

私のアカウント > ログイン & ロック解除 > MORE LOG IN OPTIONS

デバイスでログイン

ヘルプセンターで表示:

<https://bitwarden.com/help/log-in-with-device/>

デバイスでログイン

あなたはマスターパスワードの代わりにセカンダリデバイスを使用してBitwardenにログインできることを知っていましたか？デバイスでログインすることは、認証へのパスワードレスのアプローチであり、現在ログインしている特定のデバイスに認証リクエストを送信することでマスターパスワードを入力する必要をなくします。[私たちのゼロ知識暗号化実装について学ぶ](#)。

デバイスでのログインは、ウェブ保管庫、ブラウザ拡張機能、デスクトップアプリ、モバイルアプリで開始できます。これらのアプリから発行されたリクエストは、モバイルアプリとデスクトップアプリで承認できます。

デバイスでログインする準備をしてください

デバイスでログインを設定するには：

- 通常通りに初期化アプリ（ウェブ保管庫、ブラウザ拡張機能、デスクトップ、またはモバイルアプリ）にログインして、少なくとも一度Bitwardenがあなたのデバイスを認識できるようにしてください。

① Note

シークレットモードまたはプライベートブラウジングを使用すると、Bitwardenはあなたのブラウザを登録できないため、プライベートブラウザウィンドウのデバイスでログインすることはできません。

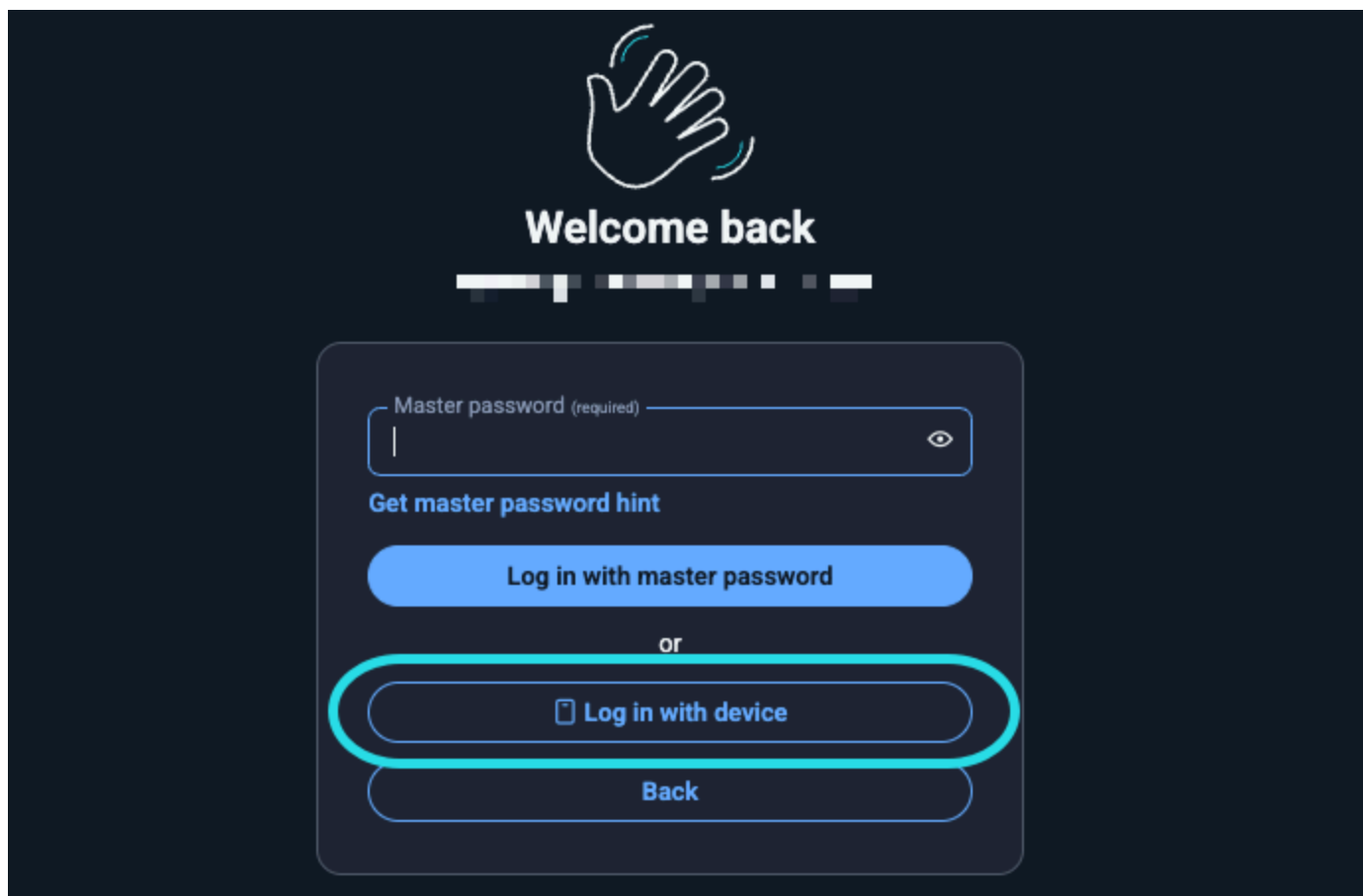
- 認証アプリ（モバイルアプリまたはデスクトップアプリ）で認識されたアカウントを持っている。アカウントを認識するには、そのデバイスにいつでも成功裏にログオンしたことが必要です。
- 承認アプリを開き、 **設定**を開き、**アカウントのセキュリティ**または**セキュリティセクション**で、**ログインリクエストの承認**をオンにします。

① Note

エンタープライズ組織のメンバーとして、[SSOポリシーが必要](#)である場合、**デバイスでログインオプション**を使用することはできません。あなたは代わりに[SSOを使用してログイン](#)する必要があります。

デバイスでログインする

起動アプリのログイン画面で、メールアドレスを入力し、**続ける**を選択します。次に、**デバイスでログインオプション**を選択します：



Log in with a device

デバイスでログインを使用すると、現在ログインしていて、オプションを有効にしたモバイルアプリやデスクトップアプリに認証リクエストが送信され、承認が求められます。初期化クライアントと承認クライアントのフィンガープリントフレーズを比較し、一致した場合は、承認デバイスでログインを確認を選択します。これはあなたのアカウントのフィンガープリントフレーズとは異なるユニークなフィンガープリントであることにメモしてください。

リクエストは承認または拒否されない場合、15分後に期限切れになります。ログインリクエストを受け取っていない、またはF-Droidを使用している場合は、モバイルアプリから保管庫を手動で同期してみてください。

Note

デバイスでログインオプションを使用しても、現在有効な二段階ログイン方法を使用する必要があります。

それはどのように動作するか

デバイスでログインが開始されたとき：

1. 開始クライアントは、アカウントのメールアドレス、ユニークな認証リクエスト公開キー^a、およびアクセスコードを含むリクエストをPOSTし、それをBitwardenデータベースの認証リクエストテーブルに送信します。

2. 登録されたデバイス、つまりログインしていてBitwardenデータベースに**デバイス固有のGUID**が保存されているモバイルアプリやデスクトップアプリは、リクエストを提供されます。
3. リクエストが承認されると、承認するクライアントは、リクエストに含まれるauth-request公開キーを使用して、アカウントのマスターキーとマスターパスワードハッシュを暗号化します。
4. 承認されたクライアントは、暗号化されたマスターキーと暗号化されたマスターパスワードハッシュを認証リクエストレコードにPUTし、リクエストが完了したとマークします。
5. 初期化するクライアントは、暗号化されたマスターキーと暗号化されたマスターパスワードハッシュをGETします。
6. 初期化するクライアントは、その後、auth-requestのプライベートキーを使用してマスターキーとマスターパスワードハッシュを**ローカル**で復号化します。
7. 初期化クライアントは、アクセスコードと完了した認証リクエストを使用して、ユーザーをBitwarden IDサービスで認証します。

- Auth-request公開鍵と秘密鍵は、パスワードレスのログインリクエストごとに一意に生成され、リクエストが存在する限りのみ存在します。リクエストは承認または拒否されない場合、15分ごとに期限切れとなりデータベースから削除されます。