ESAおよびSMA用のAD FSを使用したSAML SSO外部認証の設定

内容

はじめに

このドキュメントでは、Cisco ESAおよびSMAでの外部認証用のSAML IDプロバイダーとしてActive Directoryフェデレーションサービス(ADFS)を設定する方法について説明します。

前提条件

このドキュメントでは、エンジニアが他の方法では確認できないサードパーティ製アプリケーションの概要を示します。

- Cisco Eメールセキュリティアプライアンス(ESA)およびセキュリティ管理アプライアンス(SMA)の最新バージョンに対して、Active Directoryフェデレーションサービス(AD FS)2012および2016を使用したSecurity Assertion Markup Language(SAML)外部認証の設定手順。
- 特別な導入固有の設定を含まない、基本的なラボでの手順。
- 実稼働環境とは異なる可能性がある、ラボ環境での動作例。

⚠ 注意：この手順を実行する前に、サービスプロバイダー(SP)の設定を完了してください。を

⚠ 参照。

要件

- Microsoft Active Directory Federation Services (AD FS) 2012または2016
- Cisco Eメールセキュリティアプライアンス(ESA)およびセキュリティ管理アプライアンス(SMA)の最新バージョン。

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

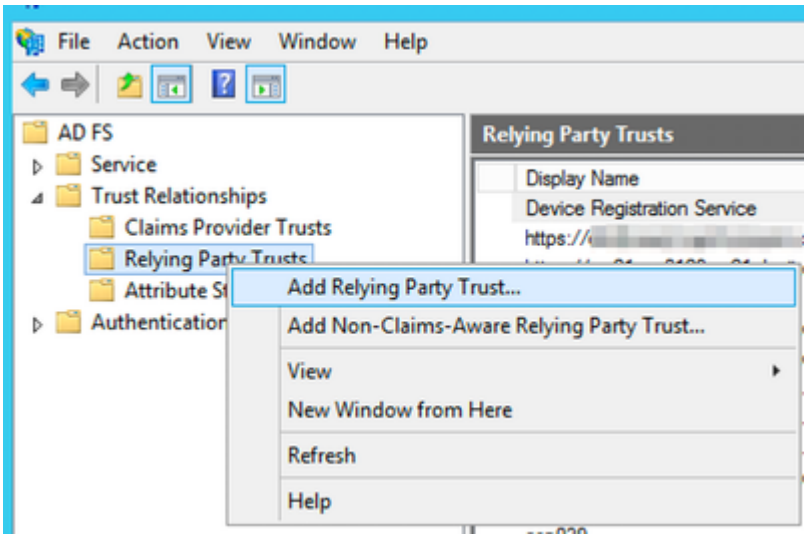
SAML用のADFS IDP設定手順

証明書利用者信頼の設定

2つのオプションのいずれかを使用して、AD FSで証明書利用者信頼を作成します。

方法A:SPメタデータをインポートして証明書利用者信頼を作成する

1. Administrative ToolsからAD FS Managementコンソールを開きます。
2. AD FS管理コンソールで、[信頼された関係]を展開し、[証明書利用者信頼]を右クリックして、[証明書利用者信頼の追加]を選択します。



証明書利用者信頼の追加

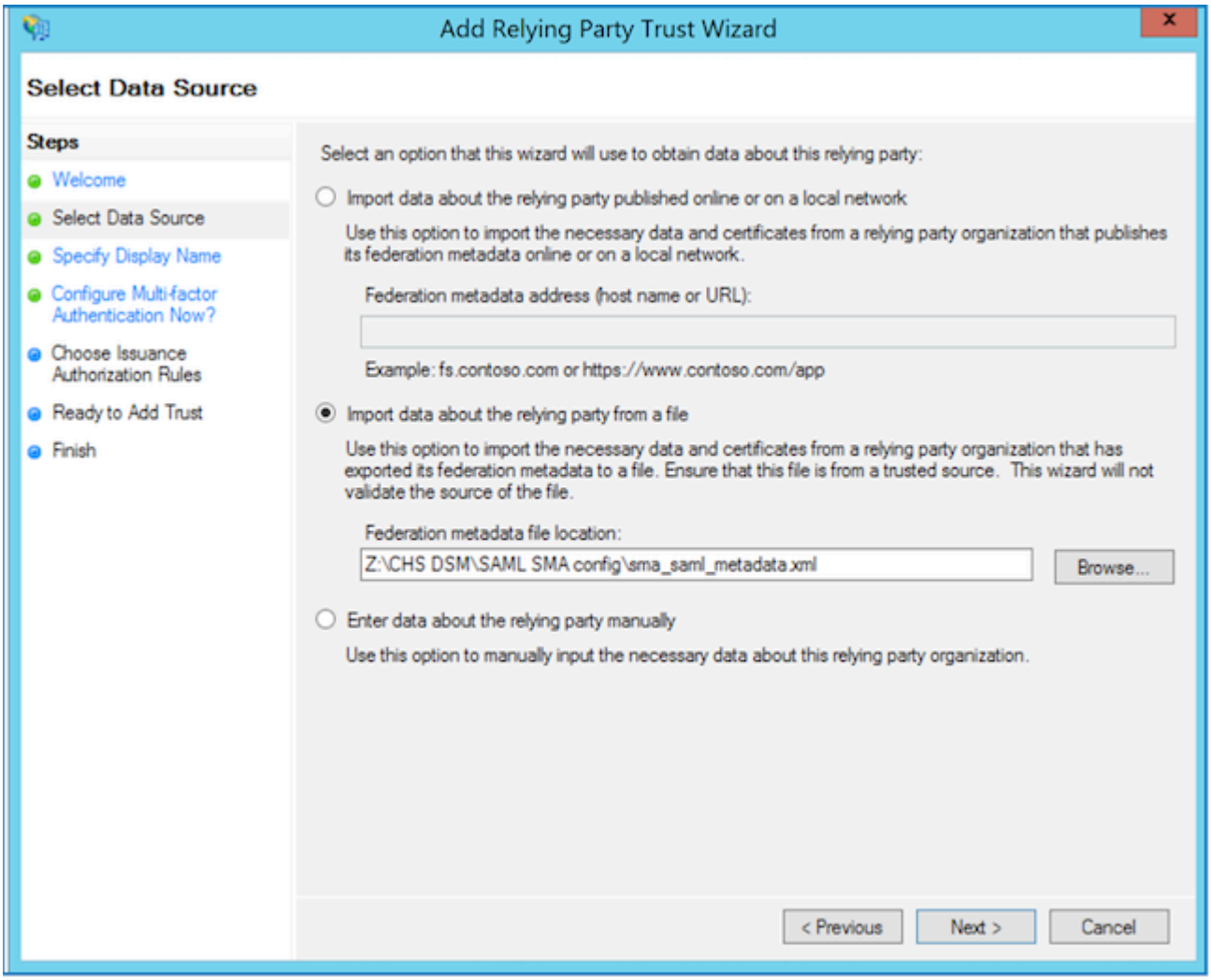
ヒント: Microsoft証明書利用者信頼

次の2つのオプションのいずれかを使用して続行します。

- オプションA：証明書利用者に関するデータをファイルからインポートします。ESAまたはSMAサービスプロバイダー(SP)のmetadata.xmlファイルをアップロードします。
- オプションB：証明書利用者のデータを手動で入力します。このオプションでは、手動設定の手順を示します。

オプションA：証明書利用者に関するデータをファイルからインポートします。ESAまたはSMAサービスプロバイダー(SP)のmetadata.xmlファイルをアップロードします。

1. ファイルから証明書利用者に関するデータをインポートするオプションを選択し、Nextを選択します。



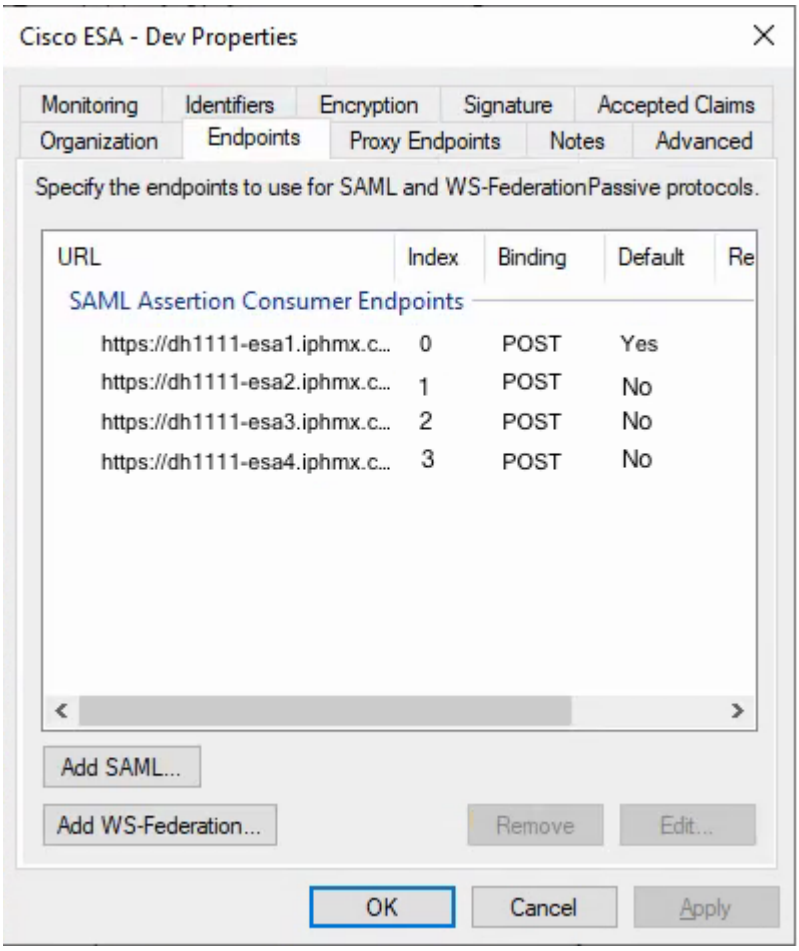
ESA/SMAメタデータファイルのインポート

- この証明書利用者信頼を識別するための表示名を指定し、Nextを2回選択します。
- 発行承認規則では、Permit all usersを選択してからNextを選択します。
- Ready to Add Trustページで、デフォルトの設定を受け入れ、Nextを選択します。
- [Finish] を選択します。これにより、証明書利用者信頼の[要求規則の編集]ダイアログが開きます。このダイアログについては、「発行変換規則 – 要求」を参照してください。

証明書利用者信頼のプロパティ – エンドポイント

この手順は、クラスタに複数のESAが存在する場合にのみ実行します。

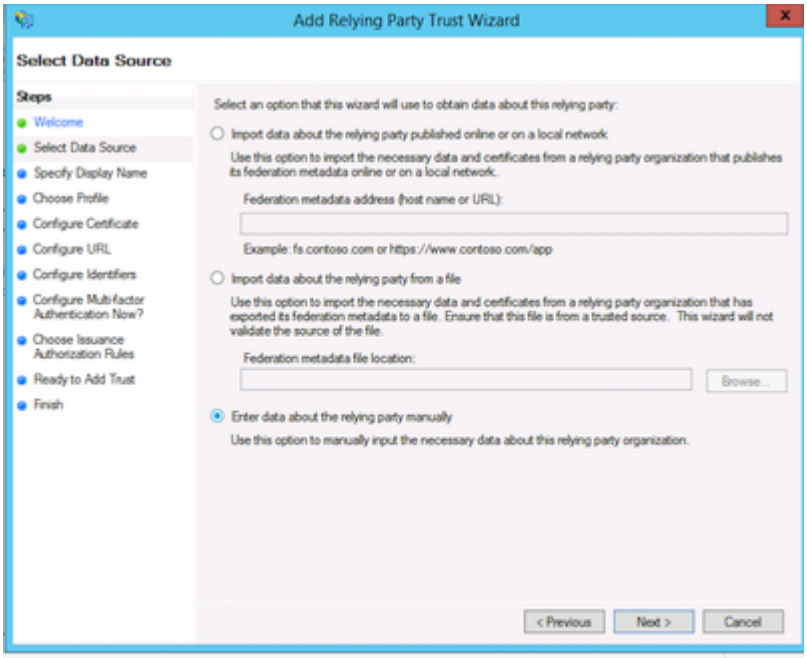
1. 証明書利用者信頼のプロパティ> Endpointsを開きます。
2. 各ESA到達可能URLアドレスを追加し、OKを選択します。
3. インデックス値は0からカウントされます。つまり、0、1、2、3です。
4. 1つのエントリだけをDefault = Yesに設定します。
5. 残りのエントリをDefault = Noに設定します。



証明書利用者信頼のプロパティ – エンドポイント

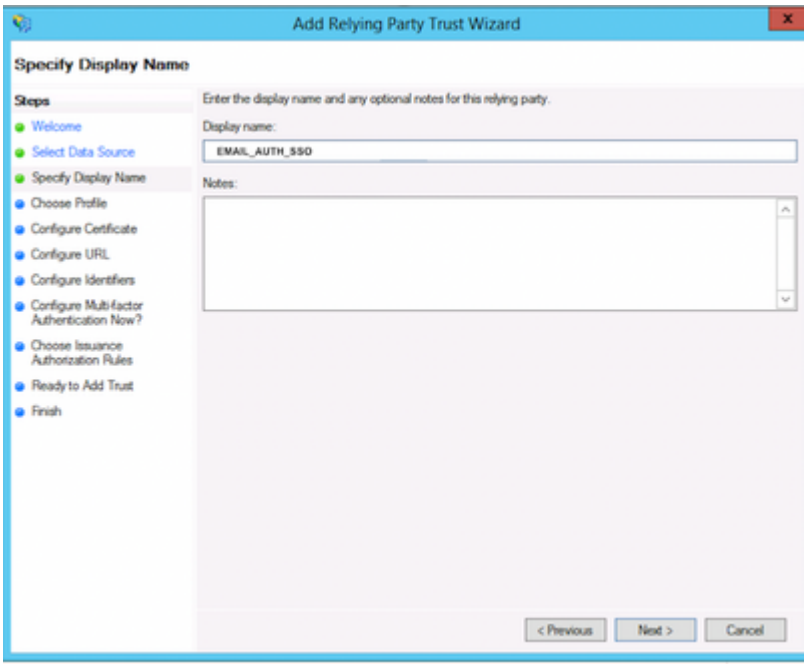
オプションB：証明書利用者のデータを手動で入力します。このオプションでは、手動設定の手順を示します。

1. Enter data about the relying party manuallyを選択します。



ヒント：表示名は、ESAまたはSMA SAMLの証明書利用者信頼を識別するために選択する名前です。

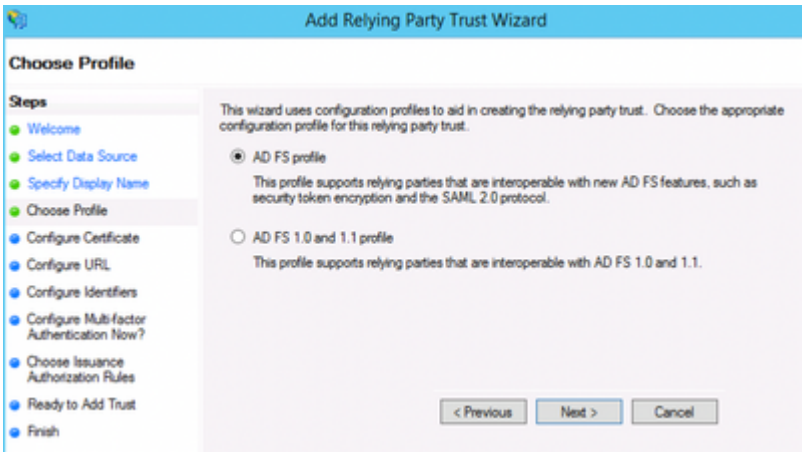
1. サービスプロバイダーの表示名を入力します（ESA_SPなど）。



サービスプロバイダープロファイルの名前を作成します

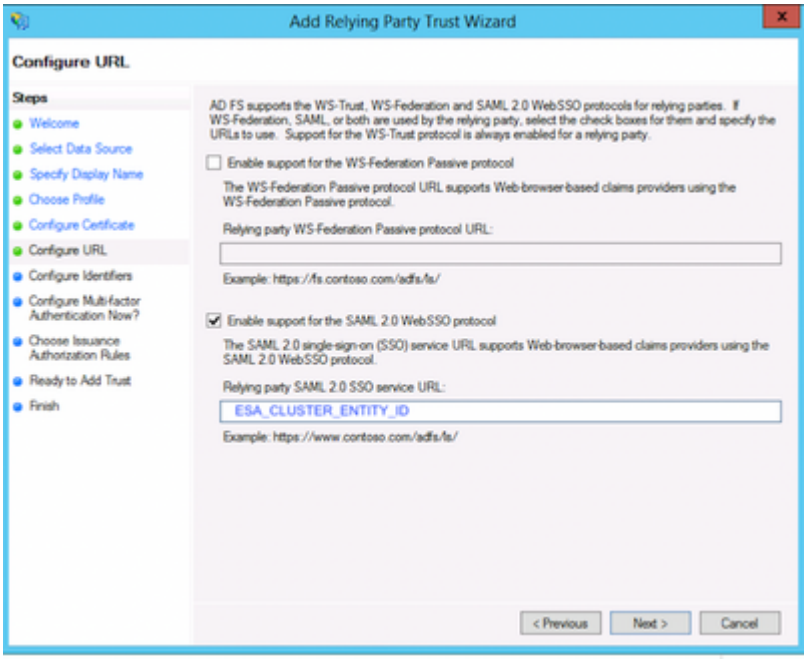
ヒント:クレームルールと発行変換ルールの役割

1. プロファイルオプションAD FS profileを選択します。



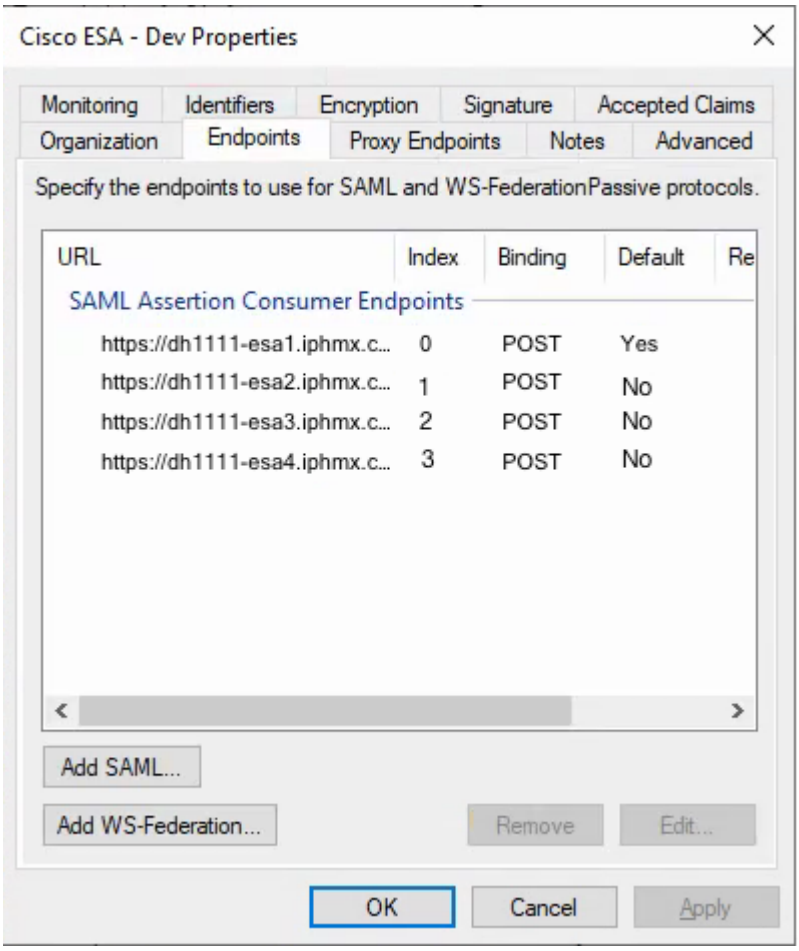
SAML 2.0を使用するAD FSプロファイルオプション

1. ESAサービスプロバイダー(SP)の設定からパブリック証明書をロードします。
2. Configure URLで、Enable support for the SAML 2.0 single-sign-on (SSO)を選択します。
3. SPプロファイルのエンティティID値を使用して、証明書利用者SAML 2.0 SSOサービスURLを入力します。



発行承認規則 – すべてのユーザーを許可する

1. 発行承認規則の場合は、Permit all users to access this relying partyを選択します。



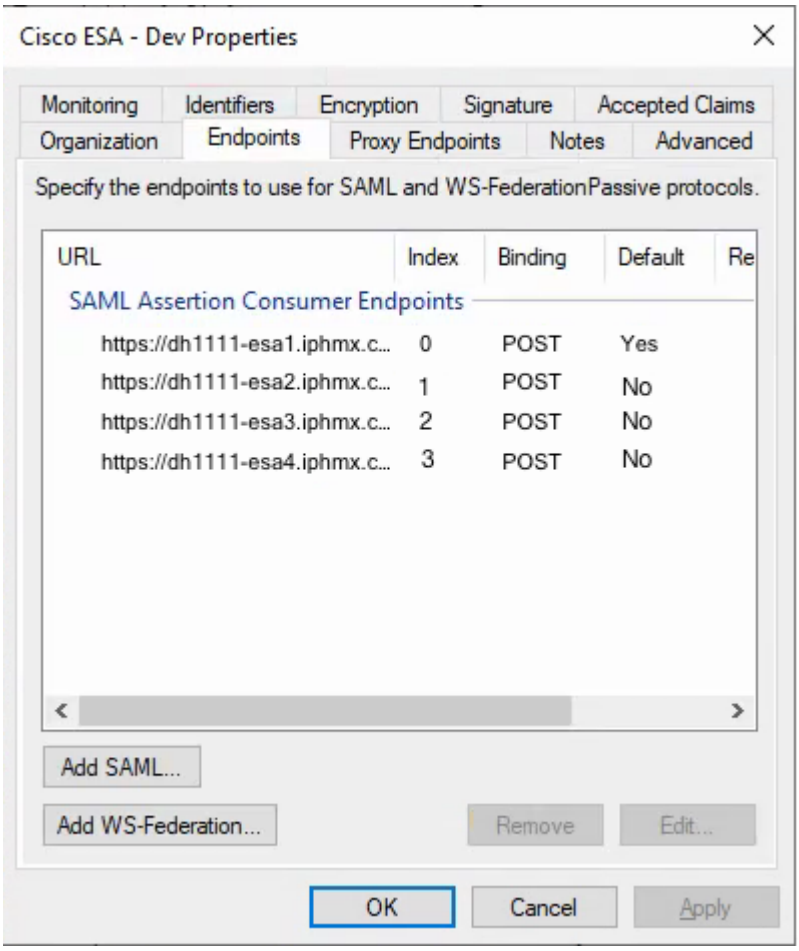
発行承認規則の選択

1. Nextを選択して、Finishページに移動します。

証明書利用者信頼エンドポイントの設定（クラスタのみ）

この手順は、クラスタに複数のESAが存在する場合にのみ実行します。

1. 証明書利用者信頼のプロパティ> Endpointsを開きます。
2. 各ESA到達可能URLアドレスを追加し、OKをクリックします。
3. エンドポイントのインデックス値を0から始めて設定します（0、1、2、3など）。
4. 1つのエンドポイントだけをDefault = Yesに設定します。残りのエンドポイントをDefault = Noに設定します

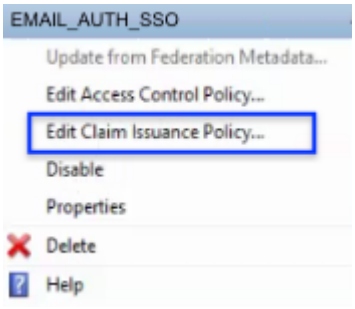


発行承認規則 – すべてのユーザーを許可する

- 完了ステップでは、「発行変換規則」で説明した、証明書利用者信頼の[要求規則の編集]ダイアログを開始します。

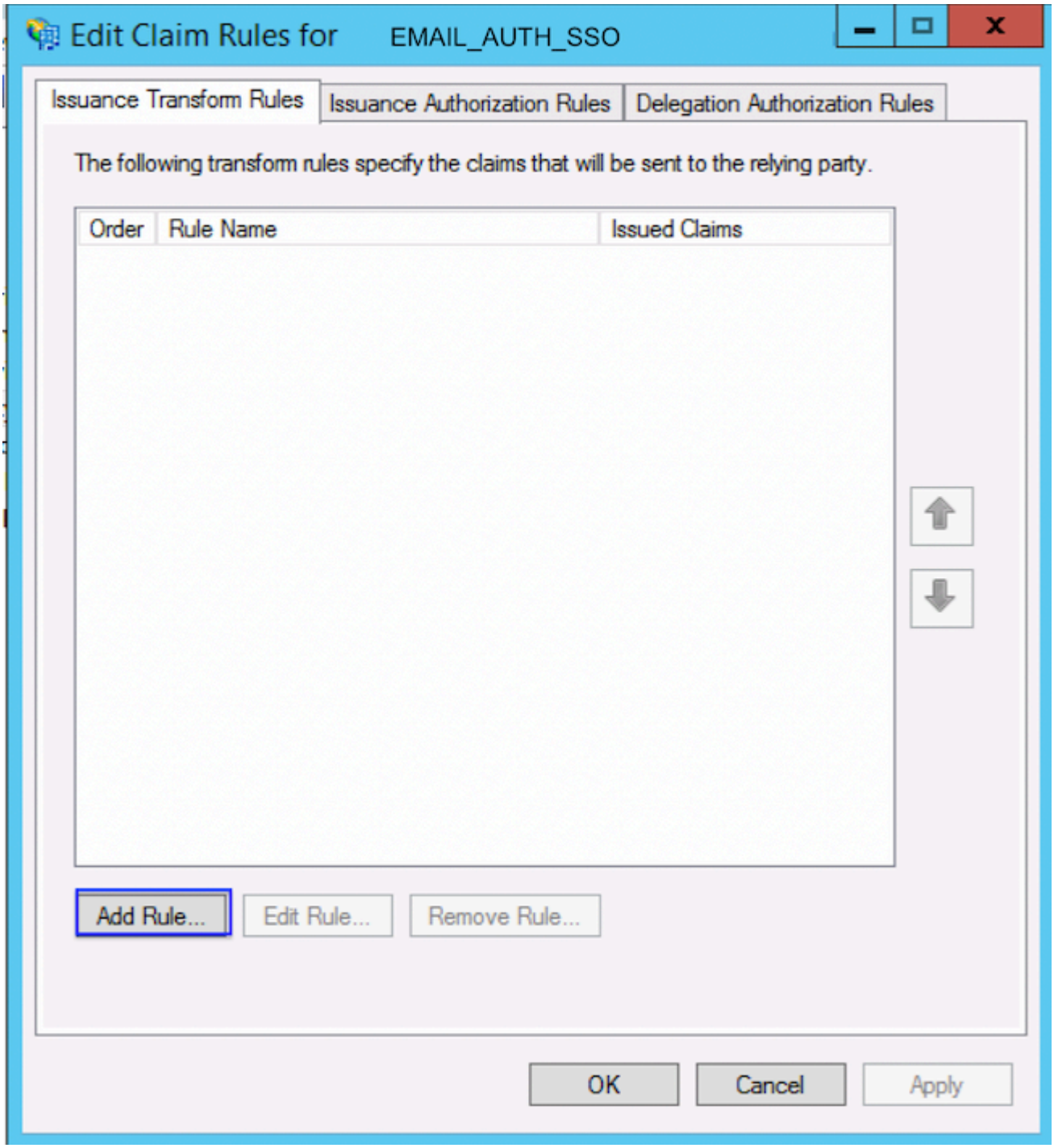
発行変換規則 – 請求

- Edit Claims Issuance Policyを選択します。



要求発行ポリシーの編集

- [Add Rule] を選択します。

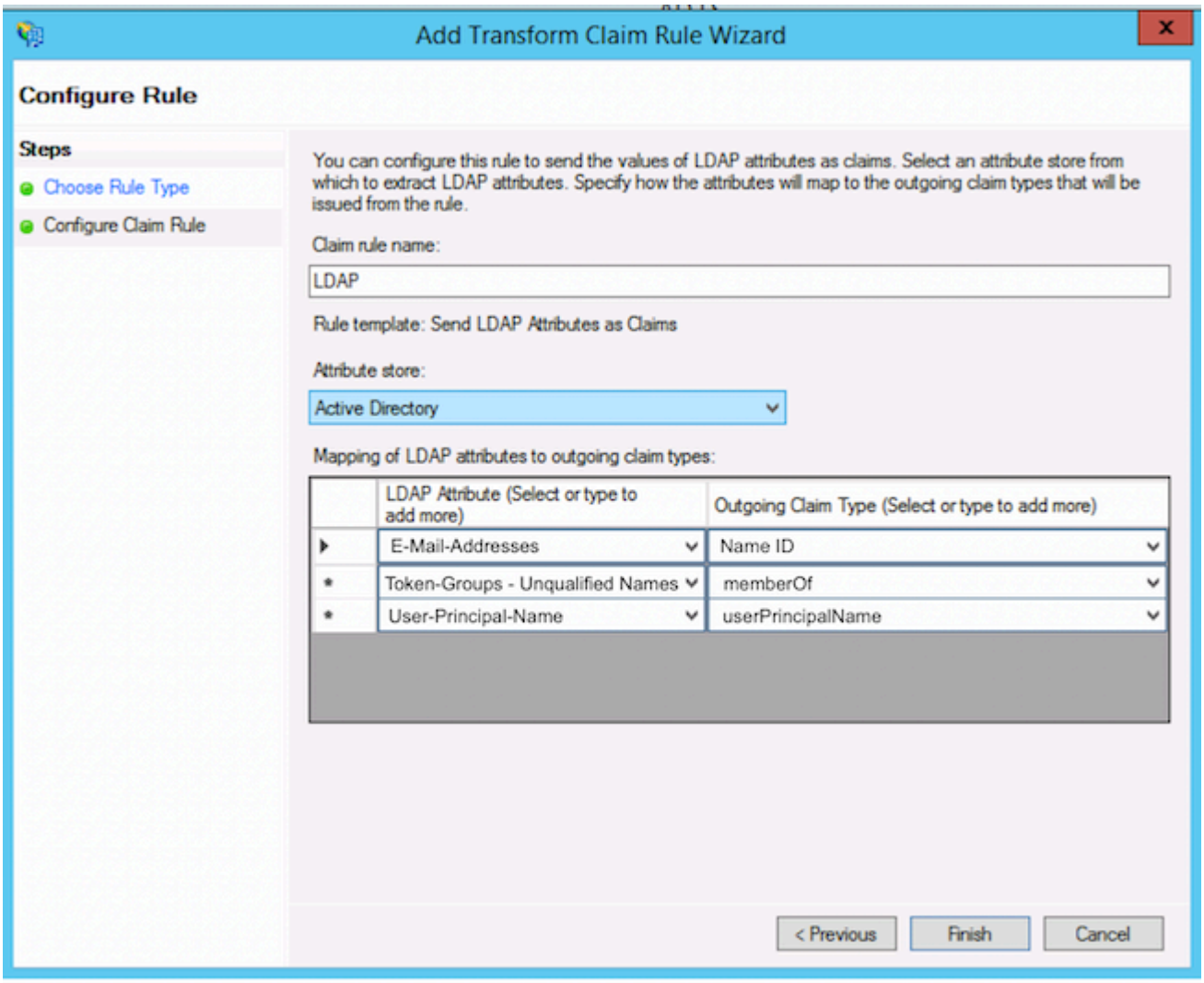


発行変換ルールの追加

ここに示す値は、ESAが外部認証設定でグループ名を入力できるようにする一般的な値です。

ヒント：マッピングの値は、管理者のプリファレンスに基づいて異なる場合があります。

ヒント：以下に示すサンプルでは、出力方向の要求タイプとしてmemberOfとuserPrincipalNameを手動で入力します。ドロップダウンリストから名前IDを選択します。



クレームルールの変換

- [Finish] を選択します。

IdPメタデータのダウンロードとESAへのアップロード

証明書利用者信頼と要求ルールの設定が完了したら、IDプロバイダー(IdP)メタデータをエクスポートし、ESAにアップロードします。

⚠ 注意: AD FSサービスを再起動すると、アクティブな認証セッションが中断される可能性があります。この手順は、必要に応じて、メンテナンスの時間帯に実行してください。

- 必要に応じて、AD FSサービスを再起動します。
- 次のコマンドを実行します。

```
net stop adfssrv
net start adfssrv
```

- 次のURLからメタデータファイルをダウンロードします。

https://myserver.domain.com/FederationMetadata/2007-06/FederationMetadata.xml

- 終了し、ESAクラスタに戻ります。

確認

1. ESAまたはSMAで、IdPメタデータのインポートが正常に完了したことを確認します。
2. SAMLシングルサインオン(SSO)を使用して、管理ログインをテストします。
3. 予期されたグループ要求が受信され、役割マッピングが外部認証構成で予期したとおりに入力されていることを確認してください。

関連情報

-

- Cisco E メール セキュリティ アプライアンス：エンドユーザ ガイド
- Ciscoコンテンツセキュリティ管理アプライアンス – エンドユーザガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。