CUCM 및 AD FS 2.0으로 Single Sign-On 구성

목차

소개

이 문서에서는 Cisco Unified Communications Manager 및 Active Directory Federation Service에서 SSO(Single Sign-On)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CUCM(Cisco Unified Communications Manager)
- AD FS(Active Directory Federation Service)에 대한 기본 지식

실습 환경에서 SSO를 활성화하려면 다음 컨피그레이션이 필요합니다.

- AD FS가 설치된 Windows Server.
- LDAP 동기화가 구성된 CUCM
- 표준 CCM 슈퍼 사용자 역할이 선택된 최종 사용자.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Windows Server(AD FS 2.0 포함)
- CUCM 10.5.2

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 정보

Windows Server 2008 R2를 사용하는 AD FS 2.0에 대한 절차가 제공됩니다. 이 단계는 Windows Server 2016의 AD FS 3.0에서도 작동합니다.

Windows 서버에 AD FS 2.0 다운로드 및 설치

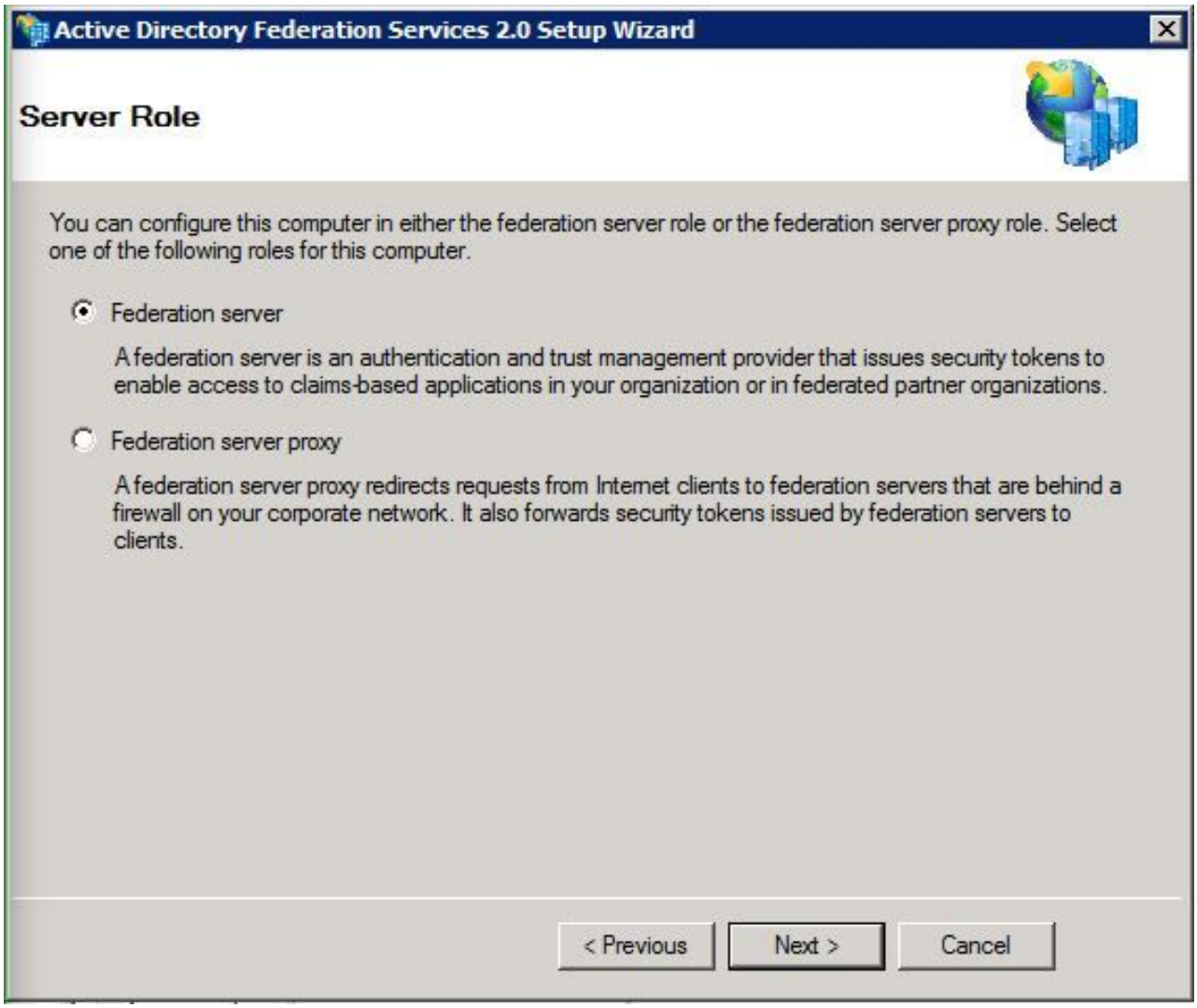
1단계. Download AD FS 2.0(AD FS 2.0 다운로드)으로 이동합니다.

2단계. Windows Server에 따라 적절한 다운로드를 선택했는지 확인합니다.

3단계. 다운로드한 파일을 Windows 서버로 이동합니다.

4단계. 설치를 진행합니다.

5단계. 프롬프트가 표시되면 Federation Server(페더레이션 서버)를 선택합니다.



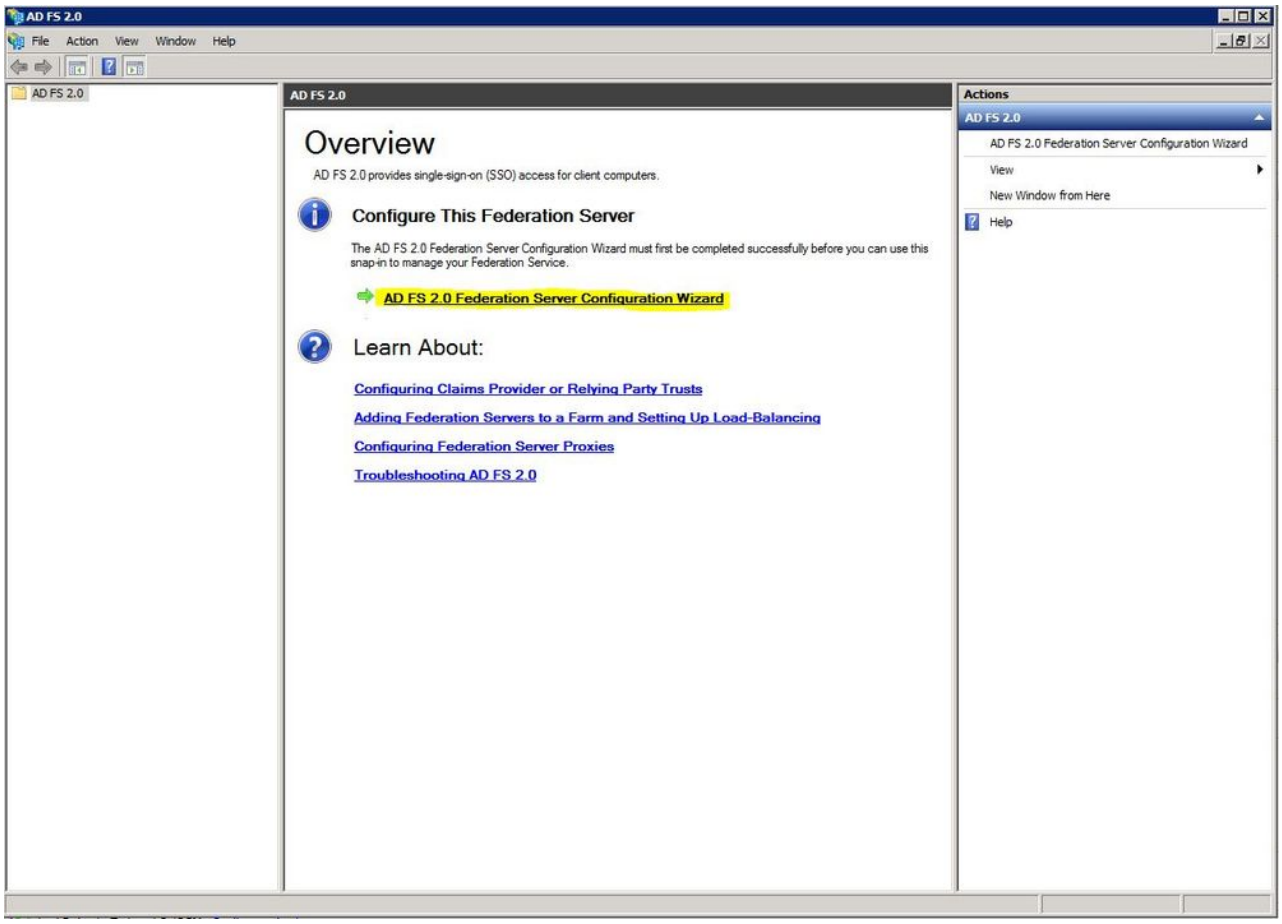
6단계. 일부 종속성이 자동으로 설치됩니다. 설치가 완료되면 [마침]을 클릭합니다.

이제 서버에 AD FS 2.0이 설치되었으므로 일부 컨피그레이션을 추가해야 합니다.

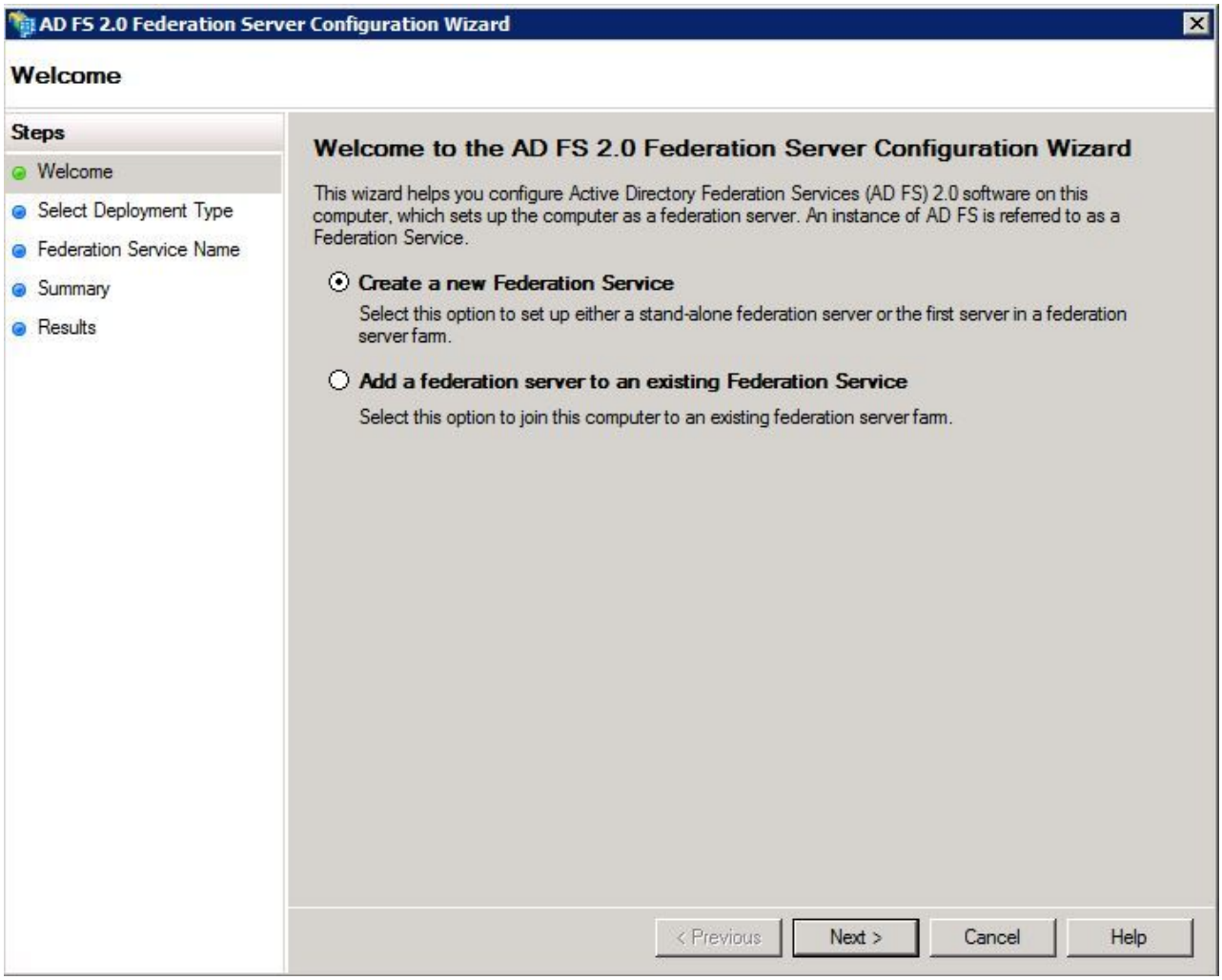
Windows 서버에서 AD FS 2.0 구성

1단계. 설치 후 AD FS 2.0 창이 자동으로 열리지 않으면 시작을 클릭하고 AD FS 2.0 관리를 검색하여 수동으로 열 수 있습니다.

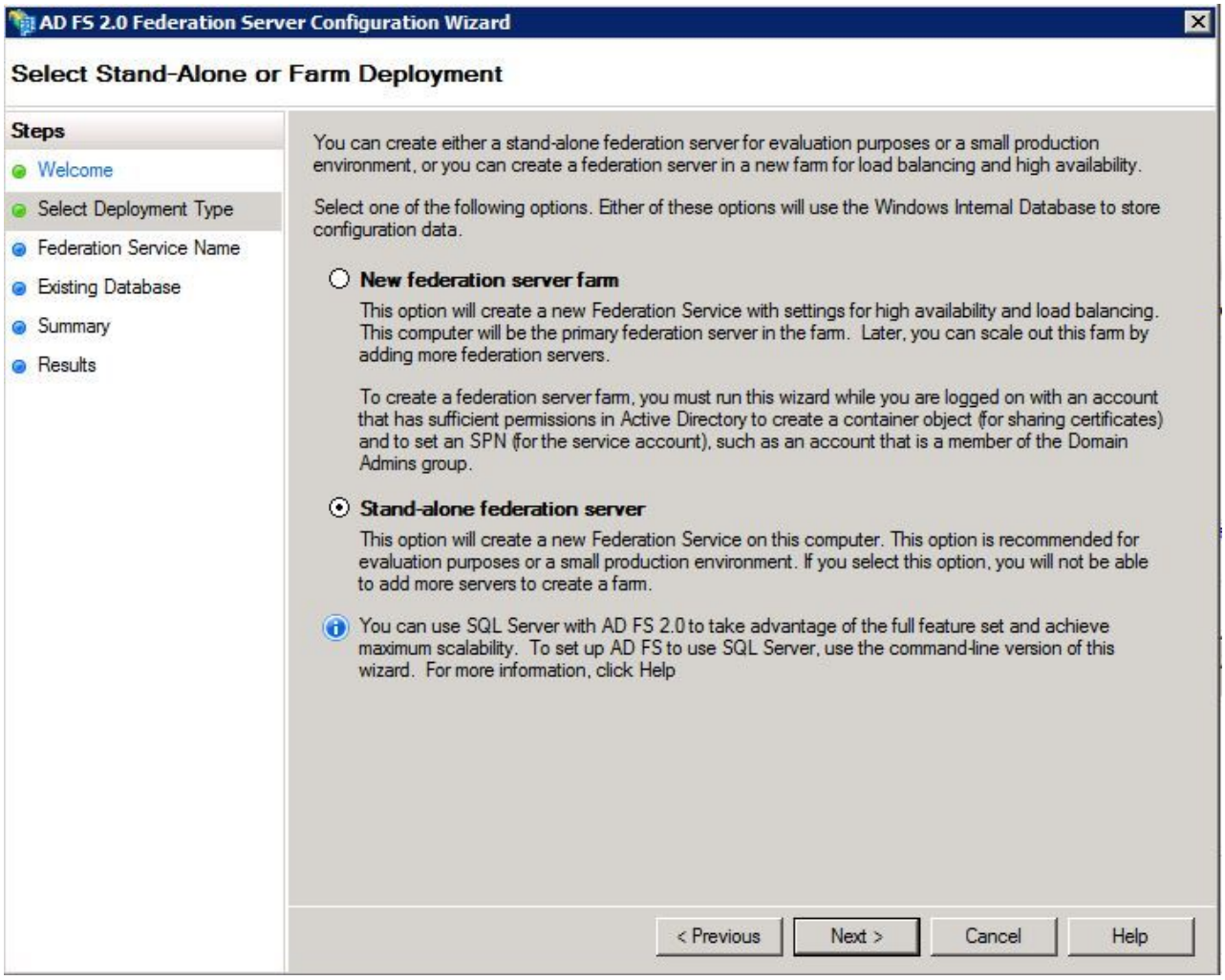
2단계. AD FS 2.0 Federation Server Configuration Wizard를 선택합니다.



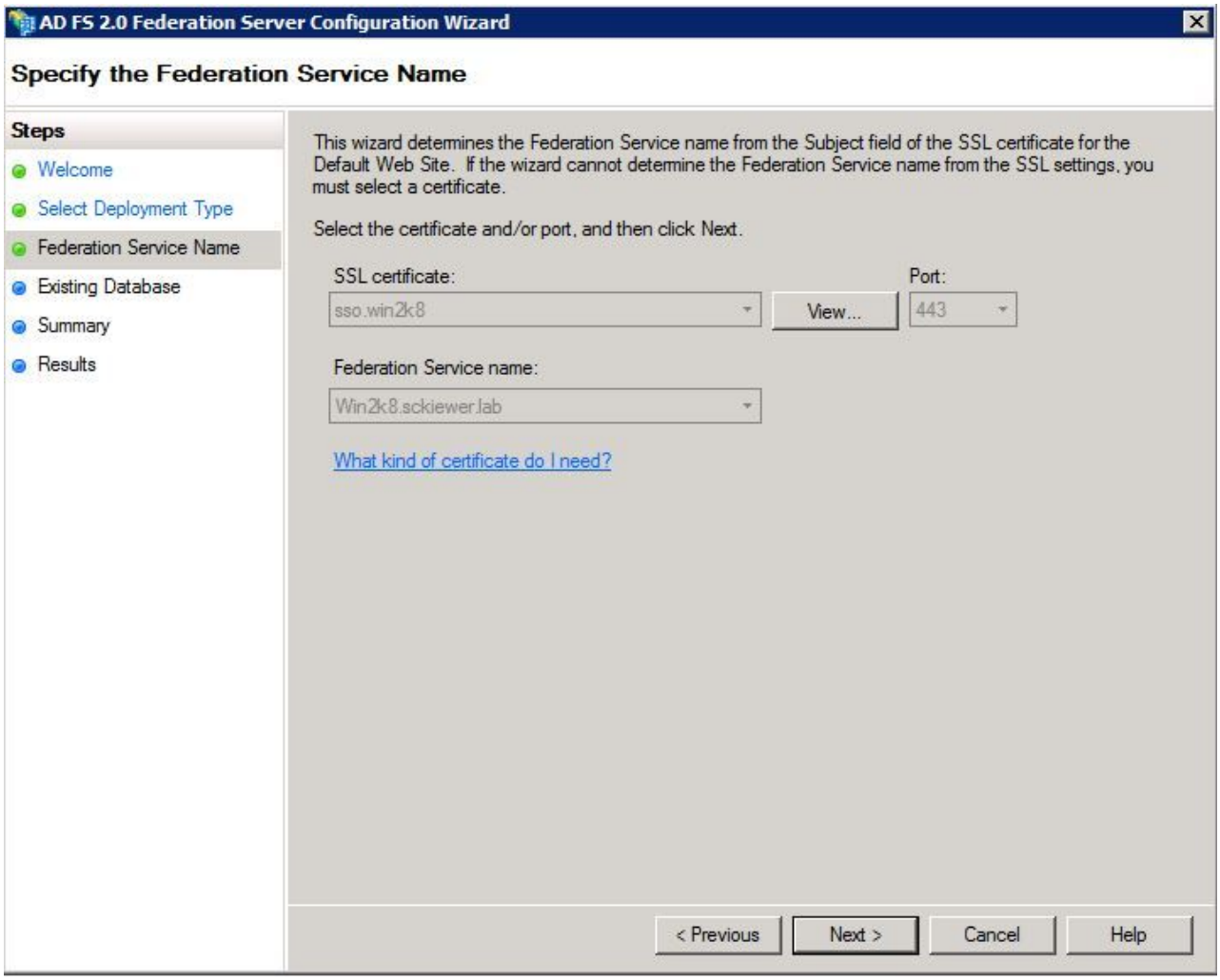
3단계. 그런 다음 Create a new Federation Service(새 페더레이션 서비스 만들기)를 클릭합니다.



4단계. 대부분의 환경에서는 독립형 페더레이션 서버만으로도 충분합니다.



5단계. 다음으로 인증서를 선택하라는 메시지가 표시됩니다. 서버에 인증서가 있으면 이 필드가 자동으로 채워집니다.



6단계. 서버에 이미 AD FS 데이터베이스가 있는 경우 계속하려면 데이터베이스를 제거해야 합니다.

7단계. 마지막으로, Next(다음)를 클릭할 수 있는 요약 화면에 표시됩니다.

Idp 메타데이터를 CUCM으로 가져오기/CUCM 메타데이터 다운로드

1단계. Windows 서버 호스트 이름/FQDN으로 URL을 업데이트하고 AD FS 서버에서 메타데이터를 다운로드합니다. https://hostname/federationmetadata/2007-06/federationmetadata.xml

2단계. Cisco Unified CM Administration(Cisco Unified CM 관리) > System(시스템) > SAML Single Sign-On(SAML 단일 로그인)으로 이동합니다.

3단계. Enable SAML SSO(SAML SSO 활성화)를 클릭합니다.

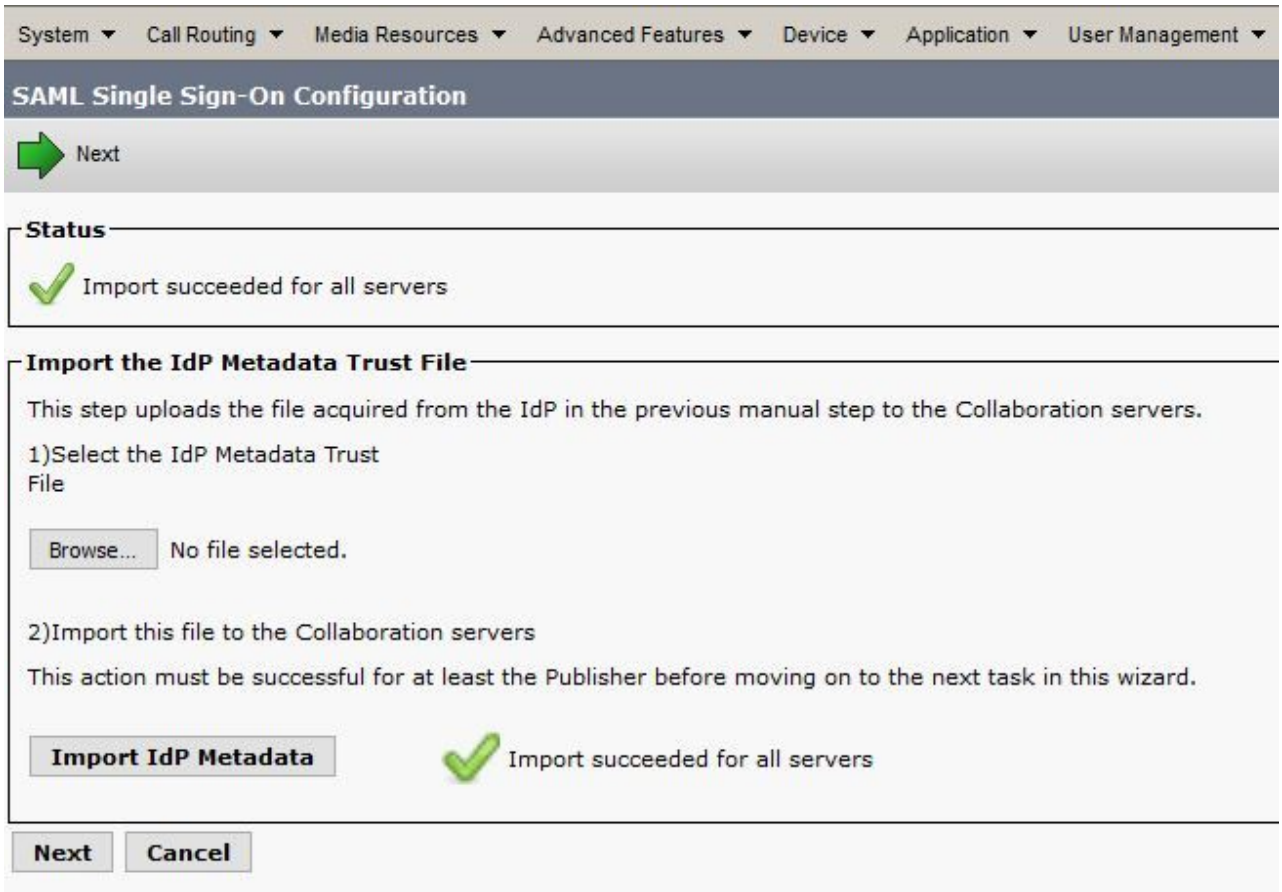
4단계. 웹 서버 연결에 대한 알림을 받으면 [계속]을 클릭합니다.

5단계. 다음으로, CUCM은 IdP에서 메타데이터 파일을 다운로드하도록 지시합니다. 이 시나리오에서는 AD FS 서버가 IdP이며 1단계에서 메타데이터를 다운로드했으므로 Next(다음)를 클

릭합니다.

6단계. Browse(찾아보기) > Step 1(단계 1)에서 .xml을 선택하고 Import IdP Metadata(IdP 메타데이터 가져오기)를 클릭합니다.

7단계. 가져오기에 성공했다는 메시지가 표시됩니다.



8단계. Next(다음)를 클릭합니다.

9단계. 이제 IdP 메타데이터를 CUCM으로 가져왔으므로 CUCM의 메타데이터를 IdP로 가져와야 합니다.

10단계. Download Trust Metadata File을 클릭합니다.

11단계. Next(다음)를 클릭합니다.

12단계. .zip 파일을 Windows Server로 이동하고 폴더에 압축을 풉니다.

CUCM 메타 데이터를 AD FS 2.0 서버로 가져오고 클레임 규칙 만들기

1단계. 시작을 클릭하고 AD FS 2.0 관리를 검색합니다.

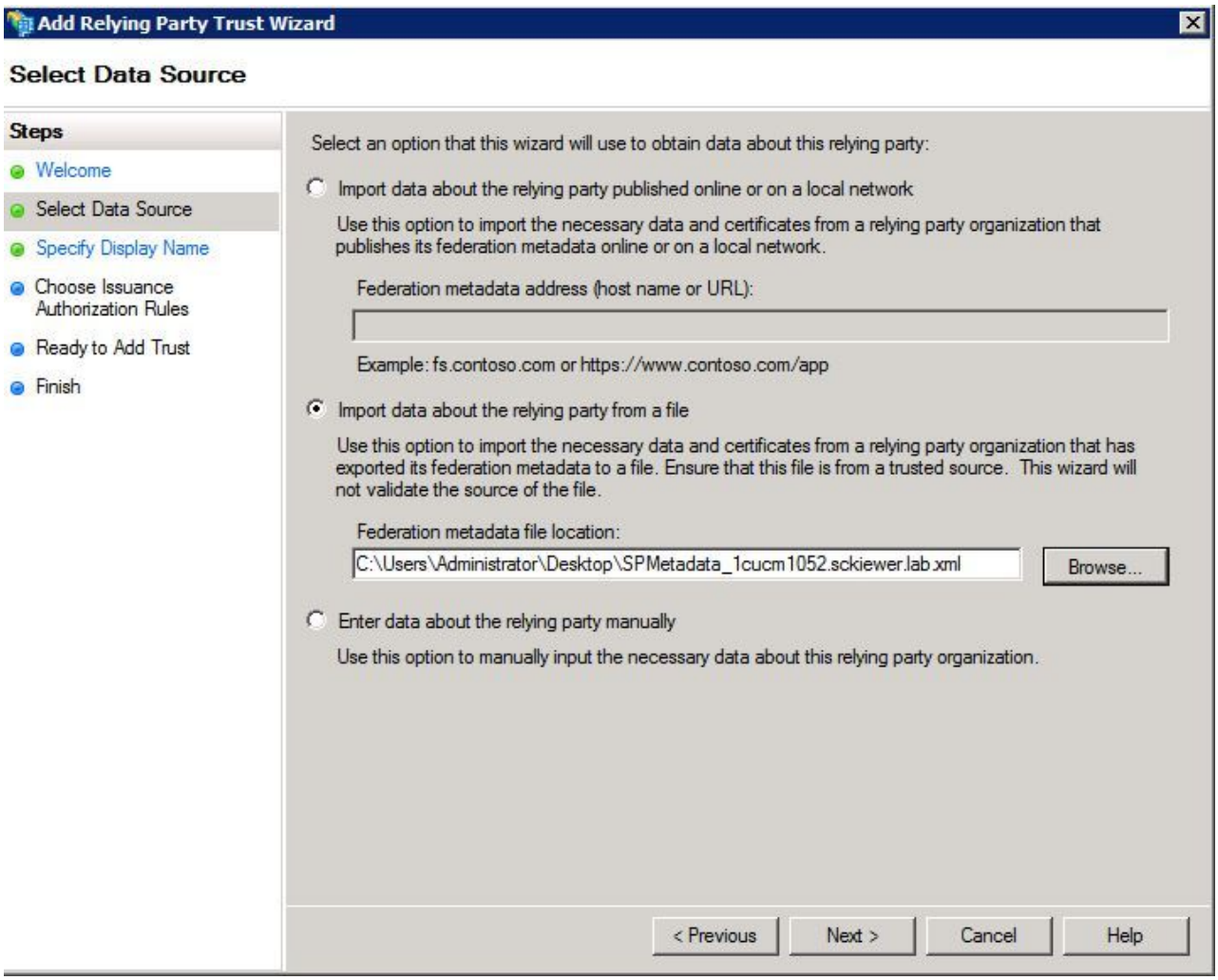
2단계. Required(필수): Add a trusted relying party(신뢰할 수 있는 당사자 추가)를 클릭합니다.

참고: 이 옵션이 표시되지 않으면 창을 닫고 다시 열어야 합니다.

3단계. Add Relying Party Trust Wizard를 연 후 Start를 클릭합니다.

4단계. 여기서 12단계에서 추출한 XML 파일을 가져와야 합니다. 파일에서 신뢰 당사자에 대한 데이터 가져오기를 선택하고 폴더 파일을 찾은 다음 게시자에 대한 XML을 선택합니다.

참고: SSO를 사용하려는 Unified Collaboration 서버에 대해 이전 단계를 사용하십시오.



5단계. Next(다음)를 클릭합니다.

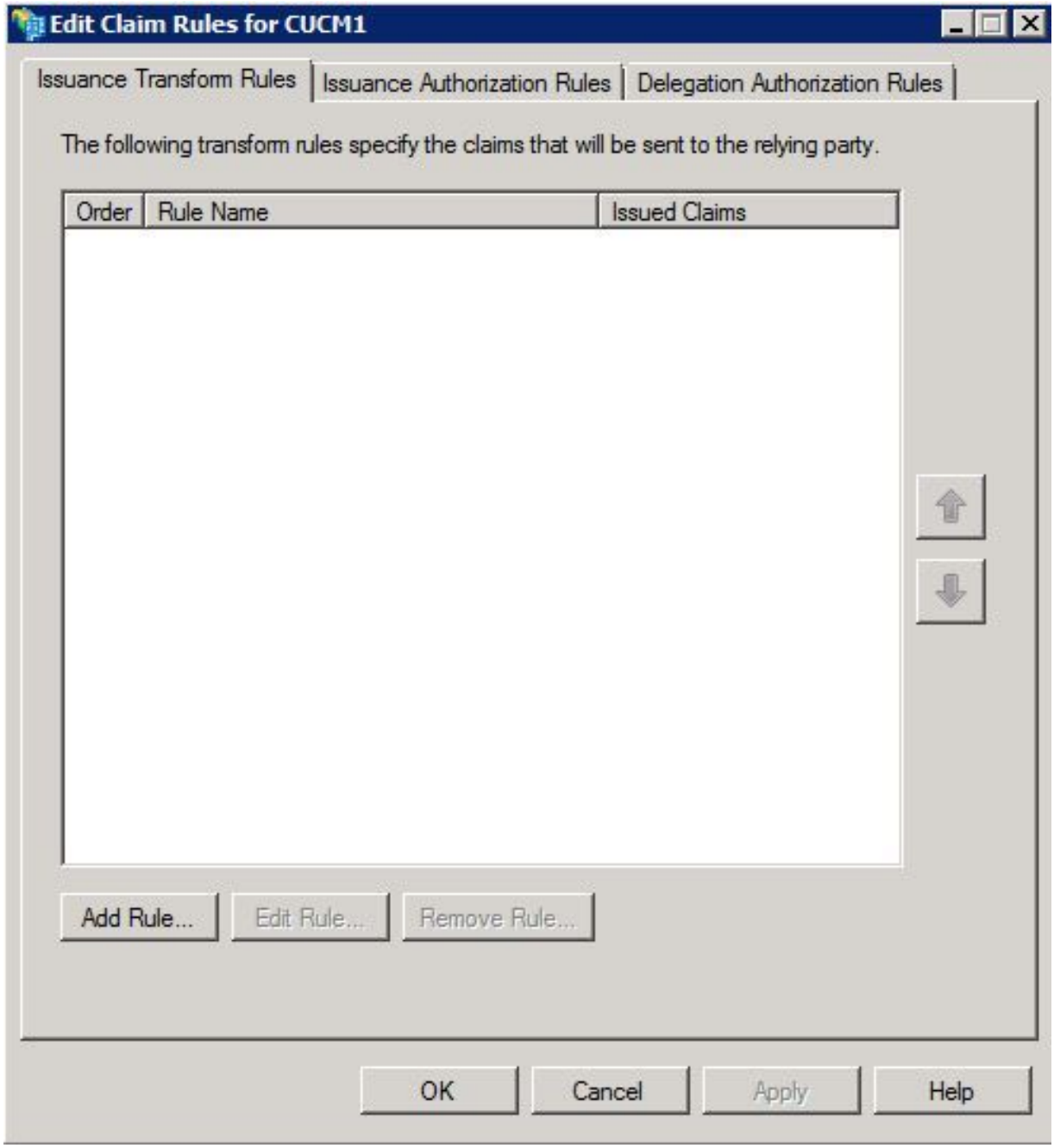
6단계. 표시 이름을 편집하고 Next(다음)를 클릭합니다.

7단계. Permit all users to access this relying party(모든 사용자가 이 신뢰 당사자에 액세스하도록 허용)를 선택하고 Next(다음)를 클릭합니다.

8단계. Next(다음)를 다시 클릭합니다.

9단계. 이 화면에서 마법사가 닫힐 때 이 신뢰 당사자 트러스트에 대한 클레임 규칙 편집 대화 상자를 연 다음 닫기를 클릭했는지 확인합니다.

10단계. Edit Claim Rules 창이 열립니다.



11단계. 이 창에서 Rule 추가를 클릭합니다.

12단계. Claim 규칙 템플릿에서 Send LDAP Attributes as Claims(LDAP 특성을 클레임으로 보내기)를 선택하고 Next(다음)를 클릭합니다.

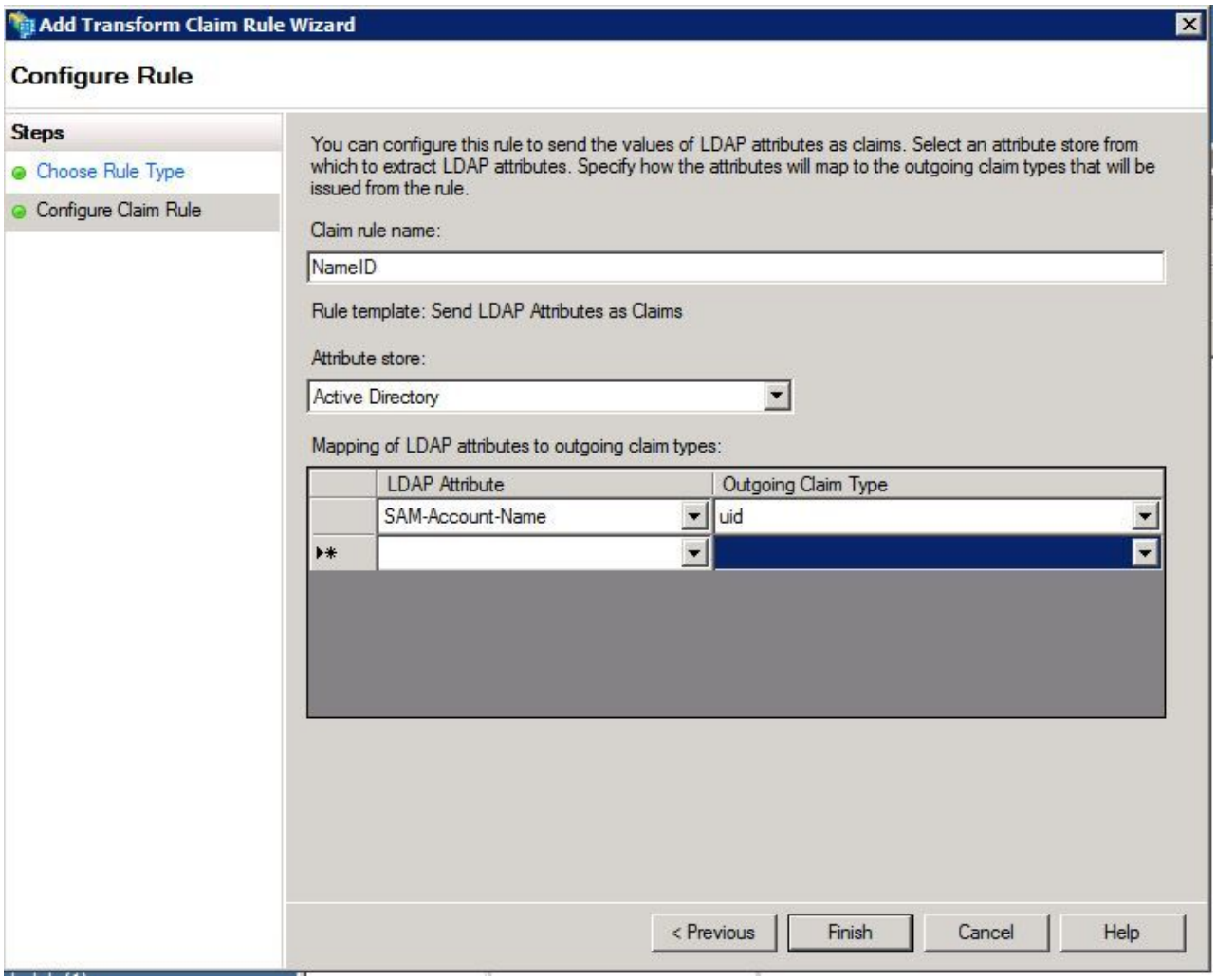
13단계. 다음 페이지에서 클레임 규칙 이름에 대한 NameID를 입력합니다.

14단계. 특성 저장소에 대한 Active Directory를 선택합니다.

15단계. LDAP 특성의 SAM-Account-Name을 선택합니다.

16단계. 발신 클레임 유형에 uid를 입력합니다.

참고: uid는 드롭다운 목록의 옵션이 아니므로 수동으로 입력해야 합니다.



17단계. Finish(마침)를 클릭합니다.

18단계. 이제 첫 번째 규칙이 완료되었습니다. Add Rule을 다시 클릭합니다.

19단계. Send Claims Using a Custom Rule(사용자 지정 규칙을 사용하여 클레임 보내기)을 선택합니다.

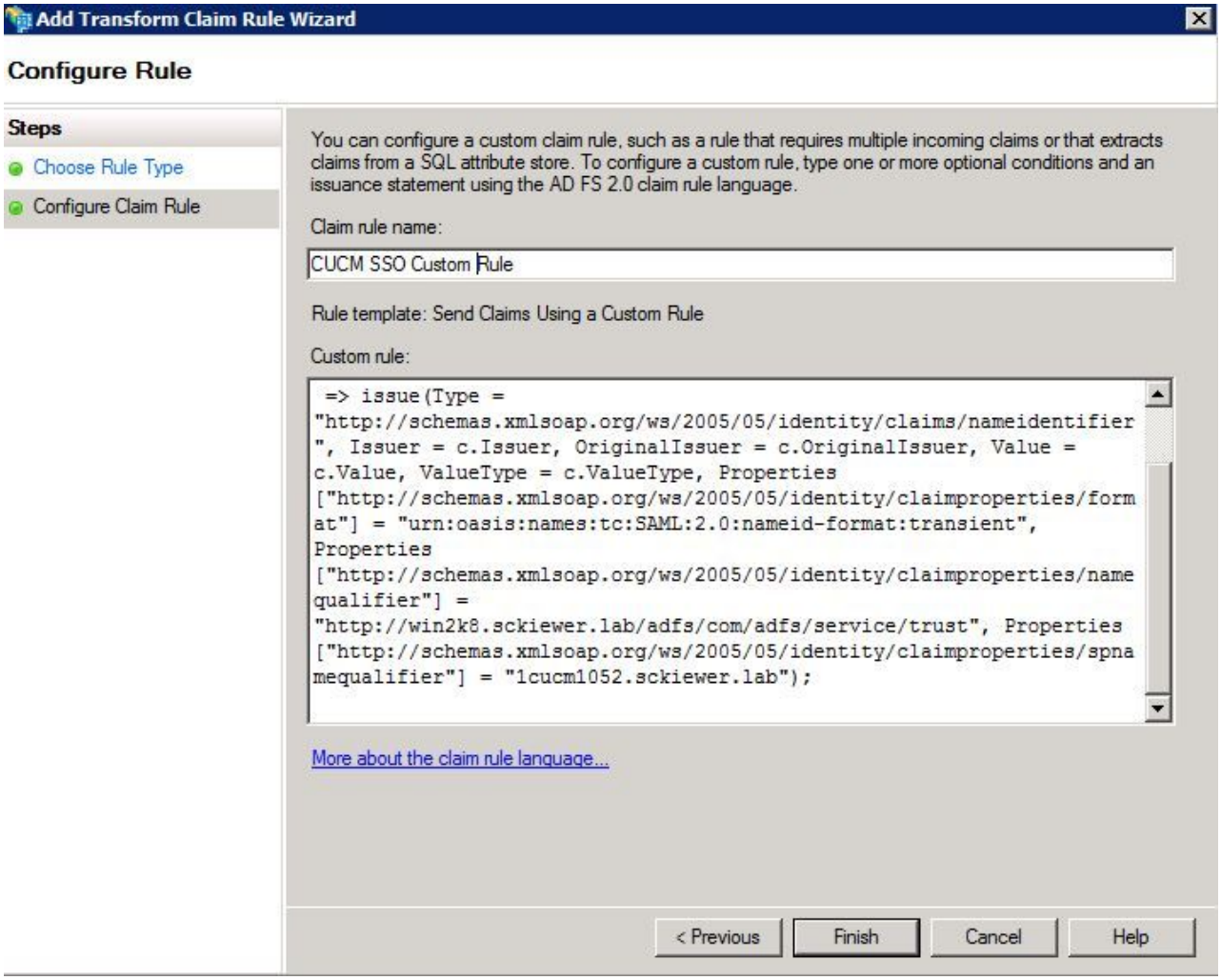
20단계. 클레임 규칙 이름을 입력합니다.

21단계. Custom rule(맞춤형 규칙) 필드에 다음 텍스트를 붙여넣습니다.

c:[== "http://schemas.microsoft.com/ws/2008/06/identity/을 입력합니다.클레임 /windowsaccountname"]
=> 문제(유형 = "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:transitionnt",속성 ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] = "http://ADFS_FEDERATION_SERVICE_NAME/com/adfs/service/trust", 속성 ["http://schemas.xmlsoap.org/ws/2005/05/id/claimproperties/spnamequalifier"] = "CUCM_ENTITY_ID");

22단계. AD_FS_SERVICE_NAME 및 CUCM_ENTITY_ID를 적절한 값으로 변경해야 합니다.

참고: AD FS 서비스 이름이 확실하지 않으면 단계에 따라 찾을 수 있습니다. CUCM 엔티티 ID는 CUCM 메타데이터 파일의 첫 번째 행에서 가져올 수 있습니다. 파일의 첫 번째 줄에 entityID=1cucm1052.sckiewer.lab과 같은 entityID가 있습니다. 클레임 규칙의 해당 섹션에 밑줄 친 값을 입력해야 합니다.



23단계. Finish(마침)를 클릭합니다.

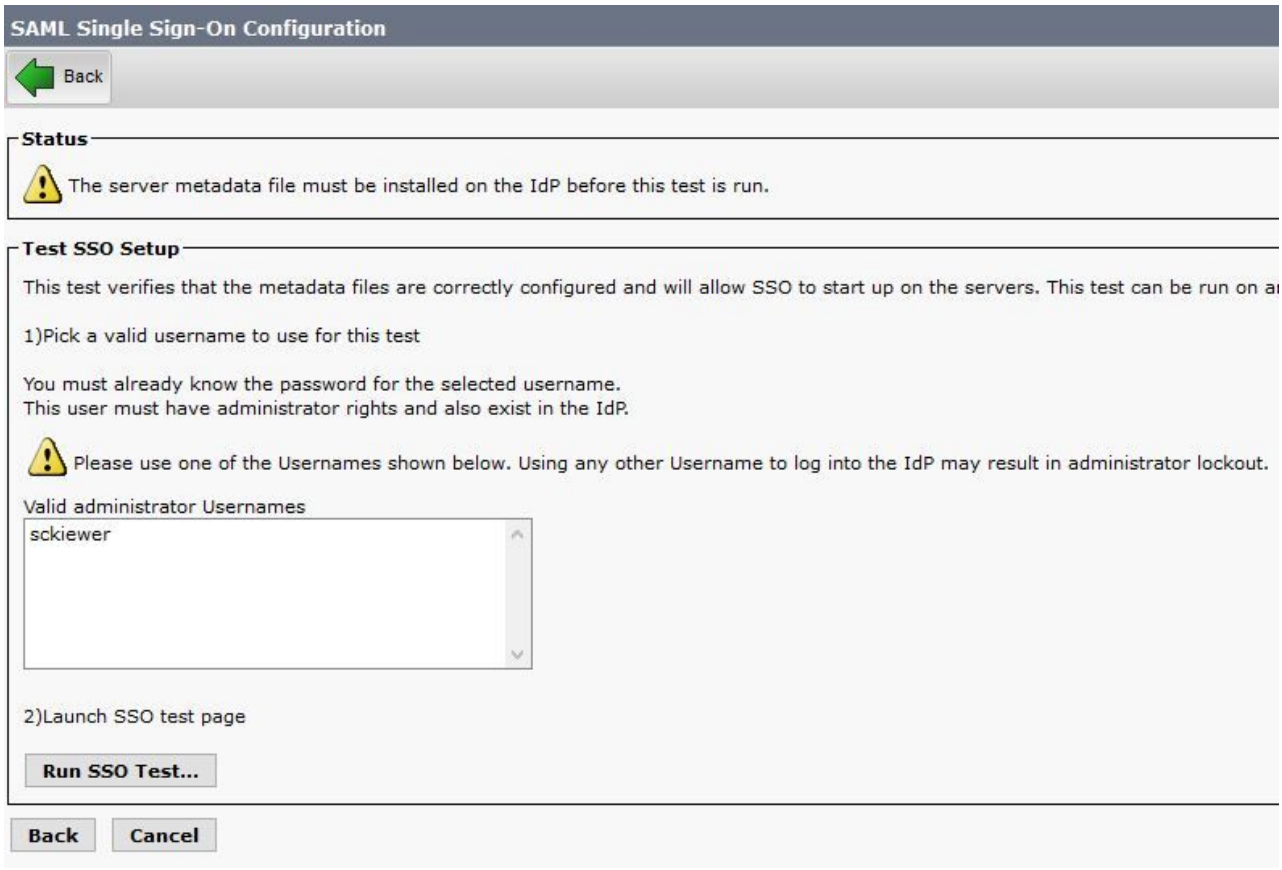
24단계. OK(확인)를 클릭합니다.

참고: 클레임 규칙은 SSO를 사용하려는 Unified Collaboration 서버에 필요합니다.

CUCM에서 SSO 활성화를 완료하고 SSO 테스트 실행

1단계. 이제 AD FS 서버가 완전히 구성되었으므로 CUCM으로 돌아갈 수 있습니다.

2단계. 최종 컨피그레이션 페이지에서 나갔습니다.



3단계. Standard CCM Super Users(표준 CCM 수퍼 사용자) 역할이 선택된 최종 사용자를 선택하고 Run SSO Test(SSO 테스트 실행)...를 클릭합니다.

4단계. 브라우저에서 팝업을 허용하는지 확인하고 프롬프트에 자격 증명을 입력합니다.

5단계. 팝업 창에서 닫기를 클릭한 다음 마침을 클릭합니다.

6단계. 웹 애플리케이션을 잠시 재시작한 후 SSO가 활성화됩니다.

문제 해결

SSO 로그를 디버그로 설정

SSO 로그를 디버그로 설정하려면 CUCM의 CLI에서 samltrace level debug를 설정해야 합니다

SSO 로그는 RTMT에서 다운로드할 수 있습니다. 로그 집합의 이름은 Cisco SSO입니다.

페더레이션 서비스 이름 찾기

페더레이션 서비스 이름을 찾으려면 [시작]을 클릭하고 AD FS 2.0 관리를 검색합니다.

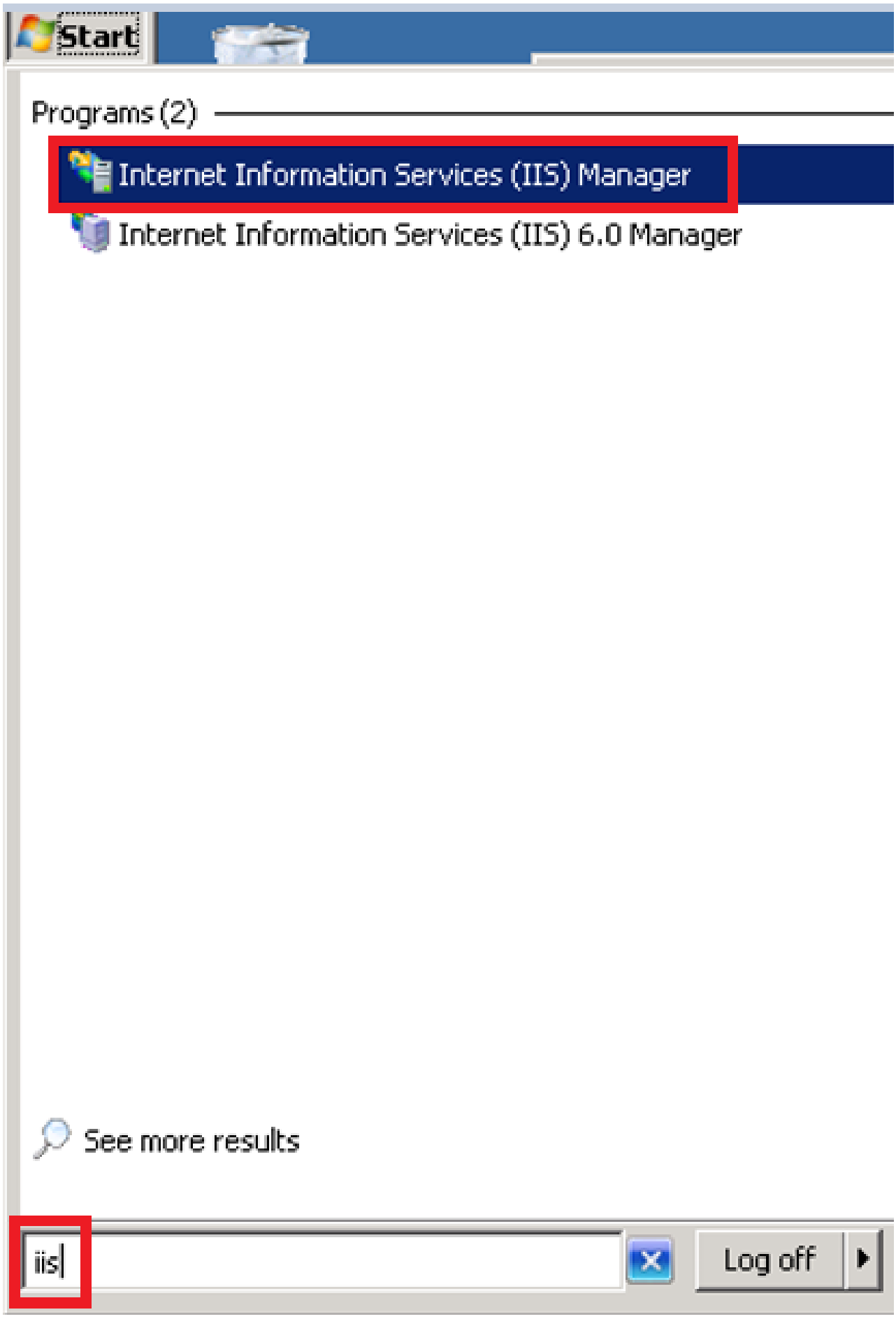
· Edit Federation Service Properties(페더레이션 서비스 속성 편집)를 클릭합니다.
· General(일반) 탭에서 Federation Service Name(페더레이션 서비스 이름)을 찾습니다.

doless Certificate And Federation Service Name(doless 인증서 및 페더레이션 서비스 이름)

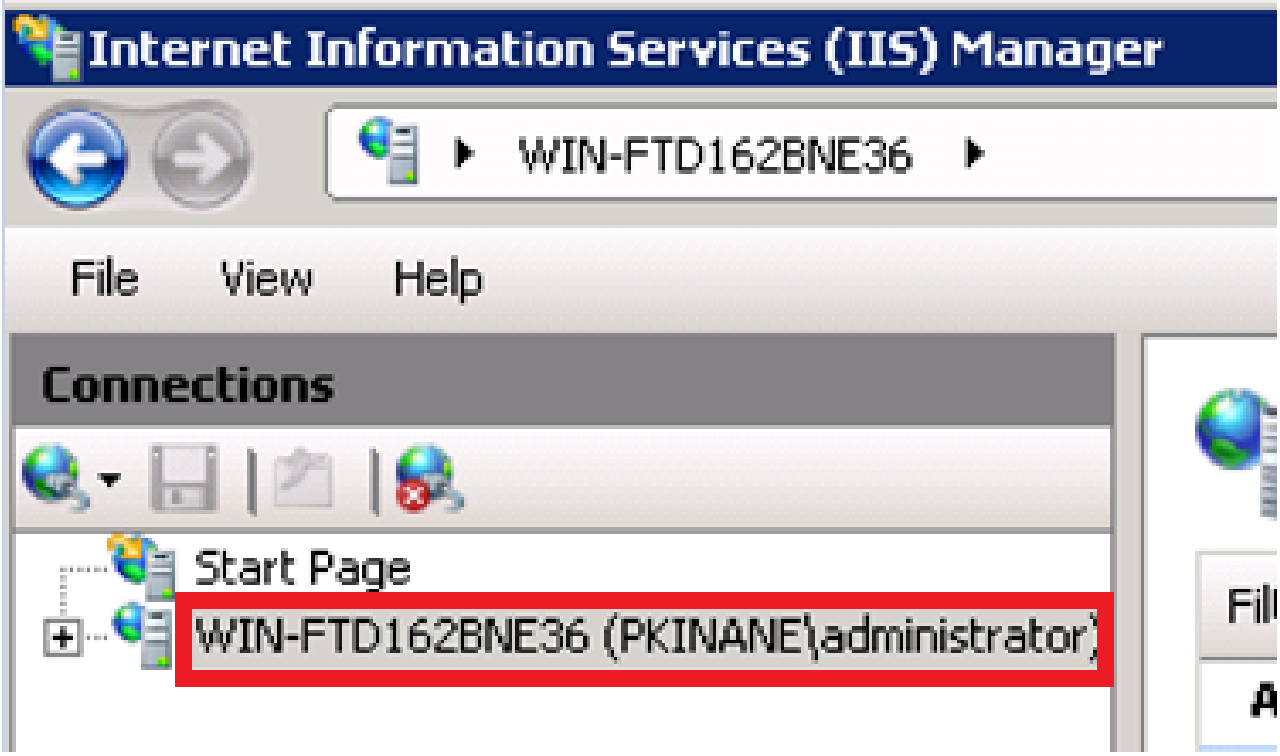
AD FS 컨피그레이션 마법사에서 이 오류 메시지를 받으면 새 인증서를 만들어야 합니다.

선택한 인증서에 doless(short-named) 주체 이름이 있으므로 선택한 인증서를 사용하여 페더레이션 서비스 이름을 확인할 수 없습니다. doless(short-named) 주체 이름 없이 다른 인증서를 선택한 후 다시 시도하십시오.

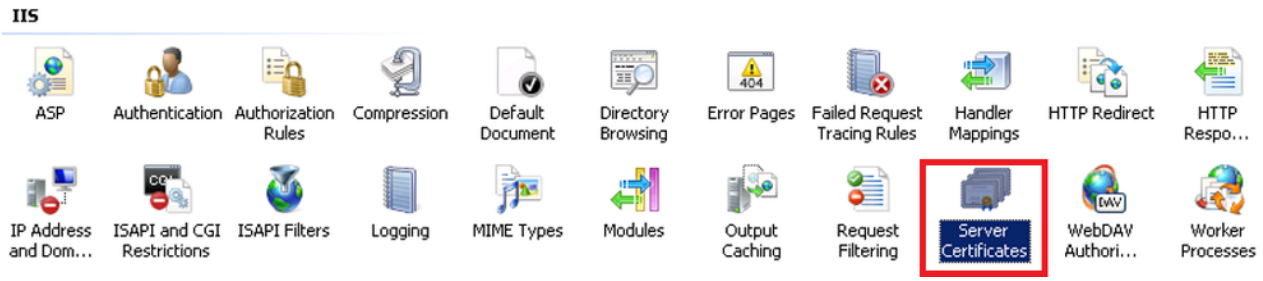
1단계. 시작을 클릭하고 iis를 검색한 다음 인터넷 정보 서비스(IIS) 관리자를 엽니다



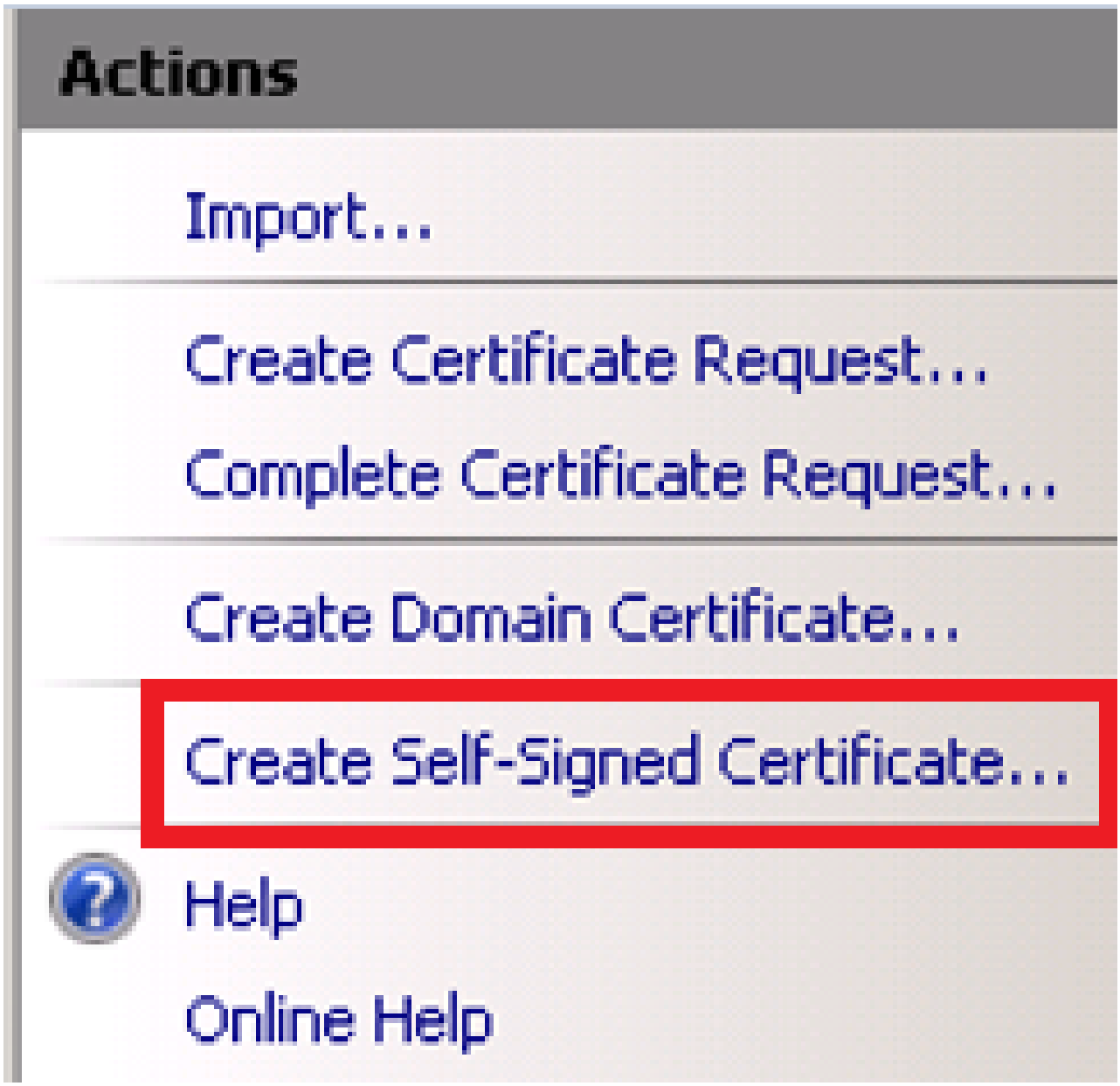
2단계. 서버 이름을 클릭합니다.



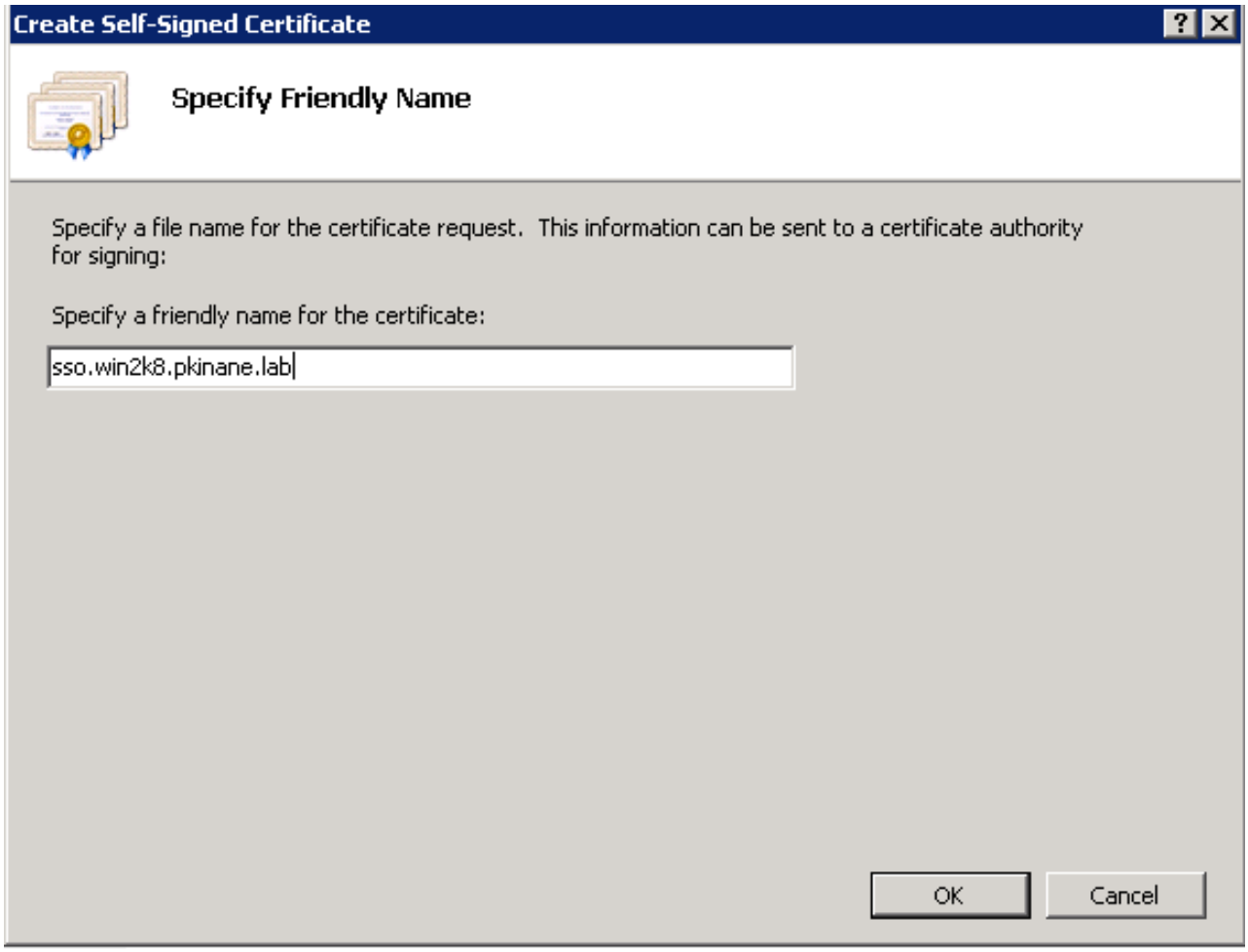
3단계. Server Certificates를 클릭합니다.



4단계. Create Self-Signed Certificate(자체 서명 인증서 생성)를 클릭합니다.



5단계. 인증서 별칭에 사용할 이름을 입력합니다.



CUCM 및 IDP 서버 간의 시간 동기화 중단

CUCM에서 SSO 테스트를 실행할 때 이 오류가 발생하면 CUCM과 동일한 NTP 서버를 사용하도록 Windows Server를 구성해야 합니다.

잘못된 SAML 응답입니다. 이는 Cisco Unified Communications Manager와 IDP 서버 간에 시간이 동기화되지 않았을 때 발생할 수 있습니다. 두 서버에서 NTP 컨피그레이션을 확인하십시오. CLI에서 "utils ntp status"를 실행하여 Cisco Unified Communications Manager에서 이 상태를 확인합니다.

Windows Server에 올바른 NTP 서버가 지정되면 다른 SSO 테스트를 수행하고 문제가 지속되는지 확인해야 합니다. 주장의 유효 기간을 기울일 필요가 있는 경우도 있다. 이 프로세스에 대한 자세한 내용은 여기를 참조하십시오.

관련 정보

- 기술 지원 및 문서 – Cisco Systems

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.