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 >

AuthO SAMLの実装

ヘルプセンターで表示:
https://bitwarden.com/help/saml-auth0/

Auth0 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**Auth0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 Auth0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。

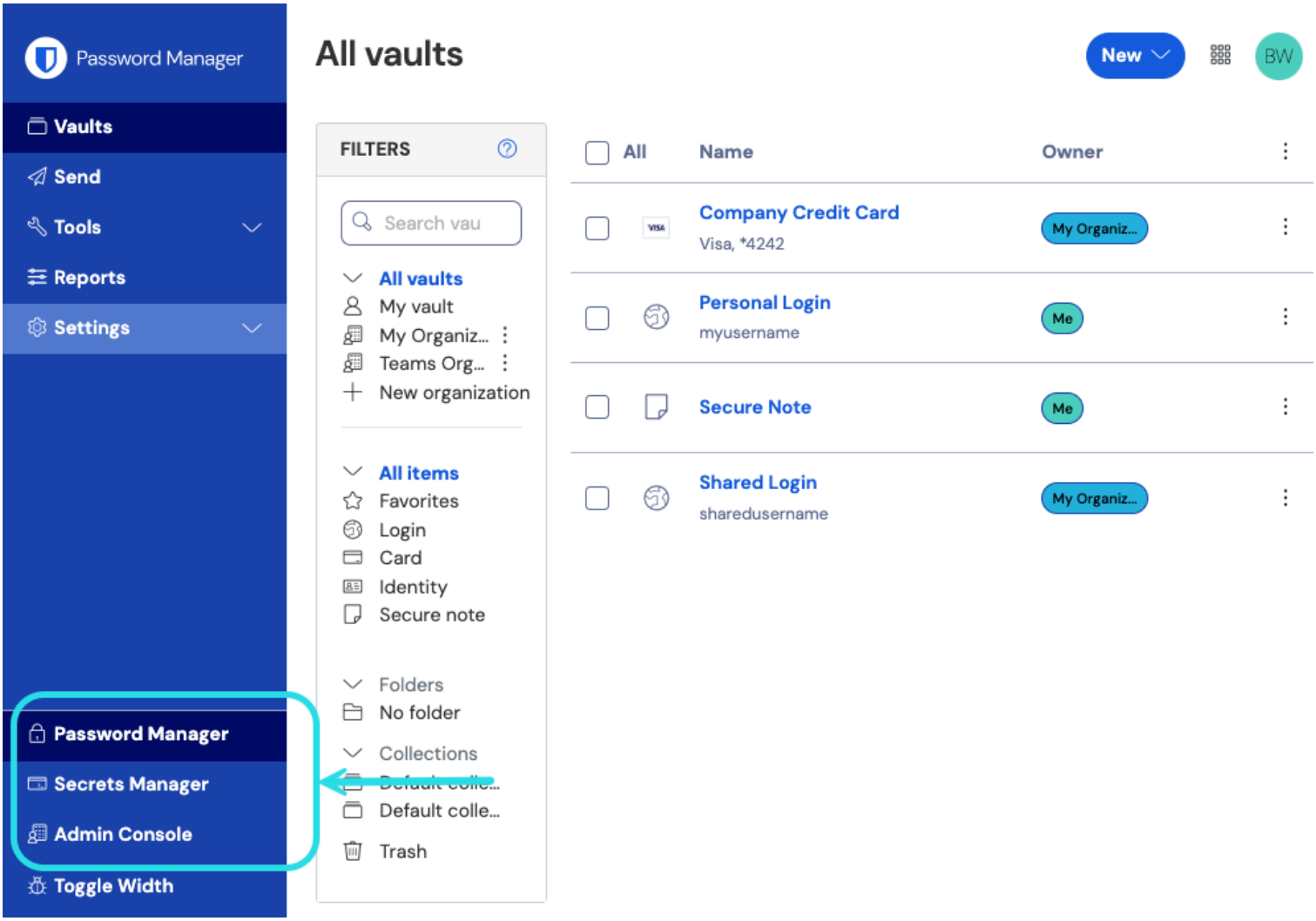
Tip

Already an SSO expert? Skip the instructions in this article and download screenshots of sample configurations to compare against your own.

Download Sample

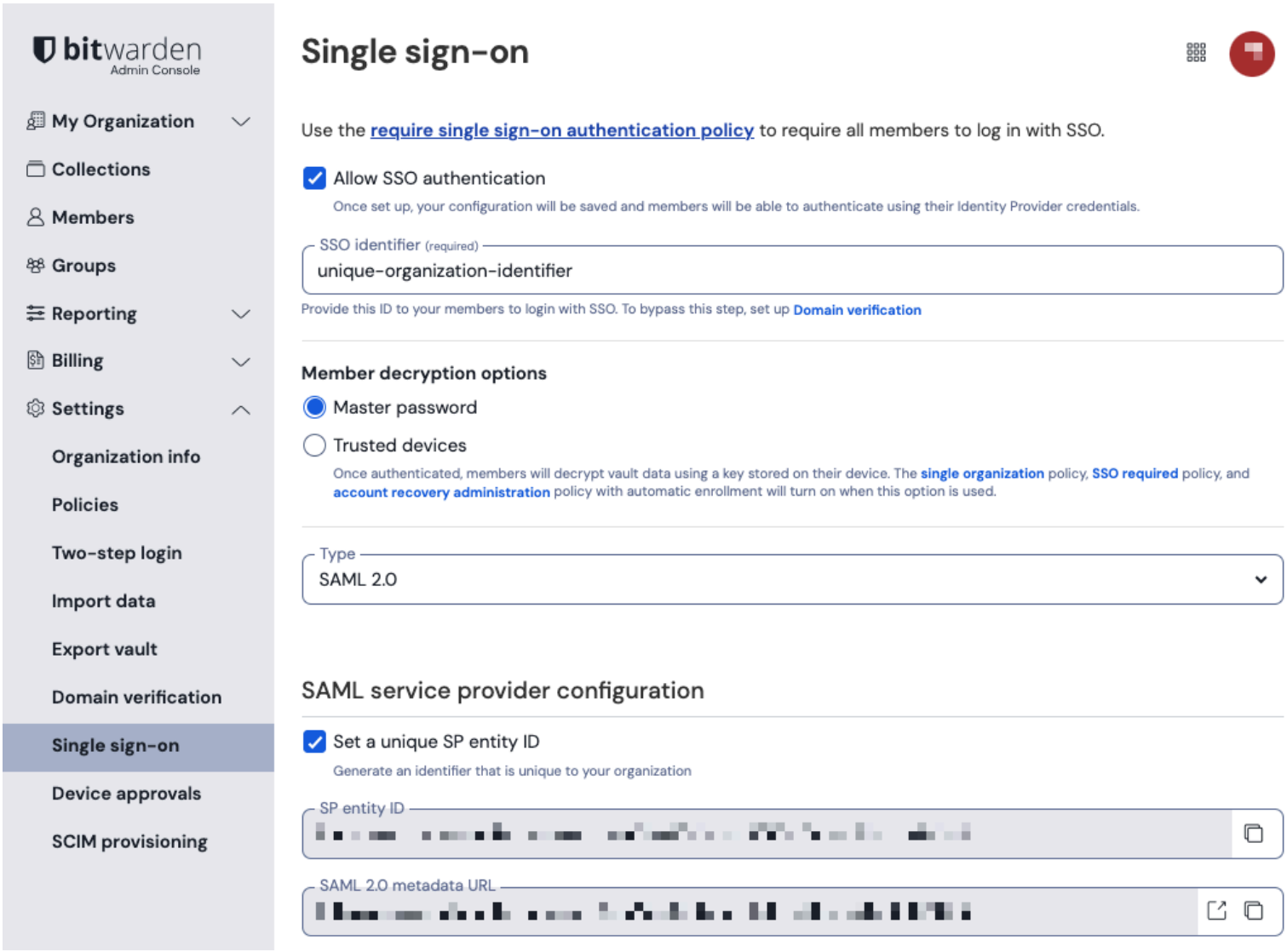
ウェブアプリでSSOを開く

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

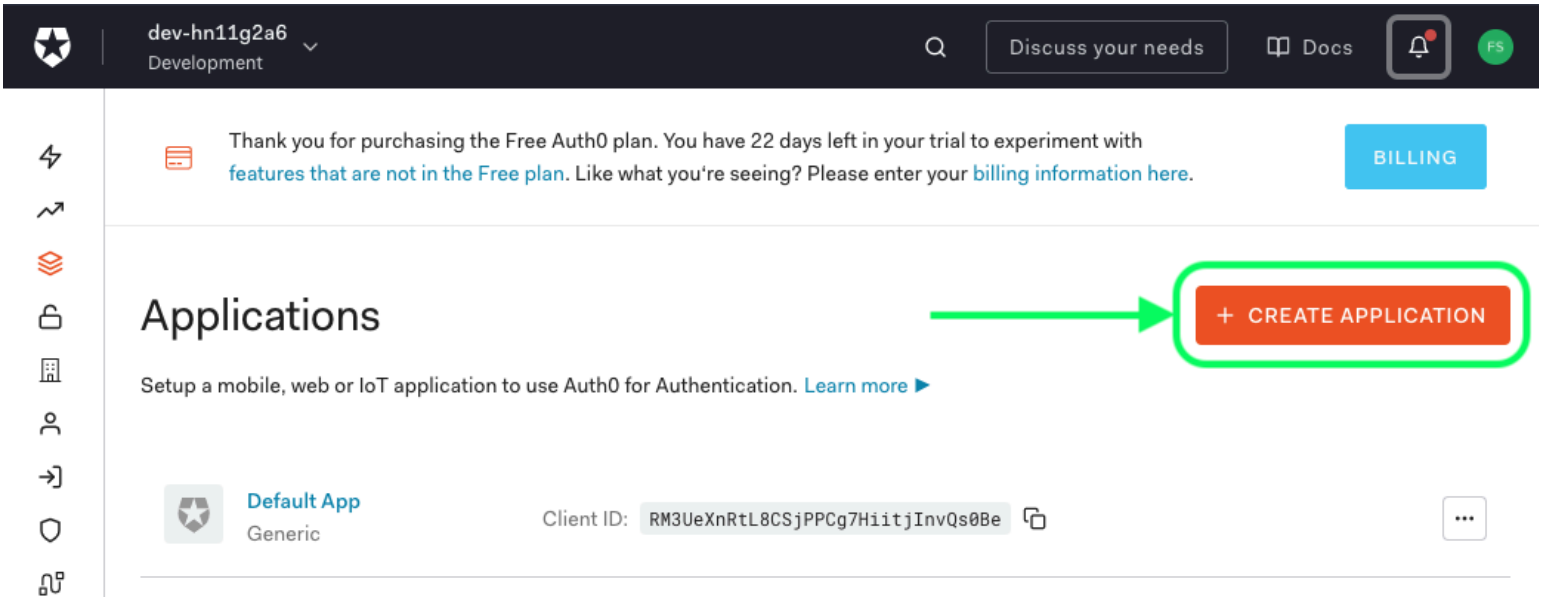
まだ作成していない場合は、あなたの**SSO識別子**を組織用に作成し、**SAML**を**タイプ**のドロップダウンから選択してください。この画面を開いたままにして、簡単に参照できるようにしてください。

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、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。

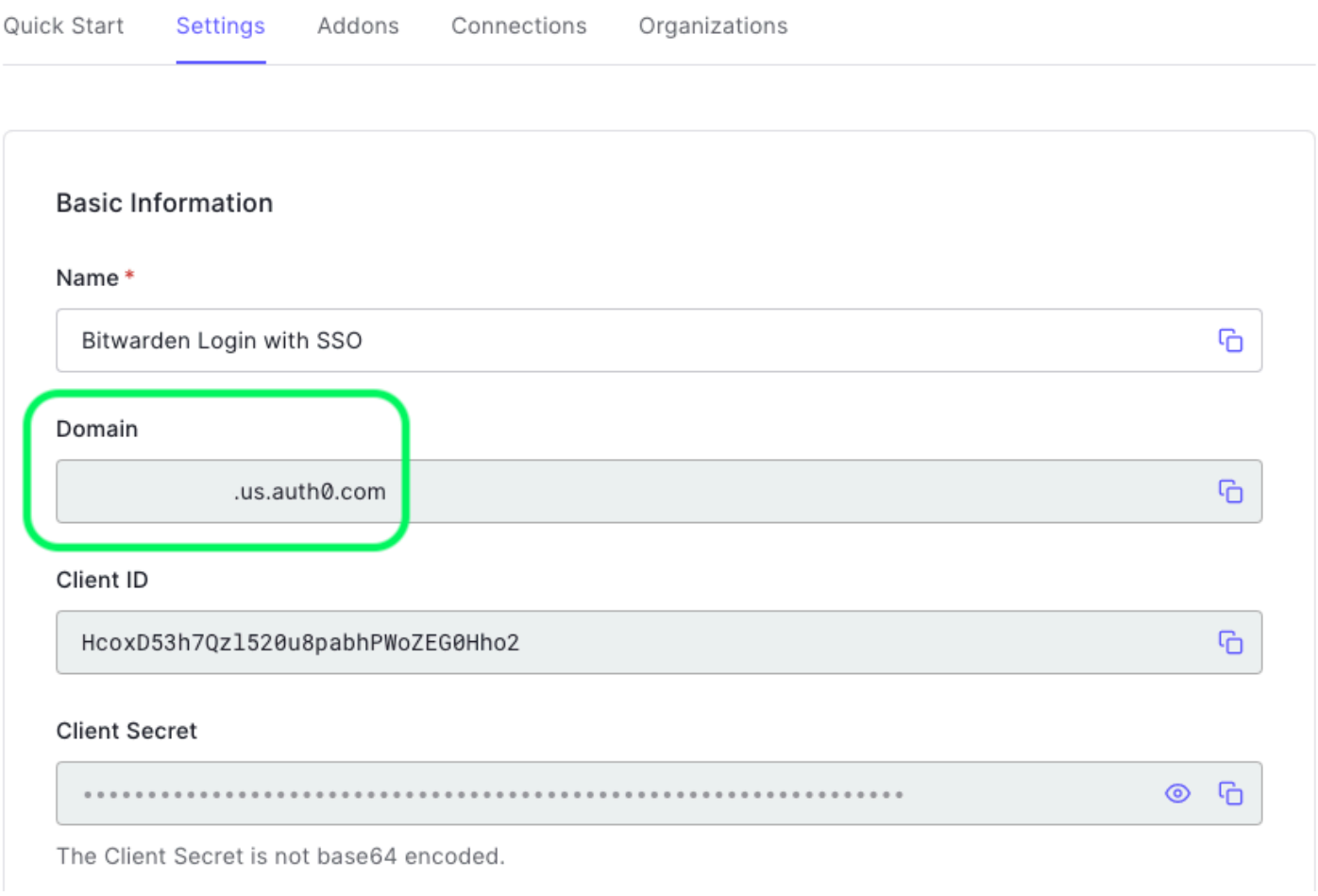
Auth0アプリケーションを作成する

Auth0ポータルで、アプリケーションメニューを使用して、**通常のWebアプリケーション**を作成します：



Auth0 Create Application

設定タブをクリックし、以下の情報を設定します。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：

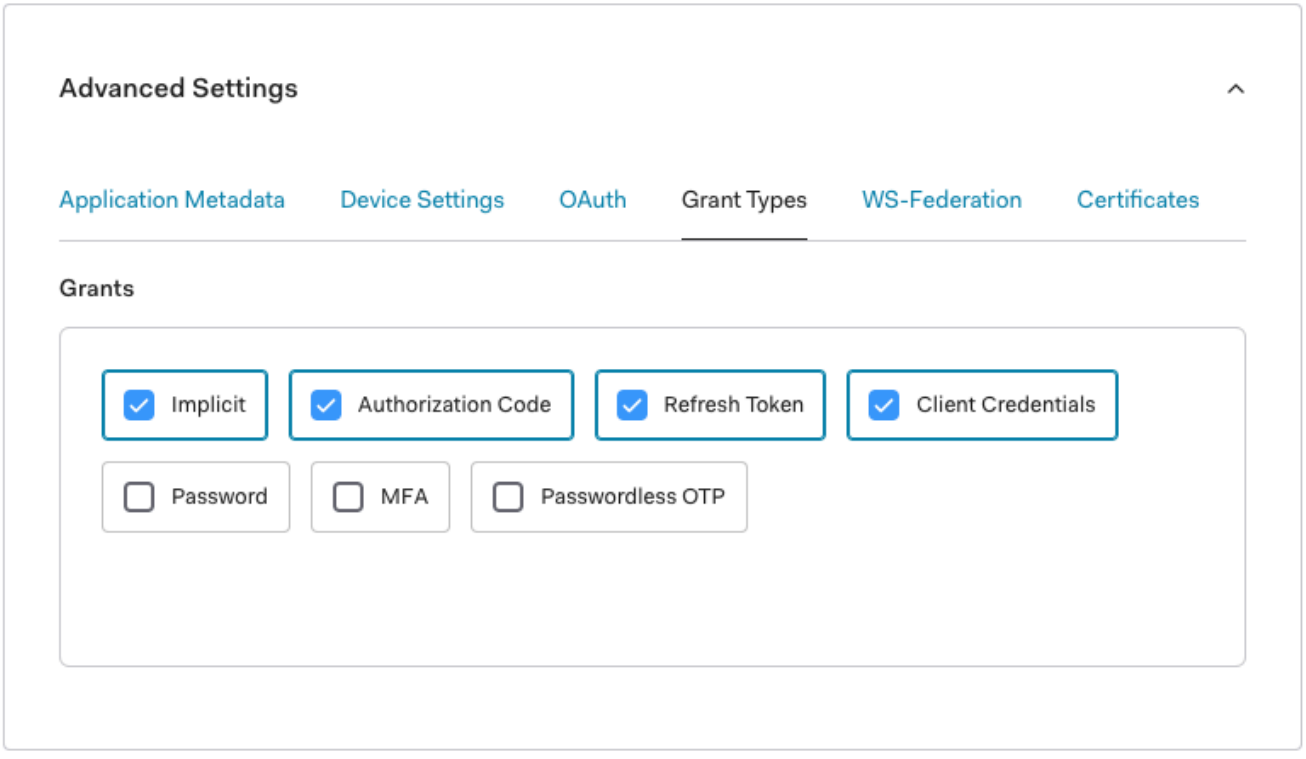


Auth0 Settings

Auth0 設定	説明
お名前	アプリケーションにBitwarden特有の名前を付けてください。
ドメイン	この値をメモしてください。それは後のステップで必要になります。
アプリケーションタイプ	**通常のウェブアプリケーション**を選択してください。
トークンエンドポイント認証方法	**投稿**（HTTP Post）を選択し、これは後で**設定する**属性にバインディングタイプとしてマッピングされます。
アプリケーションログインURI	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。
許可されたコールバックURLS	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、設定に基づいて異なります。

助成金のタイプ

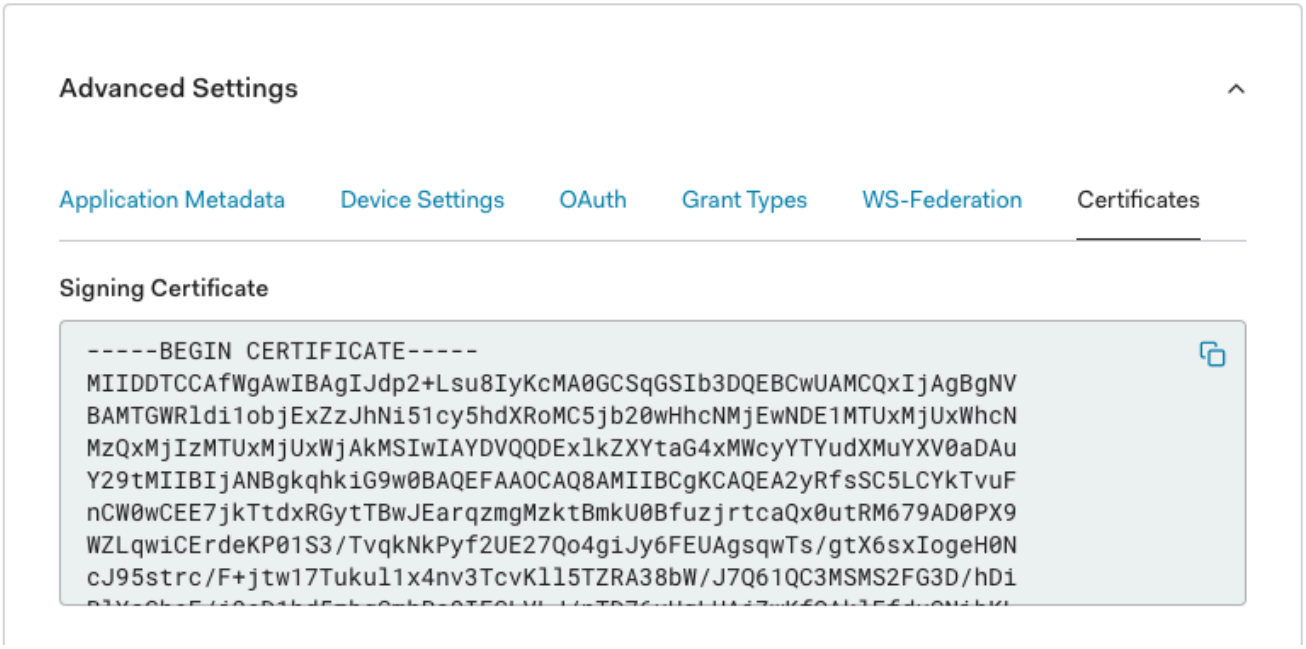
詳細設定 → 許可タイプセクションで、以下の許可タイプが選択されていることを確認してください（事前に選択されている場合があります）：



Application Grant Types

証明書

詳細設定 → **証明書**セクションで、署名証明書をコピーまたはダウンロードしてください。まだそれに何もする必要はありませんが、後でそれを参照する必要があります。

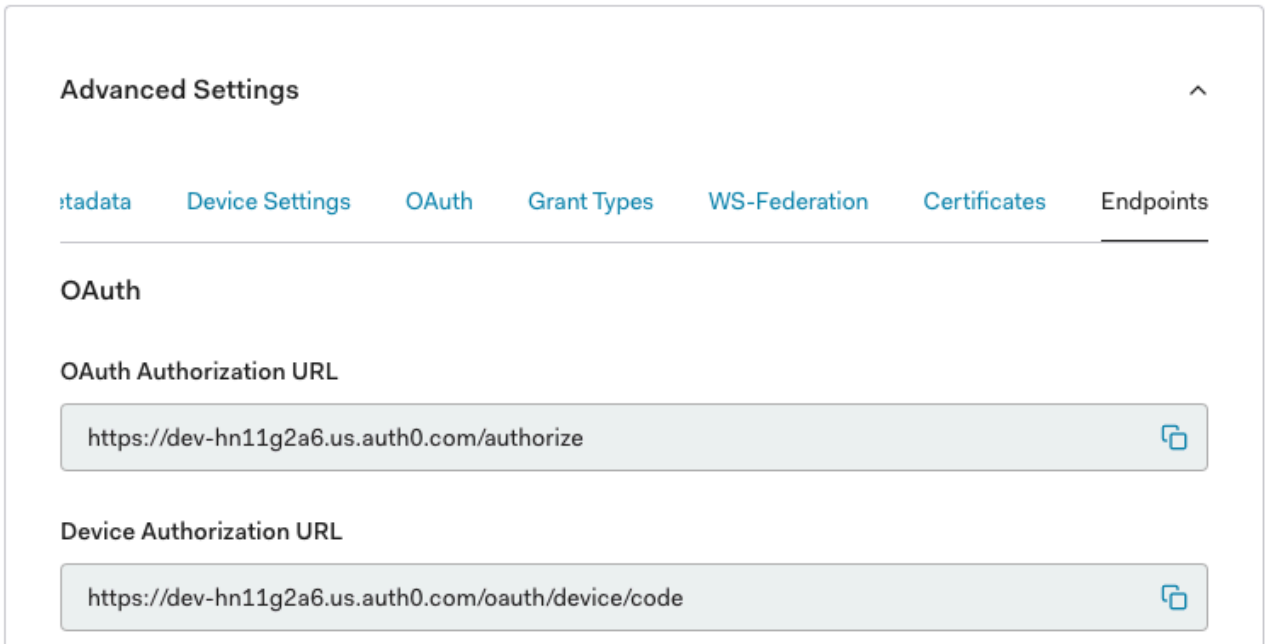


Auth0 Certificate

エンドポイント

詳細設定 → **エンドポイント**セクションで何も編集する必要はありませんが、後で参照するためにSAMLエンドポイントが必要になります。

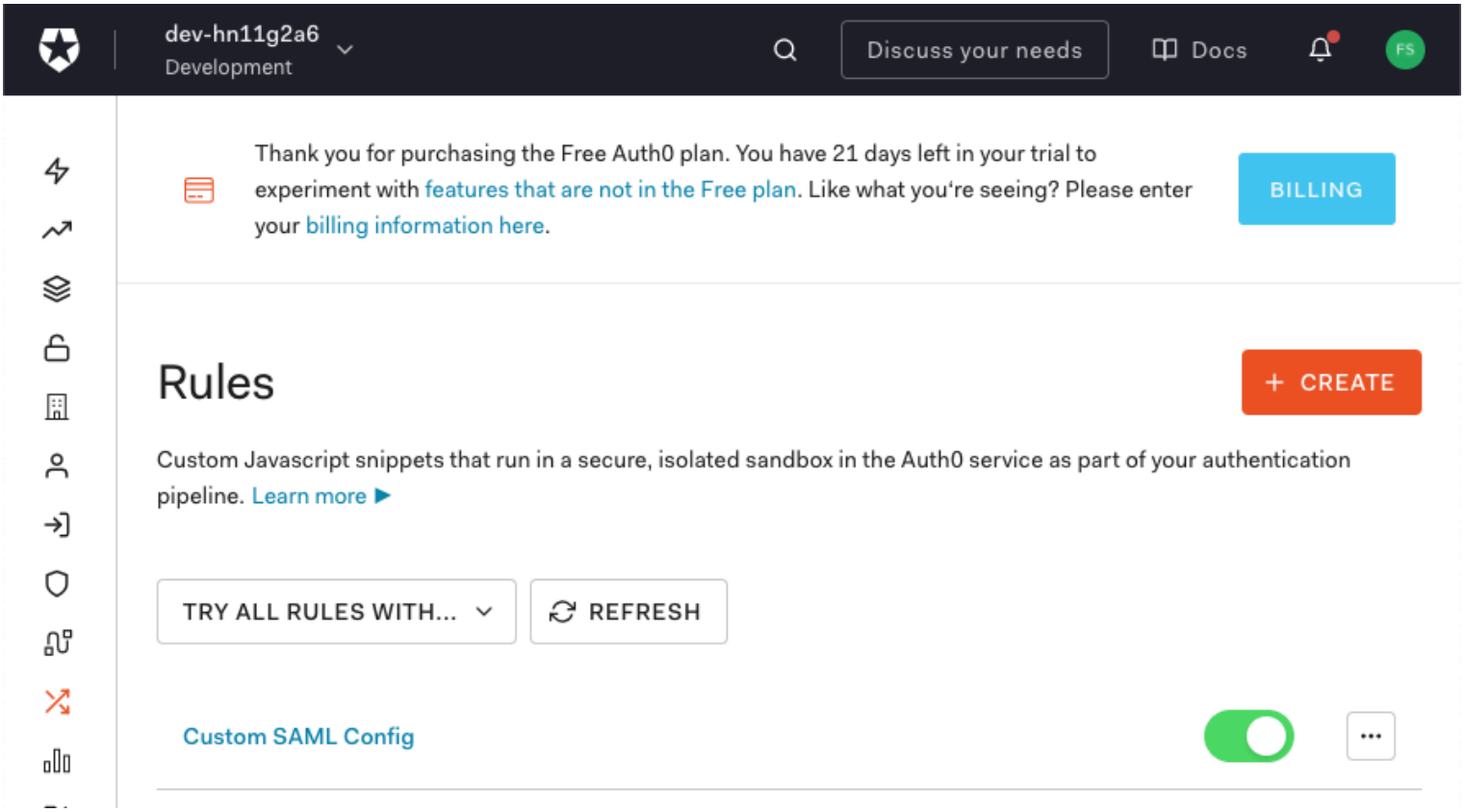
> **Tip**
> In smaller windows, the **Endpoints** tab can disappear behind the edge of the browser. If you're having trouble finding it, click the **Certificates** tab and hit the Right Arrow key (→).



Auth0 Endpoints

Auth0ルールを設定する

あなたのアプリケーションのSAMLレスポンスの振る舞いをカスタマイズするためのルールを作成してください。Auth0は数値のオプションを提供していますが、このセクションではBitwardenのオプションに特にマッピングするものだけに焦点を当てます。カスタムSAML設定ルールセットを作成するには、**認証パイプライン** → **ルール**メニューを使用して＋ **ルールを作成**します:



Auth0 Rules

次のいずれかを設定することができます:

キー	説明
署名アルゴリズム	Auth0がSAMLアサーションまたはレスポンスに署名するために使用するアルゴリズム。デフォルトでは、`rsa-sha1` が含まれますが、この値は`rsa-sha256`に設定するべきです。 この値を変更する場合、あなたは次のことを行う必要があります： -`digestAlgorithm` を`sha256`に設定します。 -Bitwardenの**最小入力署名アルゴリズム**を`rsa-sha256`に設定します。
ダイジェストアルゴリズム	SAMLアサーションまたはレスポンスのダイジェストを計算するためのアルゴリズム。デフォルトでは、`sha-1`。`signatureAlgorithm` の値も`sha256`に設定する必要があります。
サインレスポンス	デフォルトでは、Auth0はSAMLアサーションのみに署名します。これを`true` に設定して、アサーションの代わりにSAMLレスポンスに署名します。

キー	説明
名前識別子形式	デフォルトでは、urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified。この値は任意のSAML NameID形式に設定できます。もしそうなら、SP **名前ID形式**フィールドを対応するオプションに変更してください（こちらを参照）。

以下のような**スクリプト**を使用して、これらのルールを実装してください。ヘルプが必要な場合は、Auth0のドキュメンテーションを参照してください。

```Bash
function (user, context, callback) {
    context.samlConfiguration.signatureAlgorithm = "rsa-sha256";
    context.samlConfiguration.digestAlgorithm = "sha256";
    context.samlConfiguration.signResponse = "true";
    context.samlConfiguration.nameIdentifierFormat = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
    context.samlConfiguration.binding = "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect";
    callback(null, user, context);
}
```

ウェブアプリに戻る

この時点で、Auth0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

あなたがカスタムルールを設定していない限り、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。カスタムルールを設定したり、実装にさらなる変更を加えたい場合は、関連するフィールドを編集してください。

フィールド	説明
名前ID形式	NameID形式をSAMLリクエストで指定します（NameIDPolicy）。省略するには、**設定されていません**に設定します。
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	Bitwarden SAMLリクエストが署名されるか/いつ署名されるか。デフォルトでは、Auth0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、Auth0はrsa-sha1で署名します。ドロップダウンからrsa-sha256 を選択してください。ただし、カスタム署名ルールを設定している場合は除きます。

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。デフォルトでは、AuthOはSAMLアサーションに署名しますので、カスタム署名ルールを設定していない限り、このボックスをチェックしてください。
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 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AuthO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AuthOアプリケーションの**ドメイン**値を入力してください（こちらを参照）、接頭辞として`urn:`を使用します。例えば`urn:bw-help.us.auth0.com`のようになります。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	あなたのAuthOアプリケーションで指定された**トークンエンドポイント認証方法**の値と一致するように、HTTP POSTを選択してください。
シングルサインオンサービスURL	あなたのAuthOアプリケーションの**SAMLプロトコルURL**を入力してください（エンドポイントを参照）。例えば、`https://bw-help.us.auth0.com/samlp/HcpxD63h7Qzl420u8qachPWoZEG0Hho2`。
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	取得した署名証明書を貼り付け、削除します
	
	`-----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**。

アウトバウンド署名アルゴリズム	デフォルトでは、AuthOは`rsa-sha1`で署名します。`rsa-sha256` を選択してください、あなたがカスタム署名ルールを設定していない限り。

フィールド	説明
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を希望します	AuthOがSAMLリクエストの署名を期待しているかどうか。

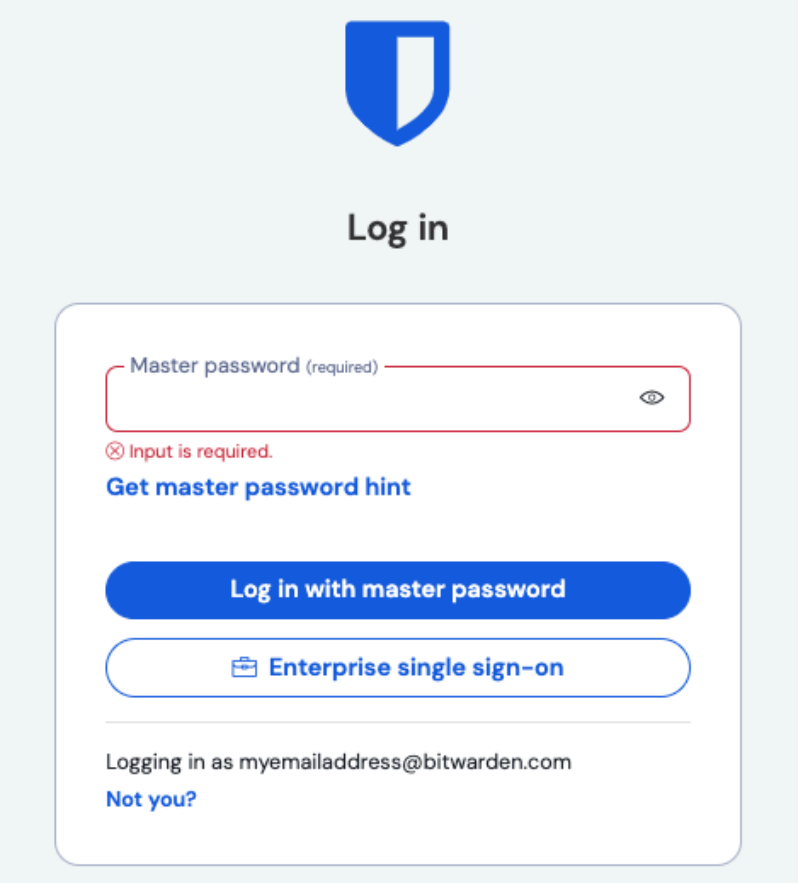
> **Note**
> X509証明書を完成させるとき、有効期限の日付をメモしてください。SSOエンドユーザーへのサービスの中断を防ぐために、証明書を更新する必要があります。証明書が期限切れになった場合でも、管理者と所有者のアカウントは常にメールアドレスとマスターパスワードでログインできます。

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

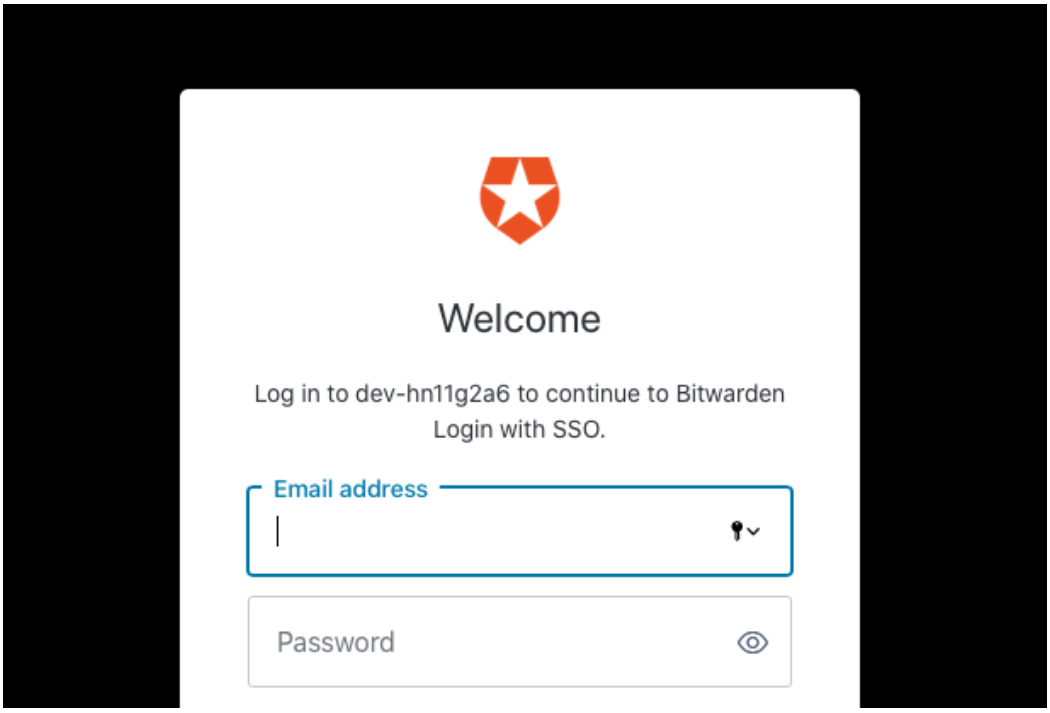
設定をテストする

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、Auth0のログイン画面にリダイレクトされます。



Auth0 Login

あなたのAuth0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。