

Managing your passkeys

In this article

- About managing your passkeys
- Adding a passkey to your account
- Upgrading an existing security key to a passkey
- Removing a passkey from your account
- Recovering a passkey
- Further reading

You may be prompted to register a passkey during sign-in, or you can choose to register a new passkey in your account settings. For 2FA users, you can upgrade existing eligible security keys into passkeys.

Who can use this feature

Personal account owners who manage their own credentials can authenticate to GitHub.com using passkeys.

About managing your passkeys

If you are connecting to GitHub.com from an eligible device and browser, GitHub may prompt you to register the device as a passkey during sign-in. You can also add passkeys to your account from your account settings. For more information, see "[Adding a passkey to your account](#)."

If you use two-factor authentication (2FA), GitHub may prompt you to upgrade existing eligible security keys (such as Mac TouchID, or Windows Hello) into passkeys after authenticating to GitHub.com. You can also upgrade eligible security keys from your account settings. For more information, see "[Upgrading an existing security key to a passkey](#)."

For information on how to remove a passkey from your account, see "[Removing a passkey from your account](#)."

Adding a passkey to your account

- 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 Under "Passkeys", click **Add a passkey**.
- 4 If prompted, authenticate with your password, or use another existing authentication method.
- 5 Under "Configure passwordless authentication", review the prompt, then click **Add passkey**.
- 6 At the prompt, follow the steps outlined by the passkey provider.
- 7 On the next page, review the information confirming that a passkey was successfully registered, then click **Done**.

Upgrading an existing security key to a passkey [🔗](#)


Notes:

- Platform support for upgrading security keys is inconsistent, so if you're seeing failures from your operating system or browser when trying to register an existing credential, we suggest that you remove and re-register the security key.
- If you have used a security key recently and it's eligible for an upgrade, an upgrade button will be shown next to the security key in the settings menu. You can use the button to trigger the upgrade flow. You can also attempt to upgrade other keys by registering them as a passkey, even if the upgrade button isn't shown.

Before starting the upgrade procedure, make sure that you are using the device that's linked to the existing security key. Then, when you click **Add a passkey** in your account settings, GitHub will automatically bump you into the "Upgrade to a passkey" flow.

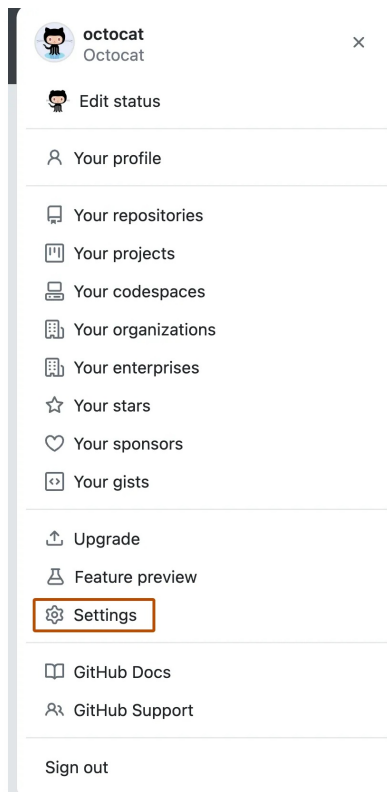
- 1 In the upper-right corner of any page, click your profile photo, then click **Settings**.



- 2 In the "Access" section of the sidebar, click  **Password and authentication**.
- 3 Under "Passkeys", click **Add a passkey**.
- 4 If prompted, authenticate with your password, or use another existing authentication method.
- 5 Under "Configure passwordless authentication", under "Upgrade your security key registration to a passkey", review the information that confirms the name of the security key to be upgraded, then click **Upgrade to passkey**.
- 6 At the prompt, follow the steps outlined by the passkey provider.
- 7 On the next page, review the information confirming that a passkey was successfully registered, then click **Done**.

Removing a passkey from your account

- 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 To the right of the passkey that you want to remove, click .
- 4 Review the information in the "Delete confirmation" pop-up window, then click **Delete**.

Recovering a passkey

Many passkeys support syncing, where your passkey is backed up by the provider's account system (iCloud, Google account, password manager, etc.). If you ever lose your device, you can recover your synced passkeys by signing in to your passkey provider.

In some cases, your passkey may be "device-bound", which means the passkey cannot be synced and is not backed up to the cloud. For example, you can register FIDO2 hardware security keys (such as a YubiKey) as a passkey, but that passkey will not be synced. If your passkey is device-bound, and you lose or wipe the device, the passkey cannot be recovered. If you are only using device-bound passkeys, it is a best practice to register passkeys on at least two different devices, in case you lose access to one.

You can see which of your passkeys are synced, and which are device-bound, under "Passkeys" in your account security settings. Synced passkeys will include a blue Synced label next to their name.

Further reading

- [About passkeys](#)
- [Signing in with a passkey](#)

Legal

