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 ›

Keycloak SAML実装

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

Keycloak SAML実装

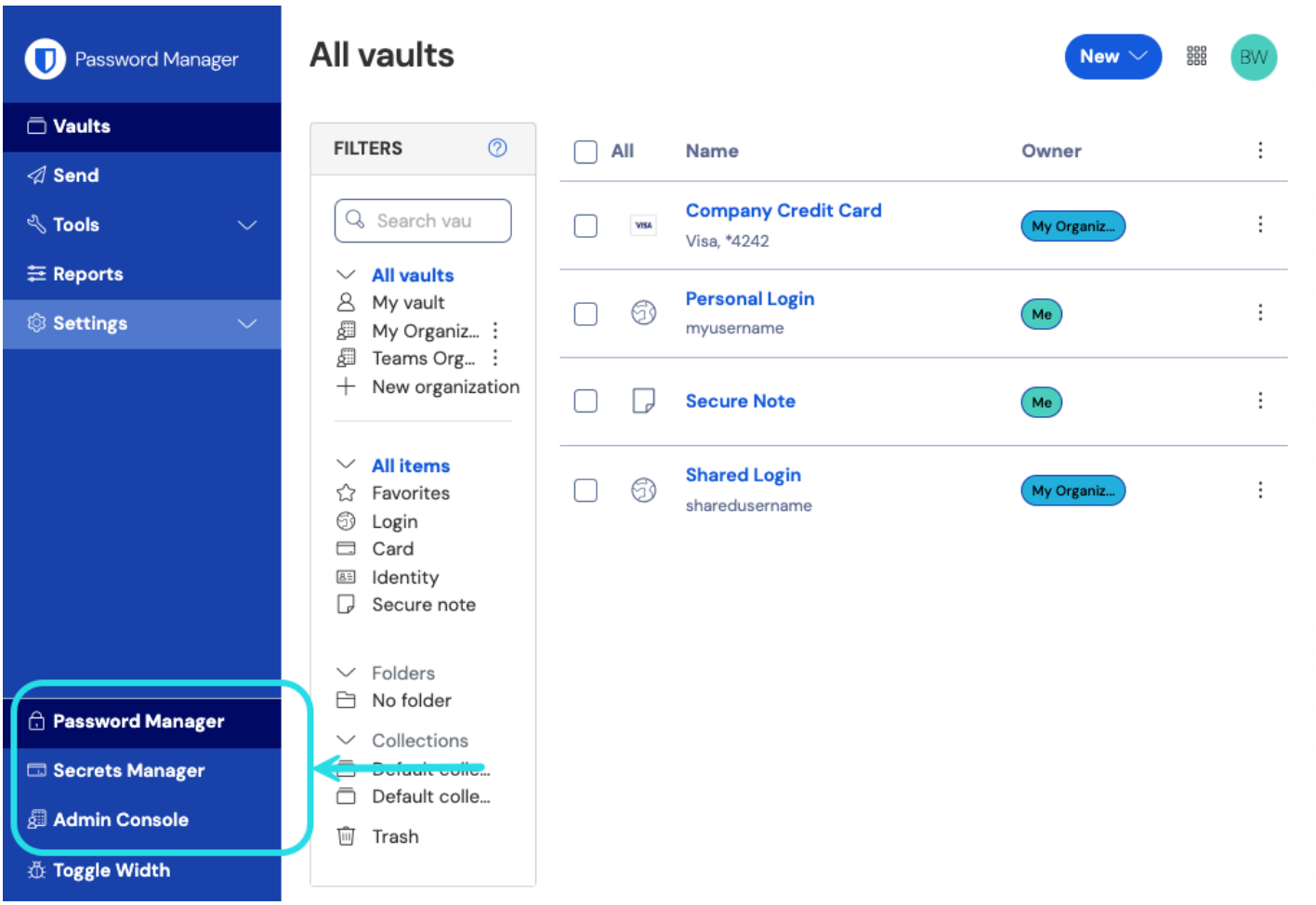
この記事には、SAML 2.0を介したSSOでのログインを設定するための**Keycloak特有の**ヘルプが含まれています。別のIdPでSSOを使用したログインの設定についてのヘルプは、SAML 2.0設定を参照してください。

設定は、Bitwardenウェブアプリと Keycloakポータル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**
> **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

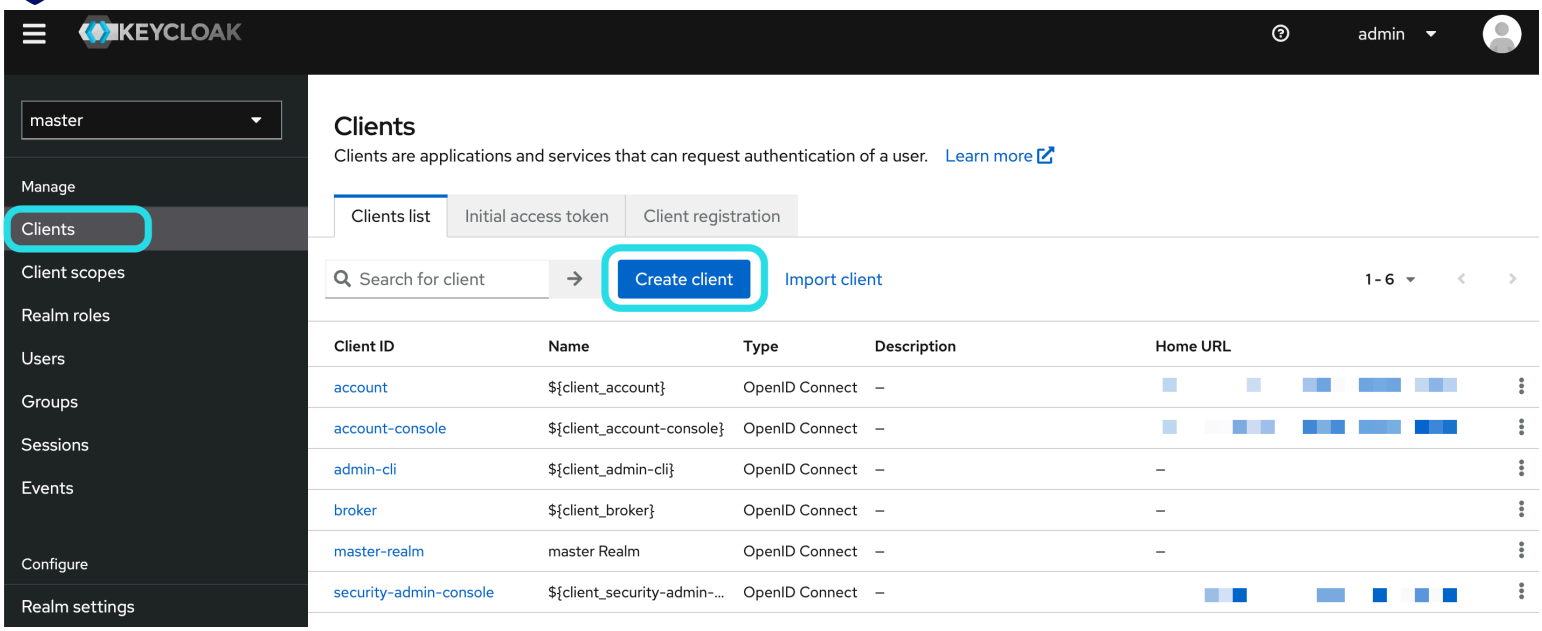
まだ作成していない場合は、あなたの組織のためのユニークな**SSO識別子**を作成し、**タイプ**のドロップダウンから**SAML**を選択してください。この画面を開いたままにして、簡単に参照できるようにしてください。

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。

Keycloakの設定

Keycloakにログインし、**クライアント** → **クライアントを作成**を選択します。



Create a Client

クライアントを作成する画面で、次のフィールドに入力してください：

フィールド	説明
クライアントタイプ	SAMLを選択してください。
クライアント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。
お名前	Keycloakクライアントの名前を自由に入力してください。

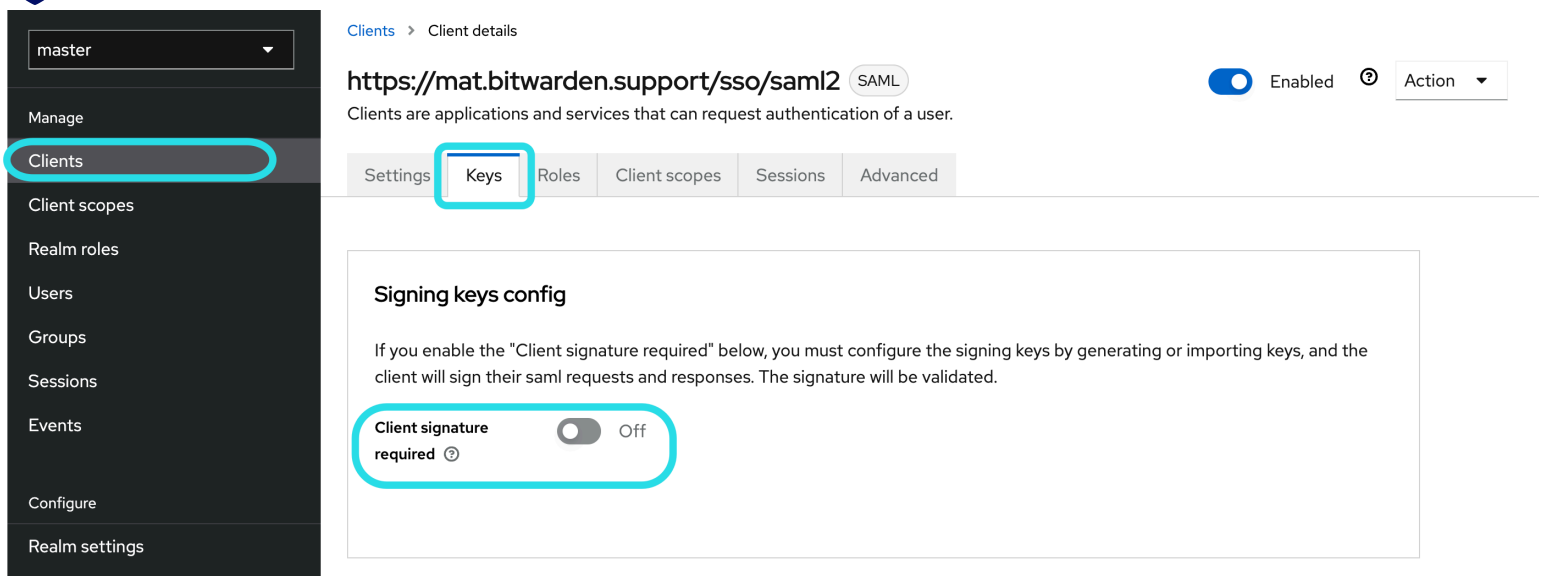
必要なフィールドに**一般設定**ページで入力したら、**次へ**をクリックしてください。

ログイン設定画面で、次のフィールドに入力してください：

フィールド	説明
有効なリダイレクトURI	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。

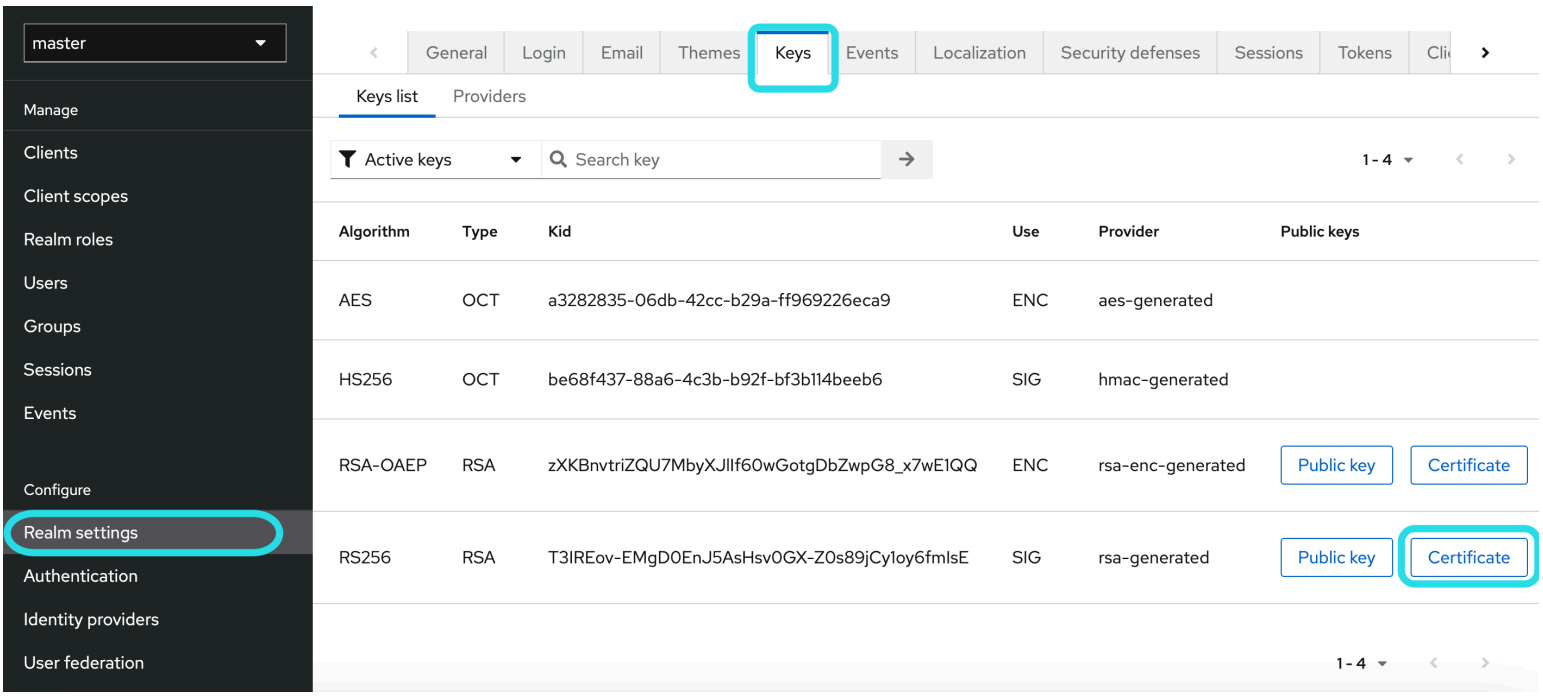
保存を選択してください。

「Keys」タブを選択し、**クライアント署名が必要**オプションを**オフ**に切り替えてください。



Keycloak Keys Config

最後に、Keycloakのメインナビゲーションで、**レルム設定**を選択し、次に**キー**タブを選択します。**RS256**証明書を探して、**証明書**を選択してください。



Keycloak RS256 Certificate

証明書の値は次のセクションで必要となります。

ウェブアプリに戻る

この時点で、Keycloak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。Bitwardenウェブアプリに戻り、ナビゲーションから**設定→シングルサインオン**を選択します。

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の応答に期待する形式を決定します。

次のフィールドを**SAMLサービスプロバイダ設定**セクションで完了してください:

フィールド	説明
名前IDの形式	**メールアドレス**を選択してください。
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。
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	KeycloakクライアントがSAMLドキュメントまたはアサーションに署名するために使用するように設定されているアルゴリズムを選択します。
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。トグルがオンの場合、 Keycloakクライアントをアサーションに署名するように設定してください。
証明書を検証する	あなたのIdPから信頼できるCAを通じて信頼できる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。

次のフィールドを**SAML IDプロバイダ設定**セクションで完了してください：

フィールド	説明
エンティティID	クライアントが作成されたKeycloakレルムのURLを入力してください。例: `https:///領域/`。 このフィールドは大文字と小文字を区別します。
バインディングの種類	**リダイレクト**を選択します。
シングルサインオンサービス URL	あなたのマスターSAML処理URLを入力してください。例えば、`https:///領域//プロトコル/saml`。
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 公開鍵証明書	前のステップでコピーされた**RS256証明書**を入力してください。 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	KeycloakクライアントがSAMLドキュメントまたはアサーションに署名するために使用するように設定されているアルゴリズムを選択します。
アウトバウンドログアウトリクエストを無効にする	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。
認証リクエストに署名が欲しい	KeycloakがSAMLリクエストの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、作業を**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

追加のKeycloak設定

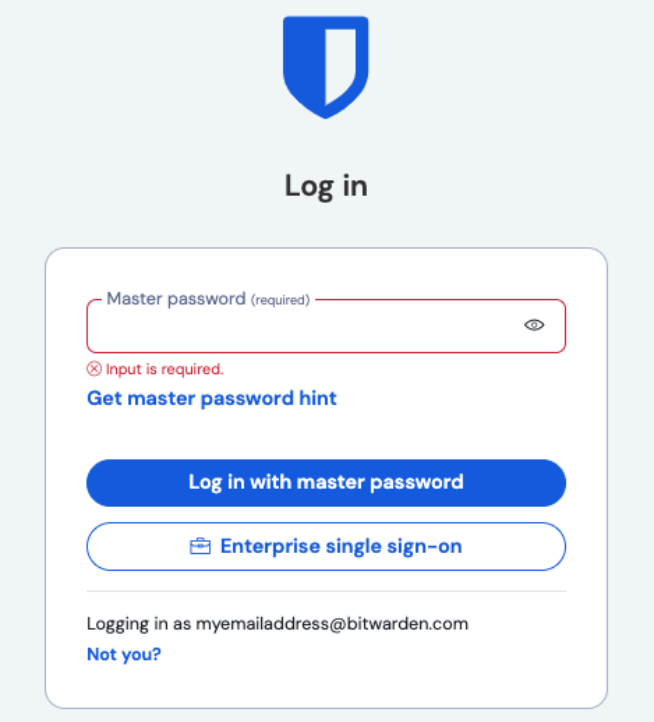
「Keycloakクライアント設定」**タブ**では、追加の構成オプションを使用できます。

フィールド	説明
書類に署名する	Keycloak領域によってSAMLドキュメントが署名されるべきかどうかを指定してください。
署名アサーション	Keycloakレルムによって SAMLアサーションが署名されるべきかどうかを指定してください。
署名アルゴリズム	**署名アサーション**が有効になっている場合、署名に使用するアルゴリズムを選択します（デフォルトは`sha-256`）。
名前ID形式	KeycloakがSAMLレスポンスで使用するName IDフォーマットを選択してください。

フォーラムが完了したら、**保存**を選択してください。

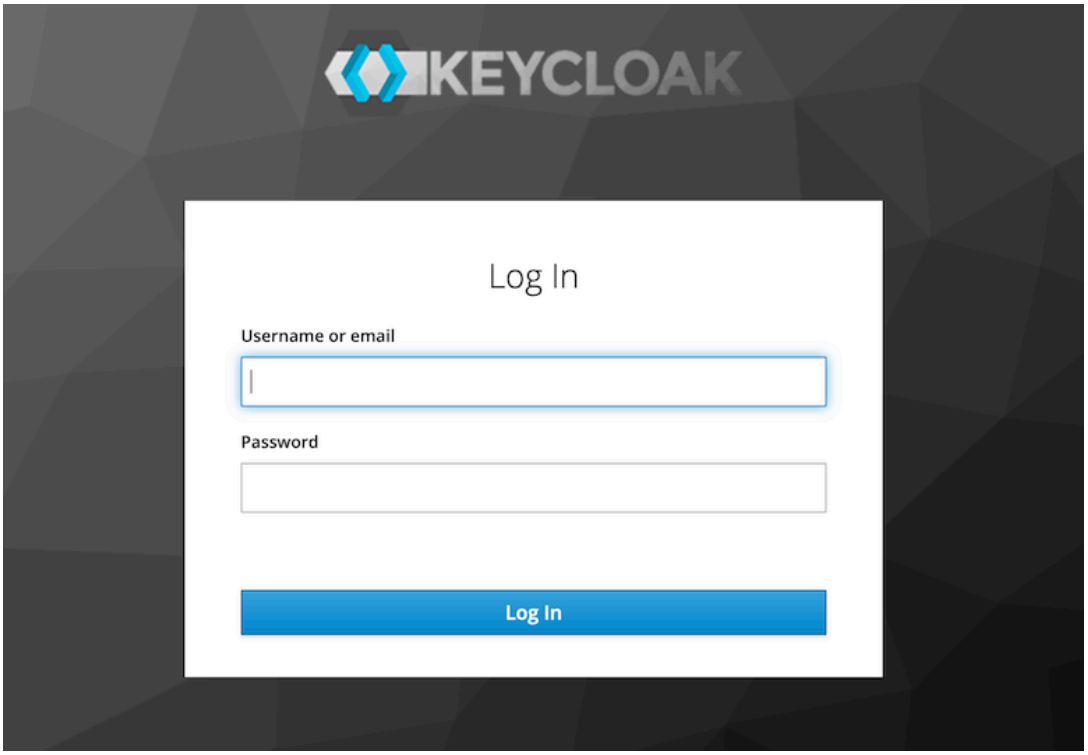
設定をテストする

設定が完了したら、https://vault.bitwarden.comに移動してテストを行います。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**ボタンを選択します。



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

設定された組織の識別子を入力し、**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、Keycloakのログイン画面にリダイレクトされます。



Keycloak Login Screen

あなたのKeycloak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。