管理者コンソール > ユーザー管理

ユーザー管理

ユーザー管理

ユーザー数

Bitwarden チームとエンタープライズ組織は、新しいユーザーを**招待**すると、ユーザーシートが自動的にスケールアップします。
指定した数値を超えないように、席の上限を設定してスケーリングを制限することができます。また、手動で席を追加することも可能です。
どのように席を追加するかに関わらず、使用しなくなった席を手動で削除する必要があります。

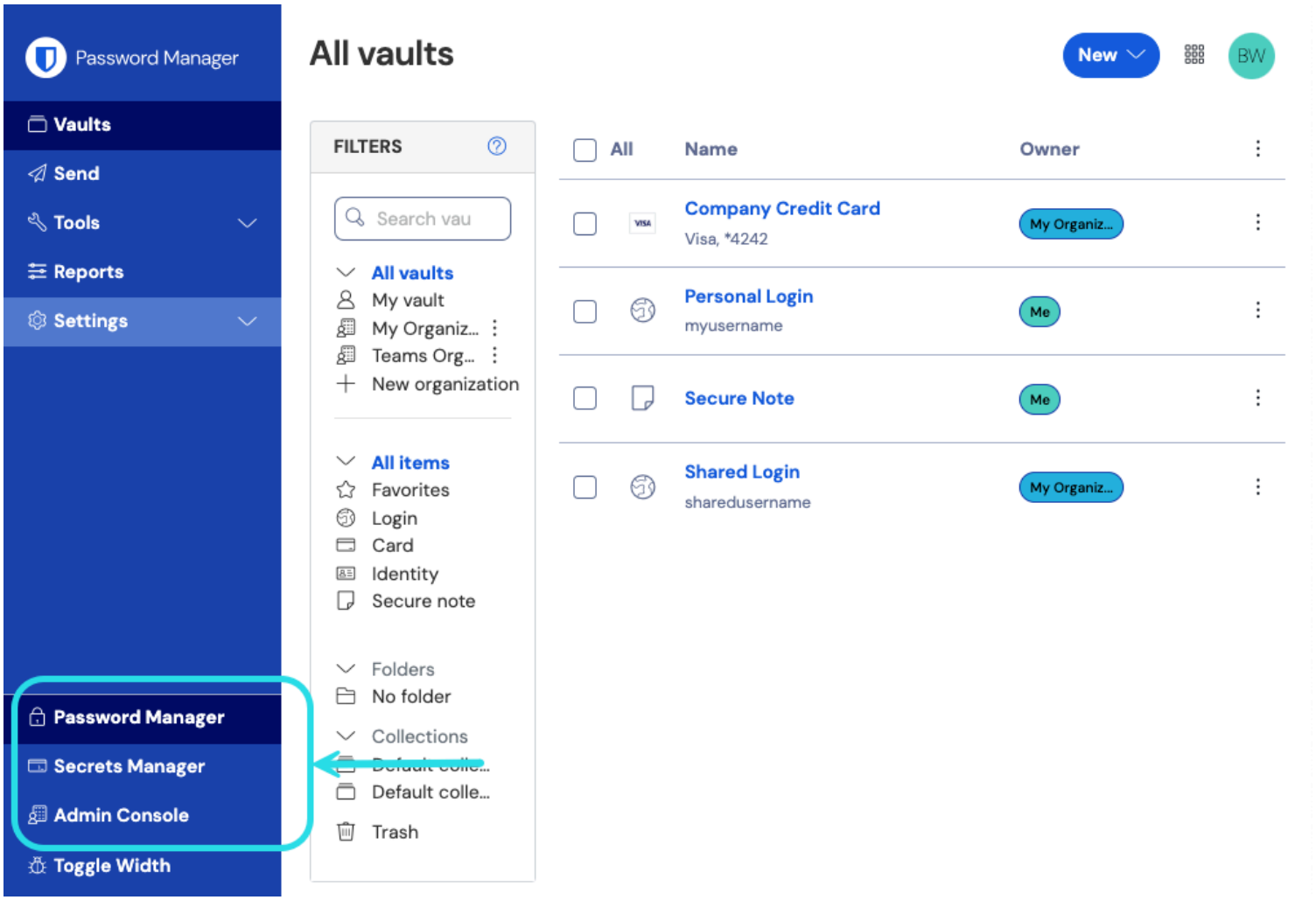
ユーザーシートの追加と削除は、将来の請求書の合計を調整します。席を追加すると、
調整されたレートで即座にファイル上のお支払い方法が請求されます。そのため、**請求周期（月/年）の残りの部分のみを支払う**ことになります。シートを削除すると、
すでに支払ったシートが使用されていない時間について**クレジットが付与される**ように、次回の請求が調整されます。

> **ⓘ Note**
> 組織所有者またはプロバイダーサービスユーザーだけが席を追加または削除できます。これは直接請求に影響を与えます。

席の制限を設定します

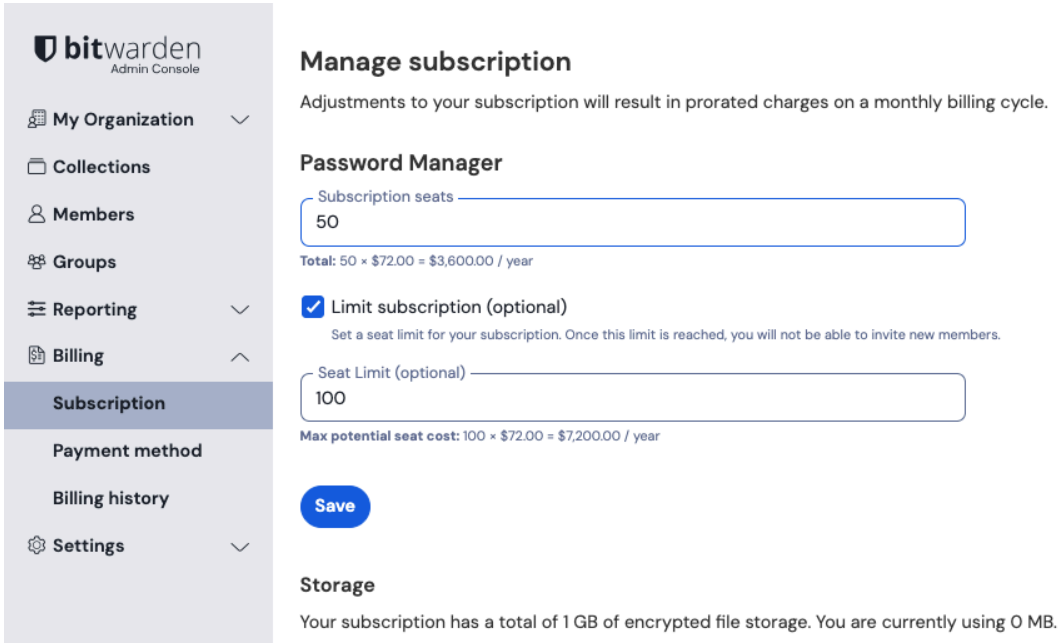
あなたの組織がスケールアップできる座席の数値に制限を設定するには：

1. Bitwardenの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. **請求書** → **サブスクリプション**に移動し、**サブスクリプションの制限**チェックボックスを確認してください：



席の制限を設定します

3. **座席制限**の入力欄に、座席制限を指定してください。

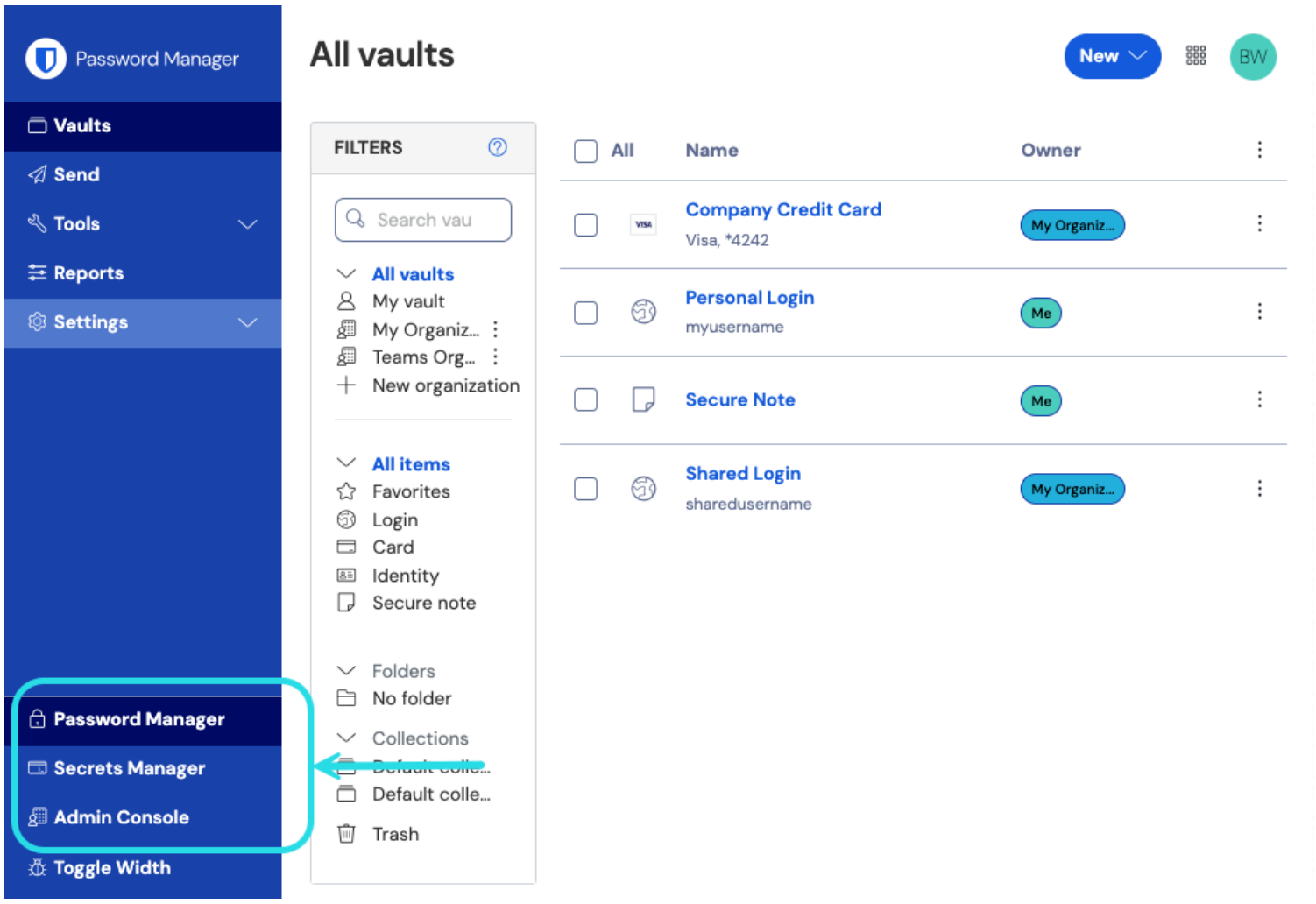
4. **保存**を選択してください。

> **Note**
> 指定された制限に達すると、制限を増やさない限り、新しいユーザーを招待することはできません。

手動で席を追加または削除します

あなたの組織に席を手動で追加または削除するには：

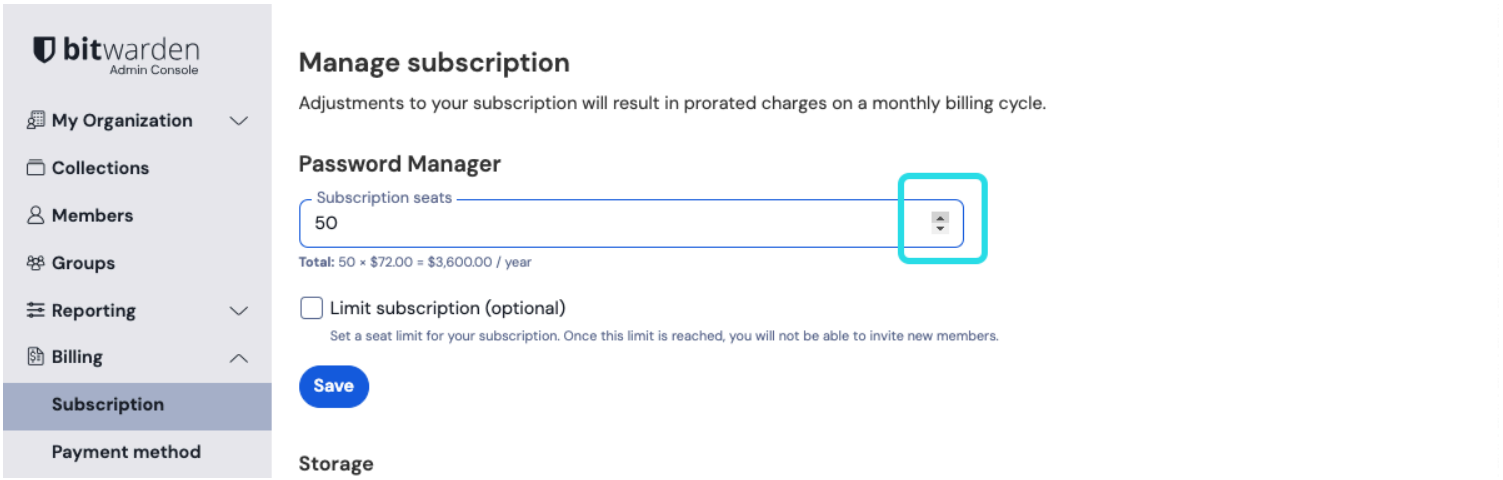
1. Bitwardenのウェブアプリにログインし、製品スイッチャー（⋮⋮⋮）を使用して管理者コンソールを開きます。



製品-スイッチャー

2. **請求書**に移動 → **サブスクリプション。**

3. **サブスクリプション席**の入力欄で、マウスオーバー矢印を使用して席を追加または削除します。



シートを追加または削除する

4. **保存**を選択してください。

> **Note**
> 指定された**席の上限**を超えて**サブスクリプションの席**を増やす場合、
> 希望のサブスクリプション席の数以上に席の上限を増やす必要があります。

ユーザーをボードに乗せる

あなたの組織のセキュリティを確保するために、
Bitwardenは新しいメンバーをオンボーディングするための3ステッププロセスを適用します、招待 → 受け入れ → 確認。

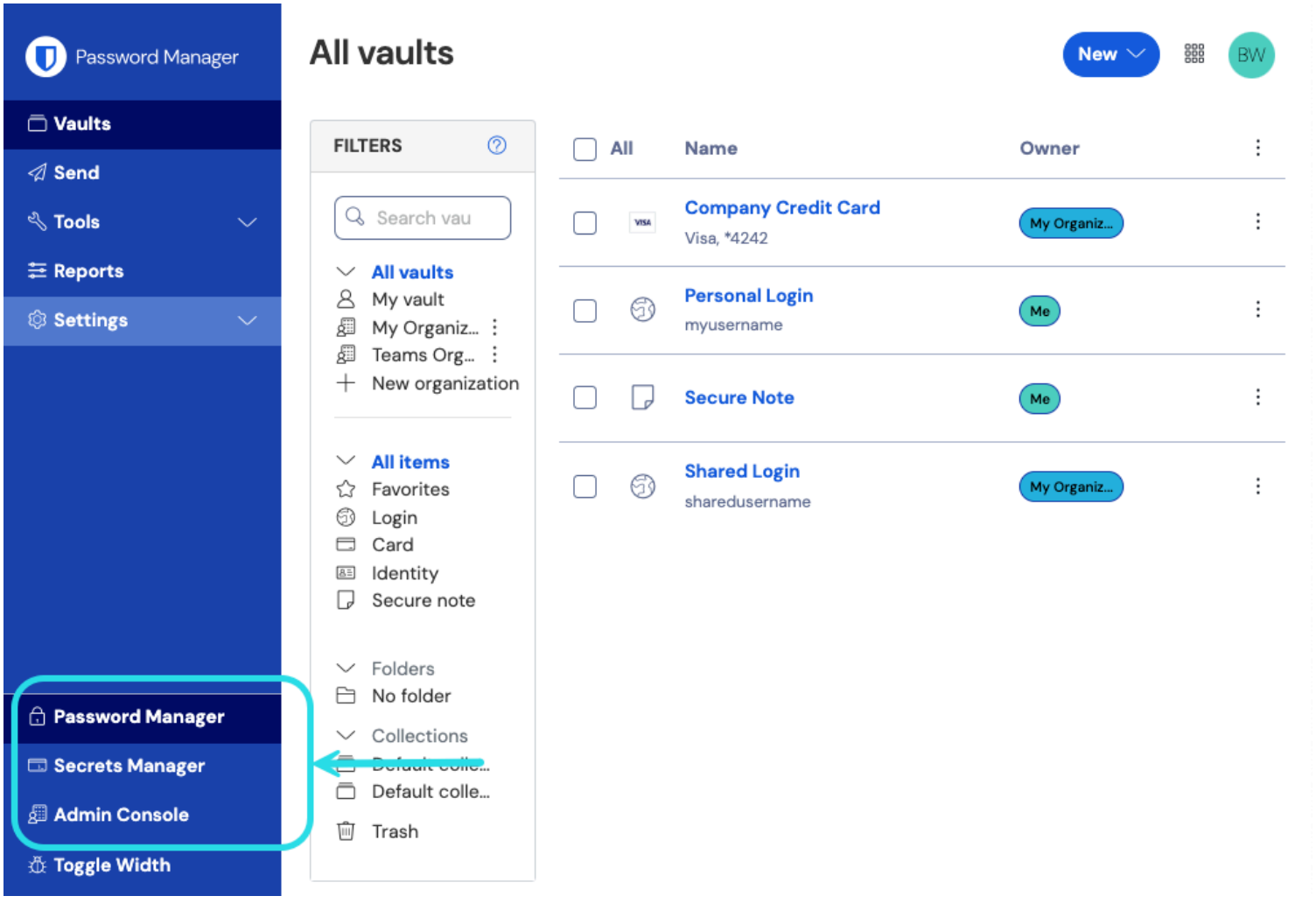
> **Tip**
> このドキュメントは、ユーザーをBitwarden組織に追加するための手動オンボーディングフローをカバーしていますが、
> Bitwardenは自動的なユーザーとグループのプロビジョニングのための2つの方法を提供しています：
>
> - エンタープライズ組織は、Azure AD、Okta、OneLogin、およびJumpCloudのSCIM統合を使用できます。
> - チームとエンタープライズ組織は、Active Directory/LDAP、Azure AD、Google Workspace、Okta、
>   およびOneLoginに対してディレクトリコネクタを使用できます。

招待

> **Tip**
> エンタープライズ組織の場合、ユーザーを招待する前にエンタープライズポリシーを設定することをお勧めします。これにより、組織への入会時にコンプライアンスが確保されます。

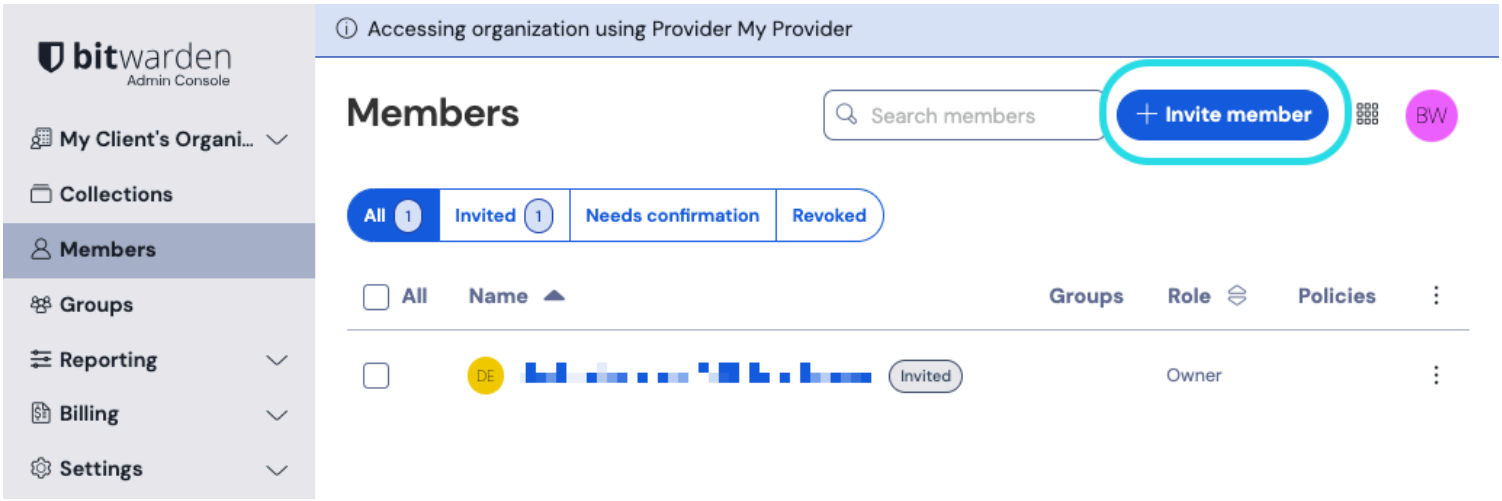
あなたの組織にユーザーを招待するには：

1. Bitwardenの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. **メンバー**に移動し、＋**ユーザーを招待**ボタンを選択します:



メンバーを招待する

3. 招待ユーザーパネルで：

- 新規ユーザーが**メールアドレス**に招待を受け取るべき場所を入力してください。
  一度に最大20人のユーザーを追加することができます。メールアドレスをカンマで区切ってください。

- 新しいユーザーに適用するために、**メンバーの役割**を選択してください。メンバーの役割は、
  これらのユーザーが組織レベルでどのような権限を持つかを決定します。

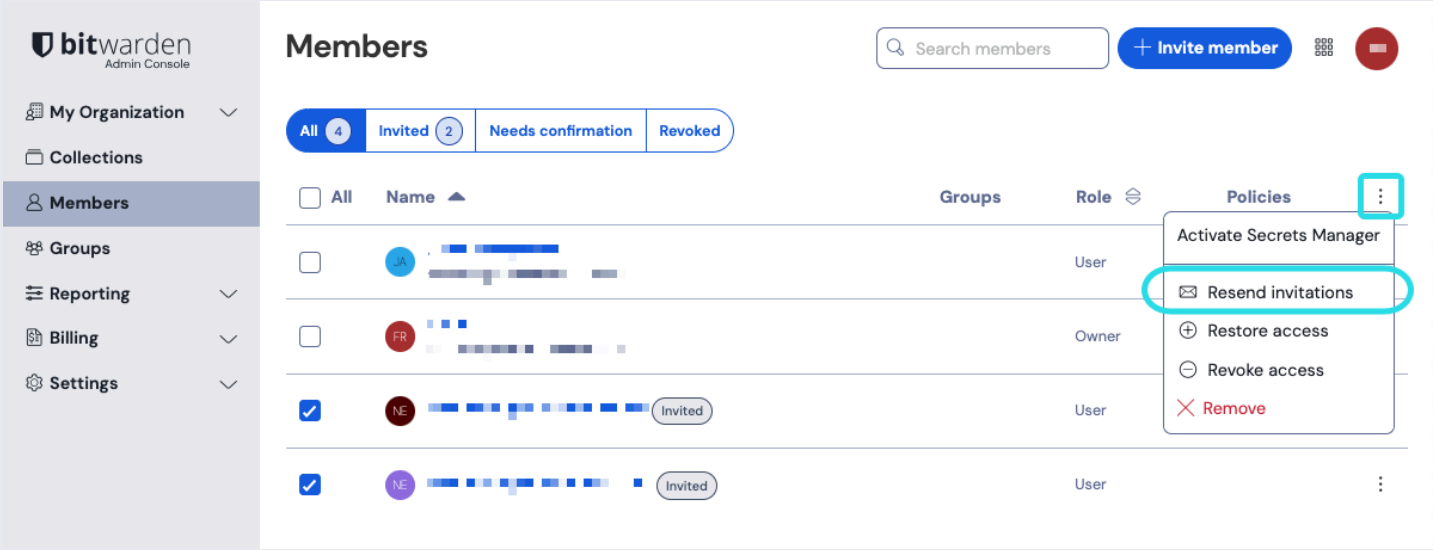
- **グループ**タブで、このユーザーを追加するグループを選択してください。

- **コレクション**タブで、このユーザーがアクセスできるように収集を選択し、
  各コレクションに対してどの権限を持つべきかを決定します。

4. 指定されたユーザーをあなたの組織に招待するために、**保存**をクリックしてください。

Note

招待状は5日後に期限切れになります、その時点でユーザーは再度招待する必要があります。各ユーザーを選択し、⋮オプションメニューを使用して、**招待を再送**することで、ユーザーを一括で再招待します。

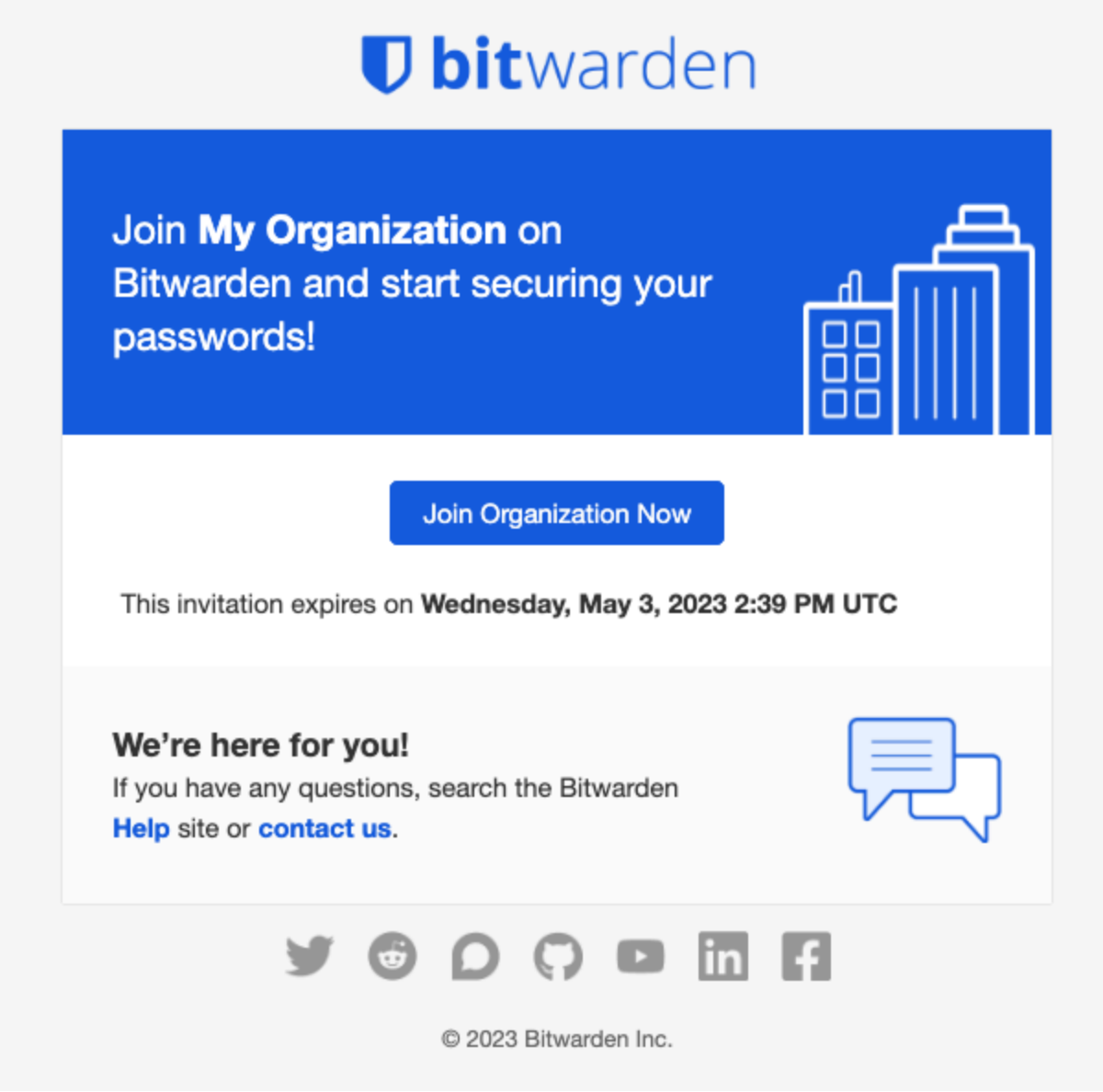


一括再招待

あなたがBitwardenを自己ホスト型で使用している場合、環境変数を使用して招待の有効期限を設定することができます。

同意

招待されたユーザーは、Bitwardenから組織に参加するための招待を含むメールアドレスを受け取ります。
メール内のリンクをクリックすると、Bitwardenのウェブアプリが開き、ユーザーはログインするか、
アカウントを作成して招待を受け入れることができます。



招待ウィンドウ

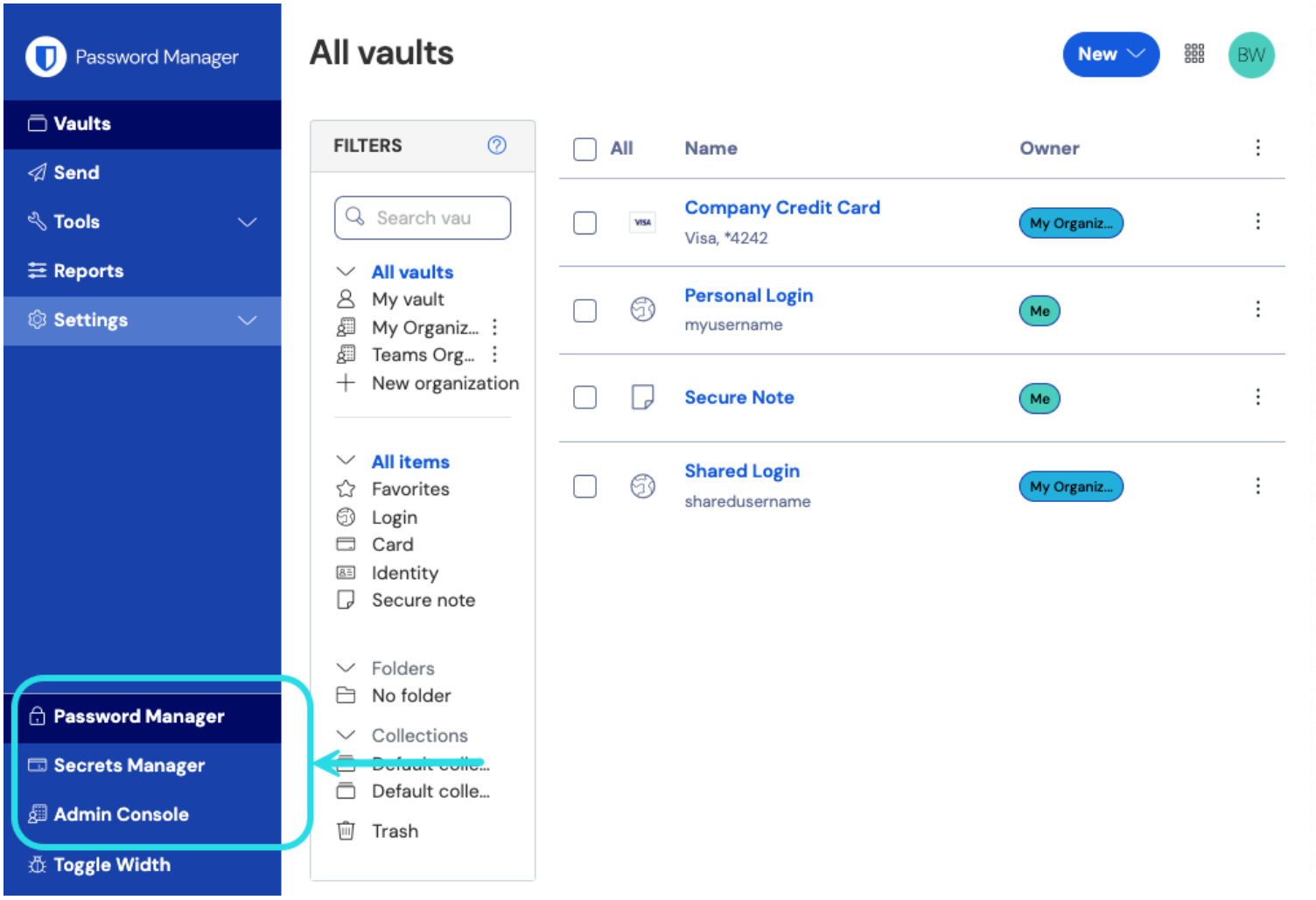
招待を受け入れると、確認され次第、組織にアクセスできることが通知されます。さらに、組電のメンバーは、招待を受け入れるときにメールアドレスが自動的に確認されます。

確認

> **Tip**
> 3ステップの招待 → 受け入れ → 確認の手順は、エンドツーエンドの暗号化を維持しながら、組織とユーザー間の安全な共有を促進するために設計されています。もっと学ぶ

あなたの組織への受け入れられた招待を確認するには：

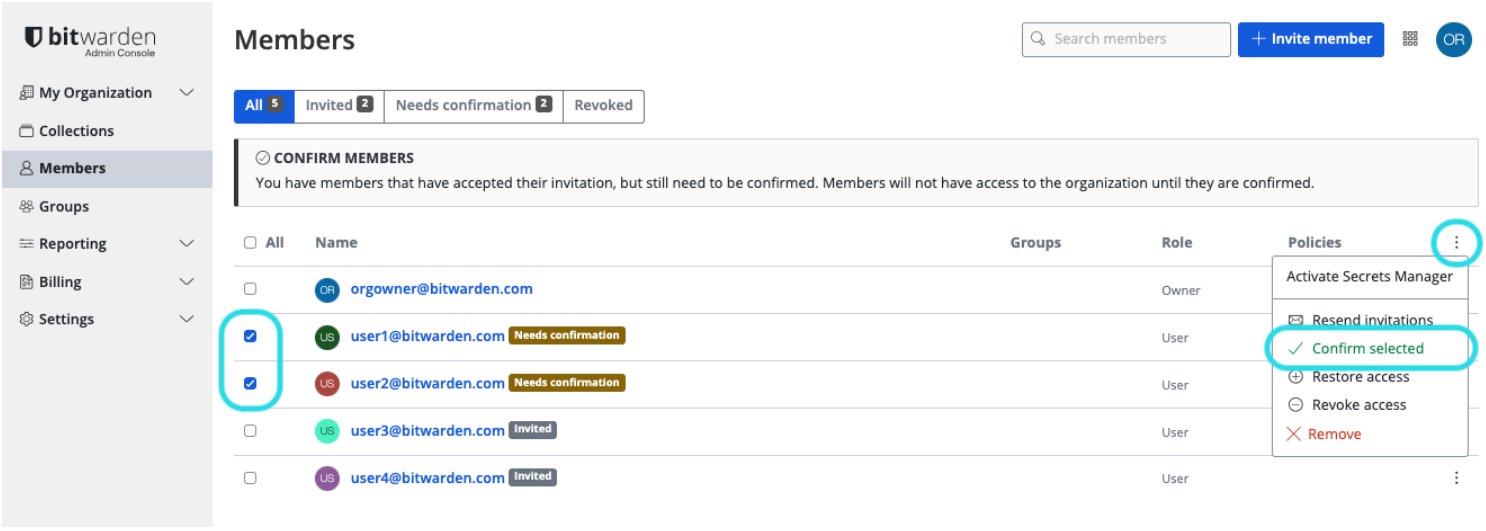
1. Bitwardenのウェブアプリにログインし、製品スイッチャーを使用して管理者コンソールを開きます(⊞):



製品-スイッチャー

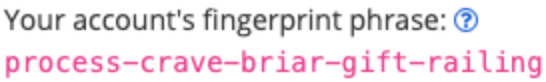
2. **メンバー**に移動してください。

3. 任意の 承認済み ユーザーを選択し、⋮オプションメニューを使用して✓ **選択したものを確認**します:



承認されたメンバーを確認してください

4. 画面上のフィンガープリントフレーズが新しいメンバーが**設定→アカウント**で見つけるものと一致していることを確認してください。



サンプルフィンガープリントフレーズ

各フィンガープリントフレーズはそのアカウントに固有であり、ユーザーを安全に追加する際の最終的な監視層を確保します。
それらが一致する場合は、**送信**を選択してください。

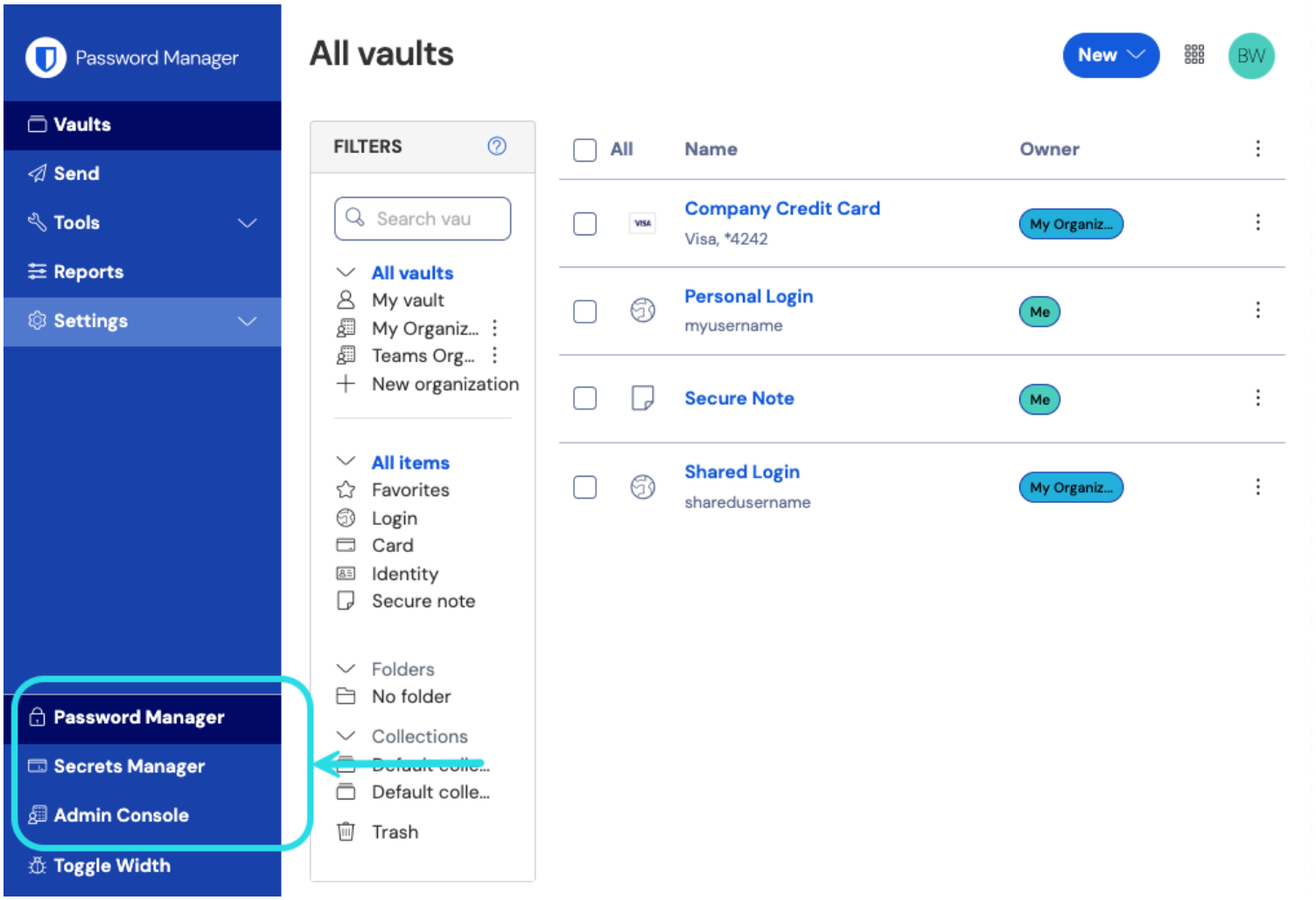
> **ⓘ Note**
>
> **「フィンガープリントフレーズの確認を求めない」**がオンになっている場合、
> ブラウザのキャッシュとクッキーをクリアすることでフィンガープリントフレーズの確認を再度有効にすることができます。

ユーザーの利用停止

> **⚠ 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。

あなたの組織からユーザーを削除するには：

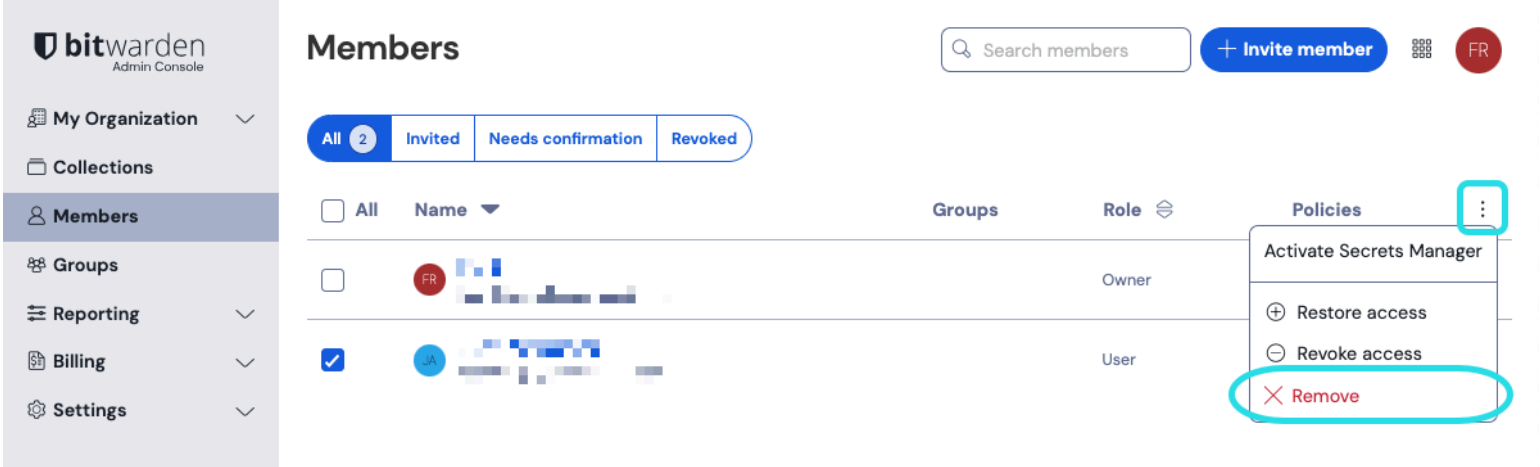
1. Bitwardenのウェブアプリにログインし、製品スイッチャー（⠿）を使用して管理者コンソールを開きます。



製品-スイッチャー

2. **メンバー**に移動してください。

3. 組織から削除したいユーザーを選択し、⋮ オプションメニューを使用して ╳ **削除**します：



メンバーを削除する

> **Tip**
> オフラインのデバイスは、組織の保管庫データを含む保管庫データの読み取り専用コピーをキャッシュします。
> これを悪意ある利用が予想される場合、メンバーがアクセスしていた資格情報は、
> 彼らを組織から削除するときに更新するべきです。

ユーザーアカウントの削除

あなたの組織からユーザーを削除しても、そのユーザーのBitwardenアカウントは削除されません。ユーザーが削除されると、
組織や共有されたアイテムとコレクションにはアクセスできなくなりますが、既存のマスターパスワードを使用してBitwardenにログインし、
個々の保管庫のアイテムには引き続きアクセスできます。

あなたの実装の詳細によりますが、以下の方法のいずれかを使用して、
デプロビジョニングされたユーザーに属するBitwardenユーザーアカウントを削除することができるかもしれません:

1. あなたが自己ホスト型のBitwardenを使用している場合、
   認証された管理者はシステム管理者ポータルからアカウントを削除することができます。

2. あなたの会社が管理する `@yourcompany.com` のメールアドレスを持つアカウントの場合、
   ログインせずに削除のワークフローを使用して、 `@yourcompany.com` の受信トレイ内で削除を確認できます。詳細については、
   アカウントまたは組織を削除をご覧ください。

アクセスを取り消す

Tip

あなたの組織がアクティブなSCIMインテグレーションを持っている場合、
ユーザーがソースディレクトリで停止または非アクティブ化されると、ユーザーの組織へのアクセスは自動的に取り消されます。

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：

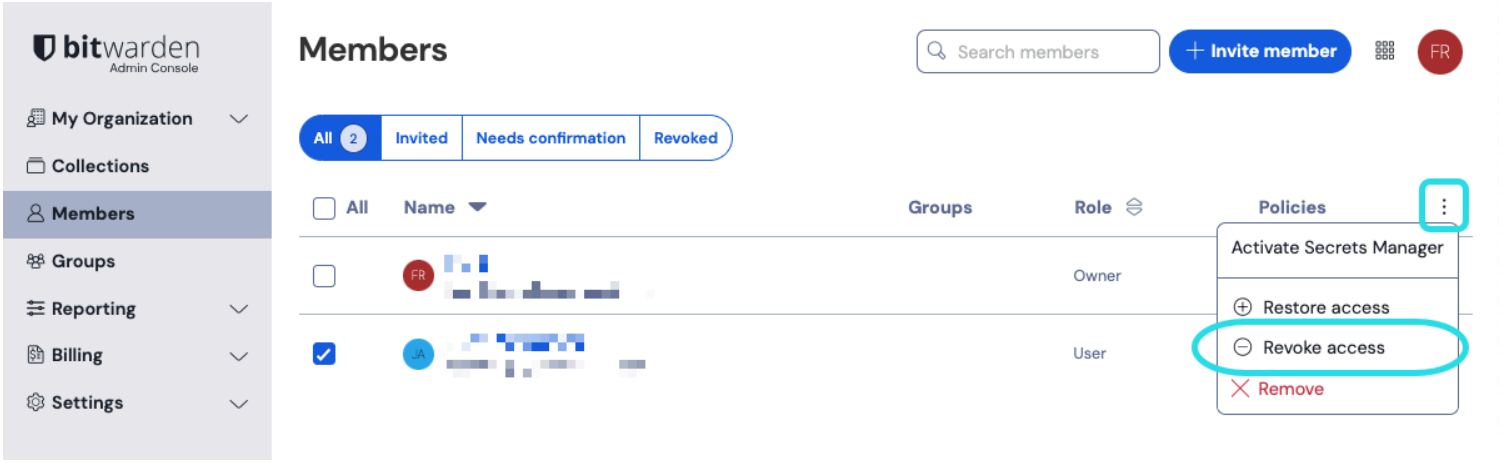
1. あらかじめアカウント回復を使用して、マスターパスワードを割り当てます。

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。

完全にメンバーを削除する代わりに、一時的に組織とその保管庫のアイテムへのアクセスを取り消すこともできます。
アクセスを取り消すには：

1. 管理者コンソールで、**メンバー**に移動します。

2. アクセスを取り消したいメンバーを選択し、⋮オプションメニューを使用して**アクセスを取り消す**：



アクセスを取り消す

Note

所有者のみ 他の所有者へのアクセスを取り消したり復元したりできます。

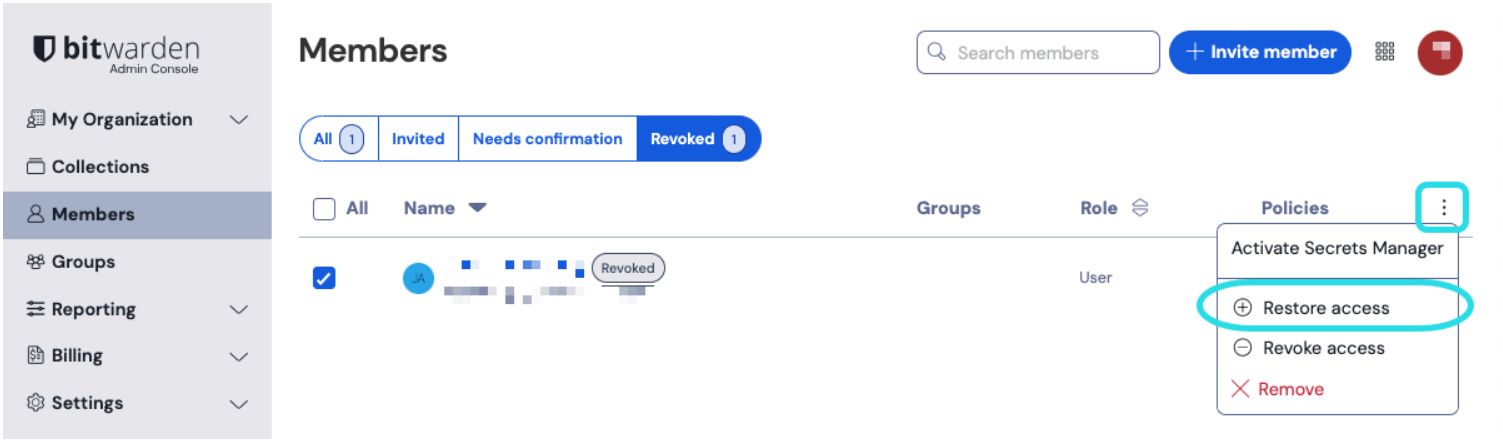
アクセスが取り消されたユーザーは、**取り消し** タブにリストされ、次の操作を行います：

- 組織の保管庫アイテム、コレクションなどにはアクセスできません。
- SSOを使用してログインする能力がない、または組織的なDuoを二段階ログインに使用することはできません。
- 組織のポリシーの対象ではありません。
- ライセンス席を占有しないでください。

アクセスを復元する

ユーザーへのアクセスを復元するには：

1. 管理者コンソールで、**メンバー**に移動します。
2. **取り消された**メンバー タブを開いてください。
3. アクセスを復元したいユーザーを選択し、⋮オプションメニューを使用して**アクセスを復元**します：

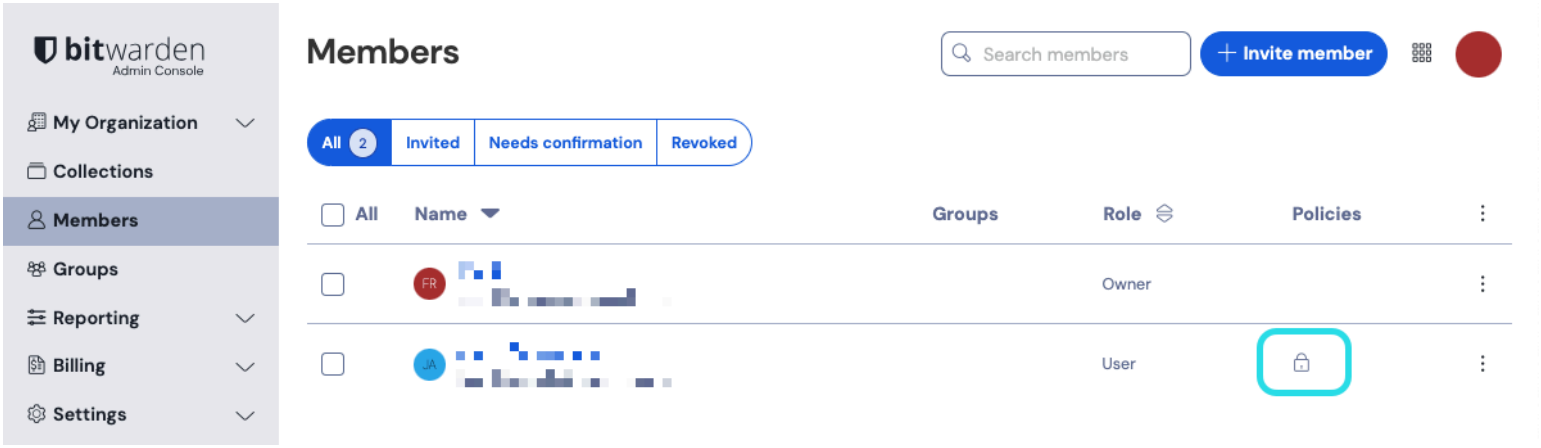


アクセスを復元する

ユーザーがアクセスを復元すると、再度招待 → 受け入れ → 確認のワークフローを経る必要はありません。

ユーザーの二要素認証ステータスを確認してください

ユーザーの二要素認証ステータスは、**メンバー**ページから表示できます。ユーザーが 🔒 アイコンを持っている場合、そのユーザーのBitwardenアカウントには二段階ログインが有効になっています。



二要素認証インジケーター