Configuring two-factor authentication

In this article

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

You can configure two-factor authentication (2FA) using a TOTP app on mobile or desktop. After you have configured 2FA using a TOTP app, 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. 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.

Warning:

- If you're a member 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 your GitHub Enterprise Server instance.
- 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.

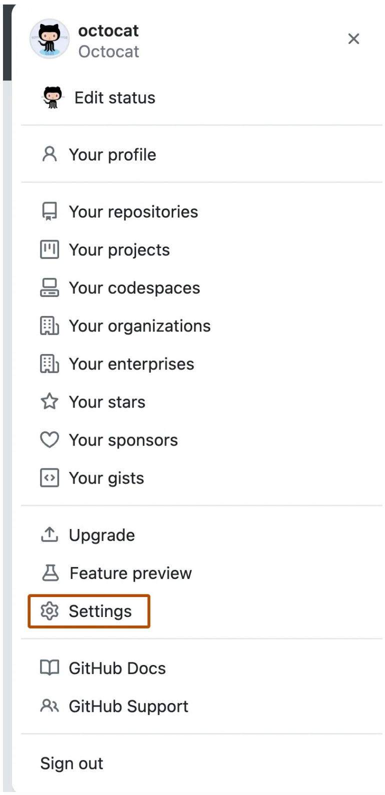
Configuring two-factor authentication using a TOTP app

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**.

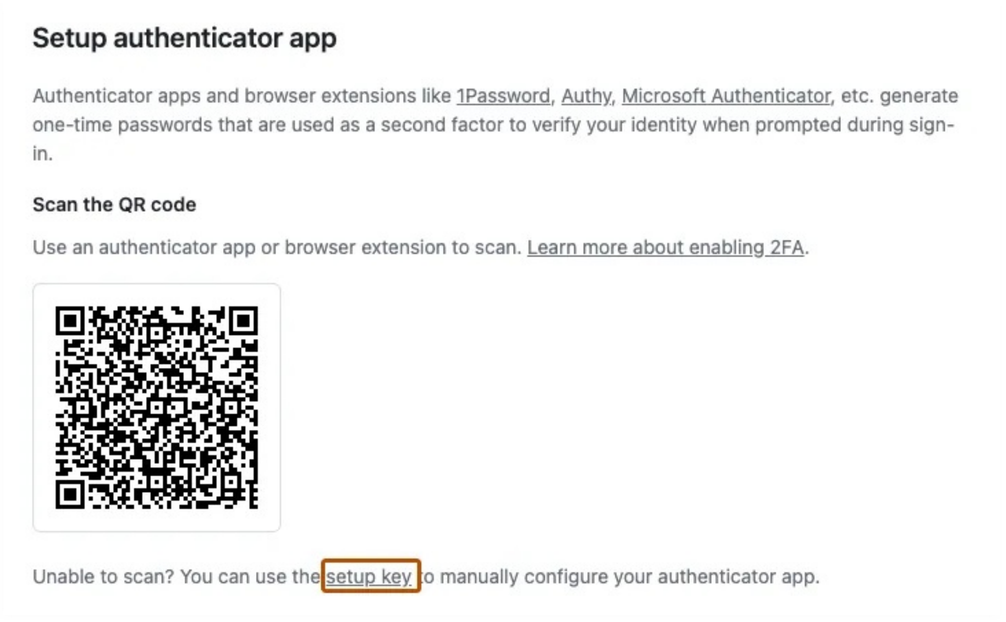


3. In the "Access" section of the sidebar, click **Password and authentication**.

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 Server.
   - 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 your GitHub Enterprise Server instance and generates a new authentication code every few seconds. On GitHub Enterprise Server, 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 a security key

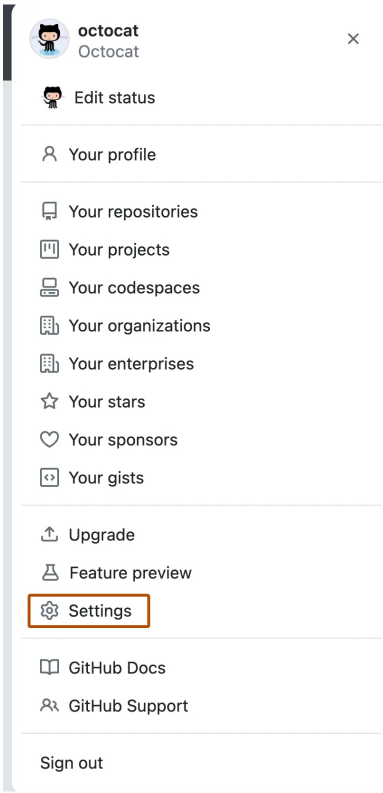
On most devices and browsers, you can use a physical security key over USB or NFC. Most browsers can use the fingerprint reader, facial recognition, or password/PIN on your device as a security key as well.

Registering a security key for your account is available after enabling 2FA with a TOTP application. 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.

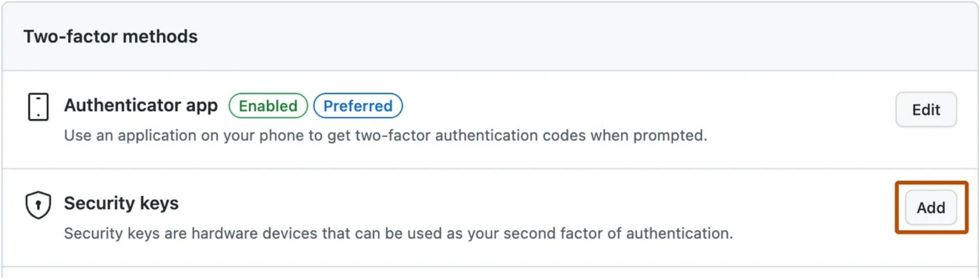
2. Ensure that you have a WebAuthn compatible security key inserted into your device, or that your device has a built-in authenticator such as Windows Hello, Face ID, or Touch ID. Most computers, phones, and tablets support this as an easier-to-use alternative to physical security keys.

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**.



Two-factor methods

Authenticator app Enabled Preferred

Use an application on your phone to get two-factor authentication codes when prompted.

Edit

Security keys

Security keys are hardware devices that can be used as your second factor of authentication.

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."

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"