Google SAML 実装

Google SAML 実装

この記事には、SAML 2.0を介したSSOでの**Google Workspace特有の**ログイン設定に関する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 Googleワークスペース管理者コンソールを同時に使用する作業を含みます。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。

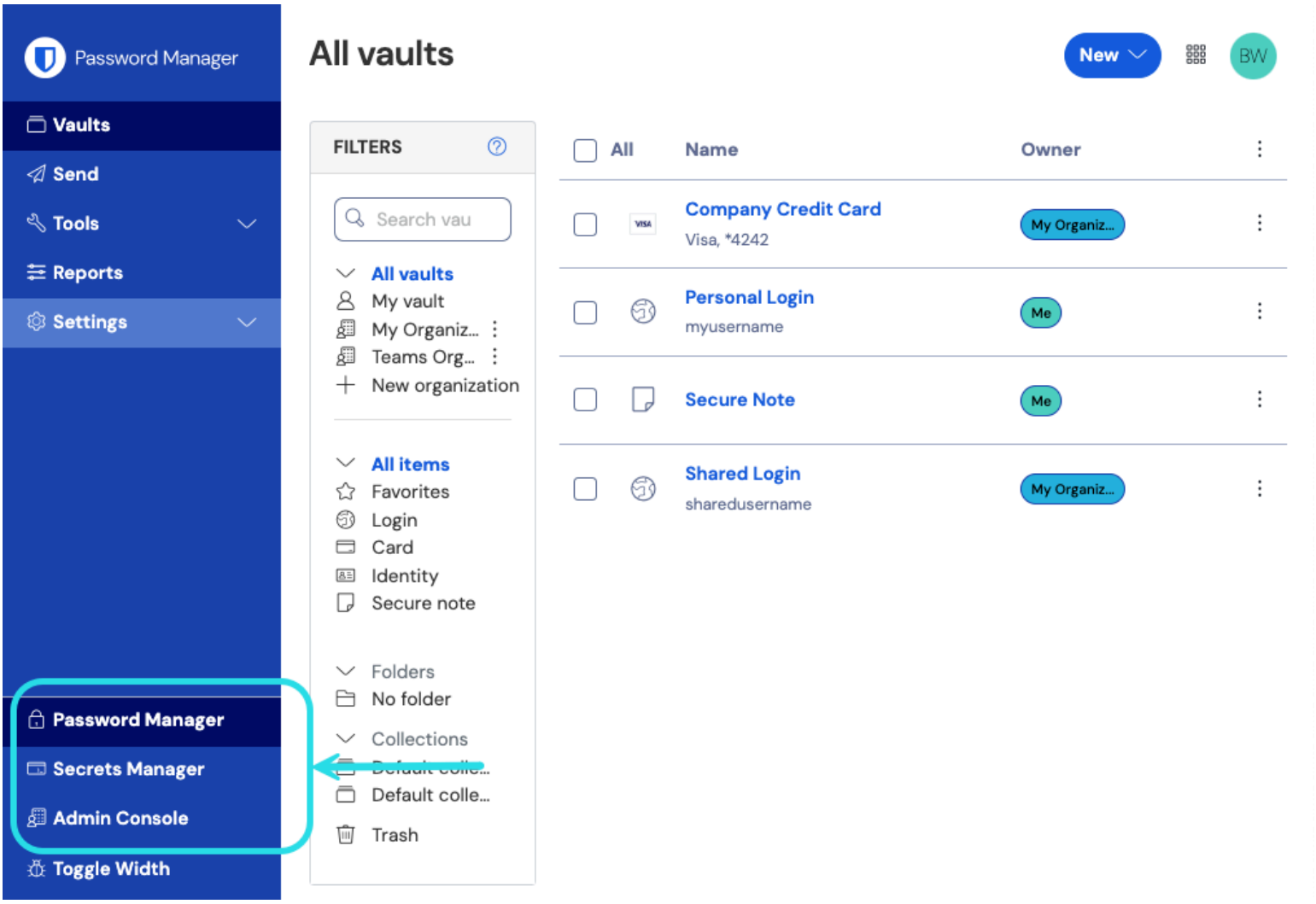
Tip

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

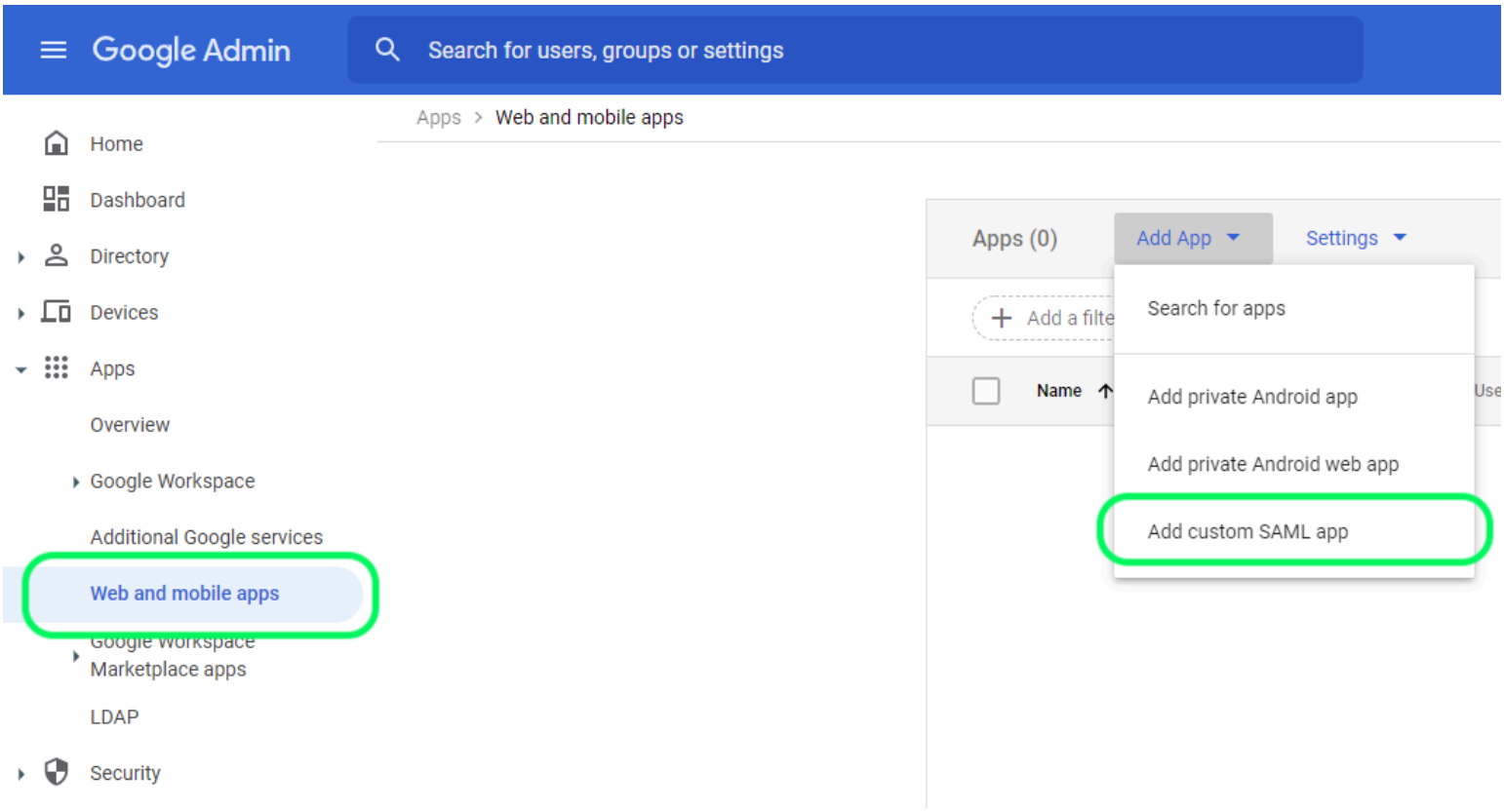
まだ作成していない場合は、あなたの組織のためのユニークな**SSO識別子**を作成し、**タイプ**のドロップダウンから**SAML**を選択してください。この画面を開いたままにして、簡単に参照できるようにしてください。

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、あなたのSPエンティティID値から組電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。

SAMLアプリを作成します

Google Workspaceの管理者コンソールで、**アプリ** → **ウェブとモバイルアプリ**をナビゲーションから選択します。
ウェブとモバイルアプリの画面で、**アプリを追加** → **カスタムSAMLアプリを追加**を選択します。



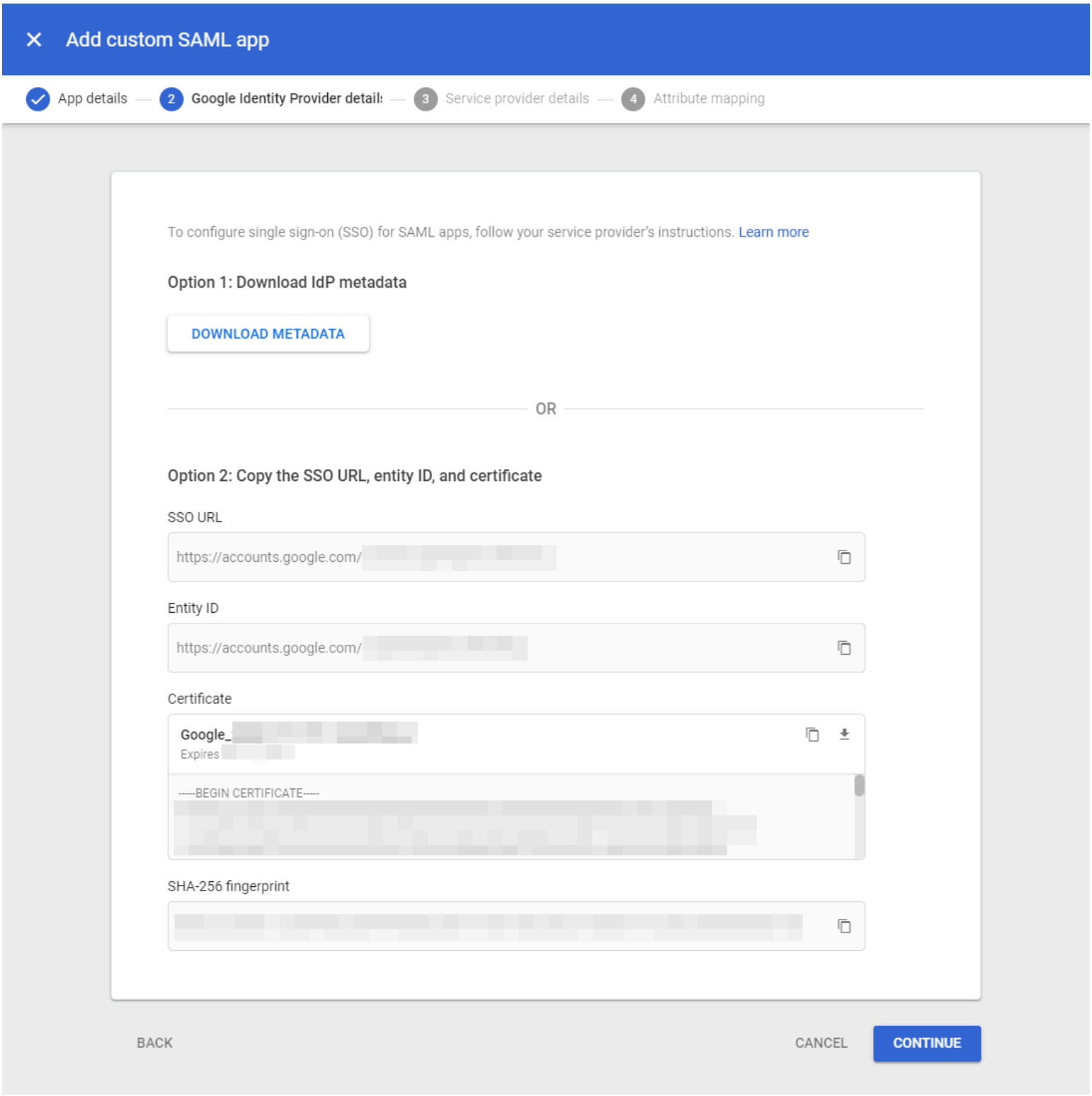
Create a SAML App

アプリの詳細

アプリ詳細画面で、アプリケーションにユニークなBitwarden専用の名前を付け、**続ける**ボタンを選択してください。

Google IDプロバイダーの詳細

Google IDプロバイダーの詳細画面で、あなたの**SSO URL**、**エンティティID**、
そして**証明書**を後のステップで使用するためにコピーしてください：



IdP Details

終了したら、**続行**を選択してください。

サービスプロバイダーの詳細

サービスプロバイダ詳細画面で、以下のフィールドを設定します:

フィールド	説明
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。
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、設定に基づいて異なります。
開始URL	必要に応じて、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に設定します。 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。
署名済みの返答	このボックスをチェックすると、WorkspaceがSAMLレスポンスに署名するようになります。チェックしない場合、ワークスペースはSAMLアサーションのみに署名します。
名前IDの形式	このフィールドを**Persistent**に設定してください。
名前ID	NameIDを入力するためのワークスペースユーザー属性を選択してください。

終了したら、**続ける**を選択してください。

属性マッピング

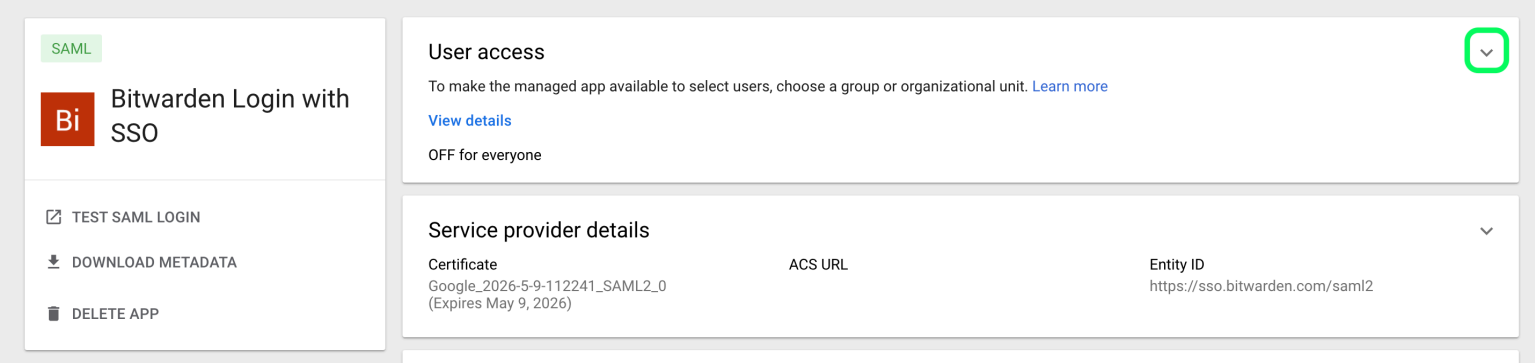
属性マッピング画面で、**マッピングを追加**ボタンを選択し、次のマッピングを構築します：

Googleディレクトリ属性	アプリの属性
プライマリーメールアドレス	メールアドレス

完了を選択してください。

アプリを起動してください

デフォルトでは、Workspace SAMLアプリは**全員に対してOFF**になります。SAMLアプリのユーザーアクセスセクションを開き、**全員に対してON**に設定するか、またはあなたのニーズに応じて特定のグループに設定してください。



User Access

あなたの変更を**保存**してください。
新しいWorkspaceアプリが既存のユーザーセッションに伝播するまでに最大24時間かかることにメモしてください。

ウェブアプリに戻る

この時点で、Google Workspace管理者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のレスポンスで期待するフォーマットを決定します。

サービスプロバイダーの設定

次のフィールドを、ワークスペース管理者コンソールで選択した選択肢に従って設定しますセットアップ中に：

フィールド	説明
名前ID形式	このフィールドをWorkspaceで選択された名前ID形式に設定します。
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。

フィールド	説明
最小入力署名アルゴリズム	デフォルトでは、Google WorkspaceはRSA SHA-256で署名します。ドロップダウンから`sha-256`を選択してください。
署名済みアサーションを期待する	BitwardenがSAMLアサーションに署名が必要かどうか。この設定は**チェックを外す**べきです。
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、しばしばワークスペース管理者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	このフィールドをWorkspaceの**エンティティID**に設定します。これは、Google IDプロバイダーの詳細セクションから取得するか、**メタデータをダウンロード**ボタンを使用して取得します。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	このフィールドをWorkspaceの**SSO URL**に設定し、Google IDプロバイダーの詳細セクションから取得するか、**メタデータをダウンロード**ボタンを使用します。
シングルログアウト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	取得した証明書を貼り付け、削除してください。 `-----BEGIN CERTIFICATE-----`

フィールド	説明
	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、 および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	デフォルトでは、Google WorkspaceはRSA SHA-256で署名します。 ドロップダウンから`sha-256` 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	Google WorkspaceがSAMLリクエストの署名を期待しているかどうか。

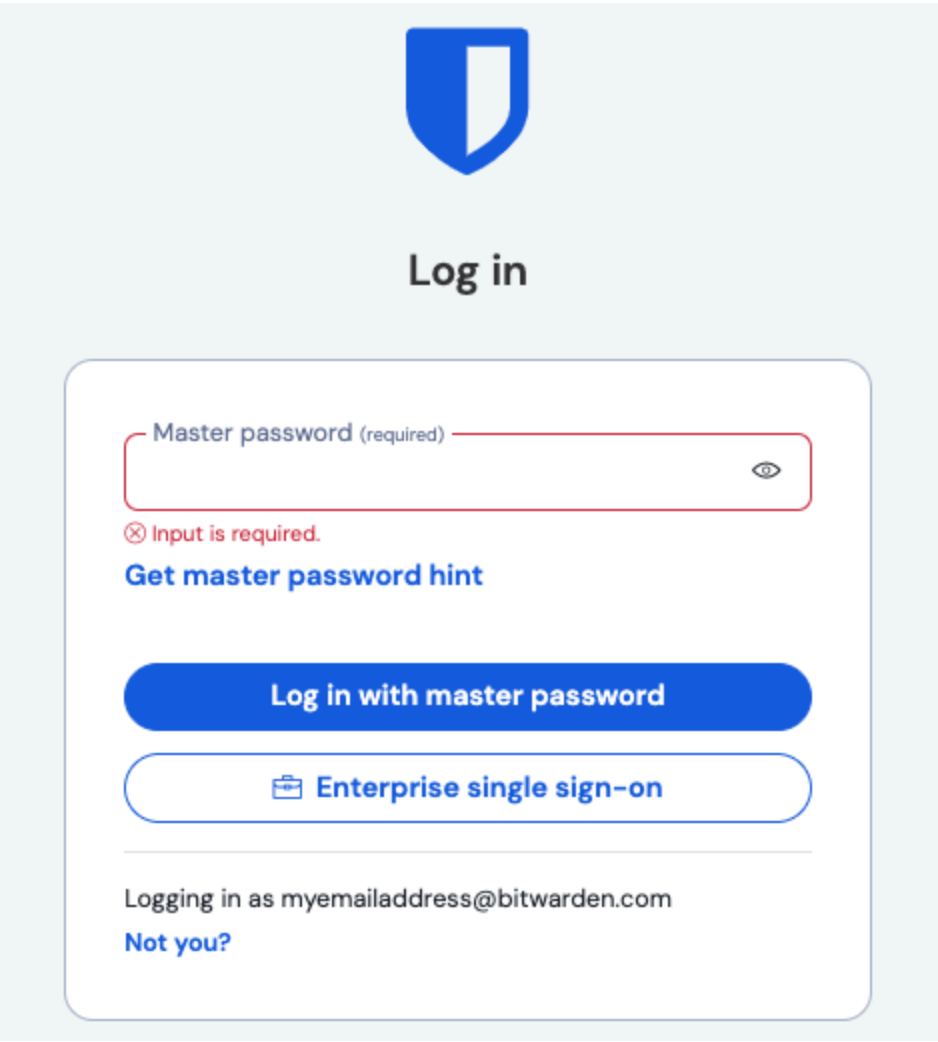
> **Note**
> X509証明書を完成させるとき、有効期限の日付をメモしてください。SSOエンドユーザーへのサービスの中断を防ぐために、
> 証明書を更新する必要があります。証明書が期限切れになった場合でも、
> 管理者と所有者のアカウントは常にメールアドレスとマスターパスワードでログインできます。

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

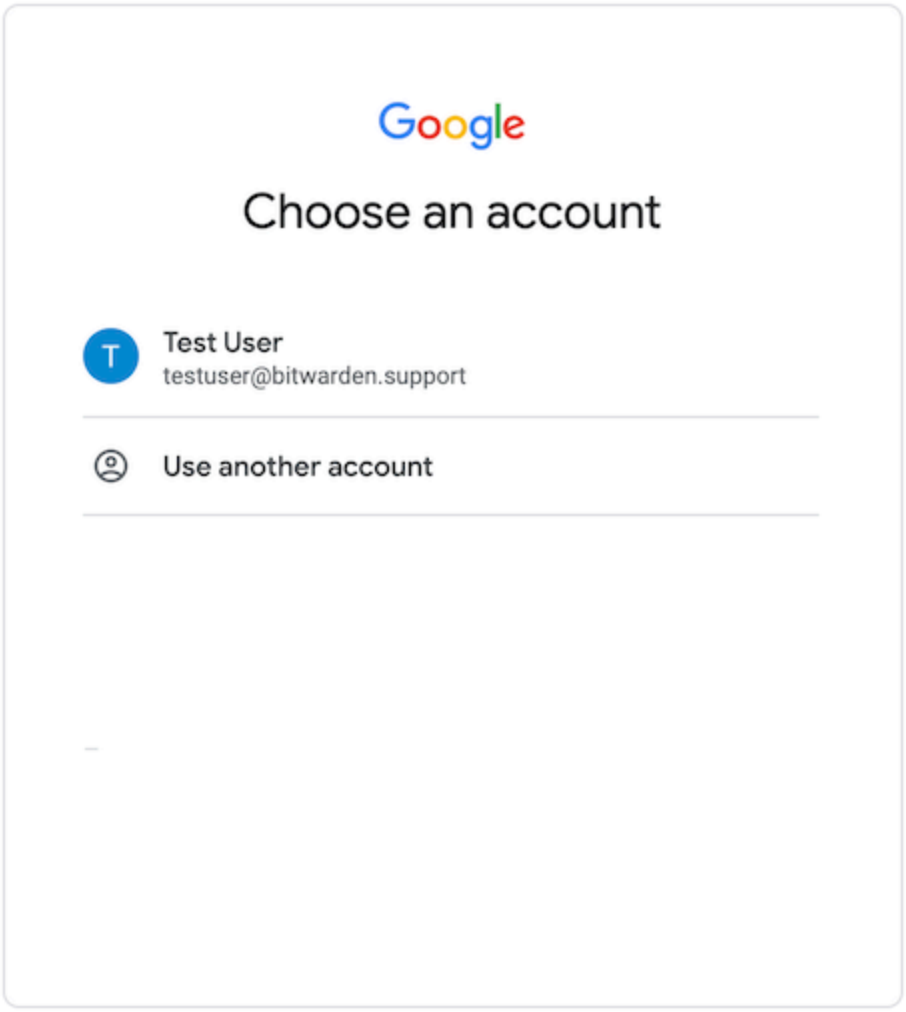
設定をテストする

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、Google Workspaceのログイン画面にリダイレクトされます。



Login

あなたのワークスペース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。