you must use the provided shortcut to reconfigure your 2FA settings and retain access to GitHub.com.

If you're a member of an enterprise with managed users, you cannot configure 2FA for your managed user account unless you're signed in as the setup user. For users other than the setup user, an administrator must configure 2FA on your identity provider (IdP).

Warning:

- If you're a member, billing manager, or outside collaborator to a private repository of an organization that requires two-factor authentication, you must leave the organization before you can disable 2FA on GitHub.com.
- If you disable 2FA, you will automatically lose access to the organization and any private forks you have of the organization's private repositories. To regain access to the organization

and your forks, re-enable two-factor authentication and contact an organization owner.

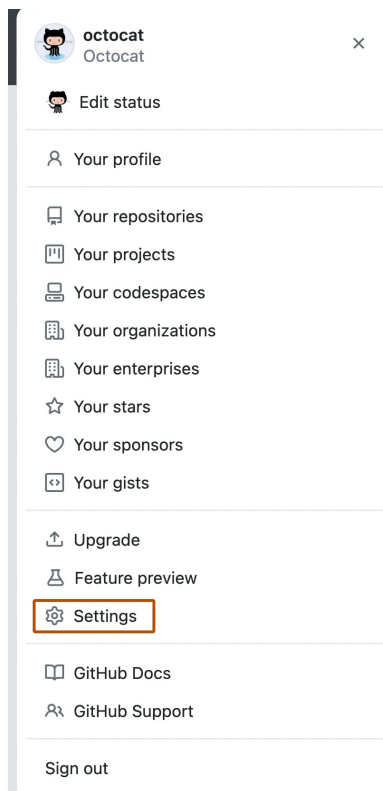
Note: You can reconfigure your 2FA settings without disabling 2FA entirely, allowing you to keep both your recovery codes and your membership in organizations that require 2FA.

Configuring two-factor authentication using a TOTP app [↗](#)

A time-based one-time password (TOTP) application automatically generates an authentication code that changes after a certain period of time. These apps can be downloaded to your phone or desktop. We recommend using cloud-based TOTP apps. GitHub is app-agnostic when it comes to TOTP apps, so you have the freedom to choose any TOTP app you prefer. Just search for `TOTP app` in your browser to find various options. You can also refine your search by adding keywords like `free` or `open source` to match your preferences.

Tip: To configure authentication via TOTP on multiple devices, during setup, scan the QR code using each device at the same time or save the "setup key", which is the TOTP secret. If 2FA is already enabled and you want to add another device, you must re-configure your TOTP app from your security settings.

- 1 Download a TOTP app of your choice to your phone or desktop.
- 2 In the upper-right corner of any page, click your profile photo, then click **Settings**.



- 3 In the "Access" section of the sidebar, click **Password and authentication**.
- 4 In the "Two-factor authentication" section of the page, click **Enable two-factor authentication**.
- 5 Under "Setup authenticator app", do one of the following:
 - Scan the QR code with your mobile device's app. After scanning, the app

displays a six-digit code that you can enter on GitHub Enterprise Cloud.

- If you can't scan the QR code, click **setup key** to see a code, the TOTP secret, that you can manually enter in your TOTP app instead.

Setup authenticator app

Authenticator apps and browser extensions like [1Password](#), [Authy](#), [Microsoft Authenticator](#), etc. generate one-time passwords that are used as a second factor to verify your identity when prompted during sign-in.

Scan the QR code

Use an authenticator app or browser extension to scan. [Learn more about enabling 2FA](#).



Unable to scan? You can use the [setup key](#) to manually configure your authenticator app.

- 6 The TOTP application saves your account on GitHub.com and generates a new authentication code every few seconds. On GitHub Enterprise Cloud, type the code into the field under "Verify the code from the app".
- 7 Under "Save your recovery codes", click **Download** to download your recovery codes to your device. Save them to a secure location because your recovery codes can help you get back into your account if you lose access.
- 8 After saving your two-factor recovery codes, click **I have saved my recovery codes** to enable two-factor authentication for your account.
- 9 Optionally, you can configure additional 2FA methods to reduce your risk of account lockout. For more details on how to configure each additional method, see "[Configuring two-factor authentication using GitHub Mobile](#)" and "[Configuring two-factor authentication using a security key](#)".

If you wish to setup a TOTP app manually, and require the parameters encoded in the QR code, they are:

- Type: `TOTP`
- Label: `GitHub:<username>` where `<username>` is your handle on GitHub, for example `monalisa`
- Secret: This is the encoded setup key, shown if you click "setup key" during configuration
- Issuer: `GitHub`
- Algorithm: The default of SHA1 is used
- Digits: The default of 6 is used
- Period: The default of 30 (seconds) is used

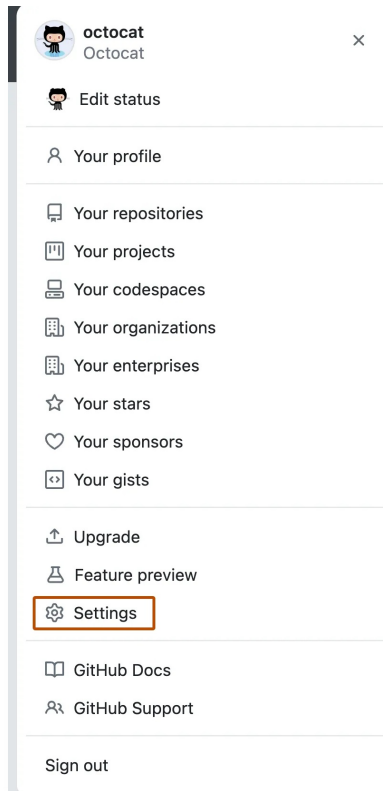
Configuring two-factor authentication using text messages [↗](#)

If you're unable to configure a TOTP app, you can also register your phone number to receive SMS messages.

Before using this method, be sure that you can receive text messages. Carrier rates may apply.

Warning: We **strongly recommend** using a TOTP application for two-factor authentication instead of SMS, and security keys as backup methods instead of SMS. GitHub Enterprise Cloud doesn't support sending SMS messages to phones in every country. Before configuring authentication via text message, review the list of countries where GitHub Enterprise Cloud supports authentication via SMS. For more information, see "[Countries where SMS authentication is supported](#)".

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



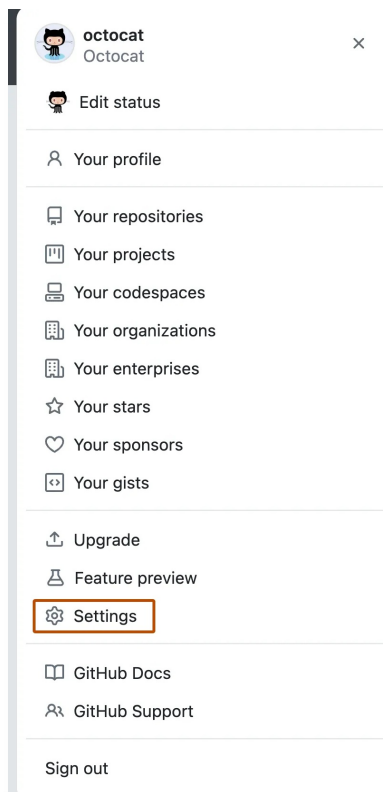
- 2 In the "Access" section of the sidebar, click ⓘ **Password and authentication**.
- 3 In the "Two-factor authentication" section of the page, click **Enable two-factor authentication**.
- 4 At the bottom of the page, next to "SMS authentication", click **Select**.
- 5 Complete the CAPTCHA challenge, which helps protect against spam and abuse.
- 6 Under "Setup SMS authentication", select your country code and type your mobile phone number, including the area code. When your information is correct, click **Send authentication code**.
- 7 You'll receive a text message with a security code. On GitHub Enterprise Cloud, type the code into the field under "Verify the code sent to your phone" and click **Continue**.
 - If you need to edit the phone number you entered, you'll need to complete another CAPTCHA challenge.
- 8 Under "Save your recovery codes", click **Download** to download your recovery codes to your device. Save them to a secure location because your recovery codes can help you get back into your account if you lose access.


- 9 After saving your two-factor recovery codes, click **I have saved my recovery codes** to enable two-factor authentication for your account.
- 10 Optionally, you can configure additional 2FA methods to reduce your risk of account lockout. For more details on how to configure each additional method, see "[Configuring two-factor authentication using GitHub Mobile](#)" and "[Configuring two-factor authentication using a security key](#)".

Configuring two-factor authentication using a passkey

Passkeys allow you to sign in securely to GitHub.com, without having to input your password. If you use two-factor authentication (2FA), passkeys satisfy both password and 2FA requirements, so you can complete your sign in with a single step. You can also use passkeys for sudo mode and resetting your password. For more information, see "[About passkeys](#)".

- 1 You must have already configured 2FA via a TOTP mobile app or via SMS.
- 2 In the upper-right corner of any page, click your profile photo, then click **Settings**.



- 3 In the "Access" section of the sidebar, click  **Password and authentication**.
- 4 Under "Passkeys", click **Add a passkey**.
- 5 If prompted, authenticate with your password, or use another existing authentication method.
- 6 Under "Configure passwordless authentication", review the prompt, then click **Add passkey**.
- 7 At the prompt, follow the steps outlined by the passkey provider.
- 8 On the next page, review the information confirming that a passkey was

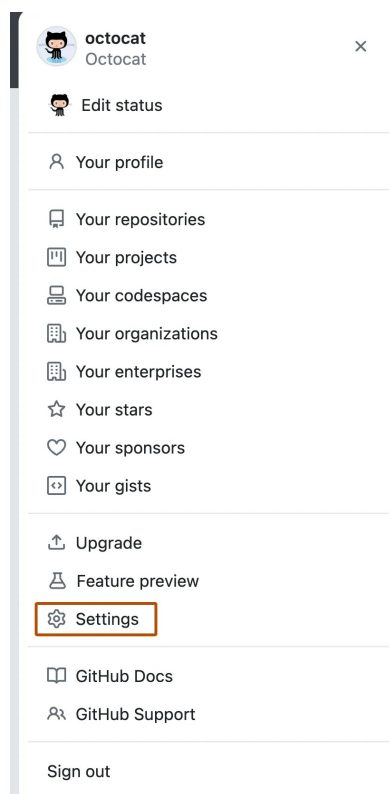
successfully registered, then click **Done**.

Configuring two-factor authentication using a security key [🔗](#)

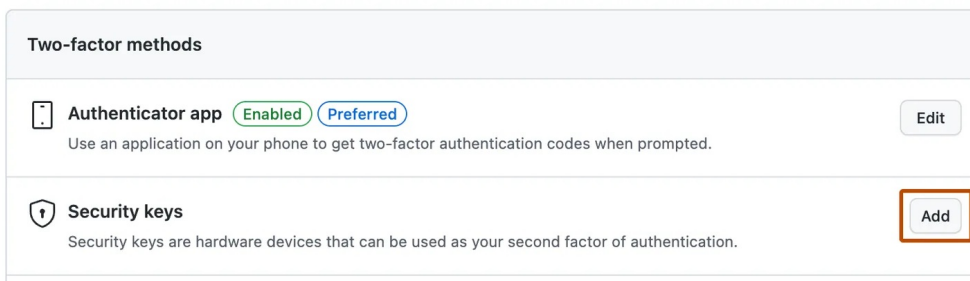
Not all FIDO authenticators can be used as passkeys, but you can still register those authenticators as security keys. Security keys are also webauthn credentials, but unlike passkeys they don't need to require user validation. Since security keys only need to verify user presence, they only count as a second factor and must be used in conjunction with your password.

Registering a security key for your account is available after enabling 2FA with a TOTP application or a text message. If you lose your security key, you'll still be able to use your phone's code to sign in.

- 1 You must have already configured 2FA via a TOTP mobile app or via SMS.
- 2 Ensure that you have a WebAuthn compatible security key inserted into your device, or that your device has a built-in authenticator such as Windows Hello, Face ID, or Touch ID. Most computers, phones, and tablets support this as an easier-to-use alternative to physical security keys.
- 3 In the upper-right corner of any page, click your profile photo, then click **Settings**.



- 4 In the "Access" section of the sidebar, click **Password and authentication**.
- 5 Next to "Security keys", click **Add**.



- 6 Under "Security keys", click **Register new security key**.
- 7 Type a nickname for the security key, then click **Add**.
- 8 Following your security key's documentation, activate your security key. If using an authenticator that's built into your device, follow the activation instructions from your operating system. You may need to select options such as `Face` , `PIN` , or `built-in sensor` to access your device's authenticator, depending on your operating system and browser.
- 9 Confirm that you've downloaded and can access your recovery codes. If you haven't already, or if you'd like to generate another set of codes, download your codes and save them in a safe place. For more information, see "[Configuring two-factor authentication recovery methods](#)."

Configuring two-factor authentication using GitHub Mobile [↗](#)

You can use GitHub Mobile for 2FA when signing into your GitHub account in a web browser. 2FA with GitHub Mobile does not rely on TOTP, and instead uses public-key cryptography to secure your account.

Once you have configured a TOTP application, or SMS, you can also use GitHub Mobile to authenticate. If, in the future, you no longer have access to GitHub Mobile, you will still be able to use security keys or TOTP applications to sign in.

- 1 You must have already configured 2FA via a TOTP mobile app or via SMS.
- 2 Install [GitHub Mobile](#).
- 3 Sign in to your GitHub Enterprise Cloud account from GitHub Mobile.

After signing in, you can now use your device for 2FA.

Further reading [↗](#)

- "[About two-factor authentication](#)"
- "[Configuring two-factor authentication recovery methods](#)"
- "[Accessing GitHub using two-factor authentication](#)"
- "[Recovering your account if you lose your 2FA credentials](#)"
- "[Managing your personal access tokens](#)"

Legal

