在CMS上配置WebApp SSO并对其进行故障排除

目录

简介

本文档介绍如何对单点登录(SSO)的思科Meeting Server (CMS) Web应用实施进行配置和故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- CMS Callbridge版本3.1或更高版本
- CMS Webbridge版本3.1或更高版本
- Active Directory 服务器
- 标识提供程序(IdP)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景

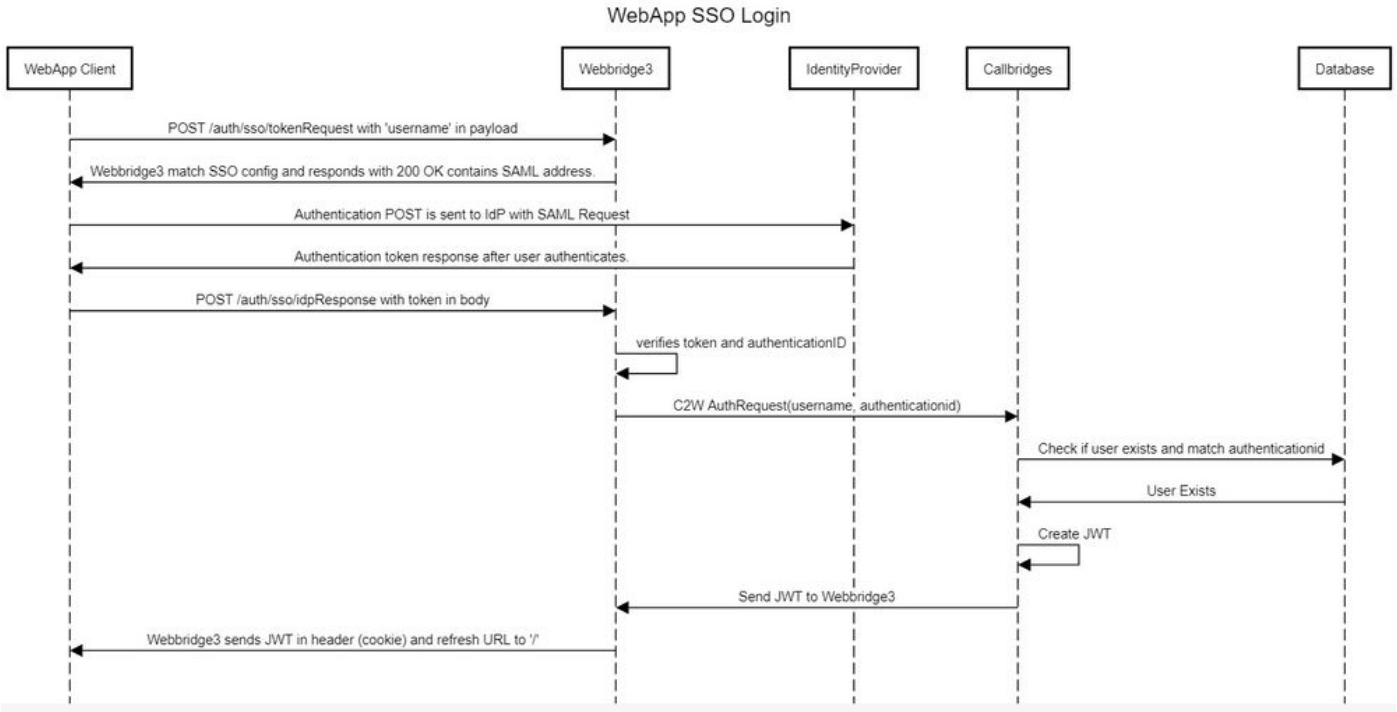
CMS 3.1及更高版本引入了用户使用SSO登录的功能，无需在用户每次登录时输入其密码，因为会与身份提供程序创建单个会话。
此功能使用安全断言标记语言(SAML) 2.0版作为SSO机制。

注意：CMS仅支持SAML 2.0中的HTTP-POST绑定，并拒绝没有HTTP-POST绑定可用的任何标识提供程序。

注意：启用SSO后，基本LDAP身份验证不再可用。

配置

网络图



ADFS安装和初始设置

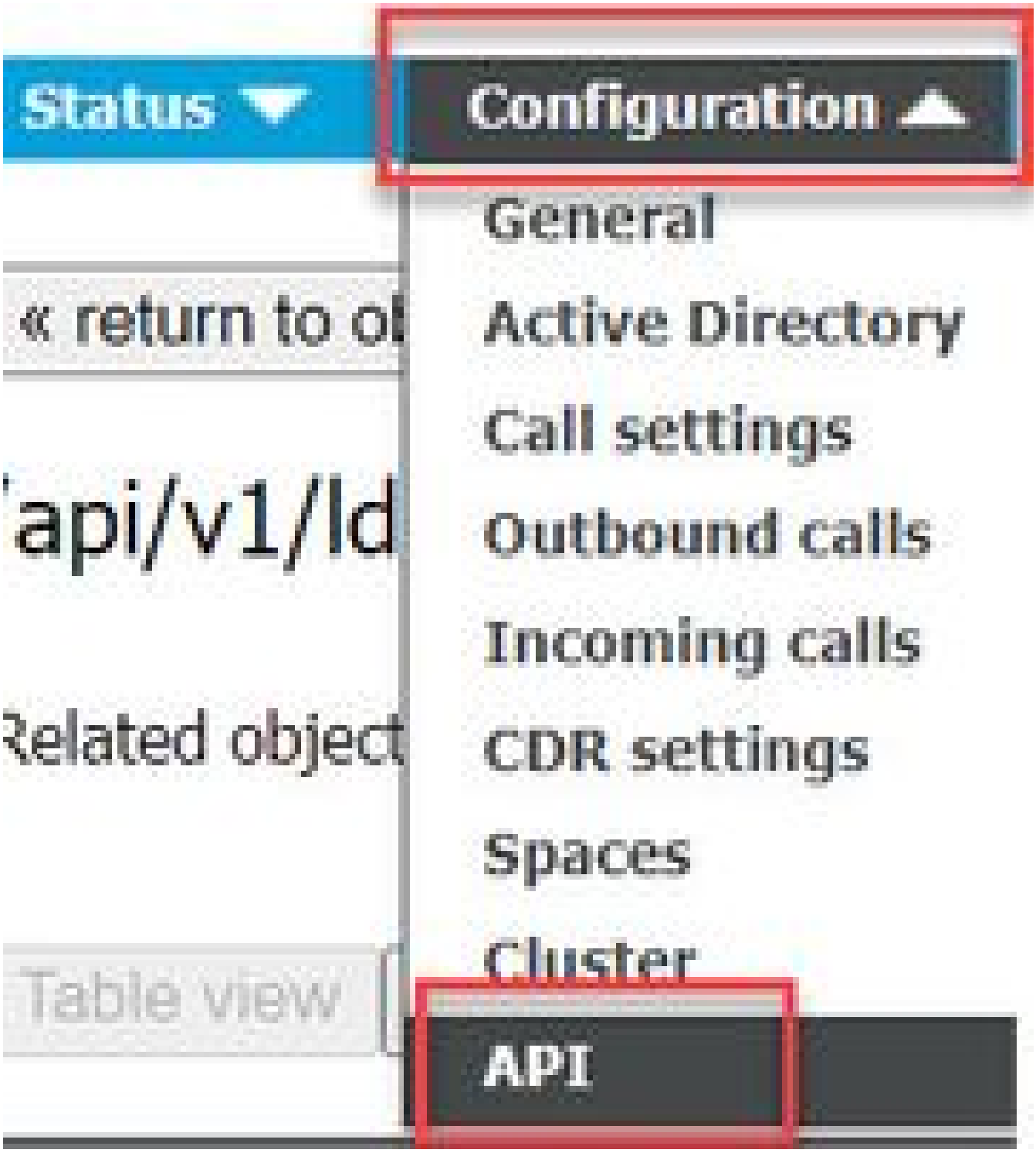
此部署方案使用Microsoft Active Directory联合身份验证服务(ADFS)作为身份提供程序(IdP)，因此，建议在此配置之前安装并运行ADFS（或目标IdP）。

将CMS用户映射到身份提供程序(IdP)

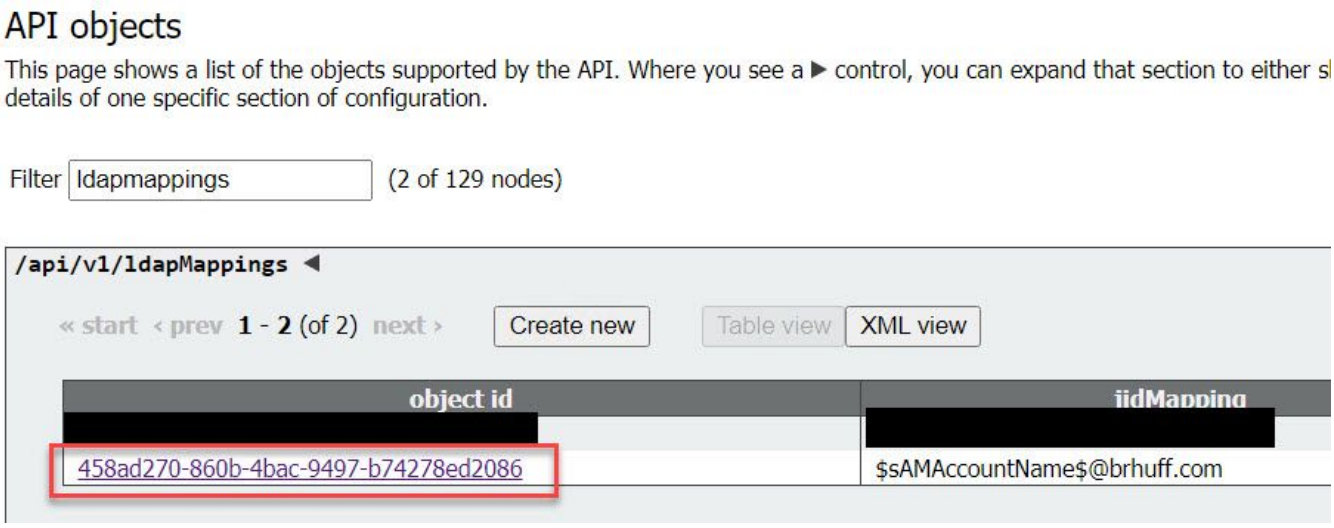
为了让用户获得有效的身份验证，必须在IdP提供的相关字段的应用编程接口(API)中映射它们。用于该操作的选项是API的ldapMapping 中的authenticationIdMapping。

1. 在CMS Web管理GUI上导航到配置> API

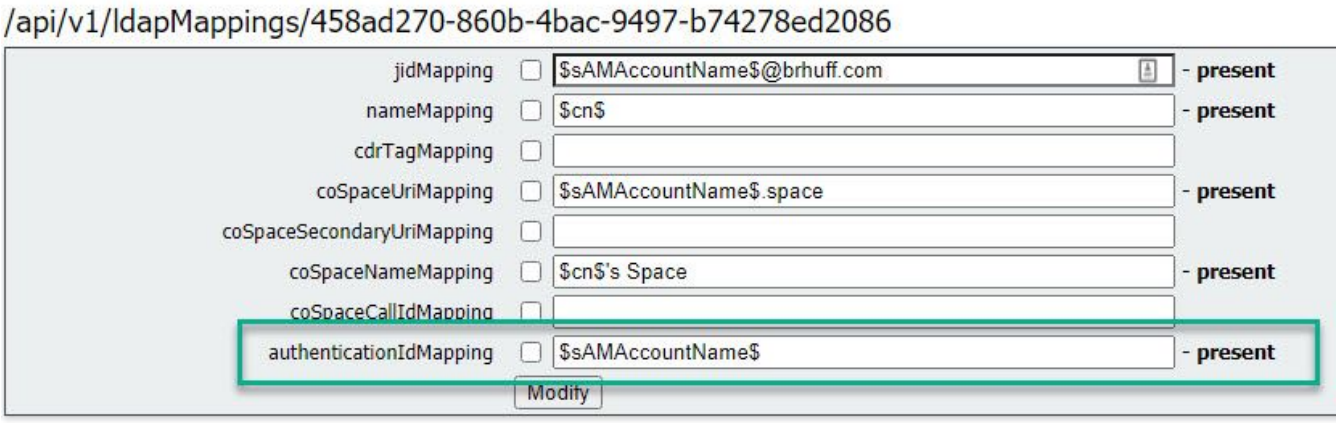
    公司



2. 在api/v1/ldapMappings/<GUID-of-Ldap-Mapping>下查找现有的（或正在创建新的）LDAP映射。



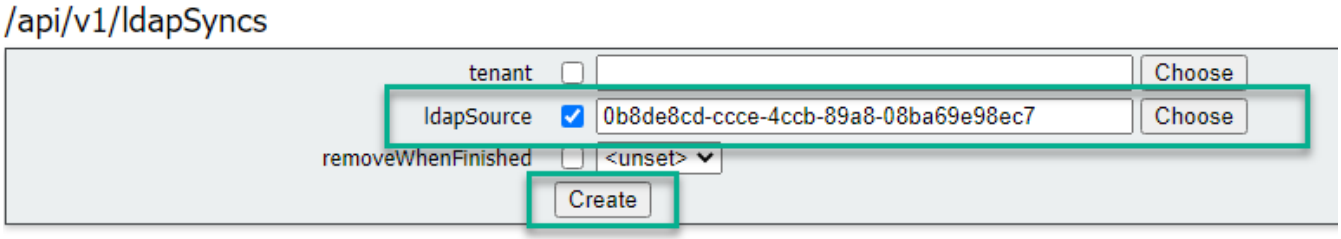
3. 在所选的ldapMapping对象中，将authenticationIdMapping更新为从IdP传递的LDAP属性。在本示例中，选项$sAMAccountNameis用作映射的LDAP属性。



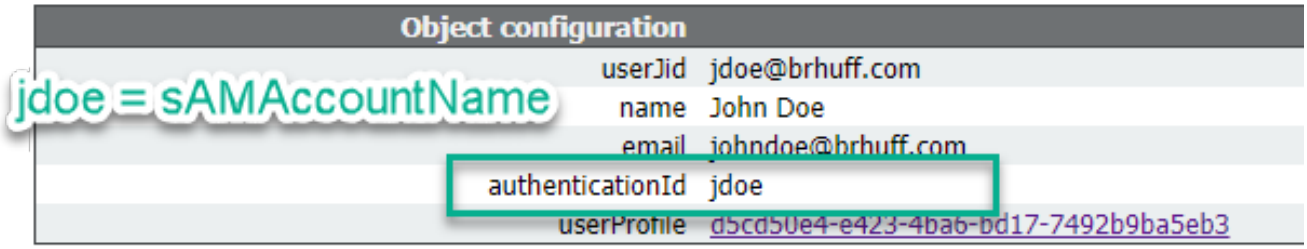
注意：callbridge/数据库使用authenticationIdMapping验证从SAMLResponse中的IdP发送的声明，并向用户提供一个JSON Web令牌(JWT)。

4. 在与最近修改的ldapMapping关联的ldapSource上执行LDAP同步：

例如:



5. 完成LDAP同步后，在CMS API中的配置> api/v1/users中进行导航，并选择已导入的用户，并验证是否已正确填充authenticationId。



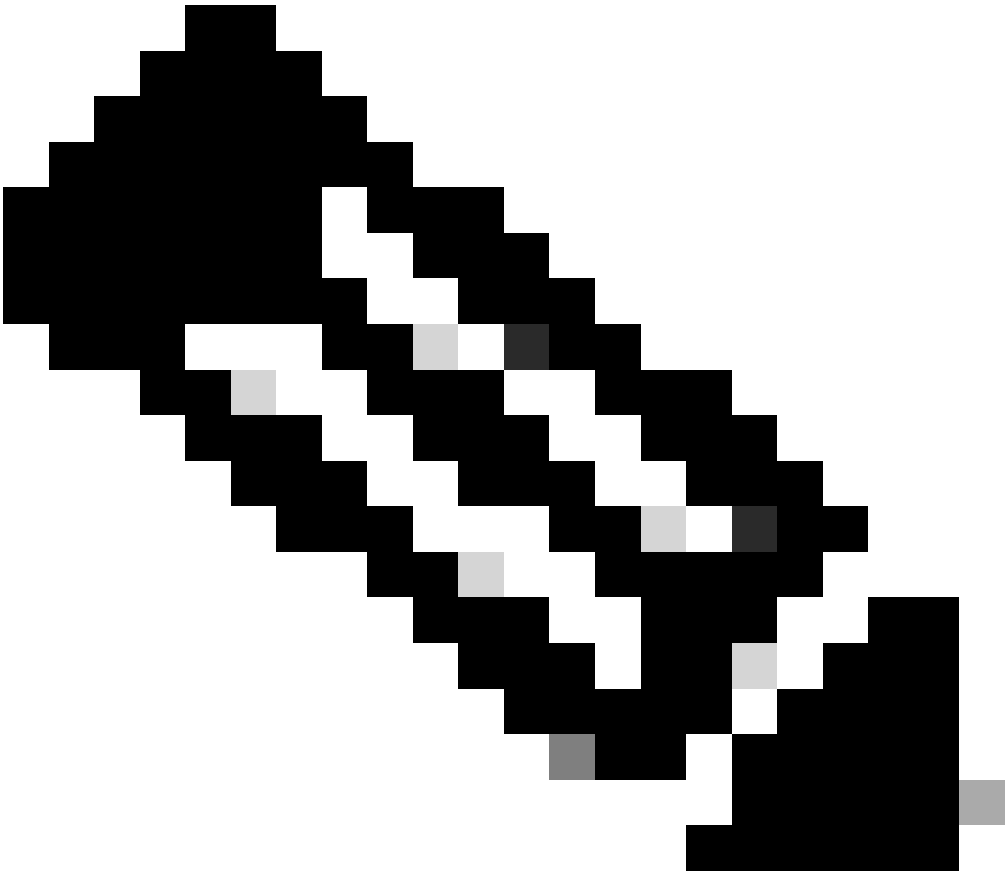
为IdP创建Webbridge元数据XML

Microsoft ADFS允许将元数据XML文件作为信赖信任方导入，以标识正在使用的服务提供程序。有几种方法可以创建元数据XML文件以实现此目的，但文件中必须存在一些属性：

具有所需值的Webbridge元数据示例：

```
<?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 -这是Webbridge3服务器地址（FQDN/主机名）用户可以通过浏览器访问的关联端口。



注意：如果存在使用单个URL的多个Webbridge，则该地址必须是负载均衡地址。

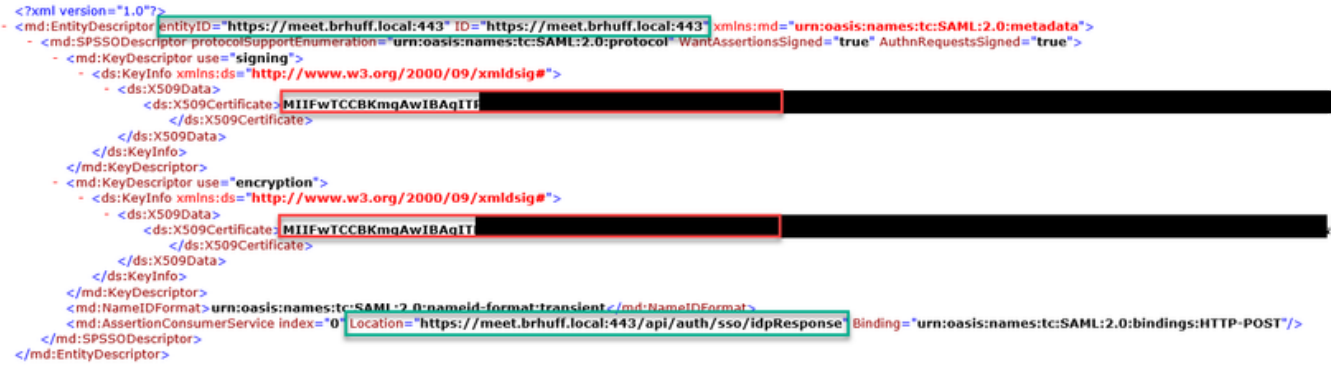
2. Location —这是Webbridge地址的HTTP-POST AssertionConsumerService的位置。这是指示IdP在登录后将经过身份验证的用户重定向到的位置。必须将此值设置为idpResponse URL：https://<WebbrdgeFQDN>：<port>/api/auth/sso/idpResponse。 例如，https://join.example.com:443/api/auth/sso/idpResponse.

3. 可选-用于签名的公钥- 这是用于签名的公钥（证书），IdP使用它来验证来自Webbridge的AuthRequest。此ID必须与上载到Webbridge上的SSO捆绑包中的私钥“sso_sign.key”匹配，以便IdP可以使用公钥（证书）验证签名。您可以使用部署中的现有证书。 在文本文件中打开证书并将内容复制到Webbridge元数据文件中。 将您的sso_xxxx.zip文件中使用的证书的匹配密钥用作sso_sign.key文件。

4. 可选-用于加密的公钥- 这是IdP用于加密发回Webbridge的SAML信息的公钥（证书）。这必须与上传到Webbridge上的SSO捆绑包中的私钥“sso_encrypt.key”匹配，以便Webbridge可以解密IdP发回的内容。 您可以使用部署中的现有证书。 在文本文件中打开证书并将内容复制到Webbridge元数据文件中。 将您的sso_xxxx.zip文件中使用的证书的匹配密钥用作

sso_encrypt.key文件。

使用可选公钥（证书）数据导入IdP的Webbridge元数据示例：

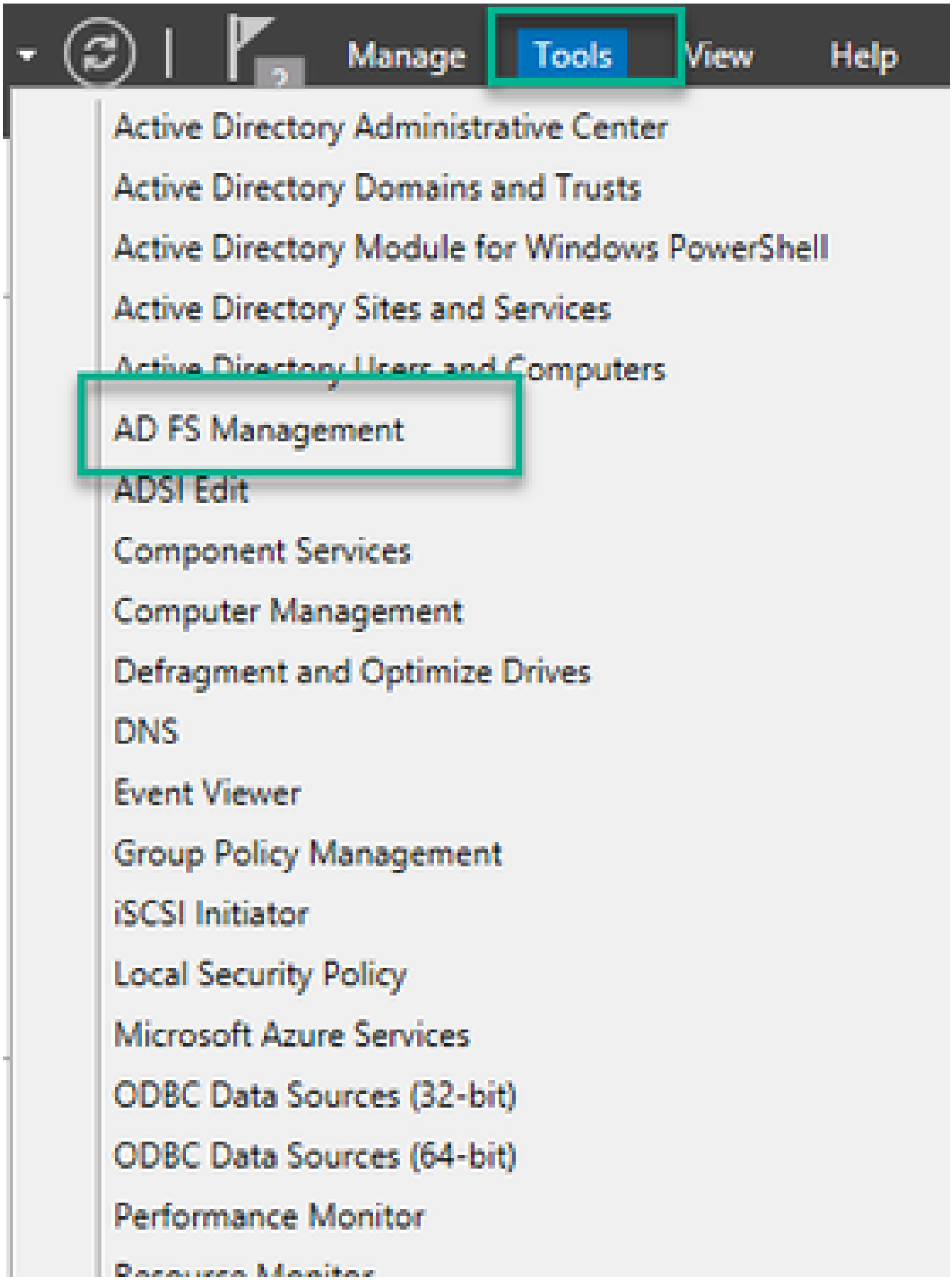


将Webbridge的元数据导入身份提供程序(IdP)

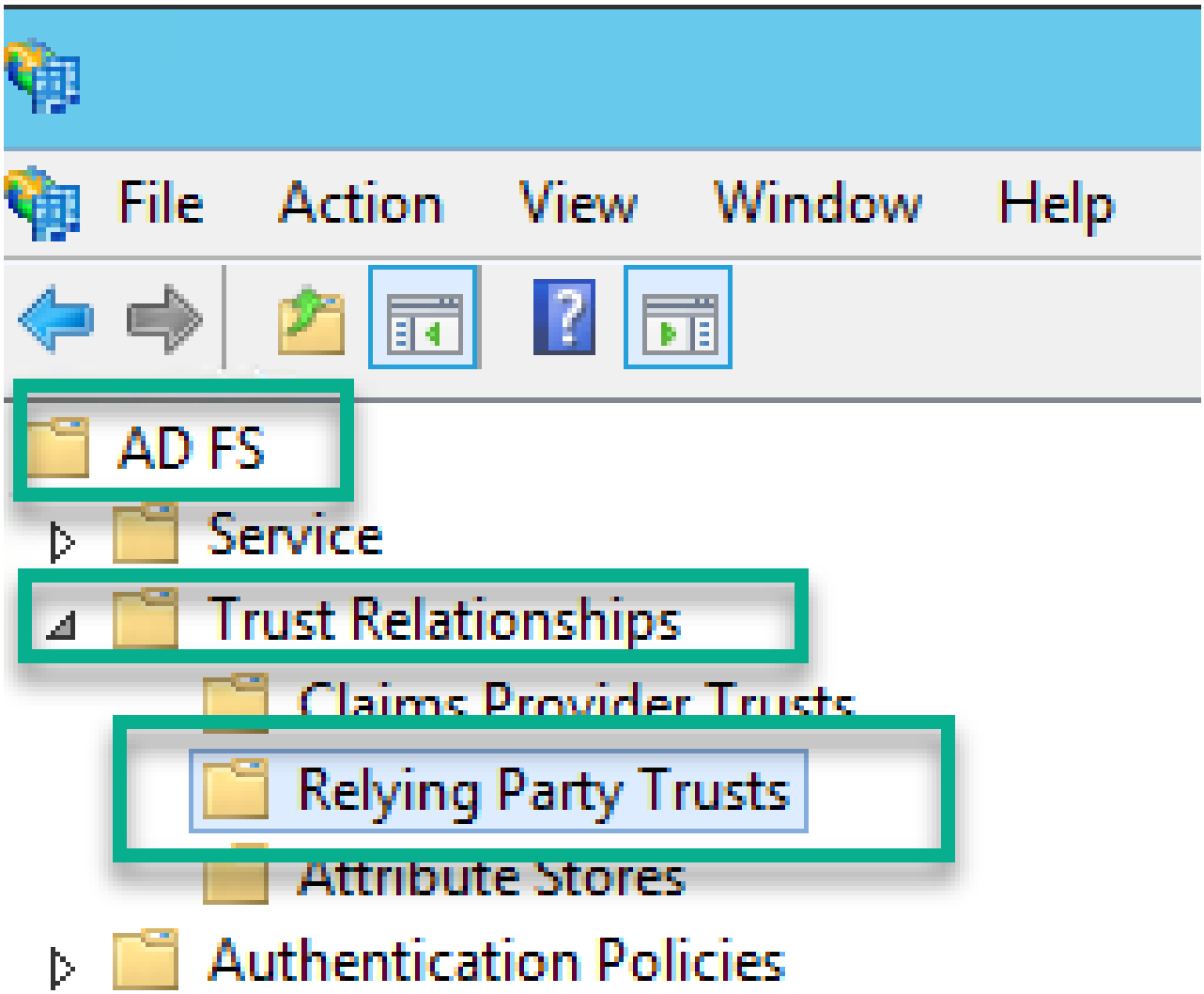
使用正确的属性创建元数据XML后，即可将文件导入Microsoft ADFS服务器以创建信赖信任方。

1. 将远程桌面连接到托管ADFS服务的Windows服务器

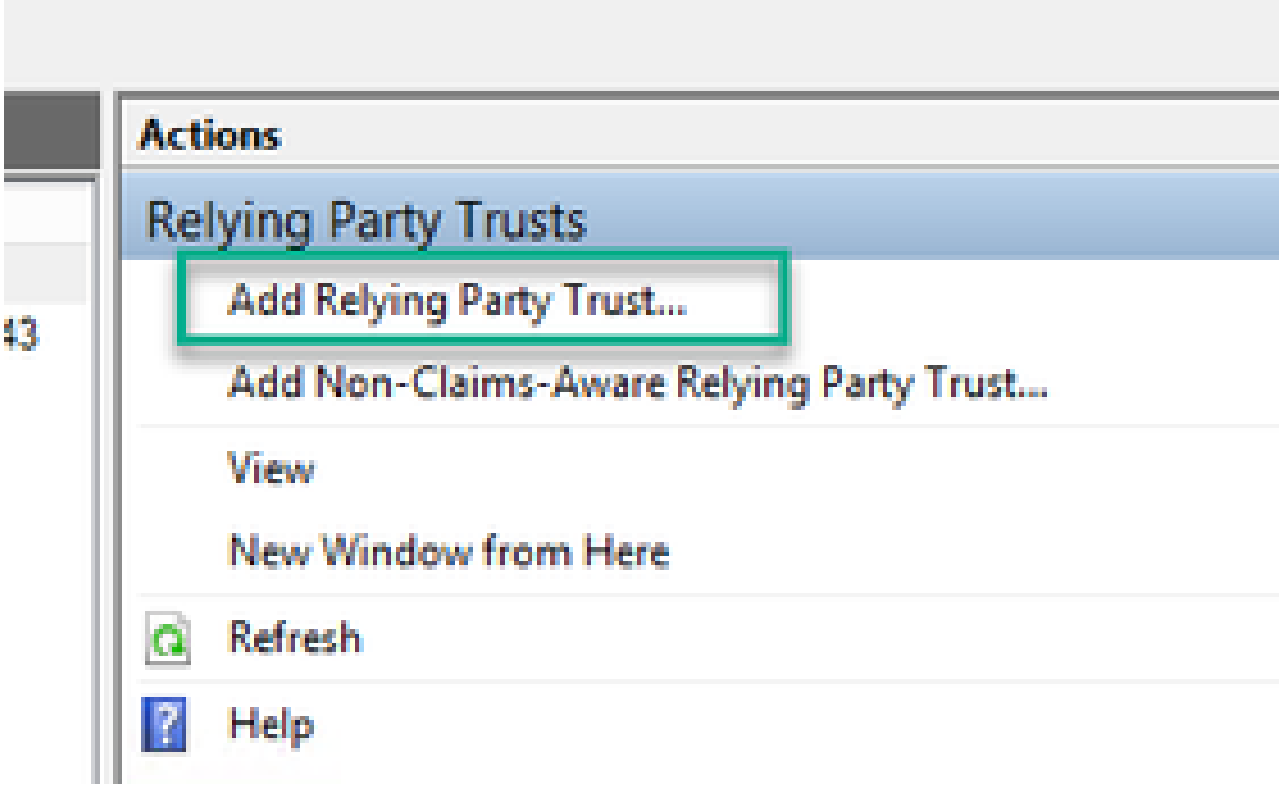
2. 打开AD FS管理控制台，通常可以通过服务器管理器访问。



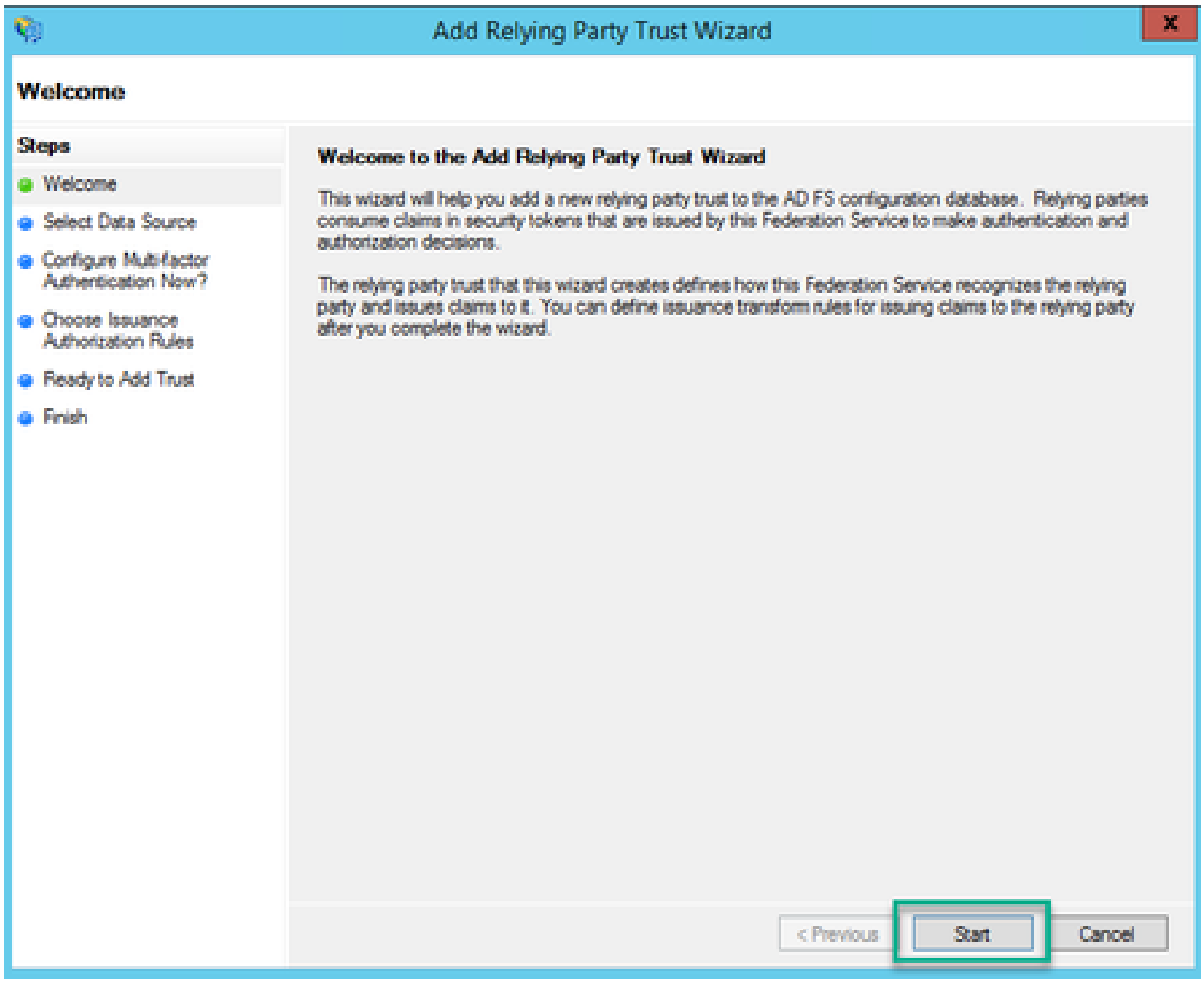
3. 进入ADFS管理控制台后，在左侧窗格中导航到ADFS >信任关系>信赖方信任。



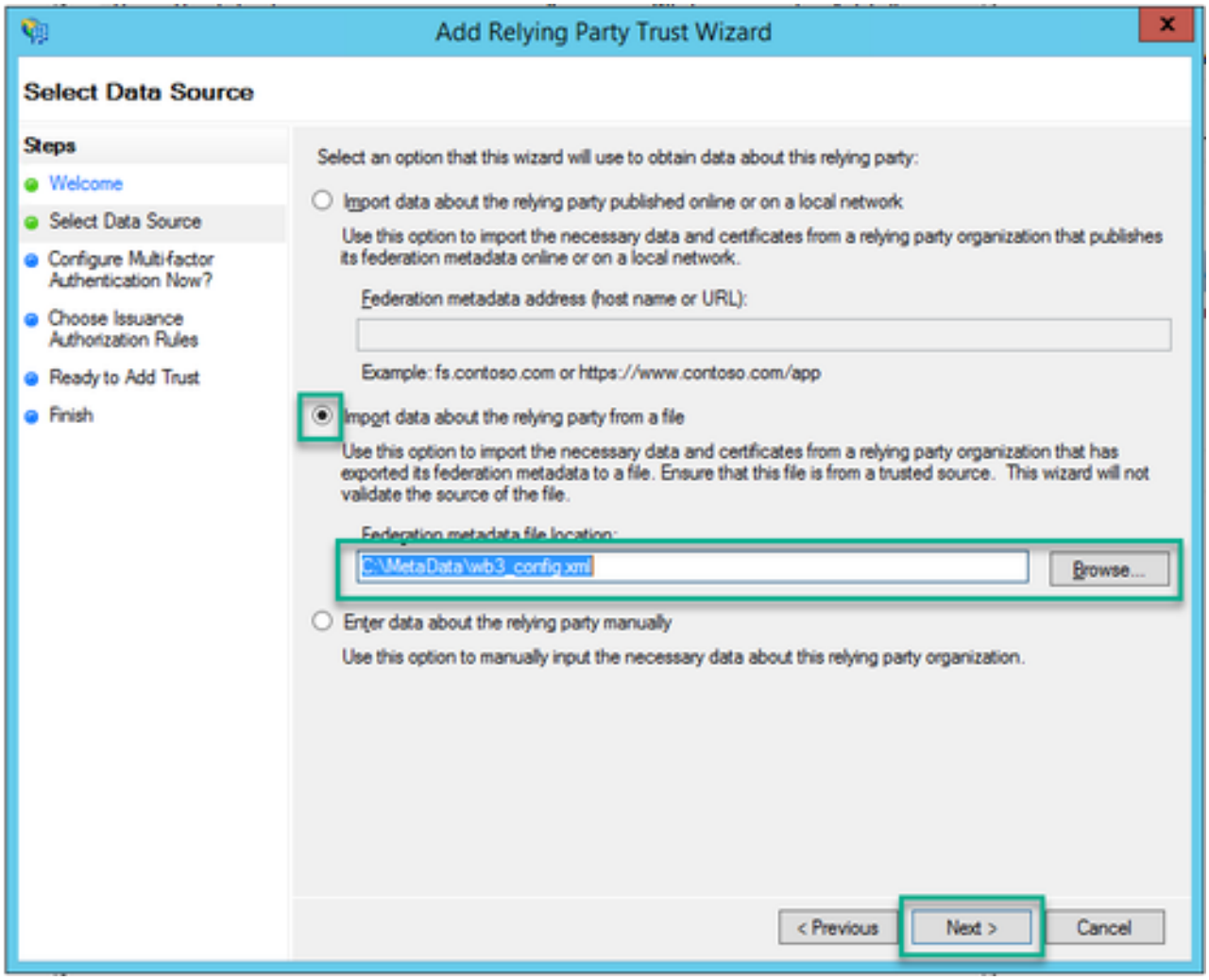
4. 在ADFS管理控制台的右窗格中选择添加信赖方信任。. 选项。



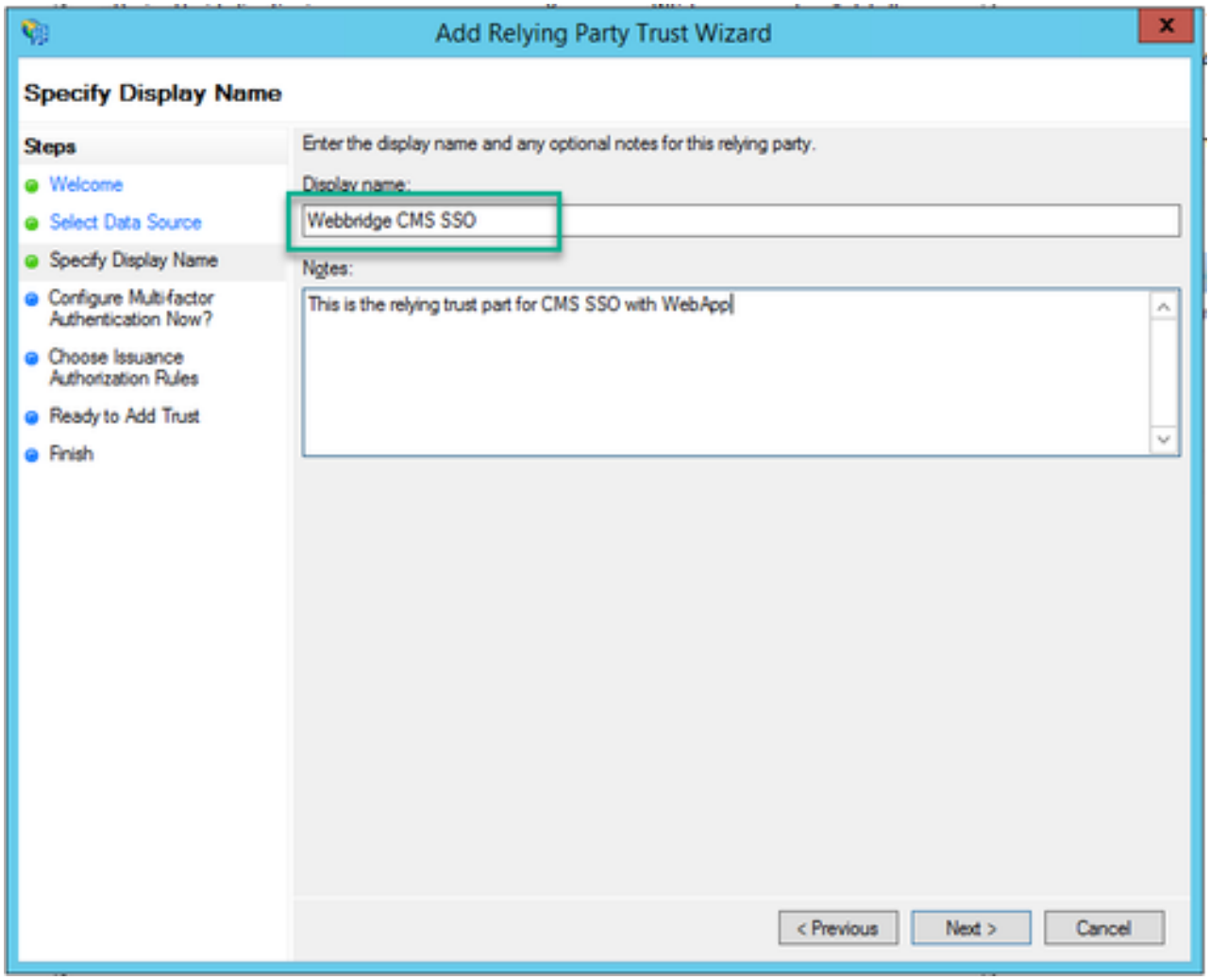
5. 进行此选择后，将打开添加信赖方信任向导。选择Start选项。



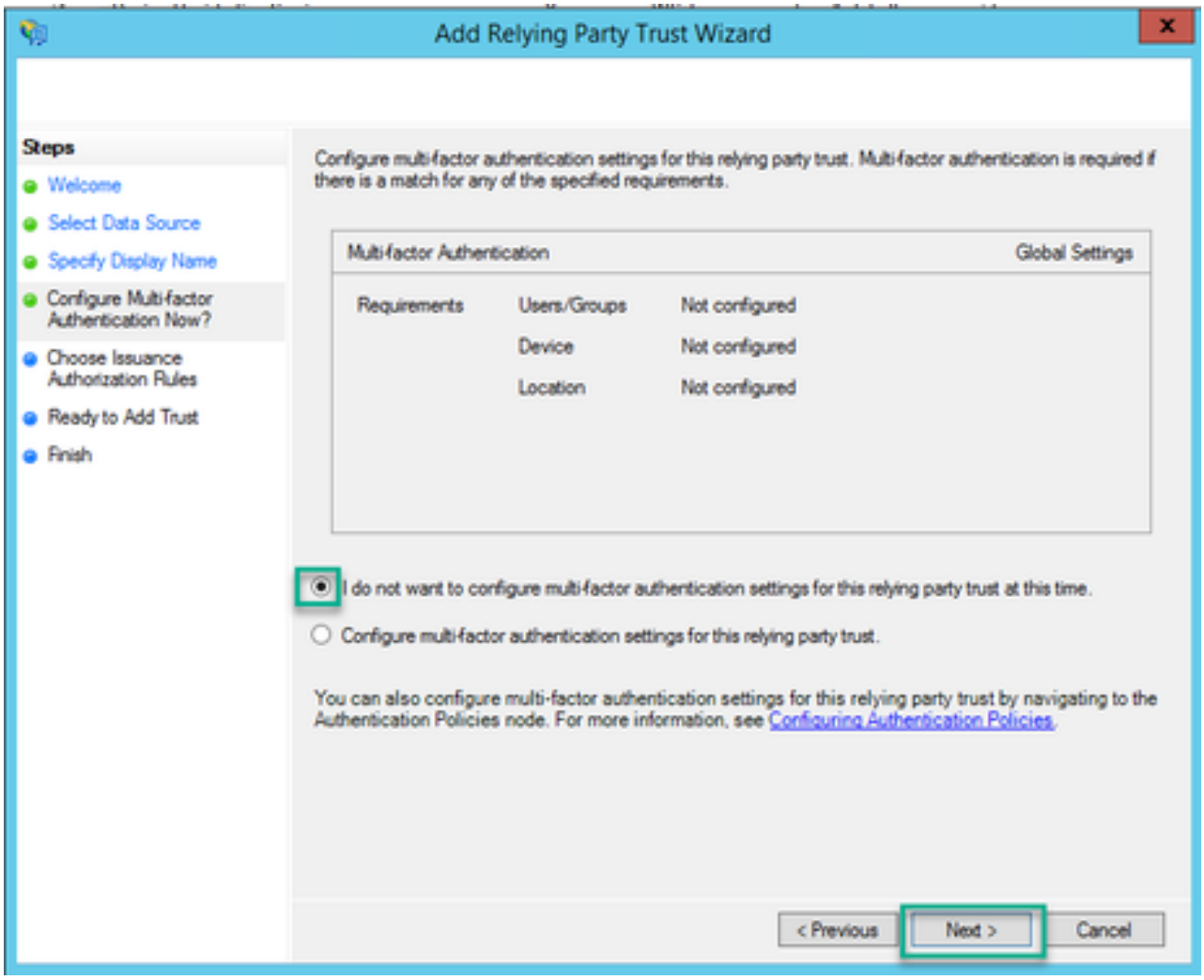
6. 在选择数据源页上，选择从文件导入有关信赖方的数据的单选按钮，然后选择浏览并导航到Webbridge元数据文件的位置。



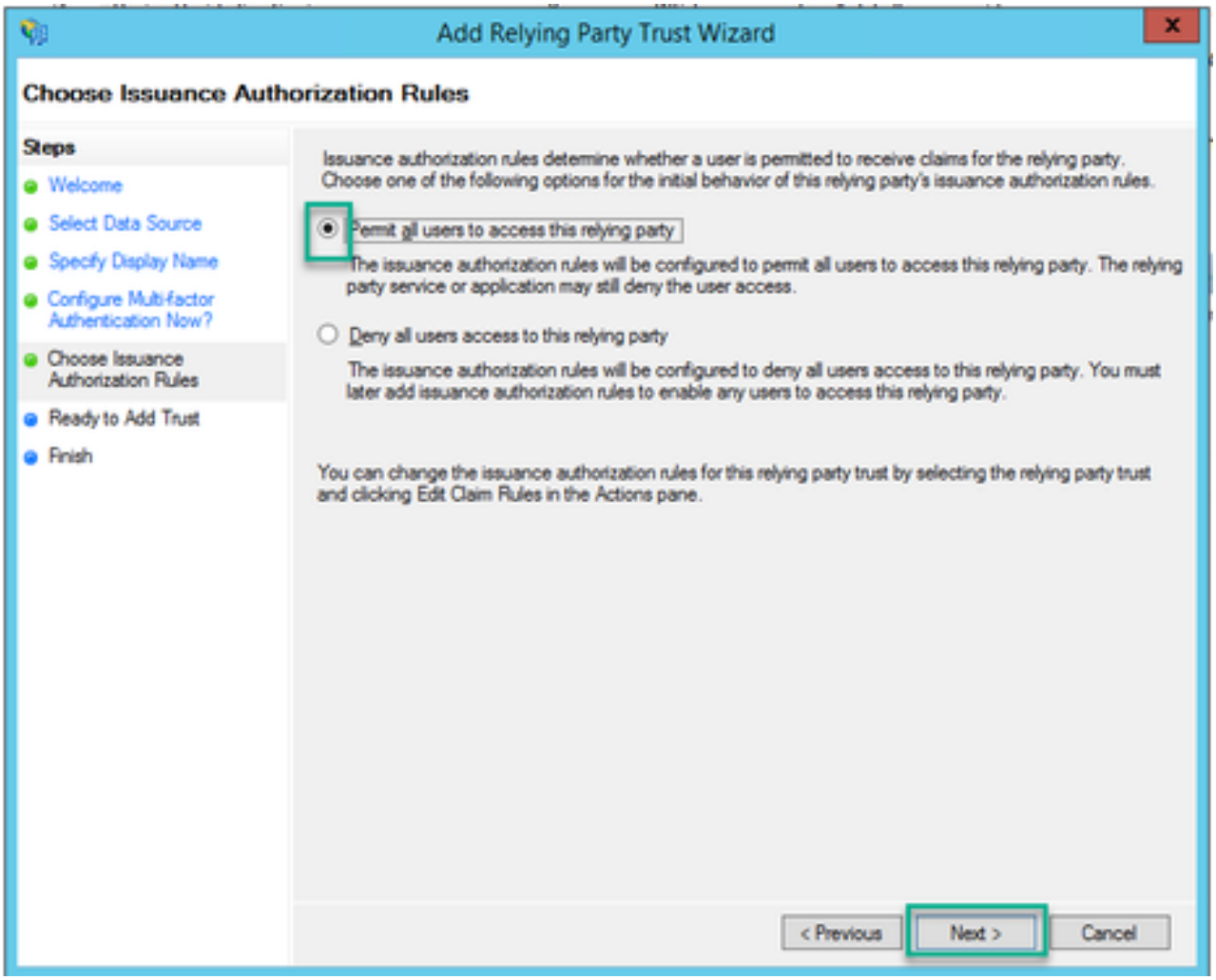
7. 在指定显示名称页上，为ADFS中的实体输入一个要显示的名称（显示名称不是用于ADFS通信的服务器名称，只是提供信息）。



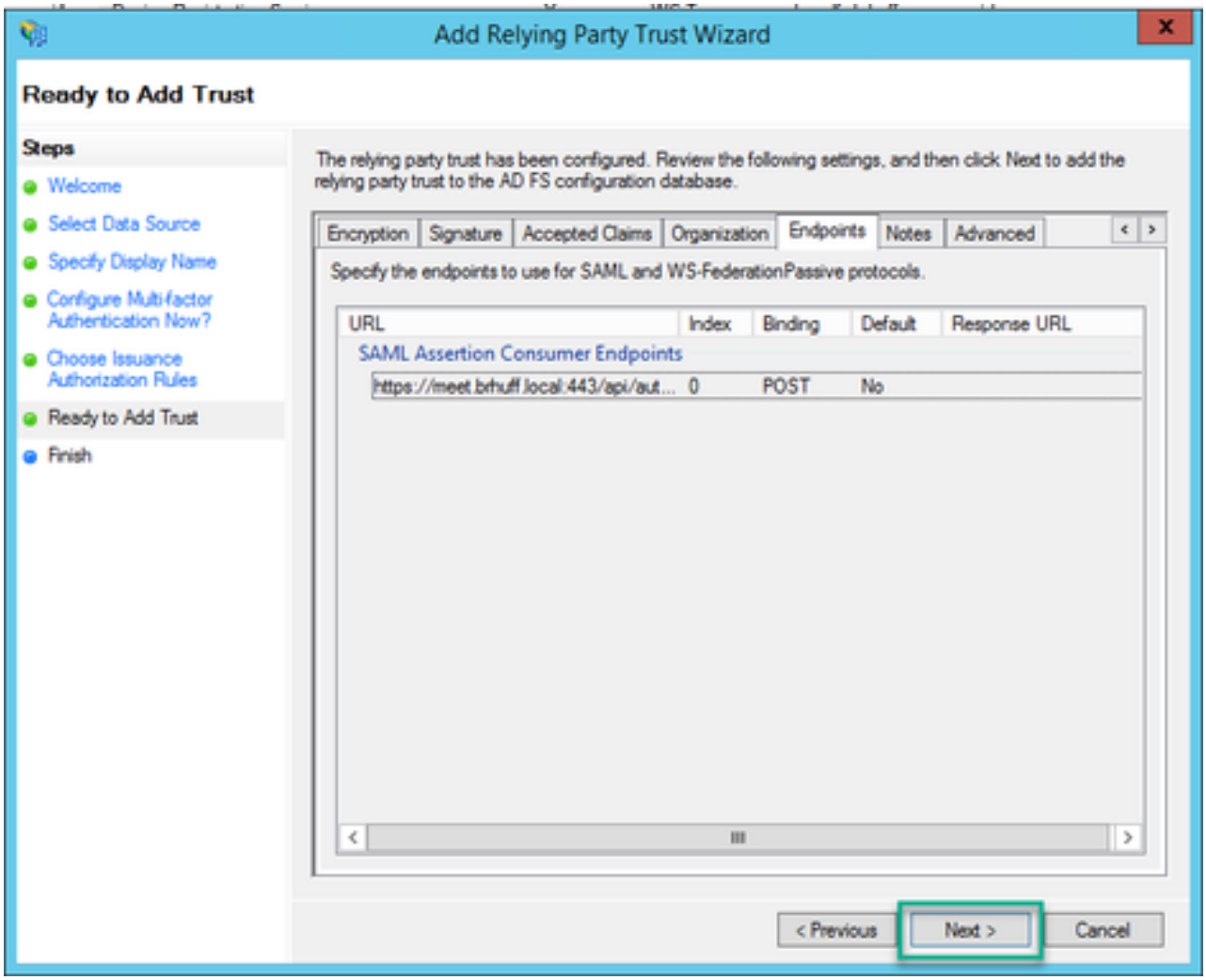
8. 在立即配置多重身份验证？页上，保留默认值并选择下一步。



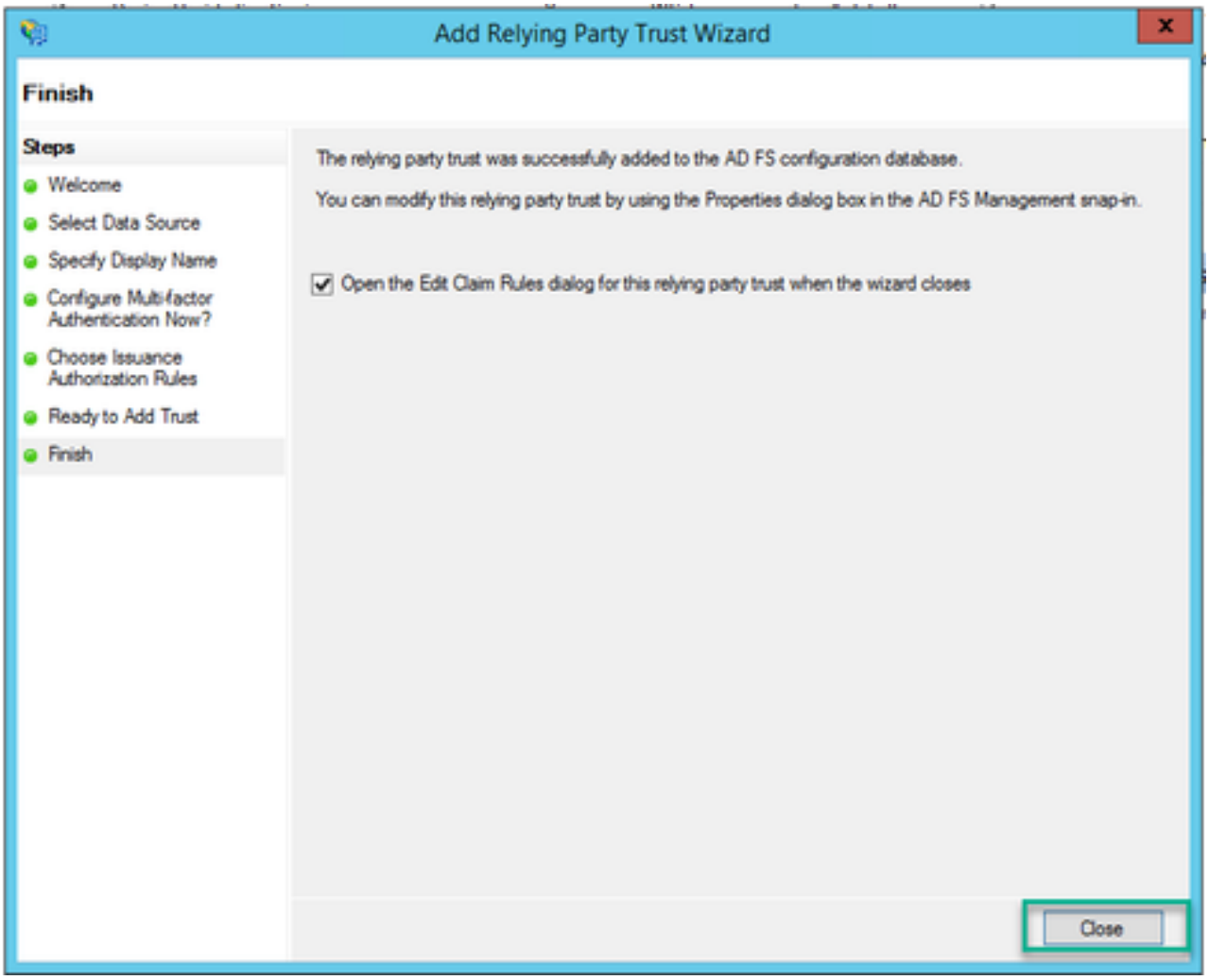
9. 在选择颁发授权规则页上，为允许所有用户访问此信赖方保留为选中状态。



10. 在准备添加信任页上，可以通过选项卡查看导入的Webbridge信赖信任方的详细信息。有关Webbridge服务提供商的URL详细信息，请检查标识符和终端。



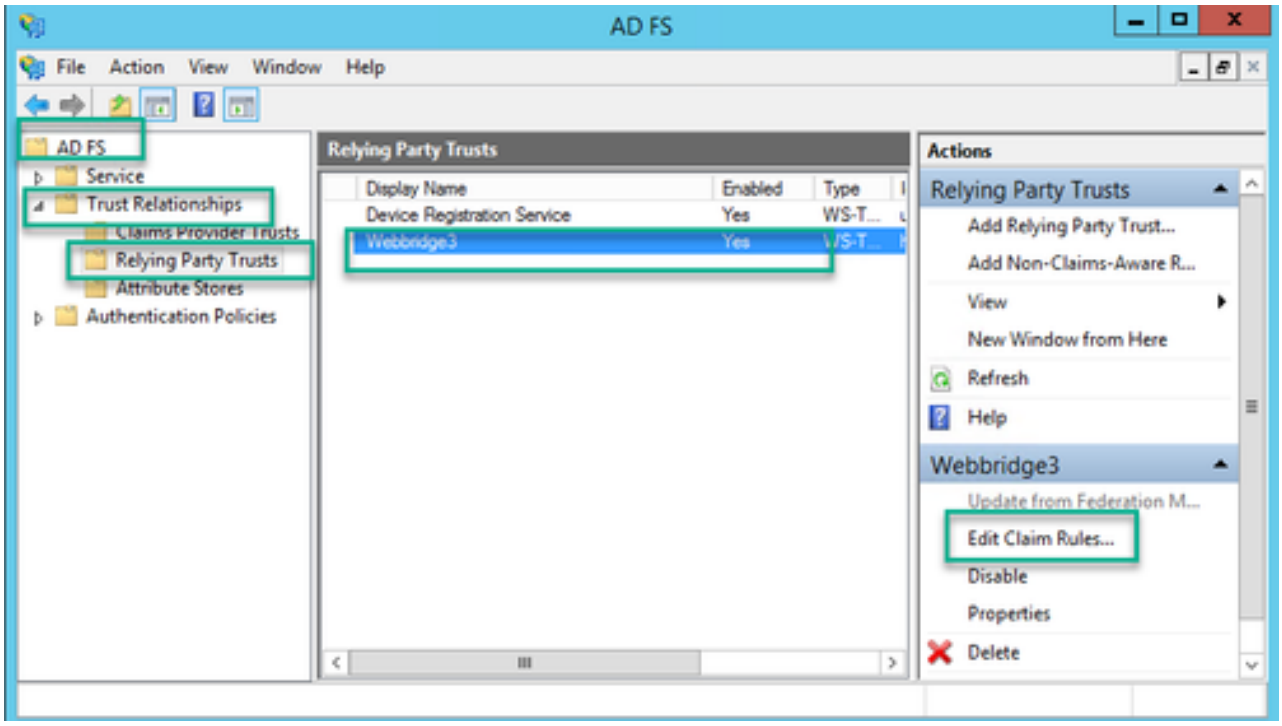
11. 在完成页上，选择关闭选项以关闭向导并继续编辑声明规则。



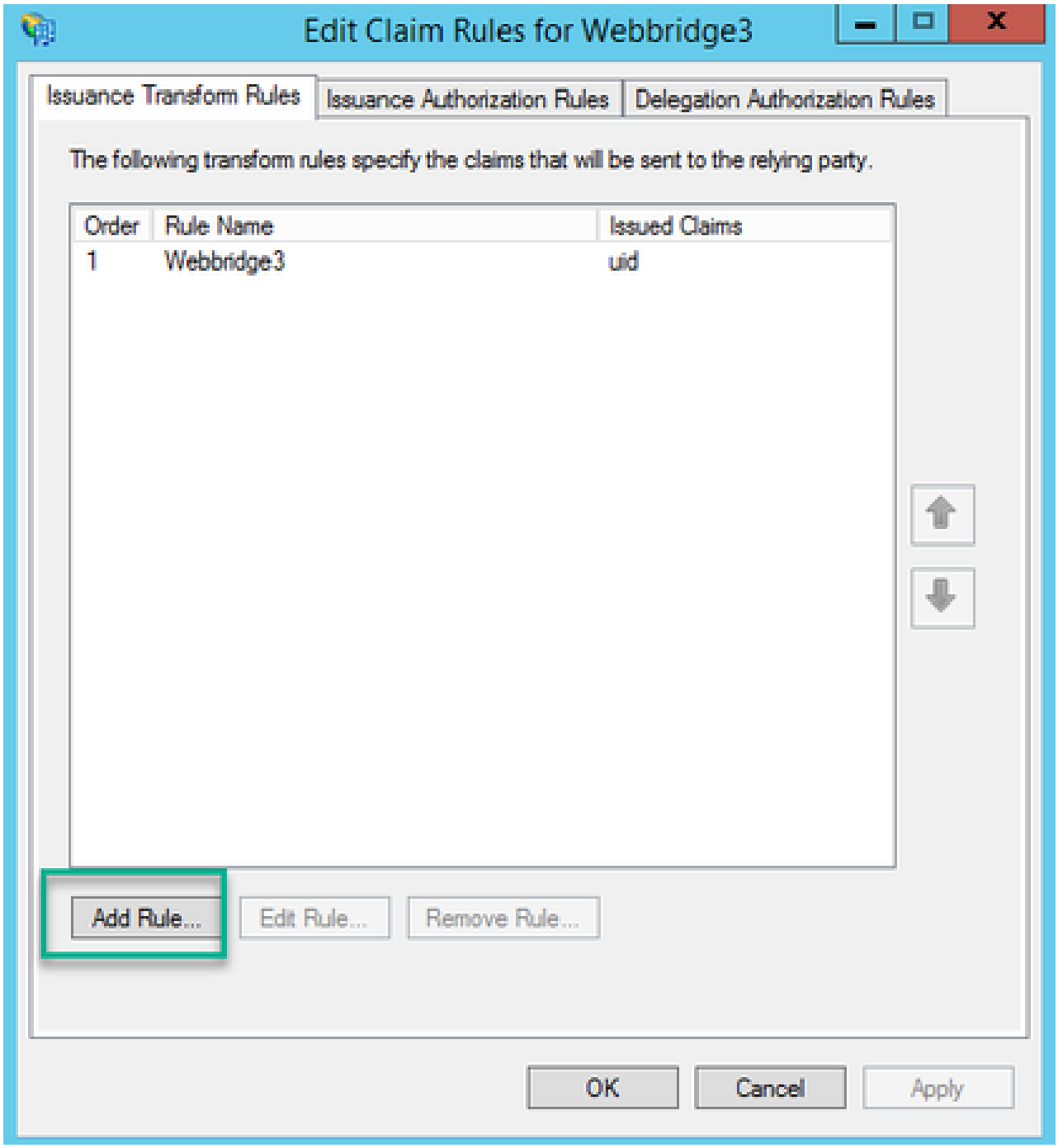
在IdP上为Webbridge服务创建声明规则

现在已经为Webbridge创建了信赖方信任，可以创建声明规则以将特定LDAP属性与要在SAML响应中向Webbridge提供的传出声明类型相匹配。

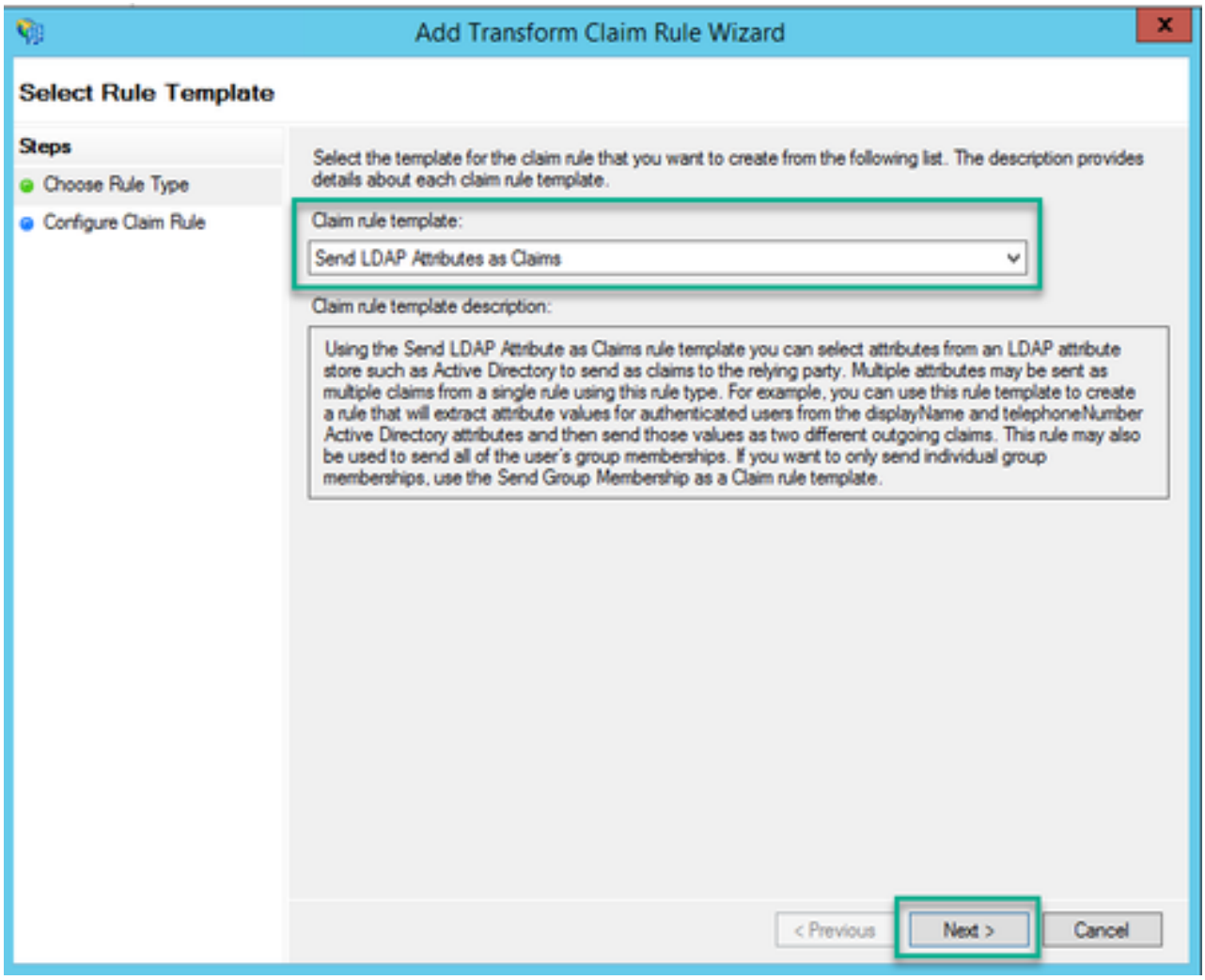
1. 在ADFS管理控制台中，突出显示Webbridge的信赖方信任，然后在右窗格中选择编辑声明规则。



2. 在“编辑<DisplayName>的申请规则”页上，选择“添加规则……”。

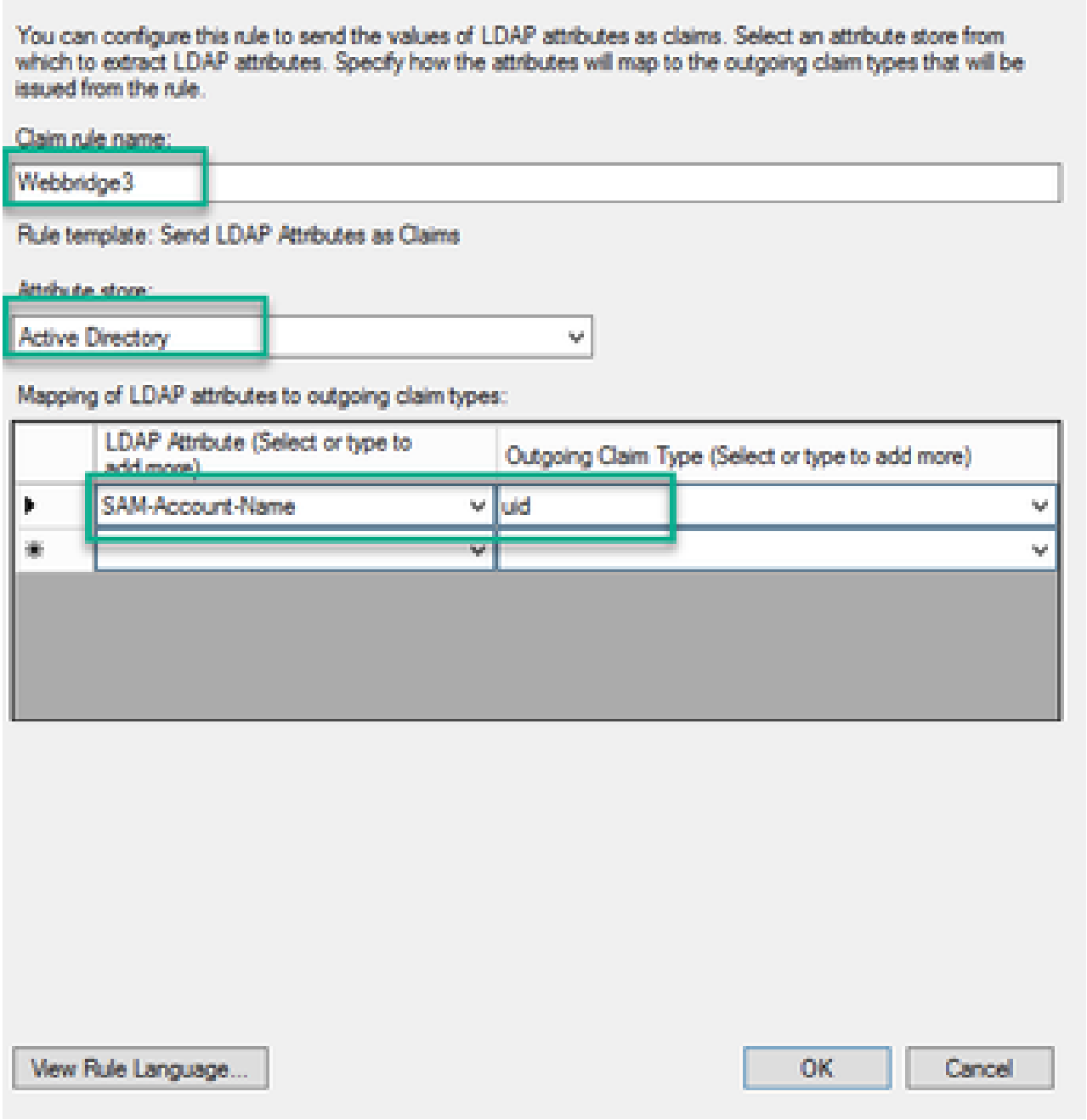


3. 在“添加转换声明规则向导”页上，为“声明规则模板”选项选择将LDAP属性作为声明发送，然后选择下一步。



4. 在配置申请规则页上，使用以下值配置信赖方信任的申请规则：

1. 声明规则名称=这必须是ADFS中为该规则指定的名称（仅用于规则参考）
2. 属性存储= Active Directory
3. LDAP属性=必须与Callbridge API中的authenticationIdMapping匹配。（例如，$sAMAccountName$。）
4. 传出声明类型 =必须与Webbridge SSO config.json中的authenticationIdMapping匹配。（例如，uid。）



为Webbridge创建SSO存档ZIP文件：

此配置是Webbridge为验证支持域、身份验证映射等的SSO配置而引用的配置。对于此部分的配置，必须考虑以下规则：

- ZIP文件必须以文件名前缀sso_开头(例如，sso_cmstest.zip)。
- 上传此文件后，Webbridge将禁用基本身份验证，并且只能将SSO用于已上传到的Webbridge。
- 如果使用了多个身份提供程序，则必须使用不同的命名架构上载单独的ZIP文件(仍然以sso_作为前缀)。

- 创建zip文件时，请确保突出显示并压缩文件内容，不要将所需文件放入文件夹并压缩该文件夹。

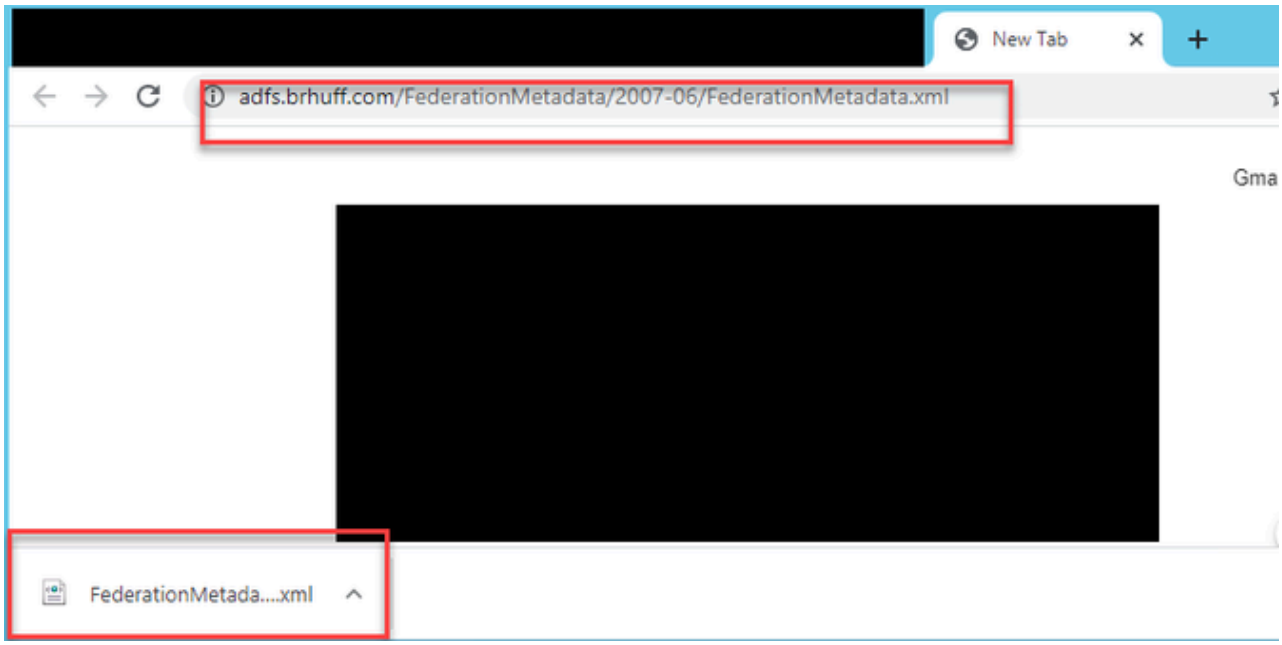
zip文件的内容由2至4个文件组成，具体取决于是否使用加密。

文件名	描述	是否必需？
idp_config.xml	这是可以由idP收集的元数据文件。在ADFS中，可通过转至 https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml找到该位置。	是
config.json	这是JSON文件，Webbridge使用该文件验证支持的域、SSO的身份验证映射。	是
sso_sign.key	这是用于在标识提供程序上配置的公共签名密钥的私钥。仅保护已签名的数据时需要	否
sso_encrypt.key	这是在身份提供程序上配置的用于公共加密密钥的私钥。仅用于保护加密数据	否

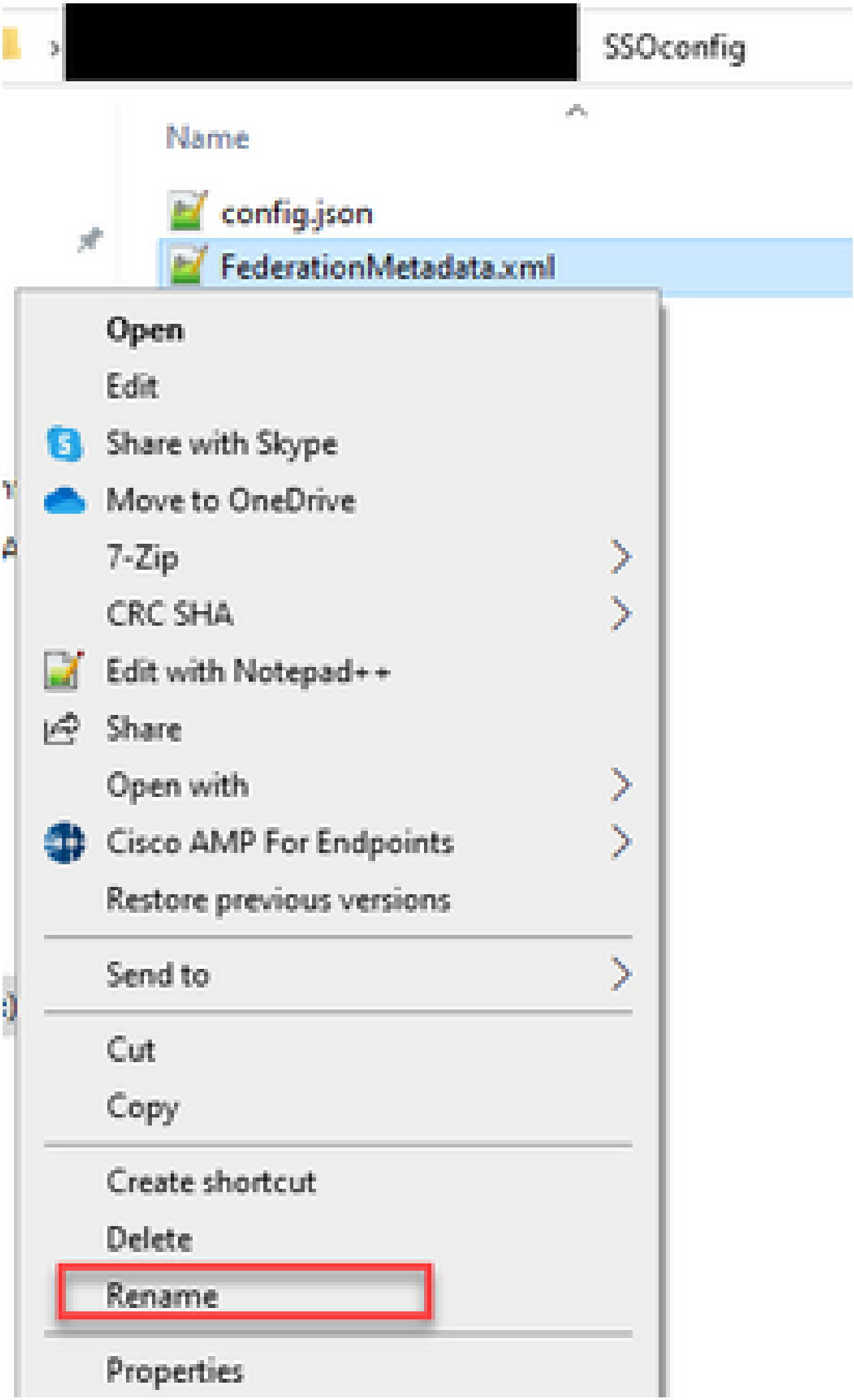
获取并配置idp_config.xml

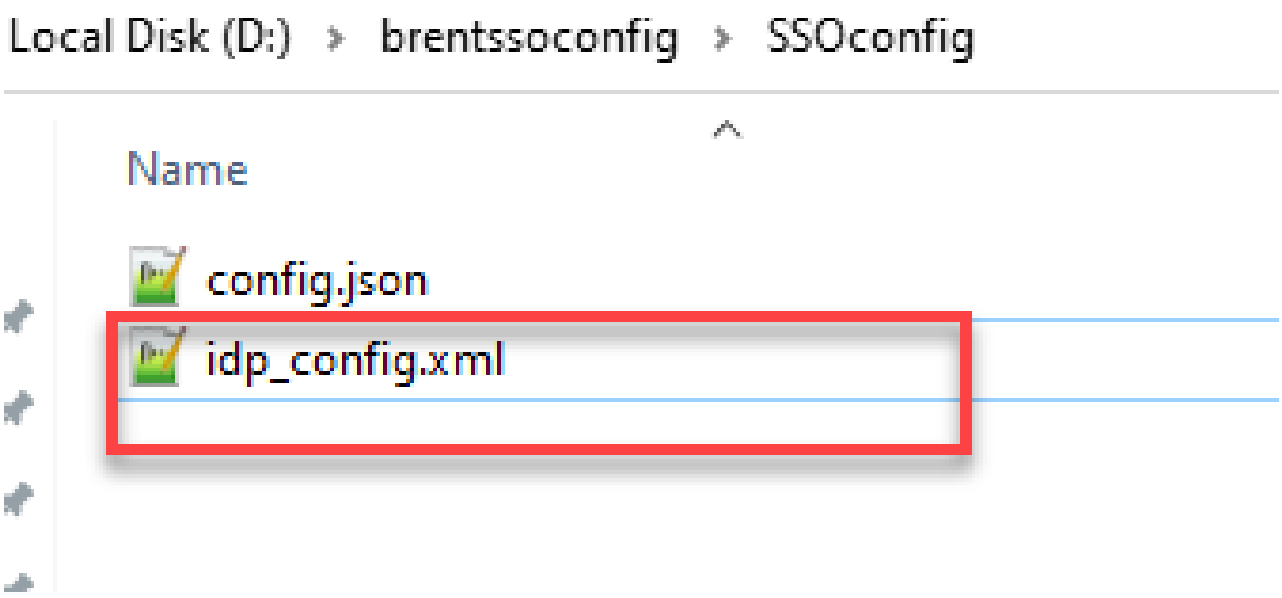
1. 在ADFS服务器（或有权访问ADFS的位置）上，打开Web浏览器。

2. 在Web浏览器中，输入URL：https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml（如果您在ADFS服务器本地，也可以使用localhost代替FQDN）。 这会下载文件FederationMetadata.xml。



3. 将下载的文件复制到正在创建zip文件的位置，然后重命名为idp_config.xml。

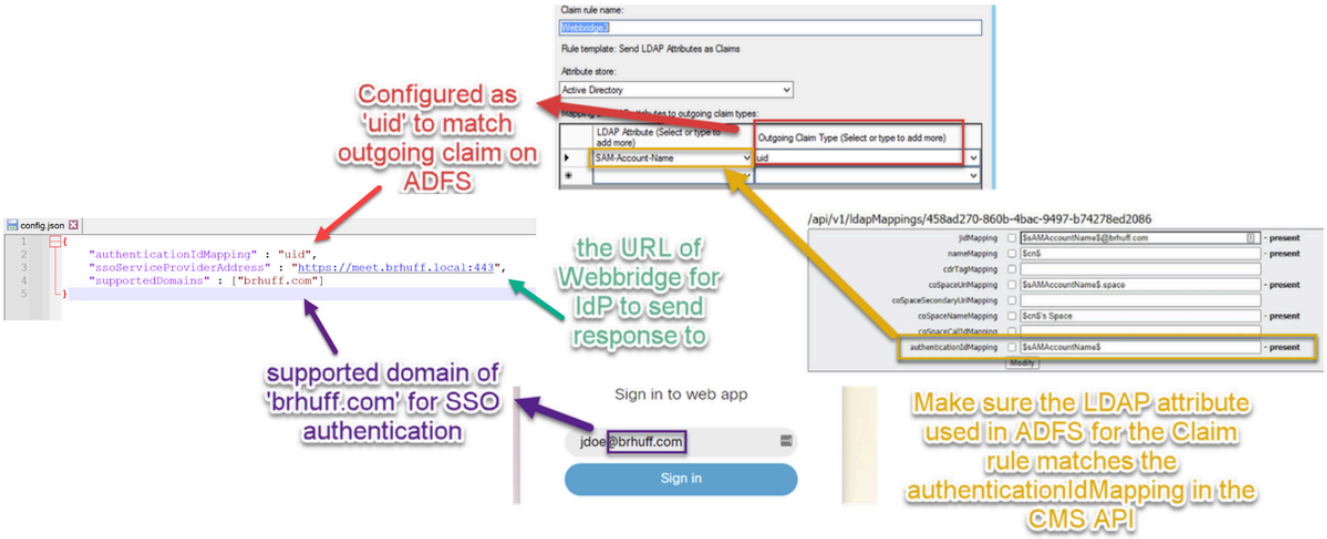

[redacted]
SSOconfig
Name
config.json
FederationMetadata.xml
Open
Edit
Share with Skype
Move to OneDrive
7-Zip
CRC SHA
Edit with Notepad++
Share
Open with
Cisco AMP For Endpoints
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties



创建包含内容的config.json文件

config.json包含以下3个属性，它们必须包含在方括号内，{ } :

1. supportedDomains -这是根据IdP进行SSO身份验证检查的域列表。多个域之间可以用逗号分隔。
2. authenticationIdMapping -这是作为传出ADFS/IdP声明规则的一部分传回的参数。此值必须与IdP上的传出声明类型的名称值匹配。声明规则。
3. ssoServiceProviderAddress -这是标识提供程序向其发送SAML响应的FQDN URL。必须是Webbridge FQDN。

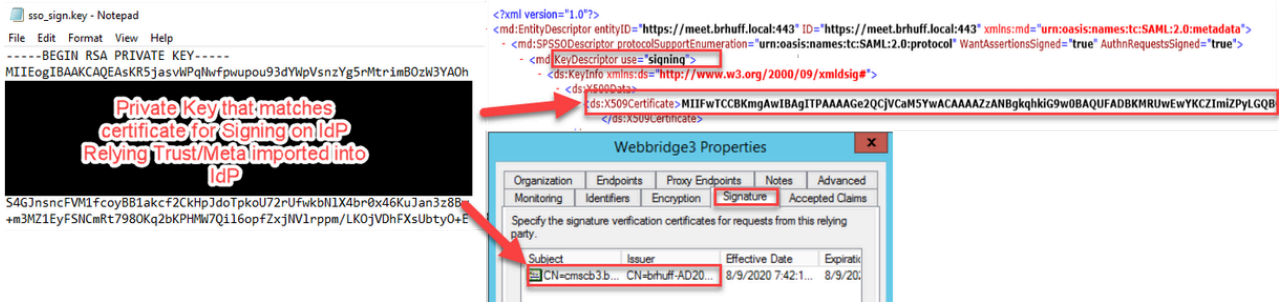


设置sso_sign.key（可选）

此文件必须包含用于登录Webbridge元数据（已导入到IdP）的证书的私钥。用于签名的证书可在ADFS中Webbridge元数据的导入期间进行设置，方法是使用<KeyDescriptor use=signing>部分下的证书信息填充X509Certificate。还可以在Webbridge信赖信任方的ADFS上的属性>签名下查看（和导入）。

在下一个示例中，您可以看到Callbridge证书(CN=cmscb3.brhuff.local)，该证书在导入到ADFS之前已添加到Webbridge元数据中。插入到sso_sign.key中的私钥是与cmscb3.brhuff.local证书的私钥。

这是可选配置，仅在要加密SAML响应时才需要。

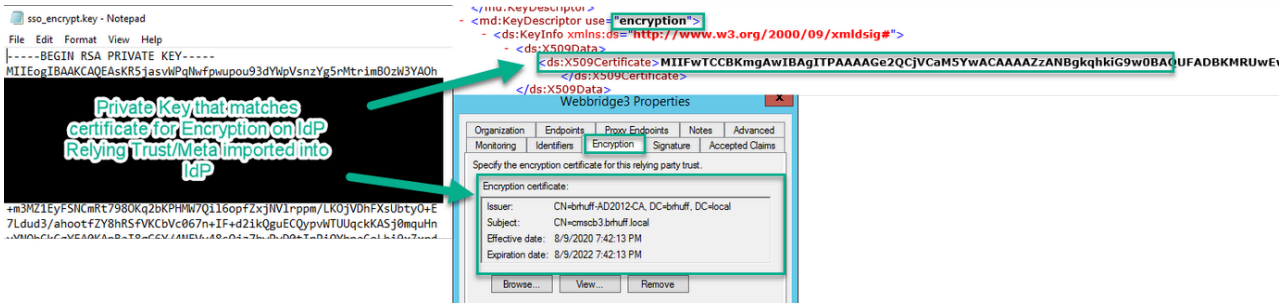


设置sso_encrypt.key（可选）

此文件必须包含用于在Webbridge元数据中加密的证书的私钥，Webbridge元数据已导入到IdP。在ADFS中导入Webbridge元数据期间，通过在<KeyDescriptor use=encryption>部分下的证书信息填充X509Certificate来设置用于加密的证书。还可以在Webbridge信赖信任方的ADFS上的属性>加密下查看（和导入）。

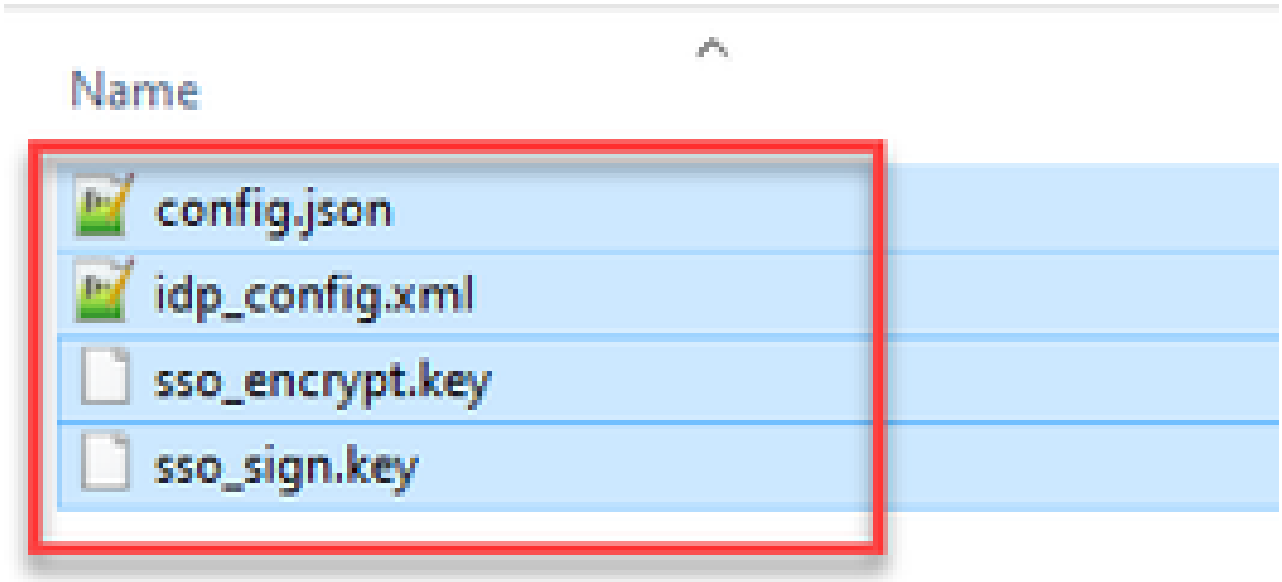
在下一个示例中，您可以看到Callbridge证书(CN=cmscb3.brhuff.local)，该证书在导入到ADFS之前已添加到Webbridge元数据中。插入“sso_encrypt.key”的私钥与cmscb3.brhuff.local证书匹配。

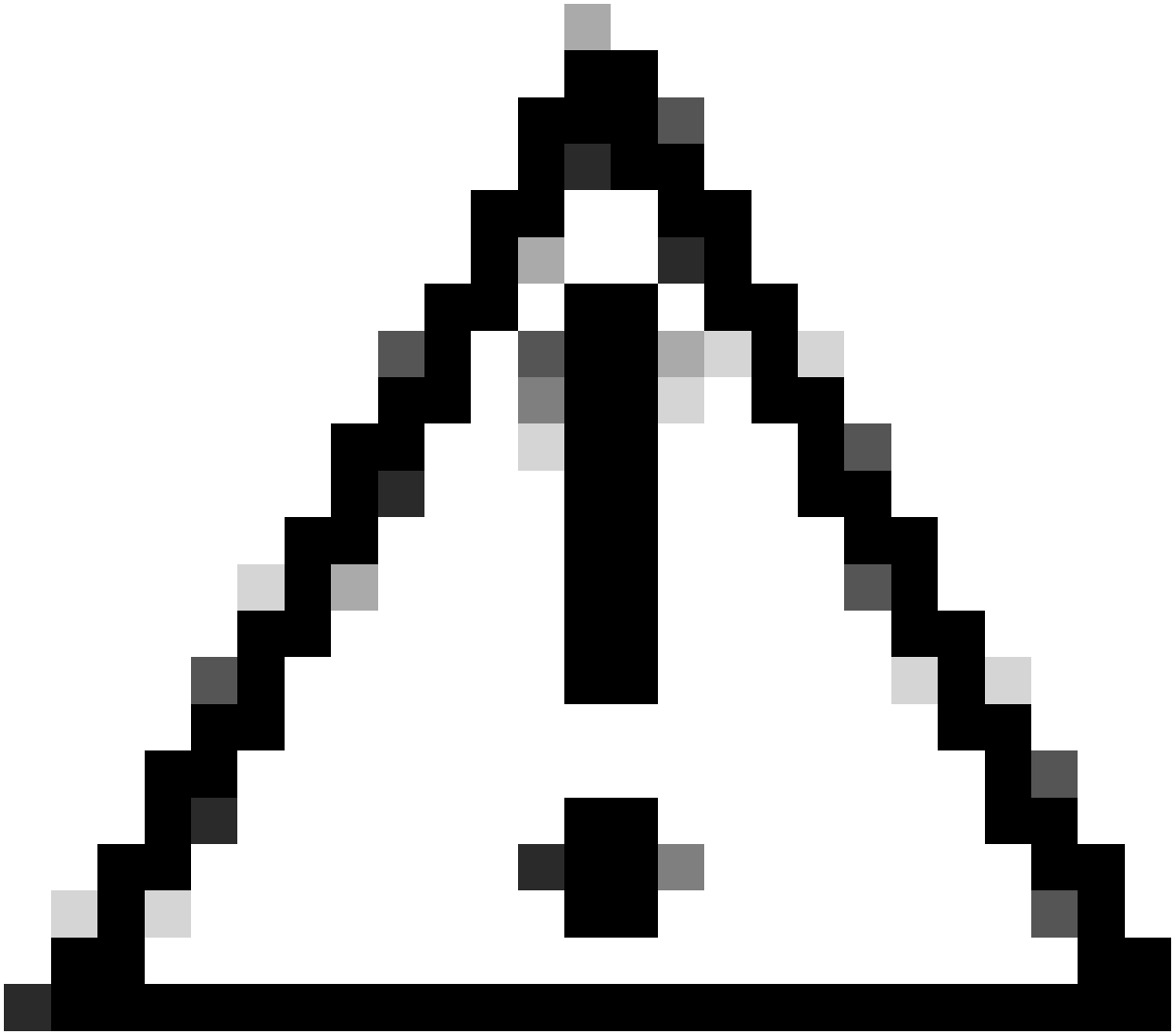
这是可选配置，只有在您打算加密SAML响应时才需要此配置。



创建SSO ZIP文件

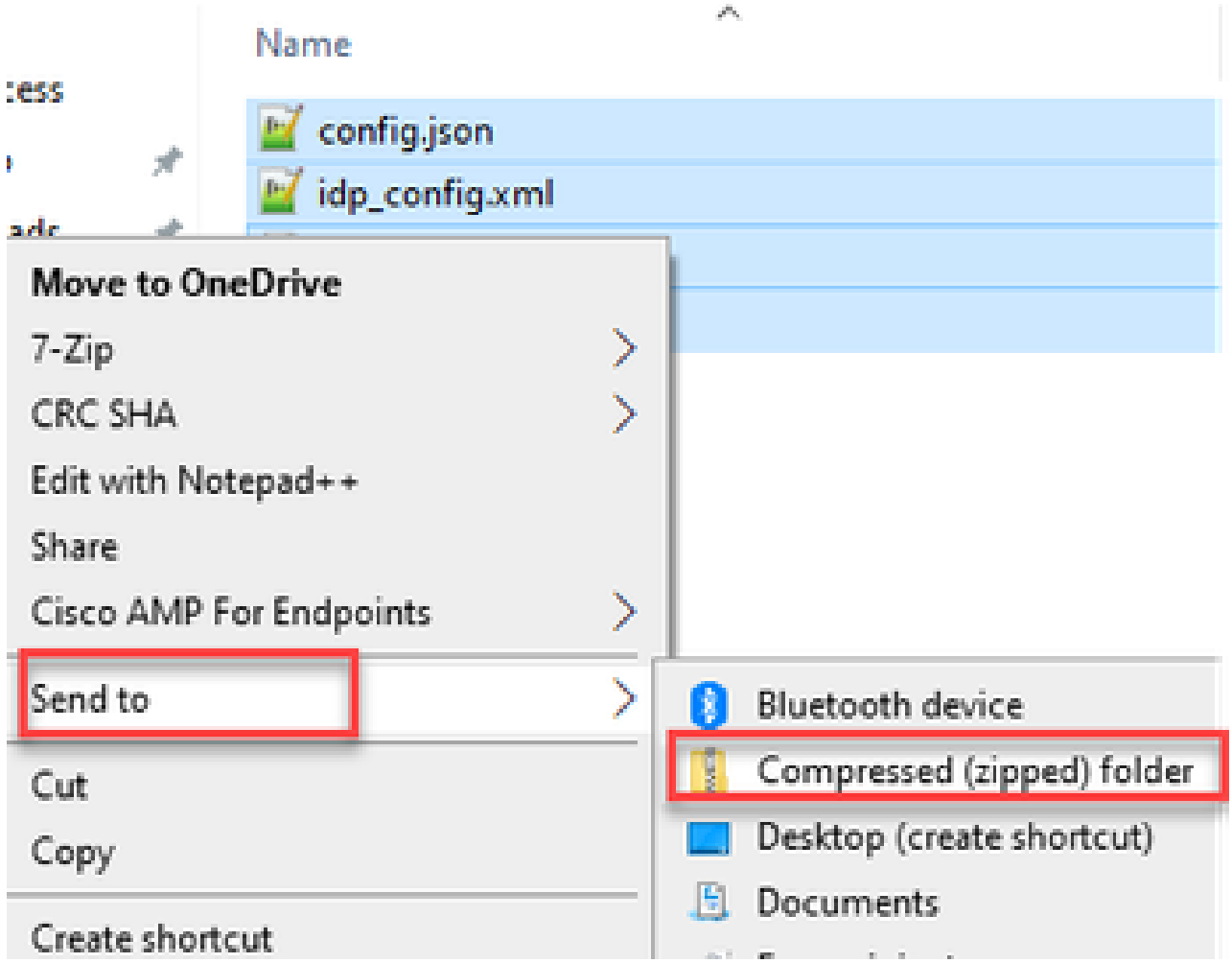
1. 突出显示要用于SSO配置文件的所有文件。



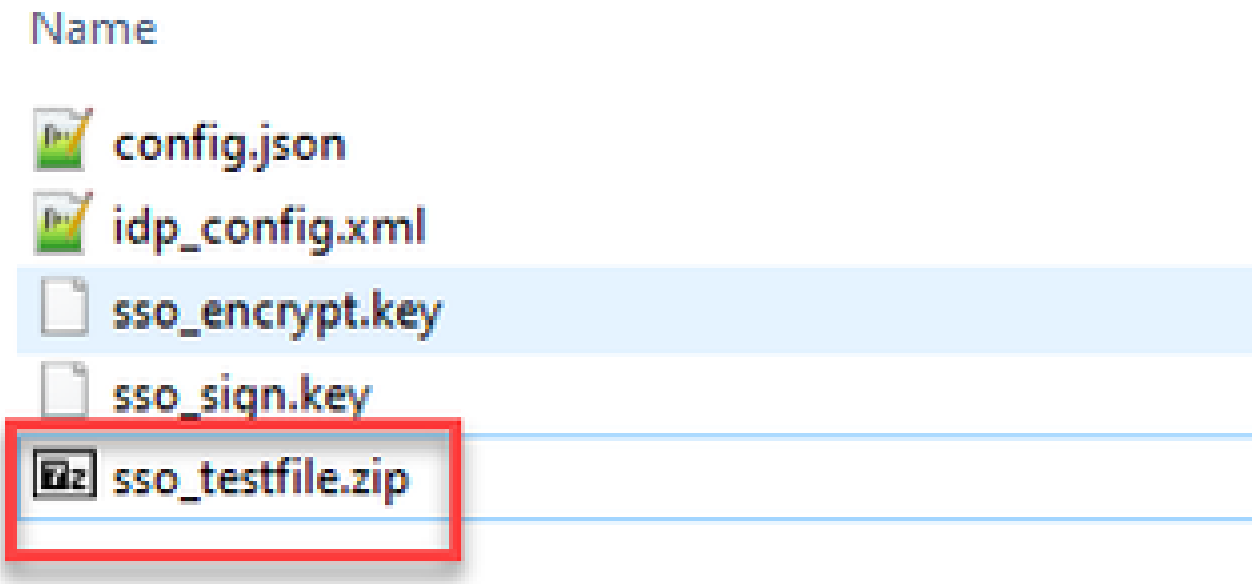


注意：请勿压缩包含文件的文件夹，因为这样会导致SSO不工作。

2. 右键单击突出显示的文件，然后选择“发送到”>“压缩的(zipped)”文件夹。



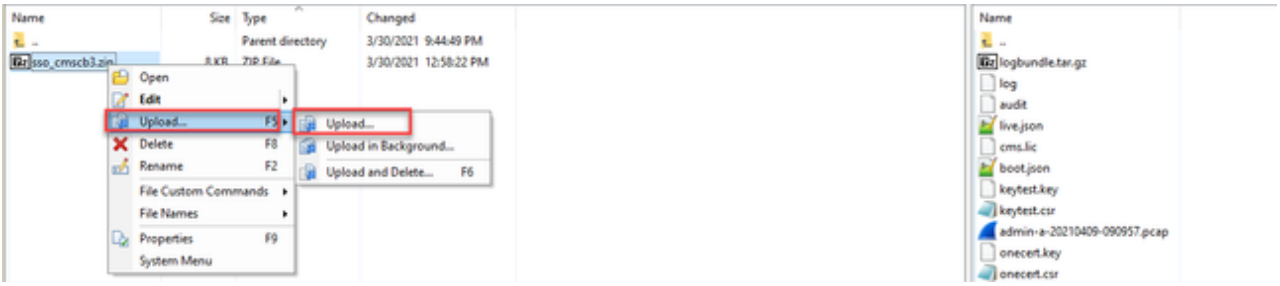
3. 压缩文件后，使用sso_前缀将其重命名为所需的名称：



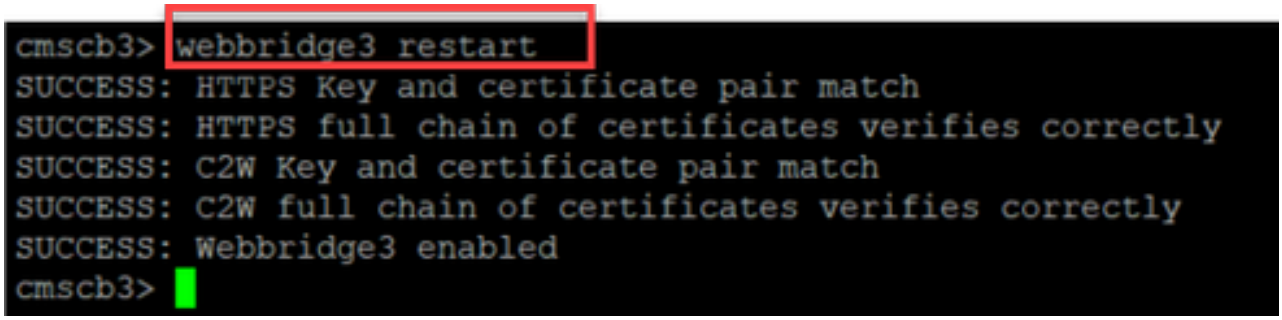
将SSO Zip文件上传到Webbridge

打开SFTP/SCP客户端（在本例中使用WinSCP），然后连接到托管Webbridge3的服务器。

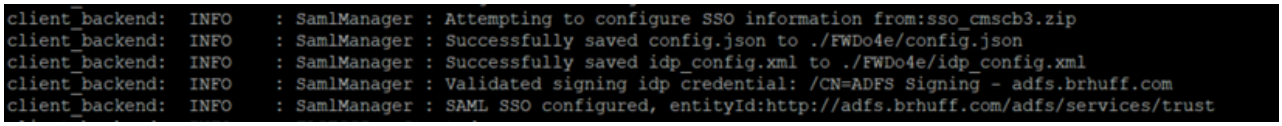
1. 在左窗格中，导航至SSO Zip文件所在的位置，然后右键单击选择上传或拖放文件。



2. 文件完全上传到Webbridge3服务器之后，请打开SSH会话并运行webbridge3 restart命令。



3. 在系统日志中，这些消息表明SSO启用成功：

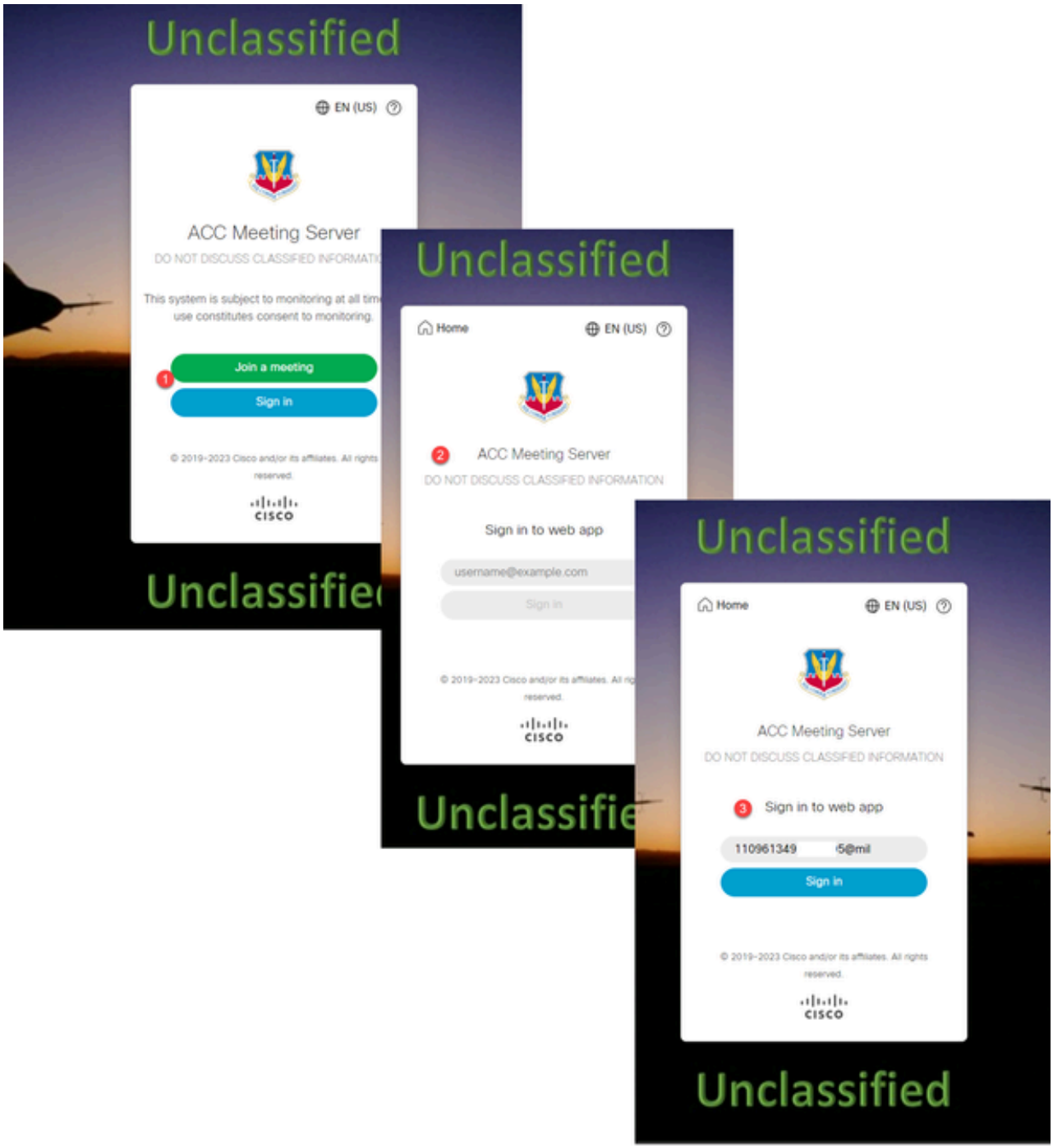


通用访问卡(CAC)

通用访问卡(CAC)是一种智能卡，可作为现役军事人员、国防部文职人员和合格承包商人员的标准标识。

以下是使用CAC卡的用户的整个登录过程：

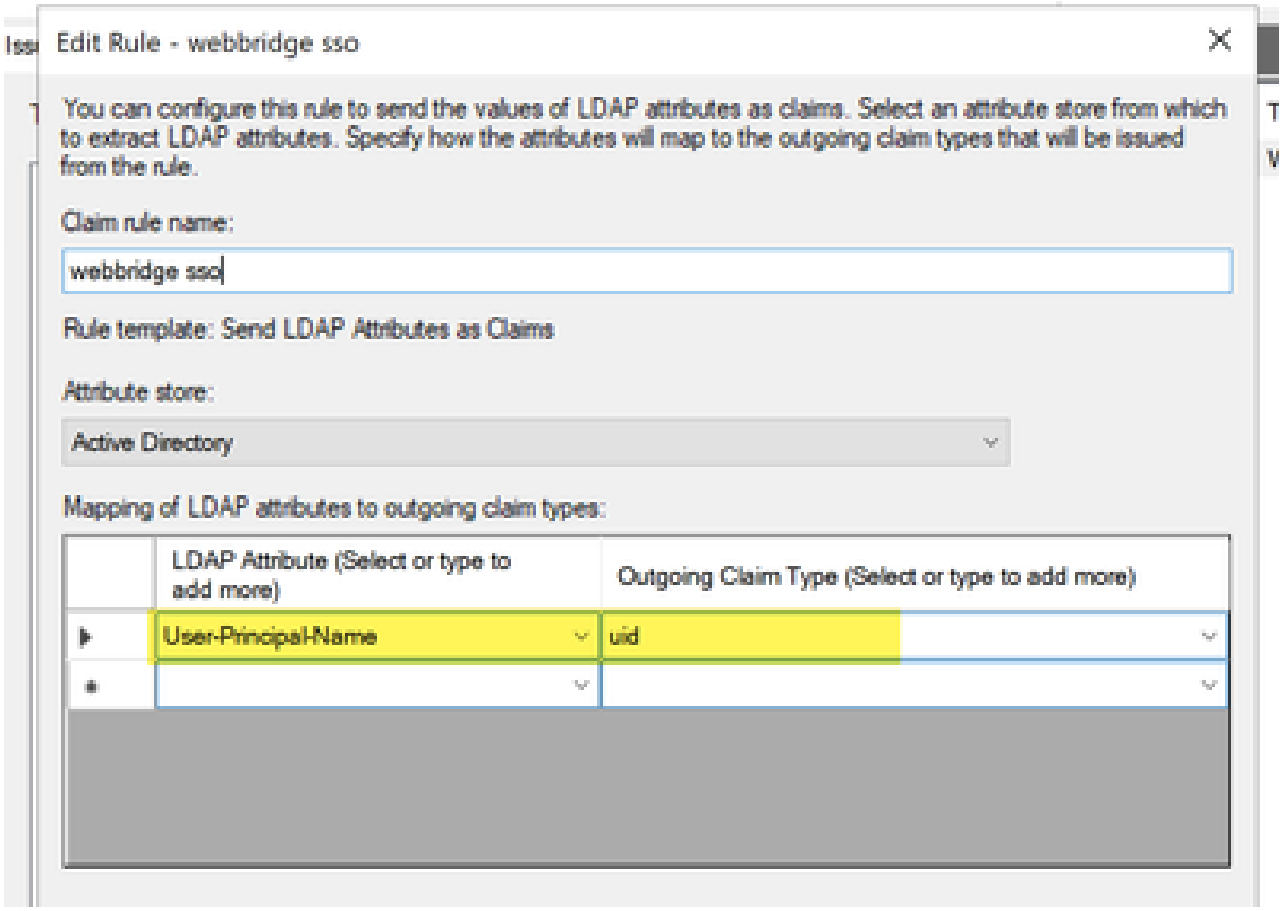
1. 打开PC并粘入CAC卡
2. 登录（有时选择证书），然后输入Pin
3. 打开浏览器
4. 导航到加入URL，然后查看加入会议或登录选项
5. 登录：输入配置为jidMapping的用户名，Active Directory将要求进行CAC登录
6. 点击登录
7. ADFS页面会短暂显示并自动填充
8. 用户将在此时登录



在Ldapmapping中配置jidMapping（这是用户登录名），与ADFS用于CAC卡一样。$userPrincipalName$例如（区分大小写）

还要为authenticationIdMapping设置相同的LDAP属性，以匹配ADFS中声明规则中使用的属性。

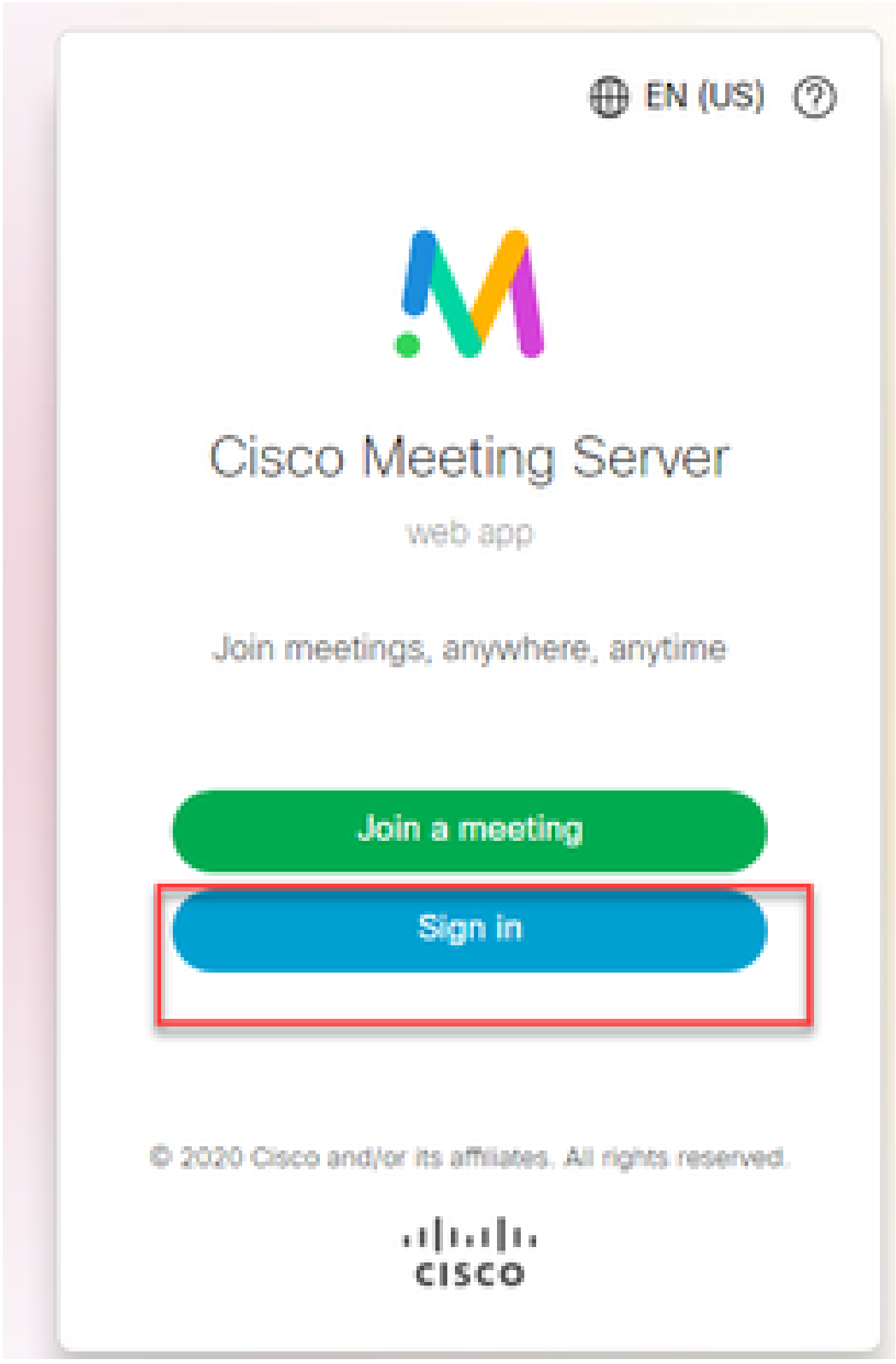
在这里，声明规则显示它将将$userPrincipalName$作为UID发送回CMS。



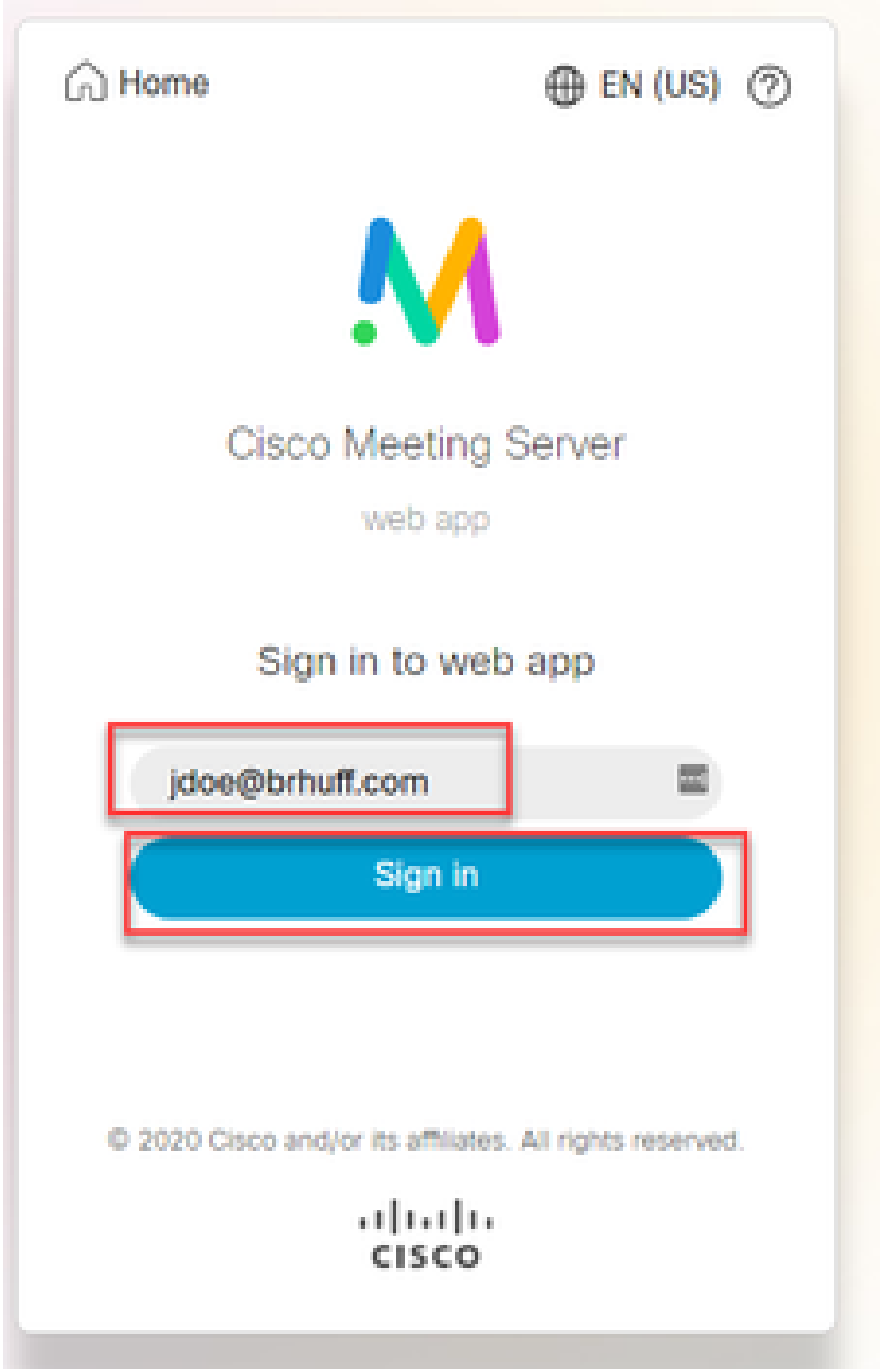
测试通过WebApp的SSO登录

现在已配置SSO，您可以测试服务器：

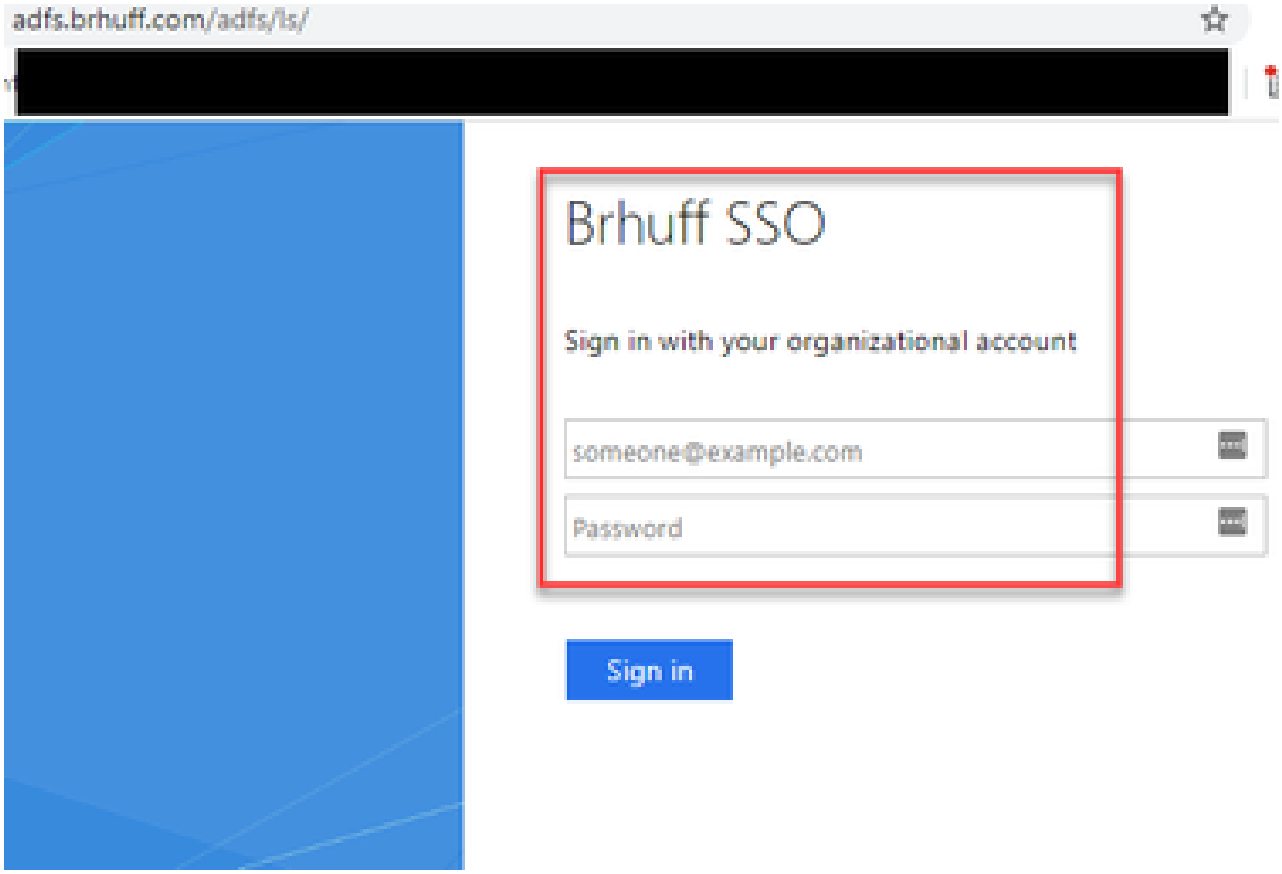
1. 导航到Web应用的Webbridge URL，然后选择登录按钮。


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

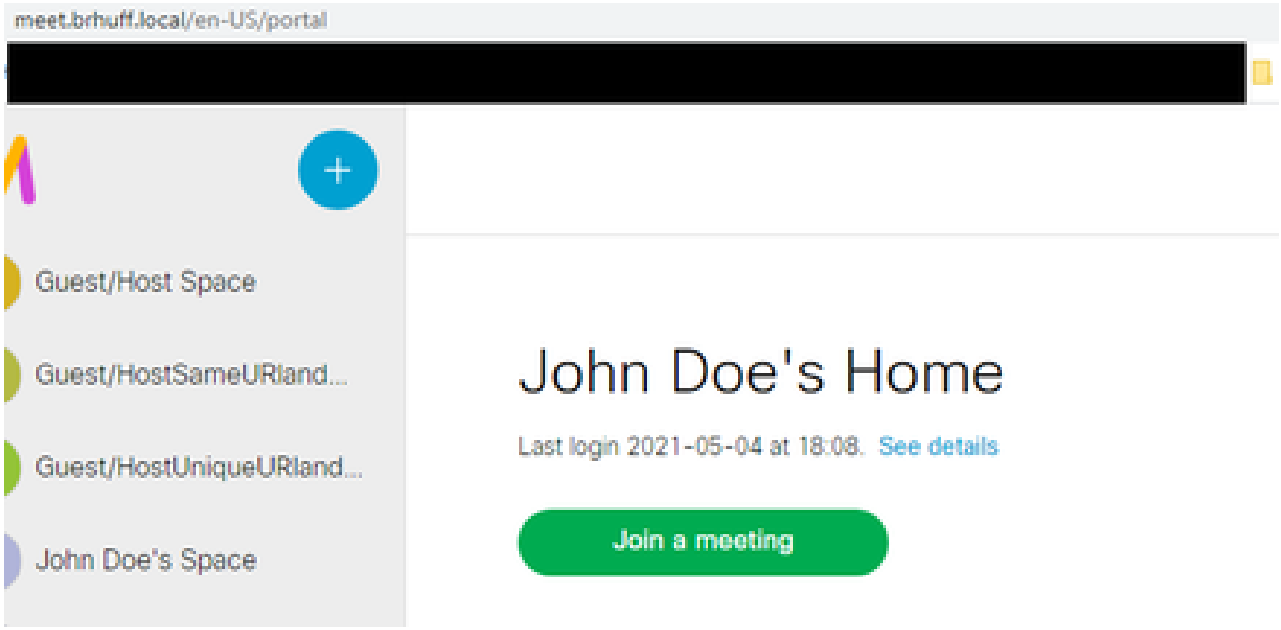
2. 系统将向用户提供输入其用户名的选项（注意此页面上没有password选项）。


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. 然后，用户被重定向到ADFS页面（在输入用户详细信息后），用户必须在此输入凭证以对IdP进行身份验证。



4. 在使用IdP输入和验证凭证后，用户使用令牌重定向，以访问Web App主页：



故障排除

基本故障排除

有关任何SSO问题的基本故障排除：

1. 确保已正确配置用于在IdP中导入作为信赖信任的Webbridge3的构造元数据，并且配置的URL与config.json中的ssoServiceProviderAddress完全匹配。
2. 确保IdP提供的并压缩到Webbridge3 sso配置文件的元数据是IdP中的最新元数据，如同服务器主机名、证书等发生任何更改一样，需要将其重新导出并压缩到配置文件中。
3. 如果使用签名和加密私钥来加密数据，请确保正确的匹配密钥是您上传到webbridge的sso_xxxx.zip文件的一部分。如有可能，尝试在不使用可选私钥的情况下进行测试，以查看SSO是否可以在没有此加密选项的情况下正常工作。
4. 确保为config.json配置了SSO域、Webbridge3 URL和期望的身份验证映射的正确详细信息，以匹配SAMLResponse。

从日志的角度尝试进行故障排除也很理想：

1. 导航到Webbridge URL时，在URL末尾放置？trace=true以启用对CMS Syslog的详细日志记录。(例如：https://join.example.com/en-US/home?trace=true)。
2. 在Webbridge3服务器上运行syslog follow以在测试期间实时捕获，或利用附加到URL的跟踪选项运行测试，并从Webbridge3和CMS Callbridge服务器收集logbundle.tar.gz。 如果Webbridge和Callbridge位于同一服务器上，则只需要一个logbundle.tar.gz文件。

Microsoft ADFS故障代码

有时，SSO进程出现故障，可能会导致IdP配置或其与IdP的通信失败。如果使用ADFS，最好查看下一个链接，确认所发现的故障并采取补救措施：

Microsoft状态代码

例如：

> client_backend：错误： SamlManager ： SAML身份验证请求_e135ca12-4b87-4443-abe1-30d396590d58失败，原因为： urn：oasis：names：tc：SAML：2.0：status：Responder

此错误表明，根据以前的文档，此故障是由于IdP或ADFS引起的，因此需要由ADFS的管理员进行处理，才能解决。

未能获取authenticationID

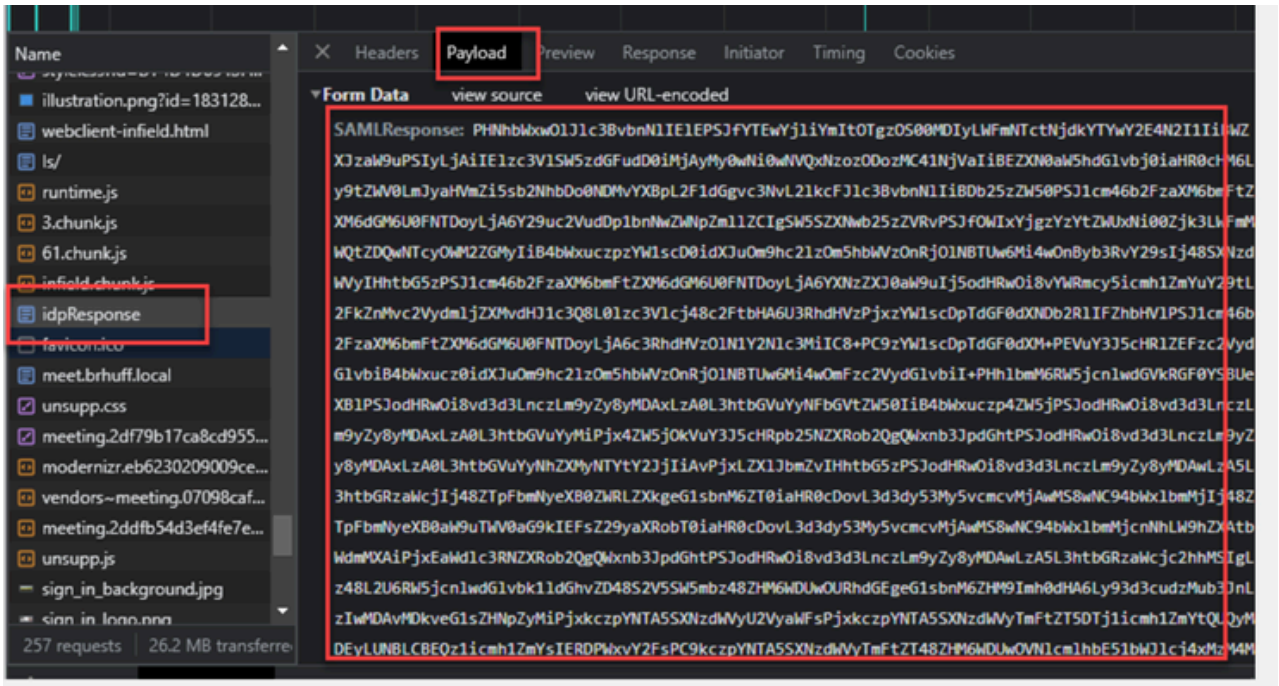
在某些情况下，在从IdP交换SAMLResponse期间，Webbridge可能会在日志中显示此错误消息，并且通过SSO登录失败：

> client_backend： INFO ： SamlManager ： [57dff9e3-862e-4002-b4fa-683e4aa6922c]无法获取authenticationId

这表示在检查在身份验证交换期间从IdP传回的SAMLResponse数据时，Webbridge3在响应中找不到有效的匹配属性(与authenticationId的config.json相比)。

如果通信未使用签名和加密私钥加密，则可通过Web浏览器从Developer Tools Network Logging提取SAML响应并使用base64进行解码。如果响应已加密，您可以从IdP端请求已解密的SAML响应。

在开发人员工具网络日志记录输出（也称为HAR数据）中，在name列下查找idpResponse，然后选择Payload查看SAML响应。 如前所述，可以使用base64解码器对此进行解码。



接收SAMLResponse数据时，请检查<AttributeStatement>部分以查找发回的属性名称，在此部分中，您可以找到从IdP配置和发送的声明类型。例如：

```
<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>

通过检查以前的名称，可以检查Attribute Statement部分下的<AttributeName>，并将每个值与SSO config.json的authenticationIdmapping部分中的设置进行比较。

在上一个示例中，您可以看到authenticationIdMapping的配置与传递的内容不完全匹配，因此导致无法找到匹配的authenticationId：

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

为了解决此问题，可以尝试两种方法：

1. 可以更新IdP传出声明规则，使其与在Webbridge3上的config.json的authenticationIdMapping中配置的完全匹配。(在http://example.com/claims/NameID的IdP上添加了声明规则)
   或者
2. 可以在Webbridge3上更新config.json，使“authenticationIdMapping”与IdP上配置的传出声明规则之一完全匹配。(即“authenticationIdMapping”以匹配属性名称之一，可以是“uid”、“<URL>/NameID”或“<URL>/CommonName”。只要与Callbridge API上配置的预期值匹配（完全匹配）（在传递时）

验证中未传递或匹配断言

有时，在从IdP交换SAMLResponse期间，Webbridge会显示以下错误，指示匹配断言失败，并跳过任何与服务器配置不匹配的断言：

client_backend：错误： SamlManager：没有通过验证的断言
client_backend： INFO ： SamlManager ：跳过断言，不在允许的受众范围内

此错误表示当从IdP查看SAMLResponse时，Webbridge找不到任何匹配的断言，因此跳过不匹配的故障，最终导致无法正常的SSO登录。

为了找到此问题，最好从IdP查看SAMLResponse。 如果通信未使用签名和加密私钥加密，则可通过Web浏览器从开发人员工具网络日志记录提取SAML响应，然后使用base64进行解码。如果响应已加密，您可以从IdP端请求已解密的SAML响应。

在查看SAMLResponse数据时，通过查看响应的<AudienceRestriction>部分，您可以找到此响应受限制的所有对象：

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

</条件>

使用<Audience>部分(https://cisco.example.com))中的值，您可以将其与Webbridge配置的config.json中的ssoServiceProviderAddress进行比较，并验证其是否完全匹配。对于本示例，您可以看到失败原因是受众与配置中的服务提供商地址不匹配，因为它具有附加的：443：

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

这要求两者之间完全匹配，以免导致此类故障。对于此示例，修复方法为以下两种方法之一：

1. 可以从config.json的ssoServiceProviderAddress部分的地址中删除：443，使其与IdP的SAMLResponse中提供的Audience字段匹配。
或者

2. 可以更新IdP中Webbridge3的元数据或信赖信任方，以便将：443附加到URL。(如果更新了元数据，则必须再次将其作为ADFS上的信赖信任方导入。但是，如果直接从IdP向导修改信赖信任方，则不需要再次导入它。)

登录Web应用失败：

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

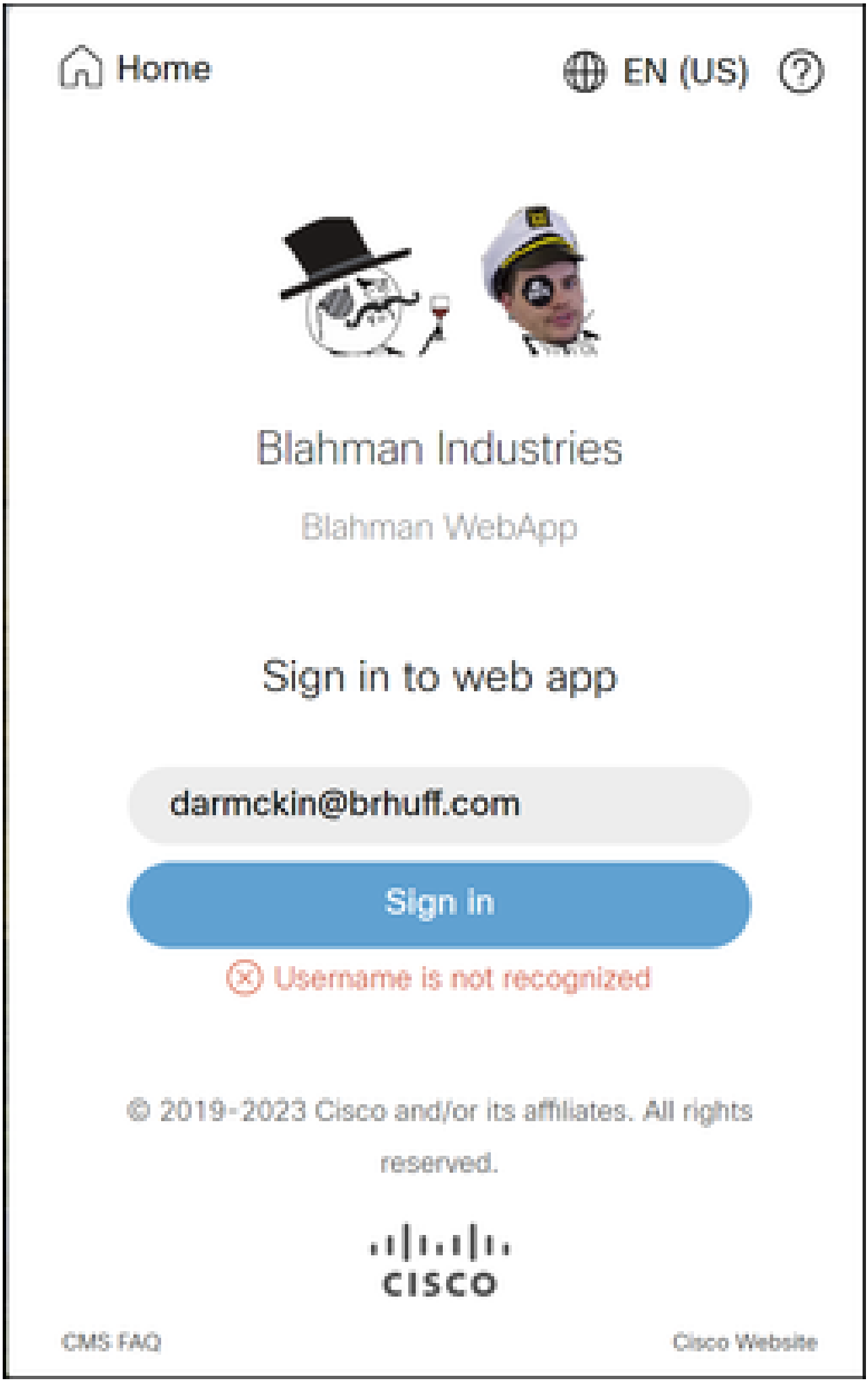
id=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c-0272-42a1-b125-136fdf5612a5 (user=steve@brhuff.com)

3月18日14:58:48.092 user.info cmscb3-1 host：server：信息：未找到要进行授权的用户

3月18日14:58:48.092 user.info cmscb3-1 host：server：信息：来自steve@brhuff.com的登录请求失败

方案 2：

用户在Web应用中输入了正确的登录信息，并在SSO页面中输入了用于向LDAP进行身份验证的正确凭证，但是他们无法登录，因为无法识别用户名。


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

无法识别用户名

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

3月18日15:08:52.399 user.warning cmscb3-1 host：server： WARNING： rejecting login attempt from user 'darmckin@brhuff.com' — authenticationId不正确

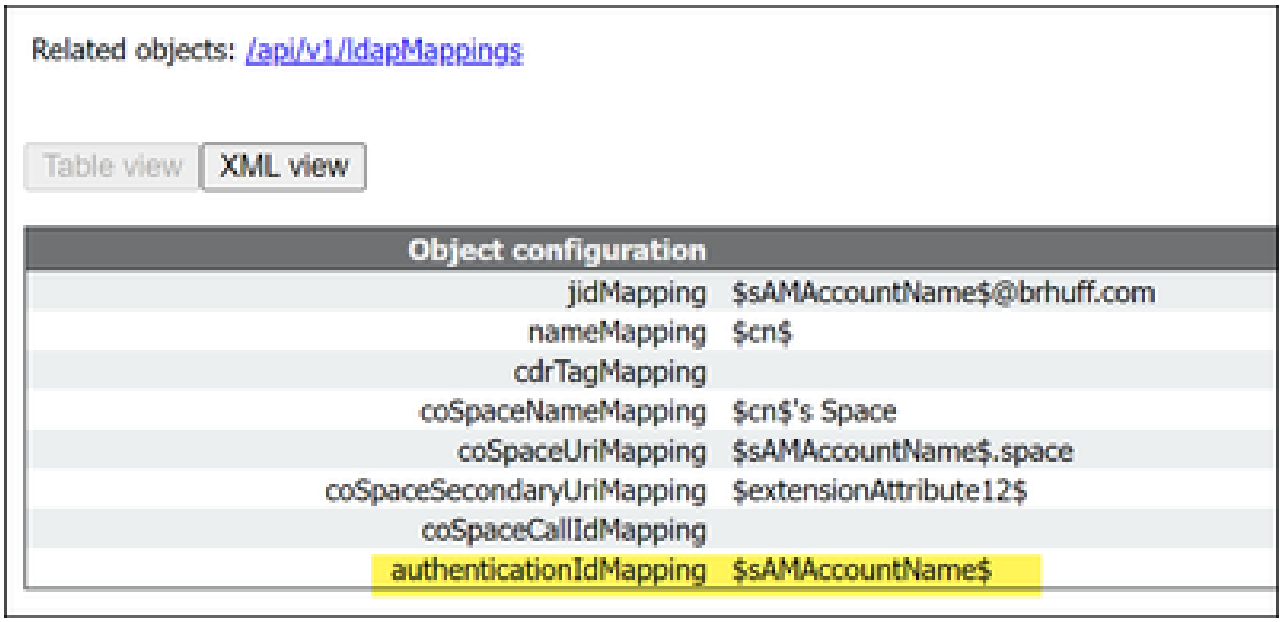
3月18日15:08:52.412 user.info cmscb3-1 host：server：信息：来自darmckin@brhuff.com的登录请求失败

CMS ldapmapping中的AuthenticationIdMapping与ADFS中用于声明规则的已配置LDAP属性不匹配。下面一行“Successfully obtain authenticationID：darmckin@brhuff.com”表示ADFS已配置声明规则，该规则具有从active directory获取darmckin@brhuff.com的属性，但CMS API > Users中的AuthenticationID显示它需要darmckin。 在CMS ldapMappings中，AuthenticationID配置为$sAMAccountName$，但ADFS中的声明规则配置为发送电子邮件地址，因此不匹配。

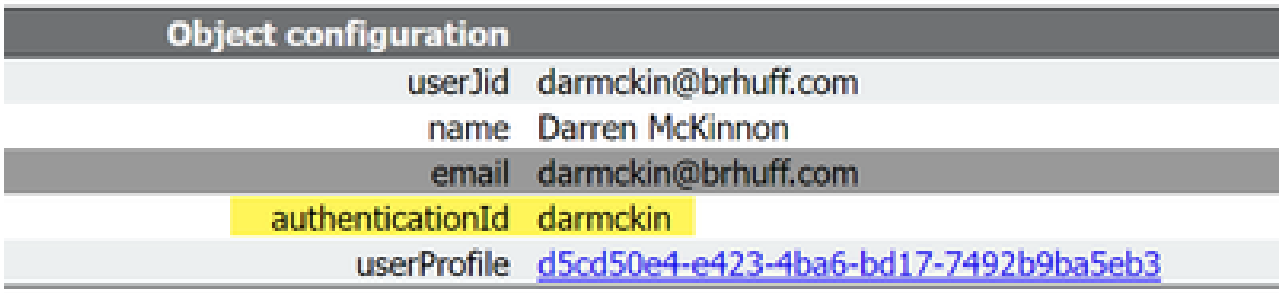
如何解决此问题：

执行下列操作之一：

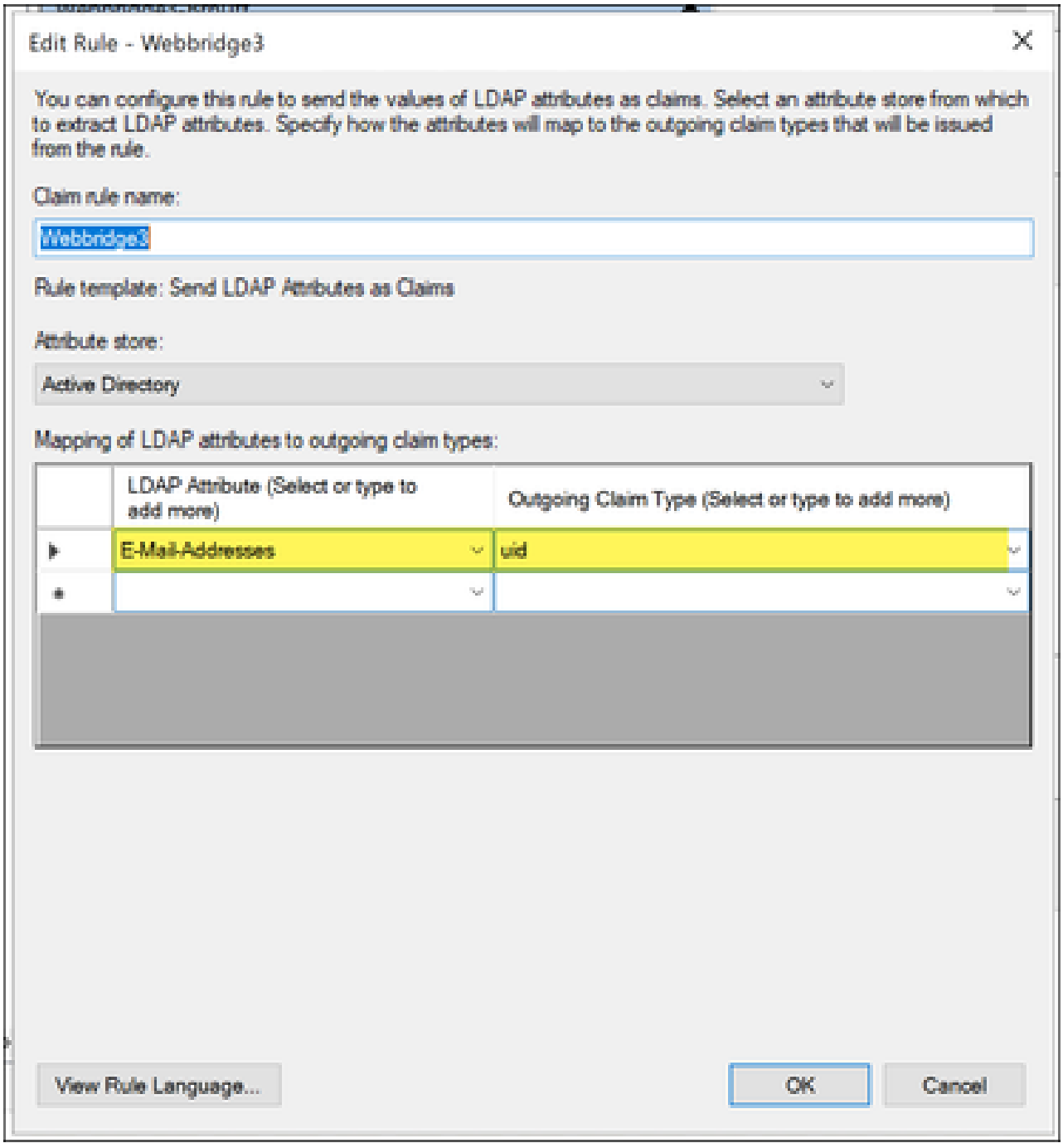
1. 更改CMS ldapmapping中的AuthenticationID以匹配ADFS上的声明规则中使用的内容，并执行新同步
2. 更改ADFS声明规则中使用的LDAP属性，以匹配CMS ldapmapping中的配置



API LDAP映射



API用户示例



来自ADFS的领款申请规则

显示工作日志的Webbridge日志示例。 在联接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：信息
：SamlManager：[7979f13c-d490-4f8b-899c-0c82853369ba]匹配的SSO sso_2024.zip in SAML Token Request

3月18日14:24:01.096 user.info cmscb3-1 client_backend：信息
：SamlManager：[7979f13c-d490-4f8b-899c-0c82853369ba]正在尝试在SAML IDP响应中查找SSO

3月18日14:24:01.101 user.info cmscb3-1 client_backend：信息：SamlManager：[7979f13c-d490-4f8b-899c-0c82853369ba]已成功获取身份验证ID：darmckin@brhuff.com

3月18日14:24:01.102 user.info cmscb3-1 host：服务器：信息：WB3Cmgr：[7979f13c-d490-4f8b-899c-0c82853369ba] AuthRequest已收到连接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：信息：来自darmckin@brhuff.com的成功登录请求

3月18日14:24:01.130 user.info cmscb3-1 host：服务器：信息：WB3Cmgr：[7979f13c-d490-4f8b-899c-0c82853369ba]正在发出JWT ID e2a860ef-f4ef-4391-b5d5-9abdfa89ba0f

3月18日14:24:01.132 user.info cmscb3-1 host：服务器：信息：WB3Cmgr： [7979f13c-d490-4f8b-899c-0c82853369ba]正在发送身份验证响应(jwt长度=1064，连接=64004556-faea-479f-aabe-691e17783aa5)

3月18日14:24:01.133 local7.info cmscb3-1 56496041063b wb3_frontend：[Auth：darmckin@brhuff.com，跟踪：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_response user_agent "Mozilla/5.0 (Windows NT 10.0； Win64； x64) AppleWebKit/537.36（KHTML，与Gecko一样）Chrome/122.0.0.0 Safari/537.36”到上行192.0.2.2:9000： upstream_response_time 0.038 request_time 0.039 msec 1710786241.133 upstream_response_length 24 200

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。