在CMS上配置并排除WebApp SSO故障

目录

简介

先决条件

- 要求
- 使用的组件

背景

配置

网络图

ADFS安装和初始设置

将CMS用户映射到身份提供程序(IdP)

为IdP创建Webbridge元数据XML

将Webbridge的元数据导入身份提供程序(IdP)

在IdP上为Webbridge服务创建声明规则

为Webbridge创建SSO存档ZIP文件：

- 获取并配置idp_config.xml
- 创建包含内容的config.jsonFile
- 设置sso_sign.key（可选）
- 设置sso_encrypt.key（可选）
- 创建SSO ZIP文件
- 将SSO Zip文件上传到Webbridge

通用访问卡(CAC)

测试通过WebApp登录的SSO

故障排除

- 基本故障排除
- Microsoft ADFS故障代码
- 未能获取authenticationID
- 在验证中未传递/匹配断言
- 在Web应用上登录失败：
  - 情形 1：
  - 方案 2：
  - 情形 3：
- 用户名无法识别
  - 情形 1：
  - 方案 2：
- 显示工作日志的Webbridge日志示例。在加入URL中使用？trace=true生成的示例：

常见问题解答 (FAQ)

- 能否扩展Webapp SSO JWT?
- 如果我关闭浏览器，是否需要重新向WebApp进行身份验证？
- WebApp SSO中如何支持多个域？

相关信息

简介

本文档介绍如何配置单点登录(SSO)的思科会议服务器(CMS)Web应用实施并对其进行故障排除。

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

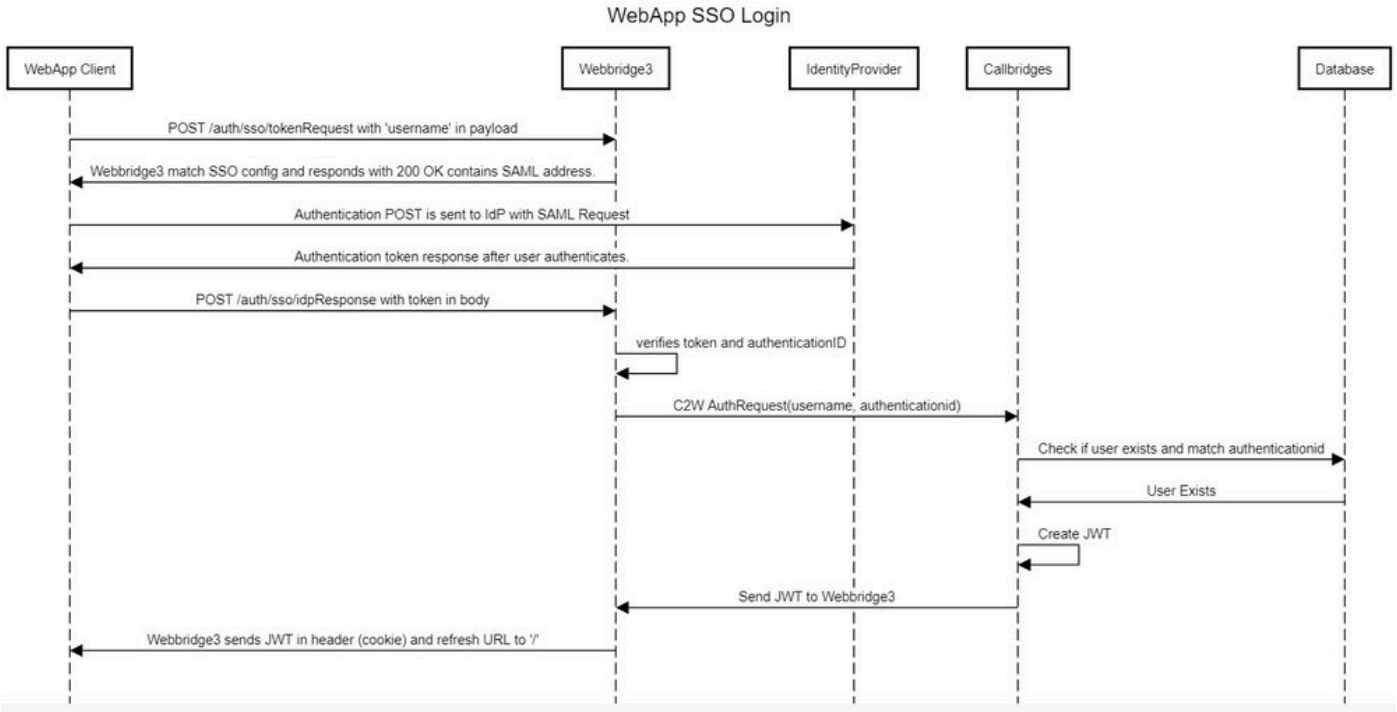
CMS 3.1及更高版本引入了用户使用SSO进行登录的功能，无需在用户每次登录时输入密码，因为单个会话由身份提供程序创建。
此功能使用安全断言标记语言(SAML)版本2.0作为SSO机制。

注意：CMS在SAML 2.0中仅支持HTTP-POST绑定，并拒绝任何没有可用HTTP-POST绑定的标识提供程序。

注意：启用SSO后，基本LDAP身份验证将不再可用。

配置

网络图



ADFS安装和初始设置

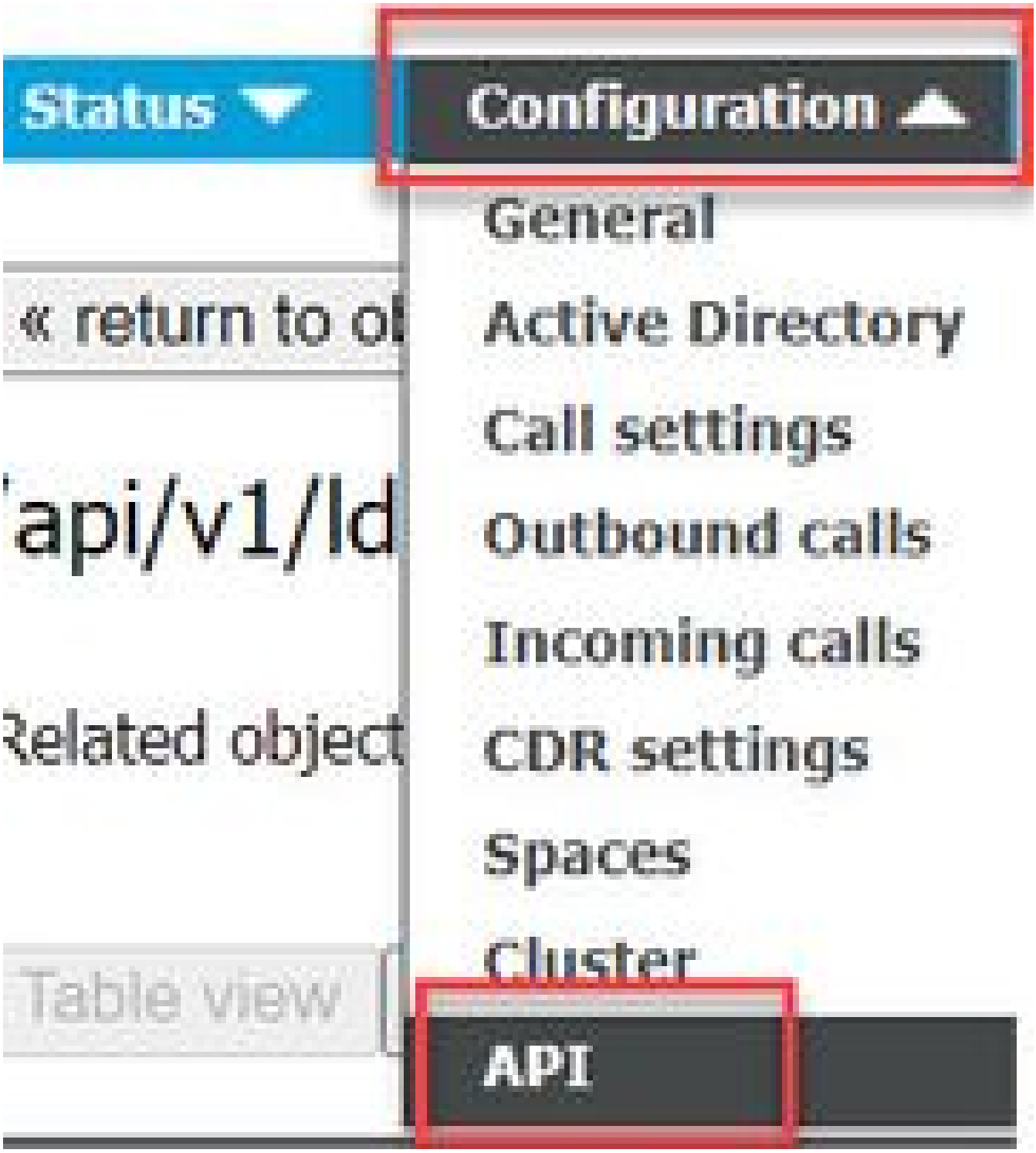
此部署方案使用Microsoft Active Directory联合身份验证服务(ADFS)作为身份提供程序(IdP)，因此，建议在此配置之前安装并运行ADFS（或目标IdP）。

将CMS用户映射到身份提供程序(IdP)

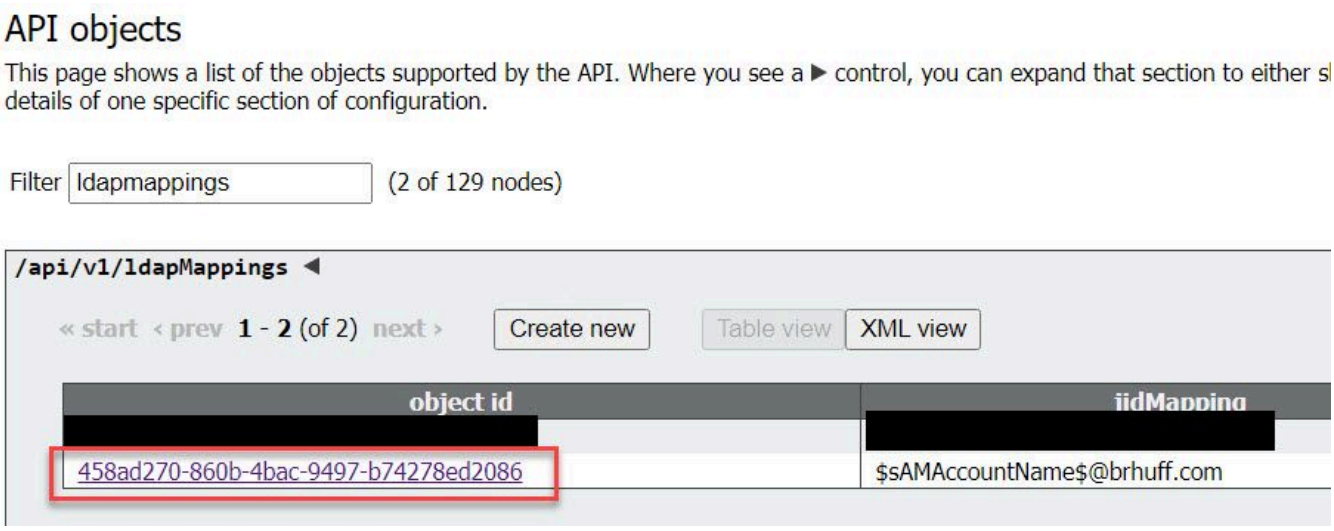
要让用户获得有效的身份验证，必须在IdP提供的相关字段的应用编程接口(API)中映射它们。用于API的ldapMapping中的选项是authenticationIdMapping。

1.在CMS Web Admin GUI上导航到Configuration > API

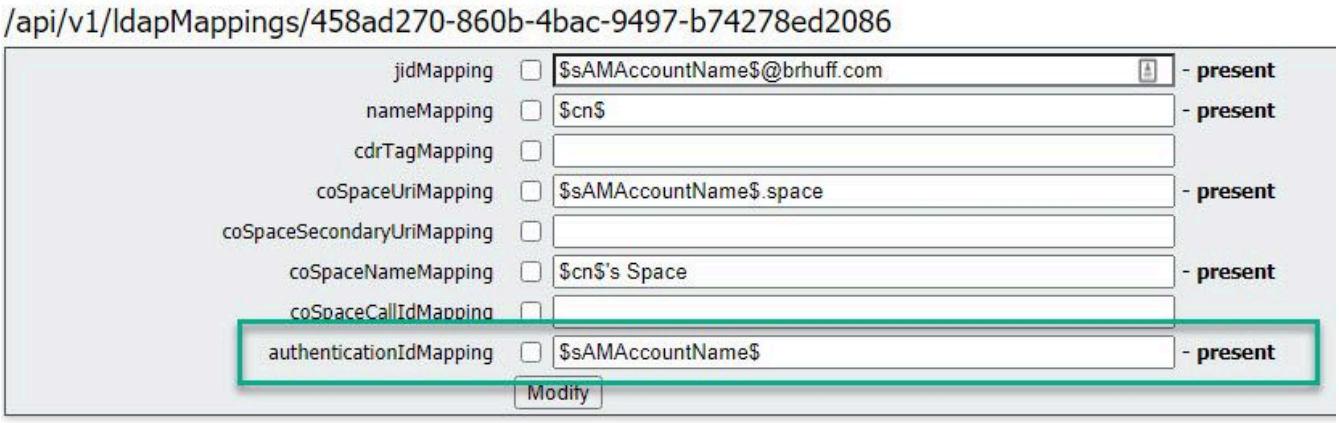
Co



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



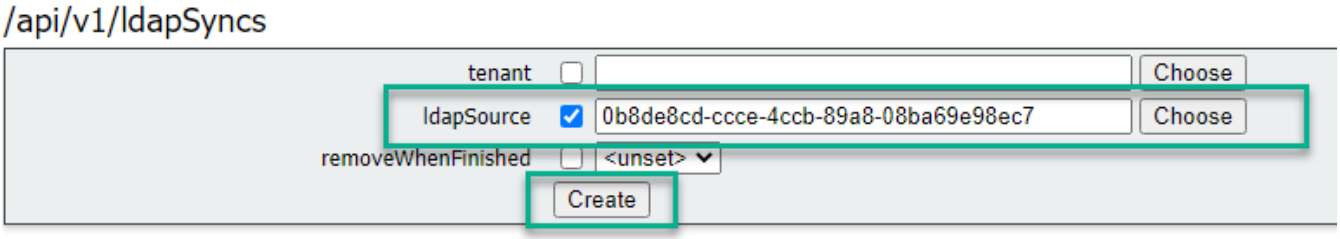
3.在所选的ldapMapping对象中，将authenticationIdMapping更新到从IdP传递的LDAP属性。在本例中，选项$sAMAccountName用作映射的LDAP属性。



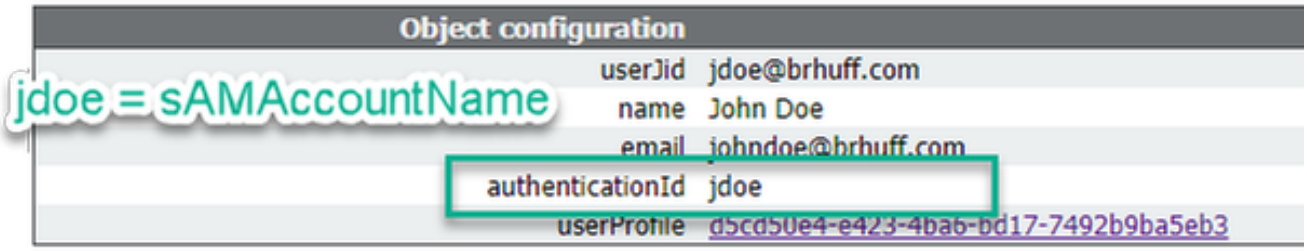
注意：callbridge/数据库使用authenticationIdMapping来验证从SAMLResponse中的IdP发送的声明，并为用户提供一个JSON Web令牌(JWT)。

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，在配置> api/v1/users中的CMS API中导航，并选择已导入的用户，并验证authenticationId是否已正确填充。



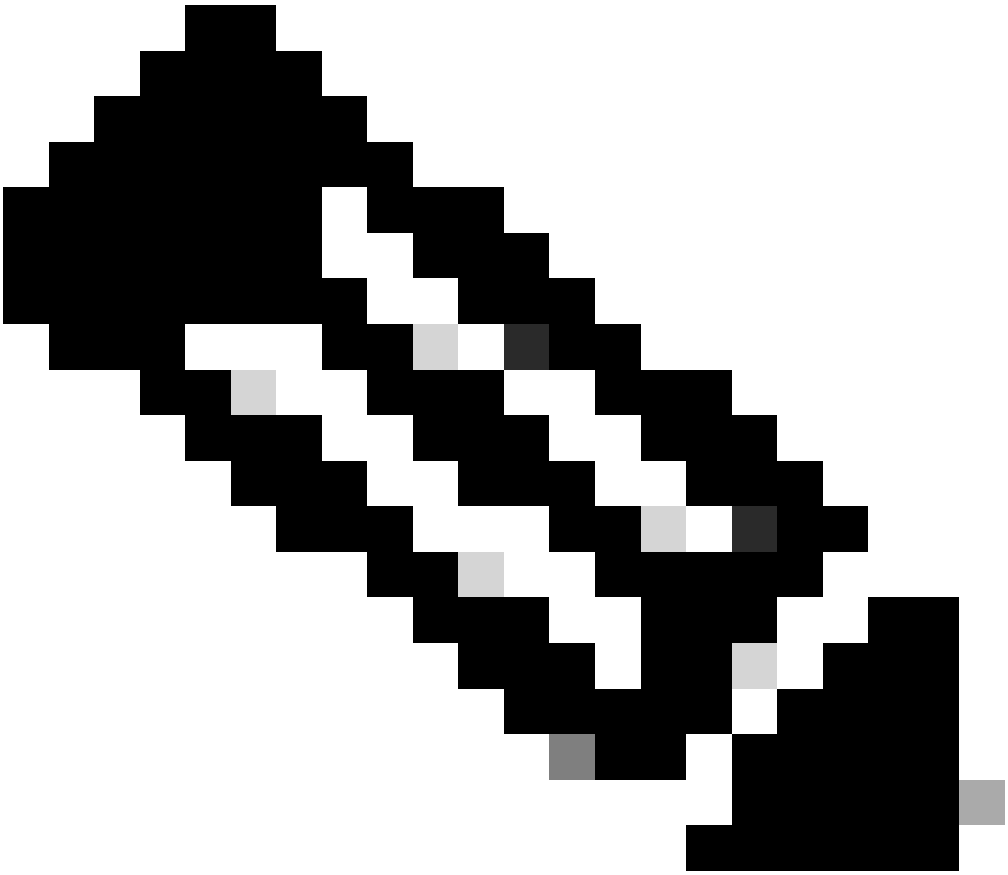
为IdP创建Webbridge元数据XML

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。为此，创建元数据XML文件有几种方法，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）和用户可通过浏览器访问的关联端口。



注意：如果有多个Web网桥使用单个URL，这必须是负载均衡地址。

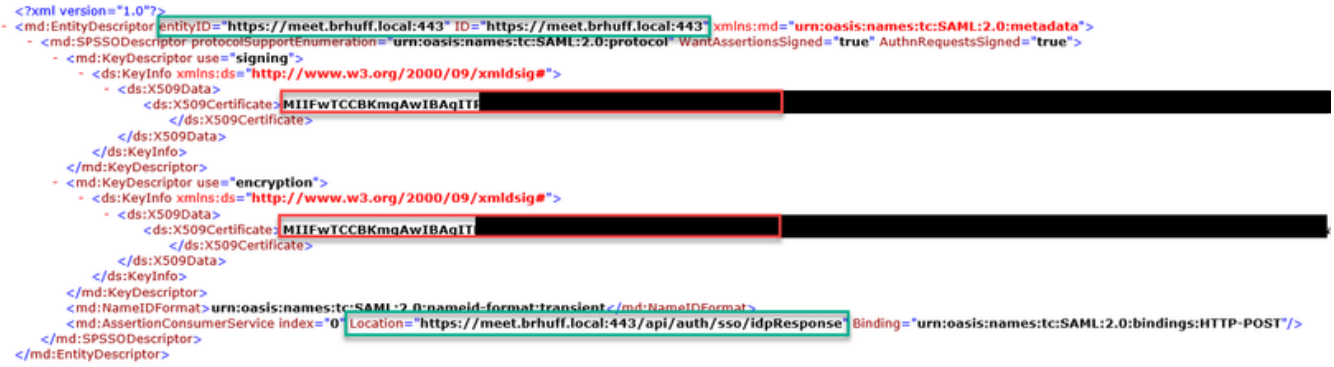
2. Location — 这是Webbridge地址的HTTP-POST AssertionConsumerService的位置。这是指示IdP在登录后将经过身份验证的用户重定向到的位置。必须将其设置为idpResponse URL:https://<WebedgeFQDN>:<port>/api/auth/sso/idpResponse。 例如，https://join.example.com:443/api/auth/sso/idpResponse.

3. 可选 — 用于签名的公钥 — 这是用于签名的公钥（证书），IdP使用该公钥来验证来自Webbridge的AuthRequest。此ID必须与上载到Webbridge上的SSO捆绑包上的私钥“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）。这必须与上载到Webbridge上的SSO捆绑包上的私钥“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：

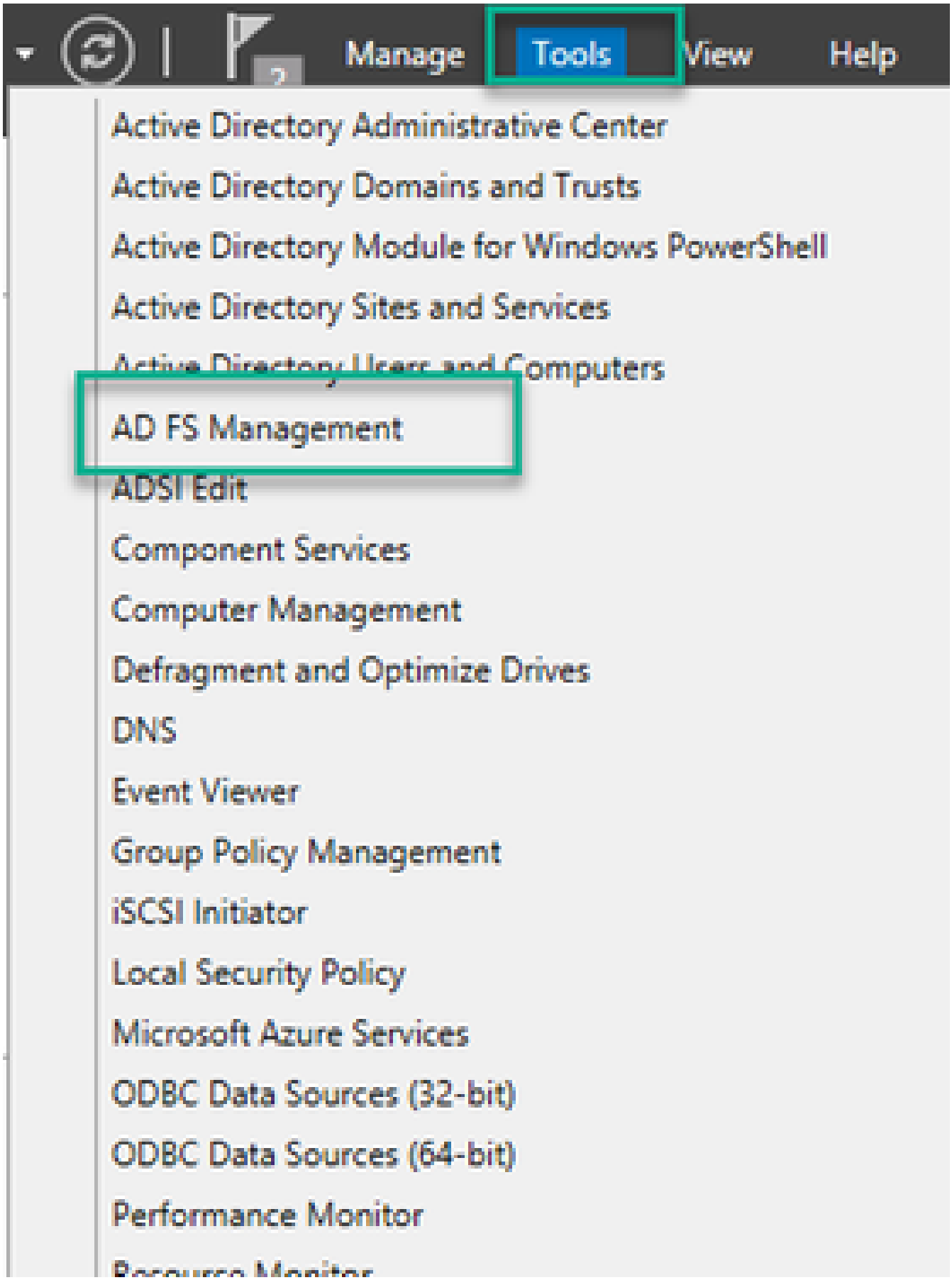


将Webbridge的元数据导入身份提供程序(IdP)

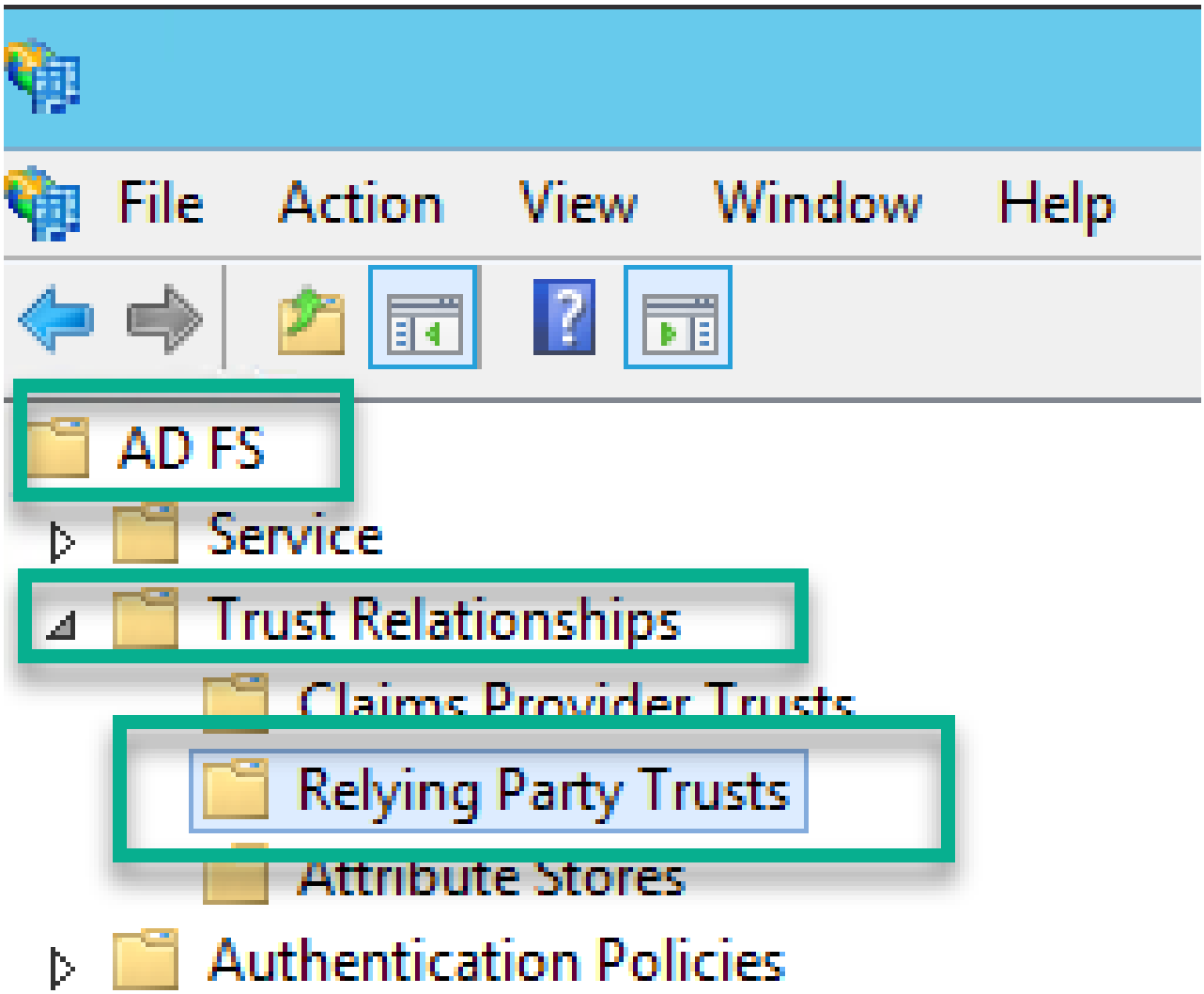
使用正确的属性创建元数据XML后，即可将文件导入Microsoft ADFS服务器以创建信赖信任方。

1.将远程桌面连接到托管ADFS服务的Windows服务器

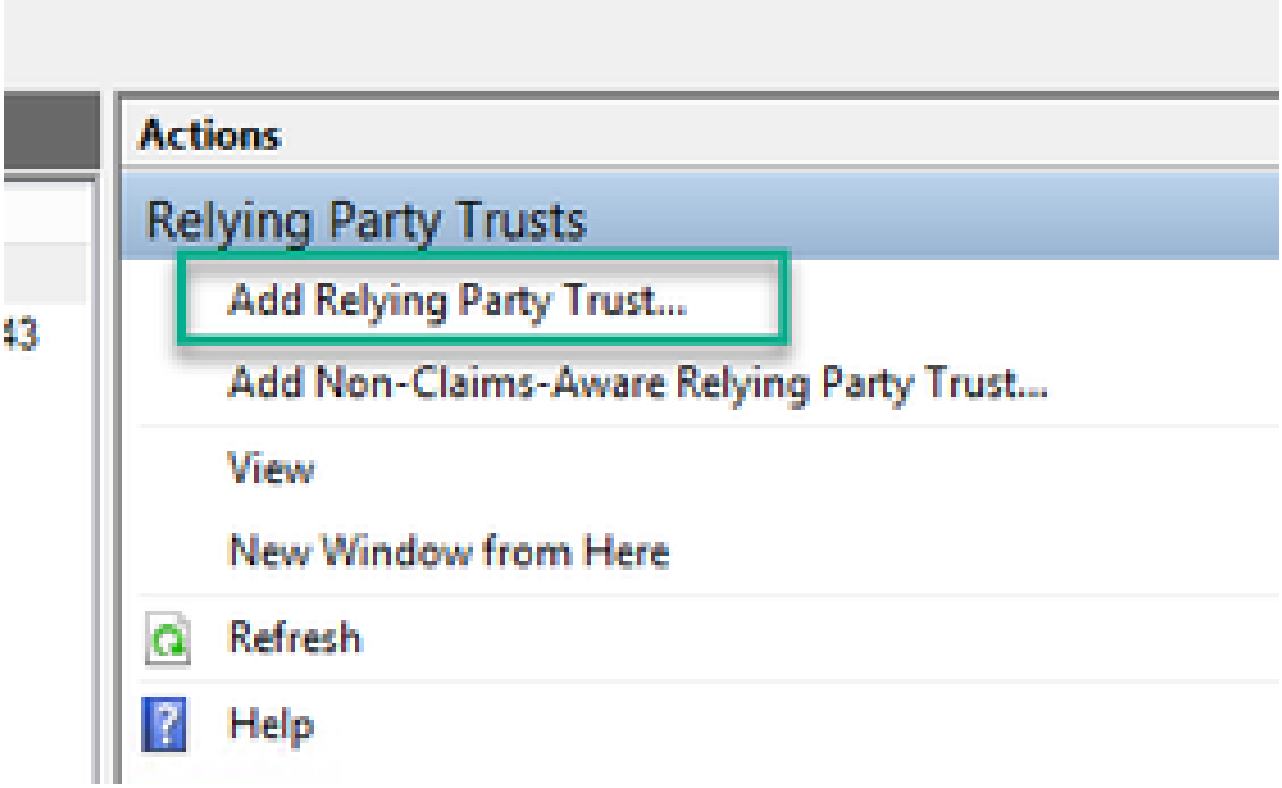
2.打开AD FS管理控制台，通常可以通过服务器管理器访问。



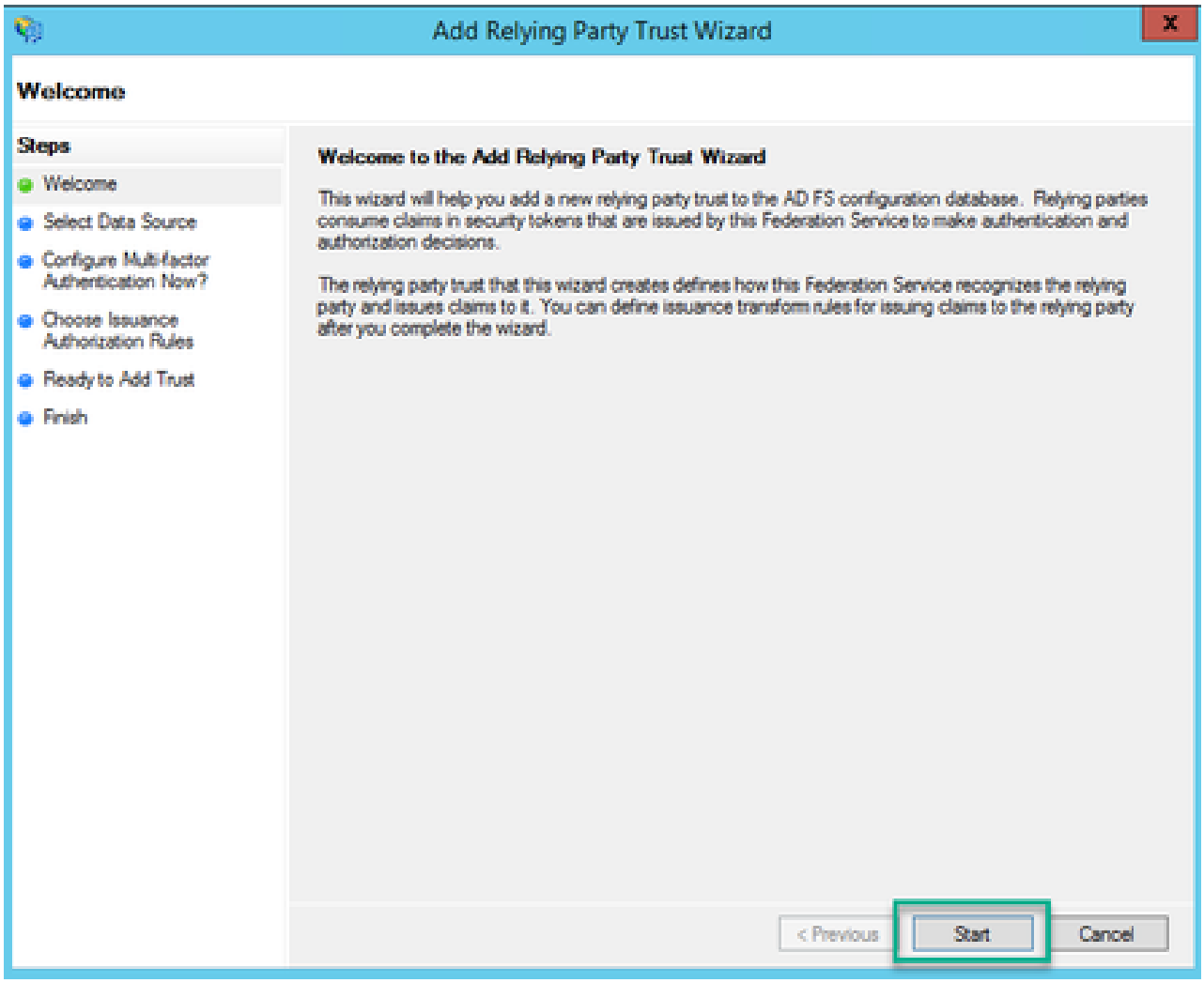
3.进入ADFS管理控制台后，在左侧窗格中导航到ADFS > Trust Relationships > Relying Party Trust。



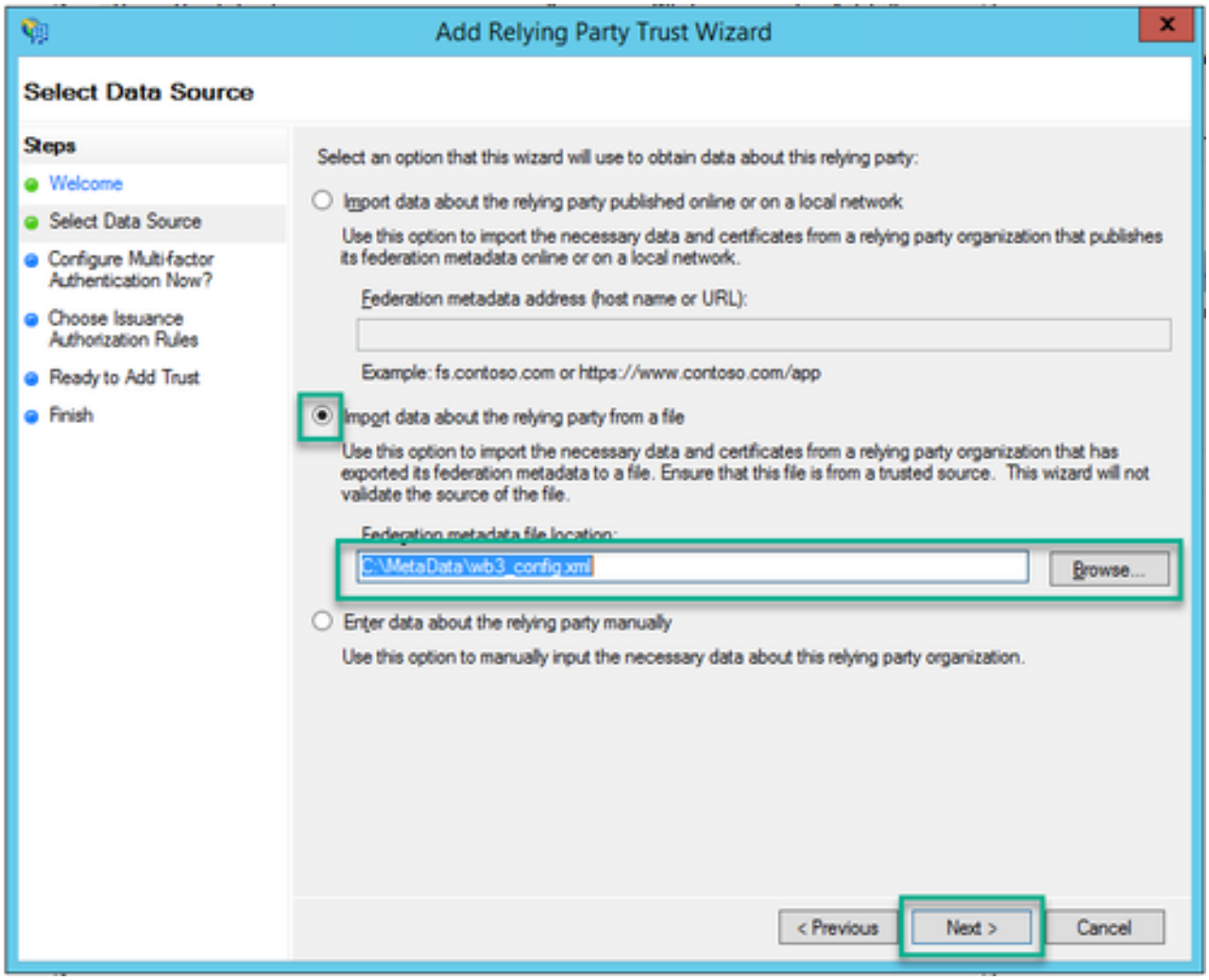
4.在ADFS管理控制台的右窗格中，选择添加信赖方信任..... 选项.



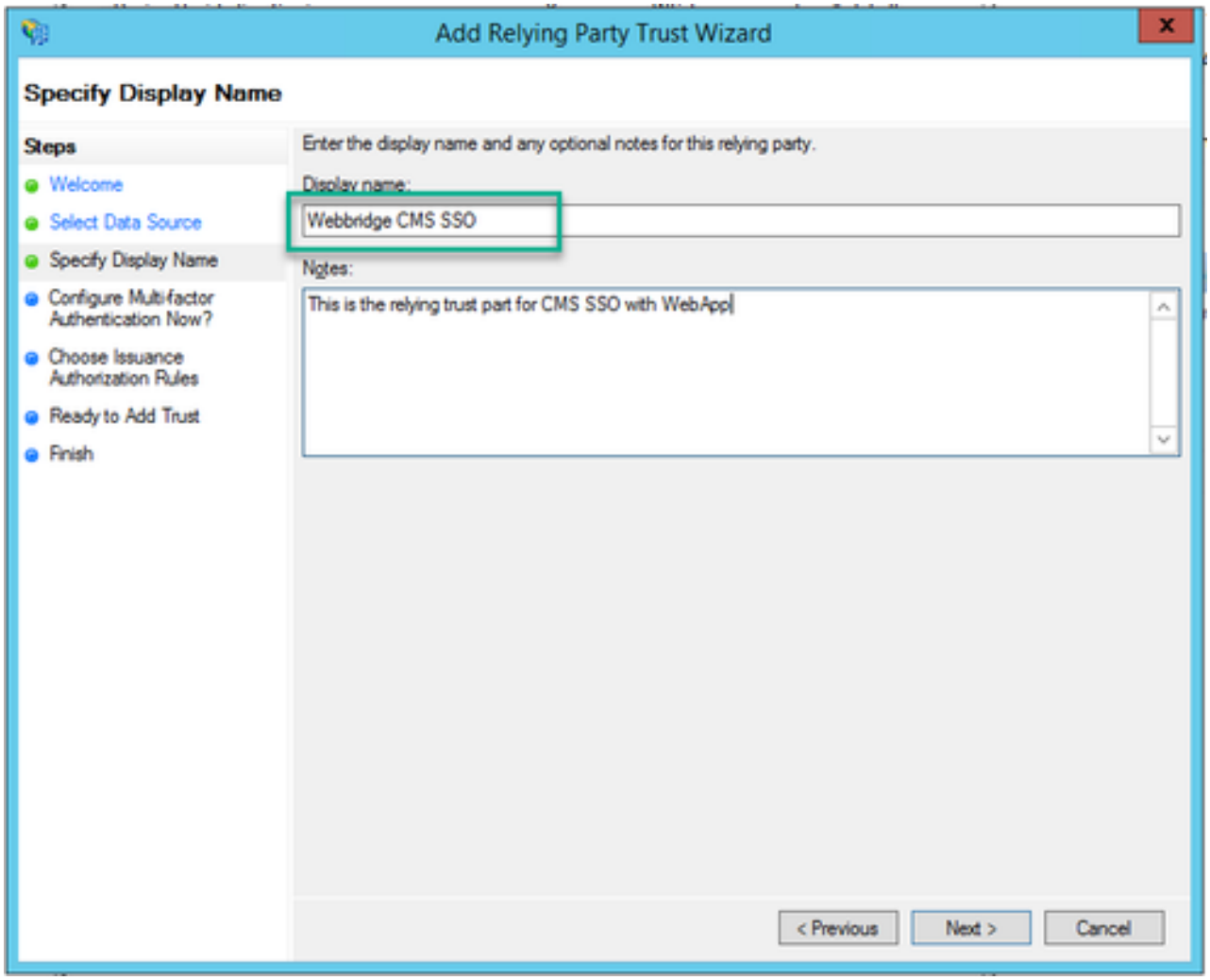
5.进行此选择后，将打开添加信赖方信任向导。选择开始选项。



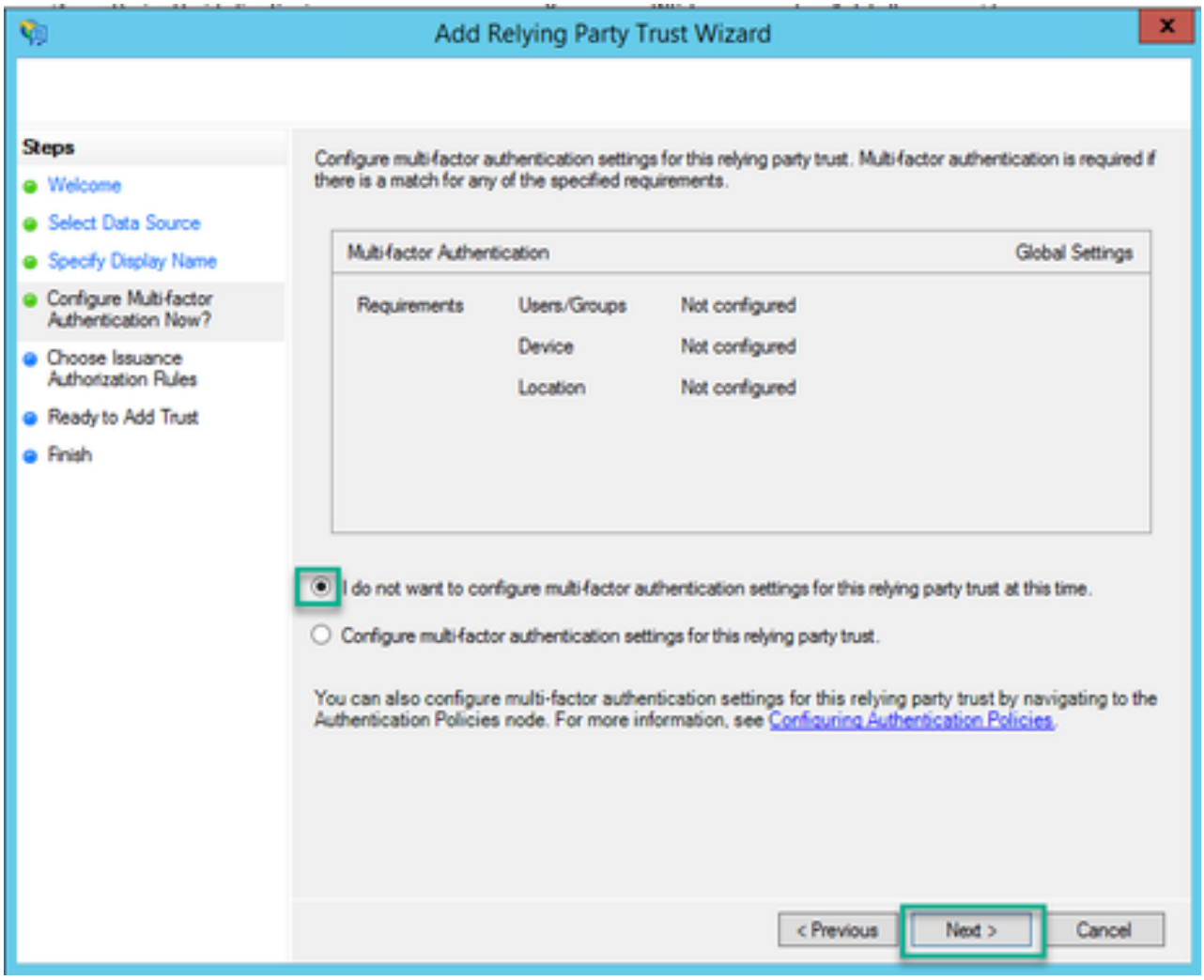
6.在选择数据源页上，选择从文件导入信赖方的数据的单选按钮，然后选择浏览，导航到Webbridge元数据文件的位置。



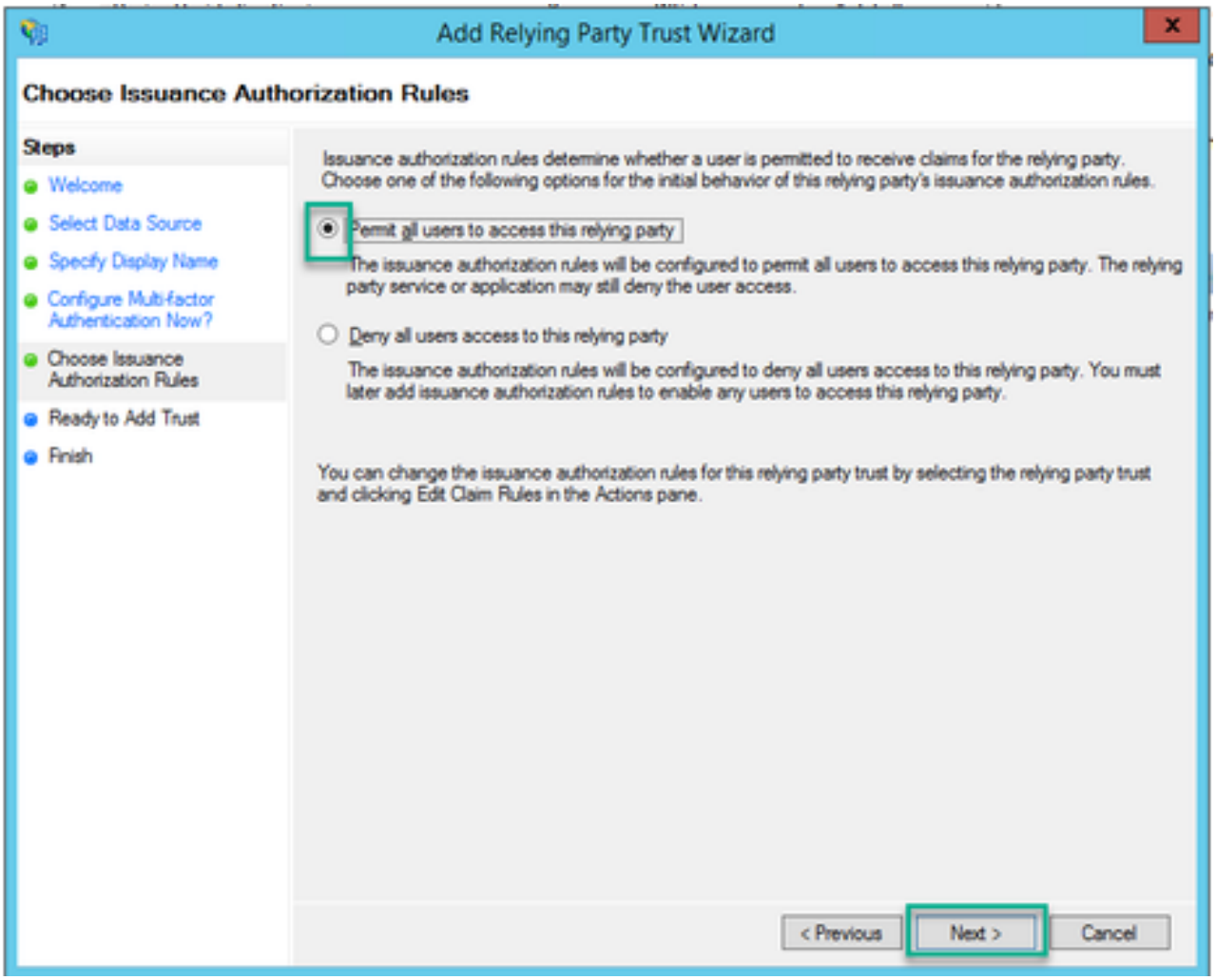
7.在指定显示名称页上，在ADFS中放入要为该实体显示的名称（显示名称不用于ADFS通信的服务器用途，只是提供信息）。



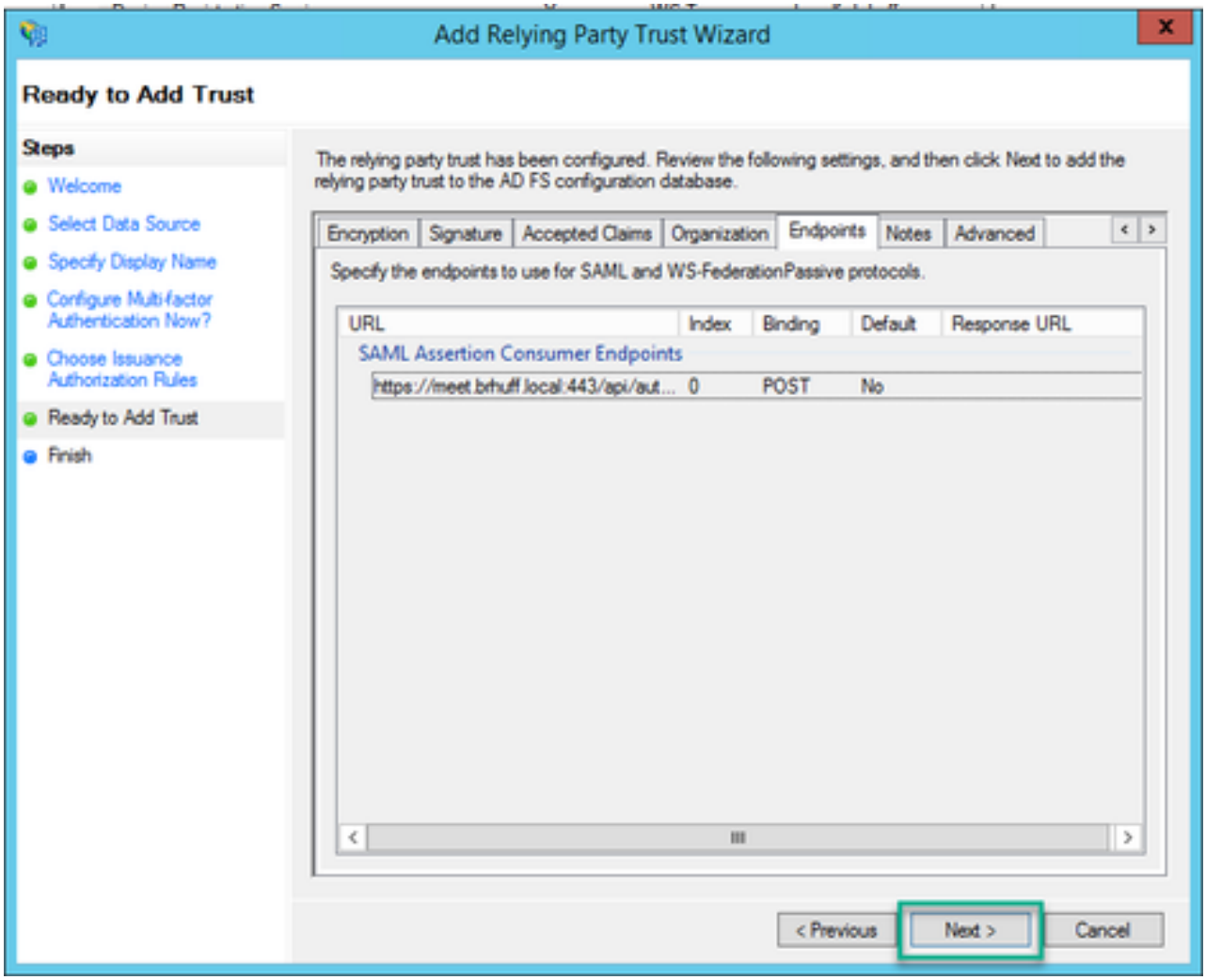
8.在Configure Multi-factor Authentication Now?页面，保留为默认值，然后选择下一步。



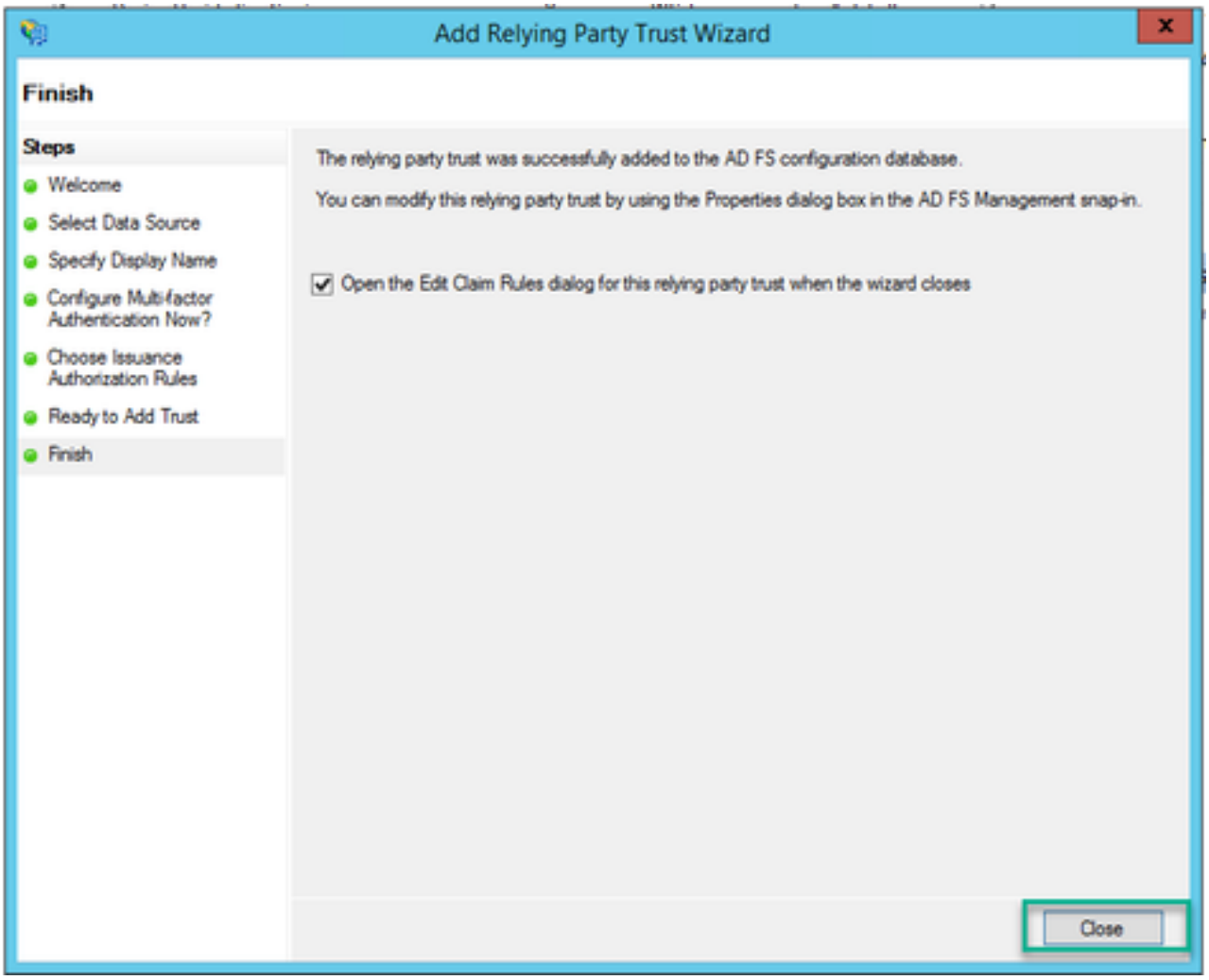
9.在Choose Issuance Authorization Rules页面上，保留为Permit all users to access this relikeparty所选项。



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



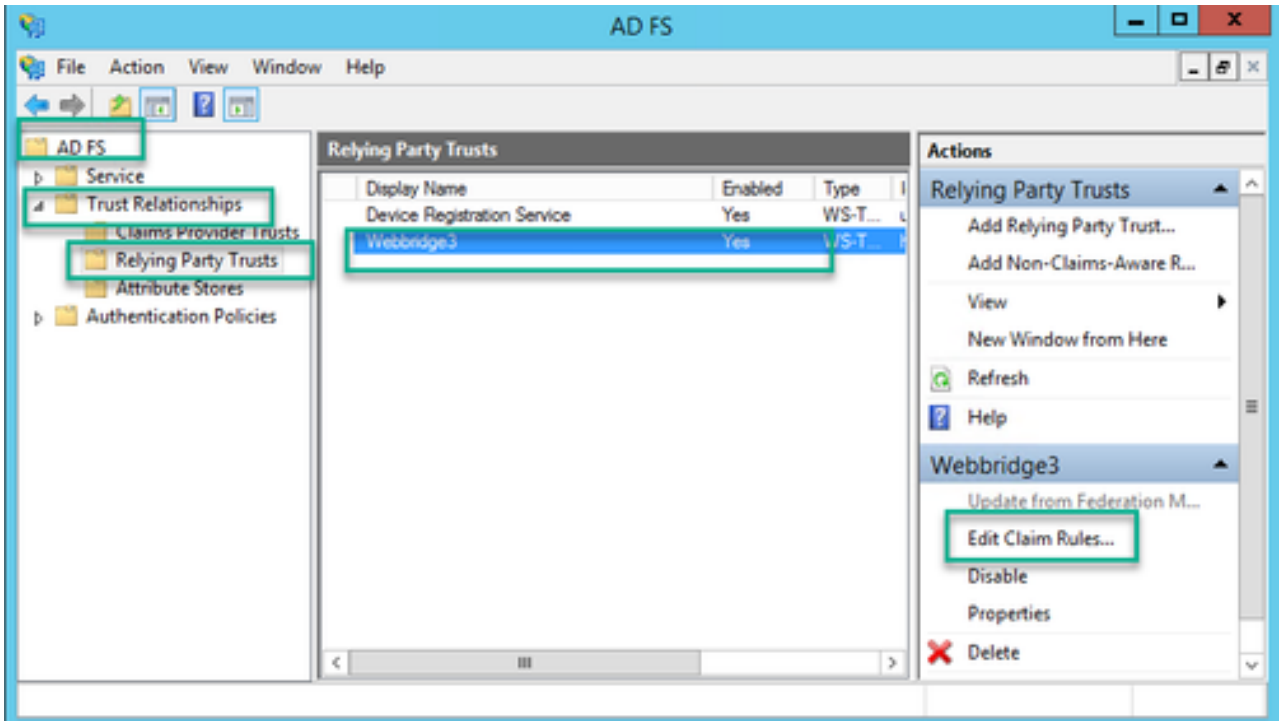
11.在完成页上，选择关闭选项以关闭向导并继续编辑声明规则。



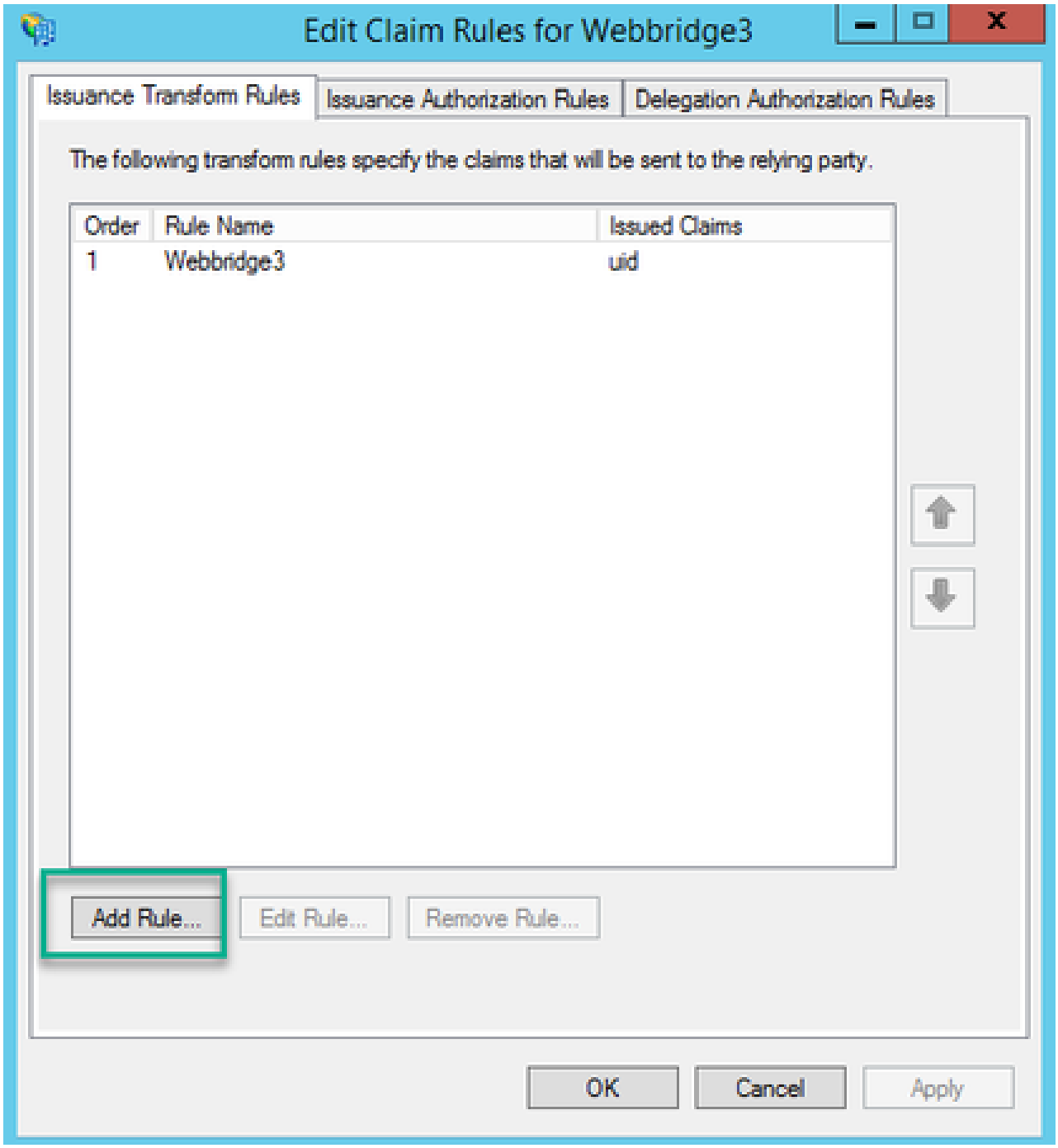
在IdP上为Webbridge服务创建声明规则

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属性与在SAML响应中提供给Webbridge的传出声明类型进行匹配。

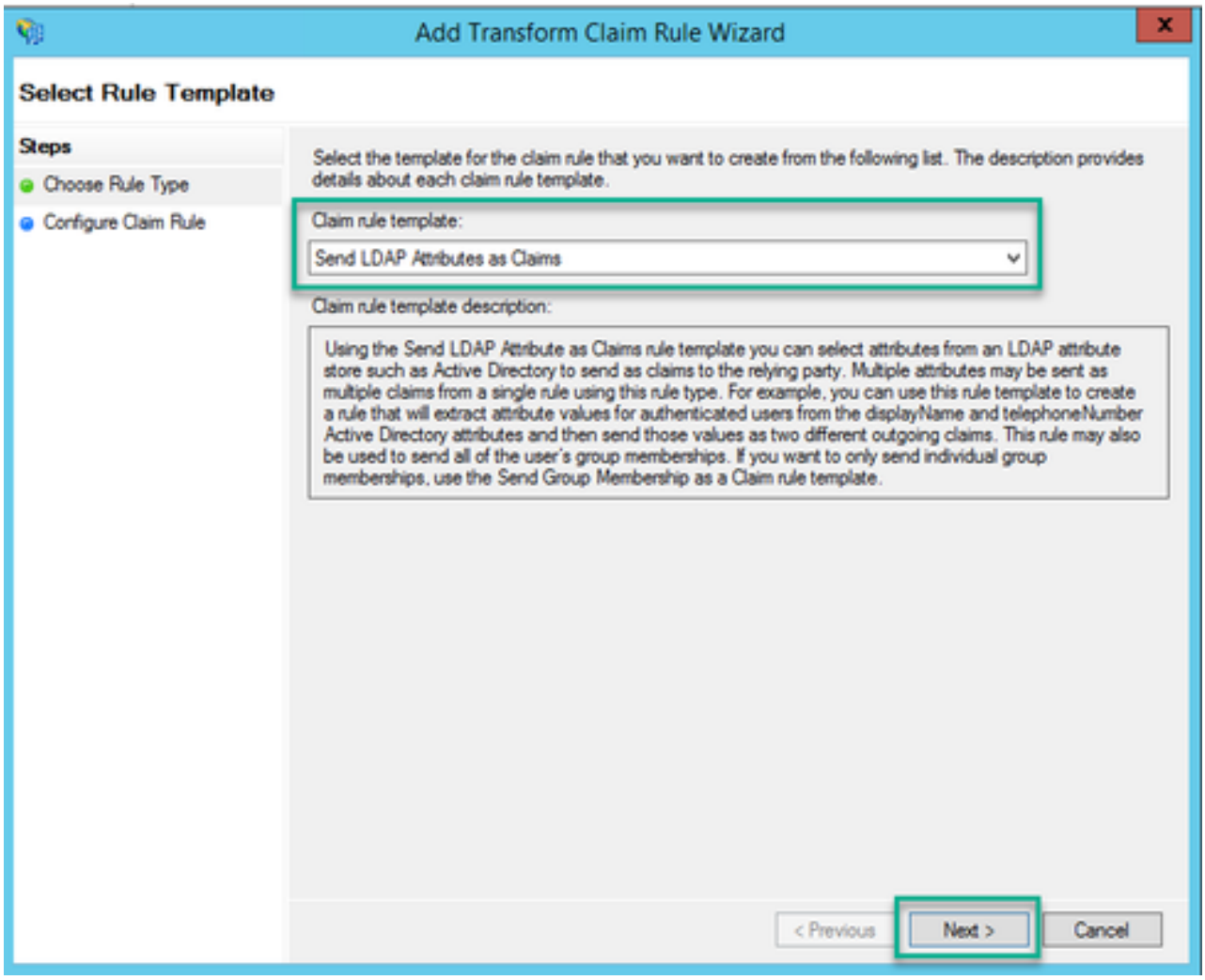
1.在ADFS管理控制台中，突出显示Webbridge的信赖方信任，然后在右侧窗格中选择编辑声明规则。



2.在“编辑<DisplayName>的索赔申请规则”页上，选择“添加规则……”.

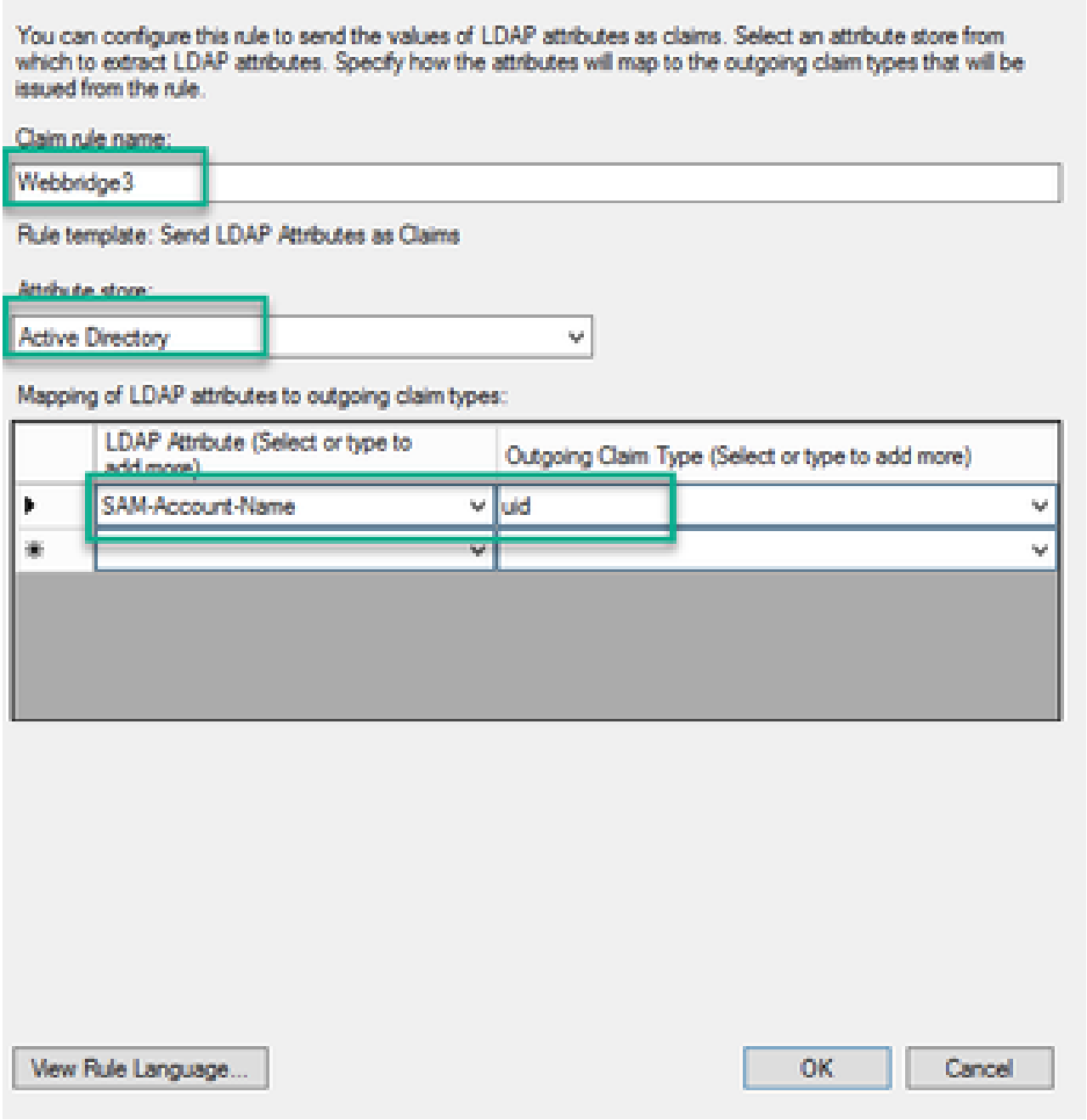


3.在Add Transform Claim Rule Wizard页上，为Claim规则模板选项选择Send LDAP Attributes as Claims，然后选择Next。



4.在配置声明规则页上，使用以下值配置信赖方信任的声明规则：

1. 领款申请规则名称=此名称必须是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=这必须与Callbridge API中的authenticationIdMapping匹配。（例如，$sAMAccountName$。）
4. 传出声明类型=此声明类型必须与Webbridge SSO config.json中的authenticationIdMapping相匹配。（例如uid。）



为Webbridge创建SSO存档ZIP文件：

此配置是Webbridge为验证受支持的域、身份验证映射等的SSO配置而引用的配置。此部分配置必须考虑以下规则：

- ZIP文件必须以sso_作为文件名的前缀(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(仍以sso_作为前缀)。

- 创建zip文件时，请务必突出显示并压缩文件内容，不要将所需的文件放入文件夹中并压缩该文件夹。

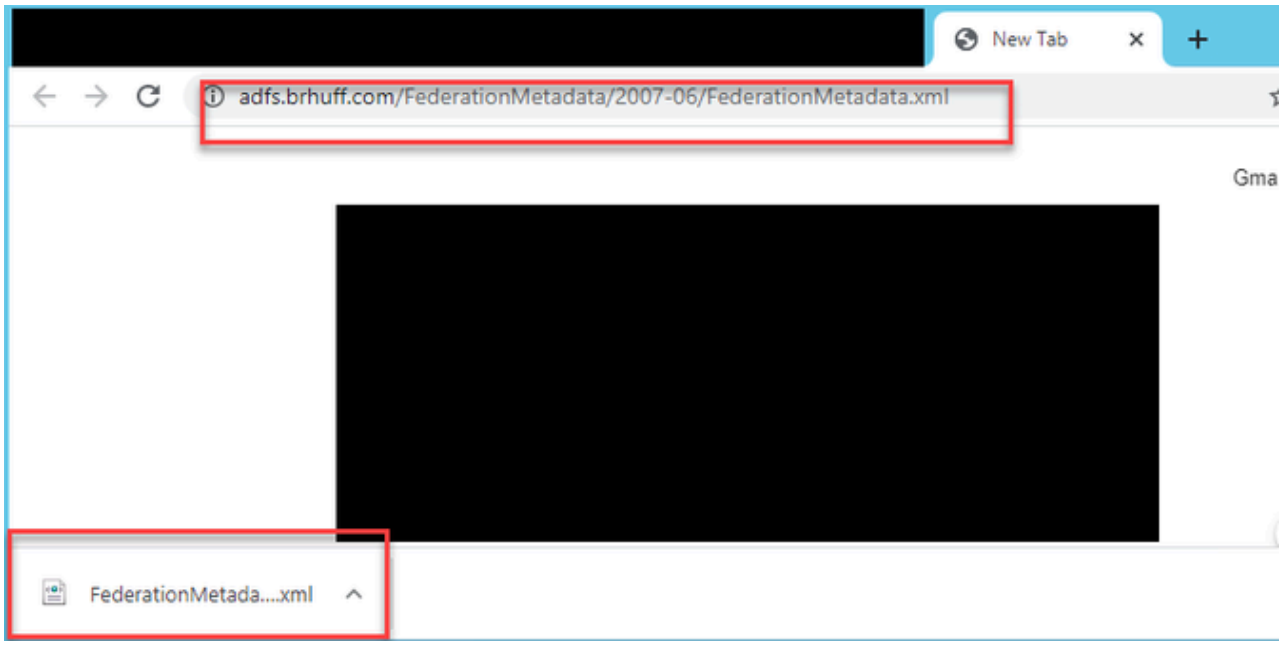
zip文件的内容由2到4个文件组成，具体取决于是否使用加密。

文件名	描述	是否必需？
idp_config.xml	这是可以由idP收集的MetaData文件。在ADFS中，可通过转到 https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml找到该地址。	YES
config.json	这是JSON文件，Webbridge使用该文件验证支持的域，即SSO的身份验证映射。	YES
sso_sign.key	这是在识别提供程序上配置的公共签名密钥的私钥。仅保护已签名数据所必需的	否
sso_encrypt.key	这是在识别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

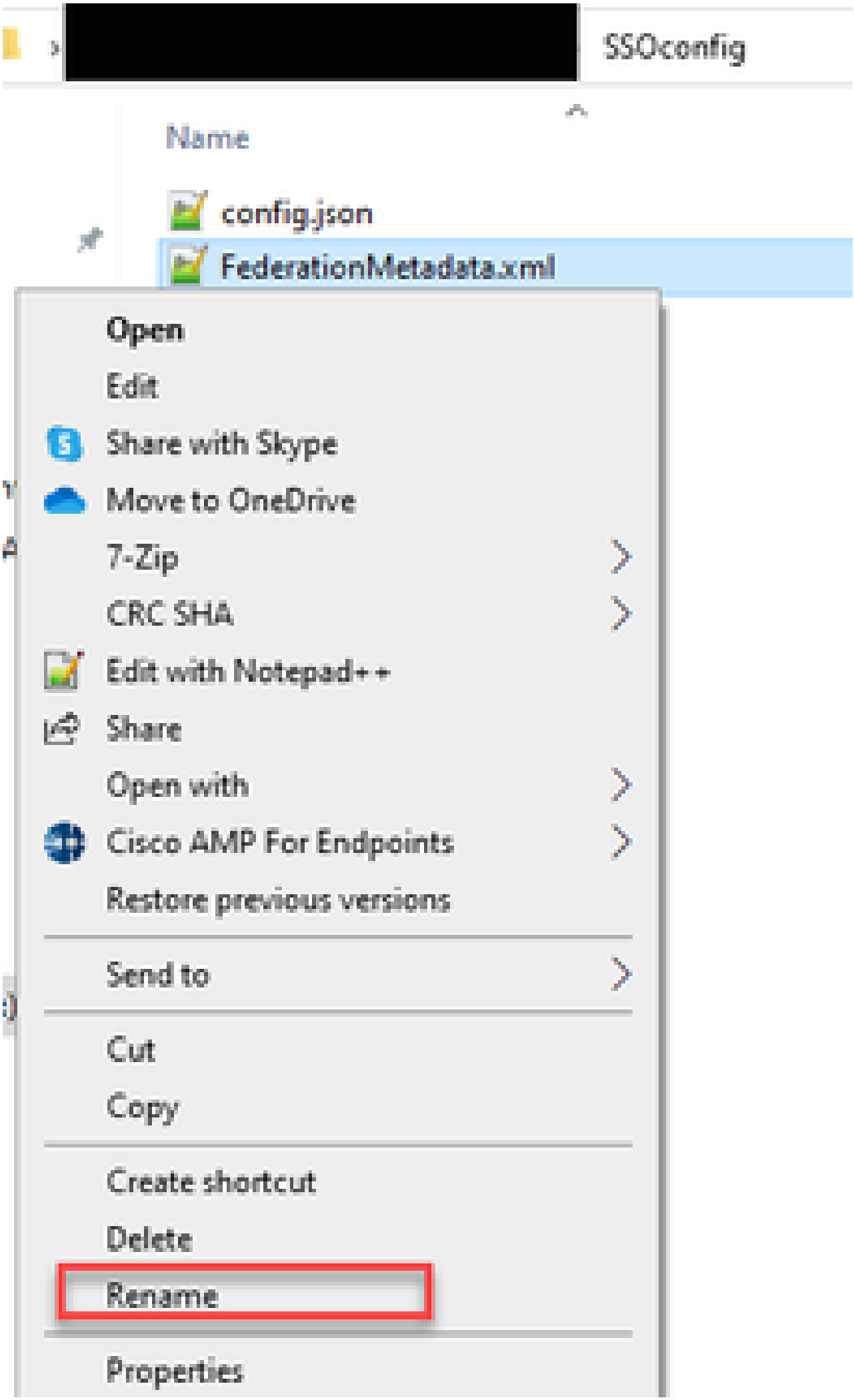
获取并配置idp_config.xml

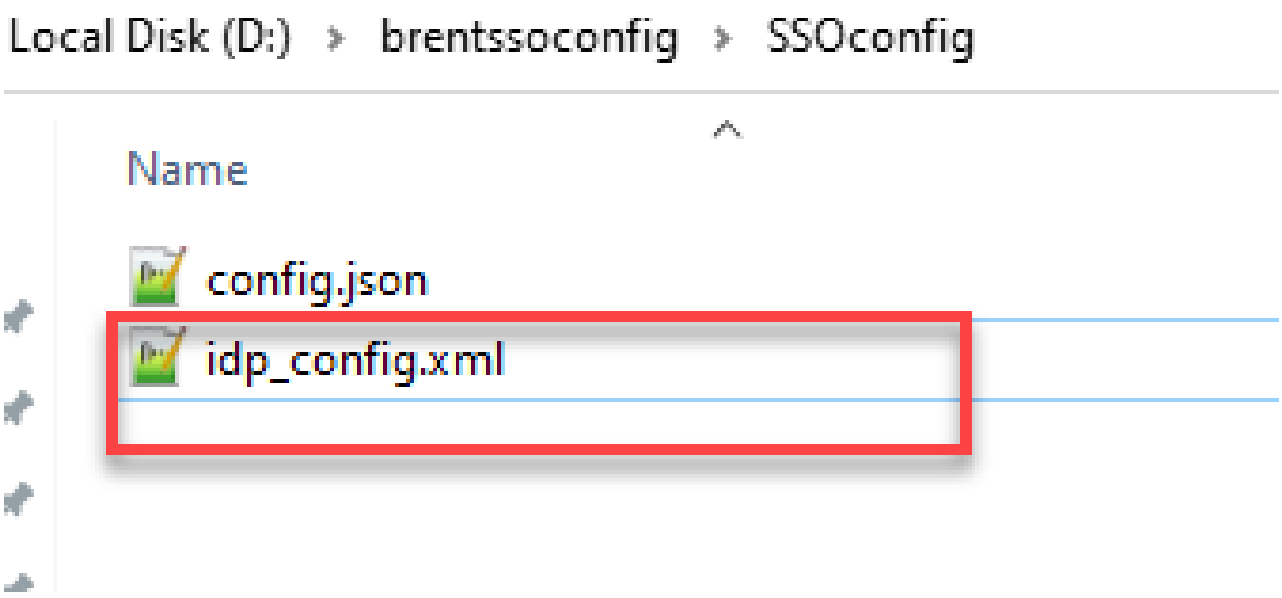
1. 在ADFS服务器（或有权访问ADFS的位置）上，打开Web浏览器。

2.在Web浏览器中，输入URL:https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml（如果您在ADFS服务器上本地，也可以使用localhost而非FQDN）。此操作将下载文件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。

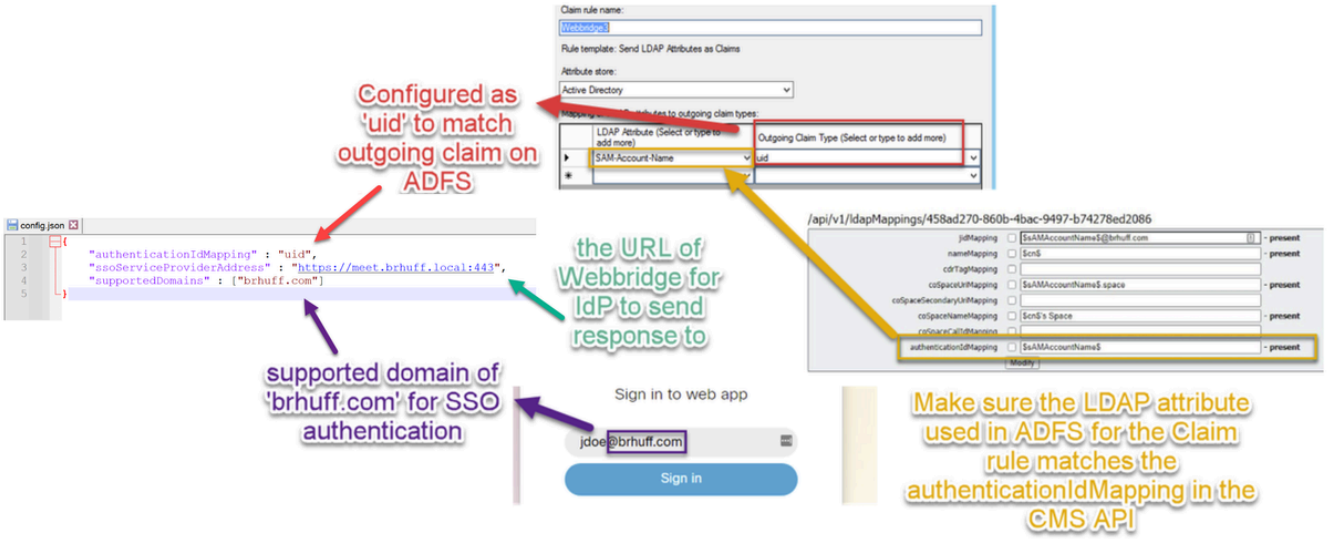

[redacted]
SSOconfig
Name
config.json
FederationMetadata.xml
Open
Edit
Share with Skype
Move to OneDrive
7-Zip
CRC SHA
Edit with Notepad++
Share
Open with
Cisco AMP For Endpoints
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties



创建包含内容的config.json文件

config.json包含这3个属性，且它们必须包含在方括号内{ }:

1. supportedDomains — 这是根据IdP检查SSO身份验证的域列表。多个域可以用逗号分隔。
2. authenticationIdMapping — 这是作为传出声明规则的一部分从ADFS/IdP传回的参数。此值必须与IdP上传出声明类型的名称值匹配。领款申请规则
3. ssoServiceProviderAddress — 这是标识提供程序向其发送SAML响应的FQDN URL。这必须是Webbridge FQDN。

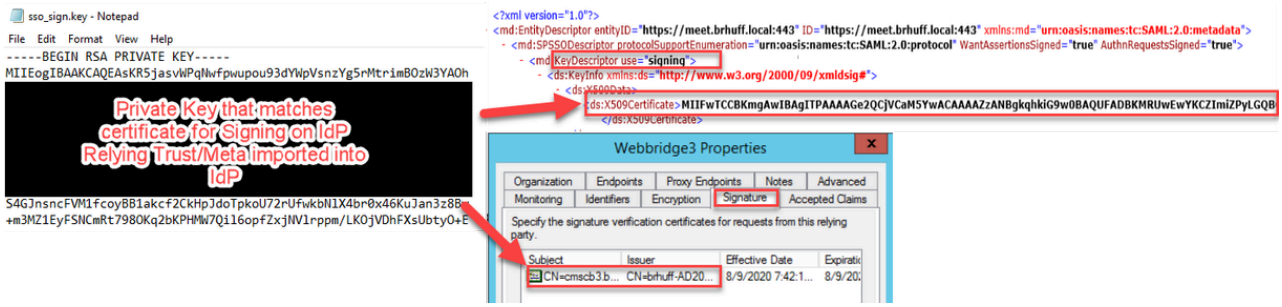


设置sso_sign.key（可选）

此文件必须包含用于在Webbridge元数据中签名的证书的私钥，Webbridge元数据已导入到IdP。通过在<KeyDescriptor use=signing>部分下使用证书信息填充X509Certificate，可在ADFS中导入Webbridge元数据期间设置用于签名的证书。也可以在Webbridge信赖信任方的ADFS上，在属性>签名下查看（和导入）它。

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。插入到sso_sign.key中的私钥是与cmscb3.brhuff.local证书匹配的私钥。

这是可选配置，仅在要加密SAML响应时才需要。

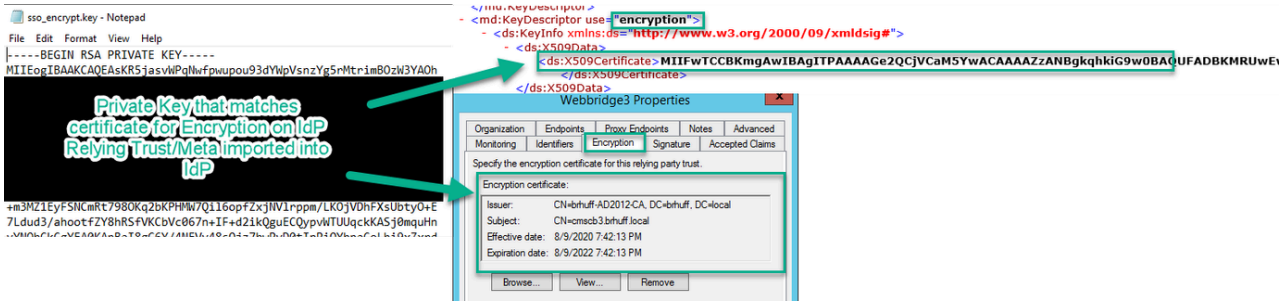


设置sso_encrypt.key（可选）

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。通过在<KeyDescriptor use=encryption>部分下使用证书信息填充X509Certificate，可在ADFS中Webbridge元数据的导入过程中设置用于加密的证书。也可以在Webbridge Reliing Trust Party中的ADFS上Properties > Encryption下查看（和导入）。

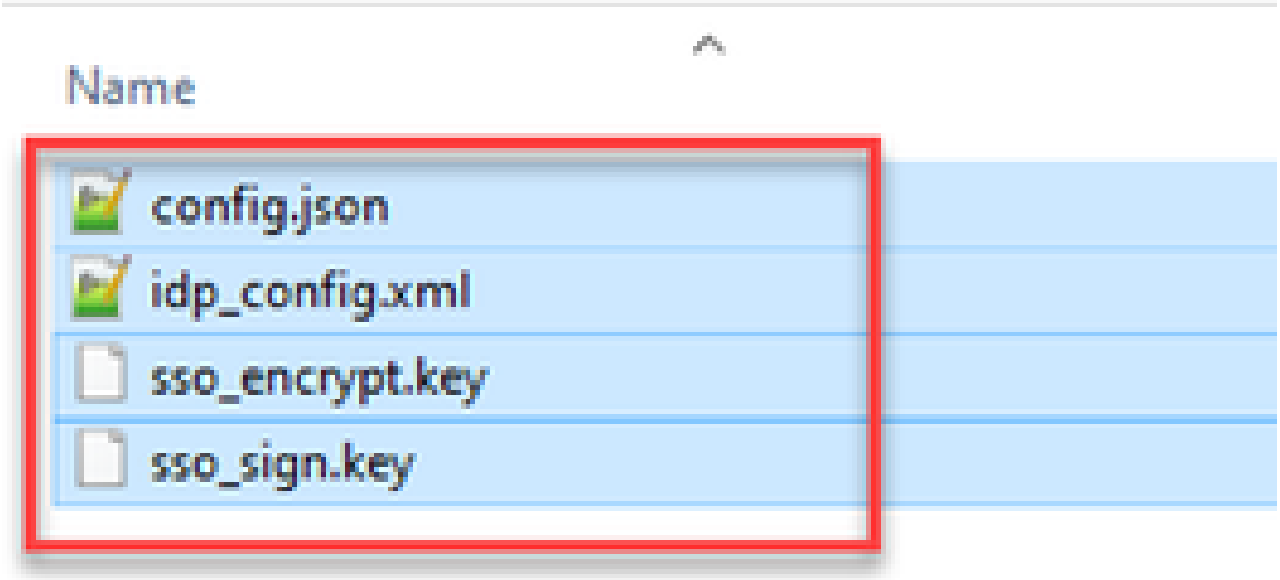
在下一个示例中，您可以看到callbridge证书(CN=cmscb3.brhuff.local)，该证书在导入到ADFS之前已添加到Webbridge元数据。插入到“sso_encrypt.key”中的私钥是与cmscb3.brhuff.local证书匹配的密钥。

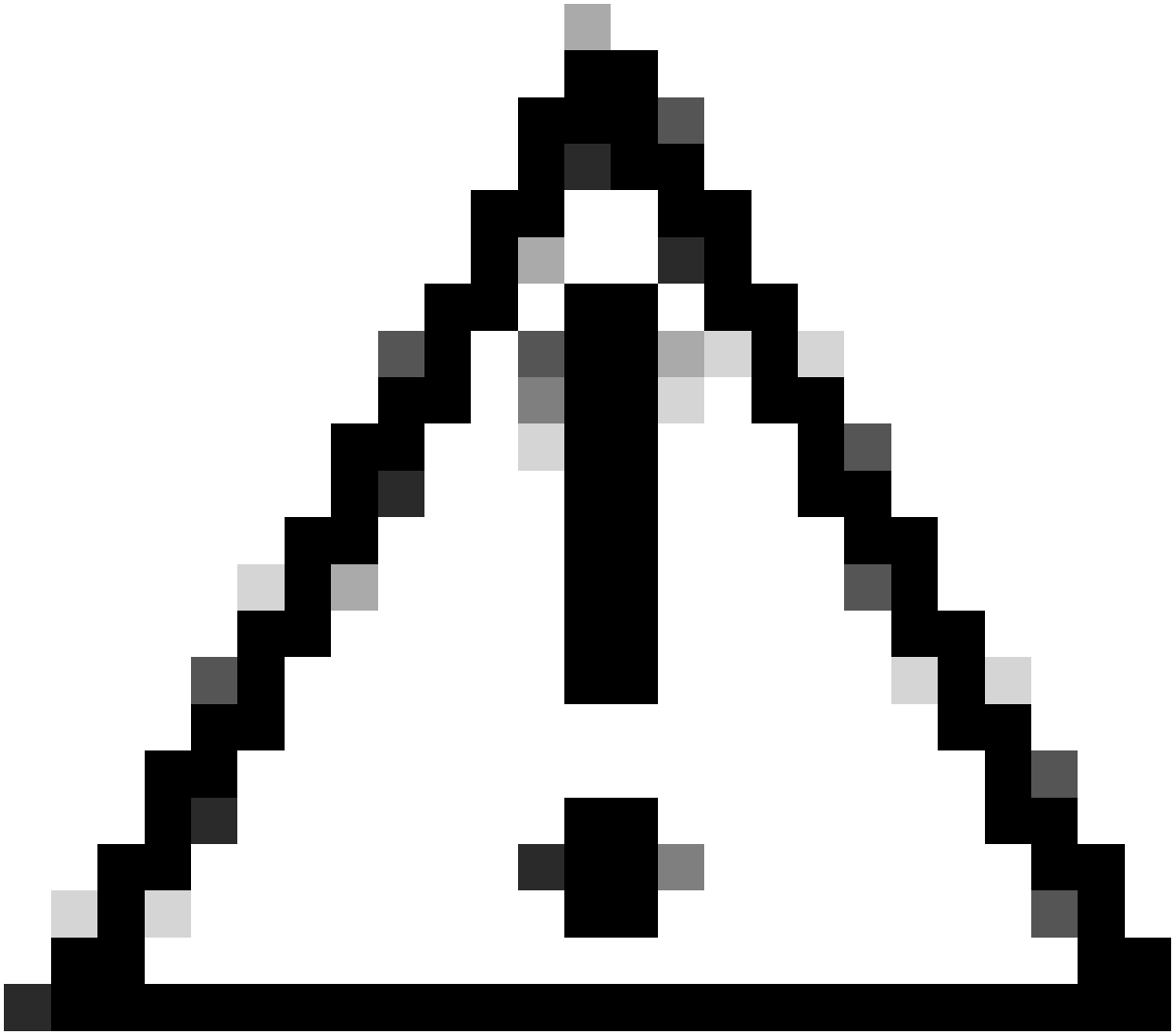
这是可选配置，只有在您打算加密SAML响应时才需要此配置。



创建SSO ZIP文件

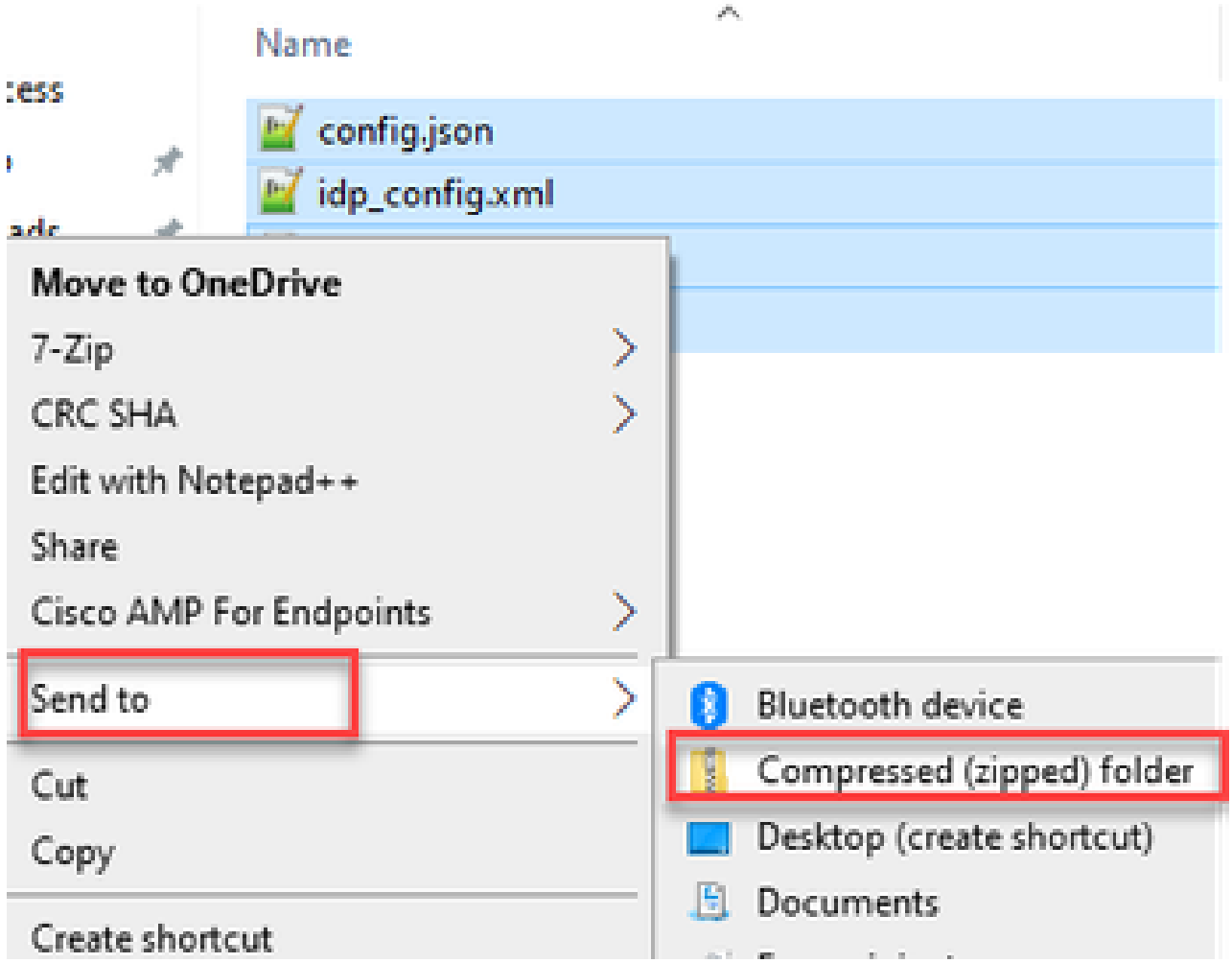
1. 突出显示要用于SSO配置文件的所有文件。



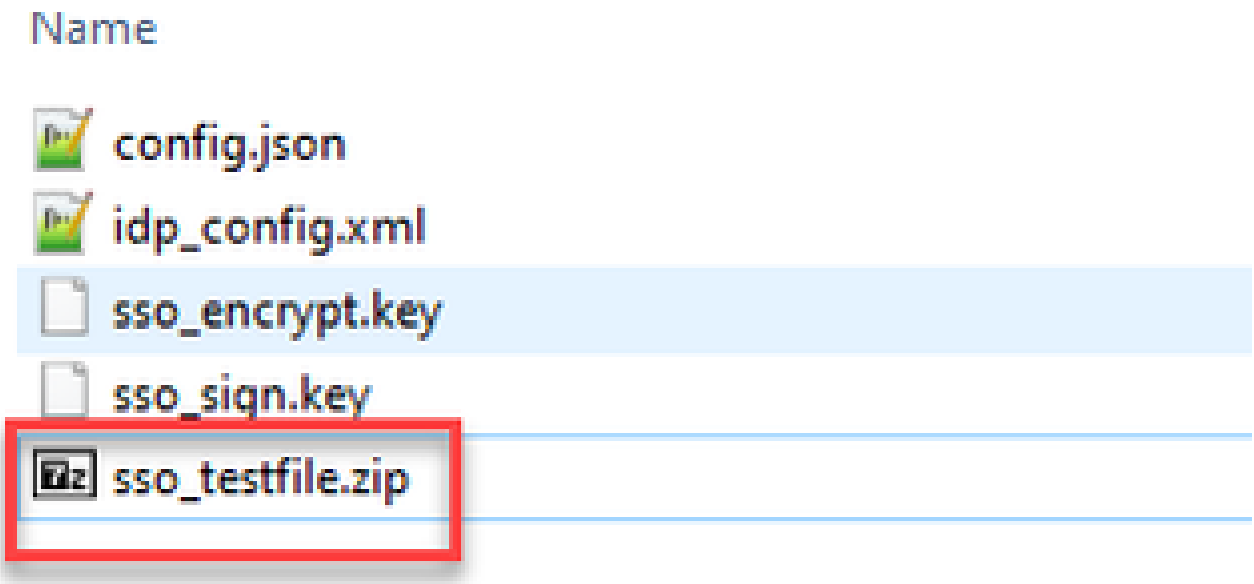


警告：请勿压缩包含文件的文件夹，因为这会导致SSO无法工作。

2.右键单击突出显示的文件，然后选择发送到>压缩(zipped)文件夹。



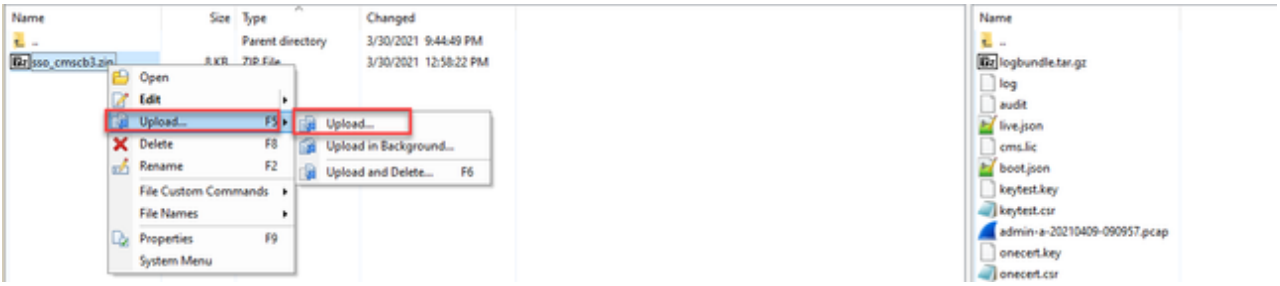
3.压缩文件后，将其重命名为带有sso_prefix的所需名称：



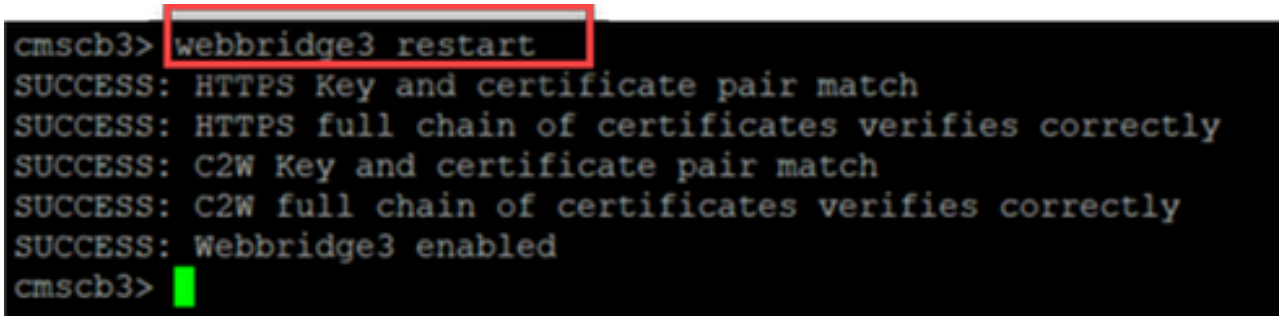
将SSO Zip文件上传到Webbridge

打开SFTP/SCP客户端（在本例中正在使用WinSCP），并连接到托管Webbridge3的服务器。

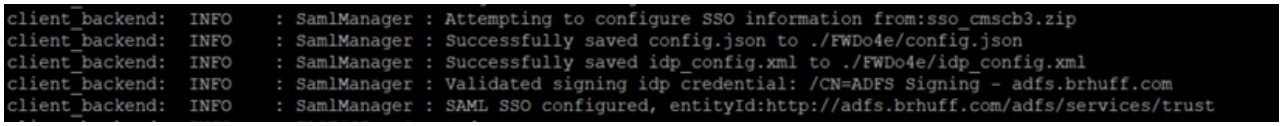
1.在左窗格中，导航到SSO Zip文件所在的位置，然后右键点击选择上传或拖放文件。



2.将文件完全上传到Webbridge3服务器后，打开SSH会话并运行命令webbridge3 restart。



3.在系统日志中，以下消息指示SSO启用成功：

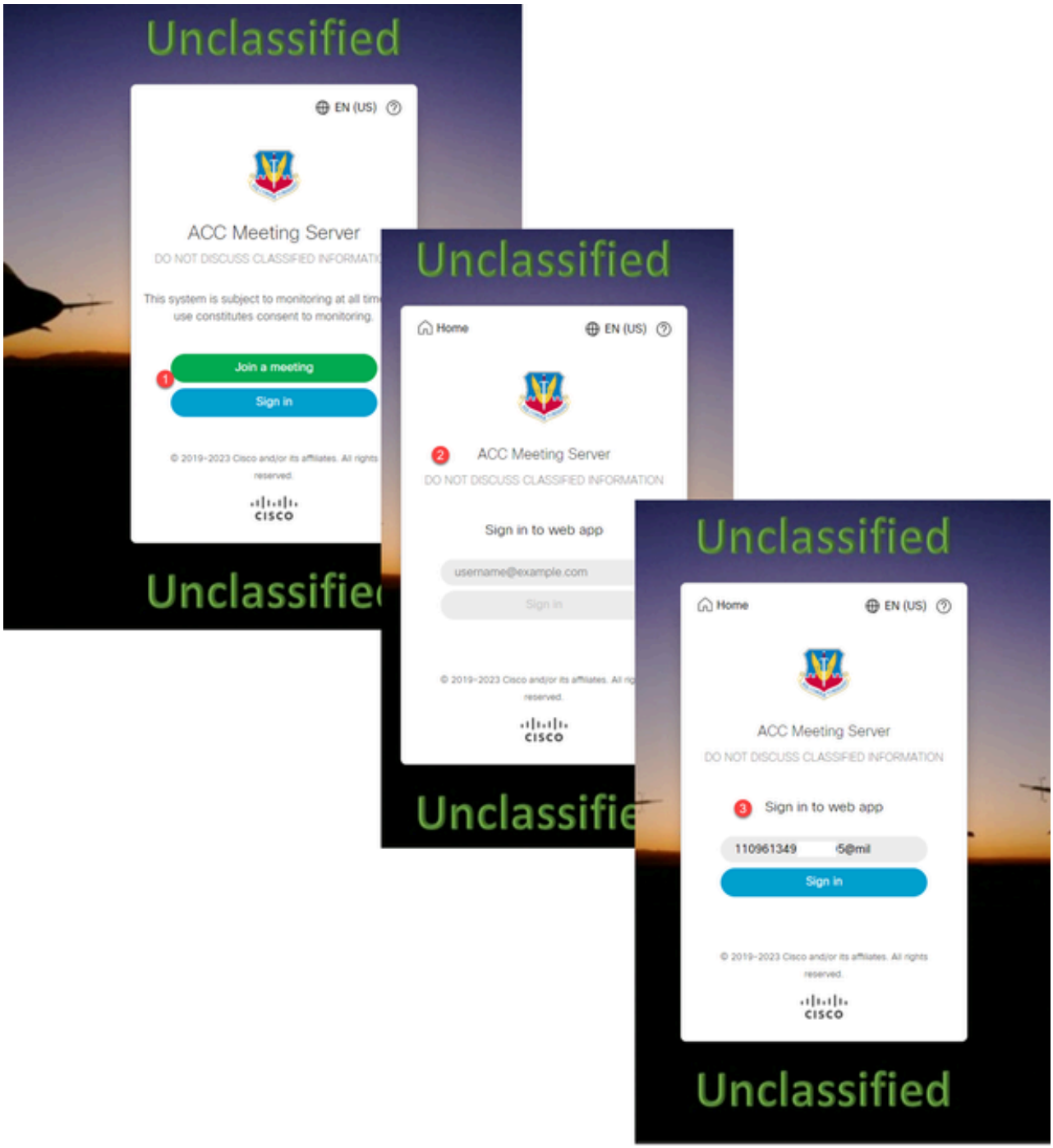


通用访问卡(CAC)

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卡用户的整个登录过程：

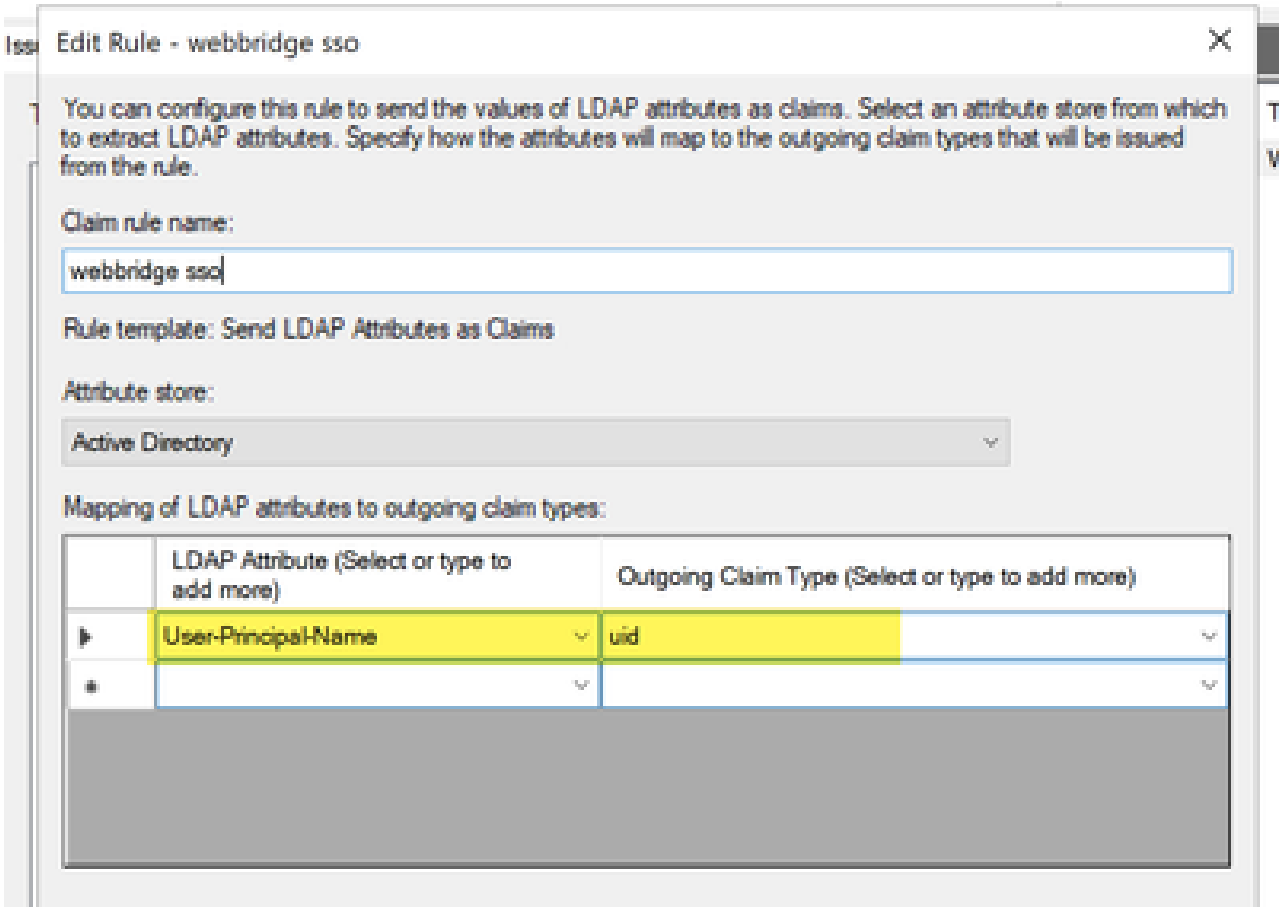
1. 打开PC，并粘住CAC卡
2. 登录（有时选择证书），然后输入Pin
3. 打开浏览器
4. 导航到加入URL并查看加入会议或登录选项
5. 登录：输入配置为jidMapping的用户名，Active Directory要求通过CAC登录进行该用户名
6. 点击登录
7. ADFS页面会短暂显示并自动填充
8. 用户此时已登录



在Ldapmapping中配置jidMapping（这是用户登录名称），与ADFS用于CAC卡的配置相同。$userPrincipalName$例如（区分大小写）

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

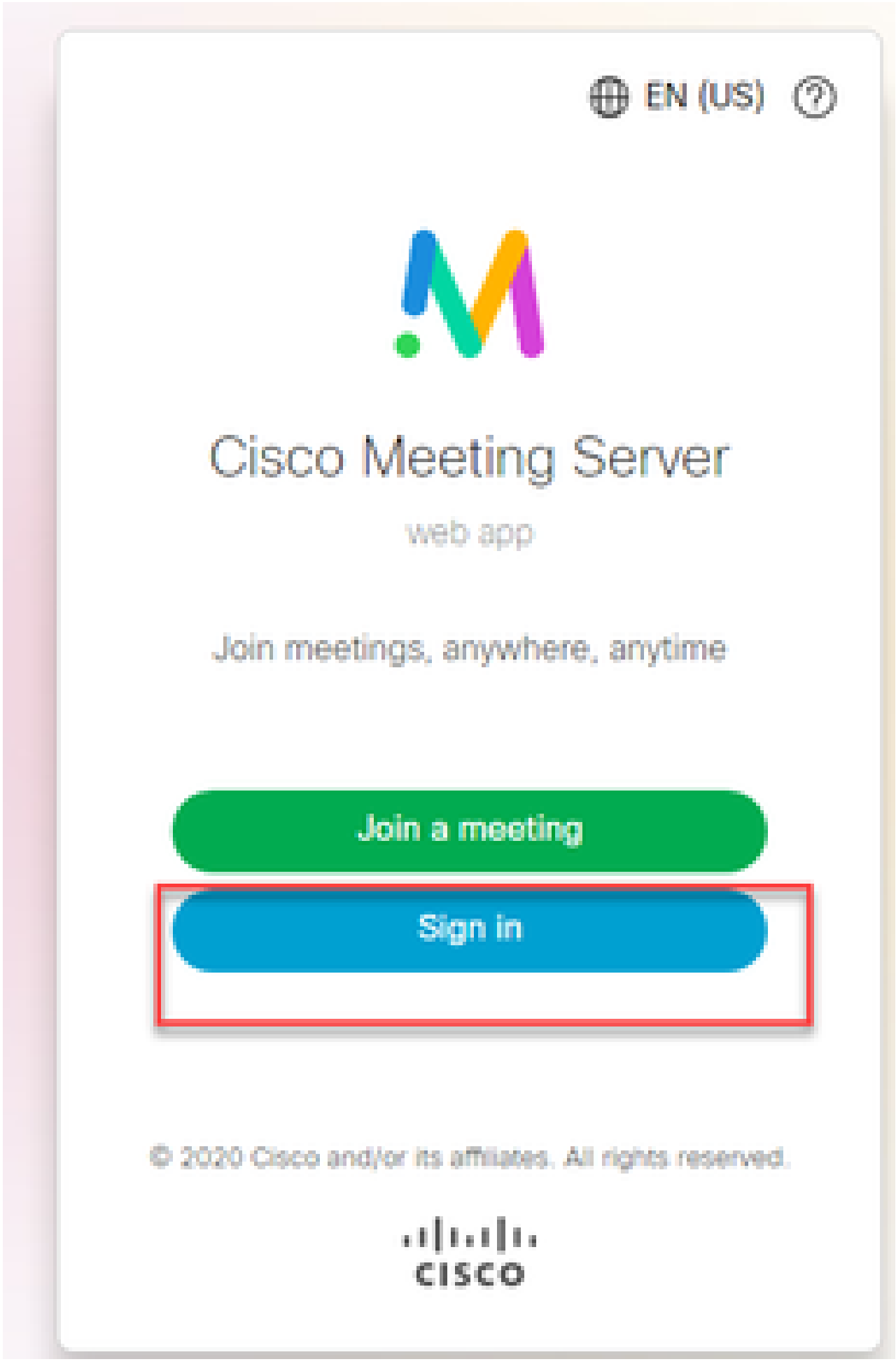
此处，声明规则显示它将将$userPrincipalName$作为UID发送回CMS。



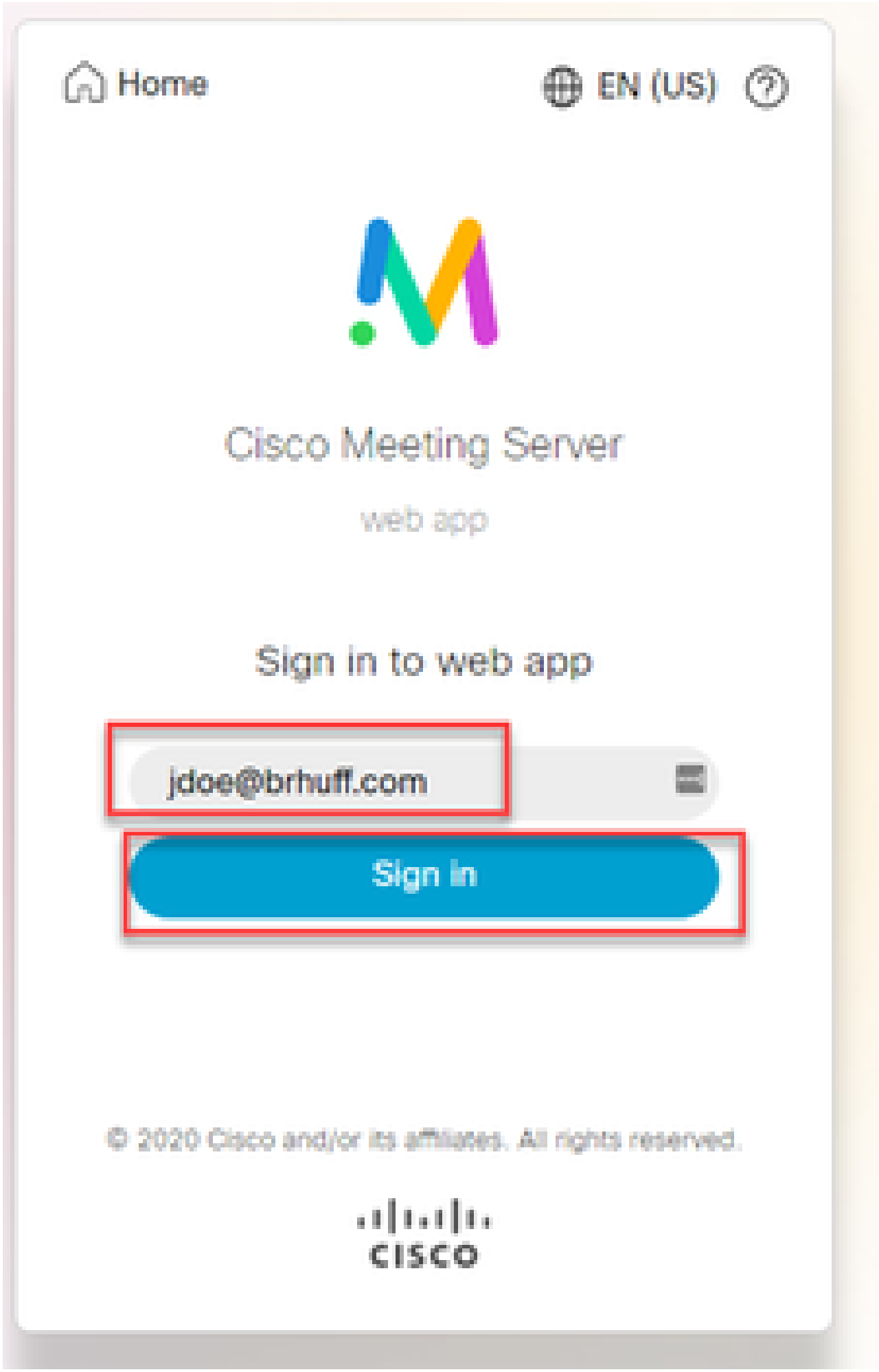
测试通过WebApp登录的SSO

配置了SSO后，您可以测试服务器：

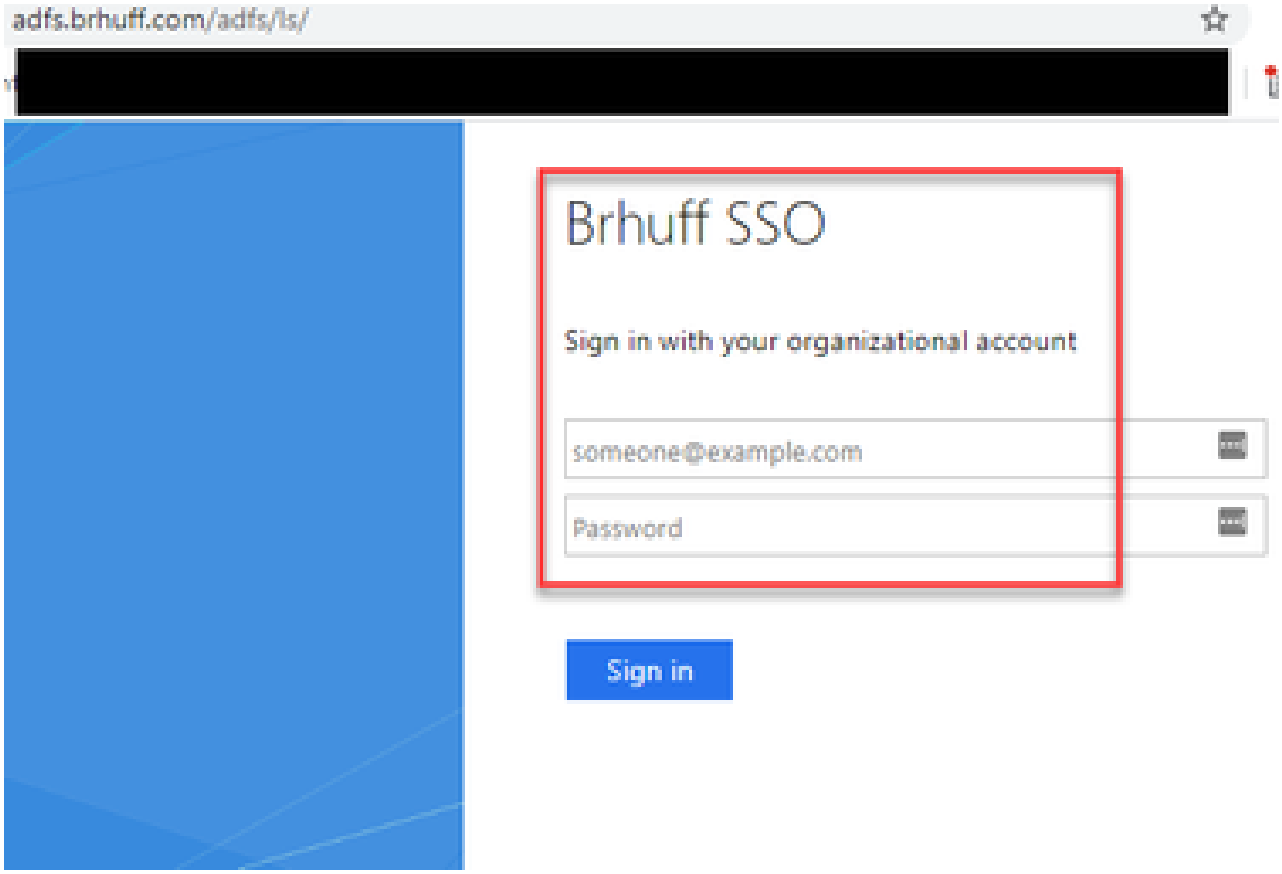
1. 导航到Web应用的Webbridge URL，然后选择登录按钮。


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

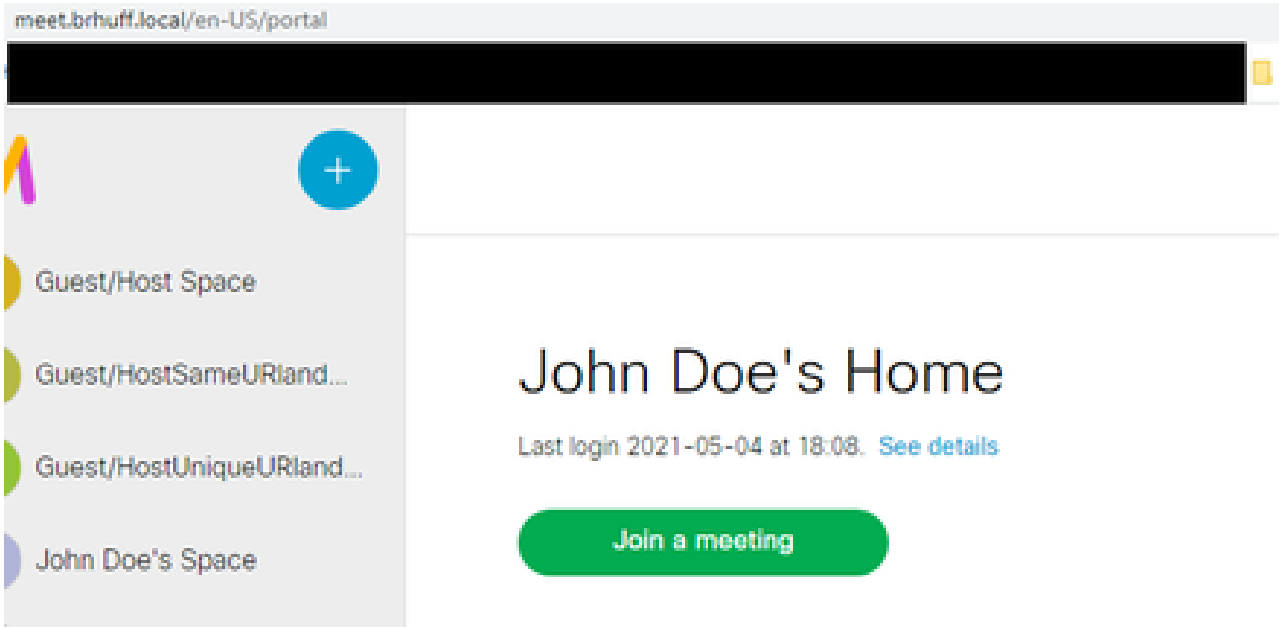
2.系统向用户显示输入其用户名的选项（请注意此页面上没有密码选项）。


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），用户必须在此页面输入其凭证以向IdP进行身份验证。



4.用户使用IdP输入并验证凭证后，使用令牌重定向以访问Web App主页：



故障排除

基本故障排除

对于任何SSO问题的基本故障排除：

1. 确保正确配置用于在IdP中作为Reliking Trust导入的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提供并压缩到Webbridge3中的元数据是IdP中的最新元数据，就像服务器主机名、证书等有任何更改一样，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。如果可能，尝试在没有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运行。
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，以与SAMLResponse匹配。

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，将?trace=true置于URL末尾，以便在CMS系统日志上启用详细日志记录。（例如：https://join.example.com/en-US/home?trace=true)。
2. 在Webbridge3服务器上运行syslog follow，以在测试期间捕获实时数据，或使用附加到URL的trace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进程发生故障会导致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以确认出现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，原因是：urn:oasis:names:tc:SAML:2.0:status:Responder

此错误表示根据之前的文档，此故障是由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SAMLR响应期间，Webbridge可以在日志中显示此错误消息，并通过SSO登录失败：

> client_backend:信息：SamlManager:[57dff9e3-862e-4002-b4fa-683e4aa6922c]未能获取authenticationId

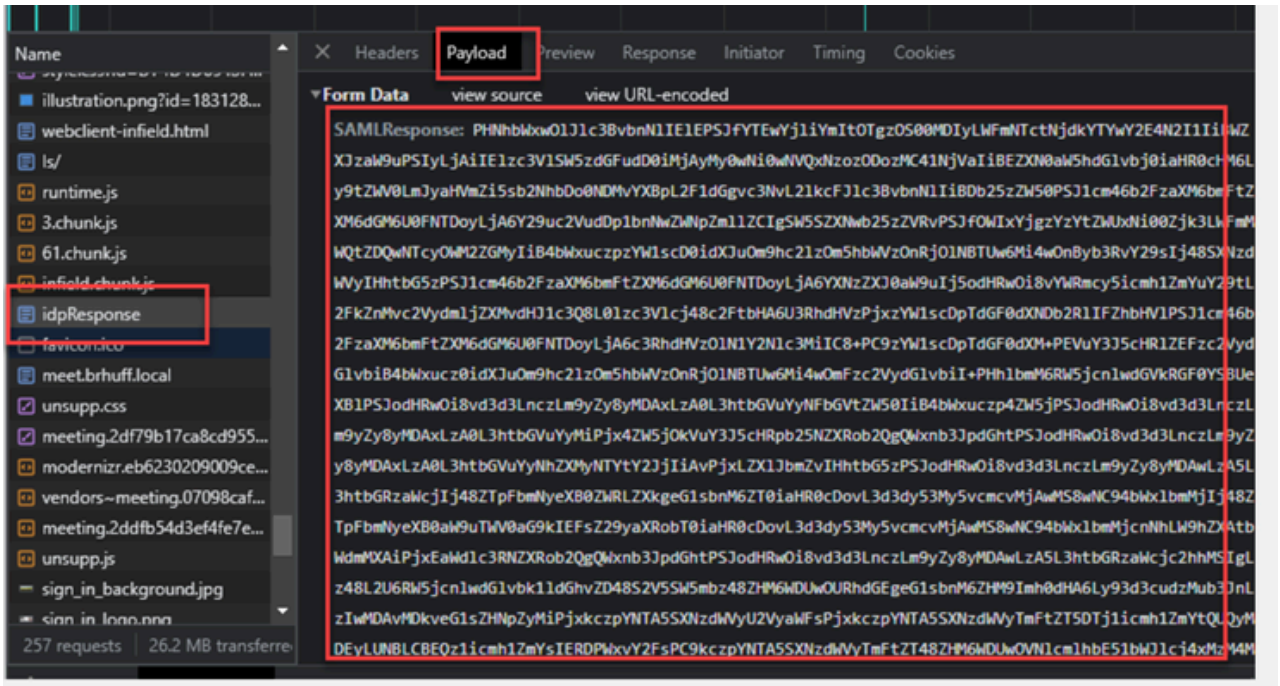
这表示在审核身份验证交换期间从IdP传回的SAMLResponse数据时，Webbridge3在响应中找不到有效的匹配属性，而其authenticationId的config.json是匹配属性。

如果通信未使用签名和加密私钥进行加密，则可以通过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，则可以从IdP端请求已解密的SAML响应。

记录网络日志时，确保选中“保留日志”复选框，以便在页面更改时不会覆盖日志。



在developer tools network logging输出（也称为HAR数据）中，在name列下查找idpResponse，并选择Payload以查看SAML响应。 如前所述，可以使用base64解码器对此进行解码。



收到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：

```
<属性语句>
<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部分中设置的值进行比较。

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，从而导致找不到匹配的authenticationId:

身份验证Id映射：http://example.com/claims/NameID

要解决此问题，可以尝试两种方法：

1. 可以更新IdP传出声明规则，使其具有与Webbridge3上config.json的authenticationIdMapping中配置的完全匹配的声明。(在http://example.com/claims/NameID的IdP上添加了领款申请规则)
   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。(即要更新的“authenticationIdMapping”以匹配属性名称之一，属性名称可以是“uid”、“<URL>/NameID”或“<URL>/CommonName”。 只要它匹配（完全匹配）通过时在Callbridge API上配置的预期值)

在验证中未传递/匹配断言

有时，在从IdP交换SAMLResponse期间，Webbridge会显示此错误，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:未通过验证的断言
client_backend:信息：SamlManager:跳过不在允许受众中的断言

此错误表明当从IdP查看SAMLR响应时，Webbridge未能找到任何匹配断言，因此跳过不匹配失败，最终导致失败的SSO登录。

为了找到此问题，最好从IdP查看SAMLR响应。如果通信未使用签名和加密私钥进行加密，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，则可以从IdP端请求已解密的SAML响应。

在查看SAMLResponse数据时，请查看响应的<AudienceRestriction>部分，您可以找到此响应受限制的所有受众：

<Conditions NotBefore=2021-03-30T19:35:37.071Z NotOnOrAfter=2021-03-30T19:36:37.071Z>
<受众限制>
<Audience>https://cisco.example.com</Audience>
</AudienceRestriction>
</Condition>

使用<Audience>部分(https://cisco.example.com))中的值，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。在本例中，您可以看到失败的原因是受众与配置中的服务提供商地址不匹配，因为它附加了:443:

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

这要求两者之间精确匹配，以免导致此类故障。在本例中。解决方法可以是以下两种方法之一：

1.可以从config.json的ssoServiceProviderAddress部分的地址中删除:443，以便它与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，则必须在ADFS上将其重新作为信赖信任方导入。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。)

另外，请注意条件NotBefore和NotONOrAfter:<条件NotBefore=2021-03-30T19:35:37.071Z NotOnOrAfter=2021-03-30T19:36:37.071Z>

如果服务器时间不正确，可能会导致时间超出条件中定义的有效期。您将要通过CLI使用命令ntp server list检查NTP服务器，以查看配置的NTP服务器，并使用ntp status检查配置的NTP服务器的状态。使用命令date验证服务器时间。

提示：如果使用本地/内部NTP服务器，请尝试配置公共NTP服务器，例如time.google.com（请确保之前配置公共DNS服务器）。

在Web应用上登录失败：

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

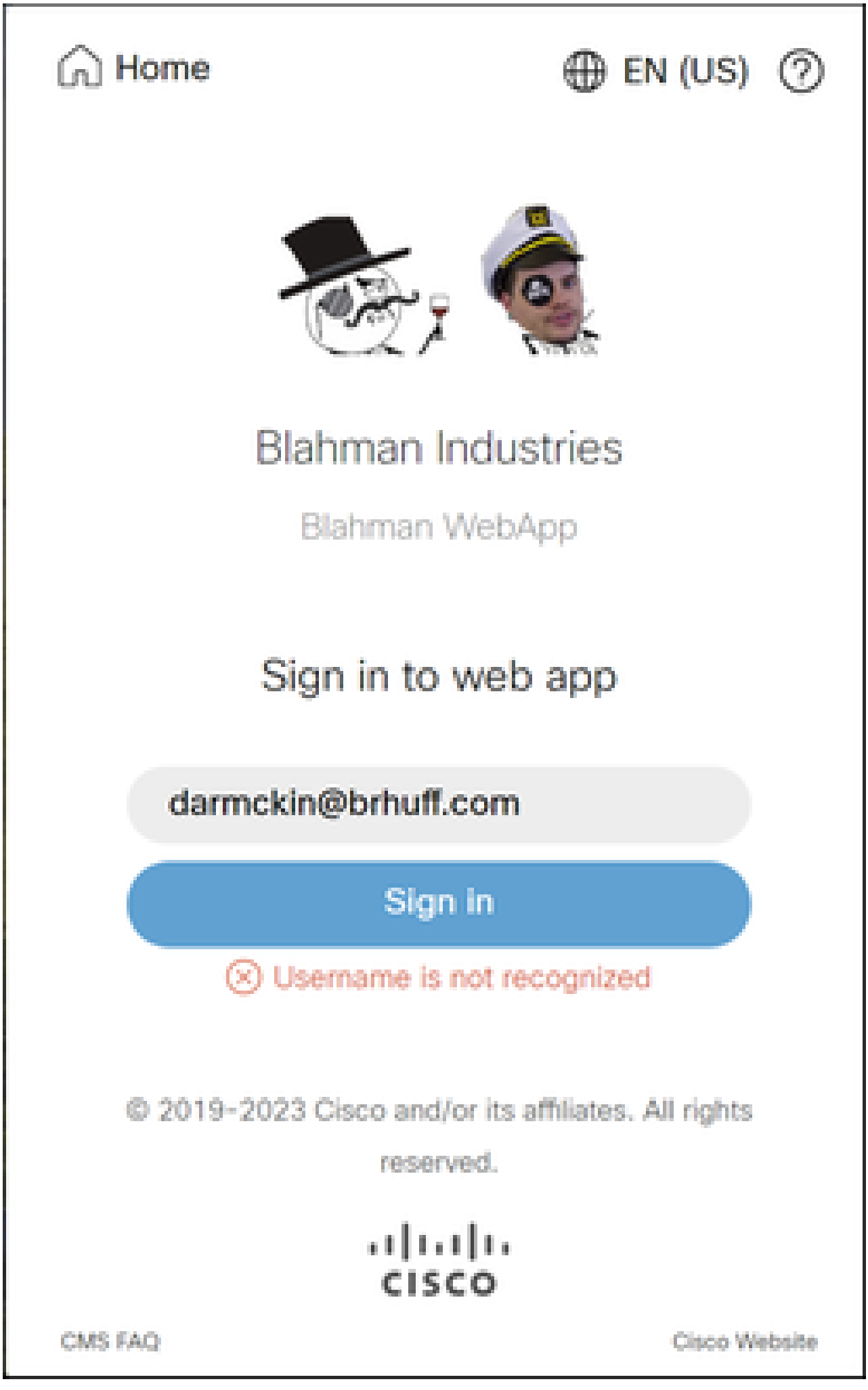
WB3Cmgr:[79e9a87e-0fa4-44df-a914-bbcabb6c87c6] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c-0272-42a1-b125-136fdf5612a5(user=steve@brhuff.com)

3月18日14:58:48.092 user.info cmscb3-1 host:server: 信息：未找到授权用户

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，并且在SSO页面中输入了正确的凭据以向LDAP进行身份验证，但他们无法登录，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

用户名无法识别

WB3Cmgr:[d626bbaf-80c3-4286-8284-fac6f71eb140] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c-0272-42a1-b125-136fdf5612a5(user=darmckin@brhuff.com)

3月18日15:08:52.399 user.warning cmscb3-1 host:server: 警告：拒绝用户'darmckin@brhuff.com'的登录尝试 — authenticationId不正确

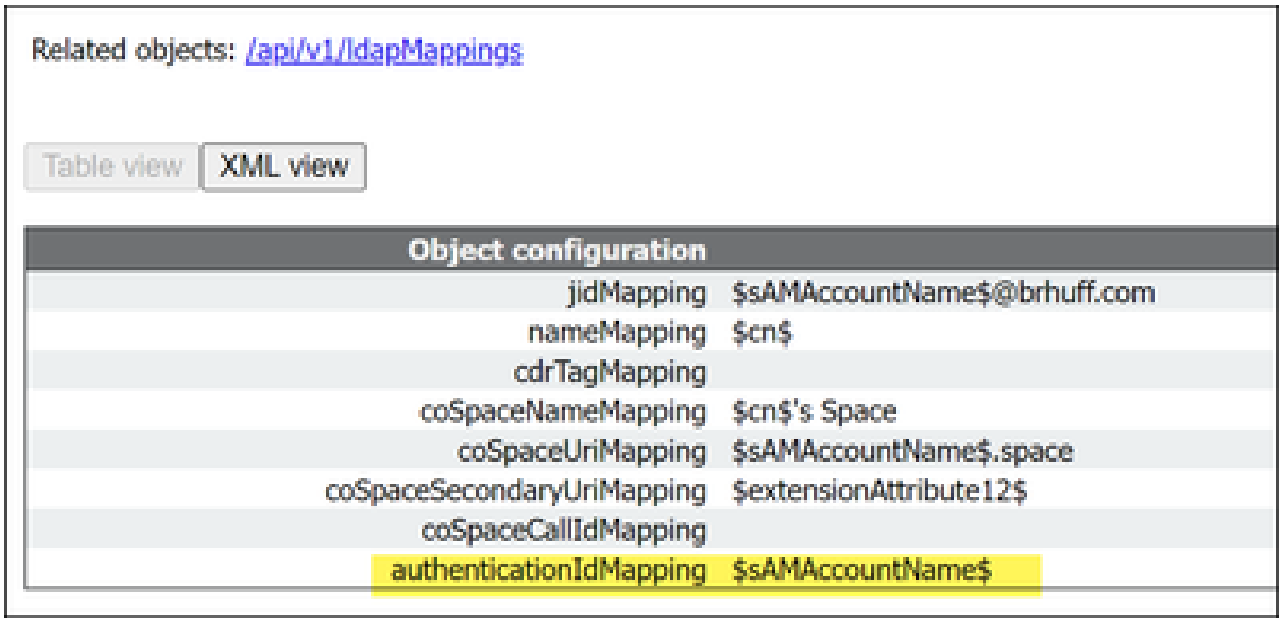
3月18日15:08:52.412 user.info cmscb3-1 host:server: 信息：来自darmckin@brhuff.com的登录请求失败

CMS ldapmapping中的AuthenticationIdMapping与ADFS中用于声明规则的已配置LDAP属性不匹配。 “Successfully obtained authenticationID:darmckin@brhuff.com”这一行表示ADFS已配置了声明规则，该属性从Active Directory获取darmckin@brhuff.com，但CMS API > Users中的AuthenticationID显示其预期值为Darmckin。 在CMS ldapMappings中，AuthenticationID配置为$sAMAccountName$，但ADFS中的声明规则配置为发送E-mail-Addresses，因此不匹配。

如何解决此问题：

请选择任一选项以缓解：

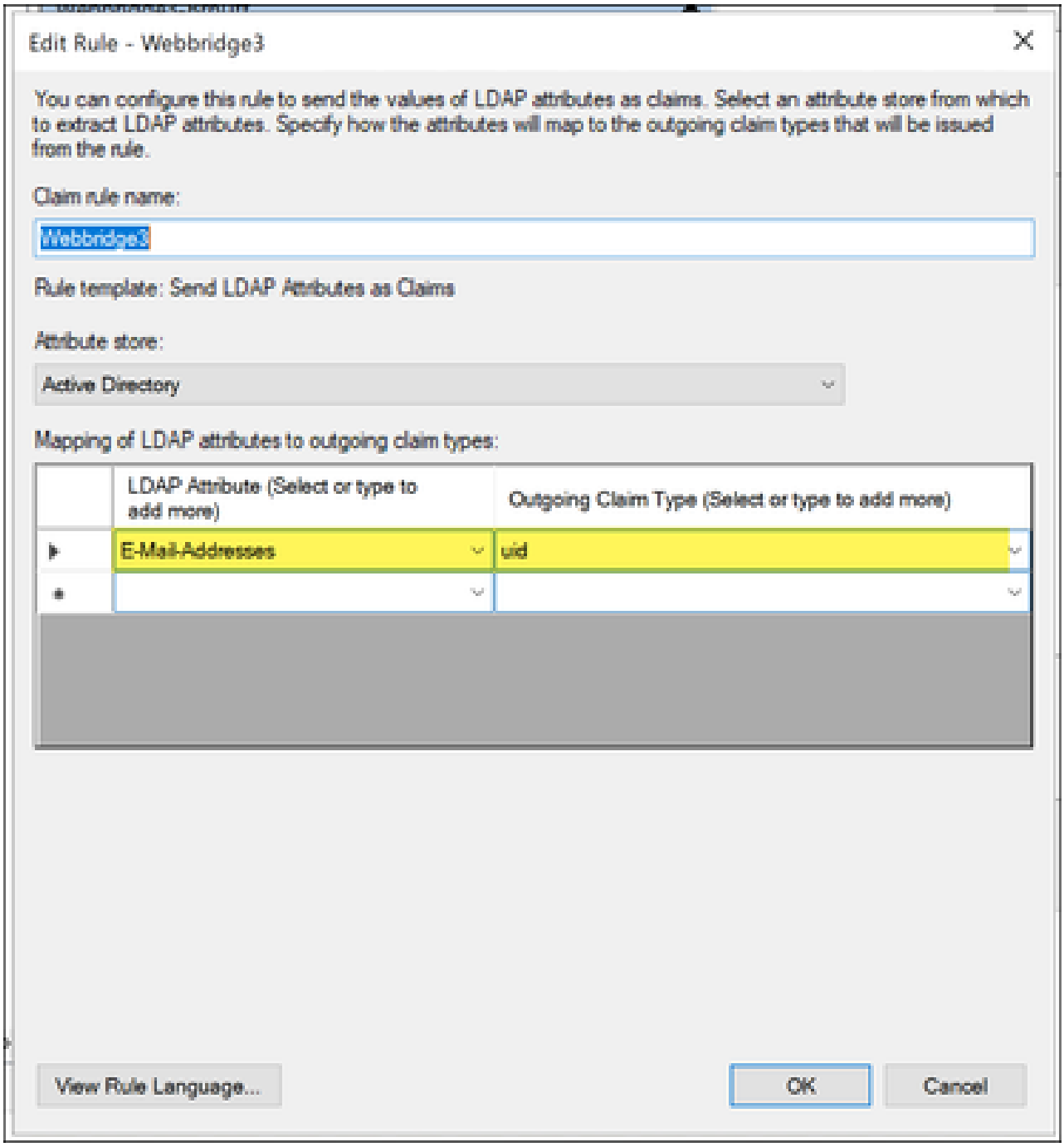
1. 更改CMS ldapmapping中的AuthenticationID以匹配ADFS上的声明规则中使用的内容，并执行新同步
2. 更改ADFS声明规则中使用的LDAP属性，以匹配CMS ldapmapping中配置的内容



API LDAPMapping

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

API用户示例



来自ADFS的声明规则

显示工作日志的Webbridge日志示例。 在加入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SAML令牌请求中的SSO sso_2024.zip

3月18日14:24:01.096 user.info cmscb3-1 client_backend: 信息：SamlManager:[7979f13c-d490-4f8b-899c-0c82853369ba]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:server: 信息：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: 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:server: 信息：WB3Cmgr:[7979f13c-d490-4f8b-899c-0c82853369ba]发出JWT ID e2a860ef-f4ef-4391-b5d5-9abdfa89ba0f

3月18日14:24:01.132 user.info cmscb3-1 host:server: 信息：WB3Cmgr:[7979f13c-d490-4f8b-899c-0c82853369ba]正在发送身份验证响应(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] 10.10.8 — [18/Mar/2024:18:24:01 +000] status 200 "POST /api/auth/sso/idpResponse HTTP/1.1" bytes_sent 0 http_referer "https://adfs.brhuff.com/" http_user_agent "Mozilla/5 (Windows NT 10.0;Win64;x64)AppleWebKit/537.36（KHTML，类似壁纸）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

常见问题解答 (FAQ)

本节重点介绍与思科会议服务器上的WebApp SSO有关的常见问题或主题。

能否扩展Webapp SSO JWT?

JSON Web令牌(JWT)是由Callbridge提供给已成功验证的Webapp客户端（已成功验证为IdP）的令牌，授予他们对WebApp服务的访问权限。在JWT内有一个到期计时器值，指示JWT的有效时间，一旦达到JWT到期时间，WebApp用户将重定向回Webbridge登录页面，需要重新验证才能重新获得访问权限。

JWT到期时间可使用“callbridge wc3jwt expiry <1-24>”(在3.8及更高版本中添加 — 更多详细信息可

在CMS 3.8发行说明或CMS MMP指南中找到)进行配置，其中数值表示要设置提供给WebApp客户端的JWT到期时间的小时数。但是，如命令所示，最大值可以设置为24小时，这意味着JWT可以保持有效的最长时间以及WebApp用户可以登录的时间是24小时。满足JWT到期时间时 — 浏览器将转储到期令牌，WebApp用户将被强制返回到WebApp登录页面。

在某些环境中，根据IdP和环境设置，可以在IdP上实施持续SSO/保持我登录功能，这将为浏览器提供从IdP进行的持续登录，即使关闭浏览器，也会保留cookie（除非通过其他方式清除）。无论SSO/IdP配置如何，当JWT过期(最长24小时)时，WebApp用户将被强制返回到WebApp登录页 — 但是，在这种情况下，在IdP上启用持续SSO的用户只需要输入在WebApp登录页上<user@domain>，无需重新验证其IdP。

一项增强功能可用于实施刷新令牌机制，以允许对WebApp进行扩展授权 — 思科漏洞ID CSCwm28758。

如果我关闭浏览器，是否需要重新向WebApp进行身份验证？

此场景的流程如下：

1. 用户登录WebApp（使用SSO身份验证方法）。
2. 用户会在某个时候关闭浏览器。
3. 用户再次打开浏览器并导航到WebApp站点。（立即或稍后进行）。

在这种情况下，会发生什么情况？

答案取决于！这完全取决于Callbridge提供的JWT在访问WebApp页面时是否过期。只要JWT仍然有效且存在于存储中，您就可以导航到WebApp页面（即使您关闭了浏览器）。 请记住，JWT的最长有效时间为24小时。

- 如果JWT仍然有效（未过期）且存在，则用户可以使用其空格等导航到WebApp页面，而无需重新进行身份验证。
- 如果JWT为INVALID(EXPIRED)，用户将被重定向到WebApp登录页面，需要重新登录WebApp。用户可能还必须根据其IdP身份验证方法重新验证其IdP（例如，如果IdP使用会话SSO或持续SSO）。

WebApp SSO中如何支持多个域？

WebApp SSO能够支持具有多个域的环境，甚至支持那些不同域指向不同身份提供程序(IdP)的环境。 请查阅思科会议服务器部署指南或联系思科TAC获取有关使用多个域的支持。

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）。