SAML SSO 컨피그레이션을 위한 AD FS 버전 2.0 설정 예

목차

소개

이 문서에서는 CUCM(Cisco Unified Communications Manager), UCXN(Cisco Unity Connection), CUCM IM and Presence 및 Cisco Prime Collaboration과 같은 Cisco Collaboration 제품에 대해 SAML(Security Assertion Markup Language) SSO(Single Sign-on)를 사용하도록 AD FS(Active Directory Federation Service) 버전 2.0을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

AD FS 버전 2.0을 설치하고 테스트해야 합니다.

> **주의:**이 설치 가이드는 랩 설정을 기반으로 하며, AD FS 버전 2.0은 Cisco Collaboration 제품의 SAML SSO에만 사용되는 것으로 가정합니다.다른 비즈니스 크리티컬 애플리케이션에서 사용하는 경우 공식 Microsoft 설명서에 따라 필요한 사용자 지정을 수행해야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- AD FS 버전 2.0
- Microsoft Internet Explorer 10
- CUCM 버전 10.5
- Cisco IM and Presence Server 버전 10.5
- UCXN 버전 10.5
- Cisco Prime Collaboration Provisioning 10.5

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

구성

AD FS 버전 2.0 IdP(Identity Provider) 메타데이터 다운로드

IdP 메타데이터를 다운로드하려면 브라우저에서 이 링크를 실행하십시오.https://<AD FS의 FQDN>/FederationMetadata/2007-06/FederationMetadata.xml.

SP(Collaboration Server) 메타데이터 다운로드

CUCM IM and Presence 서비스

웹 브라우저를 열고 CUCM에 관리자로 로그인한 다음 **System(시스템) >** SAML **Single Sign On으로 이동합니다**.

유니티 연결

웹 브라우저를 열고 UCXN에 관리자로 로그인한 다음 **System Settings(시스템 설정) >** SAML **Single Sign On으로 이동합니다**.

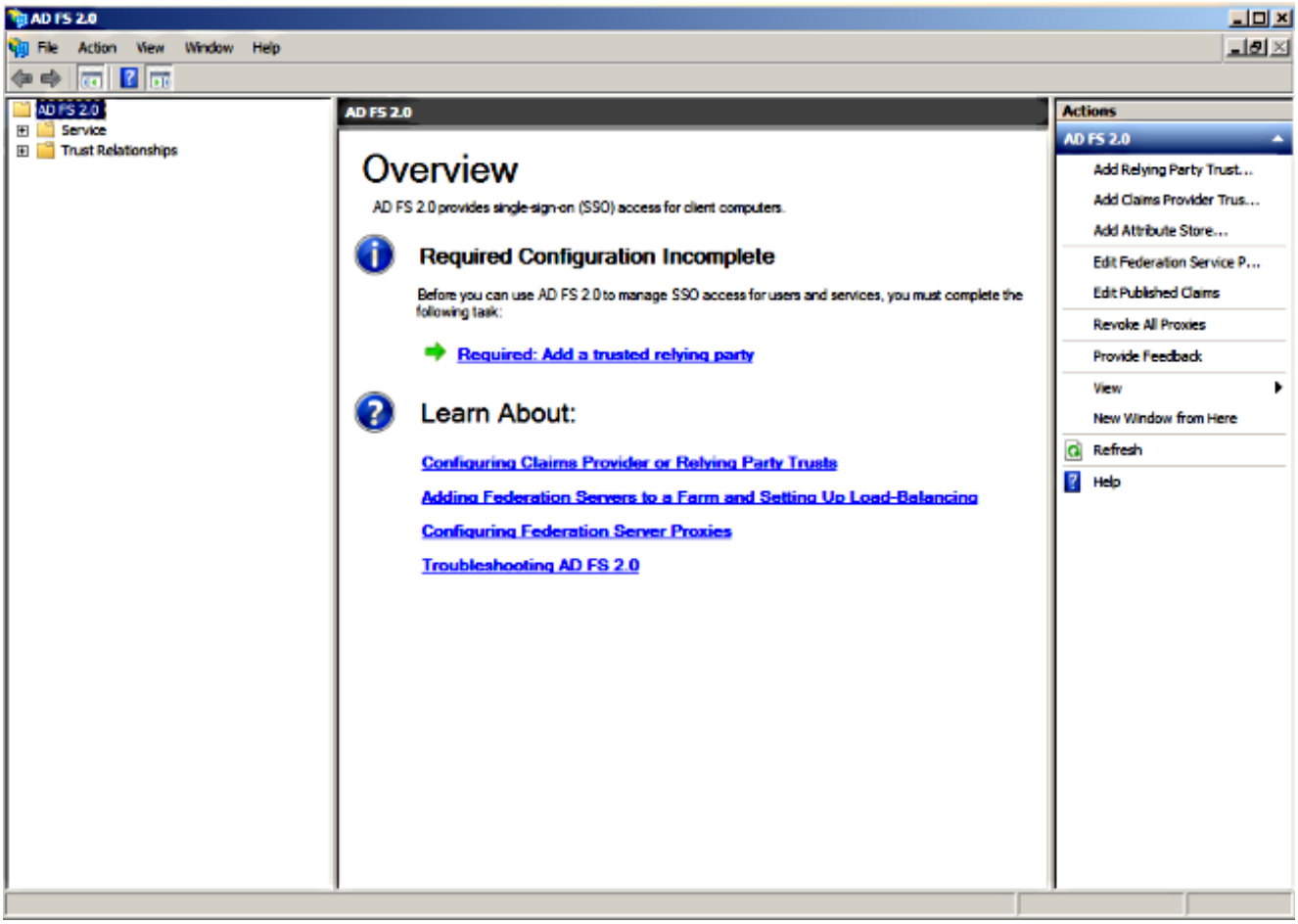
Cisco Prime Collaboration 프로비저닝

웹 브라우저를 열고 Prime Collaboration Assurance에 globaladmin으로 로그인한 다음 **Administration(관리) > System Setup(시스템 설정) > Single Sign On(단일 로그인)으로 이동합니다** .

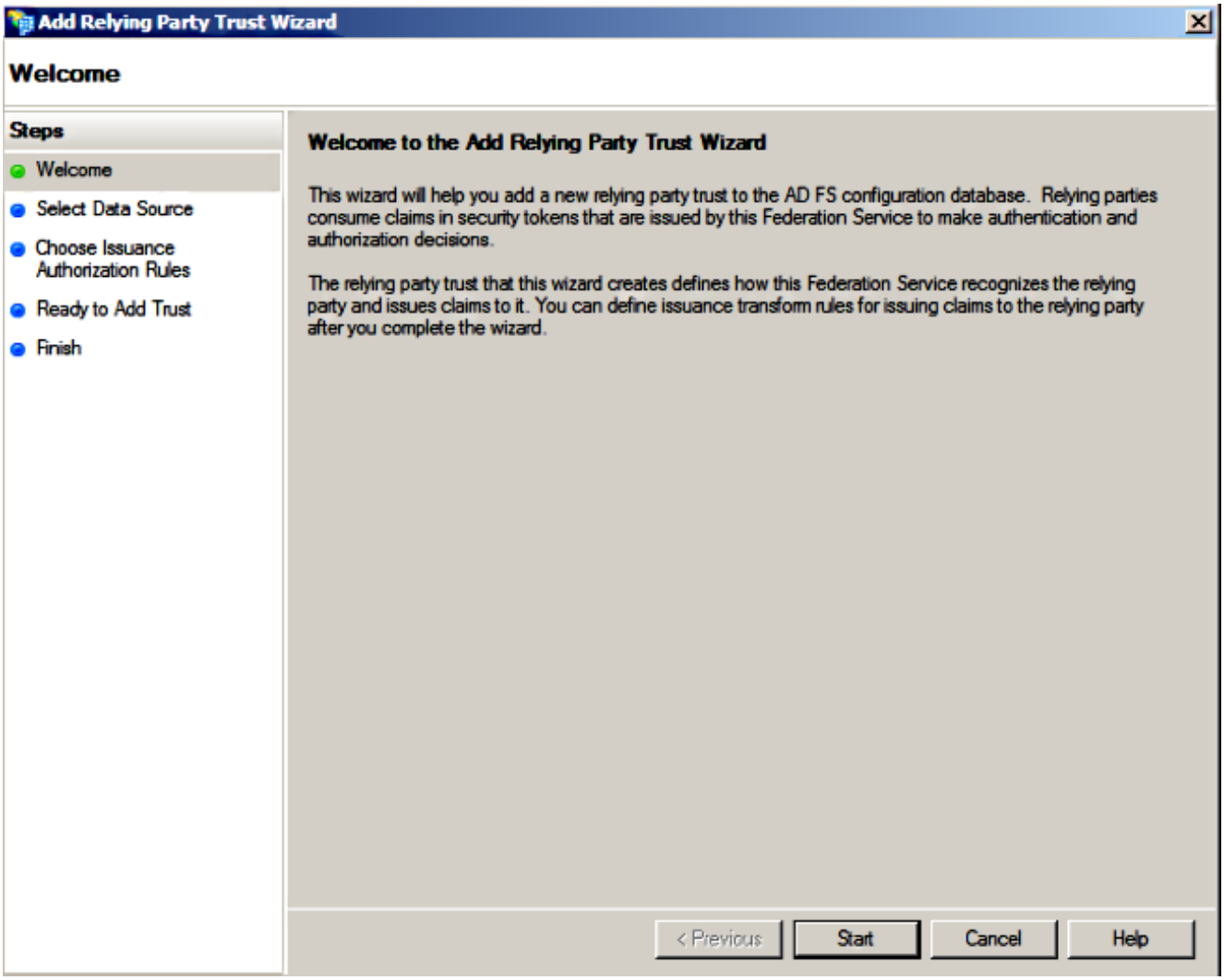
CUCM을 당사자 트러스트로 추가

1. AD FS 서버에 로그인하고 Microsoft Windows **프로그램** 메뉴에서 AD FS 버전 2.0을 시작합니다.

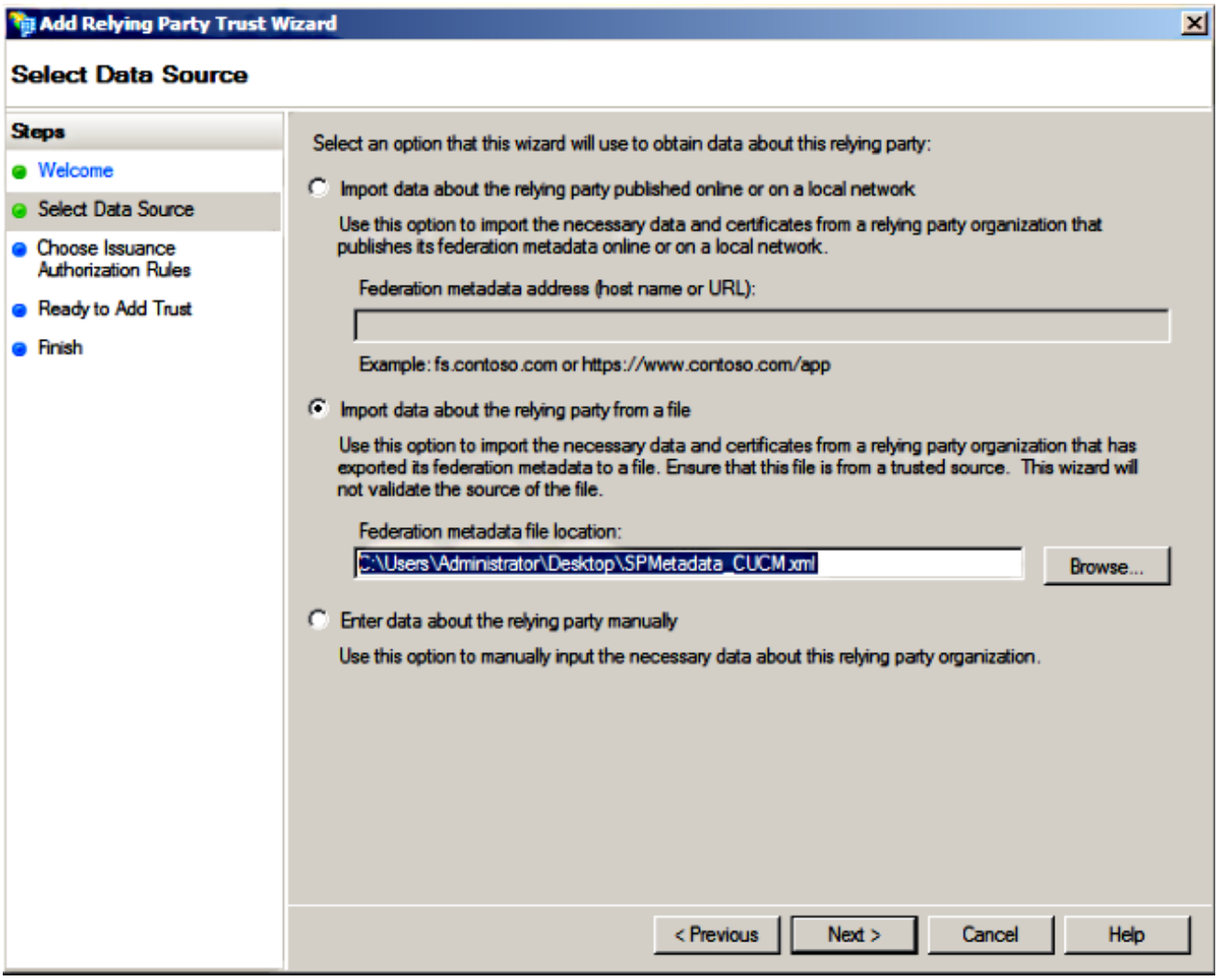
2. Add **Relying Party Trust를 선택합니다**.


AD FS 2.0
File Action View Window Help
AD FS 2.0
Service
Trust Relationships
AD FS 2.0
Overview
AD FS 2.0 provides single-sign-on (SSO) access for client computers.
Required Configuration Incomplete
Before you can use AD FS 2.0 to manage SSO access for users and services, you must complete the following task:
Required: Add a trusted relying party
Learn About:
Configuring Claims Provider or Relying Party Trusts
Adding Federation Servers to a Farm and Setting Up Load-Balancing
Configuring Federation Server Proxies
Troubleshooting AD FS 2.0
Actions
AD FS 2.0
Add Relying Party Trust...
Add Claims Provider Trus...
Add Attribute Store...
Edit Federation Service P...
Edit Published Claims
Revoke All Proxies
Provide Feedback
View
New Window from Here
Refresh
Help

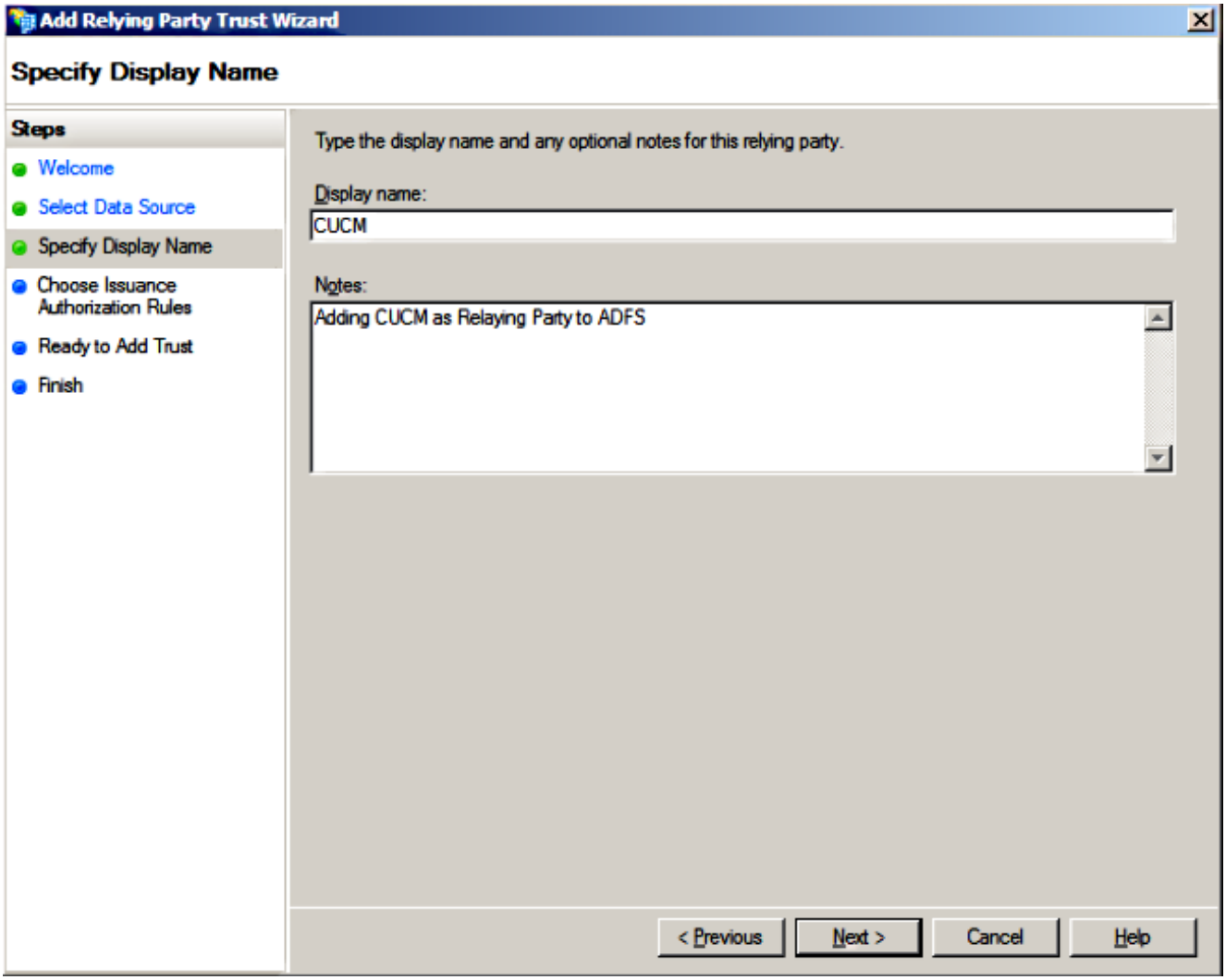
3. **시작**을 **클릭합니다**.



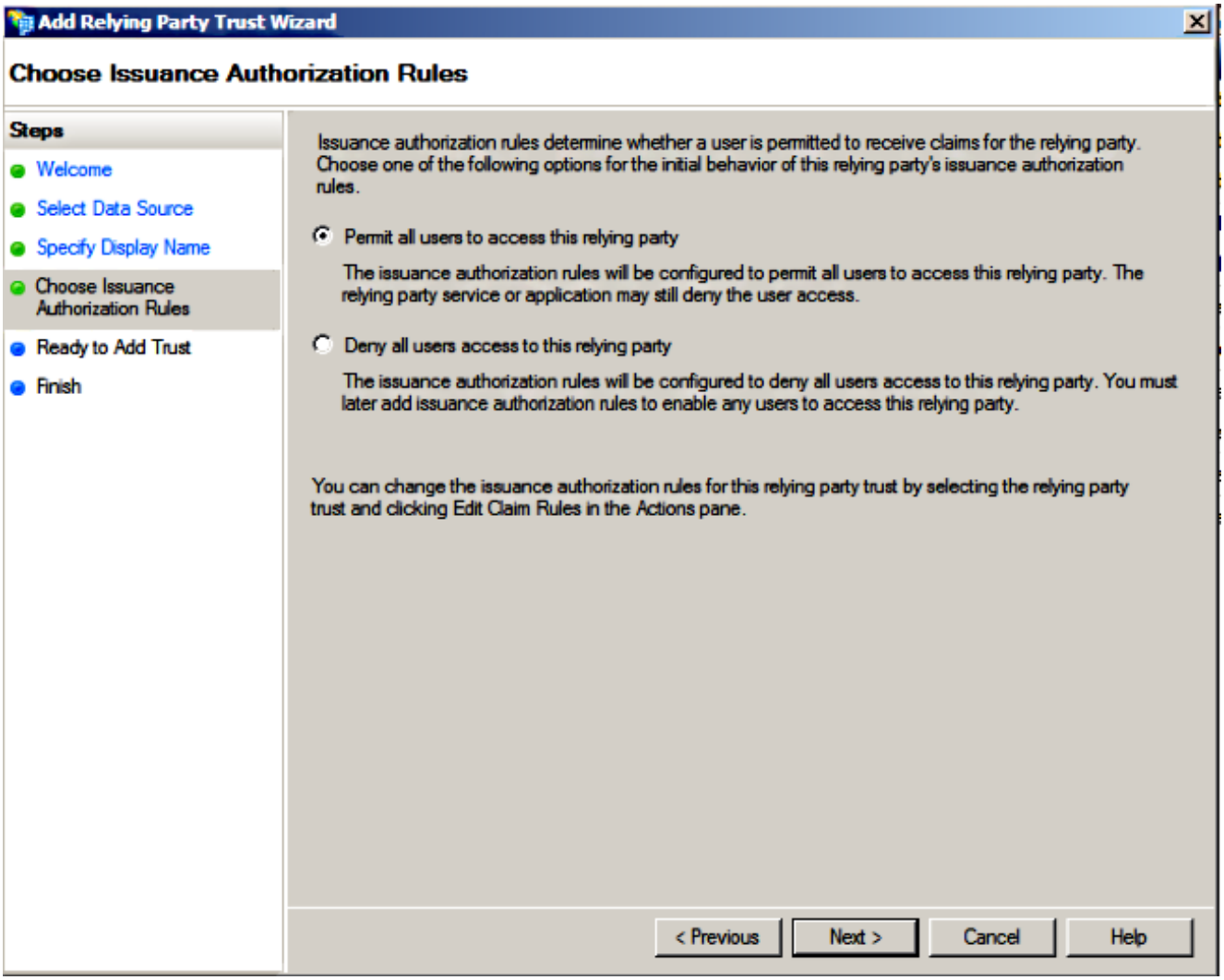
4. Import **data about the relying party about the relying party from a file** 옵션**을 선택하고** CUCM **앞부분에서** 다운로드한 SPMetadata_CUCM.xml 메타데이터 파일을 선택하고 **Next**를 클릭합니다.



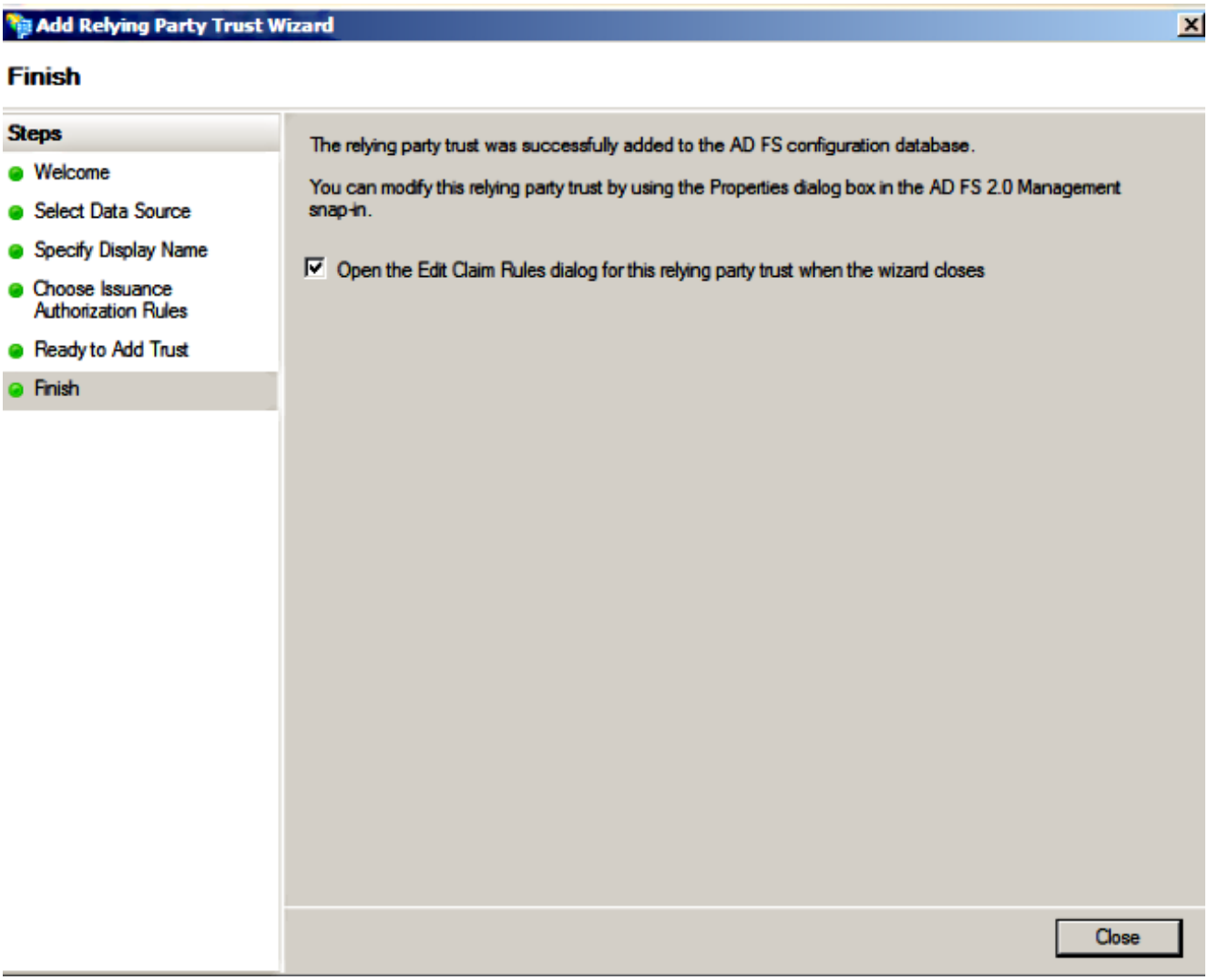
5. Display **name(표시 이름)**을 입력하고 **Next(다음)**를 클릭합니다.



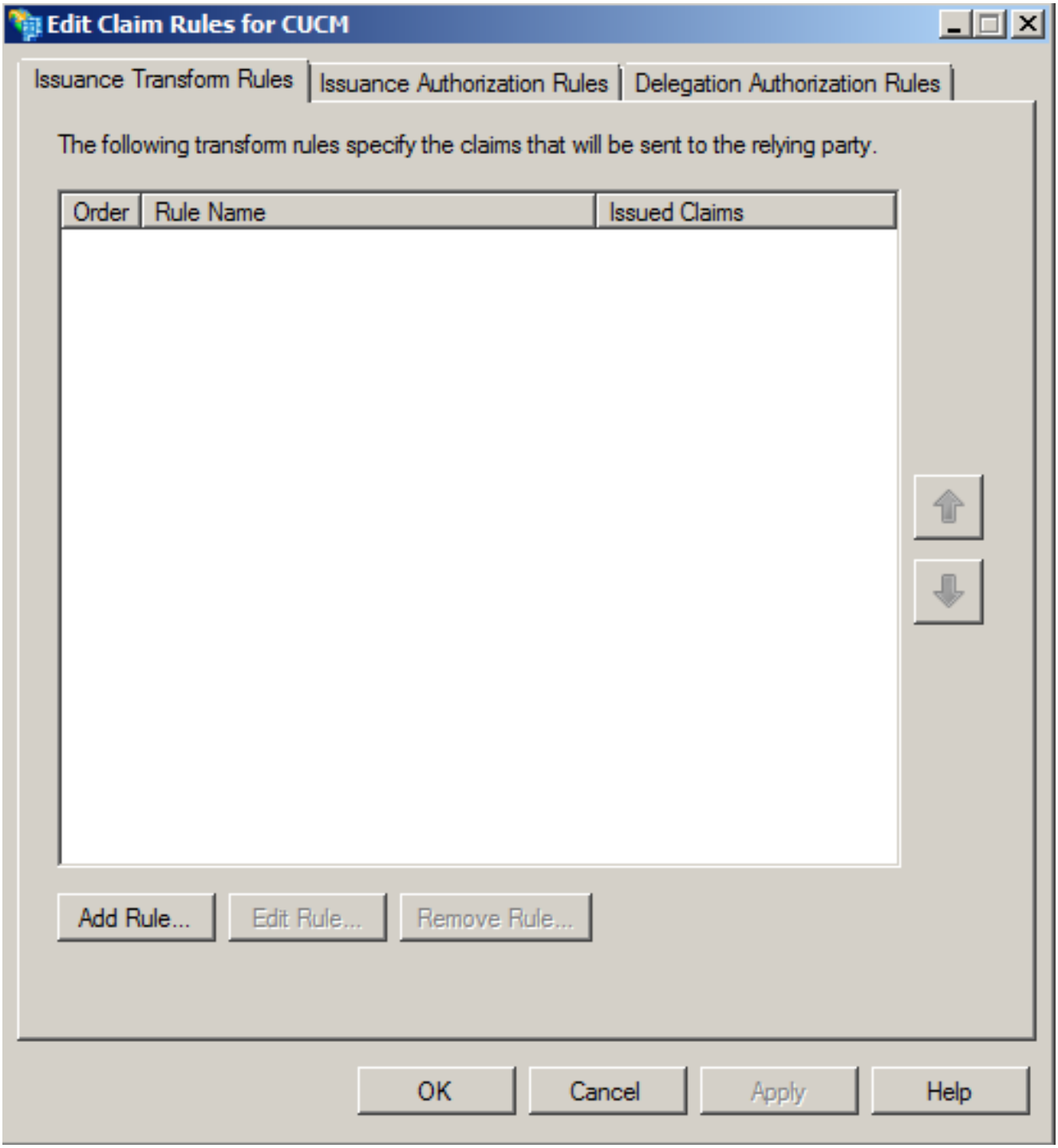
6. Permit **all users to access this relying party(모든 사용자가 이 신뢰 당사자에 액세스하도록 허용)를 선택하고** Next(다음)를 **클릭합니다.**



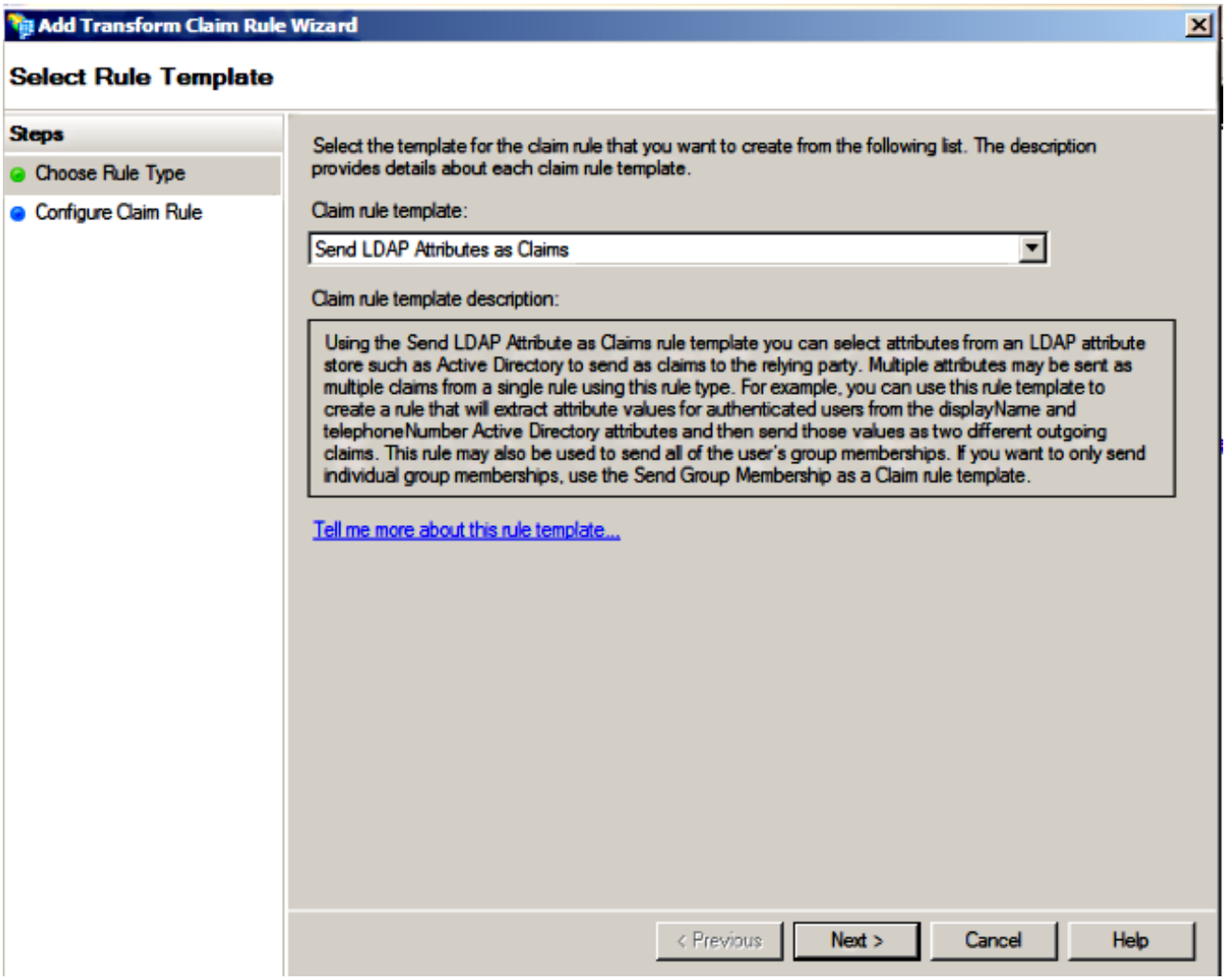
7. **마법사를 닫을 때 신뢰 당사자 트러스트에 대한 클레임 규칙 편집 대화 상자 열기**를 선택하고 **닫기**를 클릭합니다.



8. Add **Rule을 클릭합니다.**

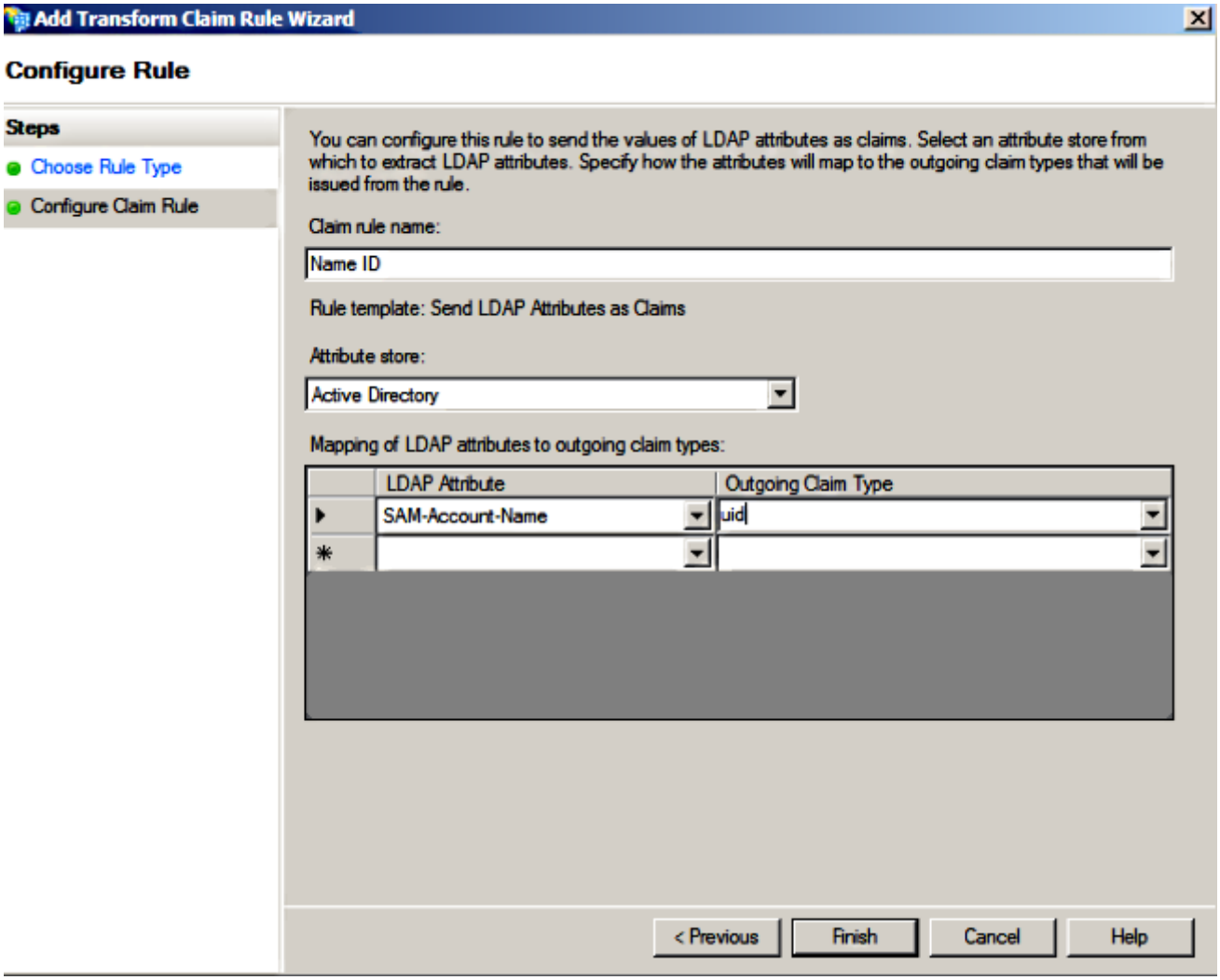


9. Send LDAP Attributes as Claims(LDAP 특성을 클레임으로 보내기)로 설정된 기본 클레임 규칙 템플릿**이 있는 Next(다음)를 클릭합니다**.

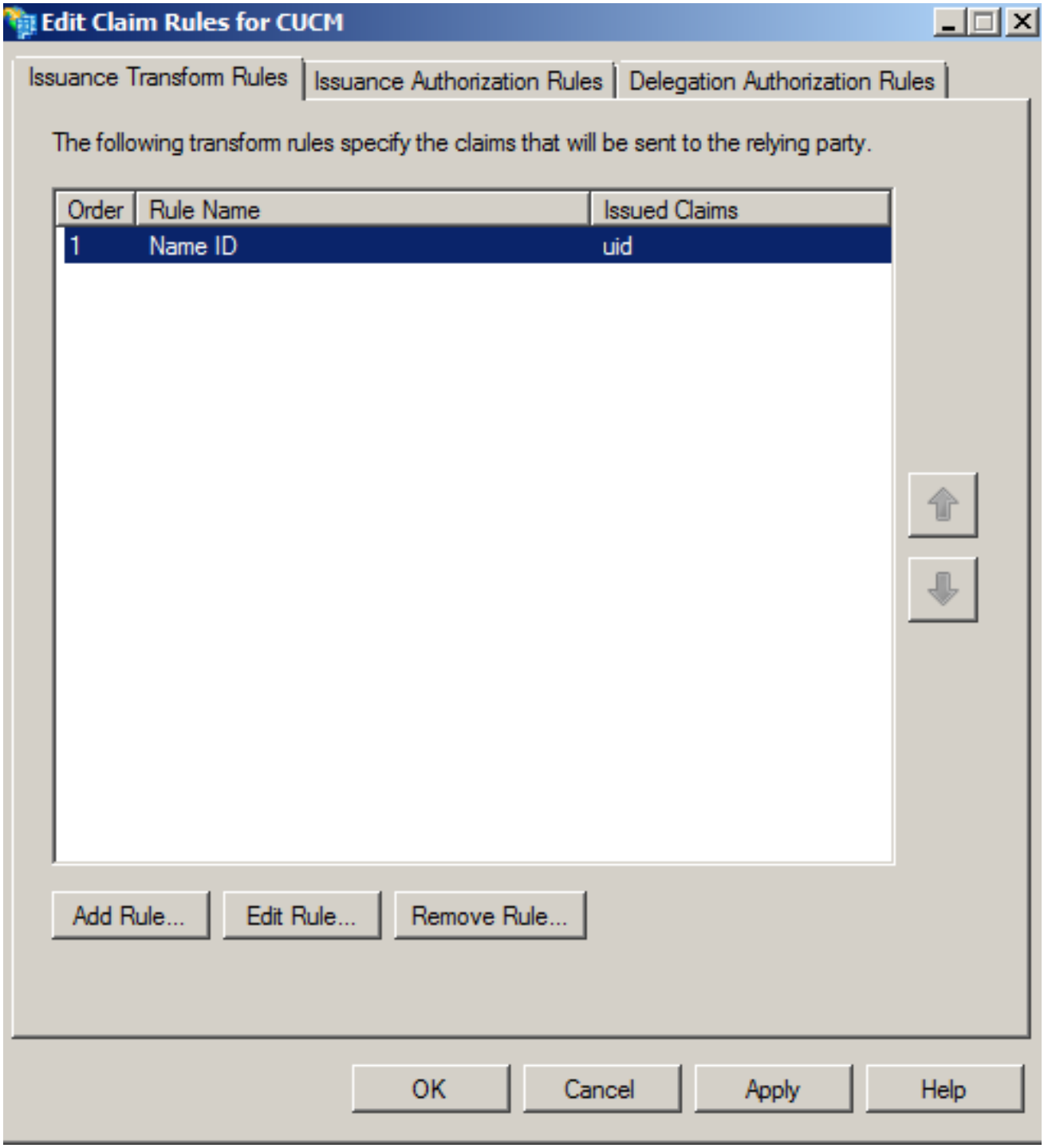


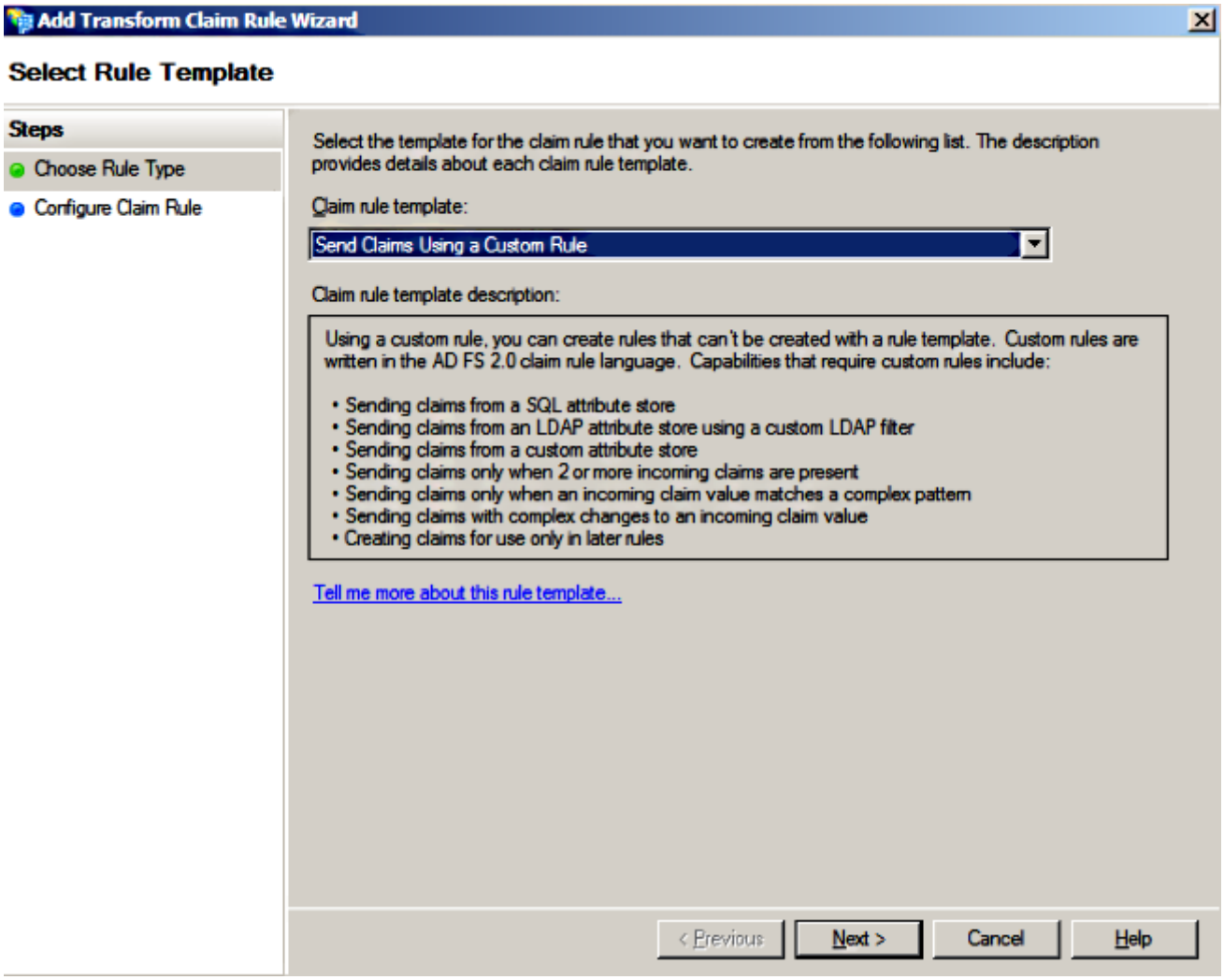
10. Configure Rule(규칙 구성)에서 Claim(클레임) 규칙 이름을 입력하고 Attribute(특성 저장소)로 **Active Directory**를 선택하고 이 이미지에 표시된 대로 **LDAP Attribute(LDAP 특성)** 및 **Outgoing Claim Type(발신 클레임 유형)을** 구성하고 **Finish(마침)를 클릭합니다**.

참고:
- LDAP(Lightweight Directory Access Protocol) 특성은 CUCM의 Directory Sync 특성과 일치해야 합니다.
- "uid"는 소문자여야 합니다.



11. Add **Rule**을 클릭하고 **Send Claims Using a Custom Rule**을 클레임 규칙 템플릿으로 선택한 후 **Next**를 클릭합니다.

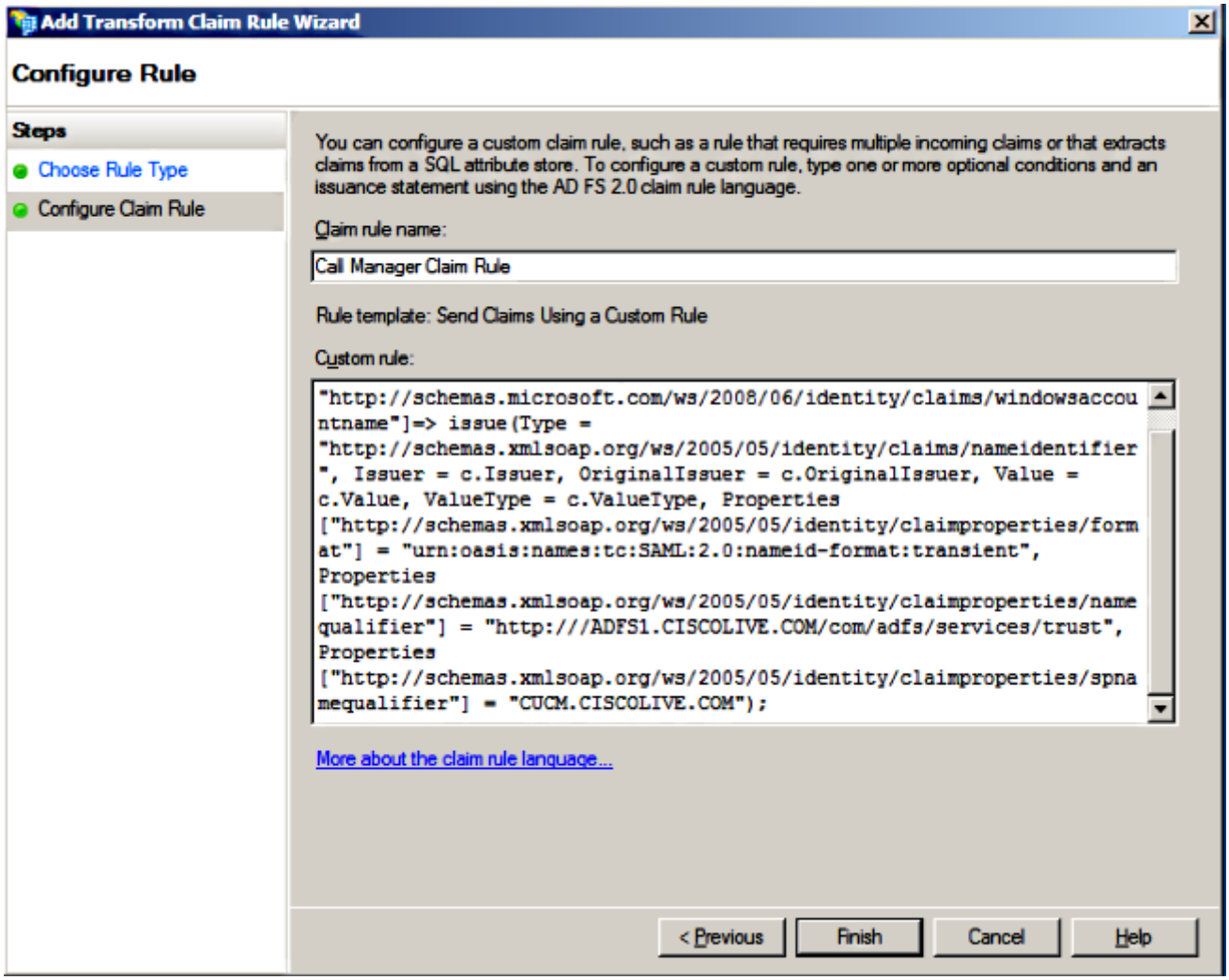

Edit Claim Rules for CUCM
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
The following transform rules specify the claims that will be sent to the relying party.
Order
Rule Name
Issued Claims
1
Name ID
uid
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply
Help



12. Claim 규칙 이름의 이름을 입력하고 Custom(사용자 지정) 규칙에 지정된 공간에 이 구문을 복사합니다.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
= "http://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier
"] = "<FQDN of CUCM>");
```

(**참고:** 이러한 예에서 텍스트를 복사하여 붙여넣는 경우 일부 워드 프로세싱 소프트웨어가 ASCII 따옴표(')를 유니코드 버전("")으로 대체한다는 점에 유의하십시오. 유니코드 버전은 클레임 규칙을 실패하게 합니다.



참고:
- 이 예에서는 CUCM 및 ADFS FQDN(Fully Qualified Domain Name)이 실습 CUCM 및 AD FS로 미리 채워져 있으며 환경에 맞게 수정해야 합니다.
- CUCM/ADFS의 FQDN은 대/소문자를 구분하며 메타데이터 파일과 일치해야 합니다.

13. **마침**을 **클릭합니다**.

14. Apply(**적용**)를 클릭한 다음 **OK(확인)를 클릭합니다.**

15. Services.msc에서 AD FS 버전 2.0 서비스를 **다시 시작합니다**.

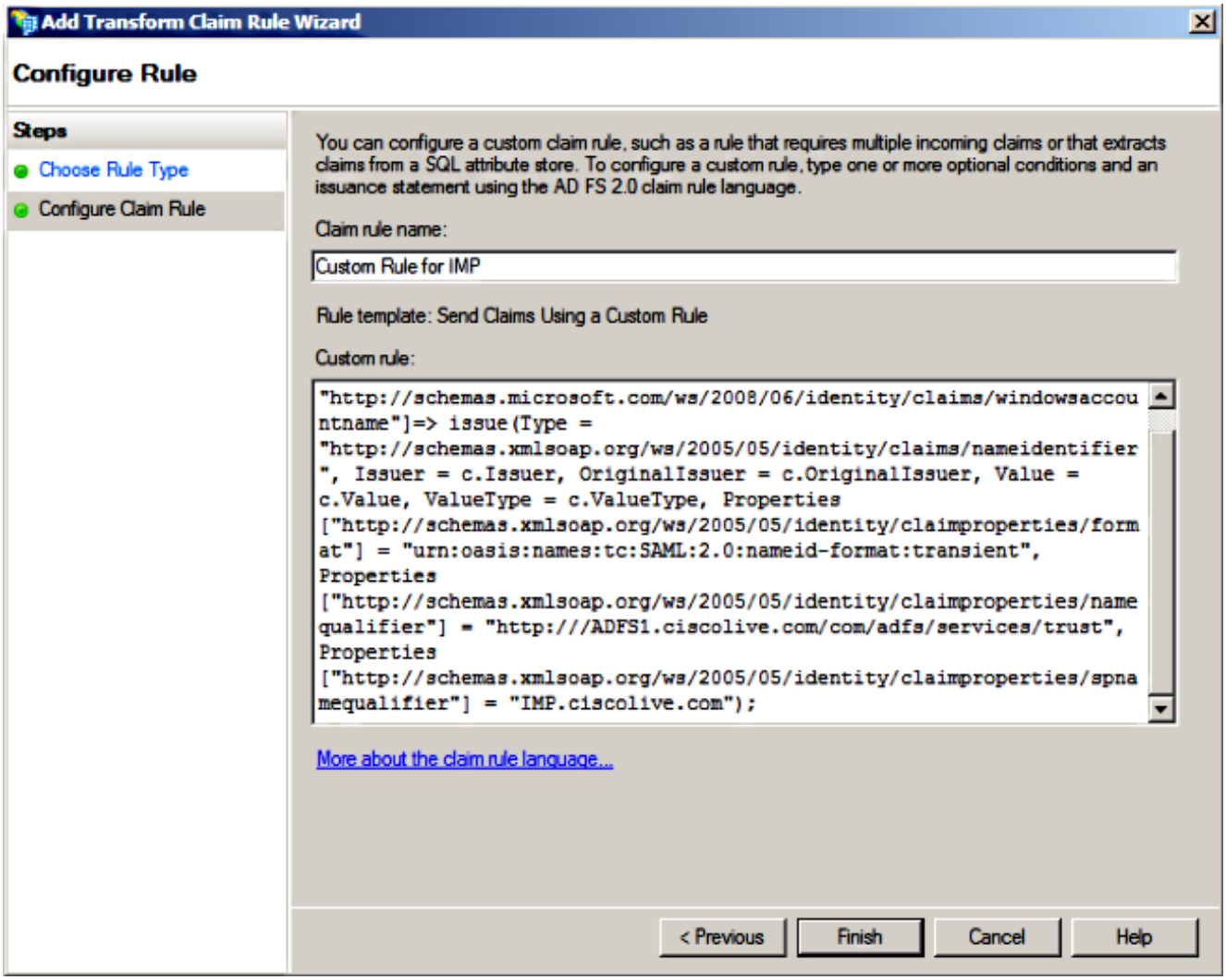
CUCM IM and Presence를 당사자 트러스트로 추가

1. CUCM을 신뢰 당사자 트러스트로 **추가**에 설명된 대로 1~11**단계를** 반복하고 2단계로 진행합니다.

2. Claim 규칙 이름의 이름을 입력하고 Custom(사용자 지정) 규칙에 지정된 공간에 이 구문을 복사합니다.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
= c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
```

```
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
= "http://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of IMP>");
```



이 예에서는 IM and Presence 및 AD FS FQDN이 Lab IM and Presence 및 AD FS로 미리 채워져 있으며 환경에 맞게 수정해야 합니다.

3. **마침**을 **클릭합니다**.

4. Apply(**적용**)를 클릭한 다음 **OK(확인)를 클릭합니다.**

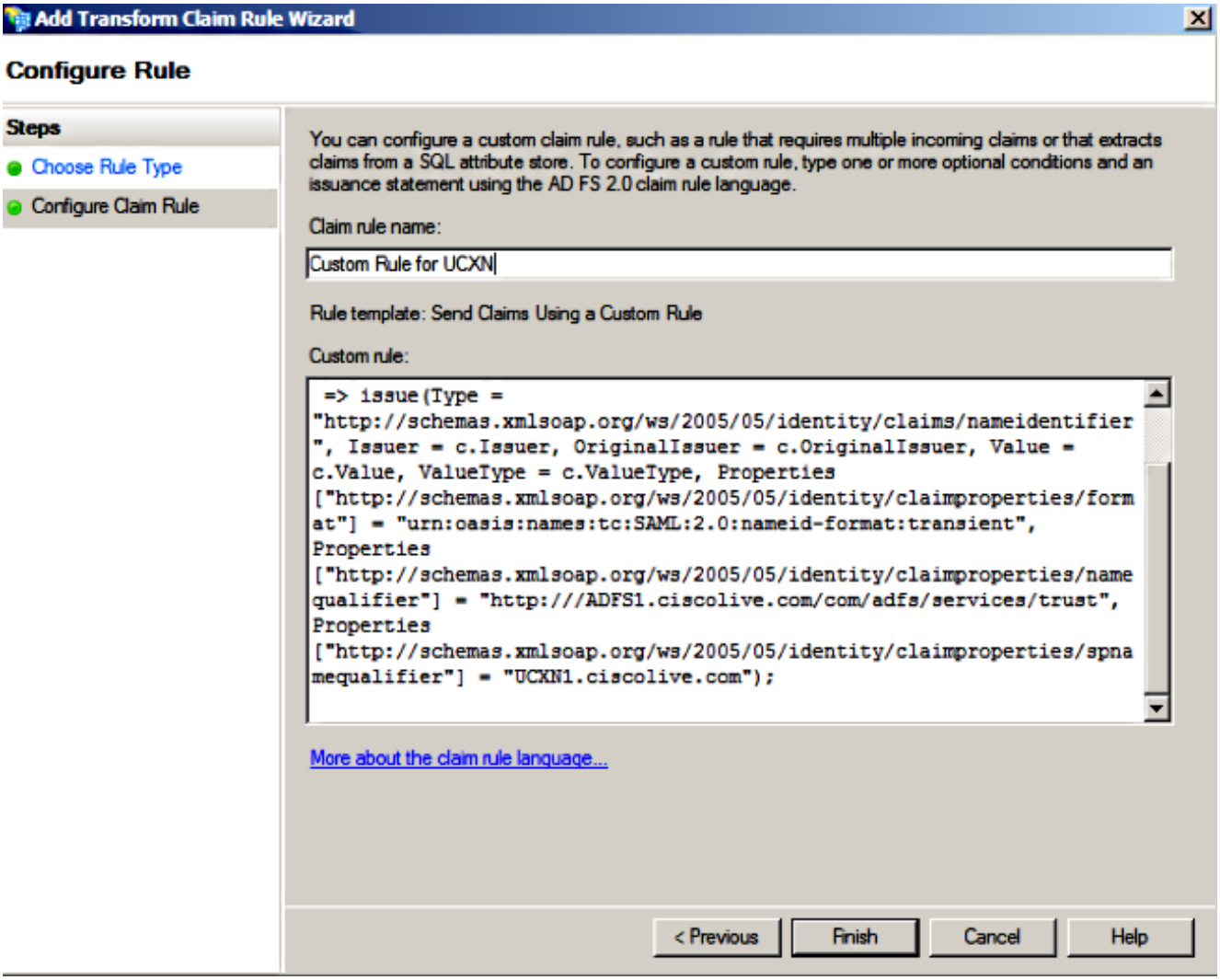
5. Services.msc에서 AD FS 버전 2.0 서비스를 **다시 시작합니다.**

UCXN을 당사자 트러스트로 추가

1. CUCM을 신뢰 당사자 트러스트로 **추가**에 설명된 대로 1~12단계**를 반복하고** 2단계로 진행합니다.

2. Claim 규칙 이름의 이름을 입력하고 Custom(사용자 지정) 규칙에 지정된 공간에 이 구문을 복사합니다.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
= c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
= "http://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of UCXN>");
```



이 예에서는 UCXN 및 AD FS FQDN이 실습 UCXN 및 ADFS로 미리 채워져 있으며 환경에 맞게 수정해야 합니다.

3. **마침**을 **클릭합니다**.

4. Apply(**적용**)를 클릭한 다음 **OK(확인)를 클릭합니다**.

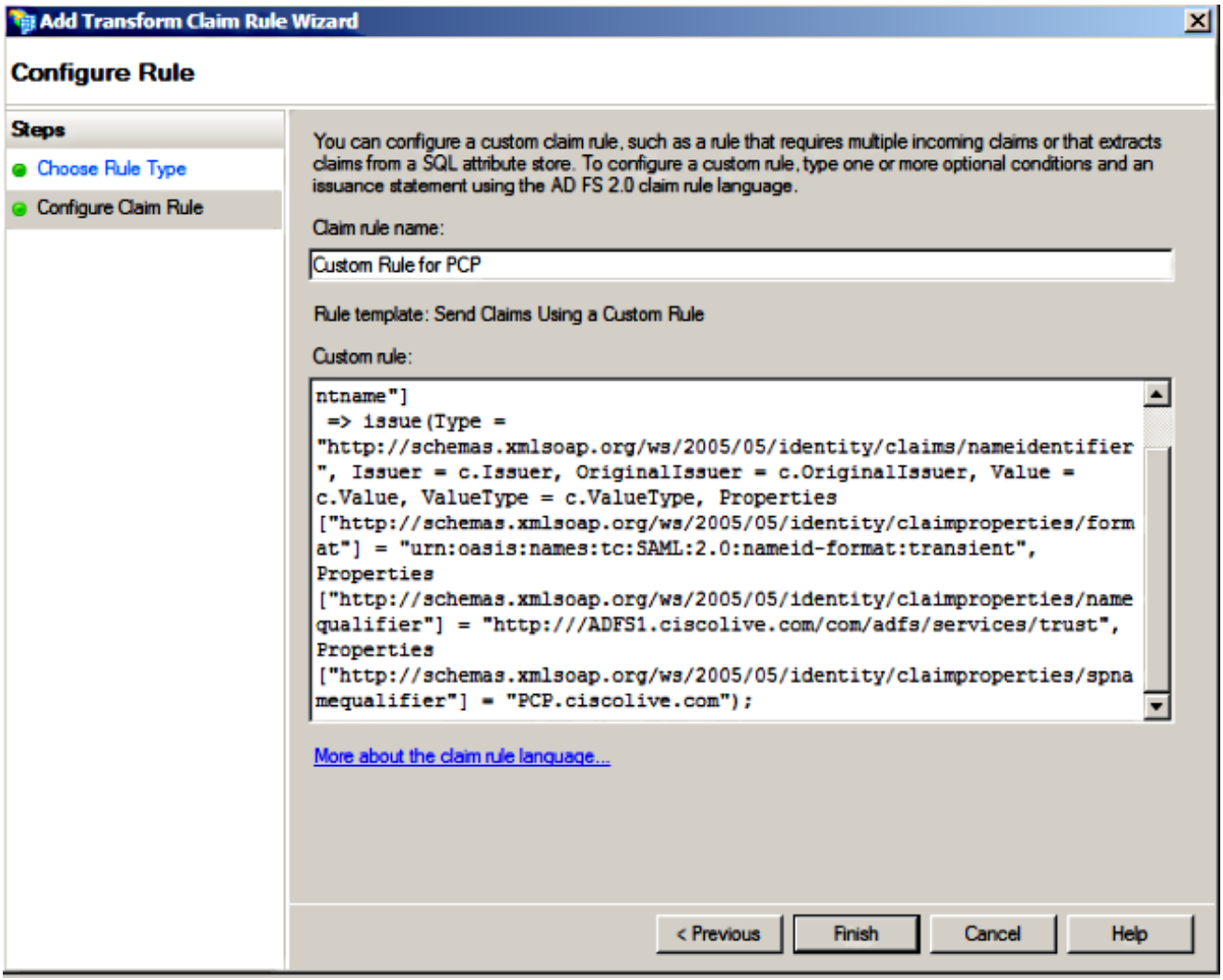
5. Services.msc에서 AD FS 버전 2.0 서비스를 **다시 시작합니다.**

Cisco Prime Collaboration 프로비저닝을 당사자 트러스트로 추가

1. CUCM을 신뢰 당사자 트러스트로 **추가**에 설명된 대로 1~12단계**를 반복하고** 2단계로 진행합니다.

2. Claim 규칙 이름의 이름을 입력하고 Custom(사용자 지정) 규칙에 지정된 공간에 이 구문을 복사합니다.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
= c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
= "http://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of PCP>");
```



Prime Provisioning 및 AD FS FQDN은 이 예에서 실습 PCP(Prime Collaboration Provisioning) 및 AD FS로 미리 채워져 있으며 환경에 맞게 수정해야 합니다.

3. **마침**을 **클릭합니다**.

4. Apply(**적용**)를 클릭한 다음 **OK(확인)를 클릭합니다**.

5. Services.msc에서 AD FS 버전 2.0 서비스를 **다시 시작합니다**.

AD FS 버전 2.0을 설정한 후 Cisco Collaboration 제품에서 SAML SSO를 사용하도록 설정합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

AD FS는 진단 데이터를 시스템 이벤트 로그에 기록합니다. AD FS 서버의 서버 관리자에서 **진단 -> 이벤트 뷰어 -> 응용 프로그램 및 서비스 -> AD FS 2.0 -> 관리를 엽니다.**

AD FS 작업에 대해 기록된 오류를 찾습니다.