配置CMS上的WebApp SSO並對其進行故障排除

目錄

簡介

必要條件

- 需求
- 採用元件

背景

設定

網路圖表

ADFS安裝和初始設定

將CMS使用者對映到身份提供程式(IdP)

為IdP建立Webbridge後設資料XML

將Webbridge的後設資料匯入身份提供程式(IdP)

為IdP上的Webbridge服務建立宣告規則

為Webbridge建立SSO存檔ZIP檔案：

- 獲取並配置idp_config.xml
- 建立包含內容的config.jsonFile
- 設定sso_sign.key（可選）
- 設定sso_encrypt.key（可選）
- 正在建立SSO ZIP檔案
- 將SSO Zip檔案上傳到Webbridge

通用存取卡(CAC)

正在測試通過WebApp的SSO登入

疑難排解

- 基本故障排除
- Microsoft ADFS故障代碼
- 無法獲取authenticationID
- 在驗證中未傳遞/匹配斷言
- 在Web應用上登入失敗：
  - 案例 1:
  - 案例 2:
  - 案例 3:
- 無法識別使用者名稱
  - 案例 1:
  - 案例 2:
- 顯示工作登入示例的Webbridge日誌。在聯接URL中使用？trace=true生成的示例：

常見問題 (FAQ)

- Webapp SSO JWT是否可以擴展？
- 如果我關閉瀏覽器，是否需要重新向WebApp進行身份驗證？
- WebApp SSO如何支援多個域？

相關資訊

簡介

本文檔介紹如何配置單一登入(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
- 標識提供程式(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

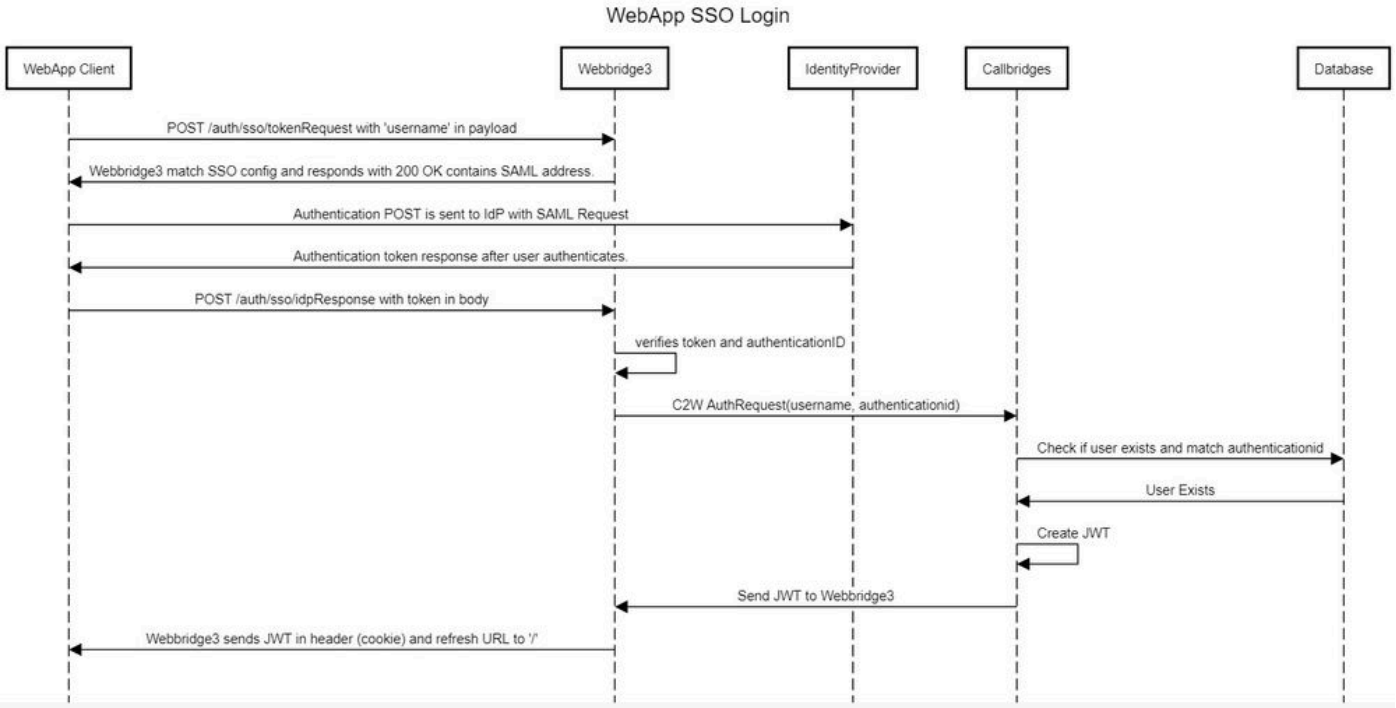
CMS 3.1及更高版本引入了使用者使用SSO登入的功能，無需在使用者每次登入時輸入密碼，因為會使用身份提供程式建立單個會話。
此功能使用安全斷言標籤語言(SAML)版本2.0作為SSO機制。

附註：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。

附註：啟用SSO後，基本的LDAP身份驗證將不再可用。

設定

網路圖表



ADFS安裝和初始設定

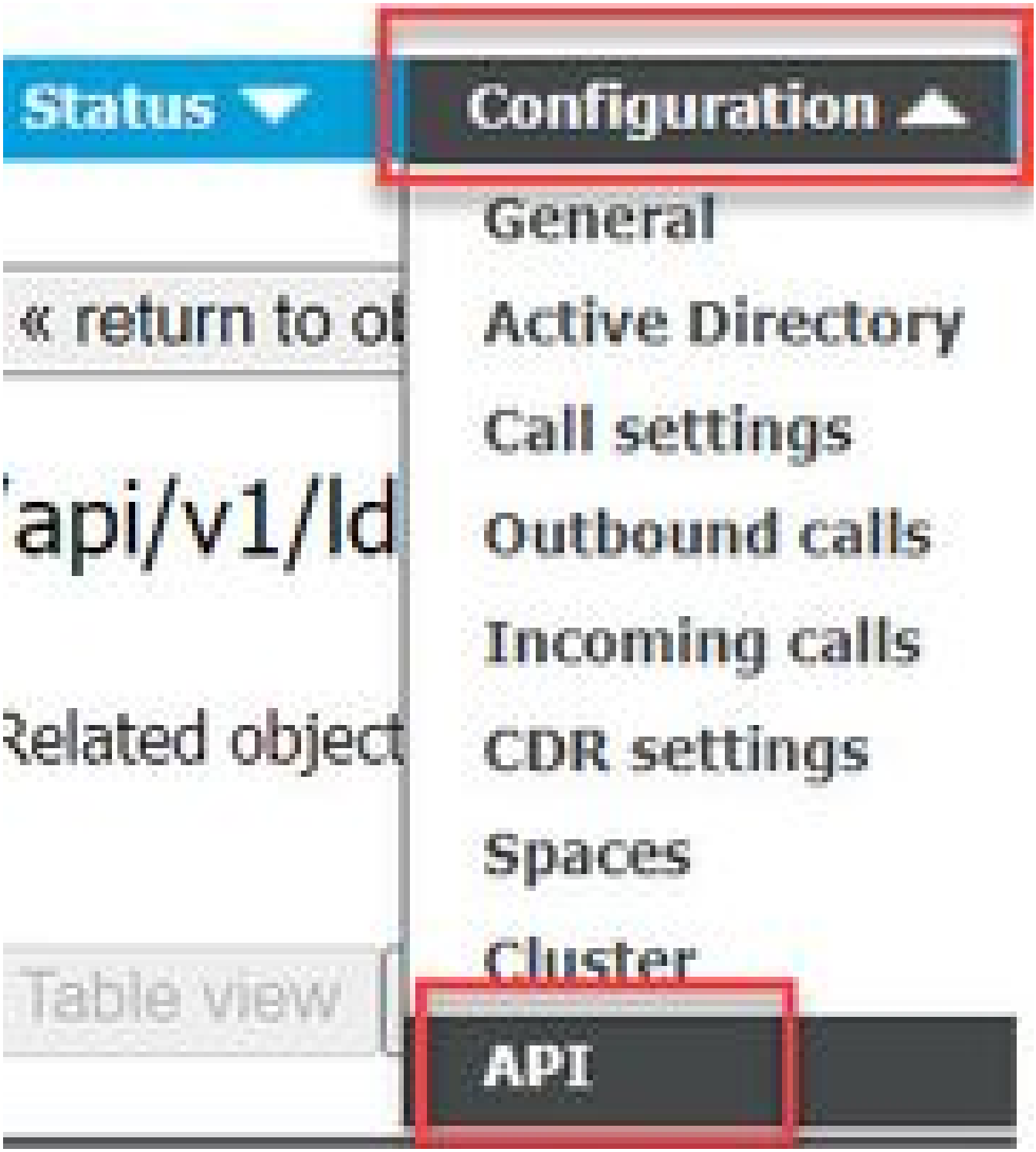
此部署方案使用Microsoft Active Directory聯合身份驗證服務(ADFS)作為身份提供程式(IdP)，因此，建議在此配置之前安裝並運行ADFS（或目標IdP）。

將CMS使用者對映到身份提供程式(IdP)

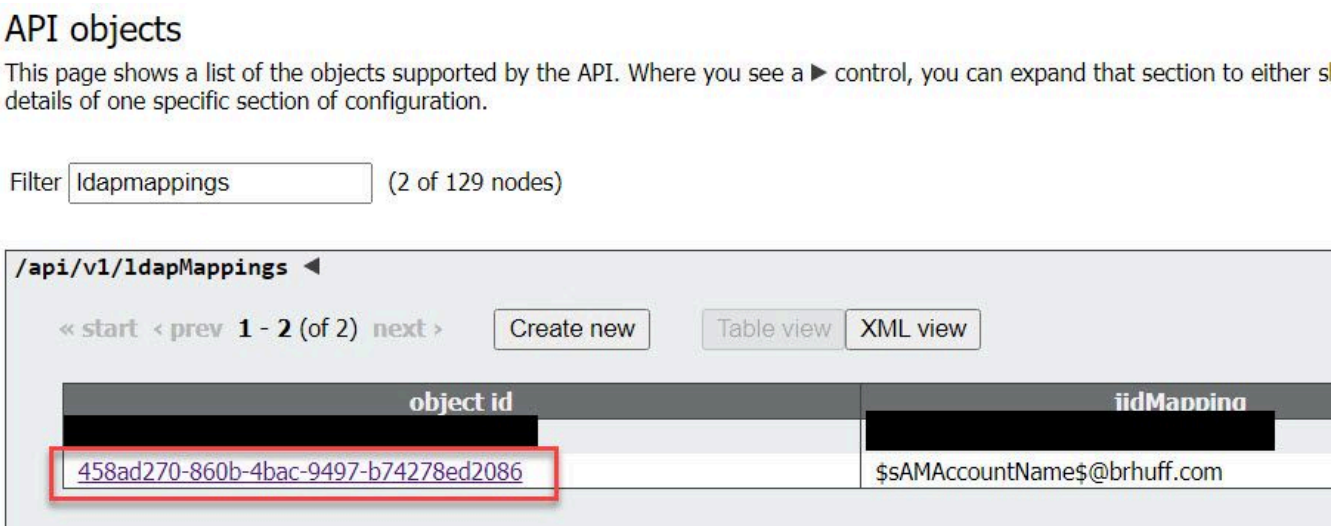
為了使使用者獲得有效的身份驗證，必須在IdP提供的相關欄位的應用程式設計介面(API)中將其對映。用於API的ldapMapping中的authenticationIdMapping選項。

1.在CMS Web Admin GUI上導航至Configuration > API

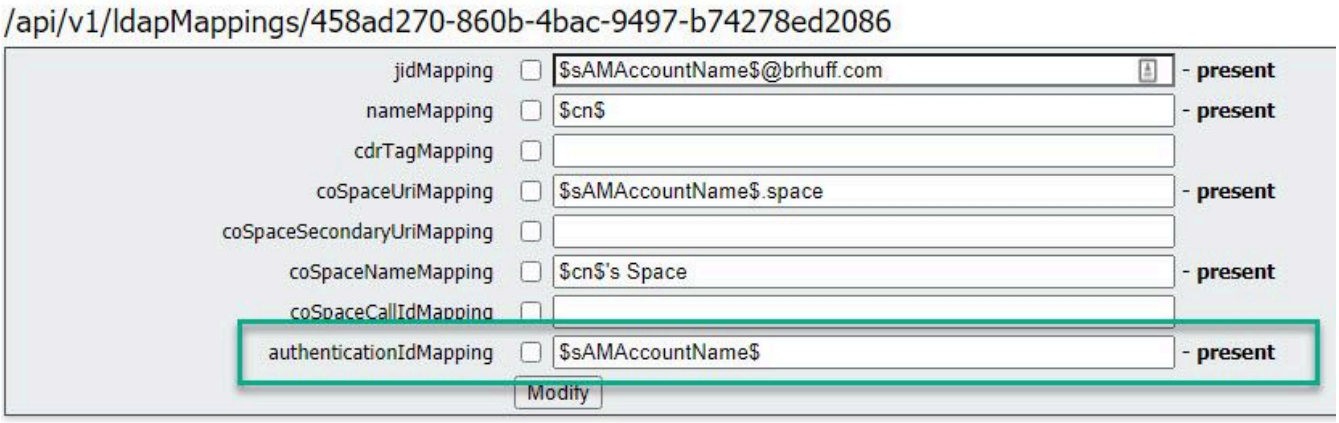
Co



2.在api/v1/ldapMappings/<GUID-of-Ldap-Mapping>下找到現有（或新建）LDAP對映。



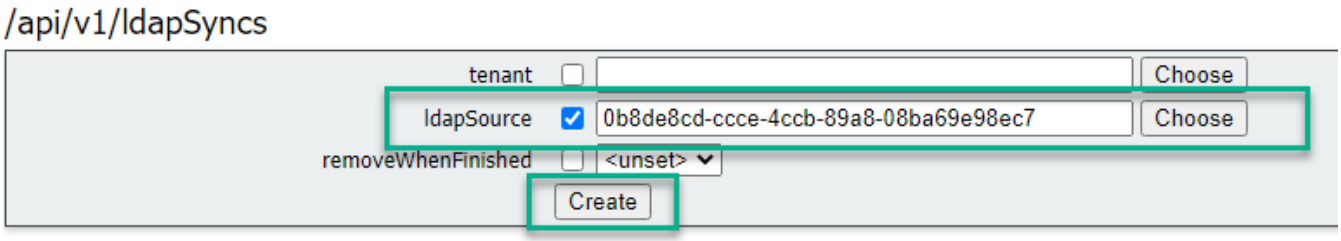
3.在選定的ldapMapping對象中，將authenticationIdMapping更新到從IdP傳遞的LDAP屬性。在本例中，選項$sAMAccountName用作對映的LDAP屬性。



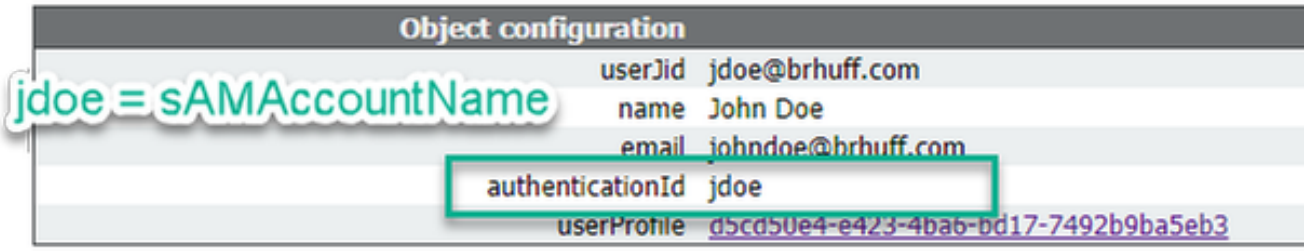
附註：authenticationIdMapping由callbridge/資料庫用於驗證從SAMLResponse中的IdP傳送的宣告，並為使用者提供一個JSON Web令牌(JWT)。

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

舉例來說：



5.完成LDAP同步後，在Configuration > api/v1/users中的CMS API中導航，並選擇已匯入的使用者，並驗證authenticationId是否正確填充。



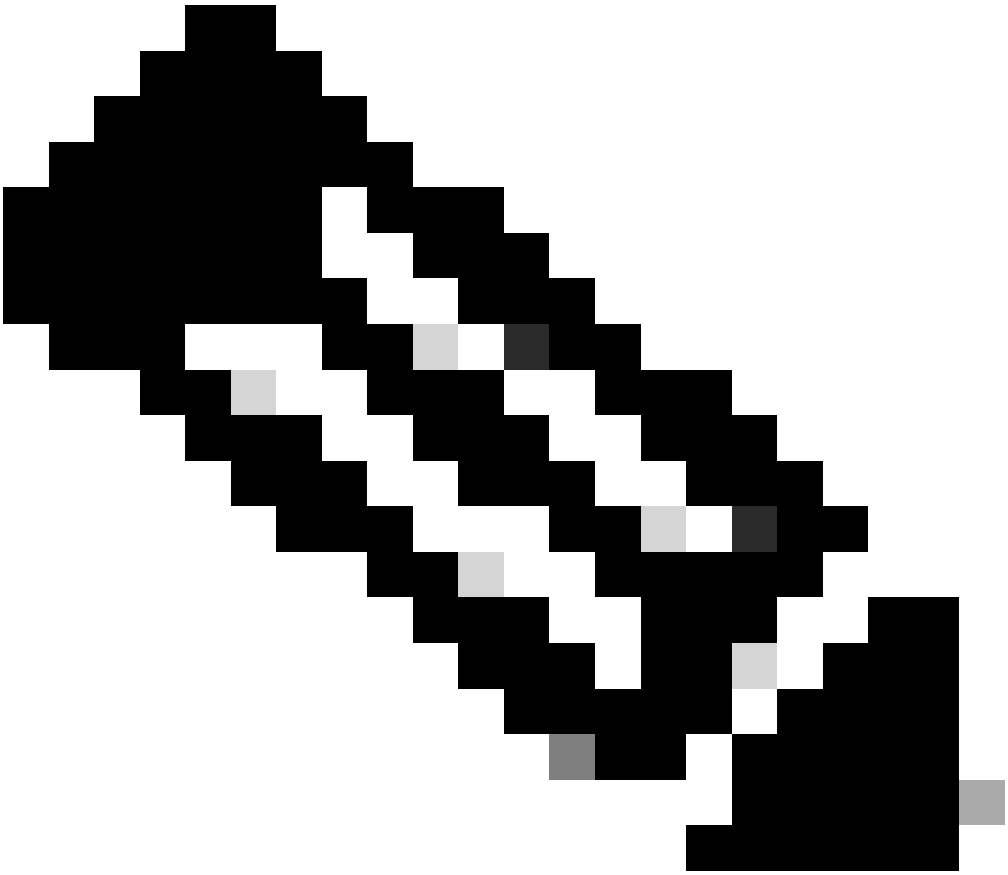
為IdP建立Webbridge後設資料XML

Microsoft ADFS允許將後設資料XML檔案作為信賴信任方匯入，以標識正在使用的服務提供程式。為此，建立後設資料XML檔案的方法有很多，但是檔案中必須存在一些屬性：

具有必需值的Webbridge後設資料的示例：

```
<?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 — 這是使用者瀏覽器可訪問的Webbridge3伺服器地址（FQDN/主機名）和相關埠。



附註：如果有多個使用單個URL的Web網橋，這必須是負載均衡地址。

2. Location — 這是Webbridge地址的HTTP-POST AssertionConsumerService所在的位置。這是指示IdP在登入後將經過身份驗證的使用者重定向到的位置。必須將其設定為idpResponse URL:https://<WebedgeFQDN>:<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（憑證），IdP將使用該公鑰驗證Webbridge的AuthRequest。此ID必須與在Webbridge上上載的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。 開啟文本檔案中的證書，並將內容複製到Webbridge後設資料檔案中。 將sso_xxxx.zip檔案中使用的證書的匹配金鑰用作sso_sign.key檔案。

4. 可選 — 用於加密的公鑰 — 這是IdP用於加密發回到Webbridge的SAML資訊的公鑰（證書）。此密碼必須與Webbridge上傳SSO捆綁包上的私鑰「sso_encrypt.key」匹配，以便Webbridge可以解密由IdP發回的內容。 您可以使用部署中的現有證書。 開啟文本檔案中的證書，並將內容複製到Webbridge後設資料檔案中。 將sso_xxxx.zip檔案中使用的證書的匹配

金鑰用作sso_encrypt.key檔案。

使用可選公鑰（證書）資料匯入IdP的Webbridge後設資料示例：

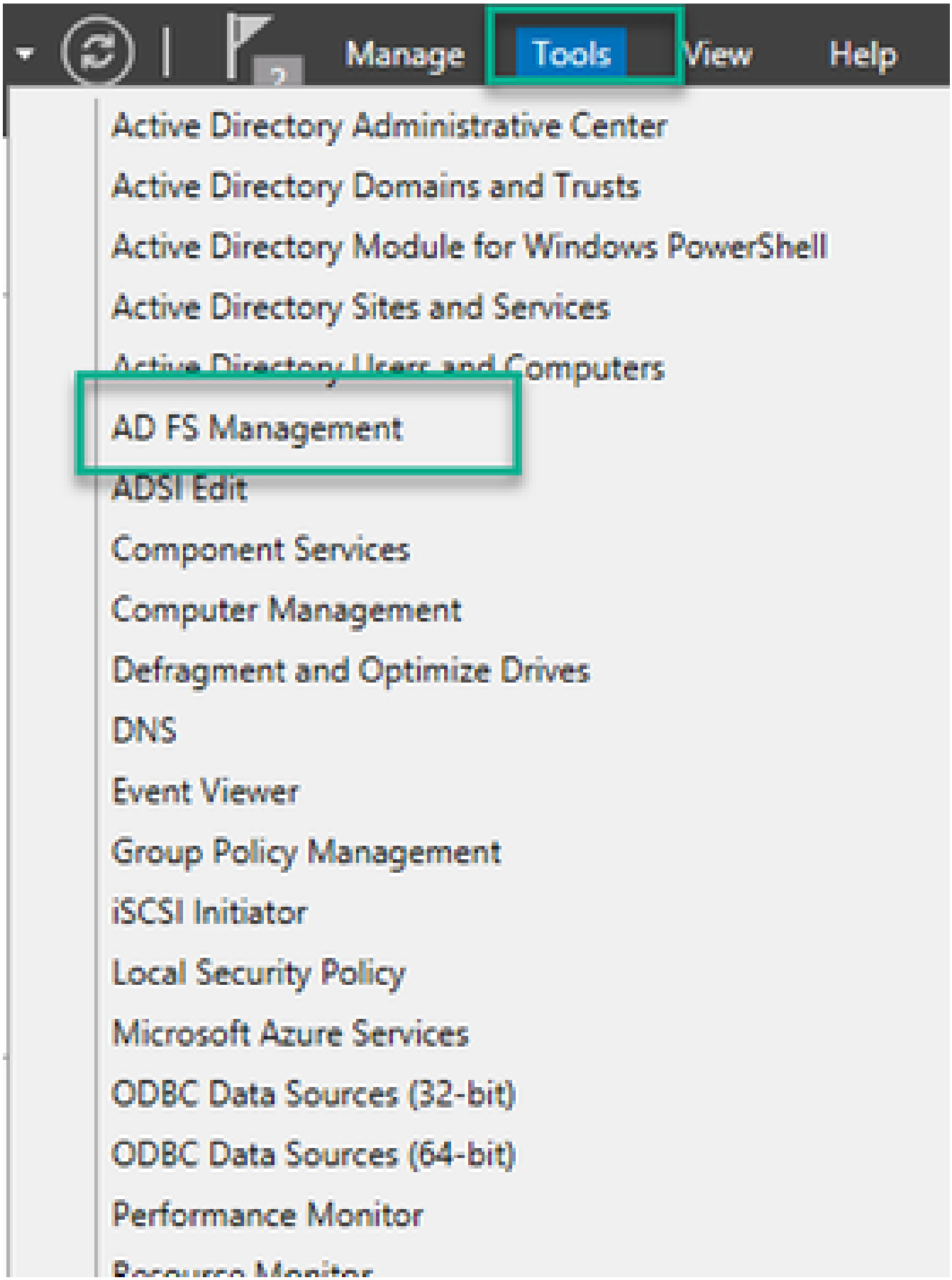

```
<?xml version="1.0"?>
- <md:EntityDescriptor entityID="https://meet.brhuff.local:443" ID="https://meet.brhuff.local:443" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  - <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" AuthnRequestsSigned="true">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

將Webbridge的後設資料匯入身份提供程式(IdP)

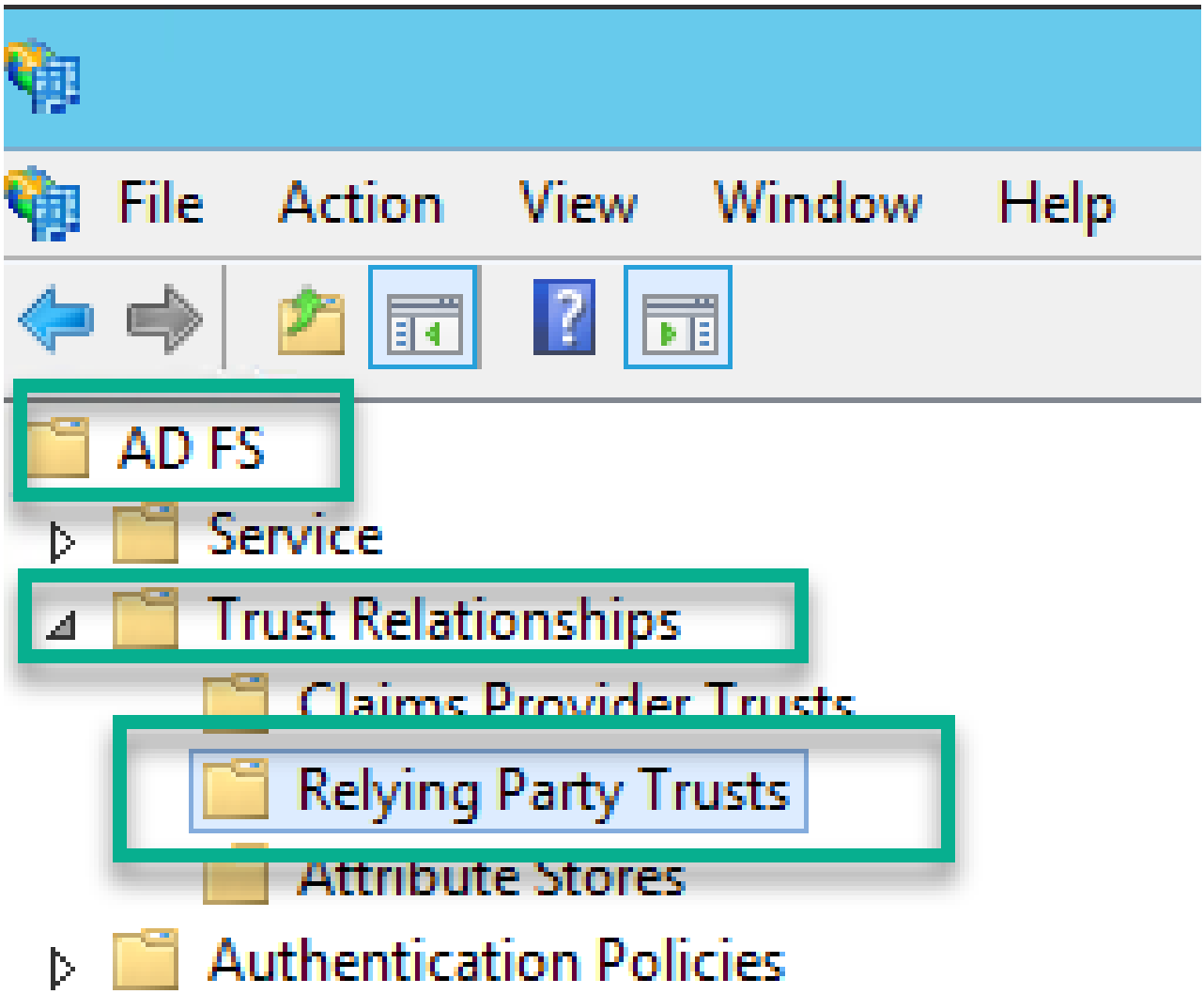
使用正確的屬性建立後設資料XML後，可以將檔案匯入到Microsoft ADFS伺服器以建立信賴信任方。

1.將遠端案頭連線到託管ADFS服務的Windows伺服器

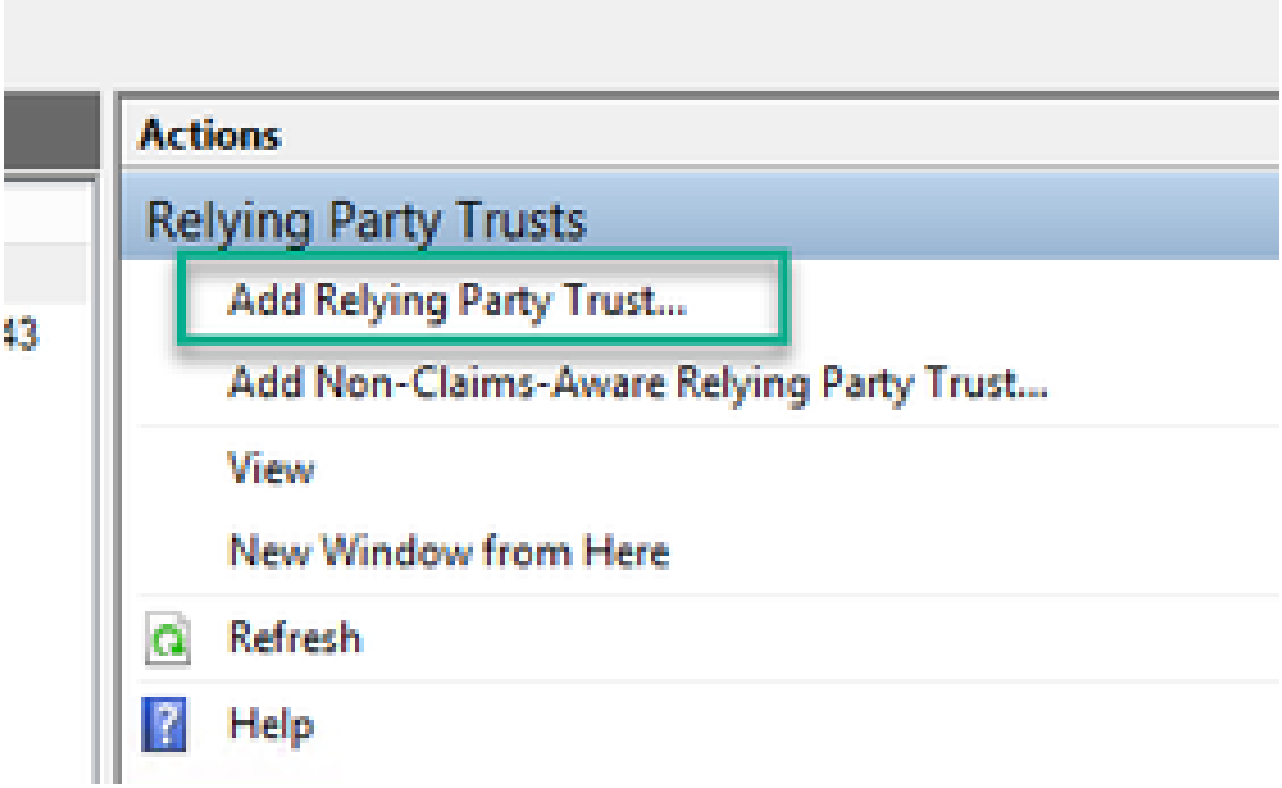
2.開啟AD FS管理控制檯，通常可以通過伺服器管理器訪問。



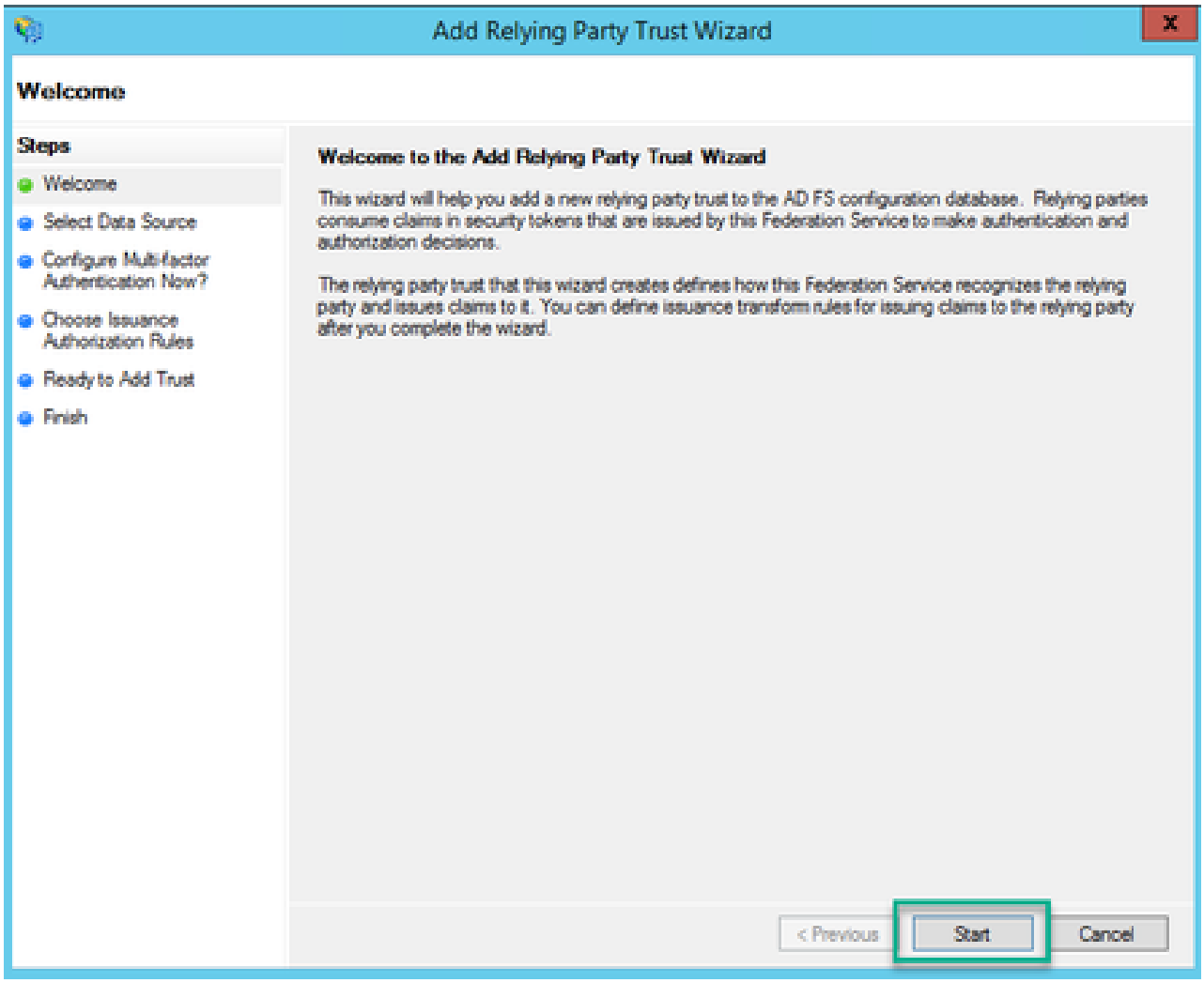
3.進入ADFS管理控制檯後，在左窗格中導航至ADFS >信任關係>信賴方信任。



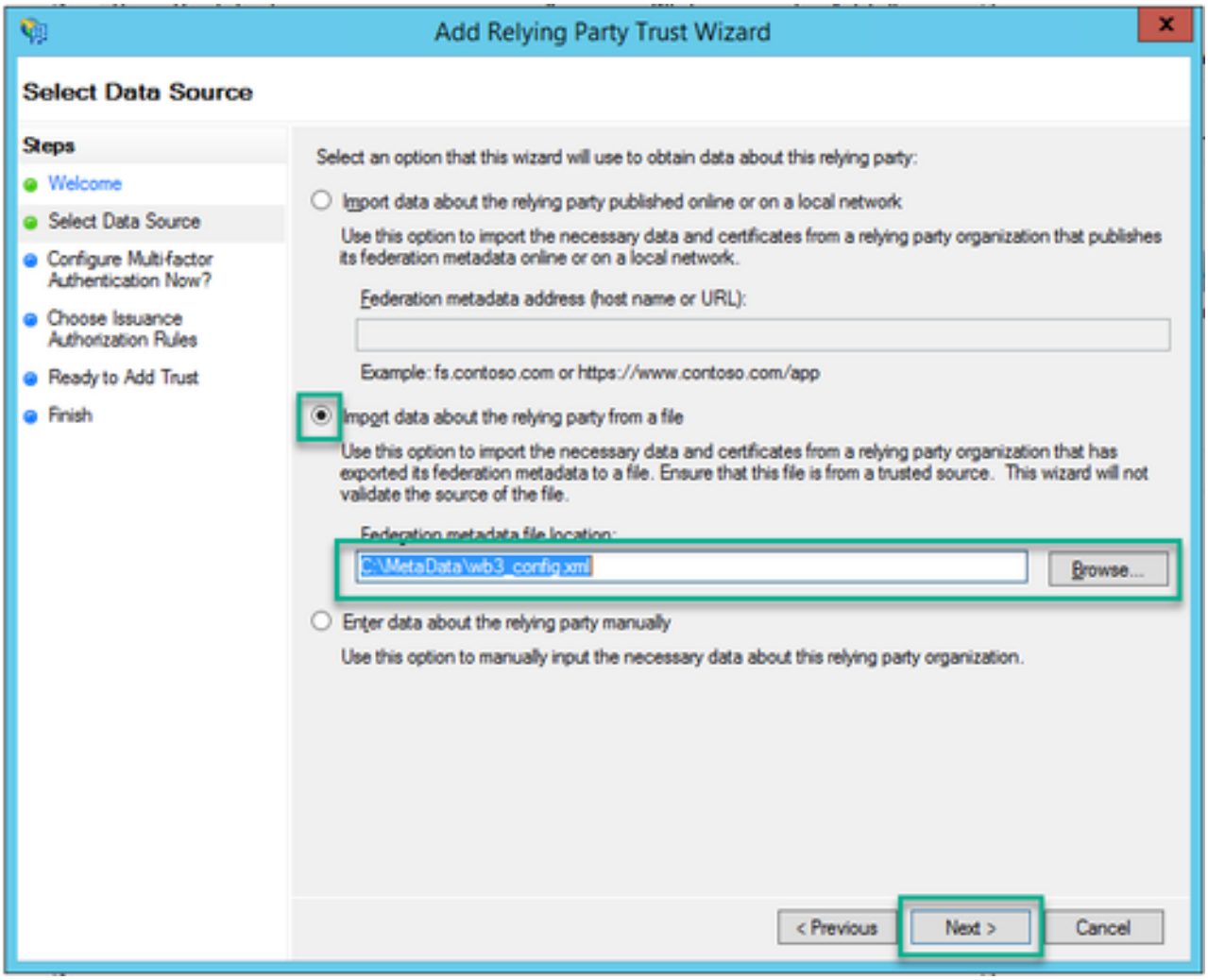
4.在ADFS管理控制檯的右窗格中，選擇新增信賴方信任…… 選項。



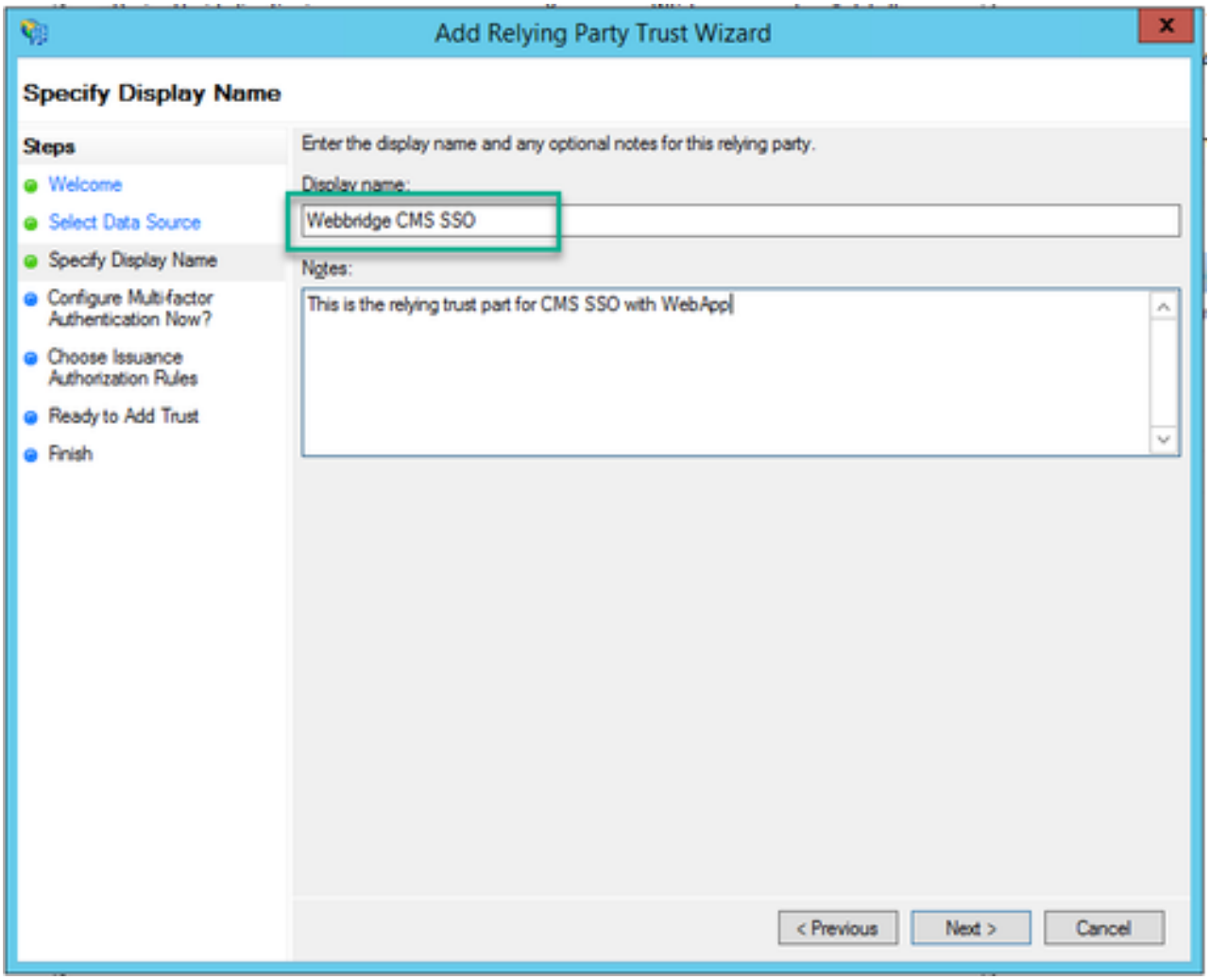
5.進行此選擇後，將開啟新增信賴方信任嚮導。選擇Start選項。



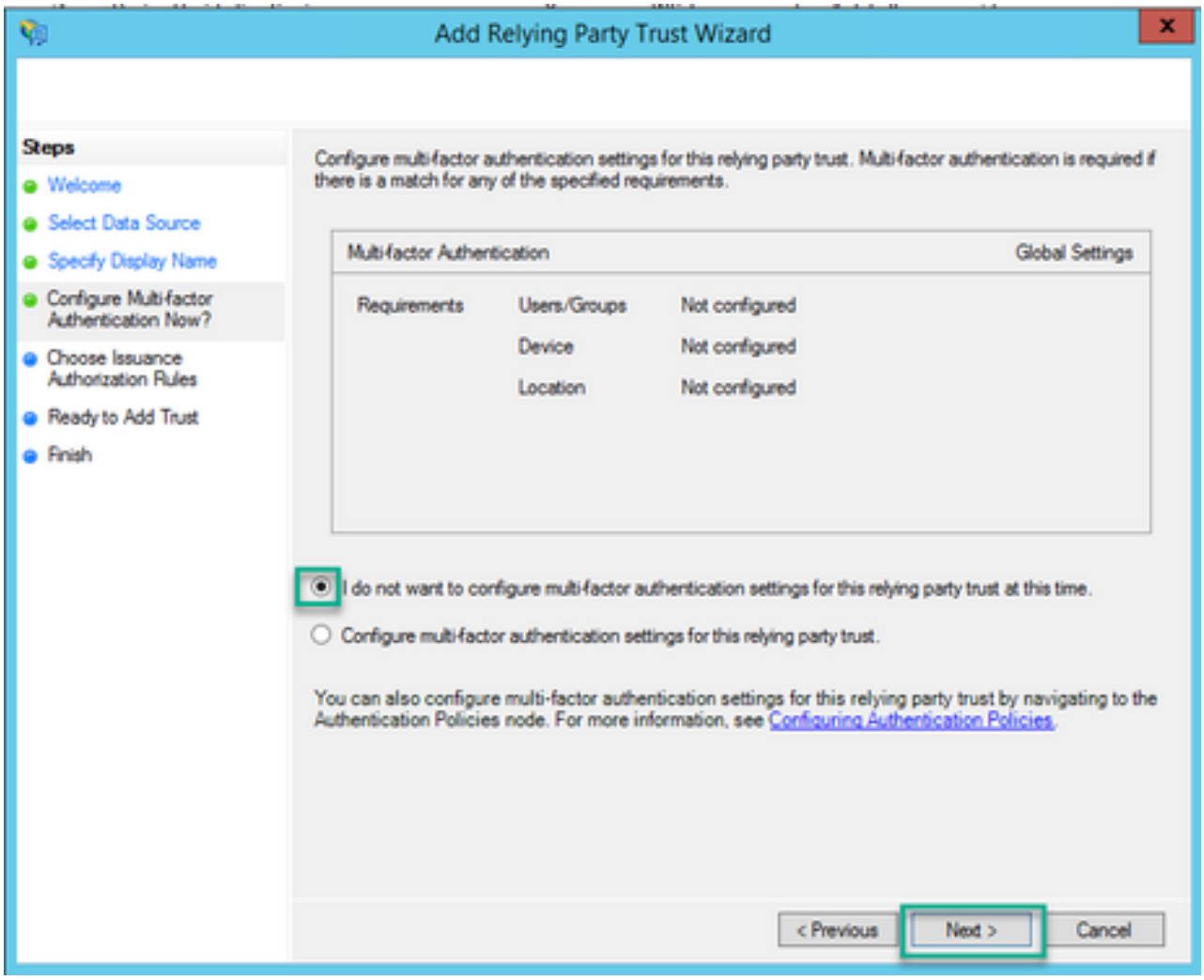
6.在「選擇資料來源」頁上，選擇從檔案匯入信賴方資料的單選按鈕，然後選擇瀏覽，然後導航到Webbridge後設資料檔案的位置。



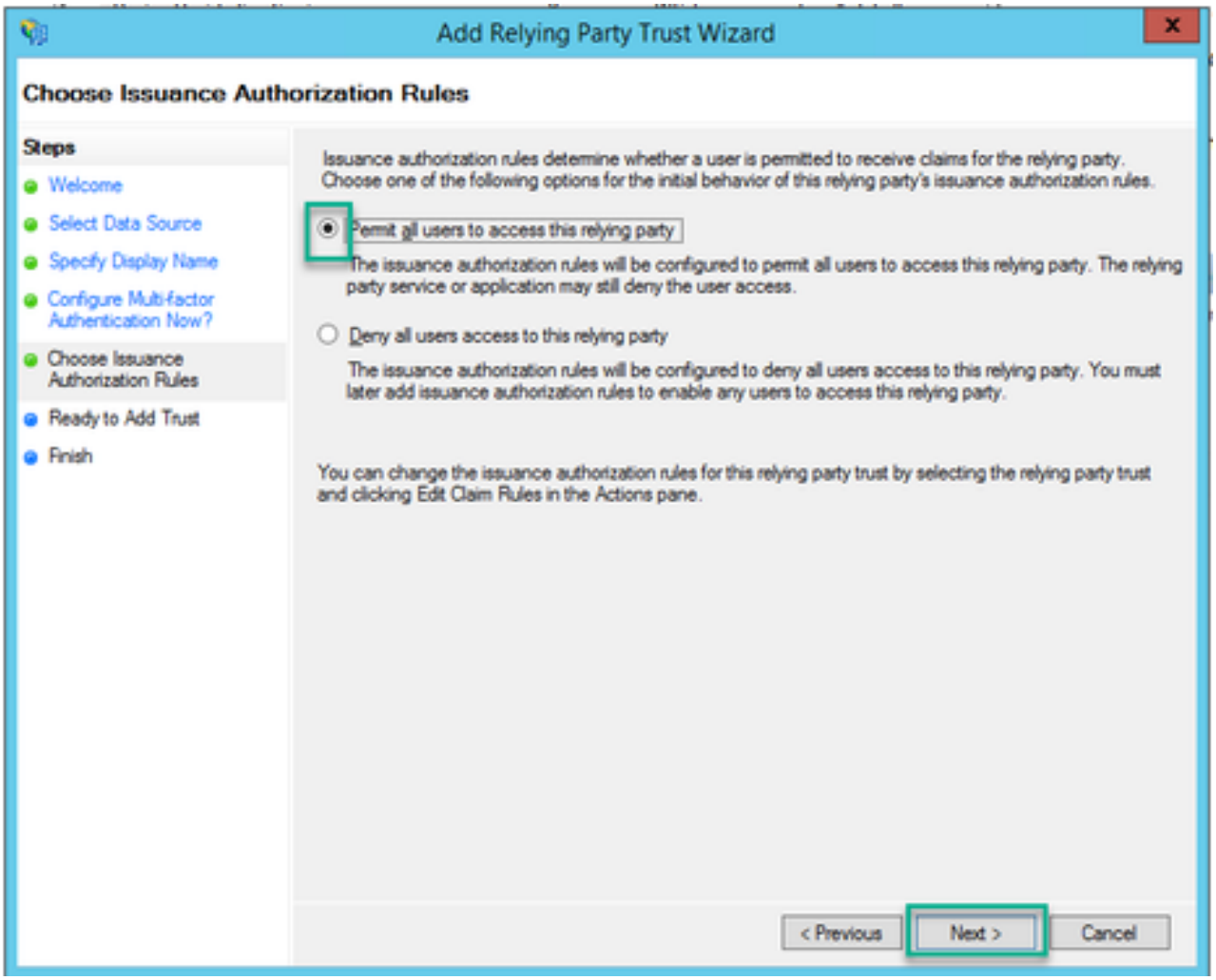
7.在指定顯示名稱頁上，在ADFS中放置要顯示的實體名稱（顯示名稱不用於ADFS通訊的伺服器用途，只是用於提供資訊）。



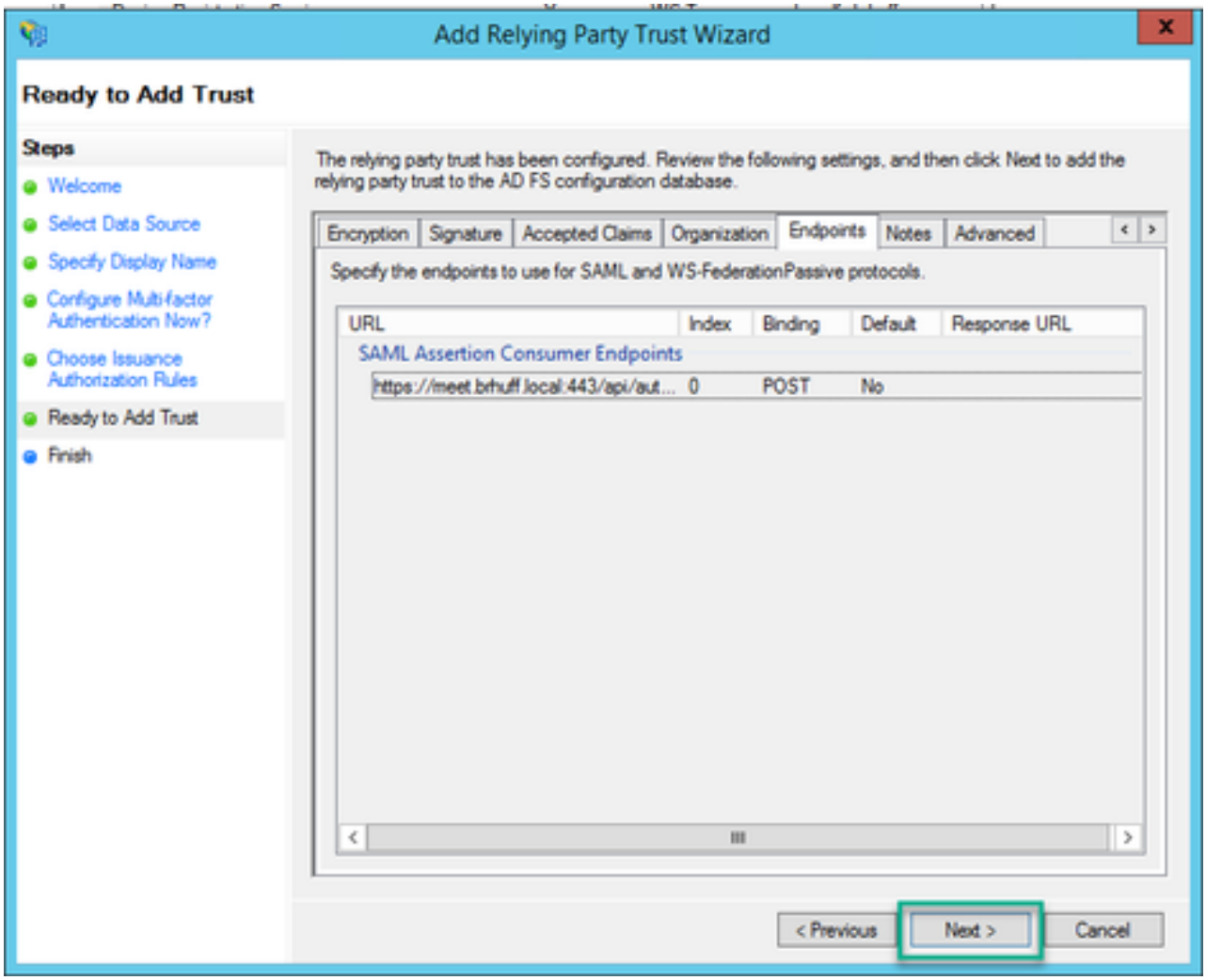
8.在「Configure Multi-factor Authentication Now？（立即配置多重身份驗證？）」上頁面，保留為預設值並選擇下一步。



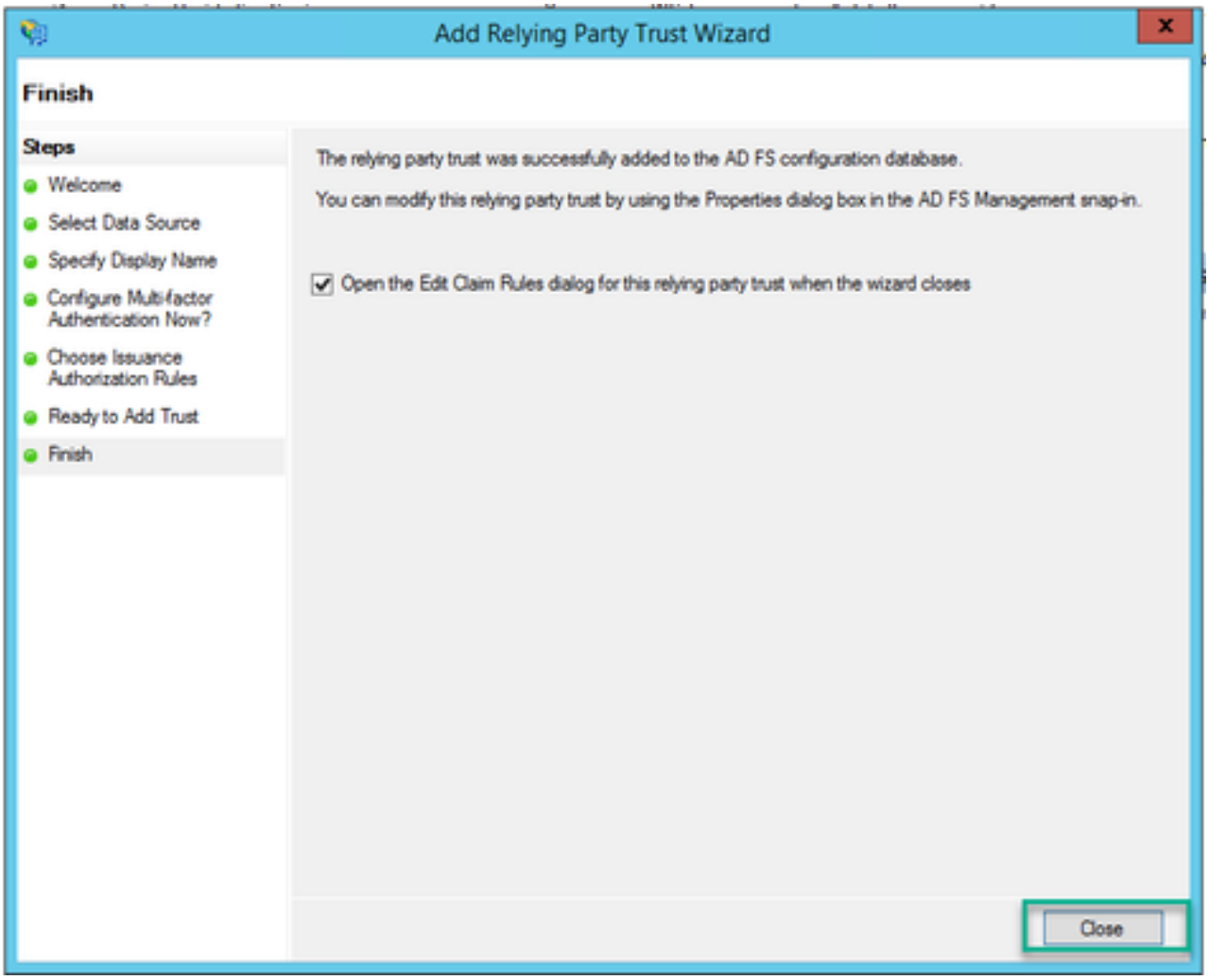
9.在選擇頒發授權規則頁面上，保留為允許所有使用者訪問此信賴方。



10.在Ready to Add Trust頁面上，可通過頁籤檢視Webbridge信賴信任方的匯入詳細資訊。檢查識別符號和終端，瞭解Webbridge服務提供程式的URL詳細資訊。



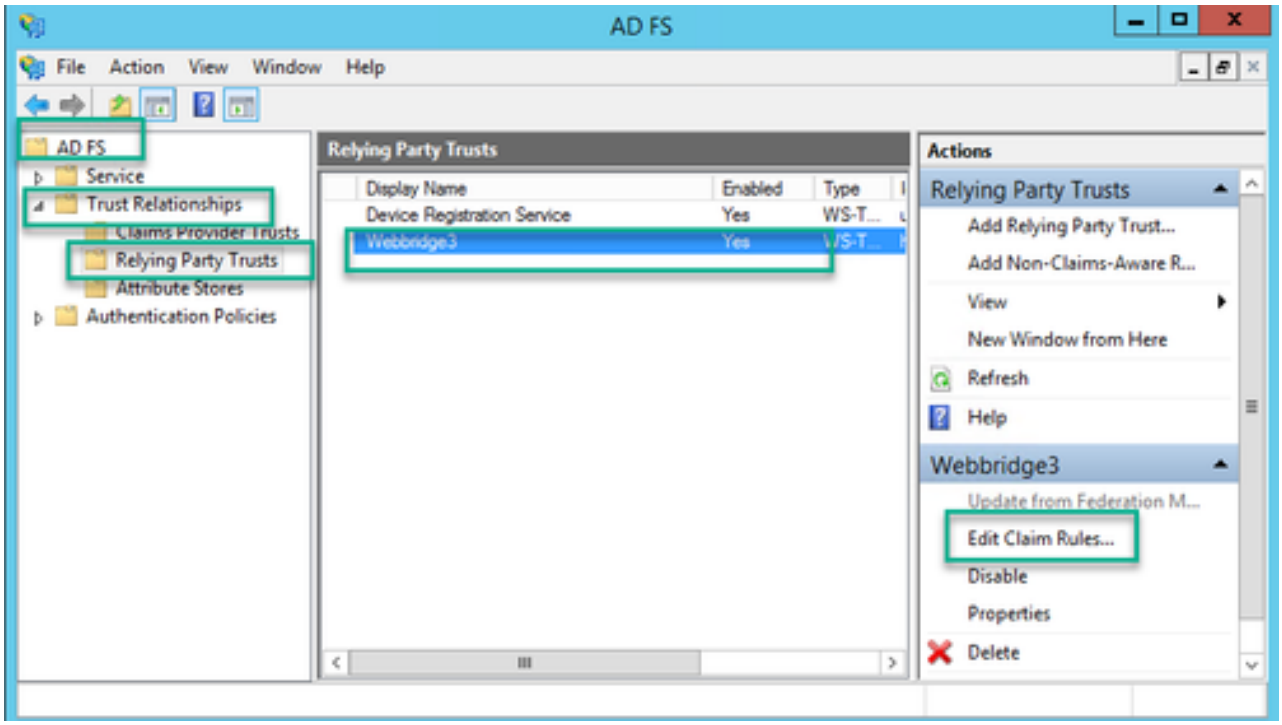
11.在完成頁面上，選擇關閉選項以關閉嚮導並繼續編輯宣告規則。



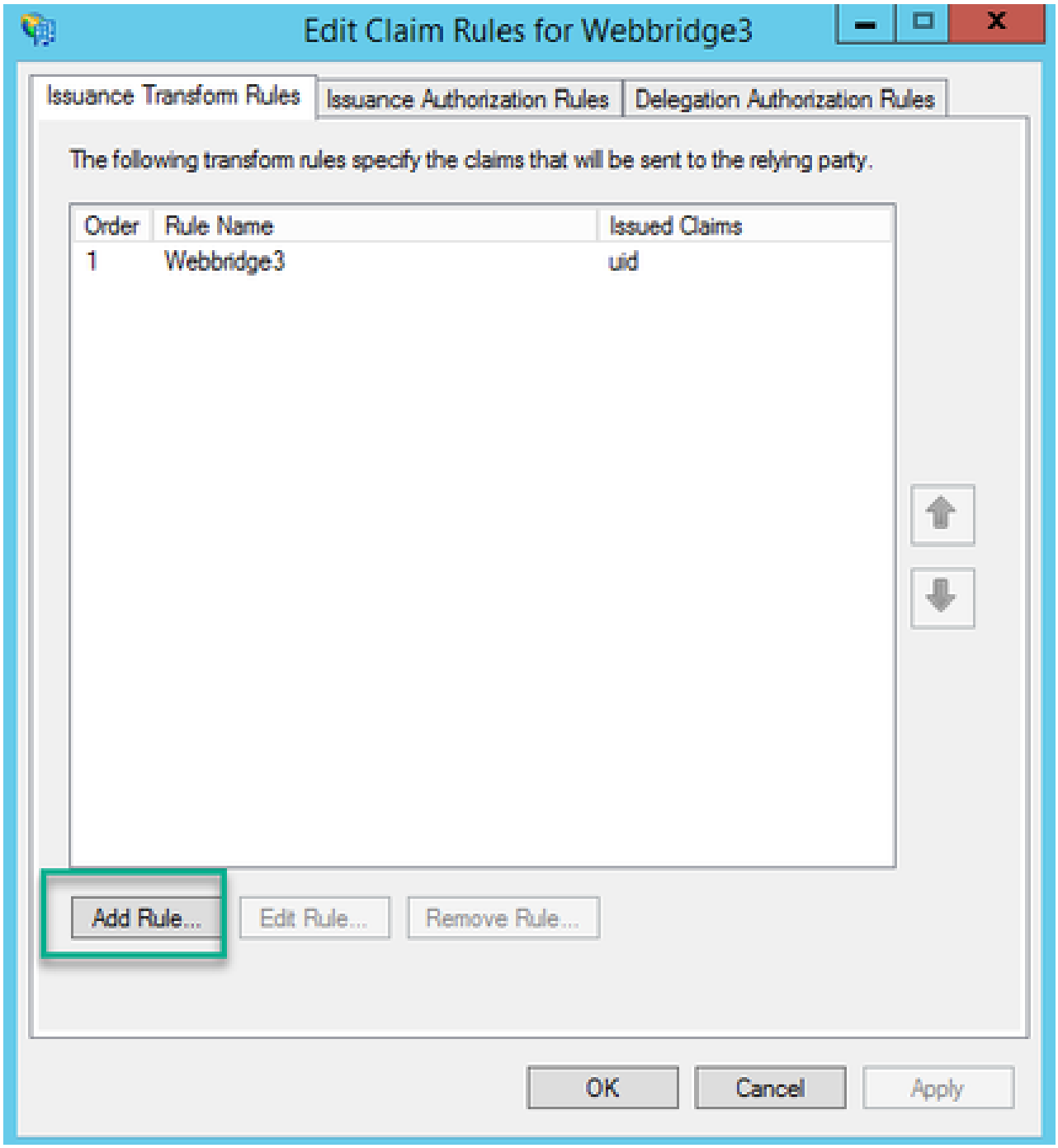
為IdP上的Webbridge服務建立宣告規則

現在，已經為Webbridge建立了信賴方信任，可以建立宣告規則以將特定LDAP屬性與在SAML響應中提供給Webbridge的傳出宣告型別進行匹配。

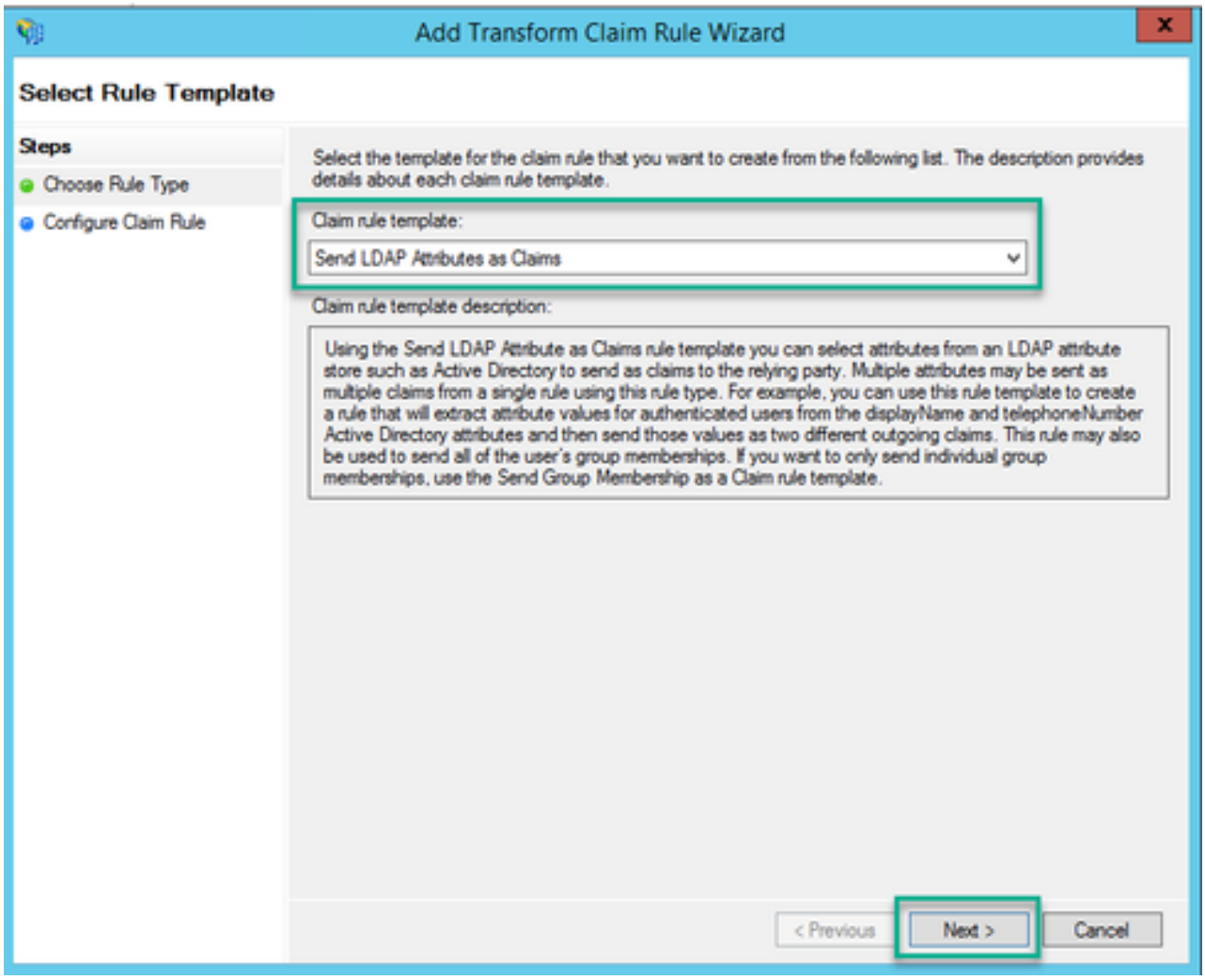
1.在ADFS管理控制檯中，選中Webbridge的信賴方信任，然後在右側窗格中選擇編輯宣告規則。



2.在「編輯<DisplayName>的宣告規則」頁上，選擇添加規則.....

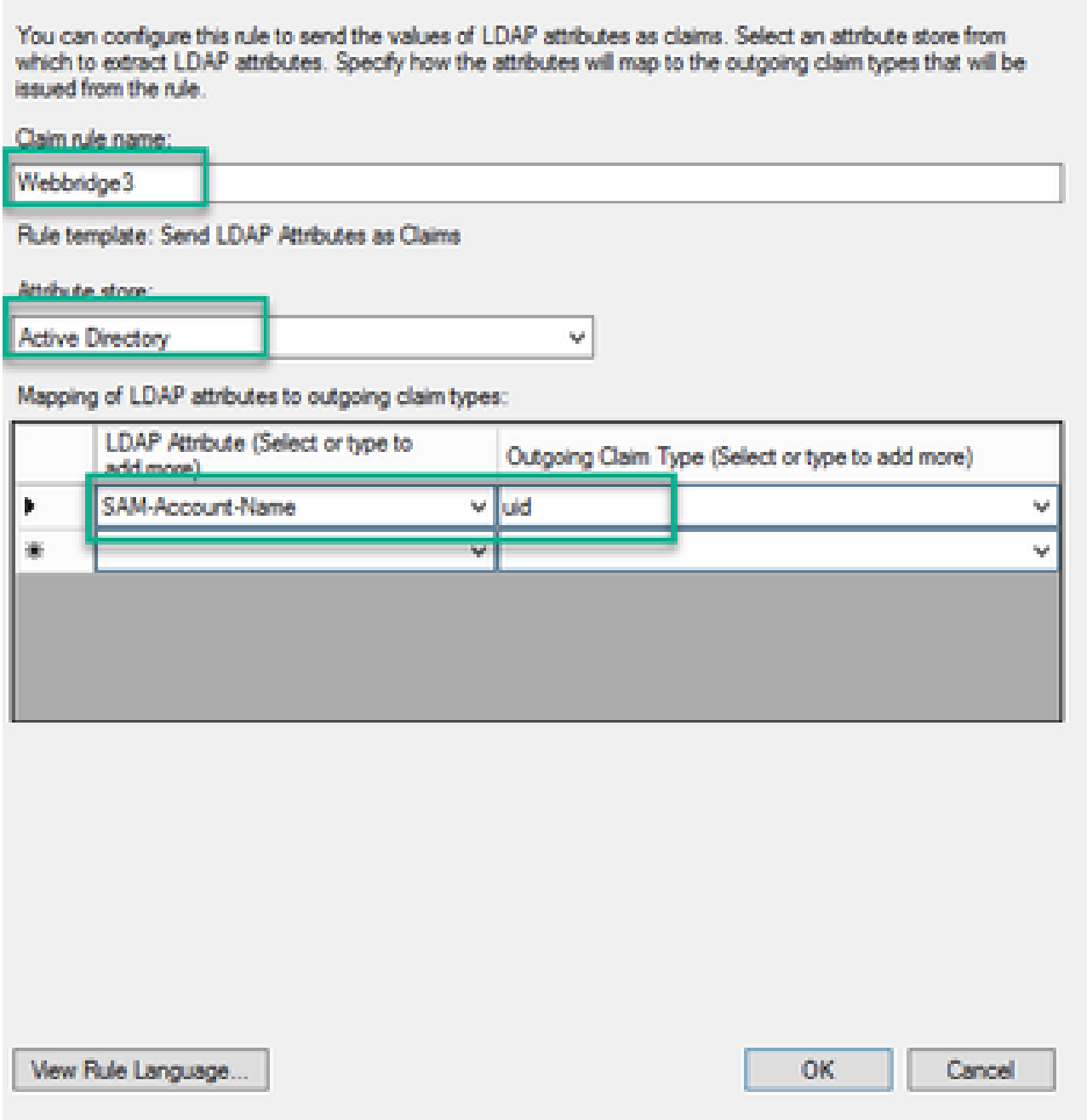


3.在「Add Transform Claim Rule Wizard」頁上，為「Claim rule template」選項選擇Send LDAP Attributes as Claims，然後選擇Next。



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ADFS中為該規則指定的名稱（僅供規則參考）
2. 屬性儲存= Active Directory
3. LDAP屬性=它必須與Callbridge API中的authenticationIdMapping匹配。（例如$sAMAccountName$。）
4. 傳出宣告類型=該型別必須與Webbridge SSO config.json中的authenticationIdMapping相匹配。（例如uid。）



為Webbridge建立SSO存檔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。必須考慮此部分配置的以下規則：

- ZIP檔案必須以sso_prefixed開頭，並將其作為檔名(例如sso_cmstest.zip)。
- 上載此檔案後，Webbridge將禁用基本身份驗證，並且只能將此檔案上載到的Webbridge使用SSO。
- 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(仍以sso_作為字首)。

- 建立zip檔案時，請務必突出顯示並壓縮檔案內容，不要將所需的檔案放入資料夾中並壓縮該資料夾。

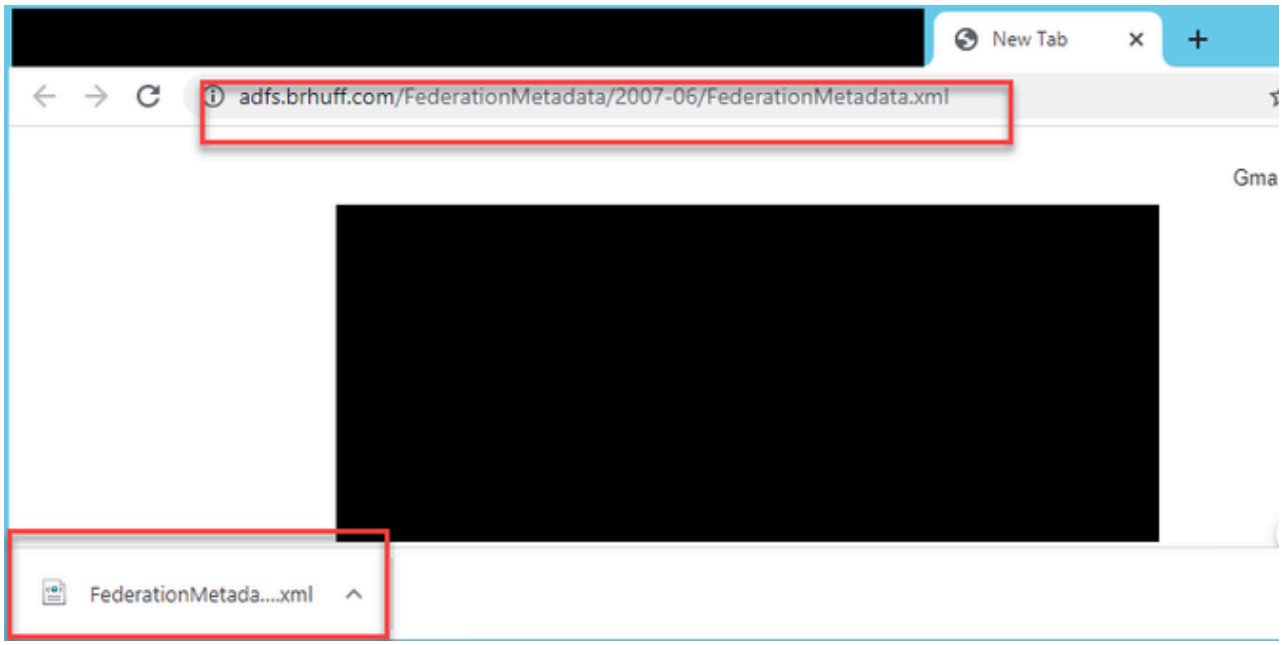
zip檔案的內容由2到4個檔案組成，具體取決於是否使用加密。

檔名	說明	是否必需？
idp_config.xml	這是可以由idP收集的後設資料檔案。在ADFS中，可通過轉至https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml找到該位置。	是
config.json	這是JSON檔案，Webbridge使用該檔案來驗證支援的域，即SSO的身份驗證對映。	是
sso_sign.key	這是在識別提供程式上配置的公共簽名金鑰的私鑰。僅需要保護已簽名資料	否
sso_encrypt.key	這是在識別提供程式上配置的用於公共加密金鑰的私鑰。僅用於保護加密資料	否

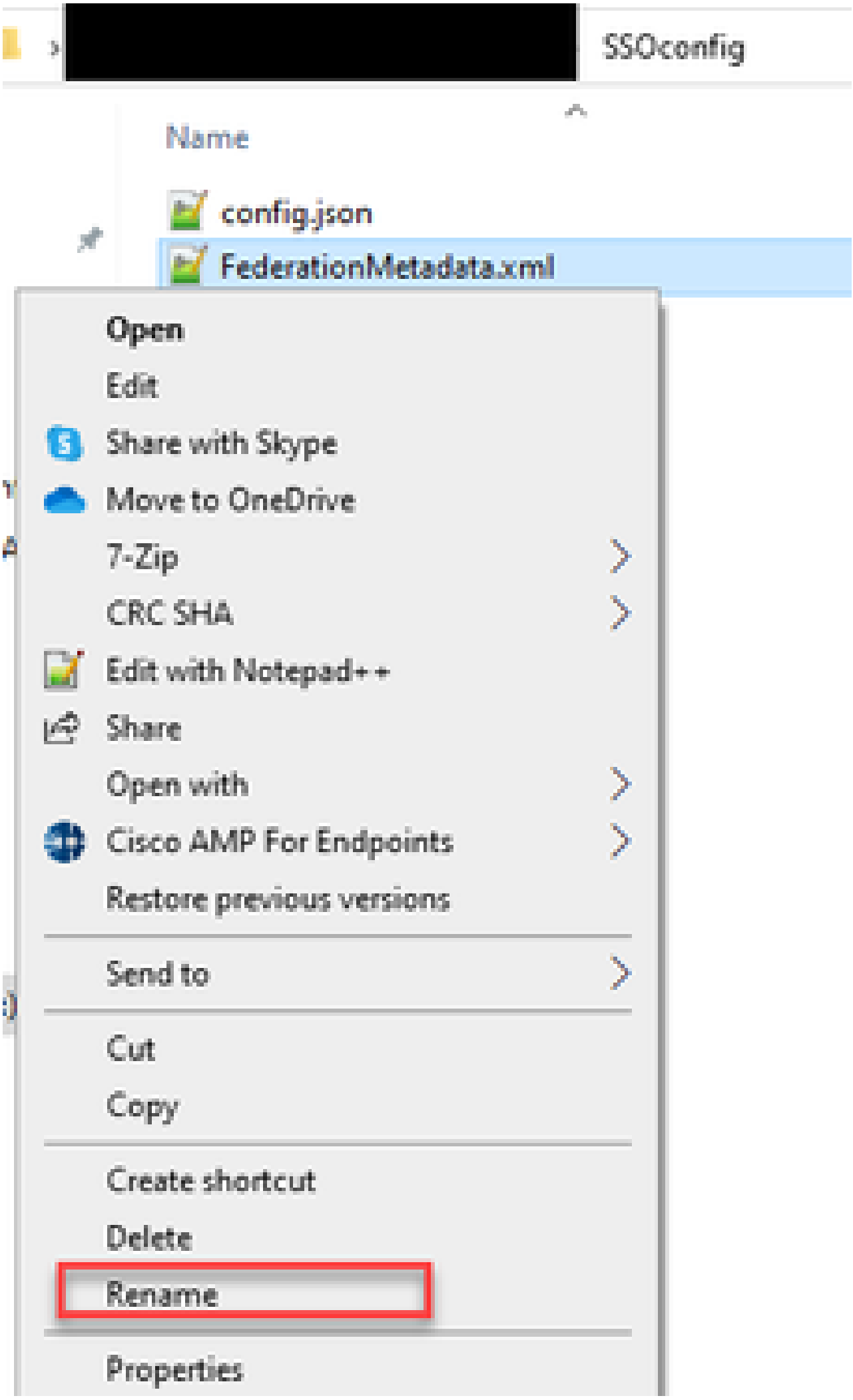
獲取並配置idp_config.xml

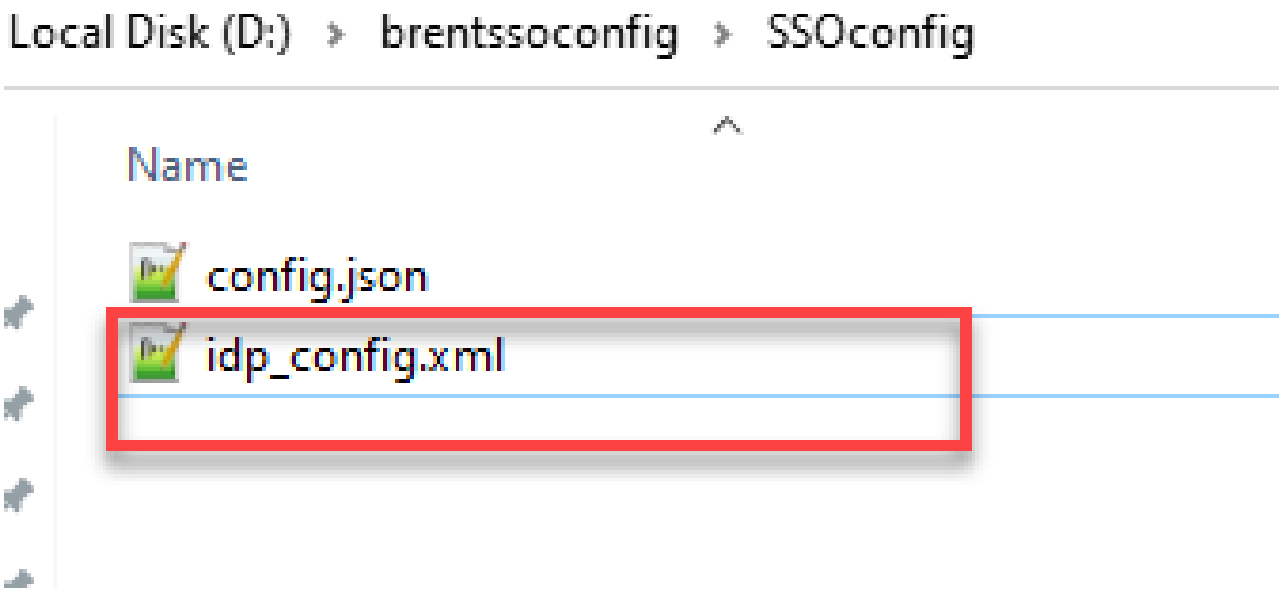
1. 在ADFS伺服器（或可以訪問ADFS的位置）上，開啟Web瀏覽器。

2.在Web瀏覽器中，輸入URL:https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml(如果您在ADFS伺服器上本地，也可以使用localhost而不是FQDN)。這將下載文件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。

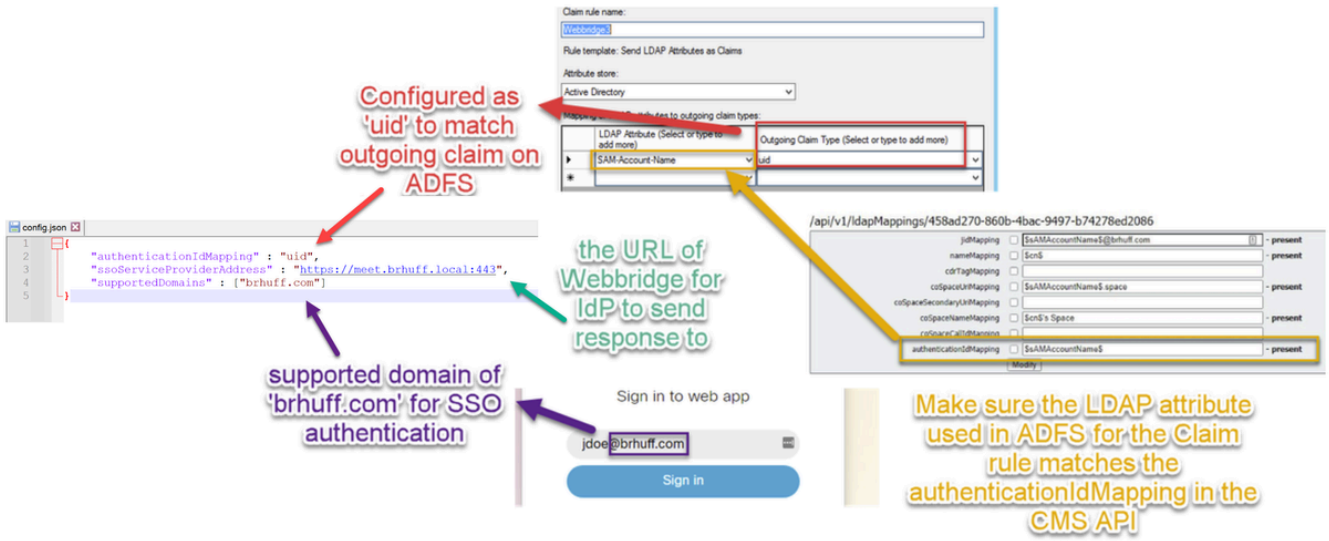

[redacted]
SSOconfig
Name
config.json
FederationMetadata.xml
Open
Edit
Share with Skype
Move to OneDrive
7-Zip
CRC SHA
Edit with Notepad++
Share
Open with
Cisco AMP For Endpoints
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties



建立包含內容的config.json檔案

config.json包含這3個屬性，且它們必須包含在方括弧中，{ }:

1. supportedDomains — 這是根據IdP檢查SSO身份驗證的域清單。可以用逗號分隔多個域。
2. authenticationIdMapping — 這是作為傳出宣告規則的一部分從ADFS/IdP傳回的引數。此值必須與IdP上傳出宣告型別的名稱值匹配。報銷申請規則。
3. ssoServiceProviderAddress — 這是標識提供程式將SAML響應傳送到的FQDN URL。此值必須是Webbridge FQDN。

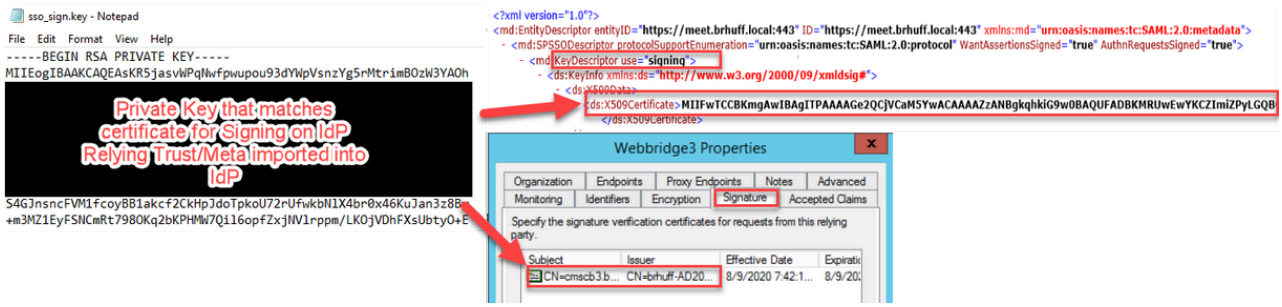


設定sso_sign.key（可選）

此檔案必須包含用於登入匯入到IdP的Webbridge後設資料的證書的私鑰。在ADFS中匯入Webbridge後設資料期間，可以使用在<KeyDescriptor use=signing>部分下的證書資訊填充X509Certificate，從而設定用於簽名的證書。也可以在Webbridge信賴信任方的屬性>簽名下，在ADFS上查看(和匯入)。

在下一個示例中，您可以看到callbridge certificate(CN=cmscb3.brhuff.local)，該證書在匯入到ADFS之前已新增到Webbridge後設資料中。插入sso_sign.key的私鑰是與cmscb3.brhuff.local憑證相符的私鑰。

這是選用組態，只有在要加密SAML回應時才需要。

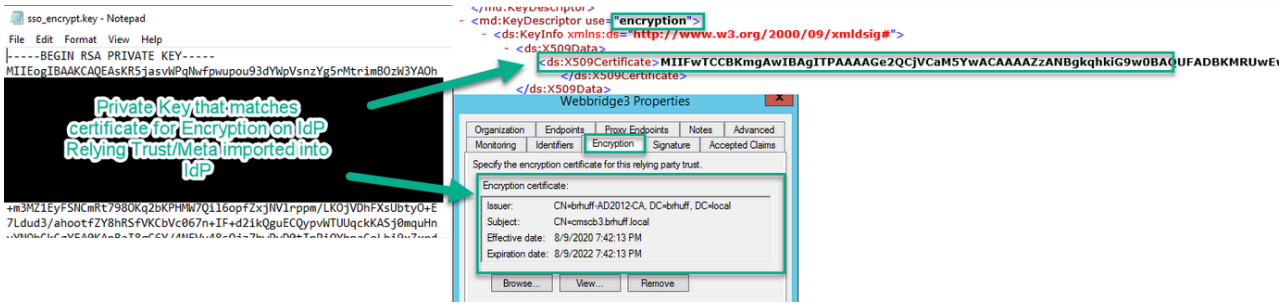


設定sso_encrypt.key（可選）

此檔案必須包含匯入到IdP的Webbridge後設資料中用於加密的證書的私鑰。在ADFS中匯入Webbridge後設資料期間，可通過在<KeyDescriptor use=encryption>部分下使用證書資訊填充X509Certificate來設定用於加密的證書。也可以在Webbridge Reliing Trust Party的ADFS上Properties > Encryption下檢視（和匯入）。

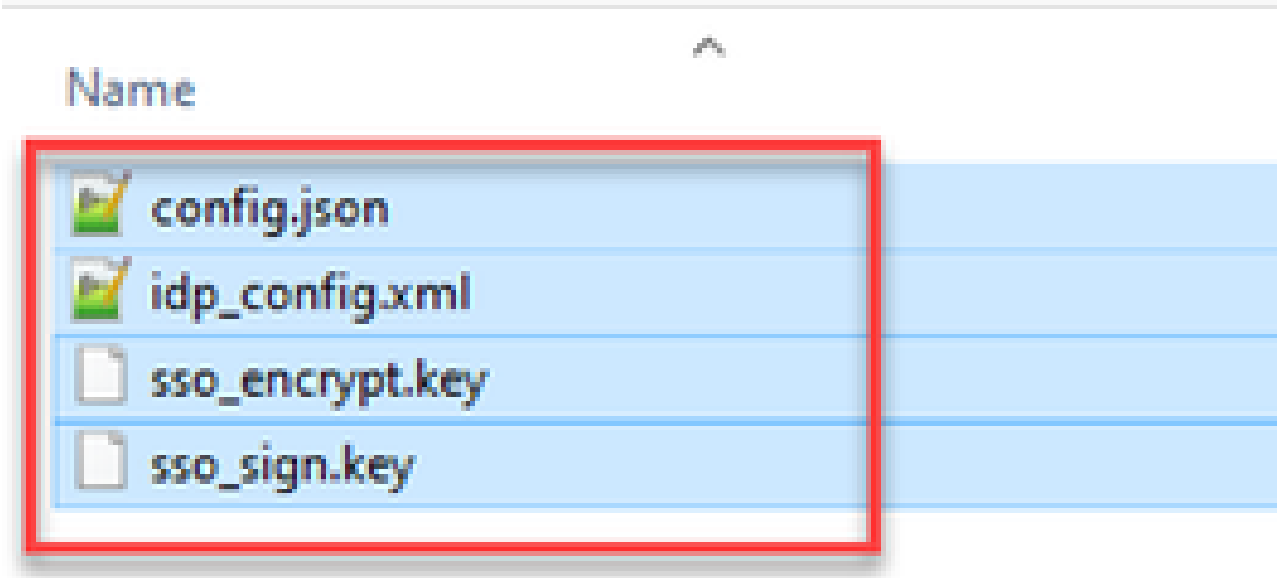
在下一個示例中，您可以看到callbridge certificate(CN=cmscb3.brhuff.local)，該證書在匯入到ADFS之前已新增到Webbridge後設資料中。插入「sso_encrypt.key」的私鑰是與cmscb3.brhuff.local證書匹配的私鑰。

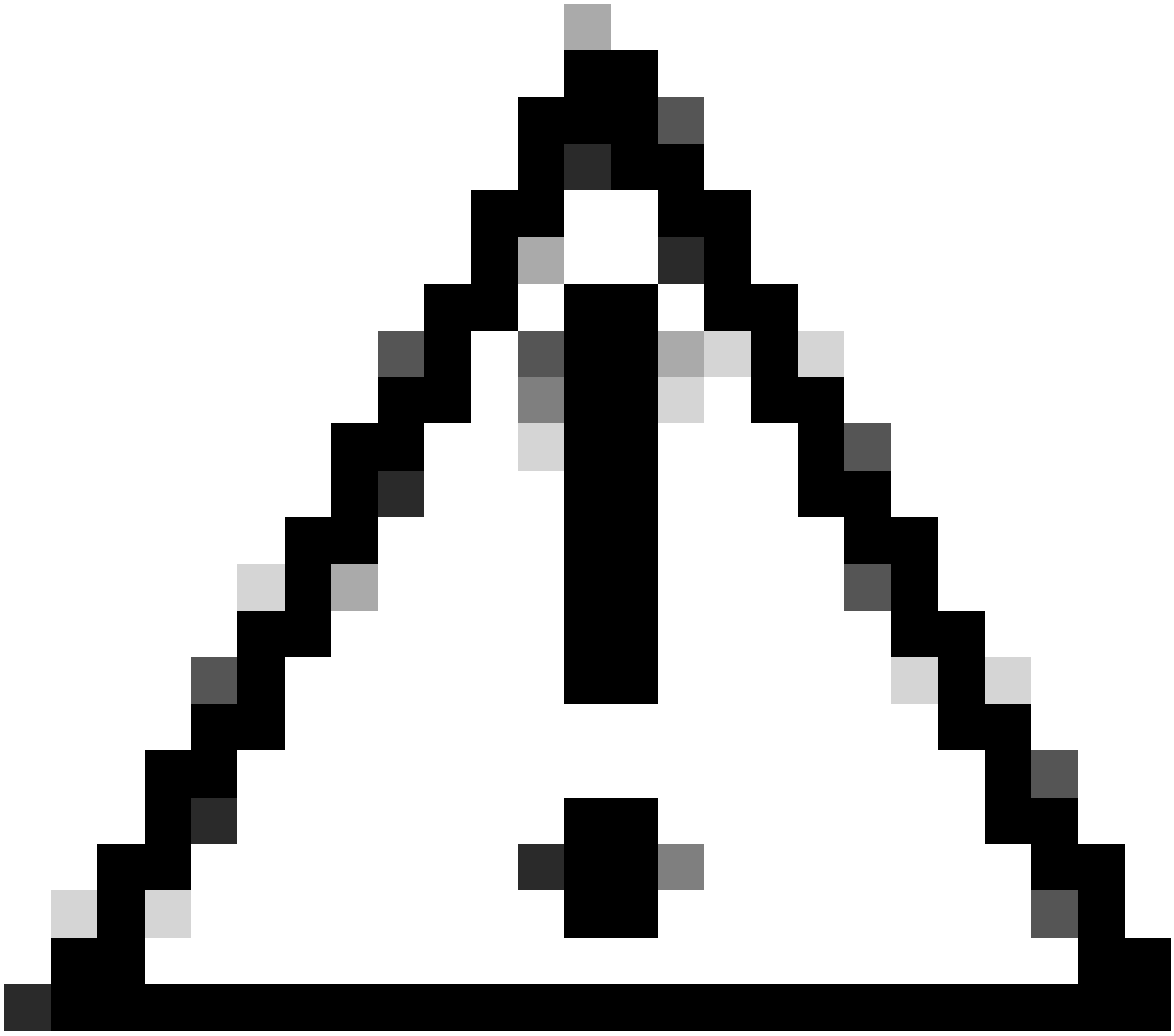
這是選用組態，只有當您打算加密SAML回應時才會需要。



正在建立SSO ZIP檔案

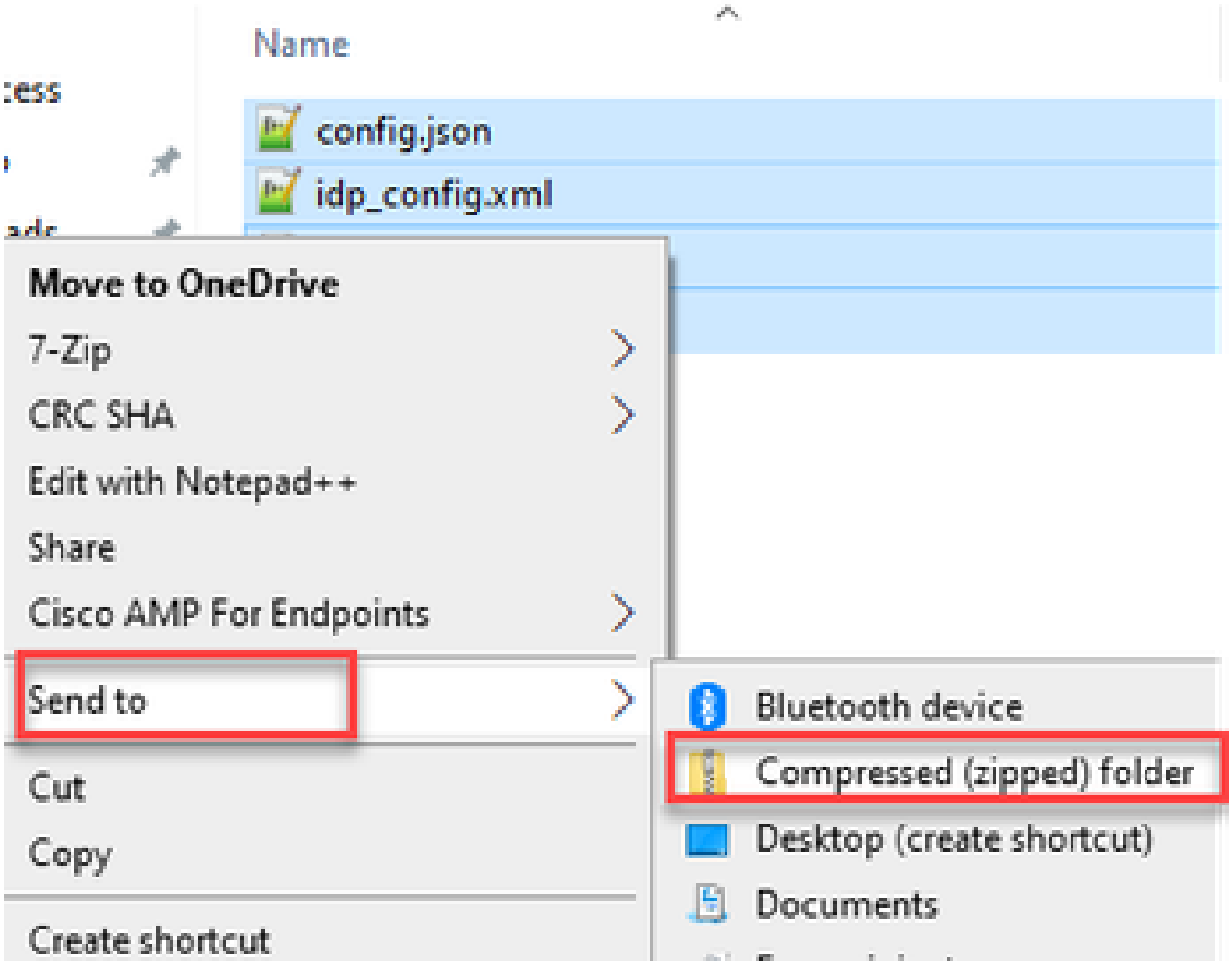
1. 突出顯示要用於SSO配置檔案的所有檔案。



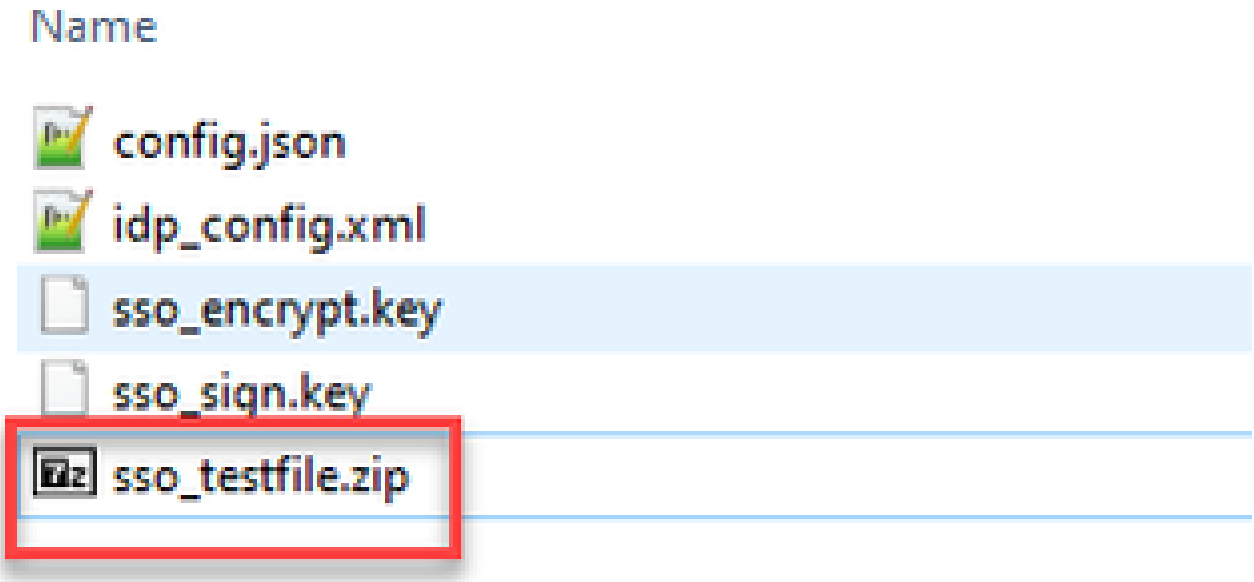


注意：請勿壓縮包含檔案的資料夾，因為這會導致SSO無法正常工作。

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。



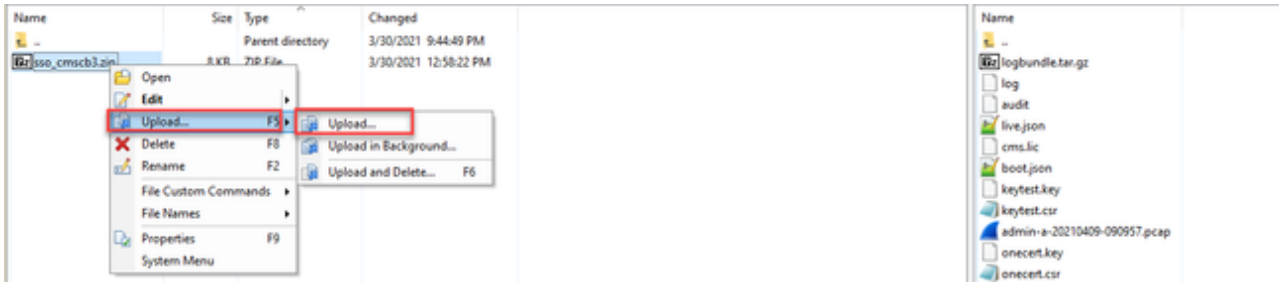
3.壓縮檔案後，將其重新命名為所需的名稱，並使用sso_ prefix:



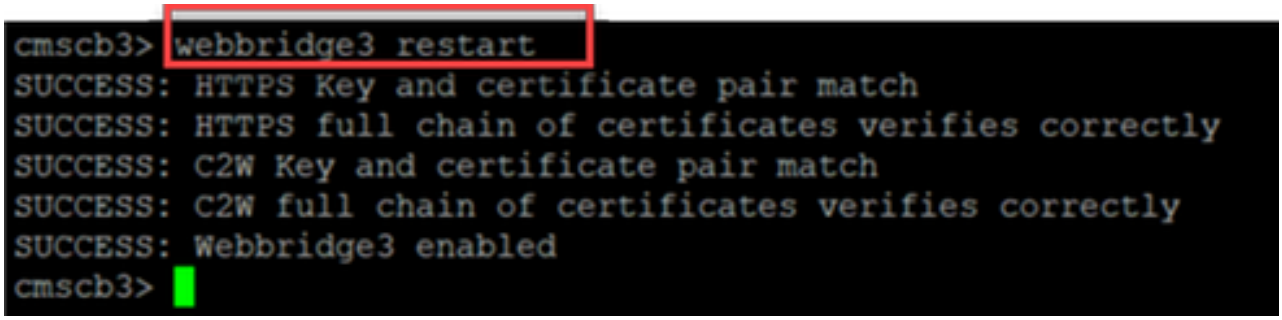
將SSO Zip檔案上傳到Webbridge

開啟SFTP/SCP客戶端（在此示例中使用的是WinSCP），然後連線到託管Webbridge3的伺服器。

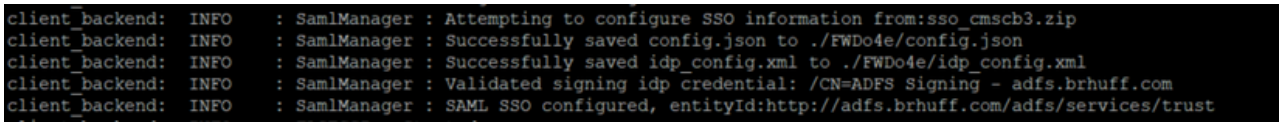
1.在左窗格中，導航到SSO Zip檔案所在的位置，然後按一下右鍵選擇上傳或拖放該檔案。



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



3.在系統日誌中，以下消息指示SSO啟用成功：

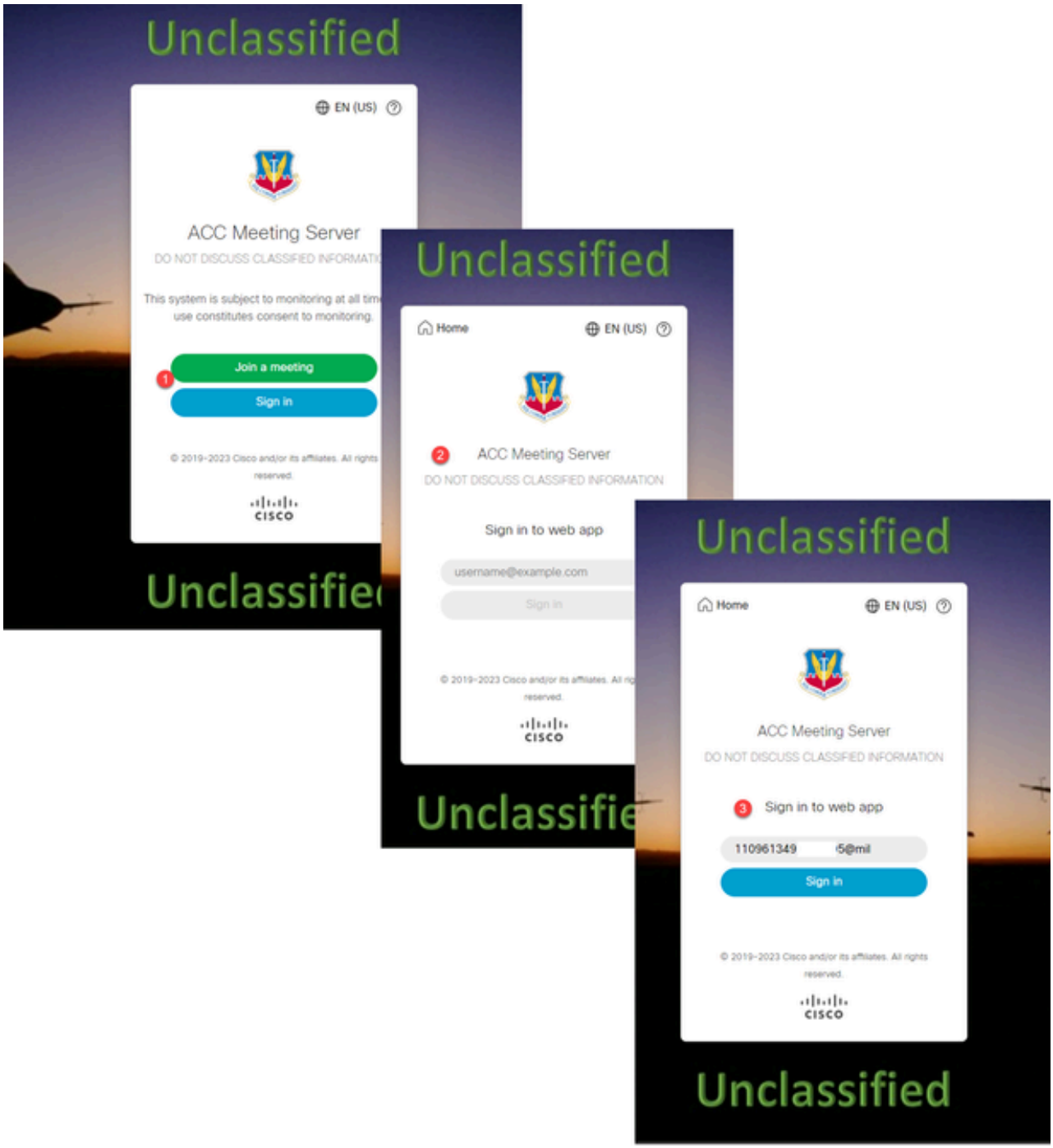


通用存取卡(CAC)

通用訪問卡(CAC)是一種智慧卡，用作現役軍事人員、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卡的使用者的整個登入過程：

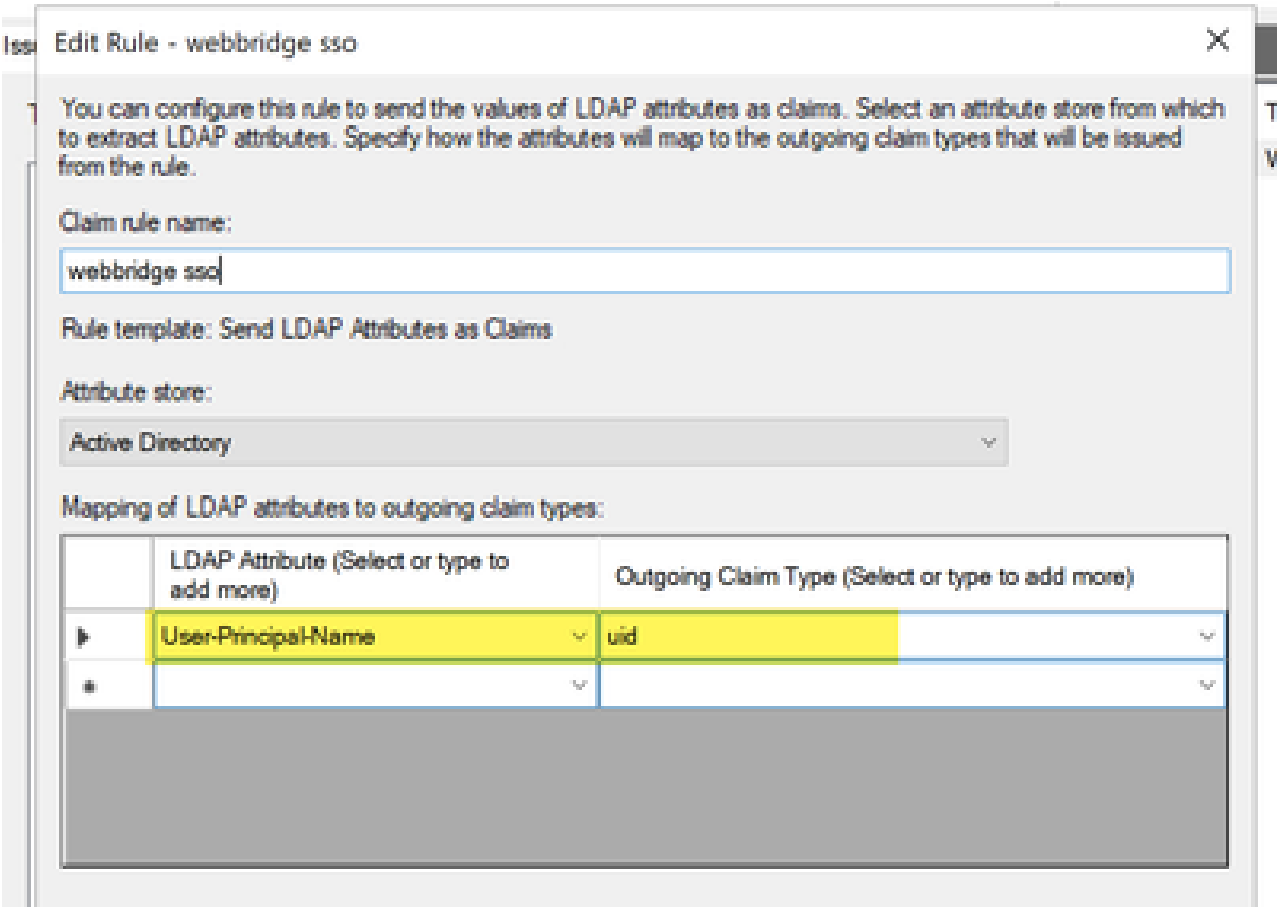
1. 開啟PC，並粘入CAC卡
2. 登入（有時選擇證書），然後輸入Pin
3. 開啟瀏覽器
4. 導航到加入URL並檢視加入會議或登入選項
5. 登入： 輸入配置為jidMapping的使用者名稱，Active Directory希望通過CAC登入進行該使用者名稱
6. 點選登入
7. ADFS頁面會短暫顯示並自動填充
8. 使用者此時已登入



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

還為authenticationIdMapping設定相同的LDAP屬性，以匹配ADFS中的宣告規則中使用的屬性。

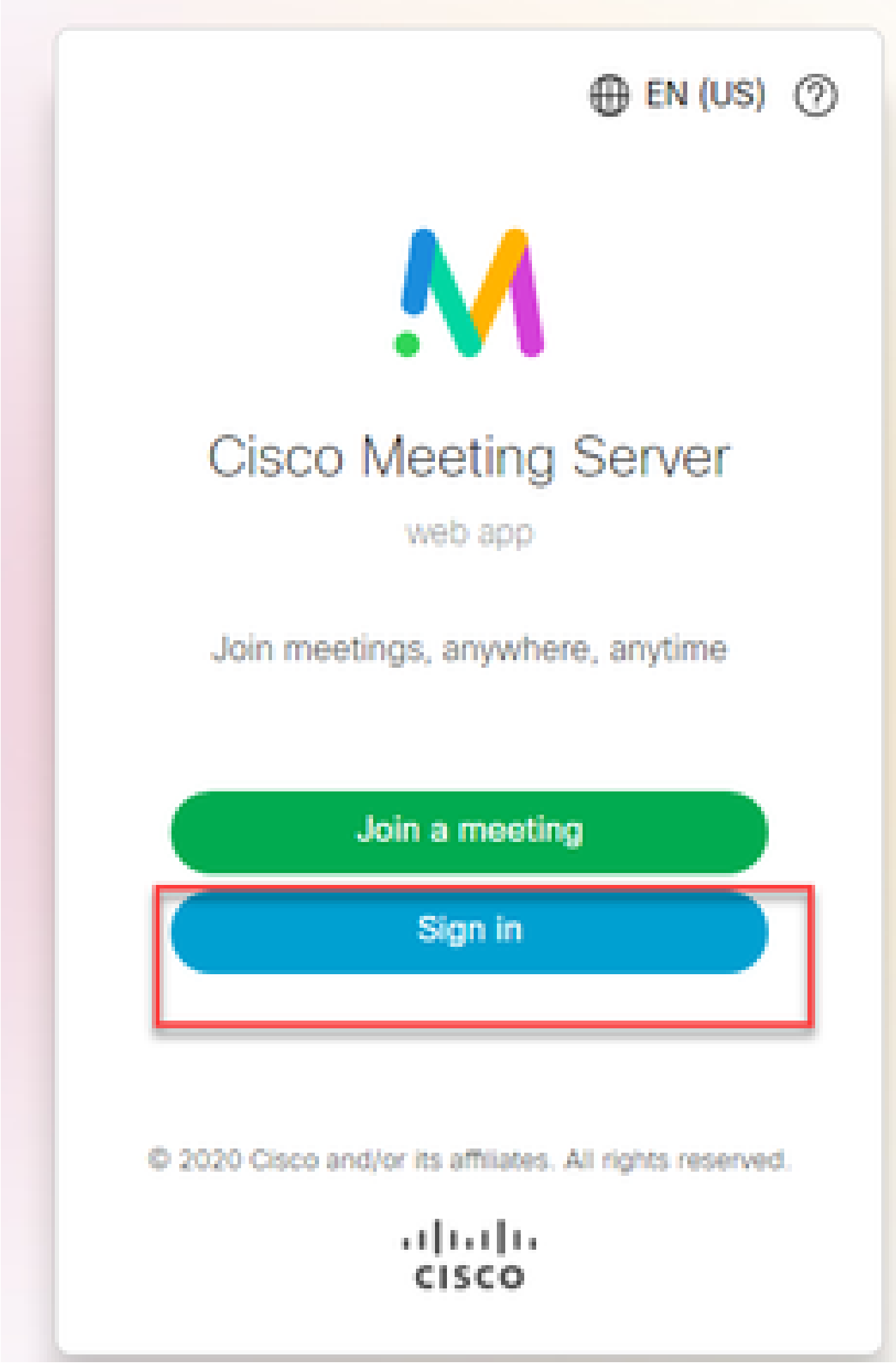
在這裡，宣告規則顯示它將將$userPrincipalName$作為UID傳送回CMS。



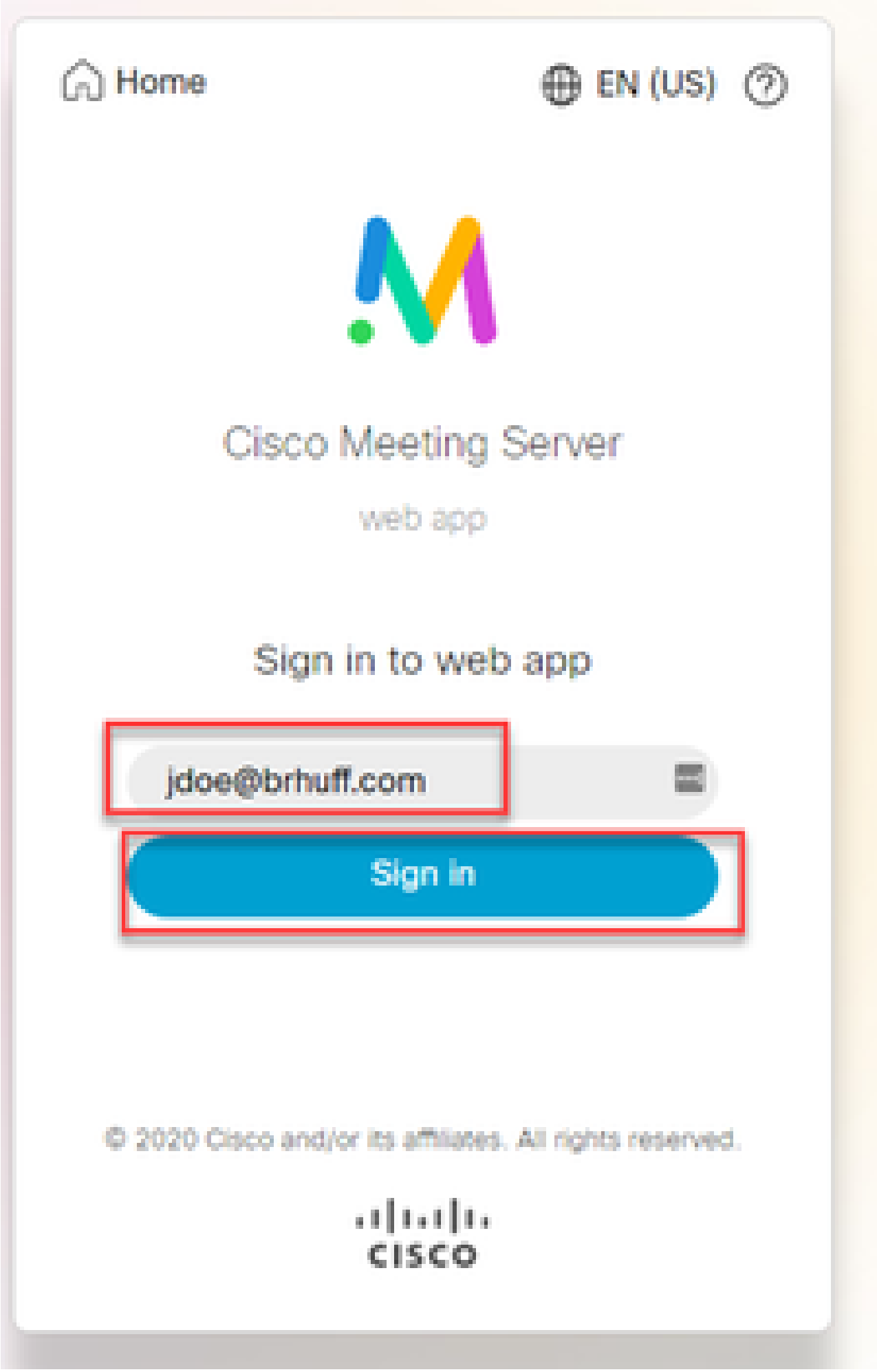
正在測試通過WebApp的SSO登入

配置了SSO後，即可測試伺服器：

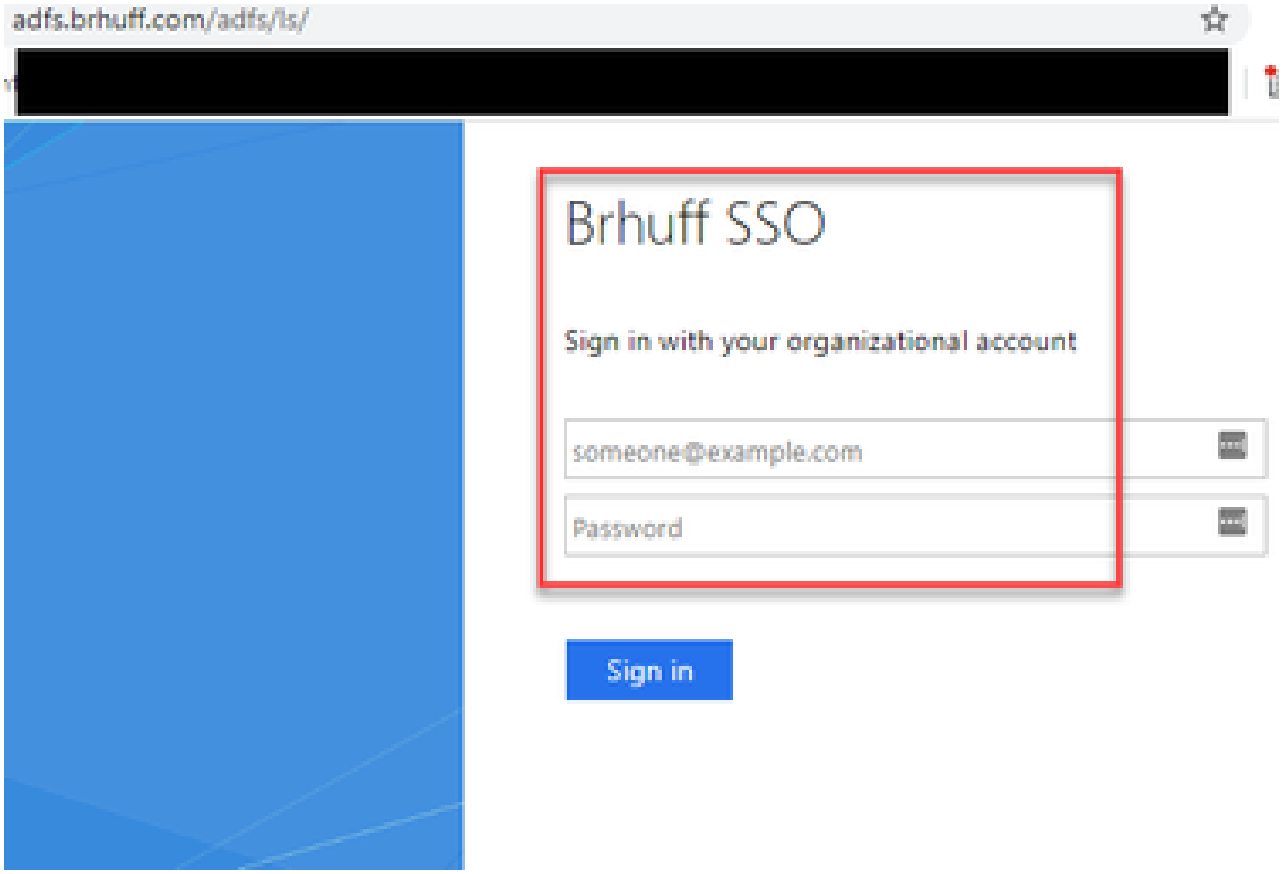
1. 導航到Web應用的Webbridge URL，然後選擇Sign in按鈕。


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

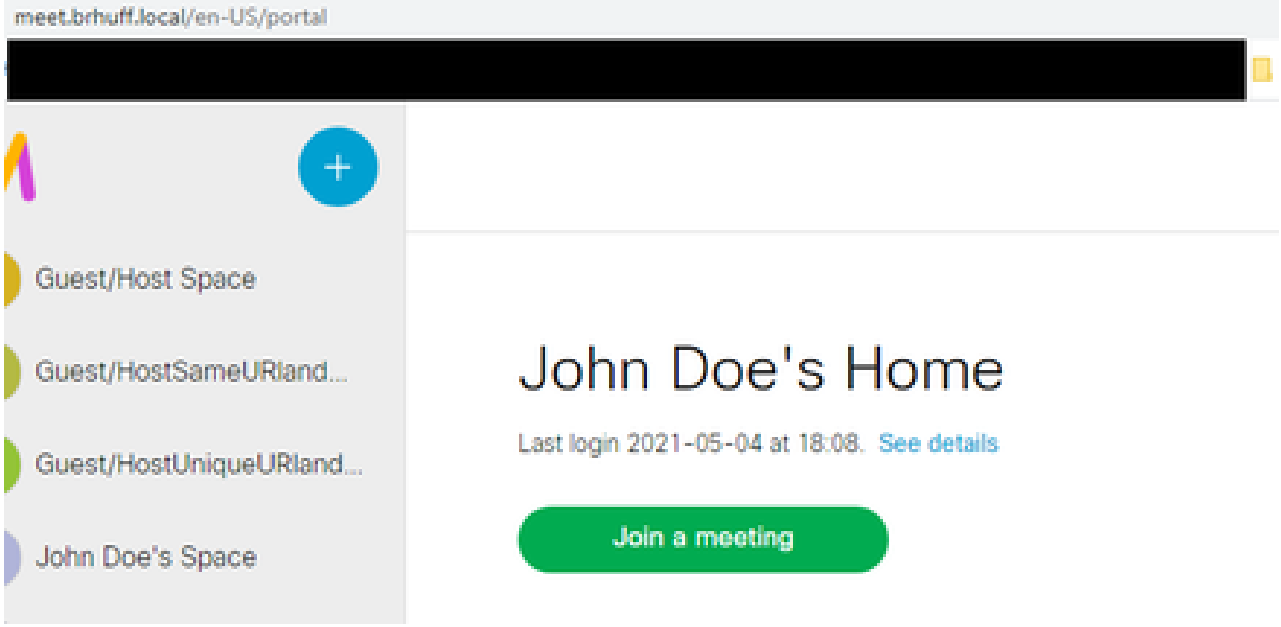
2.系統向使用者提供輸入其使用者名稱的選項（請注意此頁上沒有password選項）。


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，使用者被重定向到ADFS頁（輸入使用者詳細資訊後），使用者必須輸入其憑證才能對IdP進行身份驗證。



4.使用者使用IdP輸入並驗證憑證後，使用令牌重定向以訪問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中作為Reliing Trust匯入的Webbridge3的已構造後設資料，並且配置的URL與config.json中的ssoServiceProviderAddress完全匹配。
2. 確保IdP提供的後設資料已壓縮到Webbridge3中，因此IdP中的後設資料是最新的後設資料，就像伺服器主機名、證書等有任何更改一樣，需要將其重新匯出並壓縮到配置檔案中。
3. 如果使用簽名和加密私鑰加密資料，請確保正確的匹配金鑰是上傳到webbridge的sso_xxxx.zip檔案的一部分。如果可能，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和預期身份驗證對映的正確詳細資訊，以便從SAMLResponse匹配。

嘗試從日誌角度進行故障排除也很理想：

1. 導航到Webbridge URL時，將?trace=true放在URL末尾，以便在CMS系統日誌上啟用詳細日誌記錄。(例如：https://join.example.com/en-US/home?trace=true)。
2. 在Webbridge3伺服器上運行syslog follow，以在測試期間捕獲即時資料，或使用附加到URL的跟蹤選項運行測試，並從Webbridge3和CMS Callbridge伺服器收集logbundle.tar.gz。 如果webbridge和callbridge位於同一伺服器上，則只需一個logbundle.tar.gz檔案。

Microsoft ADFS故障代碼

有時，SSO進程出現故障會導致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出現故障並採取補救操作：

Microsoft狀態代碼

例如：

> client_backend:錯誤：SamlManager:SAML身份驗證請求_e135ca12-4b87-4443-abe1-30d396590d58失敗，原因：urn:oasis：名稱：tc:SAML:2.0：狀態：響應方

此錯誤表示根據以前的文檔，該故障是由IdP或ADFS引起的，因此需要由ADFS的管理員處理才能解決。

無法獲取authenticationID

在某些情況下，在從IdP交換SAMLR響應期間，Webbridge可以在日誌中顯示此錯誤消息，但通過SSO登入失敗：

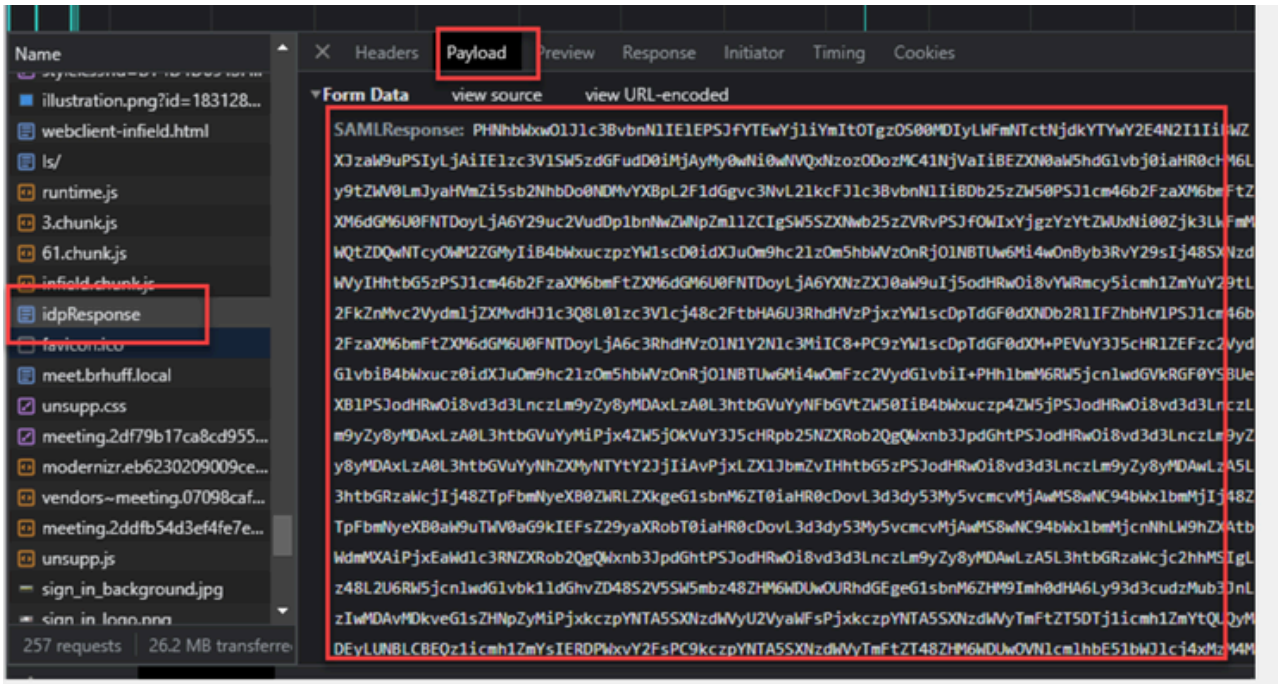
> client_backend:資訊：SamlManager:[57dff9e3-862e-4002-b4fa-683e4aa6922c]獲取身份驗證Id失敗

這表示在檢查身份驗證交換期間從IdP傳回的SAMLResponse資料時，Webbridge3在響應中找不到與authenticationId的config.json相比的有效匹配屬性。

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

記錄網路日誌時，確保選中了「保留日誌」擷取方塊，以便在頁面更改時不會覆蓋日誌。

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，可以使用base64解碼器對此進行解碼。



在接收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，您可以查詢從IdP配置和傳送的宣告型別。舉例來說：

```
<AttributeStatement>
<Attribute Name="<Commonname的URL">
<AttributeValue>testuser1</AttributeValue>
```

```
</Attribute>
<Attribute Name="<NameID的URL">
<AttributeValue>testuser1</AttributeValue>
</Attribute>
<Attribute Name="uid">
<AttributeValue>testuser1</AttributeValue>
</Attribute>
</AttributeStatement>
```

檢查以前的名稱，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，您可以看到authenticationIdMapping的配置與傳遞的內容不完全匹配，從而導致找不到匹配的authenticationId:

authenticationId對映：http://example.com/claims/NameID

為了解決此問題，可以嘗試兩種方法：

1. 可以更新IdP傳出宣告規則，使其具有與Webbridge3上config.json的authenticationIdMapping中配置的完全匹配的宣告。(在http://example.com/claims/NameID的IdP上新增宣告規則)
   或
2. 可以在Webbridge3上更新config.json，使「authenticationIdMapping」與IdP上配置的傳出宣告規則之一完全匹配。(即「authenticationIdMapping」要更新以匹配屬性名稱之一，屬性名稱可以是「uid」、「<URL>/NameID」或「<URL>/CommonName」。 只要它與（完全）通過時在Callbridge API上配置的預期值匹配)

在驗證中未傳遞/匹配斷言

有時，在從IdP交換SAMLRresponse期間，Webbridge會顯示此錯誤，指示匹配斷言失敗，並跳過任何與伺服器配置不匹配的斷言：

client_backend:錯誤：SamlManager:未通過驗證的斷言
client_backend:資訊：SamlManager:在允許的受眾中跳過斷言

此錯誤表示當從IdP檢視SAMLR響應時，Webbridge無法找到任何匹配斷言，因此跳過了非匹配失敗，最終導致失敗的SSO登入。

為了找到此問題，最好是從IdP檢視SAMLR響應。如果沒有使用簽名和加密私鑰對通訊進行加密，則可以通過Web瀏覽器從Developer Tools Network Logging提取SAML響應，並使用base64進行解碼。如果響應已加密，則可以從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受眾：

<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>部分(https://cisco.example.com))中的值，可以將其與Webbridge配置的config.json中的ssoServiceProviderAddress進行比較，並驗證其是否完全匹配。在本例中，您可以看到失敗的原因是受眾與配置中的服務提供商地址不匹配，因為它附加了:443:

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

這要求兩者之間完全匹配，以免導致此類故障。在本例中。修正方法可以是以下兩種方法中的任一種：

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

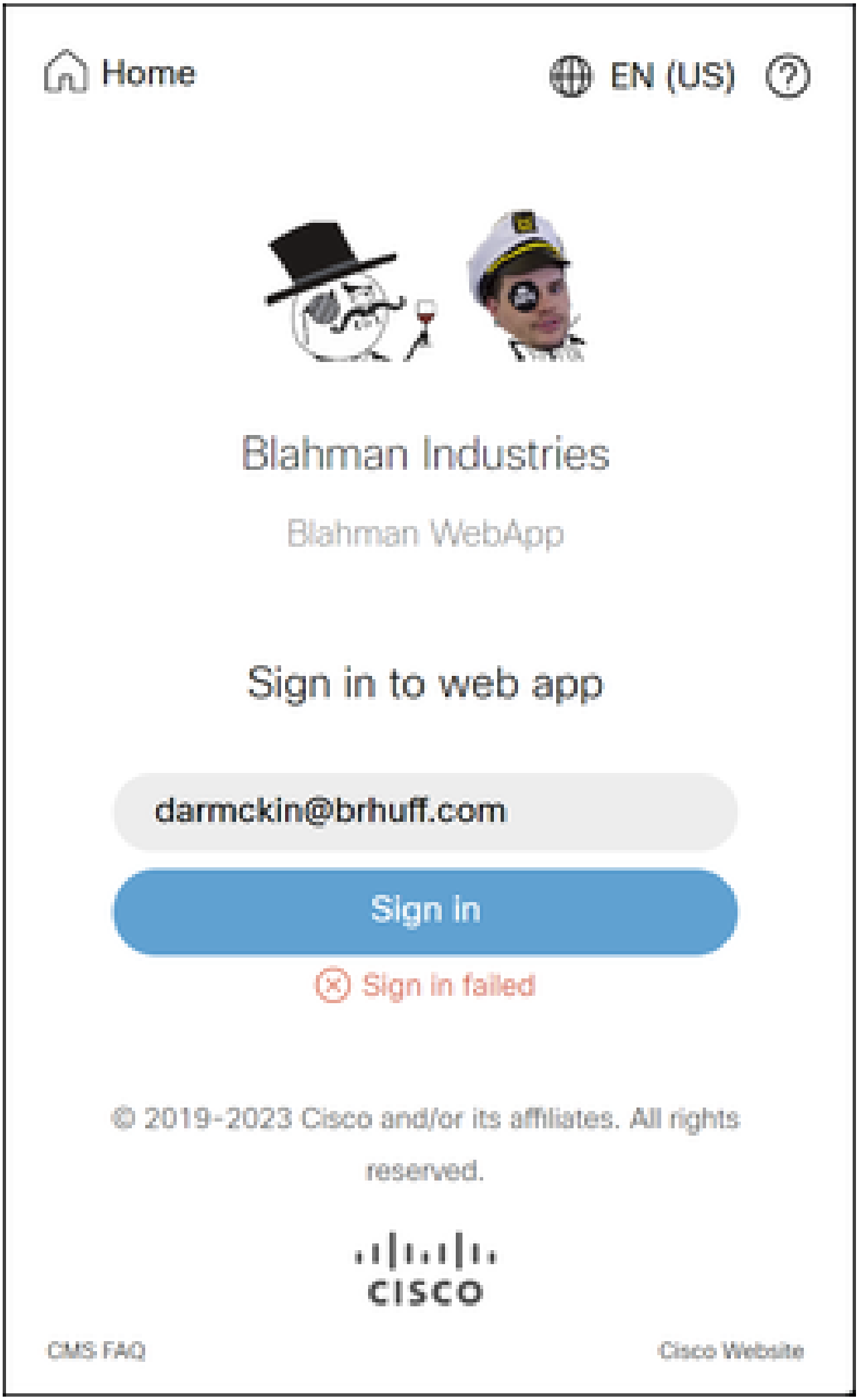
2.可以更新IdP中Webbridge3的後設資料或信賴信任方，以便將:443附加到URL。(如果更新了元資料，則必須再次將其作為ADFS上的信賴信任方導入。但是，如果直接從IdP嚮導修改信賴信任方，則不需要再次匯入它。)

另外，請注意條件NotBefore和NotONOrAfter:<條件NotBefore=2021-03-30T19:35:37.071Z NotOnOrAfter=2021-03-30T19:36:37.071Z>

如果伺服器時間不正確，則可能導致該時間超出條件中定義的有效期。您將要使用ntp server list 命令通過CLI檢查NTP伺服器，以檢查已配置的NTP伺服器，並檢查ntp status 以檢查已配置的NTP伺服器的狀態。使用命令date驗證伺服器時間。

提示：如果使用本地/內部NTP伺服器，請嘗試配置公共NTP伺服器，例如time.google.com（確保在此之前配置公共DNS伺服器）。

在Web應用上登入失敗：


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

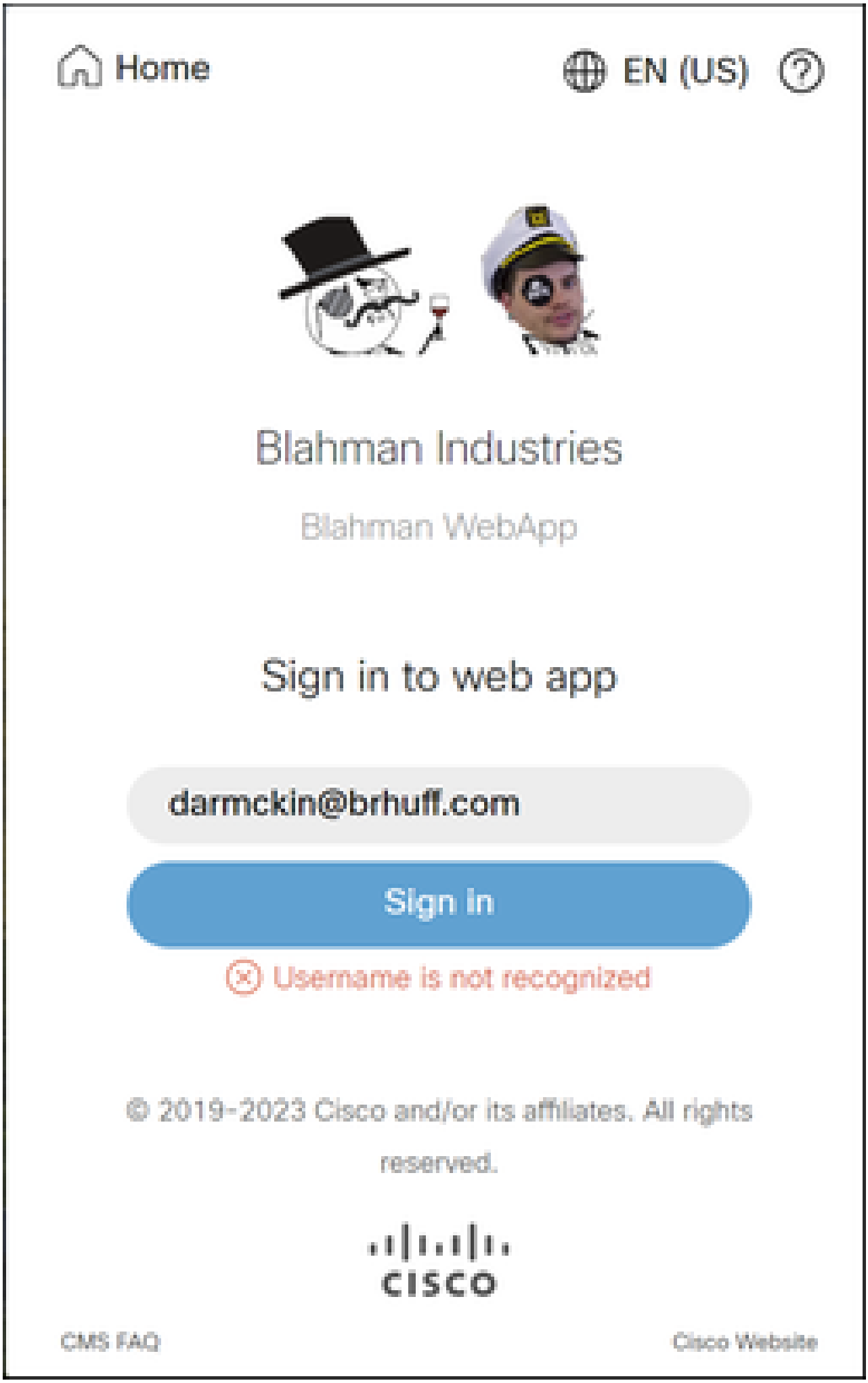
WB3Cmgr:[79e9a87e-0fa4-44df-a914-bbcabb6c87c6] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c-0272-42a1-b125-136fdf5612a5(user=steve@brhuff.com)

3月18日14:58:48.092 user.info cmscb3-1 host:server: 資訊：未找到用於授權的使用者

3月18日14:58:48.092 user.info cmscb3-1 host:server: 資訊：來自steve@brhuff.com的登入請求失敗

案例 2:

使用者在Web應用中輸入了正確的登入資訊，並在SSO頁中輸入了正確的憑據以向LDAP進行身份驗證，但無法登入，原因是無法識別使用者名稱。


Home
EN (US)
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.
CISCO
CMS FAQ
Cisco Website

無法識別使用者名稱

WB3Cmgr:[d626bbaf-80c3-4286-8284-fac6f71eb140] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5註冊=40a4026c-0272-42a1-b125-136fdf5612a5(使用者=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

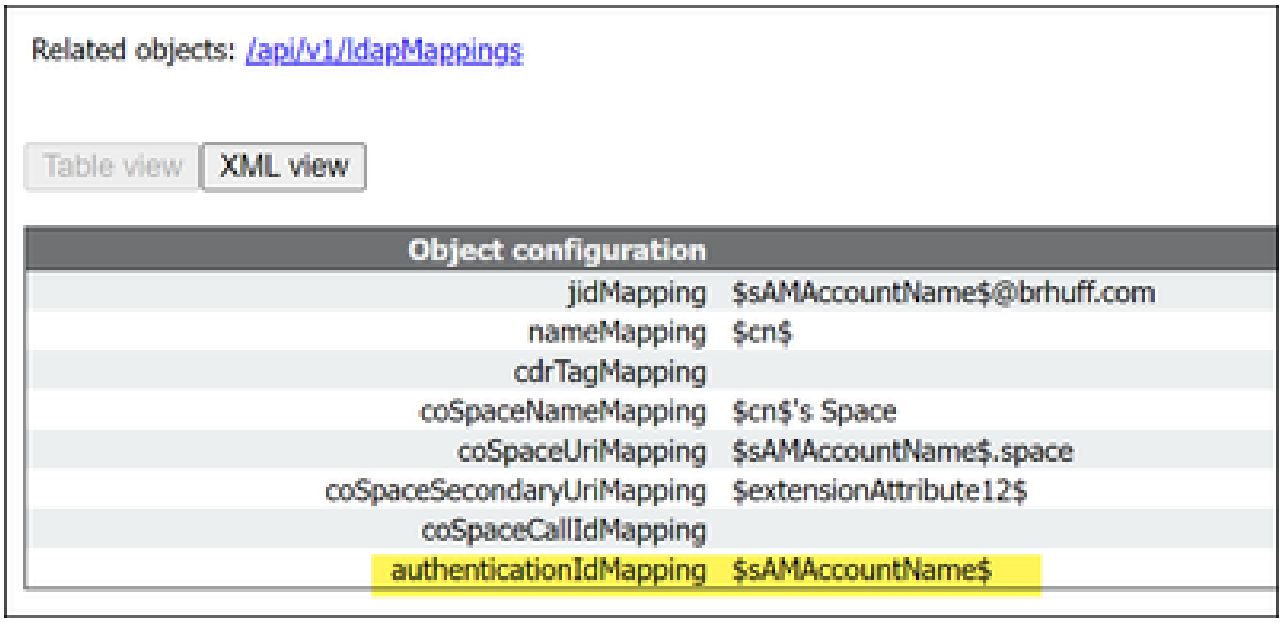
3月18日15:08:52.412 user.info cmscb3-1 host:server: 資訊：來自darmckin@brhuff.com的登入請求失敗

CMS ldapmapping中的AuthenticationIdMapping與ADFS中用於宣告規則的已配置LDAP屬性不匹配。 「Successfully obtained authenticationID:darmckin@brhuff.com」一行表示ADFS已配置宣告規則，其屬性從Active Directory中獲取darmckin@brhuff.com，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E-mail-Addresses，因此不匹配。

如何解決此問題：

執行任一選項以緩解：

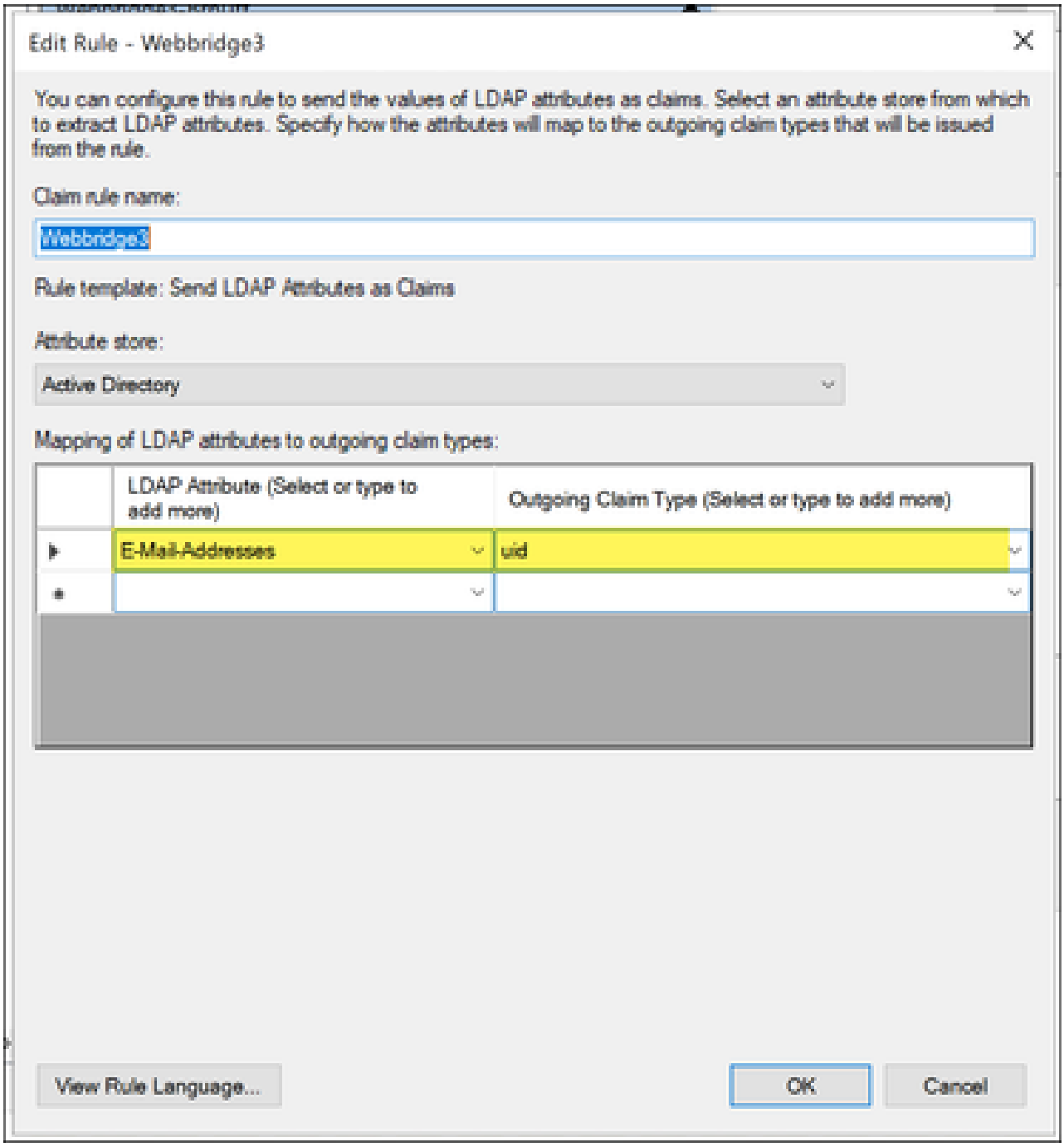
1. 更改CMS ldapmapping中的AuthenticationID以匹配ADFS上的宣告規則中使用的內容，並執行新的同步
2. 更改ADFS宣告規則中使用的LDAP屬性，以匹配CMS ldapmapping中配置的屬性



API LDAPMapping

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

API使用者示例



來自ADFS的宣告規則

顯示工作登入示例的Webbridge日誌。 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SAML令牌請求中的SSO_2024.zip

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] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c-0272-42a1-b125-136fdf5612a5(user=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: 資訊：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:server: 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, Tracing:7979f13c-d490-4f8b-899c-0c82853369ba] 10.10.10.8 — [18/Mar/2024:18:24:01 +000] status 200 "POST /api/auth/sso/idpResponse HTTP/1.1" bytes_sent 0 http_referrer "https://adfs.brhuff.com/" http_user_agent "Mozilla/5 (Windows NT 10.0;Win64;x64)AppleWebKit/537.36（KHTML，類似壁虎）Chrome/122.0.0。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

常見問題 (FAQ)

本節重點介紹思科會議伺服器上與WebApp SSO有關的常見問題或主題。

Webapp SSO JWT是否可以擴展？

JSON Web令牌(JWT)是由Callbridge提供給已成功驗證的WebApp客戶端（已成功驗證為IdP）的令牌，授予他們對WebApp服務的訪問許可權。在JWT內有一個到期計時器值，它指示JWT的有效時間，一旦達到JWT到期時間，WebApp使用者將重定向回Webbridge登入頁面，需要重新驗證才能重新獲得訪問許可權。

可以使用「callbridge wc3jwt expiry <1-24>」(在3.8及更高版本中新增 — 更多詳細資訊可在CMS

3.8發行說明或CMS MMP指南中找到)來配置JWT到期，其中數值表示要設定提供給WebApp客戶端的JWT到期時間的小時數。但是，如命令所示，最大值可以設定為24小時，這意味著JWT可以保持有效的最長時間以及WebApp使用者可以登入的時間是24小時。滿足JWT到期時間時 — 瀏覽器將轉儲到期令牌，WebApp使用者將被強制返回到WebApp登入頁面。

在某些環境中，根據IdP和環境設定，可以在IdP上實現持續SSO/保持我的登入功能，該功能將為瀏覽器提供從IdP進行的持續登入，即使關閉瀏覽器，也會保留cookie（除非通過其他方法清除）。無論SSO/IdP配置如何 — 當JWT過期時(最多24小時),WebApp使用者將被強制返回到WebApp登入頁 — 但是，在這種情況下，在IdP上啟用持續SSO使用者將只需輸入其即可<user@domain>，且無需重新驗證其IdP。

實施刷新令牌機制以允許擴展對WebApp的授權的增強功能已開啟 — 思科錯誤ID CSCwm28758。

如果我關閉瀏覽器，是否需要重新向WebApp進行身份驗證？

此情境的流程如下：

1. 使用者登入到WebApp（使用SSO身份驗證方法）。
2. 使用者會在某些時候關閉瀏覽器。
3. 使用者再次開啟瀏覽器並導航到WebApp站點。（立即或在稍後）。

在這種情況下，會發生什麼？

答案取決於！這完全取決於Callbridge提供的JWT在訪問WebApp頁面時是否過期。只要JWT仍然有效並且存在於儲存中，您就可以導航到WebApp頁面（即使您關閉了瀏覽器）。 請記住，JWT可以生效的最長時間為24小時。

- 如果JWT仍然有效(未過期)且存在，則使用者可以使用其空格等導航到WebApp頁面，而無需重新進行身份驗證。
- 如果JWT為INVALID(EXPIRED)，使用者將被重定向到WebApp登入頁面，需要重新登入到WebApp。使用者可能還必須根據其IdP身份驗證方法重新向其IdP進行身份驗證（例如，如果IdP使用會話SSO或持續SSO）。

WebApp SSO如何支援多個域？

WebApp SSO能夠支援具有多個域的環境，甚至能夠支援那些不同域指向不同身份提供程式(IdP)的環境。 請查閱思科會議伺服器部署指南或聯絡思科TAC獲取有關使用多個域的支援。

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）。