

私のアカウント > ログイン & ロック解除

パスキー-ベータでログイン

ヘルプセンターで表示:

<https://bitwarden.com/help/login-with-passkeys/>

パスキー-ベータでログイン

Note

パスキーでログインする機能は現在ベータ版です。

パスキーは、マスターパスワードとメールアドレスを使用する代わりにBitwardenにログインするために使用できます。Bitwardenにログインするために使用されるパスキーは、ユーザーの確認が必要で、これは生体認証要素やセキュリティキーのようなものを使用してパスキーへのアクセスを正常に確立する必要があることを意味します。

パスキーでログインすると、Bitwardenの二段階ログインがバイパスされますが、保管庫の復号化のためのパスキーでのログイン設定は、PRF対応ブラウザとパスキーの組み合わせのみが使用できます。PRFを使用しないパスキーは、保管庫を復号化するためにログイン後にマスターパスワードを入力する必要があります。

現在、パスキーはBitwardenウェブアプリにログインするために使用でき、他のクライアントアプリケーションへのサポートは将来のリリースで計画されています。

Note

パスキーでのログインは、シングルサインオン認証を必要とするポリシー、信頼できるデバイスでのSSO、またはキーコネクタを使用する組織のメンバーには使用できません。

パスキーを作成する

あなたは一度に最大5つのパスキーでログインすることができます。Bitwardenにログインするためのパスキーを作成するには：

1. ウェブアプリで、ナビゲーションから**設定** → **アカウント**を選択します。
2. 設定メニューから、**セキュリティページ**と**マスターパスワードタブ**を選択してください。
3. パスキーでログインセクションで、**オンにする**を選択するか、既にパスキーを設定している場合は、**新しいパスキー**を選択します。あなたのマスターパスワードを入力するように求められます。

Log in with passkey Off Beta

Use a generated passkey that will automatically log you in without a password. Biometrics, like facial recognition or fingerprint, or another FIDO2 security method will verify your identity. [Learn more about passwordless](#)

Turn on

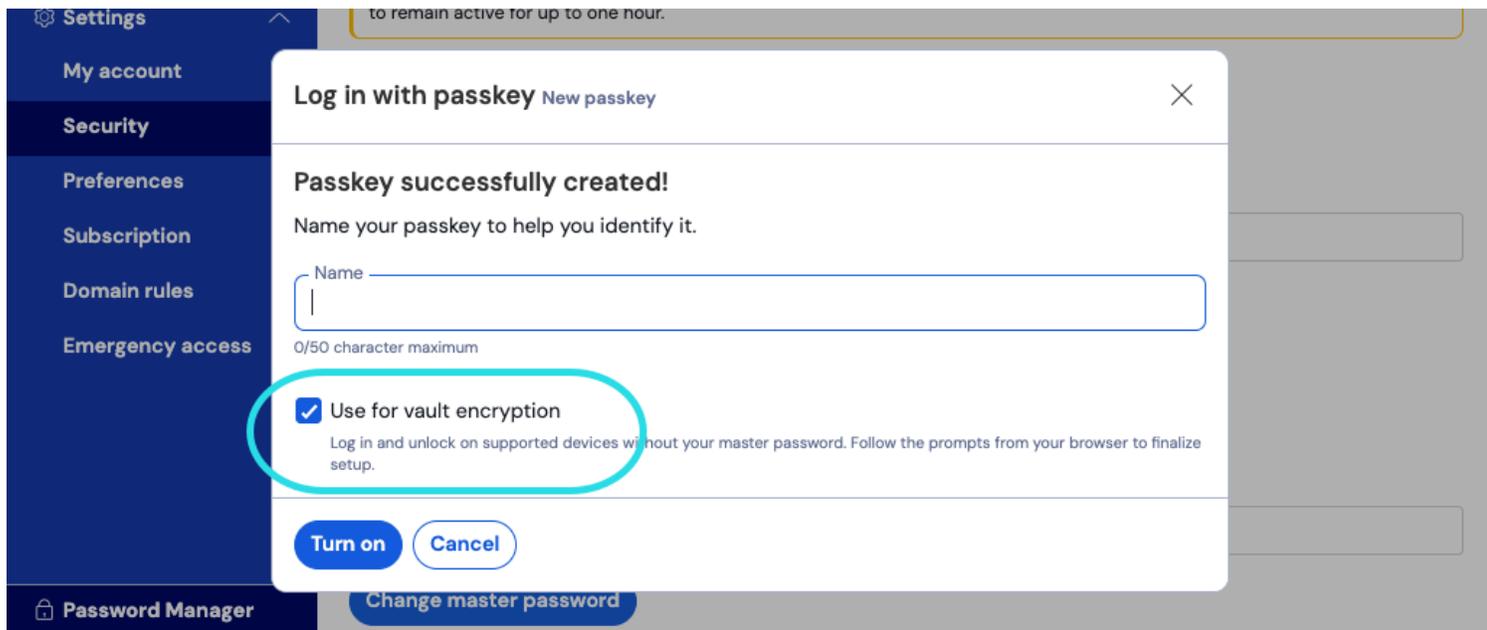
パスキーでのログインをオンにする

4. あなたのブラウザからのプロンプトに従って、FIDO2パスキーを作成してください。生体認証のような要素を使用してユーザー認証を完了するか、PINを作成することができます。

この手順中に、ブラウザが使用するデフォルトの認証をキャンセルする必要があるかもしれません。例えば、Touch IDを優先するmacOSデバイスでハードウェアセキュリティキーを使用したい場合などです。

5. あなたのパスキーに**名前**を付けてください。

6. あなたが保管庫の暗号化と復号化にパスキーを使用したくない場合は、
保管庫の暗号化に使用するチェックボックスのチェックを外してください：



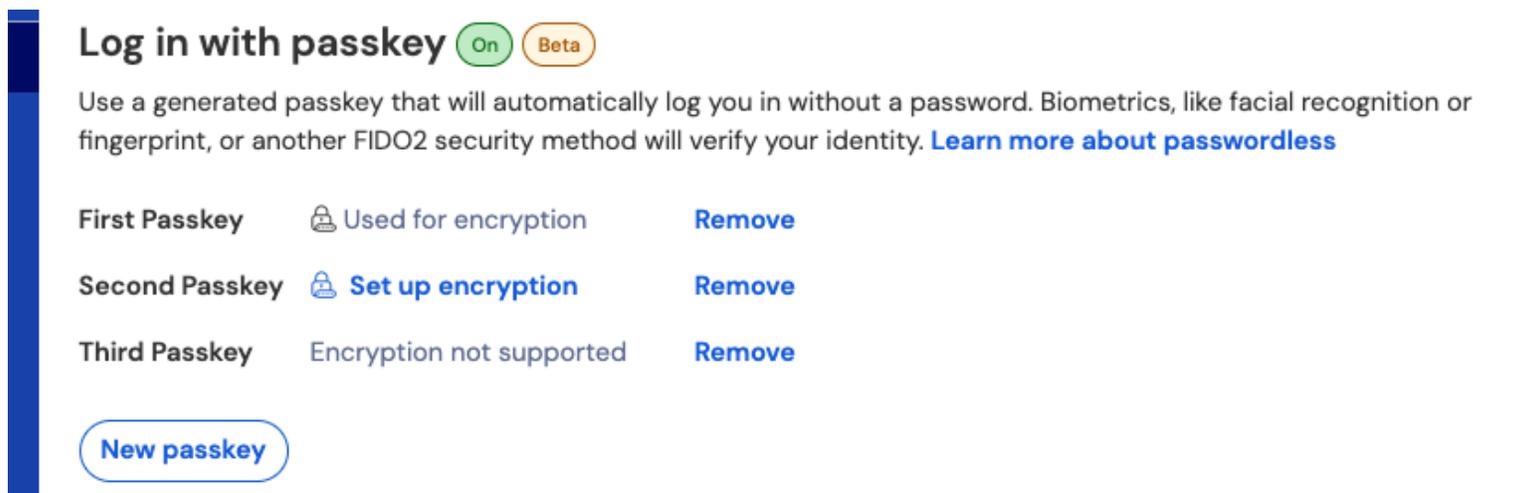
保管庫の暗号化にパスキーを使用する

あなたのパスキーとブラウザがPRF対応の場合にのみ、このオプションが表示されます。 [もっと学ぶ](#)。

7. オンにするを選択します。

暗号化の設定

あなたのパスキーとブラウザは、パスキーを保管庫の暗号化と復号化に使用するために、PRF対応でなければなりません。あなたのパスキーリストは、各パスキーが暗号化に使用されているか、サポートされているが有効化されていないか、またはサポートされていないかを表示します：



パスキーリスト

もし初めてパスキーを設定したときに保管庫の暗号化に使用のチェックボックスをチェックしなかった場合、または例えばその時に使用していたブラウザがPRF対応でなかった場合、このメニューに移動して暗号化の設定ボタンを選択してください。

パスキーを削除する

Bitwardenから既存のパスキーを削除するには、同じ画面上の**削除**ボタンを使用できます。Bitwardenからパスキーを削除しても、あなたのFIDO2認証器に保存されているプライベートキーは削除されませんが、それを使用してBitwardenにログインすることはできなくなります。

あなたのパスキーでログインしてください

あなたのパスキーが作成されたら、それを使用してBitwardenウェブアプリにログインできます：

1. Bitwardenのログイン画面で、通常メールアドレスを入力するところで**パスキーでログイン**を選択してください。
2. あなたのブラウザからのプロンプトに従ってパスキーを読み取り、これによりBitwardenとの認証が行われます。
3. あなたのパスキーが保管庫の暗号化のために設定されている場合、それで終わりです！それ以外の場合は、**マスターパスワード**を入力し、**ロック解除**を選択して保管庫のデータを復号化します。

それはどのように動作するのか

次に、パスキーでログインするメカニズムについて説明します。あなたのパスキーが**暗号化**で設定されているかどうかにより、どのタブが関連しているかが異なります。

⇒暗号化がオンになっているパスキー

パスキーを作成する

パスキーがBitwardenへのログインに登録されたとき：

- 認証器はWebAuthn APIを介して**パスキー公開鍵と秘密鍵のペア**を生成します。このキーペアは、定義上、あなたのパスキーを構成するものです。
- **PRF対称キー**は、WebAuthn APIのPRF拡張機能を介して認証器によって生成されます。このキーは、あなたのパスキーに固有の**内部秘密**とBitwardenが提供する**ソルト**から派生します。
- Bitwardenクライアントによって**PRF公開鍵と秘密鍵のペア**が生成されます。PRF公開鍵はあなたの**アカウント暗号化キー**を暗号化し、クライアントはログインしてロック解除されていることによりそれにアクセスでき、結果として得られる**PRFで暗号化されたアカウント暗号化キー**がサーバーに送信されます。
- **PRFプライベートキー**はPRF対称キー（ステップ2参照）で暗号化され、結果として得られる**PRFで暗号化されたプライベートキー**がサーバーに送信されます。
- あなたのクライアントはデータをBitwardenサーバーにSendし、あなたのアカウントのための新しいパスキー資格レコードを作成します。あなたのパスキーが保管庫の暗号化と復号化のサポートに登録されている場合、この記録には以下が含まれます：
 - パスキー名
 - パスキー公開鍵
 - PRF公開鍵
 - PRF-暗号化されたアカウント暗号化キー
 - PRF-暗号化されたプライベートキー

あなたのパスキー秘密鍵は、認証を達成するために必要であり、暗号化された形式でのみクライアントを離れます。

あなたのパスキーでログインしてください

パスキーがログインに使用され、特に、保管庫のデータを復号化するために使用される場合：

- WebAuthn APIの公開鍵暗号を使用して、あなたの認証リクエストが主張され、確認されます。
- あなたのPRF-暗号化されたアカウントの暗号化キーとPRF-暗号化されたプライベートキーがサーバーからあなたのクライアントに送信されます。
- Bitwardenから提供される同じソルトと、あなたのパスキーに固有の**内部秘密**を使用して、**PRF対称キー**がローカルで再作成されます。
- PRF対称キーは、あなたのPRFで暗号化された**プライベートキー**を復号化するために使用され、あなたのPRF**プライベートキー**が得られます。
- PRF**プライベートキー**は、PRFで暗号化された**アカウント暗号化キー**を復号化するために使用され、結果として**アカウント暗号化キー**が得られます。あなたのアカウントの暗号化キーは、あなたの保管庫のデータを復号化するために使用されます。

⇒暗号化をオフにしたパスキー

パスキーを作成する

パスキーがBitwardenへのログインに登録されたとき：

1. **パスキー公開鍵と秘密鍵のペア**が作成されます。このキーペアは、定義上、あなたのパスキーを構成するものです。
2. あなたのクライアントはデータをBitwardenサーバーにSendし、あなたのアカウントの新しいパスキー資格レコードを作成します。あなたのパスキーが保管庫の暗号化および復号化のサポートに登録されていない場合、このレコードには以下が含まれます：
 - パスキーの名前
 - パスキーの公開鍵

あなたのパスキーのプライベートキーは、認証を達成するために必要であり、暗号化された形式でのみクライアントを離れます。

あなたのパスキーでログインしてください

パスキーがログインに使用されると、あなたの認証リクエストはWebAuthn API公開鍵暗号を使用して主張され、確認されます。その後、マスターパスワードを使用して保管庫を復号化する必要があります。

あなたの暗号化キーをロテートする

アカウント暗号化キーのロテートは、保管庫暗号化に使用するために設定されたパスキーの暗号化および復号化機能を無効にします。そのパスキーがBitwardenにログインする際の認証に使用される能力は、アカウントの暗号化キーをロテートするときに**影響を受けません**。