ADFS OIDC 実装

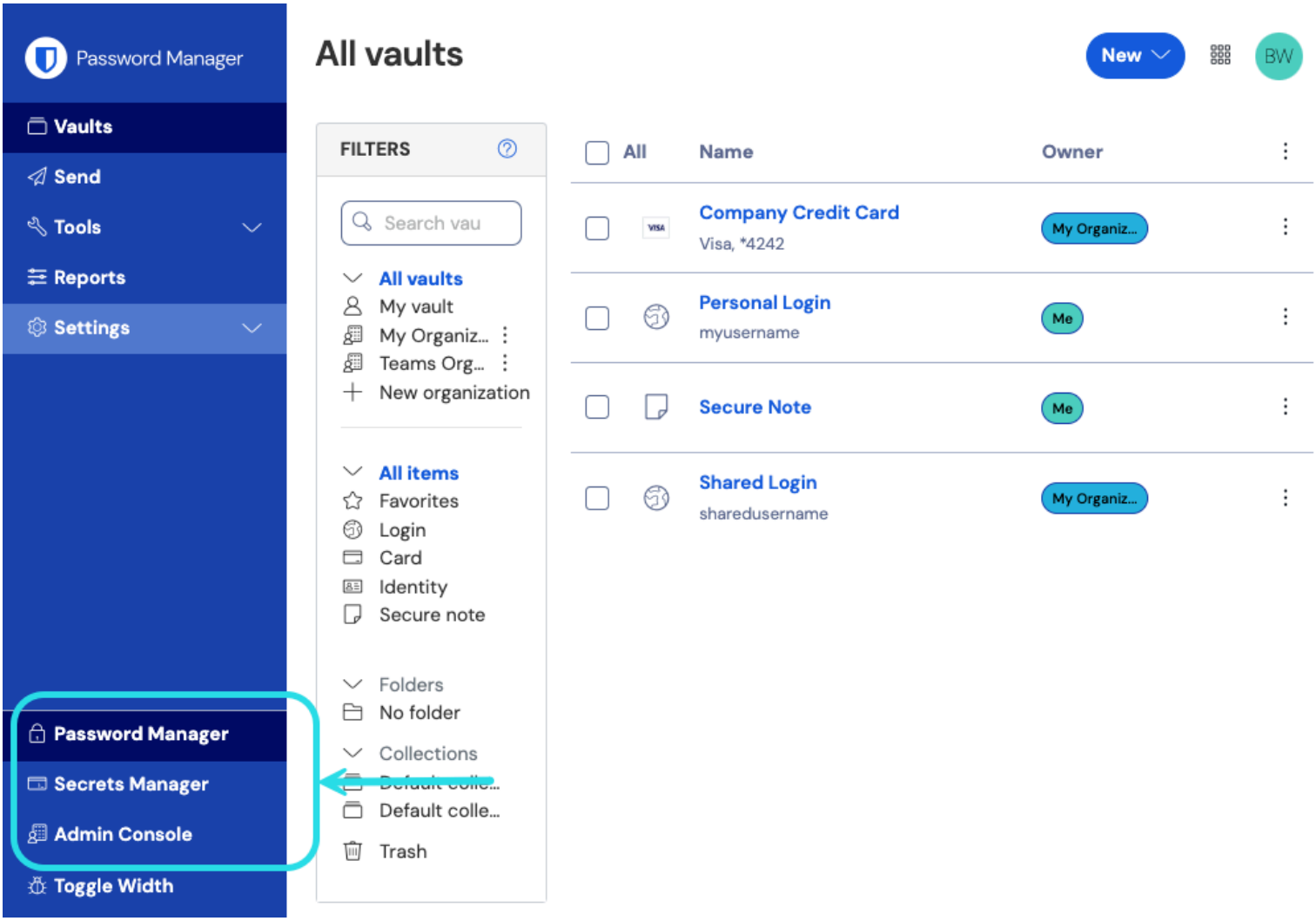
ADFS OIDC 実装

この記事には、OpenID Connect（OIDC）を介したSSOでのログインを設定するための**Active Directory Federation Services（AD FS）固有の**ヘルプが含まれています。別のOIDC IdPでのSSOを使用したログインの設定、またはSAML 2.0を介したAD FSの設定のヘルプについては、OIDC設定またはADFS SAML実装を参照してください。

設定は、BitwardenウェブアプリとAD FSサーバー管理マネージャー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。

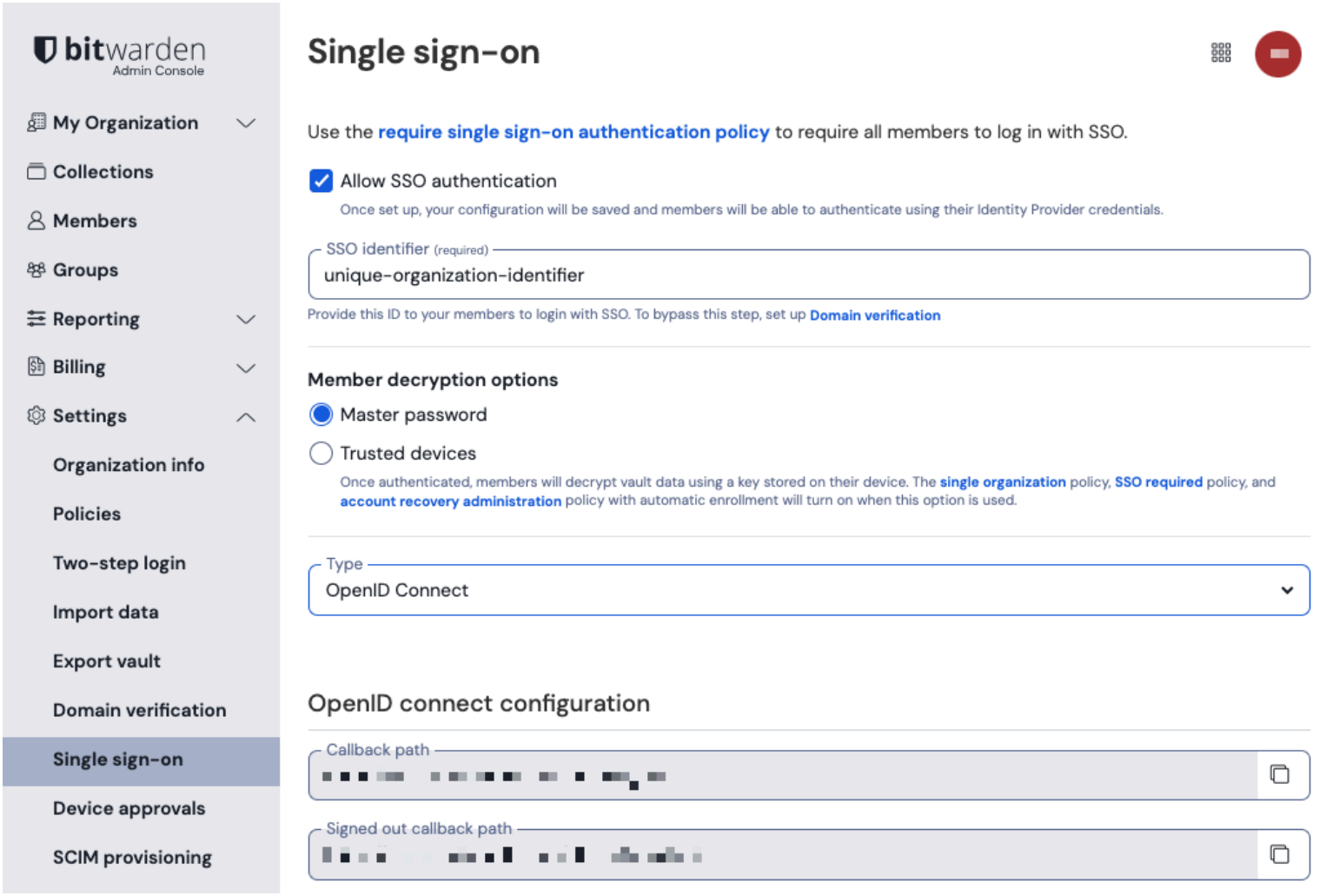
ウェブ保管庫でSSOを開く

Bitwardenの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

ナビゲーションから**設定** → **シングルサインオン**を選択してください。



OIDC設定

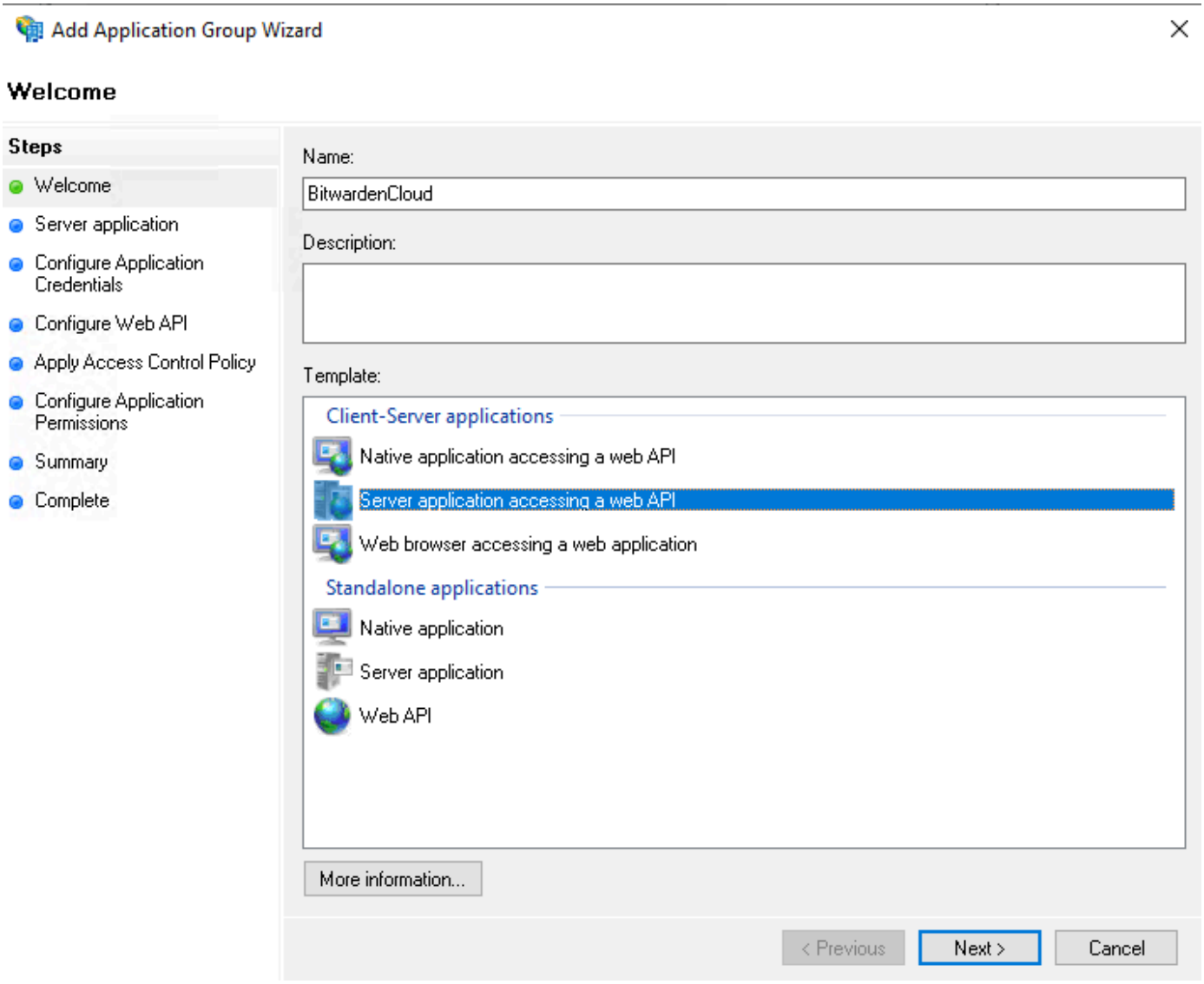
まだ作成していない場合は、あなたの組織のためのユニークな**SSO識別子**を作成してください。それ以外の場合、この画面でまだ何も編集する必要はありませんが、簡単に参照できるように開いたままにしておいてください。

> **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。

アプリケーショングループを作成する

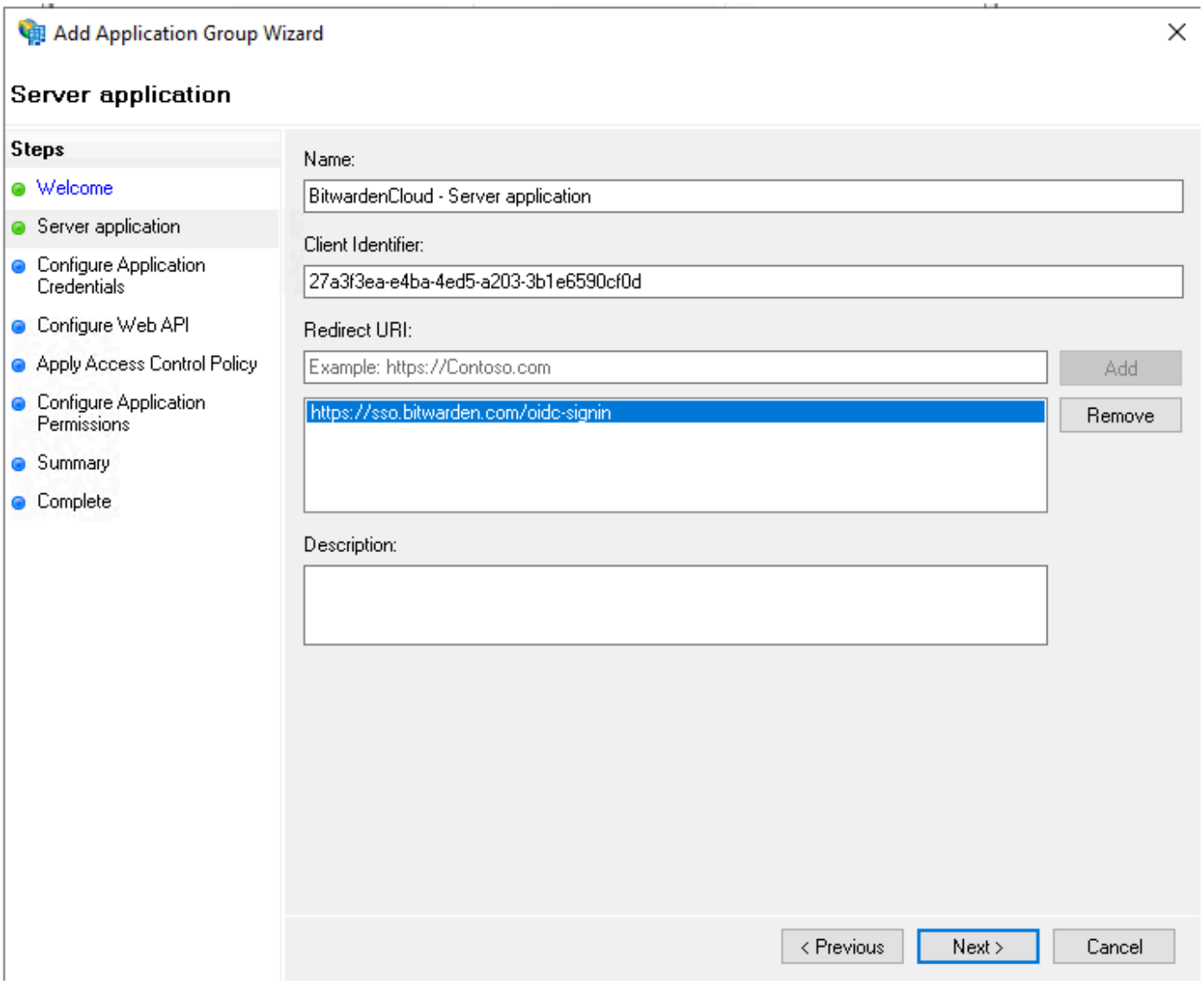
サーバーマネージャーで、**AD FS 管理**に移動し、新しいアプリケーショングループを作成します。

1. コンソールツリーで、**アプリケーショングループ**を選択し、アクションリストから**アプリケーショングループを追加**を選択します。
2. ウィザードのウェルカム画面で、**サーバーアプリケーションがWeb APIにアクセス**テンプレートを選択してください。



AD FS Add Application Group

3. サーバーアプリケーション画面上で：

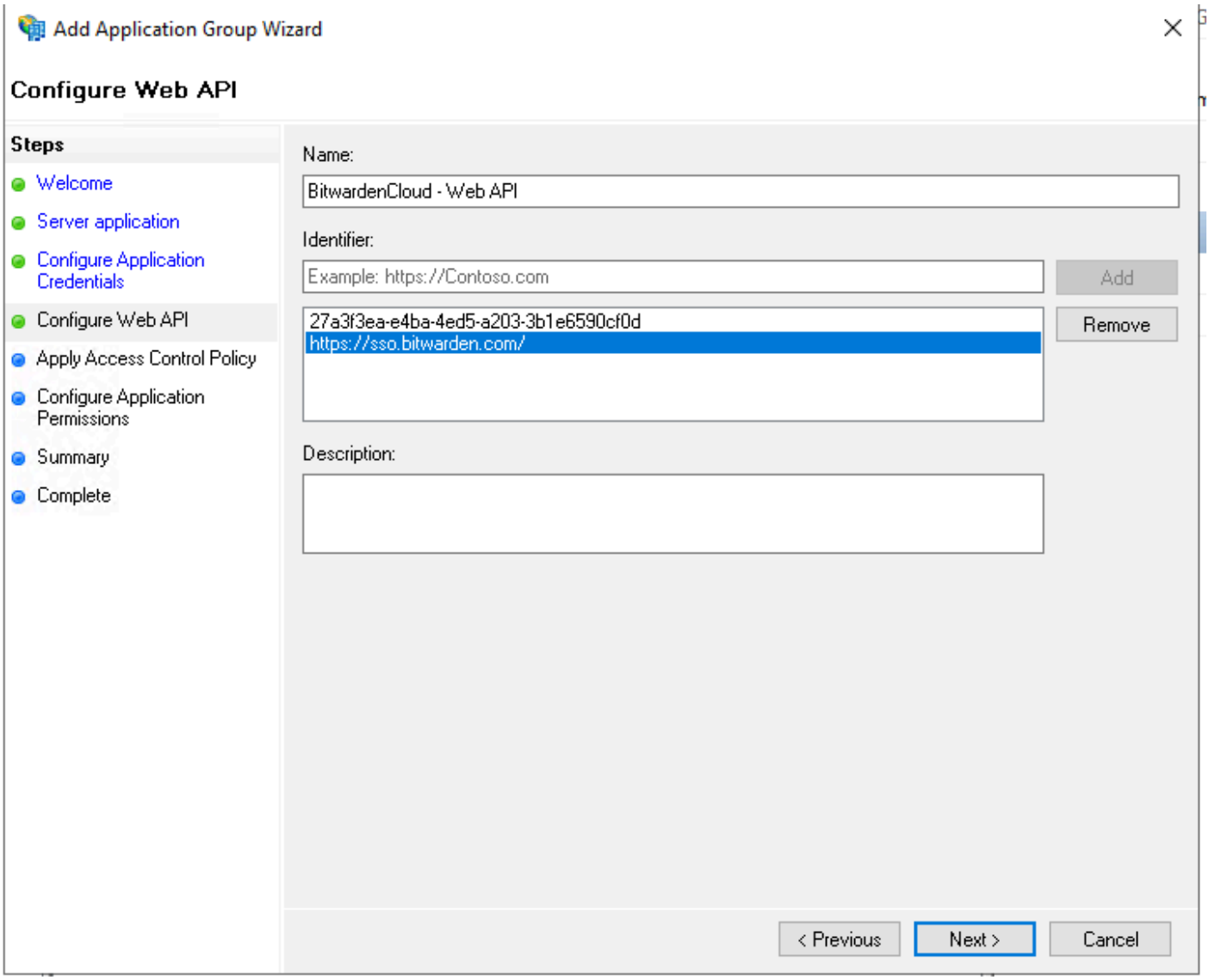


AD FS Server Application screen

- サーバーアプリケーションに**名前**を付けてください。
- **クライアント識別子**をメモしてください。この値は次のステップで必要になります。
- **リダイレクトURI**を指定してください。クラウドホストのお客様の場合、これは`https://sso.bitwarden.com/oidc-signin`または`https://sso.bitwarden.eu/oidc-signin`です。自己ホスト型のインスタンスの場合、
これは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/oidc-signin`のような形式です。

4. アプリケーション資格情報の設定画面で、**クライアントシークレット**をメモしてください。この値は次のステップで必要になります。

5. Web API設定画面で：

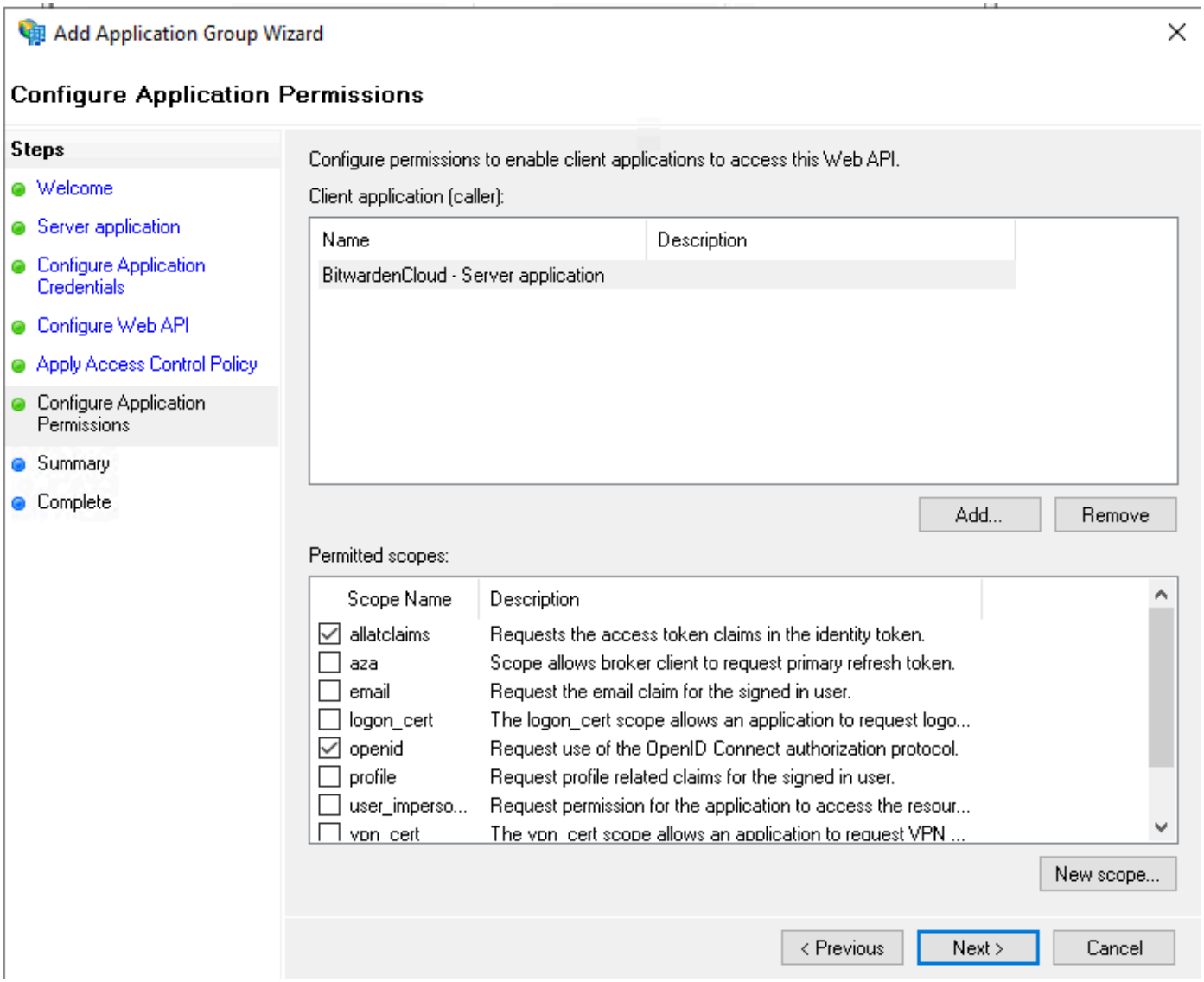


AD FS Configure Web API screen

- Web APIに**名前**を付けてください。
- **クライアント識別子**と**リダイレクトURI**を識別子リストに追加してください（ステップ2B.＆C.を参照）。

6. 「アクセス制御ポリシーの適用」画面で、アプリケーショングループに適切なアクセス制御ポリシーを設定します。

7. アプリケーション権限の設定画面で、スコープ`allatclaims`と`openid`を許可します。



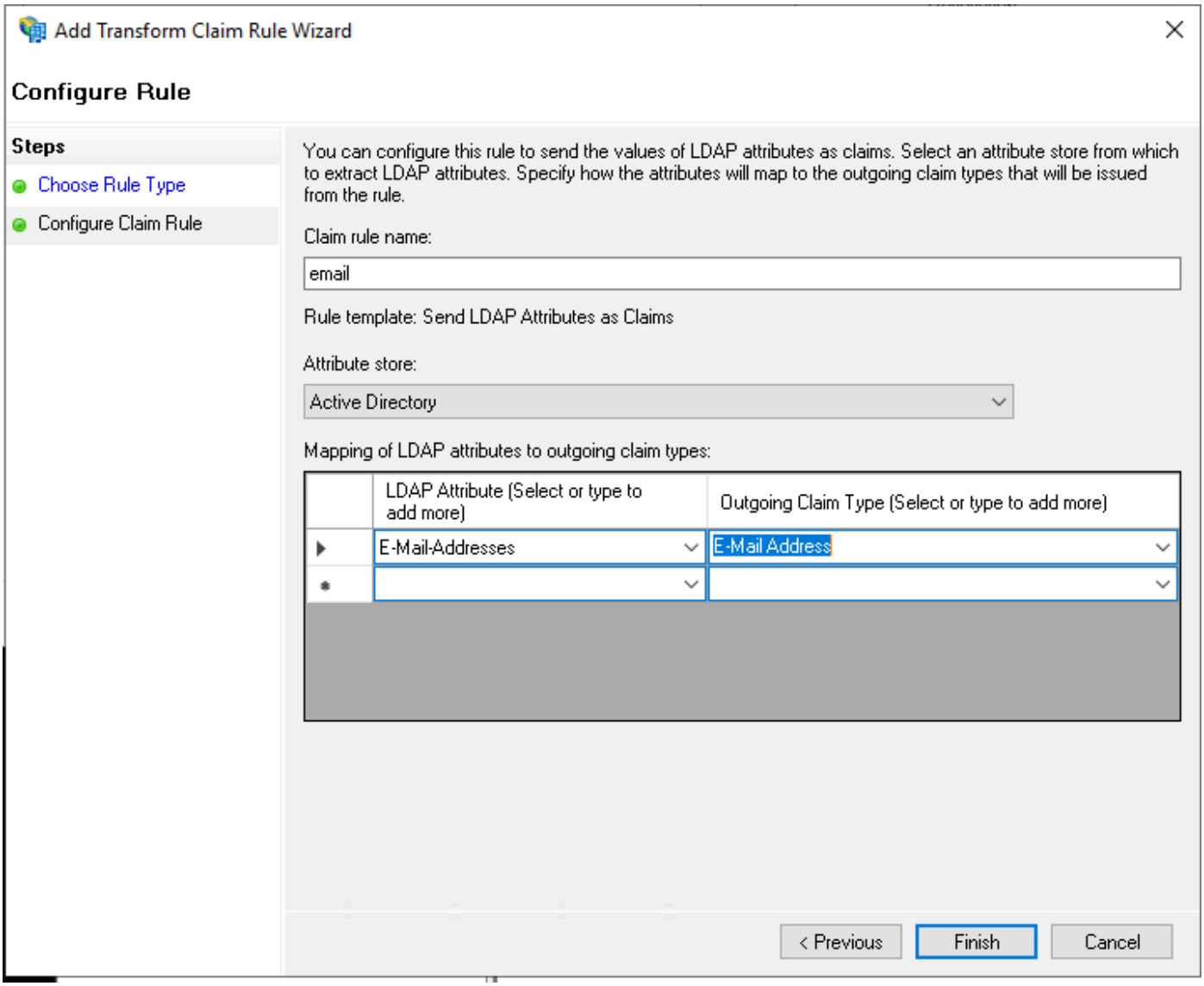
AD FS Configure Application Permissions screen

8. アプリケーショングループウィザードを完了します。

変換クレームルールを追加します

サーバーマネージャーで、**AD FS 管理**に移動し、作成されたアプリケーショングループを編集します：

1. コンソールツリーで、**アプリケーショングループ**を選択します。
2. アプリケーショングループリストで、作成したアプリケーショングループを右クリックし、**プロパティ**を選択します。
3. アプリケーションセクションで、Web APIを選択し、**編集...** を選択します。
4. **発行変換ルール**タブに移動し、**ルールを追加...**ボタンを選択します。
5. ルールタイプ選択画面で、**LDAP属性をクレームとしてSendする**を選択します。
6. 「クレームルール設定」画面で：



AD FS Configure Claim Rule screen

- ルールには**請求ルール名**を付けてください。
- LDAP属性ドロップダウンから、**E-Mail-Addresses.**を選択してください。
- 送信クレームタイプのドロップダウンから、**Eメールアドレス**を選択してください。

7. 選択 **完了。**

ウェブアプリに戻る

この時点で、AD FSサーバー管理者のコンテスト内で必要なすべてを設定しました。次のフィールドを設定するために、Bitwardenウェブアプリに戻ってください：

フィールド	説明
権限	あなたのAD FSサーバーのホスト名を入力し、`/adfs` を追加してください。例えば、`https://adfs.mybusiness.com/adfs`のようになります。
クライアントID	取得したクライアントIDを入力してください。
クライアントシークレット	取得したクライアントシークレットを入力してください。
メタデータアドレス	指定された**権限**の値に`/.well-known/openid-configuration`を追加して入力してください。例えば、`https://adfs.mybusiness.com/adfs/.well-known/openid-configuration`のようになります。
OIDCリダイレクトの振る舞い	**リダイレクト GET**を選択します。
ユーザー情報エンドポイントから請求を取得する	このオプションを有効にすると、URLが長すぎるエラー（HTTP 414）、切り捨てられたURL、および/またはSSO中の失敗が発生した場合に対応します。
カスタムスコープ	リクエストに追加するカスタムスコープを定義します（カンマ区切り）。
顧客ユーザーID請求タイプ	ユーザー識別のためのカスタムクレームタイプキーを定義します（カンマ区切り）。定義された場合、カスタムクレームのタイプは、標準のタイプに戻る前に検索されます。
メールアドレス請求タイプ	ユーザーのメールアドレスのためのカスタムクレームタイプキーを定義します（カンマ区切り）。定義された場合、カスタムクレームのタイプは、標準のタイプに戻る前に検索されます。
カスタム名前請求タイプ	ユーザーのフルネームまたは表示名のためのカスタムクレームタイプキーを定義します（カンマ区切り）。定義された場合、カスタムクレームのタイプは、標準のタイプに戻る前に検索されます。

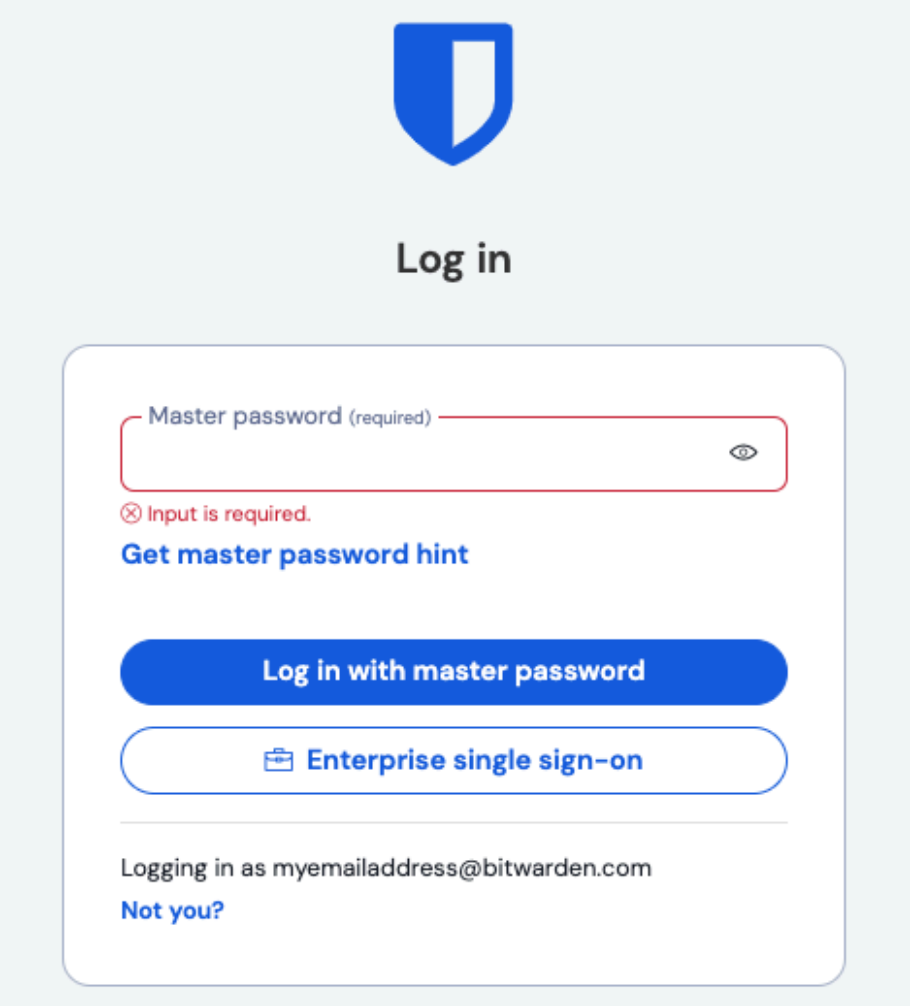
フィールド	説明
要求された認証コンテキストクラス参照値	認証コンテキストクラス参照識別子（`acr_values`）（スペース区切り）を定義してください。リスト`acr_values` を優先順位で並べてください。
応答で期待される "acr" 請求値	Bitwardenがレスポンスで期待し、検証するための`acr`クレーム値を定義してください。

これらのフィールド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ID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、AD FS SSOログイン画面にリダイレクトされます。AD FS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。