ADFSサーバで必要な属性UIDを手動で追加する

内容

はじめに

このドキュメントでは、Syntexを使用してADFS証明書利用者信頼に属性UIDを手動で追加する方法について説明します。

前提条件

要件

- ADFSサーバ
- Control Hub

使用するコンポーネント

- ADFSサーバ
- Cisco Webex Control Hub
- オンプレミスAD

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。

設定

これは、既存の属性が原因でADFSに属性の要求を追加する際に問題が発生した場合に役立ちます。

シナリオ 1

UIDまたはUIDという属性を持つ要求ルールが作成された既存の証明書利用者信頼があります。

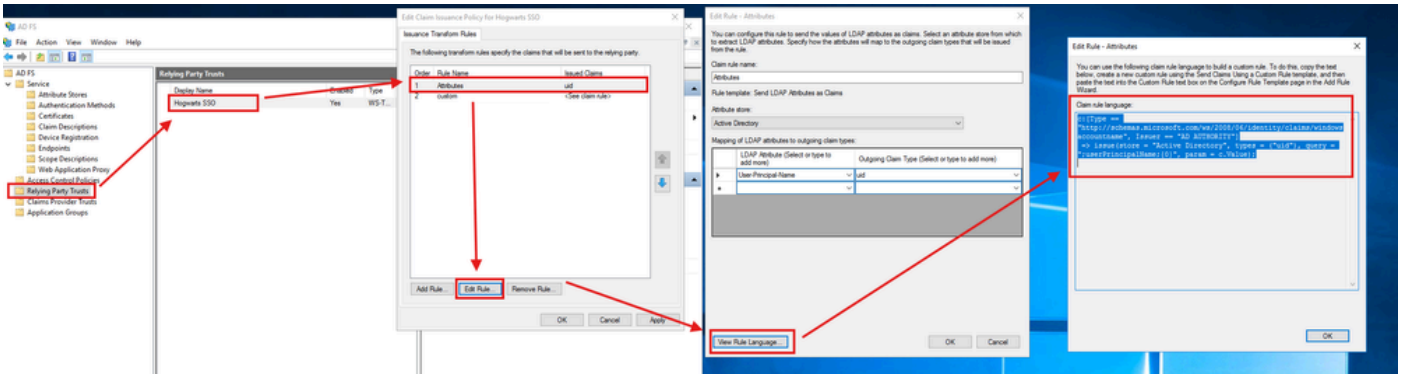
Webex(SP)は必要な属性について大文字と小文字が区別され、uidにする必要があり、SAML応答でユーザのemailAddressを渡す必要があるため、認証は失敗します。

シナリオ 2

uidという名前の属性を渡すが、AD内の必要な属性(emailAddress/UserPrincipalName)とは異なる属性に関連付けられたクレームルールを持つパーティ信頼が存在します。 これにより問題が発生します。

コンフィギュレーション

『Cisco Webexガイド』に従った理想的な設定では、ADFS設定は次のようになります。



ADFS管理者は、証明書利用者信頼 – > Webexに対して作成された信頼 – >要求発行ポリシーの編集 – >ルールの編集 – >属性 – >ルール言語の表示からこのページにアクセスできます。

プレーンテキストのルール言語は次のとおりです。

c:[タイプ==「http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname」、発行者==「AD AUTHORITY」]
=> issue(store = "Active Directory", types = ("uid"), query = ";userPrincipalName;{0}", param = c.Value);

設定が正しく表示されないので、規則言語のプレーンテキストを使用してこの規則を手動で作成します。

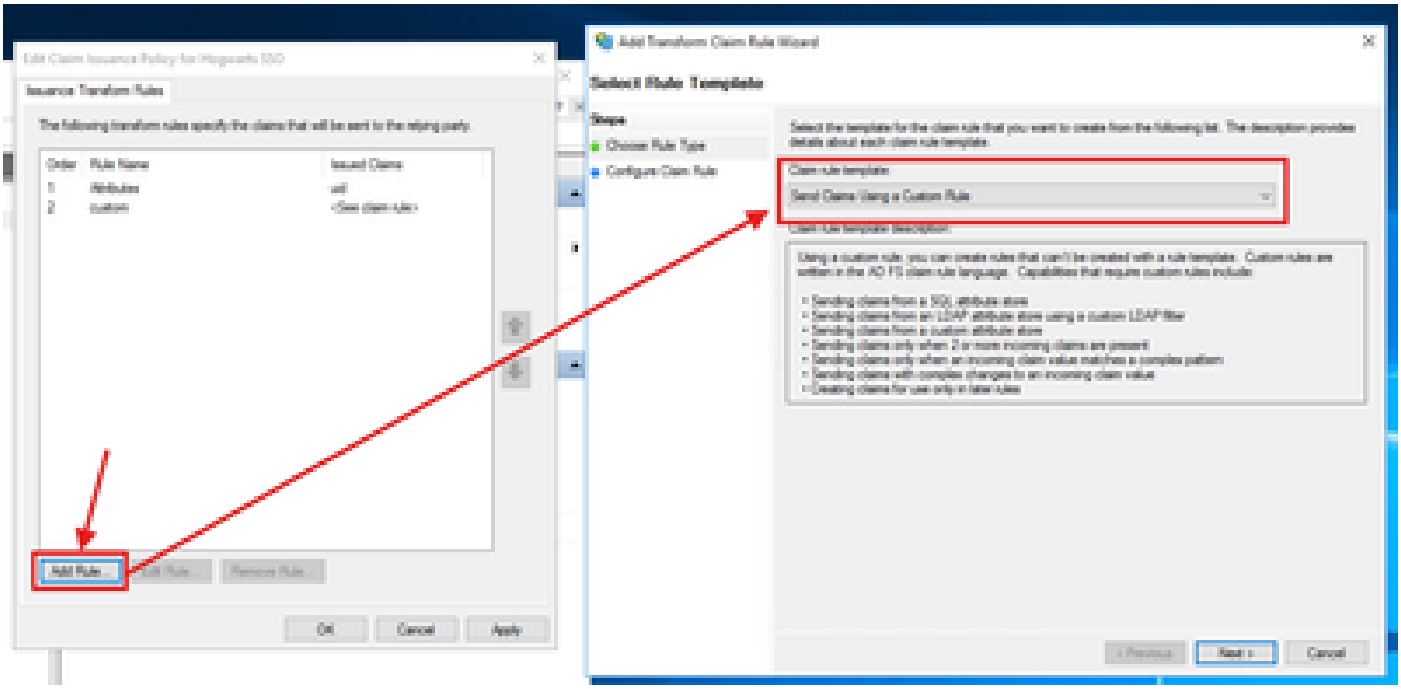
Webex証明書利用者信頼の下のADFSサーバにカスタム要求ルールを追加する

このルールを作成する手順

1. ADFSのメインペインで、作成した信頼関係を選択し、要求規則の編集を選択します。 Issuance Transform Rulesタブで、Add Ruleを選択します。

2. Send Claims Using a Custom Ruleを選択し、Nextを選択します。
3. テキストエディタ（c：から始まる）からルールをコピーし、ADFSサーバのカスタムルールボックスに貼り付けます。

これは次のようになります。



この操作が完了したら、コントロールハブからSSOをテストできます。これは期待どおりに動作する必要があります。

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。