Duo SAML 実装

Duo 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**Duo特有の**ヘルプが含まれています。
別のIdPのSSOでのログインを設定するためのヘルプは、SAML 2.0設定を参照してください。

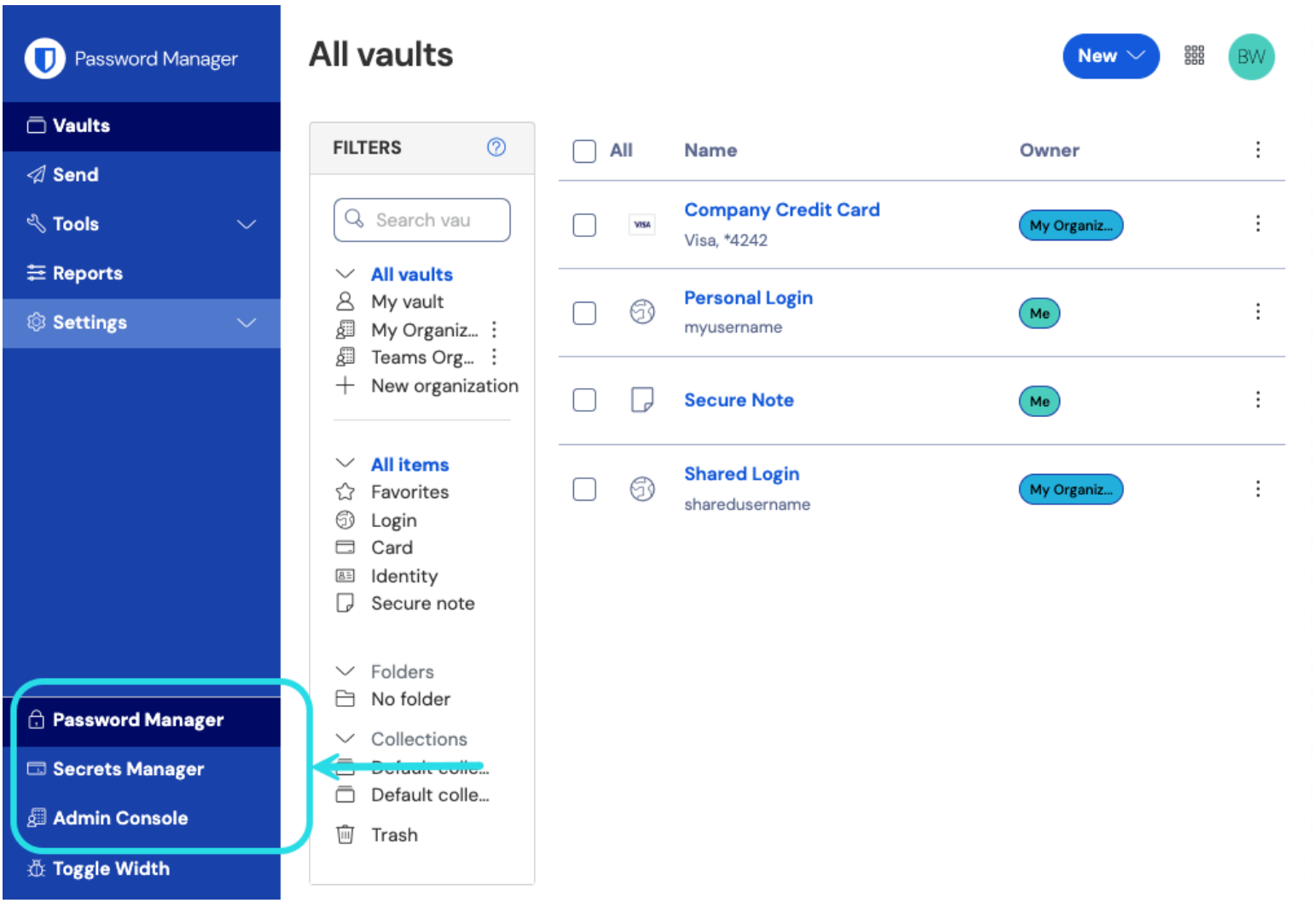
設定は、Bitwardenウェブアプリと Duo管理者ポータルを同時に操作することを含みます。進行するにあたり、両方をすぐに利用できる状態にして、記録されている順序で手順を完了することをお勧めします。

> **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

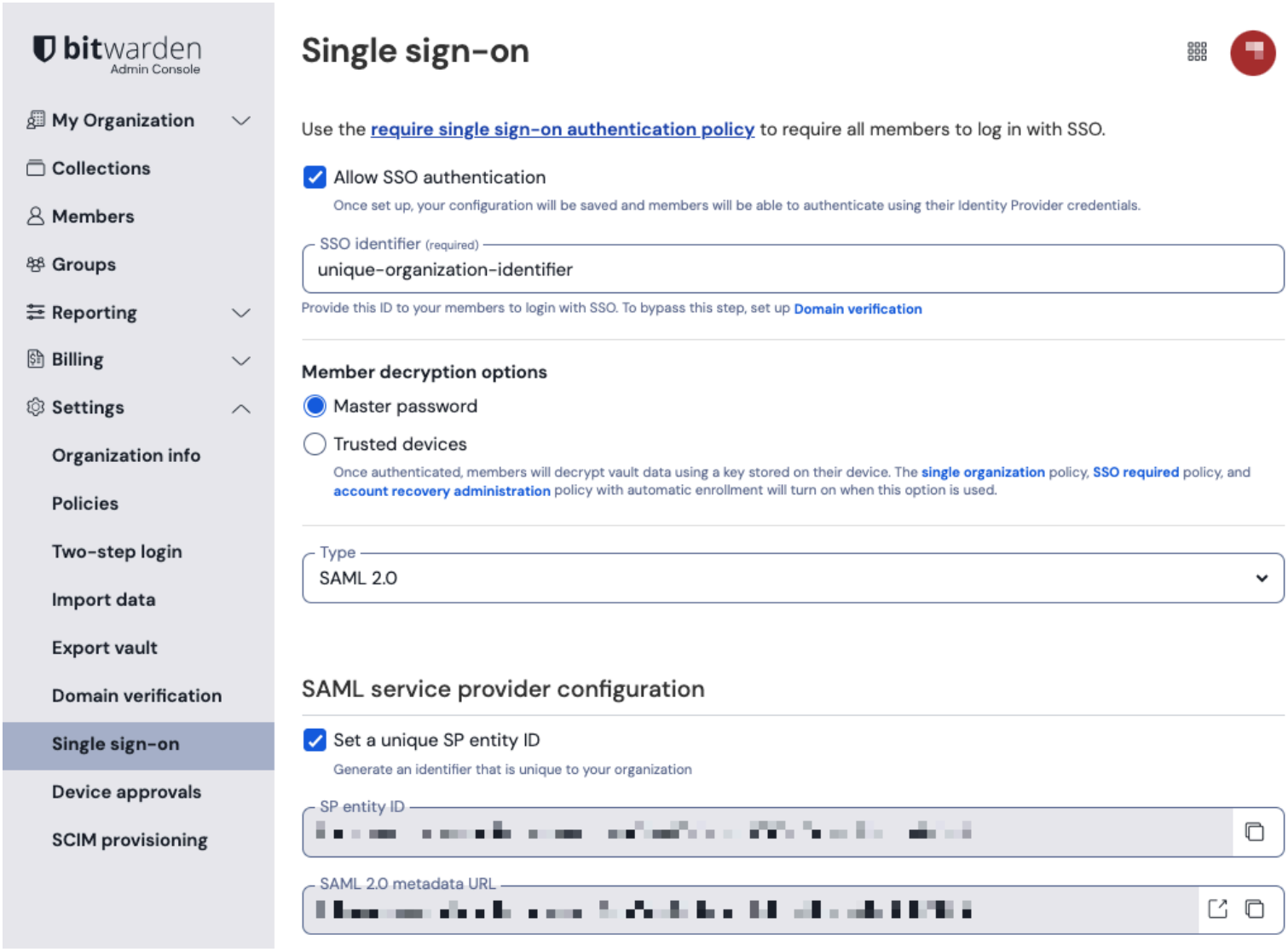
> **Warning**
>
> This article assumes that you have already set up Duo with an Identity Provider. If you haven't, see Duo's documentation for details.

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。

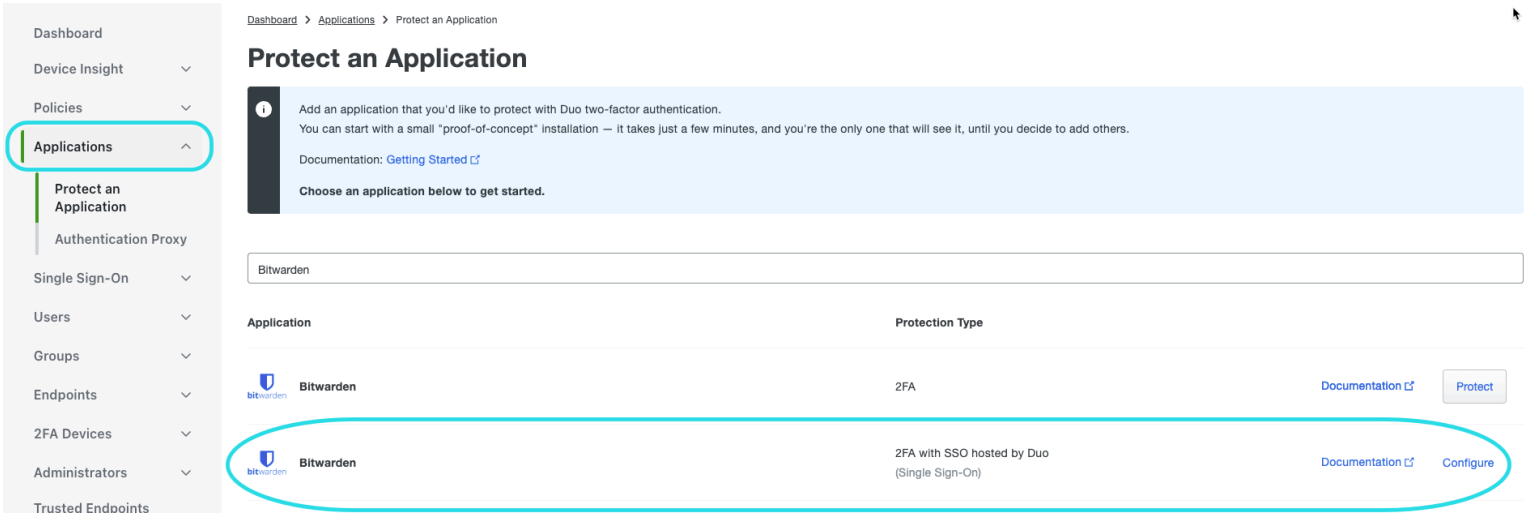
この段階で、必要に応じて**ユニークなSPエンティティIDを設定する**オプションをオフにすることができます。これを行うと、組電IDがSPエンティティID値から削除されますが、ほとんどの場合では、このオプションをオンにしておくことをお勧めします。

> **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。

アプリケーションを保護する

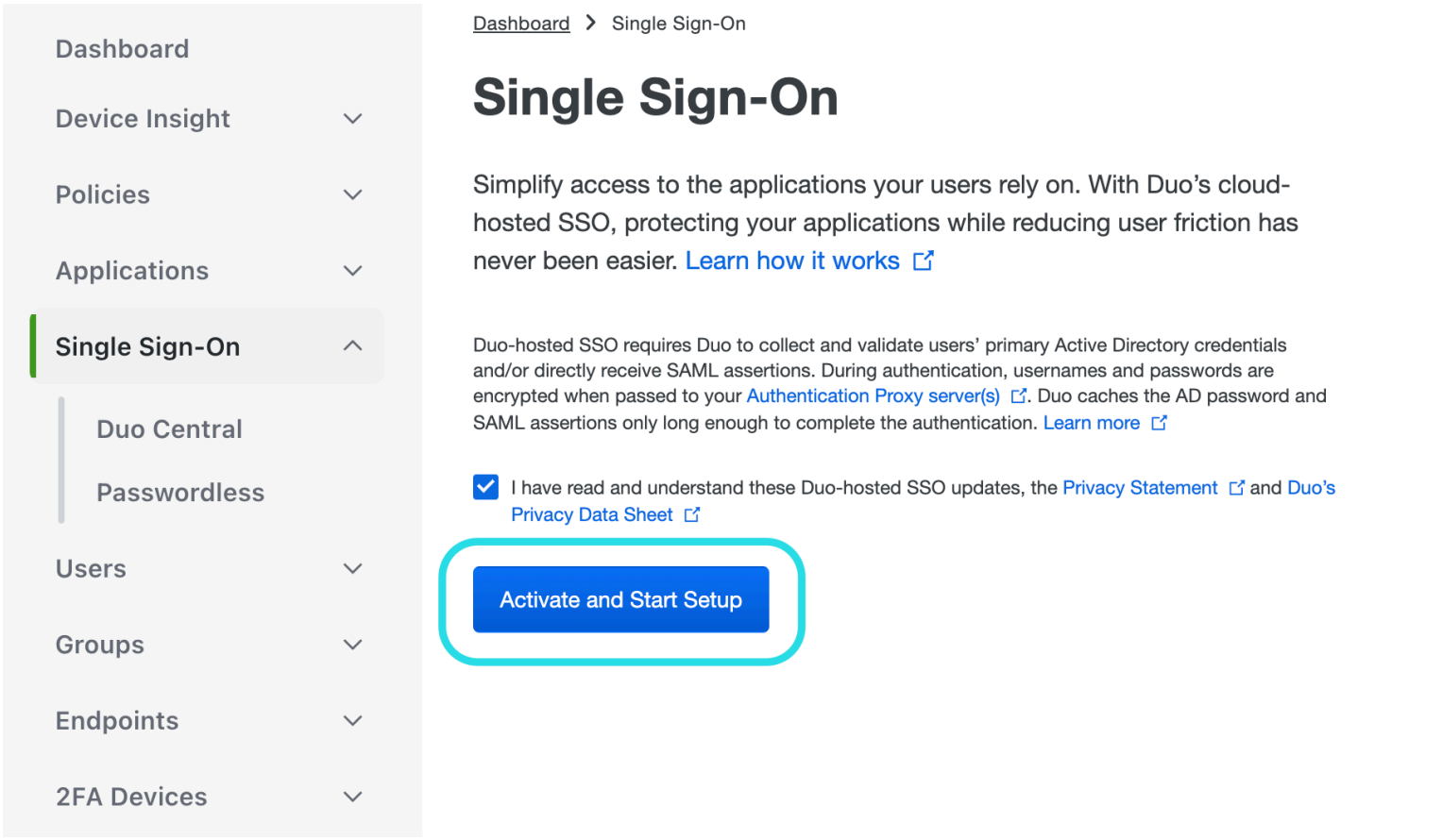
続行する前に、Duoのドキュメンテーションを参照して、Duo Single Sign-OnがあなたのSAML IDプロバイダーと認証のために設定されていることを確認してください。

Duo管理者ポータルで、**アプリケーション**画面に移動し、**アプリケーションを保護する**を選択します。検索バーに**Bitwarden**を入力し、**DuoがホストするBitwarden 二要素認証とSSO**アプリケーションの**設定**を選択します：



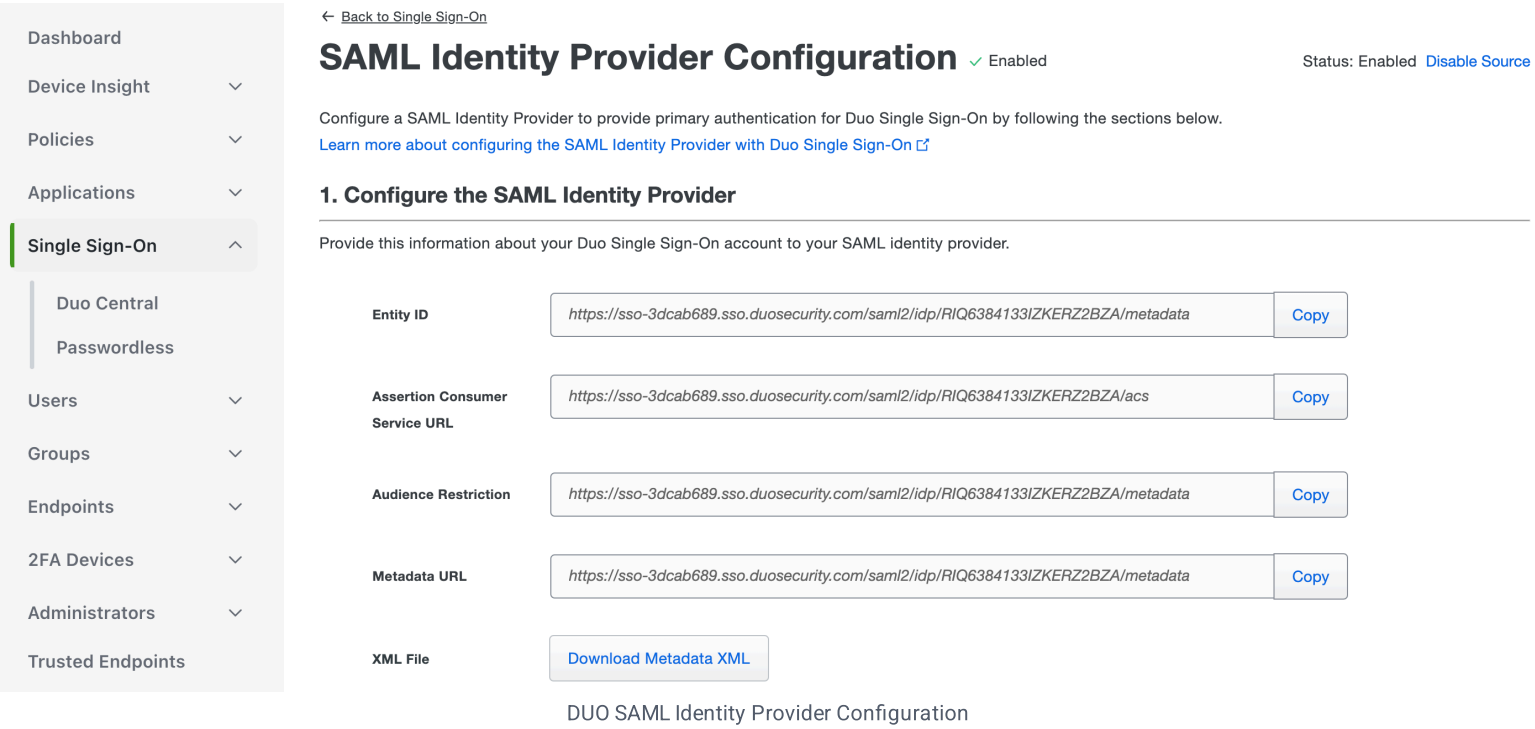
Duo Bitwarden Application

新しく作成されたアプリケーションに対して**アクティベートしてセットアップを開始**を選択します。



Duo Activation and Setup

次の手順と設定をアプリケーション設定画面で完了してください。これらの一部は、Bitwardenシングルサインオン画面から取得する必要があります：



DUO SAML Identity Provider Configuration

メタデータ

メタデータのセクションでは何も編集する必要はありませんが、後でこれらの値を使用する必要があります。

URLs for Configuration

ダウンロード

証明書をダウンロードボタンを選択して、X.509証明書をダウンロードしてください。これは設定の後半で使用する必要があります。

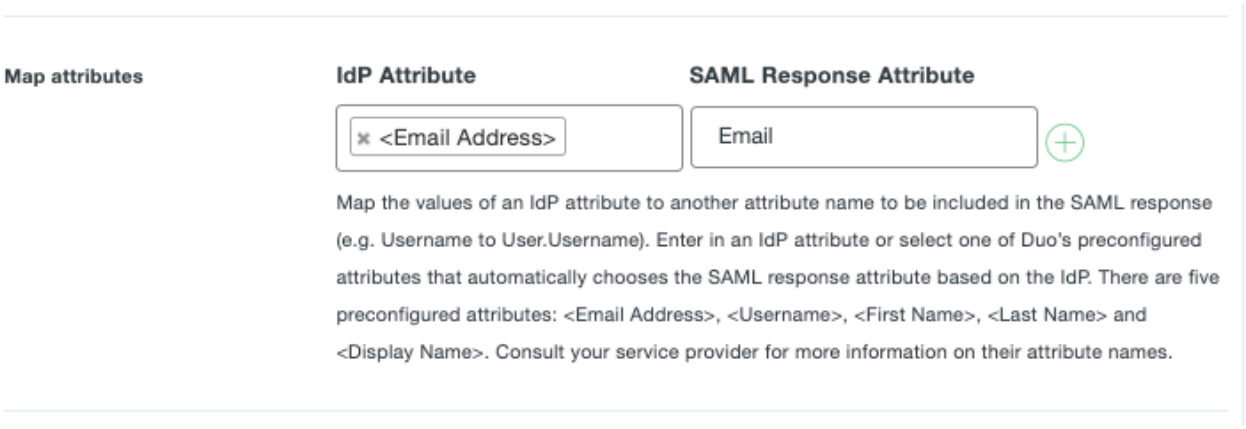
サービスプロバイダー

フィールド	説明
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。

フィールド	説明
アサーションコンシューマーサービス（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。
サービスプロバイダーログインURL	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ために、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。

SAMLレスポンス

フィールド	説明
NameID形式	このフィールドをSAML NameID形式に設定し、DuoがSAMLレスポンスでSendするようにします。
NameID属性	このフィールドを設定し、応答のNameIDを生成するDuo属性にします。
署名アルゴリズム	このフィールドをSAMLアサーションとレスポンスに使用する暗号化アルゴリズムに設定します。
署名オプション	**署名応答**を選択するか、**署名主張**を選択するか、または両方を選択してください。
地図の属性	これらのフィールドを使用して、IdP属性をSAMLレスポンス属性にマッピングします。あなたが設定したNameID属性に関係なく、IdPの`メールアドレス`属性を`メール`にマッピングします。以下のスクリーンショットのように：



Required Attribute Mapping

これらのフィールドの設定が完了したら、**保存**して変更を保存してください。

ウェブアプリに戻る

この時点で、Duo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、Duo管理者ポータルでアプリケーション設定中に選択した選択肢に従って設定してください：

フィールド	説明
名前ID形式	NameID形式をSAMLリクエストで使用する（`NameIDPolicy`）。 このフィールドを選択されたNameID形式に設定してください。
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は、`rsa-sha256`です。
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、 Duo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	BitwardenがSAMLレスポンスで受け入れる最小の署名アルゴリズム。デフォルトでは、Duoは`rsa-sha256`で署名するので、別のオプションを選択していない限り、 そのオプションをドロップダウンから選択してください。

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を求めるかどうか。このボックスをチェックしてください、もしあなたが署名確認の署名オプションを選択した場合。
証明書を検証する	あなたのIdPから信頼できるCAを通じて信頼性のある有効な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 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Duo管理者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Duoアプリケーションの**エンティティID**の値を入力してください。これはDuoアプリの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	このフィールドを**HTTP Post**に設定してください。
シングルサインオンサービスURL	Duoアプリケーションの**シングルサインオンURL**の値を入力してください。これはDuoアプリの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	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、あなたのDuoアプリケーションの**シングルログアウトURL**の値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**。

フィールド	説明
アウトバウンド署名アルゴリズム	このフィールドを選択されたSAMLレスポンス署名アルゴリズムに設定します。
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必要です	Duo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。

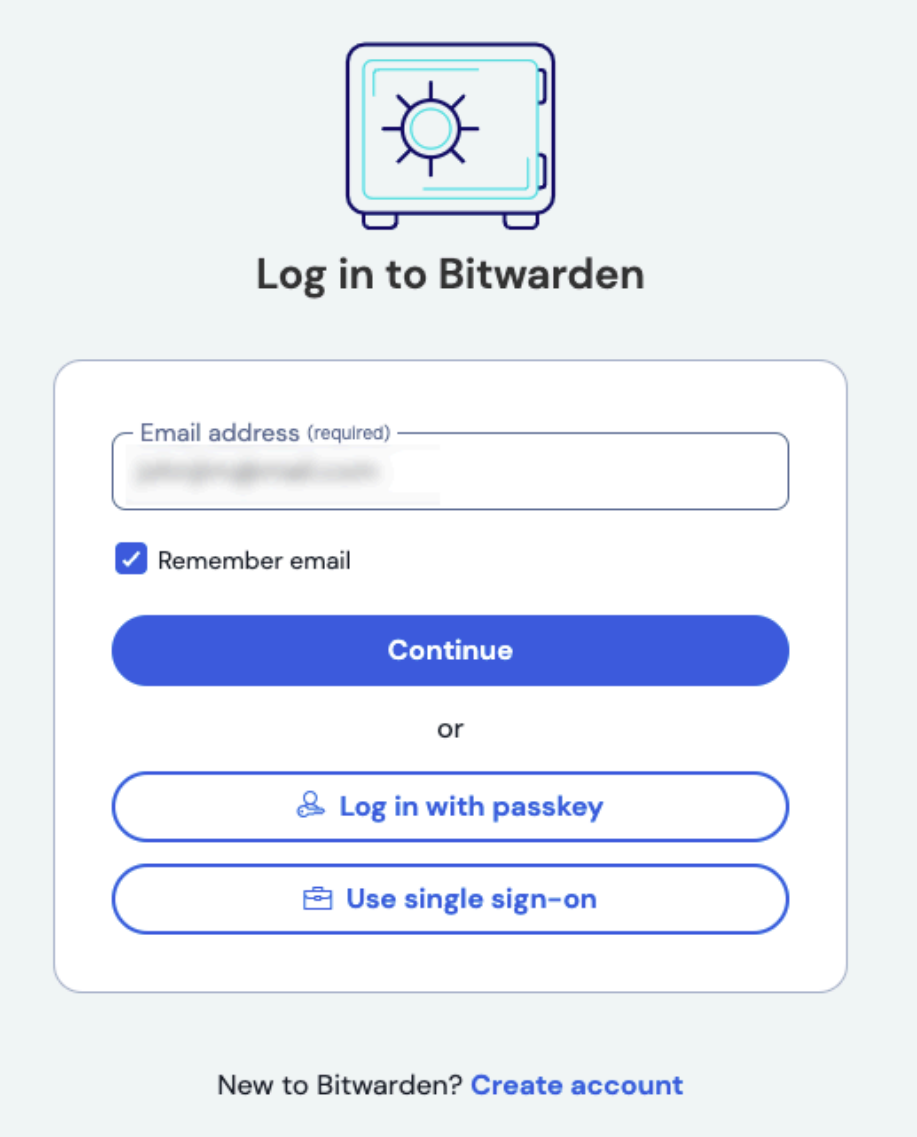
IDプロバイダーの設定が完了したら、**保存**してください。

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、
あなたはソースIdPのログイン画面にリダイレクトされます。

あなたのIdPログインとDuo二要素で認証した後、Bitwarden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。