CMSでのWebApp SSOの設定およびトラブルシューティング

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

背景

設定

ネットワーク図

ADFSのインストールと初期セットアップ

アイデンティティプロバイダー(IdP)へのCMSユーザのマッピング

IdP用のWebbridgeメタデータXMLの作成

アイデンティティプロバイダー(IdP)へのWebbridgeのメタデータのインポート

IdPでのWebbridgeサービスのクレームルールの作成

Webbridge用のSSOアーカイブZIPファイルを作成します。

- idp_config.xmlを取得して設定します
- コンテンツを含むconfig.jsonFileの作成
- sso_sign.keyの設定（オプション）
- sso_encrypt.keyを設定します（オプション）。
- SSO ZIPファイルの作成
- SSO ZipファイルをWebbridgeにアップロードします

共通アクセスカード(CAC)

WebApp経由のSSOログインのテスト

トラブルシューティング

- 基本的なトラブルシューティング
- Microsoft ADFS障害コード
- 認証IDを取得できませんでした
- 検証でアサーションが渡されませんでした/一致しませんでした
- Webアプリでサインインできませんでした：
  - シナリオ1：
  - シナリオ2：
  - シナリオ3：
- ユーザ名が認識されない
  - シナリオ1：
  - シナリオ2：
- Webbridgeのログで作業ログの例を示します。結合URLで？trace=trueを使用して生成された例：

よく寄せられる質問（FAQ）

- Webapp SSO JWTは拡張できますか。
- ブラウザを閉じた場合、WebAppへの再認証が必要ですか。

WebApp SSOでは複数ドメインをどのようにサポートしていますか。

関連情報

はじめに

このドキュメントでは、シングルサインオン(SSO)のCisco Meeting Server(CMS)Web App実装を設定およびトラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する知識があることを推奨しています。

- CMS Callbridgeバージョン3.1以降
- CMS Webbridgeバージョン3.1以降
- Active Directory サーバ
- プロバイダーの識別(IdP)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CMS Callbridgeバージョン3.2
- CMS Webbridgeバージョン3.2
- Microsoft Active Directory Windows Server 2012 R2
- Microsoft ADFS 3.0 Windows Server 2012 R2

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。

背景

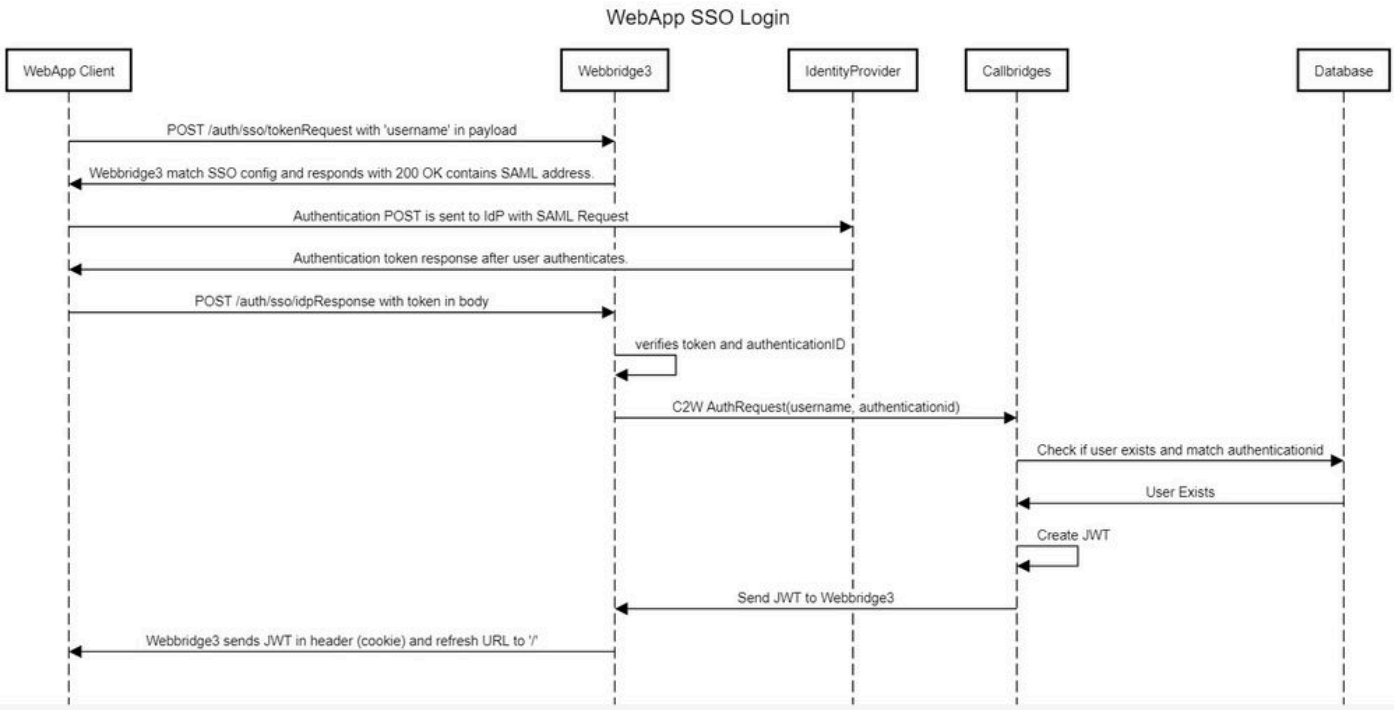
CMS 3.1以降では、IDプロバイダーを使用して1つのセッションが作成されるため、ユーザがログインするたびにパスワードを入力しなくてもSSOを使用してサインインできるようになりました。
この機能は、SSOメカニズムとしてSecurity Assertion Markup Language(SAML)バージョン2.0を使用しています。

注： CMSはSAML 2.0でHTTP-POSTバインディングのみをサポートし、使用可能なHTTP-POSTバインディングがないIDプロバイダーを拒否します。

注：SSOを有効にすると、基本的なLDAP認証は使用できなくなります。

設定

ネットワーク図



ADFSのインストールと初期セットアップ

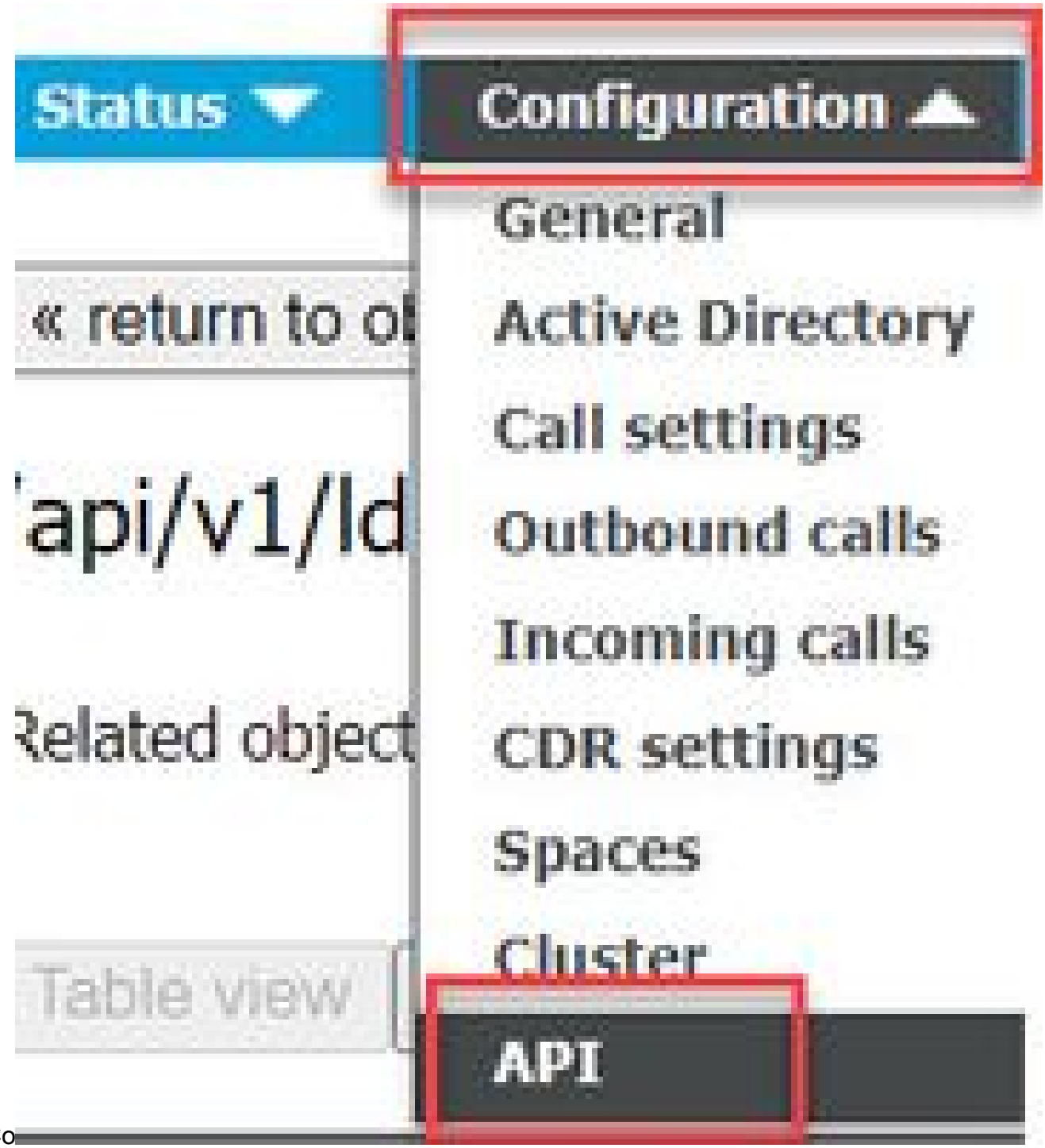
この導入シナリオでは、Identity Provider(IdP)としてMicrosoft Active Directory Federation Services(ADFS)を使用します。そのため、この構成の前にADFS（または対象のIdP）をインストールして実行することをお勧めします。

アイデンティティプロバイダー(IdP)へのCMSユーザのマッピング

有効な認証をユーザに取得させるには、IdPによって提供される相関フィールド用にアプリケーシ

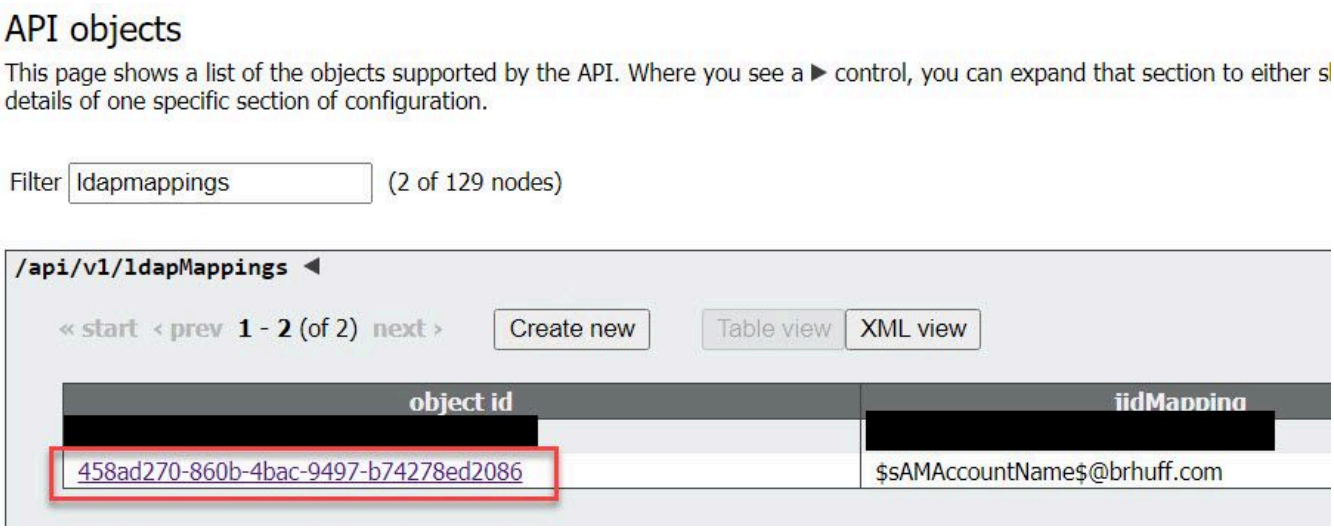
ョンプログラミングインターフェイス(API)でユーザをマッピングする必要があります。このために使用されるオプションは、APIのldapMapping内のauthenicationIdMappingです。

1. CMS Web Admin GUIで、Configuration > APIの順に移動します

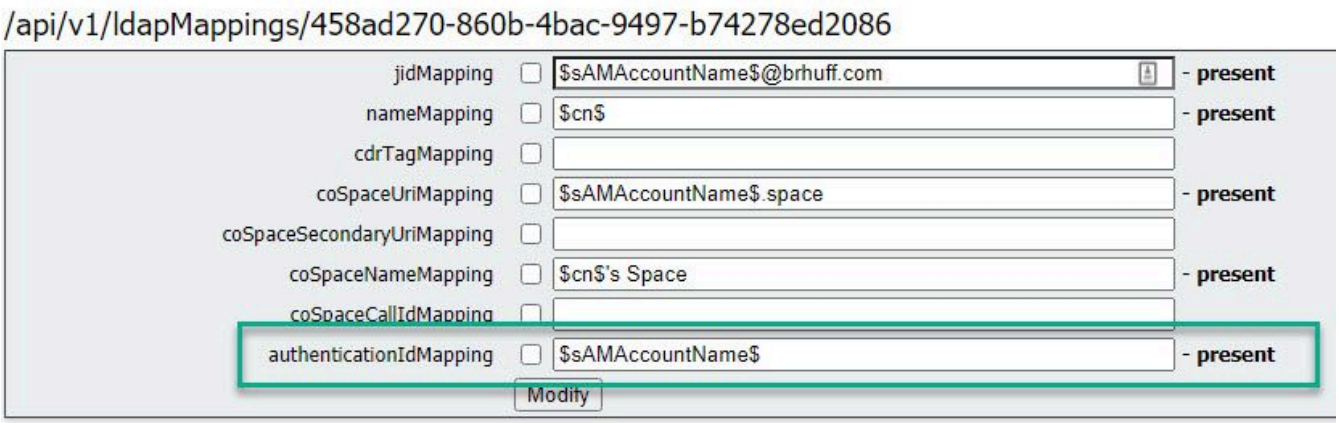


Co

2.api/v1/ldapMappings/<GUID-of-Ldap-Mapping>で既存のLDAPマッピングを見つけます（または新しいLDAPマッピングを作成します）。



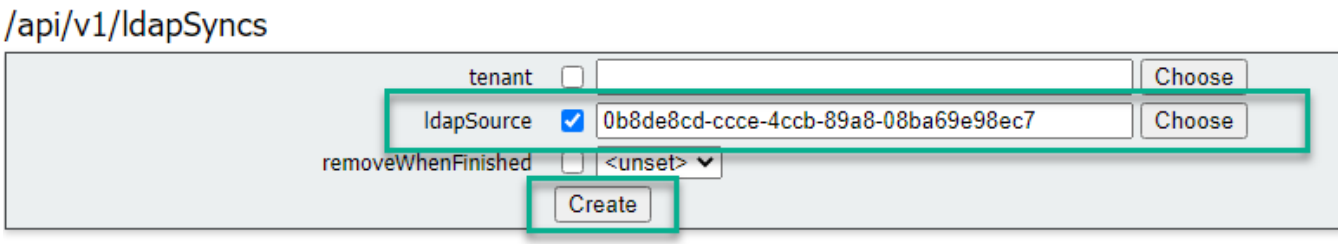
3. 選択したIdapMappingオブジェクトで、IdPから渡されるLDAP属性へのauthenticationIdMappingを更新します。この例では、オプション$sAMAccountNameisがマッピング用のLDAP属性として使用されています。



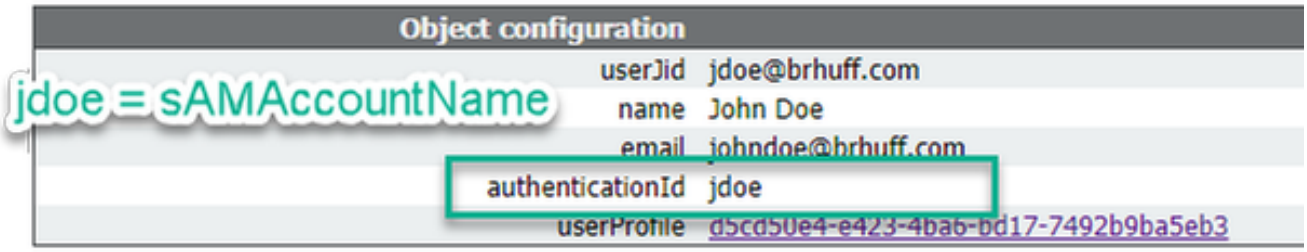
注：authenticationIdMappingは、callbridge/データベースによってSAMLResponse内のIdPから送信されたクレームを検証し、ユーザにJSON Web Token(JWT)を提供するために使用されます。

4. 最近変更されたIdapMappingに関連付けられたIdapSourceでLDAP syncを実行します。

例：



5. LDAPの同期が完了したら、CMS APIのConfiguration > api/v1/usersに移動し、インポートされたユーザを選択して、authenticationIdが正しく入力されていることを確認します。



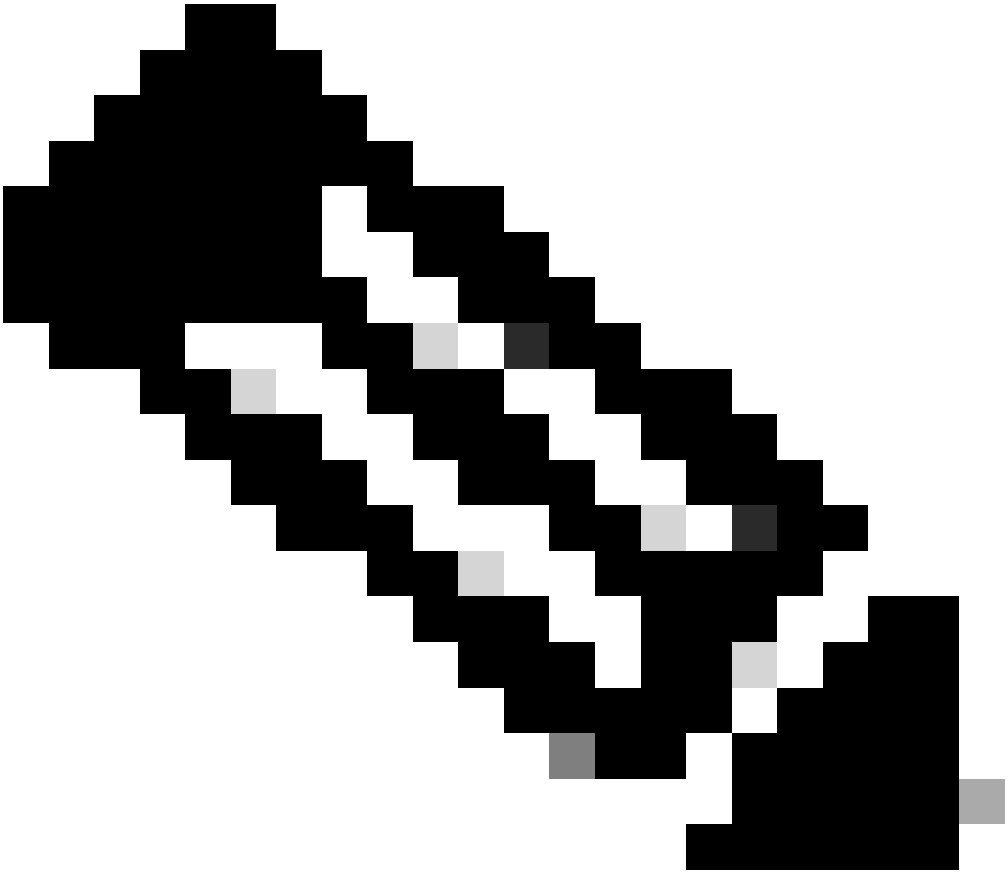
IdP用のWebbridgeメタデータXMLの作成

Microsoft ADFSを使用すると、メタデータXMLファイルを証明書利用者信頼パーティとしてインポートして、使用されているサービスプロバイダーを識別できます。この目的でメタデータXMLファイルを作成する方法はいくつかありますが、ファイルに存在する必要がある属性がいくつかあります。

必要な値を持つWebbridgeメタデータの例：

```
<?xml version="1.0"?>
- <md:EntityDescriptor entityID="https://meet.brhuff.local:443" ID="https://meet.brhuff.local:443"
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
    - <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true"
      AuthnRequestsSigned="false">
          <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
          <md:AssertionConsumerService index="0" Location="https://meet.brhuff.local:443/api/auth/sso/idpResponse"
              Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
      </md:SPSSODescriptor>
  </md:EntityDescriptor>
```

1. entityID：これは、Webbridge3サーバアドレス（FQDN/ホスト名）と、ユーザのブラウザが到達可能な関連ポートです。



注:1つのURLを使用する複数のWebbridgeがある場合、これはロードバランシングアドレスである必要があります。

2. Location：これは、WebbridgeアドレスのHTTP-POST AssertionConsumerServiceがある場所です。これは、サインイン後に認証されたユーザをリダイレクトする場所をIdPに指示するものです。これは、idpResponse URL:https://<WebbridgeFQDN>:<port>/api/auth/sso/idpResponseに設定する必要があります。 たとえば、https://join.example.com:443/api/auth/sso/idpResponse に保存します。

3. オプション：署名用の公開キー：これは署名用の公開キー（証明書）であり、WebbridgeからのAuthRequestを確認するためにIdPによって使用されます。これは、WebbridgeにアップロードされたSSOバンドルの秘密キー「sso_sign.key」と一致している必要があります。これにより、IdPは公開キー（証明書）を使用して署名を検証できます。展開から既存の証明書を使用できます。 テキストファイルで証明書を開き、Webbridgeメタデータファイルに内容をコピーします。 sso_xxxx.zipファイルで使用されている証明書に一致するキーをsso_sign.keyファイルとして使用します。

4. オプション：暗号化用の公開キー：これは、Webbridgeに返信されるSAML情報を暗号化するためにIdPで使用する公開キー（証明書）です。これは、Webbridgeにアップロードされたsso バンドルの秘密キー「sso_encrypt.key」と一致している必要があります。一致していないと、WebbridgeはIdPによって返信された内容を復号化できません。 展開から既存の証明書を使用できます。 テキストファイルで証明書を開き、Webbridgeメタデータファイルに内容をコピーします。 sso_xxxx.zipファイルで使用されている証明書に一致するキーをsso_encrypt.keyファイルとして使用します。

オプションの公開キー（証明書）データを使用してIdPにインポートされるWebbridgeメタデータの例：

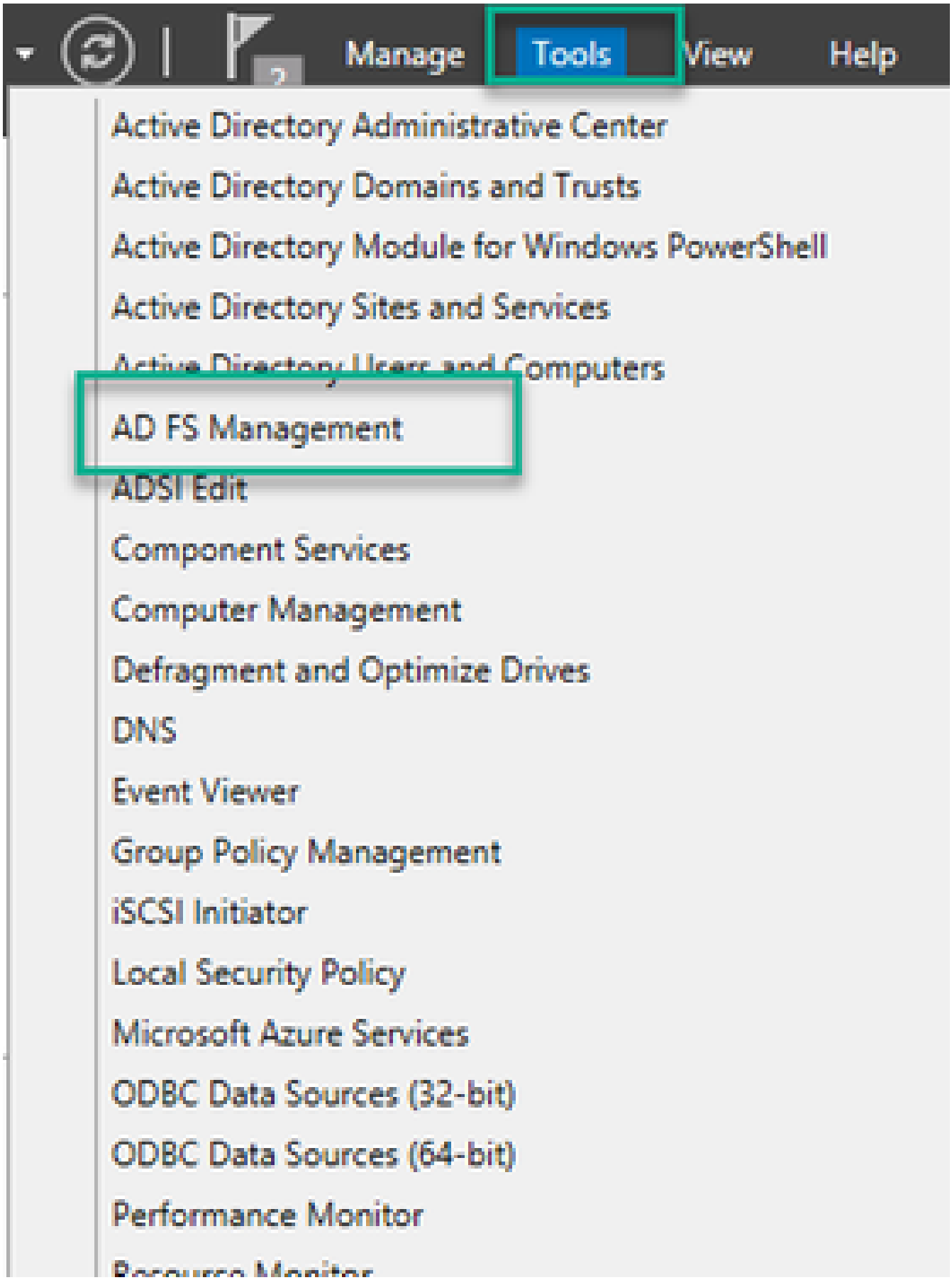
```
<?xml version="1.0"?>
- <md:EntityDescriptor entityID="https://meet.brhuff.local:443" ID="https://meet.brhuff.local:443" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  - <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" AuthnRequestsSigned="true">
    - <md:KeyDescriptor use="signing">
      - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        - <ds:X509Data>
            <ds:X509Certificate>MIIFwTCCBKmgAwIBAgIT[redacted]
              </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>
    - <md:KeyDescriptor use="encryption">
      - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        - <ds:X509Data>
            <ds:X509Certificate>MIIFwTCCBKmgAwIBAgIT[redacted]
              </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
      <md:AssertionConsumerService index="0" Location="https://meet.brhuff.local:443/api/auth/sso/idpResponse" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
    </md:SPSSODescriptor>
  </md:EntityDescriptor>
```

アイデンティティプロバイダー(IdP)へのWebbridgeのメタデータのインポート

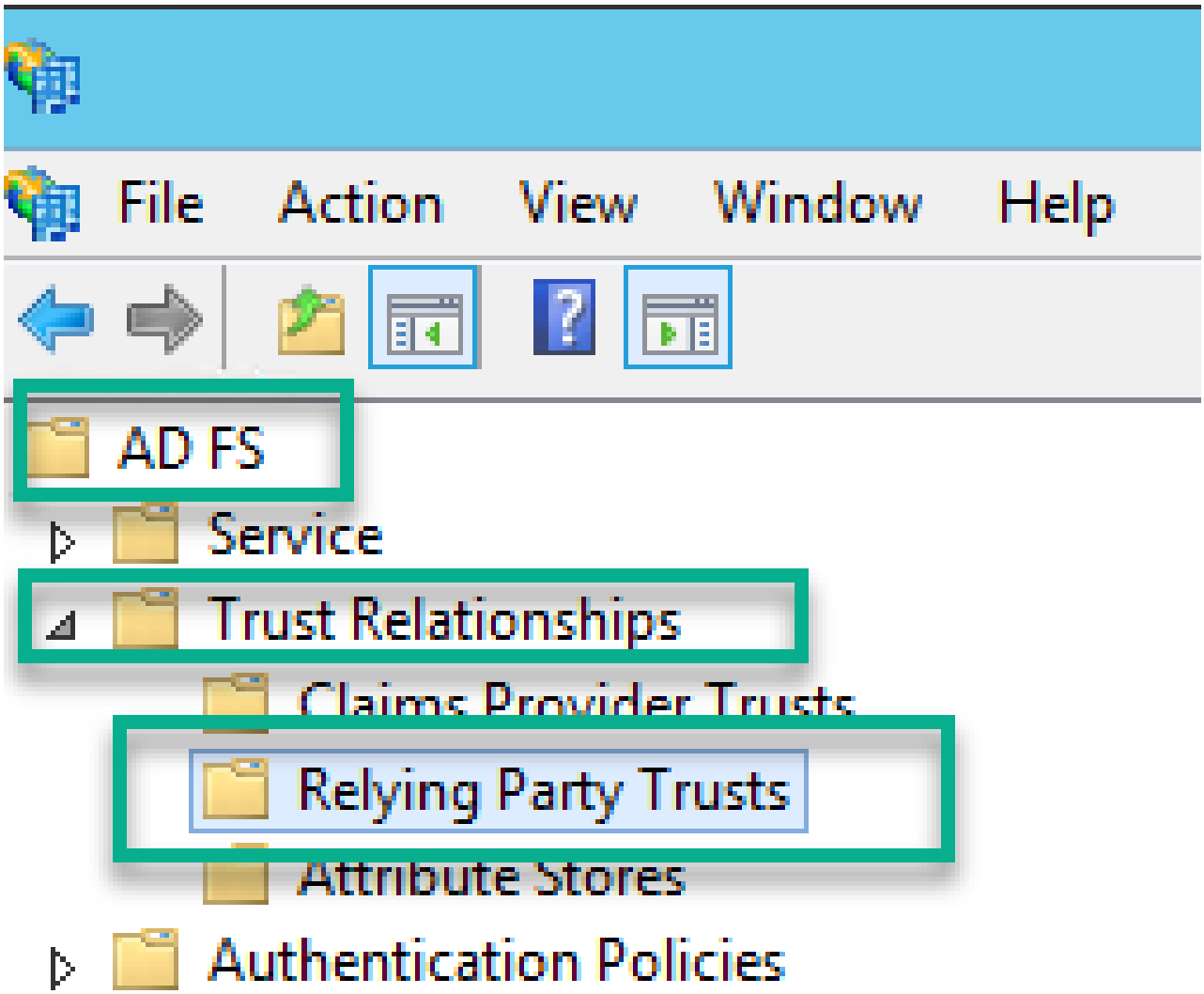
適切な属性を使用してメタデータXMLが作成されたら、そのファイルをMicrosoft ADFSサーバにインポートして、証明書利用者信頼を作成できます。

1. ADFSサービスをホストしているWindows Serverへのリモートデスクトップ

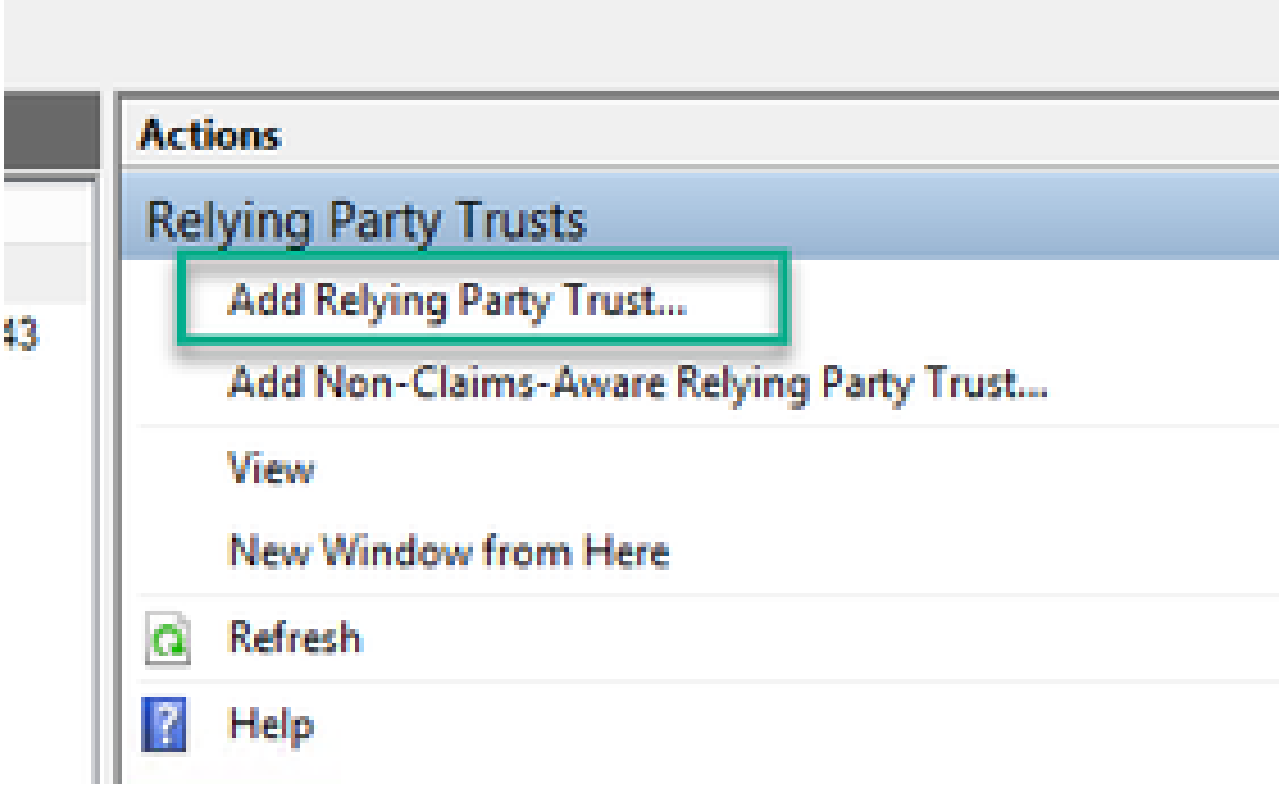
2. AD FS管理コンソールを開きます。通常は、サーバーマネージャーからアクセスできます。



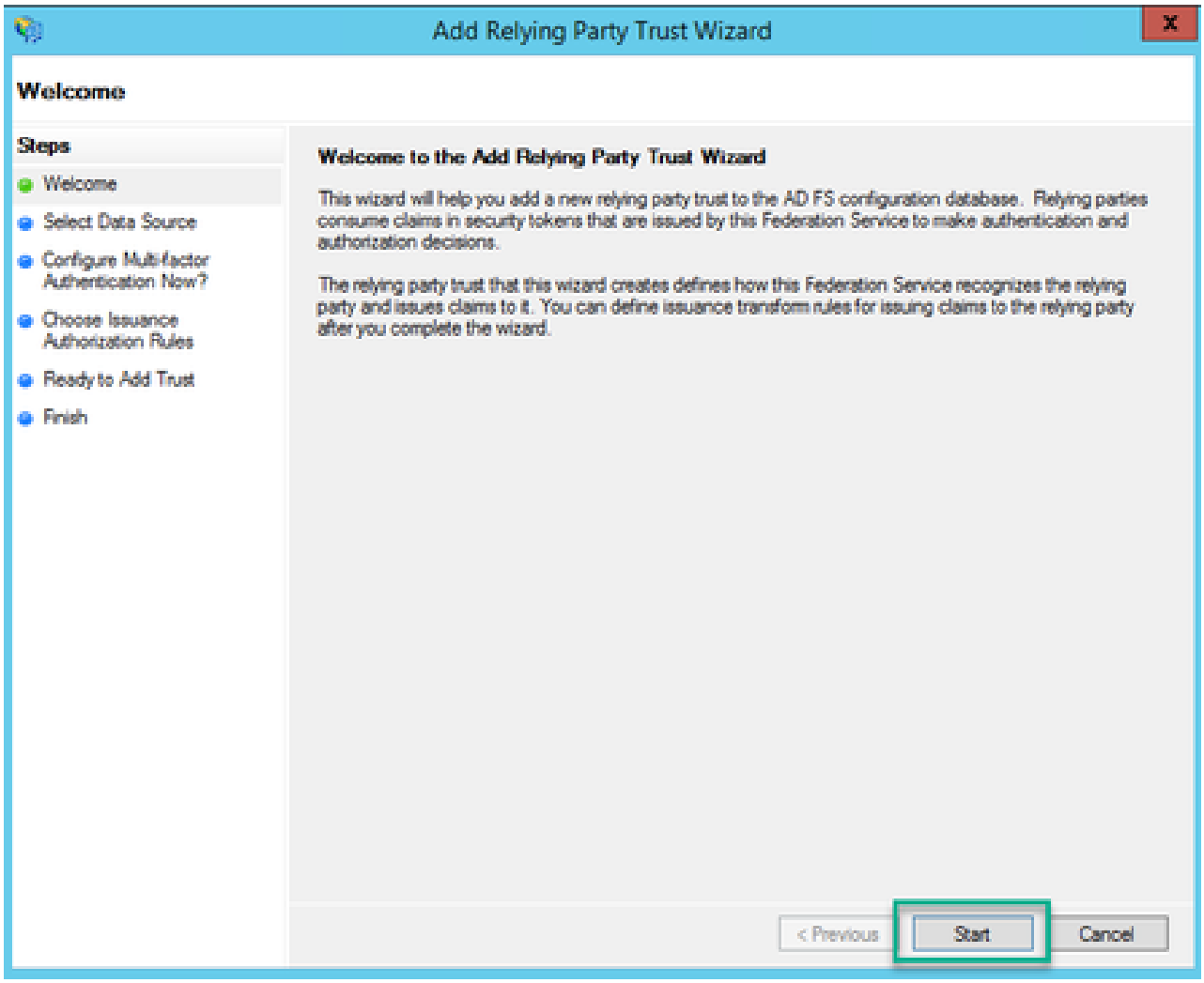
3. ADFS管理コンソールが表示されたら、左側のペインでADFS > Trust Relationships > Relying Party Trustの順に移動します。



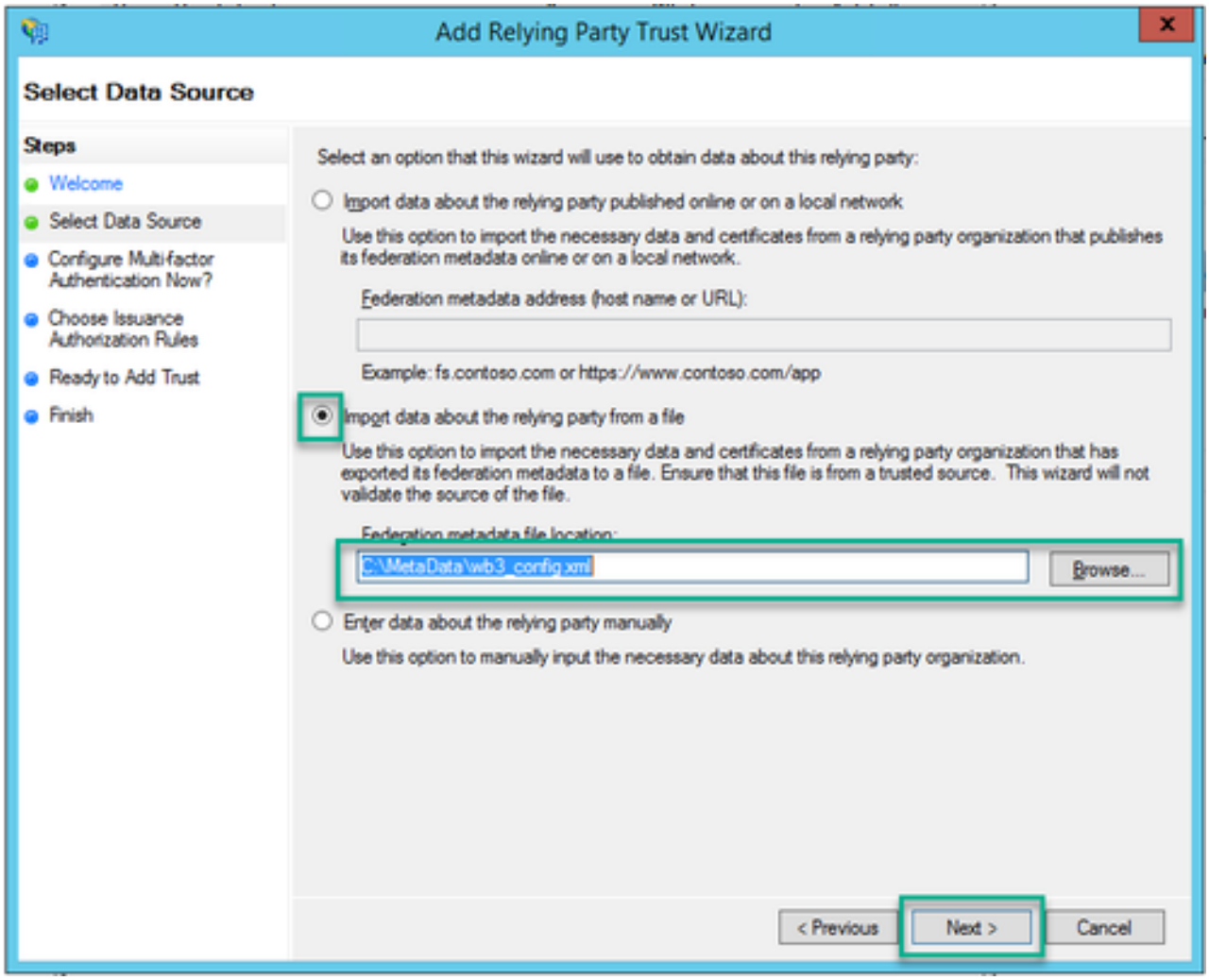
4. ADFS管理コンソールの右側のウィンドウで、[証明書利用者信頼の追加...]オプションを選択します。



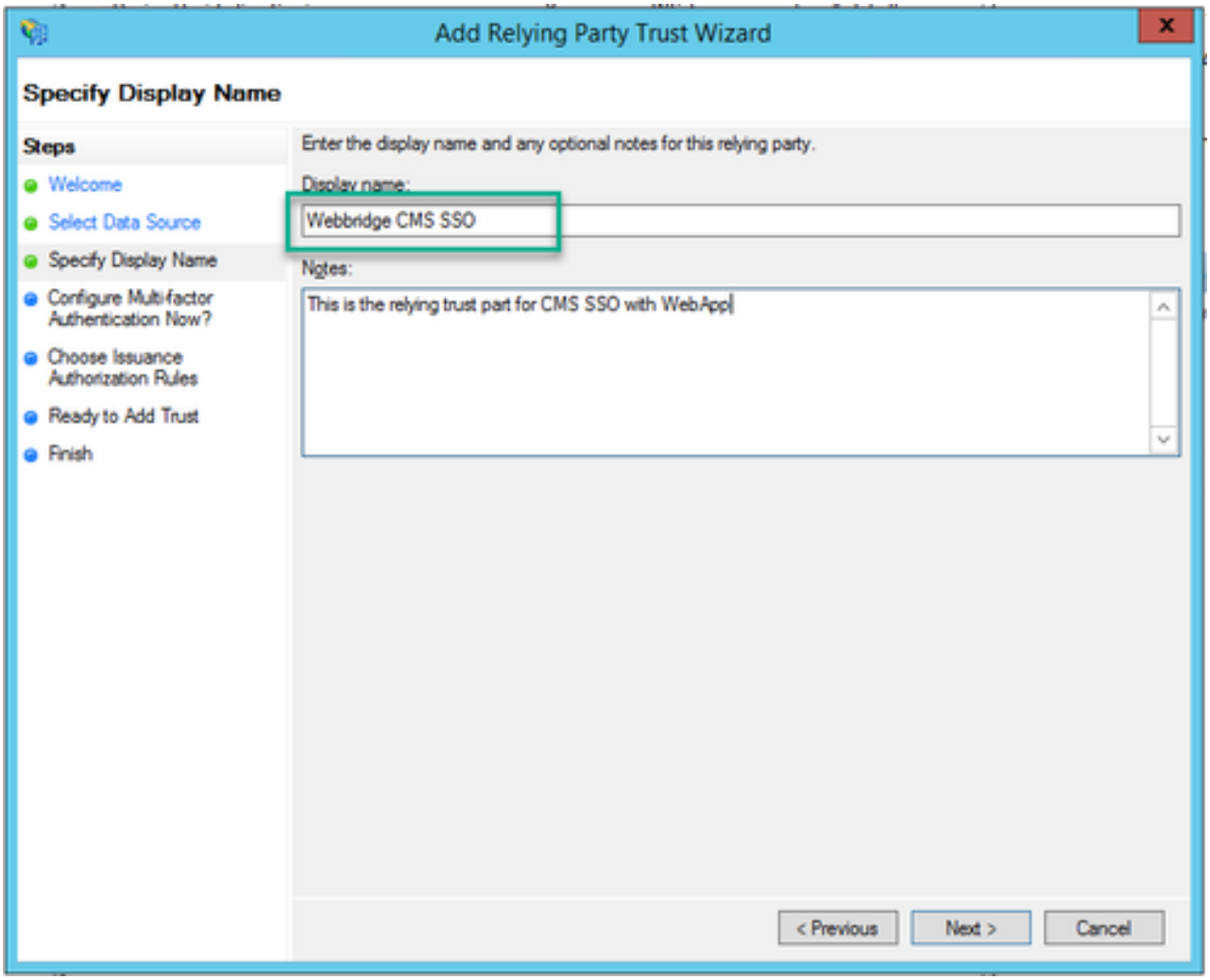
5. これを選択すると、証明書利用者信頼の追加ウィザードが開きます。Start オプションを選択します。



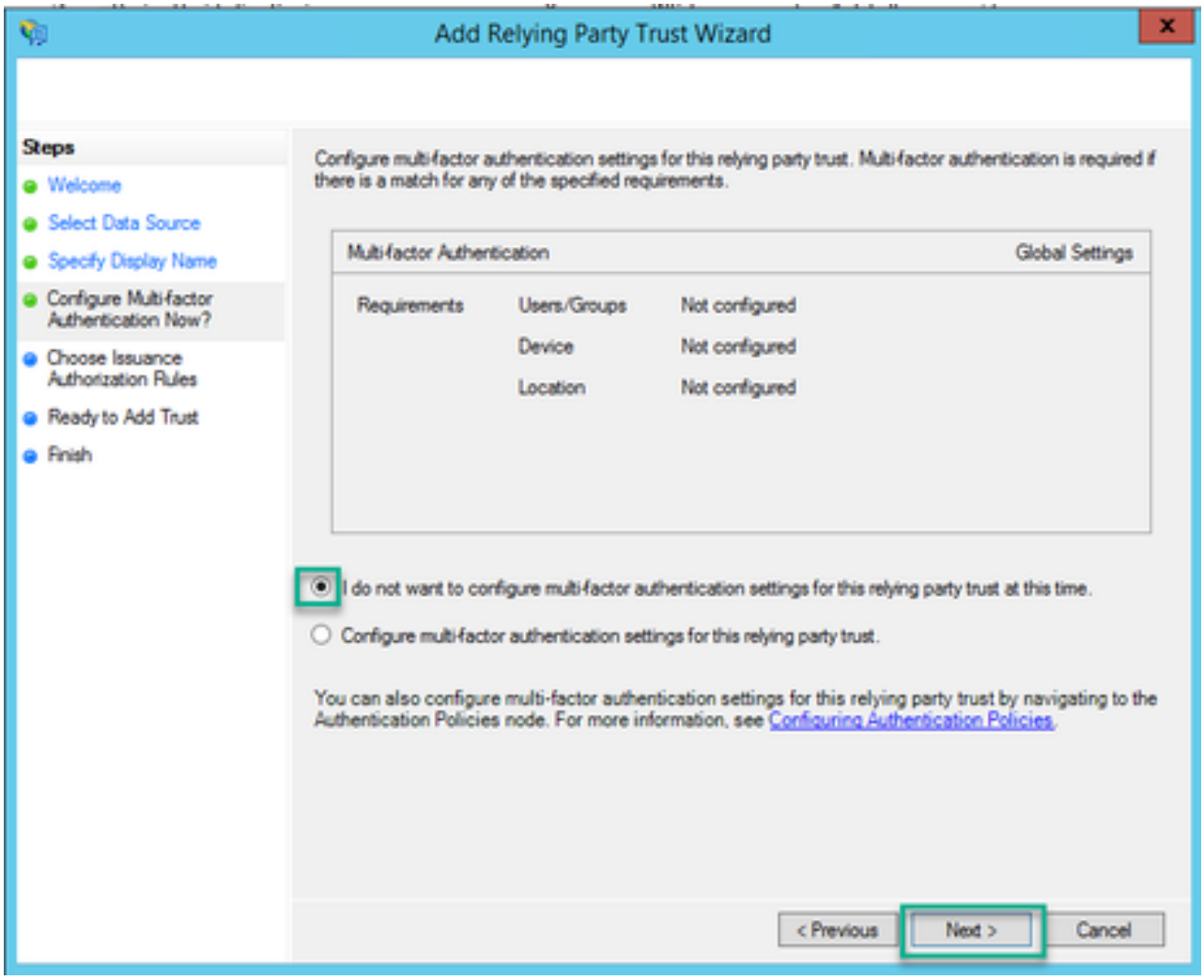
6. Select Data SourceページでImport data about the relying party from a fileのオプションボタンを選択し、Browse を選択して、Webbridge MetaDataファイルの場所に移動します。



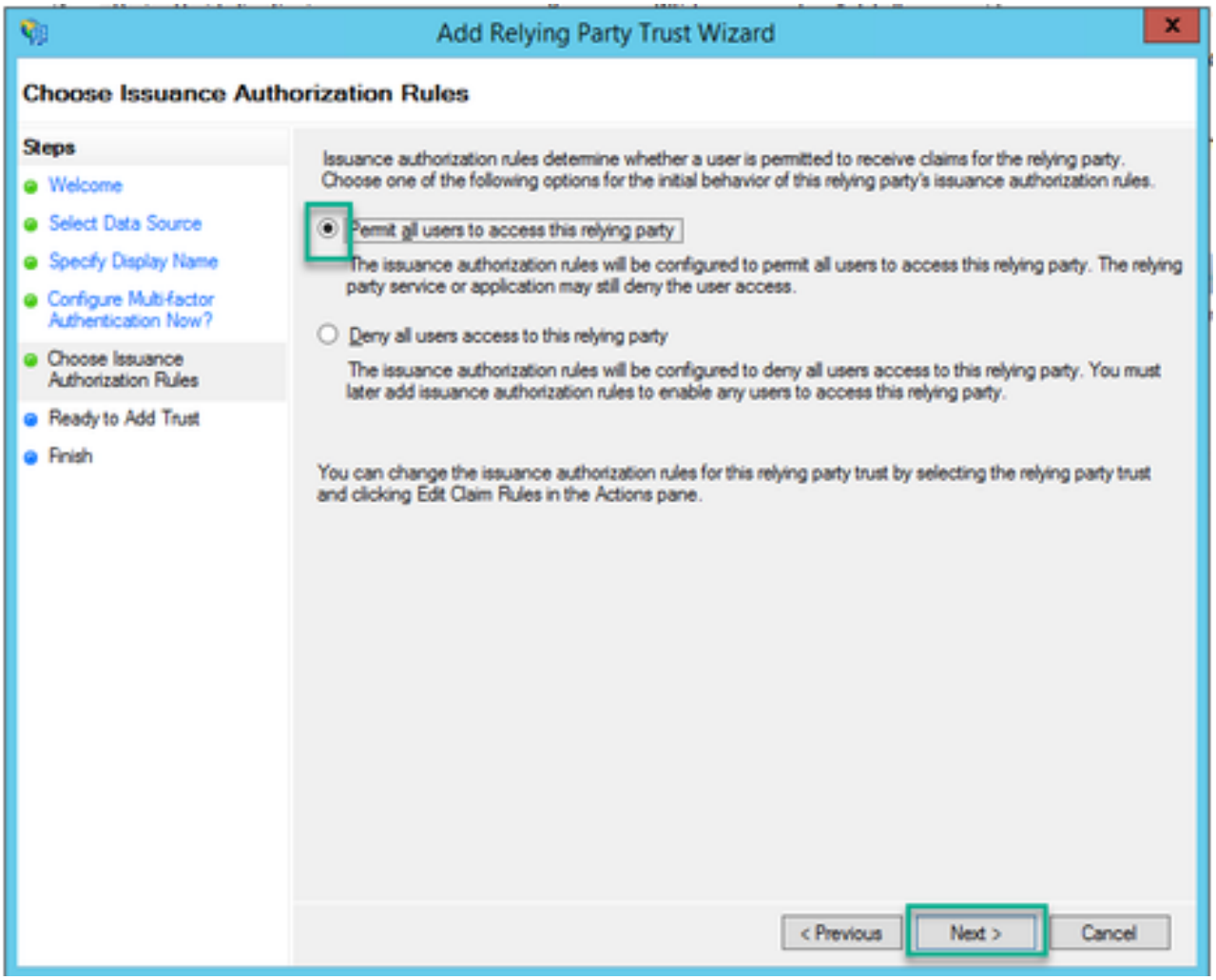
7. 「表示名の指定」ページで、ADFS内のエンティティに対して表示される名前を入力します（表示名はADFS通信のサーバー目的ではなく、単に情報を提供するためのものです）。



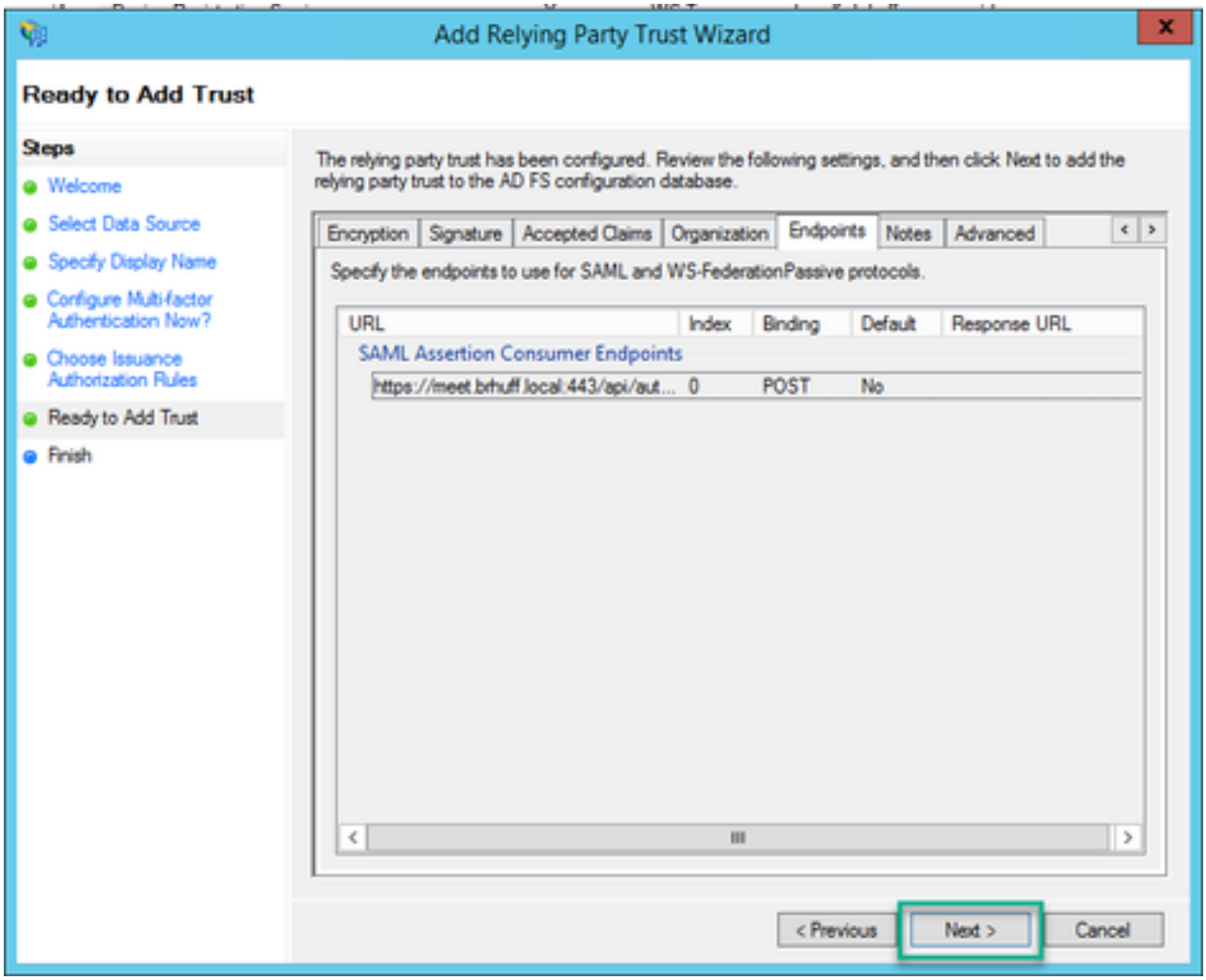
8. 「Configure Multi-factor Authentication Now?」ページで、デフォルトのままにして「Next」を選択します。



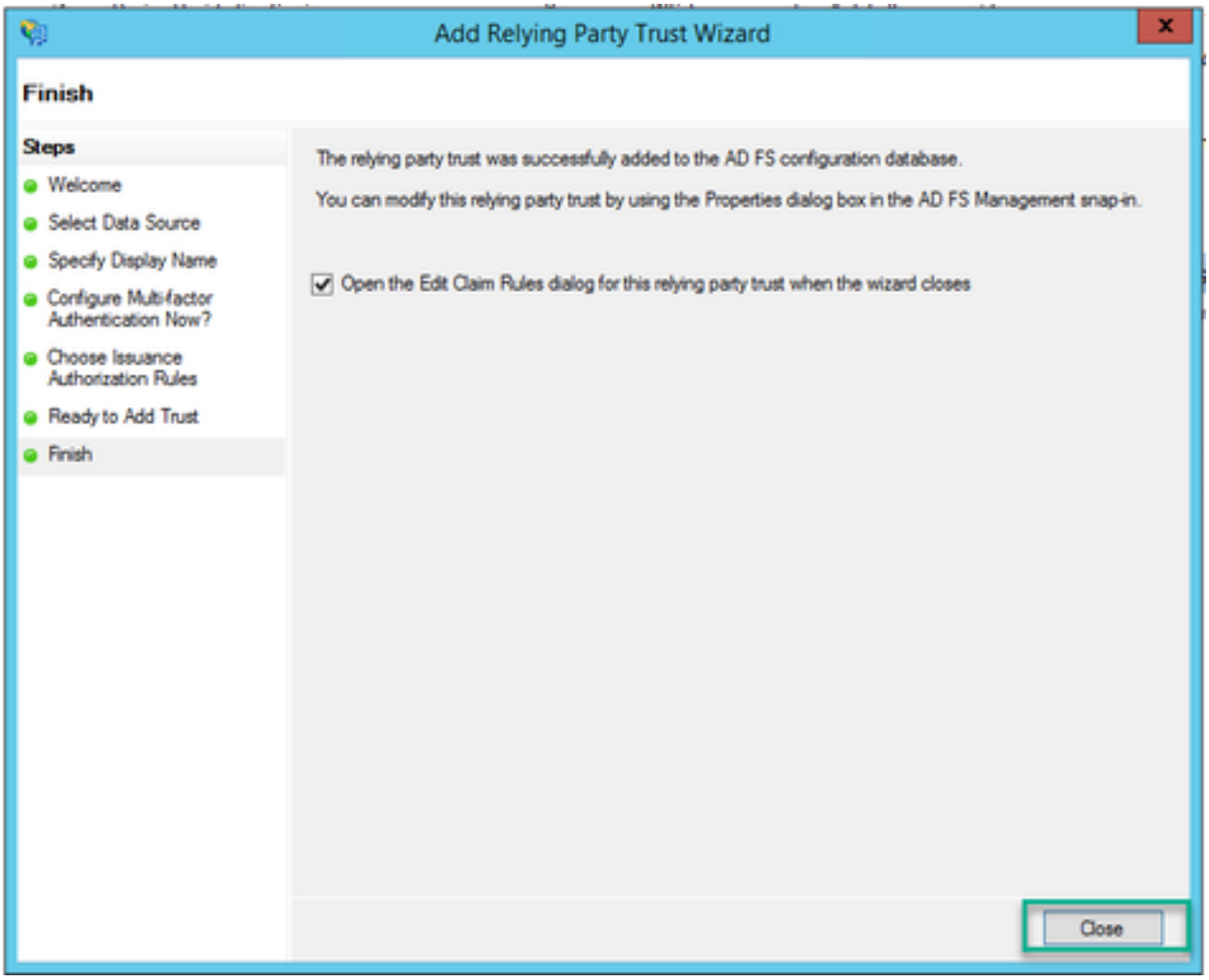
9. Choose Issuance Authorization Rulesページで、Permit all users to access this relying partyにチェックマークを付けたままにします。



10. 信頼を追加する準備の完了ページで、Webbridgeの証明書利用者信頼のインポートされた詳細をタブで確認できます。WebbridgeサービスプロバイダーのURLの詳細については、識別子とエンドポイントを確認します。



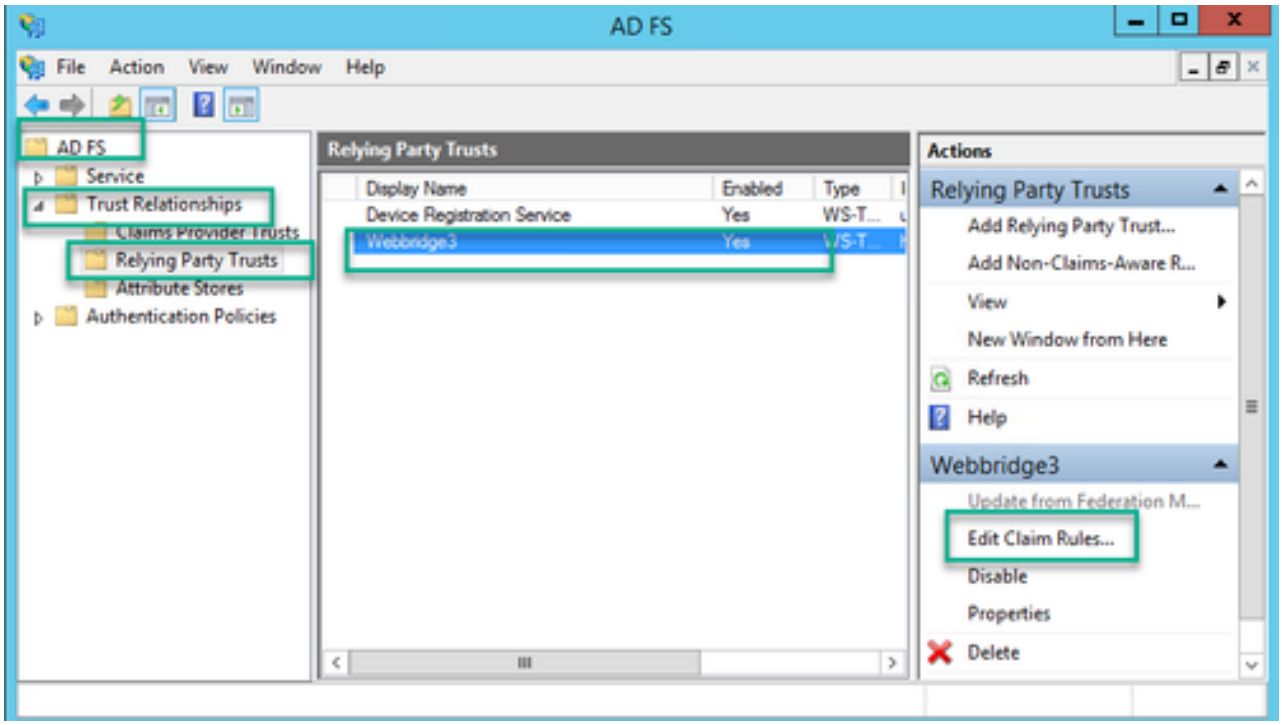
11. [完了]ページで、[閉じる]オプションを選択してウィザードを閉じ、要求ルールの編集を続行します。



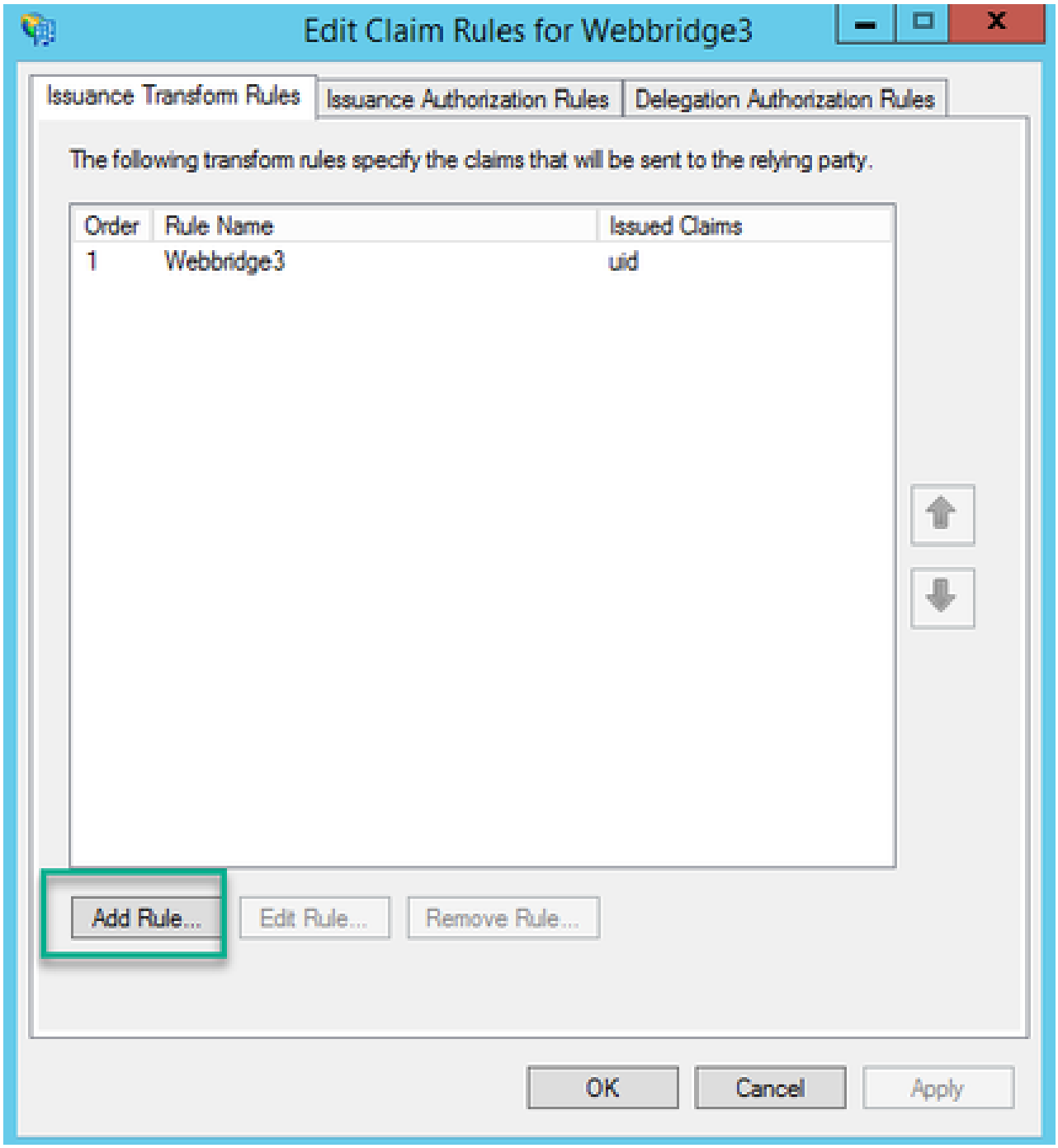
IdPでのWebbridgeサービスのクレームルールの作成

証明書利用者信頼がWebbridge用に作成されたので、SAML応答でWebbridgeに提供される発信要求タイプに特定のLDAP属性を一致させるために、要求規則を作成できます。

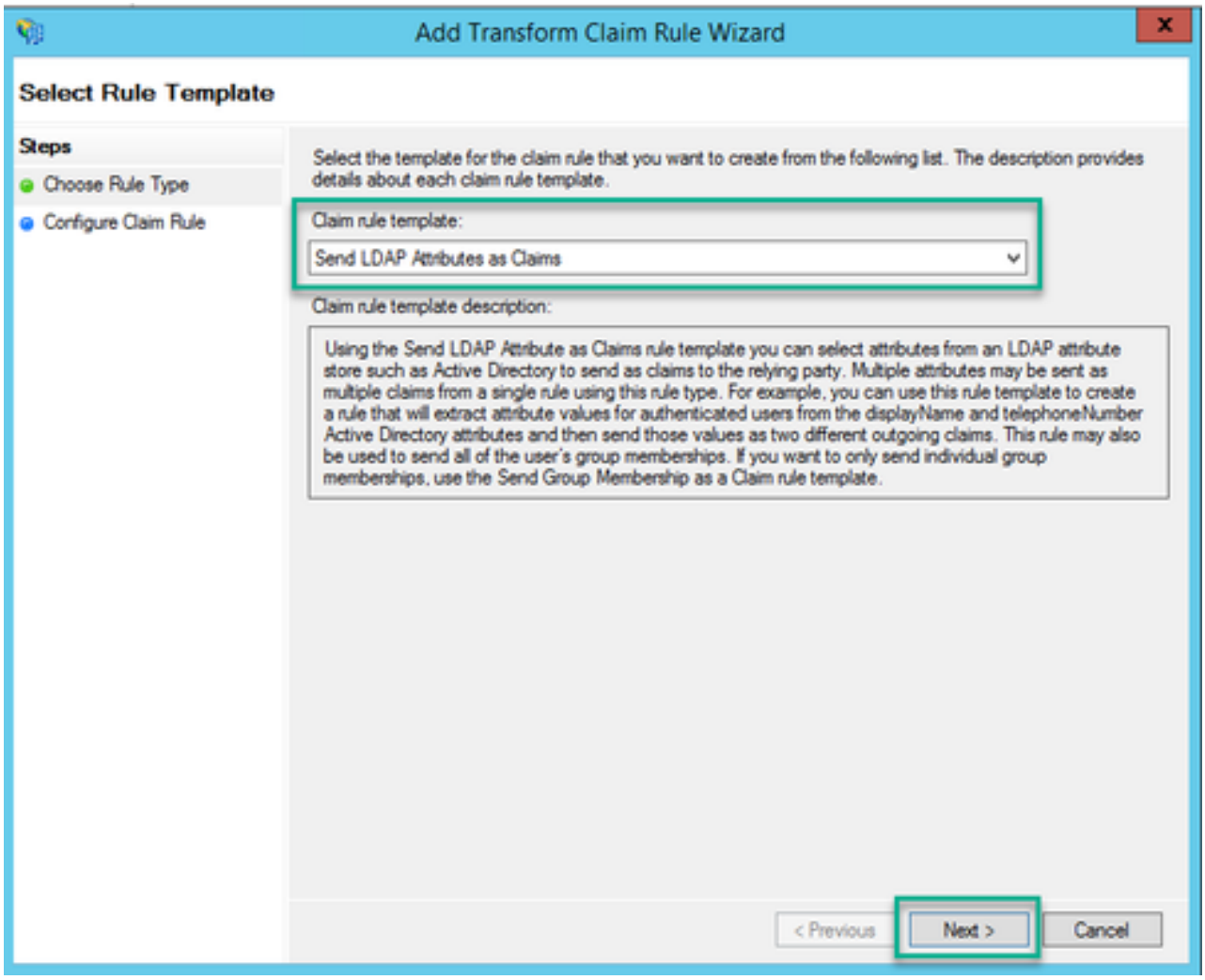
1. ADFS管理コンソールで、Webbridgeの証明書利用者信頼を強調表示し、右側のペインで要求規則の編集を選択します。



2. <DisplayName>様のクレームルールの編集ページで、ルールの追加...を選択します。

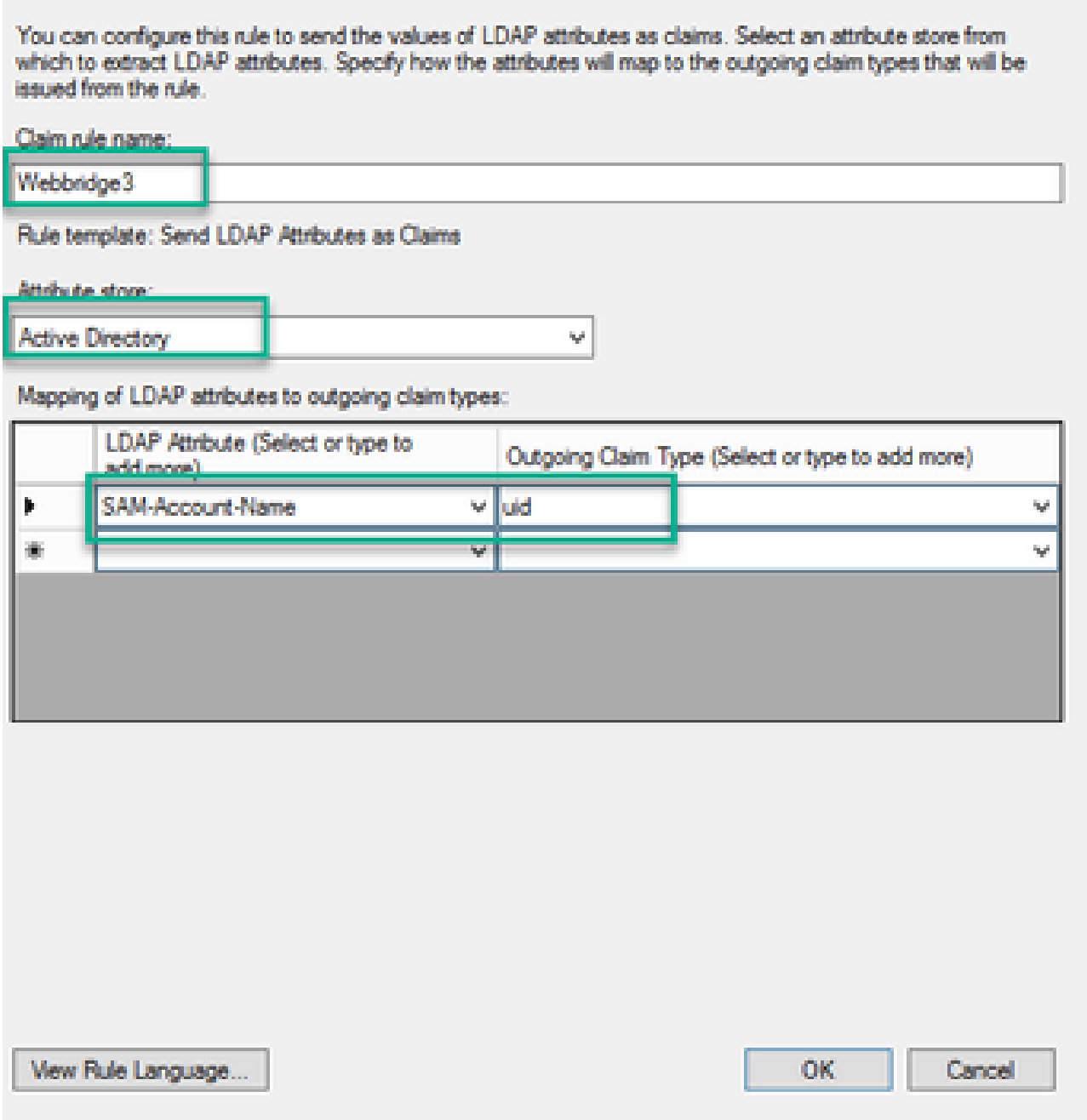


3. Add Transform Claim Rule Wizardページで、Claim Rule templateオプションに対してSend LDAP Attributes as Claimsを選択し、Nextを選択します。



4. 要求規則の構成ページで、証明書利用者信頼の要求規則を次の値で構成します。

    1. クレームルール名 =これはADFSのルールに与えられた名前である必要があります（ルール参照のみ）
    2. 属性ストア= Active Directory
    3. LDAP Attribute = Callbridge APIのauthenticationIdMappingと一致している必要があります（例： $sAMAccountName$）。
    4. 発信クレームタイプ =これは、Webbridge SSOのconfig.json内のauthenticationIdMappingと一致する必要があります。（例：uid）。



Webbridge用のSSOアーカイブZIPファイルを作成します。

この設定は、サポートされているドメインや認証マッピングなどのSSO設定を検証するためにWebbridgeが参照するものです。設定のこの部分では、次のルールを考慮する必要があります。

- ZIPファイルは、ファイル名の前にsso_を付けて開始する必要があります(sso_cmstest.zipなど)。
- このファイルがアップロードされると、Webbridgeは基本認証を無効にし、このファイルがアップロードされたWebbridgeにはSSOのみを使用できます。
- 複数のアイデンティティプロバイダーを使用する場合は、別のZIPファイルを別の命名スキ

ーマでアップロードする必要があります(ただし、sso_のプレフィックスは付けます)。
- zipファイルを作成するときは、ファイルの内容を強調表示してzip圧縮し、必要なファイルをフォルダに入れてzip圧縮しないでください。

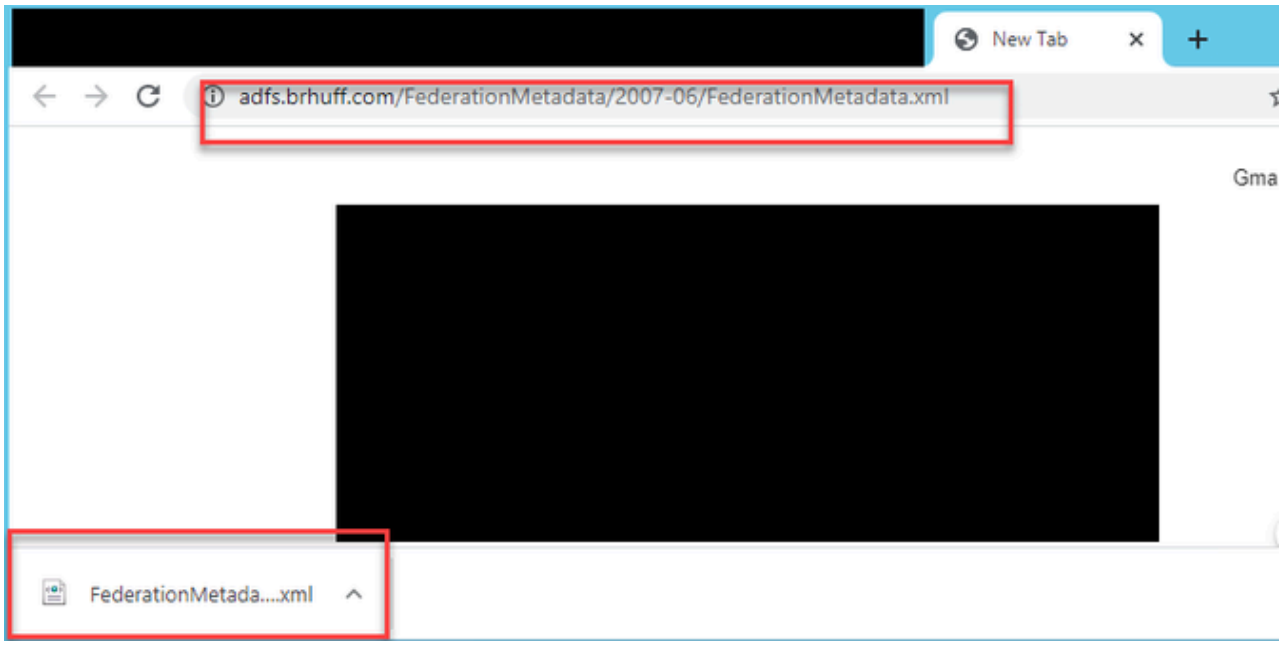
zipファイルの内容は、暗号化が使用されているかどうかに応じて、2 ~ 4ファイルで構成されます。

filename	説明	必要?
idp_config.xml	これは、idPで収集できるMetaDataファイルです。ADFSでは、https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xmlに移動することで、これを見つけることができます。	はい
config.jsonファイル	これは、Webbridgeがサポートされているドメイン、SSOの認証マッピングを検証するために使用するJSONファイルです。	はい
sso_署名。キー	これは、IDプロバイダーで設定された公開署名キーの秘密キーです。署名されたデータのセキュリティ保護にのみ必要	NO
sso_encrypt.key（暗号化キー）	これは、IDプロバイダーで構成された公開暗号化キーの秘密キーです。暗号化されたデータの保護にのみ必要	NO

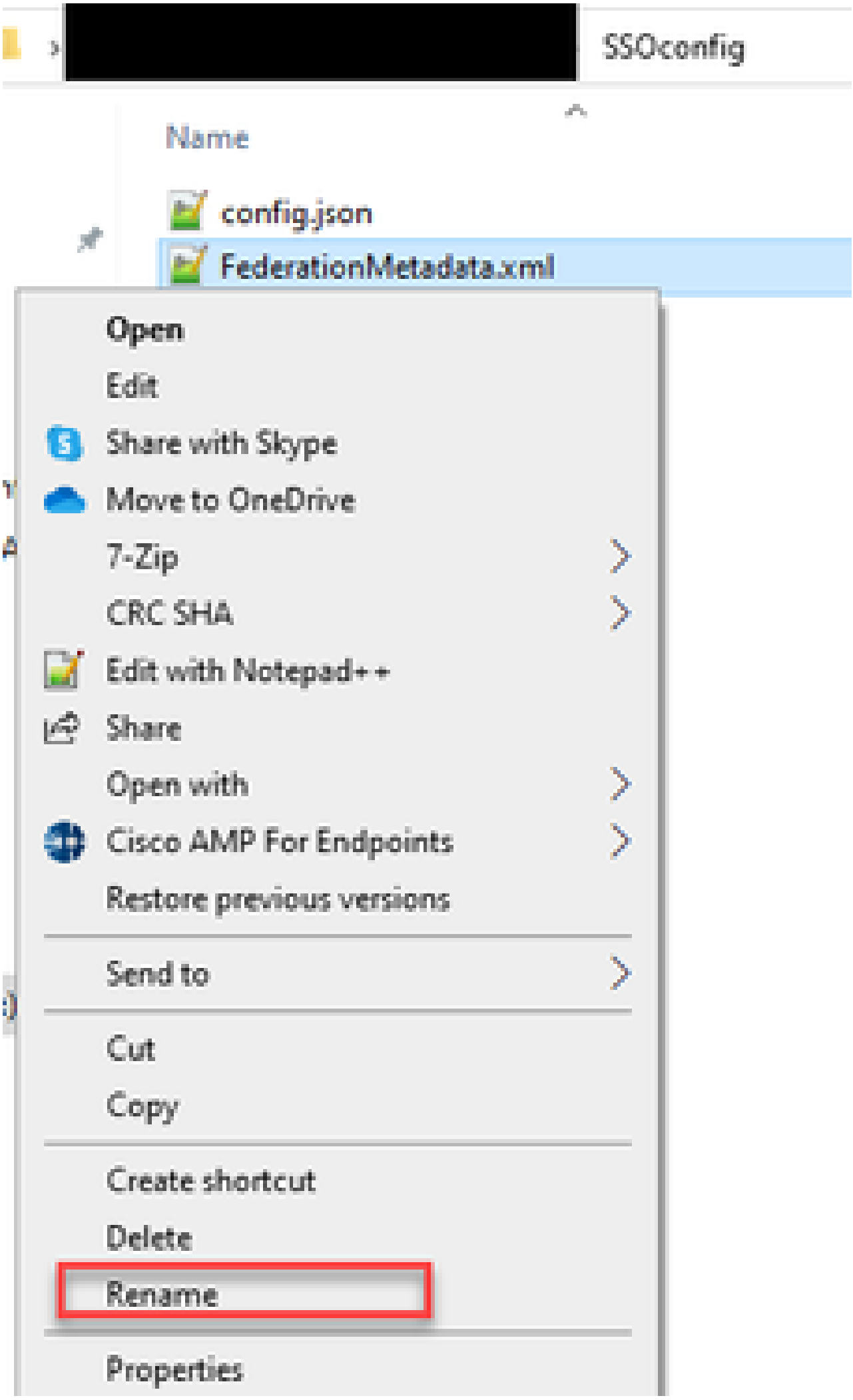
idp_config.xmlを取得して設定します

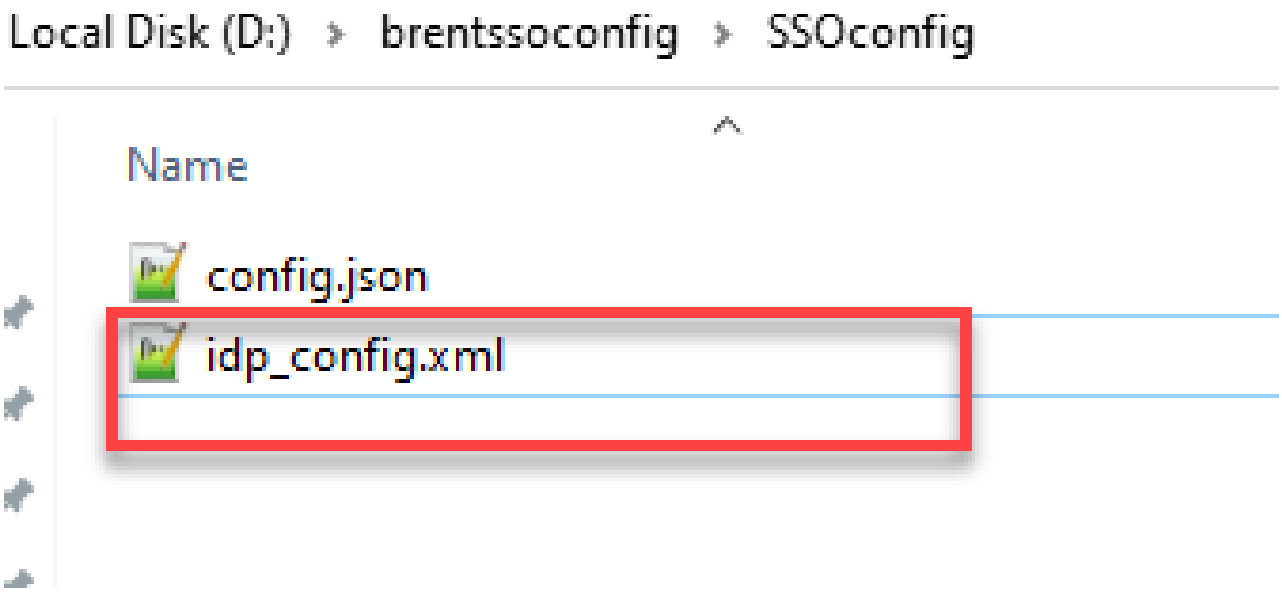
1. ADFSサーバ（またはADFSにアクセスできる場所）で、Webブラウザを開きます。

2. WebブラウザでURL https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xmlを入力します（ADFSサーバでローカルに作業している場合は、FQDNの代わりにlocalhostを使用することもできます）。 これにより、ファイルFederationMetadata.xmlがダウンロードされます。



3. zipファイルを作成する場所にダウンロードしたファイルをコピーし、idp_config.xmlに名前を変更します。

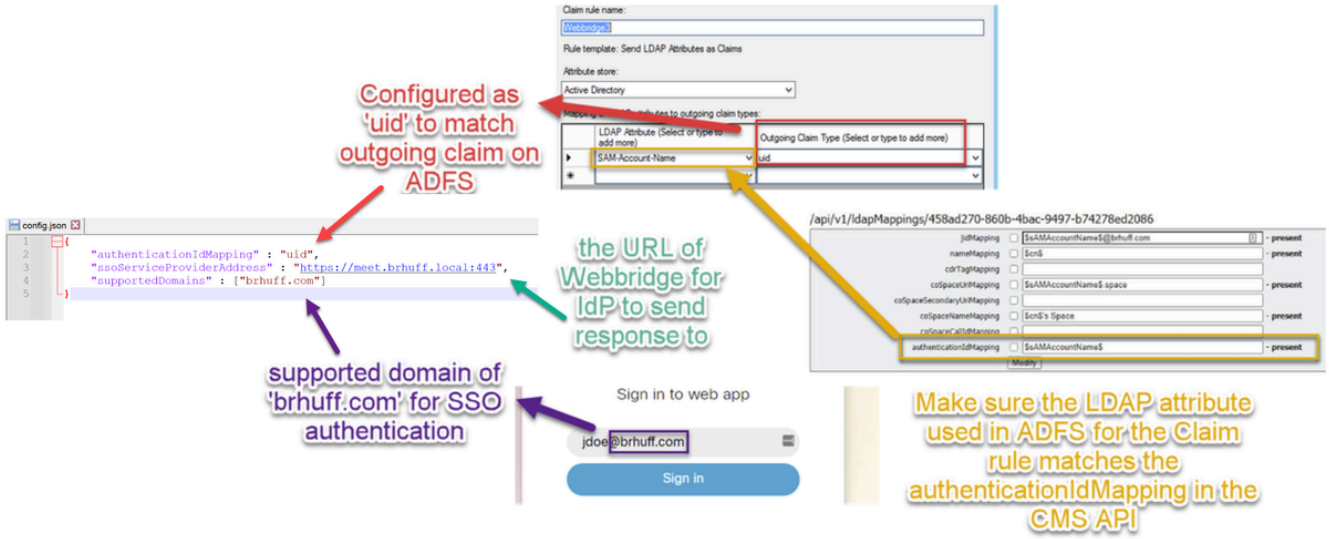

[redacted]
SSOconfig
Name
config.json
FederationMetadata.xml
Open
Edit
Share with Skype
Move to OneDrive
7-Zip
CRC SHA
Edit with Notepad++
Share
Open with
Cisco AMP For Endpoints
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties



コンテンツを含むconfig.jsonファイルの作成

config.jsonには次の3つの属性が含まれており、これらは角カッコ{ } : 内に含まれている必要があります。

1. supportedDomains:IdPに対してSSO認証がチェックされるドメインのリストです。複数のドメインはカンマで区切ることができます。
2. authenticationIdMapping : これは、ADFS/IdPから出力要求ルールの一部として返されるパラメータです。これは、IdPの出力要求タイプの名前の値と一致する必要があります。クレームルール :
3. ssoServiceProviderAddress : これは、IDプロバイダーがSAML応答を送信する先のFQDN URLです。これはWebbridgeのFQDNである必要があります。

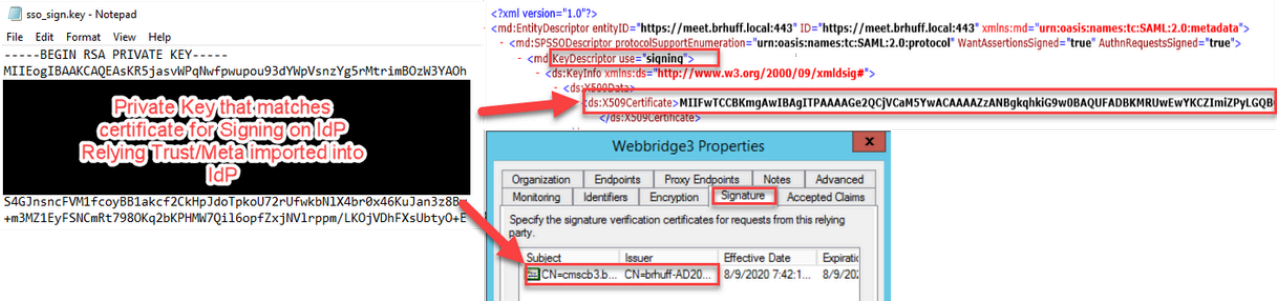


sso_sign.keyの設定（オプション）

このファイルには、IdPにインポートされたWebbridgeメタデータでの署名に使用される証明書の秘密キーが含まれている必要があります。署名に使用される証明書は、ADFSでのWebbridgeメタデータのインポート中に、<KeyDescriptor use=signing>セクションの下の証明書情報を使用してX509Certificateを設定することで設定できます。また、ADFSのWebbridge証明書利用者信頼パーティのProperties > Signatureで表示（およびインポート）することもできます。

次の例では、ADFSにインポートされる前にWebbridgeメタデータに追加されたcallbridge証明書(CN=cmscb3.brhuff.local)を確認できます。sso_sign.keyに挿入された秘密キーは、cmscb3.brhuff.local証明書と一致する秘密キーです。

これはオプションの設定であり、SAML応答を暗号化する場合にのみ必要です。

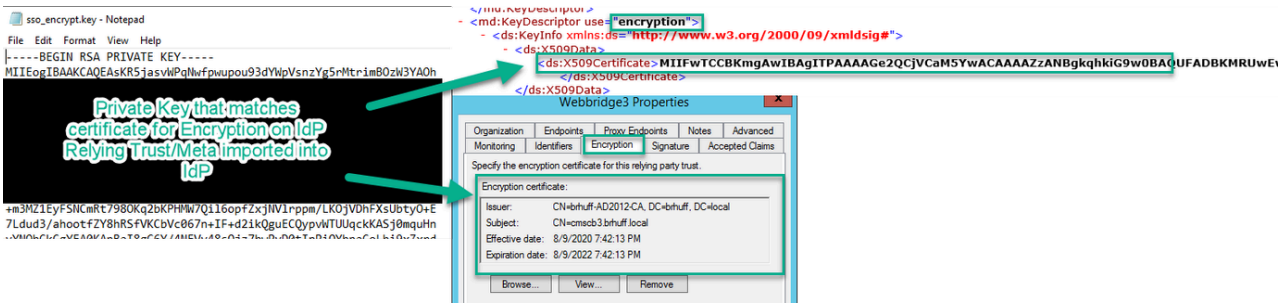


sso_encrypt.keyを設定します（オプション）。

このファイルには、IdPにインポートされたwebbridgeメタデータ内の暗号化に使用される証明書の秘密キーが含まれている必要があります。暗号化に使用される証明書は、ADFSでのWebbridgeメタデータのインポート中に、X509Certificateに<KeyDescriptor use=encryption>セクションの証明書情報を設定することで設定できます。また、ADFSのWebbridge証明書利用者信頼パーティのProperties > Encryptionで表示（およびインポート）することもできます。

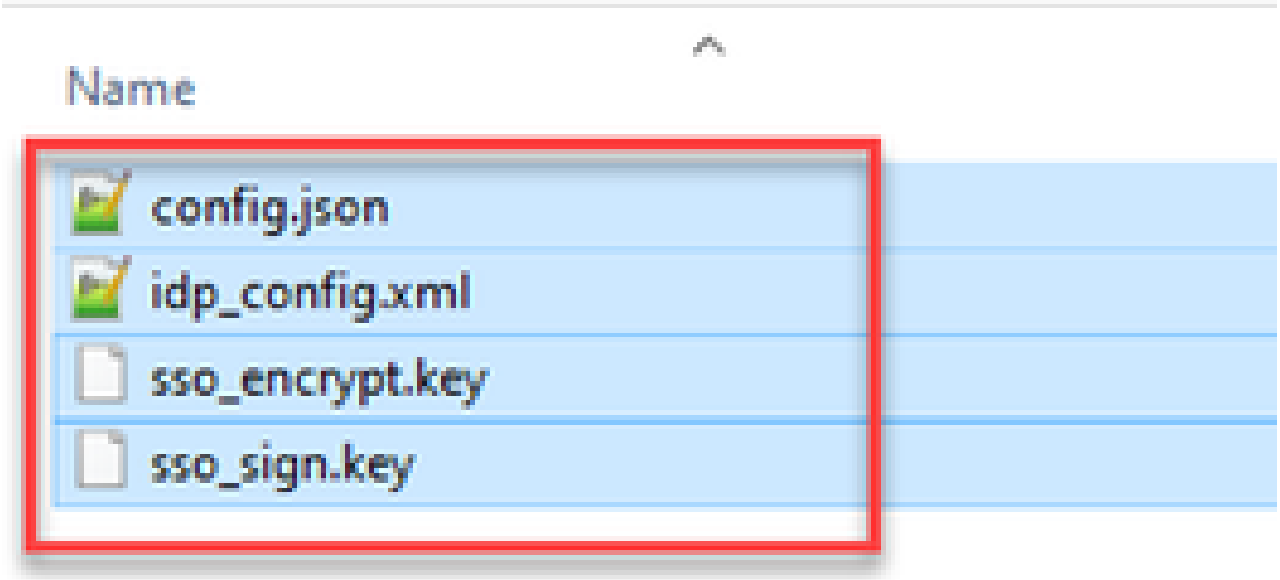
次の例では、ADFSにインポートされる前にWebbridgeメタデータに追加されたcallbridge証明書(CN=cmscb3.brhuff.local)を確認できます。「sso_encrypt.key」に挿入された秘密キーは、cmscb3.brhuff.local証明書と一致する秘密キーです。

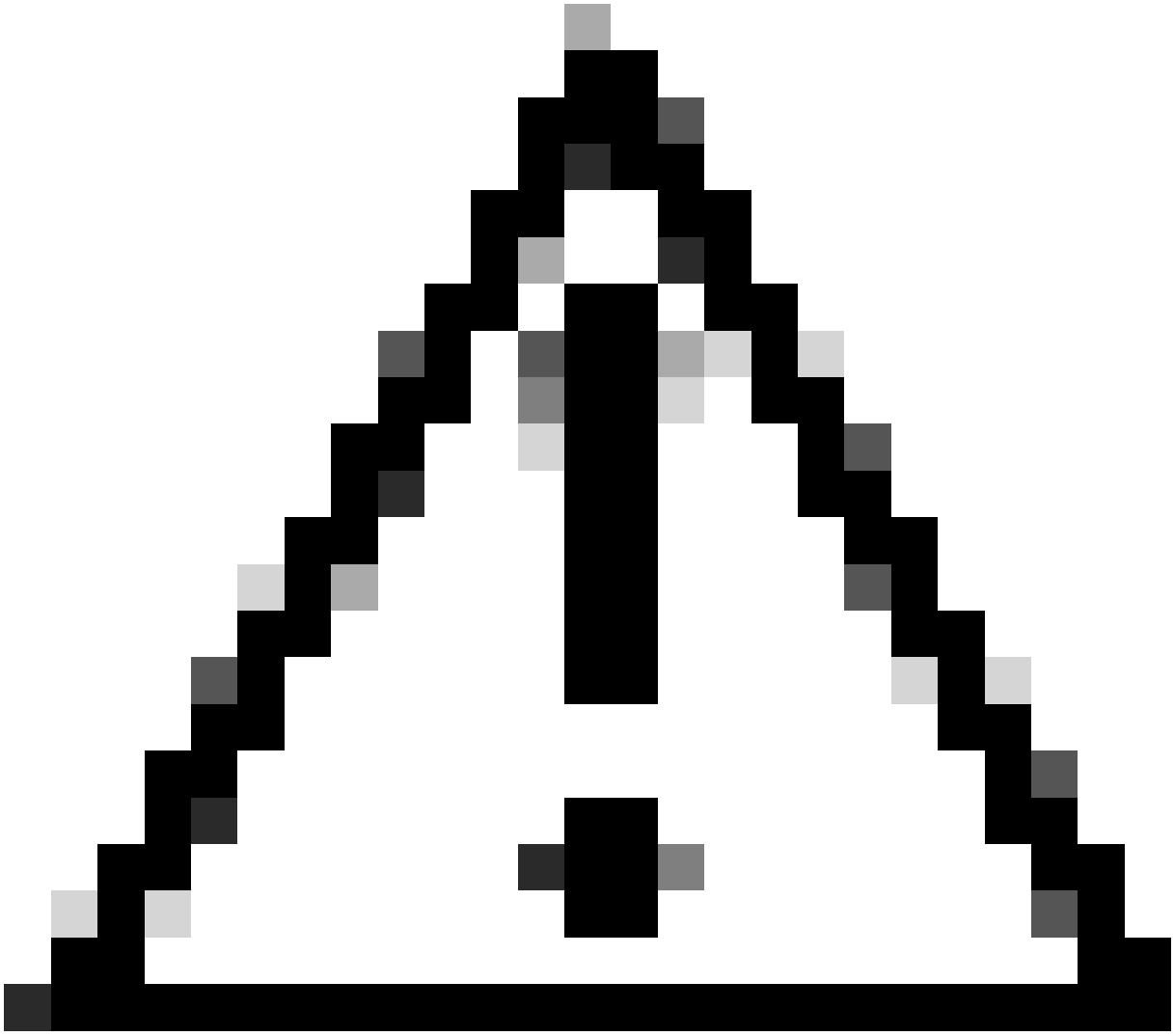
これはオプションの設定であり、SAML応答を暗号化する場合にのみ必要です。



SSO ZIPファイルの作成

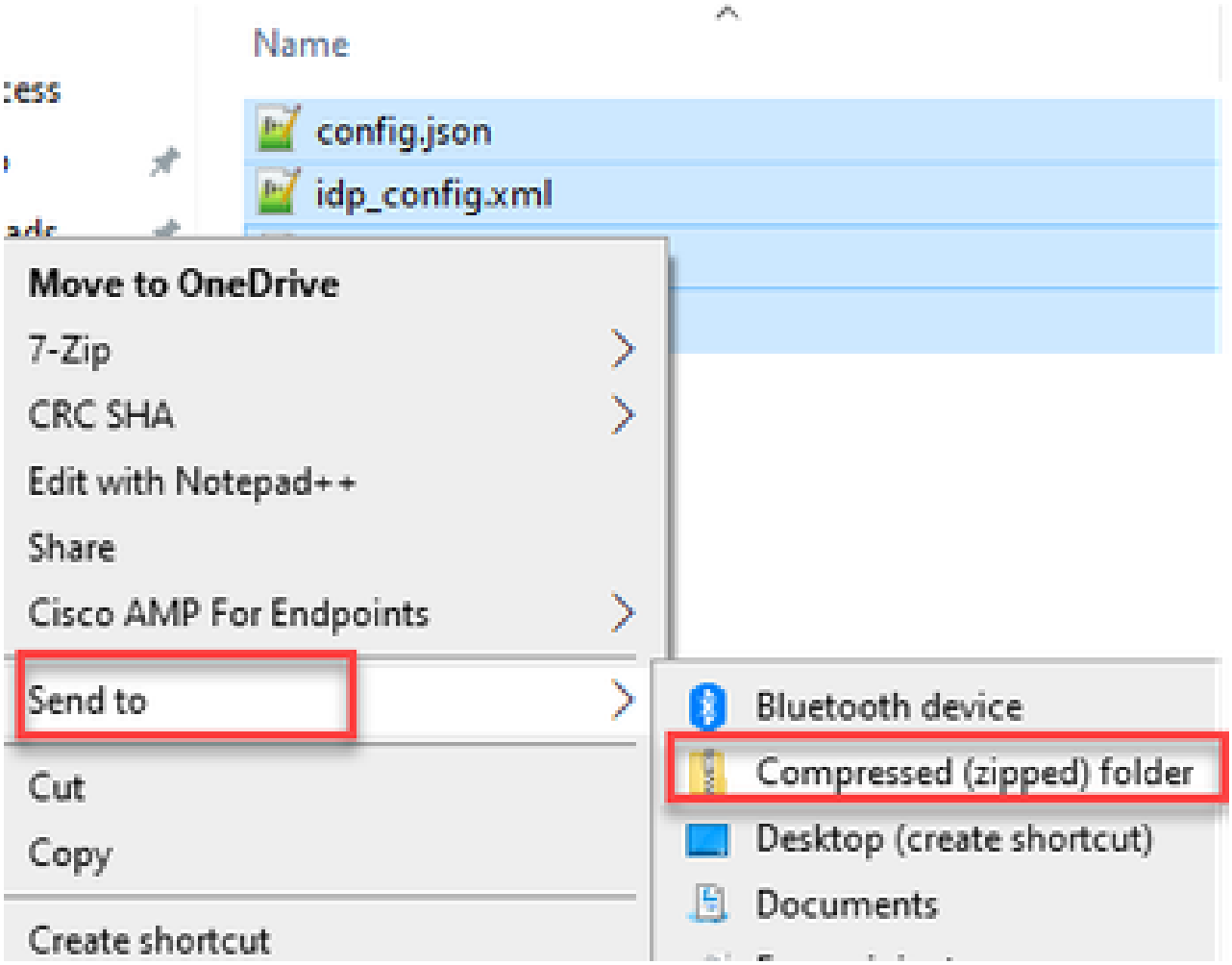
1. SSO構成ファイルに使用するすべてのファイルを強調表示します。



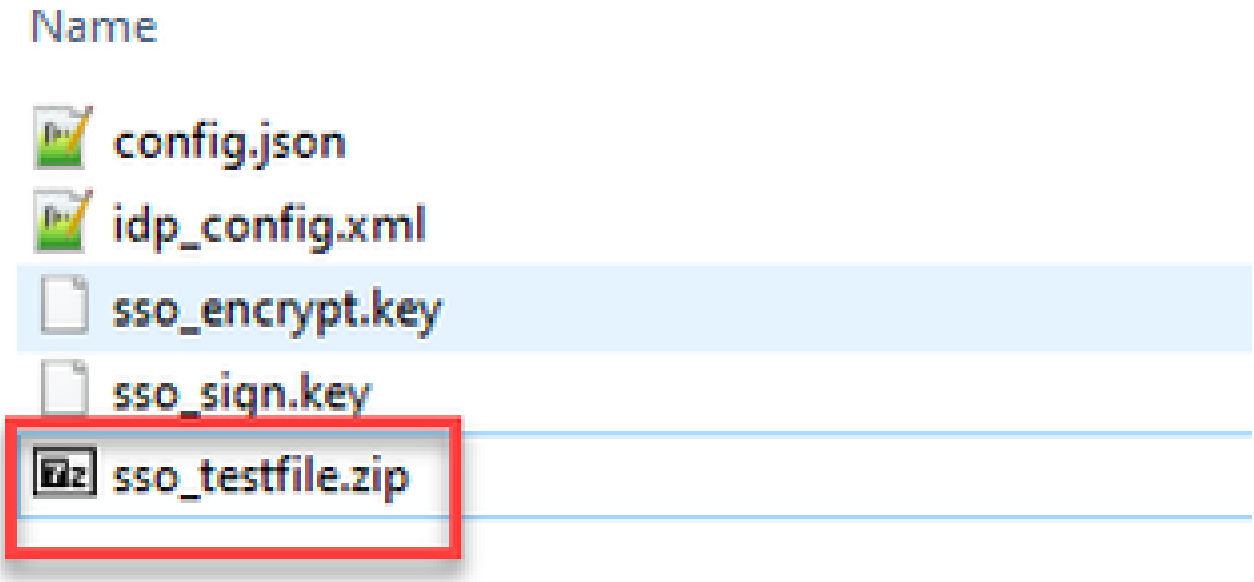


注意：ファイルが含まれているフォルダは圧縮しないでください。圧縮するとSSOが機能しなくなります。

2. ハイライトファイルを右クリックし、送信>圧縮（zip形式）フォルダを選択します。



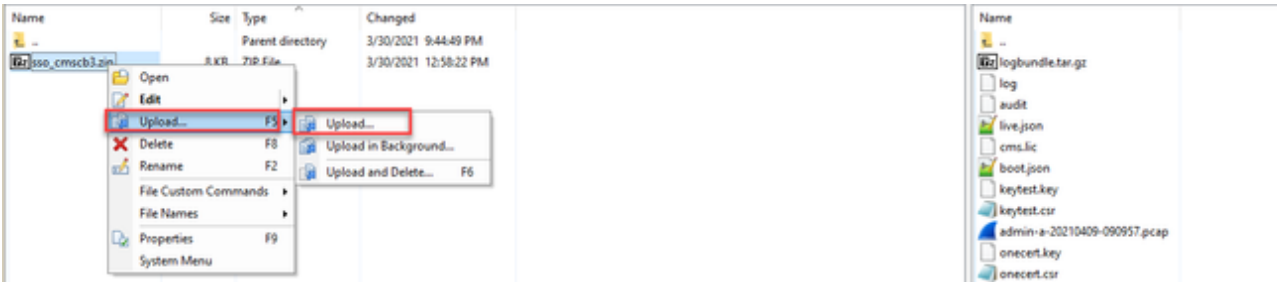
3. ファイルを圧縮したら、sso_プレフィクスを使用して目的の名前にファイルを変更します。



SSO ZipファイルをWebbridgeにアップロードします

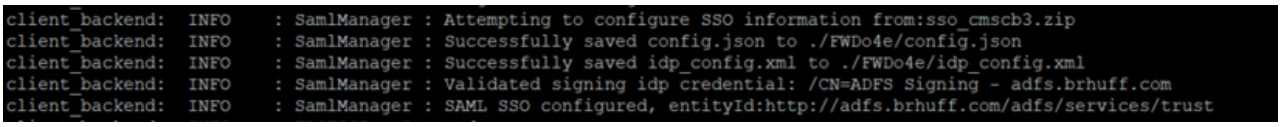
SFTP/SCPクライアントを開き（この例ではWinSCPが使用されています）、Webbridge3をホストするサーバに接続します。

1. 左側のペインで、SSO Zipファイルがある場所に移動し、右クリックしてアップロードを選択するか、ファイルをドラッグアンドドロップします。



2. ファイルが完全にWebbridge3サーバにアップロードされたら、SSHセッションを開いてコマンドwebbridge3 restartを実行します。

3. syslogでは、次のメッセージはSSOのイネーブルが成功したことを示します。



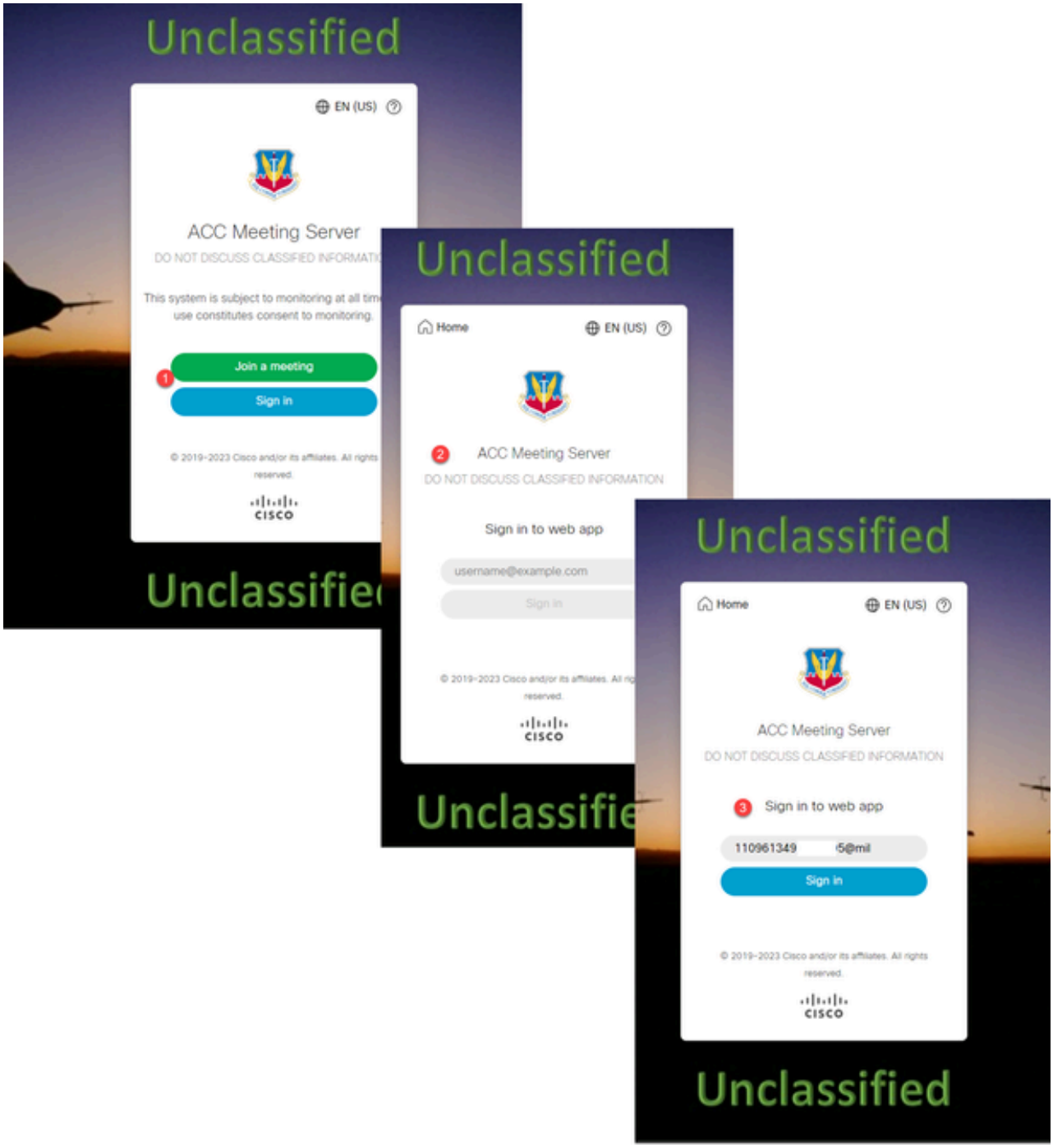
共通アクセスカード(CAC)

共通アクセスカード(CAC)は、現役の軍関係者、国防総省の民間従業員、および適格な契約作業員の標準的なIDとして機能するスマートカードです。

CACカードを使用するユーザのサインインプロセス全体を次に示します。

1. PCの電源を入れ、CACカードに貼り付けます
2. ログインし（証明書を選択する場合もあります）、PINを入力します。
3. ブラウザーを開く
4. 参加URLに移動し、会議に参加するオプションまたはサインインするオプションを確認します
5. サインイン： Active DirectoryがCACログインから要求しているjidMappingとして設定

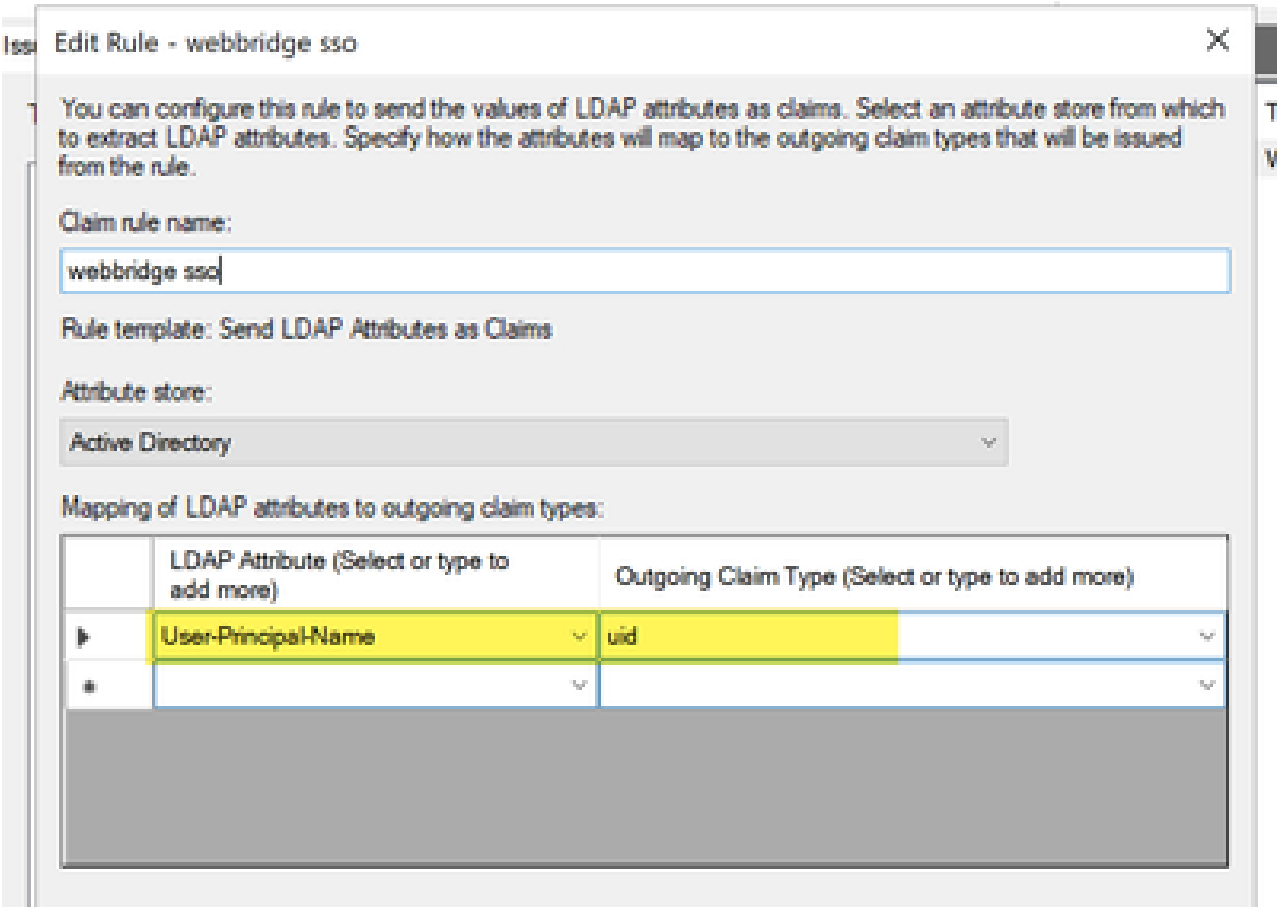
されているユーザ名を入力します
6. サインインを押す
7. ADFSページが短時間表示され、自動的に入力されます
8. ユーザはこの時点でログインしています。



ADFSがCACカードに使用するものと同じものとして、jidMapping（これはユーザのサインイン名です）をLdapmappingで設定します。 $userPrincipalName$など（大文字と小文字が区別されます）

また、ADFSのクレームルールで使用される属性と一致するように、authenticationIdMappingに同じLDAP属性を設定します。

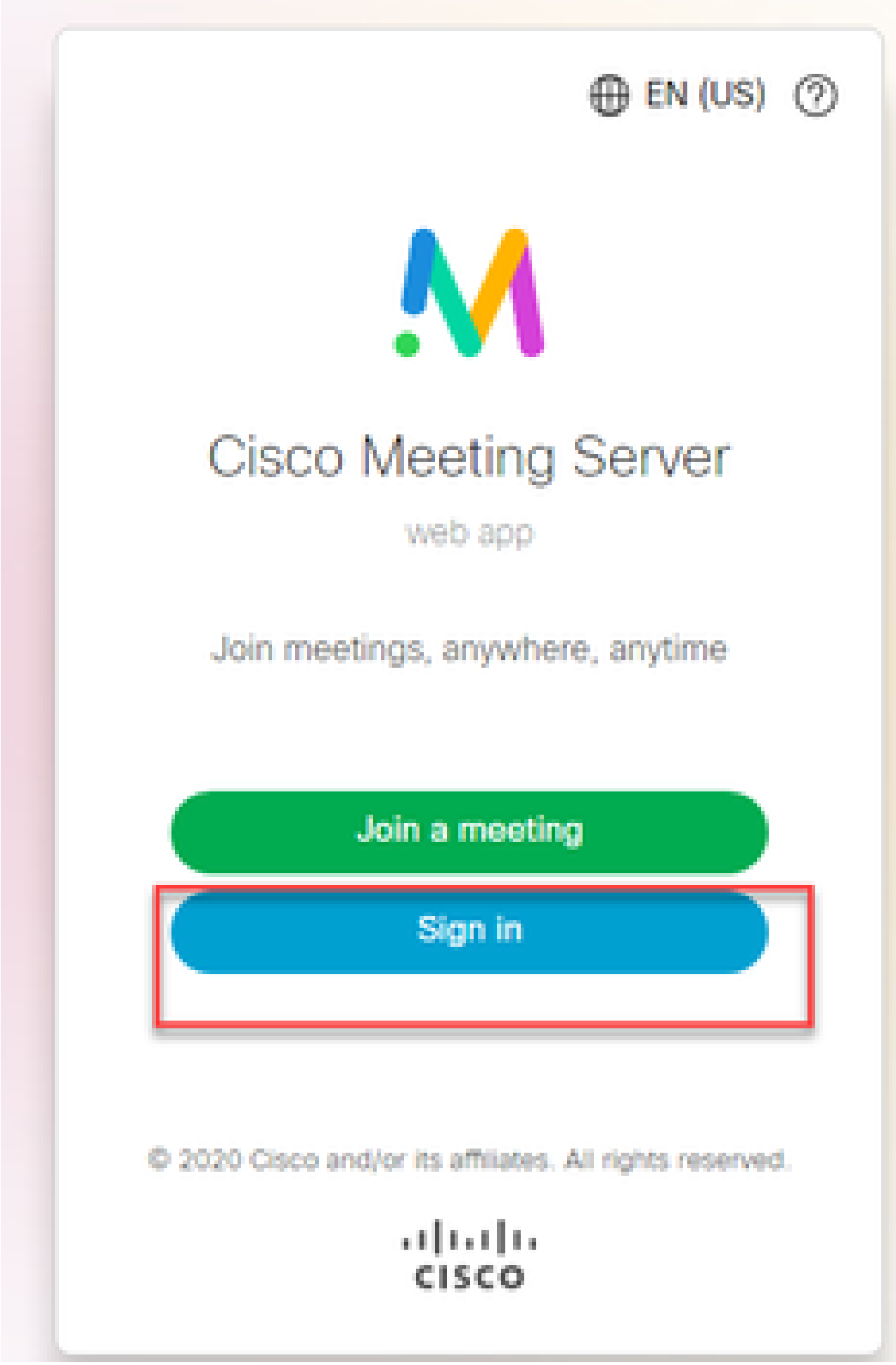
このクレームルールは、$userPrincipalName$をUIDとしてCMSに返信することを示しています。



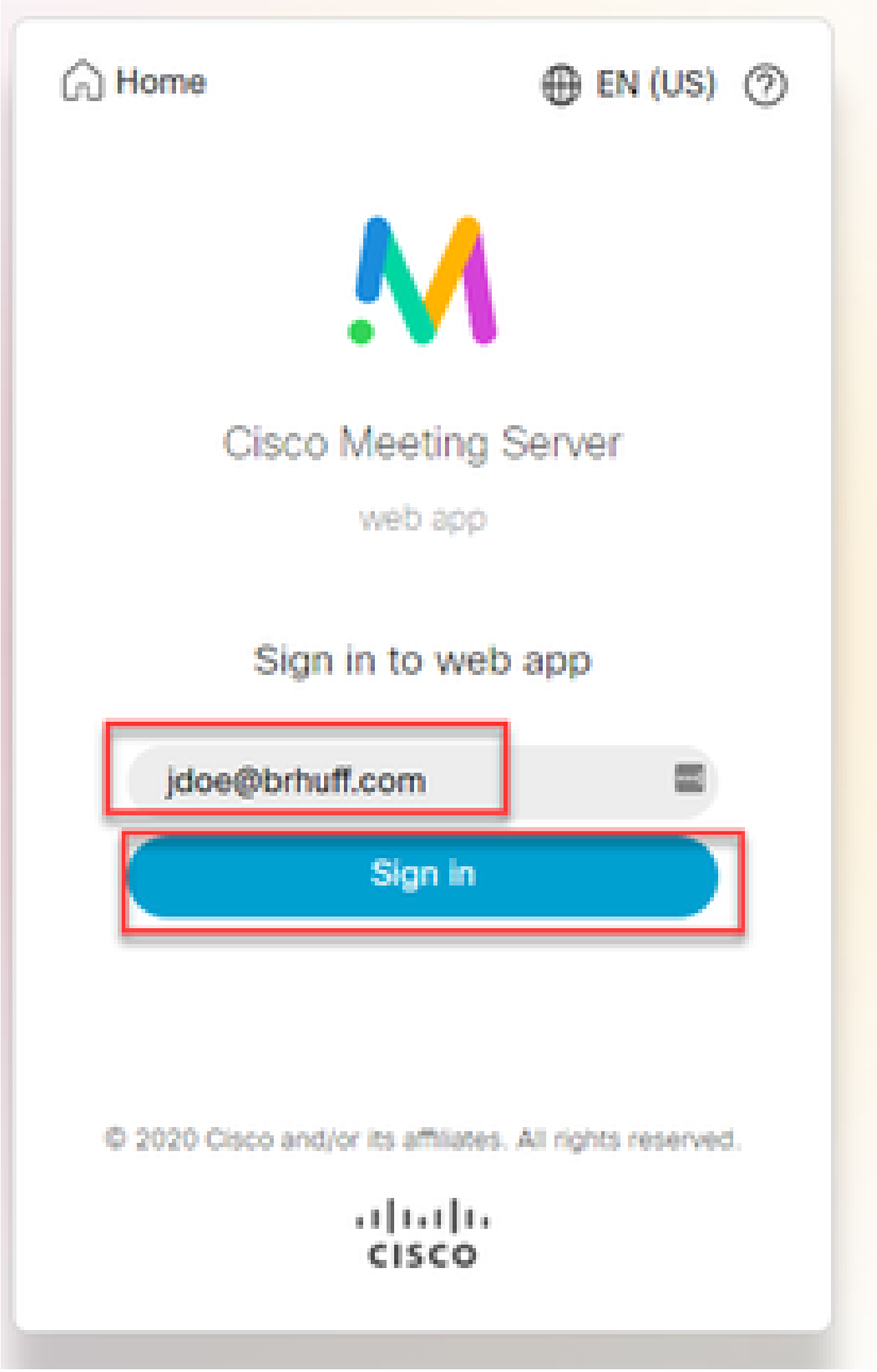
WebApp経由のSSOログインのテスト

SSOが設定されたので、次のようにサーバをテストできます。

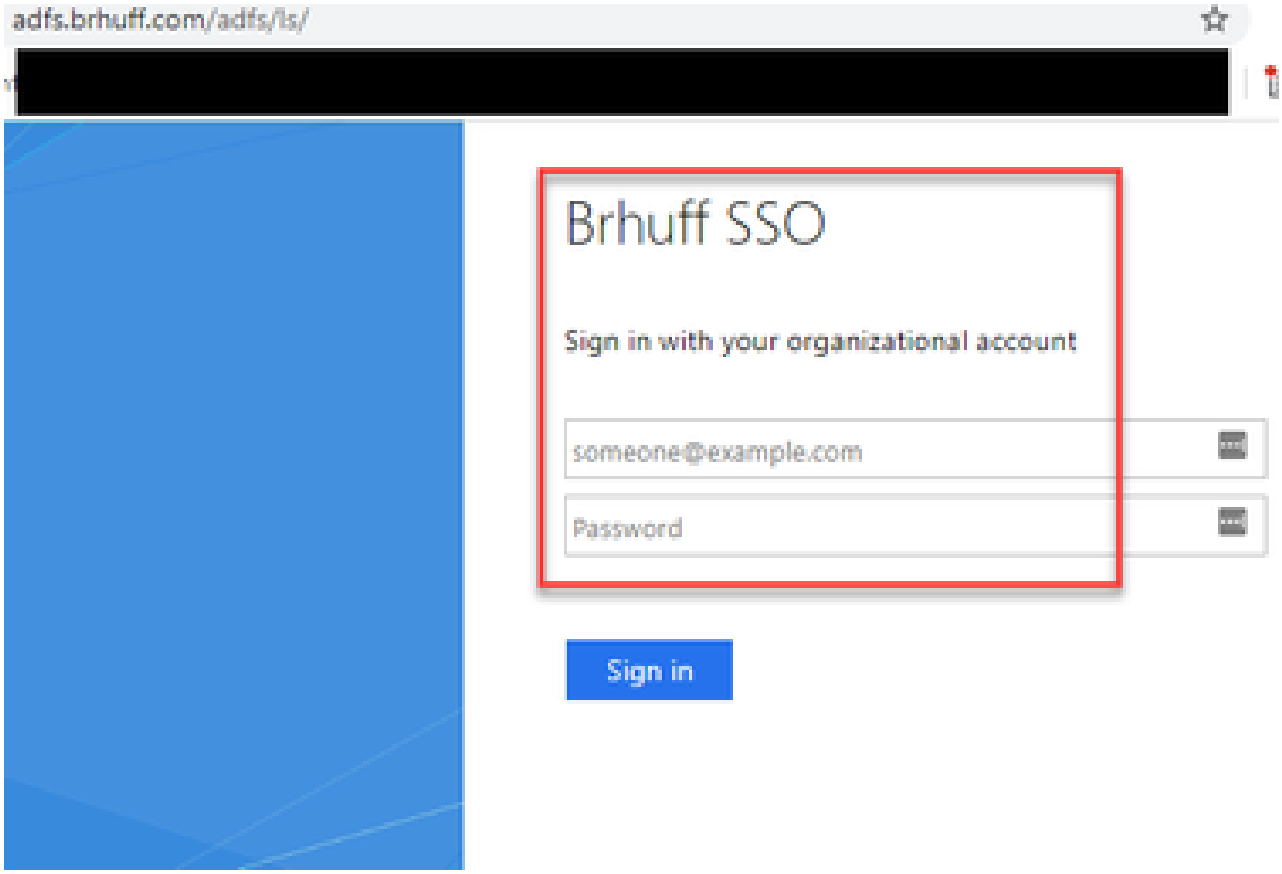
1. WebアプリケーションのWebbridge URLに移動し、Sign inボタンを選択します。


EN (US)
Cisco Meeting Server
web app
Join meetings, anywhere, anytime
Join a meeting
Sign in
© 2020 Cisco and/or its affiliates. All rights reserved.
cisco

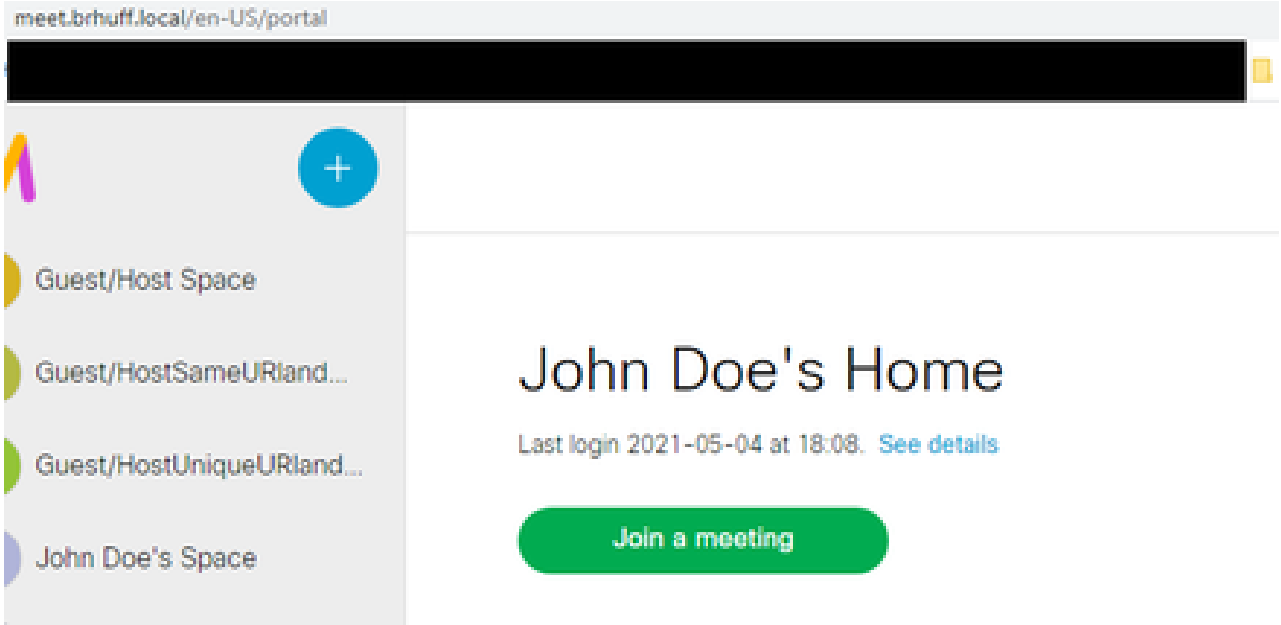
2. ユーザーには、ユーザー名を入力するオプションが表示されます（このページにはパスワード・オプションがないことに注意してください）。


Home
EN (US)
Cisco Meeting Server
web app
Sign in to web app
jdoe@brhuff.com
Sign in
© 2020 Cisco and/or its affiliates. All rights reserved.
CISCO

3. ユーザは、ADFSページにリダイレクトされます（ユーザ詳細の入力後）。このページで、ユーザはIdPに対して認証するためにクレデンシャルを入力する必要があります。



4. ユーザーは、IdPを使用して資格情報を入力および検証した後、Web Appホームページにアクセスするためのトークンでリダイレクトされます。



トラブルシューティング

基本的なトラブルシューティング

SSO問題の基本的なトラブルシューティングの場合：

1. IdPでの証明書信頼としてのインポートに使用されるWebbridge3用に構築されたメタデータが正しく設定されていること、および設定されたURLがconfig.json内のssoServiceProviderAddressと正確に一致することを確認します。
2. IdPから提供され、Webbridge3 ssoコンフィギュレーションファイルに圧縮されたメタデータが、IdPから取得した最新のメタデータであることを確認します。これは、サーバのホスト名や証明書などに変更があった場合と同様に、再エクスポートして、コンフィギュレーションファイルに圧縮する必要があります。
3. 署名と暗号化の秘密キーを使用してデータを暗号化する場合は、正しい一致キーがwebbridgeにアップロードしたsso_xxxx.zipファイルの一部であることを確認します。可能であれば、オプションの秘密キーを使用せずにテストを試み、この暗号化オプションを使用せずにSSOが機能するかどうかを確認してください。
4. SSOドメイン、Webbridge3 URL、およびSAMLResponseから一致する予想される認証マッピングの正しい詳細を使用してconfig.jsonが設定されていることを確認します。

また、ログの観点からトラブルシューティングを試みることも理想的です。

1. WebbridgeのURLに移動するときは、URLの最後に?trace=trueを付けて、CMS syslogでの詳細なロギングを有効にします。(例：https://join.example.com/en-US/home?trace=true)。
2. Webbridge3サーバでsyslog followを実行して、テスト中にライブキャプチャを行うか、URLにトレースオプションを追加してテストを実行し、Webbridge3およびCMSコールブリッジサーバからlogbundle.tar.gzを収集します。 webbridgeとcallbridgeが同じサーバにある場合、必要なのは単一のlogbundle.tar.gzファイルだけです。

Microsoft ADFS障害コード

場合によっては、SSOプロセスに障害が発生し、IdP設定またはIdPとの通信に障害が発生する可能性があります。ADFSを使用する場合は、次のリンクを確認して障害が発生していることを確認し、修復アクションを実行することが理想的です。

Microsoftステータスコード

次に例を示します。

> client_backend：エラー：SamlManager:SAML認証要求_e135ca12-4b87-4443-abe1-30d396590d58が次の理由で失敗しました： urn:oasis:names:tc:SAML:2.0:status:Responder

このエラーは、前のドキュメントによると、IdPまたはADFSが原因で障害が発生したため、解決するにはADFSの管理者による処理が必要であることを示しています。

認証IDを取得できませんでした

SAMLResponseをIdPから交換し直している間に、Webbridgeがログに次のエラーメッセージを表示し、SSO経由でのログインに失敗する場合があります。

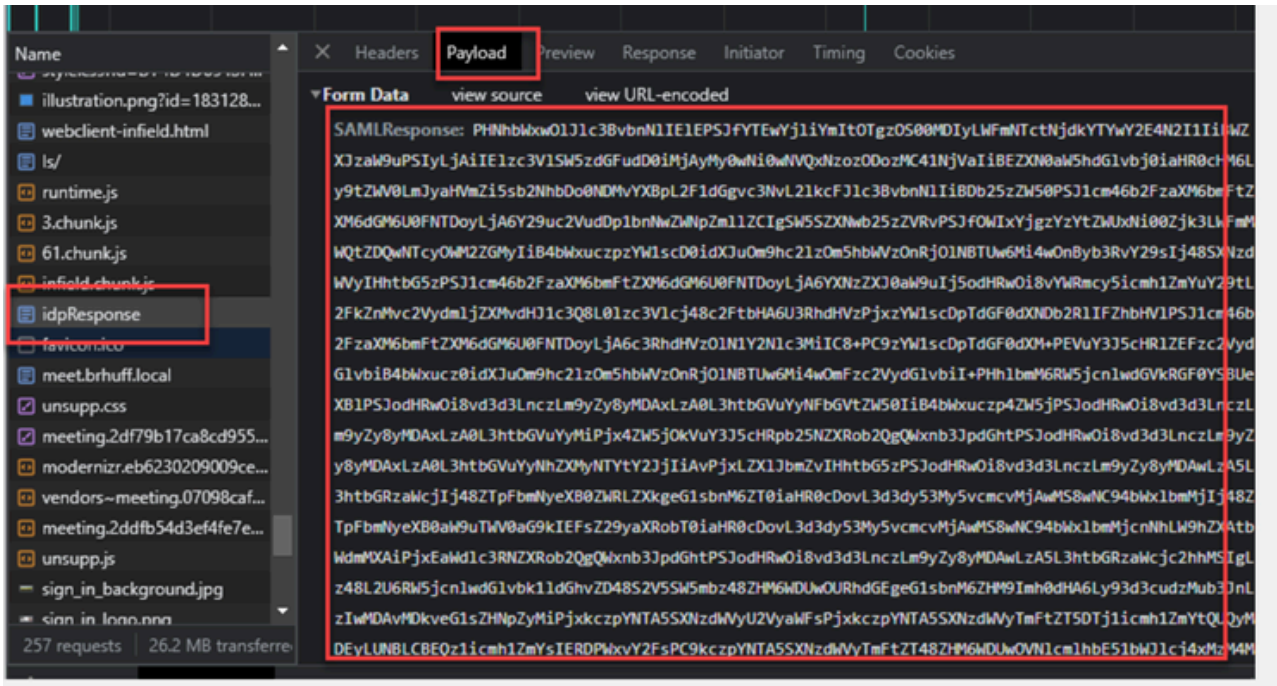
> client_backend:INFO:SamlManager:[57dff9e3-862e-4002-b4fa-683e4aa6922c] Failed obtaining an authenticationId

このことは、認証交換中にIdPから返されたSAMLResponseデータを確認する際に、Webbridge3では、authenticationIdに対するconfig.jsonと比較して、応答に有効な照合属性が見つからなかったことを示しています。

通信が署名と暗号化の秘密キーを使用して暗号化されていない場合、SAML応答はWebブラウザ経由でDeveloper Tools Network Loggingから抽出し、base64を使用してデコードできます。応答が暗号化されている場合は、IdP側から復号化されたSAML応答を要求できます。

ネットワークのログを記録する際は、「ログを保存」のチェックボックスを必ずオンにして、ページ変更時にログが上書きされないようにします。

開発者ツールのネットワークロギング出力（HARデータとも呼ばれる）で、name列の下のidpResponseを探してPayloadを選択し、SAML応答を確認します。 前述したように、これはbase64デコーダを使用してデコードできます。



SAMLResponseデータを受信する際は、<AttributeStatement>のセクションを確認して返信される属性名を探します。このセクション内には、設定された要求タイプとIdPから送信された要求タイプがあります。例：

<属性ステートメント>
<Attribute Name="<共通名のURL">
<AttributeValue>testuser1</AttributeValue>
</属性>
<Attribute Name="<NameIDのURL">
<AttributeValue>testuser1</AttributeValue>
</属性>
<Attribute Name="uid">
<AttributeValue>testuser1</AttributeValue>
</属性>
</AttributeStatement>

前の名前を確認して、Attribute Statementセクションの下の<AttributeName>を確認し、各値をSSO config.jsonのauthenticationIdmappingセクションで設定されている値と比較できます。

前の例では、authenticationIdMappingの設定が渡された内容と正確に一致せず、一致するauthenticationIdを見つけられなかったことを確認できます。

認証IDマッピング：http://example.com/claims/NameID

この問題を解決するには、次の2つの方法があります。

1. Webbridge3のconfig.jsonのauthenticationIdMappingで設定されている内容と正確に一致するクレームを持つように、IdP送信クレームルールを更新できます。
(http://example.com/claims/NameIDのIdPに追加されたクレームルール)
または

2. Webbridge3でconfig.jsonを更新して、「authenticationIdMapping」がIdPで設定された出力要求ルールの1つとして正確に一致するようにできます。(つまり、「authenticationIdMapping」を更新して、属性名（「uid」、「<URL>/NameID」、または「<URL>/CommonName」）のいずれかに一致するようにします。 渡されたときにCallbridge APIで設定される期待値と（正確に）一致する限り)

検証でアサーションが渡されませんでした/一致しませんでした

IdPからのSAMLResponseの交換中に、アサーションの照合に失敗したことを示す次のエラーがWebbridgeで表示され、サーバ設定に一致しないアサーションがスキップされることがあります。

client_backend：エラー： SamlManager：検証に合格したアサーションがありません
client_backend：情報：SamlManager：許可された対象ユーザーに含まれないアサーションをスキップしています

このエラーは、IdPからSAMLResponseを確認する際に、Webbridgeが一致するアサーションを見つけられず、一致しない障害をスキップし、最終的に失敗したSSOログインが発生したことを示します。

この問題を特定するには、IdPからSAMLResponseを確認することが理想的です。 通信が署名と暗号化の秘密キーを使用して暗号化されていない場合、SAML応答はWebブラウザを介してDeveloper Tools Network Loggingから抽出し、base64を使用してデコードできます。応答が暗号化されている場合は、IdP側から復号化されたSAML応答を要求できます。

SAMLResponseデータを調べる場合、応答の<AudienceRestriction>セクションを見ると、この応答が制限されているすべての対象ユーザーを確認できます。

<条件NotBefore=2021-03-30T19:35:37.071Z NotOnOrAfter=2021-03-30T19:36:37.071Z>
<対象者制限>
<Audience>https://cisco.example.com</Audience>
</AudienceRestriction>
</条件>

<Audience>セクション(https://cisco.example.com))の値を使用して、Webbridge設定のconfig.json内のssoServiceProviderAddressと比較し、完全に一致するかどうかを検証できます。この例では、視聴者のアドレスに「:443」が追加されているため、視聴者が設定内のサービスプロバイダーのアドレスと一致しないことが失敗の原因であることがわかります。

ssoServiceProviderAddress:https://cisco.example.com:443

このような障害が発生しないようにするには、これらの間で完全に一致する必要があります。この例では、次の2つの方法のいずれかが修正されています。

1. config.jsonのssoServiceProviderAddressセクションのアドレスから:443を削除して、IdPのSAMLResponseで提供されるAudienceフィールドに一致するようにできます。

または

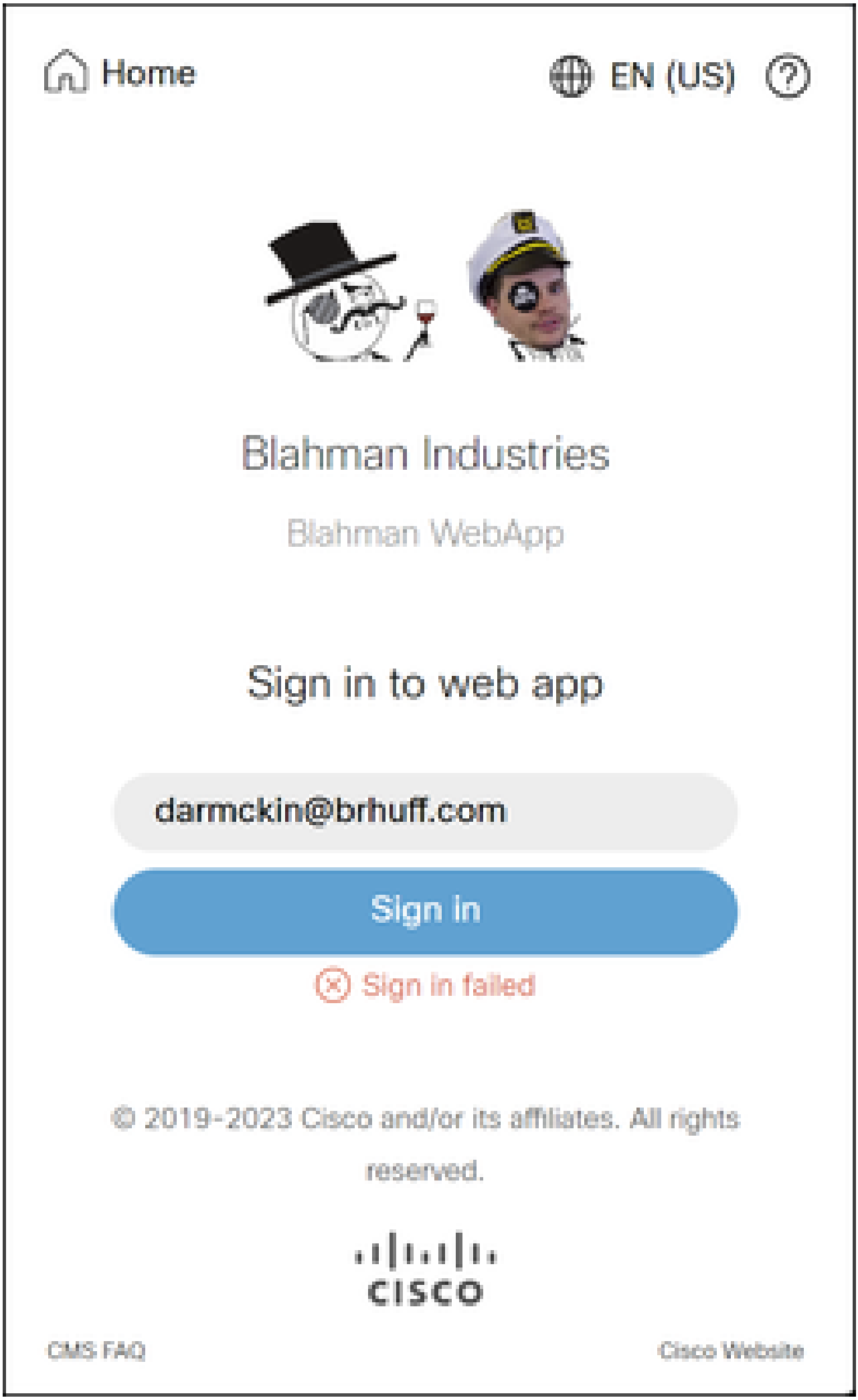
2. IdP内のWebbridge3のメタデータOR証明書利用者信頼は、URLに:443を追加するように更新できます(メタデータを更新する場合は、ADFS上の証明書利用者信頼として再度インポートする必要があります。ただし、IdPウィザードから直接証明書利用者信頼を変更した場合は、再インポートする必要はありません)。

また、条件NotBeforeおよびNotONOrAfter: <Conditions NotBefore=2021-03-30T19:35:37.071Z NotOnOrAfter=2021-03-30T19:36:37.071Z>に注意してください。

サーバの時刻が正しくない場合、その時刻は条件で定義された有効期間の範囲外になる可能性があります。CLIを使用してNTPサーバを確認します。その際、ntp server list コマンドを使用して設定されているNTPサーバを確認し、ntp status コマンドを使用して設定されているNTPサーバの状態を確認します。date コマンドを使用してサーバの時刻を確認します。

ヒント：ローカル/内部NTPサーバを使用している場合は、time.google.comなどのパブリックNTPサーバを設定してみてください（前にパブリックDNSサーバを設定したことを確認してください）。

Webアプリでサインインできませんでした：


Home
EN (US)
Blahman Industries
Blahman WebApp
Sign in to web app
darmckin@brhuff.com
Sign In
Sign in failed
© 2019-2023 Cisco and/or its affiliates. All rights reserved.
CISCO
CMS FAQ
Cisco Website

user.info cmscb3-1 client_backend:INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] SAMLトークン要求のSSO_2024.zipと一致

3月19日10:47:07.927 user.info cmscb3-1 client_backend:INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Attempting to find SSO in SAML Token Request

3月19日10:47:07.930 user.info cmscb3-1 client_backend:INFO : SamlManager :[63cdc9ed-ab52-455c-8bb2-9e925cb9e16b]正常に生成されたSAMLトークン

シナリオ 2：

ユーザがwebbridgeサインインページのSSO zipファイルにないドメインを使用してサインインしようとしました。 クライアントは、ユーザが入力したユーザ名のペイロードを含むtokenRequestを送信します。 Webbridgeはログイン試行をただちに停止します。

CMS Webbridgeトレース（?trace=trueが使用されている場合）

3月18日14:54:52.698 user.err cmscb3-1 client_backend:ERROR : SamlManager : Invalid SSO login attempt

Mar 18 14:54:52.698 user.info cmscb3-1 client_backend: INFO : SamlManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] SAMLトークン要求でSSOを見つけられませんでした

3月18日14:54:52.698 user.info cmscb3-1 client_backend:INFO : SamlManager :[3f93fd14-f4c9-4e5e-94d5-49bf6433319e] SAMLトークン要求でSSOを検出しようとしています

シナリオ 3：

ユーザが正しいユーザ名を入力し、SSOサインインページが表示されます。 ユーザはここに正しいユーザ名とパスワードも入力しますが、「Sign in Failed」が表示されます

CMS Webbridgeトレース（?trace=trueが使用されている場合）

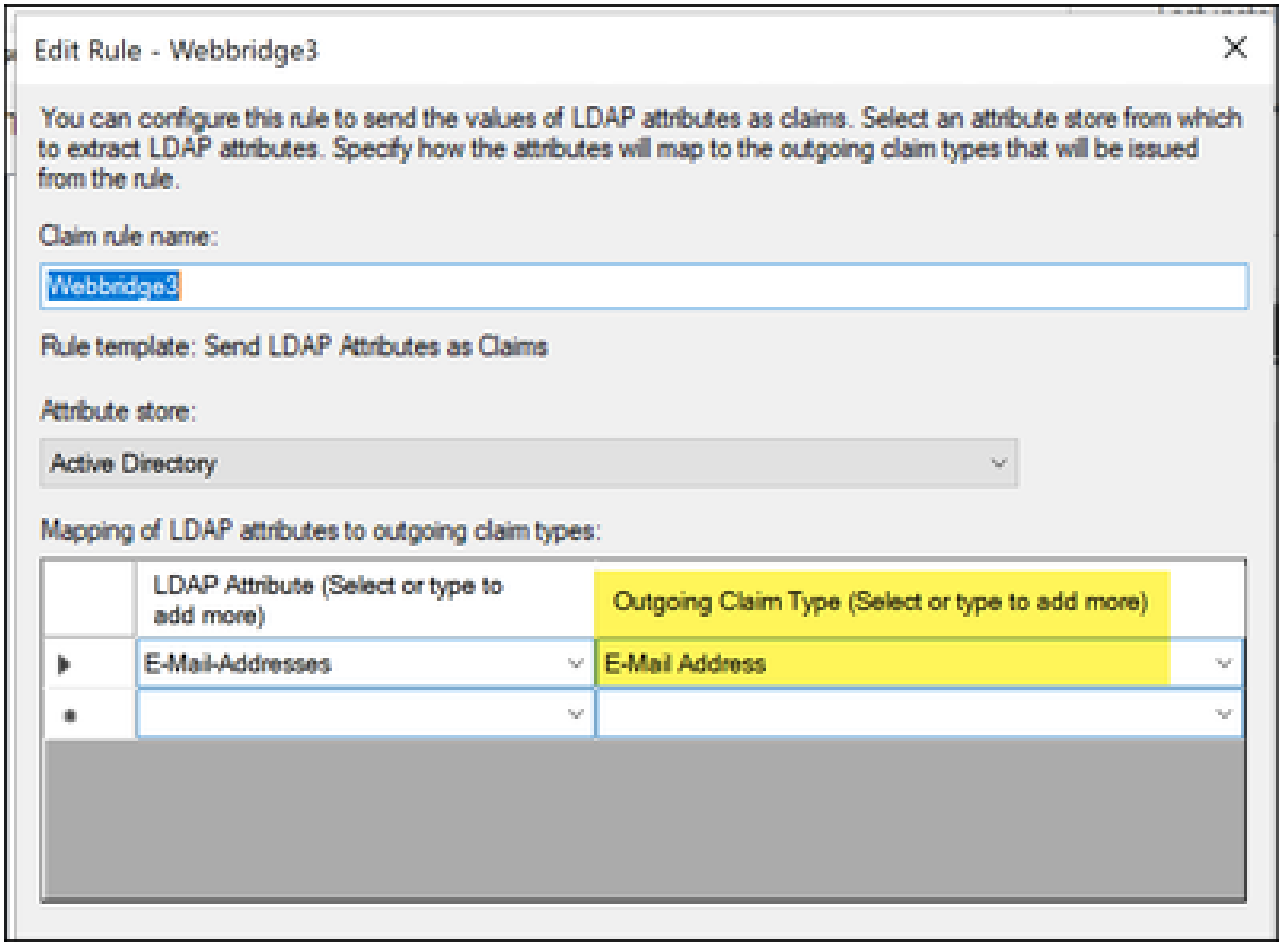
3月19日16:39:17.714 user.info cmscb3-1 client_backend:INFO : SamlManager :[ef8fe67f-685c-4a81-9240-f76239379806] SAMLトークン要求のSSO_2024.zipと一致

3月19日16:39:17.714 user.info cmscb3-1 client_backend：情報： SamlManager :[ef8fe67f-685c-4a81-9240-f76239379806] Attempting to find SSO in SAML IDP Response

3月19日16:39:17.720 user.err cmscb3-1 client_backend：エラー：SamlManager：署名付きSAMLアサーションにauthenticationIdのマッピングされた要素が見つかりません

Mar 19 16:39:17.720 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Failed obtaining an authenticationID

シナリオ3の原因は、IdPのクレームルールで使用されているクレームタイプが、webbridgeにアップロードされたSSO zipファイルで使用されるconfig.jsonファイルのauthenticationIdMappingと一致していなかったことです。 WebbridgeはSAML応答を調べ、属性名がconfig.jsonで設定されている名前と一致することを予期しています。



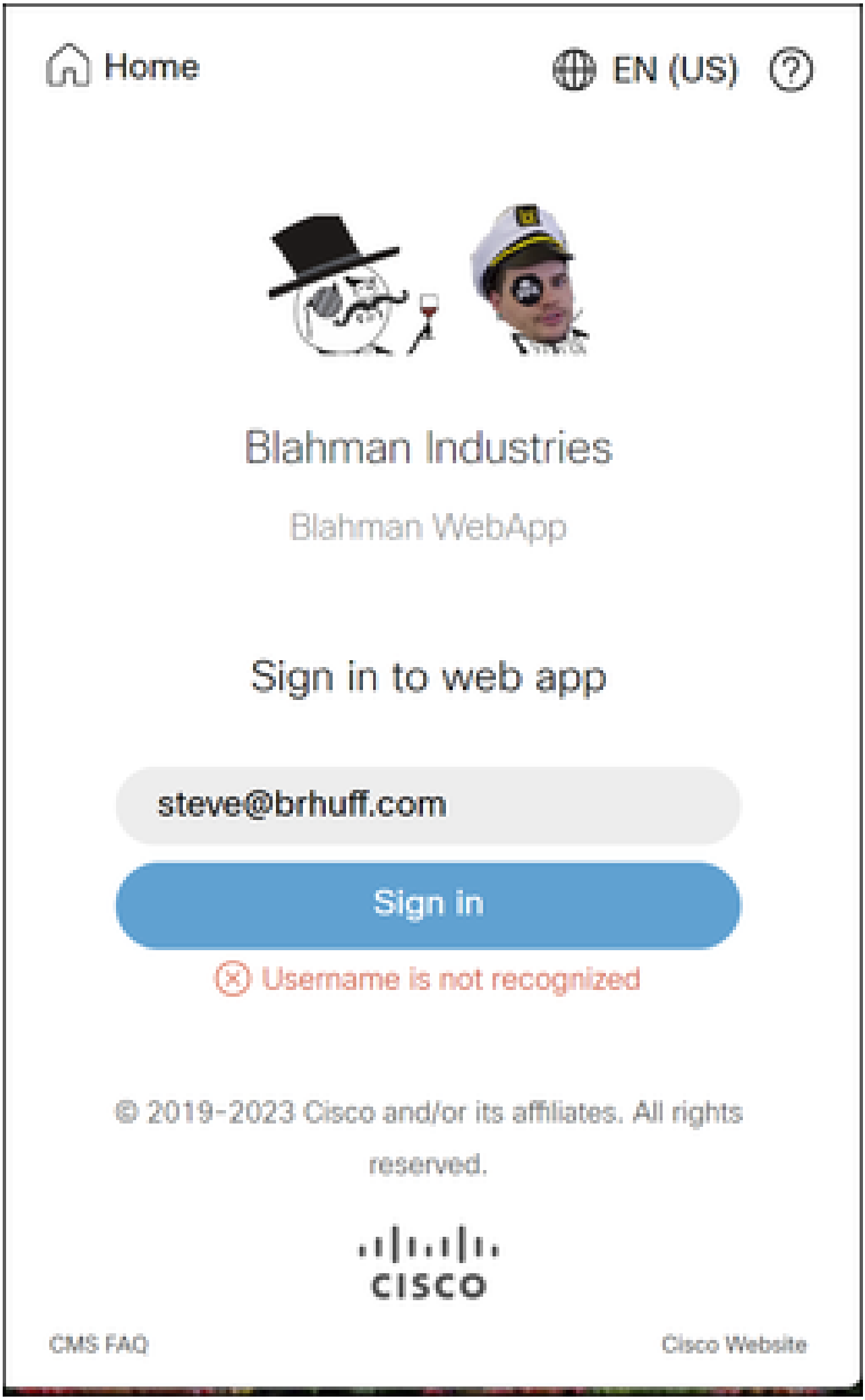
ADFSのクレームルール

config.jsonの例

ユーザ名が認識されない

シナリオ１：

ユーザが誤ったユーザ名でサインインした（ドメインが、webbridge3にアップロードされたSSO zipファイルの内容と一致するが、ユーザが存在しない）



ユーザ名が認識されない

user.info cmscb3-1 client_backend:INFO : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] SAMLトークン要求のSSO_2024.zipと一致

3月18日14:58:47.777 user.info cmscb3-1 client_backend:INFO : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] Attempting to find SSO in SAML Token Request

3月18日14:58:47.780 user.info cmscb3-1 client_backend:INFO : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6]正常に生成されたSAMLトークン

3月18日14:58:48.072 user.info cmscb3-1 client_backend:INFO : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] SAMLトークン要求のSSO_2024.zipと一致

3月18日14:58:48.072 user.info cmscb3-1 client_backend:INFO : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] Attempting to find SSO in SAML IDP Response

Mar 18 14:58:48.077 user.info cmscb3-1 client_backend: INFO : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] Successfully obtain authenticationID:darmckin@brhuff.com

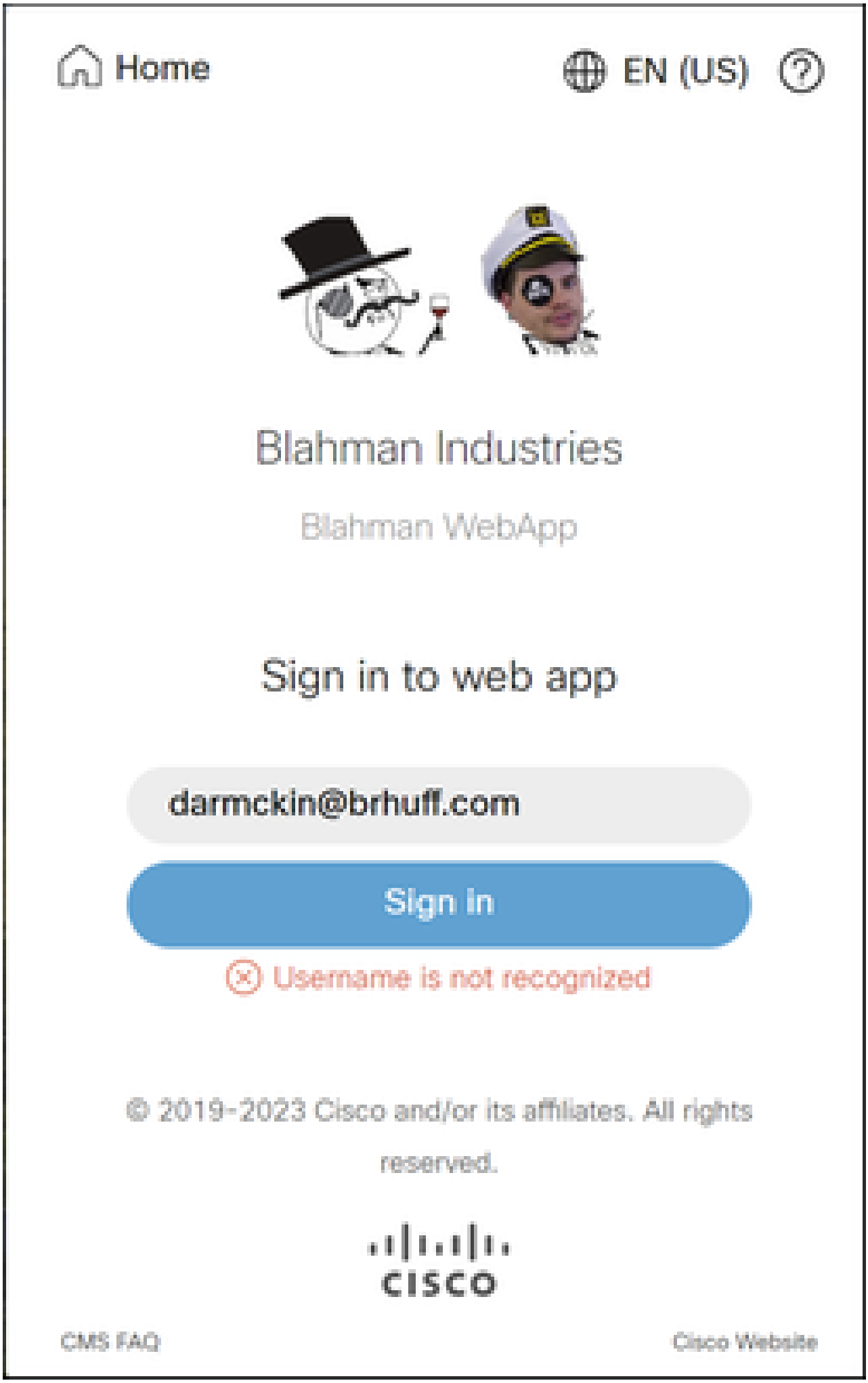
Mar 18 14:58:48.078 user.info cmscb3-1 host:server:INFO : WB3Cmgr: [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c-024 2a1-b125-136fdf5612a5(user=steve@brhuff.com)

3月18日14:58:48.092 user.info cmscb3-1 host:server:INFO : no user found for authorization

3月18日14:58:48.092 user.info cmscb3-1 host:server:INFO: unsuccessful login request from steve@brhuff.com

シナリオ 2：

ユーザがWebアプリに正しいサインイン情報を入力し、SSOページでLDAP認証のための正しいクレデンシャルも入力しましたが、ログインに失敗し、「ユーザ名が認識されません」と表示されます。



ユーザ名が認識されない

user.info cmscb3-1 client_backend:INFO : SamlManager :[d626bbaf-80c3-4286-8284-fac6f71eb140] SAMLトークン要求のSSO_2024.zipと一致

3月18日15:08:52.114 user.info cmscb3-1 client_backend:INFO : SamlManager :[d626bbaf-80c3-4286-8284-fac6f71eb140] Attempting to find SSO in SAML Token Request

3月18日15:08:52.117 user.info cmscb3-1 client_backend:INFO : SamlManager :[d626bbaf-80c3-4286-8284-fac6f71eb140]正常に生成されたSAMLトークン

3月18日15:08:52.386 user.info cmscb3-1 client_backend:INFO : SamlManager :[d626bbaf-80c3-4286-8284-fac6f71eb140] SAMLトークン要求のSSO_2024.zipと一致

3月18日15:08:52.386 user.info cmscb3-1 client_backend:INFO : SamlManager :[d626bbaf-80c3-4286-8284-fac6f71eb140] Attempting to find SSO in SAML IDP Response

3月18日15:08:52.391 user.info cmscb3-1 client_backend:INFO : SamlManager :[d626bbaf-80c3-4286-8284-fac6f71eb140]認証ID:darmckin@brhuff.comを正常に取得しました

Mar 18 15:08:52.391 user.info cmscb3-1 host:server:INFO : WB3Cmgr: [d626bbaf-80c3-4286-8284-fac6f71eb140] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c 272-42a1-b125-136fdf5612a5 (user=darmckin@brhuff.com)

Mar 18 15:08:52.399 user.warning cmscb3-1 host:server: WARNING : rejecting login attempt from user 'darmckin@brhuff.com' — authenticationId incorrect

3月18日15:08:52.412 user.info cmscb3-1 host:server:INFO: unsuccessful login request from darmckin@brhuff.com

CMS ldapmappingのAuthenticationIdMappingが、ADFSのクレームルールに使用されている設定済みのLDAP属性と一致しません。「Successfully obtain authenticationID:darmckin@brhuff.com」という行は、ADFSにはActive Directoryから darmckin@brhuff.comを取得する属性で設定されたクレームルールがあることを示していますが、CMS API > UsersのAuthenticationIDはがdarmckinであることを示示しています。 CMS ldapMappingsでは、AuthenticationIDは$sAMAccountName$として設定されていますが、ADFSのクレームルールは電子メールアドレスを送信するように設定されているため、これは一致しません。

修正方法：

次の点を軽減するには、いずれかの方法を実行します。

1. CMS ldapmappingのAuthenticationIDをADFSのクレームルールで使用されている値に一致するように変更し、新しい同期を実行します
2. ADFS要求ルールで使用されるLDAP属性を、CMS ldapmappingで設定されたものと一致するように変更します

Related objects: /api/v1/ldapMappings

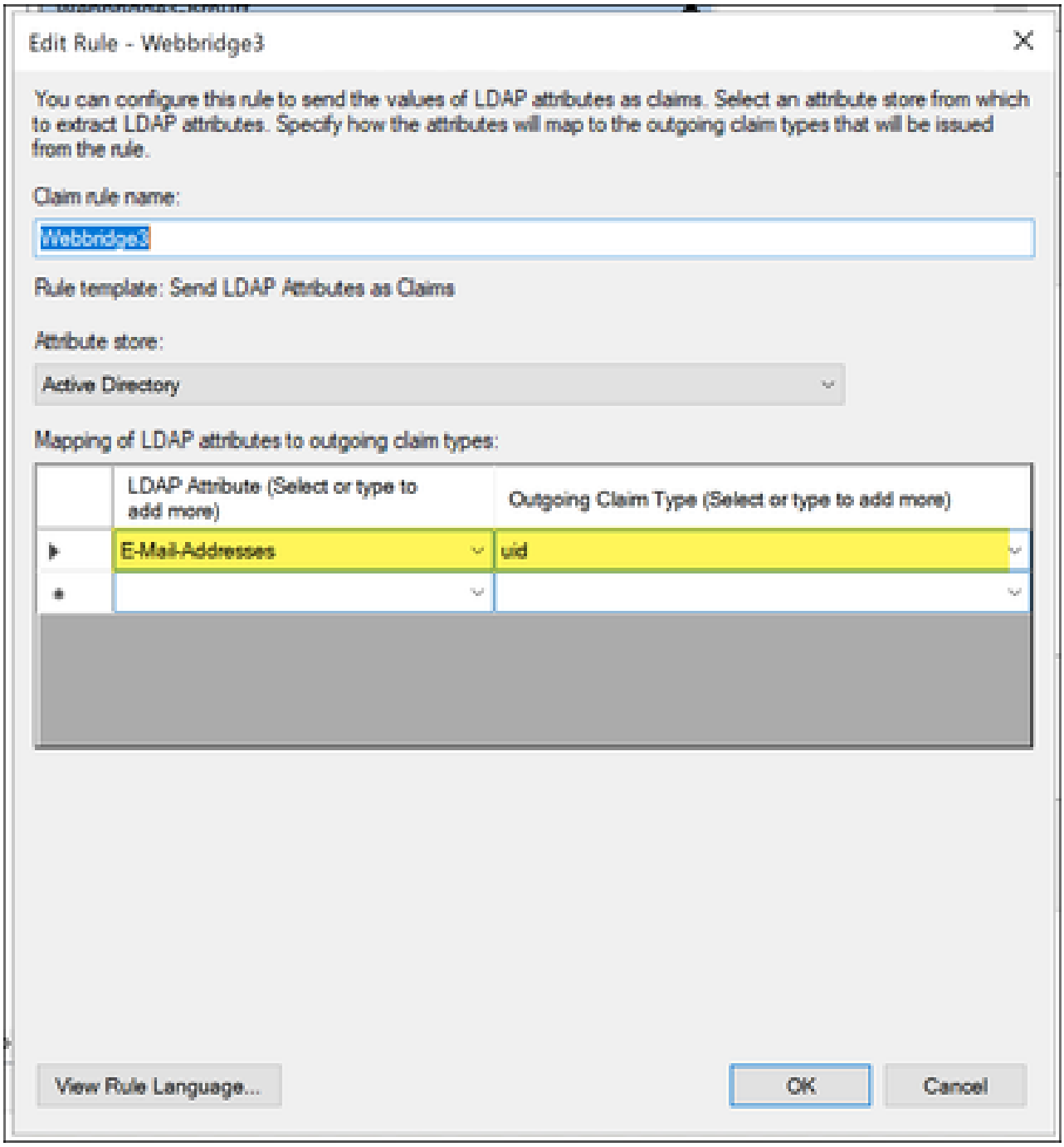
Table view | XML view

Object configuration	
jidMapping	$sAMAccountName$@brhuff.com
nameMapping	cn
cdrTagMapping	
coSpaceNameMapping	cn's Space
coSpaceUriMapping	$sAMAccountName$.space
coSpaceSecondaryUriMapping	$extensionAttribute12$
coSpaceCallIdMapping	
authenticationIdMapping	$sAMAccountName$

API LDAPマッピング

Object configuration	
userJid	darmckin@brhuff.com
name	Darren McKinnon
email	darmckin@brhuff.com
authenticationId	darmckin
userProfile	d5cd50e4-e423-4ba6-bd17-7492b9ba5eb3

APIユーザの例



ADFSからのクレームルール

Webbridgeのログで作業ログの例を示します。 結合URLで？trace=trueを使用して生成された例：

3月18日14:24:01.096 user.info cmscb3-1 client_backend:INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] SAMLトークン要求のSSO_2024.zipと一致

3月18日14:24:01.096 user.info cmscb3-1 client_backend:INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] Attempting to find SSO in SAML IDP Response

3月18日14:24:01.101 user.info cmscb3-1 client_backend:INFO : SamlManager :[7979f13c-d490-4f8b-899c-0c82853369ba]正常に認証を取得しました

ID:darmckin@brhuff.com

3月18日14:24:01.102 user.info cmscb3-1 host:server:INFO : WB3Cmgr: [7979f13c-d490-4f8b-899c-0c82853369ba] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c-4 2a1-b125-136fdf5612a5(user=darmckin@brhuff.com)

3月18日14:24:01.130 user.info cmscb3-1 host:server:INFO : successful login request from darmckin@brhuff.com

3月18日14:24:01.130 user.info cmscb3-1ホスト：サーバ：情報：WB3Cmgr:[7979f13c-d490-4f8b-899c-0c82853369ba] issuing JWT ID e2a860ef-f4ef-4391-b5d5-abdfa89ba0f

3月18日14:24:01.132 user.info cmscb3-1ホスト：サーバ：情報：WB3Cmgr:[7979f13c-d490-4f8b-899c-0c82853369ba] sending auth response (jwt length=1064, connection=64004556-faea-479f-aabe-691e17783aa5)

3月18日14:24:01.133 local7.info cmscb3-1 56496041063b wb3_frontend: [Auth:darmckin@brhuff.com, Tracing:7979f13c-d490-4f8b-899c-0c82853369ba] 10.10.10.8 - [2024年3月18日：18:24:01 +000] status "POST /api/auth/sso/idpResponse HTTP/1.1" bytes_sent 0 http_referer "https://adfs.brhuff.com/" http_user_agent "Mozilla/5.0 (Windows NT 10.0; win64; x64) AppleWebKit/537.36（GeckoのようなKHTML）Chrome/122.0.0。Safari/537.36" to upstream 192.0.2.2:9000: upstream_response_time 0.038 request_time 0.039ミリ秒1710786241.133 upstream_response_length 24 200

よく寄せられる質問（FAQ）

このセクションでは、Cisco Meeting Server上のWebApp SSOに関するFAQやトピックを取り上げます。

Webapp SSO JWTは拡張できますか。

JSON Web Token(JWT)は、正常に認証された（IdPに対して正常に認証された）Webappクライアントに Callbridgeによって提供されるトークンで、WebAppサービスへのアクセスを許可します。JWT内の有効期限タイマー値は、JWTが有効である期間を示します。JWTの有効期限に達すると、WebAppユーザはページのWebbridgeログインにリダイレクトされ、アクセスを取り戻すために再認証が必要になります。

JWTの期限切れは、WebAppクライアントに提供されるJWTの有効期限を設定したい時間数を数値で表した「callbridge wc3jwt expiry <1-24>」(3.8以降で追加 – 詳細は『CMS 3.8リリースノート』または『CMS MMPガイド』を参照)を利用して設定できます。ただし、このコマンドで確認できるように、最大値は24時間に設定できます。これは、JWTを有効なまま維持できる最長時間と、WebAppユーザがログインできる最長時間が24時間であることを意味します。JWTの有効期限に達すると、ブラウザは有効期限が切れたトークンをダンプし、WebAppユーザはWebApp口グインページに強制的に戻されます。

一部の環境では、IdPと環境の設定に応じて、永続的SSO/Keep me signed in機能をIdPに実装できます。これにより、ブラウザを閉じてもCookieが保持されるIdPから永続的なcookedがブラウザに提供されます（他の方法でクリアされない限り）。 SSO/IdPの設定に関係なく、JWTが期限切れになると（最大24時間）、WebAppユーザはWebAppログインページに強制的に戻されます。ただし、IdPでPersistent SSOが有効になっているこのシナリオでは、ユーザはWebAppログインページに<user@domain>を入力するだけで、IdPへの再認証は不要です。

WebAppに対する拡張認証を可能にするための更新トークンメカニズムの実装に関する機能拡張(Cisco Bug ID CSCwm28758)が公開されています。

ブラウザを閉じた場合、WebAppへの再認証が必要ですか。

このシナリオのフローは次のとおりです。

1. ユーザはWebAppにログインします（SSO認証方式を使用）。
2. ユーザは、いずれかの時点でブラウザを閉じます。
3. ユーザがブラウザを再度開き、WebAppサイトに移動します。（すぐに、または後で）。

このシナリオでは何が起こりますか。

この答えはそれにかかっています！Callbridgeが提供するJWTがWebAppページへのアクセス時に期限切れになるかどうかは完全に依存します。JWTが有効でストレージに存在している限り、ブラウザを閉じてもWebAppページに移動できます。 JWTの有効期間は最大24時間であることに注意してください。

- JWTがまだVALID (NOT EXPIRED) and Presentの場合、ユーザはスペースを使用してWebAppページに移動できます。その際、再認証は必要ありません。
- JWTがINVALID(EXPIRED)の場合、ユーザはWebAppのログインページにリダイレクトされ、WebAppに再ログインする必要があります。ユーザは、IdP認証方式に応じて、IdPに対する再認証を必要とする場合もあります（たとえば、IdPがセッションSSOまたはパーシステントSSOを使用している場合）。

WebApp SSOでは複数ドメインをどのようにサポートしていますか。

WebApp SSOは、複数のドメインを持つ環境だけでなく、これらの異なるドメインが異なるアイデンティティプロバイダー(IdP)を指す環境もサポートできます。 Cisco Meeting Server導入ガイドを参照するか、Cisco TACに連絡して、複数ドメインの使用に関するサポートを受けてください。

関連情報

- シスコのテクニカルサポートとダウンロード

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。