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 ›

JumpCloud SAML 実装

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

JumpCloud SAML 実装

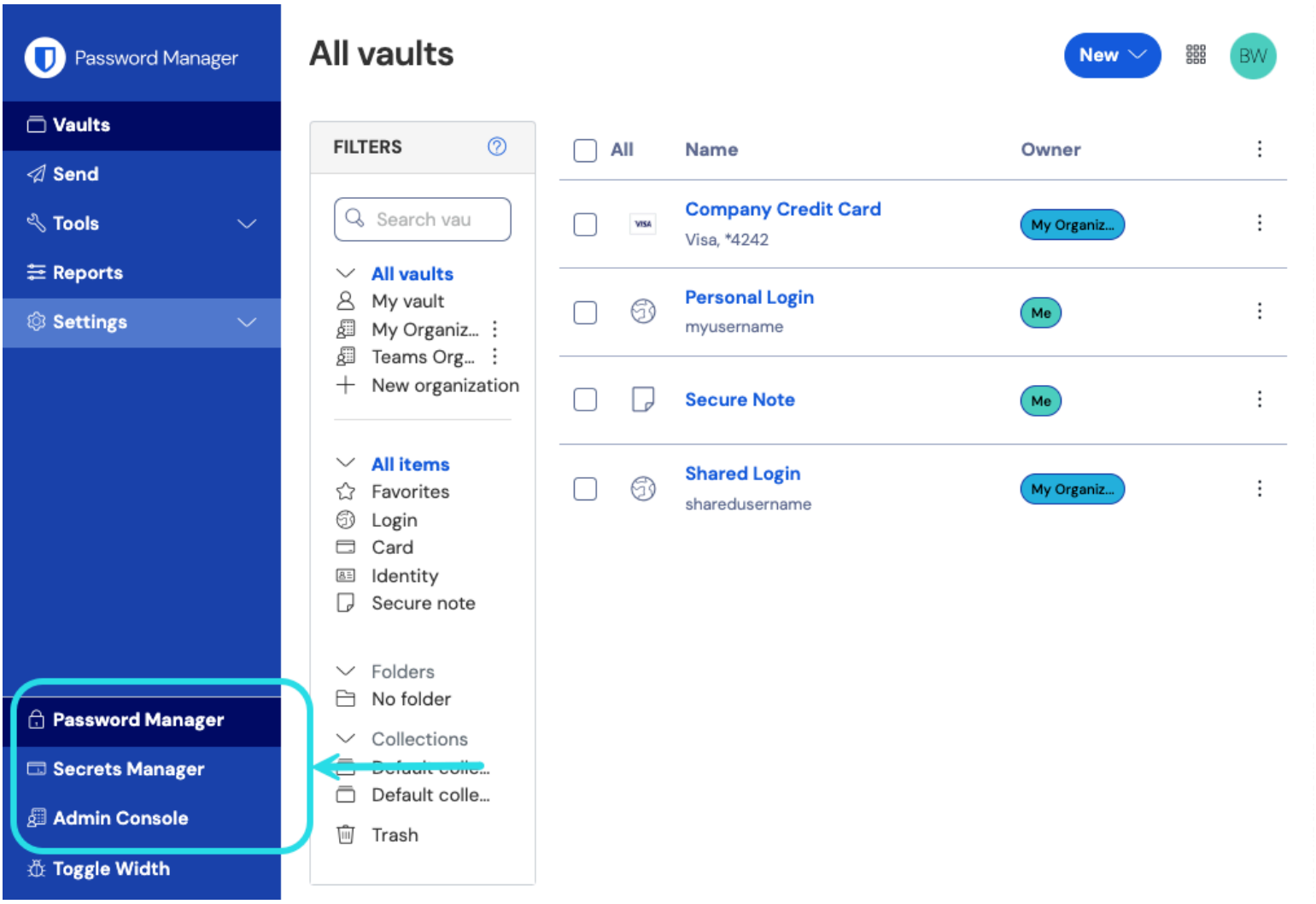
この記事には、SAML 2.0を介したSSOでのログインを設定するための**JumpCloud特有の**ヘルプが含まれています。
別のIdPでSSOを使用したログインの設定についてのヘルプは、SAML 2.0設定を参照してください。

設定は、Bitwardenウェブアプリと JumpCloudポータルの両方で同時に作業を行うことを含みます。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**
>
> **Already an SSO expert?** Skip the instructions in this article and download screenshots of sample configurations to compare against your own.
>
> Download Sample

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

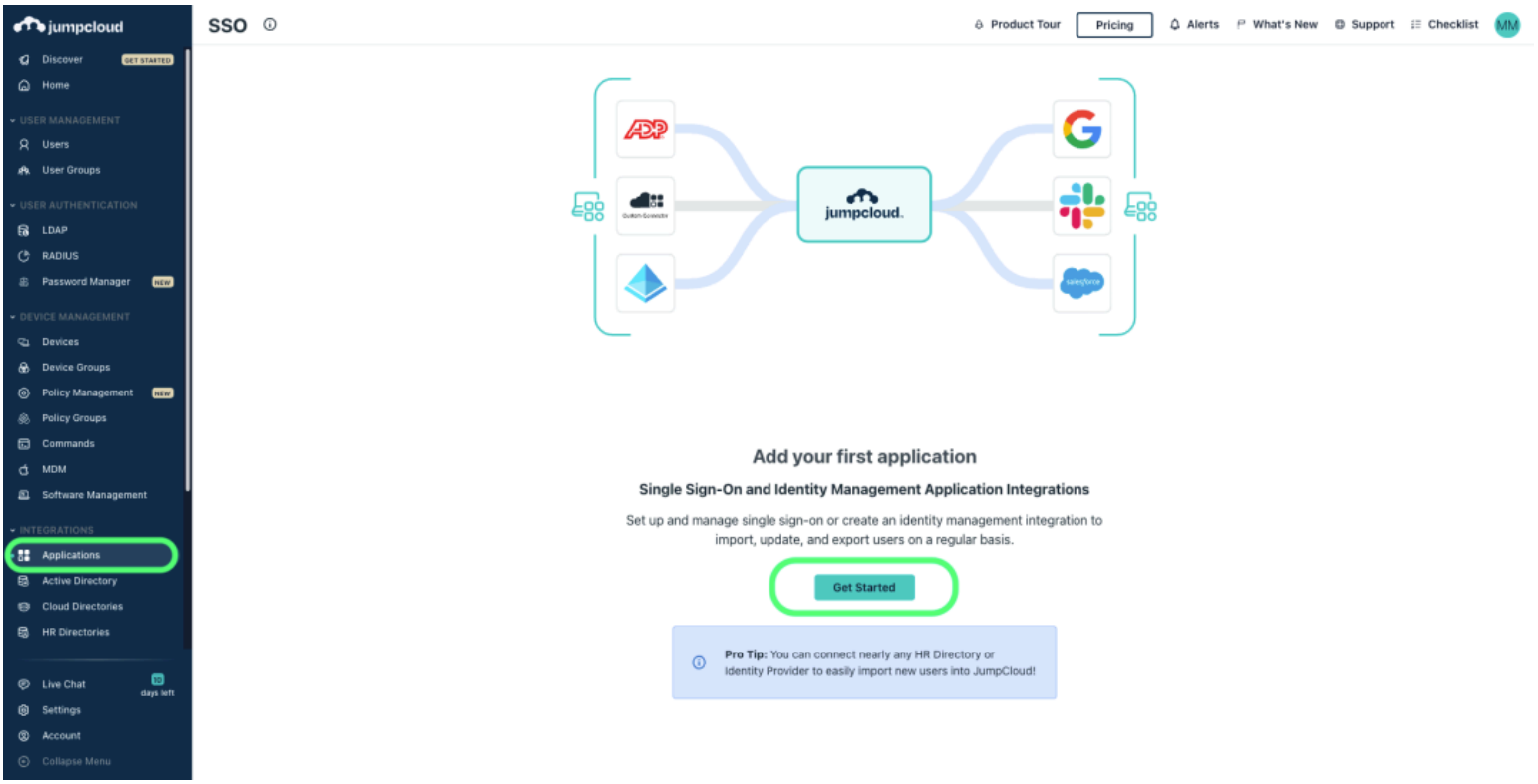
まだ作成していない場合は、あなたの**SSO識別子**を組織用に作成し、**タイプ**のドロップダウンから**SAML**を選択してください。
この画面を開いたままにして、簡単に参照できるようにしてください。

この段階で、必要に応じて**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、ほとんどの場合では、このオプションをオンにしておくことを推奨します。

> **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。

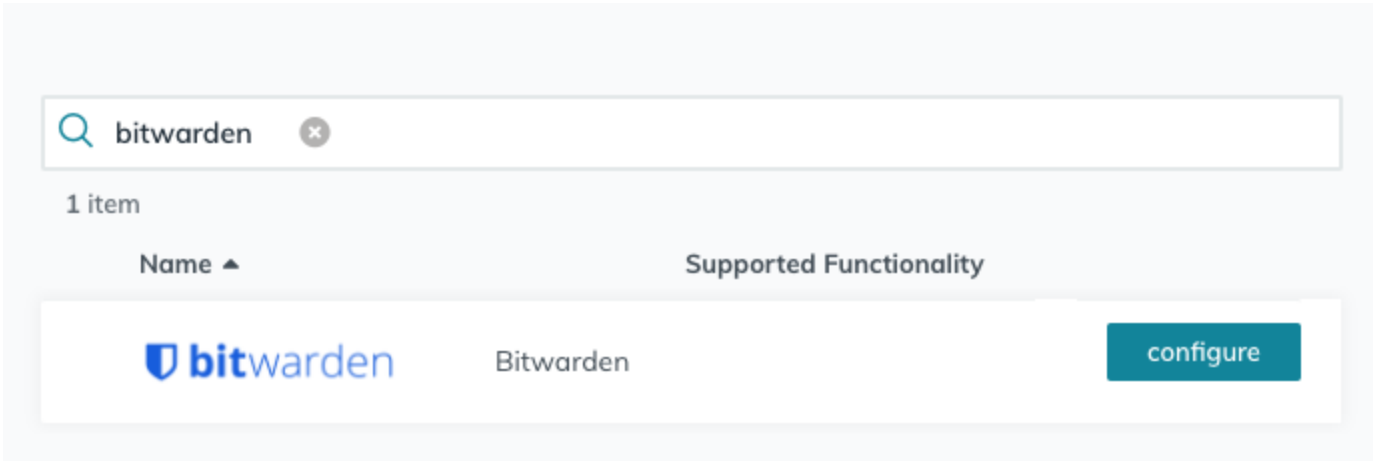
JumpCloud SAMLアプリケーションを作成する

JumpCloudポータルで、メニューから**アプリケーション**を選択し、**開始**ボタンを選択します：



Create Bitwarden app Jumpcloud

検索ボックスに`Bitwarden`を入力し、**設定**ボタンを選択します:



Configure Bitwarden

> **Tip**
>
> If you are more comfortable with SAML, or want more control over things like NameID Format and Signing Algorithms, create a **Custom SAML Application** instead.

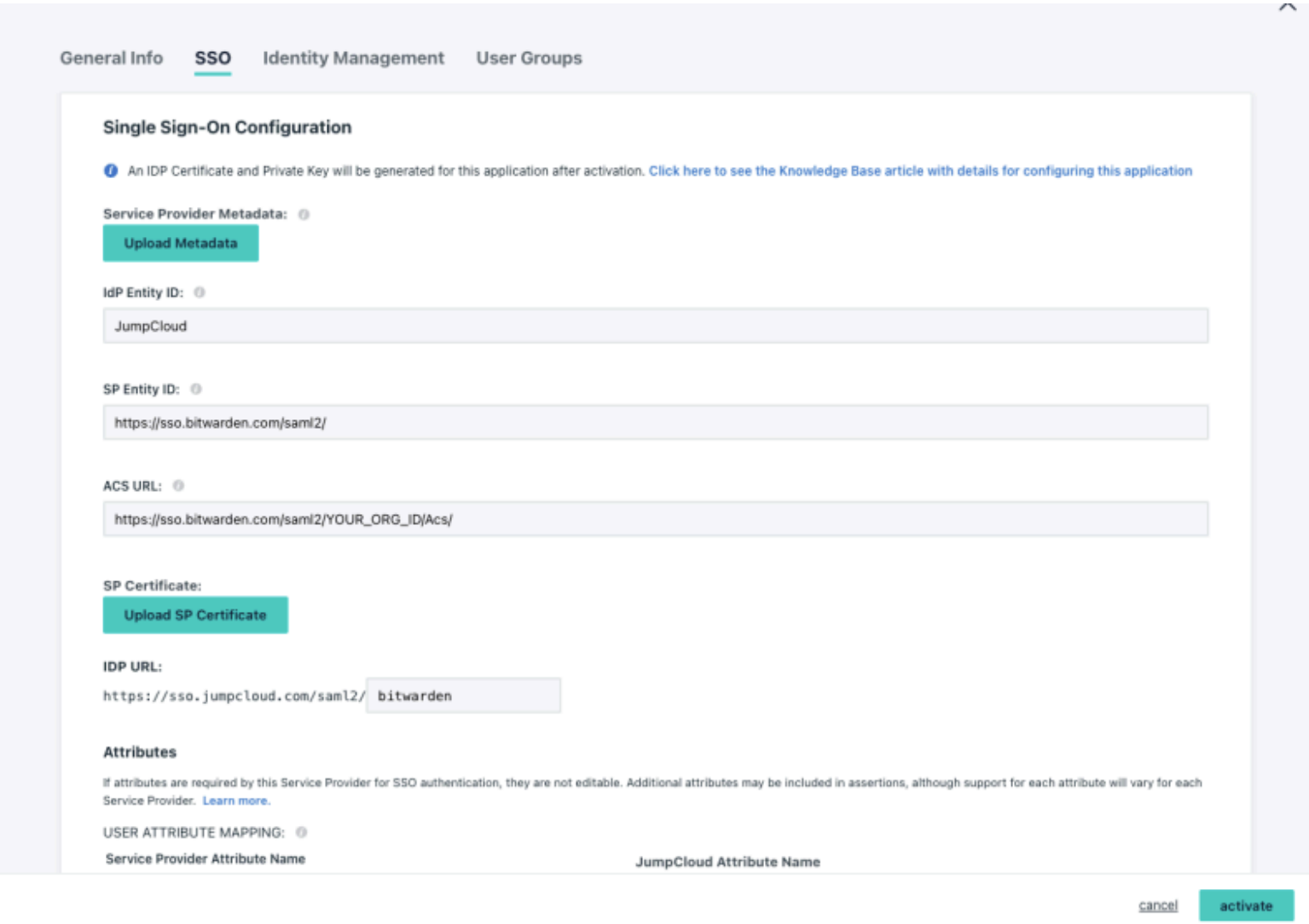
一般情報

「**一般情報**」セクションで、以下の情報を設定してください：

フィールド	説明
ディスプレイラベル	アプリケーションにBitwarden特有の名前を付けてください。

シングルサインオン設定

シングルサインオン設定セクションで、以下の情報を設定します：



Jumpcloud SSO configuration

フィールド	説明
IdPエンティティID	このフィールドを一意で、Bitwarden特有の値に設定します。例えば、`bitwardensso_yourcompany`。
SP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。
ACS URL	このフィールドを事前に生成された**アサーションコンシューマーサービス(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。

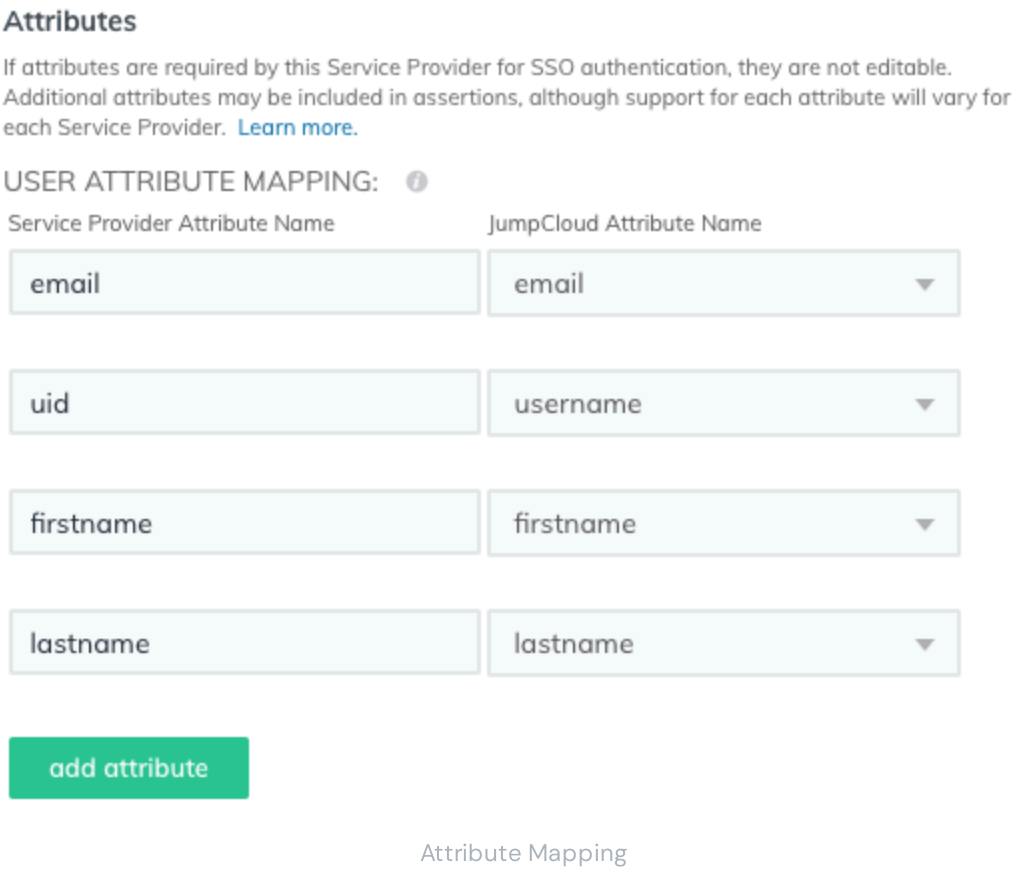
カスタムSAMLアプリのみ

カスタムSAMLアプリケーションを作成した場合、次の**シングルサインオン設定**フィールドも設定する必要があります：

フィールド	説明
SAMLSubject NameID	JumpCloud属性を指定してください。これはSAMLレスポンスでNameIDとして送信されます。
SAMLSubject NameID形式	SAMLレスポンスで送信されるNameIDの形式を指定してください。
署名アルゴリズム	SAMLアサーションまたはレスポンスに署名するためのアルゴリズムを選択してください。
サインの主張	デフォルトでは、JumpCloudはSAMLレスポンスに署名します。このボックスをチェックして、SAMLアサーションに署名してください。
ログインURL	あなたのユーザーがSSO経由でBitwardenにログインするURLを指定してください。 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、これはあなたの設定されたサーバーURLによって決定されます。例えば、`https://your.domain.com/#/sso`などです。

属性

シングルサインオン設定 → **属性**セクションで、次のSP → IdP属性マッピングを構築します。
JumpCloudでBitwardenアプリケーションを選択した場合、これらはすでに構築されているはずです：

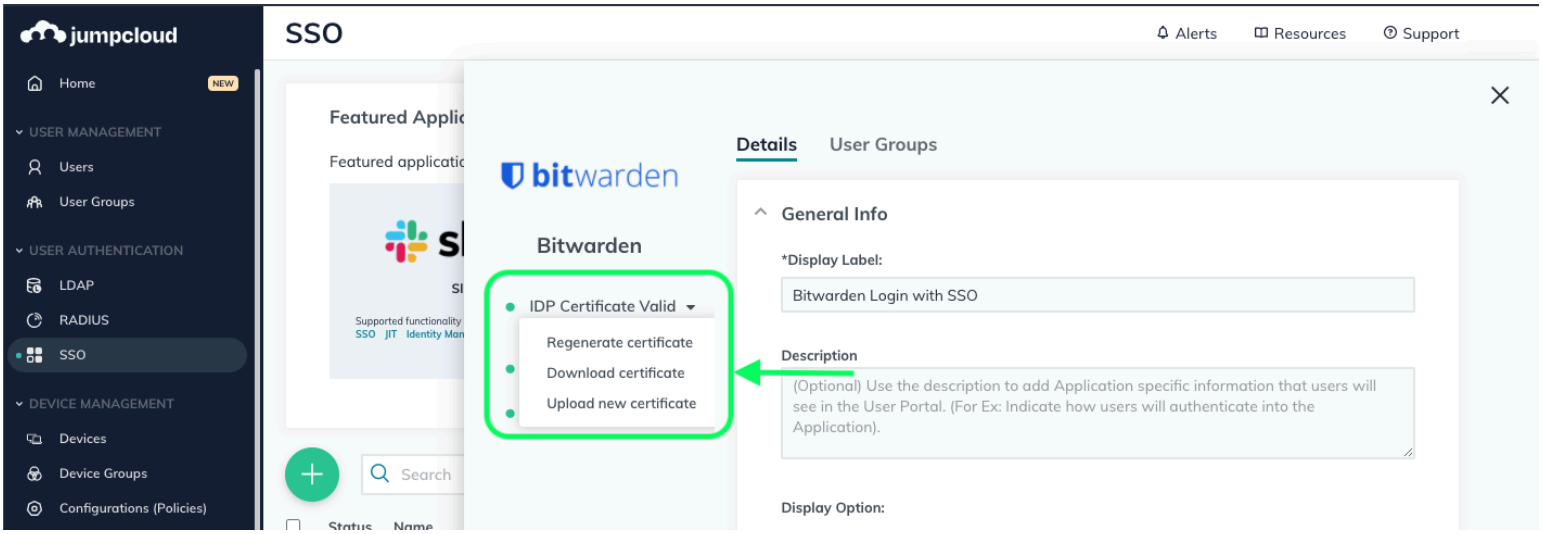


Attribute Mapping

終了したら、**アクティベート**ボタンを選択してください。

証明書をダウンロードしてください

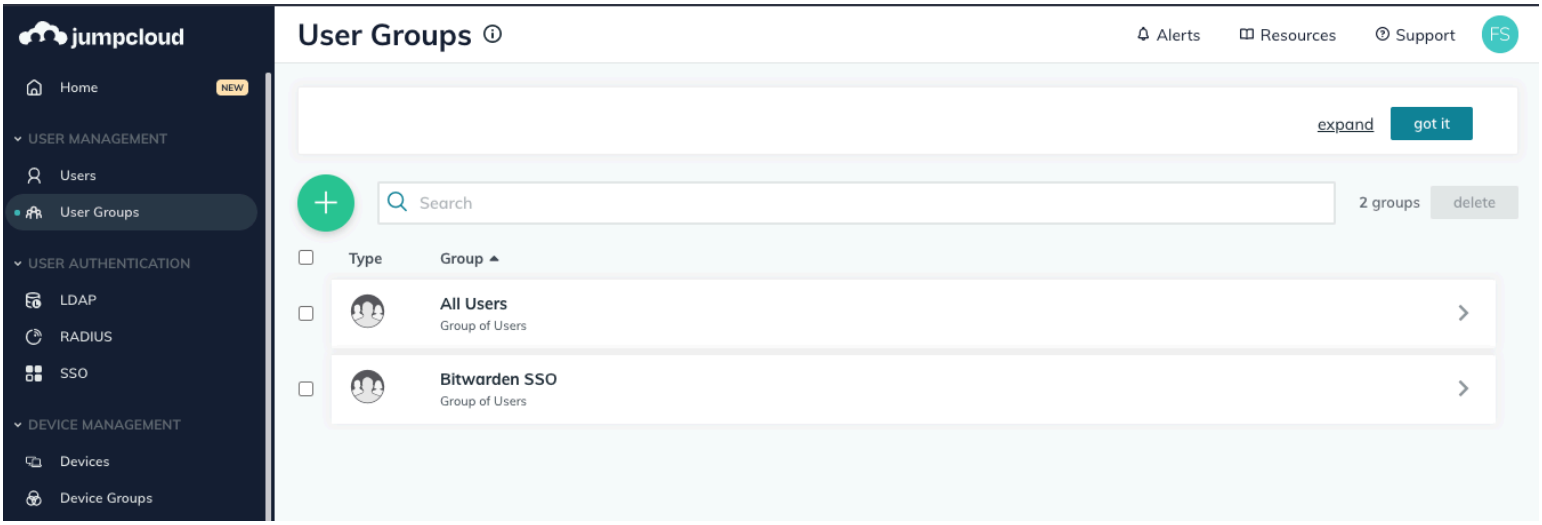
アプリケーションが有効化されたら、作成されたBitwardenアプリケーションを開くために再度**SSO**メニューオプションを使用してください。**IDP証明書**のドロップダウンを選択し、**証明書をダウンロード**します。



Download Certificate

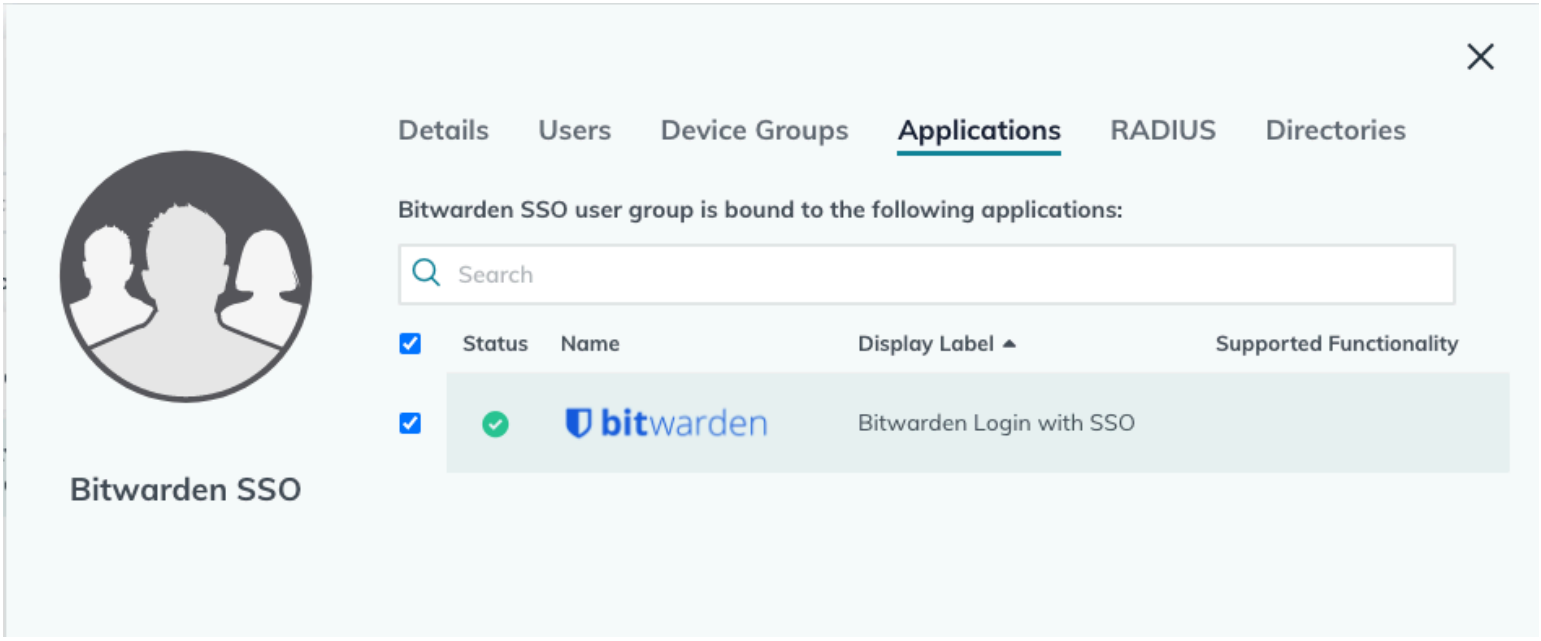
ユーザーグループをバインドする

JumpCloudポータルで、メニューから**ユーザーグループ**を選択します。



User Groups

Bitwarden専用のユーザーグループを作成するか、またはすべてのユーザーのデフォルトユーザーグループを開きます。いずれの場合でも、**アプリケーション**タブを選択し、そのユーザーグループの作成したBitwarden SSOアプリケーションへのアクセスを有効にします:



Bind App Access

> **Tip**
> Alternatively, you can bind access to user groups directly from the **SSO → Bitwarden Application** screen.

ウェブアプリに戻る

この時点で、JumpCloudポータル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のウェブ保管庫に戻ってください。

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、JumpCloud Portalでアプリ作成中に選択した選択肢に従って設定します：

フィールド	説明
名前ID形式	カスタムSAMLアプリケーションを作成した場合、これを指定されたSAMLSubject NameIDフォーマットに設定します。それ以外の場合は、**未指定**にしてください。
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。

フィールド	説明
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。デフォルトでは、JumpCloudはリクエストの署名を必要としません。
最小入力署名アルゴリズム	カスタムSAMLアプリケーションを作成した場合、選択した署名アルゴリズムにこれを設定してください。それ以外の場合は、`rsa-sha256`のままにしてください。
署名付きのアサーションが欲しい	カスタムSAMLアプリケーションを作成した場合、JumpCloudの**Sign Assertion**オプションを設定した場合は、このボックスをチェックしてください。それ以外の場合は、チェックを外してください。
証明書を検証する	あなたのIdPから信頼できるCAを通じて信頼性と有効性のある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イメージ内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JumpCloudポータル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	JumpCloudの**IdPエンティティID**を入力してください。これはJumpCloudのシングルサインオン設定画面から取得できます。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	**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	JumpCloudの**IdP URL**を入力してください。これはJumpCloudのシングルサインオン設定画面から取得できます。

フィールド	説明
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。

X509公開証明書	取得した証明書を貼り付け、削除してください。
	
	`-----BEGIN CERTIFICATE-----`
	
	そして
	
	`-----証明書の終わり-----`
	
	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**は認証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	カスタムSAMLアプリケーションを作成した場合、 選択した署名アルゴリズムにこれを設定してください。それ以外の場合は、`rsa-sha256`のままにしてください。
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を希望します	JumpCloudがSAMLリクエストの署名を期待しているかどうか。

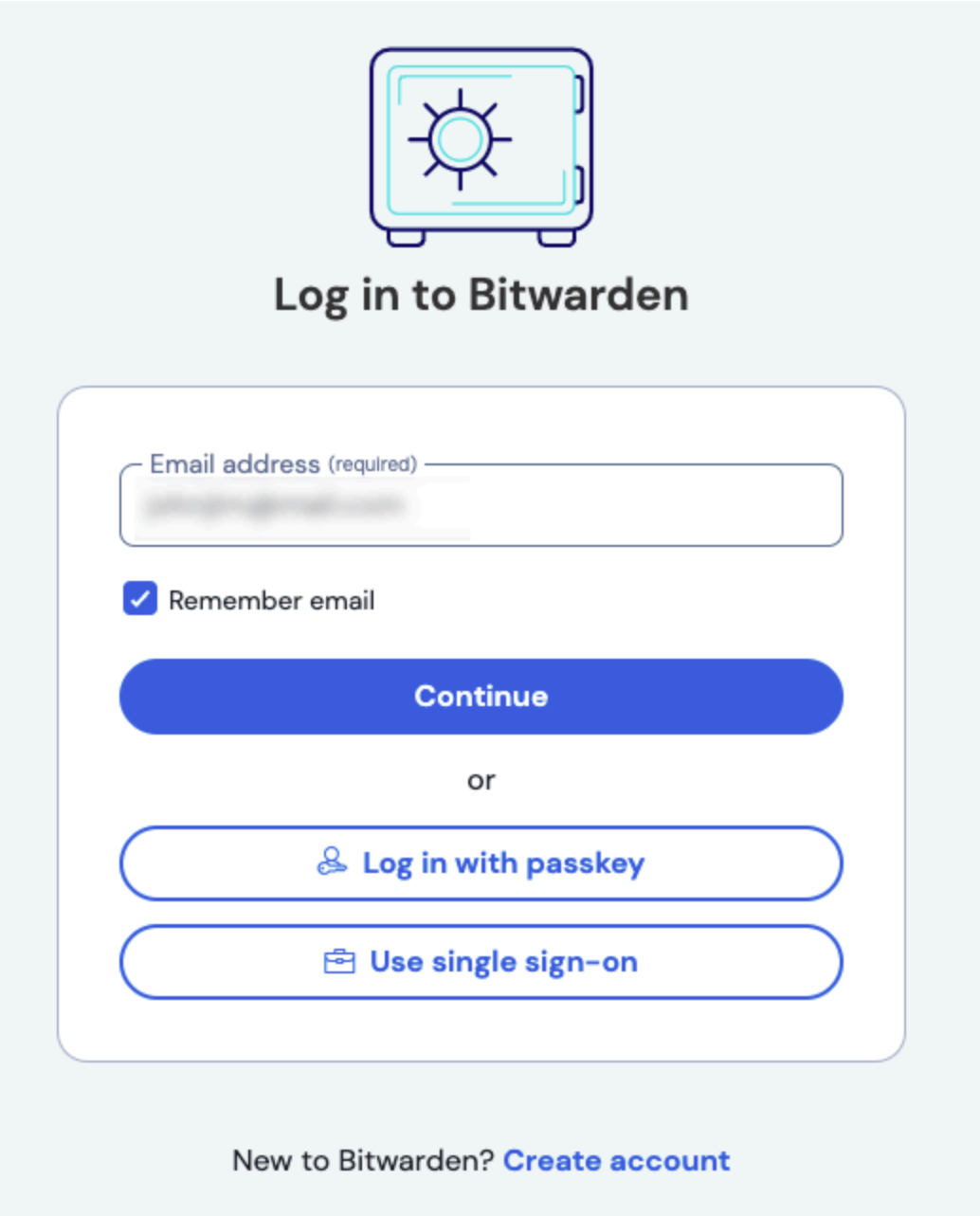
Note
X509証明書を完成させるとき、有効期限の日付をメモしてください。SSOエンドユーザーへのサービスの中断を防ぐために、
証明書を更新する必要があります。証明書が期限切れになった場合でも、
管理者と所有者のアカウントは常にメールアドレスとマスターパスワードでログインできます。

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

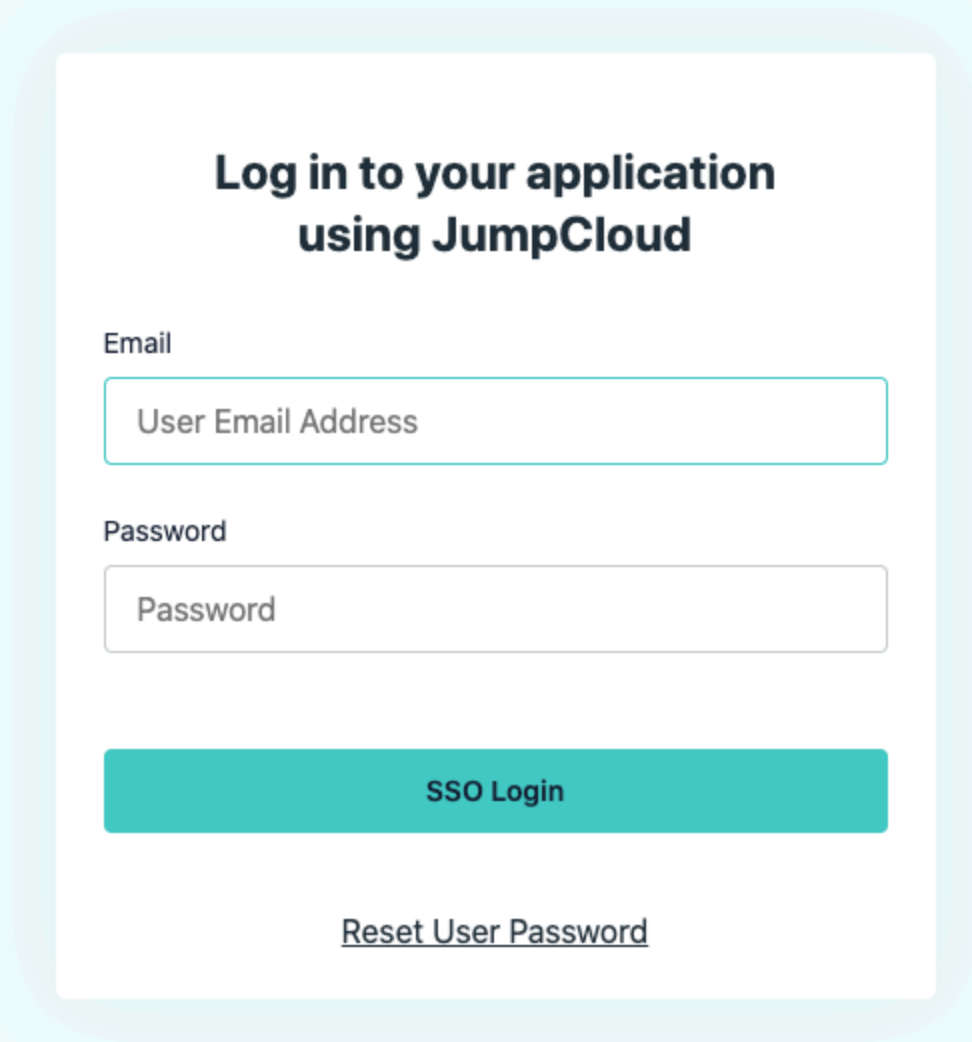
設定をテストする

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、JumpCloudのログイン画面にリダイレクトされます。



JumpCloud Login

あなたのJumpCloudの資格情報で認証した後、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。