About mandatory two-factor authentication

In this article

Enable mandatory two-factor authentication to secure your account and maintain access to GitHub.com.

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.

About eligibility for mandatory 2FA

Your account is selected for mandatory 2FA if you have taken some action on GitHub that shows you are a contributor. Eligible actions include:

- Publishing an app or action for others.
- Creating a release for your repository.
- Contributing to specific high-importance repositories, such as the projects tracked by the Open Source Security Foundation.
- Being an administrator of a high-importance repository.
- Being an organization owner for an organization containing repositories or other users.
- Being an enterprise administrator.

GitHub is continually assessing improvements to our account security features and 2FA requirements, so these criteria may change over time.

Note: If your account has an education coupon active, it is exempt from mandatory 2FA.

About mandatory 2FA for organizations and enterprises

Mandatory 2FA is required by GitHub itself to improve security for both individual developers and the broader software development ecosystem. Your administrator may also require 2FA enablement as a requirement to join their organization or enterprise, but those requirements are separate from this program.

Your account's eligibility for mandatory 2FA **does not** impact the eligibility of other

individuals. For example, if you are an organization owner, and your account is eligible for mandatory 2FA, that does not impact the eligibility of other accounts within your organization.

> **Note:** GitHub Enterprise Managed Users and on-premise GitHub Enterprise Server users are **not** required to enable 2FA. Mandatory 2FA enablement only applies to users with a password on GitHub.com.

About failure to enable mandatory 2FA

If you do not enable 2FA within the 45 day setup period, and you allow the 7 day grace period to expire, you will not be able to access GitHub.com until you enable 2FA. If you attempt to access GitHub.com, you will be prompted to enable 2FA.

If you fail to enable mandatory 2FA, tokens that belong to your account will continue to function since they are used in critical automation. These tokens include personal access tokens and OAuth tokens issued to applications to act on your behalf. Enabling 2FA will not revoke or change the behavior of tokens issued for your account. However, locked accounts will not be able to authorize new apps or create new PATs until they've enabled 2FA.

About required 2FA methods

We recommend setting up a time-based one-time password (TOTP) app as your primary 2FA method, and adding a passkey or security key as a backup. If you don't have a passkey or security key, the GitHub Mobile app is a good backup option as well. SMS is reliable in most countries, but has security risks that some threat models may not work with.

Currently, we don't support passkeys or security keys as primary 2FA methods since they are easy to lose and do not support sync across a wide enough range of devices. As passkeys are more widely adopted and sync support is more prevalent, we will support them as a primary method.

- About TOTP apps and mandatory 2FA
- About SAML SSO and mandatory 2FA
- About email verification and mandatory 2FA

> **Note:** We recommend retaining cookies on GitHub.com. If you set your browser to wipe your cookies every day, you'll never have a verified device for account recovery purposes, as the `_device_id` cookie is used to securely prove you've used that device previously. For more information, see "Recovering your account if you lose your 2FA credentials."

About TOTP apps and mandatory 2FA

TOTP apps are the recommended 2FA factor for GitHub. For more information on configuring TOTP apps, see "Configuring two-factor authentication."

If you do not want to download an app on your mobile device, there are multiple options for standalone TOTP apps that run across platforms. For desktop applications, we recommend KeePassXC, and for browser-based plugins, we recommend 1Password.

You can also manually set up any app that generates a code compatible with RFC 6238. For more information on manually setting up a TOTP app, see "Configuring two-factor authentication." For more information on RFC 6238, see TOTP: Time-Based One-Time Password Algorithm in the IETF documentation.

Note: If you are using FreeOTP for 2FA, you may see a warning about weak cryptographic parameters. GitHub uses an 80 bit secret to ensure compatibility with older versions of Google Authenticator. 80 bits is lower than the 128 bits recommended by the HOTP RFC, but at this time we have no plans to change this and recommend ignoring this message. For more information, see HOTP: An HMAC-Based One-Time Password Algorithm in the IETF documentation.

About SAML SSO and mandatory 2FA

If you have been selected for mandatory 2FA, you must enroll in 2FA on GitHub.com even if your company already requires single sign-on (SSO) with 2FA. While SSO with 2FA is a powerful way to protect organization or enterprise-owned resources, it does not protect user-owned content on GitHub.com unrelated to an organization or enterprise, nor does it protect a user's profile and settings.

GitHub only requires you to perform 2FA on the initial authentication and for sensitive actions, so even if you have to perform corporate 2FA every day to access GitHub, you will rarely have to perform 2FA a second time through GitHub. For more information on sensitive actions, see "Sudo mode."

About email verification and mandatory 2FA

When you log in to GitHub.com, email verification does not count as 2FA. Your account's email address is used for password resets, which are a form of account recovery. If an attacker has access to your email inbox, they can reset the password for your account and pass the email device verification check, reducing your account's protection to a single factor. We require a second factor to prevent this scenario, so that second factor must be distinct from your email inbox. When you enable 2FA, we will no longer perform email verification on login.

About your privacy with mandatory 2FA

If you have been selected for mandatory 2FA, that **does not** mean you have to provide GitHub with your phone number. You only have to provide your phone number if you use SMS for 2FA. Instead, we recommend configuring a TOTP app as your primary 2FA method. For more information, see "Configuring two-factor authentication."

Note: Your region may not be listed in the available SMS options. We monitor SMS delivery success rates on a per region basis, and disallow setup for regions that have poor delivery rates. If you don't see your region on the list, you must set up a TOTP app instead. For more information on supported regions for SMS, see "Countries where SMS authentication is supported."