Recovering your account if you lose your 2FA credentials

In this article

If you lose access to your two-factor authentication credentials, you can use your recovery codes, or another recovery option, to regain access to your account.

Warnings:

- For security reasons, GitHub Enterprise Cloud 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.

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."

Using a two-factor authentication recovery code

Use one of your recovery codes to automatically regain entry into your account. You may have saved your recovery codes to a password manager or your computer's downloads folder. The default filename for recovery codes is `github-recovery-codes.txt`. For more information about recovery codes, see "Configuring two-factor authentication recovery methods."

1. Type your username and password to prompt authentication.

   Warning: If you protect your personal account with two-factor authentication but do not know your password, you will need to start a two-factor authentication recovery request. For more information, see "Request help with two-factor authentication."

2. Under "Having problems?", click **Use a recovery code or request a reset**.
3. Type one of your recovery codes, then click **Verify**.

Authenticating with a passkey

If you have added a passkey to your account, you can use your passkey to automatically regain access to your account. Passkeys satisfy both password and 2FA requirements, so you don't need to know your password in order to recover your account. For more information, see "About passkeys."

Authenticating with a security key

If you configured two-factor authentication using a security key, you can use your security key as a secondary authentication method to automatically regain access to your account. For more information, see "Configuring two-factor authentication."

Authenticating with a fallback number

> **Note:** Configuring a fallback SMS number in addition to your primary SMS number is no longer supported. Instead, we strongly recommend registering multiple authentication methods.

If you lose access to your preferred TOTP app or phone number, you can provide a two-factor authentication code sent to your fallback number to automatically regain access to your account.

Authenticating with a verified device, SSH token, or personal access token

If you know your password for GitHub.com but don't have the two-factor authentication credentials or your two-factor authentication recovery codes, you can have a one-time password sent to your verified email address to begin the verification process and regain access to your account.

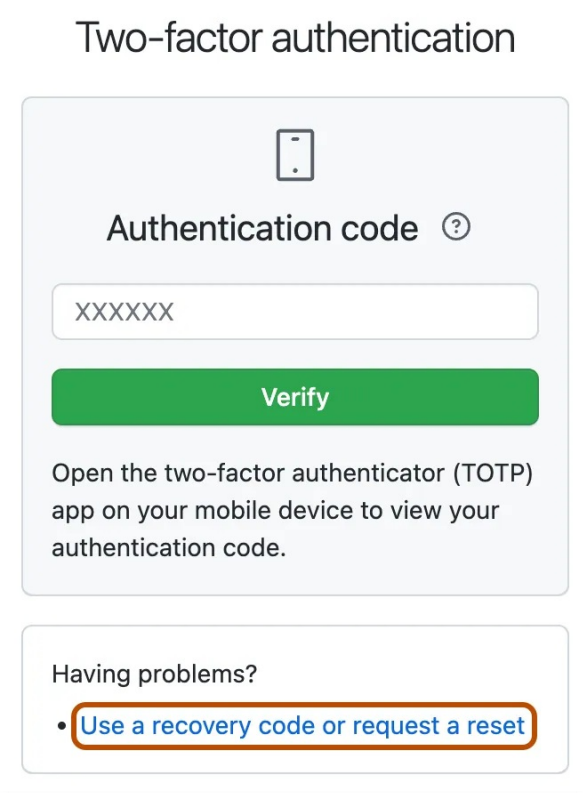
> **Note**: For security reasons, regaining access to your account by authenticating with a one-time password can take up to three business days. GitHub will not review additional requests submitted during this time.

You can use your two-factor authentication credentials or two-factor authentication recovery codes to regain access to your account anytime during the 3-5 day waiting period.

1. Type your username and password to prompt authentication.

   > **Warning**: If you protect your personal account with two-factor authentication but do not know your password, you will need to start a two-factor authentication recovery request. For more information, see "Request help with two-factor authentication."

2. Under "Having problems?", click **Use a recovery code or request a reset**.



3. Under "Locked out?", click **Recover your account or unlink an email address**.
4. Click **I understand, get started** to request a reset of your authentication settings.
5. Click **Send one-time password** to send a one-time password to all eligible addresses associated with your account. Only verified emails are eligible for account recovery. If you've restricted password resets to your primary and/or backup addresses, these addresses are the only addresses eligible for account recovery.
6. Under "One-time password", type the temporary password from the recovery email GitHub sent, then click **Verify email address**.
7. Choose a recovery verification factor.
    - If you've used your current device to log into this account before and would like to use the device for verification, click **Verify with this device**. Device verification is recorded with cookies, and won't be available if your browser deletes cookies regularly.
    - If you've previously set up an SSH key on this account and would like to use the SSH key for verification, click **SSH key**.
    - If you've previously set up a personal access token and would like to use the personal access token for verification, click **Personal access token**.
8. A member of GitHub Support will review your request and email you within three business days. If your request is approved, you'll receive a link to complete your account recovery process. If your request is denied, the email will include a way to contact support with any additional questions.

Requesting help with two-factor authentication

If you have forgotten your password and you've lost access to your two-factor authentication credentials, you can start account recovery to regain access to your account. You'll need to verify your identity using a recovery authentication factor, such

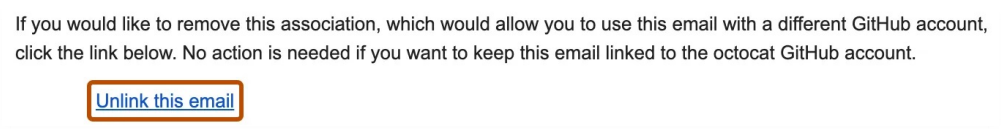
as an SSH key or previously verified device. If no recovery methods are available, you can choose to unlink your email address from your account.

1. Click **Forgot password?**.
2. Enter a primary or backup email address associated with your account on GitHub.com, then click **Send password reset email.**
3. Check your email for a link to reset your password. You must click on this link within three hours of receiving the email. If you don't see an email from us, make sure to check your spam folder.
4. Click on the link in the email, then under "Having problems?", click **Start a 2FA recovery request**.
5. To complete your recovery request, you'll need to verify an alternative authentication factor. Choose a recovery verification factor.
    - If you've used your current device to log into this account before and would like to use the device for verification, click **Verify with this device**. Device verification is recorded with cookies, and won't be available if your browser deletes cookies regularly.
    - If you've previously set up an SSH key on this account and would like to use the SSH key for verification, click **SSH key**.
    - If you've previously set up a personal access token and would like to use the personal access token for verification, click **Personal access token**.
6. A member of GitHub Support will review your request and email you within three business days. If your request is approved, you'll receive a link to complete your account recovery process. If your request is denied, the email will include a way to contact support with any additional questions.

Unlinking your email address

Alternatively, if no recovery methods are available, you can choose to unlink your email address from your account. The email address is then available for you to link it to a new or existing account, maintaining your commit history. For more information, see "Unlinking your email address from a locked account."

1. To begin unlinking an email address from the locked account, click **Start unlinking email**.
2. On the "Unlink Email" screen, click **Continue**.
3. In the inbox of the email account you want to unlink, open the email with the subject "[GitHub] Unlink this email."
    - Optionally, to unlink multiple email accounts, in the inbox of each account you want to unlink, open the email with the subject "[GitHub] Unlink this email," then complete the following steps.
4. In the email, click **Unlink this email**.



5. To finish unlinking your email, on GitHub.com, click **Unlink**.
6. Optionally, to create a new account and link your newly unlinked email, click **Create a new account**.

Further reading

- "Configuring two-factor authentication recovery methods"