SAMLを使用したADFSバージョン3.0でのUmbrellaの設定

内容

はじめに

このドキュメントでは、Cisco UmbrellaとActive Directory Federation Services(ADFS)バージョン3.0の間でSAMLを設定する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づくものです。

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ました。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。

概要

この記事では、Cisco UmbrellaとActive Directory Federation Services(ADFS)バージョン3.0の間でSAMLを設定する方法について説明します。ADFSを使用してSAMLを設定する方法は、ウィザード内で1 ~ 2クリックのプロセスではなく、ADFSを正しく動作させるために変更する必要があるため、Umbrellaの他のSAML統合とは異なります。

この記事では、SAMLとADFSを連携させるために必要な変更について詳しく説明します。主な手順は、最初にADFS環境とCisco Umbrellaの間の暗号化を無効にし、次にUmbrella中継パーティ設定にいくつかの発行変換カスタム要求ルールを追加することです。

これらの手順は、既存の動作中のADFS設定でのみ実行してください。Cisco Umbrellaサポートでは、特定の環境でADFSを設定する際の支援やサポートは提供できません。

現時点では、これらの手順でサポートされているのはADFSバージョン3.0(Windows Server 2012 R2)だけです。ADFSの以前のバージョン（2.0または2.1）または以降のバージョン(4.0)は、Umbrella SAML統合で動作できますが、これはテストされておらず、証明されていません。ADFSのバージョンが異なり、統合のためにシスコのサポートチームと製品チームの協力に関心がある場合は、Cisco Umbrellaサポートまでお問い合わせください。

SAML初期設定の前提条件は、Umbrellaのドキュメント「Identity Integrations: Prerequisites」に記載されています。 これらの手順を完了したら、この記事のADFS固有の手順を引き続き使用して設定を完了できます。

Umbrellaドキュメントの手順には、SAML(ADFS)メタデータをUmbrellaにアップロードする必要があると記載されています。このURLに移動してXMLファイルをアップロードすると、メタデータにアクセスできます。

```
https://{your-ADFS-domain-name}/federationmetadata/2007-06/federationmetadata.xml
```

暗号化の無効化

1. AD FS管理を開きます。Trust Relationshipsを展開し、Relying Party Trustsを選択します。

2. Umbrella証明書利用者（または名前を付けたもの）を右クリックし、Propertiesを選択します。

3. Encryptionタブを選択します。

4. 「削除」を選択して、暗号化用の証明書を削除します。

5. OKを選択して画面を閉じます。

新しい発行変換要求ルールの追加

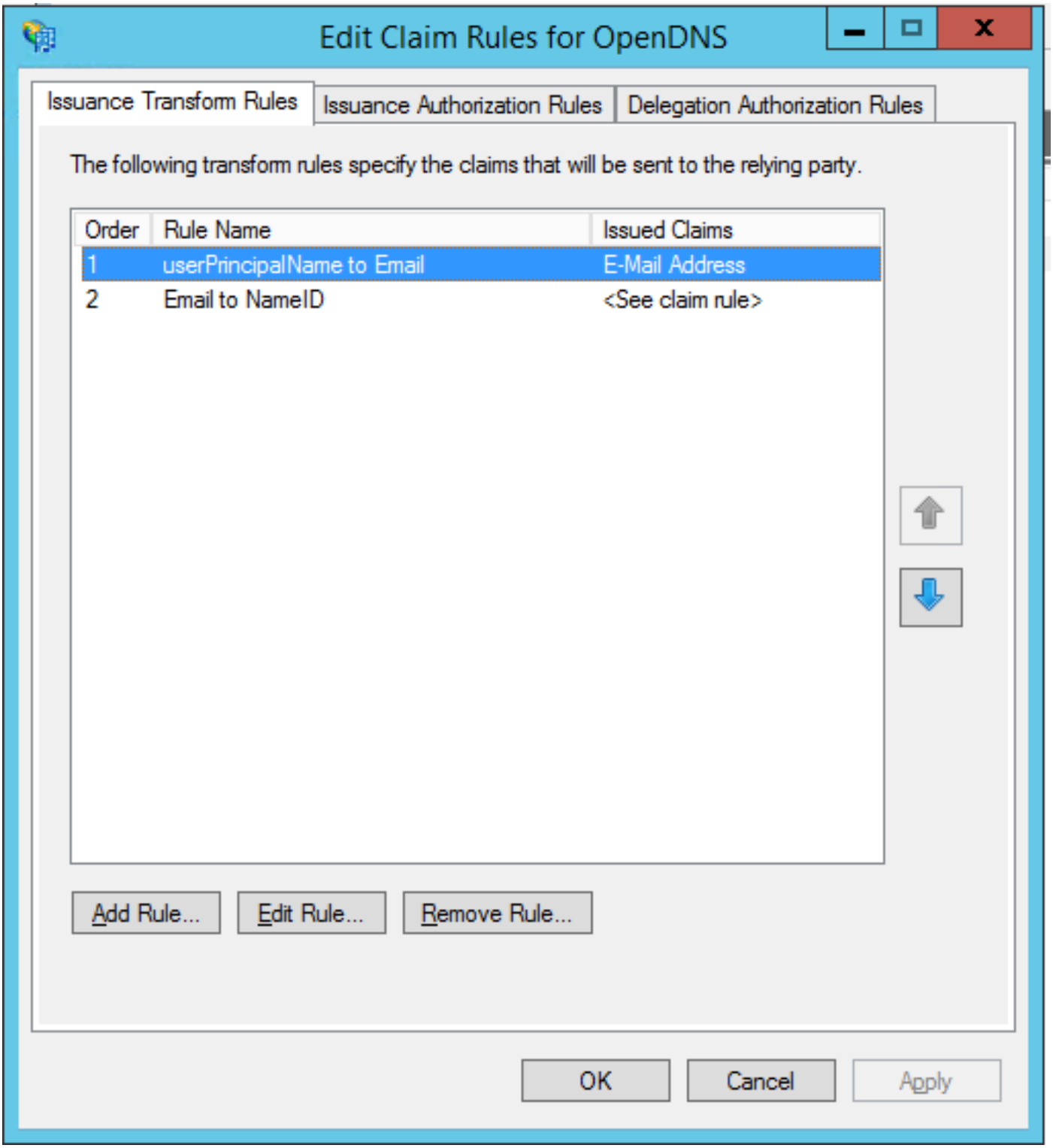
1. AD FS管理を開きます。Trust Relationshipsを展開し、Relaying Party Trustsを選択します。

2. Umbrella中継パーティ（または名前を付けたもの）を右クリックし、[要求規則の編集]を選択します。

3. 「発行変換ルール」で、「ルールの追加」を選択します。

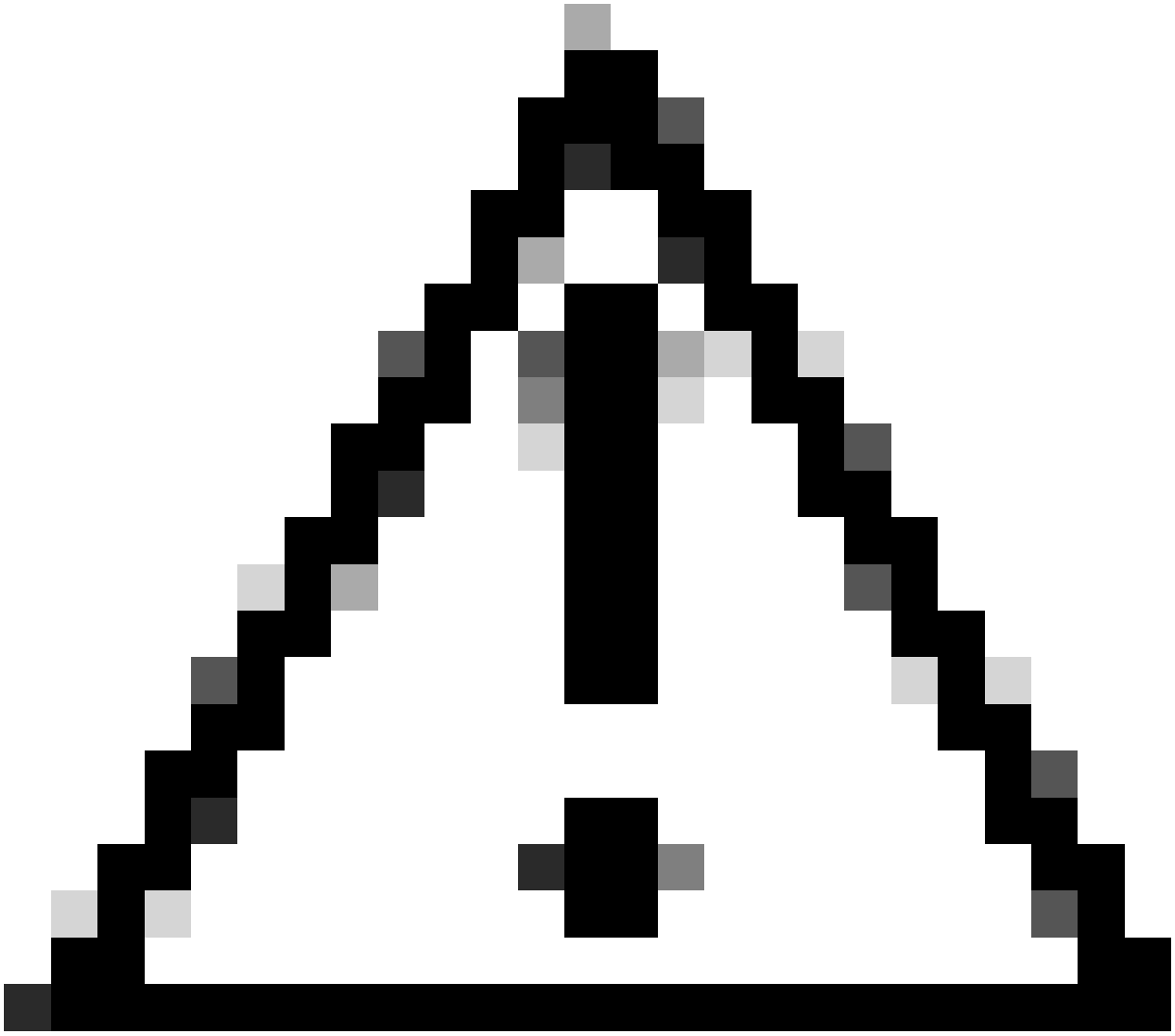
4. [カスタム規則を使用して要求を送信する]を選択します。

追加できるルールのリストについては、このスクリーンショットを参照してください。



これらの各ルールを追加すると、統合が機能し始めます。

トランスフォームルール



注意：これらのルールはテスト済みであり、UmbrellaのADFSラボ環境と、お客様の数台の実稼働環境で機能しています。お客様の環境に合わせて修正してください。

---

userPrincipalNameを電子メールアドレスに

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/em
```

NameIDへの電子メール

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

付録：「mail」属性を使用したログイン

デフォルトでは、ADFSはユーザをUPN（ユーザプリンシパル名）で認証します。 ユーザーの電子メールアドレス（Umbrellaアカウント名）がUPNと一致しない場合は、追加の手順が必要です。Cisco UmbrellaダッシュボードでAD FSを設定して電子メールアドレスでのログインを許可する方法については、ナレッジベースの記事「How do I configure AD FS in the Cisco Umbrella Dashboard」を参照してください。

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。