bitwarden | ヘルプセンターの記事

管理者コンソール > SSOでログイン >

Microsoft Entra ID SAML 実装

ヘルプセンターで表示:
https://bitwarden.com/help/saml-microsoft-entra-id/

Microsoft Entra ID SAML 実装

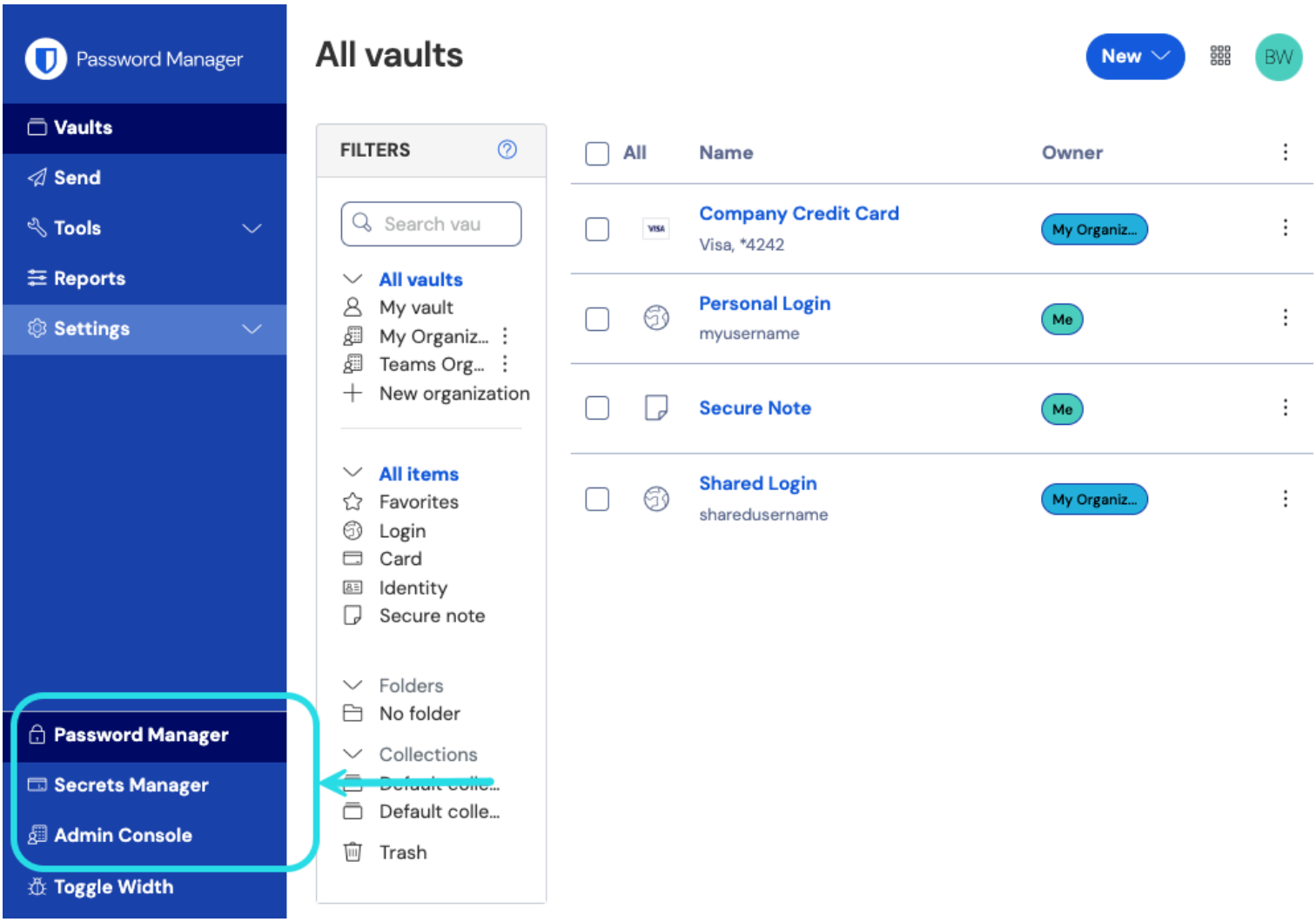
この記事には、SAML 2.0を介したSSOでのログインを設定するための**Azure特有の**ヘルプが含まれています。
別のIdPでSSOを使用したログインの設定についてのヘルプは、SAML 2.0設定を参照してください。

設定は、Bitwardenウェブアプリと Azure Portalを同時に操作することを含みます。進行するにあたり、両方をすぐに利用できる状態にして、記録されている順序で手順を完了することをお勧めします。

> **Tip**
> **すでにSSOの専門家ですか？**この記事の指示をスキップして、
> 自分の設定と比較するためのサンプル設定のスクリーンショットをダウンロードしてください。
>
> タイプ：アセット-ハイパーリンク ID：7CKe4TX98FPF86eAimKgak

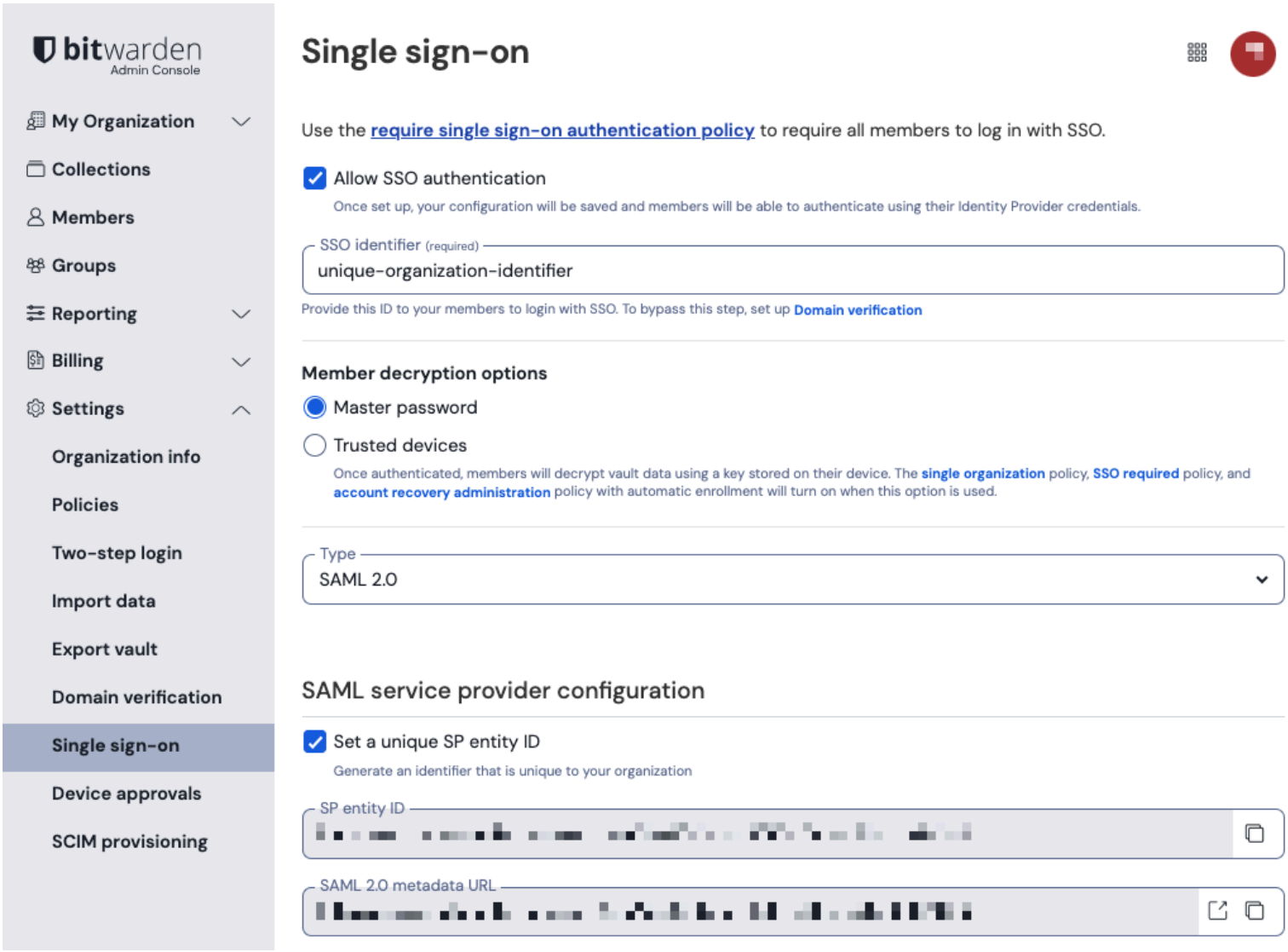
ウェブアプリでSSOを開く

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

あなたの組織の**設定** → **シングルサインオン**画面を開きます：



SAML 2.0設定

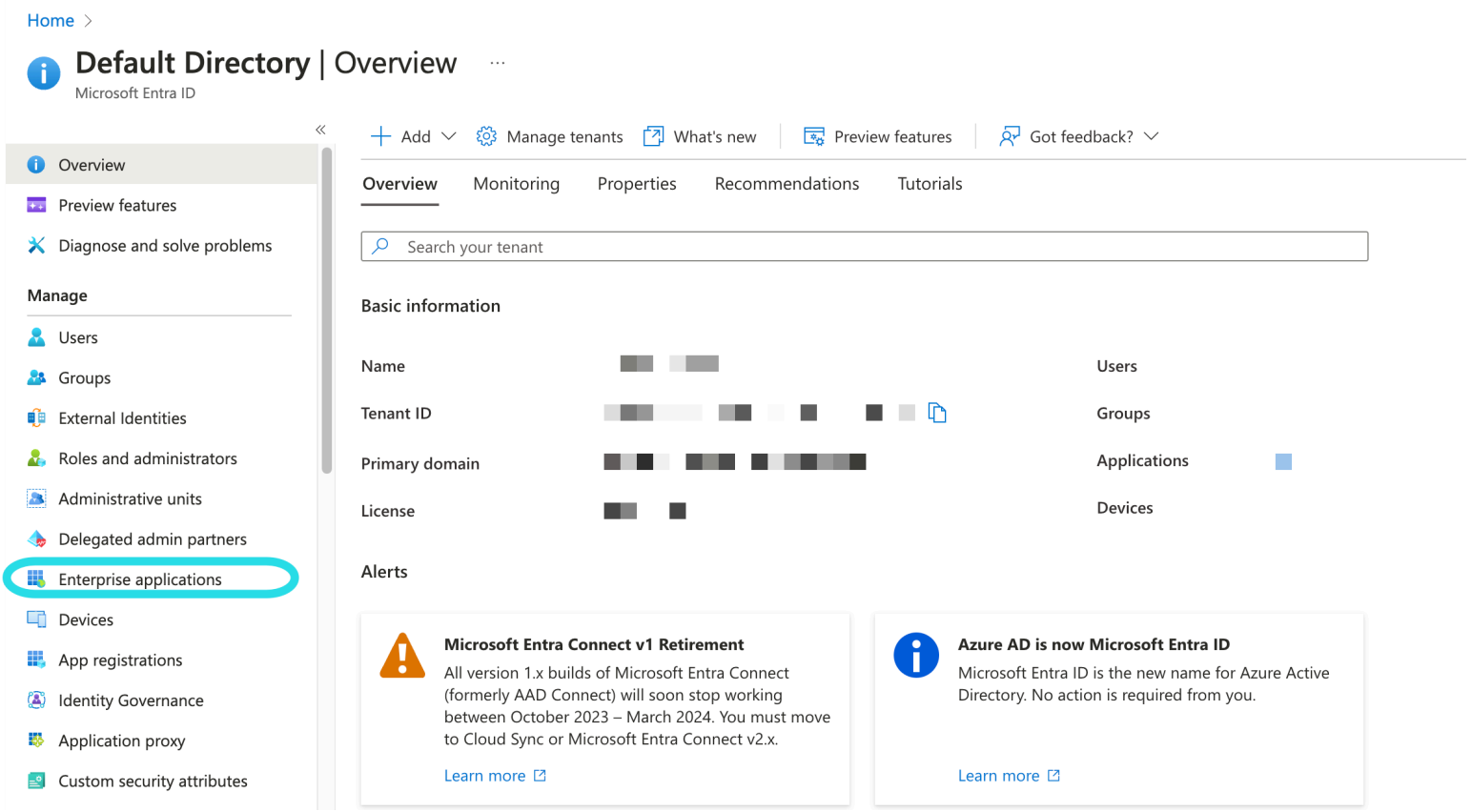
まだ作成していない場合は、あなたの**SSO識別子**を組織用に作成し、**タイプ**のドロップダウンから**SAML**を選択してください。
この画面を開いたままにして、簡単に参照できるようにしてください。

この段階で、必要であれば**ユニークなSPエンティティIDを設定する**オプションをオフにすることができます。これを行うと、
組電IDがSPエンティティID値から削除されますが、ほとんどの場合、このオプションをオンにしておくことをお勧めします。

> **Tip**
> 代替の**メンバー復号化オプション**があります。信頼できるデバイスでのSSOの使い方またはキーコネクターの使い方を学びましょう。

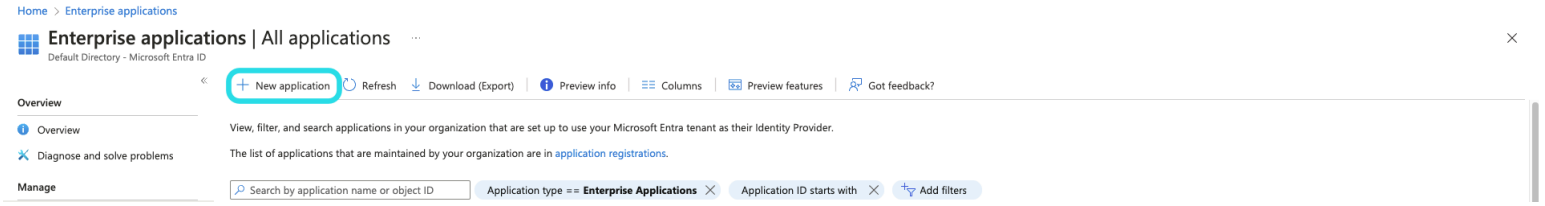
エンタープライズアプリケーションを作成する

Azure Portalで、**Microsoft Entra ID**に移動し、ナビゲーションメニューから**エンタープライズアプリケーション**を選択します:



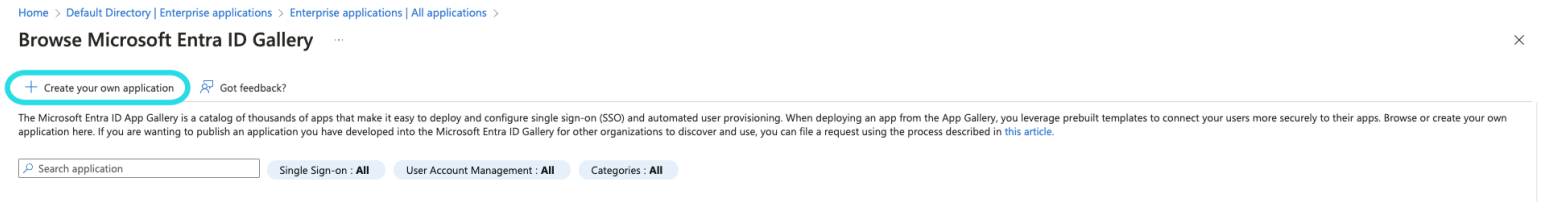
Enterprise applications

＋ **新しいアプリケーション** ボタンを選択してください:



Create new application

Microsoft Entra IDギャラリー画面で、＋ **あなた自身のアプリケーションを作成する**ボタンを選択します:

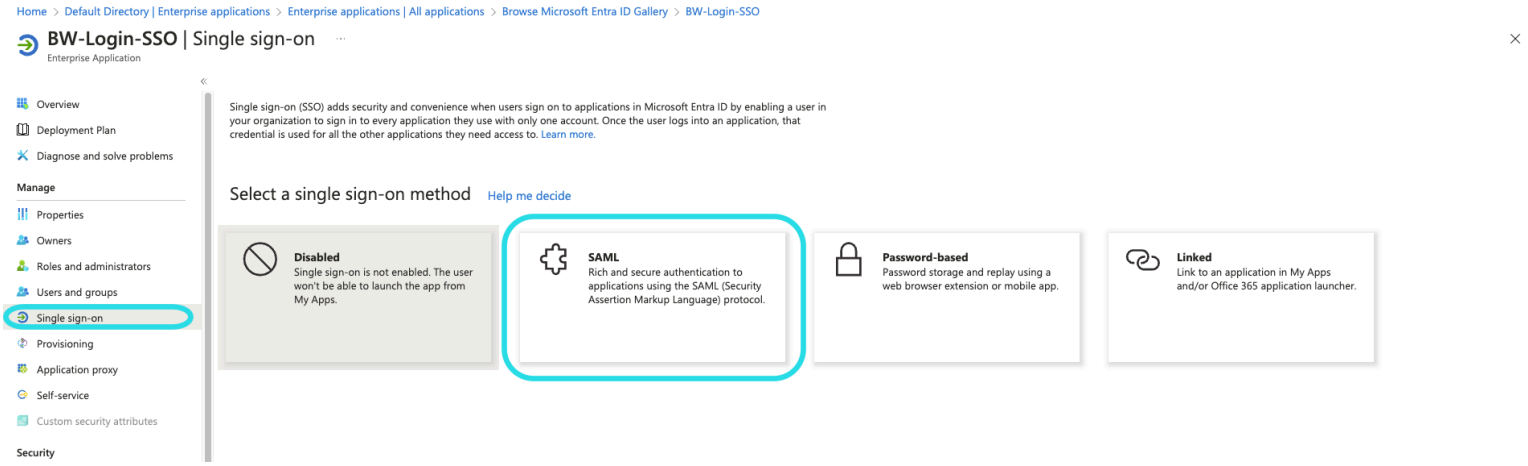


Create your own application

あなた自身のアプリケーションを作成する画面で、アプリケーションにユニークでBitwarden特有の名前を付け、（ギャラリー以外）のオプションを選択してください。終了したら、**作成**ボタンをクリックしてください。

シングルサインオンを有効にする

アプリケーション概要画面から、ナビゲーションから**シングルサインオン**を選択してください。



Configure Single sign-on

シングルサインオン画面で、**SAML**を選択してください。

SAML設定

基本的なSAML設定

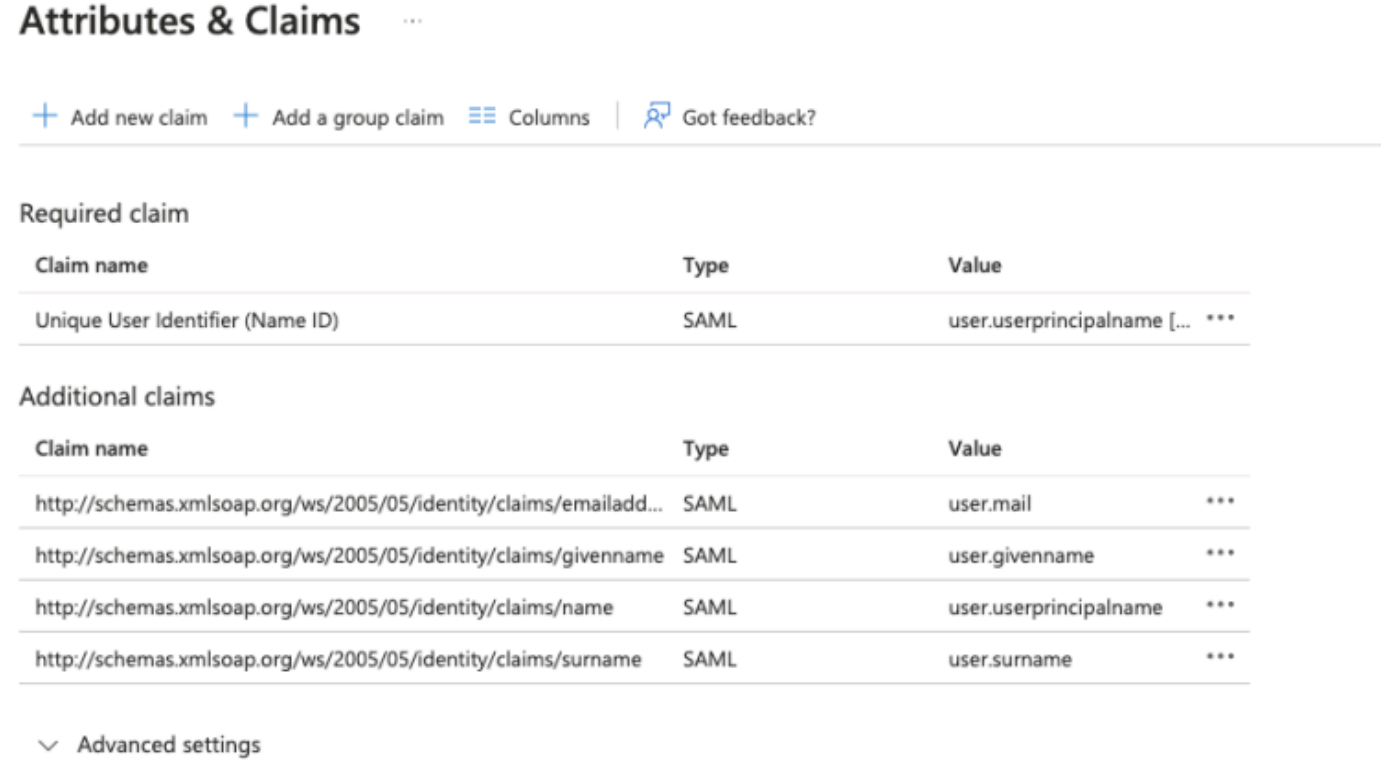
編集ボタンを選択し、次のフィールドを設定してください：

フィールド	説明
識別子（エンティティID）	このフィールドを事前に生成された**SPエンティティID**に設定します。 この自動生成された値は、組織の**設定 → シングルサインオン**画面からコピーでき、設定により異なります。
返信URL （アサーション消費者サービスURL）	このフィールドを事前に生成された**Assertion Consumer Service (ACS) URL**に設定します。 この自動生成された値は、組織の**設定→シングルサインオン**画面からコピーでき、設定により異なります。
URLにサインイン	このフィールドを、ユーザーがBitwardenにアクセスするためのログインURLに設定してください。 クラウドホストのお客様の場合、これは`https://vault.bitwarden.com/#/sso`または`https://vault.bitwarden.eu/#/sso`です。自己ホスト型のインスタンスの場合、これはあなたが設定したサーバーURLによって決まります。例えば、`https://your-domain.com/#/sso`などです。

ユーザー属性＆クレーム

Azureによって構築されるデフォルトのクレームは、SSOでのログインで動作しますが、必要に応じてこのセクションを使用して、AzureがSAMLレスポンスで使用するNameIDフォーマットを設定することができます。

編集ボタンを選択し、**ユニークユーザー識別子（名前ID）**エントリを選択してNameIDクレームを編集します：



NameID請求の編集

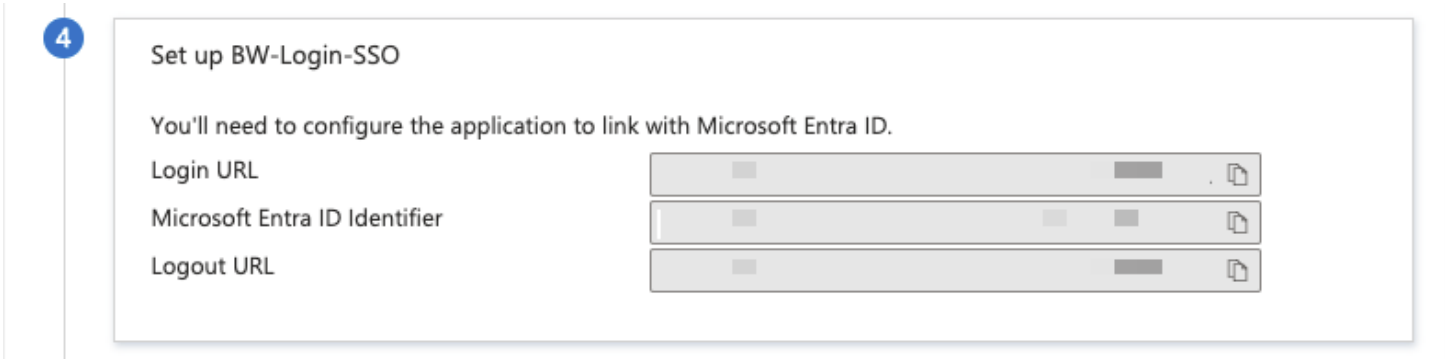
オプションには、デフォルト、メールアドレス、永続的、未指定、およびWindowsの資格付けられたドメイン名が含まれます。詳細については、Microsoft Azureのドキュメンテーションを参照してください。

SAML署名証明書

後のステップで使用するために、Base64証明書をダウンロードしてください。後のステップで。

あなたのアプリケーションを設定してください。

このセクションの**ログインURL**と**Microsoft Entra ID識別子**をコピーまたはメモして、後のステップで使用してください：

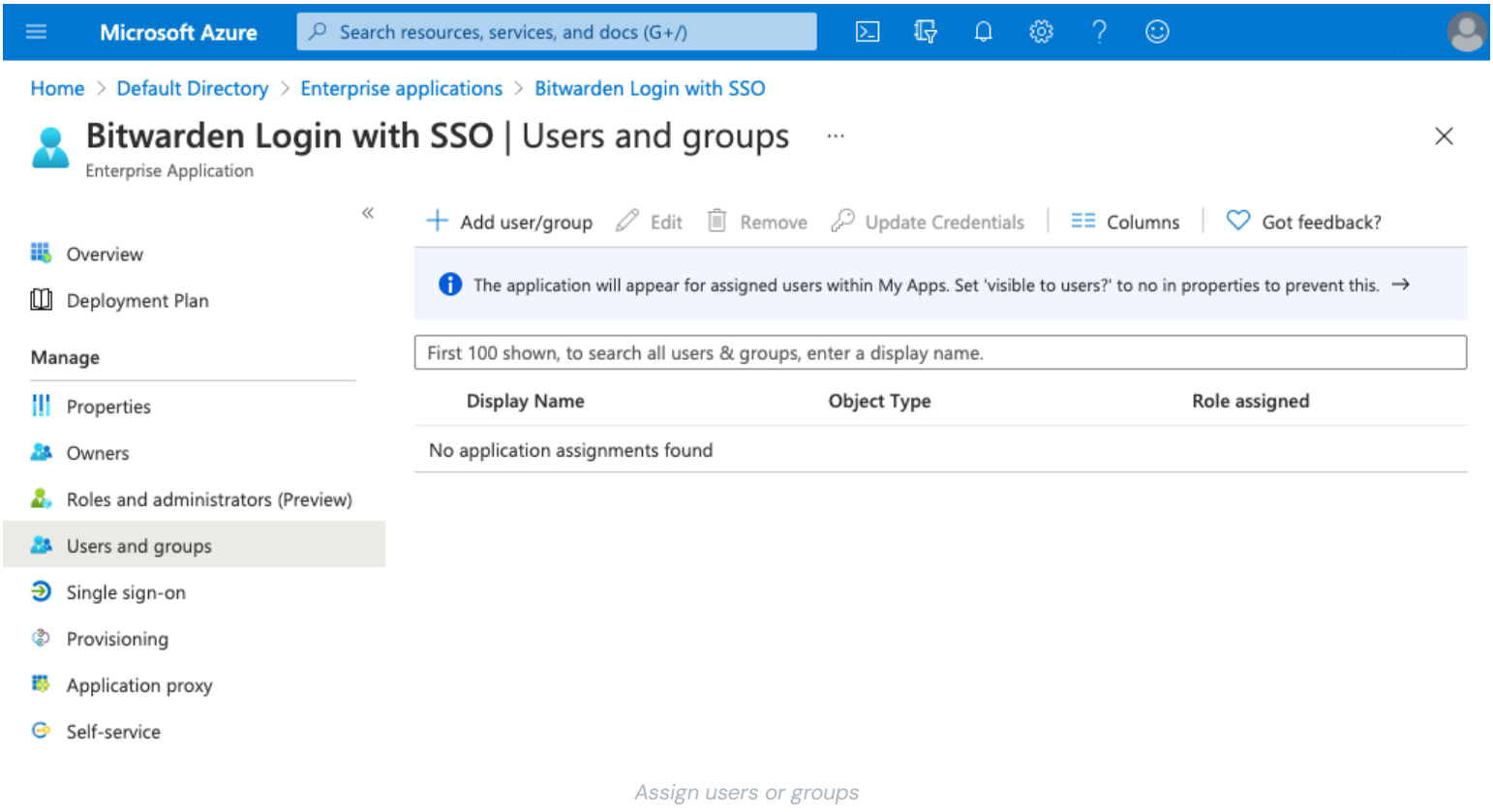


Azure URLs

> **Note**
> If you receive any key errors when logging in via SSO, try copying the X509 certificate information from the Federation Metadata XML file instead.

ユーザーとグループ

ナビゲーションから**ユーザーとグループ**を選択してください。



ユーザーまたはグループレベルでSSOアプリケーションへのログインアクセスを割り当てるには、**ユーザー/グループを追加**ボタンを選択してください。

ウェブアプリに戻る

この時点で、Azure Portalのコンテキスト内で必要なすべてを設定しました。設定を完了するためにBitwardenウェブアプリに戻ってください。

シングルサインオン画面は、設定を2つのセクションに分けています：

- **SAML サービス プロバイダーの構成によって、** SAML リクエストの形式が決まります。
- **SAML IDプロバイダーの設定**は、SAMLのレスポンスで期待する形式を決定します。

サービスプロバイダーの設定

次のフィールドを設定してください:

フィールド	説明
名前ID形式	デフォルトでは、Azureはメールアドレスを使用します。あなたがこの設定を変更した場合、対応する値を選択してください。それ以外の場合は、このフィールドを**未指定**または**メールアドレス**に設定します。

フィールド	説明
アウトバウンド署名アルゴリズム	BitwardenがSAMLリクエストに署名するために使用するアルゴリズム。
署名行動	SAMLリクエストが署名されるかどうか/いつ署名されるか。
最小入力署名アルゴリズム	デフォルトでは、AzureはRSA SHA-256で署名します。ドロップダウンから`rsa-sha256`を選択してください。
署名されたアサーションが欲しい	BitwardenがSAMLアサーションに署名が必要かどうか。
証明書を検証する	あなたのIdPから信頼できるCAを通じて信頼性のある有効な証明書を使用するときは、このボックスをチェックしてください。自己署名証明書は、適切な信頼チェーンがBitwardenログインのSSO Dockerイメージと一緒に設定されていない限り、失敗する可能性があります。

サービスプロバイダーの設定が完了したら、作業を**保存**してください。

IDプロバイダーの設定

IDプロバイダーの設定では、アプリケーションの値を取得するために、しばしばAzure Portalを参照する必要があります。

フィールド	説明
エンティティID	Azure Portalの**アプリケーションの設定**セクションから取得した、あなたのMicrosoft Entra ID識別子を入力してください。このフィールドは大文字と小文字を区別します。
バインディングタイプ	**HTTP POST** または**リダイレクト**に設定します。
シングルサインオンサービスURL	Azure Portalの**アプリケーションの設定**セクションから取得したログインURLを入力してください。
シングルログアウトサービスURL	現在、SSOでのログインはSLOを**サポートしていません。** このオプションは将来の開発のために計画されていますが、 ご希望であれば**ログアウトURL**で事前に設定することができます。
X509公開証明書	ダウンロードした証明書を貼り付け、削除します `-----BEGIN CERTIFICATE-----` そして

フィールド	説明
	-----証明書終了----- 証明書の値は大文字と小文字を区別し、余分なスペース、キャリッジリターン、 その他の余分な文字**は証明書の検証に失敗する原因となります**。
アウトバウンド署名アルゴリズム	デフォルトでは、AzureはRSA SHA-256で署名します。ドロップダウンから`rsa-sha256` を選択してください。
アウトバウンドログアウトリクエストを無効にする	現在、SSOでの**ログインは**SLOをサポートしていません。 このオプションは将来の開発のために計画されています。
認証リクエストに署名が必要です	AzureがSAMLリクエストの署名を期待しているかどうか。

Note

X509証明書を完成させるとき、有効期限の日付をメモしてください。SSOエンドユーザーへのサービスの中断を防ぐために、
証明書を更新する必要があります。証明書が期限切れになった場合でも、
管理者と所有者のアカウントは常にメールアドレスとマスターパスワードでログインできます。

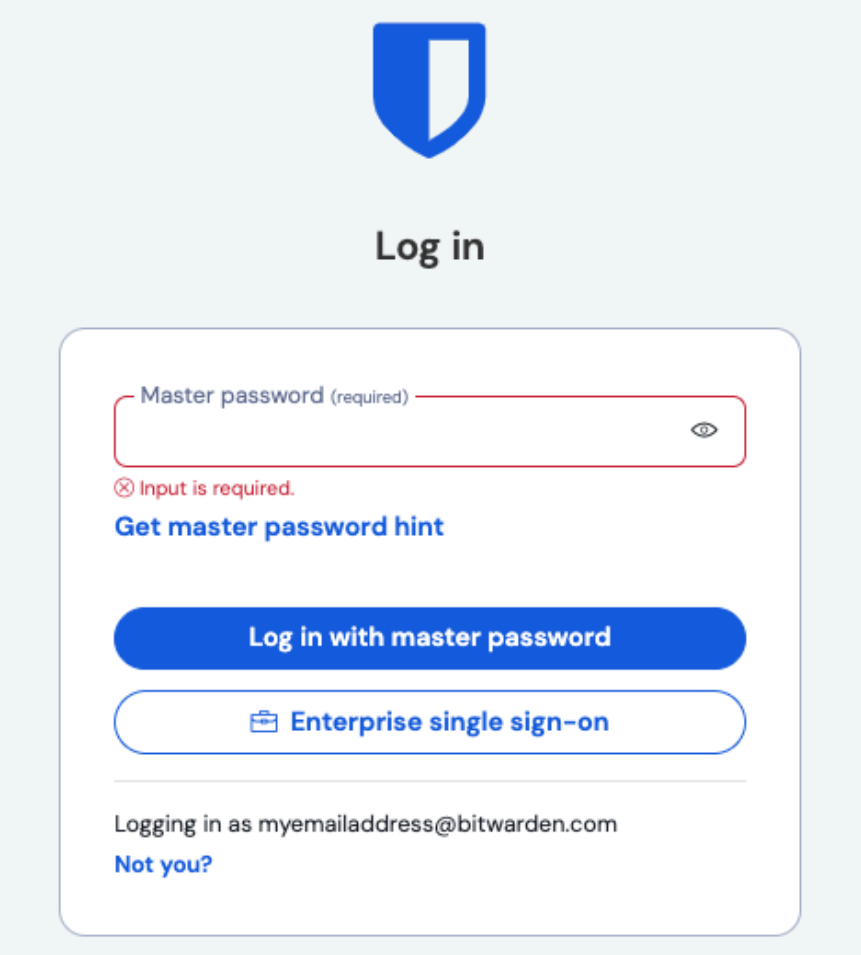
IDプロバイダーの設定が完了したら、**保存**してください。

Tip

シングルサインオン認証ポリシーを有効にすることで、ユーザーにSSOでログインすることを要求することができます。メモしてください、
これは単一の組織ポリシーも同時に活性化する必要があります。もっと学ぶ

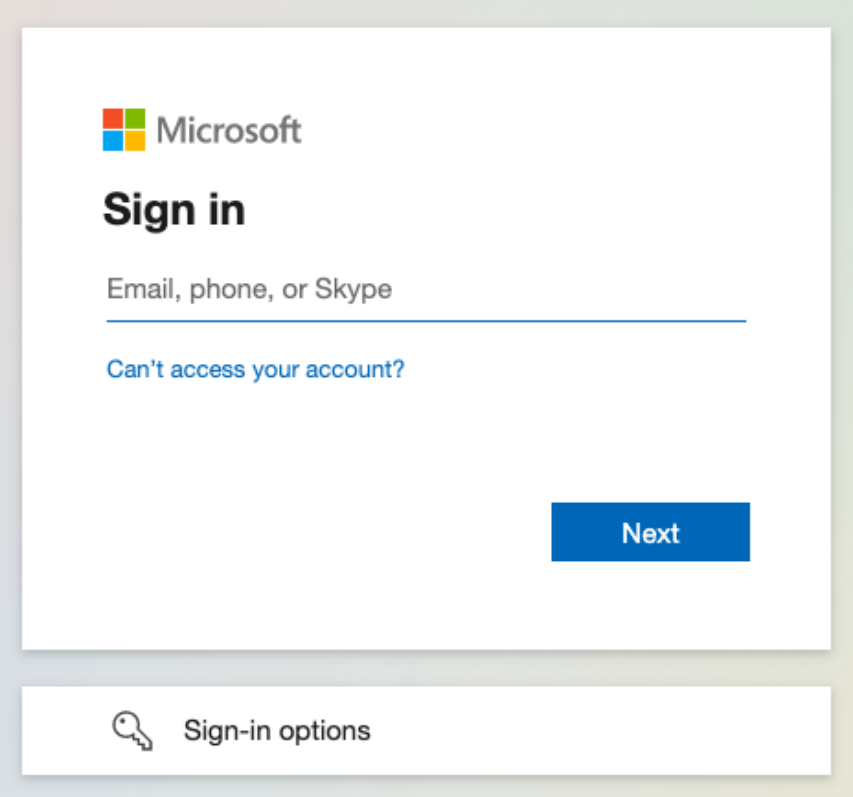
設定をテストする

設定が完了したら、https://vault.bitwarden.comに移動して、メールアドレスを入力し、**続行**を選択し、
エンタープライズシングルオンボタンを選択してテストしてください。



エンタープライズシングルサインオンとマスターパスワード

設定された組織識別子を入力し、**ログイン**を選択してください。あなたの実装が正常に設定されている場合、Microsoftのログイン画面にリダイレクトされます。



Azure login screen

あなたのAzureの認証情報で認証した後、Bitwardenのマスターパスワードを入力して保管庫を復号化してください！

> **ⓘ Note**
> Bitwardenは勝手なレスポンスをサポートしていませんので、あなたのIdPからログインを開始するとエラーが発生します。
> SSOログインフローはBitwardenから開始されなければなりません。Azure SAML管理者は、
> ユーザーがBitwardenウェブ保管庫ログインページに誘導されるようにアプリ登録を設定することができます。
>
> 1. 既存のBitwardenボタンを無効にするには、**すべてのアプリケーション**ページで現在のBitwardenエンタープライズアプリケーションに移動し、プロパティを選択し、**ユーザーに表示**オプションを**いいえ**に設定します。
> 2. **アプリ登録**に移動して、**新規登録**を選択することでアプリ登録を作成します。
> 3. アプリケーションに名前を付けてください。例えば、**Bitwarden SSO**など。リダイレクトURLを指定しないでください。
>   フォーラムを完了するには、**登録**を選択してください。
> 4. アプリが作成されたら、ナビゲーションメニューにある**ブランディング＆プロパティ**に移動します。
> 5. 次の設定をアプリケーションに追加してください：
>   1. エンドユーザーの認識のためにロゴをアップロードしてください。Bitwardenのロゴはここから取得できます。
>   2. **ホームページのURL**をあなたのBitwardenクライアントログインページ、例えば`https://vault.bitwarden.com/#/login`または`your-self-hostedURL.com`に設定します。
>
> このプロセスが完了すると、指定されたユーザーはBitwardenアプリケーションを持つことになり、
> それによりユーザーは直接Bitwardenのウェブ保管庫ログインページにリンクされます。