認証器を介した二段階ログイン

認証器を介した二段階ログイン

サードパーティーの認証アプリを使用した二段階ログイン（例えば、2FAS、Ravio、またはAegis）は、
すべてのBitwardenユーザーに無料で利用可能です。

> **Note**
>
> Google Authenticatorなどの認証アプリは、新しいモバイルデバイスへの簡単な移行のために、
> 自動的にあなたの2FAトークンをバックアップしません。これらの場合、
> 各トークンの認証リカバリーコードを手動で保存する必要があります。
>
> 他のアプリ、例えばAuthyは、デバイス間でのバックアップと同期をサポートしています。これらの場合、
> 強力なバックアップパスワードを設定し、それをあなたのBitwarden保管庫に記録しておくことを確認してください。

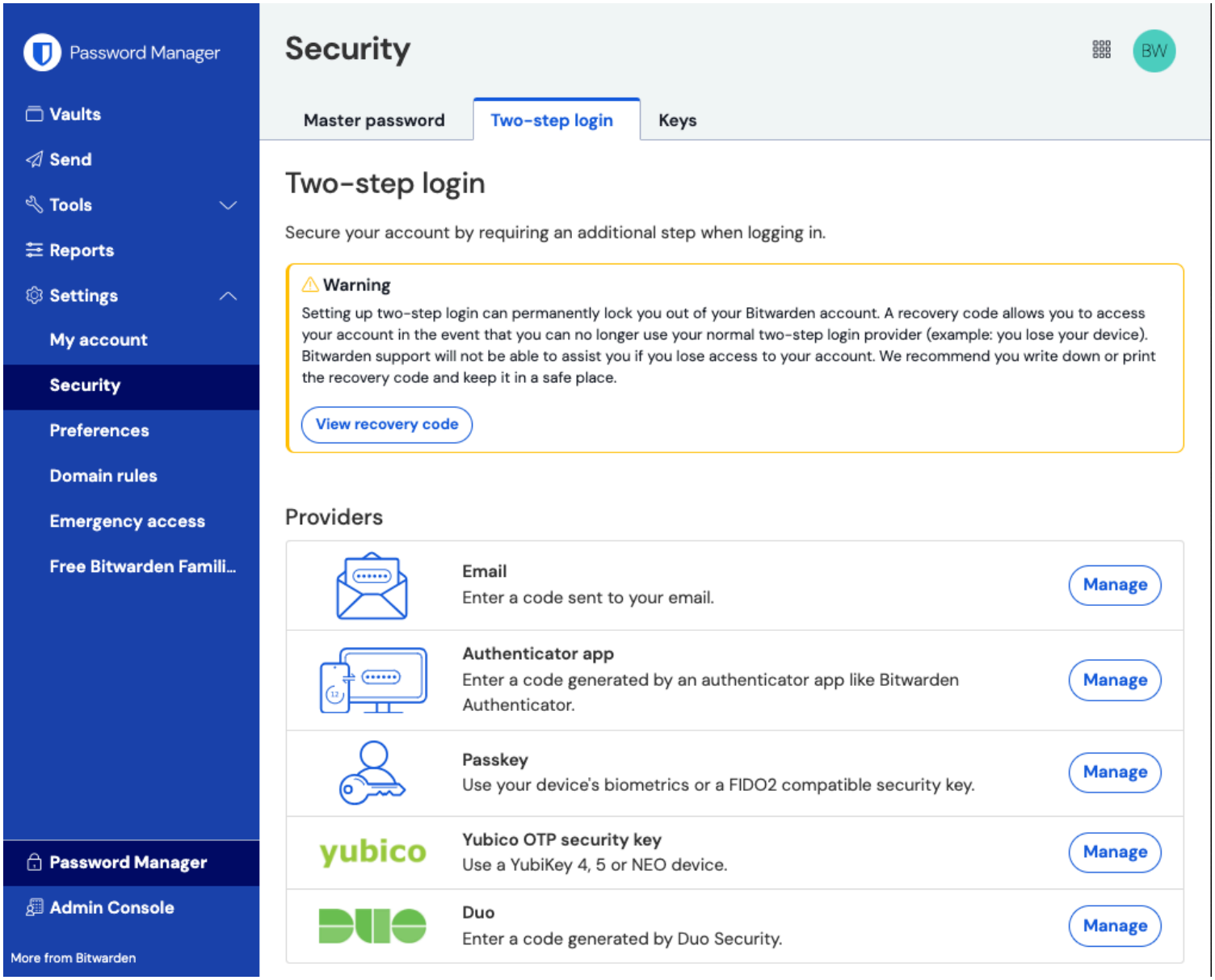
認証器を設定する

認証アプリを使用して二段階ログインを有効にするには：

> **Warning**
>
> **2ステップログインデバイスへのアクセスを失うと、リカバリーコードを安全な場所に書き込み保存するか、
> 代替の2ステップログイン方法を有効にして利用可能にしていない限り、永久に保管庫からロックアウトされる可能性があります。**
>
> リカバリーコードを取得してください、任意の方法を有効にした直後の**二段階ログイン**画面から。

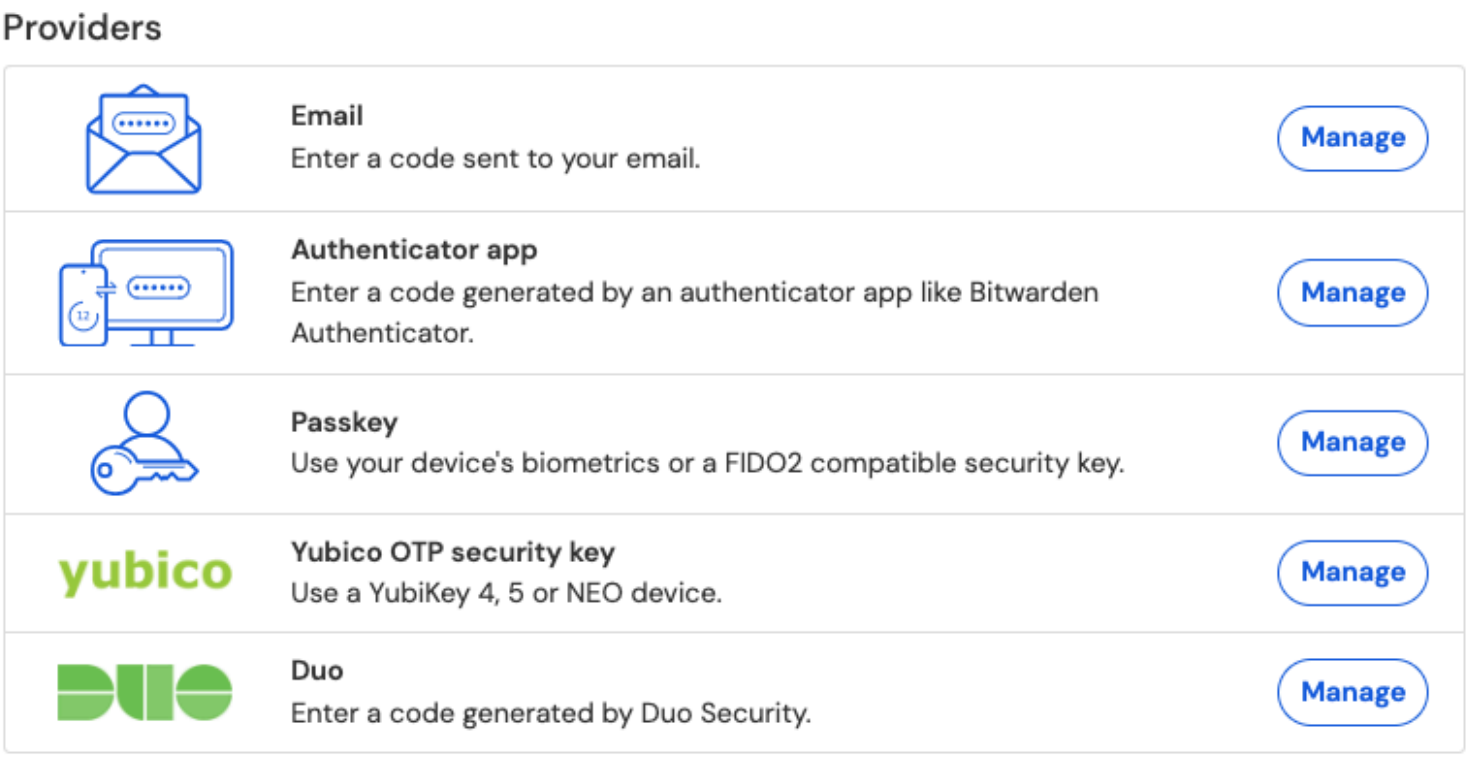
1. Bitwardenウェブアプリにログインしてください。

2. ナビゲーションから**設定** → **セキュリティ** → **二段階ログイン**を選択します。



2段階認証

3. **認証アプリ**のオプションを探し、**管理**ボタンを選択します:



管理ボタンを選択してください

続行するにはマスターパスワードを入力するように求められます。

4. あなたの選択した認証アプリでQRコードをスキャンしてください。

   まだモバイルデバイスに認証アプリがない場合は、ダウンロードしてQRコードをスキャンしてください。私たちはAuthyをお勧めします。

5. 一度スキャンすると、あなたの認証アプリは6桁の認証コードを返します。ウェブ保管庫のダイアログボックスにコードを入力し、**有効にする**ボタンを選択します。

   緑色の有効メッセージは、認証器を介した二段階ログインが有効になったことを示します。

6. **閉じる**ボタンを選択し、**認証アプリ**オプションが有効になっていることを確認します。これは、緑色のチェックボックス（✓）で示されます。

> **Note**
> 私たちは、何かが誤って設定されていた場合に備えて、
> 二段階ログインをテストする前にアクティブなウェブ保管庫タブを開いておくことをお勧めします。
> それが動作していることを確認したら、Bitwardenのすべてのアプリからログアウトして、
> 各アプリで二段階ログインを必要とするようにします。最終的には自動的にログアウトされます。

複数のデバイスでのセットアップ

あなたのBitwardenアカウントが複数のデバイスで使用されている場合、
2FAは追加の互換性のあるデバイスで動作するように有効にすることができます。追加のデバイスに2FAを追加するには、
上記の手順に従ってQRコードを追加のデバイスでスキャンするか、QRキーを手動で入力して追加のデバイスで2FAを有効にします。

認証器を使用してください

以下は、**認証アプリ**があなたの優先度が最も高い有効な方法であると仮定しています。認証器を使用して保管庫にアクセスするには：

1. あなたのBitwardenの保管庫にログインし、メールアドレスとマスターパスワードを入力してください。

   あなたの認証アプリからの6桁の認証コードを入力するように求められます。

2. あなたの認証アプリを開き、Bitwarden保管庫の6桁の認証コードを見つけてください。
   このコードを保管庫のログイン画面に入力してください。通常、認証コードは30秒ごとに変わります。

   > **Tip**
   >
   > **私を覚えておいてください**のボックスをチェックして、30日間デバイスを記憶します。あなたのデバイスを記憶すると、二段階ログインのステップを完了する必要がなくなります。

3. ログインを完了するには、**続ける**を選択してください。

ログインした後、保管庫を**ロック解除**するために二段階ログインの手順を完了する必要はありません。
ログアウトとロックの動作を設定するためのヘルプは、保管庫タイムアウトオプションを参照してください。