

私のアカウント > 2段階ログイン >

FIDO2 WebAuthnを介した二 段階ログイン

ヘルプセンターで表示:

<https://bitwarden.com/help/setup-two-step-login-fido/>

FIDO2 WebAuthnを介した二段階ログイン

FIDO2 WebAuthn資格情報を使用した二段階ログインは、すべてのBitwardenユーザーに無料で利用可能です。

FIDO2 WebAuthn認定の資格情報は何でも使用できます。これには、YubiKey、SoloKey、Nitrokeyなどのセキュリティキー、およびWindows HelloやTouch IDのようなネイティブの生体認証オプションが含まれます。

💡 Tip

新しいU2Fのみのキーは**アカウントに追加できません**。ただし、既存のFIDO U2Fセキュリティキーは引き続き使用可能であり、二段階ログイン→FIDO2 WebAuthnを管理するダイアログで**(FIDOから移行)**とマークされます。

FIDO2 WebAuthnは、ほとんどのBitwardenアプリケーションと互換性があります。それをサポートしていないバージョンを使用したい場合は、代替の二段階ログイン方法をオンにすることを確認してください。サポートされているアプリケーションには以下のものがあります：

- デバイス上のウェブ保管庫とFIDO2対応ブラウザ。
- ブラウザ拡張機能は、FIDO2対応ブラウザ用です。
- デスクトップアプリ Windows 10以上で。
- モバイルアプリ AndroidおよびiOS 13.3+用、FIDO2対応ブラウザ付き。

FIDO2 WebAuthnの設定

FIDO2 WebAuthnを使用した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る限り、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。

Password Manager

Vaults

Send

Tools

Reports

Settings

My account

Security

Preferences

Domain rules

Emergency access

Free Bitwarden Famili...

Password Manager

Admin Console

More from Bitwarden

Security

Master password
Two-step login
Keys

Two-step login

Secure your account by requiring an additional step when logging in.

Warning

Setting up two-step login can permanently lock you out of your Bitwarden account. A recovery code allows you to access your account in the event that you can no longer use your normal two-step login provider (example: you lose your device). Bitwarden support will not be able to assist you if you lose access to your account. We recommend you write down or print the recovery code and keep it in a safe place.

[View recovery code](#)

Providers

	<p>Email</p> <p>Enter a code sent to your email.</p>	Manage
	<p>Authenticator app</p> <p>Enter a code generated by an authenticator app like Bitwarden Authenticator.</p>	Manage
	<p>Passkey</p> <p>Use your device's biometrics or a FIDO2 compatible security key.</p>	Manage
	<p>Yubico OTP security key</p> <p>Use a YubiKey 4, 5 or NEO device.</p>	Manage
	<p>Duo</p> <p>Enter a code generated by Duo Security.</p>	Manage

2段階認証

3. FIDO2 WebAuthn オプションを探し、管理ボタンを選択します。

Providers

	Email Enter a code sent to your email.	Manage
	Authenticator app Enter a code generated by an authenticator app like Bitwarden Authenticator.	Manage
	Passkey Use your device's biometrics or a FIDO2 compatible security key.	Manage
	Yubico OTP security key Use a YubiKey 4, 5 or NEO device.	Manage
	Duo Enter a code generated by Duo Security.	Manage

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。

- あなたのセキュリティキーに親しみやすい**名前**を付けてください。
- セキュリティキーをデバイスのUSBポートに差し込み、**キーを読む**を選択してください。
あなたのセキュリティキーにボタンがある場合は、それに触れてください。

Note

Windows HelloまたはパスキーをサポートするmacOSデバイスを含む一部のデバイスは、ネイティブFIDO2認証デバイスであり、これらのオプションをデフォルトとして提供します。セキュリティキーまたは他の認証器を登録したい場合、他のオプションを開くために**別の方法を試す**、**その他のオプション**、または**キャンセル**ボタンを選択する必要があるかもしれません。

- 保存**を選択します。緑色の**有効**メッセージは、FIDO2 WebAuthnを使用した二段階ログインが正常に有効になり、キーが緑色のチェックボックス (✓) で表示されることを示します。
- 閉じる**ボタンを選択し、緑色のチェックボックス (✓) **で示されるように**、FIDO2 WebAuthn✓オプションが有効になっていることを確認します。

このプロセスを繰り返して、最大5つのFIDO2 WebAuthnセキュリティキーをアカウントに追加します。

① Note

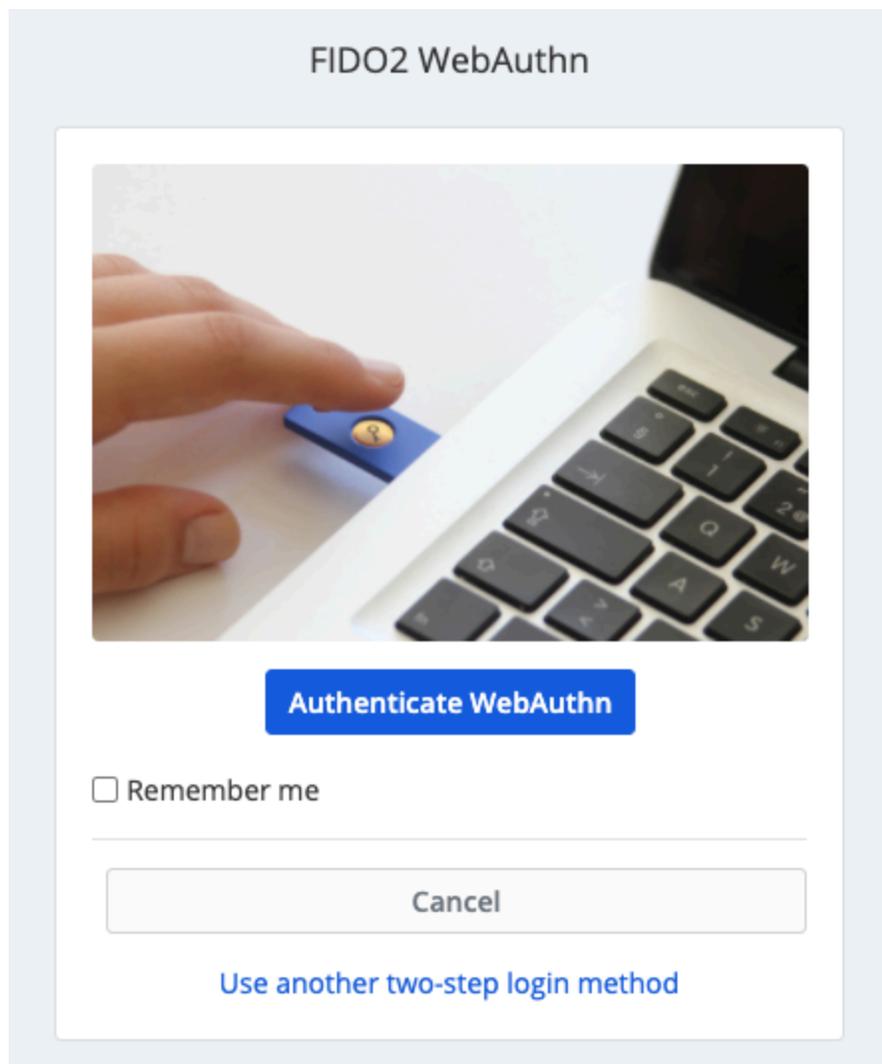
私たちは、何かが誤って設定されていた場合に備えて、二段階ログインをテストする前にアクティブなウェブ保管庫タブを開いておくことをお勧めします。それが動作していることを確認したら、Bitwardenのすべてのアプリからログアウトして、各アプリで二段階ログインを必要とするようにします。最終的には自動的にログアウトされます。

FIDO2 WebAuthnを使用する

以下は、**FIDO2 WebAuthn**があなたの**最優先で有効化された方法**であると仮定しています。FIDO2 WebAuthnデバイスを使用して保管庫にアクセスするには：

1. 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。

あなたのデバイスのUSBポートにセキュリティキーを挿入するように求められます。それがボタンを持っていれば、それに触れてください。



FIDO2-プロンプト

 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。

ログイン後、保管庫をロック解除するために二段階ログインの設定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。

NFCトラブルシューティング

YubiKeyや他のハードウェアセキュリティキーのようなNFC機能を持つFIDO2認証器を使用している場合、デバイスによってNFCリーダーの物理的な位置が異なるため（例えば、電話の上部対下部、または前面对背面）、デバイス内のNFCリーダーを見つける練習が必要かもしれません。

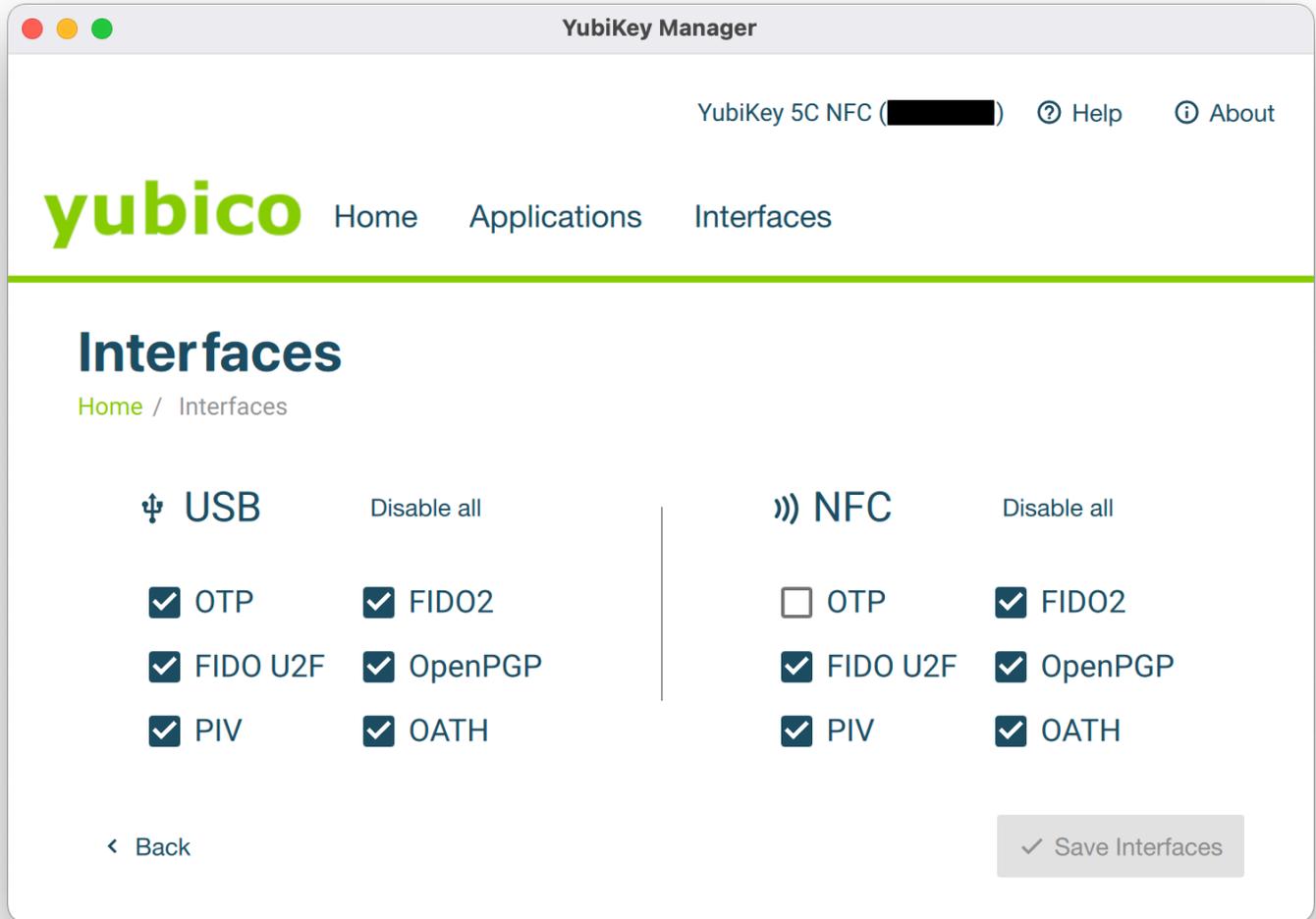
 Tip

ハードウェアのセキュリティキーは通常、物理的なプラグを持っており、NFCが難しい場合にはより確実に動作します。

YubiKey NFCのトラブルシューティング

モバイルデバイスでは、YubiKeyが連続して2回読み取られるシナリオに遭遇することがあります。これが発生したときは、デバイスのブラウザがYubiKeyワンタイムパスワードのウェブページ (<https://demo/yubico.com/yk>) を開き、デバイスが複数回のNFC読み取りを示すために複数回振動することがわかります。

これを解決するには、[YubiKey 管理](#)アプリケーションを使用して、キーのNFC → ワンタイムパスワードインターフェースを無効にします:



YubiKey 管理

Warning

NFCを無効にすると、このキーでYubiKey経由の二段階ログイン（ワンタイムパスワード）をNFC経由で使用することができなくなります。このシナリオでは、USB経由のワンタイムパスワードは期待通りに機能します。