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 mobile app. You can also add a security key.

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.

Configuring two-factor authentication using a TOTP mobile app

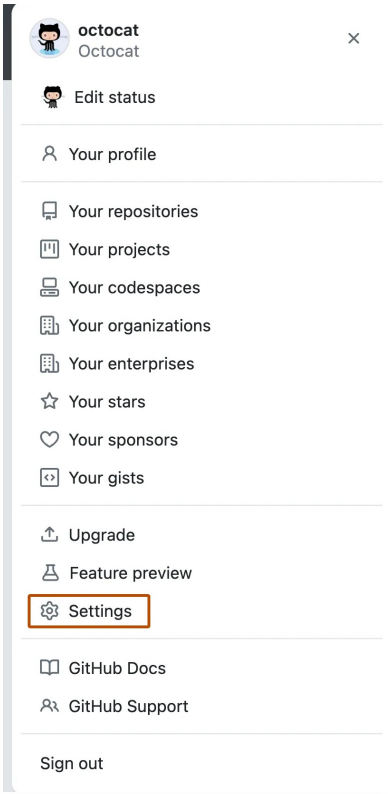
A time-based one-time password (TOTP) application automatically generates an authentication code that changes after a certain period of time. We recommend using cloud-based TOTP apps such as:

- 1Password
- Authy
- LastPass Authenticator
- Microsoft Authenticator

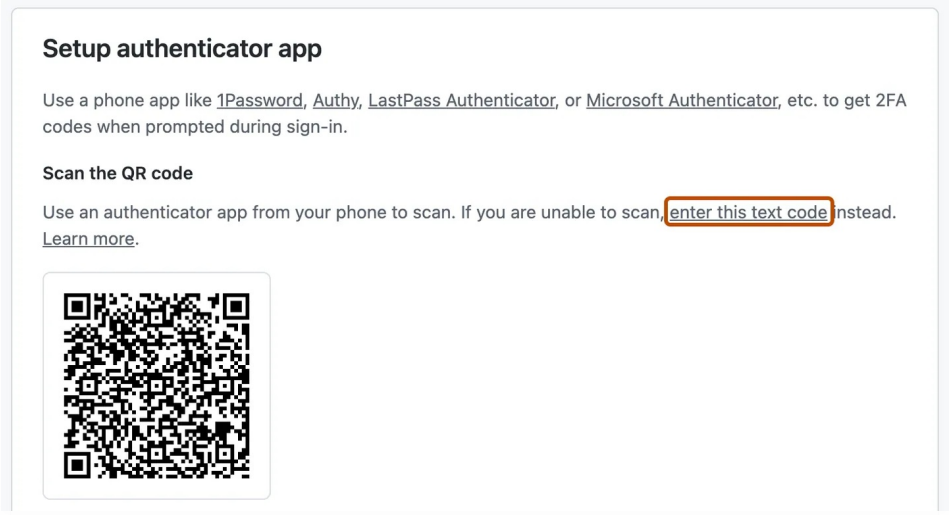
Tip: To configure authentication via TOTP on multiple devices, during setup, scan the QR code using each device at the same time. If 2FA is already enabled and you want to add another device, you must re-configure your TOTP app from your security settings.

1. Download a TOTP app.

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



3. In the left sidebar, click **Account security**.
4. In the "Two-factor authentication" section of the page, click **Enable two-factor authentication**.
5. Under "Two-factor authentication", select **Set up using an app** and click **Continue**.
6. Under "Authentication verification", 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 **enter this text code** to see a code that you can manually enter in your TOTP app instead.



7. The TOTP mobile 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 "Enter the six-digit code from the application".

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" and "Configuring two-factor authentication".

11. After you've saved your recovery codes and enabled 2FA, we recommend you sign out and back in to your account. In case of problems, such as a forgotten password or typo in your email address, you can use recovery codes to access your account and correct the problem.

Configuring two-factor authentication using a security key

After you configure 2FA, using a time-based one-time password (TOTP) mobile app, you can add a security key, like a fingerprint reader or Windows Hello. The technology that enables authentication with a security key is called WebAuthn. WebAuthn is the successor to U2F and works in all modern browsers. For more information, see "WebAuthn" and "Can I Use."

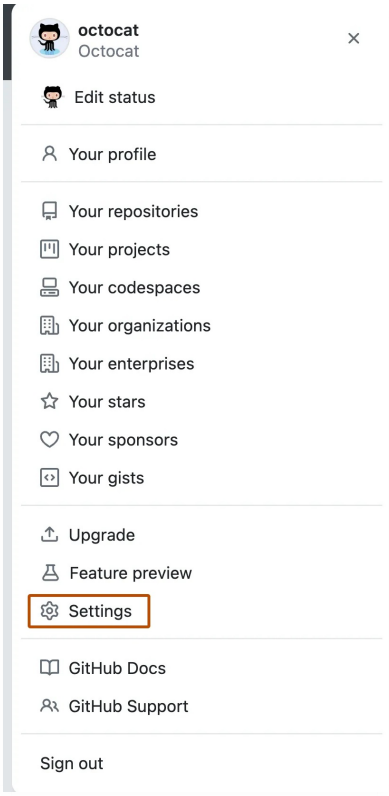
On most devices and browsers, you can use a physical security key over USB or NFC. Most browsers can use the fingerprint reader, facial recognition, or password/PIN on your device as a security key as well.

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.

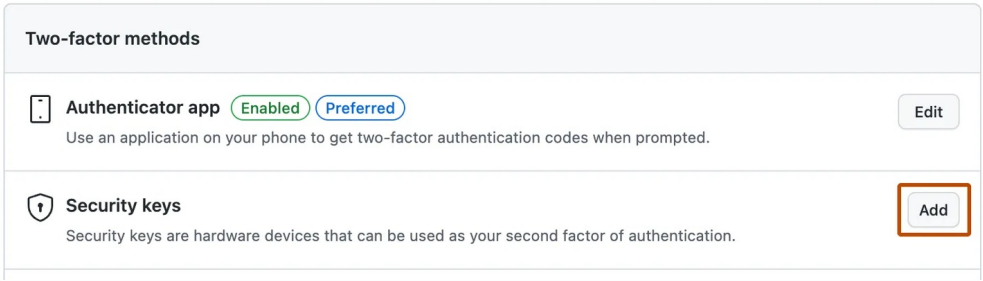
1. You must have already configured 2FA via a TOTP mobile app.

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 left sidebar, click **Account security**.
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."
10. After you've saved your recovery codes and enabled 2FA, we recommend you sign out and back in to your account. In case of problems, such as a forgotten password or typo in your email address, you can use recovery codes to access your account and correct the problem.

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"