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 >

ADFS SAMLの実装

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

ADFS 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**Active Directory Federation Services (AD FS)専用**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 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。

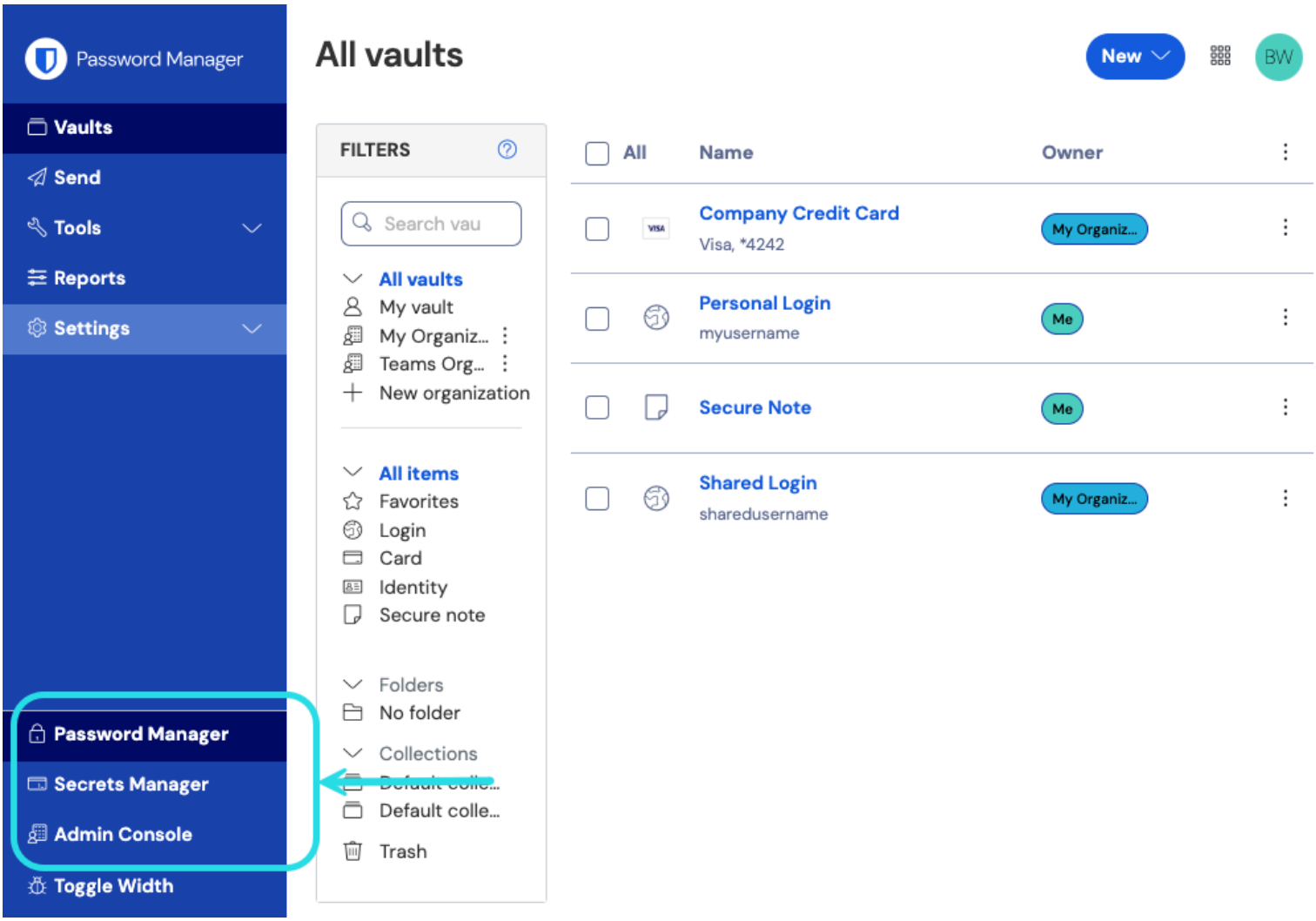
Tip

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

Download sample

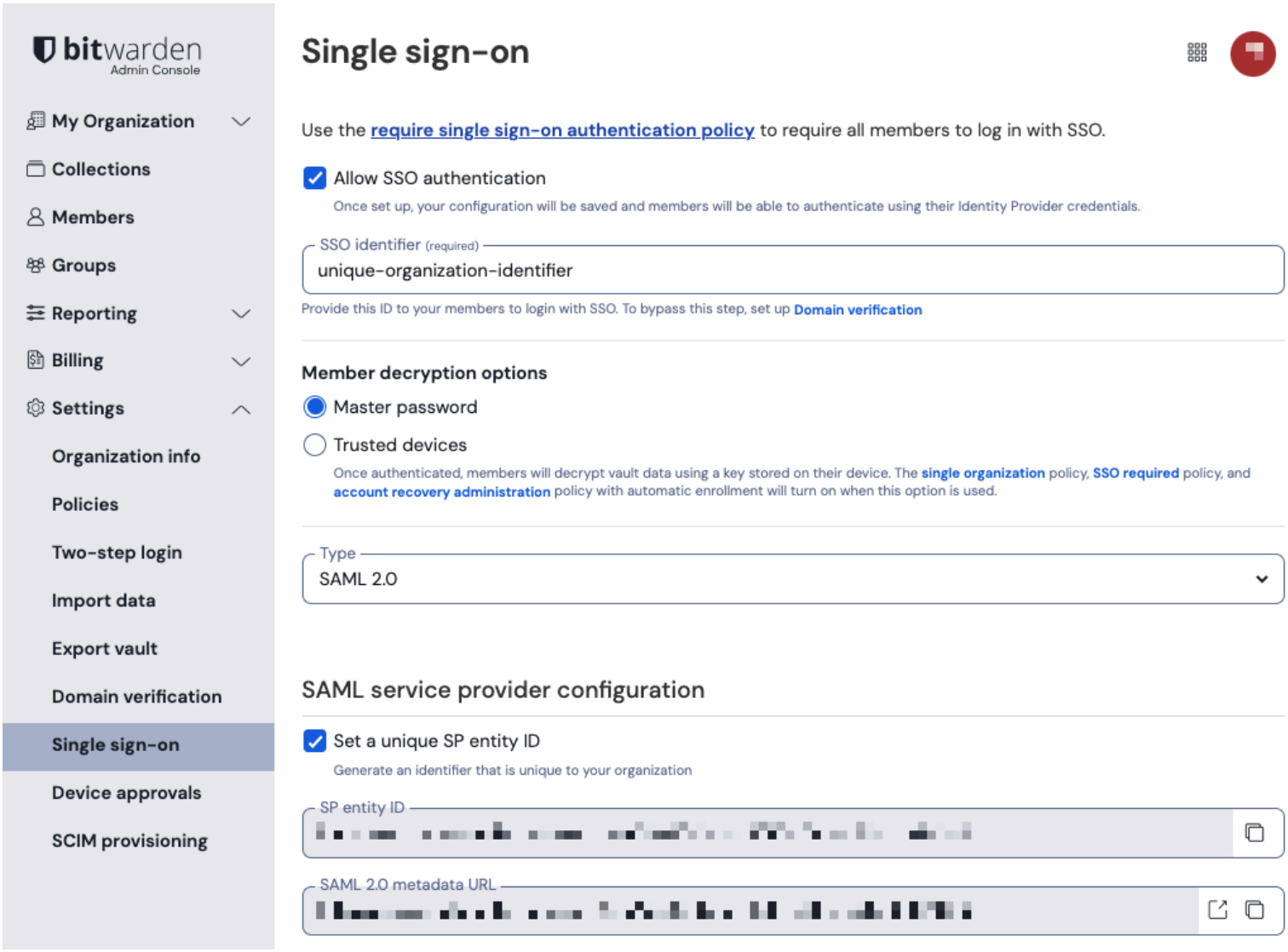
ウェブアプリでSSOを開く

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。

あなたは、この段階で**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、組电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。

信頼関係パーティーを作成します

AD FSサーバーマネージャーで、**ツール** → **AD FS管理** → **アクション** → **信頼するパーティーの信頼を追加**を選択します。ウィザードで、次の選択を行ってください：

1. ウェルカム画面で、**クレーム対応**を選択してください。
2. データソース選択画面で、**依存パーティについてのデータを手動で入力する**を選択してください。

3. 「表示名を指定」画面で、Bitwarden専用の表示名を入力してください。

4. URL設定画面で、**SAML 2.0 WebSSOプロトコルのサポートを有効にする**を選択します。

   - **依存パーティSAML 2.0 SSOサービスURL**の入力欄に、アサーションコンシューマーサービス（ACS）URLを入力してください。
     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。

5. **アクセス制御ポリシーを選択**画面で、あなたのセキュリティ基準を満たすポリシーを選択してください。

6. **識別子の設定**画面で、SPエンティティIDを信頼するパーティの識別子として追加します。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。

7. **アクセス制御ポリシーの選択**画面で、希望のポリシーを選択します（デフォルトでは、**全員に許可**）。

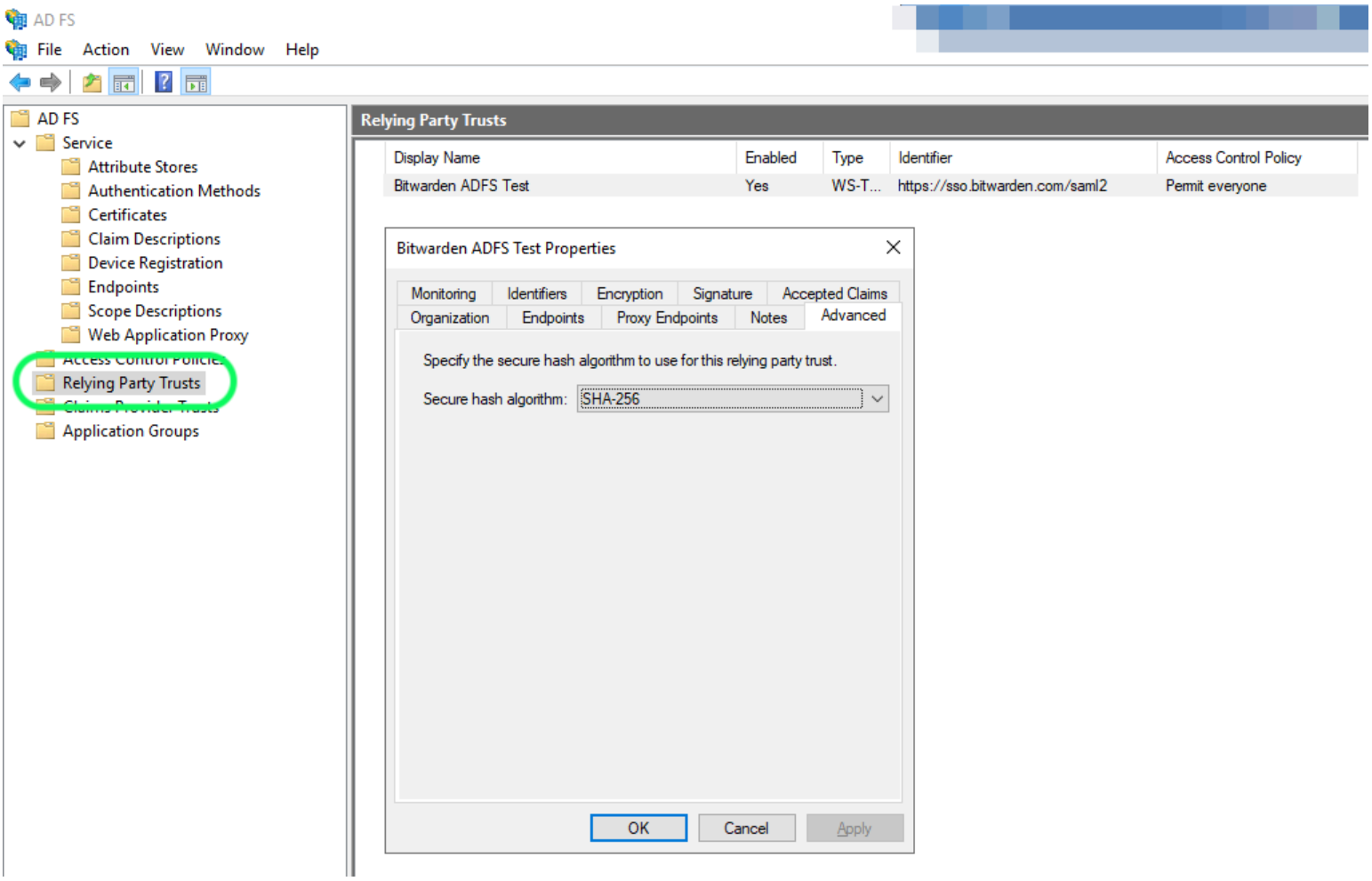
8. **信頼を追加する準備ができました**画面で、選択した項目を確認してください。

高度なオプション

信頼するパーティの信頼が作成されると、左側のファイルナビゲータから**信頼するパーティの信頼**を選択し、正しい表示名を選択することで、その設定をさらに構成することができます。

ハッシュアルゴリズム

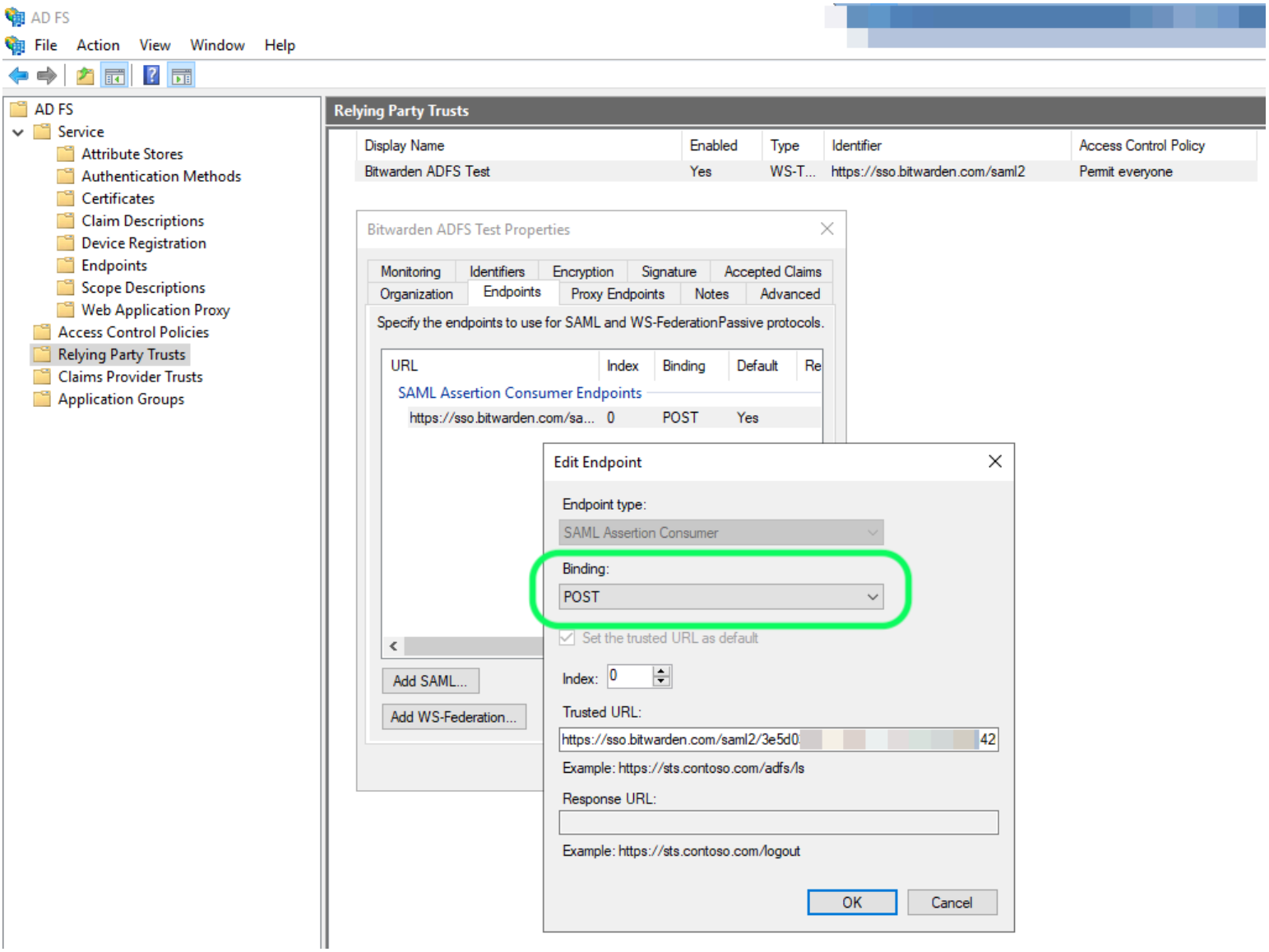
セキュアハッシュアルゴリズムを変更するには（デフォルトではSHA-256）、**詳細**タブに移動します。



Set a Secure Hash Algorithm

エンドポイントバインディング

エンドポイント**バインディング**（デフォルトではPOST）を変更するには、**エンドポイント**タブに移動し、設定されたACS URLを選択します：

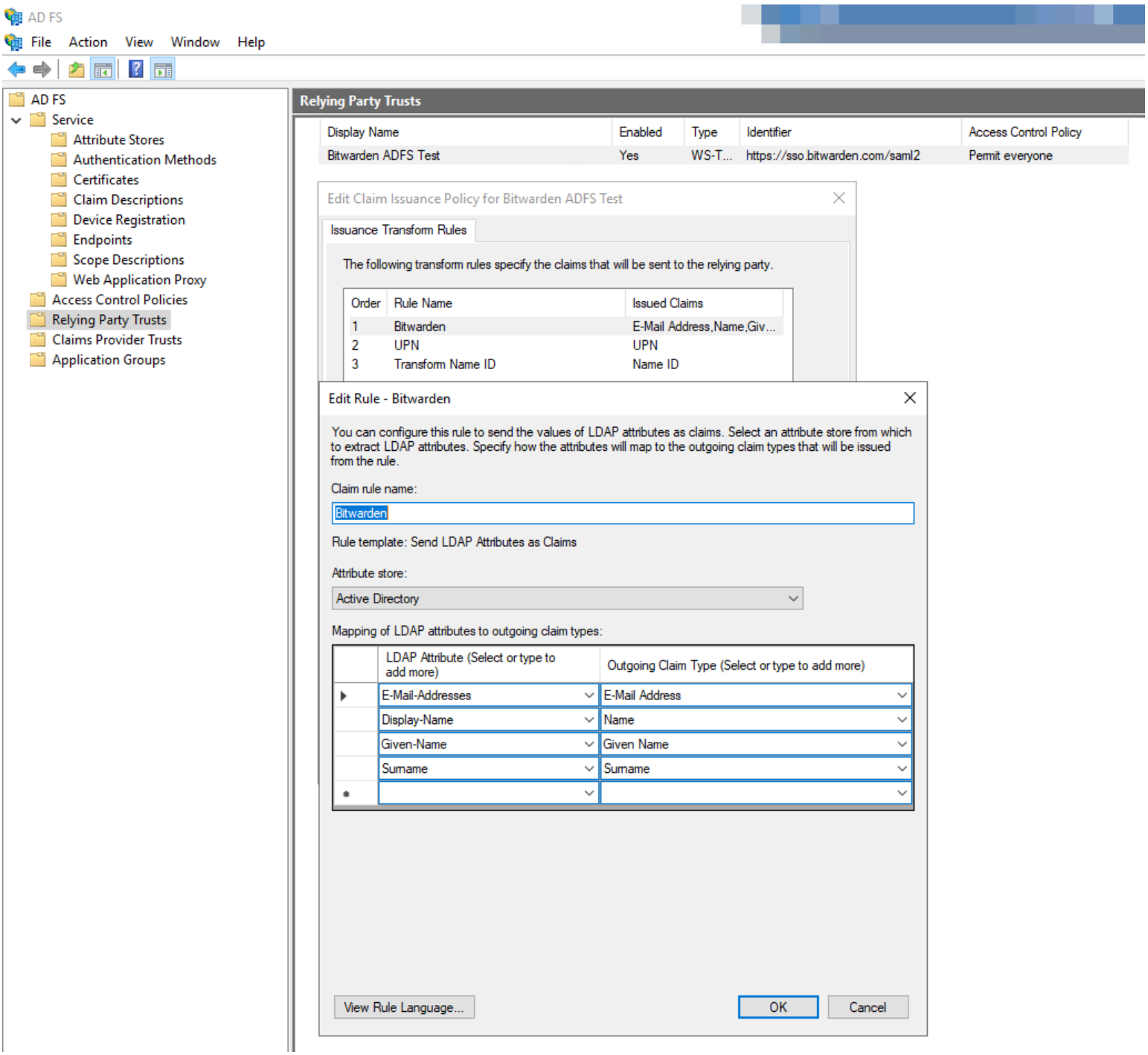


Edit Endpoint

請求発行ルールの編集

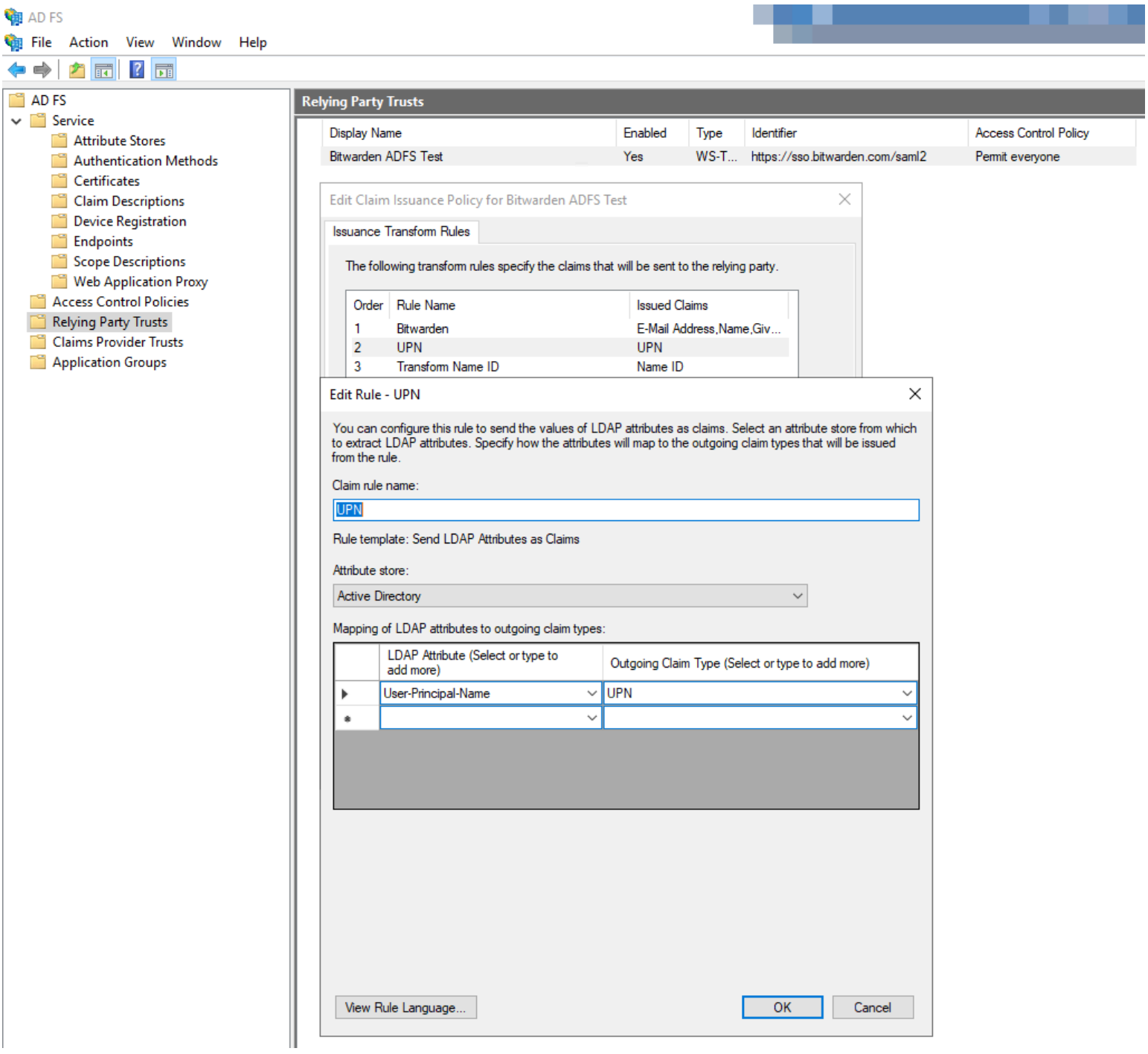
適切なクレーム、**Name ID**を含む、がBitwardenに渡されることを確認するためのクレーム発行ルールを構築します。
次のタブはサンプルのルールセットを示しています：

⇒Rule 1



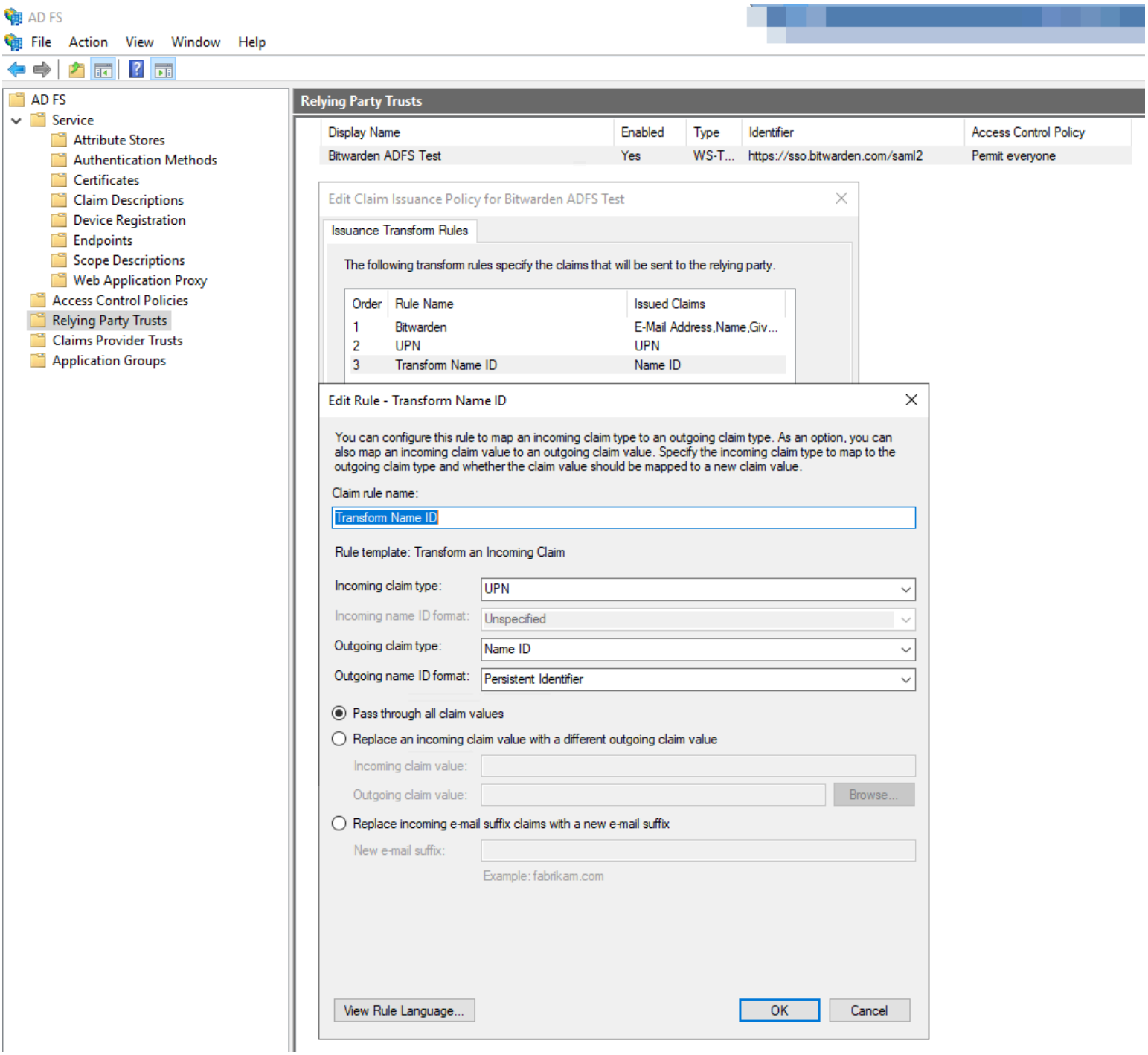
ADFS Rule 1

⇒Rule 2



ADFS Rule 2

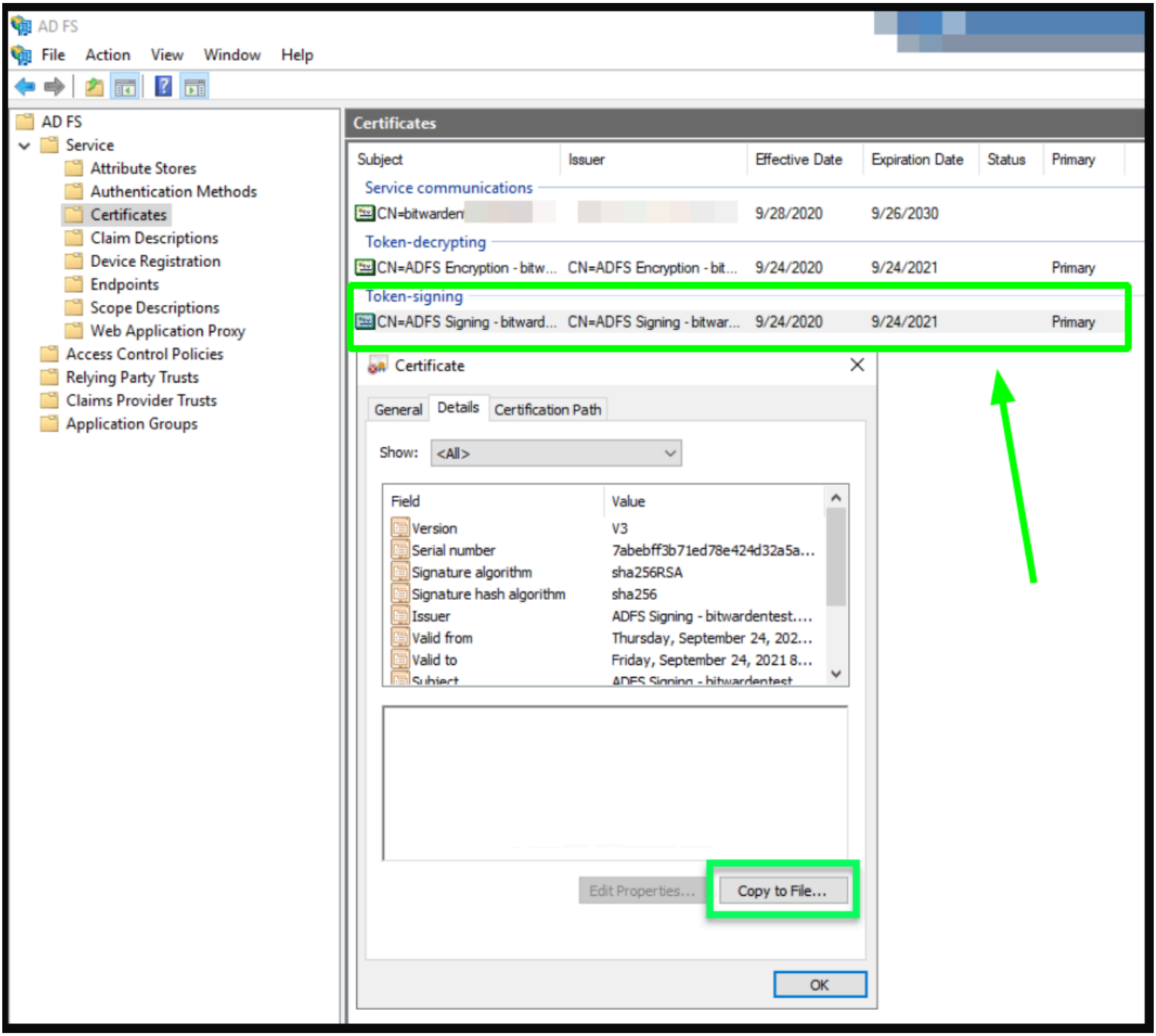
⇒Rule 3



ADFS Rule 3

証明書を取得する

左側のファイルナビゲーターで、**AD FS** → **サービス** → **証明書**を選択して、証明書のリストを開きます。**トークン署名**証明書を選択し、その**詳細**タブに移動し、**ファイルにコピー...**ボタンを選択してBase-64エンコードされたトークン署名証明書をエクスポートします。

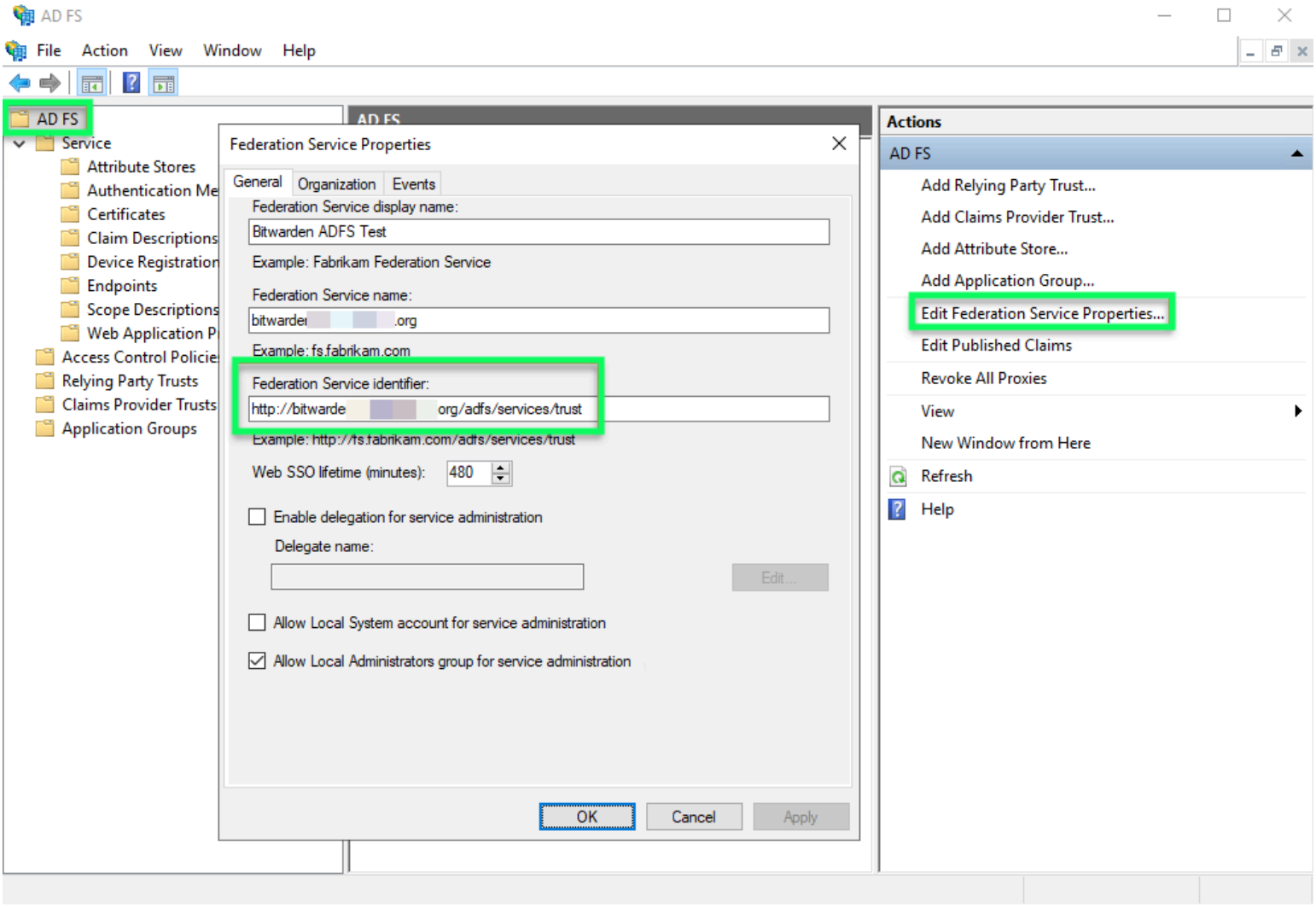


Get token-signing Certificate

この証明書は後のステップで必要になります。

連盟サービス識別子を取得します

左側のファイルナビゲーターで、**AD FS**を選択し、右側のオプションメニューから**連盟サービスのプロパティを編集**を選択します。
連盟サービスプロパティウィンドウで、**連盟サービス識別子**をコピーします。



Get Federation Service Identifier

この識別子は後のステップで必要になります。

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形式を決定します。

サービスプロバイダーの設定

サービスプロバイダー設定セクションで、以下のフィールドを設定します:

フィールド	説明
名前ID形式	**送信名ID形式**を選択します。これは請求発行ルールを構築する際に選択されます（**ルール3**を参照）。
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	デフォルトでは、AD FSは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。ただし、異なるアルゴリズムを使用するようにAD FSを設定している場合は除きます。
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。
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ログインの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、値を取得するためにAD FSサーバーマネージャーを参照する必要がよくあります。

フィールド	説明
エンティティID	取得したフェデレーションサービス識別子を入力してください。メモしてください、これは**HTTPSを使用しないかもしれません**。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	デフォルトでは、AD FSはHTTP POSTエンドポイントバインディングを使用します。**HTTP POST** を選択してください、異なる方法を使用するようにAD FSを設定している場合を除きます。
シングルサインオンサービスURL	SSOサービスエンドポイントを入力してください。この値は、**サービス→エンドポイント**タブでAD FSマネージャーで管理できます。エンドポイントURLは**SAML2.0/WS-FederationのURLパス**として記載されており、通常は`https://your-ドメイン/adfs/ls`のようなものです。`FederationMetadata.`

フィールド	説明

X509公開証明書	`xml`
	ドキュメントのSingleSignOnServceの設定キーから正確な値を取得することができます。
	
	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
	
	`-----証明書終了-----`
	
	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、AD FSは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。ただし、異なるアルゴリズムを使用するようにAD FSを設定している場合は除きます。
アウトバウンドログアウトリクエストを無効にする	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必要です	AD FSがSAMLリクエストの署名を期待するかどうか。

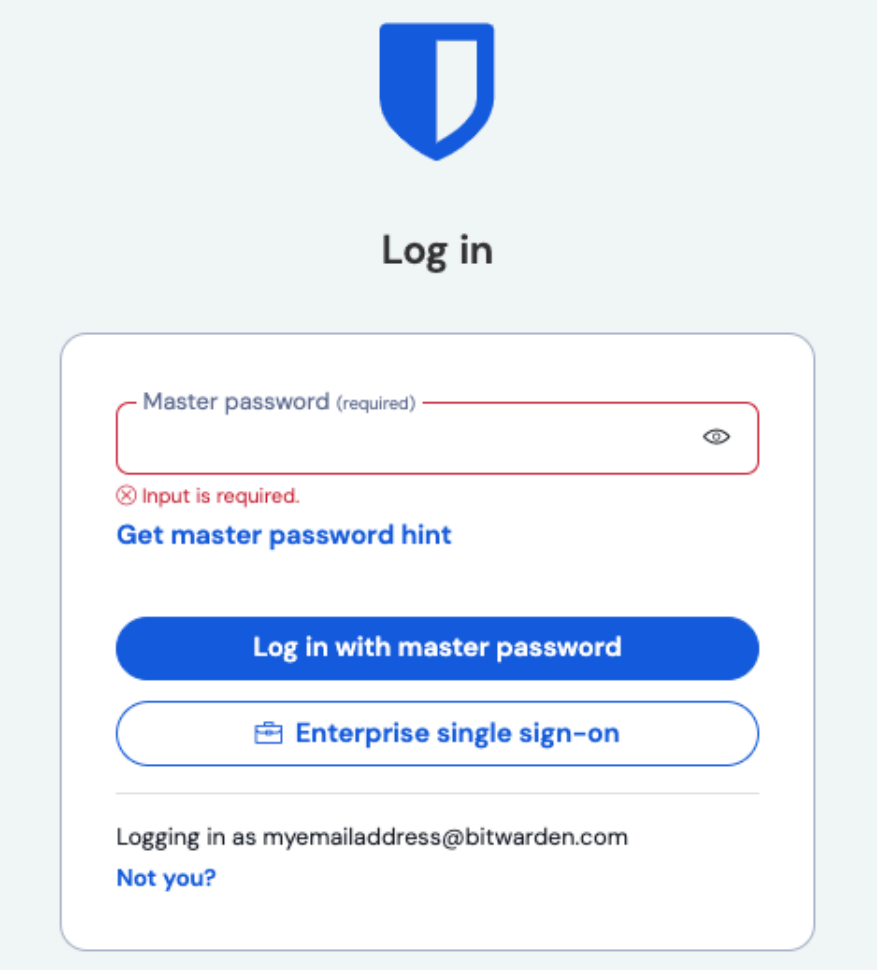
> **Note**
> X509証明書を完成させるとき、有効期限の日付をメモしてください。SSOエンドユーザーへのサービスの中断を防ぐために、
> 証明書を更新する必要があります。証明書が期限切れになった場合でも、
> 管理者と所有者のアカウントは常にメールアドレスとマスターパスワードでログインできます。

IDプロバイダーの設定が完了したら、**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、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。