About passkeys

In this article

Passkeys allow you to sign in safely and easily, without requiring a password and two-factor authentication.

> **Who can use this feature**
> Personal account owners who manage their own credentials can authenticate to GitHub.com using passkeys.

About passkeys

Passkeys allow you to sign in securely to GitHub.com, without having to input your password. If you use two-factor authentication (2FA), passkeys satisfy both password and 2FA requirements, so you can complete your sign in with a single step. You can also use passkeys for sudo mode and resetting your password.

Passkeys are pairs of cryptographic keys (a public key and a private key) that are stored by an authenticator you control. The authenticator can prove that a user is present and is authorized to use the passkey. Authenticators prove authorization with a PIN, passcode, biometric, or device password, depending on the authenticator's capabilities and configuration. Authenticators come in many forms, such as an iPhone or Android device, Windows Hello, a FIDO2 hardware security key, or a password manager.

When you sign in to GitHub.com using a passkey, your authenticator uses public key cryptography to prove your identity to GitHub without ever sending the passkey. Passkeys are bound to a website domain, like `GitHub.com`, and require a secure connection, meaning that the web browser will refuse to authenticate to a lookalike phishing website. These properties make passkeys highly phishing-resistant, and much harder to attack than SMS or TOTP 2FA, which can be phished.

Cloud-backed passkey services allow passkeys to be synced across devices (such as Apple devices, Android devices, or password managers) so they can be used from more places and are less easily lost. Once you have set up a synced passkey on one device, that passkey is available to use across multiple devices using the same service. For example, if you register a passkey with your iCloud account using your MacBook's Touch ID, you can then use that passkey with your face, fingerprint, PIN, or device password interchangeably across multiple devices tied to the same iCloud account.

For more information about adding a passkey to your account, see "Managing your passkeys."

For 2FA users, if you already have passkey-eligible security keys registered to your account for 2FA, you can upgrade these existing credentials into passkeys in your account settings. When you use an eligible security key to sign in, you'll also be asked if you want to upgrade it to a passkey. For more information, see "Managing your

passkeys."

About authenticators

Some authenticators allow passkeys to be used with nearby devices. For example, perhaps you want to sign in to GitHub.com using a bluetooth-enabled laptop that's not set up with a passkey. If you have registered a passkey on your phone, you might opt to scan a QR code, or trigger a push notification to your phone, in order to complete the sign in securely. For more information, see "Signing in with a passkey."

Other authenticators create device-bound passkeys, meaning they can only be used on a single authenticator. These passkeys cannot be backed up or moved to another authenticator. Some passkey providers may offer device-bound passkeys as an option during passkey creation, while other providers may not offer the choice between device-bound and synced passkeys.

Authenticators can also be portable devices. Passkeys stored on FIDO2 hardware security keys are also "device-bound," but they have the advantage of being portable and can be attached to other devices in a variety of ways (USB, NFC or Bluetooth). On some platform and web browser combinations, FIDO2 security keys may be the only way to use passkeys.

For information on whether your device and operating system support passkeys, see Device support in the Passkeys.dev documentation, and Web Authentication API in the CanIUse documentation.

Feedback

You can share your feedback on passkeys with GitHub. To join the conversation, see "[Feedback] Passkeys for passwordless authentication."

Further reading

- Managing your passkeys
- Signing in with a passkey
- About two-factor authentication