AD FS 버전 2.0으로 클러스터당 단일 SAML IdP 연결/계약 구성

목차

소개

이 문서에서는 AD FS(Active Directory Federation Service)를 사용하여 클러스터당 SAML(Single Security Assertion Markup Language) IdP(Identity Provider) 연결/계약을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco CUCM(Unified Communications Manager) 11.5 이상
- Cisco Unified Communications Manager IM and Presence 버전 11.5 이상
- Active Directory Federation Service 버전 2.0

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Active Directory Federation Service 버전 2.0을 IdP로 사용
- Cisco Unified Communications Manager 버전 11.5
- Cisco IM and Presence Server 버전 11.5

배경 정보

SAML SSO의 경우 SP(서비스 제공자)와 IdP 간의 신뢰 범위가 되어야 합니다. 이 신뢰는 신뢰(메타데이터)가 교환될 때 SSO 구현의 일부로 생성됩니다. CUCM에서 메타데이터를 다운로드하여 IdP에 업로드하고, IdP에서 메타데이터를 다운로드한 다음 CUCM에 업로드합니다.

이전 CUCM 11.5, 시작 노드는 메타데이터 파일을 생성하고, 클러스터의 다른 노드에서 메타데이터 파일을 수집합니다. 모든 메타데이터 파일을 단일 zip 파일에 추가한 다음 관리자에게 제공합니다 .관리자는 이 파일의 압축을 풀고 IdP에서 각 파일을 프로비저닝해야 합니다.예를 들어 8노드 클러스터의 메타데이터 파일 8개를 예로 들 수 있습니다.

클러스터당 단일 SAML IdP 연결/계약은 11.5에서 도입됩니다. 이 기능의 일부로 CUCM은 클러스터의 모든 CUCM 및 IMP 노드에 대해 단일 서비스 공급자 메타데이터 파일을 생성합니다.메타데이터 파일의 새 이름 형식은 **<hostname>-single-agreement.xml입니다.**

기본적으로 한 노드에서 메타데이터를 생성하여 클러스터의 다른 SP 노드에 푸시합니다.따라서 프로비저닝, 유지 보수 및 관리가 용이합니다.예를 들어, 8노드 클러스터에 대한 메타데이터 파일 1개가 있습니다.

클러스터 전체 메타데이터 파일은 키 쌍을 사용하는 멀티서버 tomcat 인증서를 사용합니다. 이는 클러스터의 모든 노드에 대해 동일하게 사용됩니다.메타데이터 파일에는 클러스터의 각 노드에 대한 ACS(Assertion Consumer Service) URL 목록도 있습니다.

CUCM 및 Cisco IM and Presence 버전 11.5 SSO 모드, **클러스터 전체**(클러스터당 하나의 메타데이터 파일) 및 노드당(기존 모델)을 모두 지원합니다.

이 문서에서는 AD FS 2.0을 사용하여 SAML SSO의 클러스터 전체 모드를 구성하는 방법에 대해 설명합니다.

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

1단계. CUCM에서 SP 메타데이터를 내보냅니다.

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

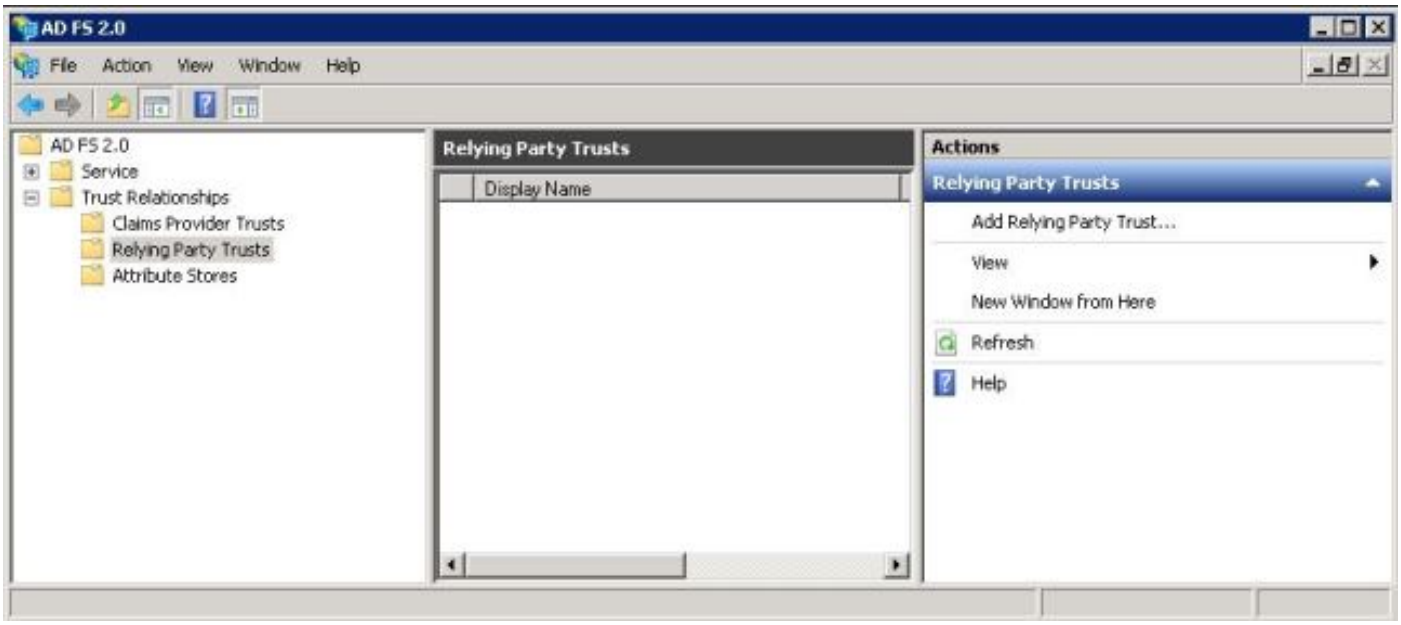
기본적으로 **Cluster Wide** 라디오 버튼이 선택됩니다.Export **All Metadata를 클릭합니다** **.<hostname>-single-agreement.xml** 이름으로 관리자에게 제공되는 메타데이터 데이터 파일

2단계. AD FS에서 IDP 메타데이터를 다운로드합니다.

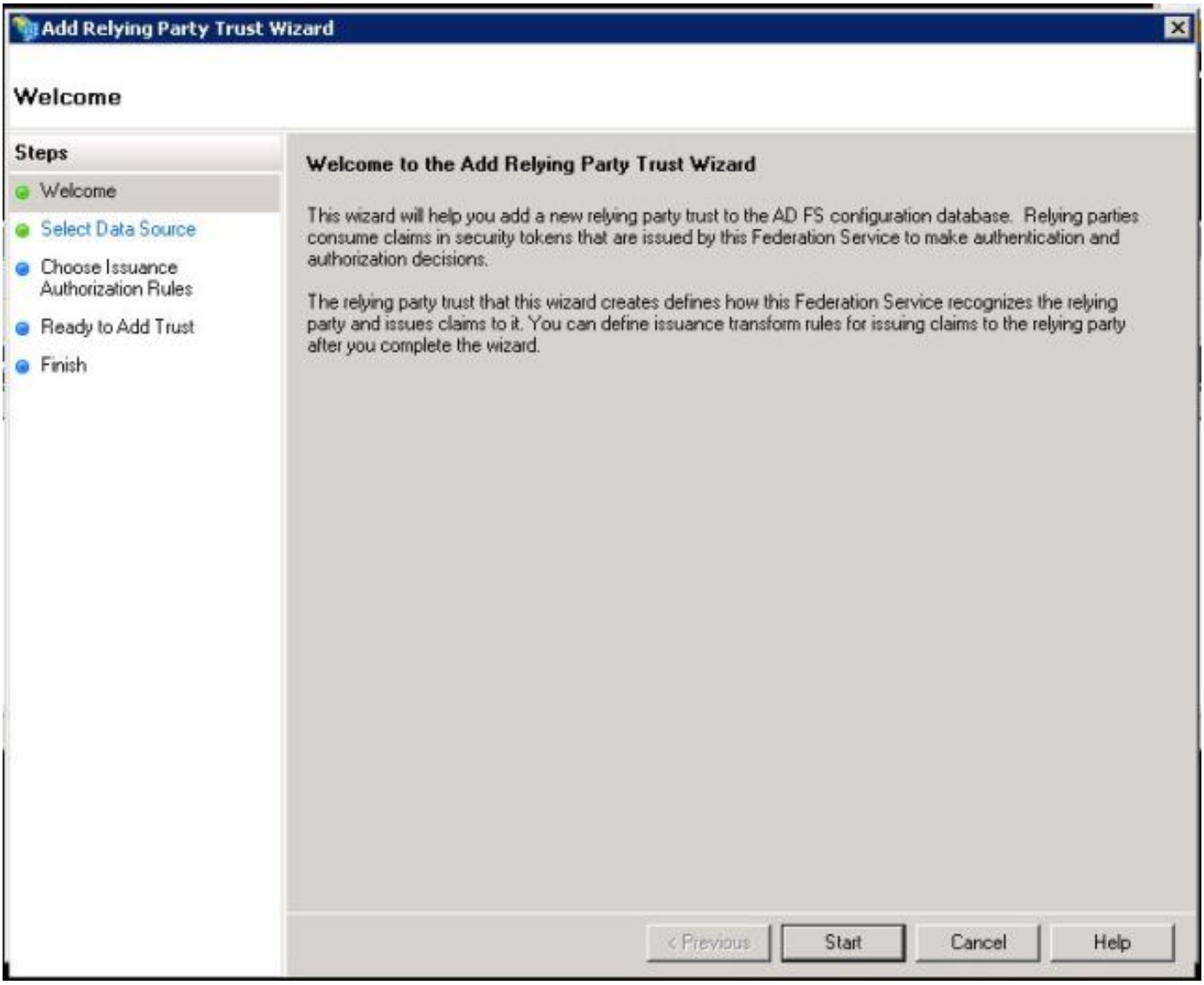
IdP 메타데이터를 다운로드하려면 https:// <AD FS의 FQDN>/federationmetadata/2007-06/federationmetadata.xml 링크를 참조하십시오.

3단계. IdP 프로비저닝

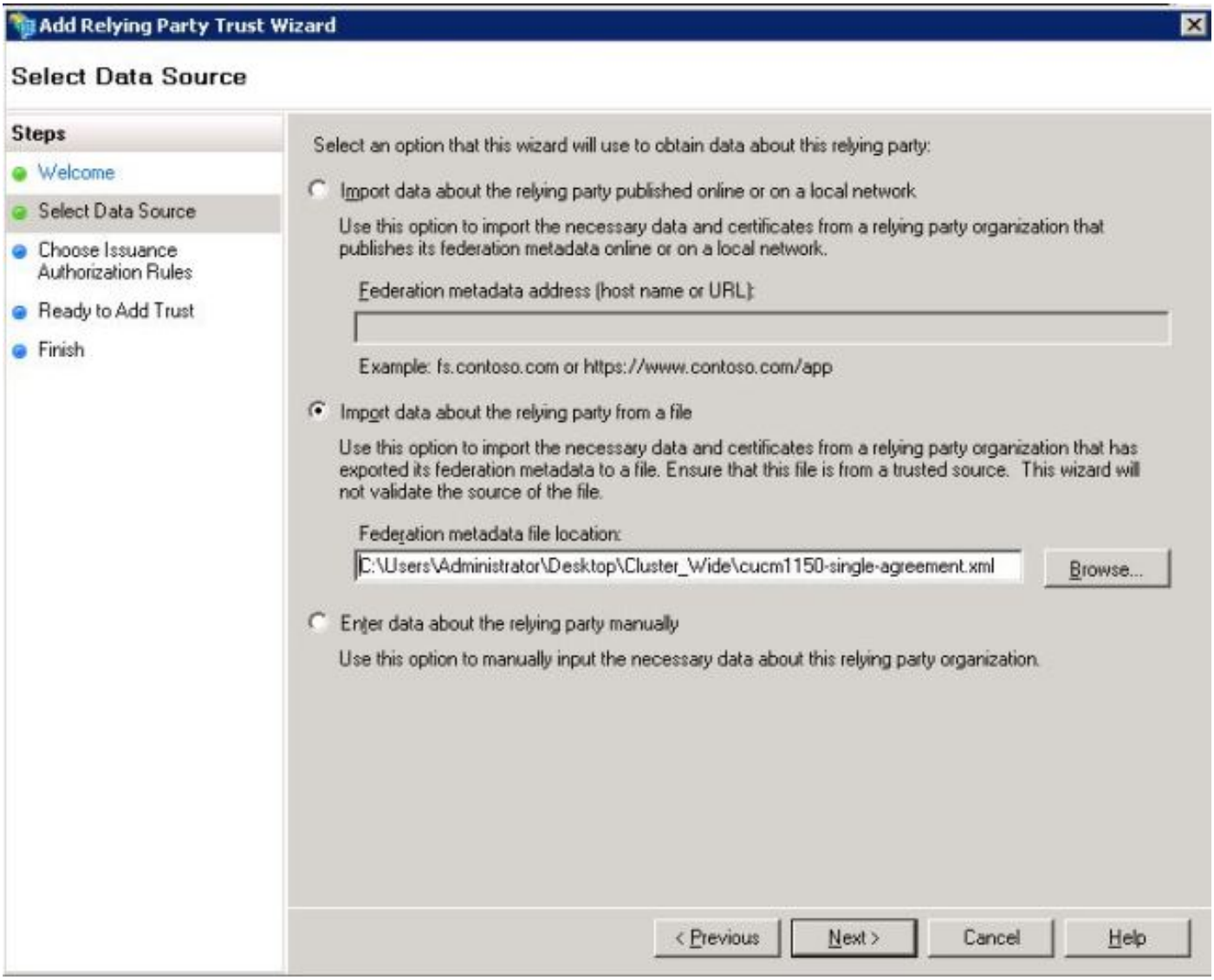
이미지에 표시된 대로 **AD FS 2.0 관리/신뢰 관계 배송/신뢰 당사자 트러스트로 이동합니다**.Add **Relying Party Trust를 클릭합니다**.



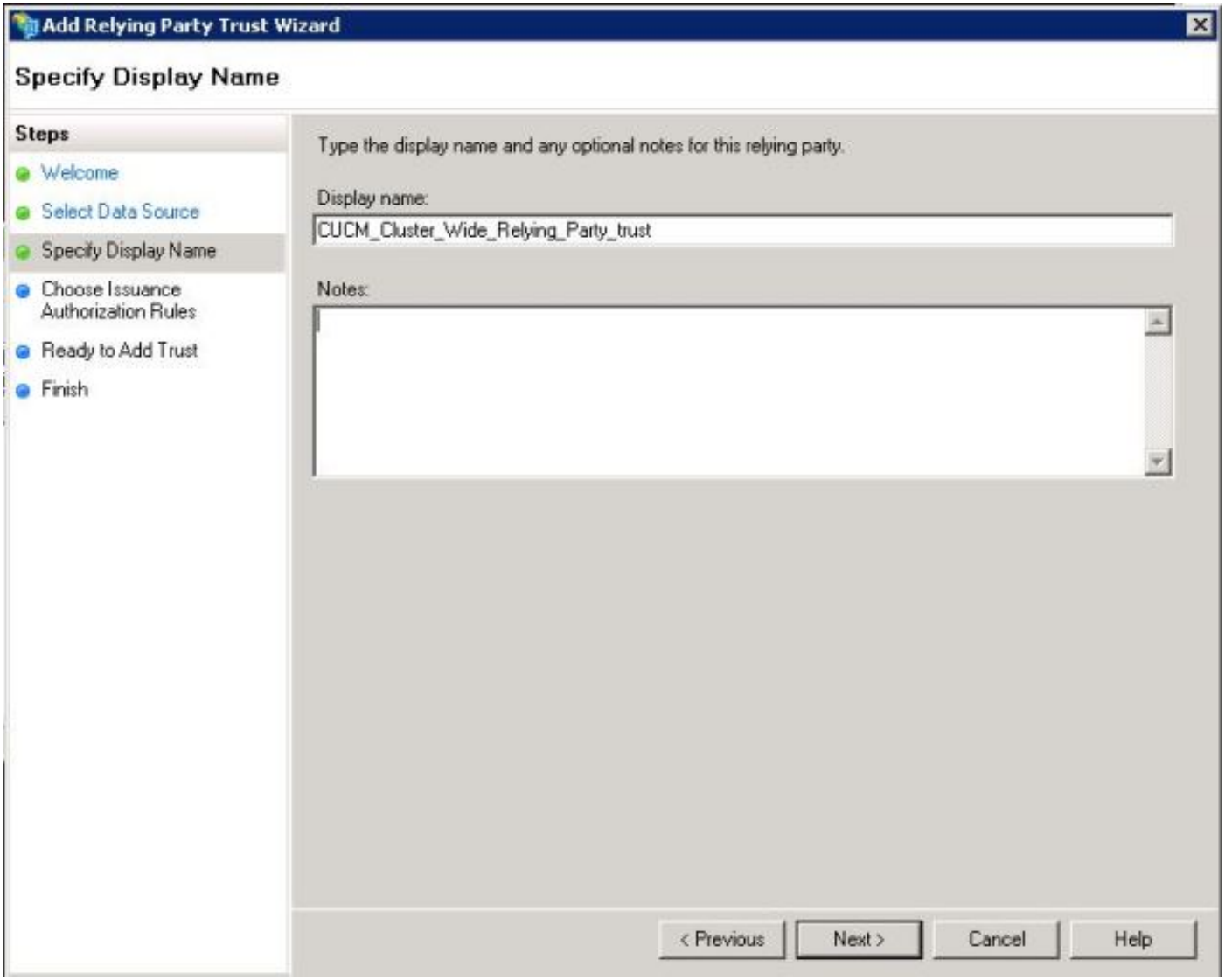
이미지에 표시된 대로 Add Relying Party Trust Wizard(신뢰 당사자 트러스트 추가 마법사)가 열리고 이제 Start(**시작**)를 클릭합니다.



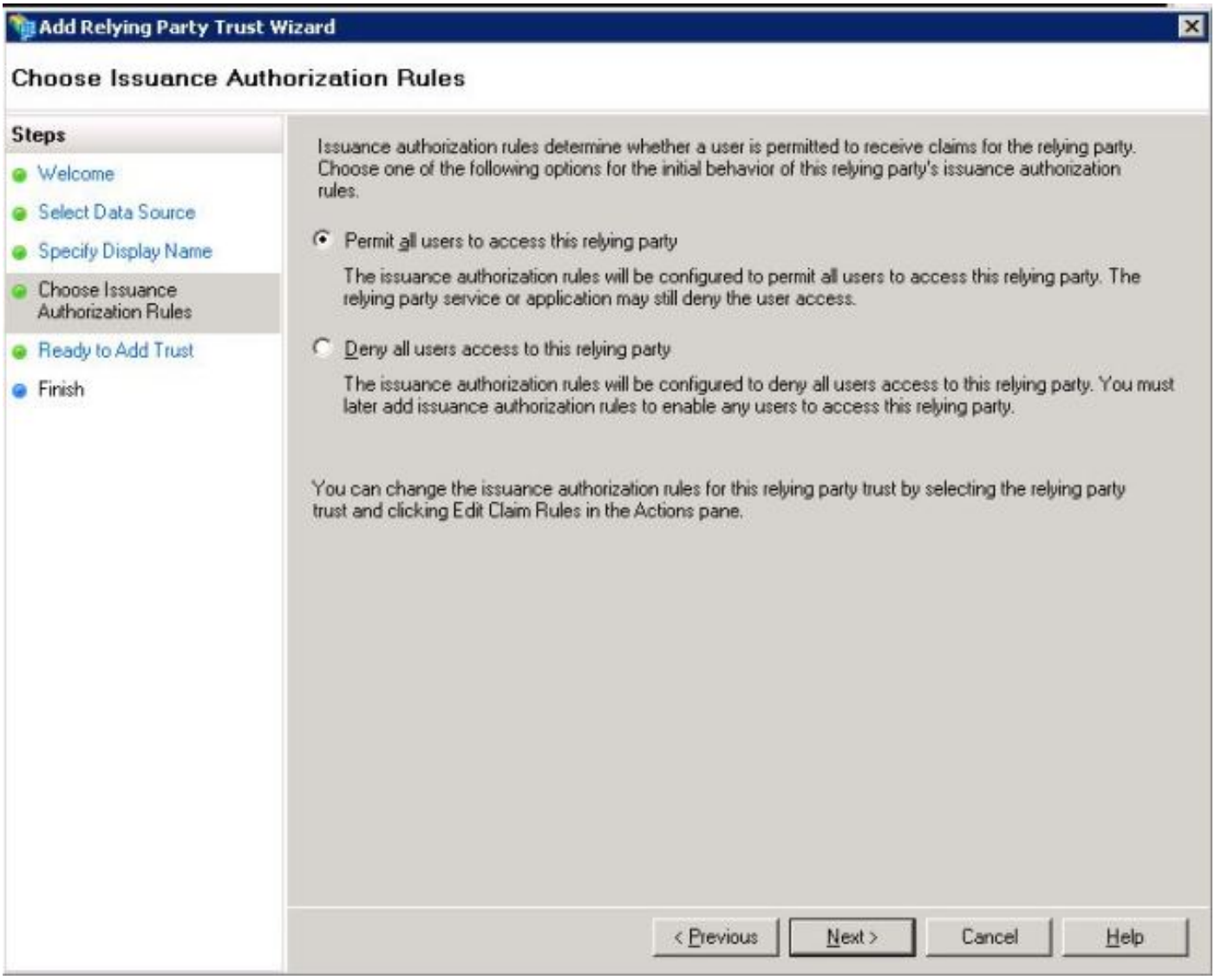
파일에서 신뢰 당사자에 대한 데이터 가져오기를 클릭합니다.CUCM SAML SSO 구성 페이지에서 다운로드한 SP 메타데이터를 찾습니다.그런 다음 **다음**을 클릭합니다(이미지에 표시됨).



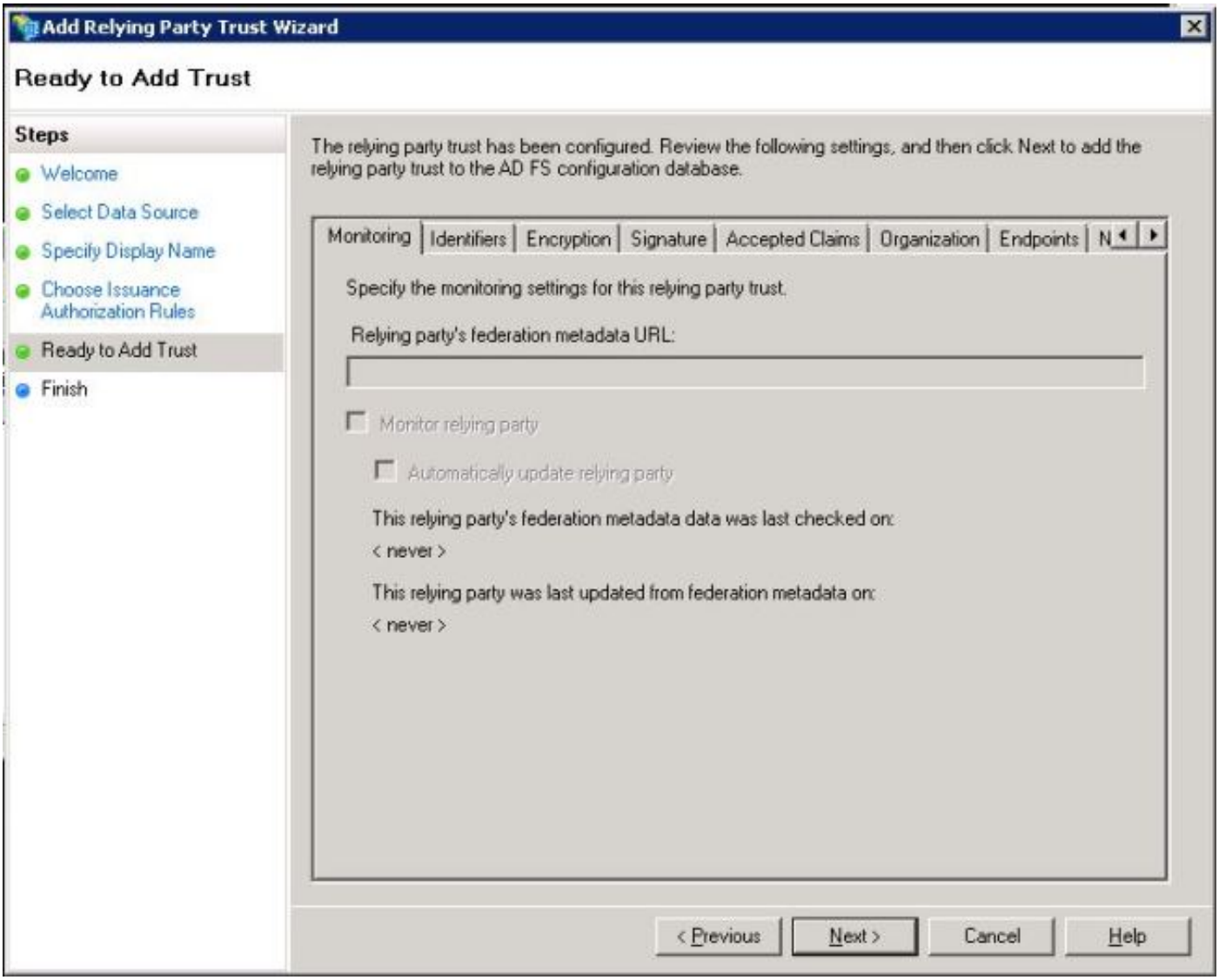
Display Name(표시 이름) 및 Relying Party(신뢰 당사자)에 대한 선택적 메모를 입력합니다.이미지에 표시된 대로 Next(다음)를 클릭합니다.



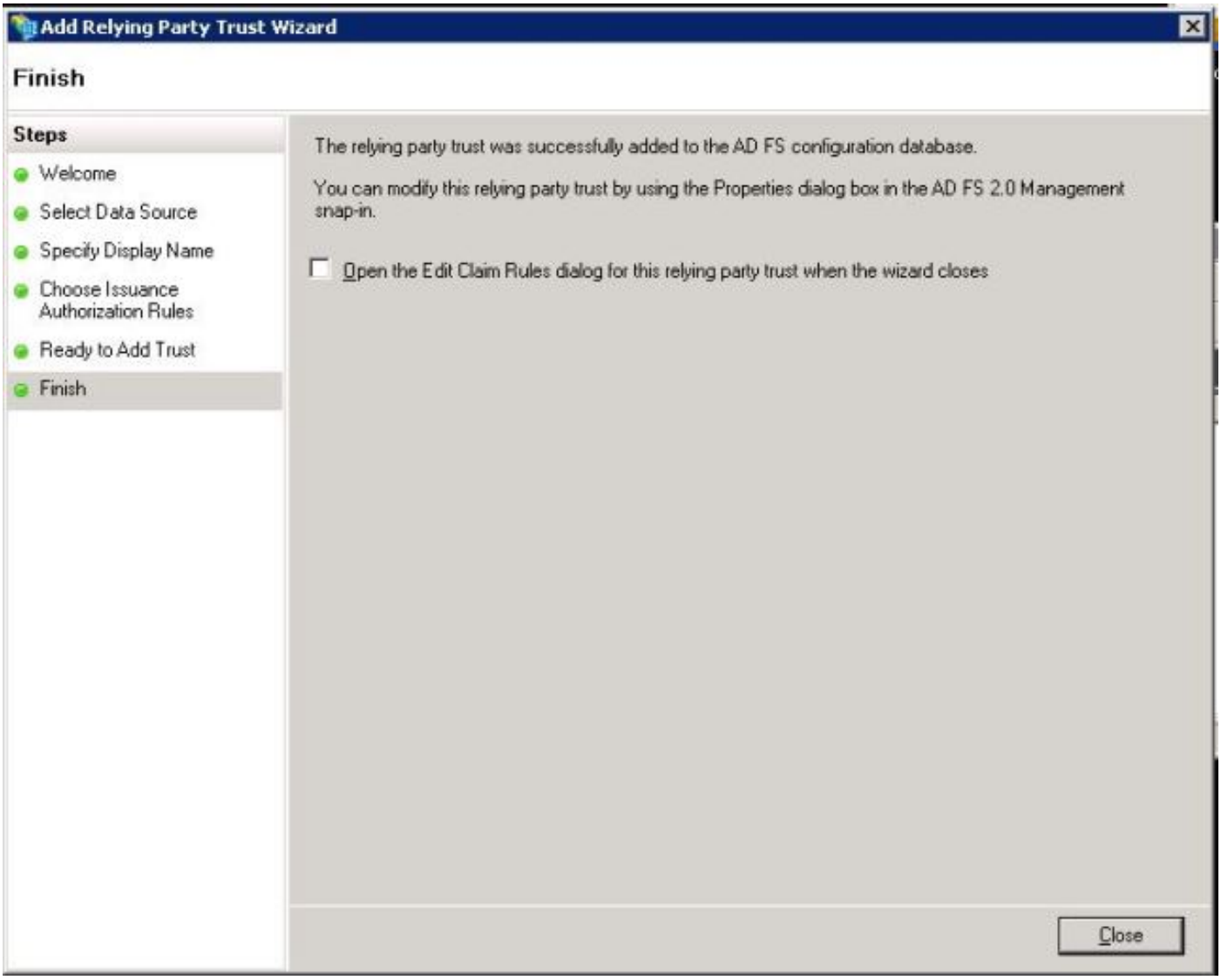
Permit **all users to access this relying party(모든 사용자가 이 신뢰 당사자**에 액세스하도록 허용)를 선택하여 모든 사용자가 이 신뢰 당사자에 액세스하도록 허용한 다음 이미지에 표시된 대로 **Next(다음**)를 클릭합니다.



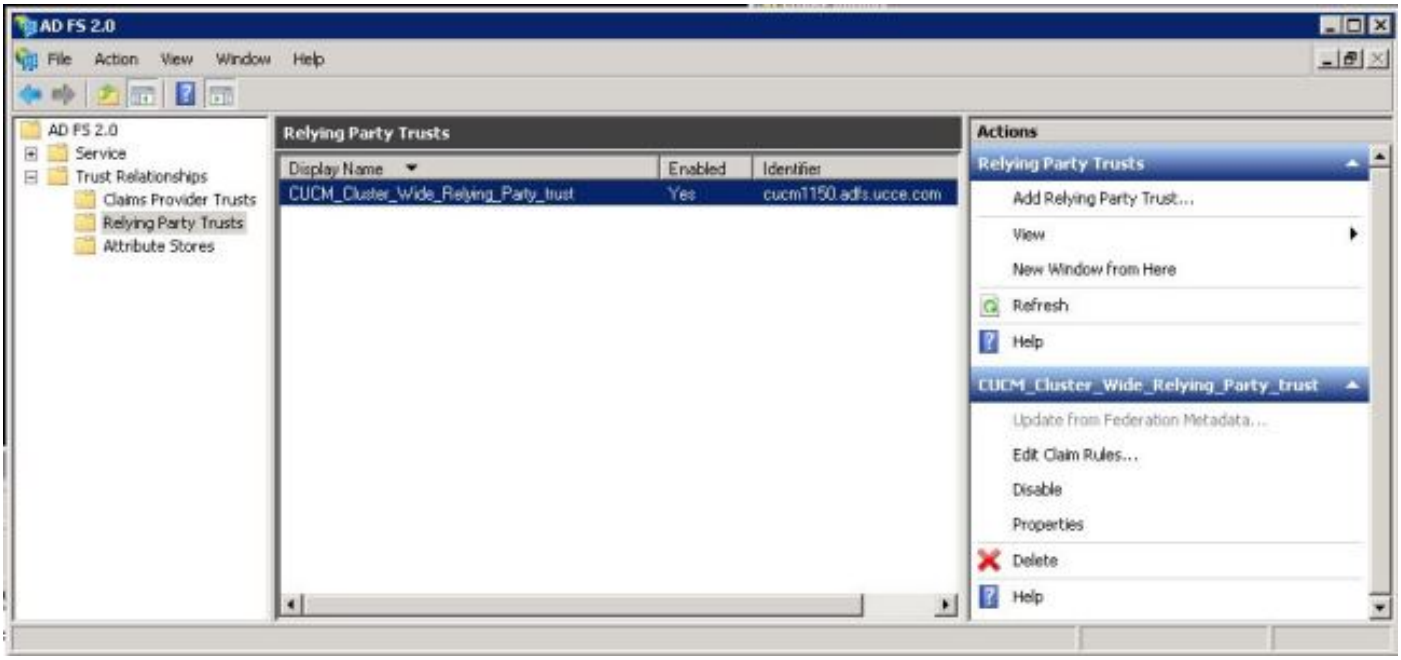
Ready to **Add Trust**(신뢰 추가 준비) 페이지에서 구성된 당사자 트러스트에 대한 설정을 검토할 수 있습니다.이제 이미지에 표시된 대로 Next(다음)를 클릭합니다.



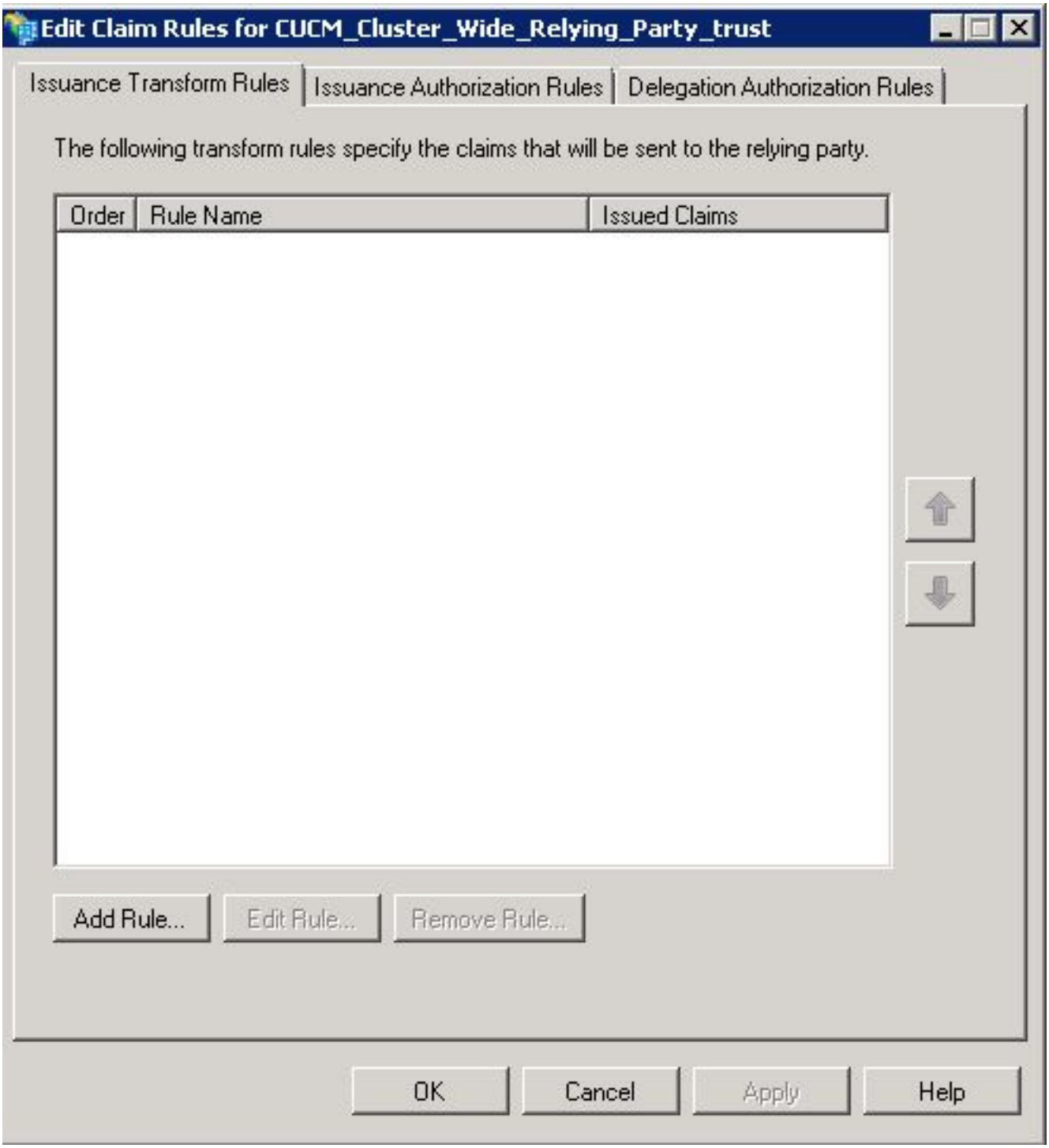
마침 페이지에서 신뢰 당사자 트러스트가 AD FS 구성 데이터베이스에 성공적으로 추가되었음을 확인합니다.다음 이미지에 표시된 대로 Box(상자)를 선택 취소하고 **Close(닫기)**를 클릭합니다.



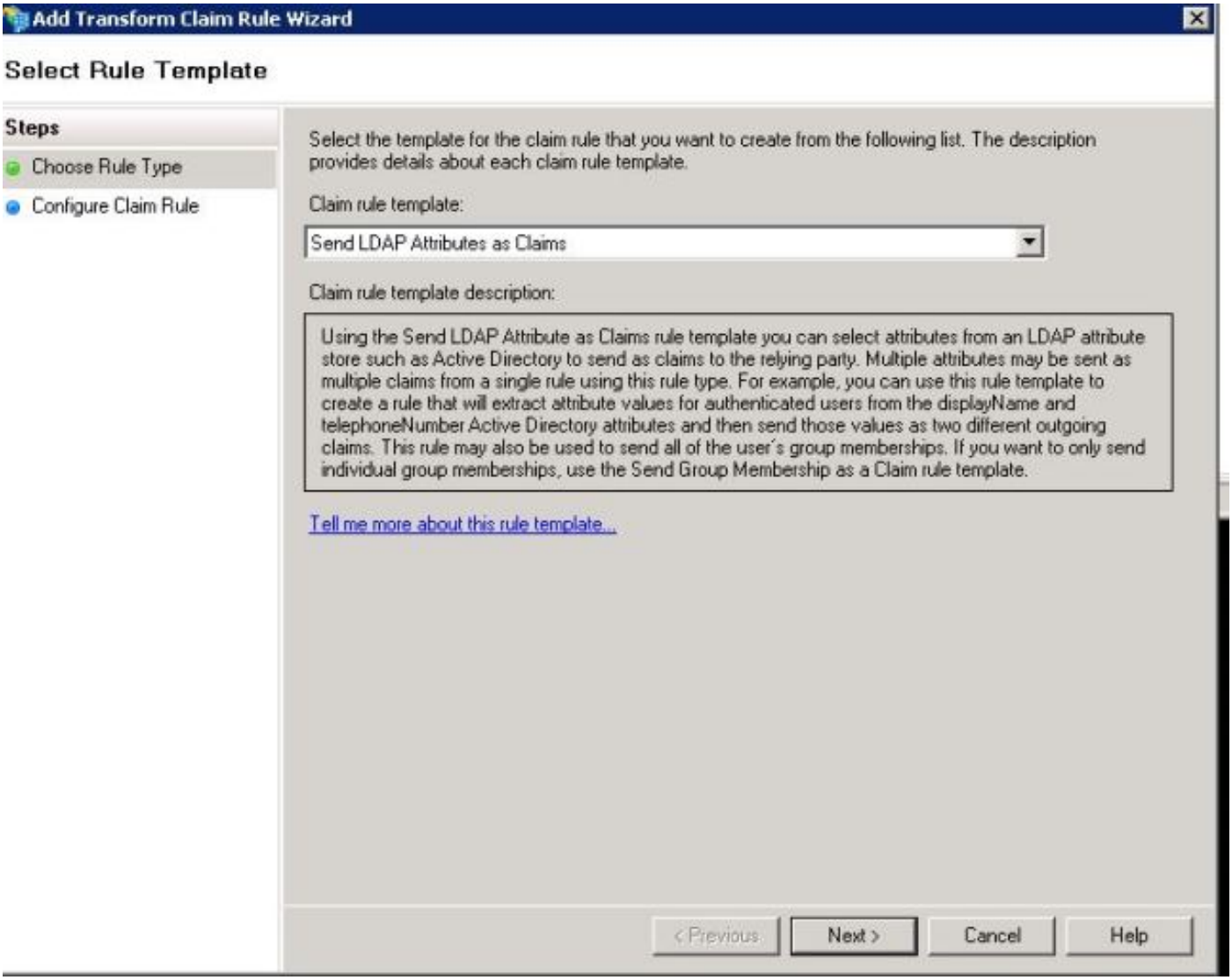
Relying Party Trust(**신뢰 당사자 트러스트**)를 마우스 오른쪽 버튼으로 클릭하고 **Edit Claim Rules(클레임 규칙 수정)를 클릭합니다**.



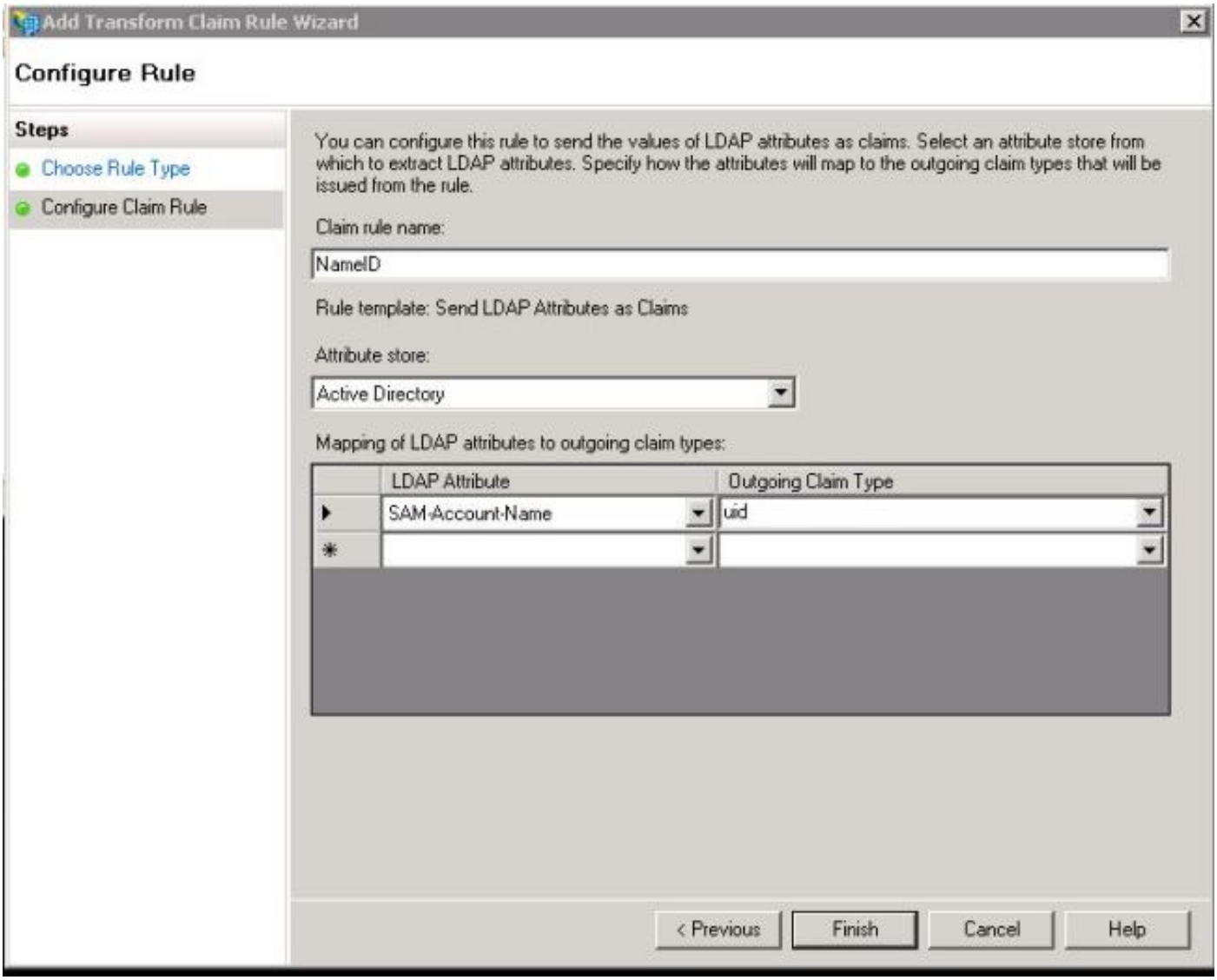
이제 이미지에 표시된 대로 **Add Rule.**을 클릭합니다.



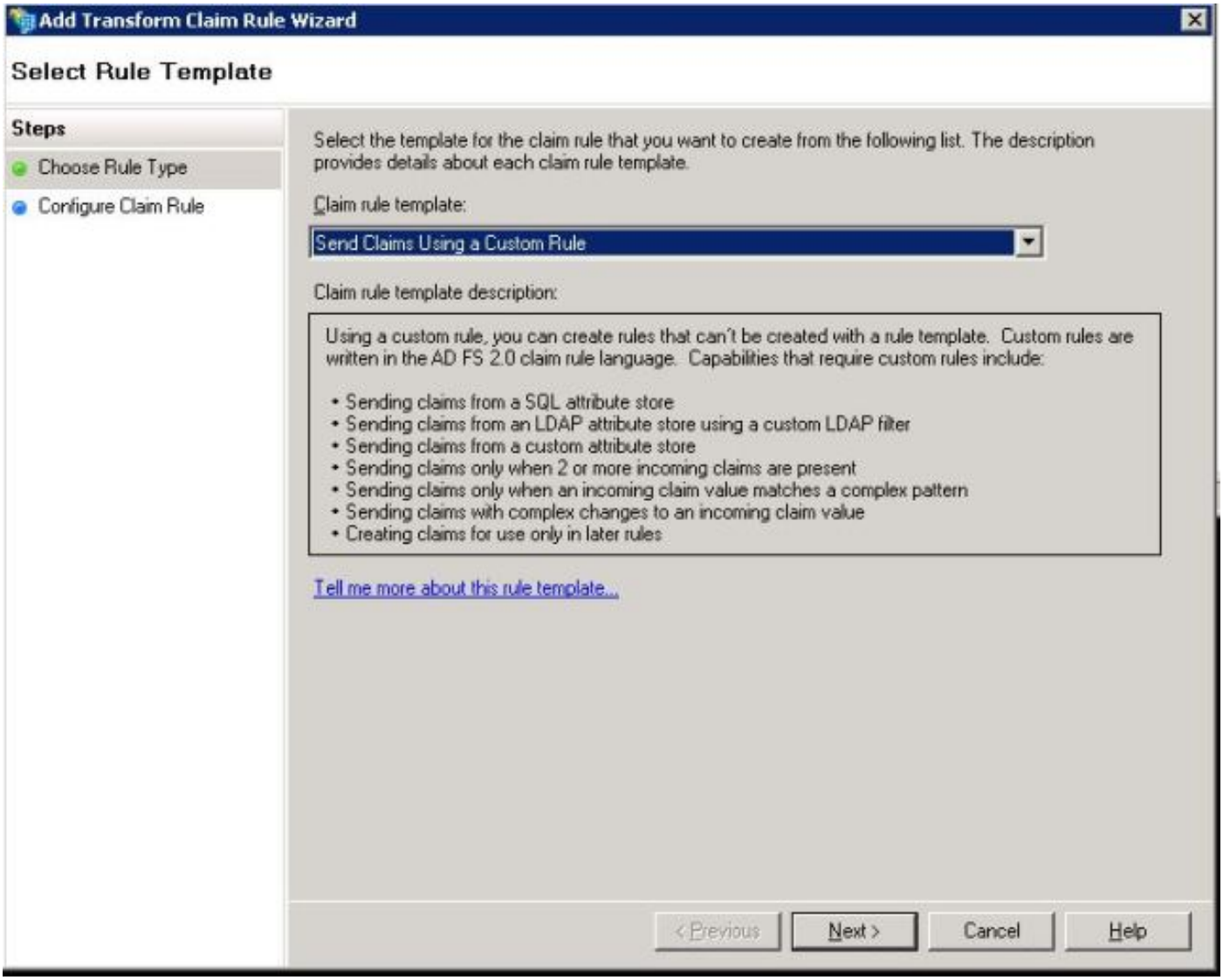
Add **Transform Claim Rule(변형 클레임 규칙 추가)**이 열리면 **Next(다음)**를 클릭하고 다음 이미지와 같이 기본 클레임 규칙 템플릿 **Send LDAP Attributes as Claims(LDAP 특성을 클레임으로 전송)**를 클릭합니다.



이 이미지**에** 표시된 대로 Configure Claim Rule을 클릭합니다.LDAP 특성은 CUCM의 LDAP 디렉토리 컨피그레이션에서 LDAP 특성과 일치해야 합니다.발신 클레임 유형을 uid로 **관리합니다**.이미지에 표시된 대로 **마침**을 클릭합니다.



신뢰 당사자에 대한 사용자 지정 규칙을 추가합니다.Add **rule을 클릭합니다**.Send **Claims using a Custom Rule(사용자 지정 규칙을 사용하여 클레임 보내기)을** 선택한 다음 이미지에 표시된 대로 **Next(다음)**를 클릭합니다.



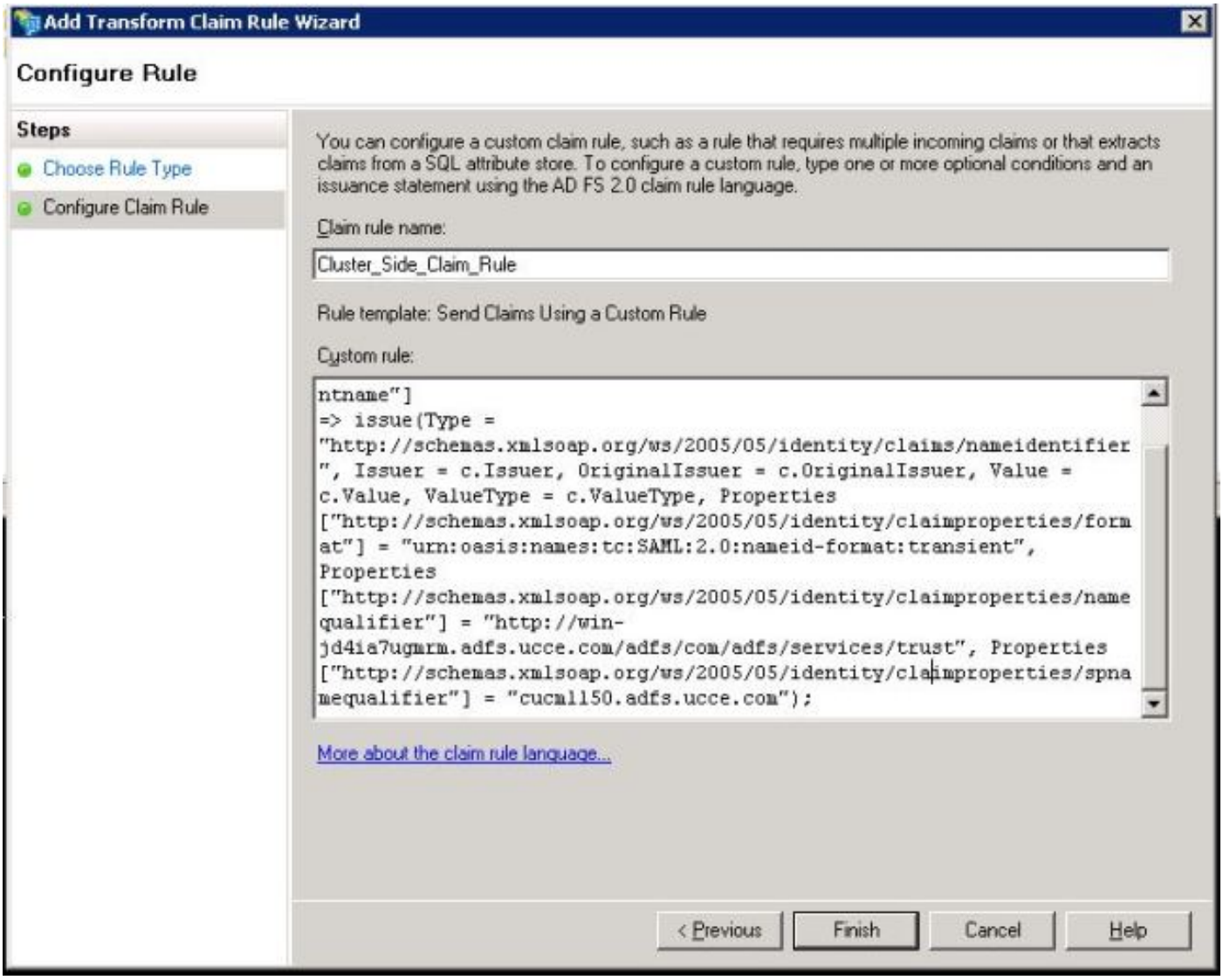
Configure Claim(클레임 구성) 규칙에서 Claim Rule Name(클레임 규칙 이름)을 입력한 다음 Claim(클레임) 규칙의 Namequalifier 및 spname 한정자를 수정하는 마법사의 Custom Rule(맞춤형 규칙) 필드에 Claim Rule Name(클레임 규칙 이름)과 Past(이전)를 복사합니다.이미지에 표시된 대로 Finish(마침)를 클릭합니다.

클레임 규칙:

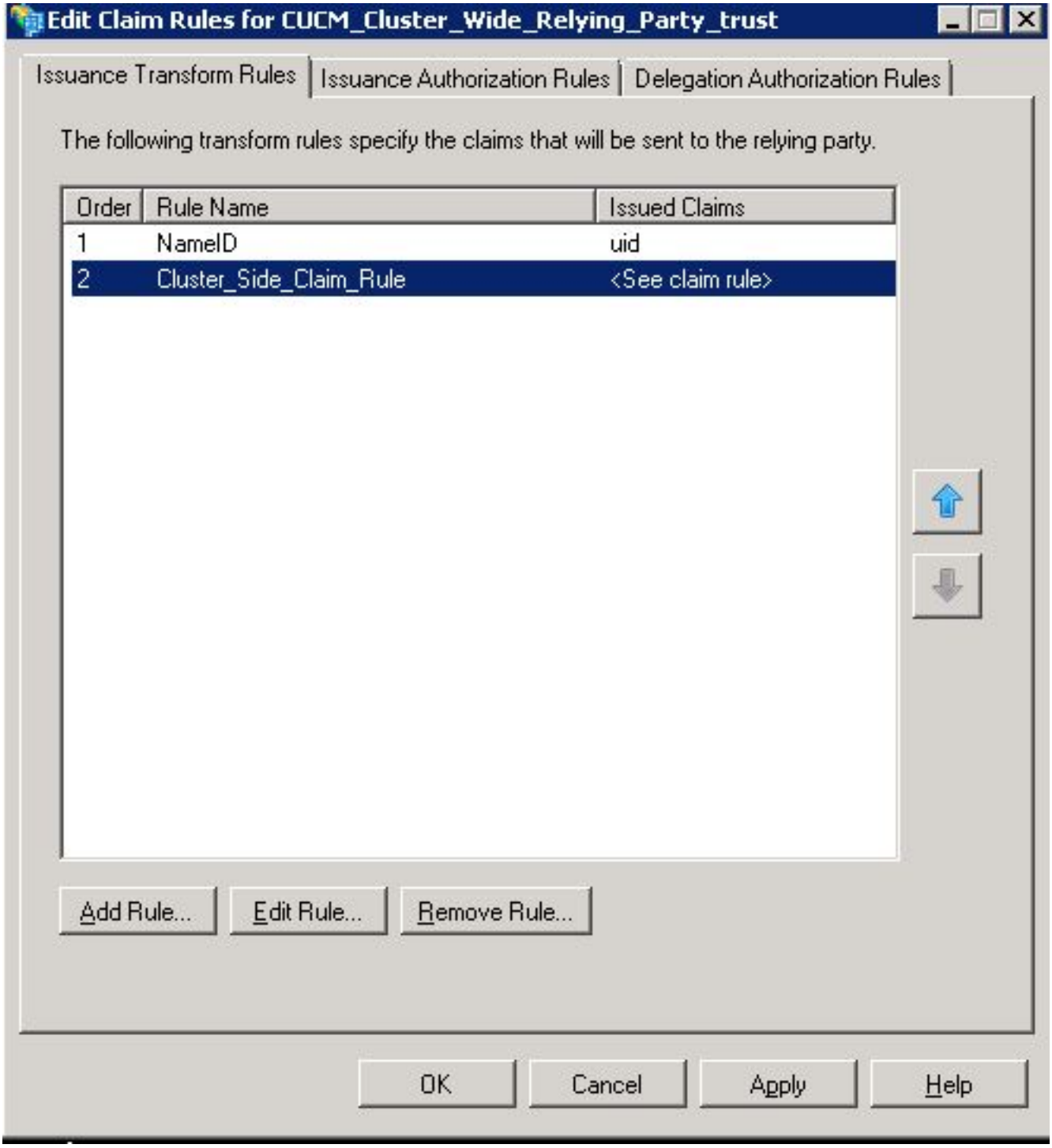
```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]

=> 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>/adfs/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"<Entity ID in the SP Metadata>");
```

Entity ID = Open the SP metadata and check the Entity ID. Basically, its the CUCM Publisher's FQDN.



이미지에 표시된 대로 Apply(적용)를 **클릭한** 다음 **OK(확인)를 클릭합니다**.

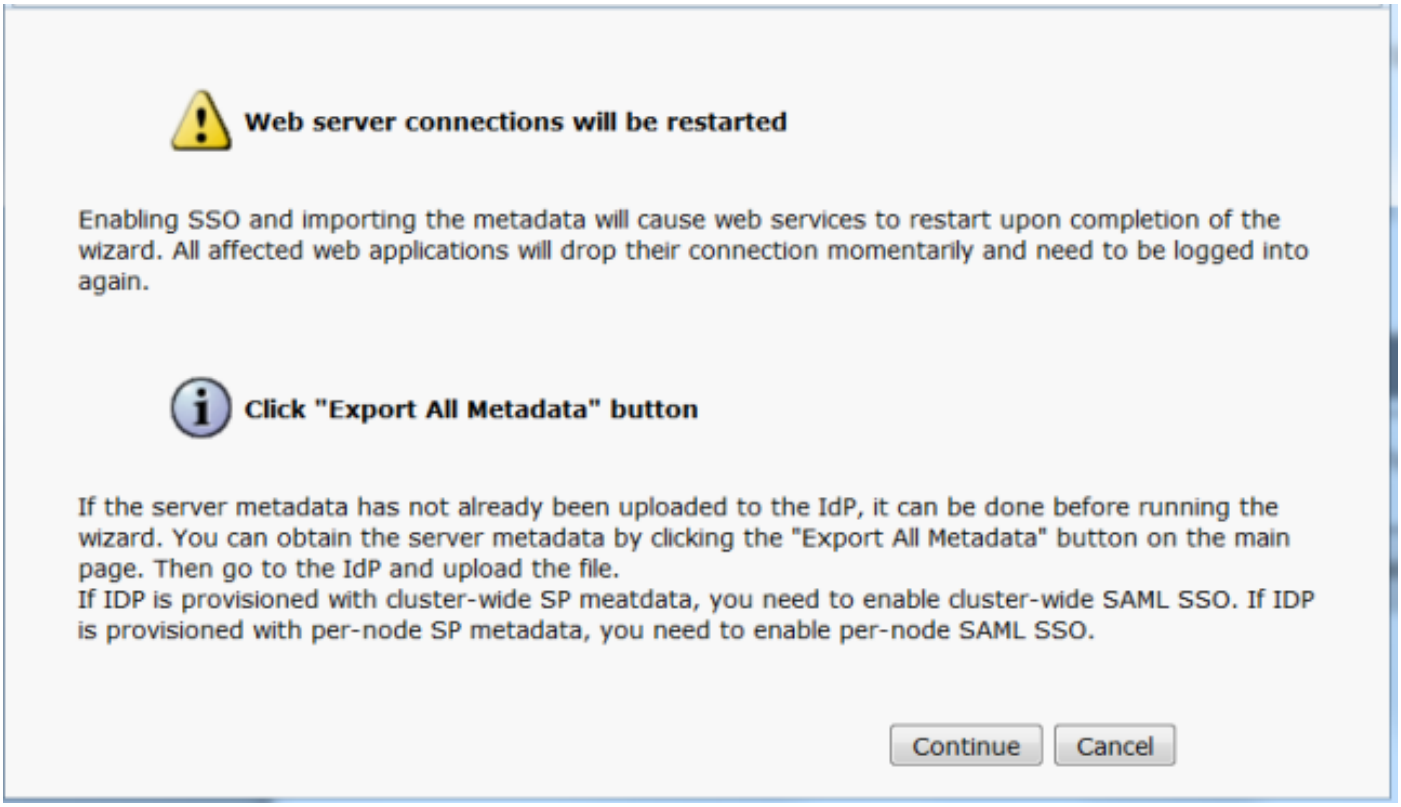


4단계. SAML SSO 활성화

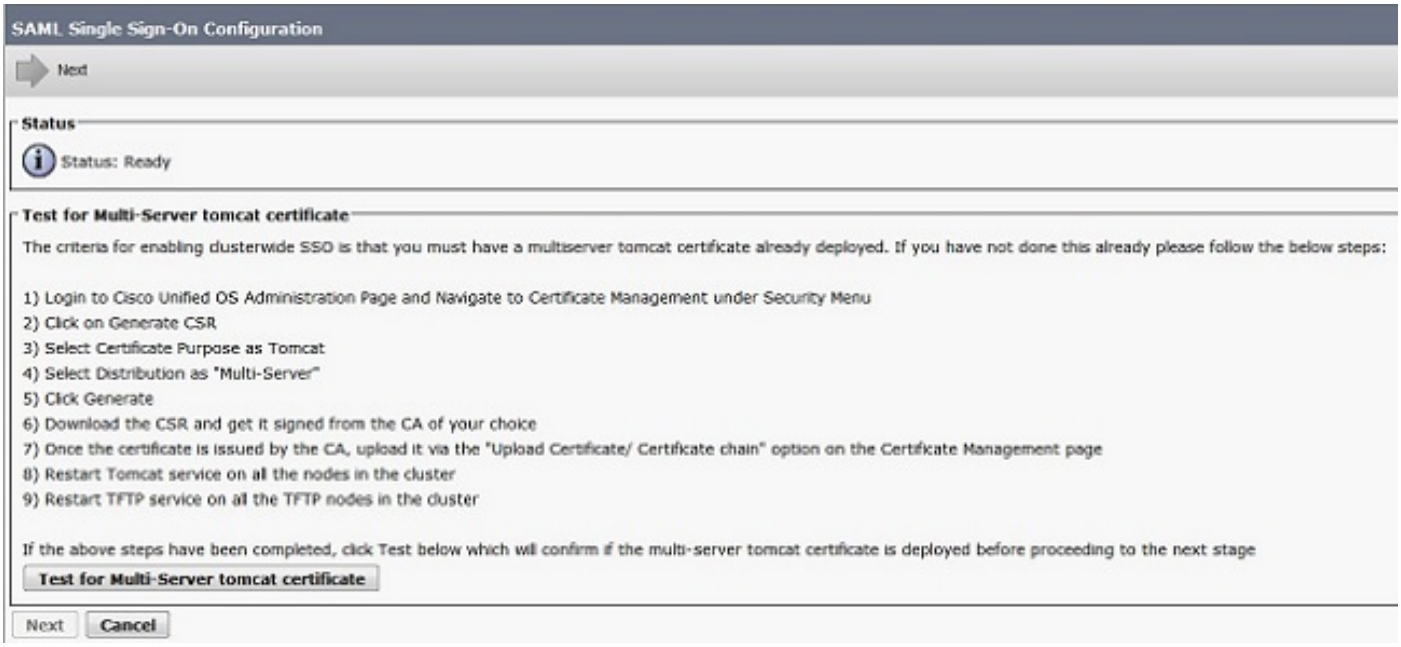
웹 브라우저를 열고 CUCM에 관리자로 로그인한 다음 System(시스템) **> SAML Single Sign On으로 이동합니다**.

기본적으로 **Cluster Wide** 라디오 버튼이 선택됩니다.이미지**에** 표시된 대로 Enable Saml SSO를 클릭합니다.

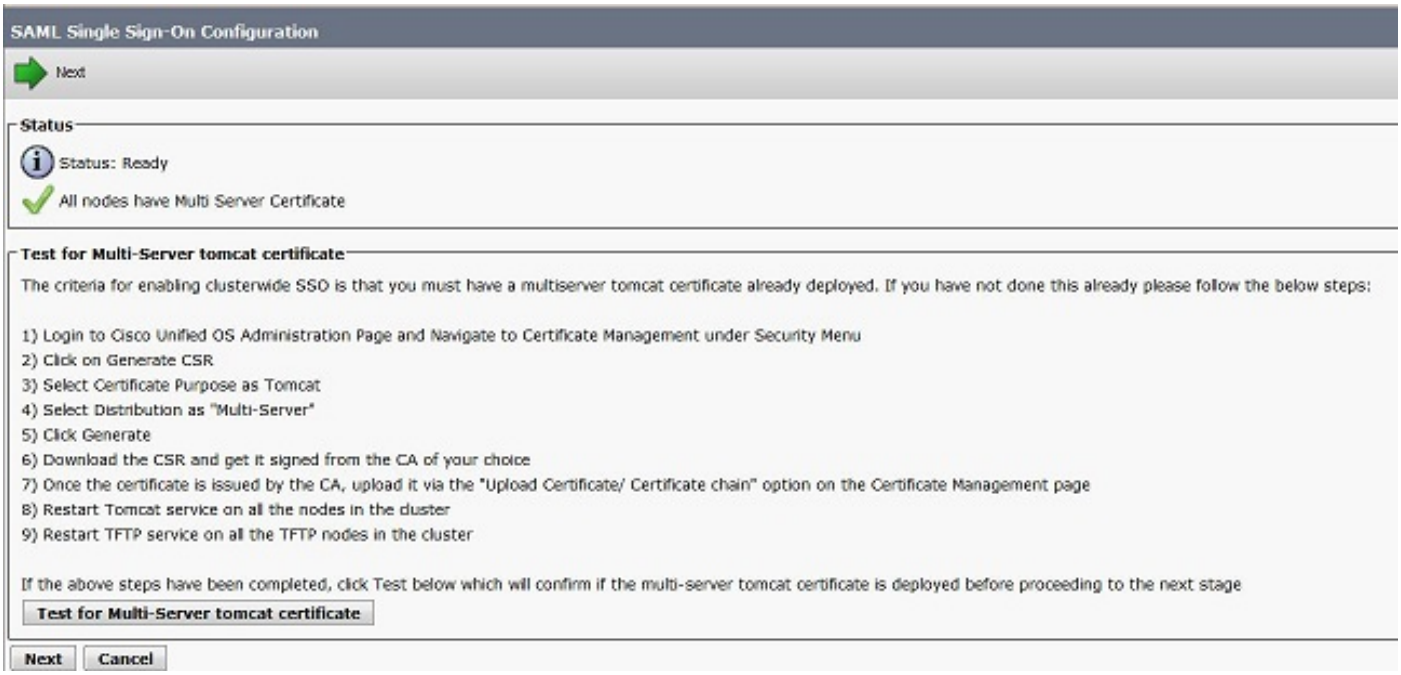
이미지에 표시된 대로 팝업에서는 웹 서버 재시작에 대한 경고 및 idp에 따라 클러스터 전반의 SAML SSO 또는 노드별 SAML SSO를 선택하는 정보를 알립니다.Continue(**계속)를 클릭합니다**.



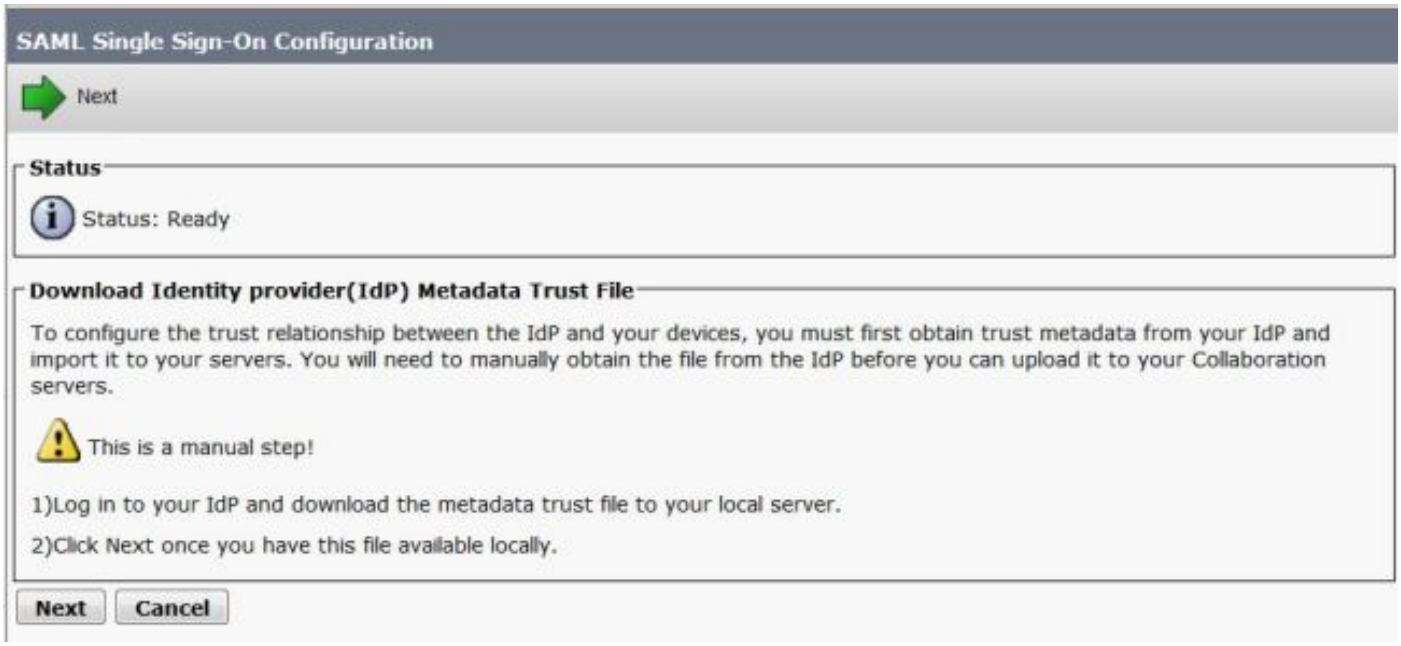
클러스터 전체 SSO를 활성화하는 기준은 멀티서버 tomcat 인증서가 이미 구축되어 있어야 한다는 것입니다.이미지**에** 표시된 대로 **Test for Multi-Server tomcat Certificate**를 클릭합니다.



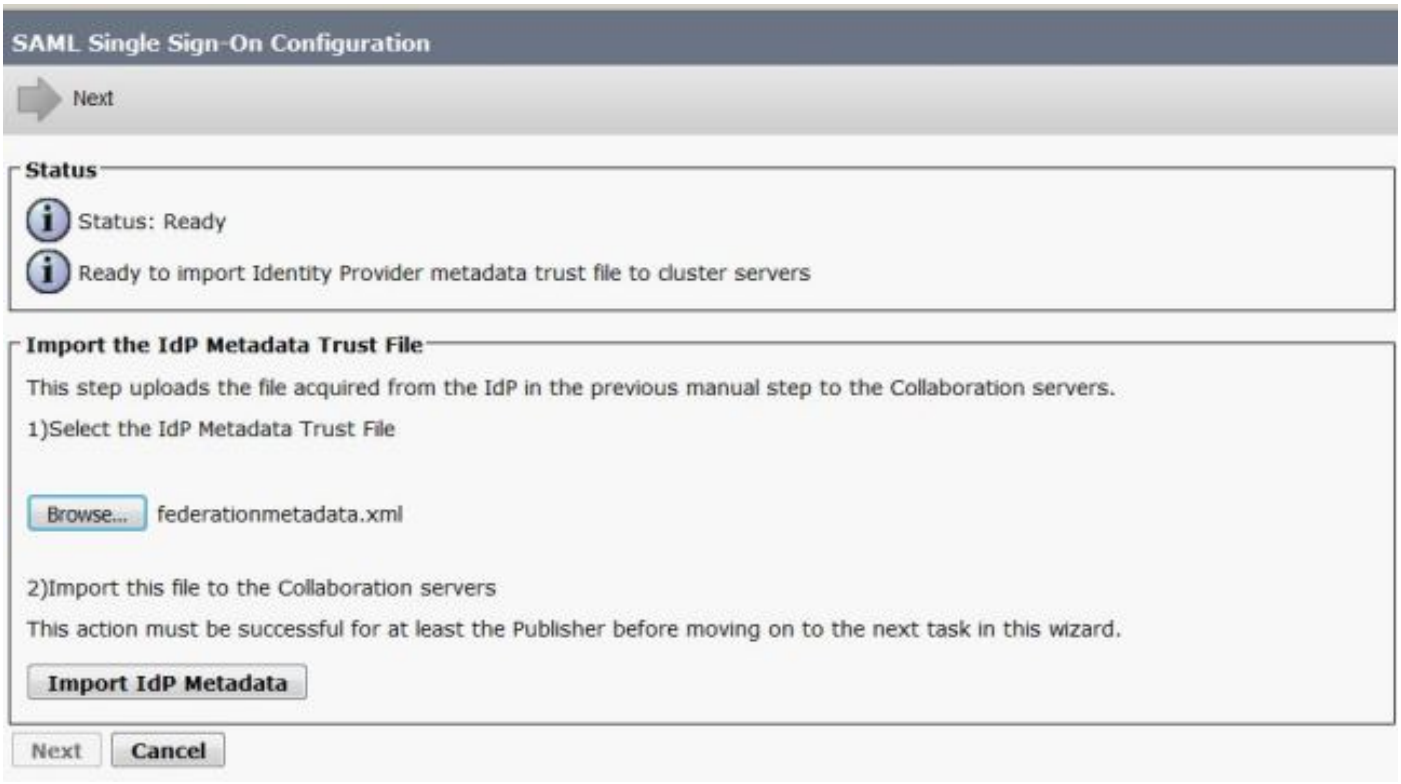
확인되면 모든 노드에 Multi Server Certificate(다중 서버 인증서)가 있으며 All Nodes have Multi Server Certificate(모든 노드에 다중 서버 인증서 있음)가 표시됩니다. 그런 다음 이미지에 표시된 대로 Next(다음)를 클릭합니다.



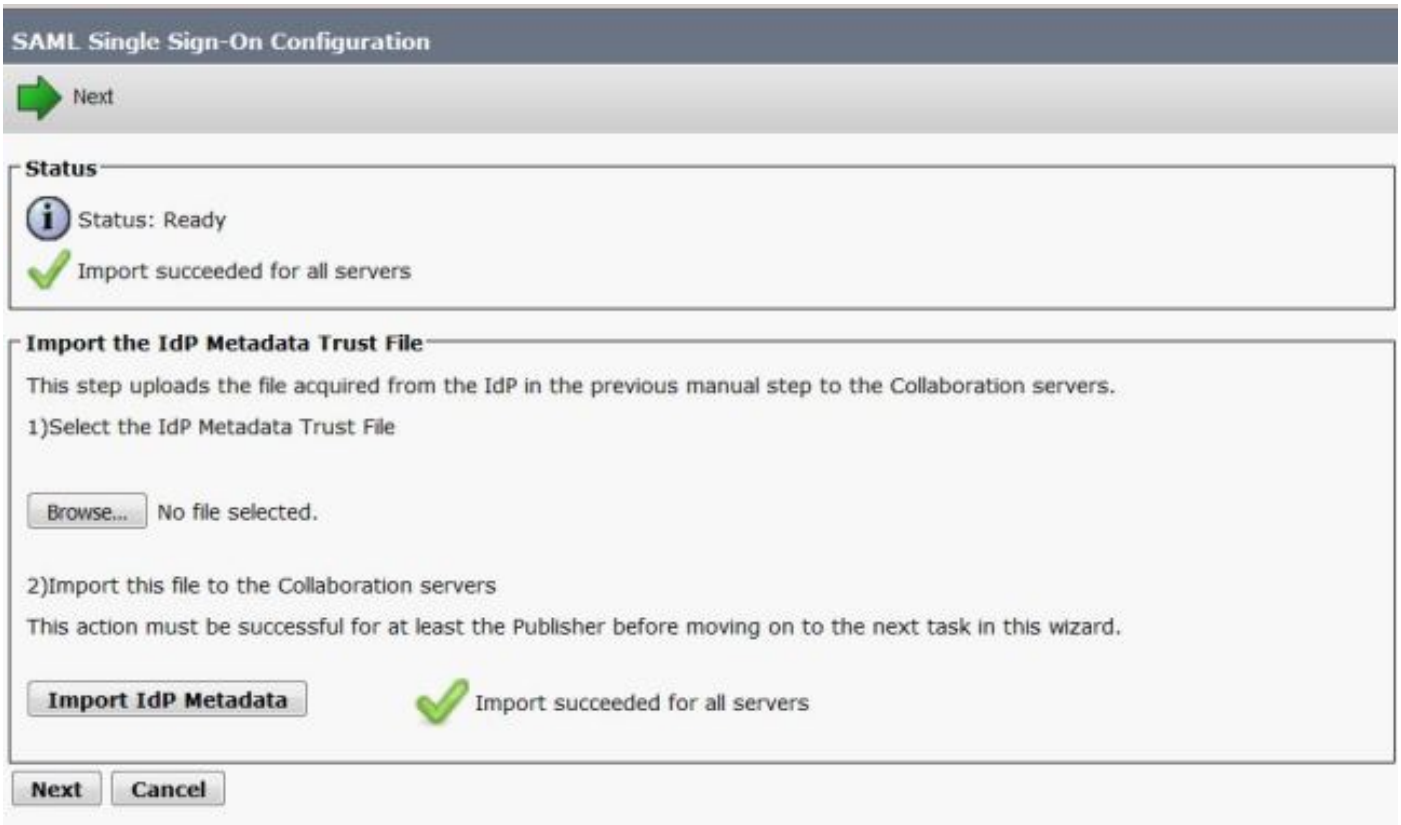
이미지에 표시된 대로 다음을 클릭합니다.



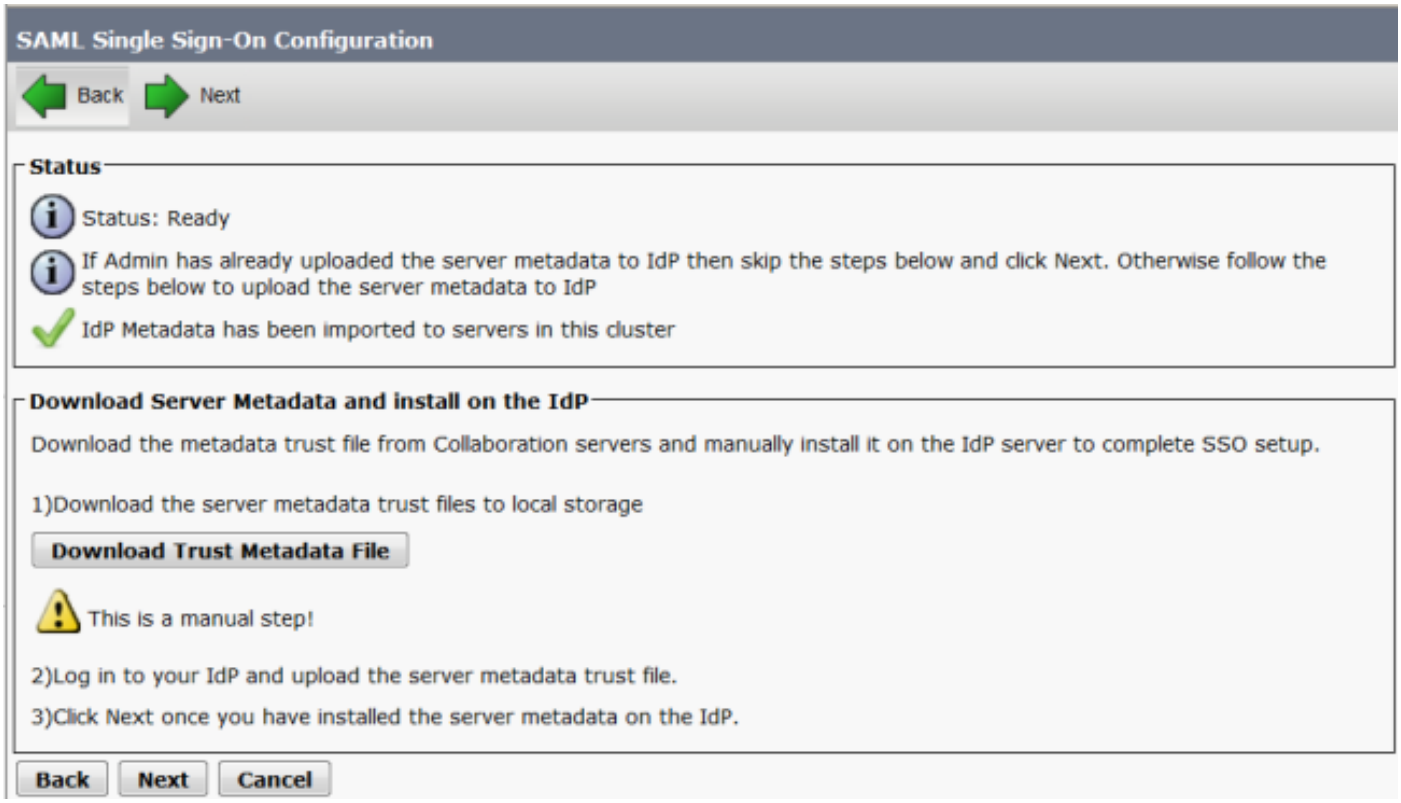
다운로드한 IdP 메타데이터를 찾아 선택합니다.이미지에 표시된 대로 Import IdP Metadata를 클릭합니다.



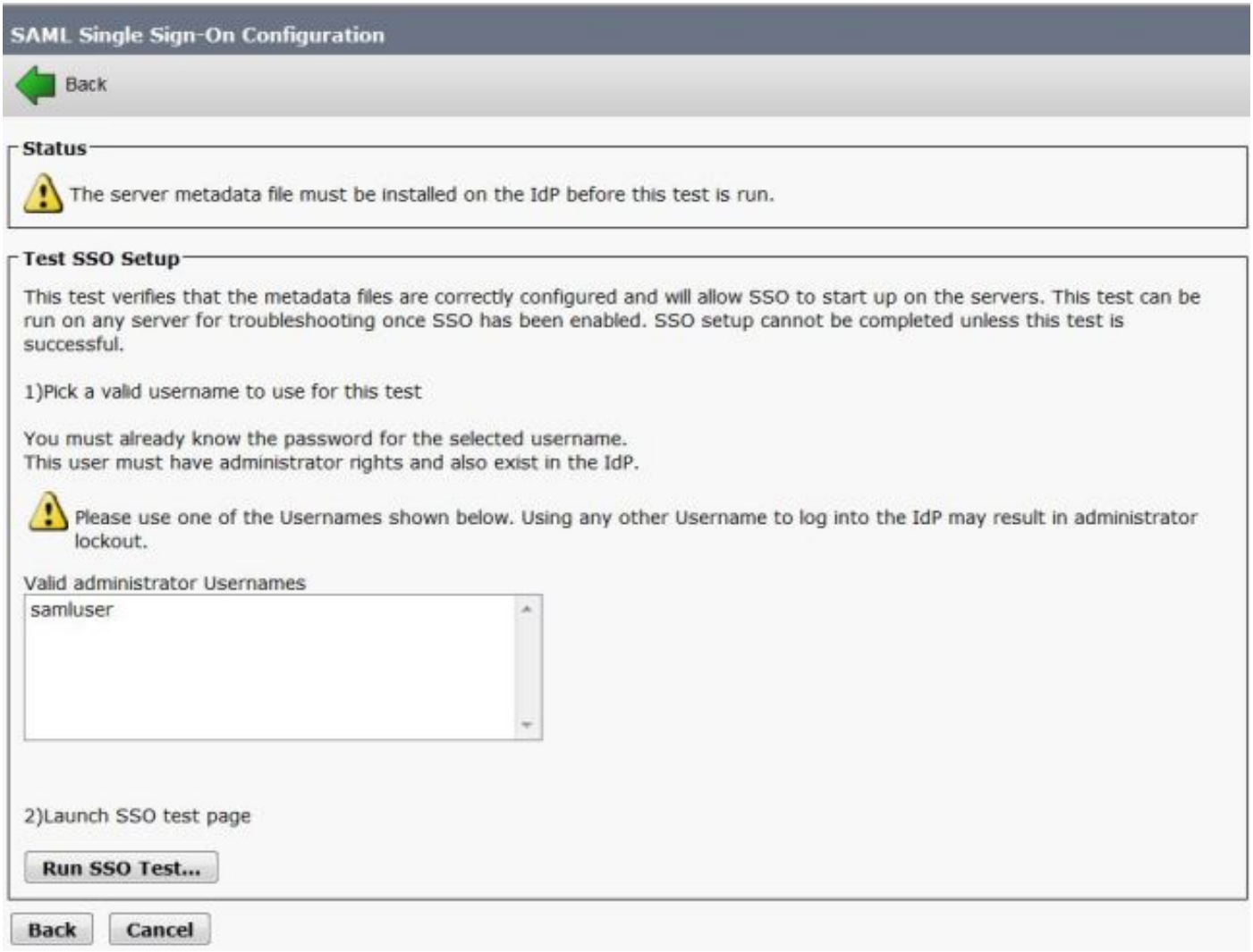
이 페이지에서는 모든 서버에 대해 가져오기 성공 확인을 한 다음 이미지에 표시된 대로 **다음**을 클릭합니다.



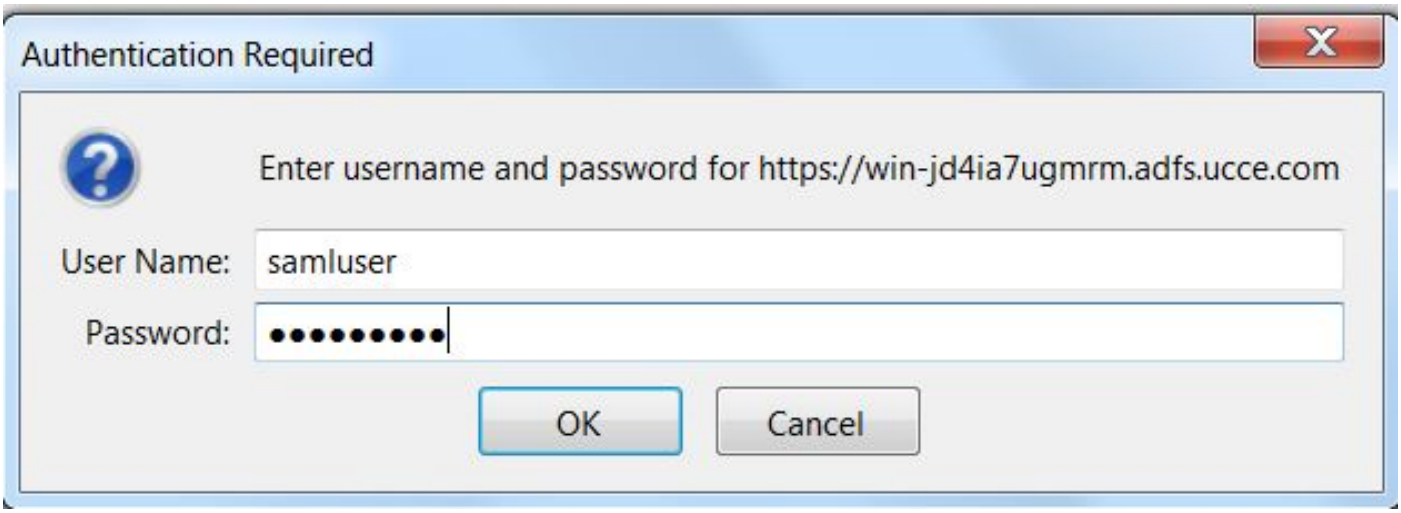
이미지에 표시된 대로 **Next(다음)**를 클릭합니다. 초기 SAML SSO 컨피그레이션 페이지에서 SP 메타데이터를 이미 내보냈기 때문입니다.



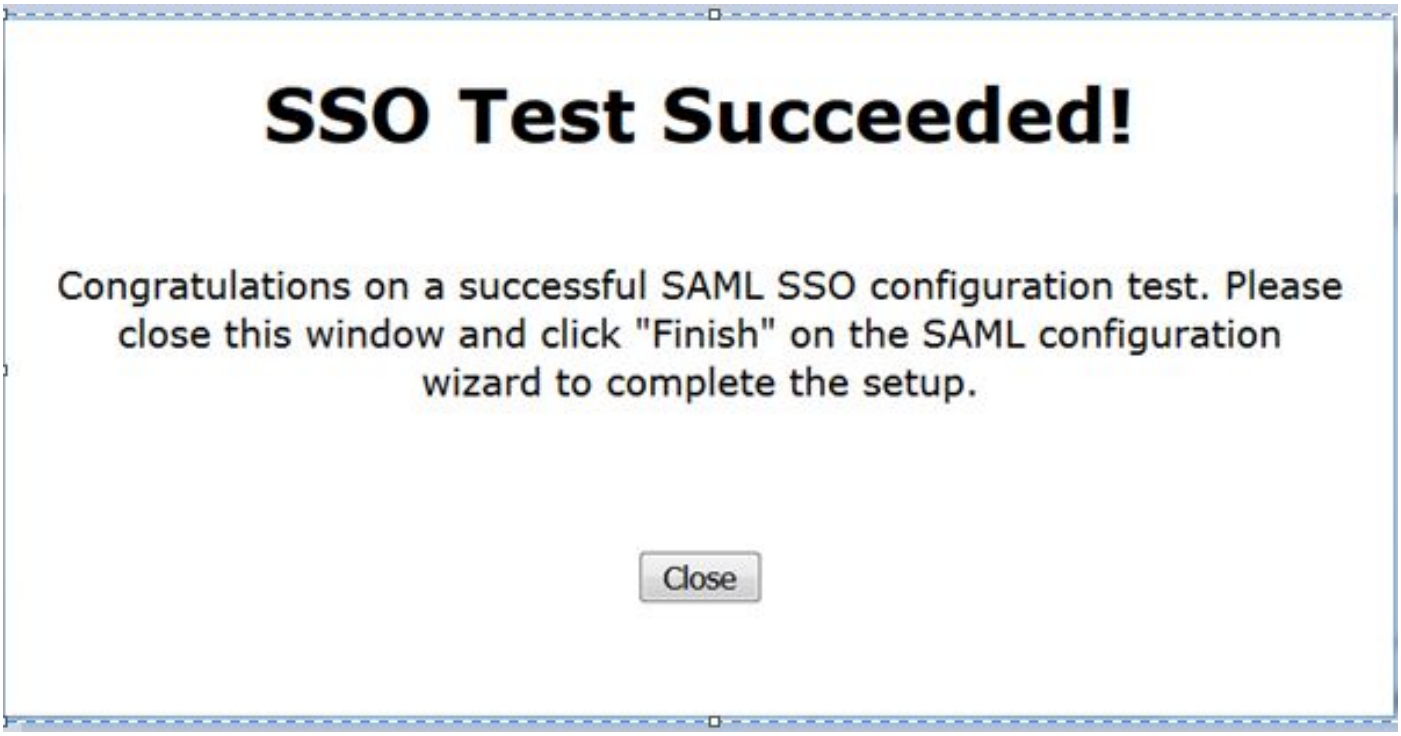
CUCM은 LDAP 디렉토리와 동기화되어야 합니다.마법사는 LDAP 디렉토리에 구성된 유효한 관리자 사용자를 표시합니다.사용자를 선택하고 이미지에 표시된 대로 **SSO 테스트 실행**을 클릭합니다.



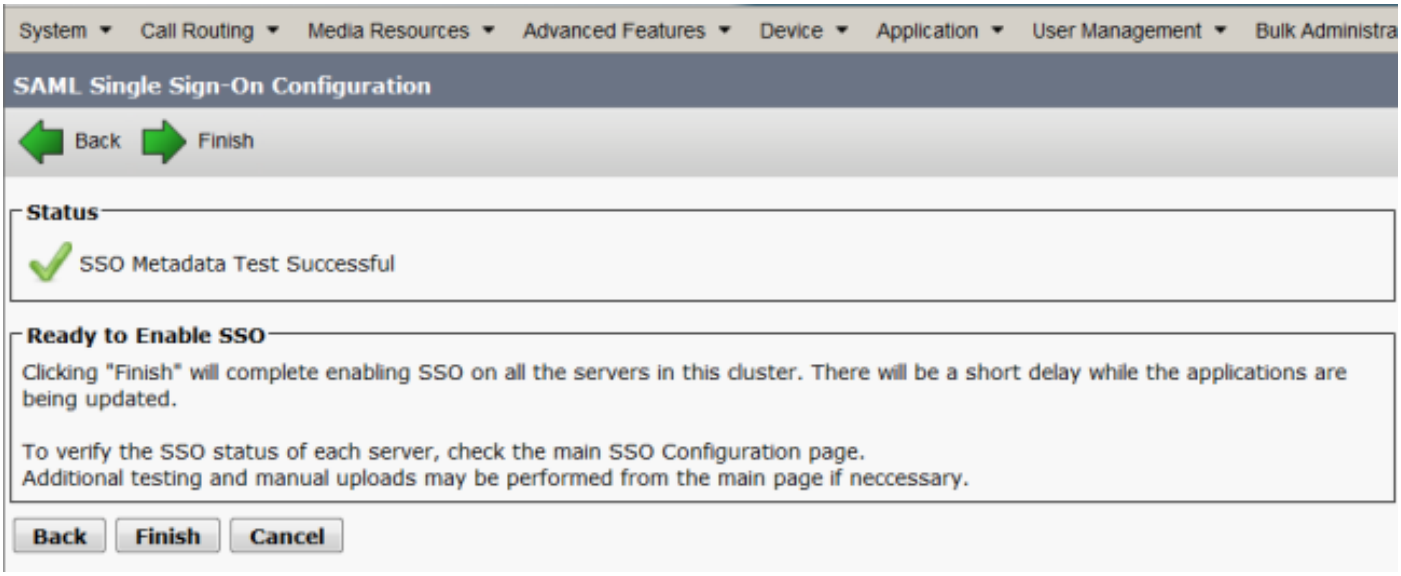
이미지에 표시된 대로 프롬프트되면 사용자 ID와 각 비밀번호를 입력합니다.



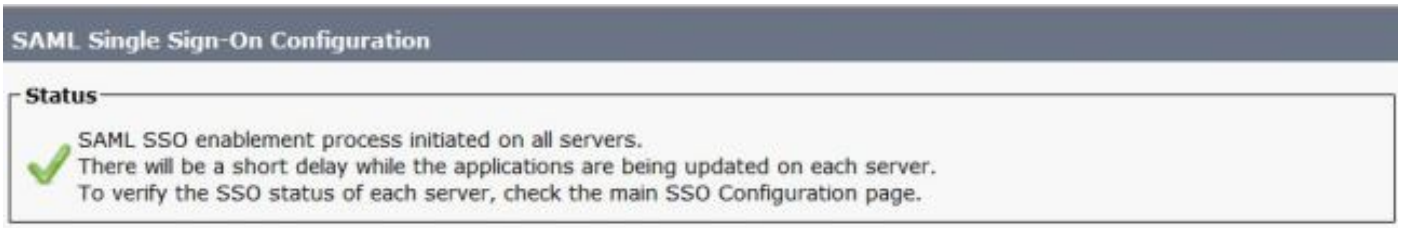
이미지에 표시된 것처럼, 테스트가 Succeeded(성공)입니다.



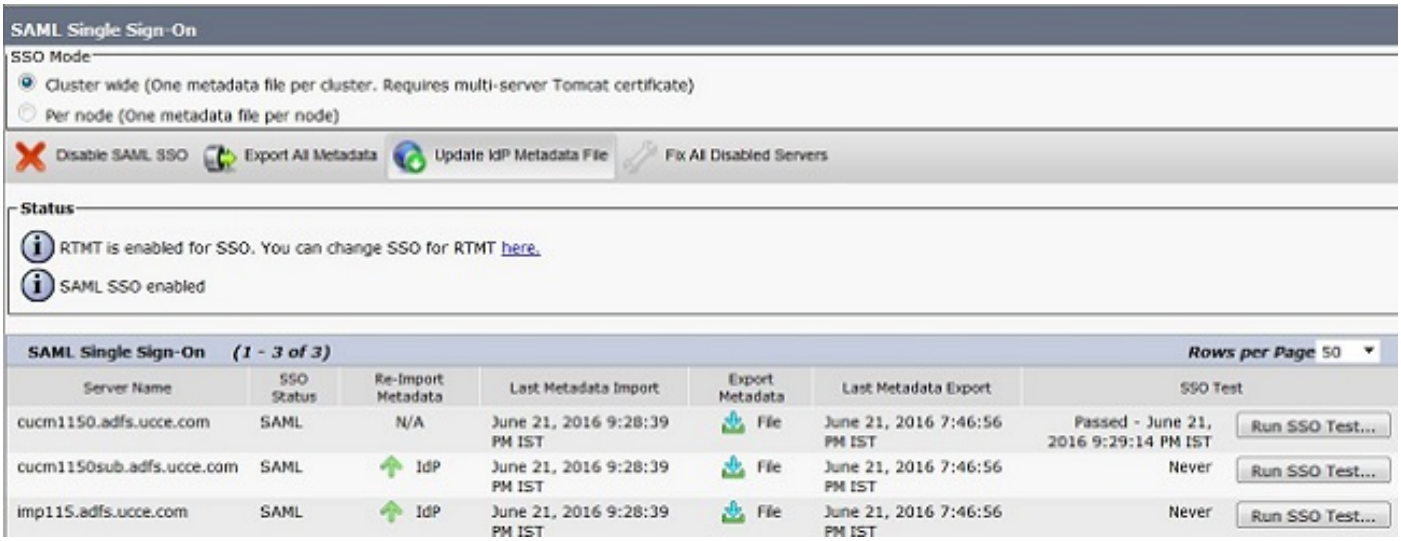
이미지에 표시된 대로 Finish(**마침)를** 클릭하여 SSO 활성화 컨피그레이션을 완료합니다.



이미지에 표시된 페이지는 모든 서버에서 SAML SSO 활성화 프로세스가 시작되었음을 확인합니다.



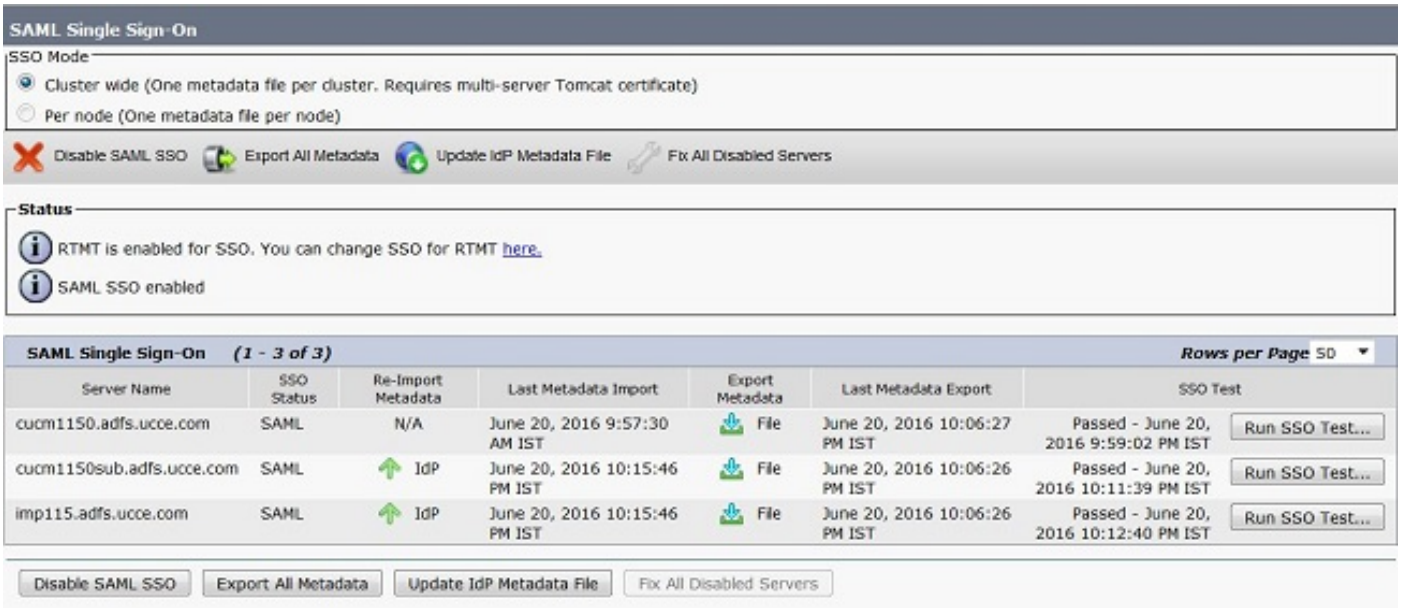
SAML SSO 자격 증명을 사용하여 로그아웃하고 CUCM에 다시 로그인합니다.**[시스템] >SAML Single Sign On**으로 이동합니다. 이미지에 표시된 대로 클러스터의 다른 노드에 대해 SSO 테스트 실행을 누릅니다.



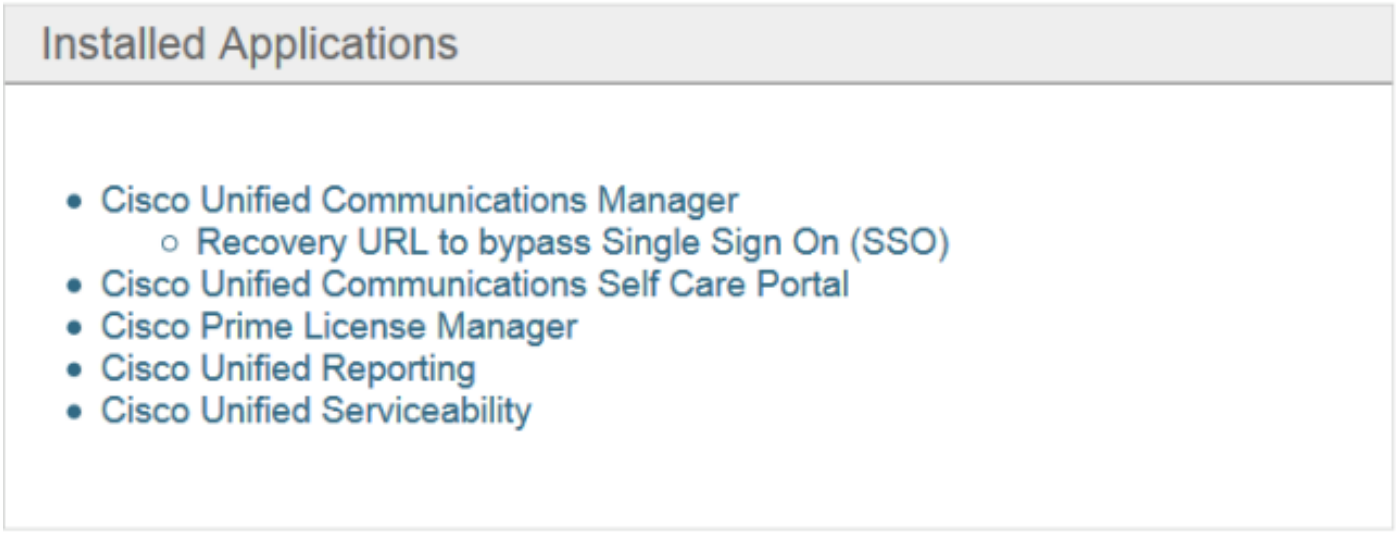
다음을 확인합니다.

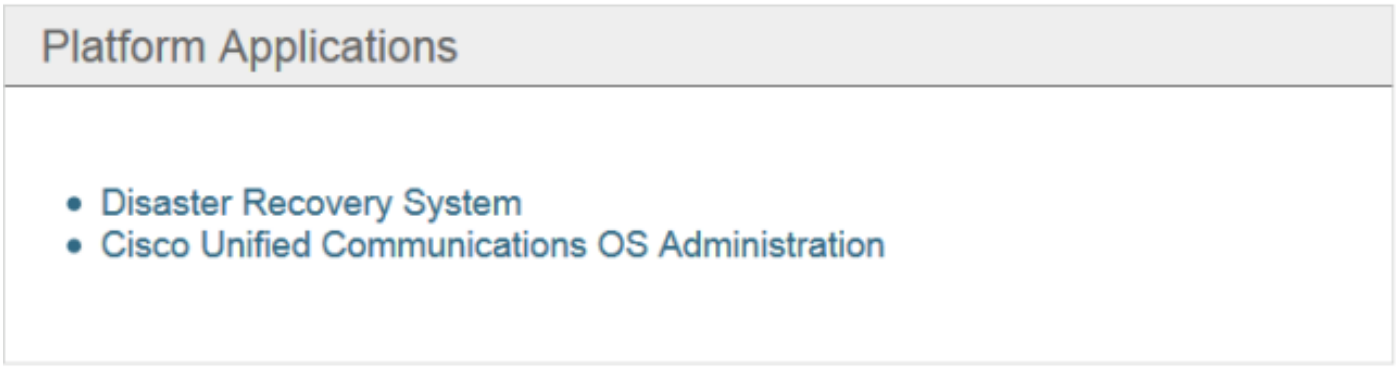
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

SAML SSO가 활성화된 노드에 대해 SSO 테스트가 성공했는지 확인합니다.System(**시스템) > SAML Single Sign On으로 이동합니다**.Successful SSO 테스트에는 Passed(통과) 상태가 표시됩니다.



SAML SSO가 활성화되면 이 이미지와 같이 CUCM 로그인 페이지에 대해 설치된 애플리케이션 및 플랫폼 애플리케이션이 나열됩니다.





SAML SSO가 활성화되면 다음 이미지와 같이 IM and Presence 로그인 페이지에 대해 설치된 애플리케이션 및 플랫폼 애플리케이션이 나열됩니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

SSO 로그를 디버깅하도록 설정하려면 명령 **set samltrace level DEBUG**를 사용합니다.

RTMT를 사용하여 SSO 로그를 수집하거나 CLI를 사용하여 **activelog /tomcat/logs/ssosp/log4j/*.log** 위치**에서** 수집합니다.

SSO 로그의 예는 생성된 메타데이터와 다른 노드로 전송되는 메타데이터를 보여줍니다.

```
2016-05-28 14:59:34,026 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call GET
API to generate Clusterwide SP Metadata in the Local node.
2016-05-28 14:59:47,184 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call to
post the generated SP Metadata to other nodes
2016-05-28 14:59:47,185 INFO  [http-bio-443-exec-297] cluster.SAMLSSOClusterManager -
Begin:postClusterWideSPMetaData
2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Nodes
[cucm1150, cucm1150sub.adfs.ucce.com]
2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post
ClusterWideSPMetadata to the cucm1150
2016-05-28 14:59:47,187 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post
ClusterWideSPMetadata to the cucm1150sub.adfs.ucce.com
```