あなたの組織を管理してください

あなたの組織を管理してください

> **Note**
> 完全なBitwardenのオンボーディングの概要については、詳細情報を得るために、このガイドをご覧ください。

シークレットマネージャーを使用する組織として、元々パスワードマネージャーで使用されていた多くのツールを共有します。この記事では、これらの一般的な領域をカバーし、適切な場所で文書を共有するリンクを提供します。

> **Note**
> Bitwardenの組織にまったく新しい場合は、組織管理者としてのスタートガイドの記事をチェックすることをお勧めします。

容易なオンボーディング

ポリシーは、エンタープライズ組織がメンバーに対してセキュリティルールを強制することを可能にします。例えば、二段階ログインの使用を義務付けることができます。一部のポリシーは主にパスワードマネージャーに適用されますが、シークレットマネージャーのユーザーに広く適用されるポリシーもいくつかあります。

- 2段階認証が必要です
- マスターパスワードの要件
- マスターパスワードのリセット
- 単一組織
- シングルサインオン認証
- 保管庫のタイムアウト

> **Tip**
> Bitwardenに新しく参加された方は、ユーザーをオンボーディングする前にポリシーを設定することをお勧めします。

ユーザー管理

シークレットマネージャーの組織でのユーザー管理は、パスワードマネージャーを使用する組織と似ていますが、シークレットマネージャー固有の要素には、組織のメンバーにシークレットマネージャーへのアクセスを許可すること、メンバーの役割の違い、そしてユーザーシートとサービスアカウントを指定することが含まれます。

オンボーディング

あなたのBitwarden組織にユーザーをオンボーディングするためのいくつかの異なる方法があります。ここでは、よく使われる方法のいくつかを強調しています:

手動

Bitwardenのウェブ保管庫は、新しいユーザーをあなたの組織に招待するためのシンプルで直感的なインターフェースを提供します。この方法は、小規模な組織やAzure ADやOktaのようなディレクトリサービスを使用していない組織に最適です。始め方を学びましょう。

SCIM

Bitwardenサーバーは、有効なSCIM APIキーを持つと、ユーザーとグループのプロビジョニングおよびデプロビジョニングのためのあなたのIDプロバイダからのリクエストを受け入れるSCIMエンドポイントを提供します。この方法は、SCIM対応のディレクトリサービスまたはIdPを使用する大規模な組織に最適です。始め方を学びましょう。

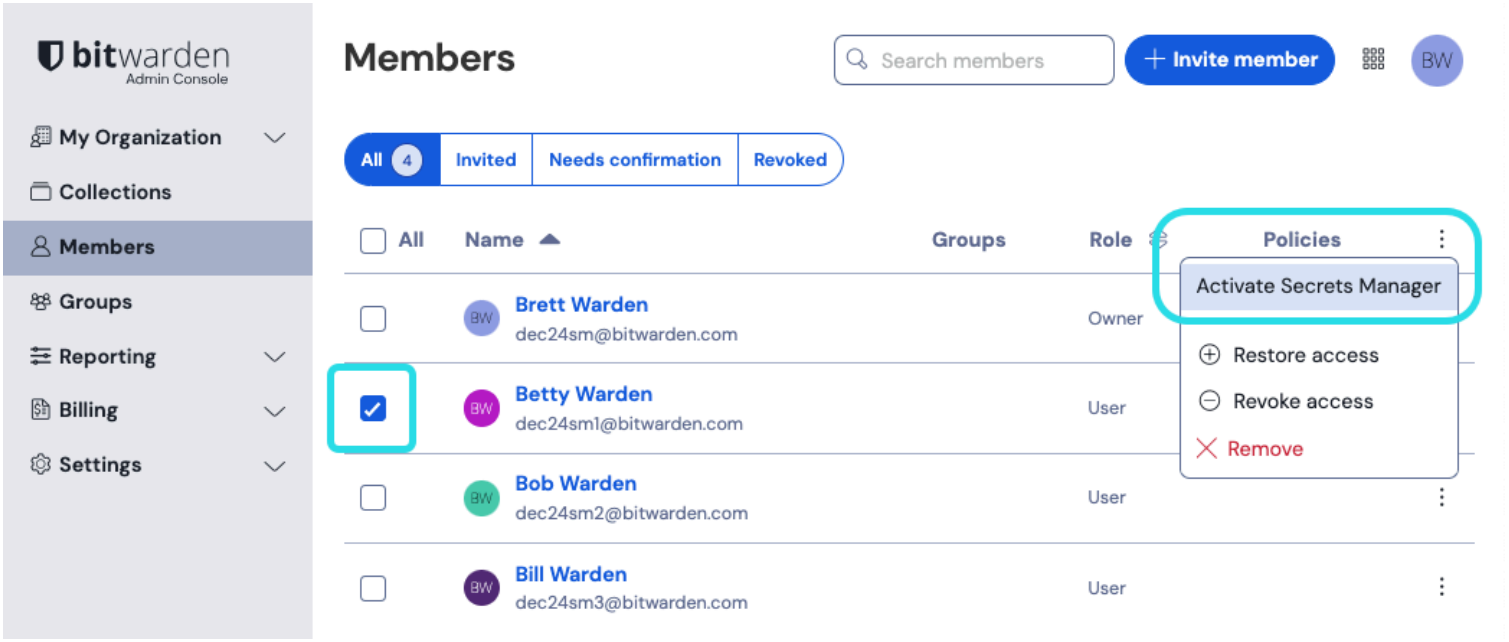
ディレクトリ-コネクタ

Directory Connectorは、選択したソースディレクトリサービスから引き出すことにより、Bitwarden組織のユーザーとグループを自動的にプロビジョニングします。この方法は、SCIMをサポートしていないディレクトリサービスを使用する大規模な組織に最適です。始め方を学びましょう。

シークレットマネージャーへのアクセス

一度オンボーディングが完了したら、組織の個々のメンバーにシークレットマネージャーへのアクセスを許可してください。

1. あなたの組織の**メンバー**表示を開き、シークレットマネージャーへのアクセスを許可したいメンバーを選択してください。
2. ⋮ メニューを使用して、選択したメンバーにアクセス権を付与するために **シークレットマネージャーを有効にする**を選択します。



シークレットマネージャーのユーザーを追加します

> **Tip**
> メンバーにシークレットマネージャーへのアクセスを与えても、自動的に保存されたプロジェクトや秘密へのアクセスが与えられるわけではありません。次に、プロジェクトへのアクセスを人々やグループに割り当てる必要があります。

メンバーの役割

次の表は、シークレットマネージャー内で各メンバーの役割が何を管理できるかを概説しています。ベータ版では、ユーザーはパスワードマネージャーで割り当てられたのと同じメンバーの役割をシークレットマネージャーに持っています。

メンバーロール	説明
ユーザー	ユーザーは自分自身のシークレット、プロジェクト、サービスアカウント、およびアクセストークンを作成することができます。これらのオブジェクトは作成後に編集することができます。 ユーザーは、既存のオブジェクトと対話するためにプロジェクトまたはサービスアカウントに割り当てられる必要があり、**読むことができる**または**読み書きができる**アクセスを与えることができます。
管理者	管理者は自動的にすべての秘密、プロジェクト、サービスアカウント、およびアクセストークンへの**読み取り、書き込み**のアクセス権を持っています。 管理者は自分自身にシークレットマネージャーへのアクセスを割り当てることができ、また他のメンバーにシークレットマネージャーへのアクセスを割り当てることもできます。
オーナー	所有者は自動的にすべての秘密、プロジェクト、サービスアカウント、およびアクセストークンへの**読み取り、書き込み**のアクセス権を持っています。 所有者は自分自身にシークレットマネージャーへのアクセスを割り当てることができ、他のメンバーにもシークレットマネージャーへのアクセスを割り当てることができます。

ⓘ Note
カスタム役割は現在、シークレットマネージャーのオプションでスコープされていませんが、特定のパスワードマネージャーまたはより広範な組織の能力を割り当てるためにまだ使用することができます。

グループ

グループは個々のメンバーを関連付け、特定のプロジェクトへのアクセスと権限をスケーラブルな方法で提供します。新しいメンバーを追加するときは、そのメンバーをグループに追加して、そのグループの設定された権限を自動的に継承させます。もっと学ぶ

管理者コンソールでグループが作成されたら、シークレットマネージャーのウェブアプリからプロジェクトにそれらを割り当ててください。

シングルサインオン(SSO)

SSOでログインするのは、Bitwardenが提供するシングルサインオンのソリューションです。SSOを使用したログインを使用すると、エンタープライズ組織は既存のIDプロバイダーを利用して、SAML 2.0またはOpen ID Connect（OIDC）プロトコルを使用してユーザーをBitwardenに認証できます。始め方を学びましょう。

アカウント回復の管理

アカウントの回復は、指定された管理者がエンタープライズ組織のユーザーアカウントを回復し、従業員がマスターパスワードを忘れた場合にアクセスを復元することを可能にします。アカウント回復は、アカウント回復管理ポリシーを有効にすることで組織で活性化することができます。始め方を学びましょう。

イベントログ

イベントログは、あなたのチームまたはエンタープライズ組織内で発生するイベントのタイムスタンプ付きレコードです。シークレットマネージャーのイベントは、組織の保管庫の**レポート → イベントログ**と、サービスアカウントのイベントログページの両方から利用できます。

イベントログはエクスポート可能で、無期限に保持されます。多くのイベントはすべてのBitwarden製品に適用され、一部はパスワードマネージャーに特化していますが、シークレットマネージャーは特に以下をログに記録します：

- サービスアカウントによってアクセスされた秘密

セルフホスティング

エンタープライズ組織は、LinuxとWindowsマシン上のDockerを使用して、自己ホスト型のBitwardenシークレットマネージャーを管理できます。あなたが以前に自己ホスト型のBitwardenを使用したことがない場合、このガイドを使用して正しい方向に進んでください。

すでにエンタープライズBitwarden組織を自己ホスト型で管理していて、そのサーバー上でシークレットマネージャーにアクセスしたい場合：

1. あなたのクラウドホストされたBitwarden組織でシークレットマネージャーのサブスクリプションにサインアップしてください。
2. 最低でも2023.10.0に自己ホスト型サーバーを更新してください。
3. クラウド ホスト型組織から新しいライセンス ファイルを取得し、セルフホスト型サーバーにアップロードします。

> **ⓘ Note**
> Bitwardenの統一自己ホスト型デプロイメントオプションでは、自己ホスト型シークレットマネージャーの管理はサポートされていません。チームとエンタープライズ組織は、標準のLinuxまたはWindowsのインストールを使用すべきです。