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 >

AWS SAML 実装

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

AWS SAML 実装

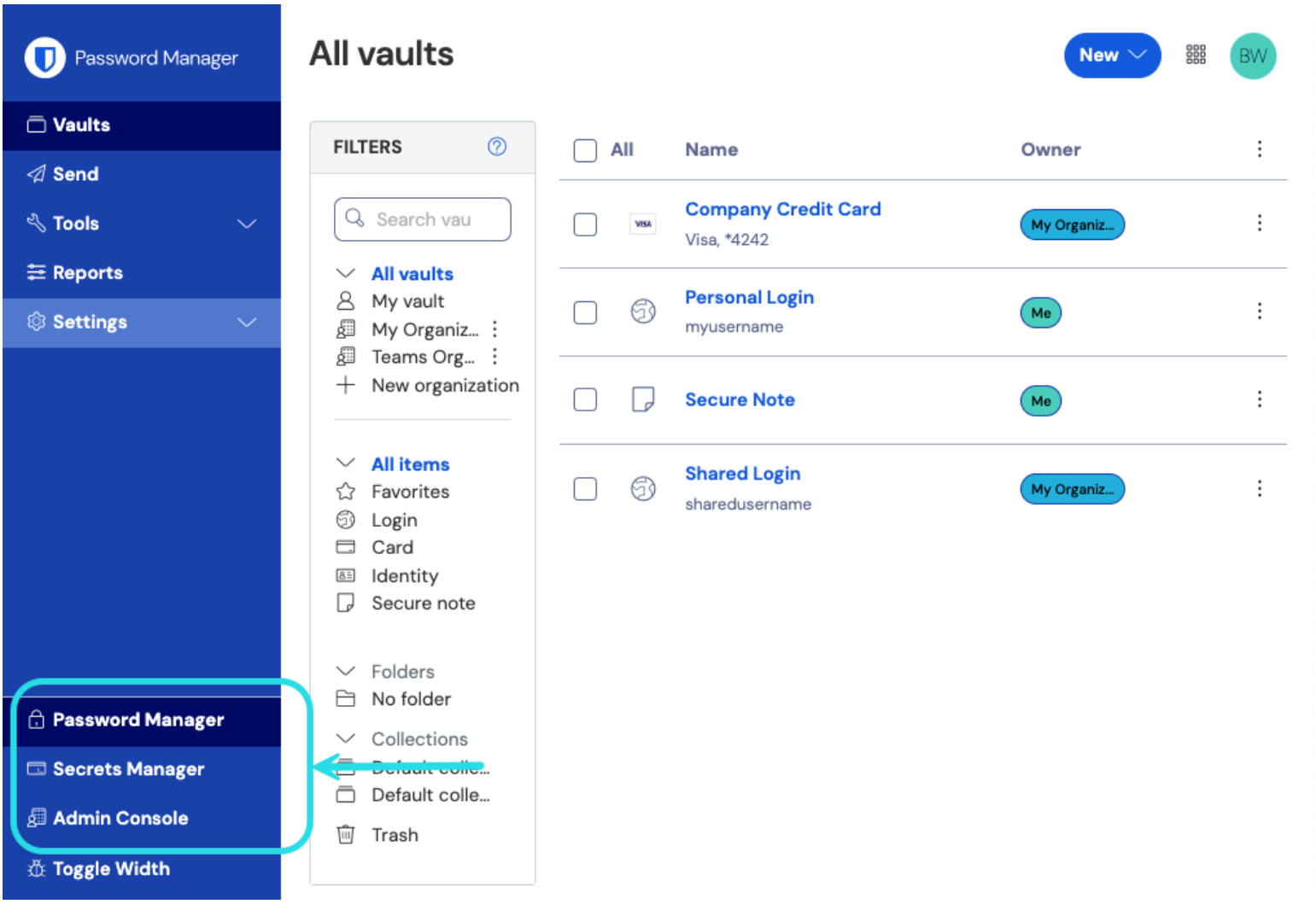
この記事には、SAML 2.0を介したSSOでのログインを設定するための**AWS特有の**ヘルプが含まれています。
別のIdPでSSOを使用したログインの設定についてのヘルプは、SAML 2.0設定を参照してください。

設定は、Bitwardenウェブアプリと AWSコンソー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**
>
> **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：K4Z8nyORzKkHKIJIZ4hh1

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

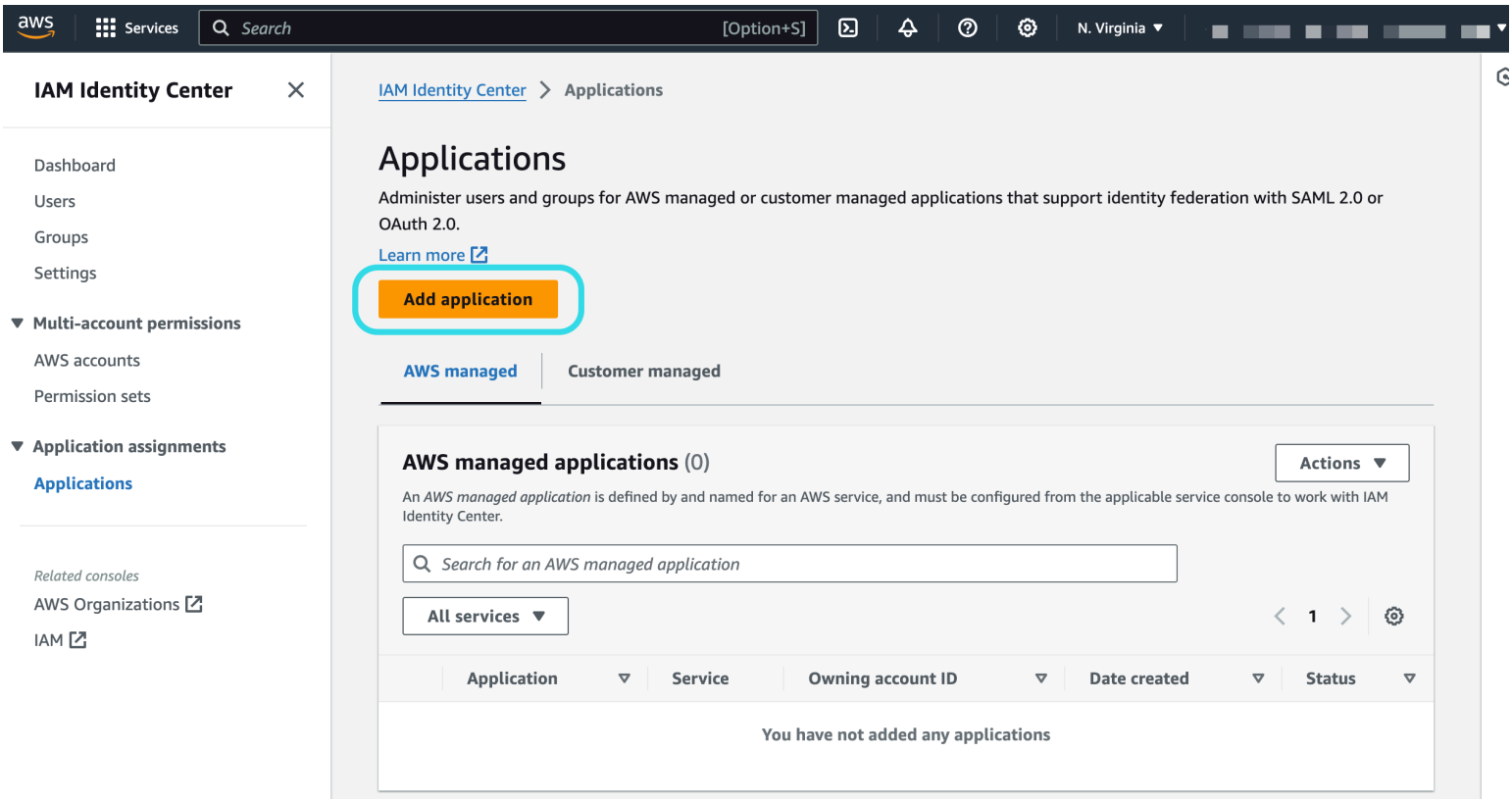
まだ作成していない場合は、あなたの**SSO識別子**を組織用に作成し、**タイプ**のドロップダウンから**SAML**を選択してください。
この画面を開いたままにして、簡単に参照できるようにしてください。

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、
あなたのSPエンティティID値から組織IDが削除されますが、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。

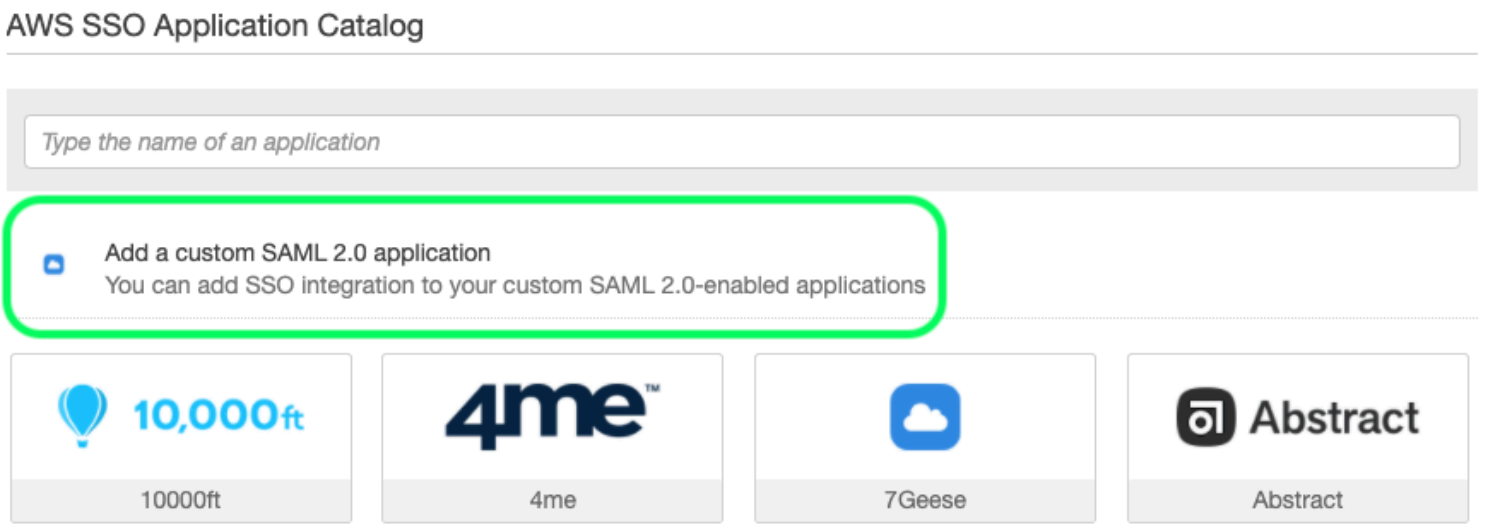
AWS SSOアプリケーションを作成します

AWSコンソールで、**AWS SSO**に移動し、ナビゲーションから**アプリケーション**を選択し、
新しいアプリケーションを追加ボタンを選択します：



新しいアプリケーションを追加する

検索バーの下で、**カスタムSAML 2.0アプリケーションを追加**のオプションを選択します：



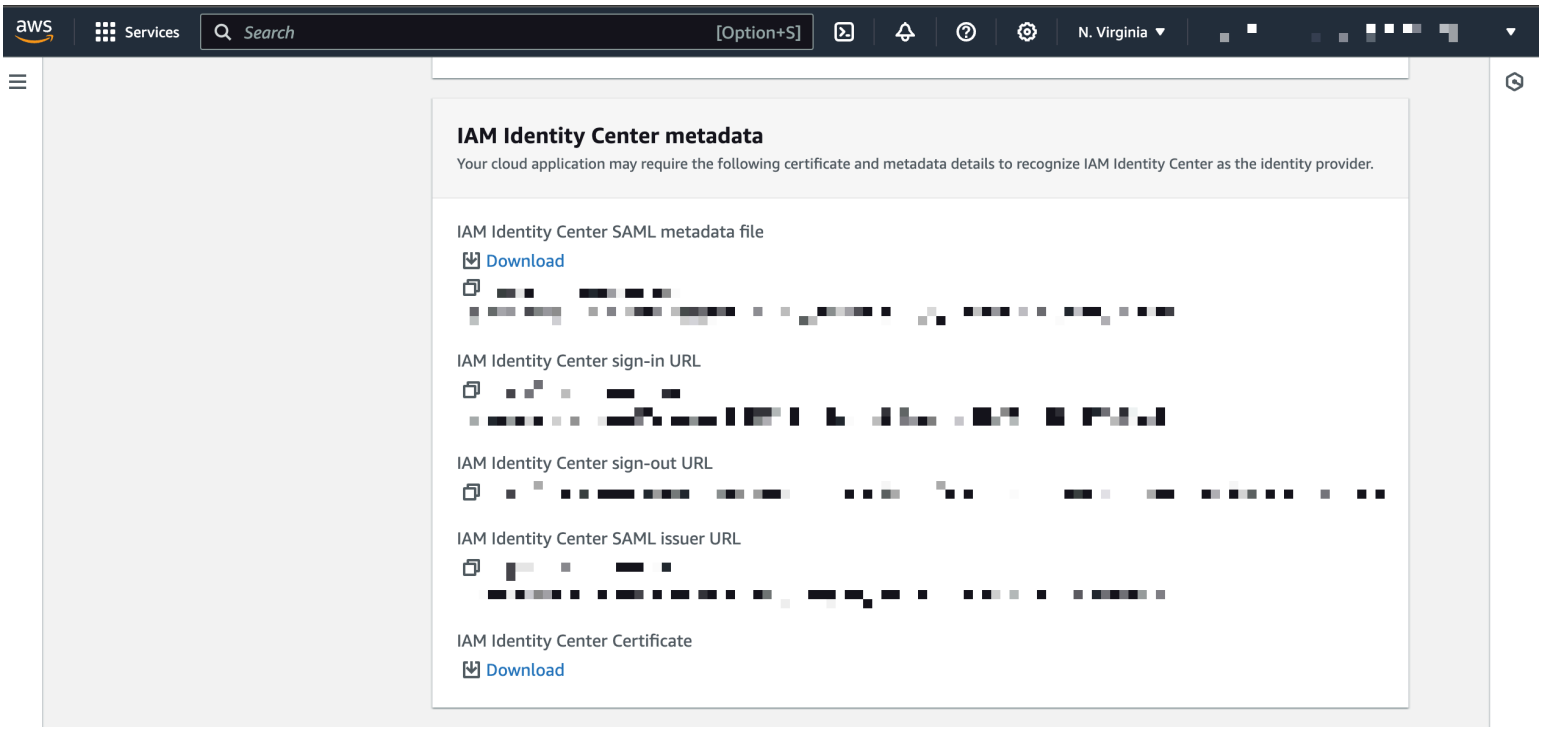
カスタムSAMLアプリを追加する

詳細

アプリケーションにユニークでBitwarden特有の**表示名**を付けてください。

AWS SSOメタデータ

このセクションの情報は、後の設定ステップで必要になります。**AWS SSOサインインURL**と**AWS SSO発行者URL**をコピーし、**AWS SSO証明書**をダウンロードしてください：



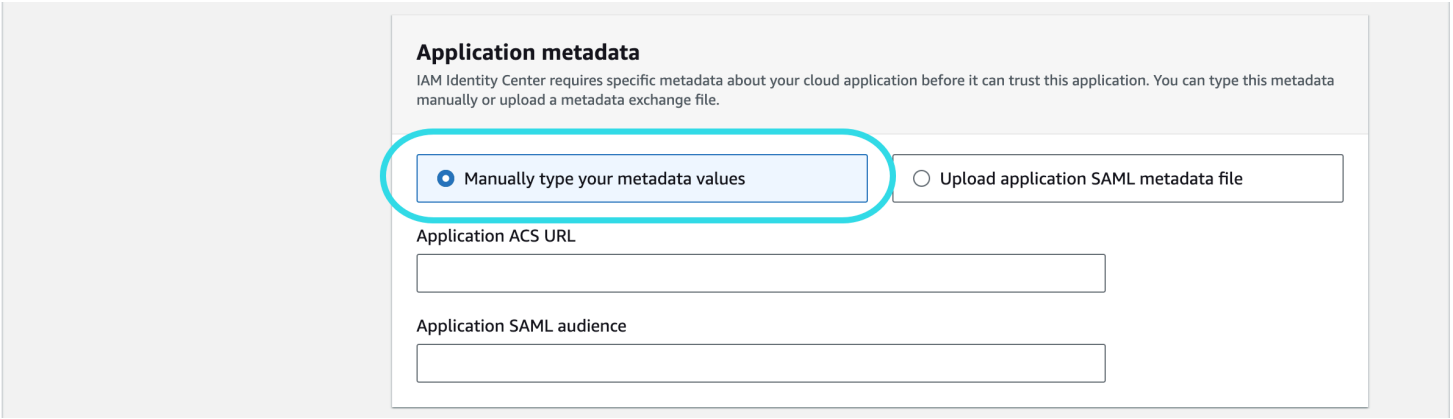
AWS SSOメタデータ

アプリケーションのプロパティ

アプリケーション開始URLフィールドに、ユーザーがBitwardenにアクセスするためのログインURLを指定します。
クラウドホストのお客様の場合、これは常に`https://vault.bitwarden.com/#/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/#/sso`のようなものです。

アプリケーションのメタデータ

アプリケーションのメタデータセクションで、メタデータの値を手動で入力するオプションを選択してください。



メタデータの値を入力してください

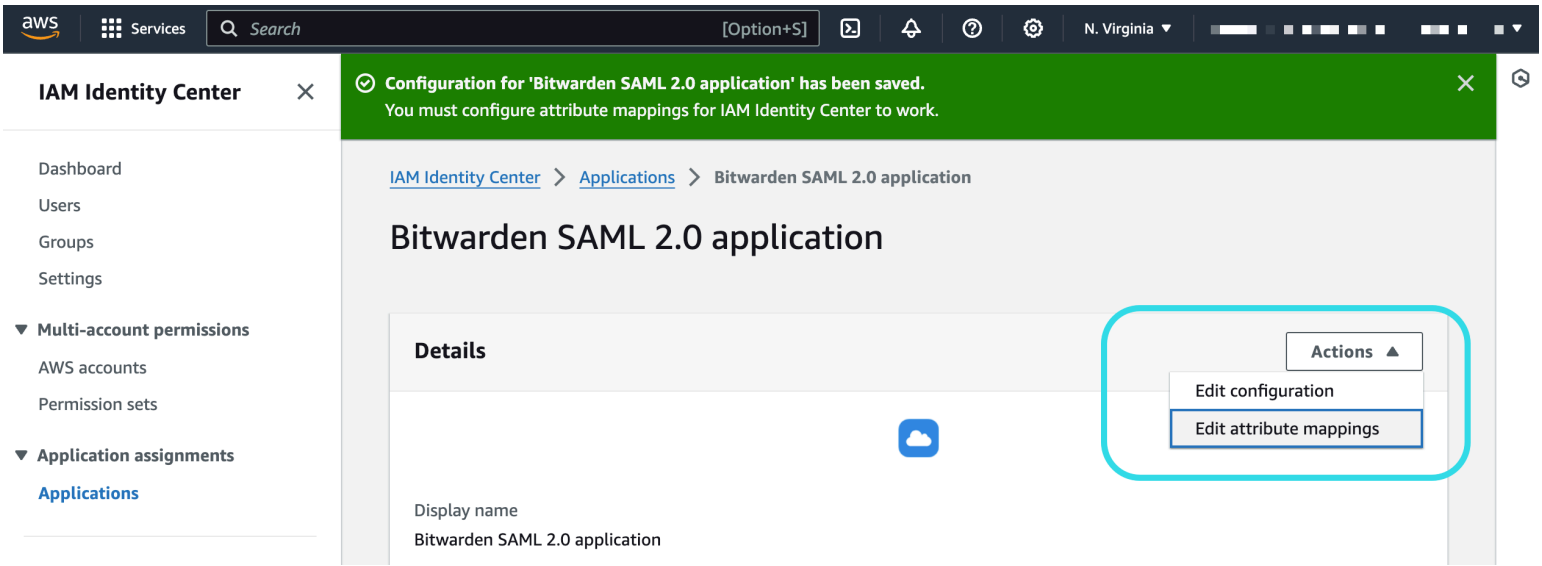
次のフィールドを設定してください:

フィールド	説明
アプリケーションACS 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。
アプリケーション SAML オーディエンス	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。

終了したら、**変更を保存**を選択してください。

属性マッピング

属性マッピングタブに移動し、次のマッピングを設定します:

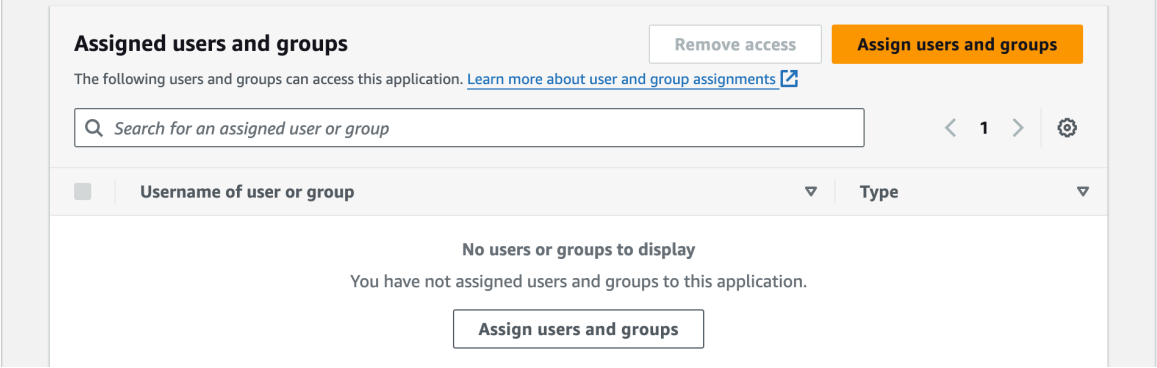


属性マッピング

アプリケーション内のユーザー属性	この文字列値またはユーザー属性をAWS SSOにマップします	形式
件名	`${user:email}`	メールアドレス
メールアドレス	`${user:email}`	特定されていません

割り当てられたユーザー

割り当てられたユーザータブに移動し、**ユーザーを割り当てる**ボタンを選択します：



ユーザーを割り当てる

アプリケーションには個々のレベルでユーザーを割り当てることができますし、グループごとにも割り当てることができます。

ウェブアプリに戻る

この時点で、AWSコンソー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

サービスプロバイダーの設定はすでに完了しているはずですが、次のフィールドのいずれかを編集することを選択することができます：

フィールド	説明
名前ID形式	**メールアドレス**に設定します。
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、AWS SSOはSHA-256で署名します。これを変更していない限り、ドロップダウンから`sha256`を選択してください。

フィールド	説明
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されることを期待しているかどうか。
証明書を検証する	あなたのIdPから信頼できるCAを通じて信頼された有効な証明書を使用するときには、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with 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AWSコンソー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	**AWS SSO発行者URL**を入力してください。これはAWSコンソールのAWS SSOメタデータセクションから取得できます。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	**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	**AWS SSOサインインURL**を入力してください。これはAWSコンソールのAWS SSOメタデータセクションから取得できます。
シングルログアウトサービスURL	SSOでのログインは現在、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、AWSコンソールの**AWS SSOメタデータ**セクションから取得したAWS SSOサインアウト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、削除してください。
	`-----BEGIN CERTIFICATE-----`
	そして
	`-----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、

フィールド	説明
	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、AWS SSOは`sha256`で署名します。 これを変更していない限り、ドロップダウンから`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欲しい	AWS SSOがSAMLリクエストに署名を期待するかどうか。

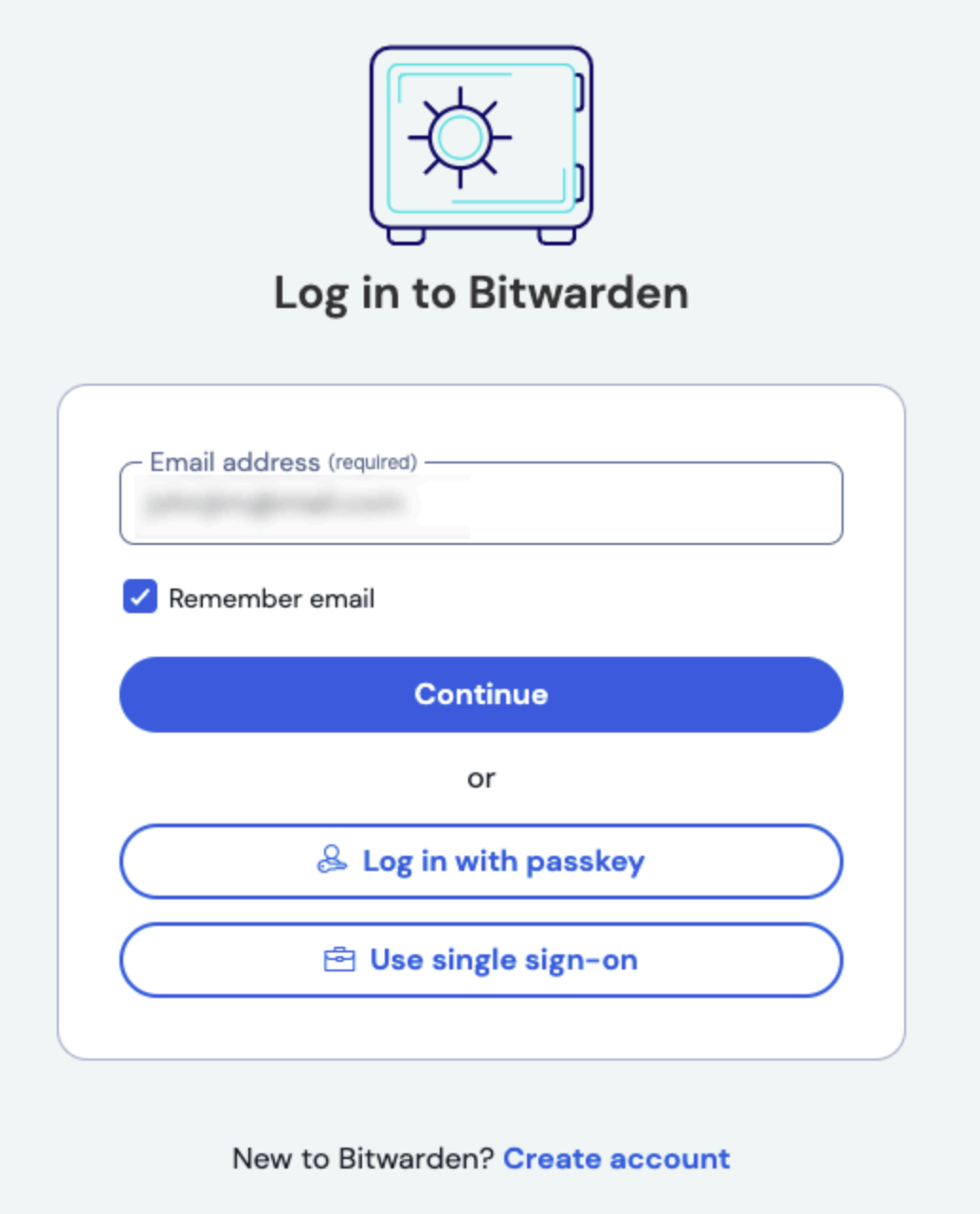
Note
X509証明書を完成させるとき、有効期限の日付をメモしてください。SSOエンドユーザーへのサービスの中断を防ぐために、
証明書を更新する必要があります。証明書が期限切れになった場合でも、
管理者と所有者のアカウントは常にメールアドレスとマスターパスワードでログインできます。

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

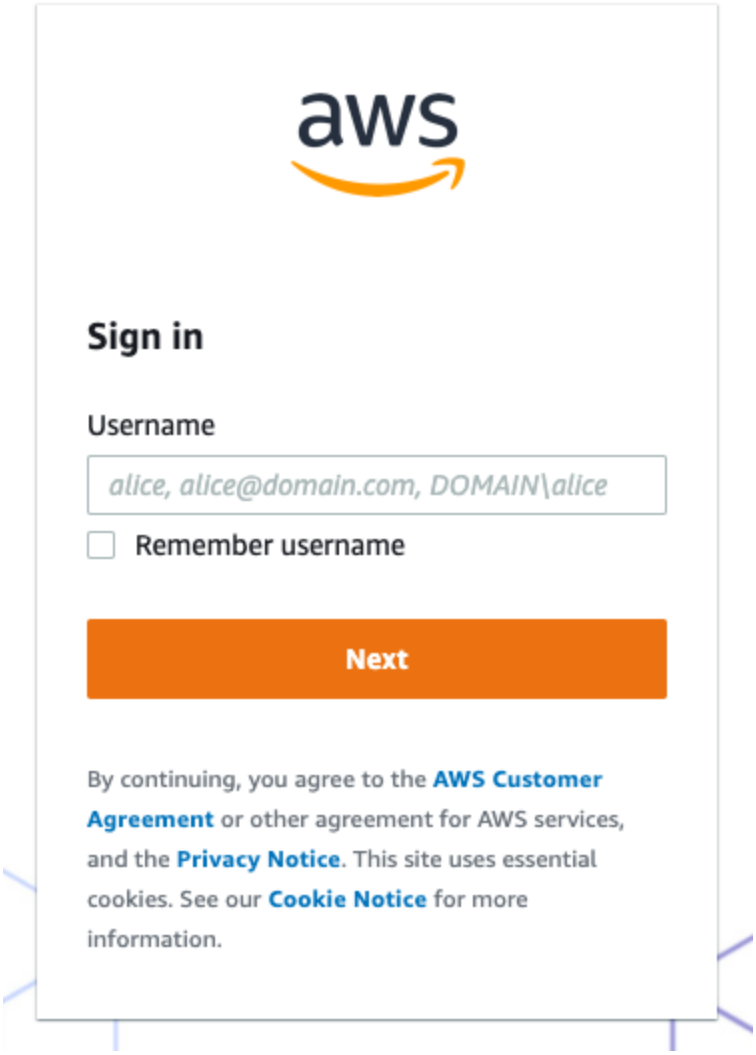
設定をテストする

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、**続ける**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、AWS SSOのログイン画面にリダイレクトされます。



AWSログイン画面

あなたのAWS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。