在CMS上配置並排除WebApp SSO故障

目錄

簡介

本文檔介紹如何配置單次登入(SSO)的Cisco Meeting Server (CMS) Web App實施並對其進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- CMS Callbridge版本3.1或更高版本
- CMS Webbridge版本3.1或更高版本
- Active Directory伺服器
- 辨識提供者(IdP)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CMS Callbridge版本3.2
- CMS Webbridge版本3.2
- Microsoft Active Directory Windows Server 2012 R2
- Microsoft ADFS 3.0 Windows Server 2012 R2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景

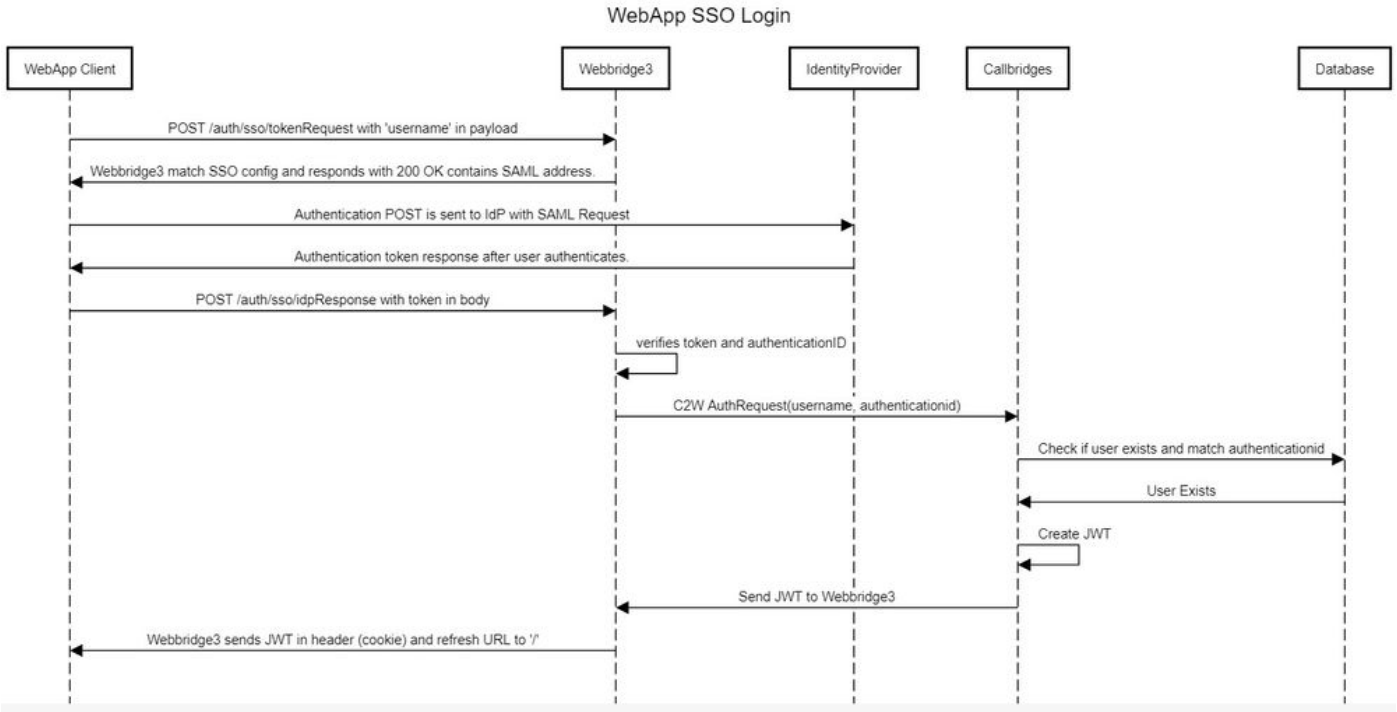
CMS 3.1及更高版本引入了使用者使用SSO登入的功能，無需在每次使用者登入時輸入密碼，因為會與身份提供商建立單個會話。
此功能使用Security Assertion Markup Language (SAML) 2.0版作為SSO機制。

注意：CMS僅支援SAML 2.0中的HTTP-POST繫結，並拒絕任何沒有HTTP-POST繫結的標識提供程式。

注意：啟用SSO後，基本的LDAP身份驗證不再可用。

設定

網路圖表



ADFS安裝和初始安裝

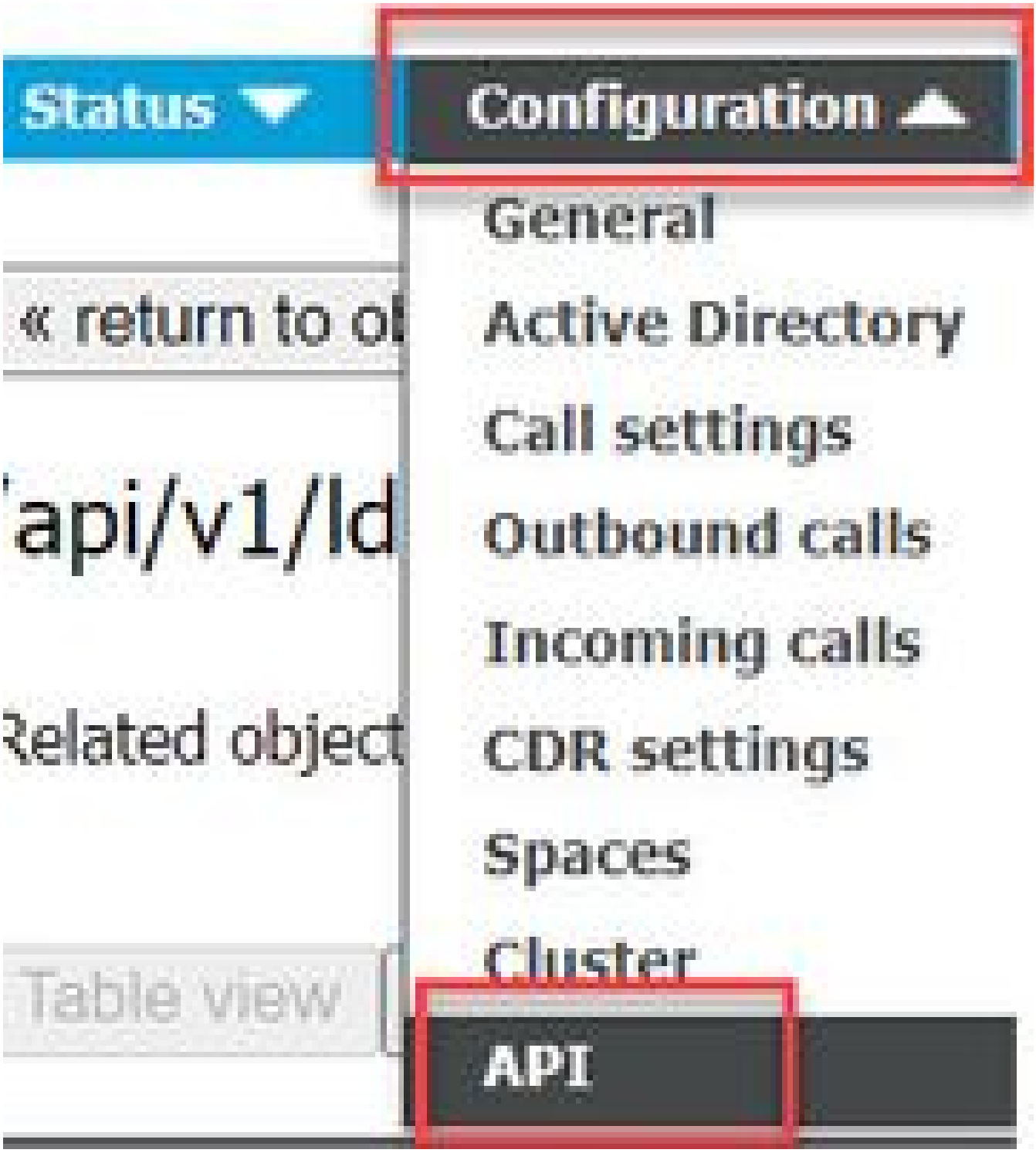
此部署方案使用Microsoft Active Directory Federation Services (ADFS)作為身份提供程式(IdP)，因此，建議在此配置之前安裝和運行ADFS（或目標IdP）。

將CMS使用者對映到身份提供程式(IdP)

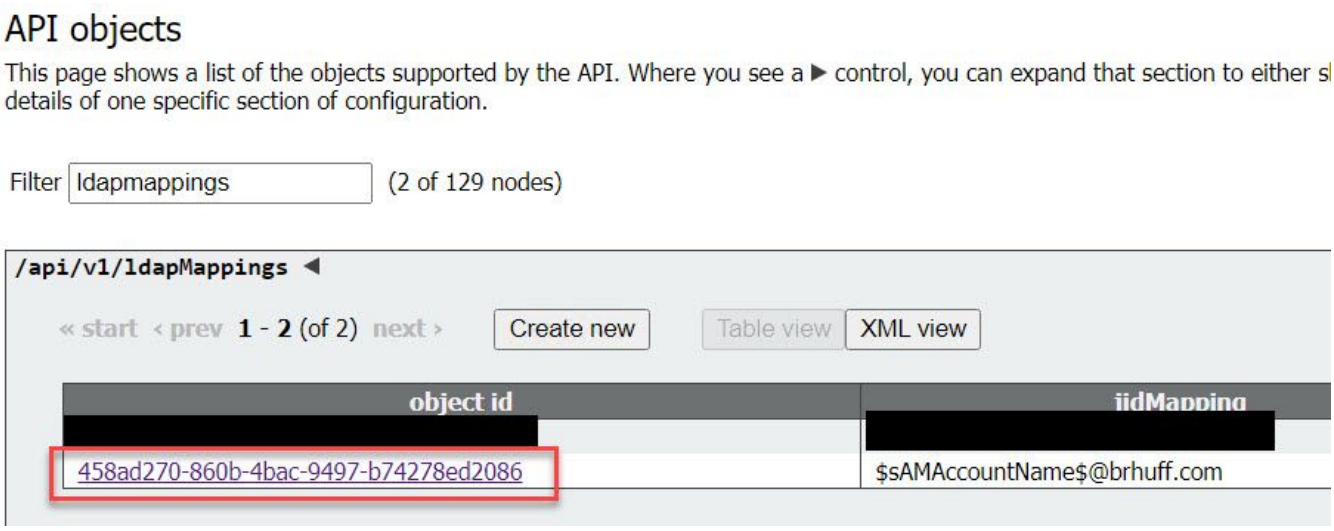
為了讓使用者獲得有效的驗證，必須在應用程式設計介面(API)中對應由IdP提供的相關欄位。用於該操作的選項是API的ldapMapping 中的authenticationIdMapping。

1. 在CMS Web Admin GUI上導航到配置> API

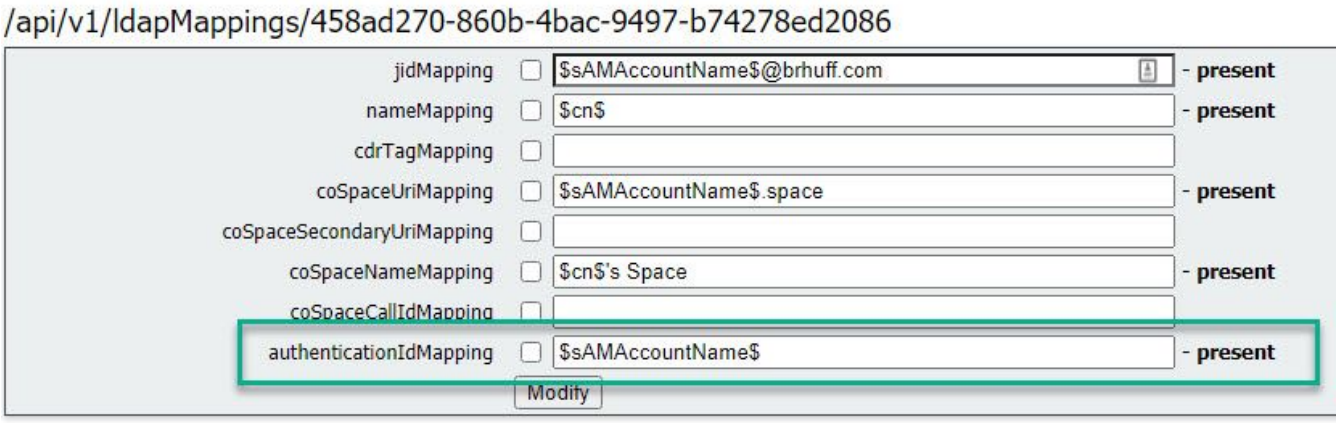
Co



2. 在api/v1/ldapMappings/<GUID-of-Ldap-Mapping>下查詢現有的（或正在建立新的）LDAP對映。



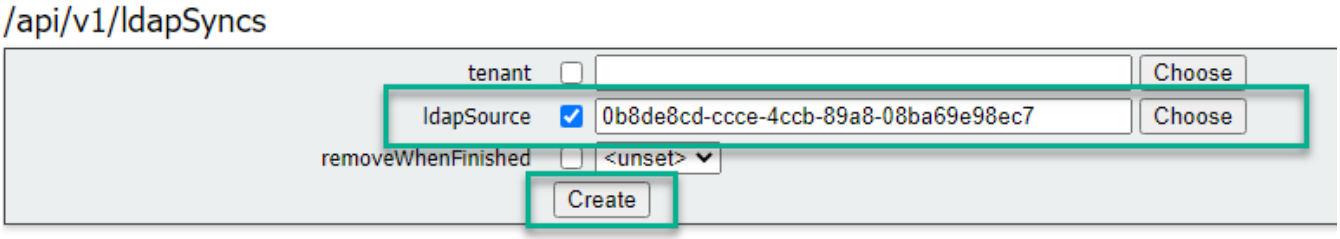
3. 在選定的ldapMapping對象中，將authenticationIdMapping更新為從IdP傳遞的LDAP屬性。在本示例中，選項$sAMAccountNameis用作LDAP屬性進行對映。



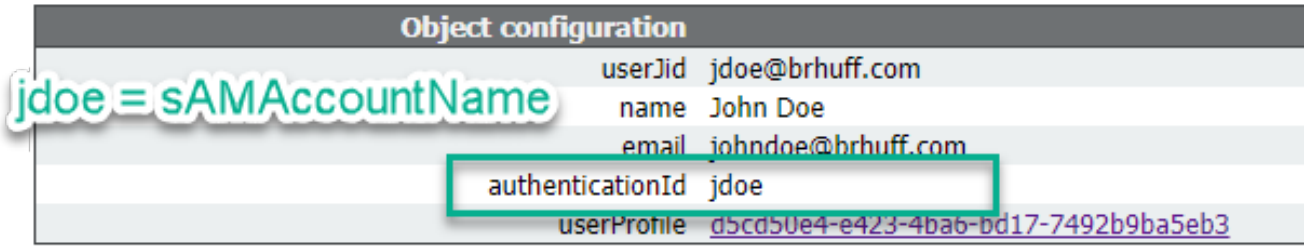
注意：callbridge/資料庫使用authenticationIdMapping來驗證SAMLResponse中IdP傳送的宣告，並為使用者提供一個JSON Web令牌(JWT)。

4. 對與最近修改的ldapMapping關聯的ldapSource執行LDAP同步：

舉例來說：



5. 完成LDAP同步後，在Configuration > api/v1/users中導航到CMS API，然後選擇已導入的使用者，並驗證是否已正確填充authenticationId。



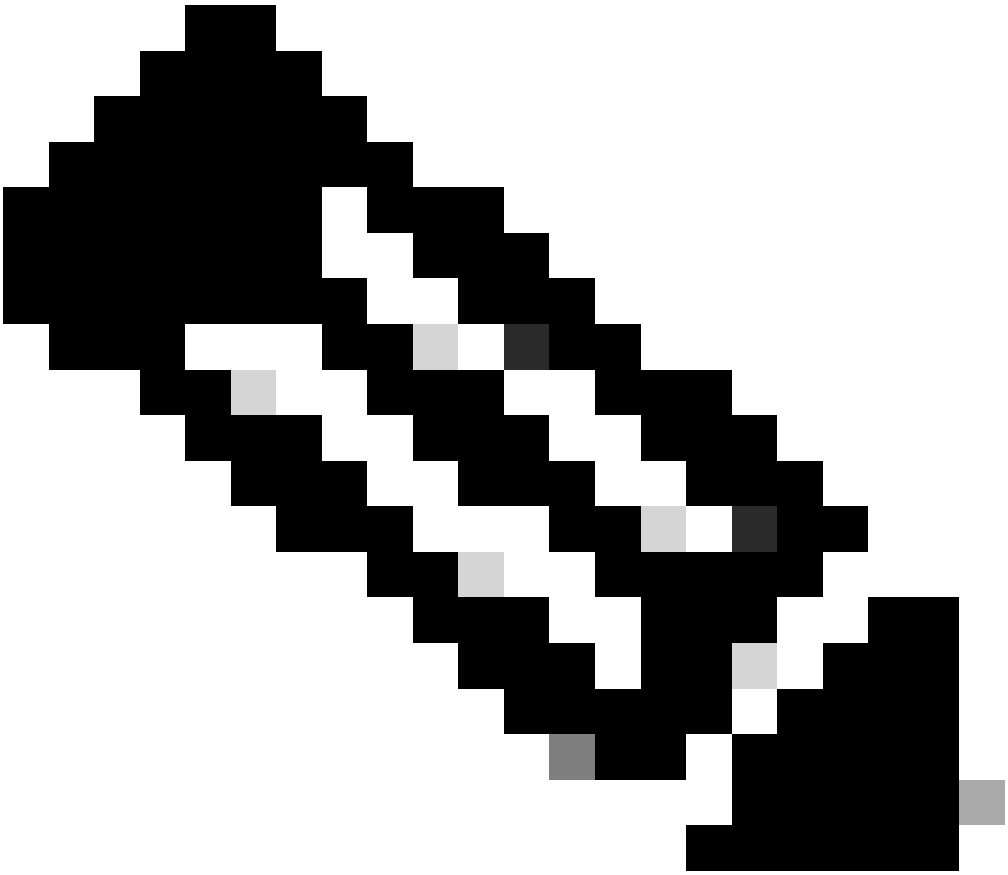
建立IdP的Webbridge中繼資料XML

Microsoft ADFS允許將後設資料XML檔案作為信賴方導入，以標識正在使用的服務提供商。建立中繼資料XML檔案的方法有幾種，但是檔案中必須存在一些屬性：

具有必要值的Webbridge中繼資料範例：

```
<?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 -這是Webbridge3伺服器地址（FQDN/主機名）和可供使用者透過瀏覽器訪問的關聯埠。



注意：如果有多個Webbridge使用單個URL，則這必須是負載均衡地址。

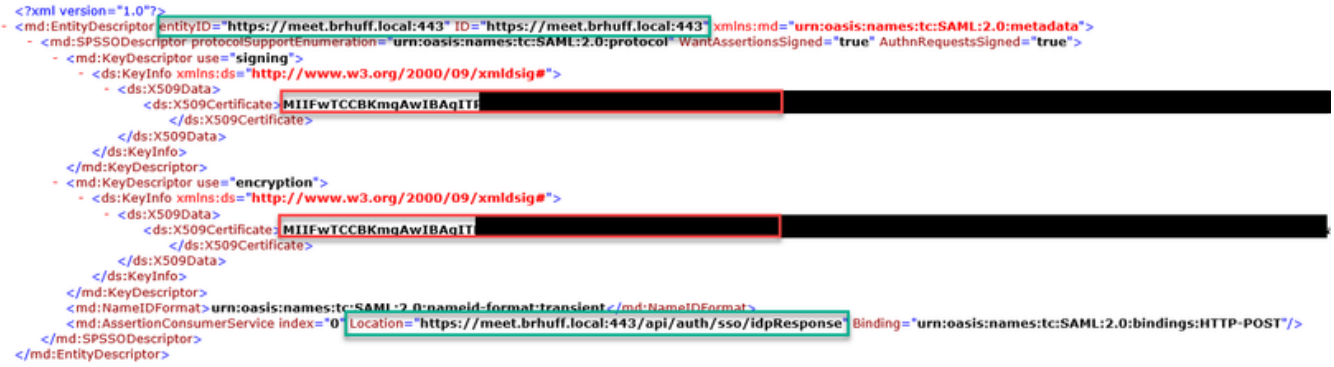
2. Location —這是Webbridge地址的HTTP-POST AssertionConsumerService的位置。這可以告知IdP在登入後重定向經過身份驗證的使用者。這必須設定為idpResponse URL：https://<WebbrdgeFQDN>：<port>/api/auth/sso/idpResponse。 例如，https://join.example.com:443/api/auth/sso/idpResponse。

3. 可選-用於簽名的公鑰- 這是用於簽名的公鑰（證書），IdP使用該公鑰驗證來自Webbridge的AuthRequest。這必須與上傳到Webbridge上的SSO捆綁包上的私鑰「sso_sign.key」匹配，以便IdP可以使用公鑰（證書）驗證簽名。您可以使用部署中的現有證書。 在文本檔案中打開證書，並將內容複製到Webbridge後設資料檔案中。 使用您的sso_xxxx.zip檔案中所使用之憑證的相符金鑰作為sso_sign.key檔案。

4. 可選-用於加密的公鑰 -這是IdP用於加密發回Webbridge的SAML資訊的公鑰（證書）。這必須與上傳到Webbridge上的SSO捆綁包上的私鑰「sso_encrypt.key」匹配，以便Webbridge可以解密IdP返回的內容。 您可以使用部署中的現有證書。 在文本檔案中打開證書，並將內容複製到Webbridge後設資料檔案中。 使用您的sso_xxxx.zip檔案中所使用之憑證的相符金鑰作為

sso_encrypt.key檔案。

使用可選公鑰（證書）資料導入IdP的Webbridge後設資料示例：

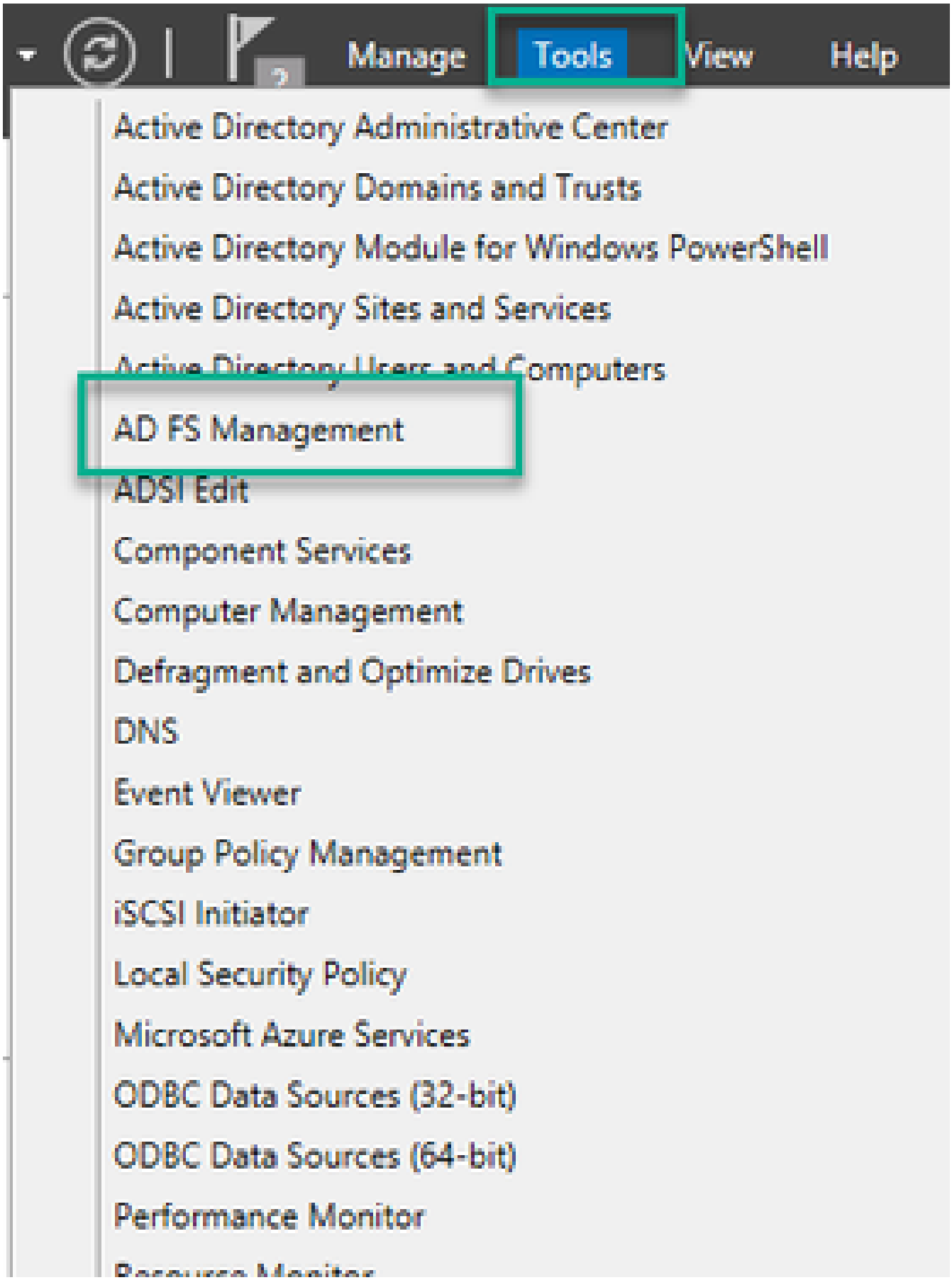


將Webbridge的中繼資料匯入辨識提供者(IdP)

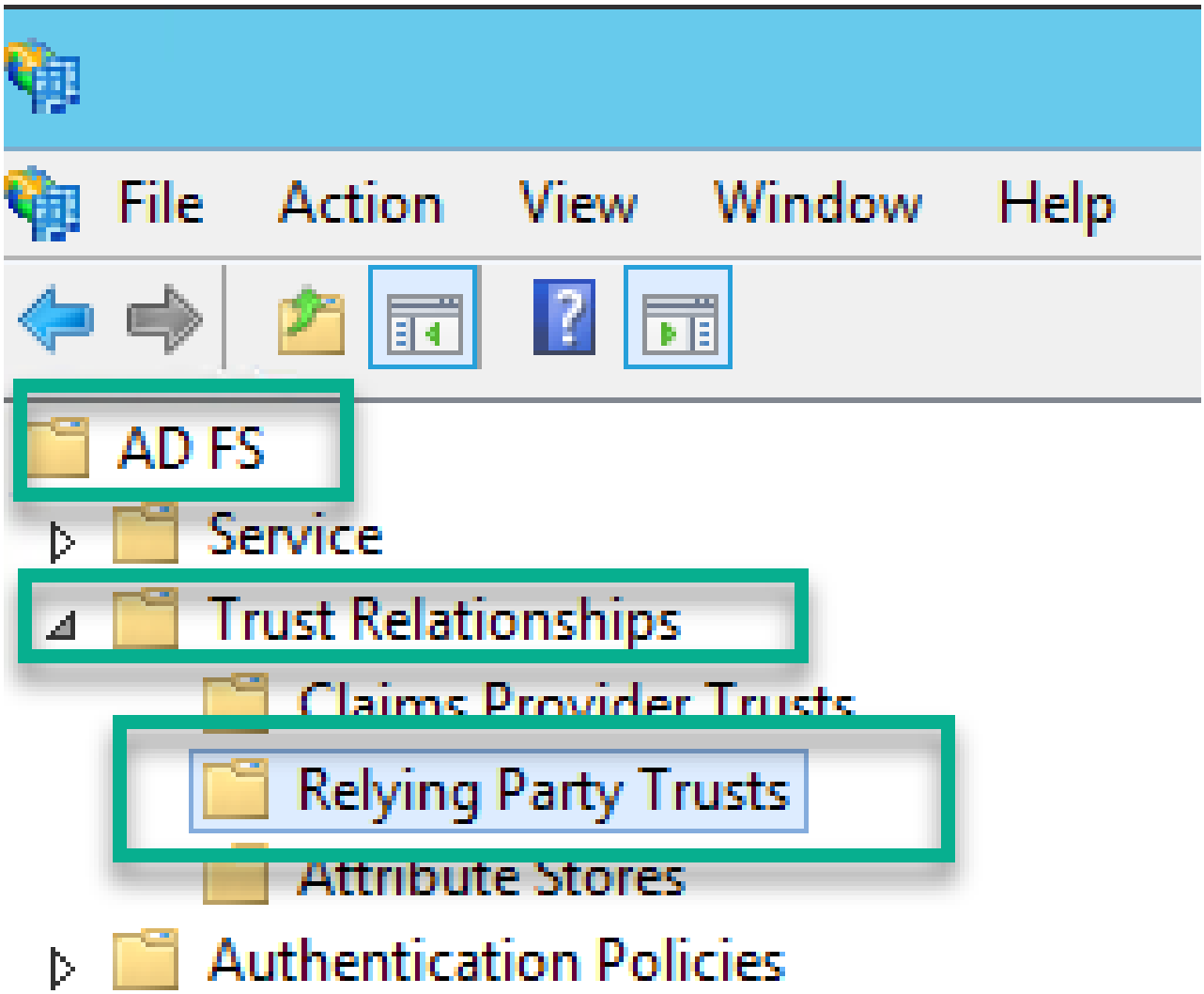
使用適當的屬性建立中繼資料XML後，檔案即可匯入Microsoft ADFS伺服器以建立信賴關係人。

1. 將遠端案頭連線到託管ADFS服務的Windows Server

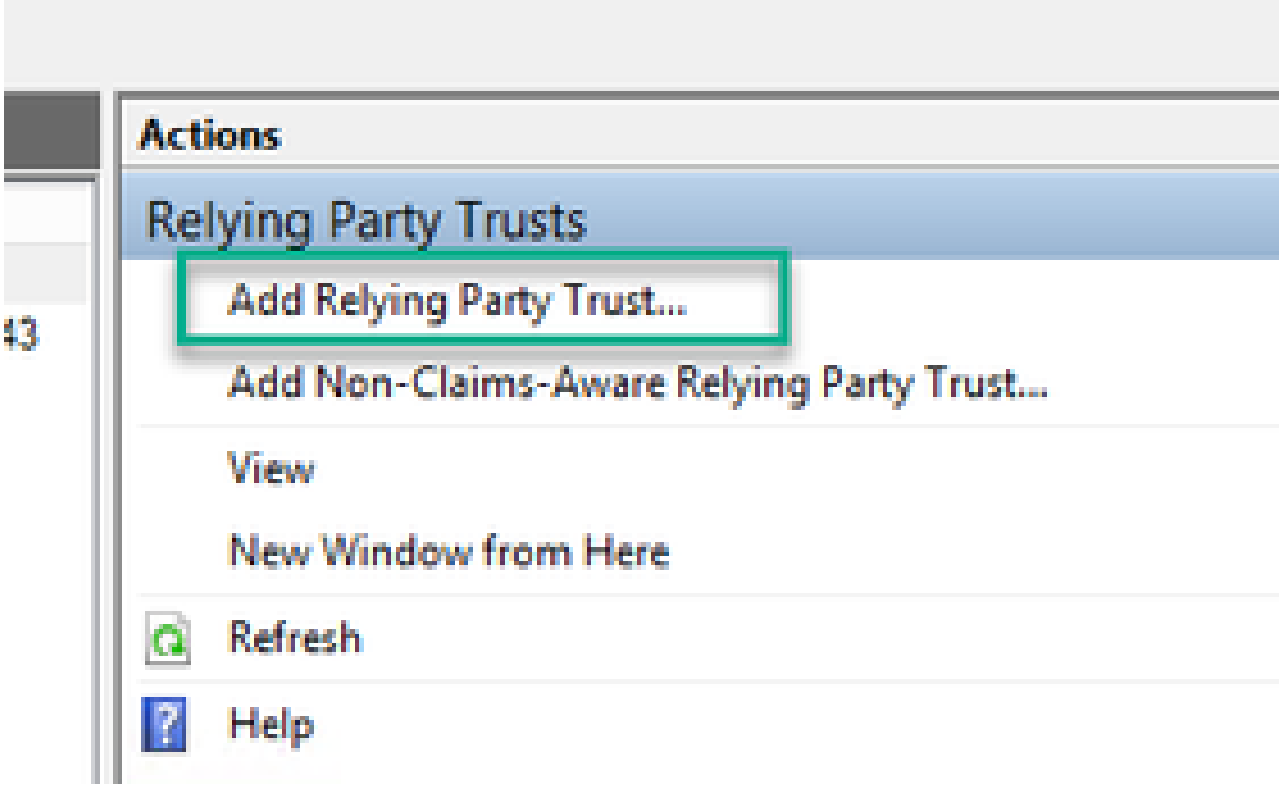
2. 開啟AD FS管理主控台，通常可透過「伺服器管理員」存取。



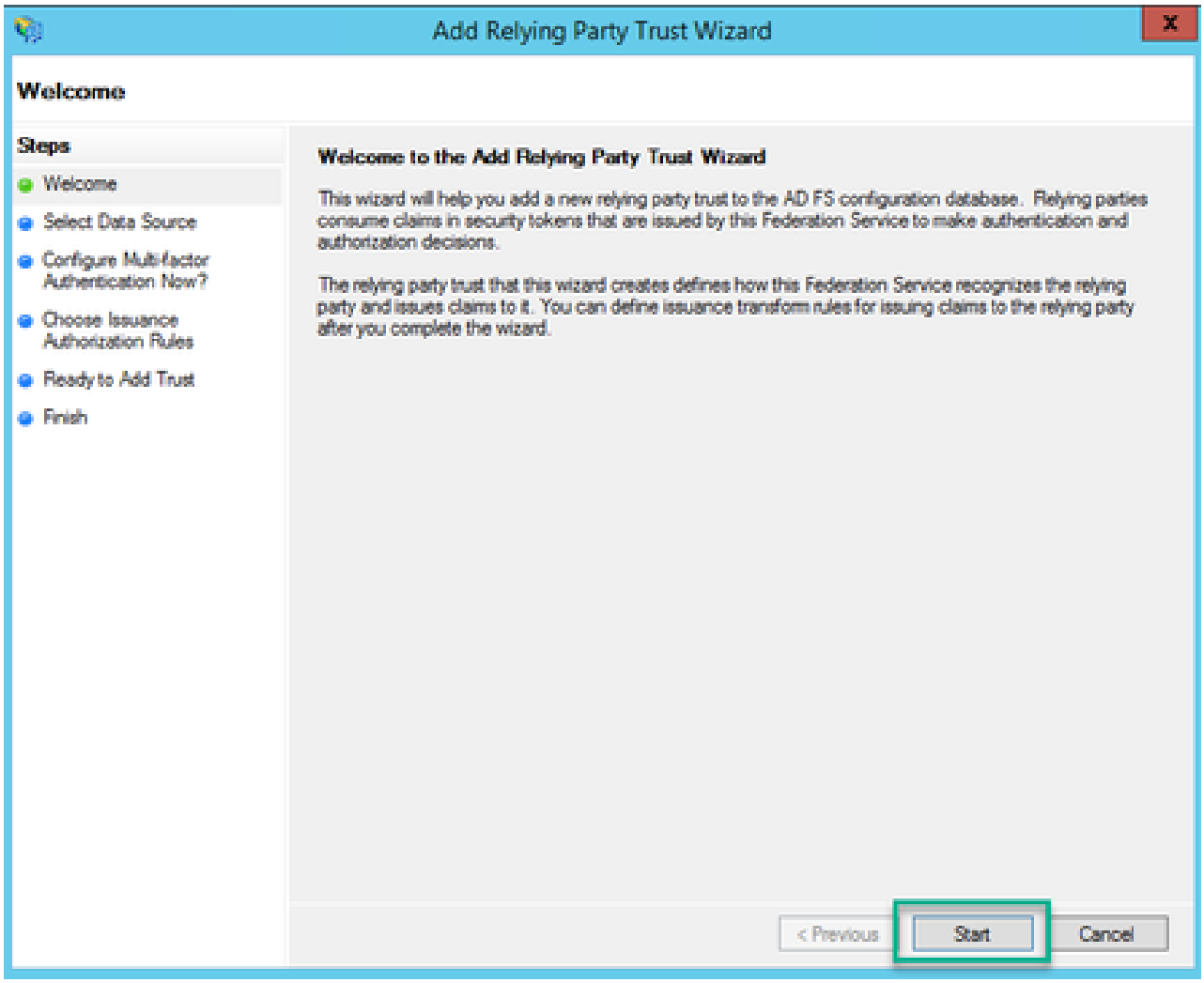
3. 進入「ADFS管理」控制檯後，在左側窗格中導航到ADFS >信任關係>信賴方信任。



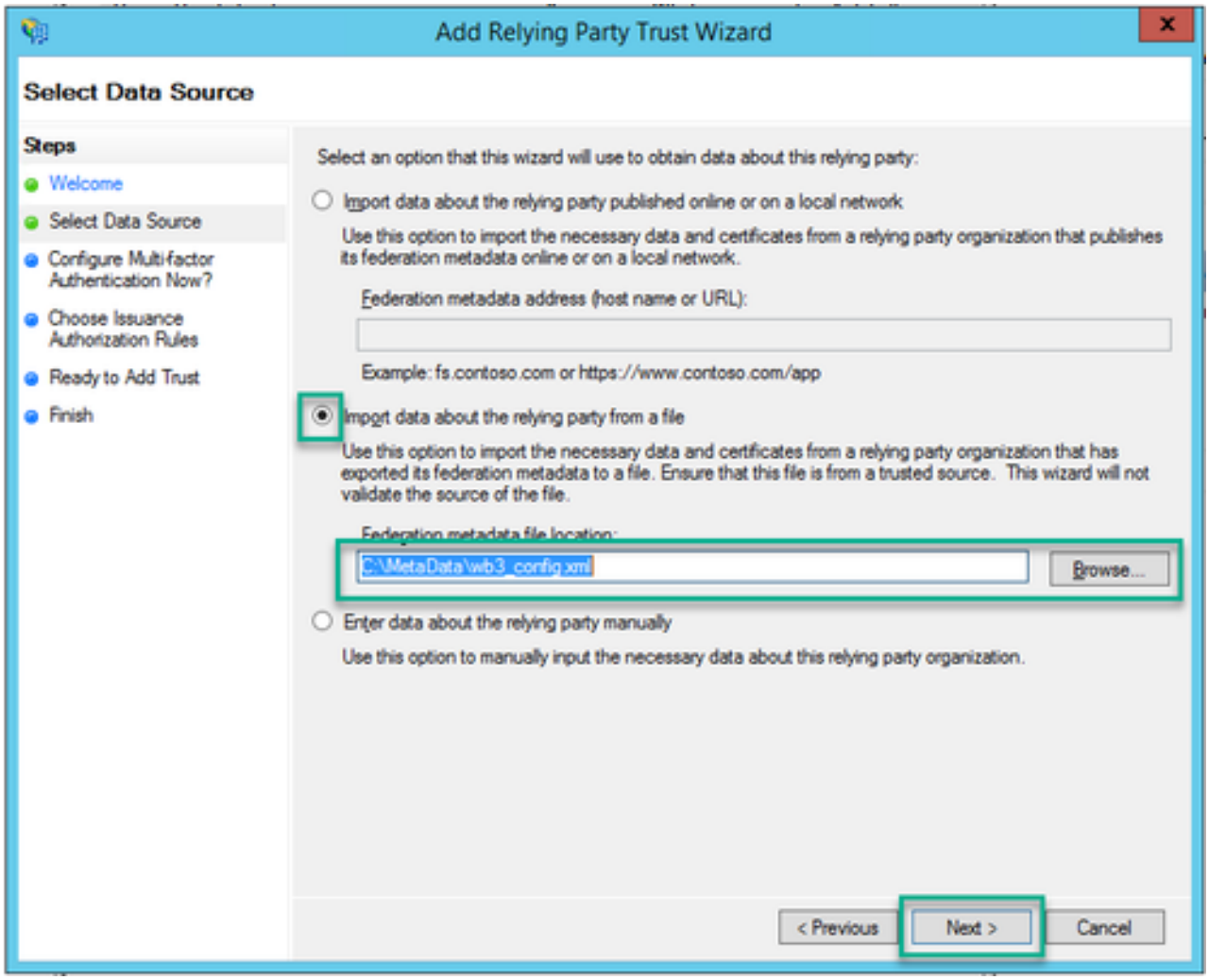
4. 在「ADFS管理控制檯」的右窗格中，選擇增加信賴方信任……選項。



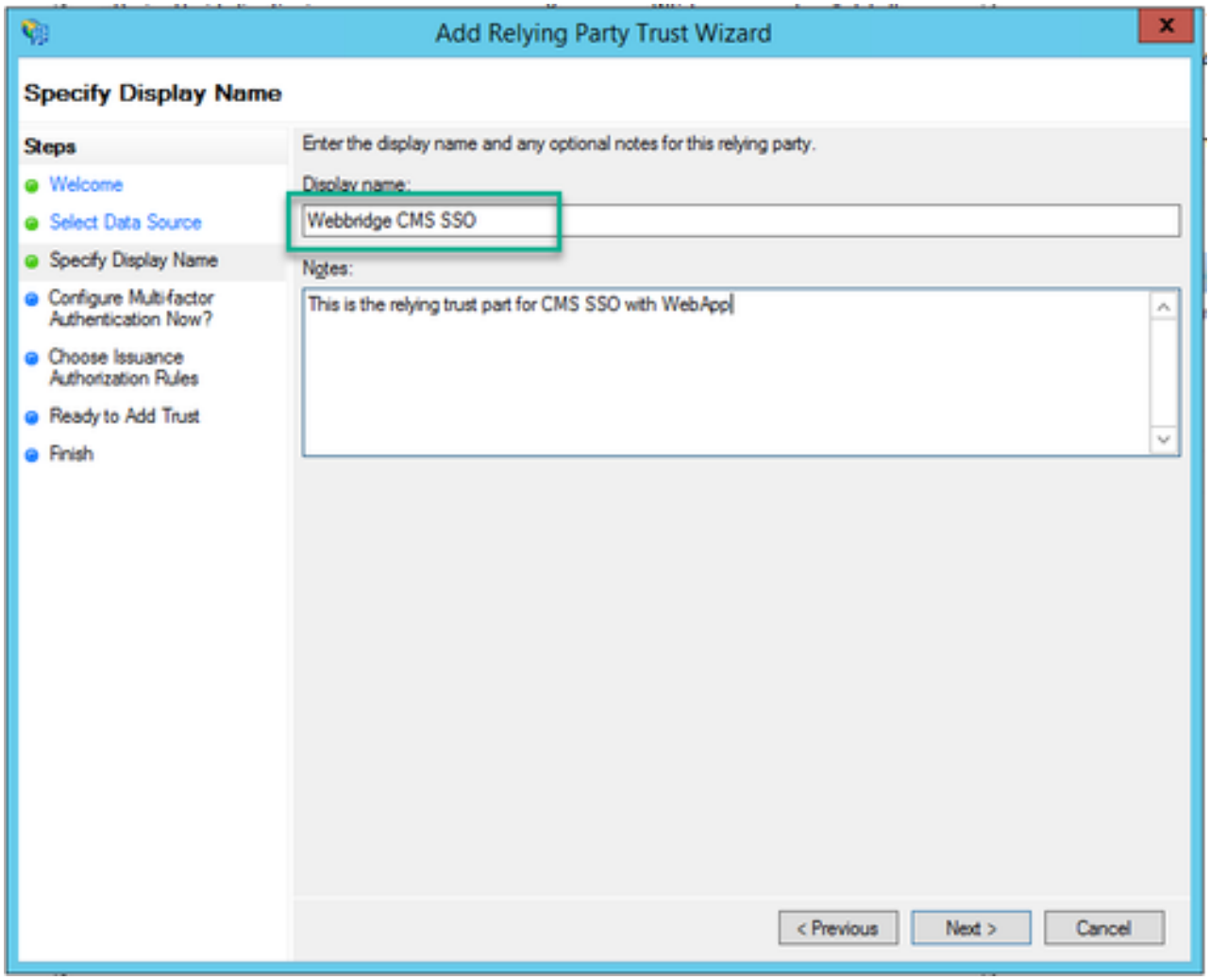
5. 進行此選擇後，將打開增加信賴方信任嚮導。選擇Start 選項。



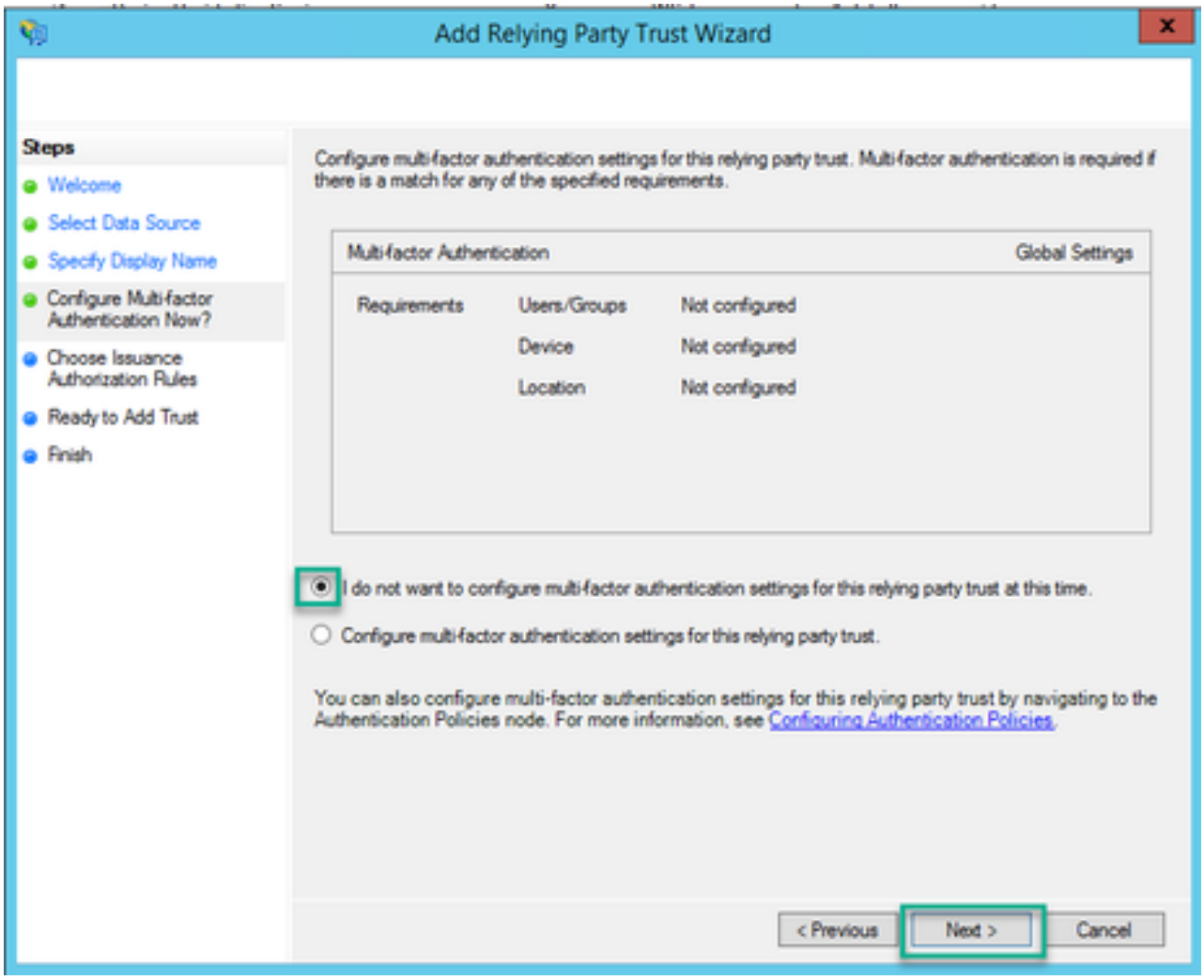
6. 在「選擇資料來源」頁上，選擇從檔案導入有關信賴方的資料單選按鈕，然後選擇瀏覽並導航到Webbridge後設資料檔案的位置。



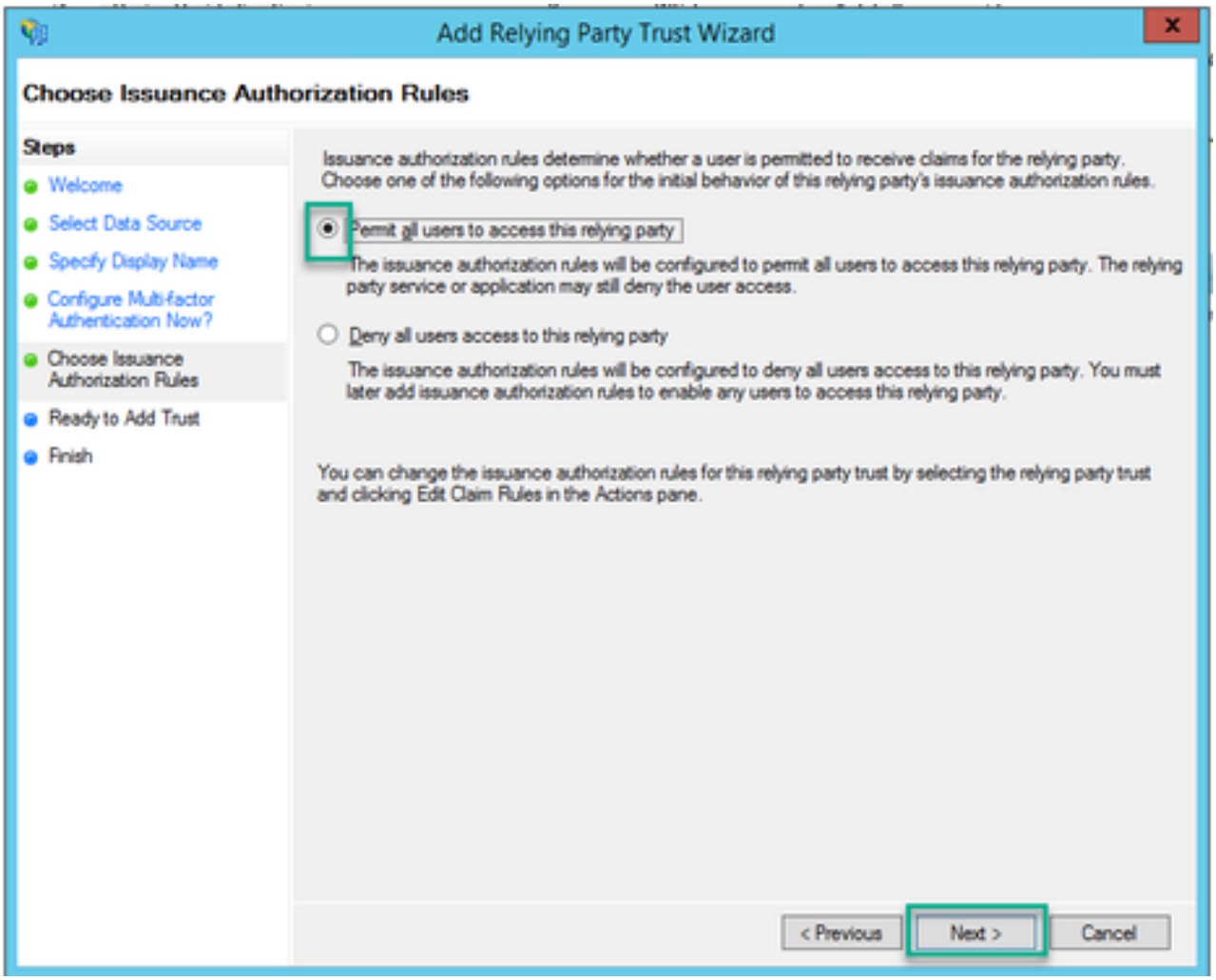
7. 在指定顯示名稱頁面上，為ADFS中的實體輸入一個名稱（顯示名稱不適用於ADFS通訊的伺服器，只是提供資訊）。



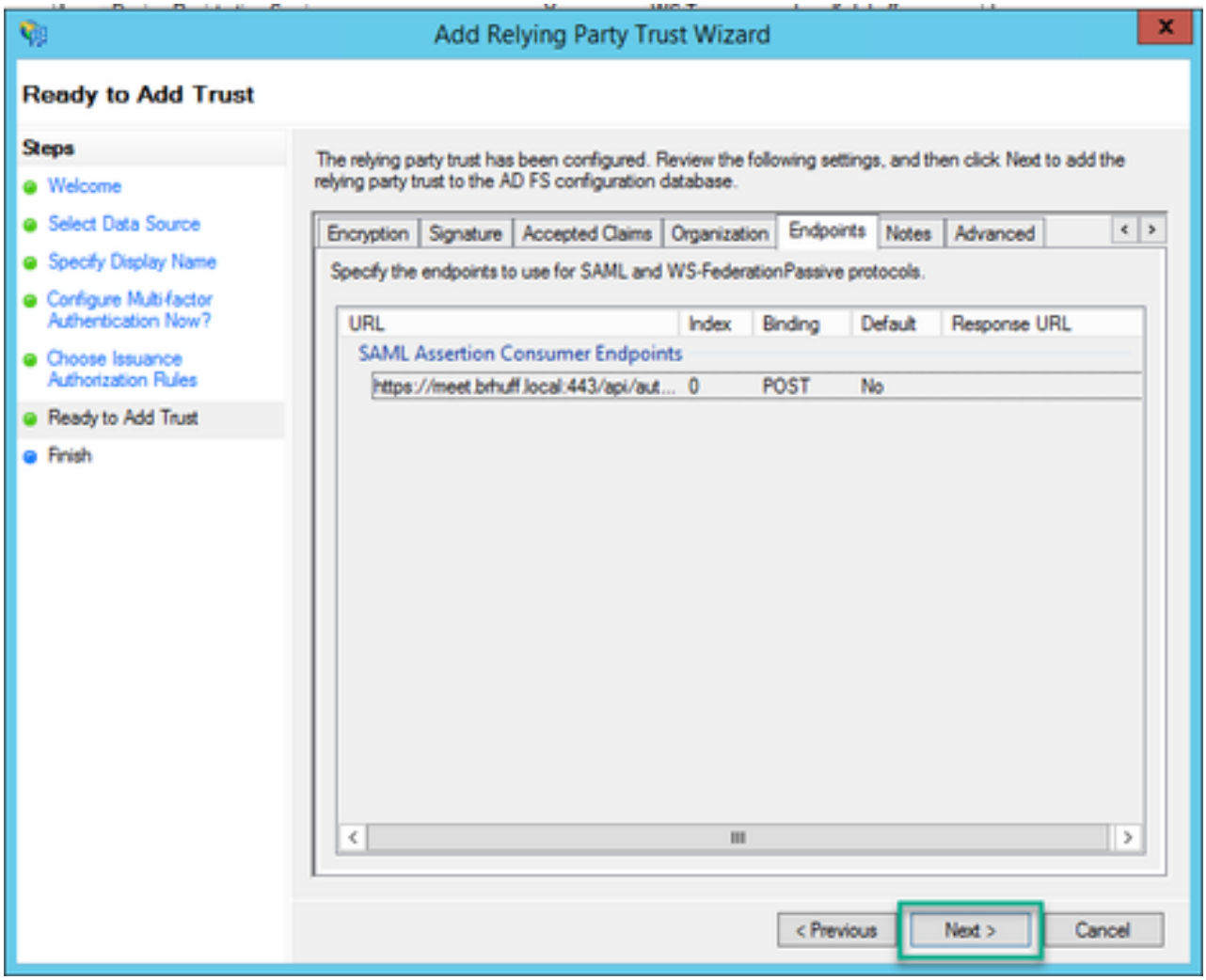
8. 在立即配置多因素身份驗證頁上，保留預設設定，然後選擇下一步。



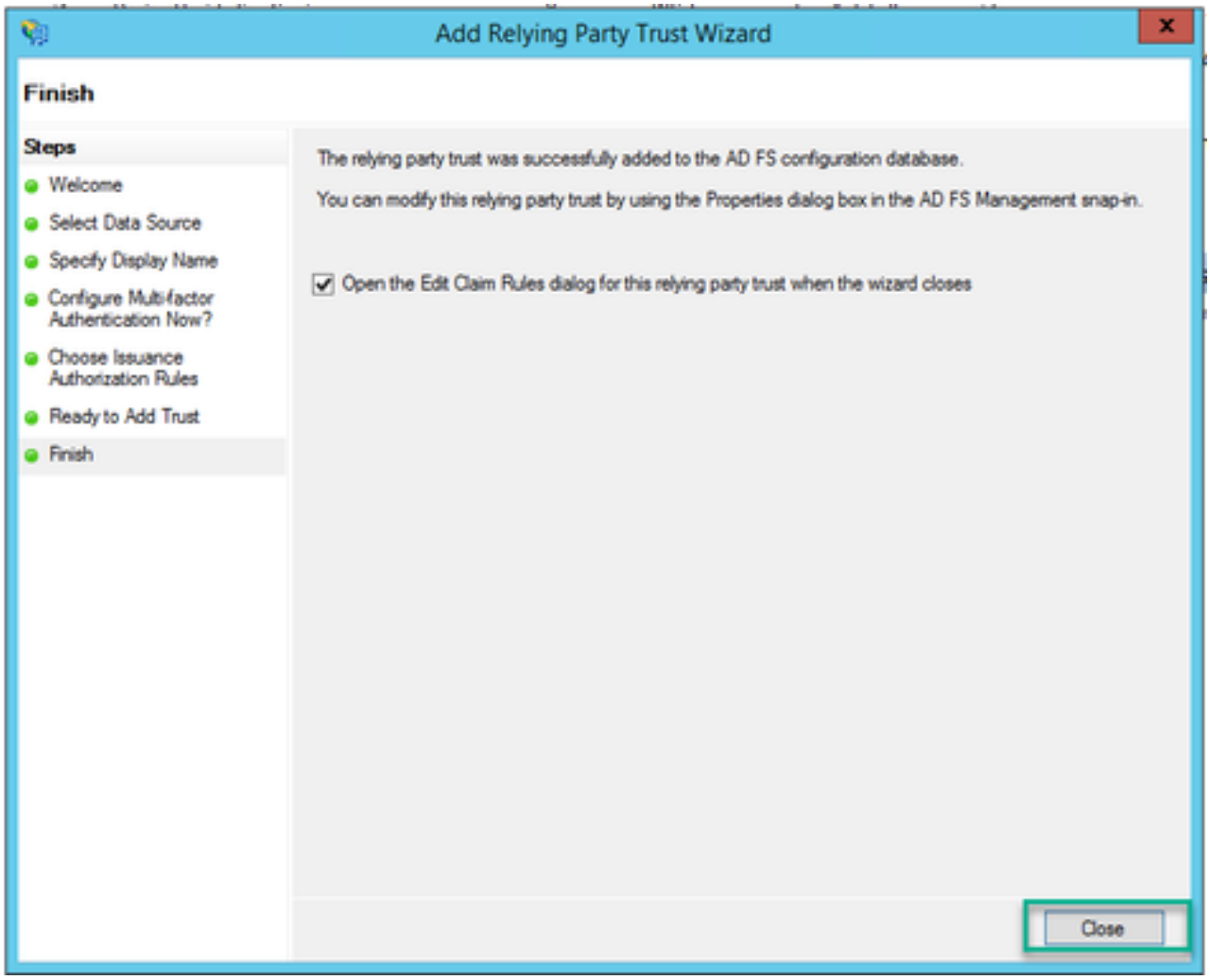
9. 在選擇頒發授權規則頁上，保留為允許所有使用者訪問此信賴方選定的狀態。



10. 在準備增加信任頁面上，可以透過頁籤檢視Webbridge的信賴信任方的導入詳細資訊。有關Webbridge服務提供商的URL詳細資訊，請檢查識別符號和終端。



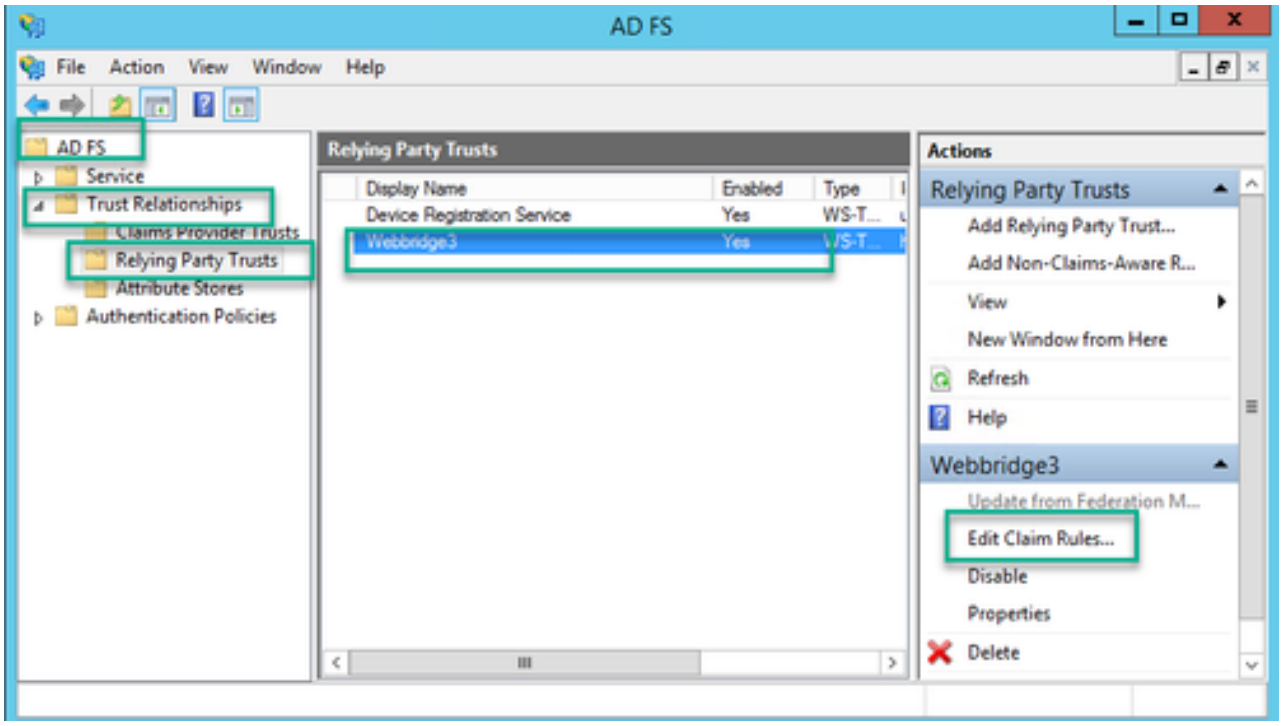
11. 在完成頁面上，選擇關閉選項以關閉嚮導並繼續編輯宣告規則。



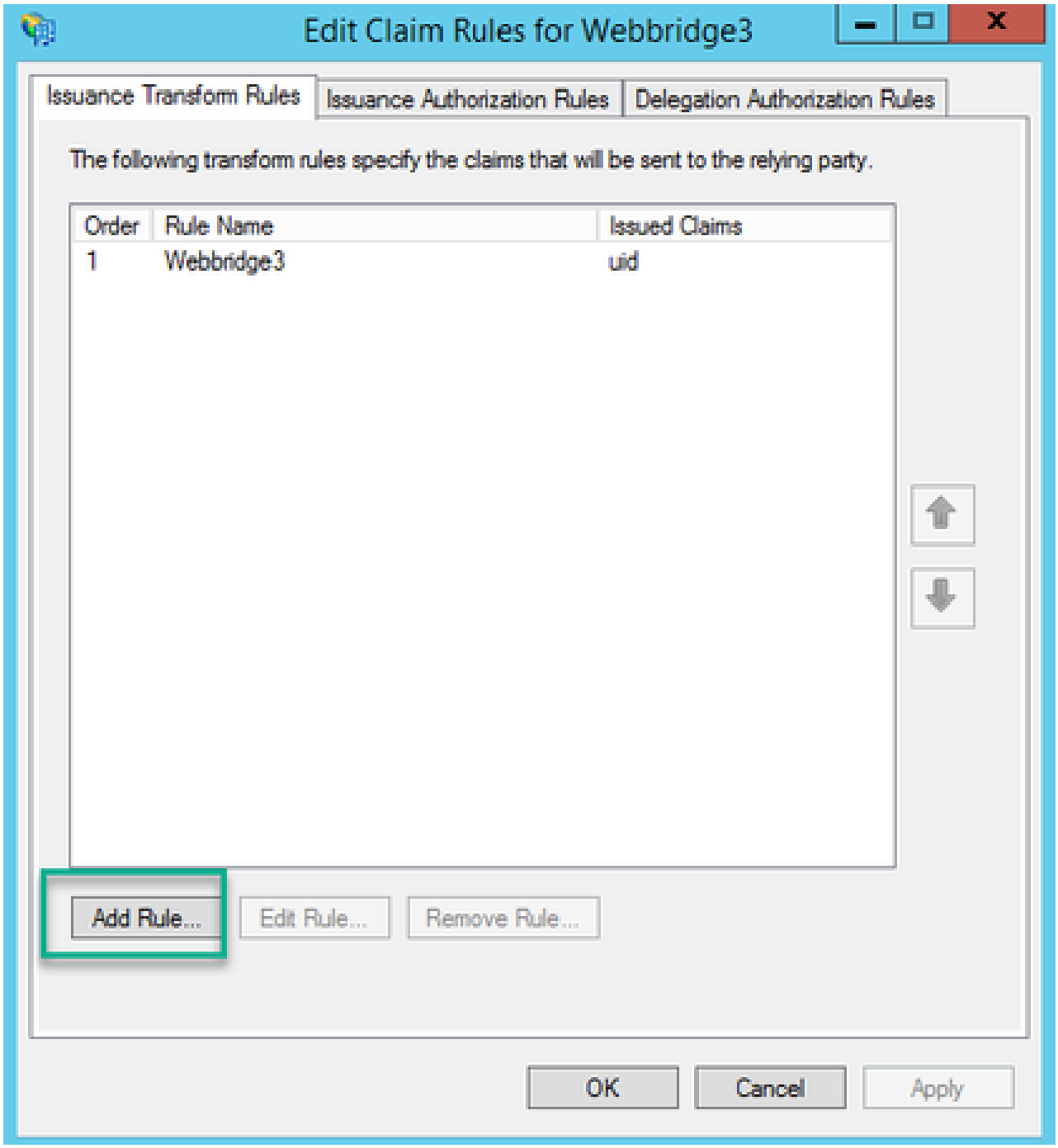
在IdP上為Webbridge服務建立宣告規則

現在已為Webbridge建立信賴方信任，可以建立宣告規則以將特定LDAP屬性與要在SAML響應中提供給Webbridge的傳出宣告型別相匹配。

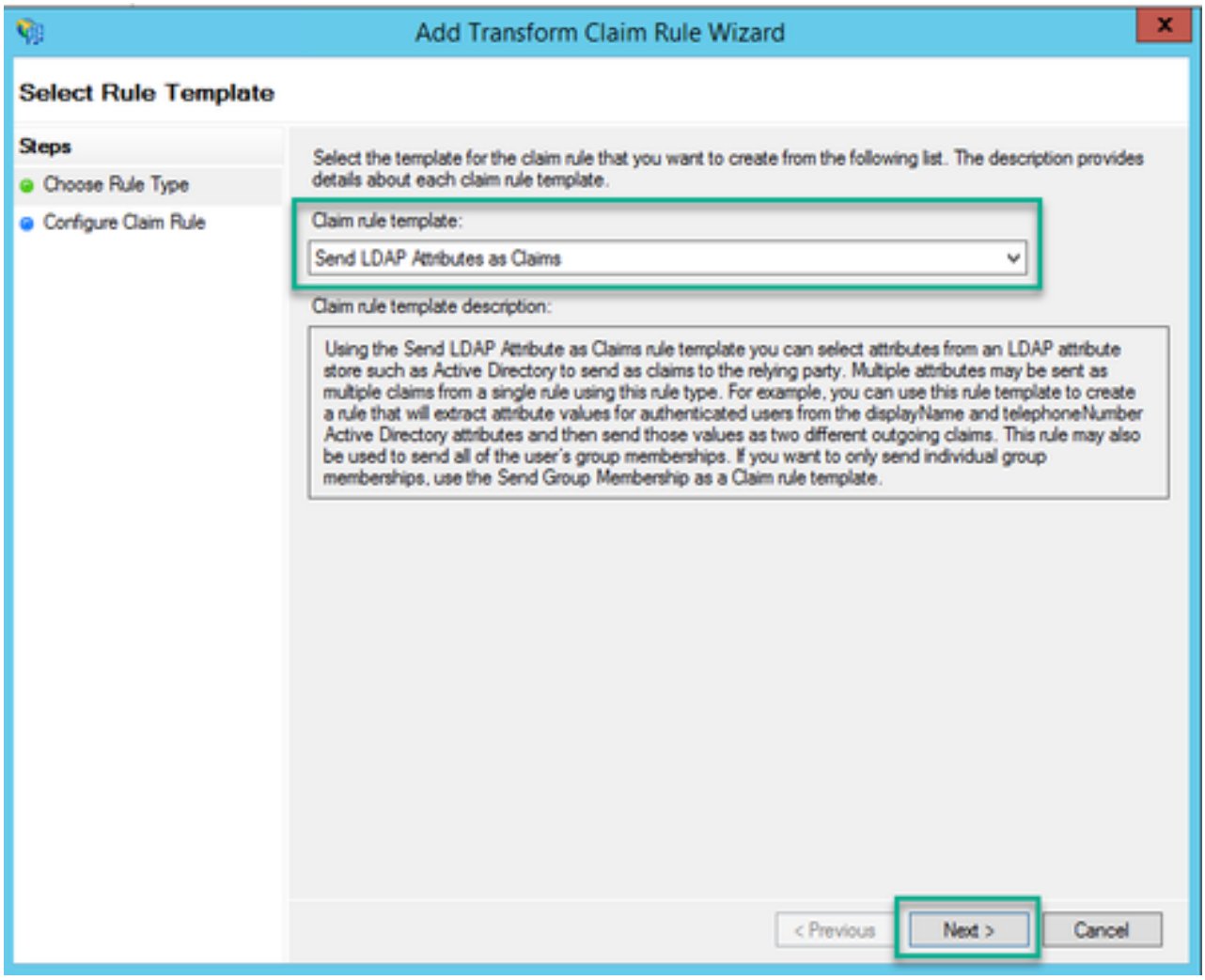
1. 在ADFS管理控制檯中，突出顯示Webbridge的信賴方信任，然後在右窗格中選擇編輯宣告規則。



2. 在「編輯<DisplayName>的領款申請規則」頁面上，選擇「增加規則.....」

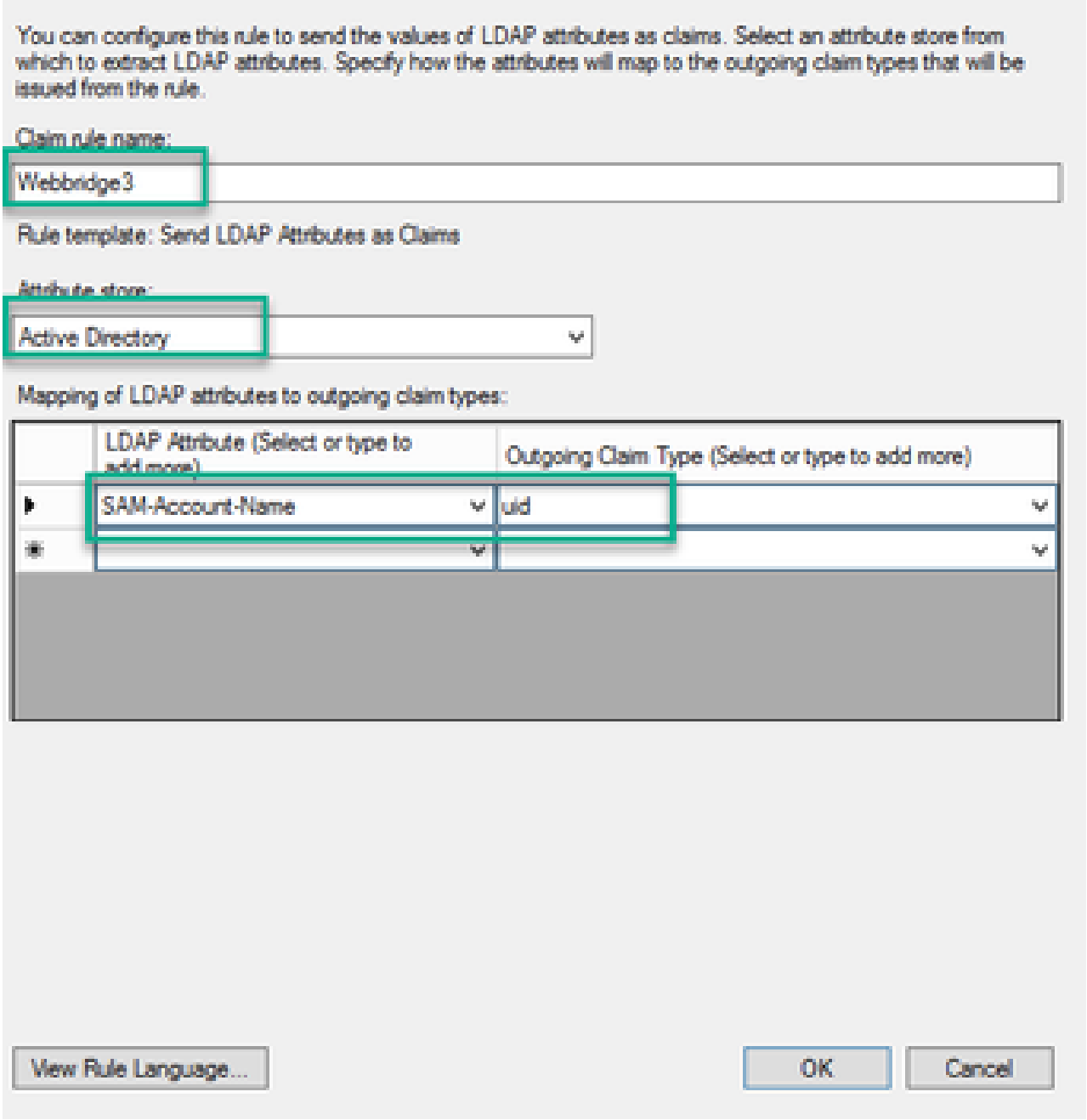


3. 在增加轉換宣告規則嚮導頁上，為「宣告規則模板」選項選擇將LDAP屬性作為宣告傳送，然後選擇下一步。



4. 在配置宣告規則頁上，使用以下值配置信賴方信任的宣告規則：

1. 宣告規則名稱=此名稱必須是指定給ADFS中規則的名稱（僅供規則參考）
2. 屬性儲存= Active Directory
3. LDAP屬性=必須與Callbridge API中的authenticationIdMapping匹配。（例如，$sAMAccountName$。）
4. 傳出宣告型別 =必須與Webbridge SSO config.json中的authenticationIdMapping匹配。（例如uid。）



為Webbridge建立SSO查扣ZIP檔案：

Webbridge引用此配置來驗證受支援的域、身份驗證對映等的SSO配置。此部分配置必須考慮以下規則：

- ZIP檔案必須以sso_開頭，且檔名帶有字首(例如sso_cmstest.zip)。
- 上傳此檔案後，Webbridge會停用基本驗證，且只有SSO可用於已上傳至的Webbridge。
- 如果使用了多個身份提供程式，則必須使用不同的命名架構上載單獨的ZIP檔案(仍然以sso_作為字首)。
- 建立zip檔案時，請務必反白並壓縮檔案內容，請勿將所需的檔案放入資料夾中並壓縮該資料

夾。

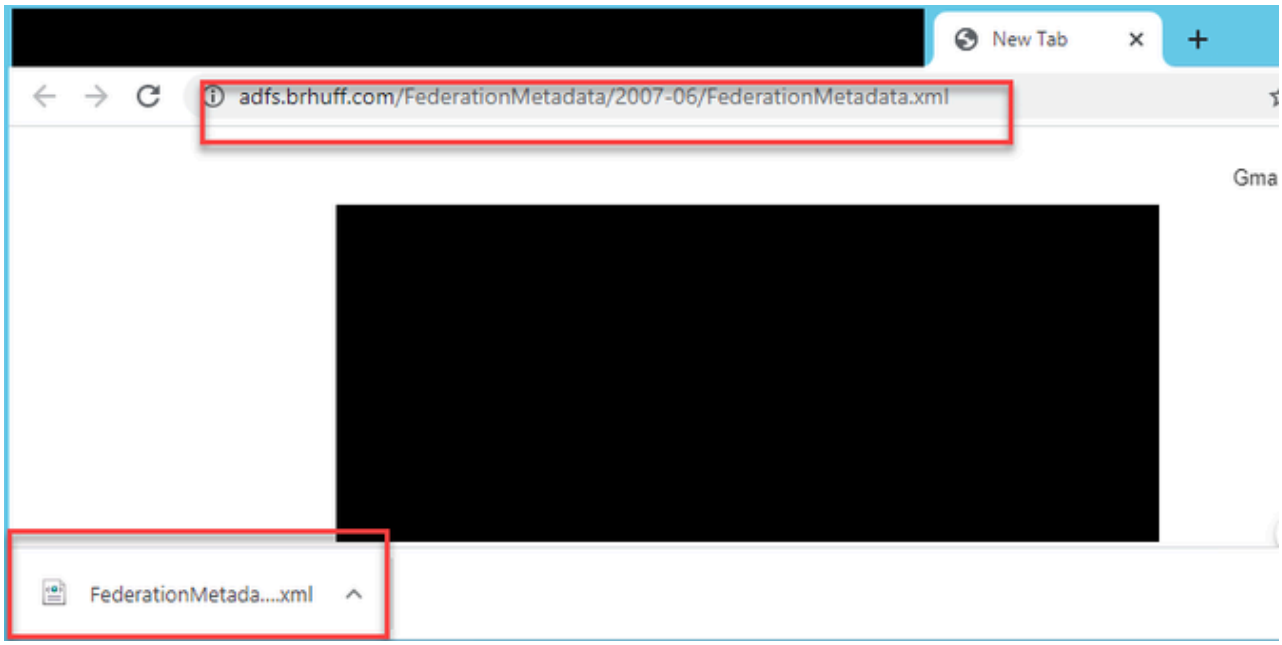
zip檔案的內容由2到4個檔案組成，視是否使用加密而定。

檔案名稱	說明	是否必要？
idp_config.xml	這是可以由idP收集的MetaData檔案。在ADFS中，可以轉到 https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml找到該域名。	是
config.json	這是JSON檔案，Webbridge使用該檔案驗證支援的域，SSO的身份驗證對映。	是
sso_sign.key	這是在辨識提供者上設定的公開簽署金鑰的私密金鑰。僅保護簽名資料所必需的	否
sso_encrypt.key	這是在辨識提供者上設定的公用加密金鑰的私密金鑰。僅用於保護加密資料	否

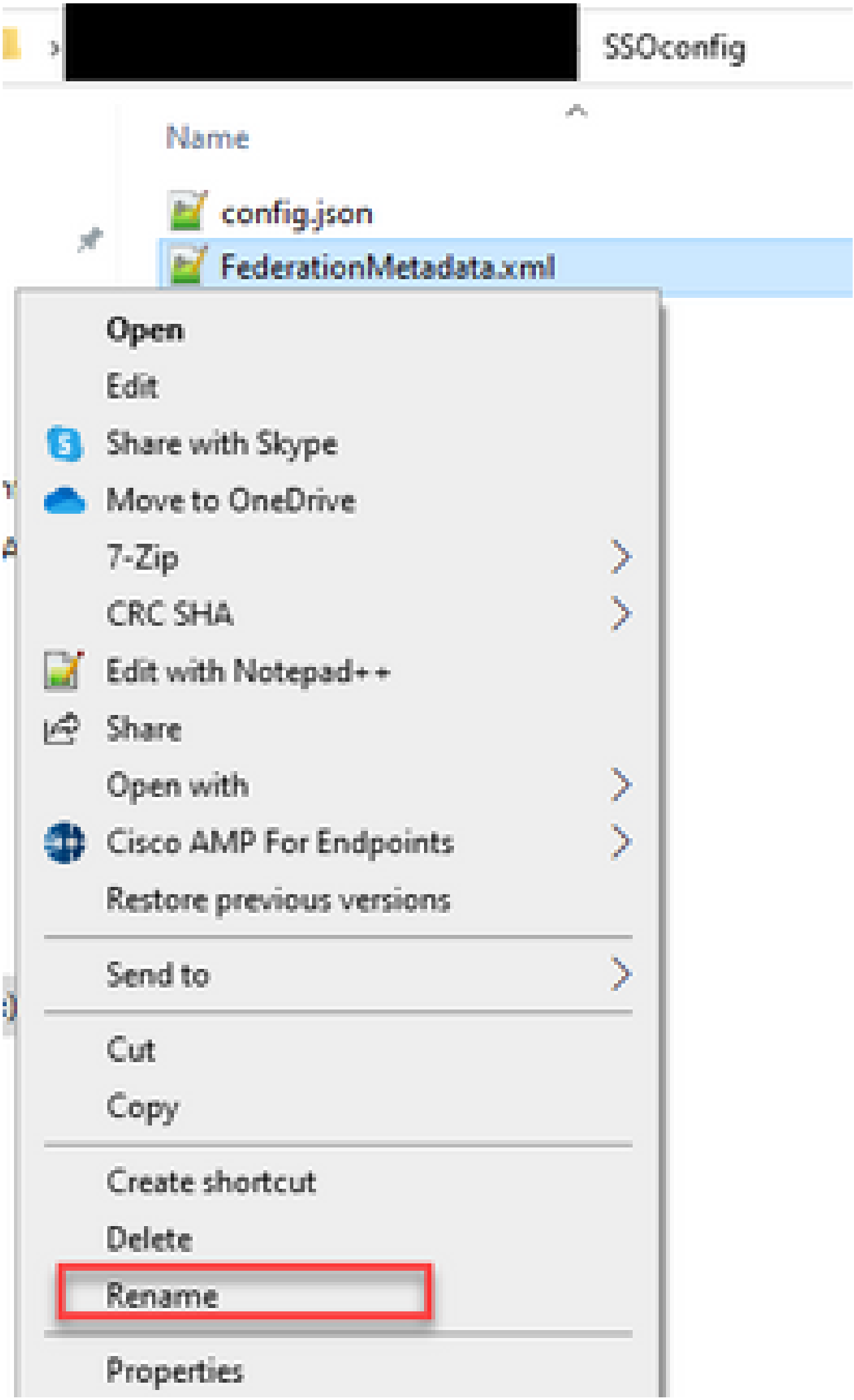
取得並設定idp_config.xml

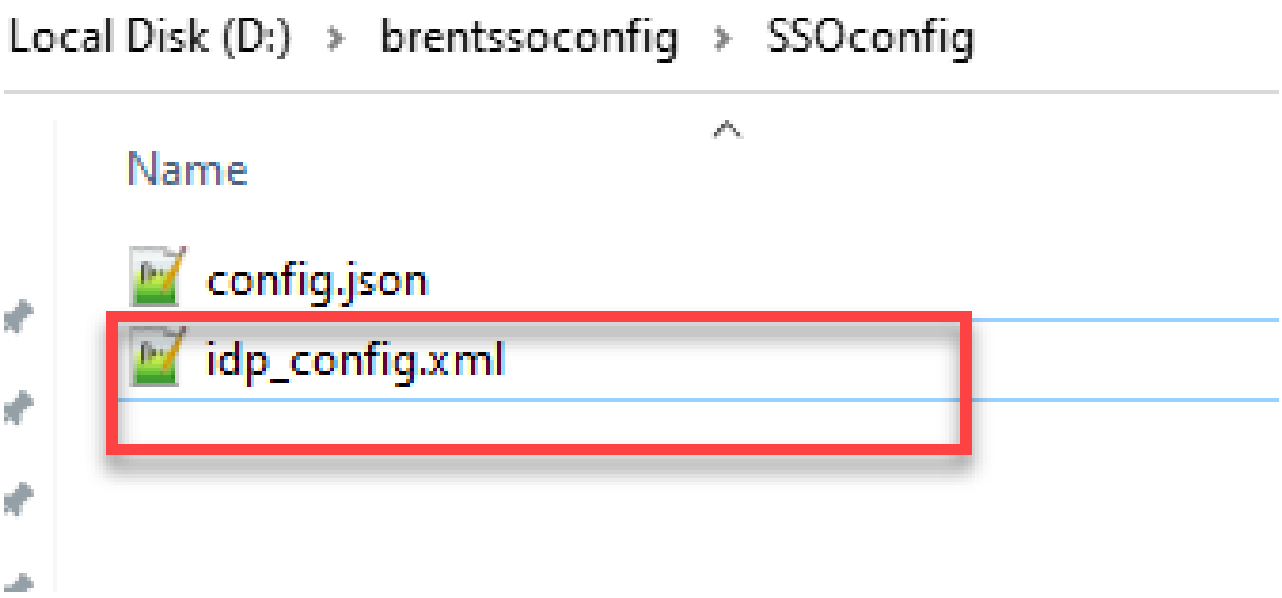
1. 在ADFS伺服器（或可以存取ADFS的位置）上，開啟Web瀏覽器。

2. 在Web瀏覽器中輸入URL：https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml（如果您在ADFS伺服器上進行本地訪問，也可以使用localhost代替FQDN）。 這會下載檔案FederationMetadata.xml。



3. 將下載的檔案複製到正在建立zip檔案的位置，並將其重新命名為idp_config.xml。

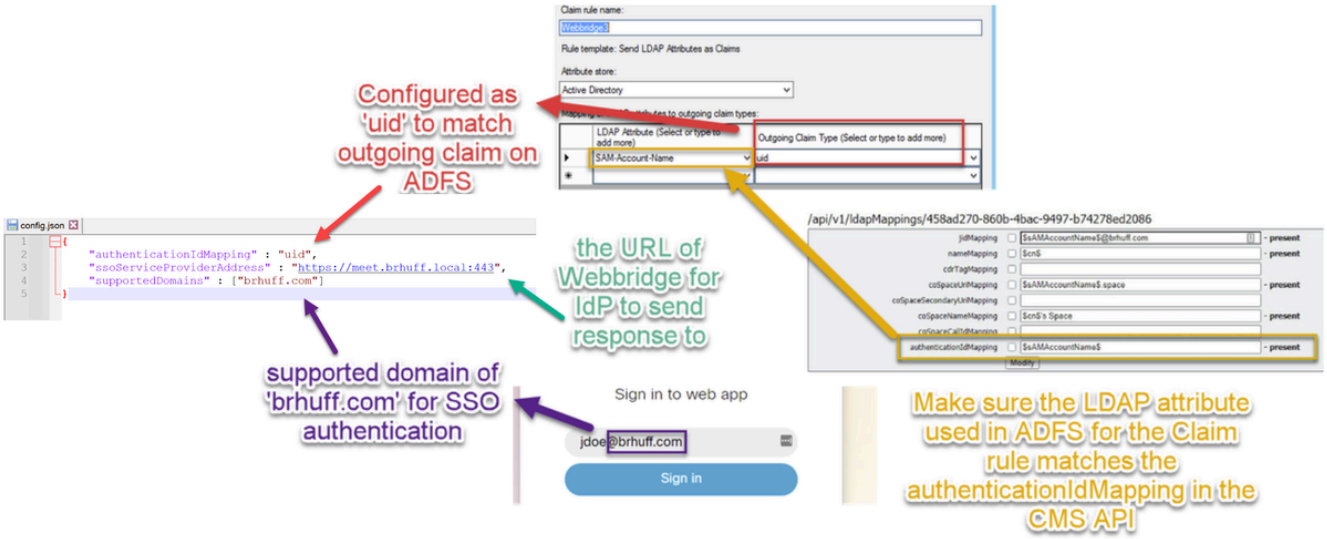

[redacted]
SSOconfig
Name
config.json
FederationMetadata.xml
Open
Edit
Share with Skype
Move to OneDrive
7-Zip
CRC SHA
Edit with Notepad++
Share
Open with
Cisco AMP For Endpoints
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties



建立包含內容的config.json檔案

config.json包含以下3個屬性，它們必須包含在方括弧{ } :

1. supportedDomains -這是根據IdP進行SSO身份驗證檢查的域的清單。多個域可以用逗號分隔。
2. authenticationIdMapping —這是作為傳出宣告規則（來自ADFS/IdP）的一部分傳回的引數。這必須與IdP上的傳出宣告型別的名稱值匹配。宣告規則。
3. ssoServiceProviderAddress -這是標識提供程式將SAML響應傳送到的FQDN URL。這必須是Webbridge FQDN。

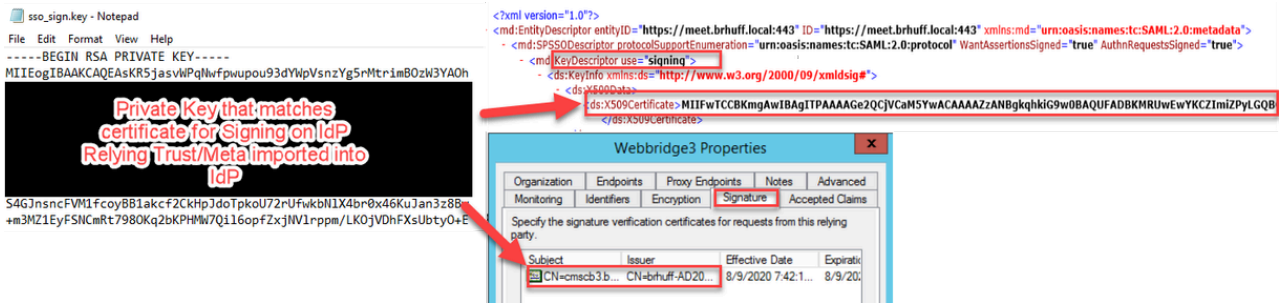


設定sso_sign.key （選擇性）

此檔案必須包含用於登入導入到IdP的Webbridge後設資料的證書的私鑰。在ADFS中導入Webbridge後設資料期間，可使用<KeyDescriptor use=signing>部分下的證書資訊填充X509Certificate，以設定用於簽名的證書。還可以在Webbridge信賴信任方的ADFS上，在屬性>簽名下檢視（和導入）此資訊。

在下一個示例中，您可以看到Callbridge證書(CN=cmscb3.brhuff.local)，該證書在導入ADFS之前已增加到Webbridge後設資料。插入到sso_sign.key中的私鑰是與cmscb3.brhuff.local證書匹配的私鑰。

這是選用組態，只有在要加密SAML回應時才需要。

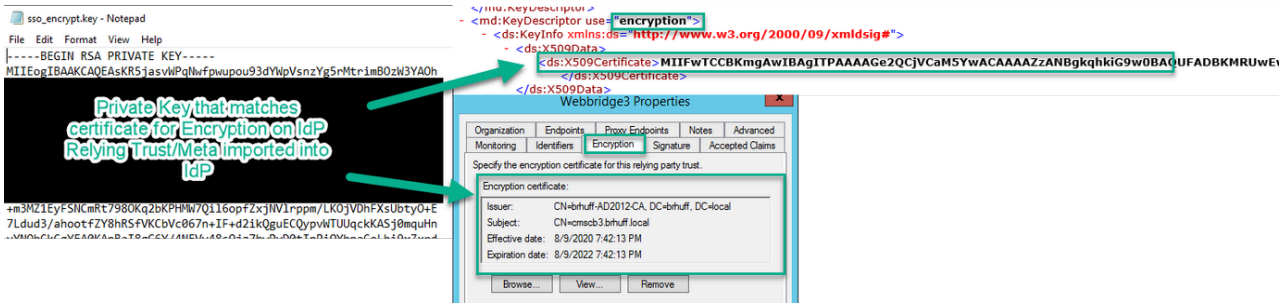


設定sso_encrypt.key（可選）

此檔案必須包含匯入IdP之Webbridge中繼資料中用於加密之憑證的私密金鑰。在ADFS中導入Webbridge後設資料期間，透過在<KeyDescriptor use=encryption>部分下使用證書資訊填充X509Certificate，可以設定用於加密的證書。還可以在Webbridge信賴方信任方的ADFS上，在屬性>加密下檢視（和導入）該金鑰。

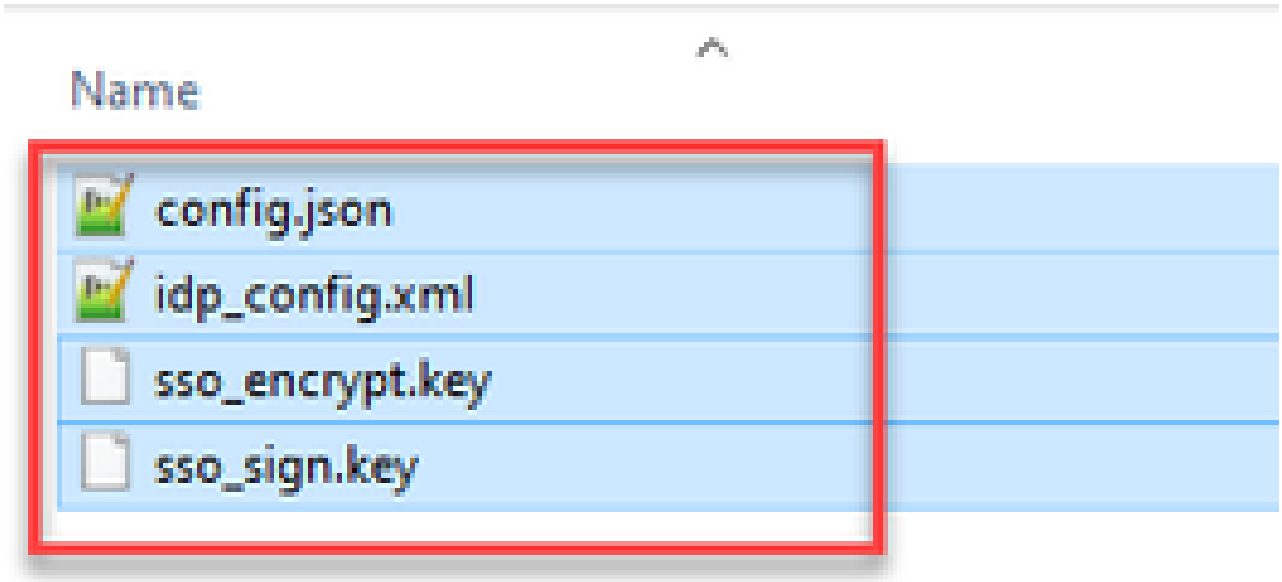
在下一個示例中，您可以看到Callbridge證書(CN=cmscb3.brhuff.local)，該證書在導入到ADFS之前已增加到Webbridge後設資料。插入「sso_encrypt.key」的私鑰與cmscb3.brhuff.local證書匹配。

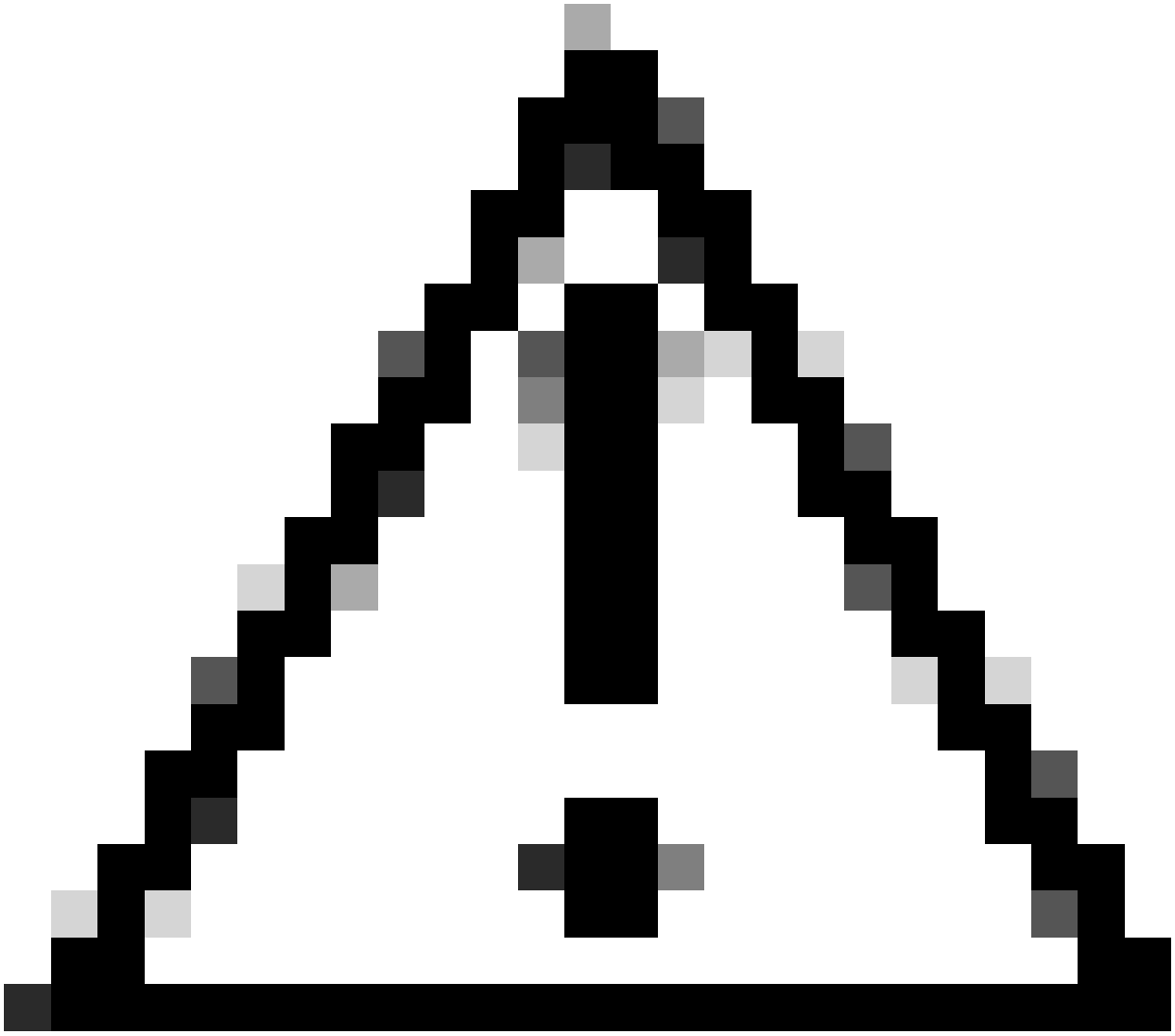
這是選用組態，只有當您打算加密SAML回應時才需要此組態。



建立SSO ZIP檔案

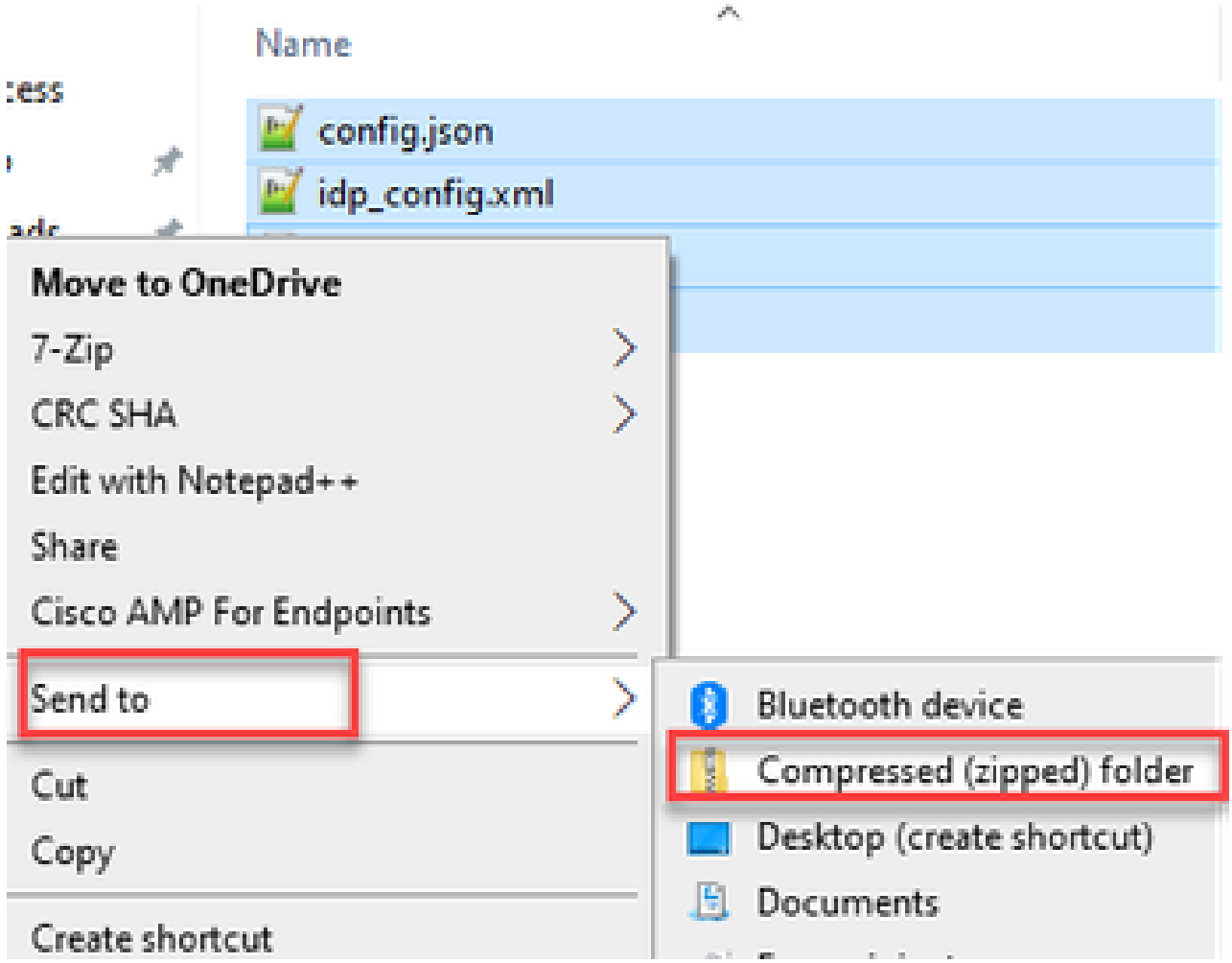
1. 突出顯示要用於SSO配置檔案的所有檔案。



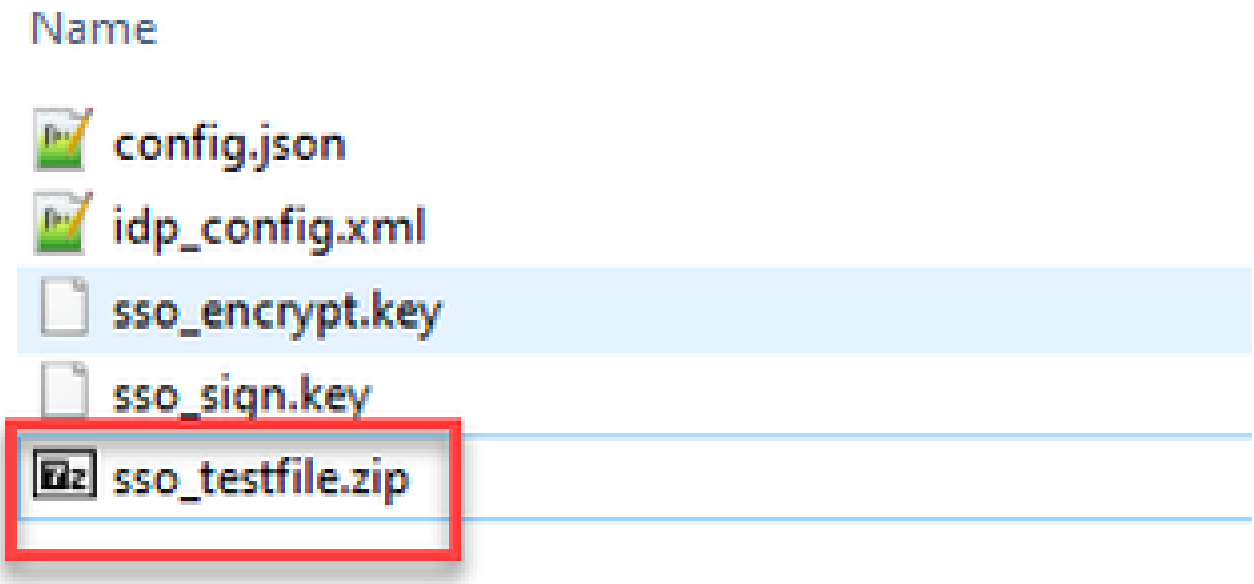


注意：請勿壓縮包含檔案的資料夾，因為這樣會導致SSO不起作用。

2. 按一下右鍵突出顯示的檔案，然後選擇「傳送到」>「壓縮(zipped)」資料夾。



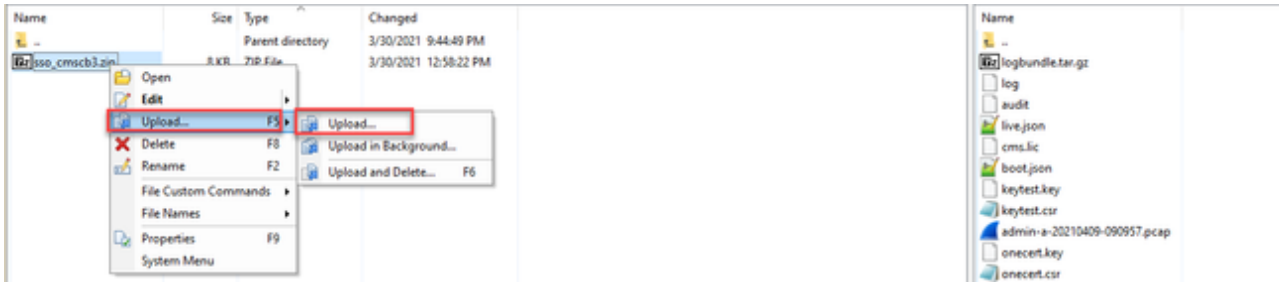
3. 檔案壓縮完成後，使用sso_字首將其重新命名為所需名稱：



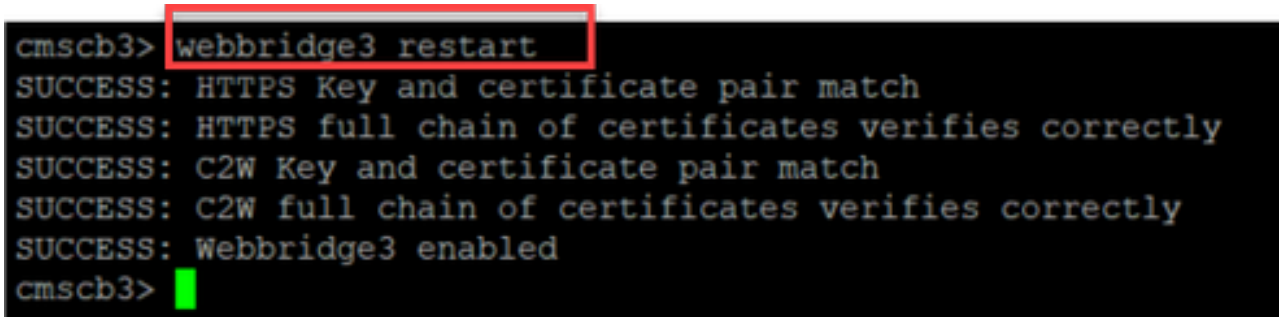
將SSO Zip檔案上傳到Webbridge

開啟SFTP/SCP使用者端（在本範例中使用的是WinSCP），然後連線到裝載Webbridge3的伺服器。

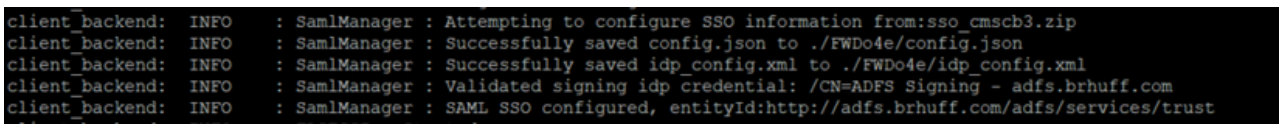
1. 在左窗格中，切換作業選項至SSO Zip檔案所在的位置，然後按一下滑鼠右鍵選取「上傳」或拖放檔案。



2. 一旦檔案完全上載到Webbridge3伺服器，打開SSH會話並運行webbridge3 restart 命令。



3. 在系統日誌中，這些消息表明SSO啟用成功：



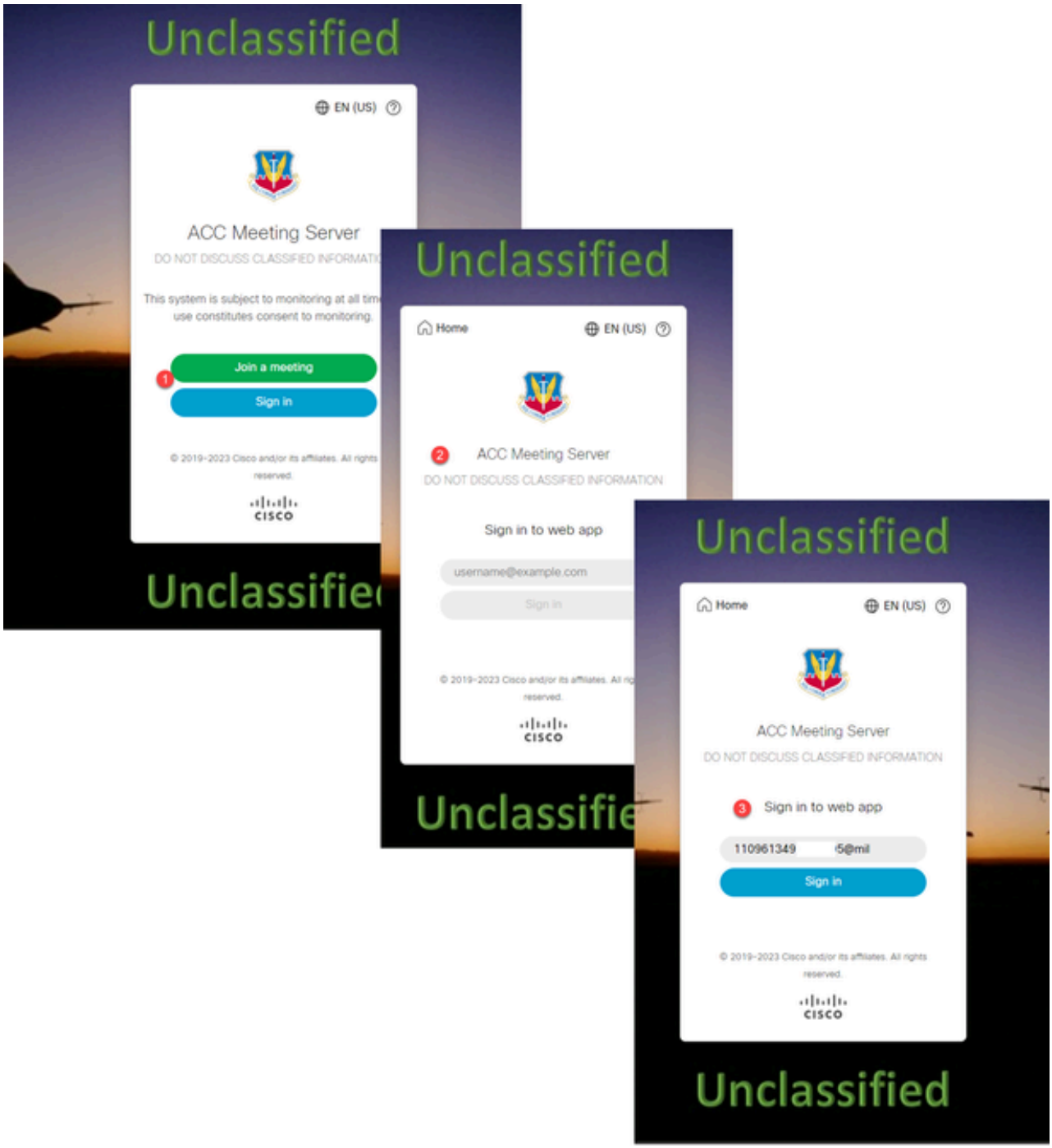
通用存取卡(CAC)

通用訪問卡(CAC)是一種智慧卡，可作為現役軍事人員、國防部文職人員和合格承包商人員的標準標識。

以下是使用CAC卡使用者的整個登入過程：

1. 打開PC，並粘入CAC卡
2. 登入（有時選擇證書），然後輸入Pin
3. 開啟瀏覽器
4. 導航到加入URL並檢視加入會議或登入選項
5. 登入：輸入配置為jidMapping的使用者名稱，Active Directory需要透過CAC登入
6. 點選登入
7. ADFS頁面會短暫顯示並自動移入

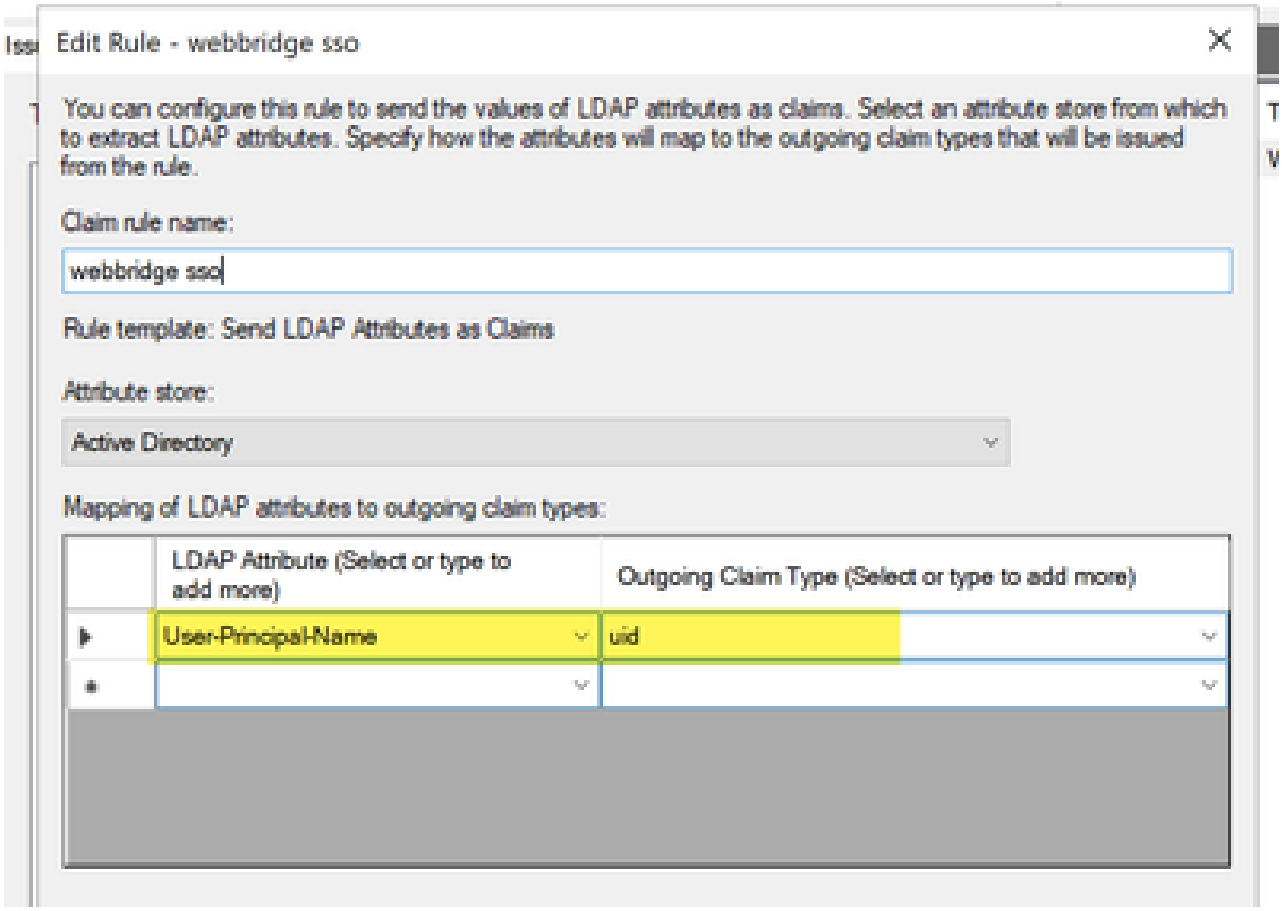
8. 使用者將在此時登入



在Ldapmapping中配置jidMapping（這是使用者登入名），與ADFS用於CAC卡的配置相同。$userPrincipalName$例如（區分大小寫）

另外，請為authenticationIdMapping設定相同的LDAP屬性，以與ADFS中的宣告規則中使用的屬性匹配。

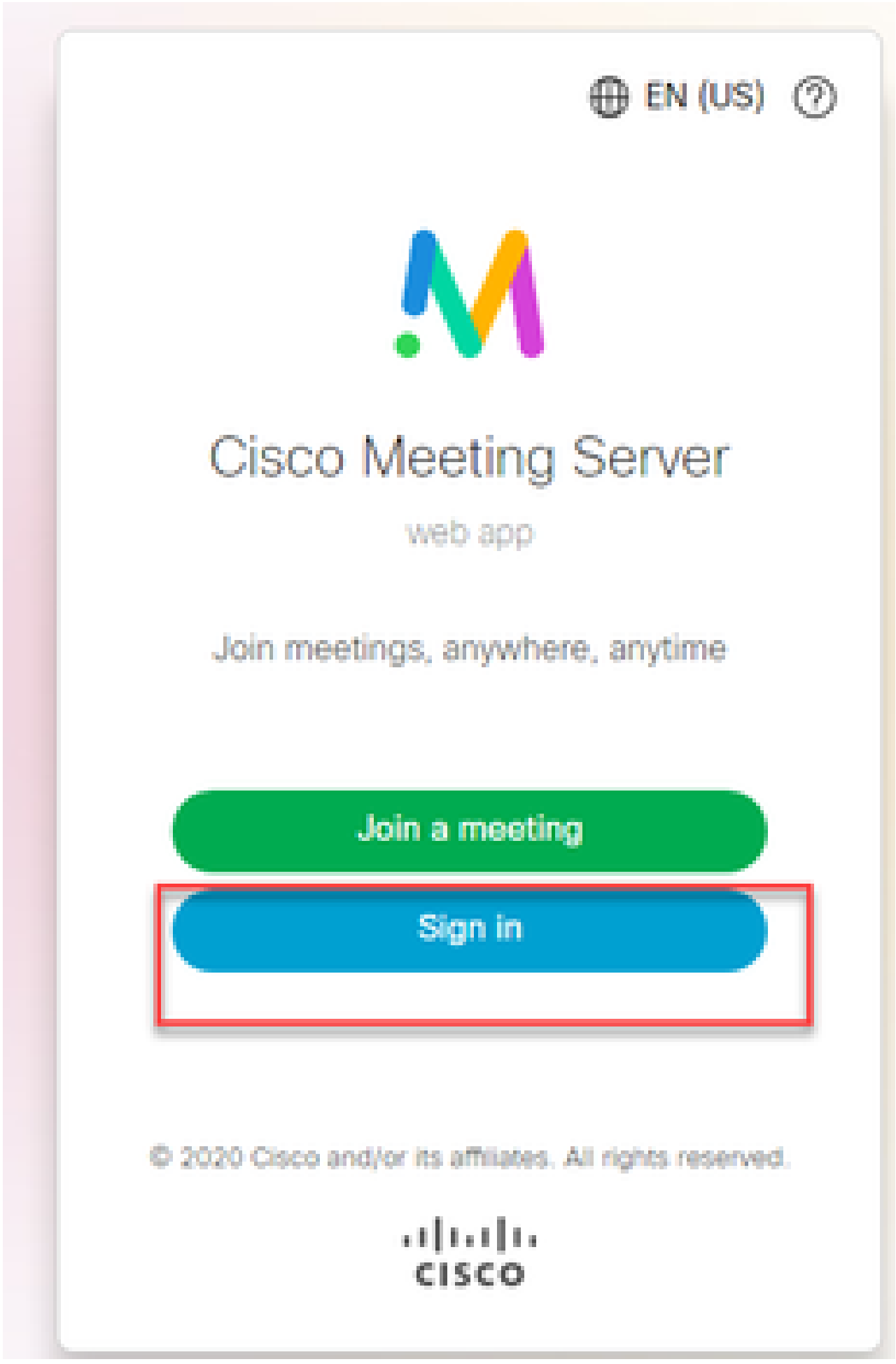
在這裡，宣告規則顯示它將將$userPrincipalName$作為UID傳送回CMS。



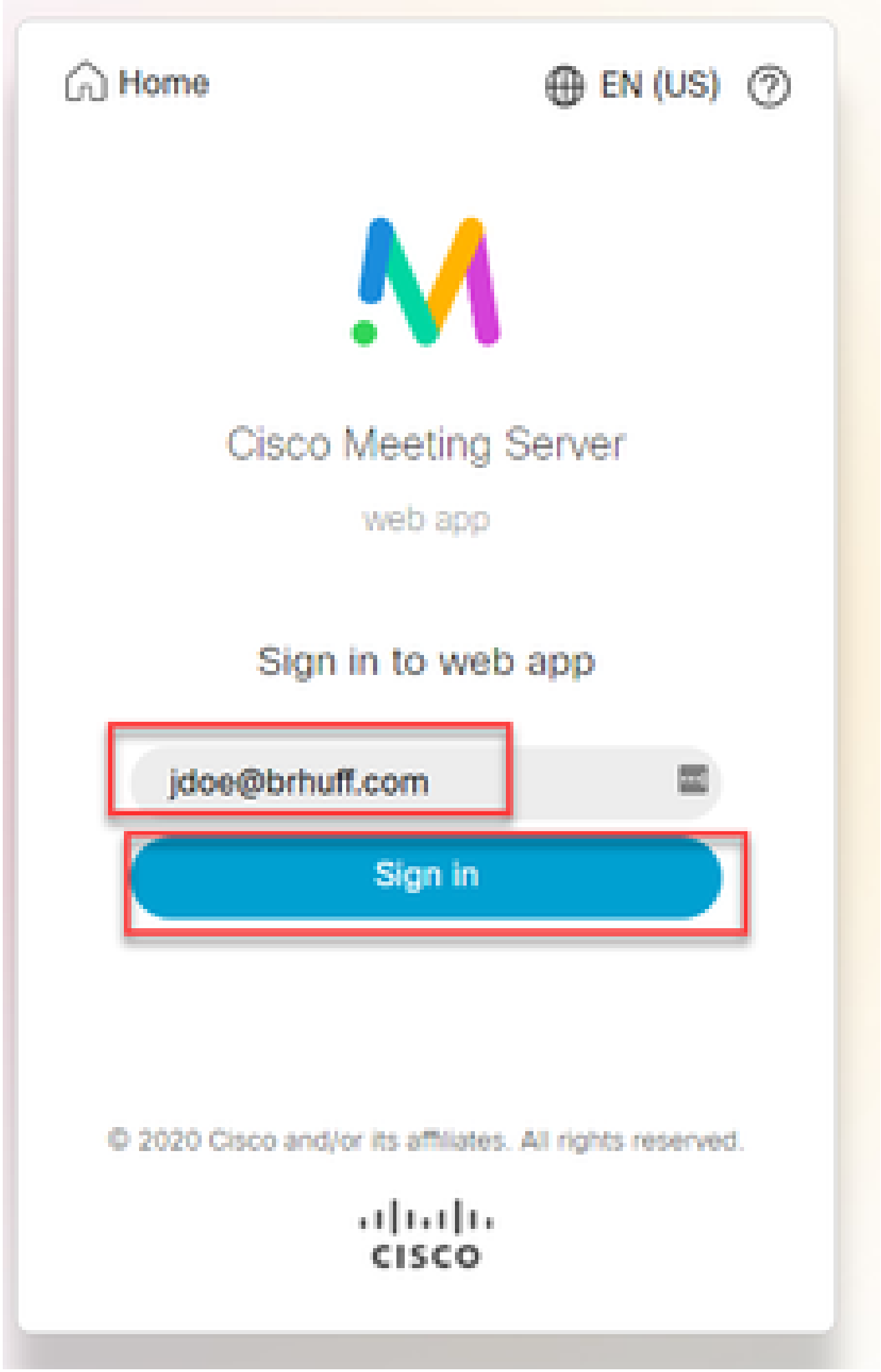
測試透過WebApp的SSO登入

現在已設定SSO，您可以測試伺服器：

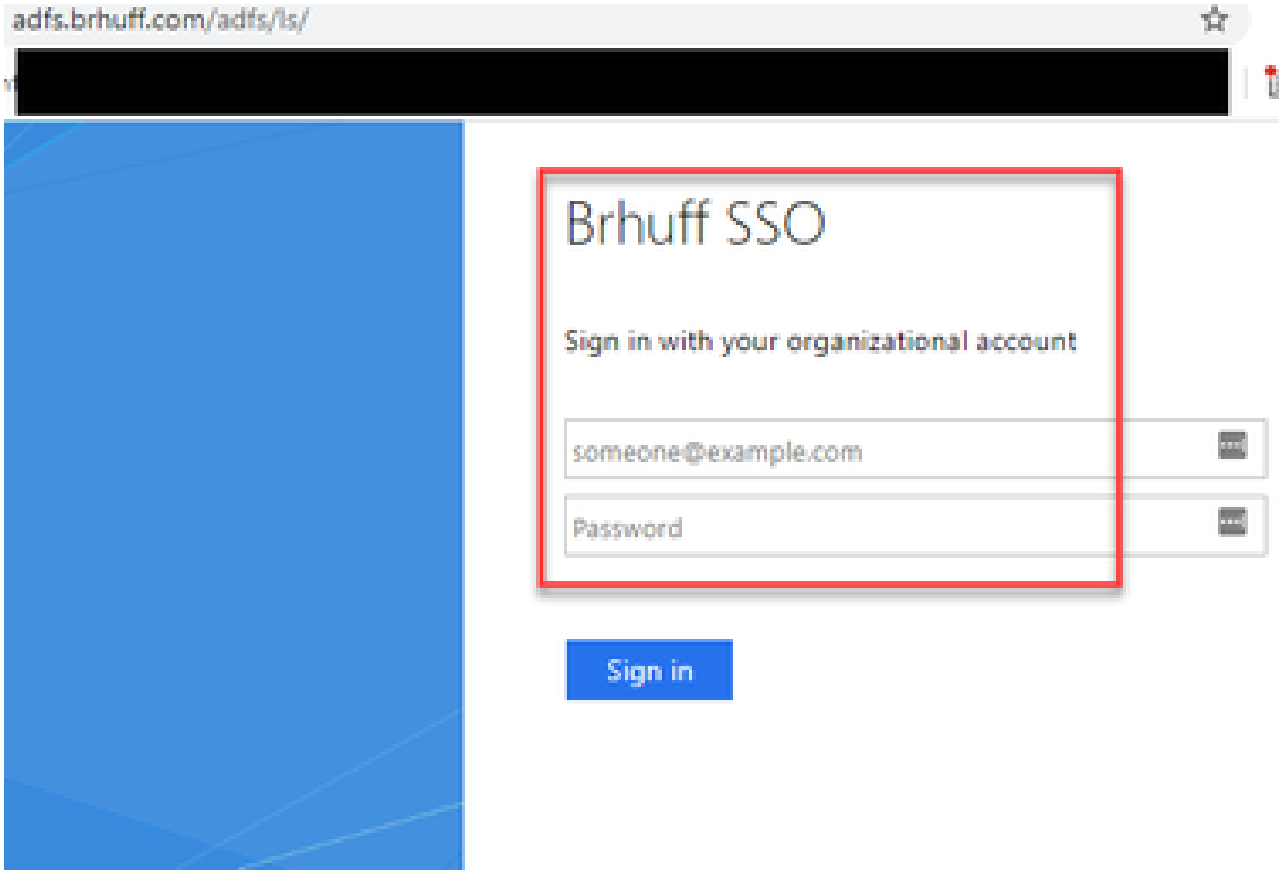
1. 導航到Web應用的Webbridge URL，然後選擇登入按鈕。


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

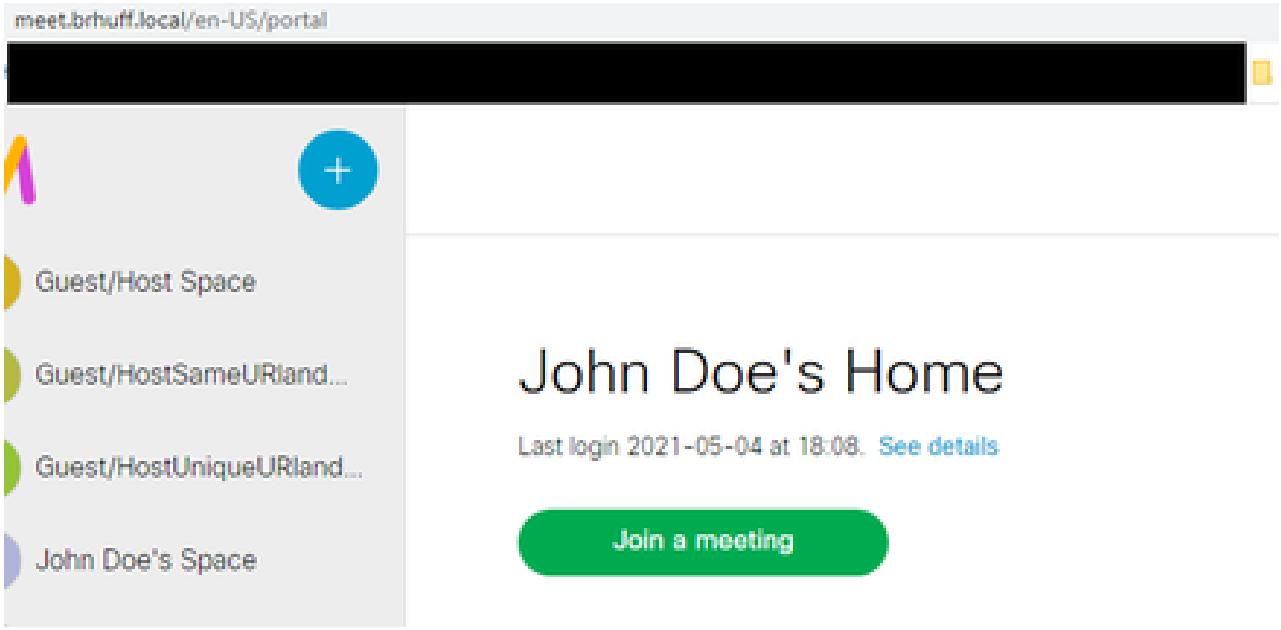
2. 使用者會看到輸入其使用者名稱的選項（請注意此頁面上沒有「密碼」選項）。


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. 然後，使用者會被重新導向至ADFS頁面（輸入使用者詳細資訊後），使用者必須在此輸入身份證明才能進行IdP驗證。



4. 使用IdP輸入並驗證憑證後，使用者會使用記號重新導向以存取Web App首頁：



疑難排解

基本故障排除

對於任何SSO問題的基本故障排除：

1. 確保已正確配置用於在IdP中導入為信賴信任的Webbridge3的構造後設資料，並且配置的URL與config.json中的ssoServiceProviderAddress完全匹配。
2. 確保IdP提供的並壓縮到Webbridge3 sso配置檔案的後設資料是來自IdP的最新後設資料，就像伺服器主機名、證書等發生更改一樣，需要將其重新導出並壓縮到配置檔案中。
3. 如果使用簽名和加密私鑰來加密資料，請確保正確的匹配金鑰是您上傳到webbridge的sso_xxxx.zip檔案的一部分。如有可能，嘗試在不使用可選私鑰的情況下進行測試，以檢視SSO是否可以在沒有此加密選項的情況下正常工作。
4. 確保為config.json配置了SSO域、Webbridge3 URL和從SAMLResponse匹配的EXPECTED身份驗證對映的正確詳細資訊。

嘗試從日誌角度進行故障排除也很理想：

1. 導航到Webbridge URL時，請在URL末尾放置？trace=true，以便在CMS Syslog中啟用詳細日誌記錄。(例如：https://join.example.com/en-US/home?trace=true)。
2. 在Webbridge3伺服器上運行syslog follow以在測試過程中即時捕獲，或在運行測試時在URL後附加跟蹤選項，並從Webbridge3和CMS Callbridge伺服器收集logbundle.tar.gz。 如果webbridge和callbridge位於同一台伺服器上，則只需要一個logbundle.tar.gz檔案。

Microsoft ADFS故障代碼

有時，SSO進程出現故障，可能導致IdP配置或其與IdP的通訊失敗。如果使用ADFS，最好檢視下一個連結以確認所發現的故障並採取補救操作：

Microsoft狀態代碼

例如：

> client_backend： ERROR ： SamlManager ： SAML Authentication request _e135ca12-4b87-4443-abe1-30d396590d58 failed with reason：
> urn：oasis：names：tc：SAML：2.0：status：Responder

此錯誤表示根據先前的說明檔案，失敗是因為IdP或ADFS所造成，因此必須由ADFS的管理員處理才能解決。

無法取得authenticationID

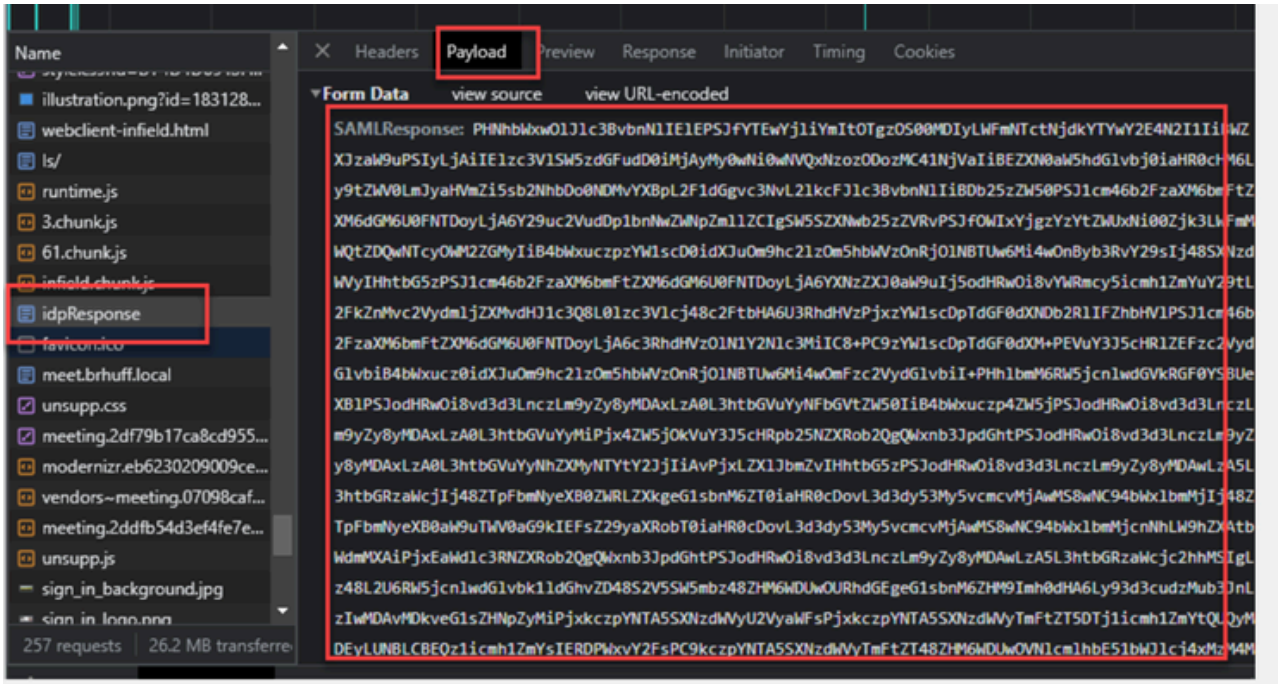
在某些情況下，在從IdP交換SAMLResponse時，Webbridge可能會在日誌中顯示此錯誤消息，但無法通過SSO登入：

> client_backend： INFO ： SamlManager ： [57dff9e3-862e-4002-b4fa-683e4aa6922c]獲取authenticationId失敗

這表示在稽核身份驗證交換期間從IdP傳回的SAMLResponse資料時，Webbridge3在響應中未找到與authenticationId的config.json相匹配的有效屬性。

如果通訊未使用簽名和加密私鑰進行加密，則可以透過Web瀏覽器從Developer Tools Network Logging提取SAML Response，並使用base64進行解碼。如果響應已加密，您可以從IdP端請求已解密的SAML響應。

在developer tools network logging輸出（也稱為HAR資料）中，在name列下查詢idpResponse，然後選擇Payload以檢視SAML響應。 如前所述，這可以使用base64解碼器進行解碼。



接收SAMLResponse資料時，請檢查<AttributeStatement>部分以查詢發回的屬性名稱，在此部分中，您可以找到從IdP配置和傳送的宣告型別。舉例來說：

```
<AttributeStatement>
<Attribute Name="<公用名的URL">
<AttributeValue>testuser1</AttributeValue>
</Attribute>
<Attribute Name="<NameID的URL">
<AttributeValue>testuser1</AttributeValue>
```

</Attribute>
<Attribute Name="uid">
<AttributeValue>testuser1</AttributeValue>
</Attribute>
</AttributeStatement>

透過檢查以前的名稱，您可以檢查Attribute Statement部分下的<AttributeName>，並將每個值與SSO config.json的authenticationIdmapping部分中設定的值進行比較。

在上一個示例中，可以看到authenticationIdMapping的配置與傳遞的內容不完全匹配，因此導致無法找到匹配的authenticationId：

authenticationIdMapping ： http://example.com/claims/NameID

為了解決此問題，可以嘗試兩種方法：

1. IdP傳出宣告規則可以更新，以具有與Webbridge3上config.json的authenticationIdMapping中配置的完全匹配的匹配宣告。(在IdP上為http://example.com/claims/NameID增加宣告規則)
   或
2. config.json可在Webbridge3上進行更新，以使「authenticationIdMapping」與IdP上配置的其中一個傳出宣告規則完全匹配。(即「authenticationIdMapping」，以便與屬性名稱之一（可以是「uid」、「<URL>/NameID」或「<URL>/CommonName」）匹配)進行更新。只要符合（完全）傳遞時Callbridge API上配置的預期值)

驗證中未傳遞/比對宣告

有時，在從IdP交換SAMLResponse期間，Webbridge會顯示此錯誤，指示匹配斷言失敗，並跳過與伺服器配置不匹配的所有斷言：

client_backend：錯誤： SamlManager：沒有任何斷言透過驗證
client_backend： INFO ： SamlManager ：跳過斷言，不在允許的對象中

此錯誤指示的是，從IdP檢視SAMLResponse時，Webbridge無法找到任何匹配的斷言，因此跳過不匹配的故障，最終導致故障的SSO登入。

為了找到此問題，最好從IdP檢視SAMLResponse。 如果通訊未使用簽名和加密私鑰加密，則可透過Web瀏覽器從Developer Tools Network Logging中提取SAML響應，然後使用base64進行解碼。如果響應已加密，您可以從IdP端請求已解密的SAML響應。

在檢視SAMLResponse資料時，檢視響應的<AudienceRestriction>部分，您可以找到此響應受限制的所有對象：

<條件NotBefore=2021-03-30T19:35:37.071Z NotOnOrAfter=2021-03-30T19:36:37.071Z>
<受眾限制>

<Audience>https://cisco.example.com</Audience>
</AudienceRestriction>
</Condition>

使用<Audience>一節(https://cisco.example.com) 中)中的值，您可以將其與Webbridge組態的config.json中的ssoServiceProviderAddress進行比較，並驗證兩者是否完全相符。對於此示例，您可以看到失敗原因是受眾與配置中的服務提供商地址不匹配，因為它有附加的：443：

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

這要求兩者之間完全匹配，以免導致類似這樣的故障。此範例的修正方法為下列兩種方法之一：

1. ：443可以從config.json的ssoServiceProviderAddress部分的地址中刪除，以便與SAMLResponse中從IdP提供的Audience欄位匹配。
或

2. 可以更新IdP中Webbridge3的中繼資料或信賴關係人，將：443附加到URL。(如果中繼資料已更新，則必須在ADFS上重新匯入為信賴關係人。但是，如果直接從IdP嚮導修改信賴方，則無需再次導入信賴方。)

登入Web App失敗：

Home

EN (US)

Blahman Industries

Blahman WebApp

Sign in to web app

darmckin@brhuff.com

Sign In

Sign in failed

CISCO

CMS FAQ

Cisco Website

WB3Cmgr： [d626bbaf-80c3-4286-8284-fac6f71eb140] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5註冊=40a4026c-0272-4 a1-b125-136fdf5612a5 (user=darmckin@brhuff.com)

3月18日15:08:52.399 user.warning cmscb3-1 host：server：警告：拒絕使用者'darmckin@brhuff.com'的登入嘗試— authenticationId不正確

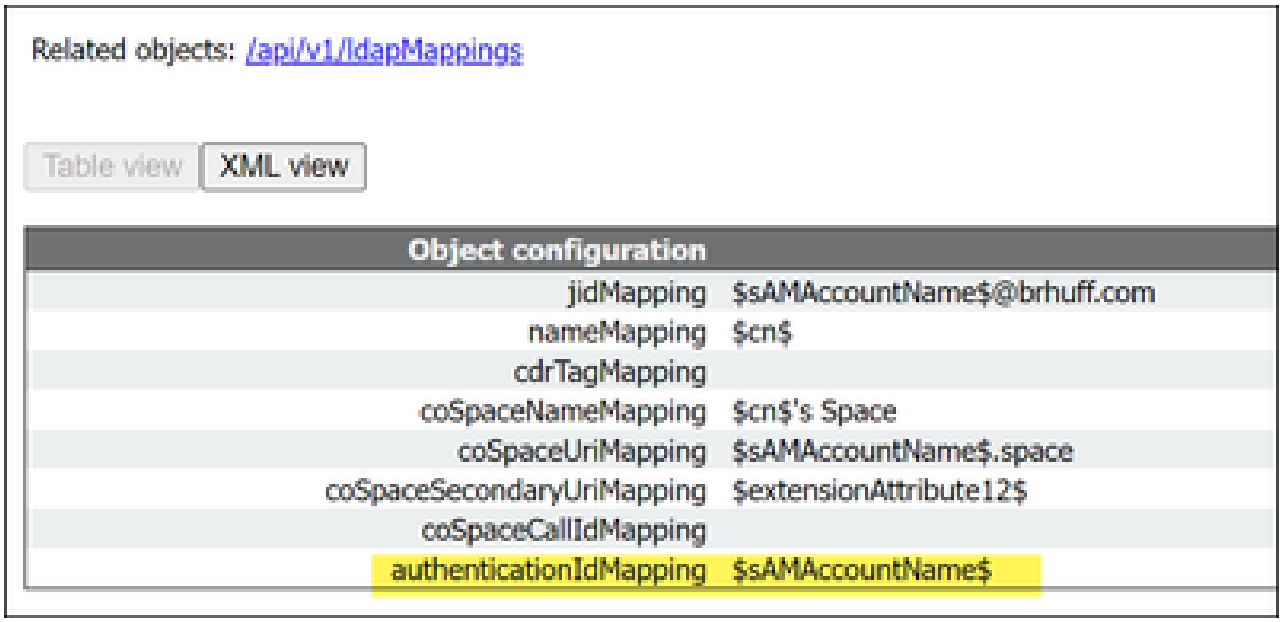
3月18日15:08:52.412 user.info cmscb3-1 host：server：資訊：來自darmckin@brhuff.com的登入請求失敗

CMS ldapmapping中的AuthenticationIdMapping與ADFS中用於宣告規則的已配置的LDAP屬性不匹配。下面一行「Successfully obtain authenticationID：darmckin@brhuff.com」表示ADFS已使用從Active Directory獲取darmckin@brhuff.com的屬性配置了宣告規則，但CMS API > Users中的AuthenticationID顯示其預期為darmckin。 在CMS ldapMappings中，AuthenticationID配置為$sAMAccountName$，但ADFS中的宣告規則配置為傳送電子郵件地址，因此不匹配。

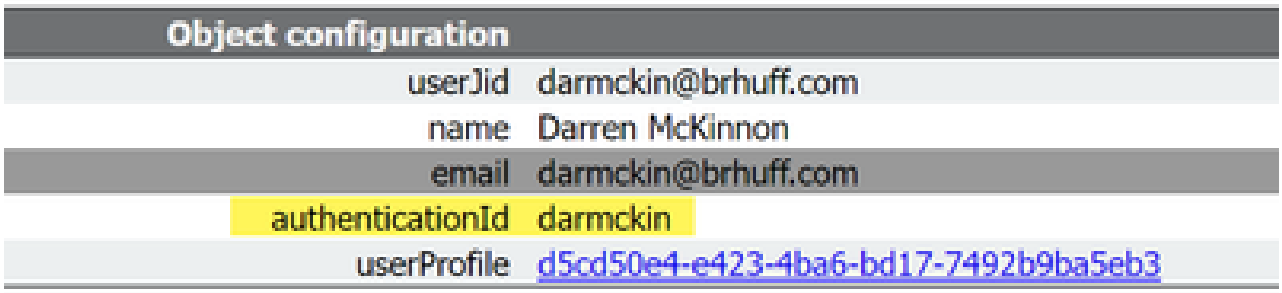
如何解決此問題：

執行下列任一項作業：

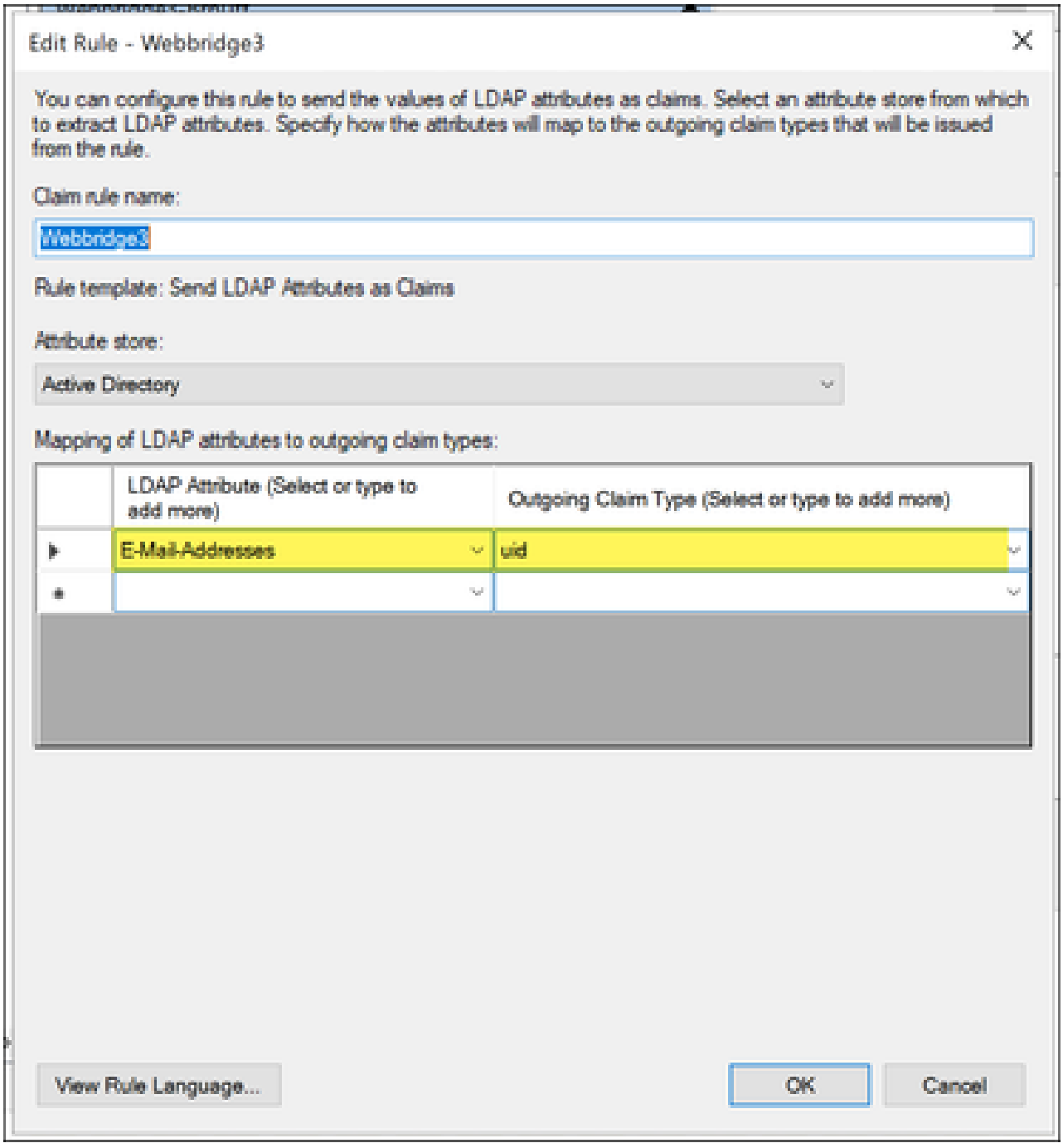
1. 更改CMS ldapmapping中的AuthenticationID以匹配ADFS上的宣告規則中使用的內容，並執行新的同步
2. 更改ADFS宣告規則中使用的LDAP屬性，以匹配CMS ldapmapping中配置的屬性



API LDAPMapping



API使用者示例



來自ADFS的宣告規則

Webbridge日誌顯示工作日誌示例。 在聯接URL中使用？trace=true生成的示例：

3月18日14:24:01.096 user.info cmscb3-1 client_backend：資訊
：SamlManager：[7979f13c-d490-4f8b-899c-0c82853369ba]匹配的SSO sso_2024.zip in SAML Token請求

3月18日14:24:01.096 user.info cmscb3-1 client_backend：資訊
：SamlManager：[7979f13c-d490-4f8b-899c-0c82853369ba]嘗試在SAML IDP響應中查詢SSO

3月18日14:24:01.101 user.info cmscb3-1 client_backend：資訊：SamlManager：[7979f13c-d490-4f8b-899c-0c82853369ba]已成功獲取身份驗證ID：darmckin@brhuff.com

3月18日14:24:01.102 user.info cmscb3-1 host：server：資訊：WB3Cmgr： [7979f13c-d490-4f8b-899c-0c82853369ba] AuthRequest已收到連線id=64004556-faea-479f-aabe-691e17783aa5註冊=40a4026c-0272-42a1-b125-136fdf5612a5 (使用者=darmckin@brhuff.com)

3月18日14:24:01.130 user.info cmscb3-1 host：server：資訊：來自darmckin@brhuff.com的成功登入請求

3月18日14:24:01.130 user.info cmscb3-1 host：server：INFO ： WB3Cmgr： [7979f13c-d490-4f8b-899c-0c82853369ba]發出JWT ID e2a860ef-f4ef-4391-b5d5-9abdfa89ba0f

3月18日14:24:01.132 user.info cmscb3-1 host：伺服器：資訊：WB3Cmgr： [7979f13c-d490-4f8b-899c-0c82853369ba]傳送身份驗證響應(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，跟蹤：7979f13c-d490-4f8b-899c-0c82853369ba] 14.0.25.247 - - [2024年3月18日：18:24:01 +0000] status 200 "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，類似於壁虎） Chrome/122.0.0.0 Safari/537.36」到上游192.0.2.2:9000：upstream_response_time 0.038 request_time 0.039 msec 1710786241.133 upstream_response_length 24 200

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。