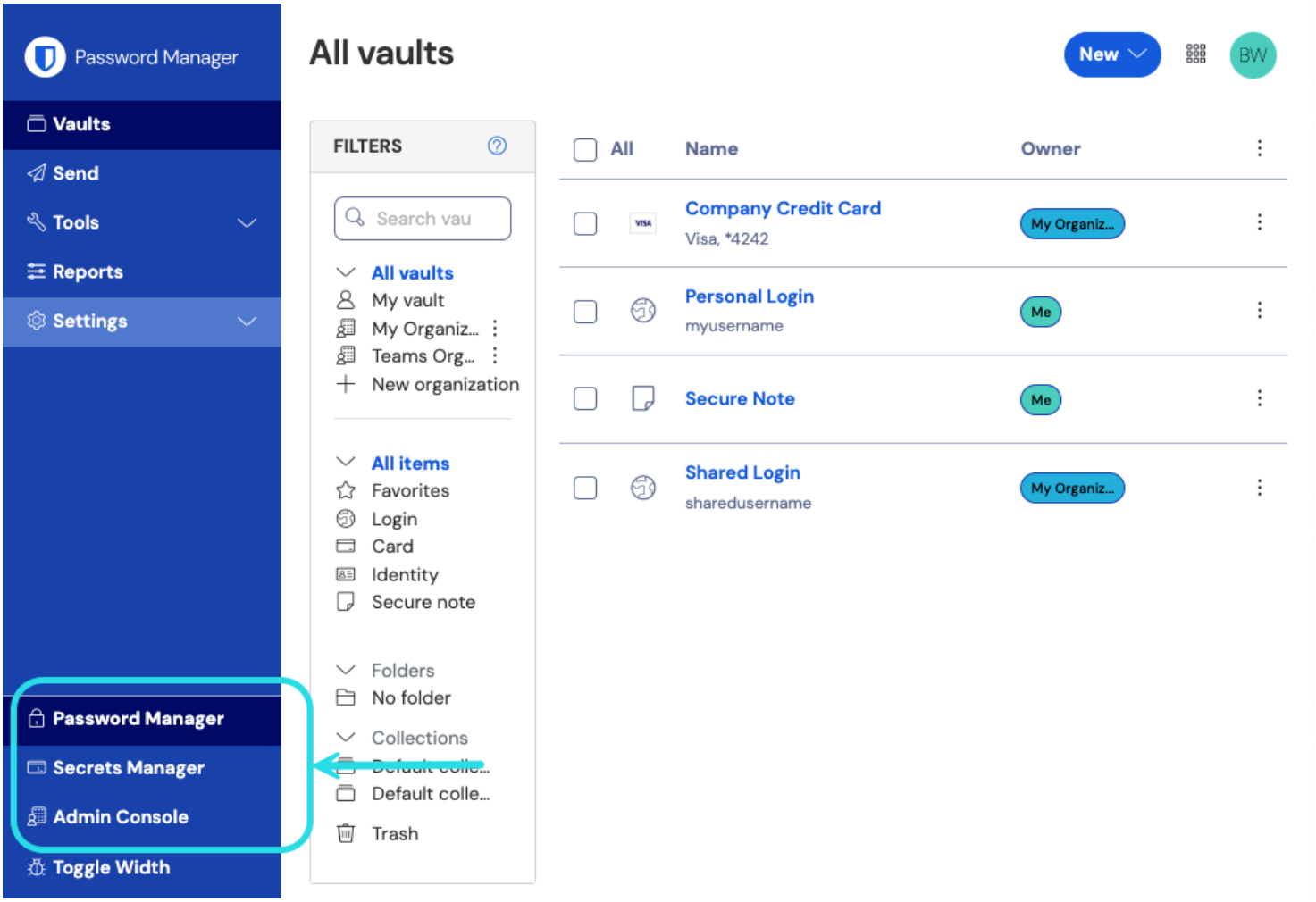
信頼できるデバイスでSSOを設定する

信頼できるデバイスでSSOを設定する

このドキュメントでは、あなたの組織に信頼できるデバイスでのSSOを追加する方法を説明します。これらの手順を完了するには、組織の所有者または管理者でなければなりません:

1. Bitwardenウェブアプリにログインし、製品スイッチャー（⁞⁞⁞）を使用して管理者コンソールを開きます。



製品-スイッチャー

2. ナビゲーションから**設定** → **ポリシー**を選択してください。
3. ポリシーのページで、信頼できるデバイスの使用に必要な次のポリシーを有効にしてください：
   - **単一組織**ポリシー。
   - **シングルサインオン認証を必要とする**ポリシー。
   - **アカウント回復管理**ポリシー。
   - アカウント回復管理ポリシーの**[新しいメンバーを自動的に登録することを要求する]**オプション。

   > **Note**
   > これらのポリシーを事前に有効にしない場合、**信頼できるデバイス**メンバーの復号化オプションを有効にすると自動的に有効になります。ただし、アカウント回復が有効になっていないアカウントがある場合、それらは信頼できるデバイスで管理者の承認を使用する前に、自己登録する必要があります。アカウント回復を有効にするユーザーは、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する必要があります。

4. ナビゲーションから**設定** > **シングルサインオン**を選択します。まだSSOを設定していない場合は、私たちのSAML 2.0またはOIDC実装のガイドを参照してください。
5. メンバー復号化オプションセクションで**信頼できるデバイス**オプションを選択してください。

一度有効化されると、ユーザーは信頼できるデバイスで保管庫の暗号化を解除することができます。

マスター パスワードを持たないメンバーが信頼できるデバイス**のみ**を使用できるようにすることが望ましい場合は、組織の招待から**[ログイン] → [エンタープライズ SSO]**を選択して JIT プロビジョニングを開始するようにユーザーに指示します。管理者/所有者は、冗長性とフェイルオーバーの目的のために、依然として**アカウントを作成**オプションを使用してマスターパスワードを持つべきです。

> ⚠ **Warning**
>
> 信頼できるデバイスを使用したSSOから他のメンバー復号化オプションへの移行は現在推奨されていません:
>
> - 何らかの理由で組織がメンバーの復号化オプションを信頼できるデバイスの暗号化からマスターパスワードに切り替える必要がある場合、**あなたは**アカウント回復を使用してマスターパスワードを発行する必要があります**全てのユーザーに対して**それらなしでオンボードした**彼らのアカウントへのアクセスを保持するために。**ユーザーは、マスターパスワードによるアカウント回復の後、ワークフローを完了するために完全にログインする必要があります。
> - 信頼できるデバイスを使用したSSOからキーコネクターへの移行はサポートされていません。

メンバーの復号化オプションを信頼されたデバイスからマスターパスワードに変更します。

メンバーの復号化オプションを信頼されたデバイスからマスターパスワードに変更すると、マスターパスワードを発行せずにユーザーアカウントがロックアウトされます。
このポリシーの変更を行うためには、以下のことが必要です：

1. アカウント回復を使用してマスターパスワードを発行します。
2. ユーザーは、アカウントの回復後に少なくとも一度ログインする必要があります。これにより、ワークフローが完全に完了し、ロックアウトを防ぐことができます。

メンバーの復号化オプションがマスターパスワードを発行せずに変更された場合、ユーザーには以下の3つのオプションが残ります：

- 削除-回復のワークフローに従ってください。
- アカウント/組織バックアップからアカウントを復元します。
- 新しいアカウントまたは組織を作成します。