Configuring two-factor authentication recovery methods

In this article

You can set up a variety of recovery methods to access your account if you lose your two-factor authentication credentials.

In addition to securely storing your two-factor authentication (2FA) recovery codes, we strongly recommend configuring two or more authentication methods to avoid losing access to your account. For more information, see "Configuring two-factor authentication."

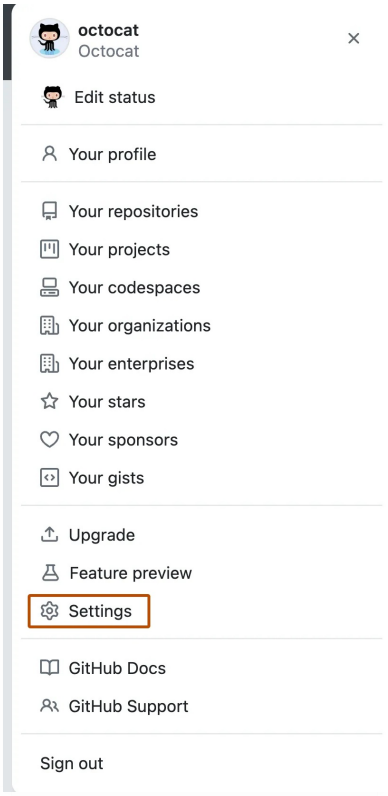
Downloading your two-factor authentication recovery codes

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 Enterprise Server using your recovery codes. You can also download your recovery codes at any point after enabling two-factor authentication.

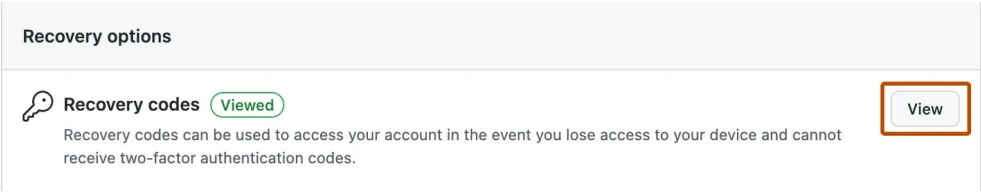
To keep your account secure, don't share or distribute your recovery codes. We recommend saving them with a secure password manager.

If you generate new recovery codes or disable and re-enable 2FA, the recovery codes in your security settings automatically update. Reconfiguring your 2FA settings without disabling 2FA will not change your recovery codes.

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



2. In the "Access" section of the sidebar, click **Password and authentication**.
3. Next to "Recovery codes," click **View**.

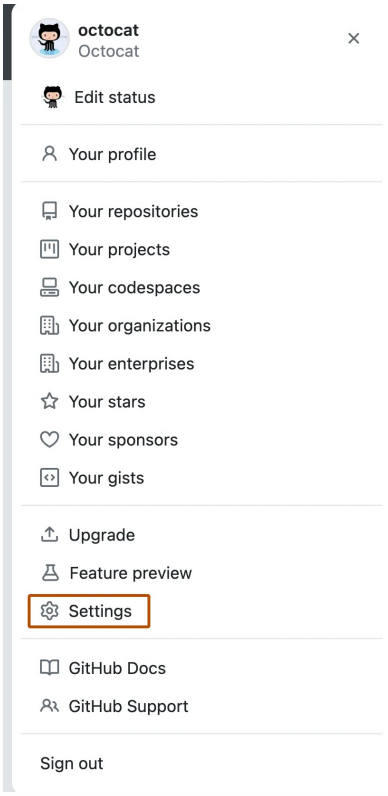


4. Save your recovery codes in a safe place. Your recovery codes can help you get back into your account if you lose access.
    - To save your recovery codes on your device, click **Download**.
    - To save a hard copy of your recovery codes, click **Print**.
    - To copy your recovery codes for storage in a password manager, click **Copy**.

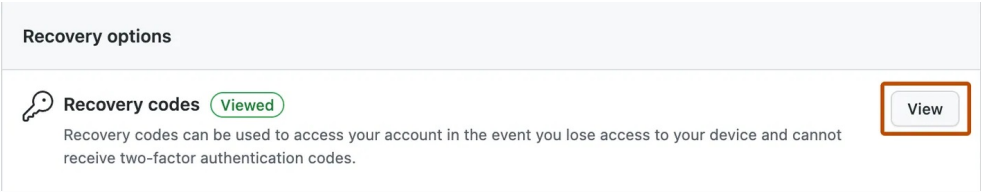
Generating a new set of recovery codes

Once you use a recovery code to regain access to your account, it cannot be reused. If you've used all 16 recovery codes, you can generate another list of codes. Generating a new set of recovery codes will invalidate any codes you previously generated.

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



2. In the "Access" section of the sidebar, click **Password and authentication**.
3. Next to "Recovery codes," click **View**.



4. Under "Generate new recovery codes", click **Generate new recovery codes**.

Configuring backups for your time-based one-time password (TOTP) app

Most TOTP apps support backups. If you lose access to your authentication device, you can use your TOTP app backup to access your authentication method and account credentials on a different authentication device, ensuring continued access to your 2FA-enabled account.

The process of configuring backups is different for each TOTP app. For some examples from popular TOTP apps, see the following documentation:

- 1Password
- Google Authenticator
- Microsoft Authenticator

Further reading

- "About two-factor authentication"
- "Configuring two-factor authentication"

- "Accessing GitHub using two-factor authentication"
- "Recovering your account if you lose your 2FA credentials"