

CMS에서 WebApp SSO 구성 및 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경](#)

[구성](#)

[네트워크 다이어그램](#)

[AD FS 설치 및 초기 설정](#)

[CMS 사용자를 IdP\(ID 공급자\)에 매핑](#)

[IdP용 Webbridge 메타데이터 XML 만들기](#)

[Webbridge의 메타데이터를 IdP\(ID 공급자\)로 가져오기](#)

[IdP에서 Webbridge 서비스에 대한 클레임 규칙 만들기](#)

[Webbridge용 SSO 아카이브 ZIP 파일을 생성합니다.](#)

[idp_config.xml 가져오기 및 구성](#)

[내용으로 config.jsonFile 만들기](#)

[sso_sign.key 설정\(선택 사항\)](#)

[sso_encrypt.key 설정\(선택 사항\)](#)

[SSO ZIP 파일 생성](#)

[Webbridge에 SSO Zip 파일 업로드](#)

[CAC\(Common Access Card\)](#)

[WebApp을 통해 SSO 로그인 테스트](#)

[문제 해결](#)

[기본 문제 해결](#)

[Microsoft ADFS 오류 코드](#)

[인증 ID를 가져오지 못했습니다.](#)

[유효성 검사에서 통과/일치하는 어설션이 없습니다.](#)

[웹 앱에서 로그인하지 못했습니다.](#)

[시나리오 1:](#)

[시나리오 2:](#)

[시나리오 3:](#)

[사용자 이름을 인식할 수 없습니다.](#)

[시나리오 1:](#)

[시나리오 2:](#)

[작동 로그를 보여주는 Webbridge 로그 예입니다. 조인 URL에서 ?trace=true를 사용하여 생성된 예:](#)

[관련 정보](#)

소개

이 문서에서는 SSO(Single Sign On)의 Cisco Meeting Server(CMS) Web App 구현을 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 숙지할 것을 권장합니다.

- CMS Callbridge 버전 3.1 이상
- CMS Webbridge 버전 3.1 이상
- Active Directory 서버
- 제공자 식별(IdP)

사용되는 구성 요소


이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경

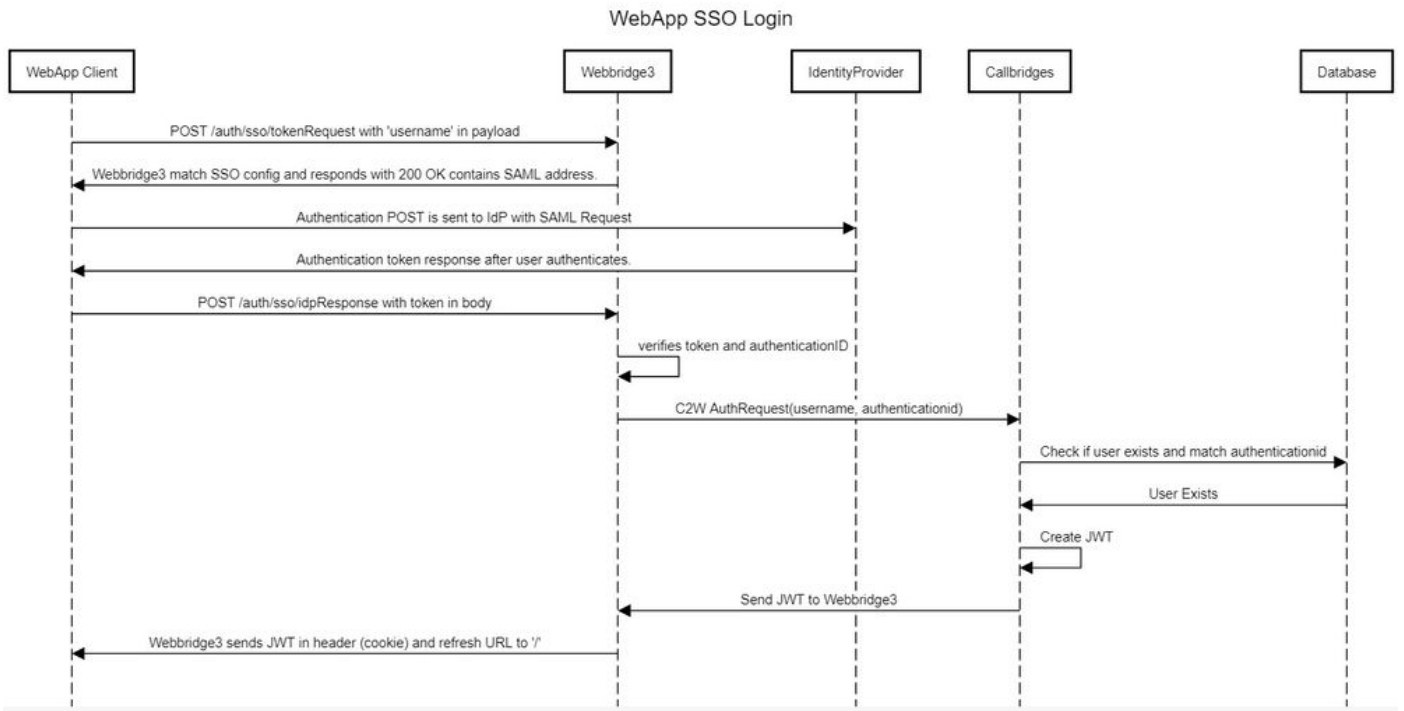
CMS 3.1 이상에서는 사용자가 로그인할 때마다 비밀번호를 입력할 필요 없이 SSO를 사용하여 로그인할 수 있는 기능을 도입했습니다. ID 제공자를 사용하여 단일 세션이 생성되기 때문입니다. 이 기능은 SAML(Security Assertion Markup Language) 버전 2.0을 SSO 메커니즘으로 사용합니다.

 참고: CMS는 SAML 2.0에서 HTTP-POST 바인딩만 지원하며 사용 가능한 HTTP-POST 바인딩이 없는 ID 제공자는 거부합니다.

 참고: SSO가 활성화된 경우 기본 LDAP 인증이 더 이상 가능하지 않습니다.

구성

네트워크 다이어그램



AD FS 설치 및 초기 설정

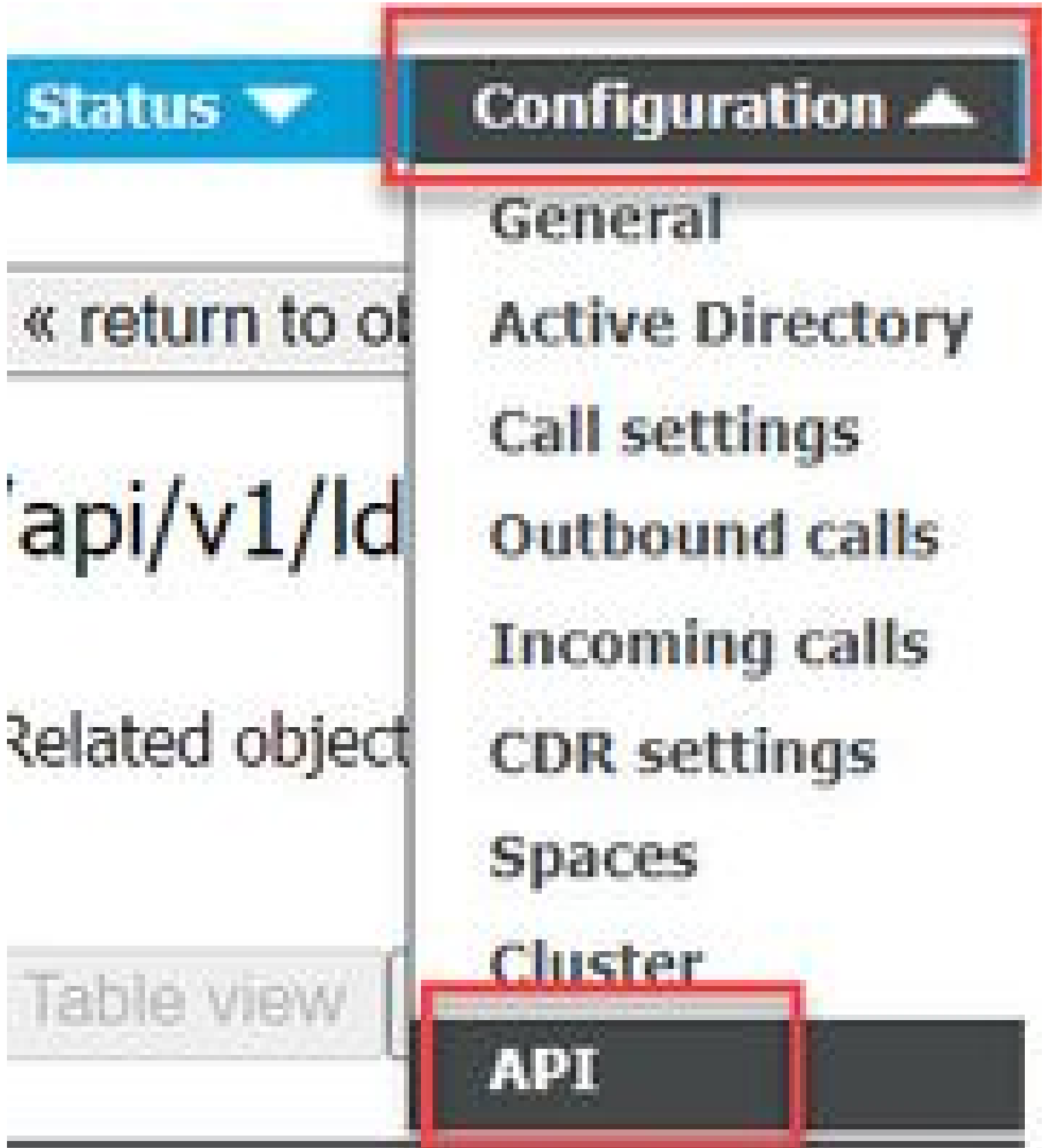
이 배포 시나리오에서는 Microsoft ADFS(Active Directory Federation Services)를 IdP(ID 공급자)로 사용하므로 이 구성 전에 ADFS(또는 의도한 IdP)를 설치하고 실행하는 것이 좋습니다.

CMS 사용자를 IdP(ID 공급자)에 매핑

사용자가 유효한 인증을 받도록 하려면 IdP에서 제공하는 상관 관계 필드에 대한 API(Application Programming Interface)에서 매핑해야 합니다. 이에 사용되는 옵션은 API의 IdpMapping에 있는 authenticationIdMapping입니다.

1. CMS 웹 관리 GUI에서 Configuration(컨피그레이션) > API(API)로 이동합니다.

공동



2. api/v1/ldapMappings/<GUID-of-Ldap-Mapping>에서 기존(또는 새) LDAP 매핑을 찾습니다.

API objects

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

Filter (2 of 129 nodes)

[/api/v1/ldapMappings](#) ◀

◀ start < prev 1 - 2 (of 2) next >

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

3. 선택한 ldapMapping 객체에서 authenticationIdMapping을 IdP에서 전달된 LDAP 특성으로 업데이트합니다. 이 예에서는 \$sAMAccountName\$ 옵션이 매핑을 위한 LDAP 특성으로 사용됩니다.

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

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

참고: callbridge/database에서 SAMLResponse의 IdP에서 보낸 클레임을 검증하고 사용자에게 JWT(JSON Web Token)를 제공하는 데 authenticationIdMapping이 사용됩니다.

4. 최근 수정된 ldapMapping과 연결된 ldapSource에서 LDAP 동기화를 수행합니다.

예를 들면 다음과 같습니다.

[/api/v1/ldapSyncs](#)

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

5. LDAP 동기화가 완료되면 Configuration(구성) > api/v1/users(api/v1/users)에서 CMS API로 이동하여 가져온 사용자를 선택하고 authenticationId가 올바르게 입력되었는지 확인합니다.

Object configuration	
userId	jdoe@brhuff.com
name	John Doe
email	johnndoe@brhuff.com
authenticationId	jdoe
userProfile	d5cd50e4-e423-4ba6-bd17-7492b9ba5eb3

jdoe = sAMAccountName

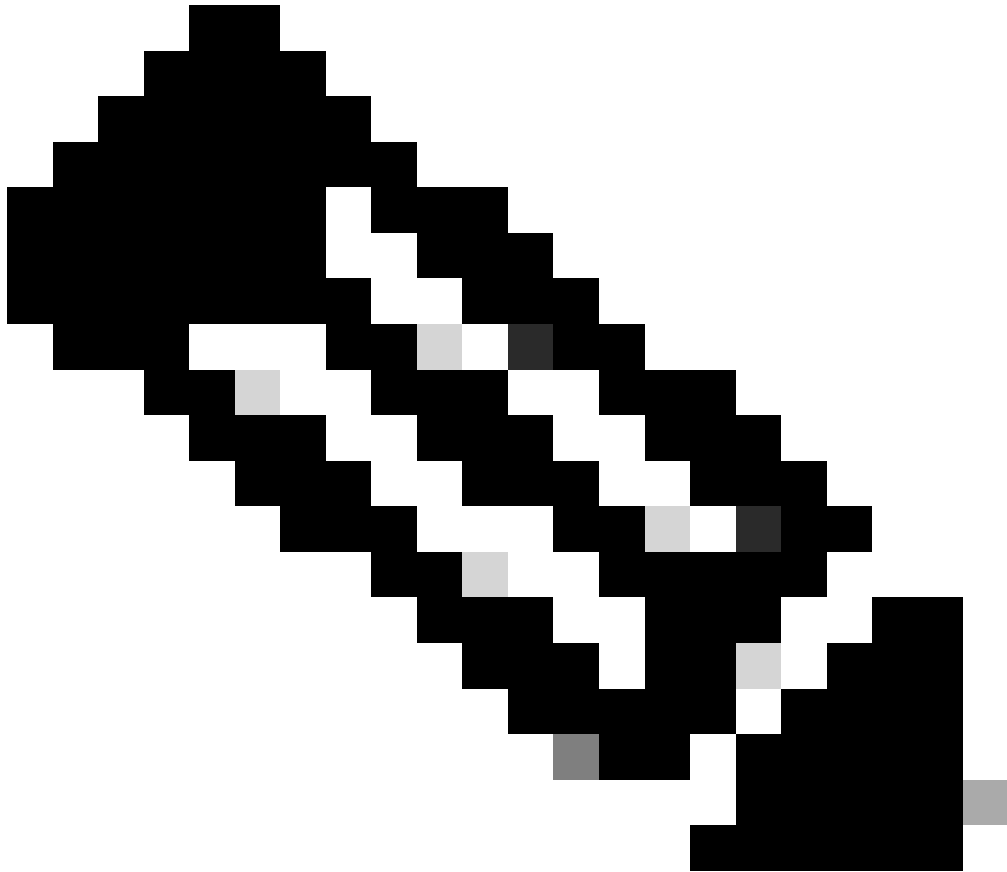
IdP용 Webbridge 메타데이터 XML 만들기

Microsoft AD FS에서는 메타데이터 XML 파일을 사용 중인 서비스 공급자를 식별하기 위한 신뢰 신뢰 당사자로 가져올 수 있습니다. 이러한 목적으로 메타데이터 XML 파일을 생성하는 방법에는 몇 가지가 있지만 파일에 몇 가지 특성이 있어야 합니다.

필수 값이 있는 Webbridge 메타데이터의 예:

```
<?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 - 사용자의 브라우저에서 연결할 수 있는 Webbridge3 서버 주소(FQDN/호스트 이름) 및 관련 포트입니다.



참고: 단일 URL을 사용하는 웹 브리지가 여러 개 있는 경우 이 주소는 로드 밸런싱 주소여야 합니다.

2. Location - Webbridge 주소에 대한 HTTP-POST AssertionConsumerService가 있는 위치입니다. 이는 로그인 후 인증된 사용자를 리디렉션할 위치를 IdP에 알려줍니다. 이 값은 idpResponse URL(<https://<WebbridgeFQDN>:<port>/api/auth/sso/idpResponse>)로 설정해야 합니다. 예: <https://join.example.com:443/api/auth/sso/idpResponse>.
3. 선택 사항 - 서명을 위한 공개 키 - IdP가 Webbridge에서 AuthRequest를 확인하는 데 사용하는 서명을 위한 공개 키(인증서)입니다. 이는 IdP가 공개 키(인증서)를 사용하여 서명을 확인할 수 있도록 Webbridge에 업로드된 SSO 번들의 개인 키 'sso_sign.key'와 일치해야 합니다. 구축의 기존 인증서를 사용할 수 있습니다. 텍스트 파일에서 인증서를 열고 내용을 Webbridge 메타데이터 파일에 복사합니다. sso_xxxx.zip 파일에 사용된 인증서의 일치 키를 sso_sign.key 파일로 사용합니다.
4. 선택 사항 - 암호화를 위한 공개 키 - IdP가 Webbridge로 다시 전송된 SAML 정보를 암호화하는 데 사용하는 공개 키(인증서)입니다. 이는 Webbridge에서 업로드된 SSO 번들의 개인 키

'sso_encrypt.key'와 일치해야 Webbridge에서 IdP로 다시 전송된 항목을 해독할 수 있습니다. 구축의 기존 인증서를 사용할 수 있습니다. 텍스트 파일에서 인증서를 열고 내용을 Webbridge 메타데이터 파일에 복사합니다. sso_xxxx.zip 파일에 사용된 인증서의 일치 키를 sso_encrypt.key 파일로 사용합니다.

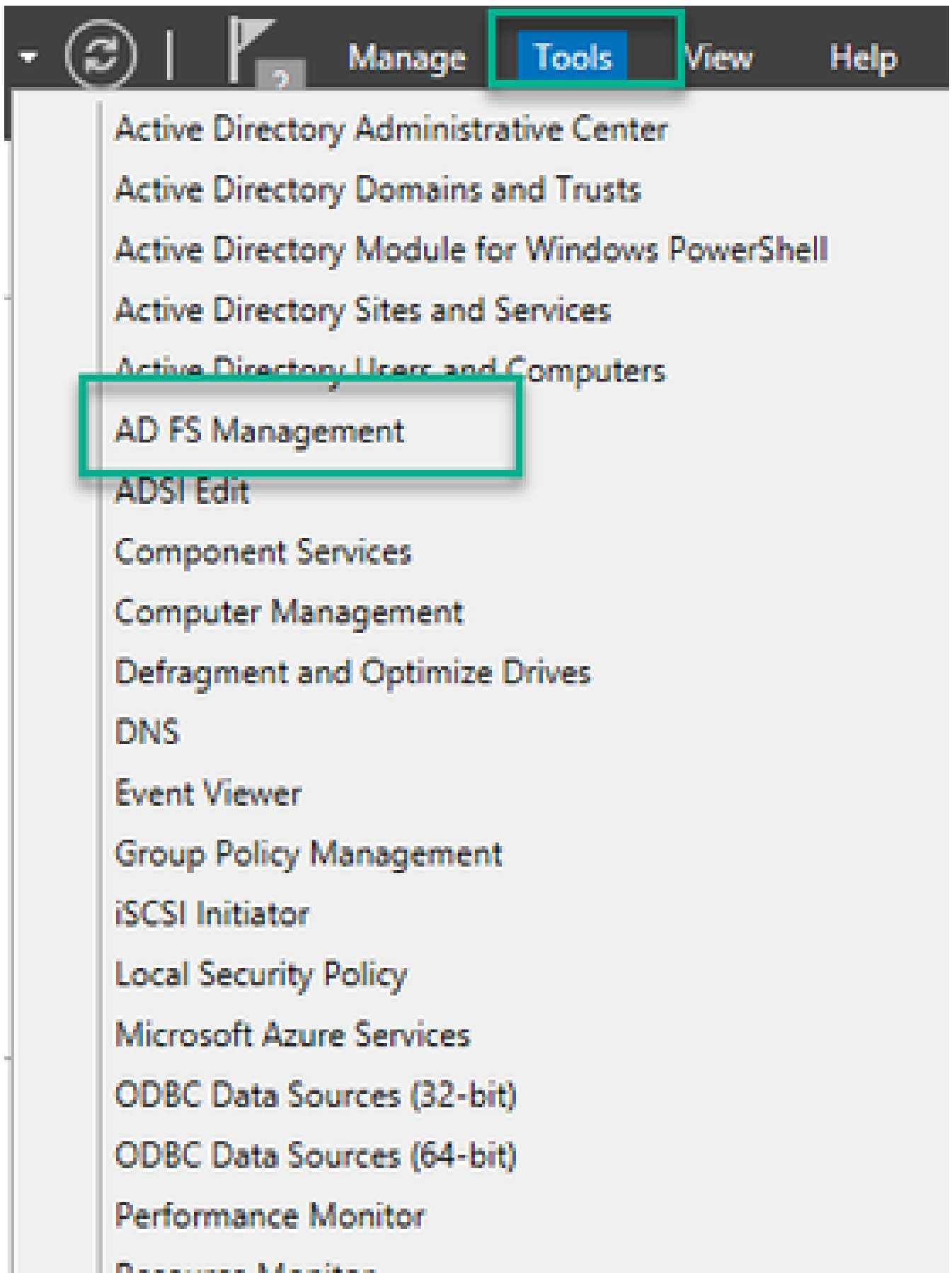
선택적 공개 키(인증서) 데이터를 사용하여 IdP로 가져올 Webbridge 메타데이터의 예:

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

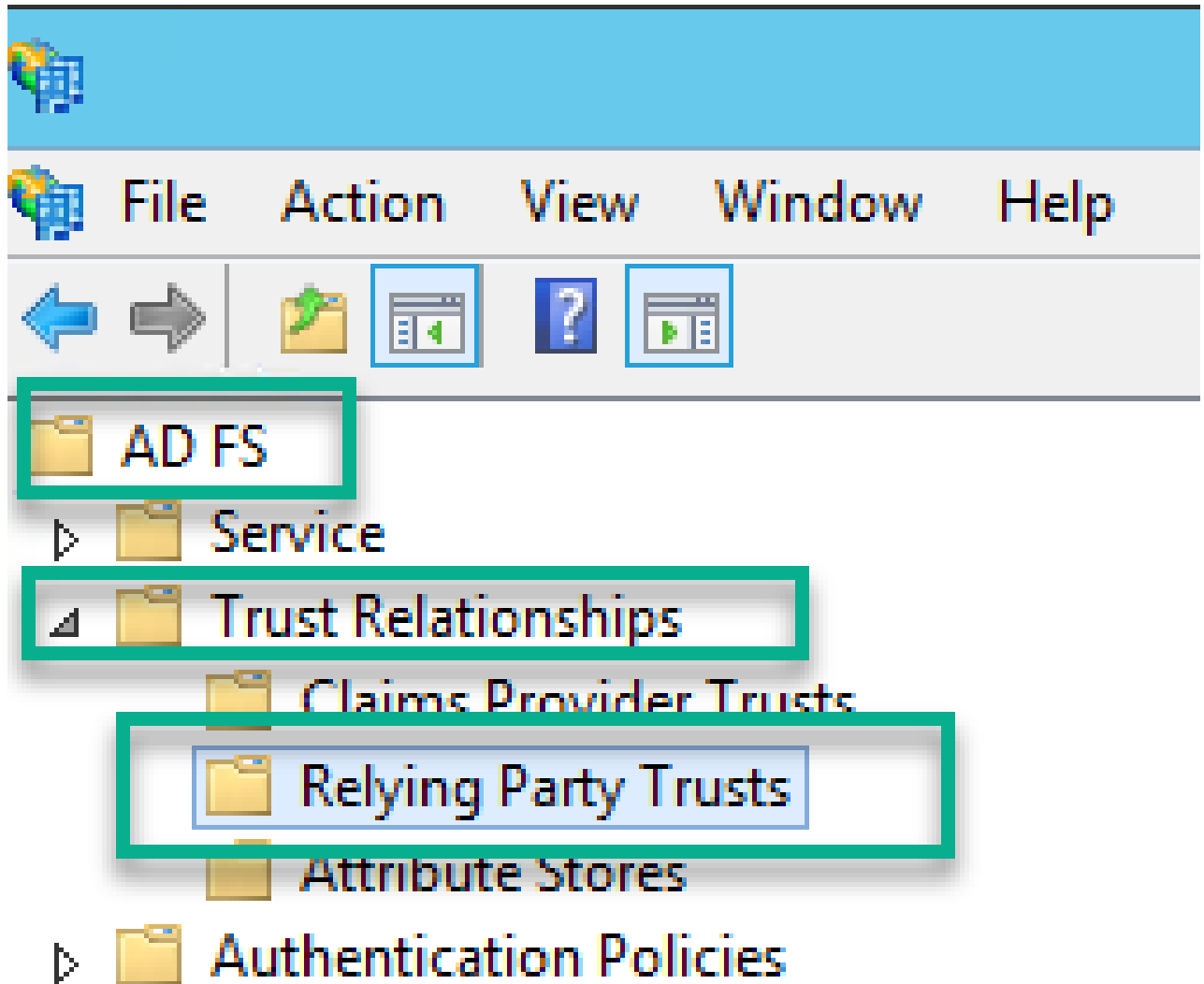
Webbridge의 메타데이터를 IdP(ID 공급자)로 가져오기

메타데이터 XML이 적절한 특성으로 만들어지면 파일을 Microsoft AD FS 서버로 가져와 신뢰 신뢰 당사자를 만들 수 있습니다.

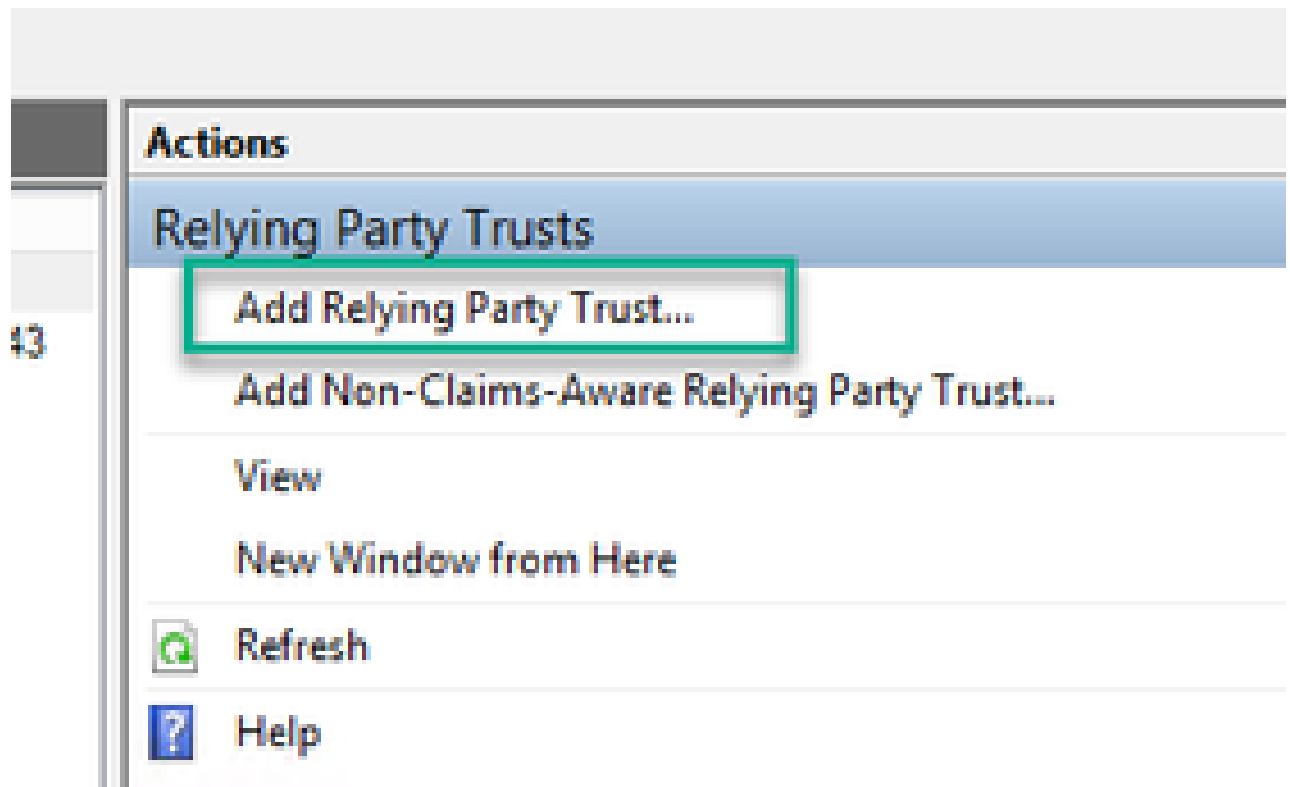
1. AD FS 서비스를 호스팅하는 Windows Server에 원격 데스크톱
2. 일반적으로 서버 관리자를 통해 액세스할 수 있는 AD FS 관리 콘솔을 엽니다.



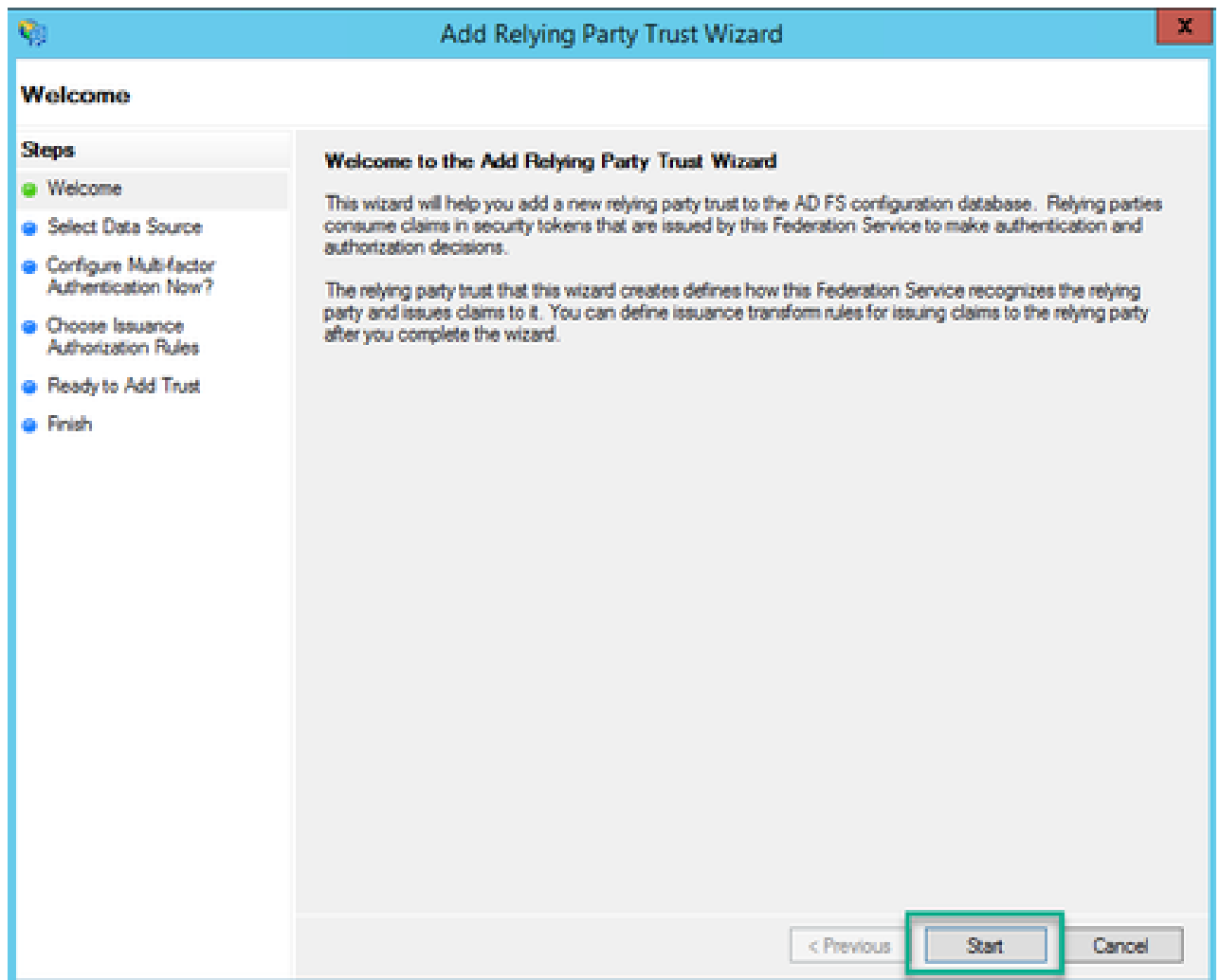
3. AD FS 관리 콘솔에서 왼쪽 창의 AD FS > Trust Relationships > Relying Party Trust로 이동합니다.



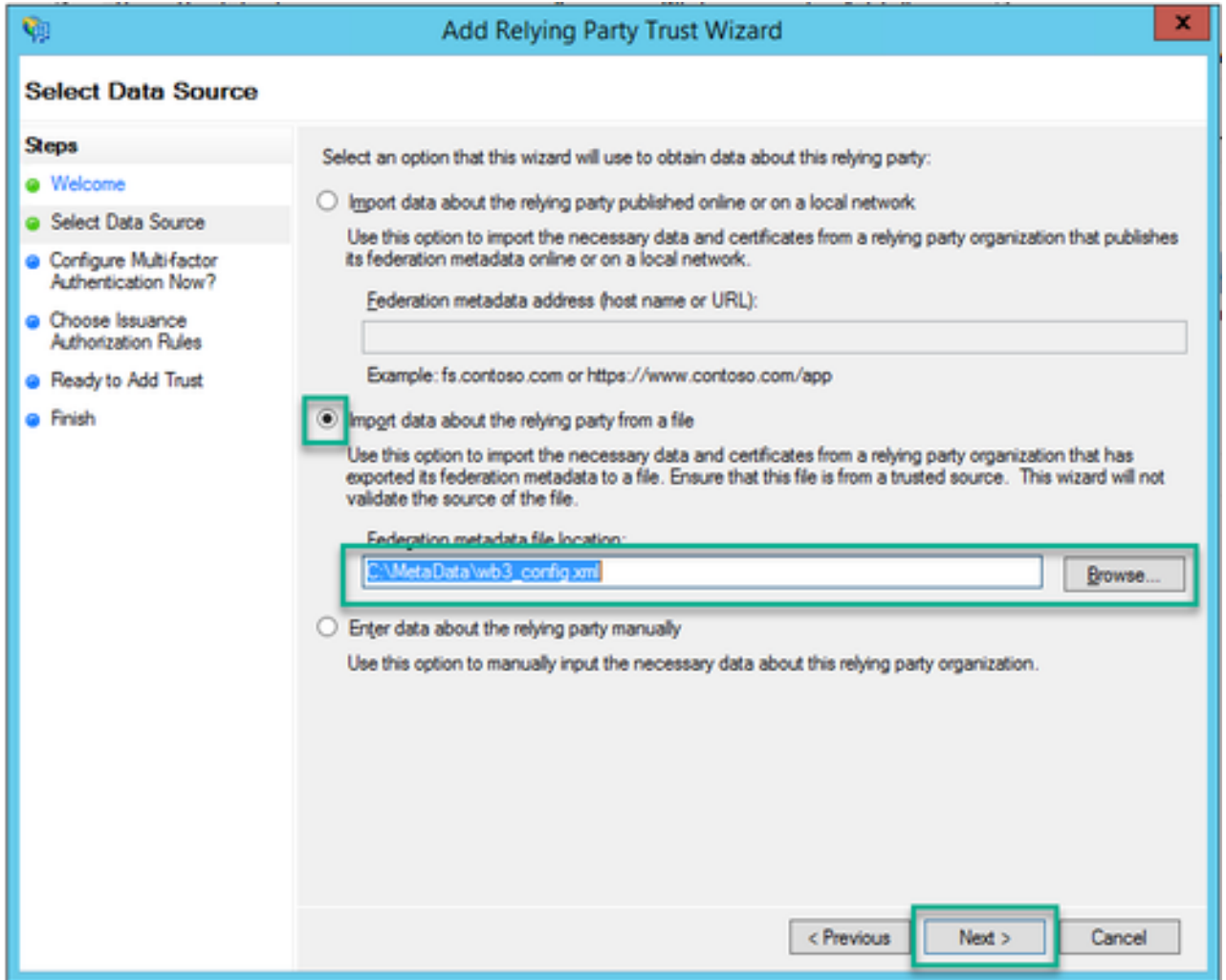
4. ADFS Management Console의 오른쪽 창에서 Add Relying Party Trust... 옵션을 선택합니다.



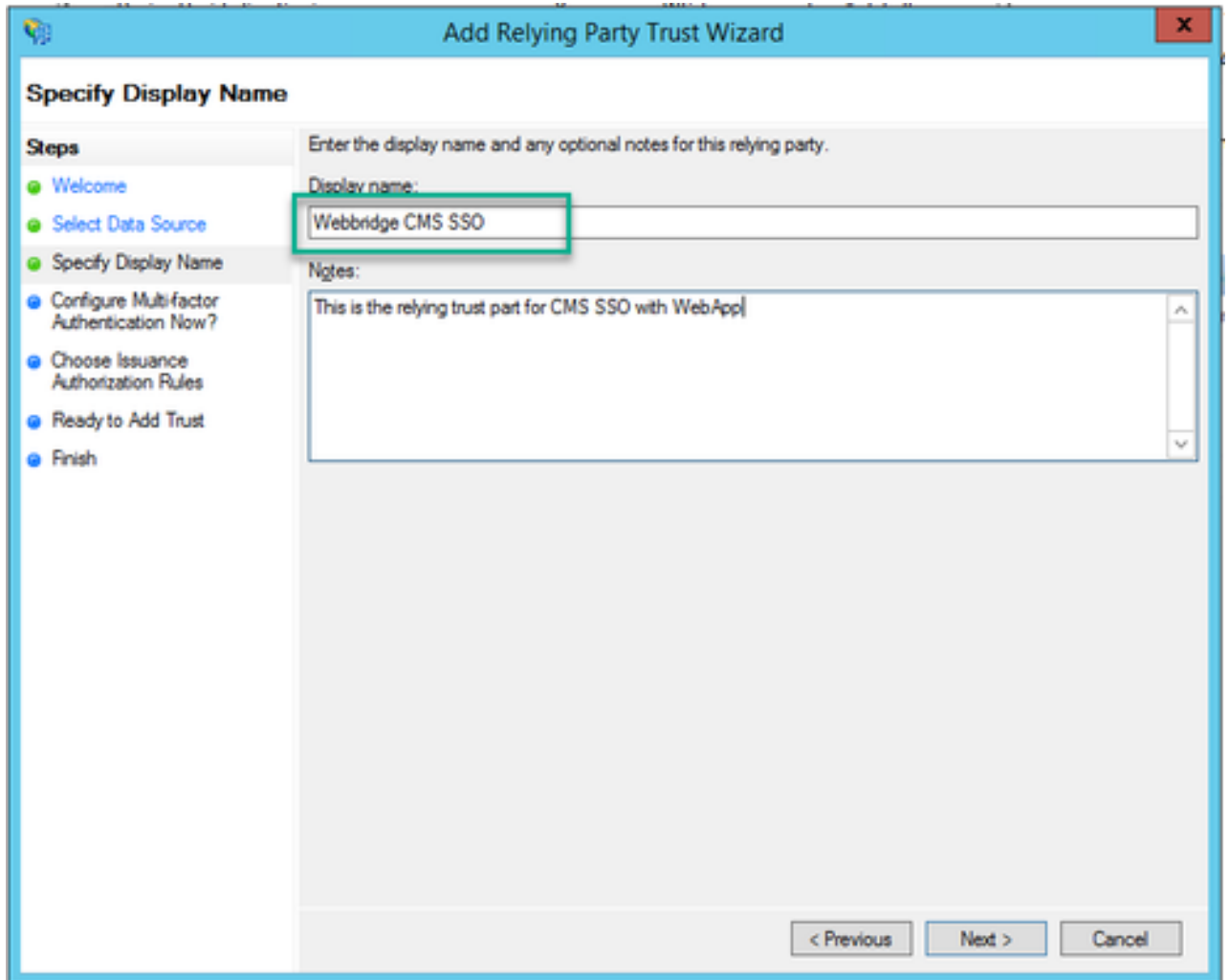
5. 이 옵션을 선택하면 당사자 Trust 추가 마법사가 열립니다. 시작 옵션을 선택합니다.



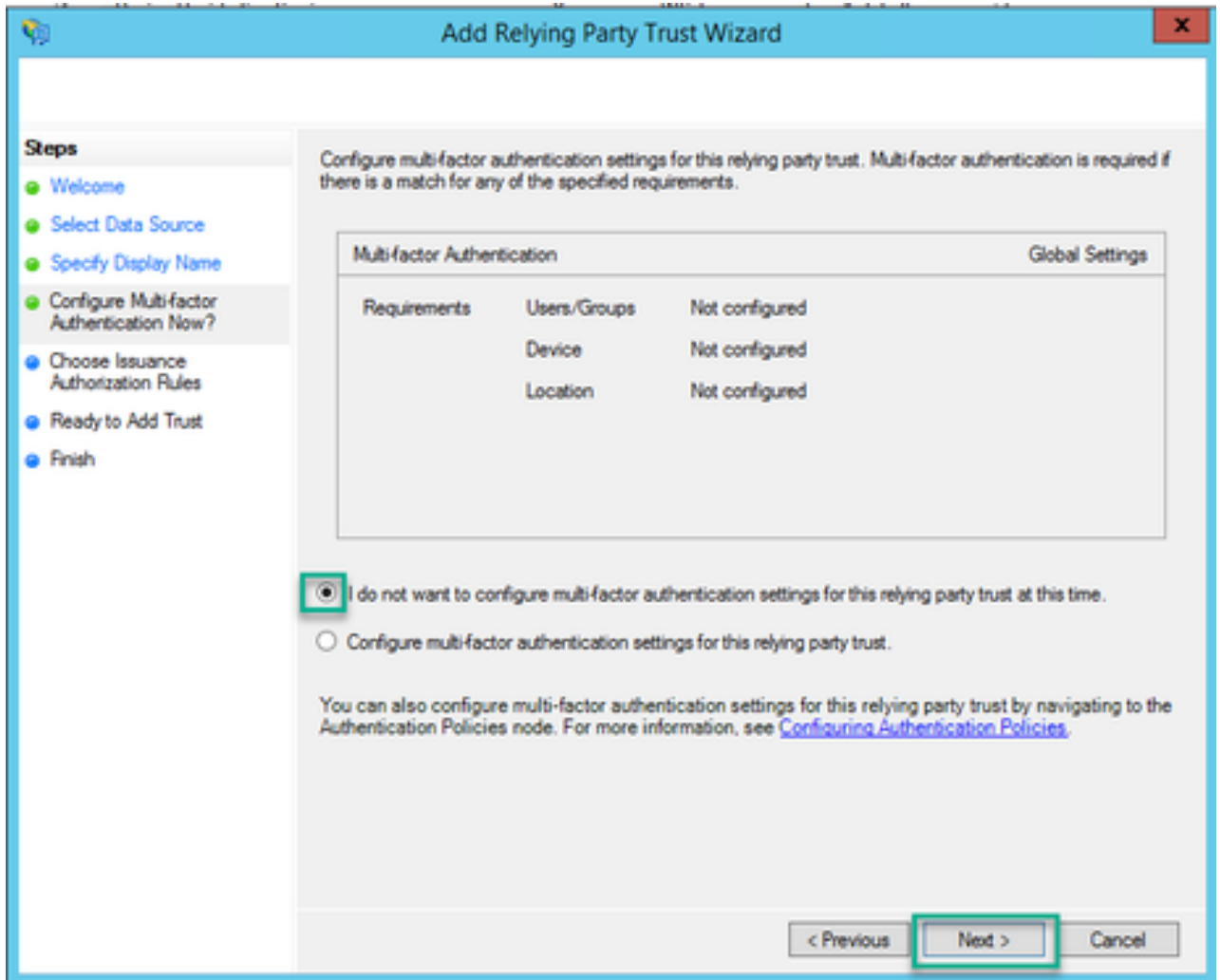
6. [데이터 소스 선택] 페이지에서 파일에서 당사자에 대한 데이터 가져오기의 라디오 버튼을 선택하고 찾아보기를 선택하여 Webbridge 메타데이터 파일의 위치로 이동합니다.



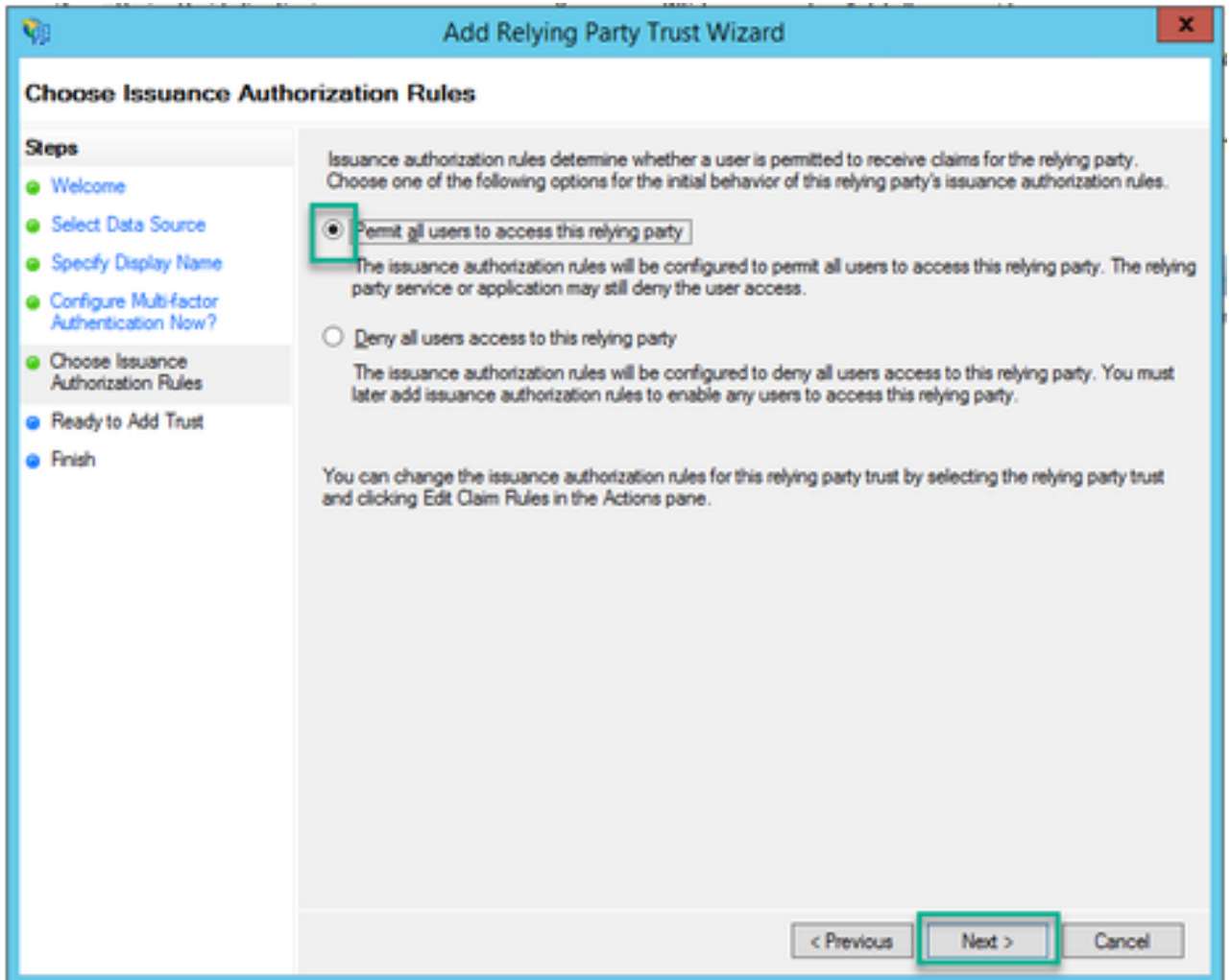
7. 표시 이름 지정 페이지에서 AD FS의 엔터티에 대해 표시할 이름을 입력합니다. 표시 이름은 AD FS 통신을 위한 서버 용도가 아니며 단순히 정보용입니다.



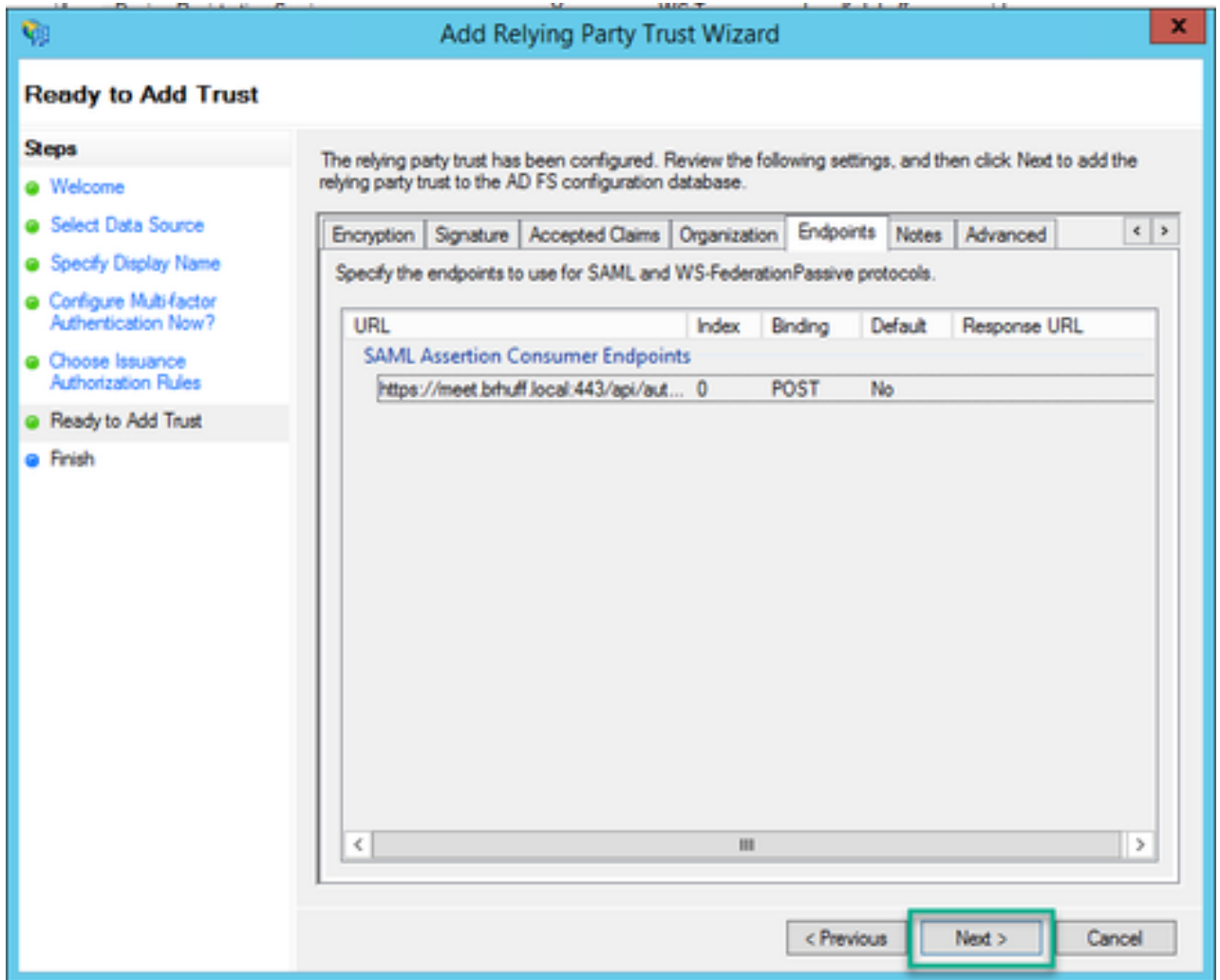
8. Configure Multi-factor Authentication Now(지금 다중 요소 인증 구성) 페이지에서 기본값으로 두고 Next(다음)를 선택합니다.



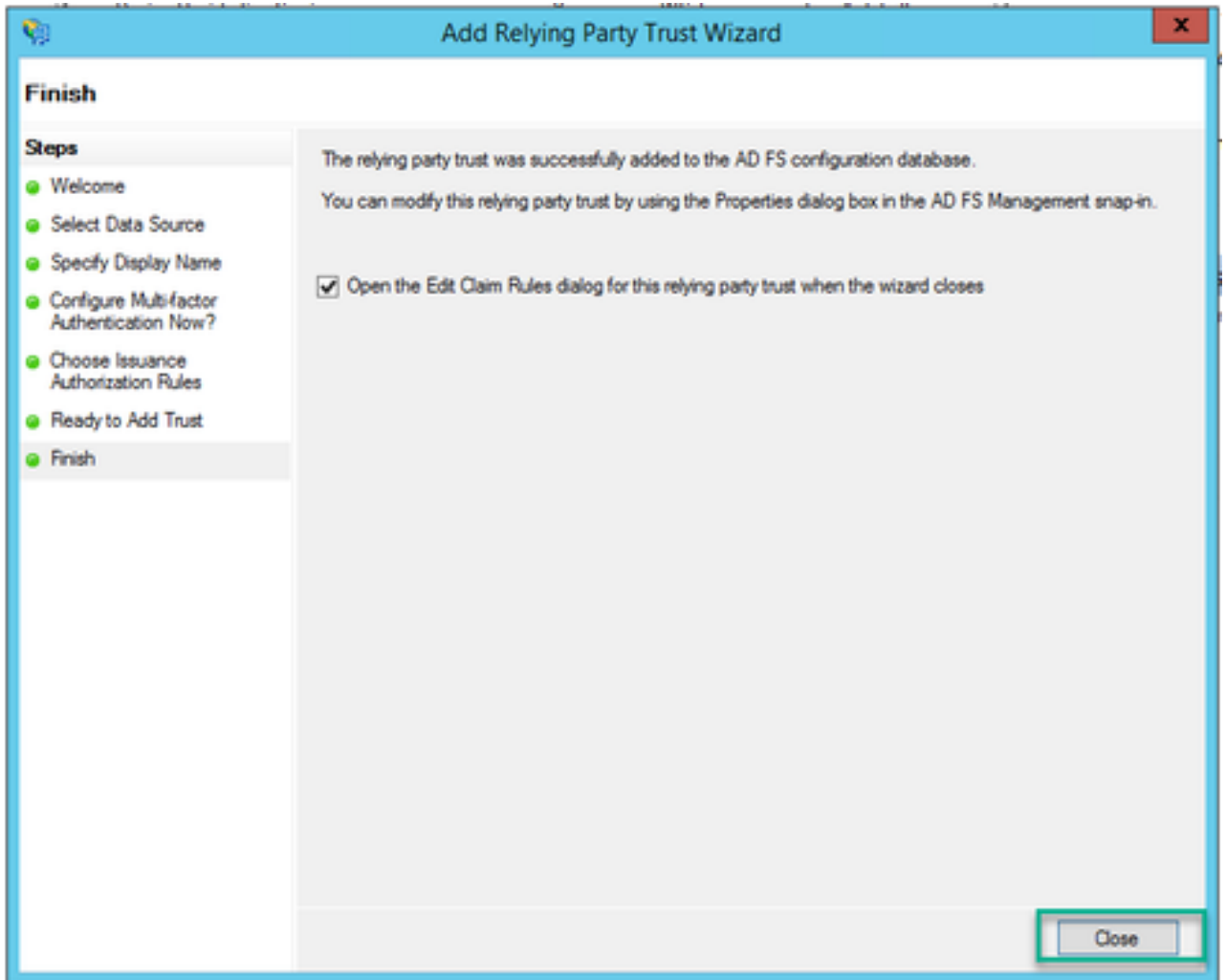
9. Choose Issuance Authorization Rules(발급 권한 부여 규칙 선택) 페이지에서 Permit all users to access this relying party(모든 사용자가 이 신뢰 당사자에 액세스하도록 허용)에 대해 선택된 것으로 합니다.



10. Ready to Add Trust(트러스트 추가 준비) 페이지에서 탭을 통해 Webbridge에 대한 Relying Trust Party(신뢰 당사자)의 가져온 세부 정보를 검토할 수 있습니다. Webbridge 서비스 공급자의 URL 세부 정보에 대한 식별자 및 엔드포인트를 확인합니다.



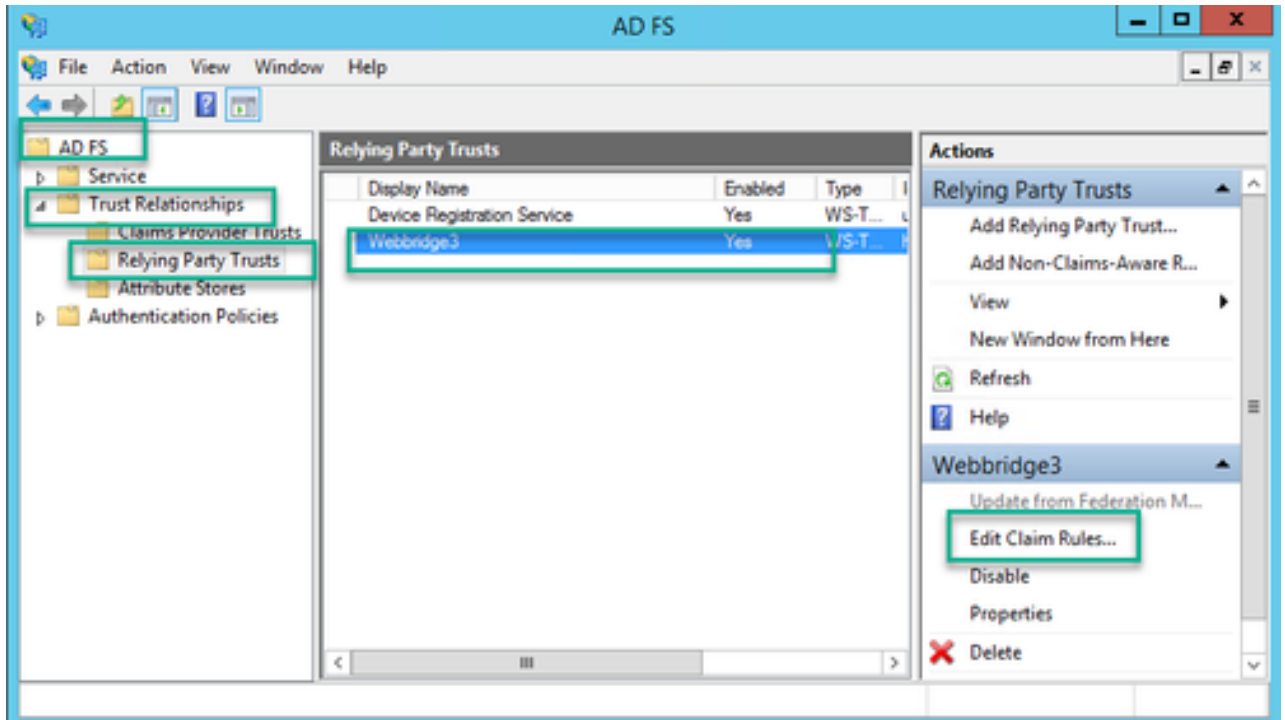
11. 완료 페이지에서 마감 옵션을 선택하여 마법사를 닫고 청구 규칙 편집을 계속합니다.



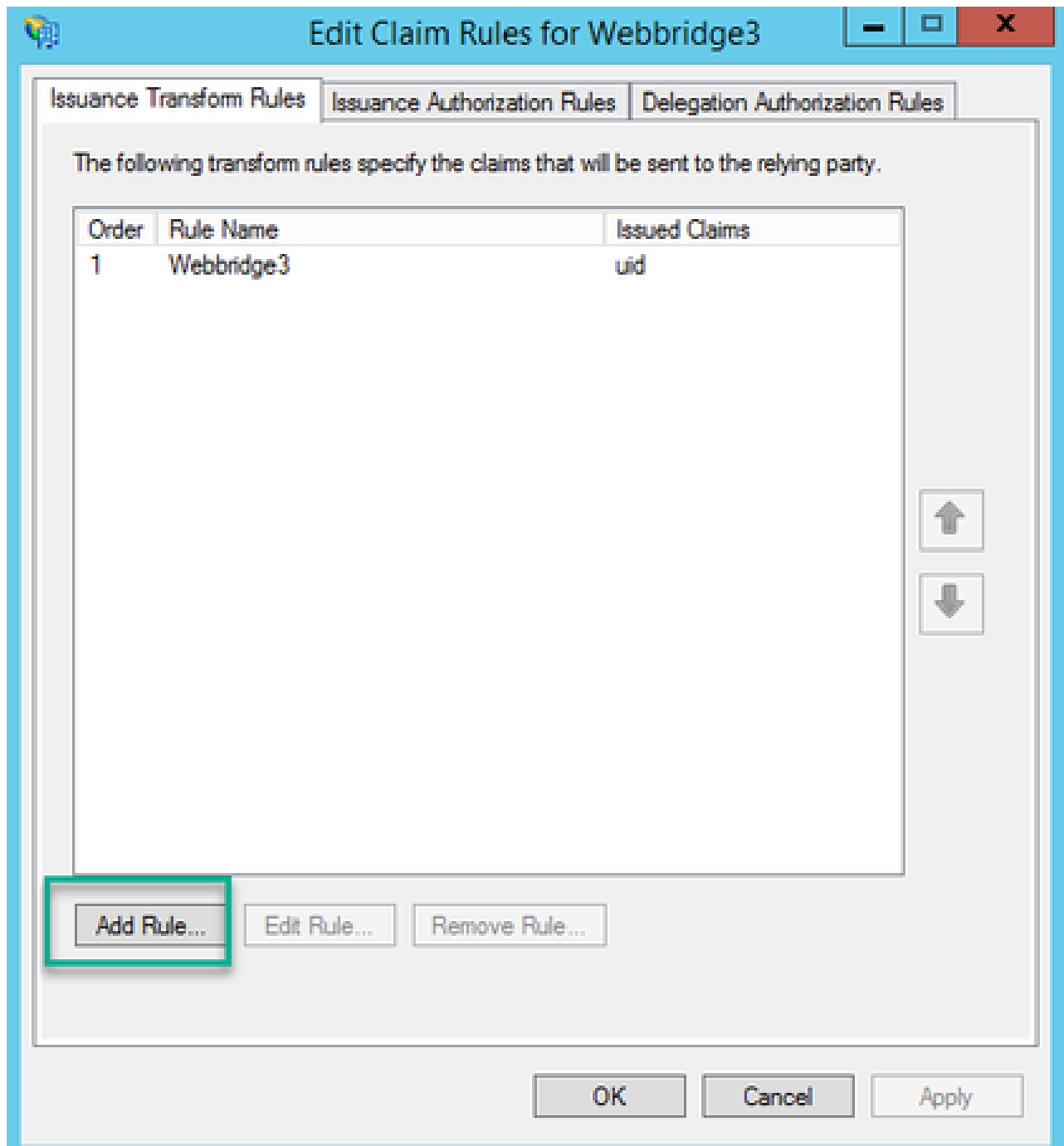
IdP에서 Webbridge 서비스에 대한 클레임 규칙 만들기

Webbridge에 대해 당사자 Trust가 생성되었으므로 SAML 응답에서 Webbridge에 제공할 발신 클레임 유형에 특정 LDAP 특성을 일치시키기 위한 클레임 규칙을 생성할 수 있습니다.

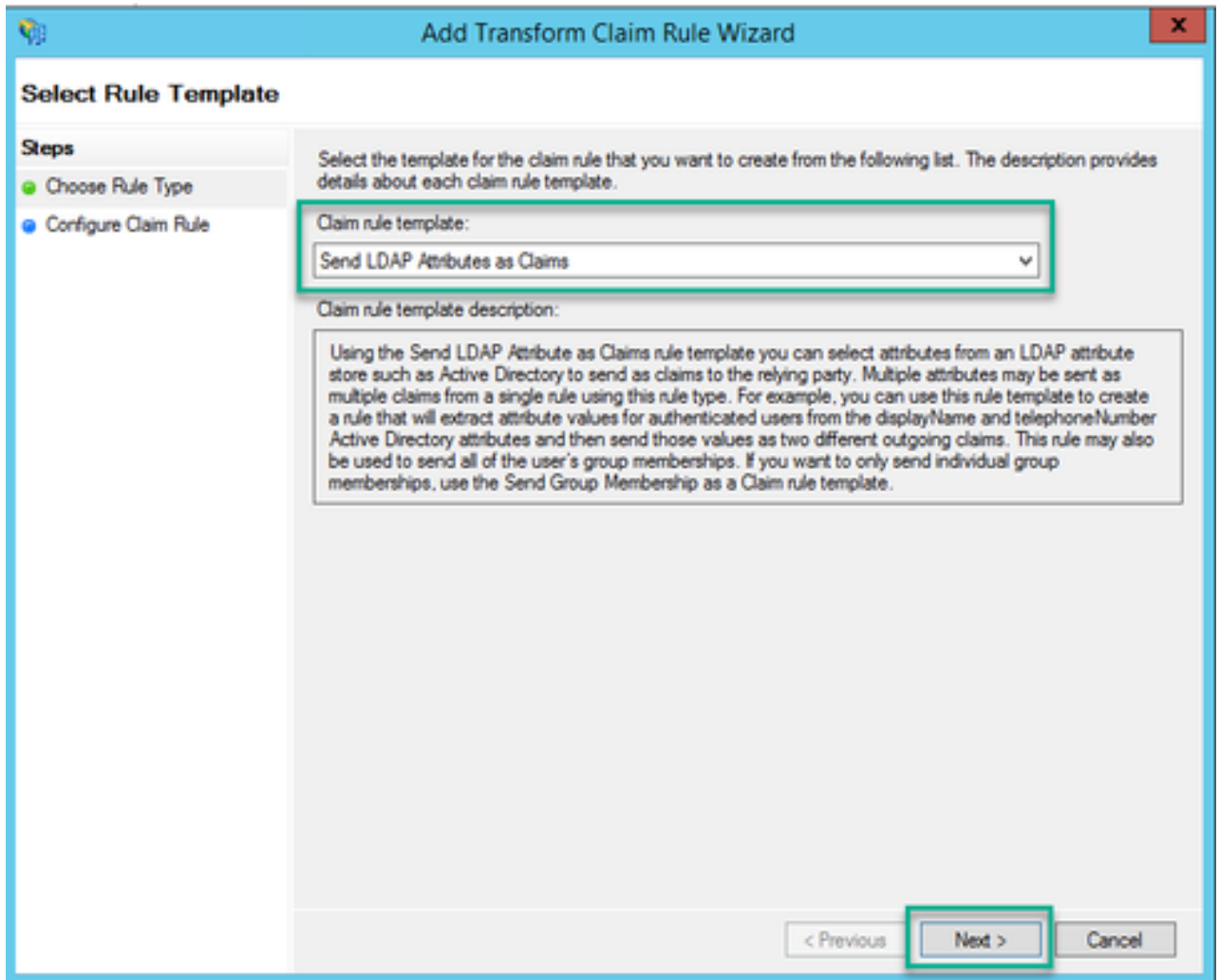
1. ADFS Management Console에서 Webbridge에 대한 당사자 Trust를 강조 표시하고 오른쪽 창에서 Edit Claim Rules(클레임 규칙 편집)를 선택합니다.



2. <DisplayName>에 대한 클레임 규칙 편집 페이지에서 규칙 추가...를 선택합니다.



3. [클레임 규칙 추가 마법사] 페이지에서 [클레임 규칙 템플릿 옵션에 대한 클레임으로 LDAP 속성 보내기]를 선택하고 [다음]을 선택합니다.



4. [클레임 규칙 구성] 페이지에서 신뢰 당사자 트러스트에 대한 클레임 규칙을 다음 값으로 구성합니다.

1. 클레임 규칙 이름 = AD FS의 규칙에 지정된 이름이어야 합니다(규칙 참조에만 해당).
2. 속성 저장소 = Active Directory
3. LDAP 특성 = Callbridge API의 authenticationIdMapping과 일치해야 합니다(예: \$sAMAccountName\$).
4. 발신 클레임 유형 = Webbridge SSO config.json의 authenticationIdMapping과 일치해야 합니다. (예: uid)

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

Claim rule name:

Webbridge3

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

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

View Rule Language...

OK

Cancel

Webbridge용 SSO 아카이브 ZIP 파일을 생성합니다.

이 컨피그레이션은 지원되는 도메인, 인증 매핑 등에 대한 SSO 컨피그레이션의 유효성을 검사하기 위해 Webbridge에서 참조하는 컨피그레이션입니다. 컨피그레이션의 이 부분에 대해 다음 규칙을 고려해야 합니다.

- ZIP 파일은 파일 이름 앞에 sso_가 붙은 상태로 시작해야 합니다(예: sso_cmstest.zip).
- 이 파일이 업로드되면 Webbridge는 기본 인증을 비활성화하며, 업로드된 Webbridge에는 SSO만 사용할 수 있습니다.
- ID 제공자가 여러 개 사용되는 경우 별도의 ZIP 파일을 다른 명명 스키마로 업로드해야 합니다.

다(sso_가 접두사로 추가됨).

- zip 파일을 만들 때는 파일 내용을 강조 표시하고 압축해야 하며 필요한 파일을 폴더에 넣고 해당 폴더를 압축하지 마십시오.

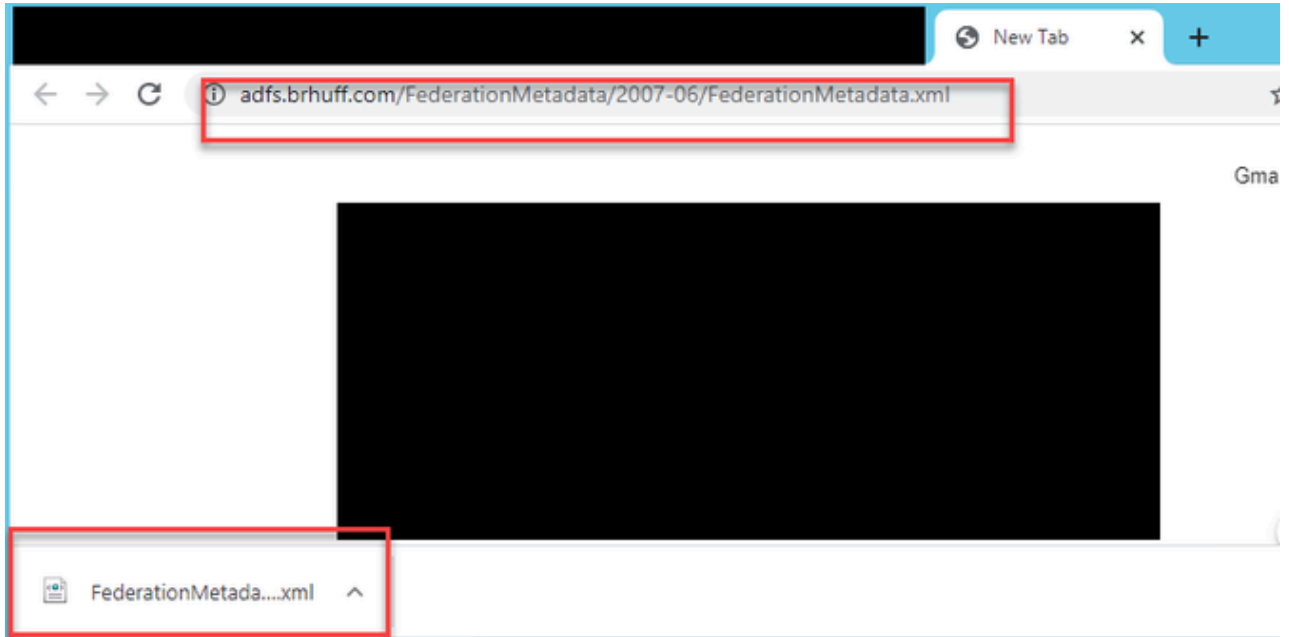
zip 파일의 내용은 암호화 사용 여부에 따라 2~4개의 파일로 구성됩니다.

파일 이름	설명	필수 ?
idp_config.xml	idP가 수집할 수 있는 메타데이터 파일입니다. AD FS에서는 <a href="https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml">https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml 으로 이동하여 찾을 수 있습니다 .	예
config.json	Webbridge에서 지원되는 도메인, SSO에 대한 인증 매핑의 유효성을 검사하는 데 사용하는 JSON 파일입니다.	예
sso_sign.key	ID 공급자에 구성된 공개 서명 키에 대한 개인 키입니다. 서명된 데이터를 보호하는 데만 필요	아니요
sso_encrypt.key	ID 공급자에 구성된 공개 암호화 키에 대한 개인 키입니다. 암호화된 데이터의 보안에만 필요	아니요

idp_config.xml 가져오기 및 구성

1. AD FS 서버(또는 AD FS에 액세스할 수 있는 위치)에서 웹 브라우저를 엽니다.

2. 웹 브라우저에서 URL <https://<ADFSFQDN>/FederationMetadata/2007-06/FederationMetadata.xml>을 입력합니다(ADFS 서버에 로컬로 있는 경우 FQDN 대신 localhost를 사용할 수도 있습니다). FederationMetadata.xml 파일을 다운로드합니다.



3. 다운로드한 파일을 zip 파일이 생성되는 위치에 복사하고 이름을 idp_config.xml로 바꿉니다.

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

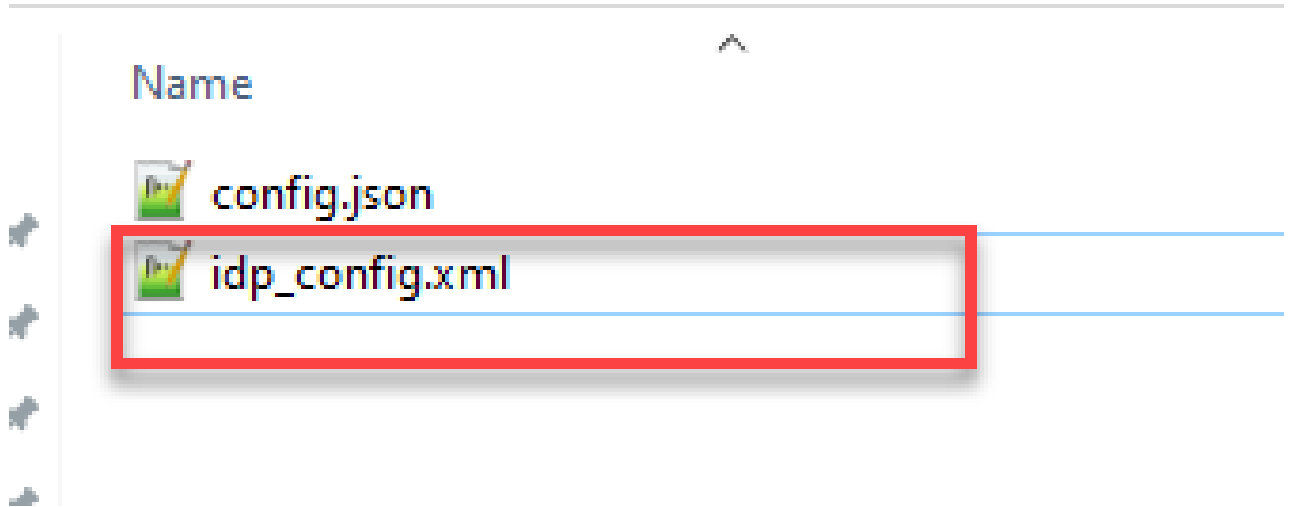
Copy

Create shortcut

Delete

Rename

Properties



내용으로 config.json 파일 만들기

config.json에는 다음 3개의 특성이 있으며 이 특성은 대괄호 안에 포함되어야 합니다.

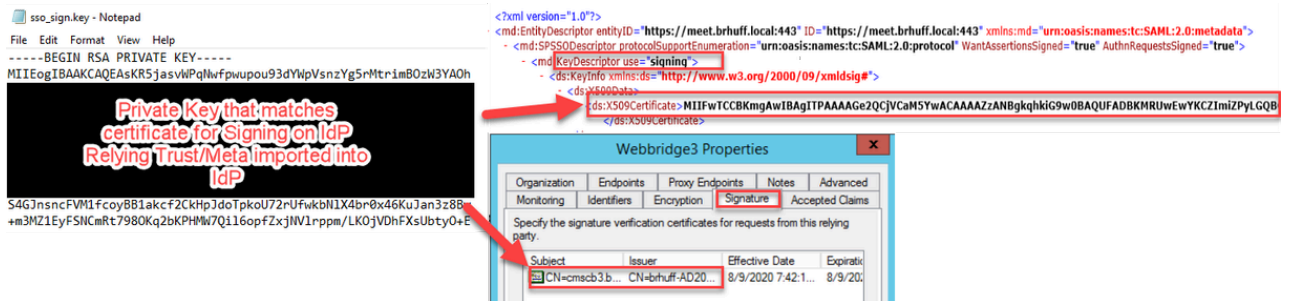
1. supportedDomains - IdP에 대해 SSO 인증을 위해 선택된 도메인 목록입니다. 여러 도메인은 쉼표로 구분할 수 있습니다.
2. authenticationIdMapping - ADFS/IdP에서 발신 클레임 규칙의 일부로 다시 전달되는 매개 변수입니다. 이 값은 IdP에서 나가는 클레임 유형의 이름 값과 일치해야 합니다. 클레임 규칙
3. ssoServiceProviderAddress - ID 공급자가 SAML 응답을 보내는 FQDN URL입니다. Webbridge FQDN이어야 합니다.

sso_sign.key 설정(선택 사항)

이 파일에는 IdP로 가져온 Webbridge 메타데이터에서 서명하는 데 사용되는 인증서의 개인 키가 포함되어야 합니다. 서명에 사용되는 인증서는 AD FS에서 Webbridge 메타데이터를 가져오는 동안 X509Certificate에 <KeyDescriptor use=signing> 섹션 아래의 인증서 정보를 입력하여 설정할 수 있습니다. 또한 Webbridge Relying Trust Party(Webbridge 신뢰 당사자)의 AD FS에서 Properties(속성) > Signature(서명)에서 보고 가져올 수도 있습니다.

다음 예에서는 ADFS로 가져오기 전에 Webbridge 메타데이터에 추가된 callbridge 인증서 (CN=cmscb3.brhuff.local)를 볼 수 있습니다. sso_sign.key에 삽입된 개인 키는 cmscb3.brhuff.local 인증서와 일치하는 키입니다.

이는 선택적인 컨피그레이션이며 SAML 응답을 암호화하려는 경우에만 필요합니다.

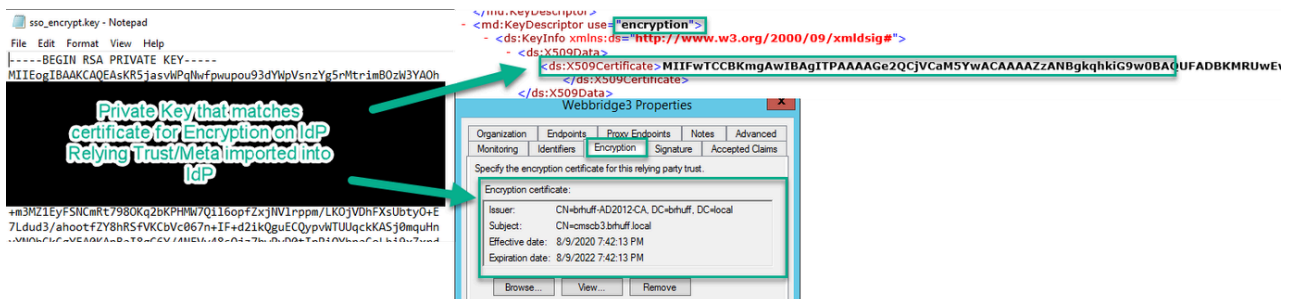


sso_encrypt.key 설정(선택 사항)

이 파일은 IdP로 가져온 webbridge 메타데이터에서 암호화에 사용된 인증서의 개인 키를 포함해야 합니다. 암호화에 사용되는 인증서는 AD FS에서 Webbridge 메타데이터를 가져오는 동안 X509Certificate에 <KeyDescriptor use=encryption> 섹션 아래의 인증서 정보를 입력하여 설정할 수 있습니다. 또한 Webbridge Relying Trust Party(Webbridge 신뢰 당사자)의 AD FS에서 Properties(속성) > Encryption(암호화)에서 보거나 가져올 수도 있습니다.

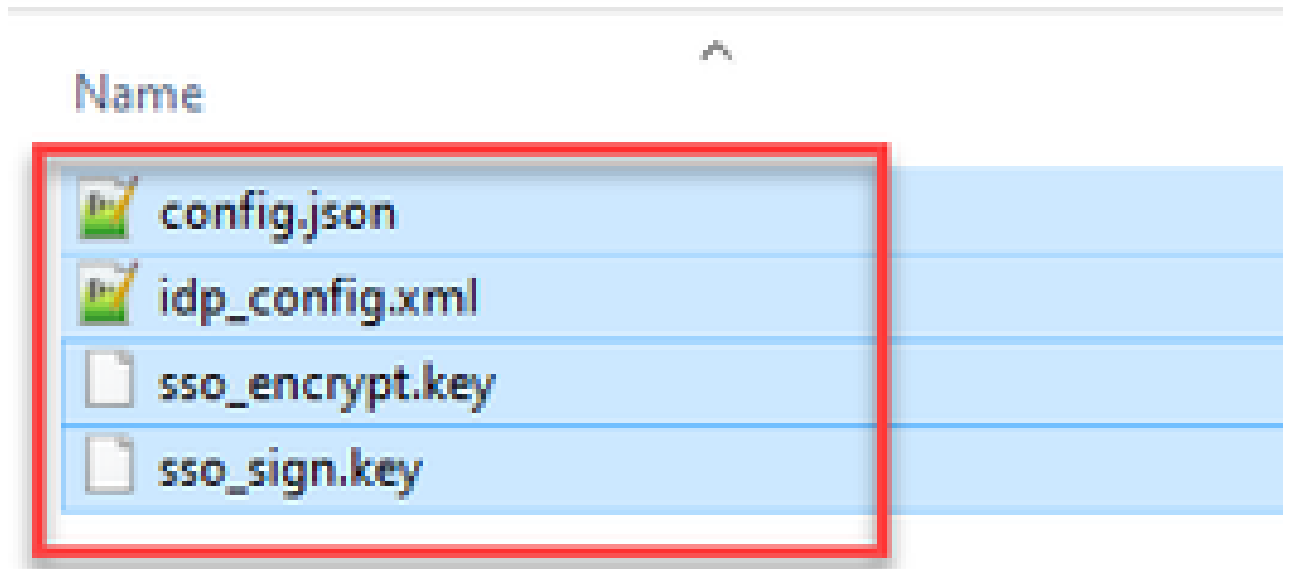
다음 예에서는 ADFS로 가져오기 전에 Webbridge 메타데이터에 추가된 callbridge 인증서 (CN=cmscb3.brhuff.local)를 볼 수 있습니다. 'sso_encrypt.key'에 삽입된 개인 키는 cmscb3.brhuff.local 인증서와 일치하는 것입니다.

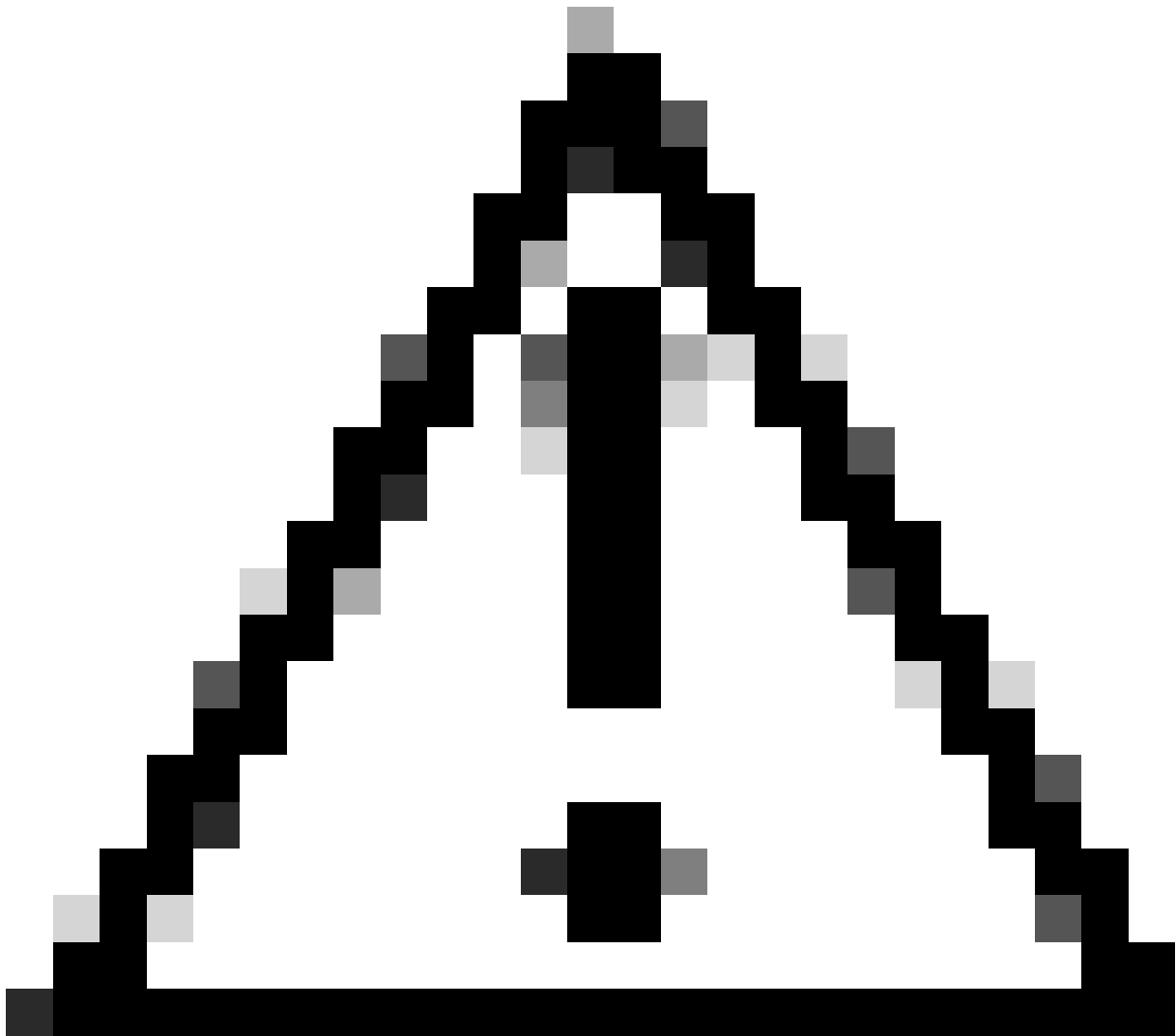
이는 선택적인 컨피그레이션이며 SAML 응답을 암호화하려는 경우에만 필요합니다.



SSO ZIP 파일 생성

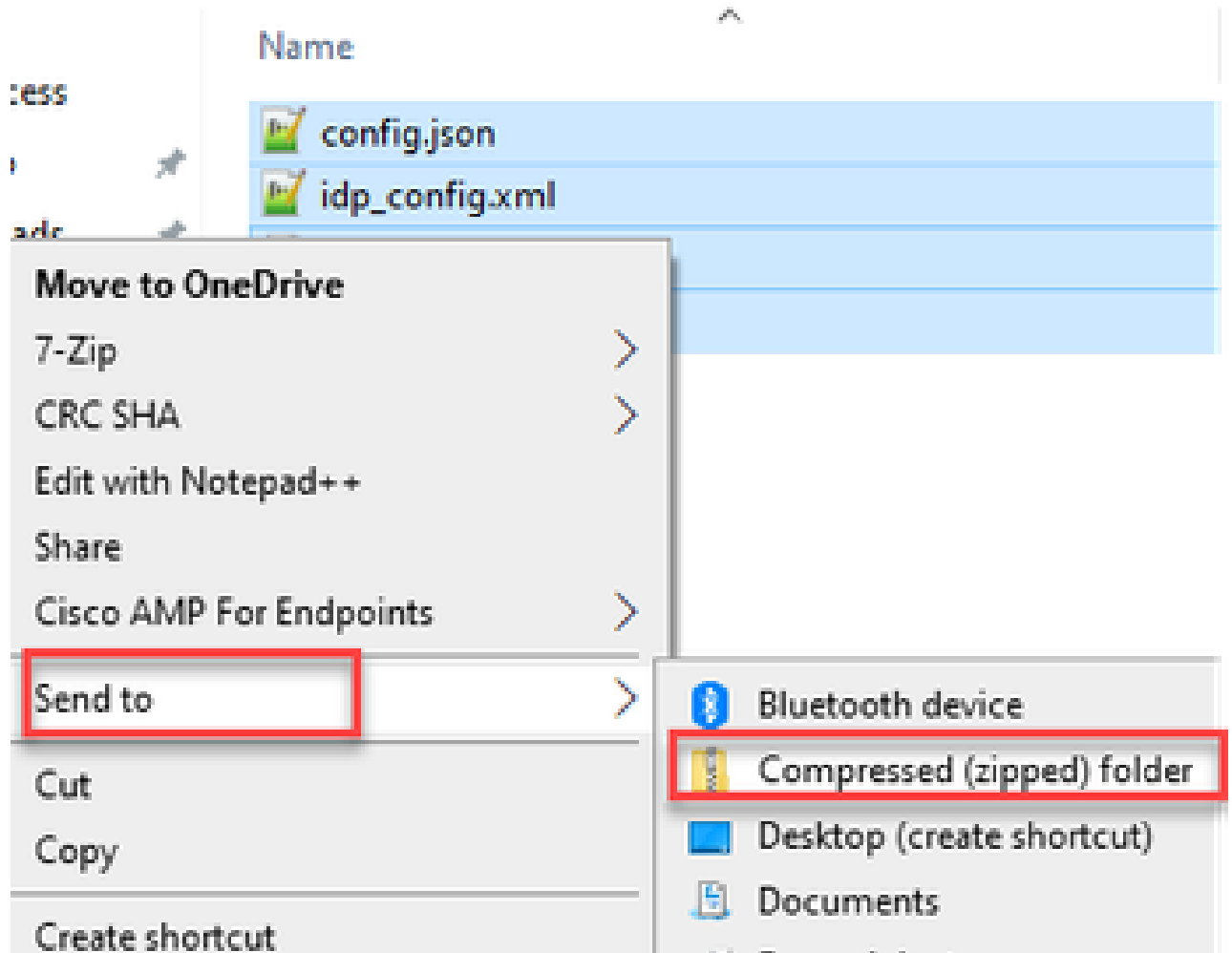
1. SSO 구성 파일에 사용할 모든 파일을 강조 표시합니다.



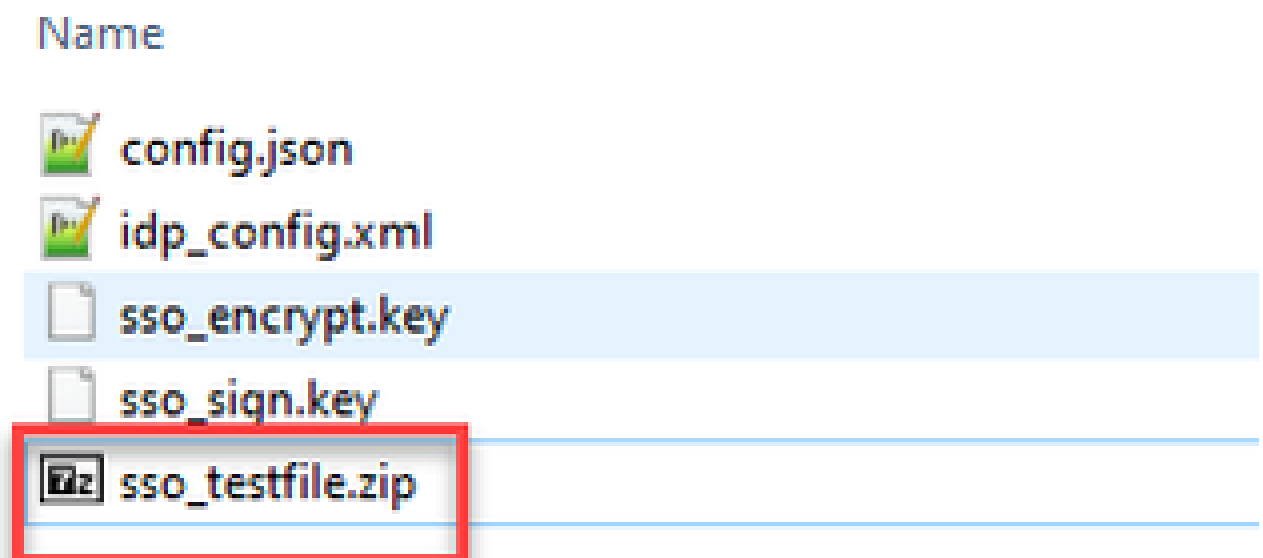


주의: SSO가 작동하지 않으므로 파일이 포함된 폴더를 압축하지 마십시오.

2. 강조 표시된 파일을 마우스 오른쪽 버튼으로 클릭하고 Send to(보내기) > Compressed (zipped)(압축(압축)) 폴더를 선택합니다.



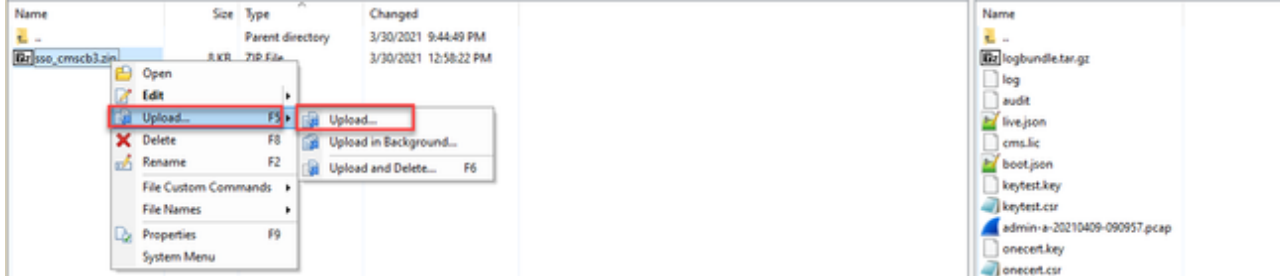
3. 파일이 압축되면 sso_prefix를 사용하여 원하는 이름으로 이름을 바꿉니다.



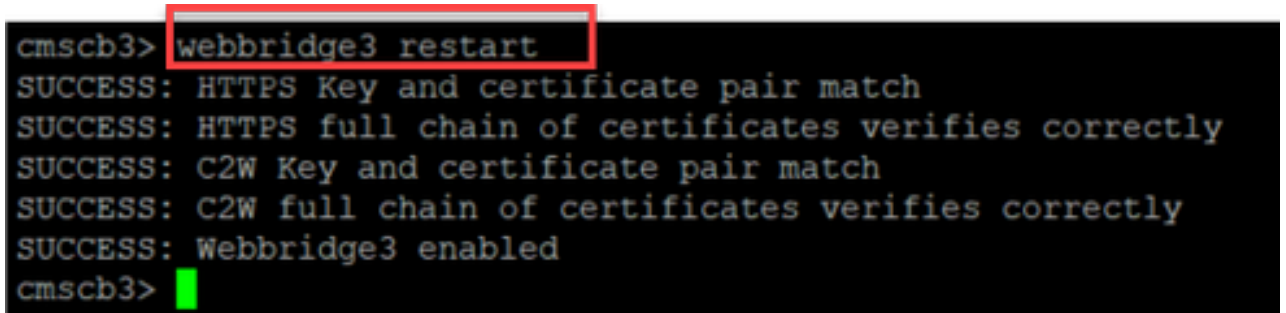
Webbridge에 SSO Zip 파일 업로드

SFTP/SCP 클라이언트를 열고(이 예에서는 WinSCP가 사용 중) Webbridge3를 호스팅하는 서버에 연결합니다.

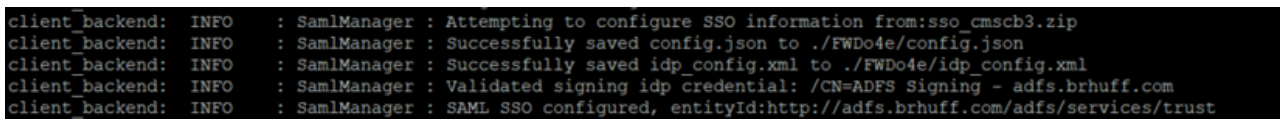
1. 왼쪽 창에서 SSO Zip 파일이 있는 위치로 이동한 다음 마우스 오른쪽 버튼으로 Select upload(업로드 선택)를 클릭하거나 파일을 끌어서 놓습니다.



2. 파일이 Webbridge3 서버에 완전히 업로드되면 SSH 세션을 열고 webbridge3 restart 명령을 실행합니다.



3. syslog에서 다음 메시지는 SSO가 성공적으로 활성화되었음을 나타냅니다.



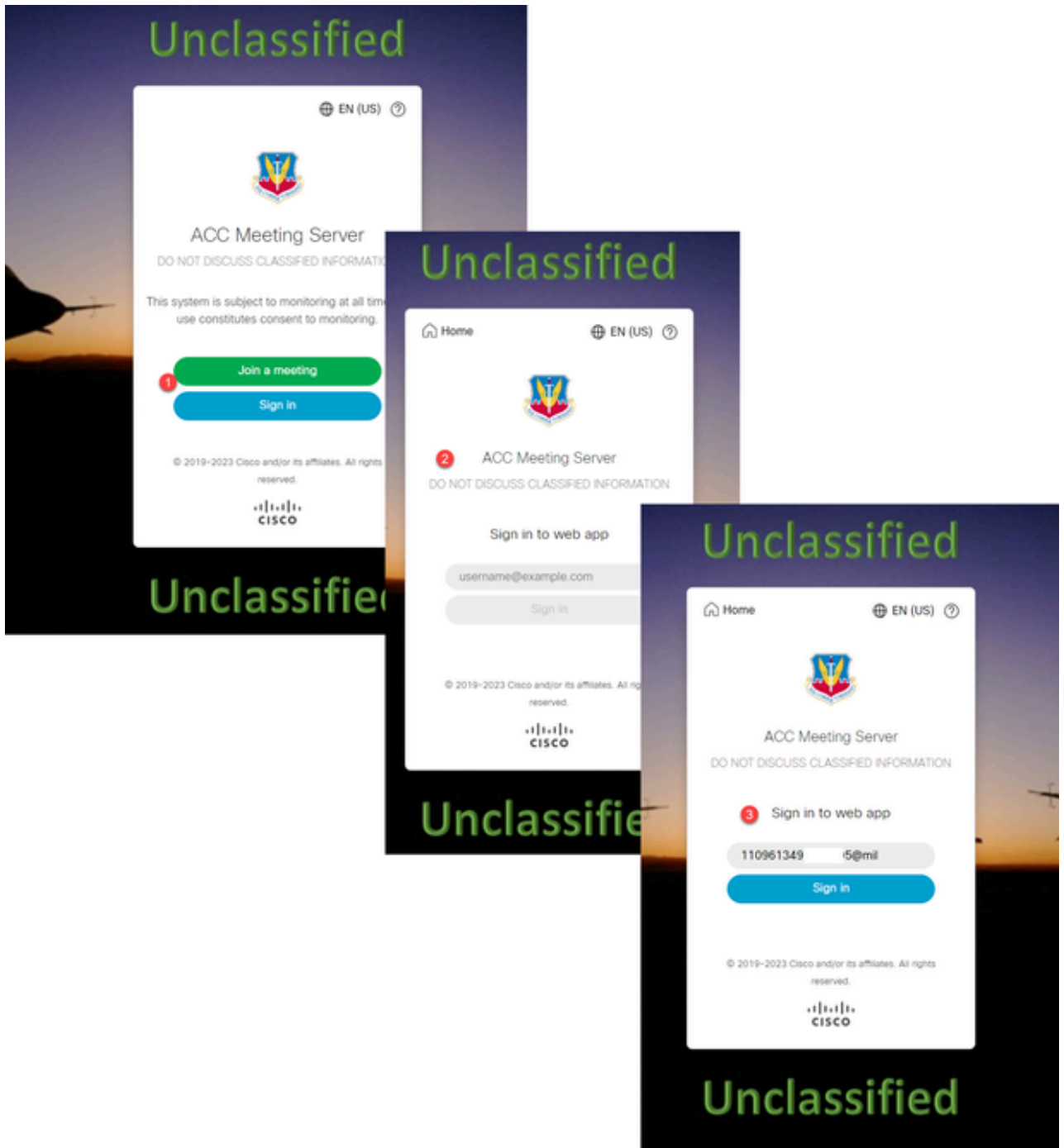
CAC(Common Access Card)

CAC(Common Access Card)는 현역 군인, DoD 민간인 직원, 적격 계약직 직원의 표준 ID 역할을 하는 스마트 카드입니다.

CAC 카드를 사용하는 사용자의 전체 로그인 프로세스는 다음과 같습니다.

1. PC를 켜고 CAC 카드를 고정합니다.
2. 로그인(인증서를 가끔 선택)하고 Pin을 입력합니다.
3. 브라우저 열기
4. 참가 URL로 이동하여 회의 참가 또는 로그인 옵션을 확인합니다
5. 로그인: jidMapping으로 구성된 사용자 이름을 입력합니다. 그러면 CAC 로그인에 Active Directory가 필요합니다.

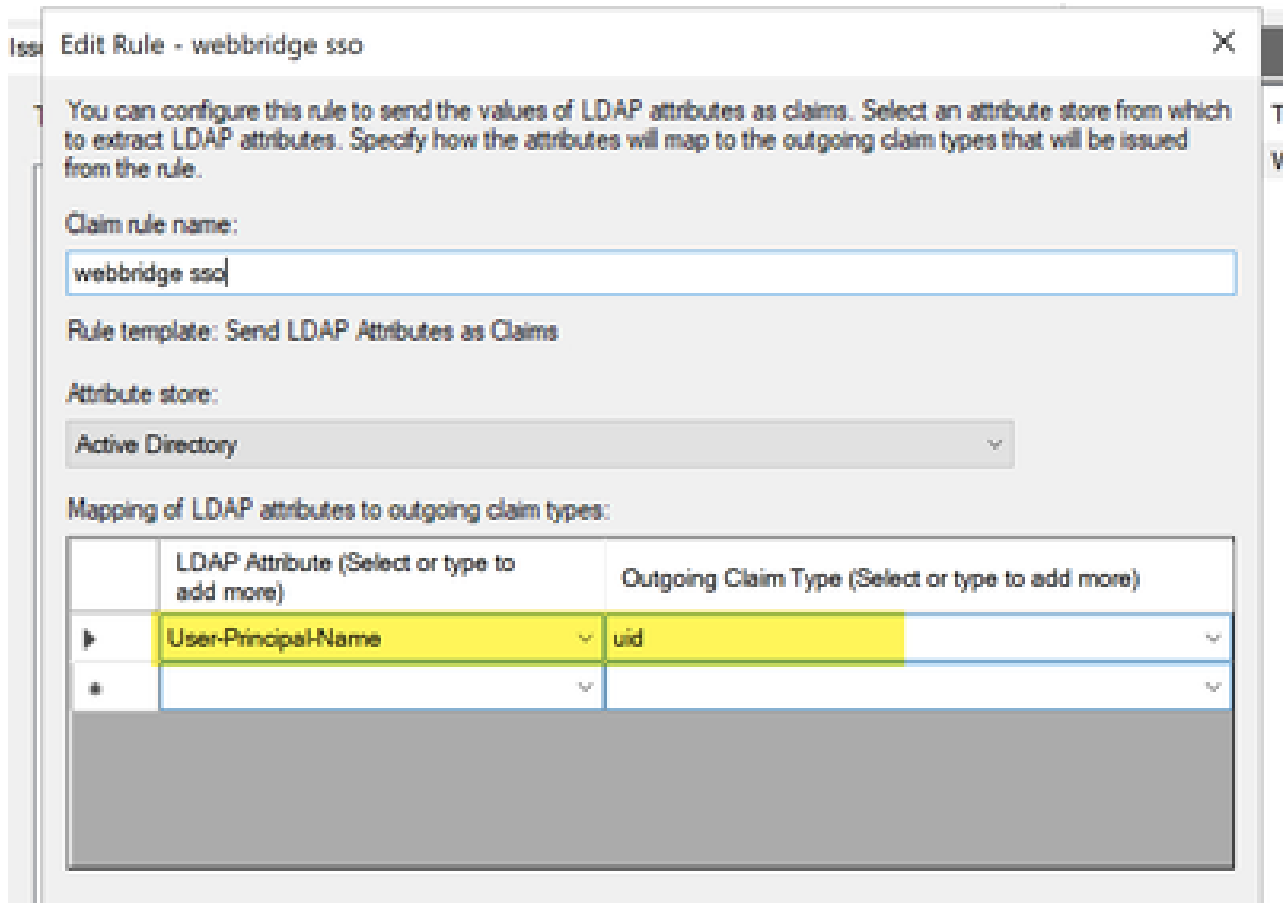
6. 방문 로그인
7. AD FS 페이지가 잠깐 나타나며 자동으로 채워집니다.
8. 사용자가 이 시점에 로그인됩니다.



Ldapmapping에서 jidMapping(사용자 로그인 이름)을 AD FS가 CAC 카드에 사용하는 것과 동일하게 구성합니다. \$userPrincipalName\$예(대/소문자 구분)

또한 AD FS의 클레임 규칙에서 사용되는 특성과 일치하도록 authenticationIdMapping에 대해 동일한 LDAP 특성을 설정합니다.

여기서 클레임 규칙은 \$userPrincipalName\$을(를) UID로 CMS에 다시 전송한다는 것을 보여줍니다.



WebApp을 통해 SSO 로그인 테스트

이제 SSO가 구성되었으므로 서버를 테스트할 수 있습니다.

1. 웹 앱의 Webbridge URL로 이동하고 Sign in(로그인) 버튼을 선택합니다.



Cisco Meeting Server

web app

Join meetings, anywhere, anytime

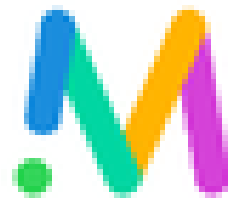
Join a meeting

Sign in

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



2. 사용자에게 사용자 이름을 입력할 수 있는 옵션이 표시됩니다(이 페이지에는 비밀번호 옵션이 없습니다).



Cisco Meeting Server

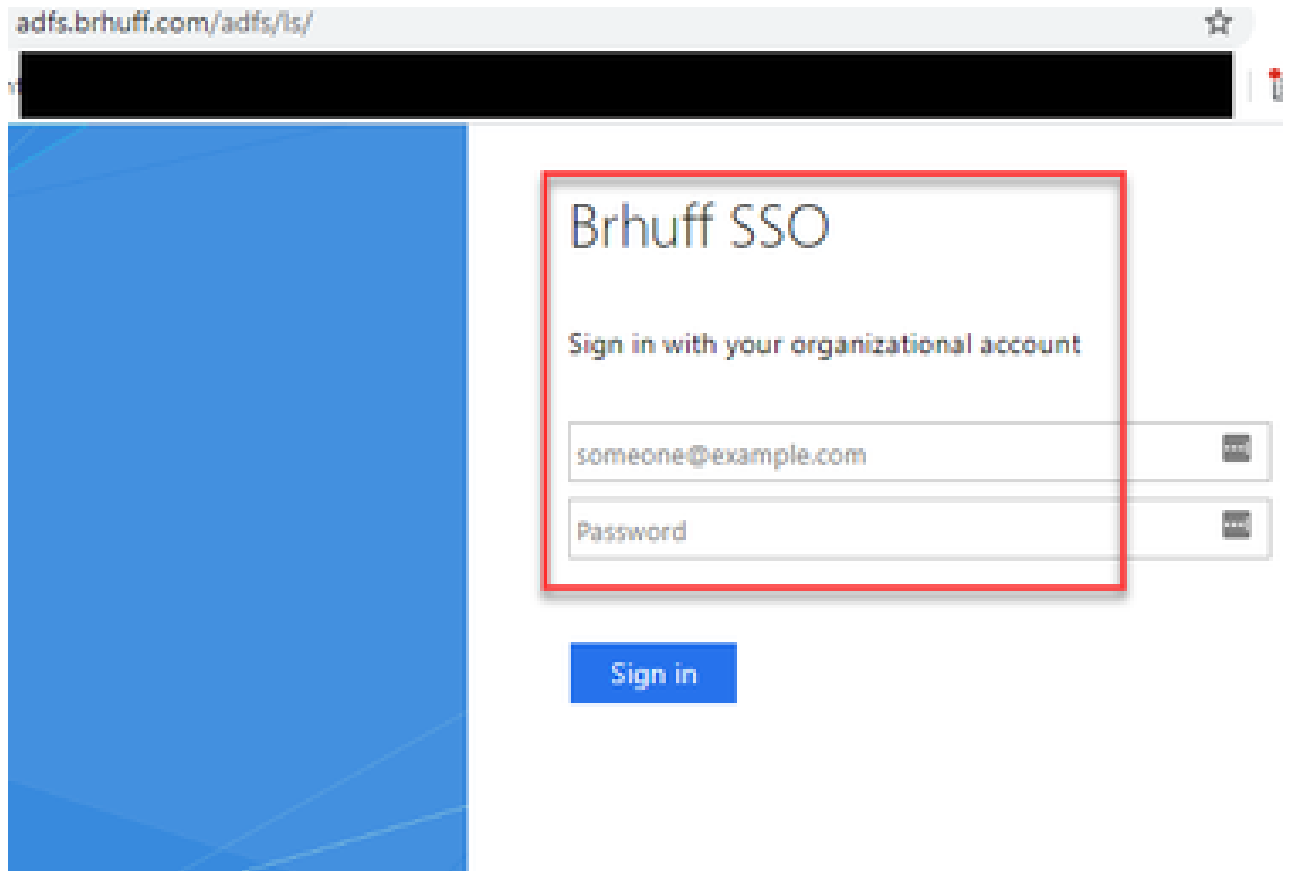
web app

Sign in to web app

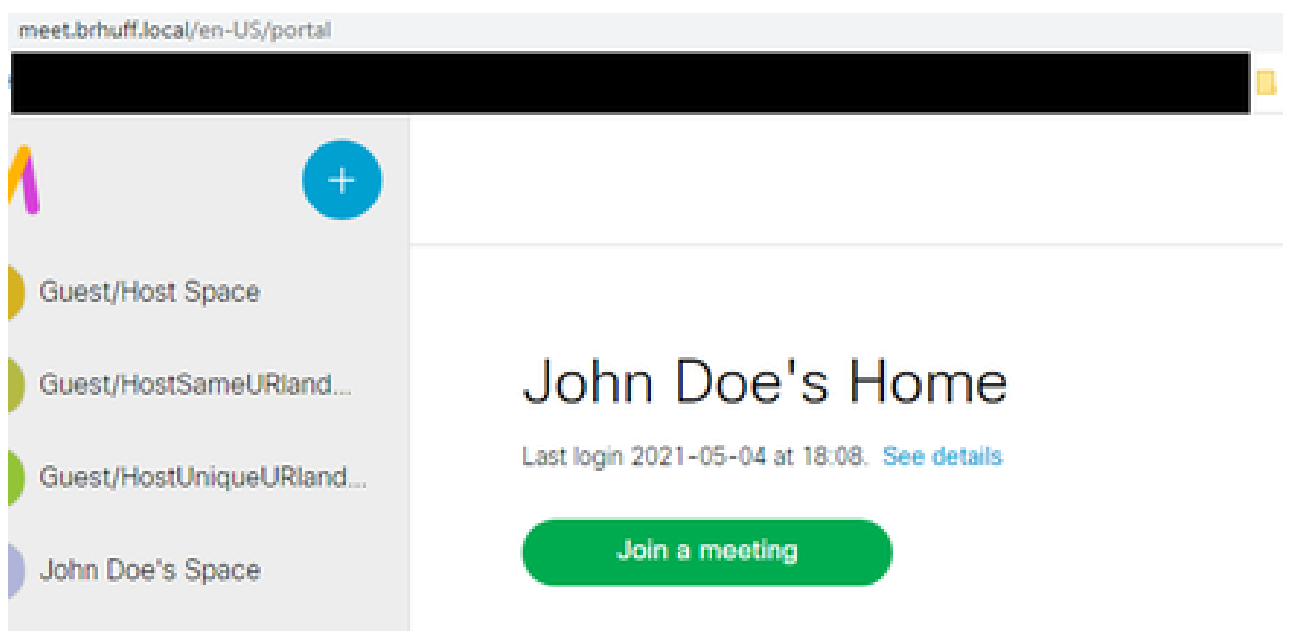
© 2020 Cisco and/or its affiliates. All rights reserved.



3. 그런 다음 사용자는 AD FS 페이지로 리디렉션됩니다(사용자 세부 정보를 입력한 후). 여기서 사용자는 IdP에 인증하기 위해 자격 증명을 입력해야 합니다.



4. 사용자가 IdP로 자격 증명을 입력하고 확인한 후 토큰으로 리디렉션되어 Web App 홈 페이지에 액세스합니다.



문제 해결

기본 문제 해결

SSO 문제의 기본 문제 해결:

1. IdP에서 Relying Trust로 가져오는 데 사용되는 Webbridge3에 대해 구성된 메타데이터가 올바르게 구성되어 있고, 구성된 URL이 config.json의 ssoServiceProviderAddress와 정확히 일치하는지 확인하십시오.
2. IdP에서 제공하고 Webbridge3 sso 구성 파일에 압축된 메타데이터가 IdP의 최신 버전인지 확인합니다. 서버 호스트 이름, 인증서 등이 변경된 경우 메타데이터를 다시 내보내고 구성 파일에 압축해야 합니다.
3. 서명 및 개인 키 암호화를 사용하여 데이터를 암호화하는 경우, 올바른 일치 키가 webbridge에 업로드한 sso_xxxx.zip 파일의 일부인지 확인합니다. 가능한 경우 선택적 개인 키 없이 테스트하여 이 암호화된 옵션 없이 SSO가 작동하는지 확인합니다.
4. config.json이 SSO 도메인, Webbridge3 URL 및 SAMLResponse에서 일치할 것으로 예상되는 인증 매핑에 대한 올바른 세부사항으로 구성되어 있는지 확인합니다.

로그 관점에서 문제 해결을 시도하는 것도 이상적입니다.

1. Webbridge URL로 이동할 때 URL의 끝에 ?trace=true를 입력하여 CMS syslog에서 자세한 로깅을 활성화합니다. (예: <https://join.example.com/en-US/home?trace=true>).
2. Webbridge3 서버에서 syslog 팔로우를 실행하여 테스트 중에 라이브 메시지를 캡처하거나 URL에 trace 옵션이 추가된 상태로 테스트를 실행하고 Webbridge3 및 CMS Callbridge 서버에서 logbundle.tar.gz를 수집합니다. webbridge와 callbridge가 동일한 서버에 있는 경우 단일 logbundle.tar.gz 파일만 필요합니다.

Microsoft ADFS 오류 코드

SSO 프로세스에 오류가 발생할 경우 IdP 컨피그레이션 또는 IdP와의 통신에 오류가 발생할 수 있습니다. ADFS를 사용하는 경우 다음 링크를 검토하여 장애가 발생했음을 확인하고 교정 작업을 수행하는 것이 좋습니다.

[Microsoft 상태 코드](#)

예를 들면 다음과 같습니다.

client_backend: 오류: SamlManager: SAML 인증 요청_e135ca12-4b87-4443-abe1-

30d396590d58이 실패했습니다. 이유: urn:oasis:names:tc:SAML:2.0:status:Responder

이 오류는 이전 설명서에 따라 IdP 또는 ADFS로 인해 오류가 발생하여 ADFS 관리자가 해결해야 함을 나타냅니다.

인증 ID를 가져오지 못했습니다.

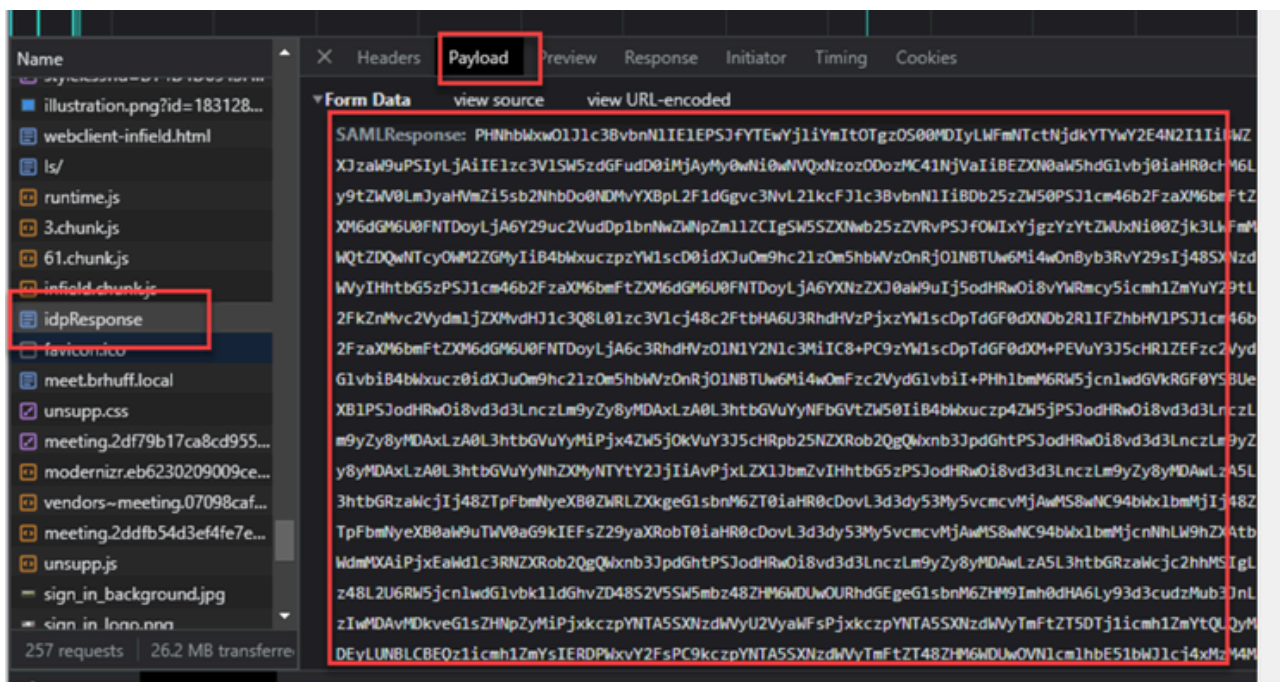
IdP에서 다시 SAMLResponse를 교환하는 동안 Webbridge가 SSO를 통한 로그인에 실패하여 로그에 이 오류 메시지를 표시할 수 있는 경우가 있습니다.

client_backend: 정보: SamlManager: [57dff9e3-862e-4002-b4fa-683e4aa6922c]
authenticationId를 가져오지 못했습니다.

이는 인증 교환 중에 IdP에서 다시 전달된 SAMLResponse 데이터를 검토할 때 Webbridge3가 authenticationId에 대한 config.json과 비교하여 응답에서 유효한 일치 특성을 찾지 못했음을 나타냅니다.

통신이 서명 및 암호화 개인 키를 사용하여 암호화되지 않은 경우 웹 브라우저를 통해 Developer Tools Network Logging에서 SAML 응답을 추출하고 base64를 사용하여 디코딩할 수 있습니다. 응답이 암호화된 경우 IdP 측에서 해독된 SAML 응답을 요청할 수 있습니다.

HAR 데이터라고도 하는 개발자 도구 네트워크 로깅 출력에서 이름 열 아래의 idpResponse를 찾고 Payload를 선택하여 SAML 응답을 확인합니다. 이전에 언급된 바와 같이, 이것은 base64 디코더를 사용하여 디코딩될 수 있다.



SAMLResponse 데이터를 수신할 때 <AttributeStatement>의 섹션을 확인하여 다시 전송된 특성 이름을 찾고 이 섹션 내에서 IdP에서 구성 및 전송된 클레임 유형을 찾을 수 있습니다. 예를 들면 다음

과 같습니다.

```
<특성문>
<Attribute Name="<commonname의 URL">
<AttributeValue>testuser1</AttributeValue>
</Attribute>
<Attribute Name="<NameID의 URL">
<AttributeValue>testuser1</AttributeValue>
</Attribute>
<Attribute Name="uid">
<AttributeValue>testuser1</AttributeValue>
</Attribute>
</AttributeStatement>
```

이전 이름을 검토하면 Attribute Statement 섹션에서 <AttributeName>을 확인하고 각 값을 SSO config.json의 authenticationIdMapping 섹션에 설정된 값과 비교할 수 있습니다.

앞의 예에서 authenticationIdMapping의 컨피그레이션이 전달된 것과 정확하게 일치하지 않으므로 일치하는 authenticationId를 찾지 못하는 것을 볼 수 있습니다.

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

이 문제를 해결하기 위해 두 가지 방법을 사용할 수 있습니다.

1. IdP 발신 클레임 규칙은 Webbridge3에 있는 config.json의 authenticationIdMapping에서 구성된 것과 정확히 일치하는 클레임을 포함하도록 업데이트할 수 있습니다. (클레임 규칙이 IdP for <http://example.com/claims/NameID>에 [추가됨](#))
또는
2. Webbridge3에서 config.json을 업데이트하여 IdP에 구성된 발신 클레임 규칙 중 하나로 구성된 것과 정확히 일치하는 'authenticationIdMapping'을 가질 수 있습니다. (즉, "uid", "<URL>/NameID" 또는 "<URL>/CommonName"과 같은 특성 이름 중 하나와 일치하도록 업데이트해야 하는 'authenticationIdMapping'입니다. (정확히) Callbridge API에 구성된 예상 값(통과 시)과 일치하는 경우

유효성 검사에서 통과/일치하는 어설션이 없습니다.

IdP에서 SAMLResponse를 교환하는 동안 Webbridge는 어설션 일치에 오류가 있음을 나타내는 이 오류를 표시하고 서버 컨피그레이션과 일치하지 않는 어설션을 건너뛵니다.

```
client_backend: 오류: SamlManager: 검증을 통과한 어설션이 없습니다.
client_backend: INFO: SamlManager: 허용된 대상에서만 어설션 건너뛰기
```

이 오류는 IdP에서 SAMLResponse를 검토할 때 Webbridge가 일치하는 어설션을 찾지 못하여 일치하지 않는 실패를 건너뛰었고 결국 실패한 SSO 로그인이 발생했음을 나타냅니다.

이 문제를 찾으려면 IdP에서 SAMLResponse를 검토하는 것이 좋습니다. 통신이 서명 및 암호화 개인 키를 사용하여 암호화되지 않은 경우, 웹 브라우저를 통해 Developer Tools Network Logging에서 SAML 응답을 추출하고 base64를 사용하여 디코딩할 수 있습니다. 응답이 암호화된 경우 IdP 측에서 해독된 SAML 응답을 요청할 수 있습니다.

SAMLResponse 데이터를 검토할 때 응답의 <AudienceRestriction> 섹션을 보면 이 응답이 다음에 대해 제한되는 모든 대상을 찾을 수 있습니다.

```
<Conditions NotBefore=2021-03-30T19:35:37.071Z NotOnOrAfter=2021-03-30T19:36:37.071Z>  
<대상 그룹 제한>  
<Audience>https://cisco.example.com</Audience>  
</AudienceRestrict>  
</조건>
```

<Audience> 섹션(<https://cisco.example.com>)의 값을 사용하여 Webbridge 컨피그레이션의 config.json의 ssoServiceProviderAddress와 비교하고 정확하게 일치하는지 확인할 수 있습니다. 이 예에서 장애가 발생한 이유는 청중이 컨피그레이션의 서비스 공급자 주소와 일치하지 않기 때문이며, 여기에 :443이 추가되어 있습니다.

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

이렇게 하면 이러한 오류가 발생하지 않도록 이러한 두 항목이 정확하게 일치해야 합니다. 이 예에서는 다음 두 방법 중 하나를 수정해야 합니다.

1. config.json의 ssoServiceProviderAddress 섹션에 있는 주소에서 :443을 제거하여 IdP의 SAMLResponse에 제공된 Audience 필드와 일치시킬 수 있습니다.
또는
2. IdP의 Webbridge3에 대한 메타데이터 또는 신뢰 당사자는 URL에 :443이 추가되도록 업데이트할 수 있습니다. 메타데이터가 업데이트되면 AD FS의 신뢰 당사자로 다시 가져와야 합니다. 그러나 IdP 마법사에서 직접 Relying Trust Party를 수정할 경우 다시 가져올 필요가 없습니다.

웹 앱에서 로그인하지 못했습니다.



Blahman Industries

Blahman WebApp

Sign in to web app

darmckin@brhuff.com

Sign in

 Sign in failed

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



user.info cmscb3-1 client_backend: INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] SAML 토큰 요청에서 SSO sso_2024.zip과 일치함

3월 19일 10:47:07.927 user.info cmscb3-1 client_backend: INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] SAML 토큰 요청에서 SSO를 찾는 중입니다.

3월 19일 10:47:07.930 user.info cmscb3-1 client_backend: 정보: SamlManager: [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] SAML 토큰을 생성했습니다.

시나리오 2:

사용자가 webbridge 로그인 페이지의 SSO zip 파일에 없는 도메인을 사용하여 로그인하려고 했습니다. 클라이언트는 사용자가 입력한 사용자 이름의 페이로드와 함께 tokenRequest를 전송합니다. Webbridge는 로그인 시도를 즉시 중지합니다.

CMS Webbridge 추적(반면 ?trace=true가 사용됨)

3월 18일 14:54:52.698 user.err cmscb3-1 client_backend: 오류: SamlManager: 잘못된 SSO 로그인 시도

3월 18일 14:54:52.698 user.info cmscb3-1 client_backend: 정보: SamlManager: [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] SAML 토큰 요청에서 SSO를 찾지 못했습니다.

3월 18일 14:54:52.698 user.info cmscb3-1 client_backend: 정보: SamlManager: [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] SAML 토큰 요청에서 SSO를 찾는 중입니다.

시나리오 3:

사용자가 올바른 사용자 이름을 입력했으며 SSO 로그인 페이지가 표시됩니다. 사용자가 여기에도 올바른 사용자 이름과 암호를 입력하지만 여전히 로그인 실패

CMS Webbridge 추적(반면 ?trace=true가 사용됨)

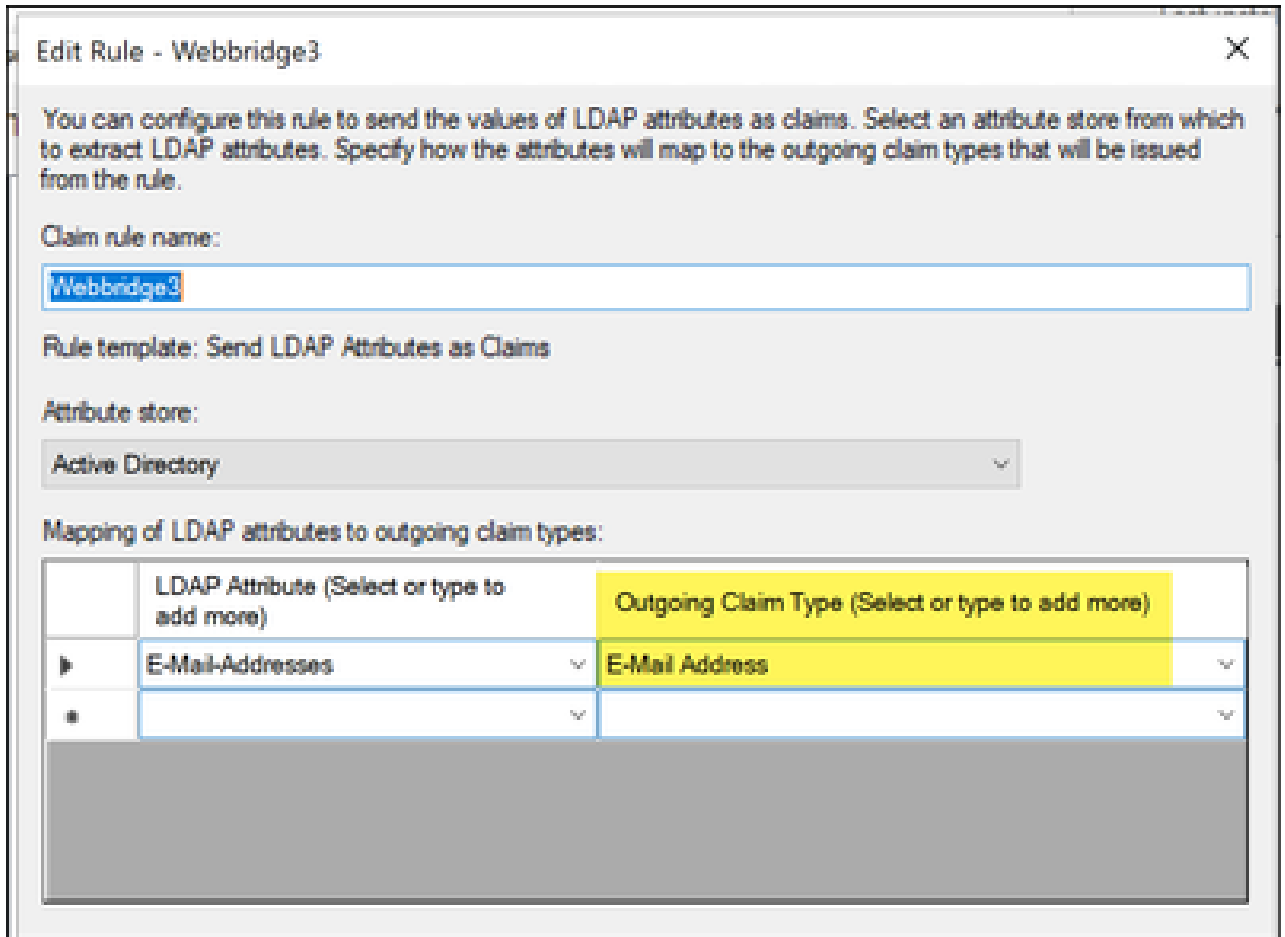
3월 19일 16:39:17.714 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] SAML 토큰 요청에서 SSO sso_2024.zip과 일치

3월 19일 16:39:17.714 user.info cmscb3-1 client_backend: 정보: SamlManager: [ef8fe67f-685c-4a81-9240-f76239379806] SAML IDP 응답에서 SSO를 찾는 중입니다.

3월 19일 16:39:17.720 user.err cmscb3-1 client_backend: 오류: SamlManager: 서명된 SAML 어설션에서 authenticationId 매핑된 요소를 찾을 수 없습니다.

3월 19일 16:39:17.720 user.info cmscb3-1 client_backend: 정보: SamlManager: [ef8fe67f-685c-4a81-9240-f76239379806] 인증 ID를 가져오지 못했습니다.

시나리오 3의 원인은 IdP의 클레임 규칙이 webbridge에 업로드된 SSO zip 파일에 사용된 config.json 파일의 authenticationIdMapping과 일치하지 않는 클레임 유형을 사용했기 때문입니다. Webbridge에서 SAML 응답을 확인하고 있으며, config.json에 구성된 것과 일치하는 특성 이름이 필요합니다.



AD FS의 클레임 규칙



config.json 예

사용자 이름을 인식할 수 없습니다.

시나리오 1:

사용자가 잘못된 사용자 이름으로 로그인했습니다(도메인이 webbridge3에 업로드된 sso zip 파일의 내용과 일치하지만 사용자가 존재하지 않음).



Blahman Industries

Blahman WebApp

Sign in to web app

steve@brhuff.com

Sign in

 Username is not recognized

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



user.info cmscb3-1 client_backend: INFO : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] SAML 토큰 요청에서 SSO sso_2024.zip과 일치

3월 18일 14:58:47.777 user.info cmscb3-1 client_backend: INFO : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] SAML 토큰 요청에서 SSO를 찾는 중입니다.

3월 18일 14:58:47.780 user.info cmscb3-1 client_backend: 정보: SamlManager: [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] SAML 토큰을 생성했습니다.

3월 18일 14:58:48.072 user.info cmscb3-1 client_backend: INFO : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] SAML 토큰 요청에서 SSO_2024.zip과 일치

3월 18일 14:58:48.072 user.info cmscb3-1 client_backend: INFO : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] SAML IDP 응답에서 SSO를 찾는 중입니다.

3월 18일 14:58:48.077 user.info cmscb3-1 client_backend: INFO : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] 인증 ID: darmckin@brhuff.com을 성공적으로 가져왔습니다.

3월 18일 14:58:48.078 user.info cmscb3-1 host:server: INFO : WB3Cmgr: [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c-0272-42a1-b125-136fdf5612a5 (user=steve@brhuff.com)

3월 18일 14:58:48.092 user.info cmscb3-1 host:server: INFO: 권한 부여를 위한 사용자를 찾을 수 없음

3월 18일 14:58:48.092 user.info cmscb3-1 host:server: INFO: steve@brhuff.com에서 로그인 요청이 실패했습니다.

시나리오 2:

사용자가 웹 앱에 올바른 로그인 정보를 입력했으며 SSO 페이지에서 LDAP를 인증하기 위한 올바른 자격 증명을 입력했지만 사용자 이름이 인식되지 않아 로그인하지 못했습니다.



Blahman Industries

Blahman WebApp

Sign in to web app

darmckin@brhuff.com

Sign in

 Username is not recognized

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



user.info cmscb3-1 host:server: INFO : 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)

3월 18일 15:08:52.399 user.warning cmscb3-1 host:server: WARNING : 사용자 'darmckin@brhuff.com'의 로그인 시도 거부 — authenticationId가 잘못되었습니다.

3월 18일 15:08:52.412 user.info cmscb3-1 host:server: INFO: darmckin@brhuff.com에서 로그인 요청이 실패했습니다.

CMS ldapmapping의 AuthenticationIdMapping이 ADFS의 클레임 규칙에 사용된 구성된 LDAP 특성과 일치하지 않습니다. 아래 줄 "인증 ID:darmckin@brhuff.com을 가져옴"은 ADFS가 Active Directory에서 darmckin@brhuff.com을 가져오는 특성으로 구성된 클레임 규칙을 가지고 있지만 CMS API > Users의 AuthenticationID에 darmckin이 예상된다는 것을 나타냅니다. CMS ldapMappings에서 AuthenticationID는 \$sAMAccountName\$(으)로 구성되지만 AD FS의 클레임 규칙은 이메일 주소를 전송하도록 구성되어 있으므로 일치하지 않습니다.

해결 방법:

다음 중 하나를 수행합니다.

1. CMS ldapmapping에서 AuthenticationID를 변경하여 AD FS의 클레임 규칙에서 사용되는 것과 일치시키고 새 동기화를 수행합니다.
2. ADFS 클레임 규칙에 사용된 LDAP 특성을 CMS ldapmapping에 구성된 것과 일치하도록 변경

Related objects: </api/v1/ldapMappings>

Table view XML view

Object configuration	
jidMapping	\$sAMAccountName@brhuff.com
nameMapping	\$cn\$
cdrTagMapping	
coSpaceNameMapping	\$cn's Space
coSpaceUriMapping	\$sAMAccountName\$.space
coSpaceSecondaryUriMapping	\$extensionAttribute12\$
coSpaceCallIdMapping	
authenticationIdMapping	\$sAMAccountName\$

API LDAP매핑

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

API 사용자 예

Edit Rule - Webbridge3

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

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

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

View Rule Language... **OK** Cancel

AD FS의 클레임 규칙

작동 로그를 보여주는 Webbridge 로그 예입니다. 조인 URL에서 ?trace=true를 사용

하여 생성된 예:

3월 18일 14:24:01.096 user.info cmscb3-1 client_backend: 정보: SamlManager: [7979f13c-d490-4f8b-899c-0c82853369ba] SAML 토큰 요청에서 SSO_2024.zip과 일치

3월 18일 14:24:01.096 user.info cmscb3-1 client_backend: 정보: SamlManager: [7979f13c-d490-4f8b-899c-0c82853369ba] SAML IDP 응답에서 SSO를 찾는 중입니다.

3월 18일 14:24:01.101 user.info cmscb3-1 client_backend: 정보: SamlManager: [7979f13c-d490-4f8b-899c-0c82853369ba] 인증 ID: darmckin@brhuff.com을 성공적으로 가져왔습니다.

3월 18일 14:24:01.102 user.info cmscb3-1 host:server: INFO : 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)

3월 18일 14:24:01.130 user.info cmscb3-1 host:server: INFO: darmckin@brhuff.com에서 로그인 요청 성공

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

3월 18일 14:24:01.132 user.info cmscb3-1 host:server: INFO : WB3Cmgr: [7979f13c-d490-4f8b-899c-0c82853369ba] 인증 응답 전송 (jwt length=1064, connection=64004556-faea-479f-aabe-691e17783aa5)

3월 18일 14:24:01.133 local7.info cmscb3-1 56496041063b wb3_frontend: [Auth:darmckin@brhuff.com, Tracing:7979f13c-d490-4f8b-899c-0c82853369ba] 14.0.25.247 - [18/Mar/2024:18:24:0000] status 200 "POST /api/auth/sso/idpResponse HTTP/1.1" bytes_sent 0_referr "<https://adfs.brhuff.com/>" http_user_agent "Mozilla/zilla 0.0(Windows NT 10.0; Win64; x64) AppleWebKit/537.36(KHTML, 예: Gecko) Chrome/122.0.0.0 Safari/537.36" - 업스트림 192.0.2.2:9000: upstream_response_time 0.038 request_time 0.039 msec 1710786241.133 upstream_response_length 24 200

관련 정보

- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.