信頼できるデバイスについて

信頼できるデバイスについて

信頼できるデバイスを使用したSSOでは、ユーザーはSSOを使用して認証し、
デバイスに保存された暗号化キーを使用して保管庫を復号化することができ、マスターパスワードを入力する必要がなくなります。
信頼できるデバイスは、ログイン試行の前に事前に登録するか、またはいくつかの異なる方法で承認する必要があります。

信頼されたデバイスとのSSOは、ビジネスエンドユーザーにパスワードレスの体験を提供し、それはゼロノウハウであり、
エンドツーエンドで暗号化されています。これにより、ユーザーは忘れたマスターパスワードによってロックアウトされるのを防ぎ、
スムーズなログイン体験を楽しむことができます。

信頼できるデバイスを使い始めてください

信頼できるデバイスでSSOを使用するためには次の手順を開始します：

1. 組織の信頼できるデバイスを使用して SSO をセットアップします。

2. 管理者にデバイスのリクエストを承認する方法についての情報を提供します。

3. エンドユーザーに信頼できるデバイスの追加方法についての情報を提供します。

それがどのように機能するか

次のタブは、異なる信頼できるデバイスの手順中に発生する暗号化プロセスとキー交換を説明しています:

⇒オンボーディング

新しいユーザーが組織に参加すると、そのユーザーのアカウント暗号化キーを組織の公開キーで暗号化することにより、**アカウント回復キー**(詳細を学ぶ)が作成されます。信頼できるデバイスとSSOを有効にするためには、アカウントの回復が必要です。

その後、ユーザーにデバイスを記憶するか、または信頼するかどうか尋ねられます。彼らがそうすることを選択したとき：

1. 新しい**デバイスキー**はクライアントによって生成されます。このキーはクライアントから出ることはありません。

2. 新しいRSAキーペア、**デバイスのプライベートキー**と**デバイスのパブリックキー**、はクライアントによって生成されます。

3. ユーザーのアカウント暗号化キーは、暗号化されていないデバイス公開キーで暗号化され、
   その結果の値が**公開キーで暗号化されたユーザーキー**としてサーバーに送信されます。

4. **デバイス公開鍵**はユーザーのアカウント暗号化キーで暗号化され、その結果の値が**ユーザーキー暗号化公開鍵**としてサーバーに送信されます。

5. **デバイスプライベートキー**は最初の**デバイスキー**で暗号化され、
   その結果の値が**デバイスキーで暗号化されたプライベートキー**としてサーバーに送信されます。

公開鍵で暗号化されたユーザーキーと**デバイスキーで暗号化されたプライベートキー**は、重要な点として、
ログインが開始されたときにサーバーからクライアントに送信されます。

ユーザーがアカウントの暗号化キーをロテートする必要がある場合、**ユーザーキー暗号化公開キー**が使用されます。

⇒ログイン中

ユーザーが既に信頼されているデバイスでSSOによる認証を行う場合:

1. ユーザーの**公開鍵で暗号化されたユーザーキー**、
   これは保管庫のデータを復号化するために使用されるアカウント暗号化キーの暗号化バージョンで、
   サーバーからクライアントに送信されます。

2. ユーザーの**デバイスキー暗号化プライベートキー**、
   その暗号化されていないバージョンは**公開キー暗号化ユーザーキー**を復号化するために必要です、サーバーからクライアントに送信されます。

3. クライアントは、**デバイスキーで暗号化されたプライベートキー**を、
   クライアントから離れることのない**デバイスキー**を使用して復号化します。

4. 現在暗号化されていない**デバイスプライベートキー**は、**公開キーで暗号化されたユーザーキー**を復号化するために使用され、
   結果としてユーザーのアカウント暗号化キーが得られます。

5. ユーザーのアカウント暗号化キーは保管庫のデータを復号化します。

⇒承認する

ユーザーがSSOで認証し、信頼されていないデバイス（つまり、**デバイス対称キー**がそのデバイスに存在しない）
で保管庫を復号化することを選択した場合、デバイスの承認方法を選択し、
オプションで将来の使用のためにそれを信頼することが必要となります。次に何が起こるかは、選択したオプションによります：

- **別のデバイスから承認する**

  1. ここに記載されているプロセスがトリガーされ、クライアントはアカウント暗号化キーを取得して復号化します。

  2. ユーザーは、復号化されたアカウント暗号化キーを使用して、保管庫のデータを復号化することができます。
     彼らがデバイスを信頼することを選択した場合、**オンボーディング**タブに記載されているように、クライアントとの信頼が確立されます。

- **管理者の承認を求める**

  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鍵**、
     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. 管理者はデバイス承認ページでリクエストを承認または拒否することができます。

  3. リクエストが管理者によって承認されると、承認したクライアントはリクエストに含まれる**auth-request公開鍵**を使用して、
     ユーザーのアカウント暗号化キーを暗号化します。

  4. 承認されたクライントは、暗号化されたアカウントの暗号化キー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. 開始クライントは暗号化されたアカウント暗号化キーをGETし、
     それを**認証リクエストのプライベートキー**を使用して**ローカルで**復号化します。

  6. 復号化されたアカウント暗号化キーを使用して、**オンボーディング**タブで説明されているように、
     クライアントとの信頼関係が確立されます。

[α] – **Auth-request public**と**private keys**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。未承認のリクエストは1週間後に期限切れになります。

- **マスターパスワードで承認**:

  1. ユーザーのアカウント暗号化キーは、
     セキュリティホワイトペーパーのユーザーログインセクションに記載されている通りに取得および復号化されます。

  2. 復号化されたアカウント暗号化キーを使用して、**オンボーディング**タブで説明されているように、
     クライアントとの信頼関係が確立されます。

⇒キーのロテート

> **Note**
> マスターパスワードを持っているユーザーのみが、アカウントの暗号化キーをロテートできます。もっと学ぶ

ユーザーがアカウント暗号化キーをロテートするとき、通常のロテーションプロセス中に：

1. **ユーザーキー暗号化公開キー**はサーバーからクライアントに送信され、その後、古いアカウント暗号化キー（別名。**ユーザーキー**により、**デバイス公開キー**が生成されます。
2. ユーザーの新しいアカウント暗号化キーは、暗号化されていないデバイス公開キーで暗号化され、その結果の値が新しい**公開キーで暗号化されたユーザーキー**としてサーバーに送信されます。
3. **デバイス公開鍵**は、ユーザーの新しいアカウント暗号化キーで暗号化され、その結果の値が新しい**ユーザーキー暗号化公開鍵**としてサーバーに送信されます。
4. ユーザーのために、サーバーのストレージに永続化された他のすべてのデバイスの信頼されるデバイス暗号化キーがクリアされます。これにより、その単一のデバイスに対してサーバーに永続化された3つの必要なキーだけが残ります（**公開キーで暗号化されたユーザーキー**、**ユーザーキーで暗号化された公開キー**、そしてこのプロセスによって変更されなかった**デバイスキーで暗号化されたプライベートキー**）。

信頼性が失われたクライアントは、**承認**タブに記載されている方法のいずれかを通じて信頼性を再確立する必要があります。

信頼できるデバイス用のキー

このテーブルは、上記の手順で使用される各キーについての詳細情報を提供します：

キー	詳細
デバイスキー	AES-256 CBC HMAC SHA-256、長さ512ビット（キー用256ビット、HMAC用256ビット）
デバイスプライベートキー & デバイスパブリックキー	RSA-2048 OAEP SHA1、長さ2048ビット
公開鍵で暗号化されたユーザーキー	RSA-2048 OAEP SHA1
ユーザーキー暗号化公開鍵	AES-256 CBC HMAC SHA-256
デバイスキー暗号化プライベートキー	AES-256 CBC HMAC SHA-256

マスターパスワードへの影響

信頼できるデバイスとのSSOはマスターパスワードの必要性を排除しますが、すべてのケースでマスターパスワード自体を排除するわけではありません:

- ユーザーが信頼できるデバイスでのSSOが有効化される**前に**オンボーディングされた場合、
  または組織の招待から**アカウントを作成**を選択した場合、そのアカウントはマスターパスワードを保持します。

- 信頼できるデバイスでのSSOが有効化された**後**にユーザーがオンボーディングされ、彼らが組織の招待から**ログイン→エンタープライズSSO**を選択した場合、JITプロビジョニングのための彼らのアカウントはマスターパスワードを持っていません。

> ⚠ **Warning**
>
> マスターパスワードがない結果としての信頼できるデバイスとのSSOを持つアカウントについては、
> 組織からの削除またはアクセス権の取り消しにより、以下の場合を除き、
> そのBitwardenアカウントへのすべてのアクセスが遮断されます：
>
> 1. あらかじめアカウント回復を使用して、マスターパスワードを割り当てます。
>
> 2. ユーザーは、アカウント回復ワークフローを完全に完了するために、アカウント回復後に少なくとも一度ログインします。

他の機能への影響

あなたのクライントのためのマスターパスワードハッシュがメモリ内に利用可能かどうかは、
クライアントアプリケーションが最初にアクセスされる方法によって決まります。それにより、
以下のような振る舞いの変化が見られるかもしれません：

機能	インパクト
確認	Bitwarden クライアント アプリケーションには、ボールト データのエクスポート、 2段階ログイン設定の変更、 API キーの取得など、通常、使用するためにマスターパスワードの入力が必要な機能が多数あります。 ユーザーがマスターパスワードを使用せずにクライアントにアクセスする場合、**これらすべての機能**はマスターパスワードの確認をメールアドレスを基にしたTOTP検証に置き換えます。
保管庫ロック/ロック解除	通常の状況下では、ロックされた保管庫はマスターパスワードを使用してロック解除できます。 ユーザーがマスターパスワードを使用せずにクライアントにアクセスする場合、 ロックされたクライアントアプリケーションは、PINまたは生体認証でのみロック解除できます。 クライアントアプリケーションにPINも生体認証も有効になっていない場合、 保管庫はロックする代わりに常にログアウトします。 ロック解除とログインは**常に**インターネット接続が必要です。
マスターパスワードの再要求	ユーザーがマスターパスワードで保管庫をロック解除しない場合、 マスターパスワードの再プロンプトは無効になります。
CLI	マスターパスワードを持っていないユーザーは、パスワードマネージャーCLIに**アクセスできません**。