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 >

OneLogin SAMLの実装

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

OneLogin SAMLの実装

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**OneLogin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 OneLogin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。

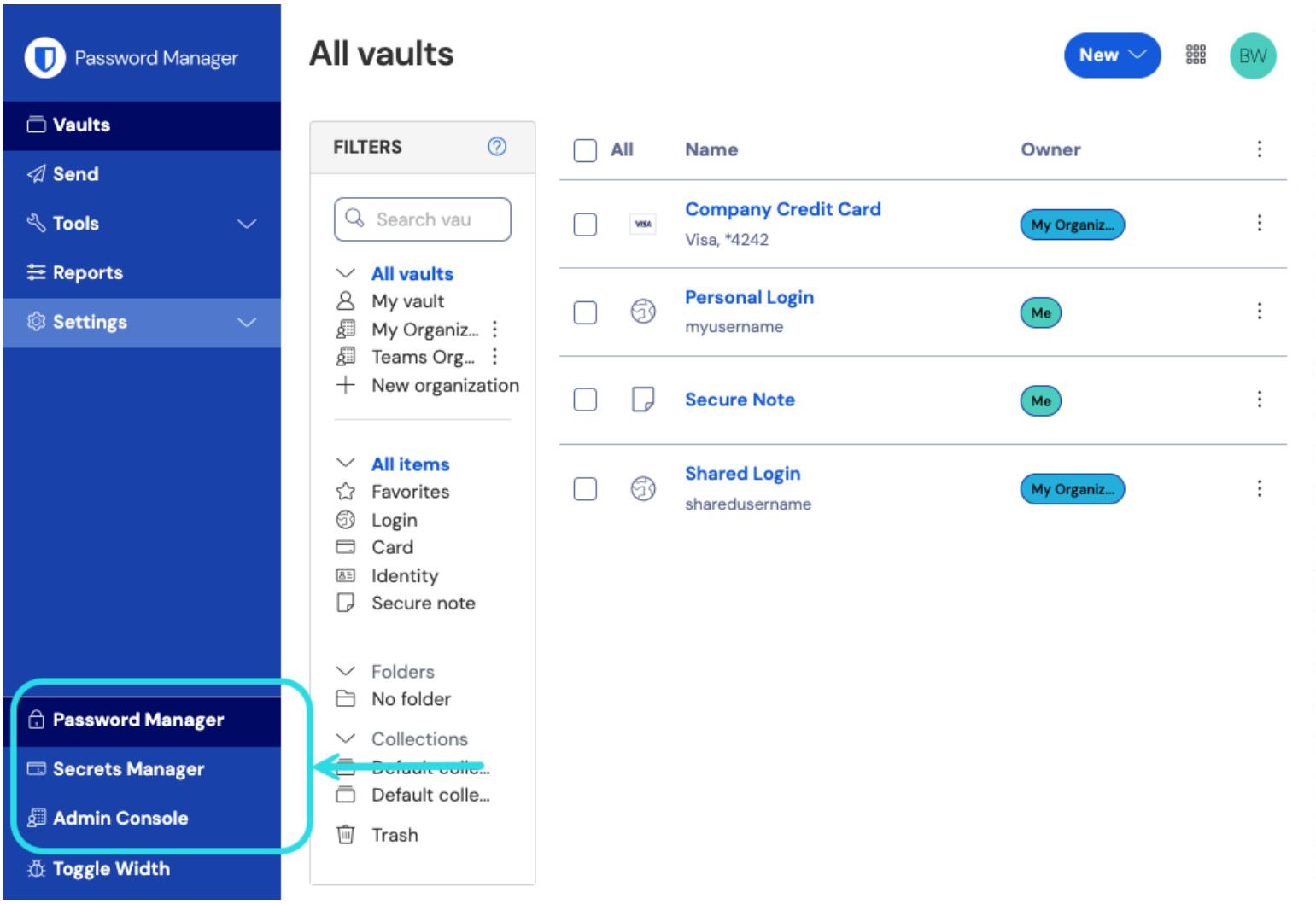
Tip

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

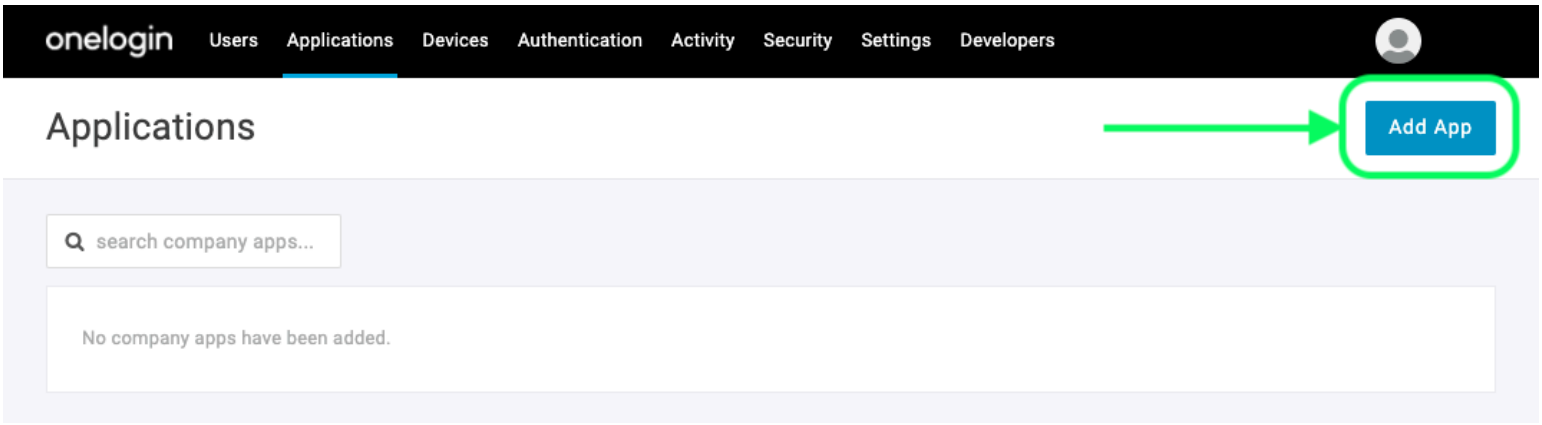
まだ作成していない場合は、あなたの組織のためのユニークな**SSO識別子**を作成し、**タイプ**のドロップダウンから**SAML**を選択してください。この画面を開いたままにして、簡単に参照できるようにしてください。

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**の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値から組电IDが削除されますが、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。

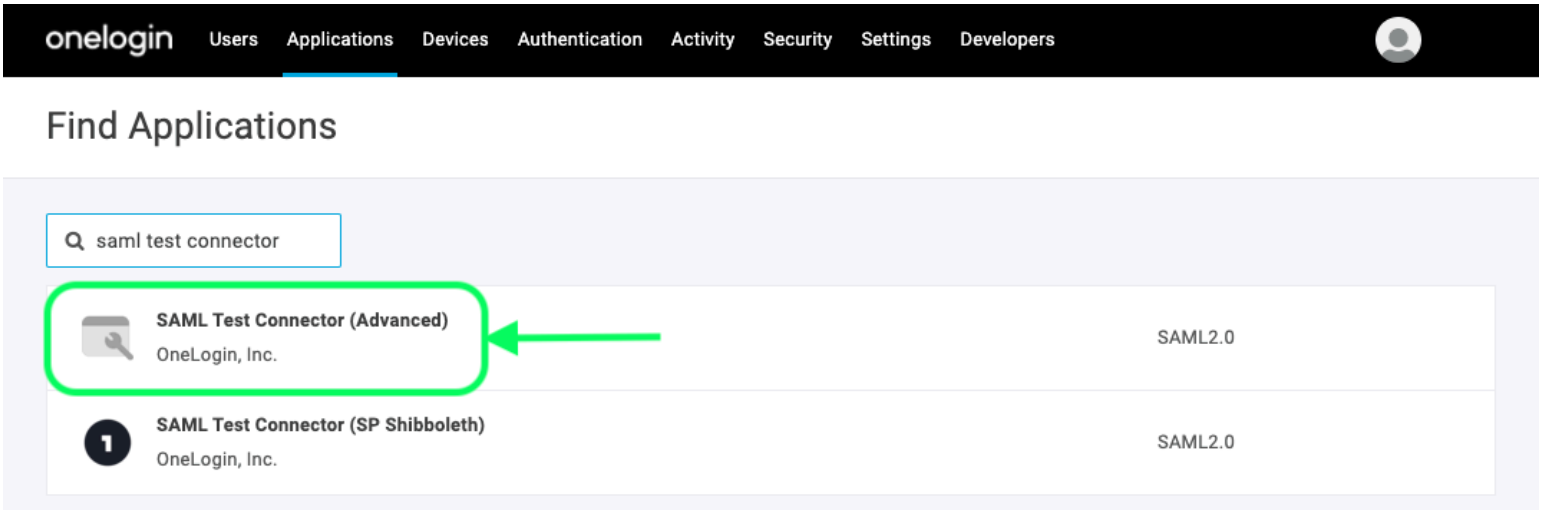
OneLoginアプリを作成します

OneLoginポータルで、**アプリケーション**画面に移動し、**アプリを追加**ボタンを選択します:



Add an Application

検索バーに`saml test connector`とタイプし、**SAML Test Connector (Advanced)**アプリを選択してください：

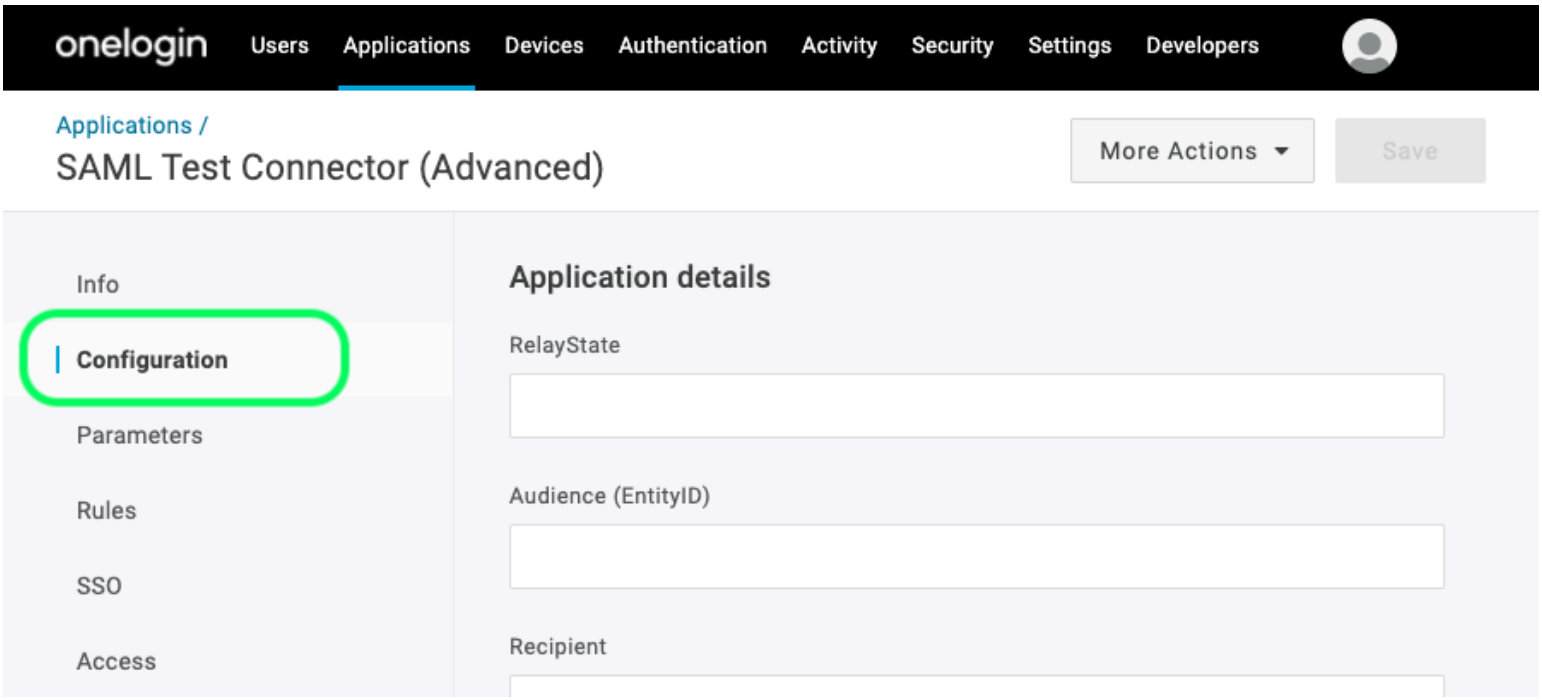


SAML Test Connector App

あなたのアプリケーションにBitwarden特有の**表示名**を付けて、**保存**ボタンを選択してください。

設定

左側のナビゲーションから**設定**を選択し、以下の情報を設定します。これらの一部はシングルサインオン画面から取得する必要があります。



App Configuration

アプリケーション設定	説明
観客 (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。
受信者	このフィールドを、**視聴者 (エンティティID)** の設定に使用された同じ事前生成された**SPエンティティID**に設定します。
ACS (コンシューマー) URL バリデーター	OneLoginによって**必須**とマークされているにもかかわらず、 このフィールドに情報を入力する必要は実際にはありません。Bitwardenと統合するためには。 次のフィールドに進んでください、**ACS (消費者) URL**。
ACS (消費者) 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。

アプリケーション設定	説明
SAML イニシエーター	**サービスプロバイダー**を選択してください。SSOでのログインは現在、IdPが開始するSAMLアサーションをサポートしていません。
SAML nameID形式	このフィールドを、SAMLアサーションに使用したいSAML NameIDフォーマットに設定します。
SAML署名要素	デフォルトでは、OneLoginはSAMLレスポンスに署名します。これを**アサーション**または**両方**に設定することができます。

設定を完了するには、**保存**ボタンを選択してください。

パラメーター

左側のナビゲーションから**パラメータ**を選択し、＋ **追加**アイコンを使用して次のカスタムパラメータを作成します:

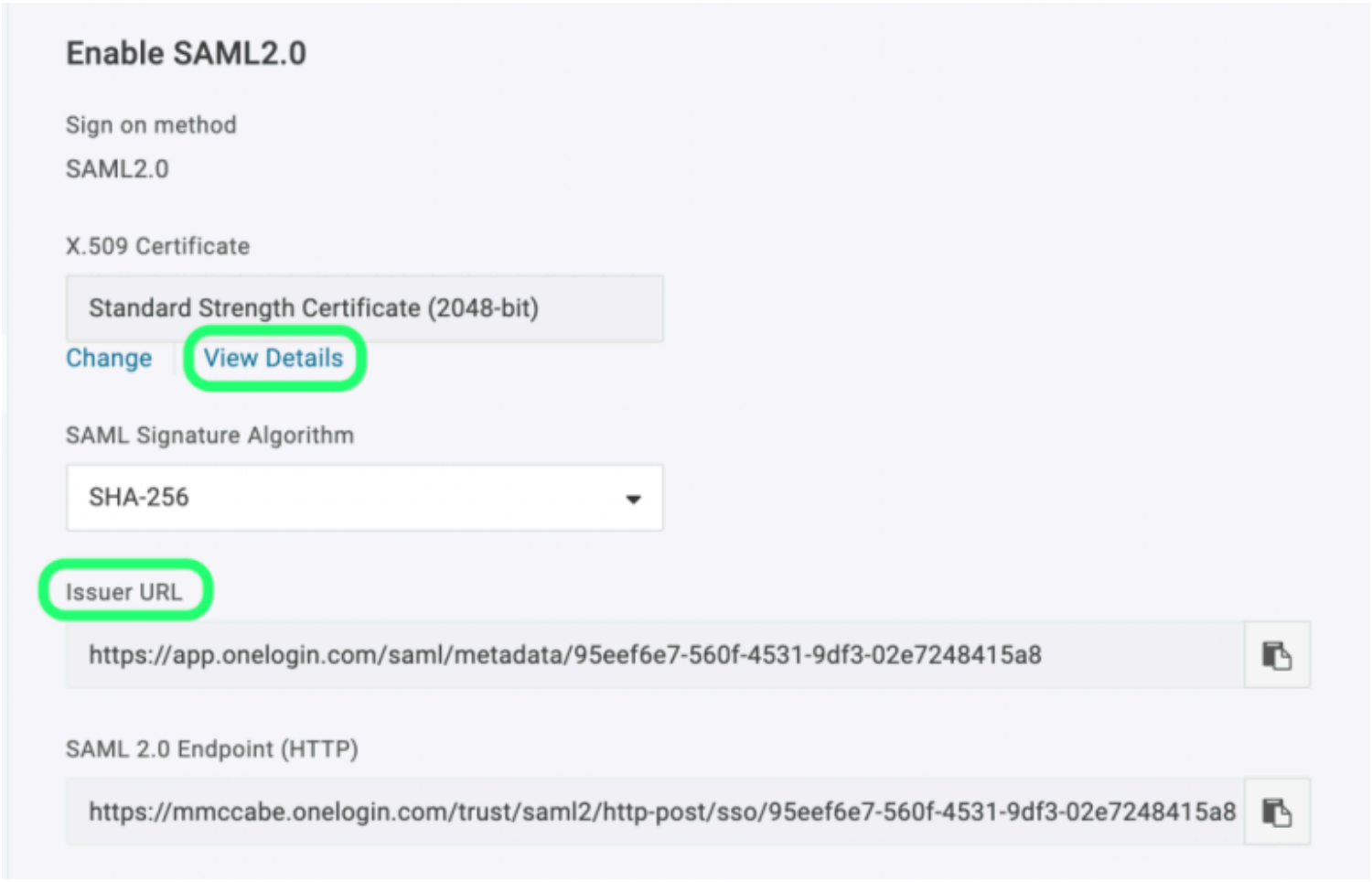
フィールド名	値
メールアドレス	Eメール
名前	名
苗字	姓

カスタムパラメータを完了するには、**保存**ボタンを選択してください。

SSO

左側のナビゲーションから**SSO**を選択し、以下を完了してください：

1. あなたのX.509証明書の下にある**詳細を表示**リンクを選択してください。



View your Cert

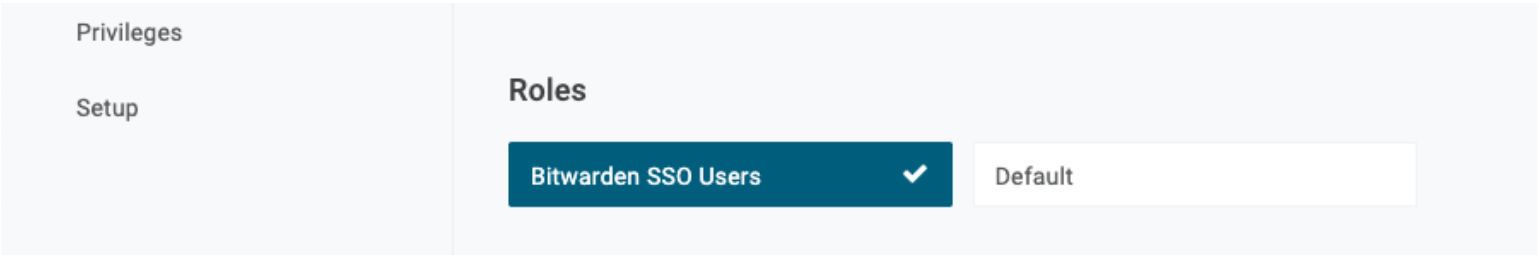
証明書画面で、X.509 PEM証明書をダウンロードまたはコピーします。後で使用する必要があるためです。コピーしたら、メインのSSO画面に戻ってください。

2. あなたの**SAML署名アルゴリズム**を設定してください。

3. あなたの**発行者URL**と**SAML 2.0エンドポイント(HTTP)**をメモしてください。これらの値はすぐに使用する必要があります。

アクセス

左側のナビゲーションから**アクセス**を選択してください。**役割**セクションで、Bitwardenを使用できるようにしたいすべての役割にアプリケーションのアクセスを割り当ててください。ほとんどの実装では、Bitwarden特有の役割を作成し、代わりにキャッチオール（例えば、**デフォルト**）に基づいて割り当てるか、既存の役割に基づいて割り当てます。



Role Assignment

ウェブアプリに戻る

この時点で、OneLogin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、設定を二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の応答に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

OneLogin Portalでアプリ作成中に選択した選択肢に従って、以下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	このフィールドを、**OneLoginのSAML nameIDフォーマット**フィールドで選択したものに設定します。アプリ設定中に。
アウトバウンド署名アルゴリズム	デフォルトでSAMLリクエストに署名するために使用されるアルゴリズム、`sha-256`。
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、OneLogin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	このフィールドを、**SAML署名アルゴリズム**アプリ設定中に選択したものに設定してください。
署名されたアサーションが欲しい	このボックスをチェックしてください、もしOneLoginの**SAML署名要素**を**アサーション**または**両方**にアプリ設定中に設定した場合。
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OneLogin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	あなたのOneLoginの**発行者URL**を入力してください。これは、OneLoginアプリのSSO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	**HTTP Post** に設定します（SAML 2.0エンドポイント（HTTP）で示されているように）。
シングルサインオンサービスURL	あなたのOneLogin **SAML 2.0エンドポイント(HTTP)**を入力してください。これはOneLoginアプリのSSO画面から取得できます。
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、ご希望であれば事前に設定することができます。

X509公開証明書	取得したX.509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、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	OneLoginSSO設定セクションで選択されたSAML署名アルゴリズム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	OneLoginがSAMLリクエストの署名を期待しているかどうか。

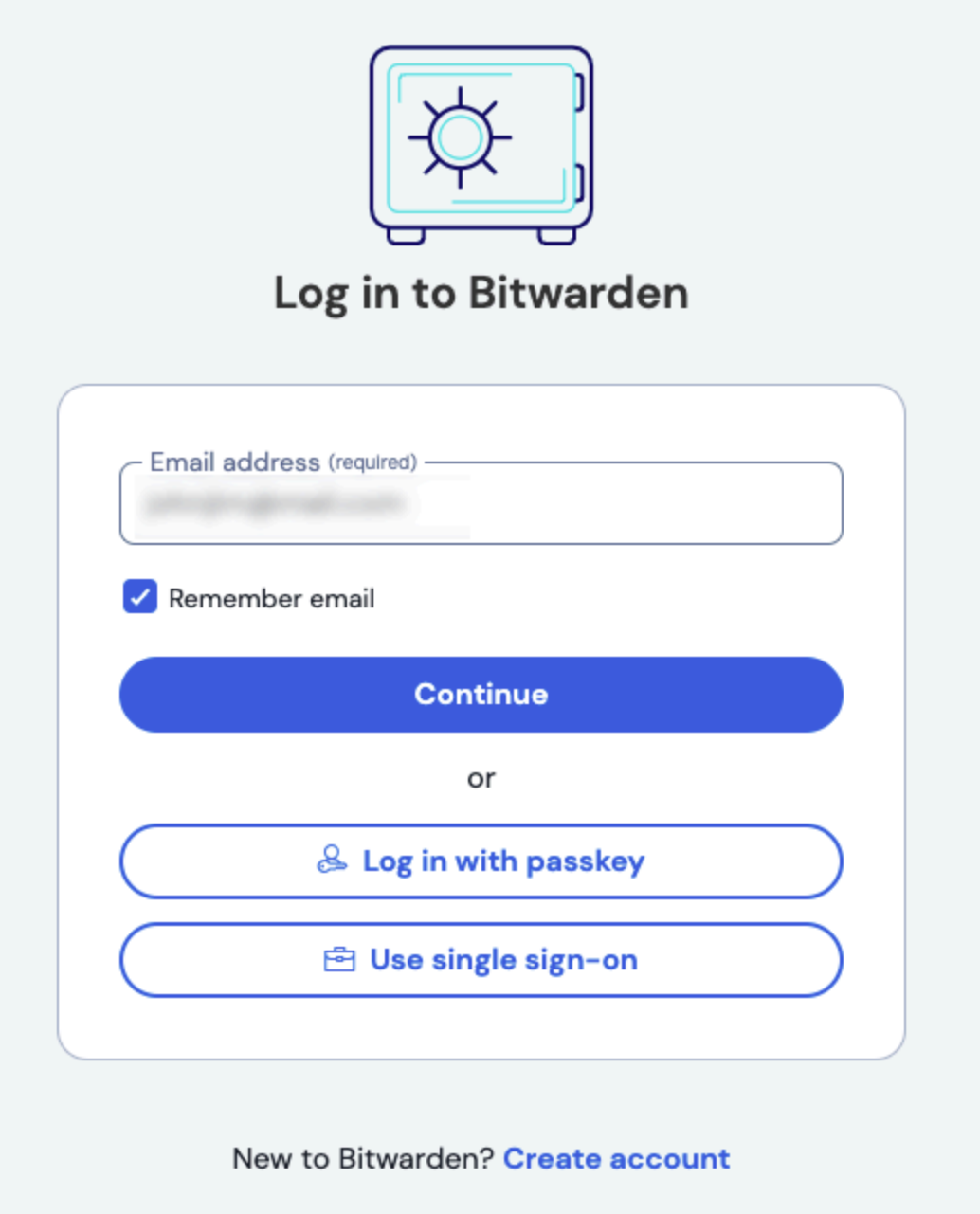
> **Note**
> X509証明書を完成させるとき、有効期限の日付をメモしてください。SSOエンドユーザーへのサービスの中断を防ぐために、証明書を更新する必要があります。証明書が期限切れになった場合でも、管理者と所有者のアカウントは常にメールアドレスとマスターパスワードでログインできます。

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

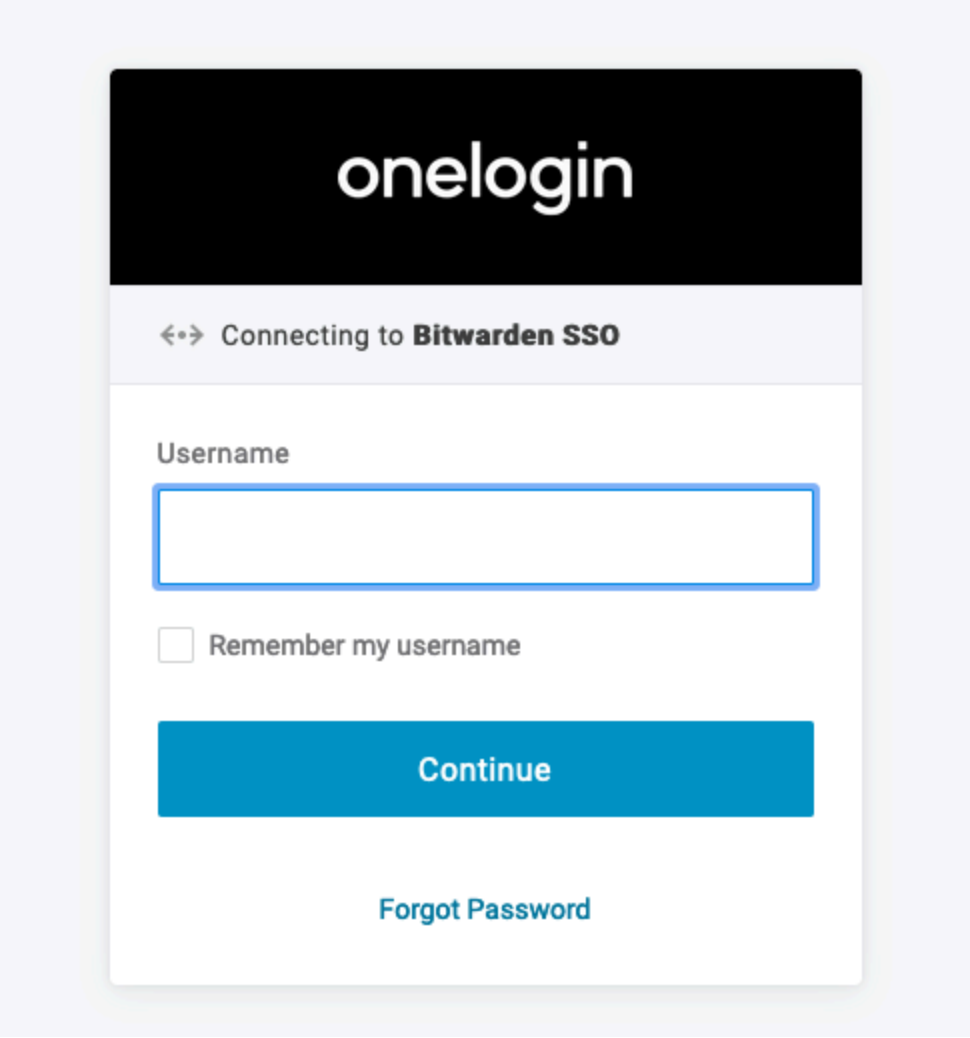
設定をテストする

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、OneLoginのログイン画面にリダイレクトされます。



OneLogin Login

OneLogin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。