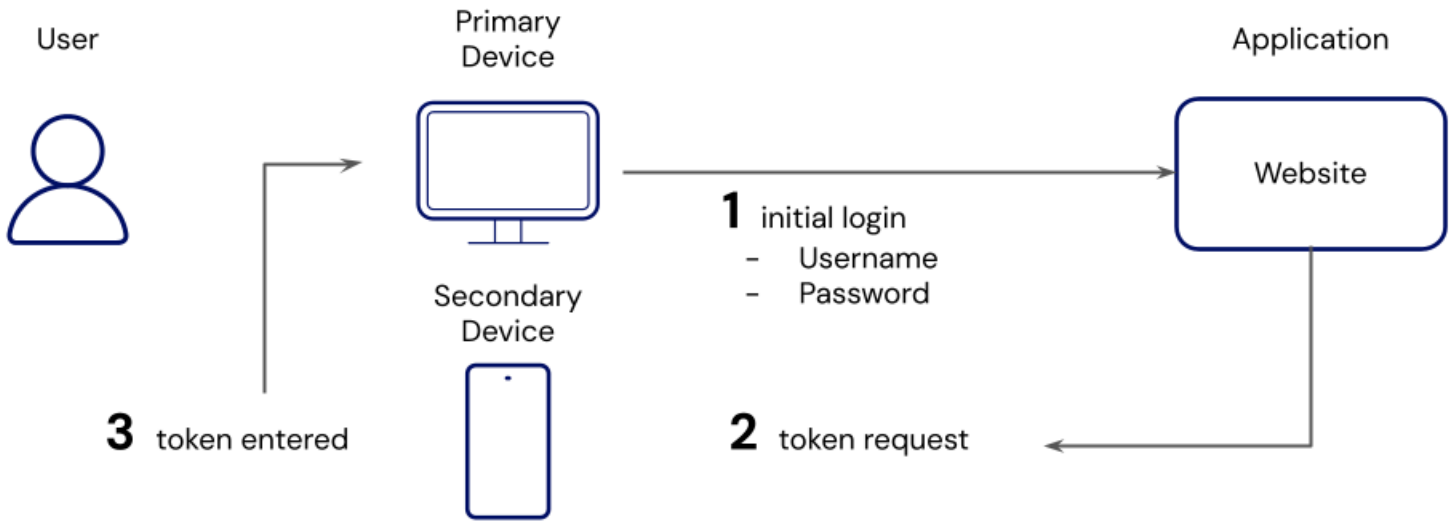
私のアカウント > 2段階ログイン

フィールドガイド–ツーステップ–ログイン

フィールドガイド–ツーステップ–ログイン

二段階ログイン（または二要素認証、2FAとも呼ばれる）は、
ウェブページやアプリがあなたの敏感なデータを保護するために一般的に使用されるセキュリティ技術です。
2ステップログインを使用するウェブページでは、ユーザー名とパスワードの他に、通常は別のデバイスから取得した追加の「トークン」（認証コードまたはワンタイムパスワード（OTP）とも呼ばれます）を入力してIDを確認する必要があります。

あなたのセカンダリデバイスからのトークンへの物理的なアクセスがなければ、
悪意のある行為者はあなたのユーザー名とパスワードを発見したとしてもウェブページにアクセスすることはできません。



基本的な二段階ログインフロー

一般的に、敏感なデータ（例えば、オンライン銀行のアカウント）を持つウェブページやアプリは、
ログイン画面以外であなたのIDを確認しようとします：

- ファイルにあるモバイルデバイスにSMS / テキストメッセージでトークンを送信します。
- モバイルデバイス上の認証アプリ（例えば、Authy）によって生成されたトークンを求める。
- 物理的なセキュリティキー（例えば、YubiKey）からトークンを探しています。

二段階ログインはどのように使用すればよいですか？

セキュリティはしばしば保護と便利さの間のトレードオフを伴うため、最終的にはあなた次第です！一般的に、
2ステップログインを使用する最も重要な2つの方法は次のとおりです：

1. Bitwardenを保護する

Bitwardenにログインするたびに、マスターパスワードを入力するだけでなく、二次手段を要求することで、すべての保管庫データを保護します。

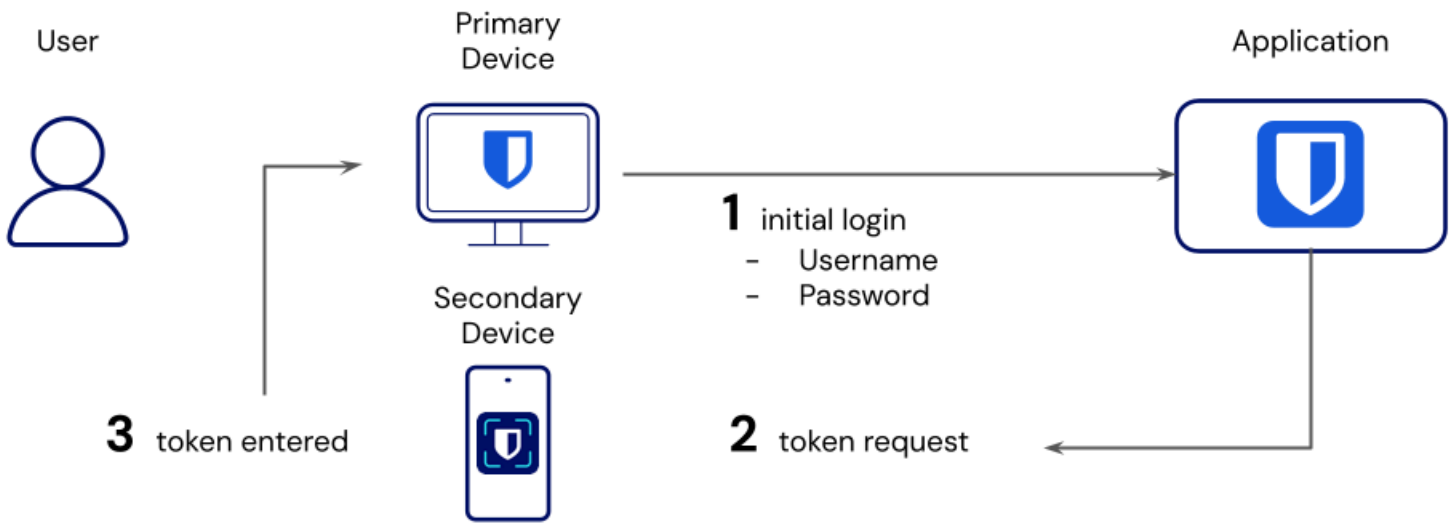
2. 重要なウェブページを保護する

一時的なワンタイムパスワード（TOTP）を要求することで、個々のウェブページをログイン時に保護します。BitwardenでTOTPを保存し、生成することができます。

Bitwardenのセキュリティ

あなたのパスワードマネージャーはすべてのログインを保存しているので、二段階ログインでそれを保護することを強くお勧めします。これにより、マスターパスワードが発見されたとしても、悪意のある行為者があなたの保管庫にアクセスするのを防ぎ、すべてのログインを保護します。

2ステップログインを有効にすると、主なログイン方法（マスターパスワード）に加えて、毎回ログインするたびに二次ステップを完了する必要があります。あなたの保管庫をロック解除するために二次ステップを完了する必要はありません、ログインするだけです。



Bitwardenにアクセスするための二段階ログイン

Bitwardenは、以下を含むいくつかの二段階ログイン方法を無料で提供しています：

- FIDO（いずれかのFIDO2 WebAuthn認定キー）
- 認証アプリを通じて（例えば、2FAS、Ravio、またはAegis）
- メールアドレス経由

プレミアムユーザー向けに、Bitwardenはいくつかの高度な二段階ログイン方法を提供しています：

- DuoセキュリティとDuo Push、SMS、電話、セキュリティキー
- YubiKey（任意の4/5シリーズデバイスまたはYubiKey NEO/NFC）

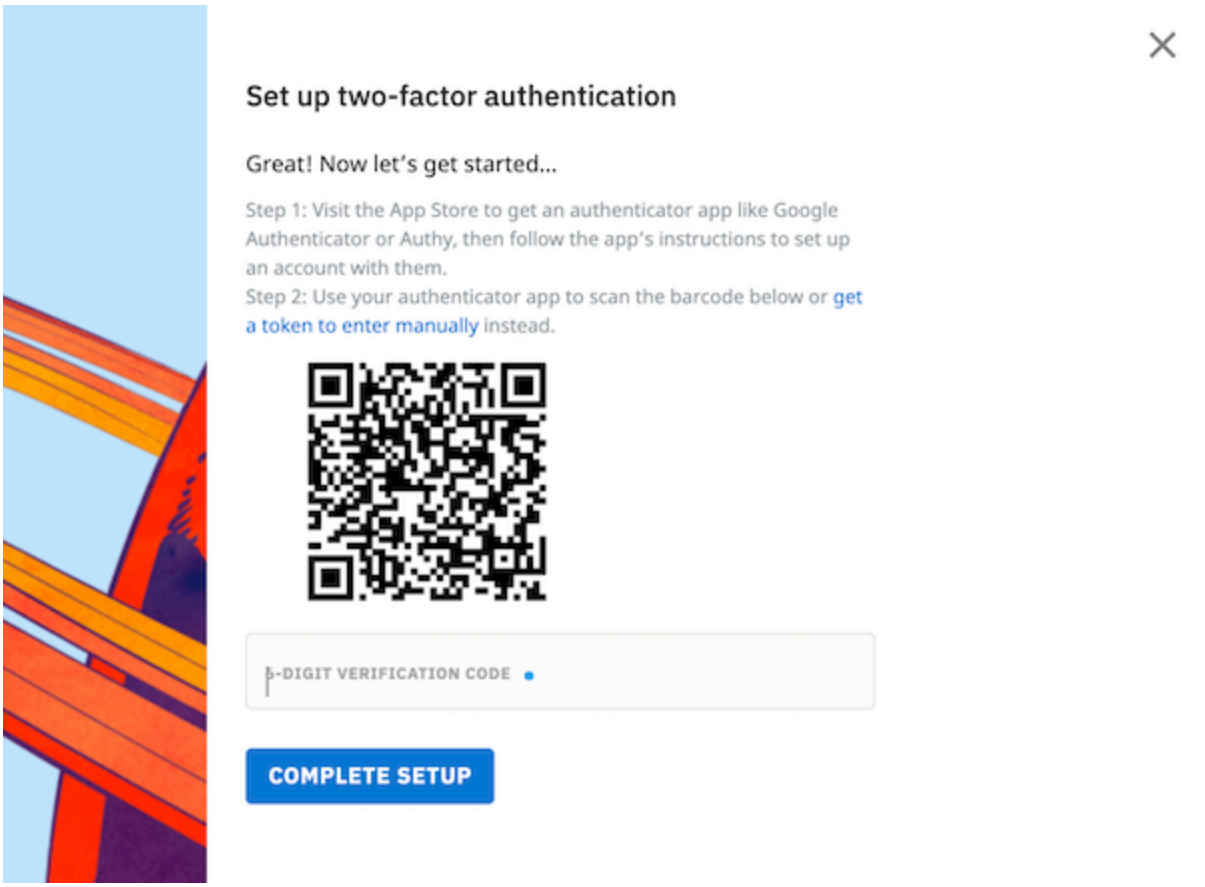
あなたの選択肢についてもっと学ぶ または、私たちの **設定ガイド**を使用して任意の方法の設定をヘルプします。

> **Note**
> Bitwardenは、SIMハイジャックを含む脆弱性のため、SMS 2FAをサポートしていません。他のアカウントに対してSMS 2FAを推奨していません、それが唯一利用可能な方法である場合を除きます。何もない状態よりはどんな2FAでも推奨されますが、SMS 2FAよりもほとんどの代替手段の方が安全です。

重要なウェブページのセキュリティ

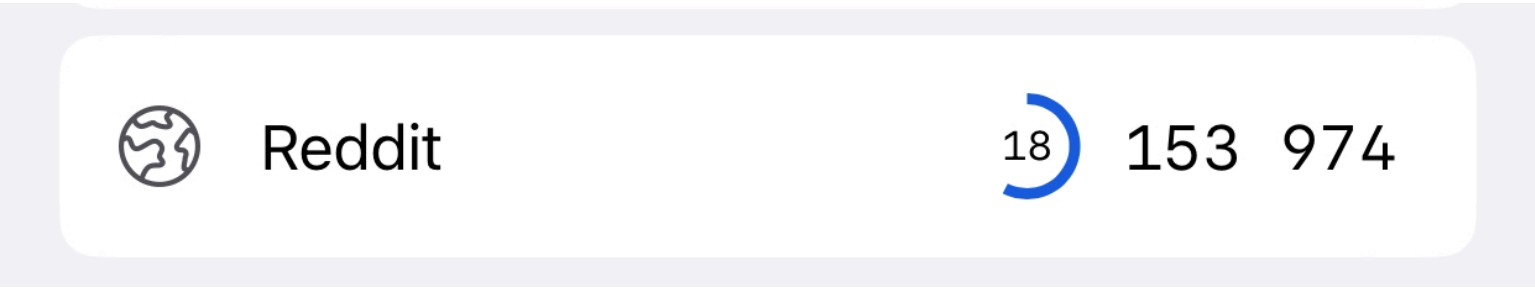
他の多くのウェブページやアプリは二段階ログインのオプションを持っており、これは特に敏感な情報（例えば、クレジットカードや銀行アカウントの数値）を保存するウェブページによく見られます。
ほとんどのウェブページの二段階ログインオプションは、**設定**、**セキュリティ**、または**プライバシー**メニューに位置しています。

2ステップログインを有効にすると、通常はこのRedditの例のようなQRコードが開きます：



2FA QRコード

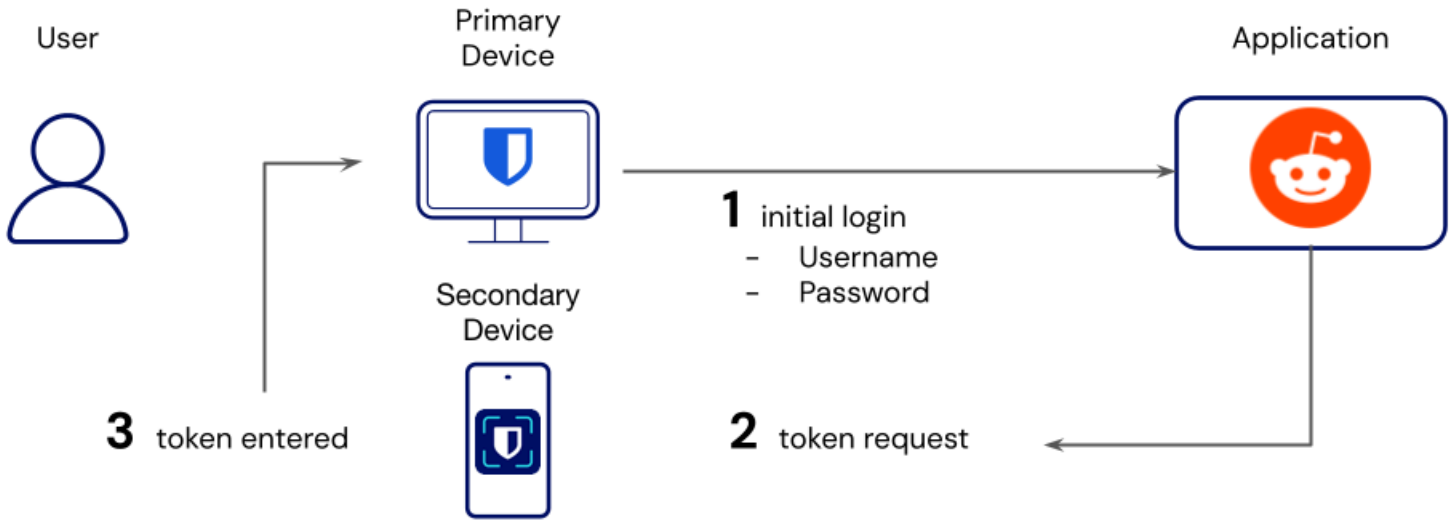
このコードを認証アプリでスキャンすると、アプリはロテートする6桁のトークンを生成できるようになり、これを使用してIDを確認できます。例えば、Authyによって生成されたこのようなものです：



TOTP トークン

Authyを使用してください

Authyを使用してRedditの二段階ログインを設定するには、**アカウント追加**ボタンをタップし、
ウェブページまたはアプリが表示するQRコードをスキャンします。QRコードをスキャンすると、6桁のトークンが生成されます。
このコードを**認証コード**の入力ボックスに入力して設定を完了してください。



Authyを使用した二段階ログイン

通常、リカバリーコードをダウンロードするオプションが提供されます。リカバリーコードのダウンロードは、
Authyがインストールされているデバイスを失っても、二段階ログインのトークンへのアクセスを失わないようにするために重要です。

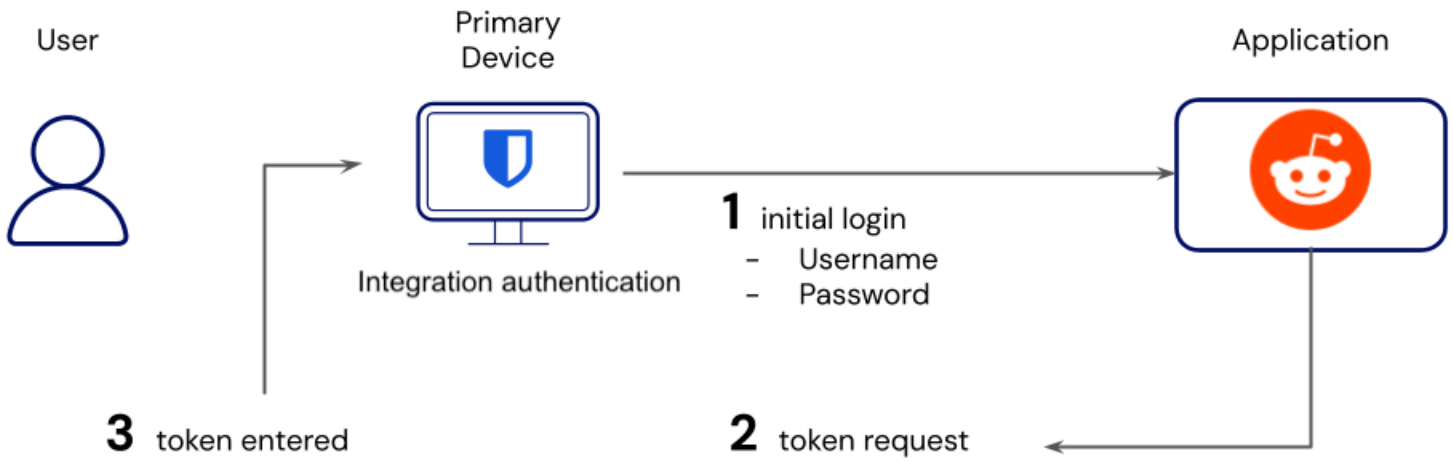
次にRedditにログインするときは、Authyからの認証コードを入力してIDを確認する必要があります。
認証コードは30秒ごとにロテートしますので、悪意のある行為者があなたのデバイスに物理的にアクセスしない限り、
あなたのコードを発見することは不可能になります。

> **Note**
> Authyは、どのデバイスでもバックアップを含むため、私たちが推奨する認証アプリです。バックアップにより、Authyがインストールされているデバイスを失っても、トークンへのアクセスを失うことはありません。Authyアプリの**アカウント**画面で**認証器バックアップ**のトグルをオンにして、この機能を使用します。
>
> 他の認証アプリには、Google AuthenticatorとFreeOTPがあり、2020年5月7日以降、Google AuthenticatorはAndroidデバイス間での認証コードの移植性を含んでいます。

Bitwarden認証器を使用してください

Authyの代わりとして、Bitwardenはプレミアムユーザー、有料組織（家族、チーム、またはエンタープライズ）のメンバーを含む、内蔵の認証器を提供しています。

BitwardenのiOSおよびAndroidは、他の認証アプリと同様にQRコードをスキャンし、6桁のトークンを生成することができます。Bitwarden認証器を使用してウェブページを保護すると、そのログイン保管庫アイテムにロテートする6桁のトークンが保存されます。あなたはまた、任意のBitwardenアプリから認証コードの秘密を手動で保管庫のアイテムに保存することもできます。



Bitwardenを使用した二段階ログイン

Bitwarden認証器の使い方を学ぶ

なぜBitwarden認証器を使用するのですか？

当然ながら、一部のユーザーはBitwardenをトークン認証に使用することに懐疑的です。覚えておいてください、セキュリティはしばしば保護と便利さの間のトレードオフを伴いますので、最善の解決策はあなた次第です。一般的に、Bitwarden認証器を使用する人々は、主に次の2つの理由からです：

1. **便利さ**

   Bitwardenのモバイルアプリやブラウザの拡張機能を使用してユーザー名とパスワードを自動入力すると、
   認証コードが自動的にクリップボードにコピーされ、簡単に貼り付けることができます。

   ブラウザの拡張機能を使用している場合、ログインのキーボードショートカット（Windows：`Ctrl + Shift + L` / macOS：`Cmd + Shift + L`）を、次にペーストのショートカット（Windows：`Ctrl + V` / macOS：`Cmd + V`）と連鎖させることで、
   瞬時にログインできます。

2. **共有**

   組織にとって、トークン検証のためのBitwarden認証器を使用する大きな利点は、チームメンバー間でトークン生成を共有する能力です。
   これにより、組織はアカウントを二段階ログインで保護しながら、
   複数のユーザーがそのアカウントにアクセスする能力を犠牲にすることなく、
   または二人の従業員がトークンを安全でない方法で共有するための調整を必要とすることなく、
   そのアカウントを保護することができます。

2FAセキュリティキーとパスキー

FIDO2 セキュリティキーは、Bitwarden アカウントに2FAを追加するための人気で安全なオプションです。
FIDO2セキュリティキーに詳しくない場合は、FIDO2に関する追加情報を得るためにFIDOアライアンスのウェブページをご覧ください。

YubiKeyデバイスは、FIDO認証プロトコルで動作するセキュリティキーであり、いくつかの使用ケースがあります。2つの用途は、
2FAセキュリティキー、またはパスキーとして使用します。

- **2FAセキュリティキー:** YubiKeyを2FAセキュリティキーとして使用すると、認証プロセスで追加のデバイスとして機能します。これは、他の主要な認証方法（マスターパスワードなど）と併用されます。YubiKeyセキュリティキーは、
  認証資格情報を提供するために物理的に接続する必要があります。

- **パスキー:** パスキーは、ログインを認証するために使用される公開鍵-秘密鍵のペアです。ユーザー名を作成し、パスワードを追加し、アカウントに2FAを追加する代わりに、シングルパスキーが使用されます。パスキー作成中、
  YubiKeyはパスキーのジェネレーターとして機能し、パスキーログインに必要な公開キーと秘密キーを生成することができます。
  YubiKeyをパスキーとして使用する方法については、ここで学ぶことができます。

Bitwardenでは、YubiKeyデバイスなどのセキュリティキーの主な使用目的は、2FA認証を提供することです。

次のステップ

あなたが二段階ログインの専門家になった今、私たちは推奨します：

- 2ステップログインの設定
- 高度な二段階ログイン方法へのアクセスのためにプレミアムを取得してください
- Bitwarden認証器を設定する
- チームとエンタープライズのための二段階ログインを設定する