About two-factor authentication

In this article

Two-factor authentication (2FA) is an extra layer of security used when logging into websites or apps. With 2FA, you have to log in with your username and password and provide another form of authentication that only you know or have access to.

> **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.

For GitHub, the second form of authentication is a code that's generated by an application on your mobile device or sent as a text message (SMS). After you enable 2FA, GitHub generates an authentication code any time someone attempts to sign into your account on GitHub.com. The only way someone can sign into your account is if they know both your password and have access to the authentication code on your phone.

After you configure 2FA, using a time-based one-time password (TOTP) mobile app, or via text message, you can add a security key, like a FIDO2 hardware security key, Apple Touch ID 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."

Optionally, you can add a passkey to your account. Passkeys are similar to security keys. However, passkeys satisfy both password and 2FA requirements, so you can sign in to your account in one step. If you have already configured a security key for 2FA that is passkey eligible, you may be prompted to upgrade your security key into a passkey during passkey registration. For more information, see "About passkeys" and "Managing your passkeys."

You can also use GitHub Mobile for 2FA after configuring a TOTP mobile app or text messages. GitHub Mobile uses public-key cryptography to secure your account, allowing you to use any mobile device that you've used to sign in to GitHub Mobile as your second factor.

You can also configure additional recovery methods in case you lose access to your two-factor authentication credentials. For more information on setting up 2FA, see "Configuring two-factor authentication" and "Configuring two-factor authentication recovery methods."

> **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."

We **strongly** urge you to enable 2FA for the safety of your account, not only on GitHub, but on other websites and apps that support 2FA. You can enable 2FA to access GitHub and GitHub Desktop.

For more information, see "Accessing GitHub using two-factor authentication."

Two-factor authentication recovery codes

When you configure two-factor authentication, you'll download and save your 2FA recovery codes. If you lose access to your phone, you can authenticate to GitHub using your recovery codes. For more information, see "Recovering your account if you lose your 2FA credentials."

Warning: For security reasons, GitHub Support will not be able to restore access to accounts with two-factor authentication enabled if you lose your two-factor authentication credentials or lose access to your account recovery methods. For more information, see "Recovering your account if you lose your 2FA credentials."

Requiring two-factor authentication in your organization

Organization owners can require that organization members, billing managers, and outside collaborators use two-factor authentication to secure their personal accounts. For more information, see "Requiring two-factor authentication in your organization."