

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を取得および設定します](#)

[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](#)

[WebbridgeへのSSO Zipファイルのアップロード](#)

[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ない/一致しない](#)

[Webアプリでサインインに失敗しました：](#)

[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ログに示された作業ログの例。結合URLで?trace=trueを使用して生成された例：](#)

[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アプリ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(IdP)の識別

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

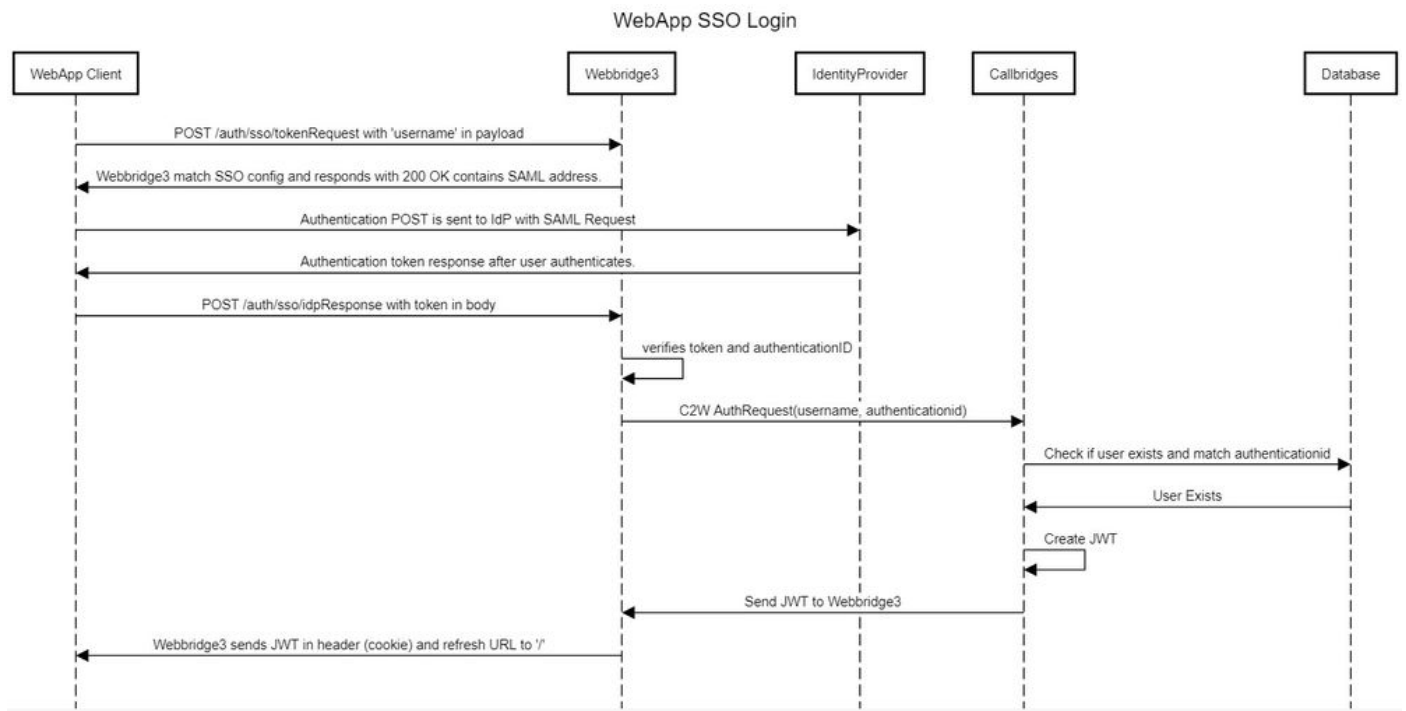
CMS 3.1以降では、IDプロバイダーで1つのセッションが作成されるため、ユーザがログインするたびにパスワードを入力しなくてもSSOを使用してサインインできる機能が導入されました。この機能は、SSOメカニズムとしてSecurity Assertion Markup Language(SAML)バージョン2.0を使用しています。

 注：CMSはSAML 2.0でのみHTTP-POSTバインディングをサポートし、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



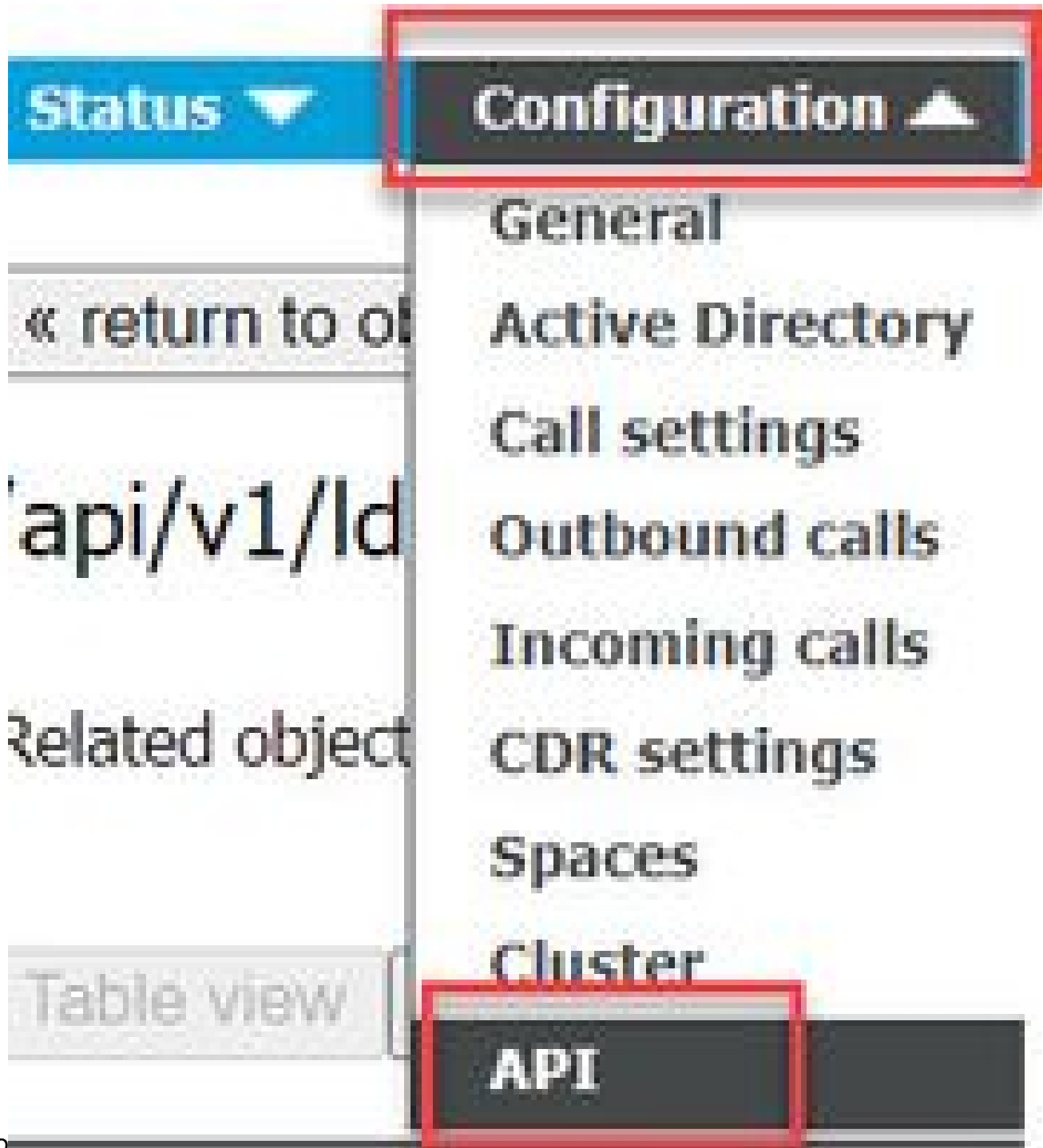
ADFSのインストールと初期セットアップ

この展開シナリオでは、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（または意図した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関連フィールドに対して、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IdapMapping内のauthenticationIdMappingです。

1. CMS Web管理GUIでConfiguration > APIに移動します。



Co

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

API objects

This page shows a list of the objects supported by the API. Where you see a ► control, you can expand that section to either see details of one specific section of configuration.

Filter (2 of 129 nodes)

[/api/v1/ldapMappings](#) ◀


◀ start < prev 1 - 2 (of 2) next >

object id	iidMapping
458ad270-860b-4bac-9497-b74278ed2086	\$sAMAccountName\$@brhuff.com

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

[/api/v1/ldapMappings/458ad270-860b-4bac-9497-b74278ed2086](#)

jidMapping	<input type="checkbox"/>	<input type="text" value="\$sAMAccountName\$@brhuff.com"/>	- present
nameMapping	<input type="checkbox"/>	<input type="text" value="\$cn\$"/>	- present
cdrTagMapping	<input type="checkbox"/>	<input type="text"/>	
coSpaceUriMapping	<input type="checkbox"/>	<input type="text" value="\$sAMAccountName\$ space"/>	- present
coSpaceSecondaryUriMapping	<input type="checkbox"/>	<input type="text"/>	
coSpaceNameMapping	<input type="checkbox"/>	<input type="text" value="\$cn\$'s Space"/>	- present
coSpaceCallIdMapping	<input type="checkbox"/>	<input type="text"/>	
authenticationIdMapping	<input type="checkbox"/>	<input type="text" value="\$sAMAccountName\$"/>	- present

 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ldapMappingに関連付けられたldapSourceでLDAP同期を実行します。

例：

[/api/v1/ldapSyncs](#)

tenant	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Choose"/>
ldapSource	<input checked="" type="checkbox"/>	<input type="text" value="0b8de8cd-ccce-4ccb-89a8-08ba69e98ec7"/>	<input type="button" value="Choose"/>
removeWhenFinished	<input type="checkbox"/>	<unset>	

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。

Object configuration	
userId	jdoue@brhuff.com
name	John Doe
email	john.doe@brhuff.com
authenticationId	jdoue
userProfile	dbcdb50e4-e423-4ba6-bd17-7492b9ba5eb3

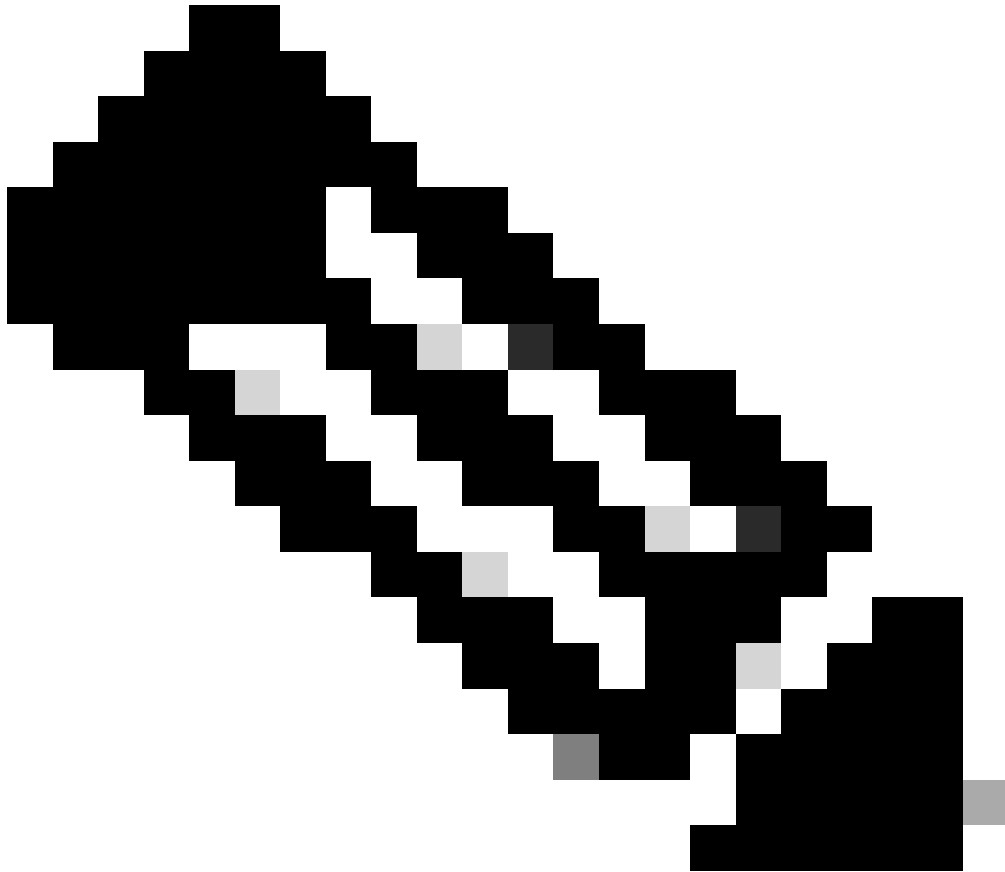
IdP用のWebbridgeメタデータXMLの作成

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、使用しているサービスプロバイダーを特定できます。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：単一の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が存在する場所です。これは、サインイン後に認証されたユーザー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、IdPが公開キー（証明書）を使用して署名を検証できるように、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。展開内の既存の証明書を使用できます。証明書をテキストファイルで開き、その内容をWebbridgeメタデータファイルにコピーします。sso_xxxx.zipファイルで使用されている証明書と一致するキーを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がIdPによって返信されたものを復号化できるように、WebbridgeにアップロードされたSSOバンドルの秘密キー「sso_encrypt.key」と一致する必要があります。展開内の既存の証明書を使用できます。証明書をテキストファイルで開き、その内容をWebbridgeメタデータファイルにコピーします。sso_xxxx.zipファイルで使用されている証明書と一致するキーを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：

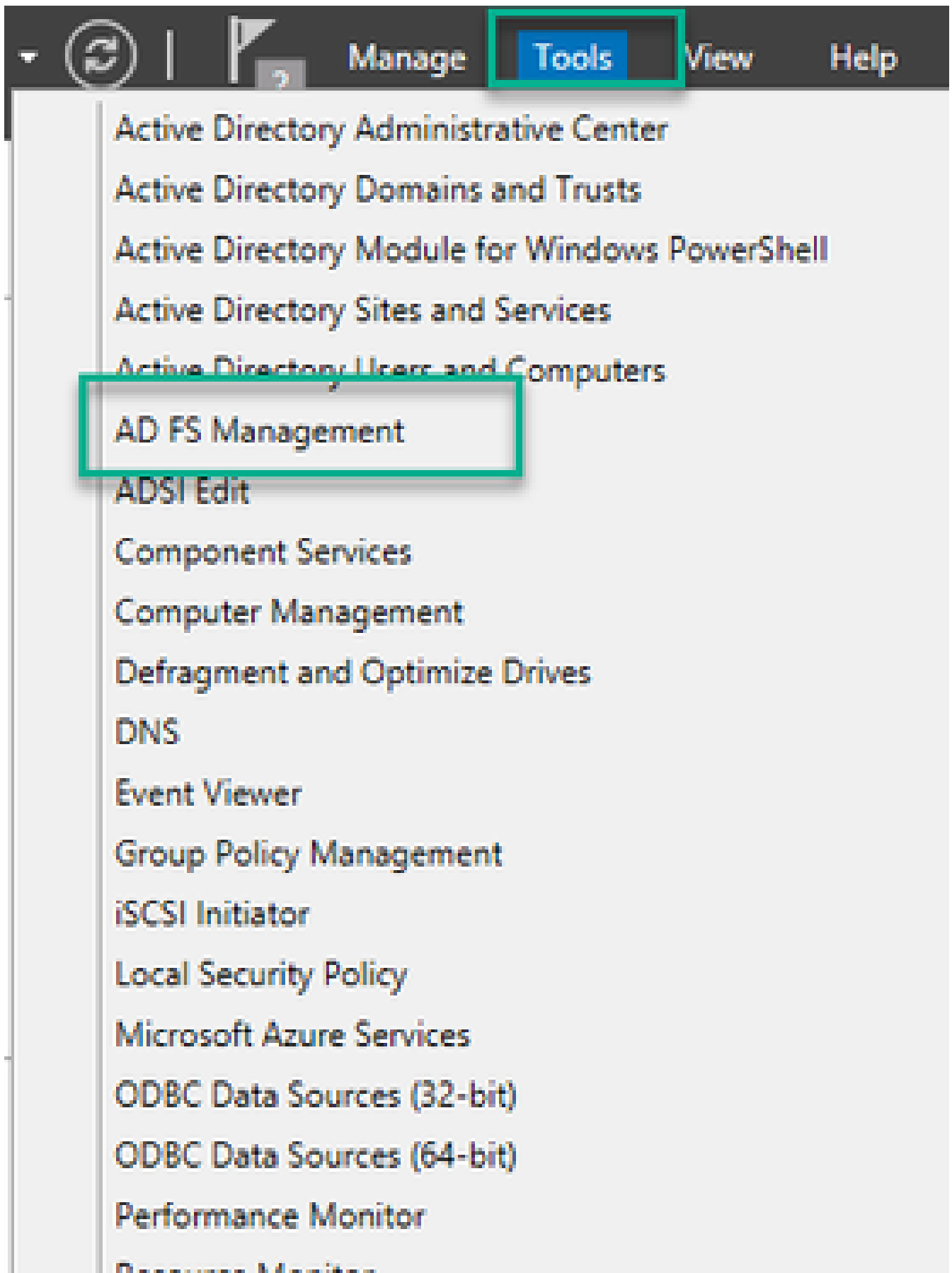
```
<?xml version="1.0"?>
- <md:EntityDescriptor entityID="https://meet.brhuff.local:443" ID="https://meet.brhuff.local:443" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
- <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" AuthnRequestsSigned="true">
- <md:KeyDescriptor use="signing">
- <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
- <ds:X509Data>
- <ds:X509Certificate>MIIFwTCCBKmqAwIBAgIT[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>MIIFwTCCBKmqAwIBAgIT[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>
```

0.

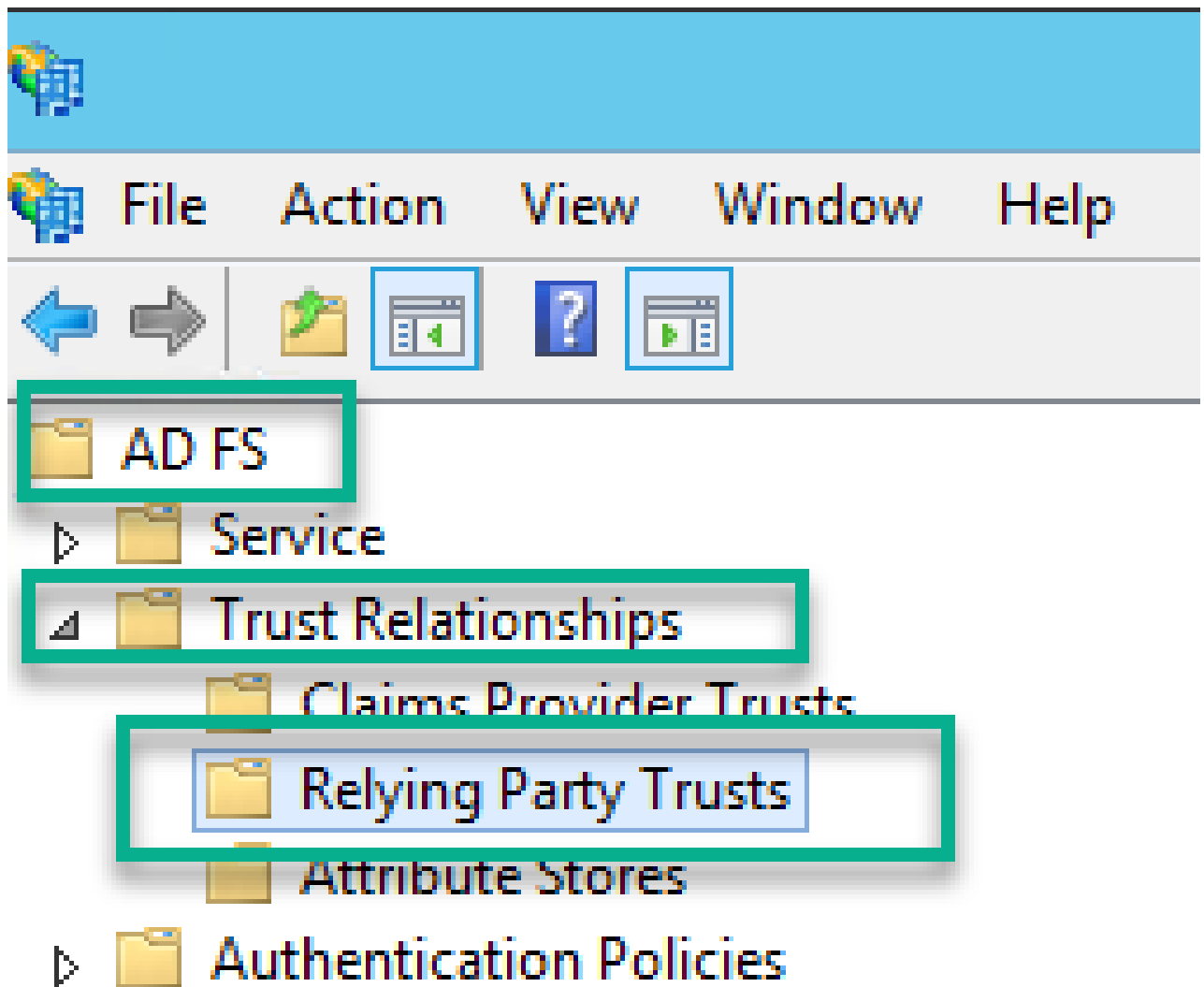
アイデンティティプロバイダー(IdP)へのWebbridgeのメタデータのインポート

適切な属性を使用してメタデータXMLが作成されたら、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。

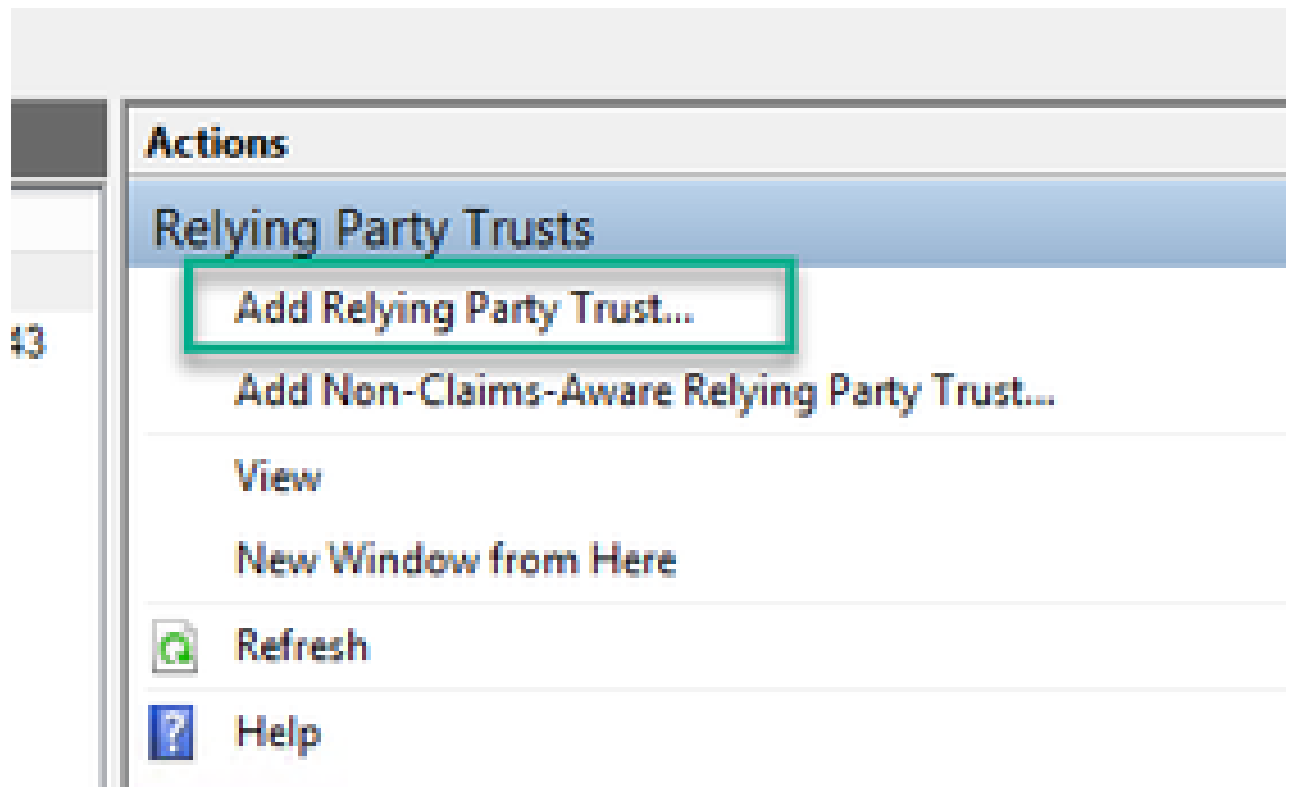
1. ADFSサービスをホストしているWindowsサーバーへのリモートデスクトップ
2. AD FS管理コンソールを開きます。このコンソールには、通常、サーバーマネージャーからアクセスできます。



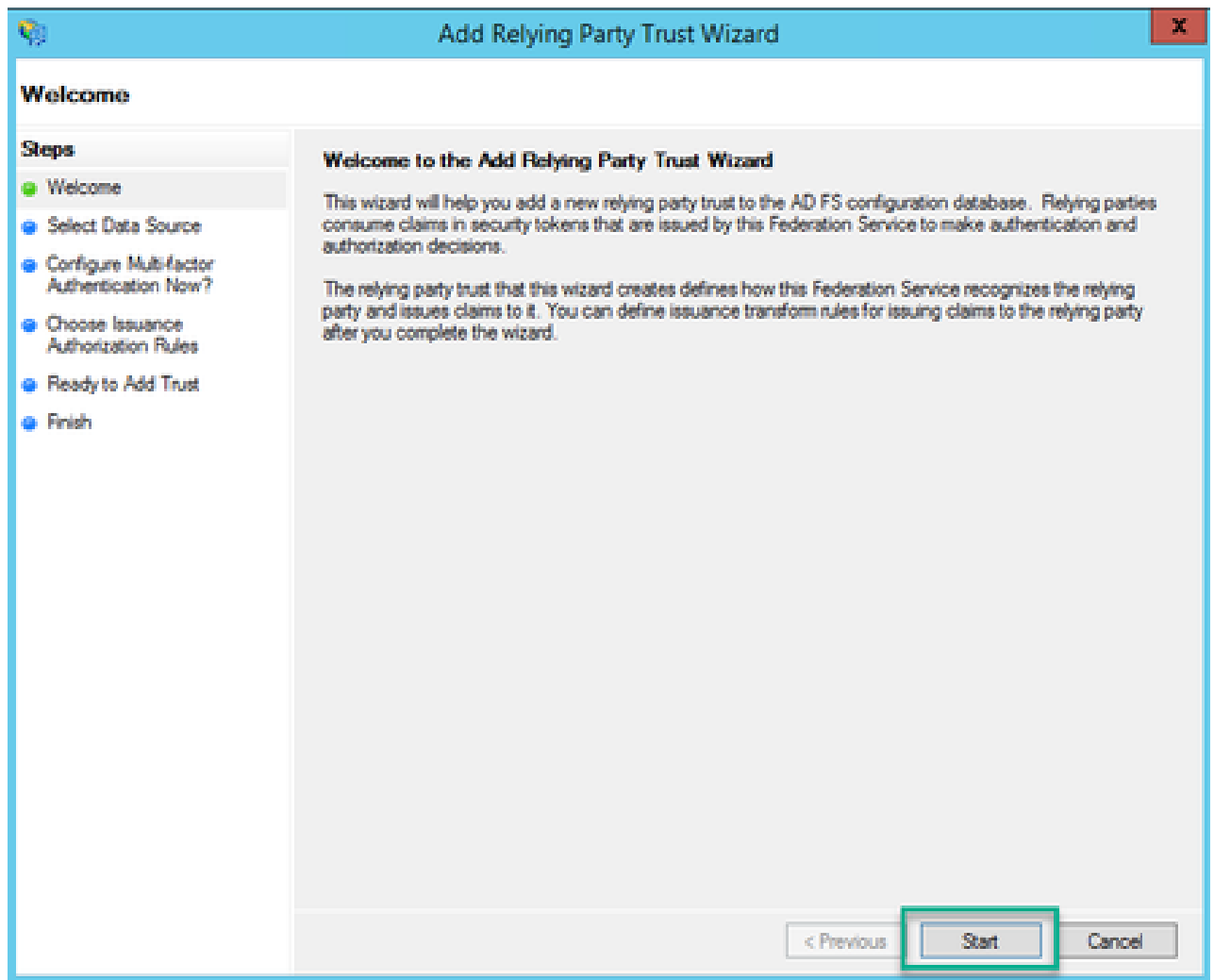
3. ADFS管理コンソールが表示されたら、左側のペインでADFS > Trust Relationships > Relying Party Trustの順に移動します。



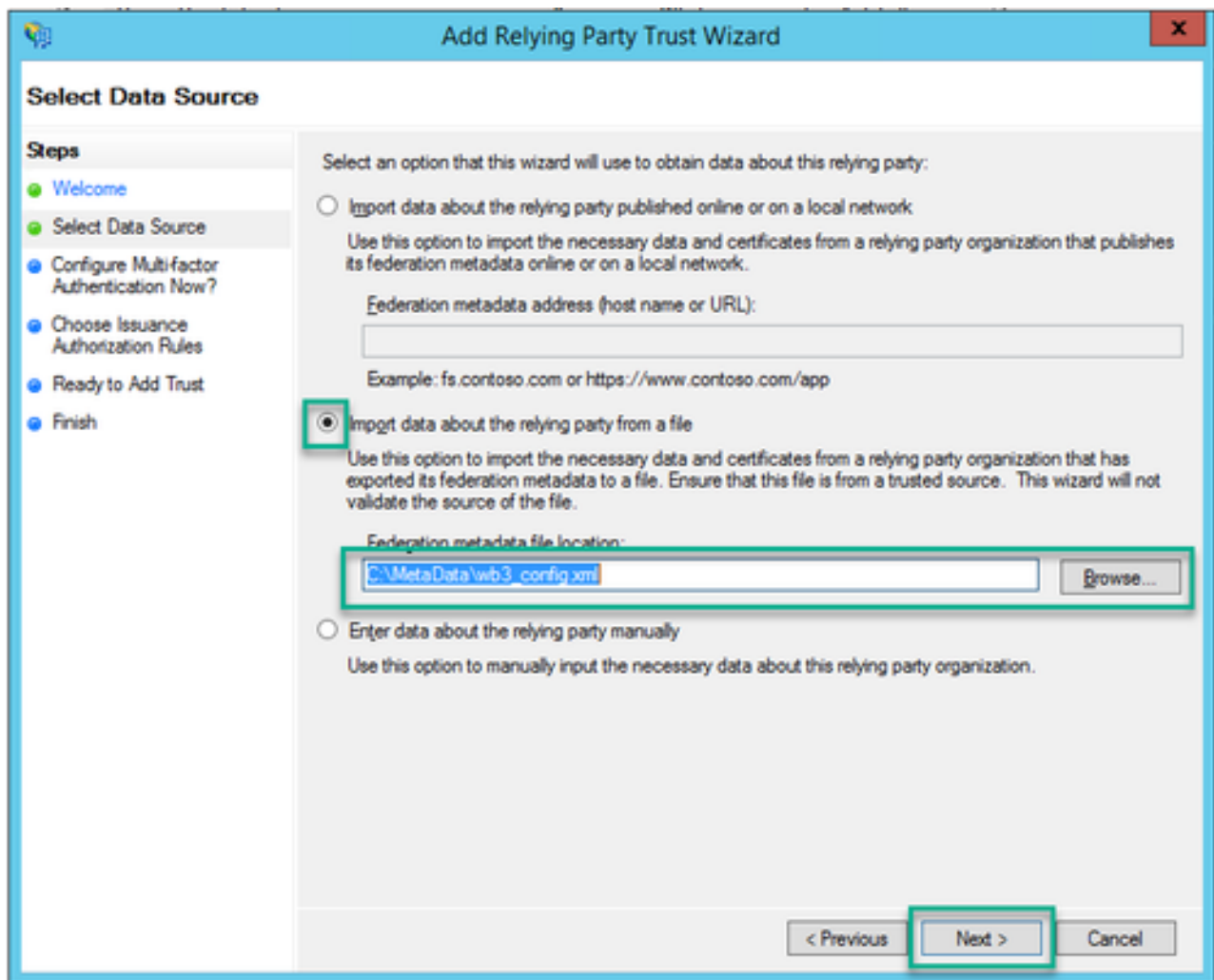
4. ADFS管理コンソールの右側のウィンドウで、[証明書利用者信頼の追加...]オプションを選択します。



5. この選択を行うと、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。



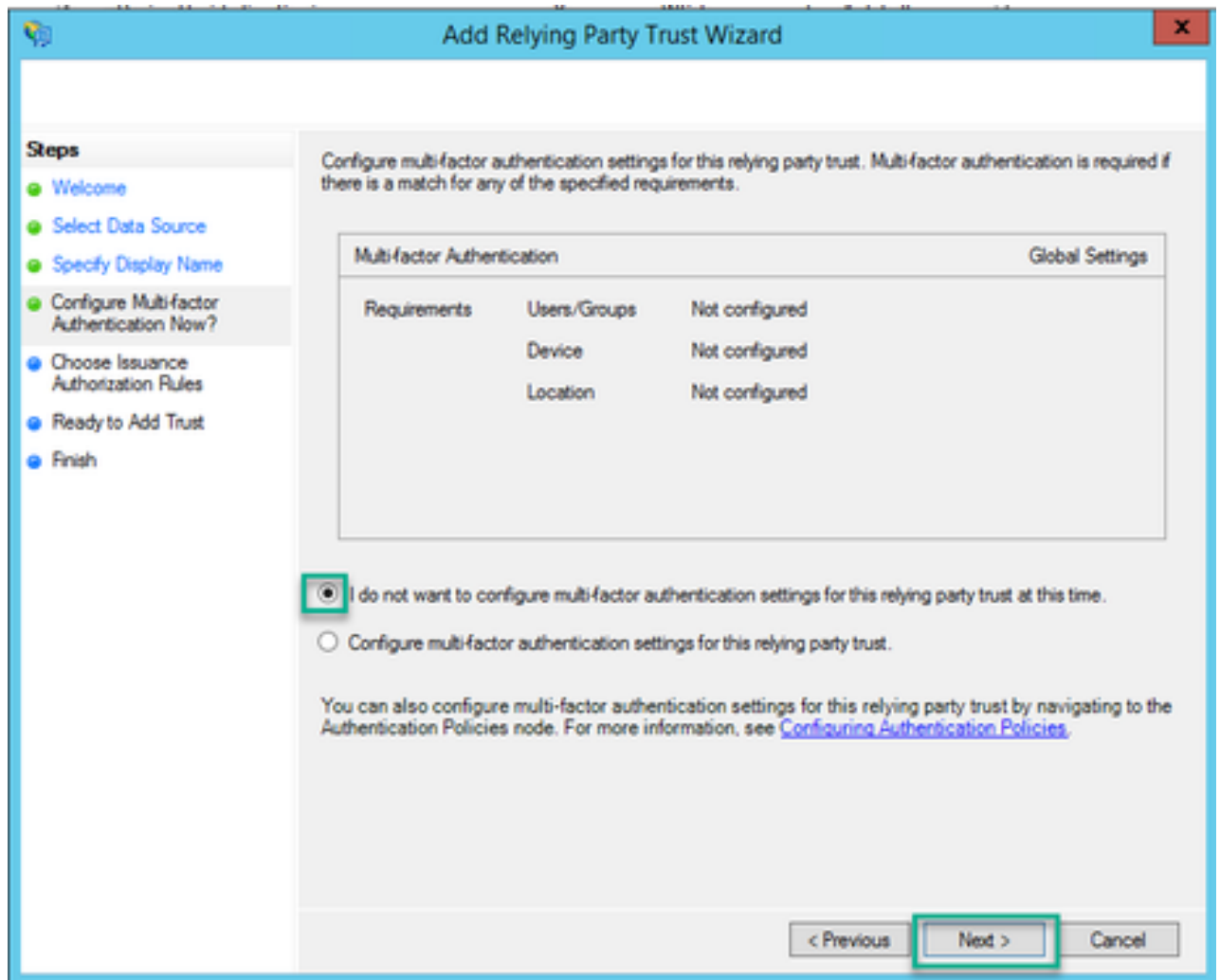
6. [データソースの選択]ページで、[ファイルから証明書利用者に関するデータをインポートする]のオプションボタンを選択し、[参照]を選択して、Webbridgeメタデータファイルの場所に移動します。



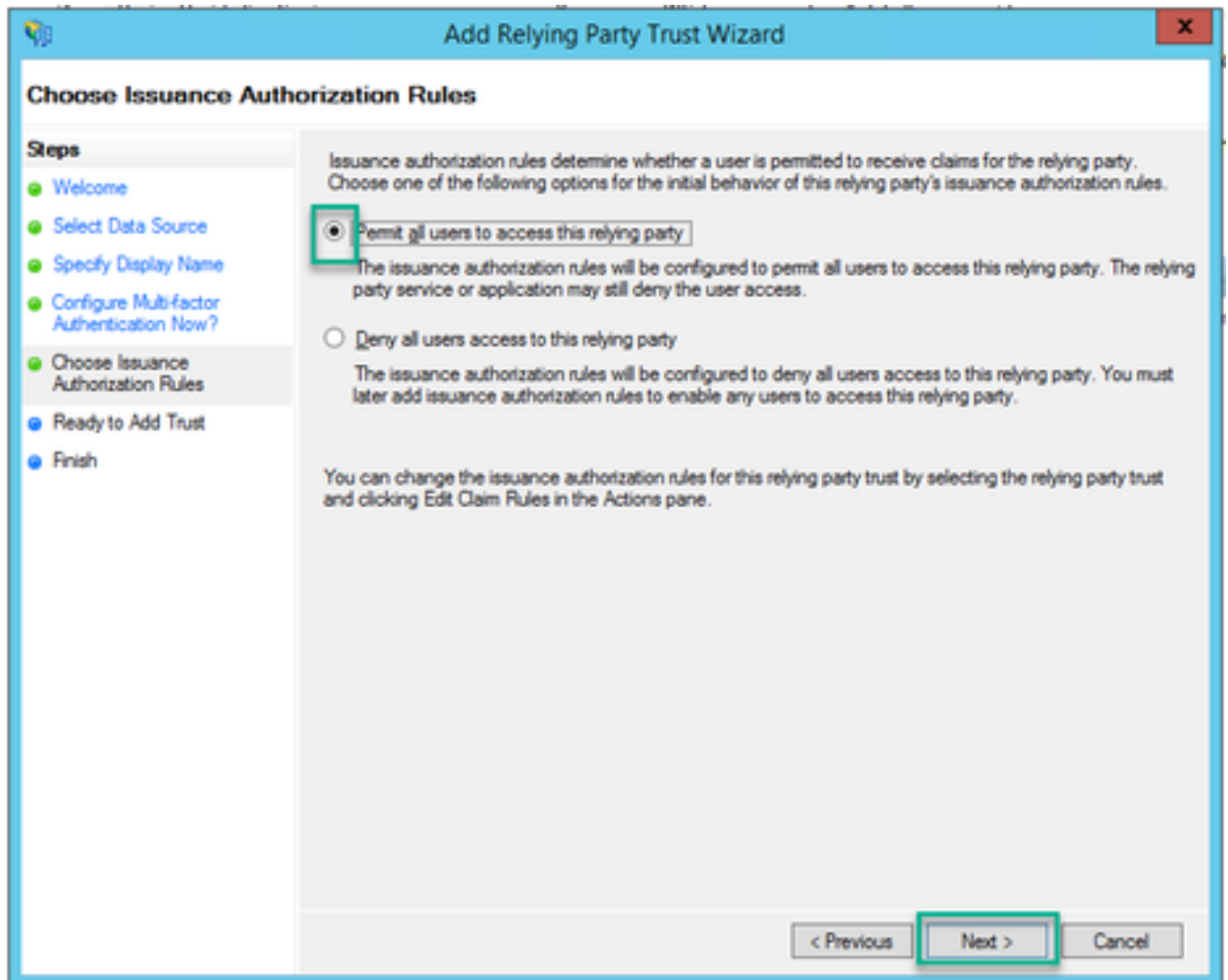
7. 「表示名の指定」ページで、ADFSのエンティティに対して表示される名前を入力します（表示名はADFS通信にサーバー目的ではなく、単に情報を提供するためのものです）。

The image shows a screenshot of the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Specify Display Name'. On the left, a 'Steps' list shows the following steps: 'Welcome', 'Select Data Source', 'Specify Display Name' (which is the current step), 'Configure Multi-factor Authentication Now?', 'Choose Issuance Authorization Rules', 'Ready to Add Trust', and 'Finish'. The main area contains the instruction 'Enter the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' label and a text input field containing 'Webbridge CMS SSO'. Below the input field is a 'Notes:' label and a text area containing 'This is the relying trust part for CMS SSO with WebApp'. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

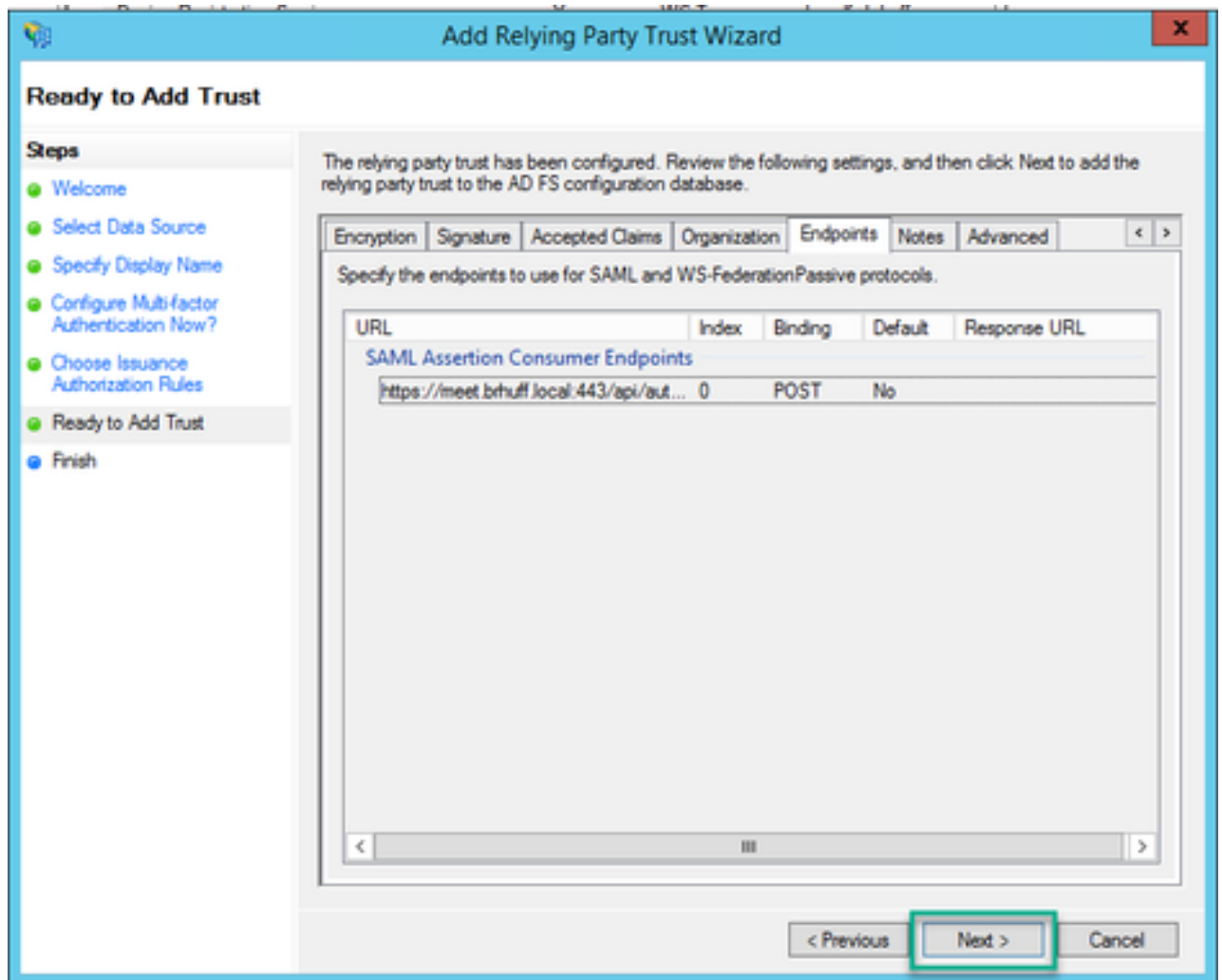
8. 「Configure Multi-factor Authentication Now?」 ページで、デフォルトのままにして「Next」を選択します。



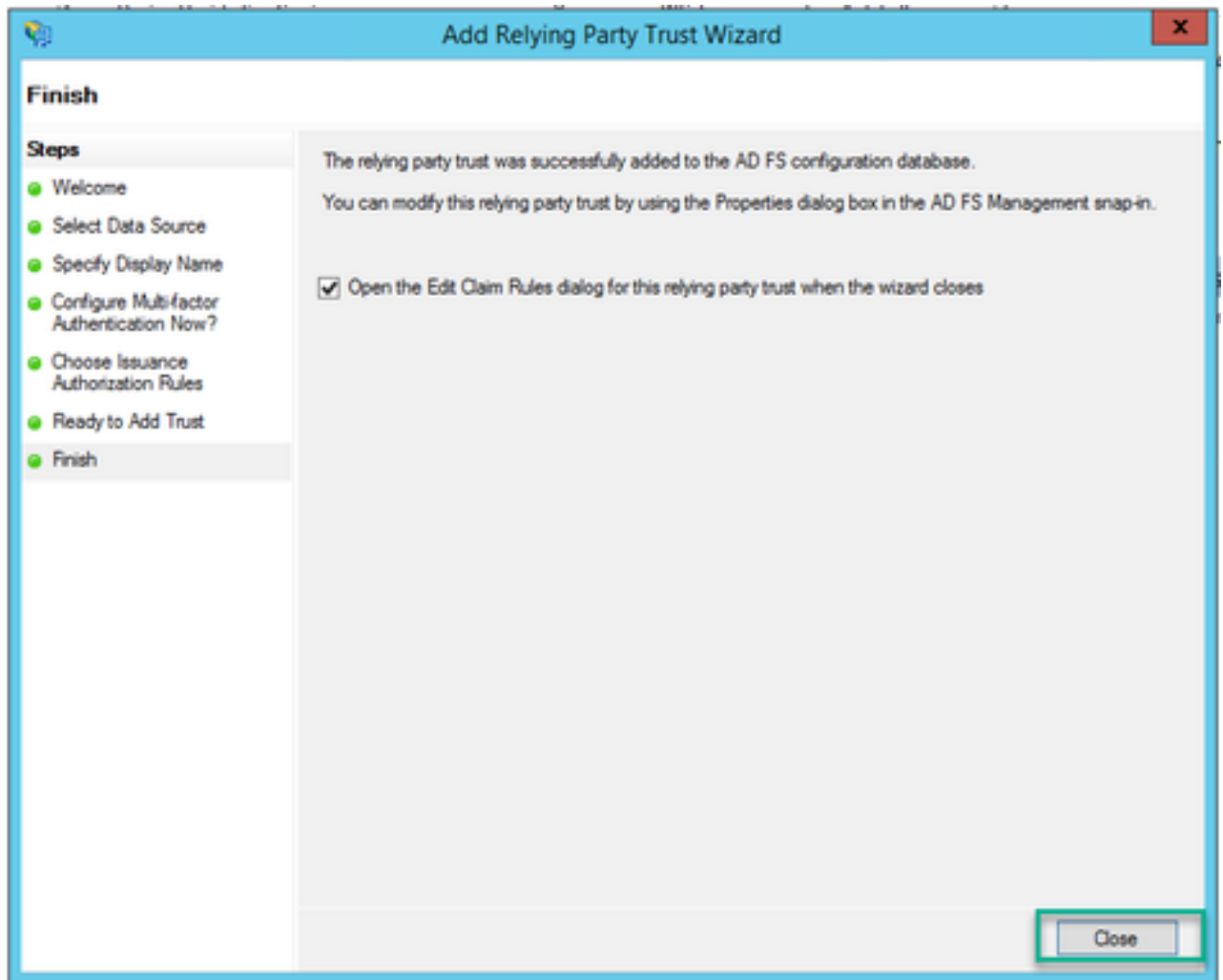
9. [Choose Issuance Authorization Rules]ページで、[Permit all users to access this relying party]を選択したままにします。



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、IDとエンドポイントを確認します。



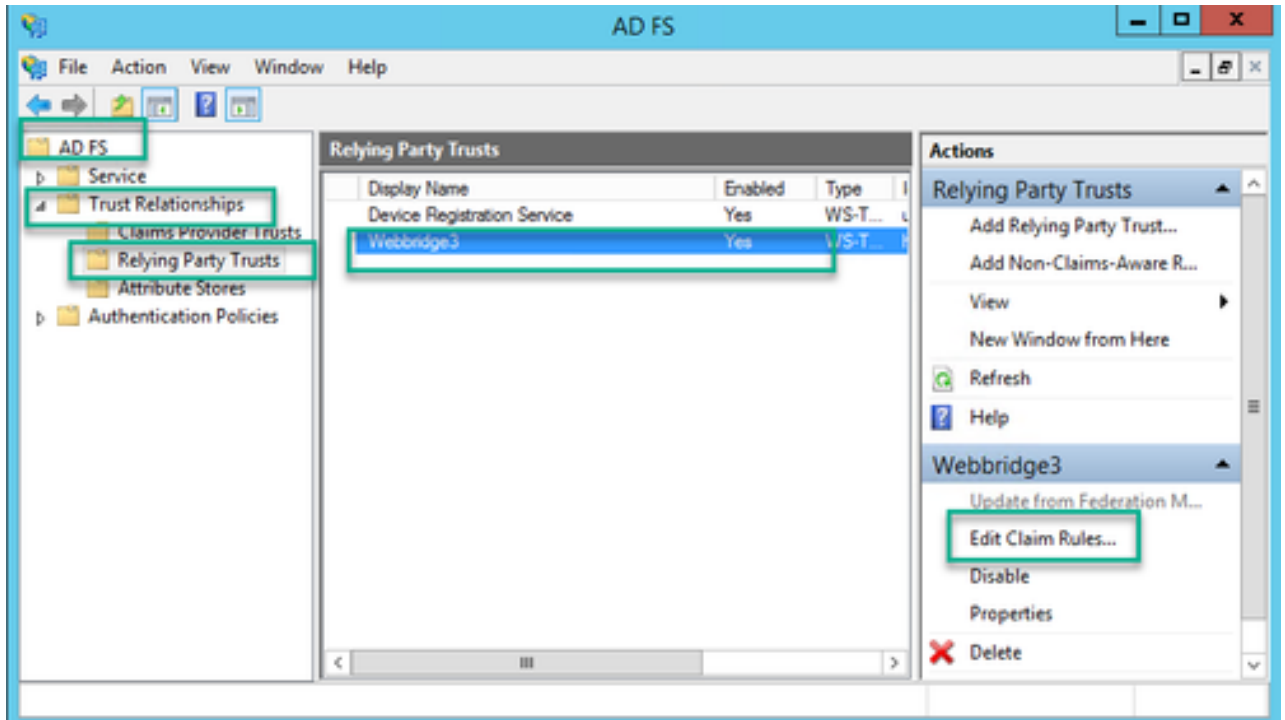
11. [完了] ページで、[閉じる]オプションを選択してウィザードを閉じ、要求ルールの編集を続行します。



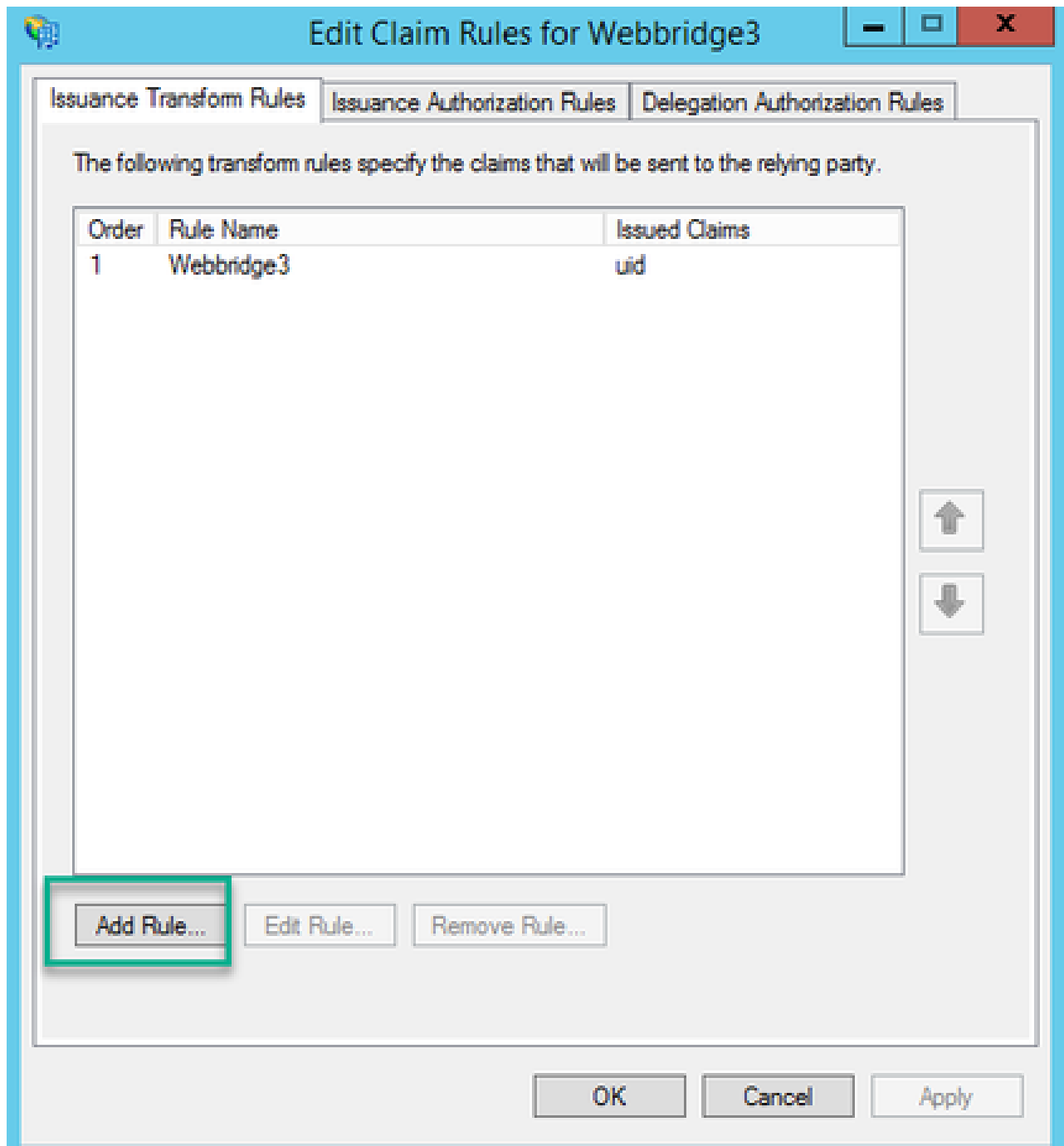
IdPでのWebbridgeサービスのクレームルールの作成

Webbridge用に証明書利用者信頼が作成されたため、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。

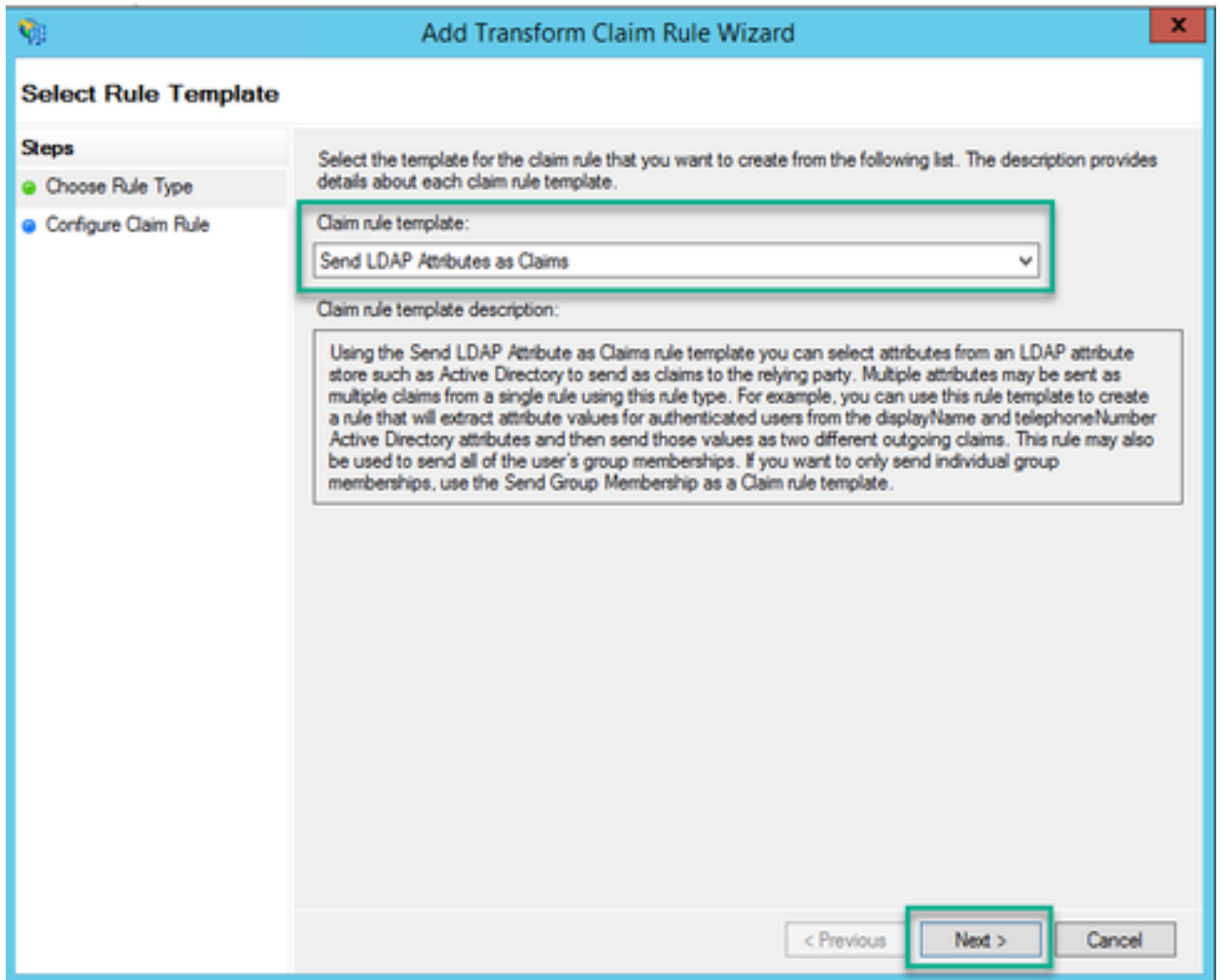
1. ADFS管理コンソールで、Webbridgeの証明書利用者信頼を強調表示し、右側のペインで要求規則の編集を選択します。



2. <DisplayName>の[要求ルールの編集]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 = ADFSでルールに指定する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属性 = 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 config.json内のauthenticationIdMappingと一致する必要があります。 (たとえば、uid) 。

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Webbridge3

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name	uid
⊞		

View Rule Language...

OK

Cancel

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(たとえば、sso_cmstest.zip)。
- 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、アップロードされたWebbridgeに対してSSOのみを使用できます。
- 複数のIDプロバイダーを使用している場合は、異なる命名スキームを使用して(sso_のプレ

フィックスを付けたまま)個別のZIPファイルをアップロードする必要があります。

- 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配置してそのフォルダをzipしないでください。

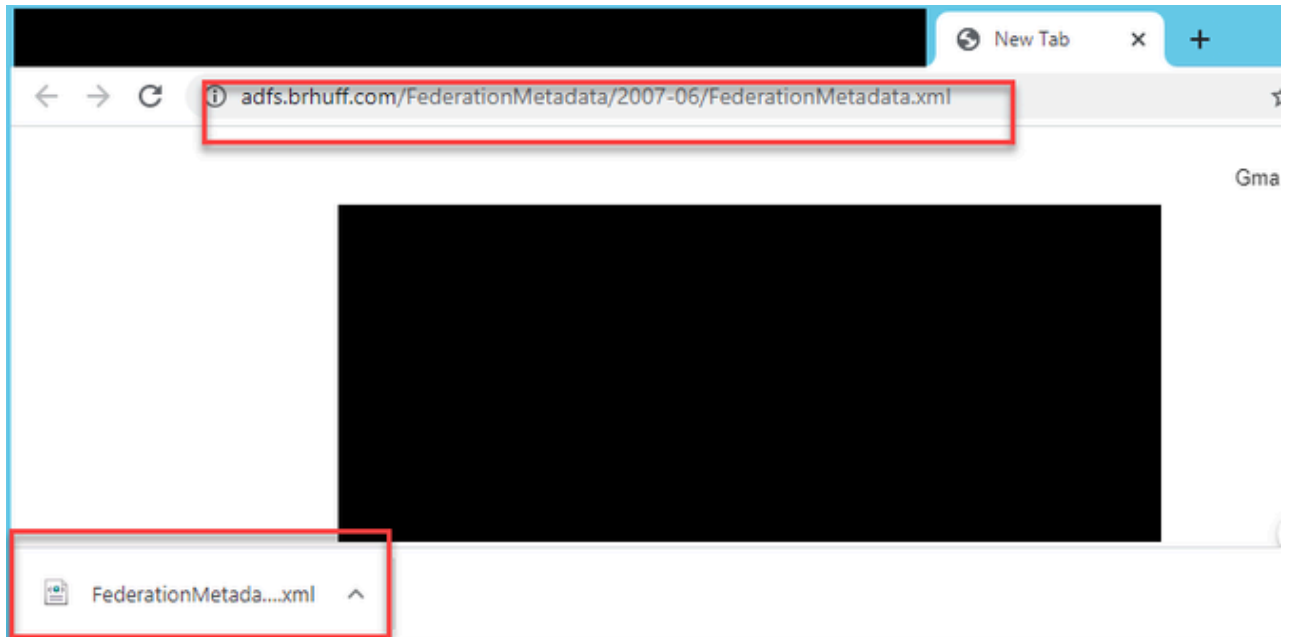
zipファイルの内容は、暗号化が使用されているかどうかによって、2～4ファイルで構成されま

filename	説明	必要?
idp_config.xml	これは、idPが収集できるMetaDataファイルです。ADFSでは、 <a href="https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml">https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml に移動して、これを見つけることができます。	はい
config.json	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_sign.keyキー	これは、IDプロバイダーで構成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セキュリティ保護にのみ必要	NO

idp_config.xmlを取得および設定します

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操作する場合は、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. ダウンロードしたファイルをzipファイルを作成する場所にコピーし、名前をidp_config.xmlに変更します。

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

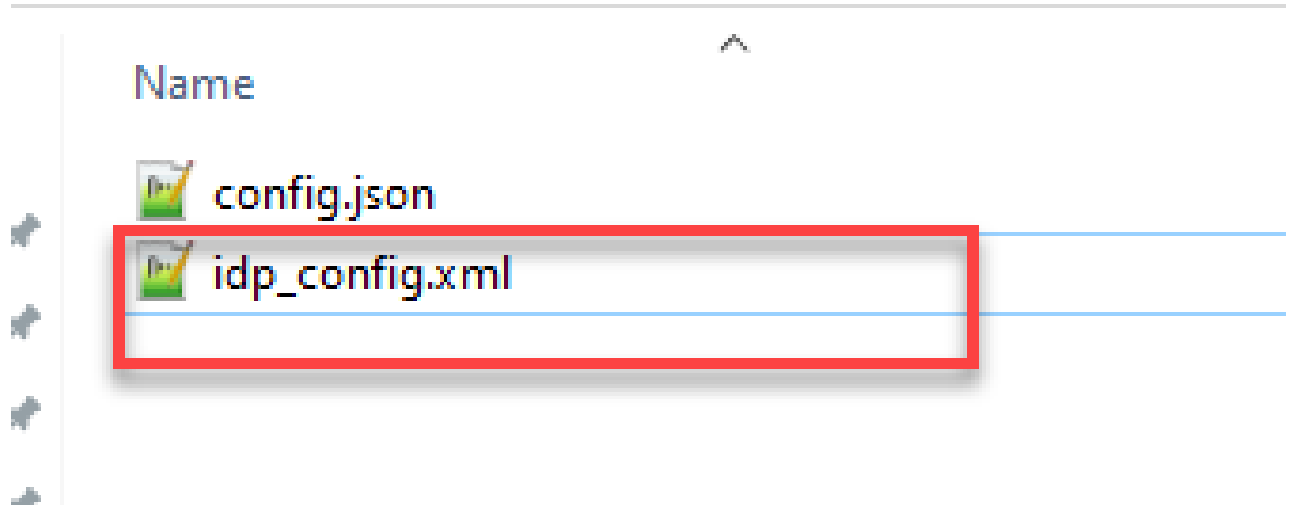
Create shortcut

Delete

Rename

Properties

Local Disk (D:) > brentssoconfig > SSOconfig



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{}で囲む必要があります。

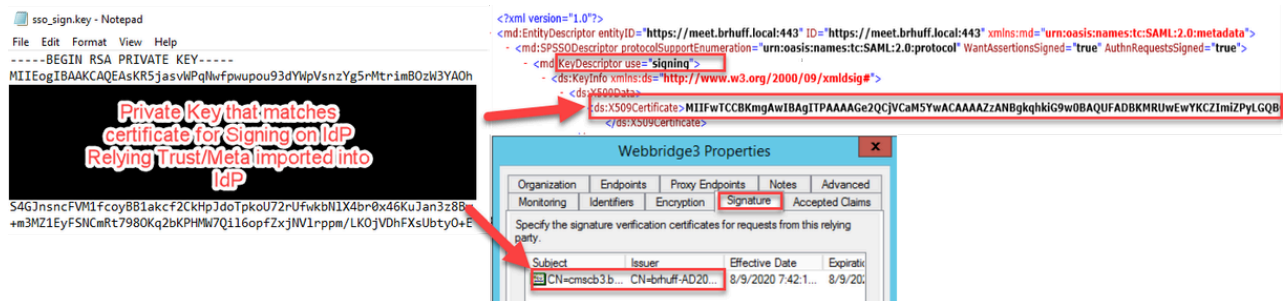
1. supportedDomains: IdPに対してSSO認証がチェックされるドメインのリストです。複数のドメインはカンマで区切ることができます。
2. authenticationIdMapping: これは、ADFS/IdPから出力要求ルールの一部として返されるパラメータです。これは、IdPの出力要求の種類の名前の値と一致する必要があります。クレームルール:
3. ssoServiceProviderAddress: これは、識別プロバイダーがSAML応答を送信する先のFQDN URLです。これはWebbridgeのFQDNである必要があります。

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。署名に使用する証明書は、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 Relying Trust Party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。

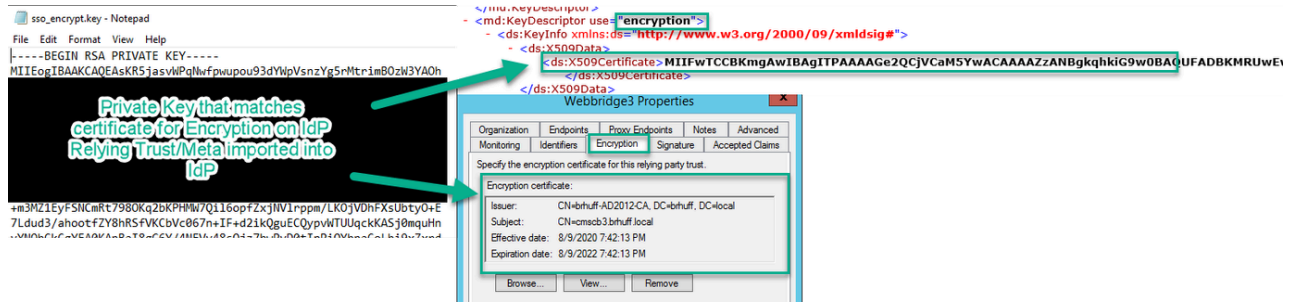


sso_encrypt.keyを設定します (オプション)。

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、<KeyDescriptor use=encryption>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 > Encryptionで表示 (およびインポート) することもできます。

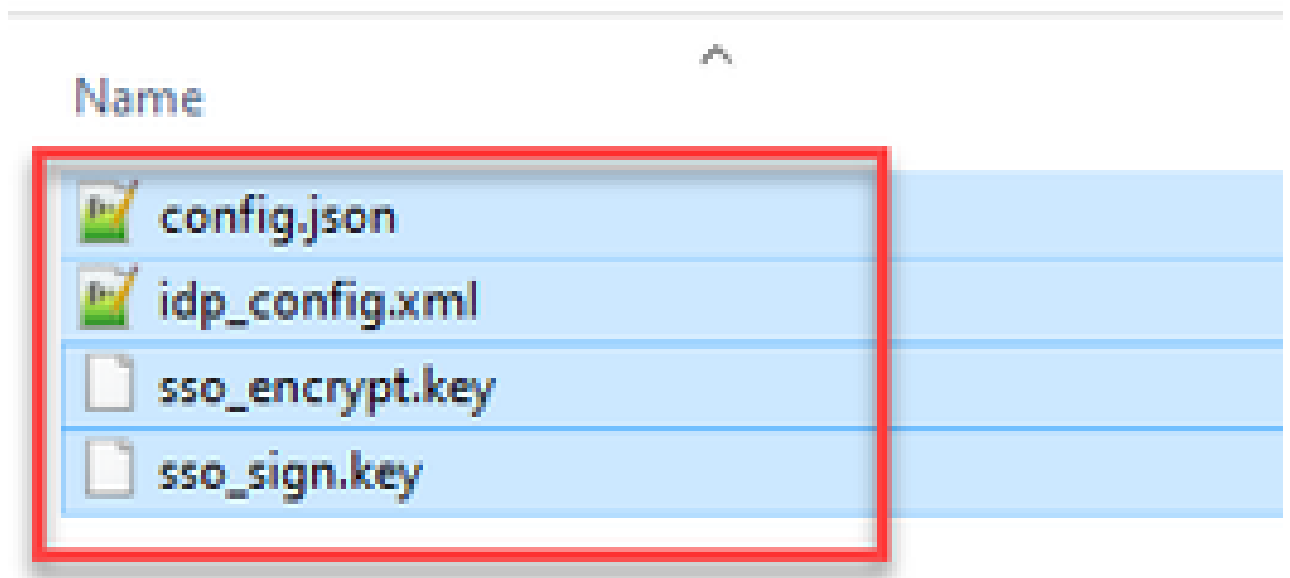
次の例では、ADFSにインポートされる前にWebbridgeメタデータに追加されたcallbridge証明書 (CN=cmscb3.brhuff.local)を確認できます。「sso_encrypt.key」に挿入された秘密キーは、cmscb3.brhuff.local証明書と一致する秘密キーです。

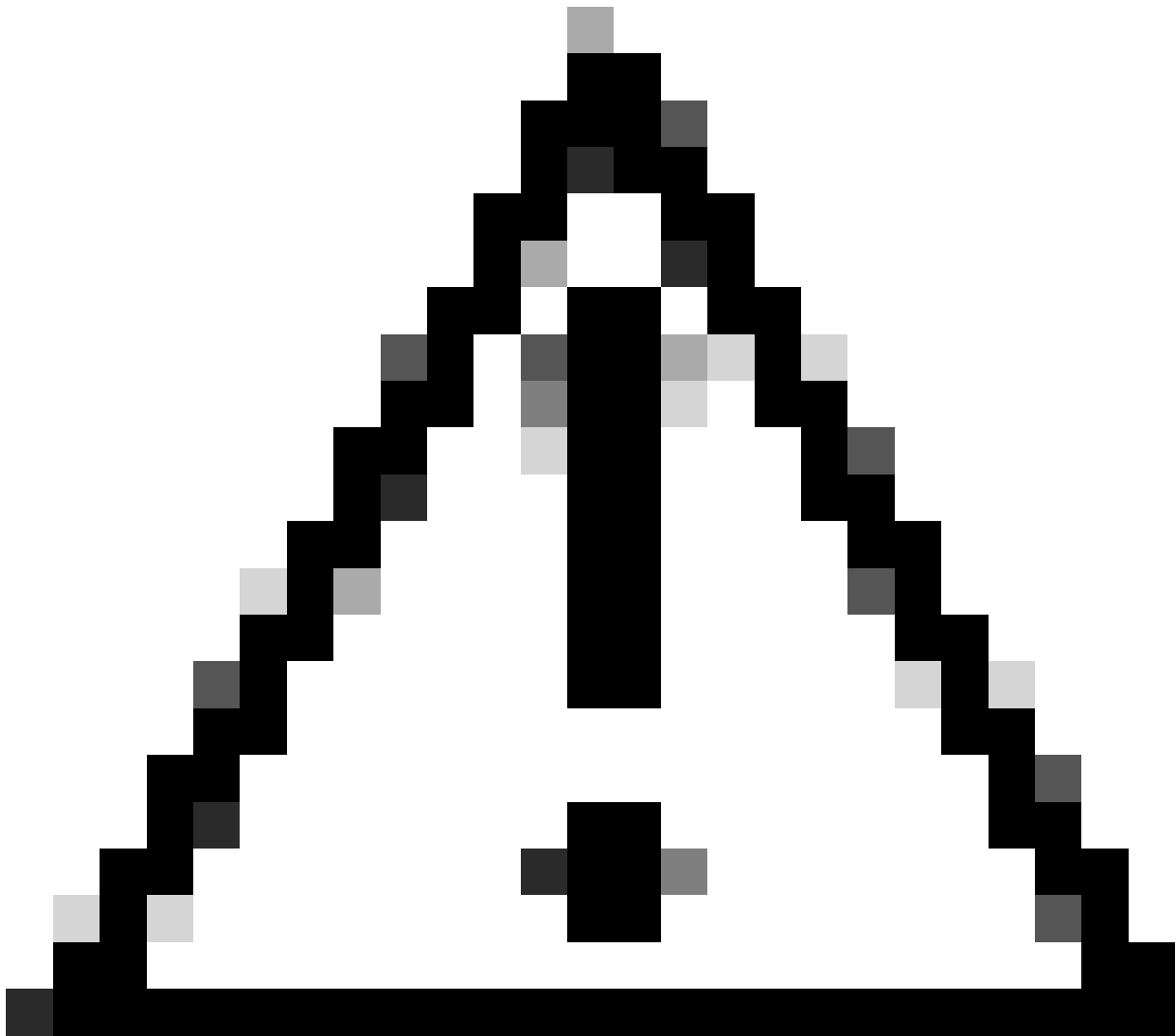
これはオプションの設定であり、SAML応答を暗号化する場合にのみ必要です。



SSO ZIPファイルの作成

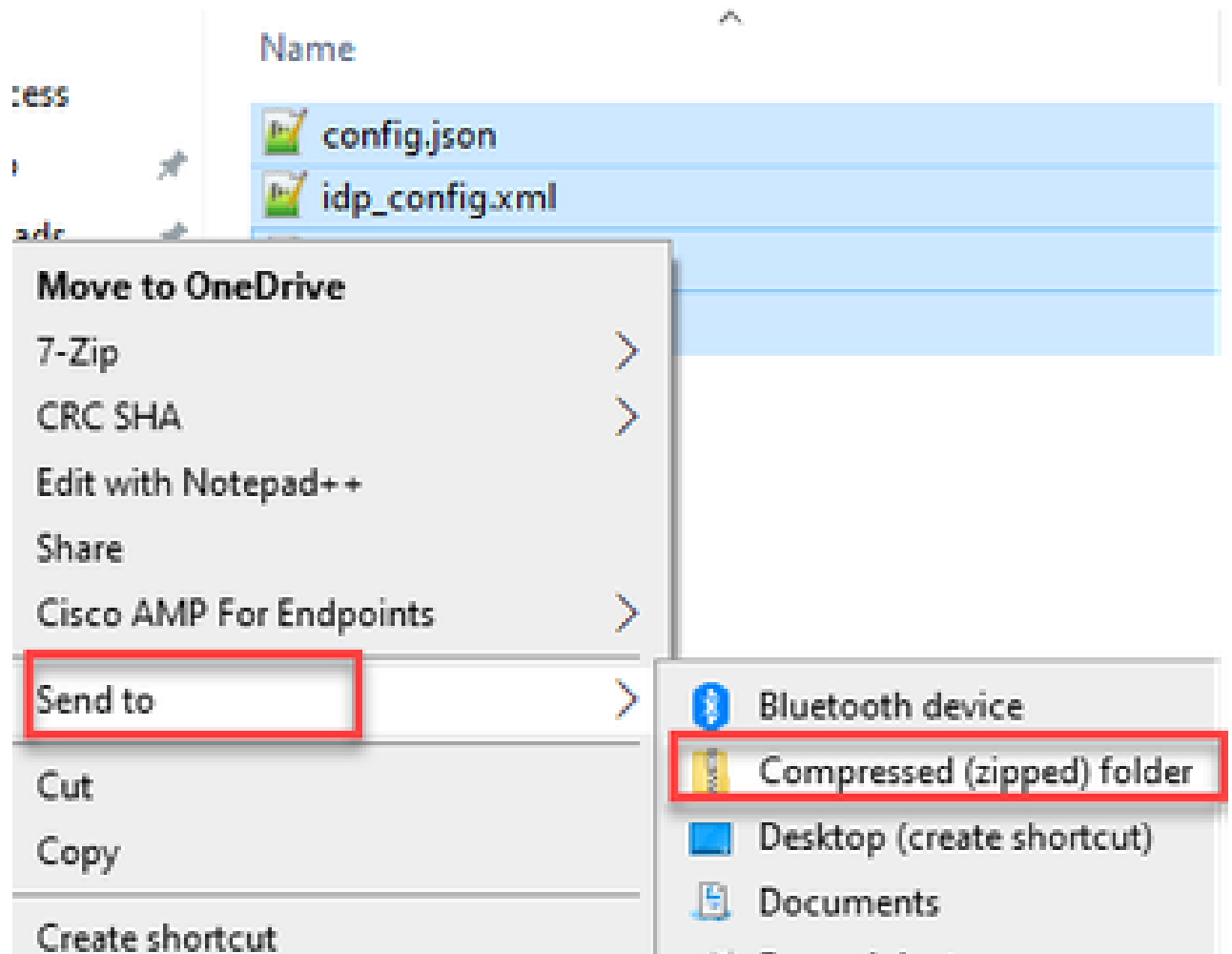
1. SSO設定ファイルに使用するすべてのファイルを強調表示します。



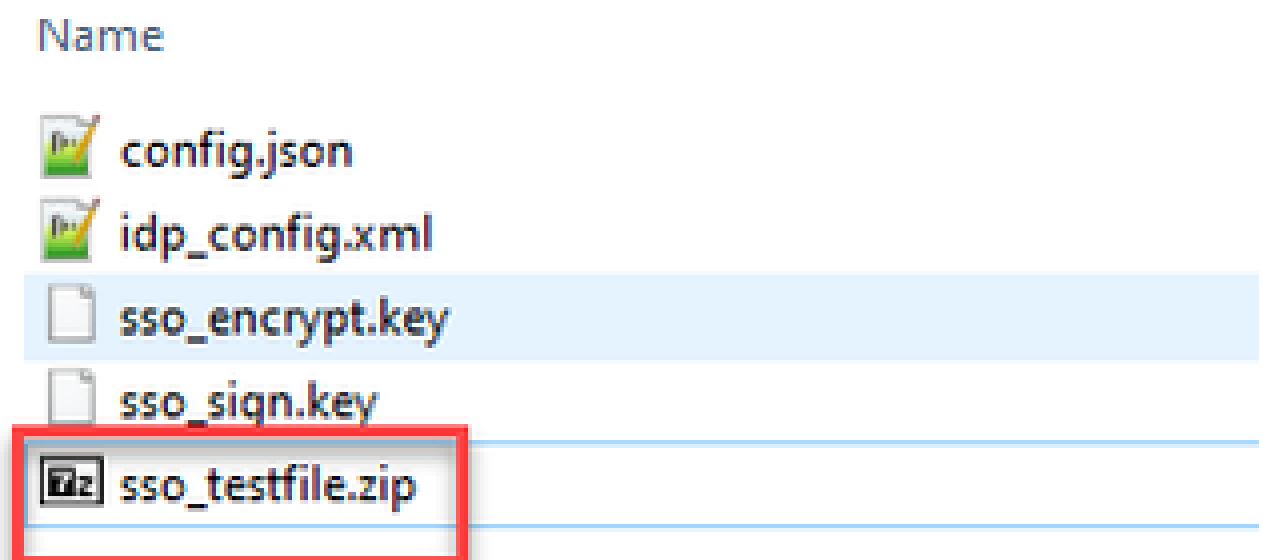


注意：ファイルが含まれているフォルダは圧縮しないでください。圧縮すると、SSOが機能しなくなります。

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



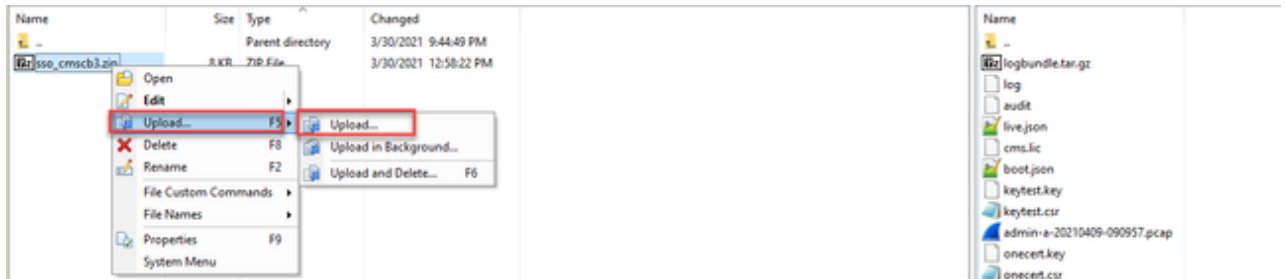
3. ファイルを圧縮した後、sso_プレフィクスを使用して目的の名前にファイル名を変更します。



WebbridgeへのSSO Zipファイルのアップロード

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ファイルが存在する場所へ移動し、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。

```
cmscb3> webbridge3 restart
SUCCESS: HTTPS Key and certificate pair match
SUCCESS: HTTPS full chain of certificates verifies correctly
SUCCESS: C2W Key and certificate pair match
SUCCESS: C2W full chain of certificates verifies correctly
SUCCESS: Webbridge3 enabled
cmscb3>
```

3. syslogで、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。

```
client_backend: INFO : SamlManager : Attempting to configure SSO information from:sso_cmscb3.zip
client_backend: INFO : SamlManager : Successfully saved config.json to ./FWDo4e/config.json
client_backend: INFO : SamlManager : Successfully saved idp_config.xml to ./FWDo4e/idp_config.xml
client_backend: INFO : SamlManager : Validated signing idp credential: /CN=ADFS Signing - adfs.brhuff.com
client_backend: INFO : SamlManager : SAML SSO configured, entityId:http://adfs.brhuff.com/adfs/services/trust
```

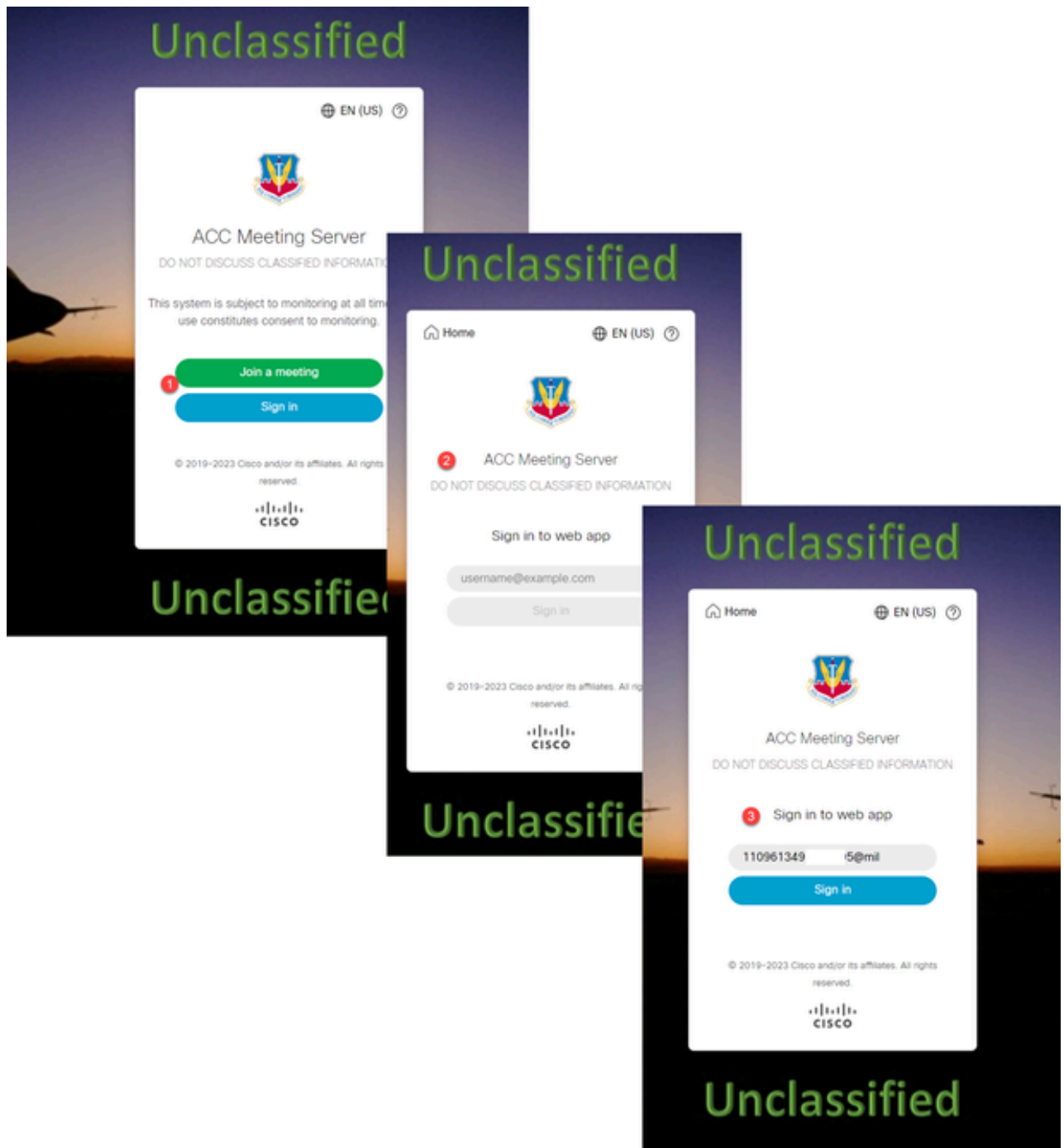
共通アクセスカード(CAC)

共通アクセスカード(CAC)は、現役の軍関係者、DoDの民間従業員、および適格な契約作業員の標準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. ブラウザを開く
4. 参加URLに移動し、会議に参加またはサインインオプションを確認します
5. サインイン：jidMappingとして設定されているユーザ名を入力します。Active DirectoryはCACログインから要求されます。

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ます。



ADFSがCACカードに使用するものと同じ方法で、jidMapping (これはユーザのサインイン名) をLdapmappingに設定します。 \$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てい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。

153 Edit Rule - webbridge sso

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

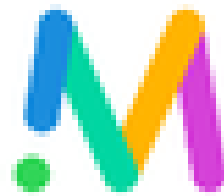
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-PrincipalName	uid
⊕		

WebApp経由のSSOログインのテスト

SSOの設定が完了したので、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。



Cisco Meeting Server

web app

Join meetings, anywhere, anytime

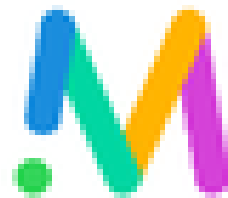
Join a meeting

Sign in

© 2020 Cisco and/or its affiliates. All rights reserved.



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) 。

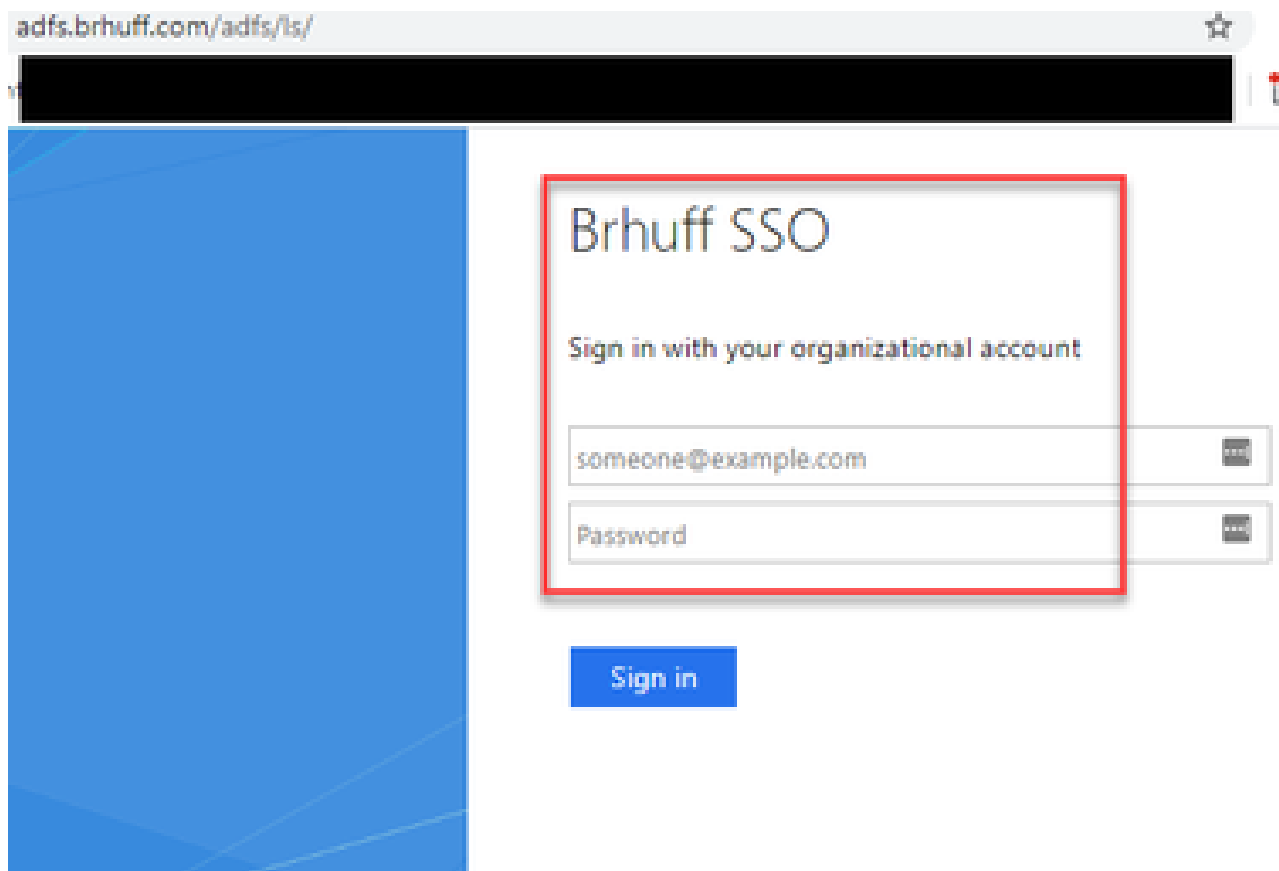


Cisco Meeting Server

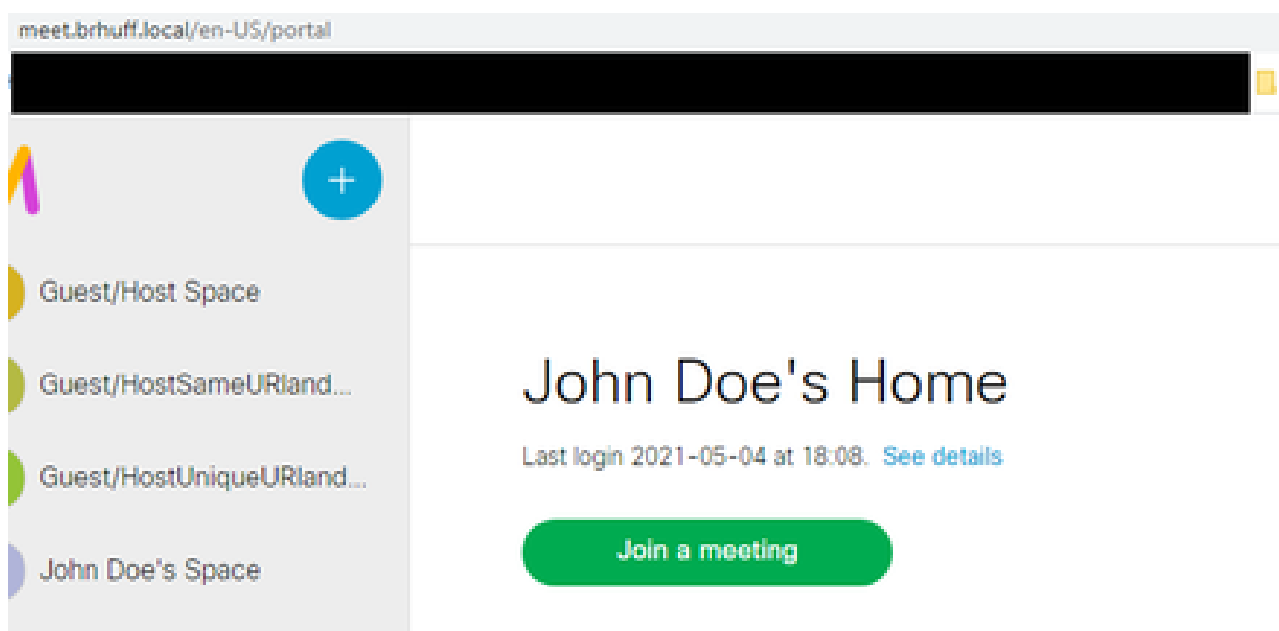
web app

Sign in to web app

3. 次に、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)。ここで、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を使用してクレデンシャル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の証明書利用者信頼としてインポートするために使用される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で、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ファイルに含まれてい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なしでテストを行い、この暗号化オプションなしでSSOが機能するかどうかを確認します。
4. SSOドメインの正しい詳細、Webbridge3 URL、およびSAMLResponseから一致する予想される認証マッピングを使用して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 URLに移動するときに、CMS syslogの詳細なロギングを有効にするには、URLの最後に?trace=trueを配置します。(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traceオプションを追加してテストを実行し、Webbridge3およびCMS Callbridge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、単一のlogbundle.tar.gzファイルだけがが必要です。

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かどうかを確認し、修復アクションを実行するのが理想的です。

[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が原因でエラーが発生したため、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ます。

認証IDを取得できませんでした

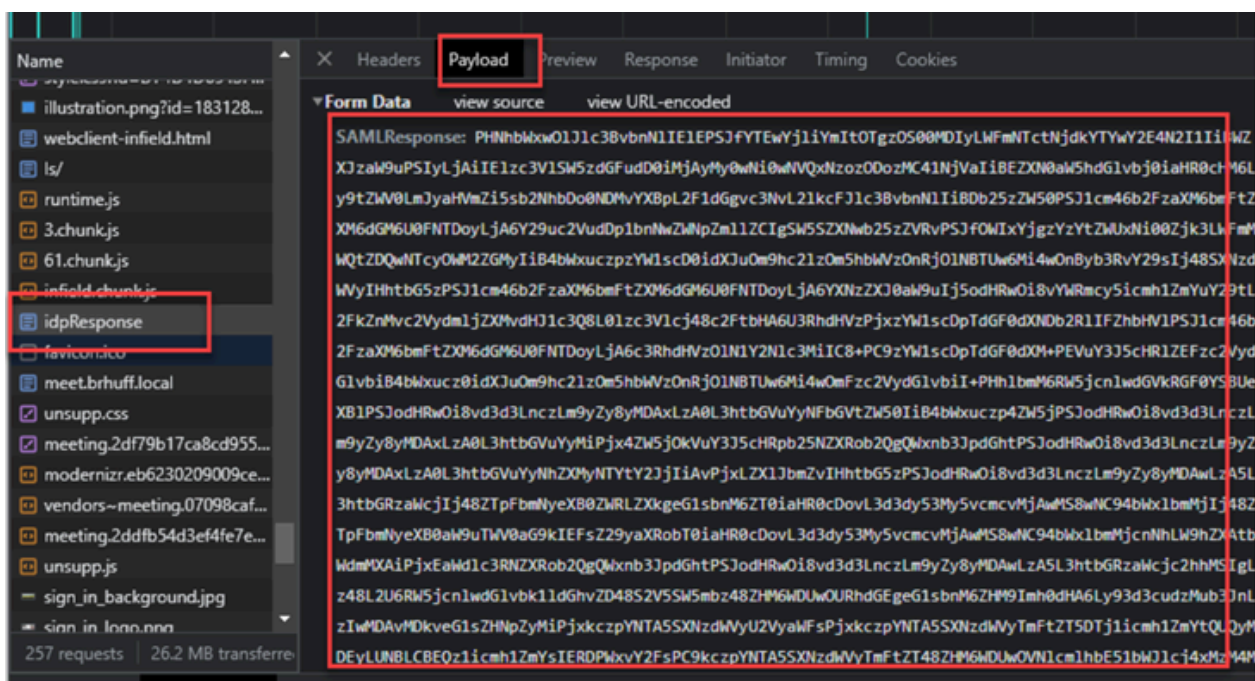
SAMLResponseをIdPから元に戻す交換中に、Webbridgeがログに次のエラーメッセージを表示し、SSO経由でのログインに失敗する場合があります。

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

これは、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が authenticationIdのconfig.jsonと比較して、応答に有効な照合属性を見つけられなかったことを示します。

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。

開発者ツールのネットワークロギング出力はHARデータとも呼ばれ、name列の下で idpResponseを探し、Payloadを選択して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データを受信する場合は、<AttributeStatement>のセクションを確認して返信される属性名を見つけます。このセクション内には、設定されてIdPから送信される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>
```

前の名前を確認すると、Attribute Statementセクションの下の<AttributeName>を調べて、それぞれの値をSSO config.jsonのauthenticationIdmappingセクションで設定した値と比較できます。

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、「uid」、「<URL>/NameID」、または「<URL>/CommonName」のいずれかの属性名に一致するように更新される「authenticationIdMapping」です。渡されたときにCallbridge APIで設定された期待値と(正確に)一致する限り)

検証でアサーションが渡されない/一致しない

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: INFO : SamlManager : 許可された対象ユーザー内に存在しないアサーショ
```


ンをスキップしています

このエラーが示しているのは、IdPからSAMLResponseを確認する際に、Webbridgeが一致するセッションを見つけられなかったため、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です。

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、Webブラウザ経由でDeveloper Tools Network LoggingからSAML応答を抽出し、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データを調べる際は、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、「Audience does NOT MATCH the Service provider address in the configuration」が原因でエラーが発生したことがわかります。これは、このアドレスの末尾に「:443」が追加されているためです。

```
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が追加されるように更新できます(メタデータが更新されている場合は、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する場合は、再インポートする必要はありません)。

Webアプリでサインインに失敗しました :



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.



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 : 情報 : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] SAMLトークンが正常に生成されました

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

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を検出できませんでした

3月18日14:54:52.698 user.info cmscb3-1 client_backend:INFO : SamlManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] Attempting to find SSO in SAML Token Request

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」と表示されます

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: ERROR : SamlManager : No authenticationId mapped element found in signed SAML Assertions

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で設定されているものと一致することを想定しています。

Edit Rule - Webbridge3

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
Webbridge3

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
E-Mail-Addresses	E-Mail Address

ADFSのクレームルール

```
1 {  
2   "authenticationIdMapping" : "uid",  
3   "ssoServiceProviderAddress" : "https://meet.brhuff.local:443",  
4   "supportedDomains" : ["brhuff.com"]  
5 }
```

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)



Blahman Industries

Blahman WebApp

Sign in to web app

steve@brhuff.com

Sign in

 Username is not recognized

© 2019-2023 Cisco and/or its affiliates. All rights reserved.



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 : 情報 : 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

3月18日14:58:48.077 user.info cmscb3-1 client_backend : 情報 : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6]正常に認証IDを取得しました
: 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-02 2a1-b125-136fdf5612a5
(user=steve@brhuff.com)

Mar 18 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を入力しましたが、ログインに失敗し、「Username is not recognized」と表示されます。



Blahman Industries

Blahman WebApp

Sign in to web app

darmckin@brhuff.com

Sign in

 Username is not recognized

© 2019-2023 Cisco and/or its affiliates. All rights reserved.



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 : 情報 : SamlManager : [d626bbaf-80c3-4286-8284-fac6f71eb140] SAMLトークンが正常に生成されました

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 : 情報 : 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る設定済みのLDAP属性と一致しません。次の行の「Successfully obtain authenticationID:darmckin@brhuff.com」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DARMCKINであることを示しています。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 :

次のいずれかの操作を行います。

1. CMS ldapmapping内のAuthenticationIDをADFSのクレームルールで使用されている値と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で設定されている属性と一致するように変更します

Related objects: </api/v1/ldapMappings>

Table view

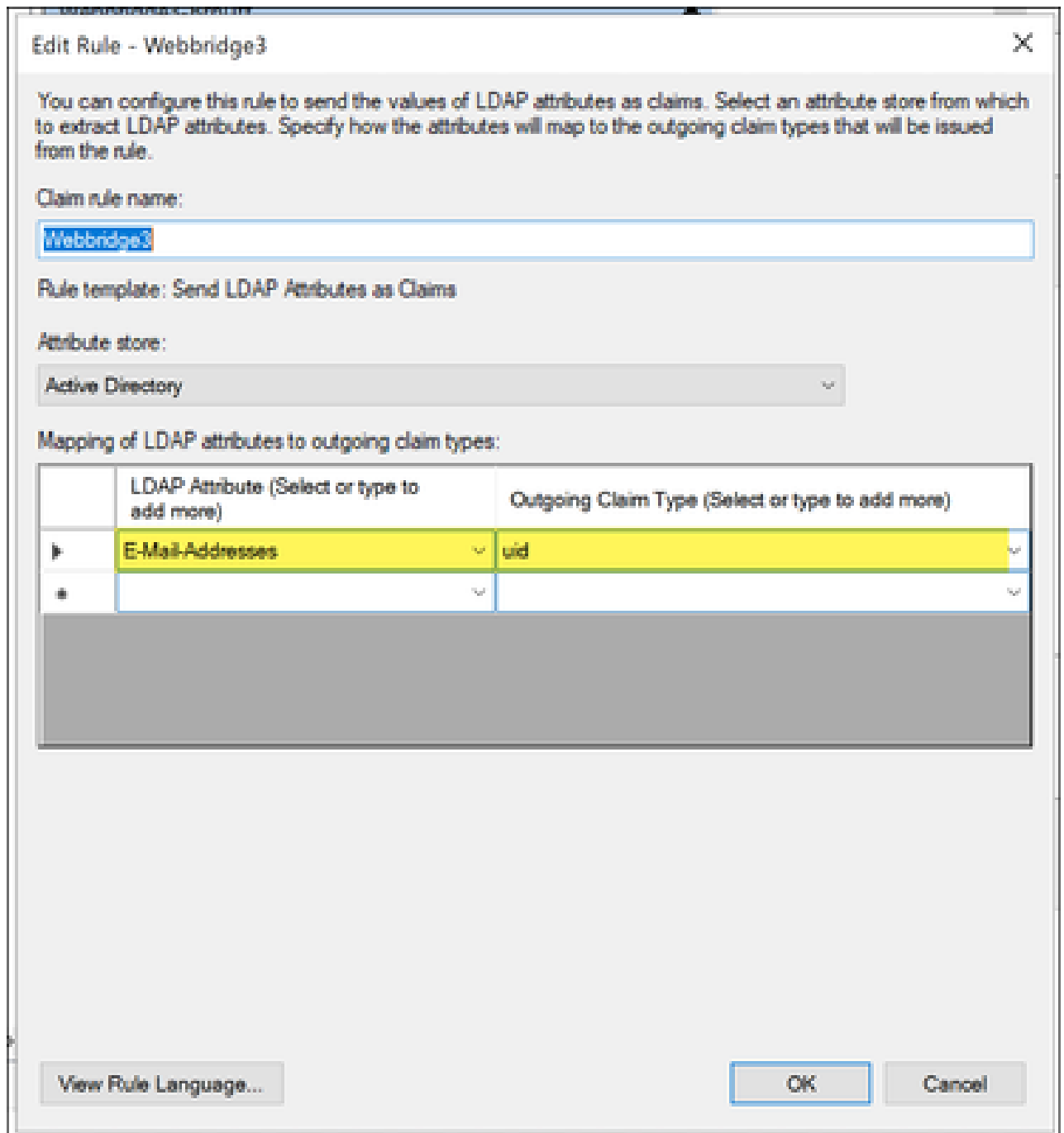
XML view

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	
userId	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ログに示された作業ログの例。 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] Successfully obtain

authenticationID:darmckin@brhuff.com

3月18日14:24:01.102 user.info cmscb3-1 host:server : 情報 : WB3Cmgr: [7979f13c-d490-4f8b-899c-0c82853369ba] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c-024 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-b5d5-9abdfa89ba0f

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] 14.0.25.247 - [2024年3月18日 : 18:24:01 +000] "ステータス0 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 (KHTML、Geckoなど) Chrome/122.0.0.0 Safari/537.36" to upstream 192.0.2.2:9000: upstream_response_time 0.038 request_time 0.039 msec 1710786241.133 upstream_response_length 24 200

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。