

ADFS 3.0을 사용하여 Cisco Unified Communications Manager에서 SAML SSO 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성 사전 확인](#)

[A 레코드](#)

[포인터\(PTR\) 레코드](#)

[Jabber Discovery Services에 SRV 레코드가 있어야 함](#)

[ADFS3 초기 컨피그레이션](#)

[ADFS를 사용하여 CUCM에서 SSO 구성](#)

[LDAP 컨피그레이션](#)

[CUCM 메타데이터](#)

[ADFS 신뢰 당사자 구성](#)

[IDP 메타데이터](#)

[CUC에서 SSO 구성](#)

[CUC 메타데이터](#)

[Expressway에서 SSO 구성](#)

[Expressway C로 메타데이터 가져오기](#)

[Expressway C에서 메타데이터 내보내기](#)

[Cisco Expressway-E에 대한 당사자 Trust 추가](#)

[새로 고침 로그인에 있는 OAuth](#)

[인증 경로](#)

[SSO 아키텍처](#)

[온프레미스 로그인 흐름](#)

[MRA 로그인 흐름](#)

[OAuth](#)

[토큰 액세스/새로 고침](#)

[OAuth 권한 부여 코드 권한 부여 플로우가 더 좋음](#)

[Kerberos 구성](#)

[Windows 인증 선택](#)

[ADFS는 Kerberos NTLM을 모두 지원합니다.](#)

[Microsoft Internet Explorer 구성](#)

[Security\(보안\) > Intranet zones\(인트라넷 영역\) > Sites\(사이트\)에서 ADFS URL 추가](#)

[보안 > 신뢰할 수 있는 사이트에 CUCM, IMP 및 Unity 호스트 이름 추가](#)

[사용자 인증](#)

[SSO에서 Jabber 로그인](#)

[문제 해결](#)

[Internet Explorer\(IE\)](#)

[IE에 추가하는 사이트](#)

[동기화 중단 문제](#)

[토큰 취소](#)

[부트스트랩 파일](#)

[SSO 실패 MSIS7066](#)

소개

이 문서에서는 Cisco CUCM(Unified Communication Manage), Cisco CUC(Unity Connection), Expressway 제품에서 Windows 2012 R2를 사용하여 ADFS 3.0을 사용하여 Single Sign-On with Active Directory Federation Service(ADFS 3.0)를 구성하는 단계에 대해 설명합니다.Kerberos 구성 단계도 이 문서에 포함되어 있습니다.

사전 요구 사항

요구 사항

Cisco에서는 SSO(Single Sign-On) 및 Windows 제품에 대한 지식을 보유하고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CUCM 11.5
- CUC 11.5
- 고속도로 12
- 다음 역할이 있는 Windows 2012 R2 서버:
 - Active Directory 인증서 서비스
 - Active Directory 페더레이션 서비스

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

구성 사전 확인

ADFS3을 설치하기 전에 다음 서버 역할이 환경에 이미 있어야 합니다.

·도메인 컨트롤러 및 DNS

·모든 서버를 포인터 레코드와 함께 A 레코드로 추가해야 합니다(IP 주소를 도메인 또는 호스트 이름으로 확인하는 DNS 레코드 유형).

A 레코드

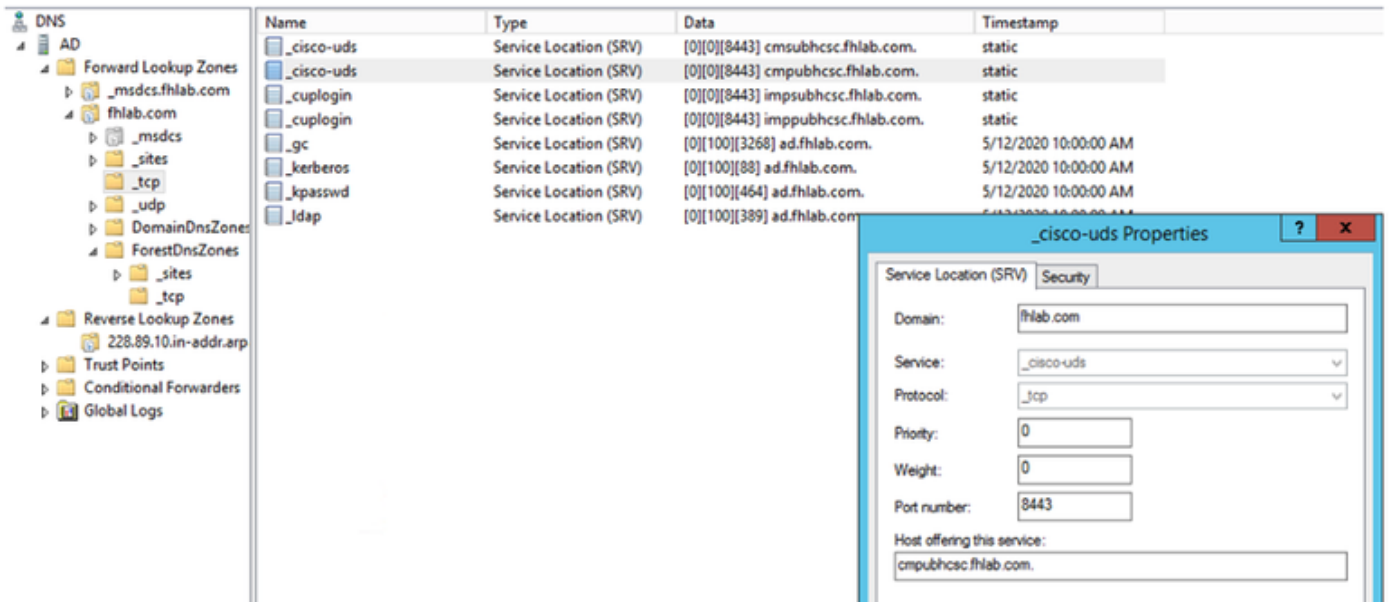
fhlab.com에서hosts cmpubhcsc, cmsubhcsc, cucpubhcsc, cucsubhcsc, expwyc, expwye, impubhcsc 및 imsubhcsc가 추가되었습니다.

Name	Type
_msdcs	
_sites	
_tcp	
_udp	
DomainDnsZones	
ForestDnsZones	
(same as parent folder)	Start of Authority (SOA)
(same as parent folder)	Name Server (NS)
(same as parent folder)	Host (A)
ad	Host (A)
cmpubhcsc	Host (A)
cmsubhcsc	Host (A)
cucpubhcsc	Host (A)
cucsubhcsc	Host (A)
expwyc	Host (A)
expwye	Host (A)
imppubhcsc	Host (A)
impsubhcsc	Host (A)

포인터(PTR) 레코드

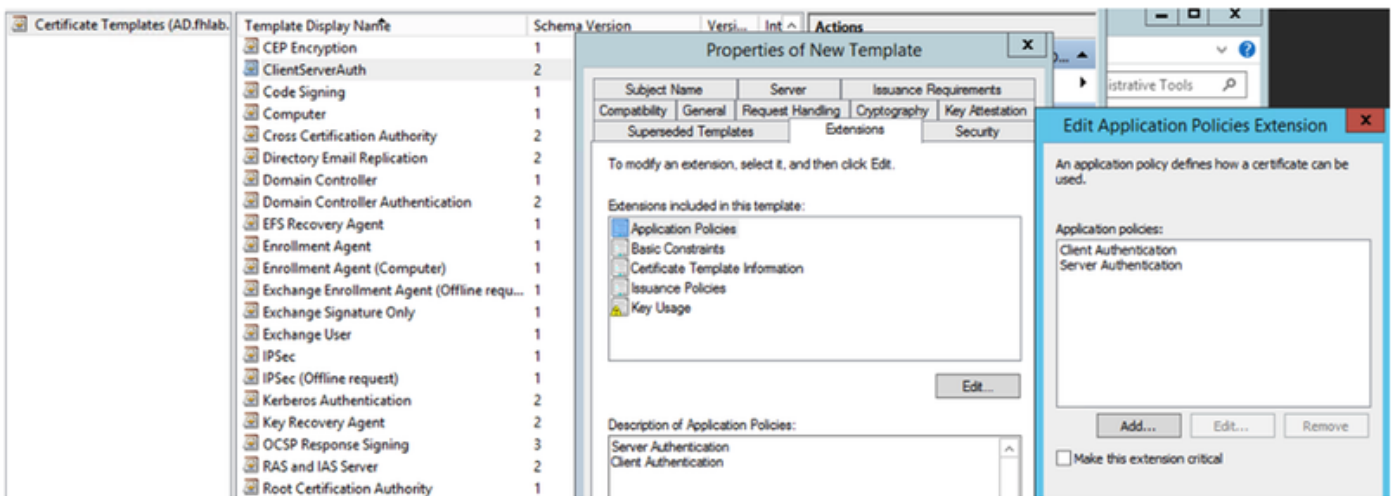
Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[14], ad.fhlab.com, hostmaster.fhlab.co...	static
(same as parent folder)	Name Server (NS)	ad.fhlab.com.	static
10.89.228.144	Pointer (PTR)	expwyc.fhlab.com.	static
10.89.228.145	Pointer (PTR)	expwye.fhlab.com.	static
10.89.228.146	Pointer (PTR)	cmpubhcsc.fhlab.com.	static
10.89.228.147	Pointer (PTR)	cmsubhcsc.fhlab.com.	static
10.89.228.148	Pointer (PTR)	imppubhcsc.fhlab.com.	static
10.89.228.150	Pointer (PTR)	impsubhcsc.fhlab.com.	static
10.89.228.151	Pointer (PTR)	cucpubhcsc.fhlab.com.	static
10.89.228.153	Pointer (PTR)	cucsubhcsc.fhlab.com.	static
10.89.228.154	Pointer (PTR)	win10.fhlab.com.	5/12/2020 10:00:00 AM
10.89.228.226	Pointer (PTR)	ad.fhlab.com.	5/12/2020 11:00:00 AM
10.89.228.227	Pointer (PTR)	win10ext.fhlab.com.	5/7/2020 4:00:00 PM

Jabber Discovery Services에 SRV 레코드가 있어야 함

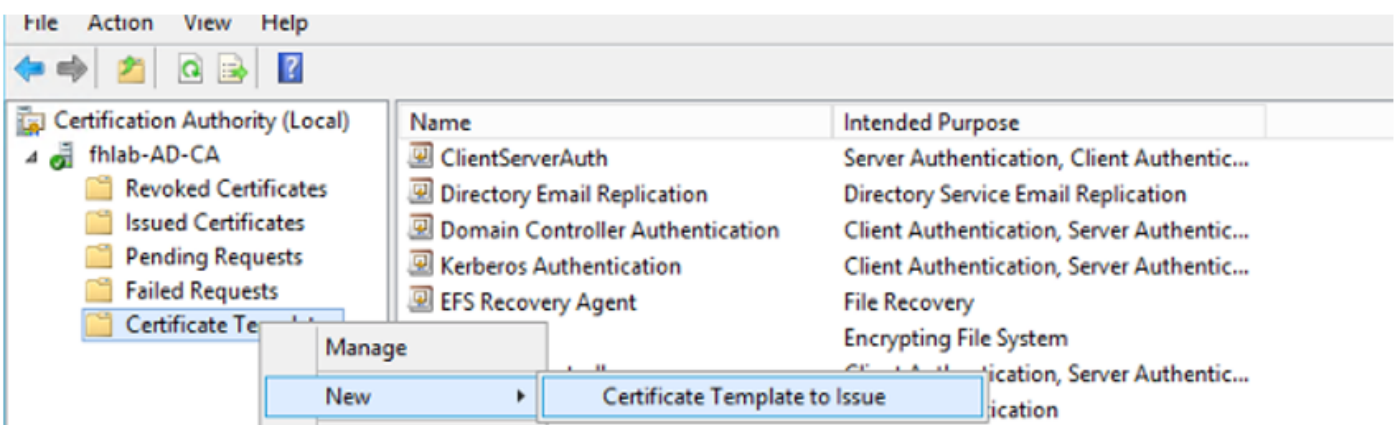


• 루트 CA(인증서가 엔터프라이즈 CA 서명)

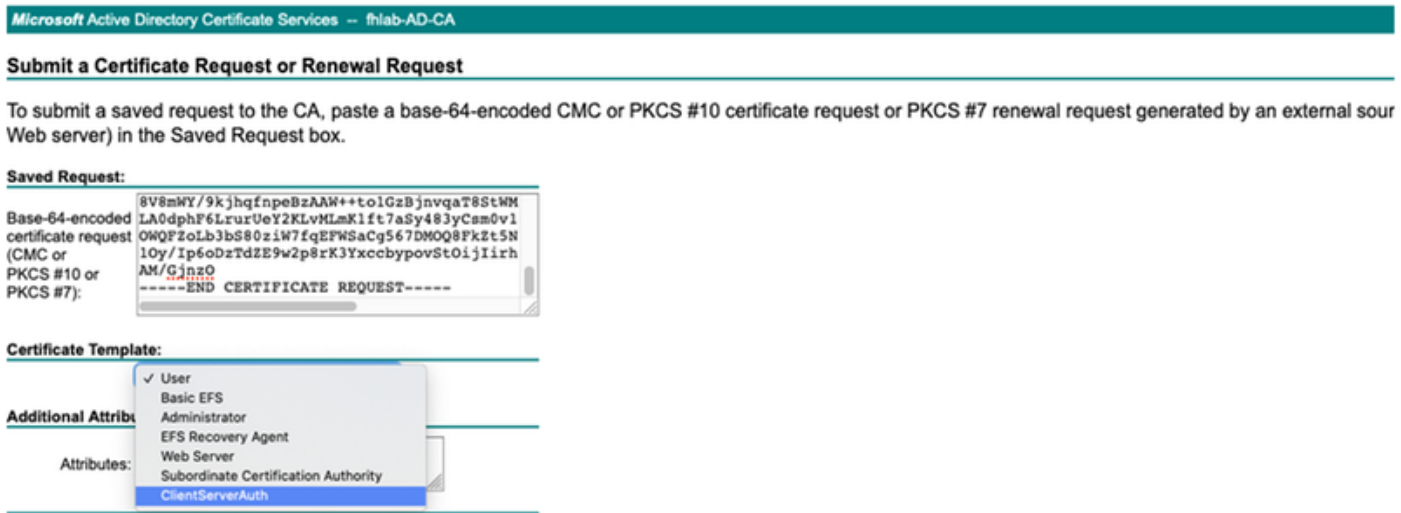
웹 서버 인증서 템플릿을 기반으로 인증서 템플릿을 만들어야 합니다. 이 템플릿은 복제되고 이름이 변경되며, Extensions(확장) 탭에서 Application Policies(애플리케이션 정책)가 수정되어 클라이언트 인증 애플리케이션 정책이 추가됩니다. 이 템플릿은 LAB 환경에서 모든 내부 인증서(CUCM, CUC, IMP 및 Expressway Core)에 서명하는 데 필요합니다. 내부 CA는 CSR(Expressway E Certificate Signing Requests)에도 서명할 수 있습니다.



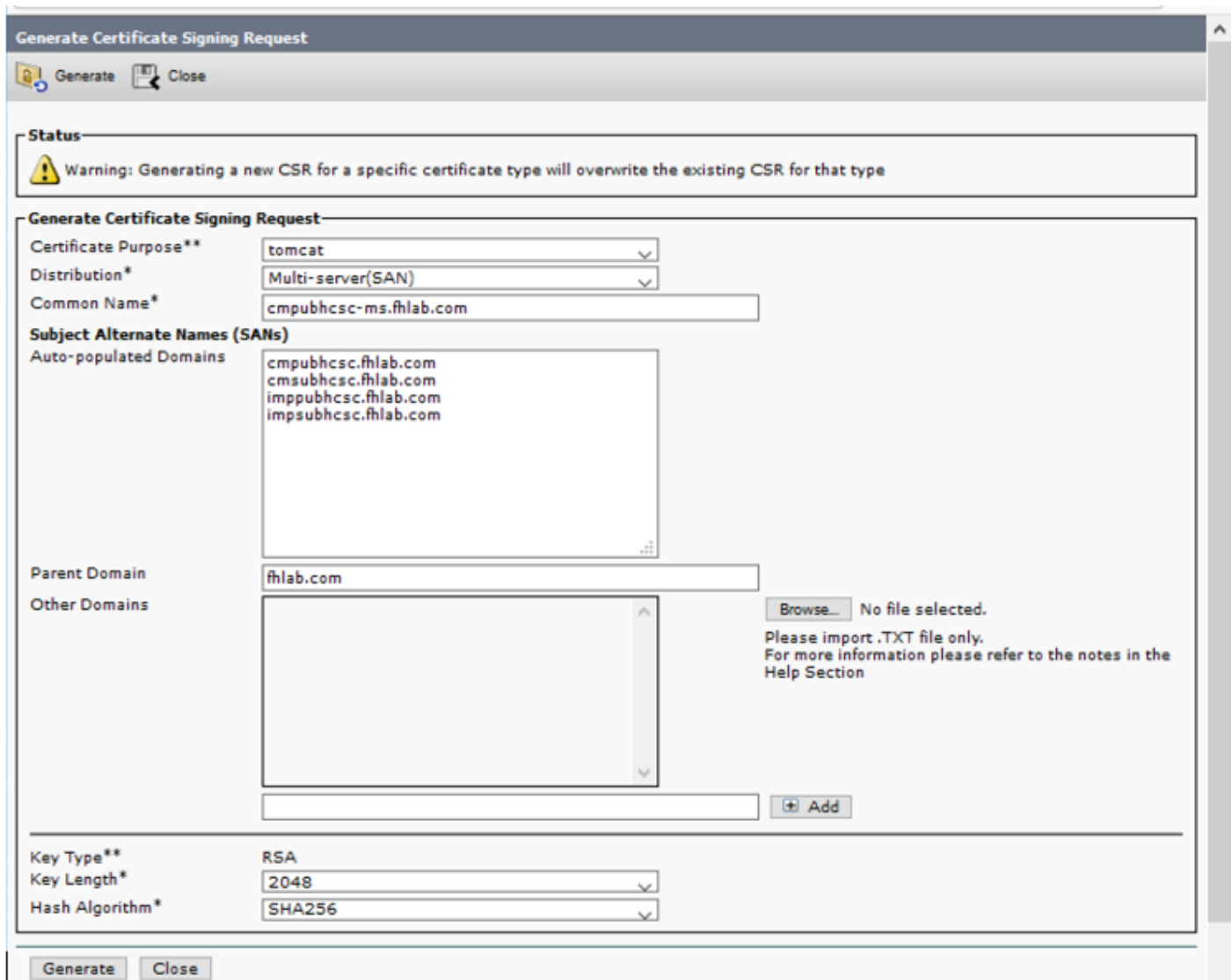
CSR에 서명할 수 있도록 생성된 템플릿을 발행해야 합니다.



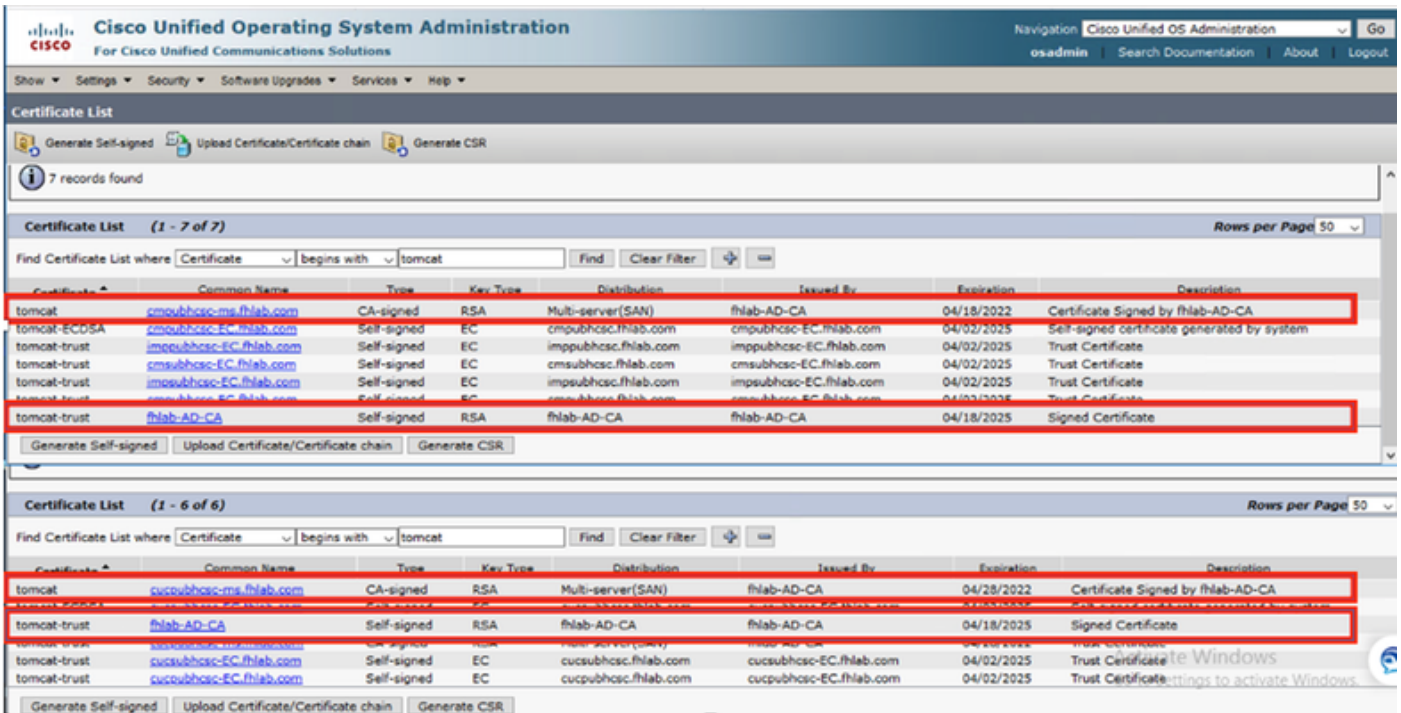
CA 인증서 웹에서 이전에 생성한 템플릿을 선택합니다.



CUCM, IMP 및 CUC Multi-Server CSR은 CA에서 생성하고 서명해야 합니다. 인증서 용도는 tomcat이어야 합니다.



CA 루트 인증서는 Tomcat Trust에 업로드하고 서명된 인증서는 tomcat에 업로드해야 합니다.



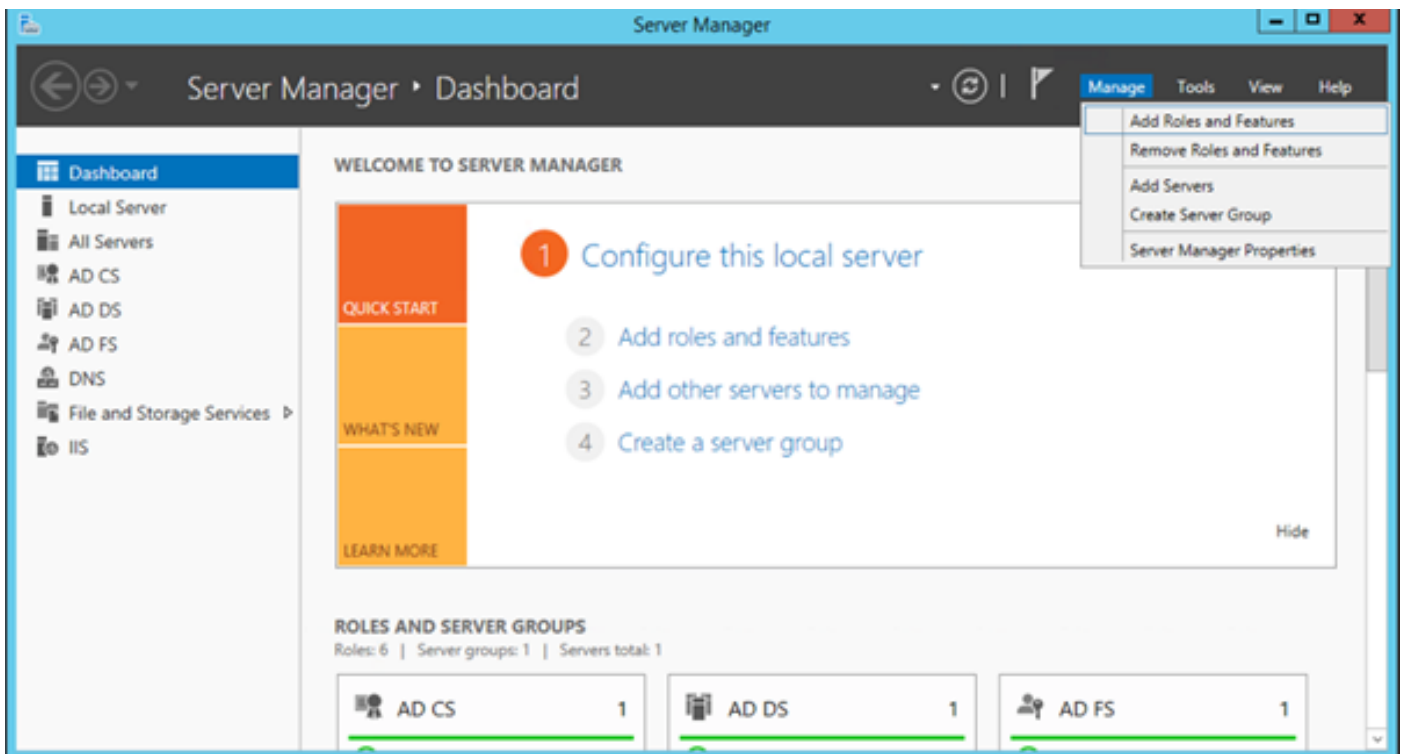
• IIS

그렇지 않은 경우 이 섹션에서는 이러한 역할의 설치를 진행합니다. 그렇지 않으면 이 섹션을 건너 뛰고 Microsoft에서 ADFS3 다운로드로 직접 진행합니다.

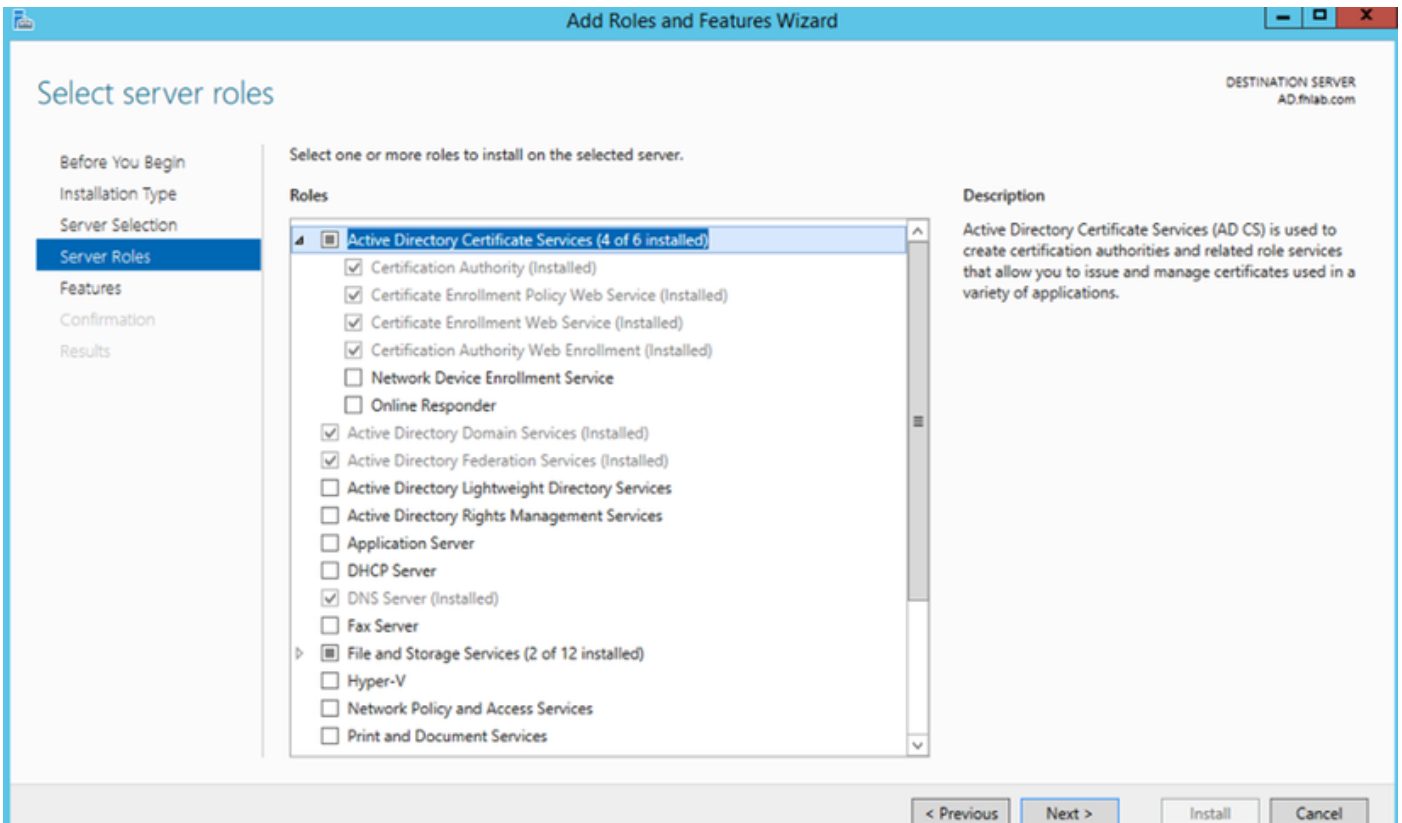
DNS와 함께 Windows 2012 R2를 설치한 후 서버를 도메인 컨트롤러로 승격합니다.

다음 작업은 Microsoft 인증서 서비스를 설치하는 것입니다.

서버 관리자로 이동하여 새 역할을 추가합니다.



Active Directory 인증서 서비스 역할을 선택합니다.



그리고 이러한 서비스를 먼저 구축합니다. CA(Certificate Authority) 인증서 등록 정책 웹 서비스 이러한 두 역할을 설치한 후 이를 구성한 다음 **Certificate Enrollment Web Service** 및 **Certificate Authority 웹 등록**을 설치합니다.구성합니다.

인증 기관을 설치할 때 IIS와 같은 추가 역할 서비스 및 기능도 추가됩니다.

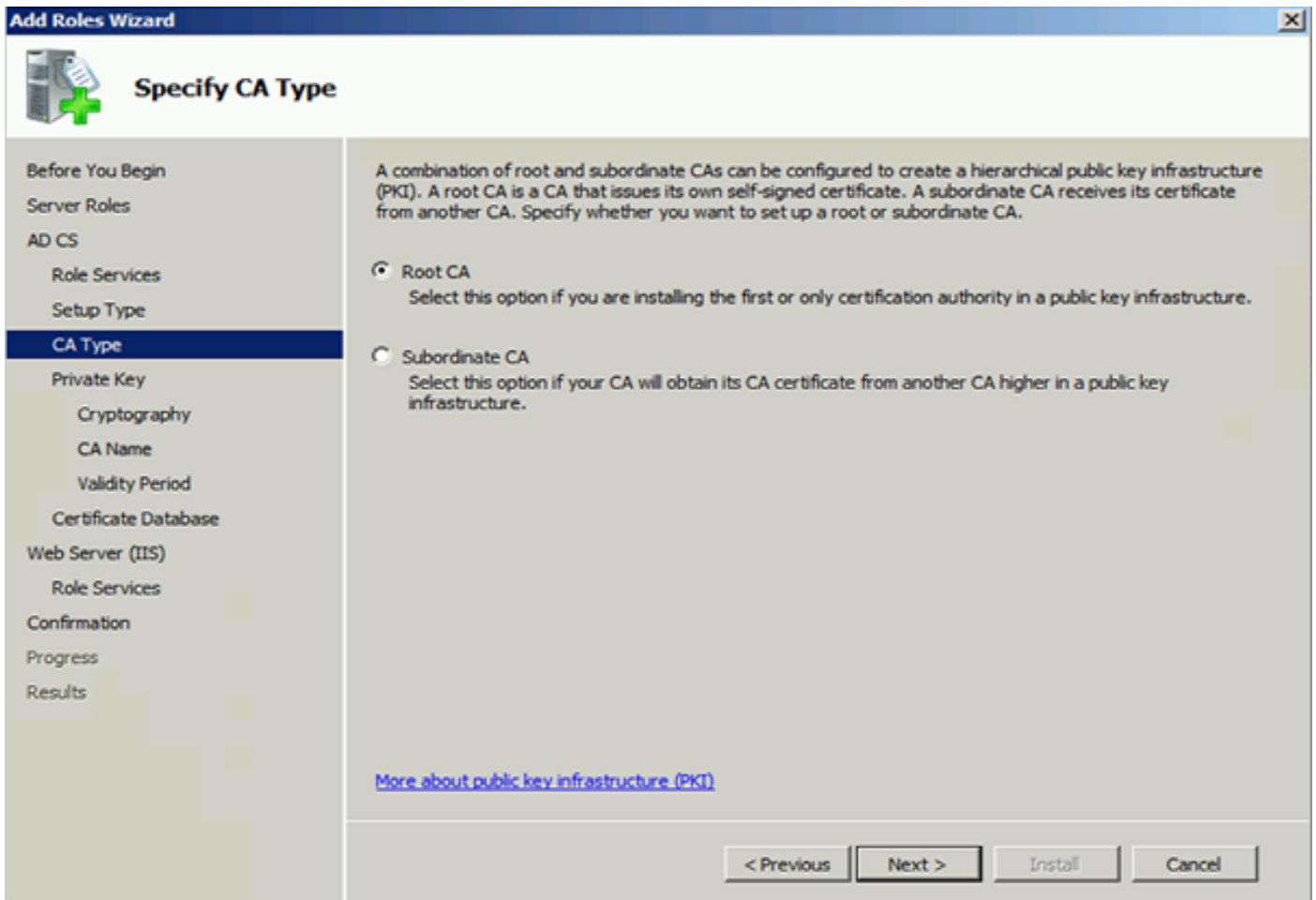
구축에 따라 엔터프라이즈 또는 독립형 을 선택할 수 있습니다.



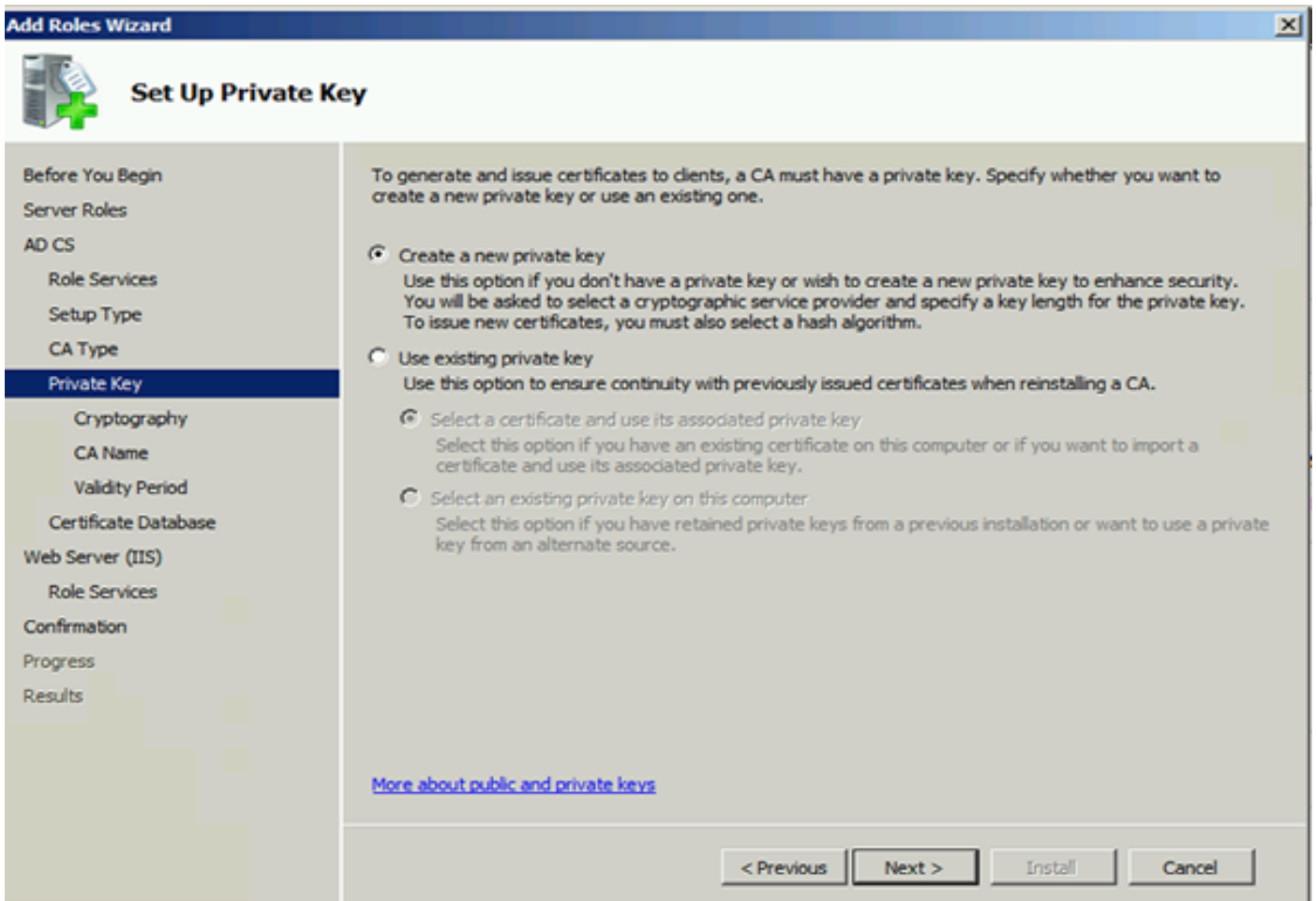
Specify Setup Type

<p>Before You Begin</p> <p>Server Roles</p> <p>AD CS</p> <p> Role Services</p> <p>Setup Type</p> <p> CA Type</p> <p> Private Key</p> <p> Cryptography</p> <p> CA Name</p> <p> Validity Period</p> <p> Certificate Database</p> <p>Web Server (IIS)</p> <p> Role Services</p> <p>Confirmation</p> <p>Progress</p> <p>Results</p>	<p>Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.</p> <p><input checked="" type="radio"/> Enterprise Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.</p> <p><input type="radio"/> Standalone Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.</p> <p>More about the differences between enterprise and standalone setup</p> <p style="text-align: right;"><input style="border: 1px solid black;" type="button" value=" < Previous "/> <input checked="" style="border: 1px solid black;" type="button" value=" Next > "/> <input style="border: 1px solid black;" type="button" value=" Install "/> <input style="border: 1px solid black;" type="button" value=" Cancel "/></p>
--	--

CA Type(CA 유형)에서 Root CA(루트 CA) 또는 Subordinate CA를 선택할 수 있습니다.조직에서 이미 실행 중인 다른 CA가 없는 경우 **Root CA**를 선택합니다.

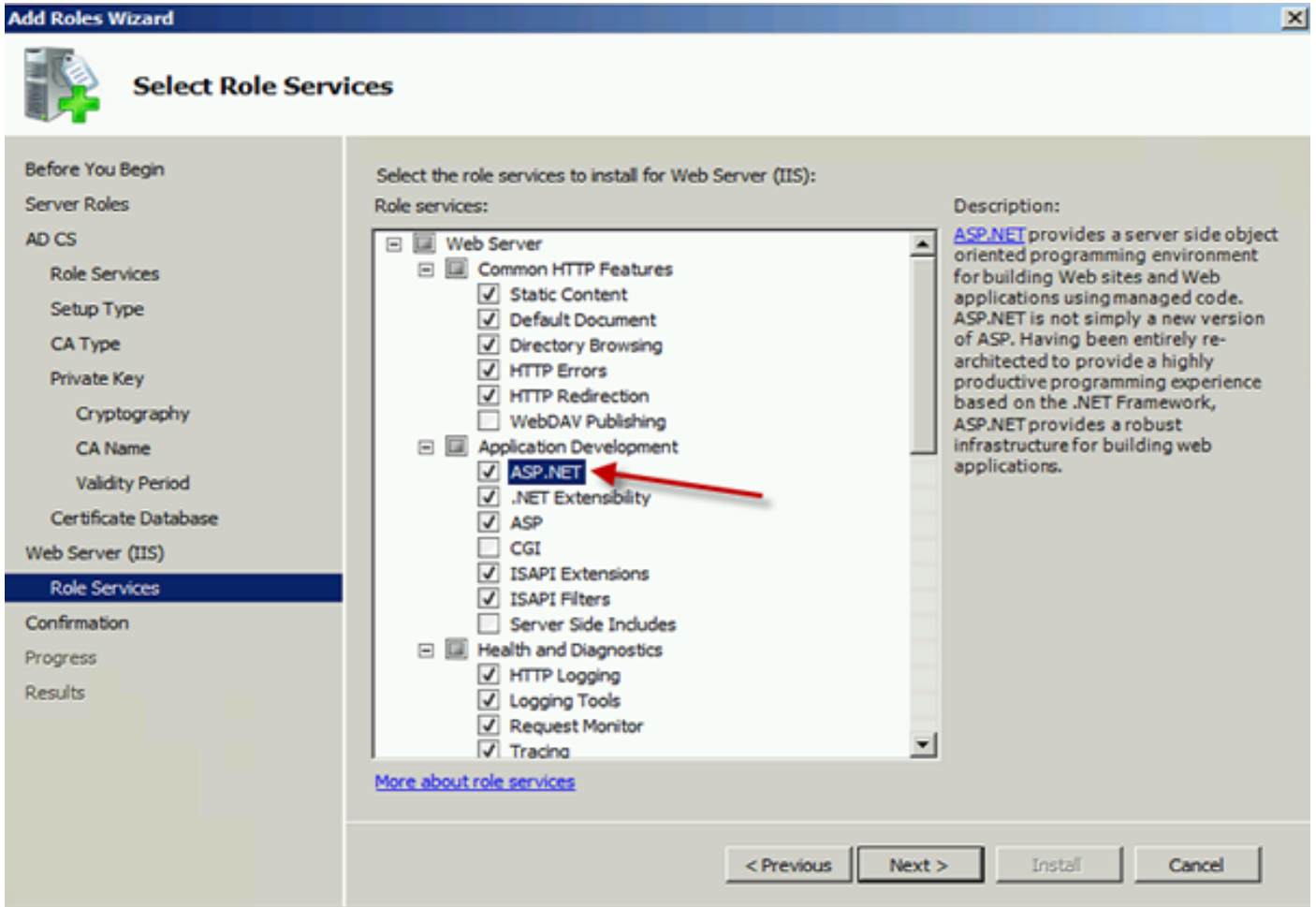


다음 단계는 CA에 대한 개인 키를 생성하는 것입니다.

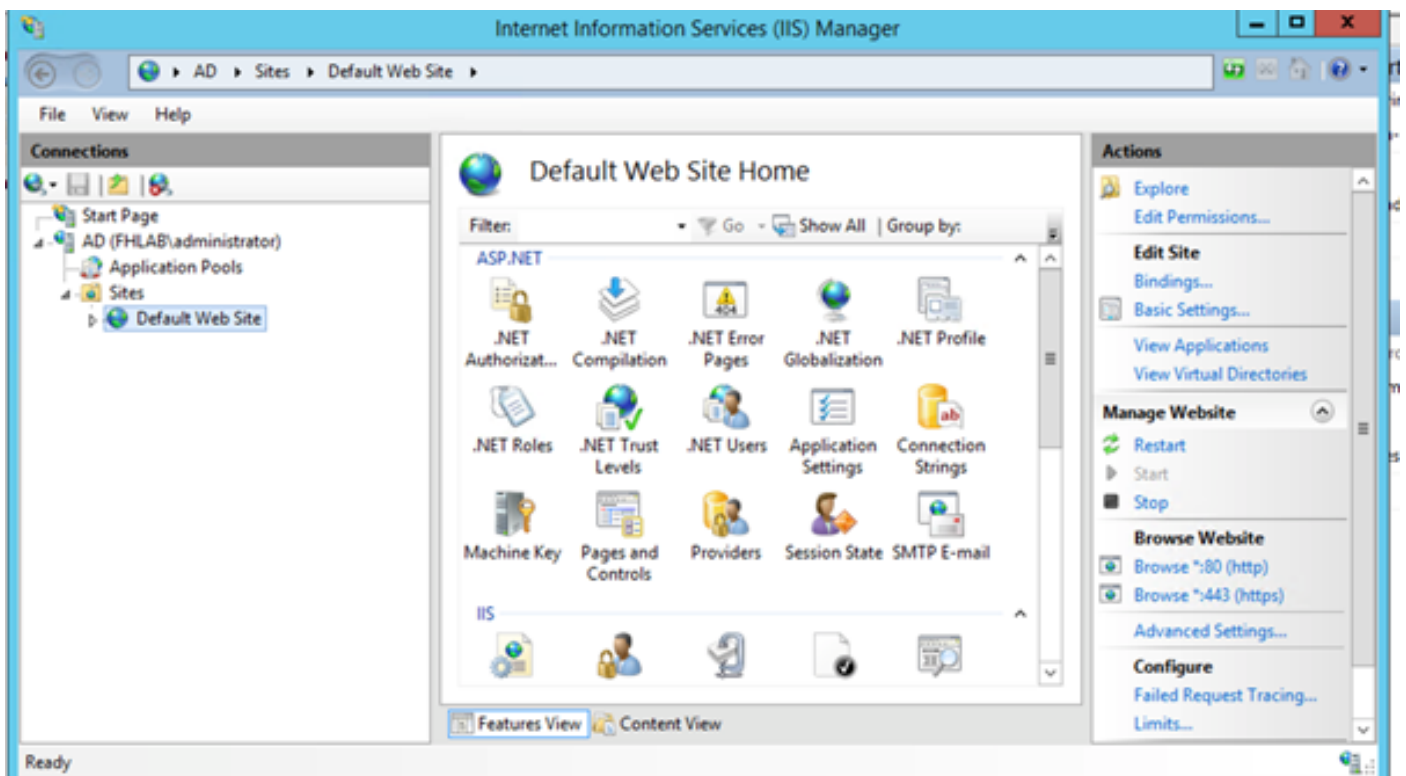


이 단계는 별도의 Windows Server 2012에 ADFS3을 설치하는 경우에만 필요합니다. CA를 구성한

후 IIS용 역할 서비스를 구성해야 합니다. 이는 CA의 웹 등록에 필요합니다. 대부분의 ADFS 배포의 경우 IIS에서 추가 역할을 사용하려면 응용 프로그램 개발에서 **ASP.NET**을 클릭하십시오.



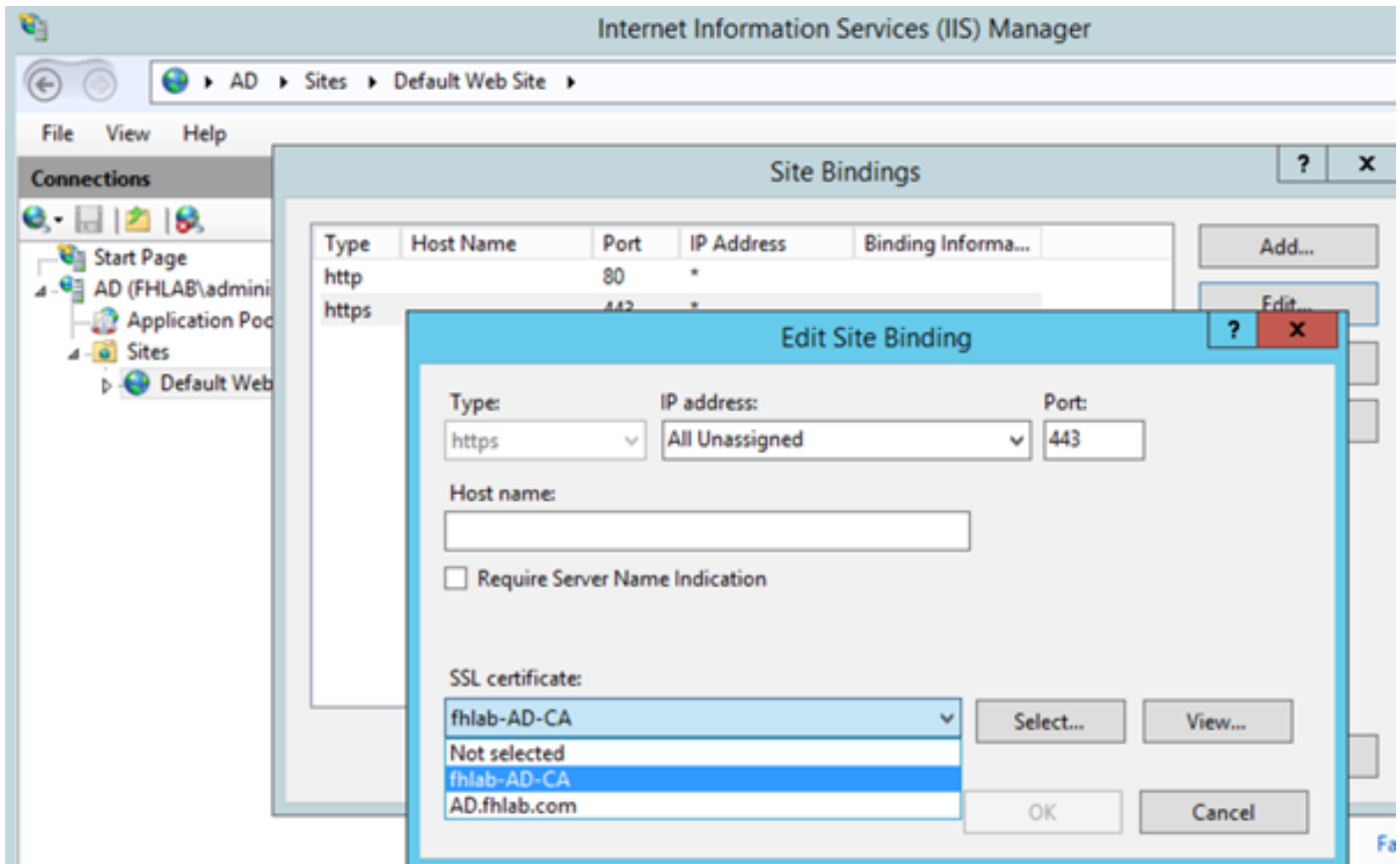
서버 관리자에서 웹 서버 > IIS를 클릭한 다음 기본 웹 사이트를 마우스 오른쪽 단추로 클릭합니다. HTTP 외에 HTTPS도 허용하려면 바인딩을 변경해야 합니다. 이는 HTTPS를 지원하기 위해 수행됩니다.



바인딩 편집을 선택합니다.



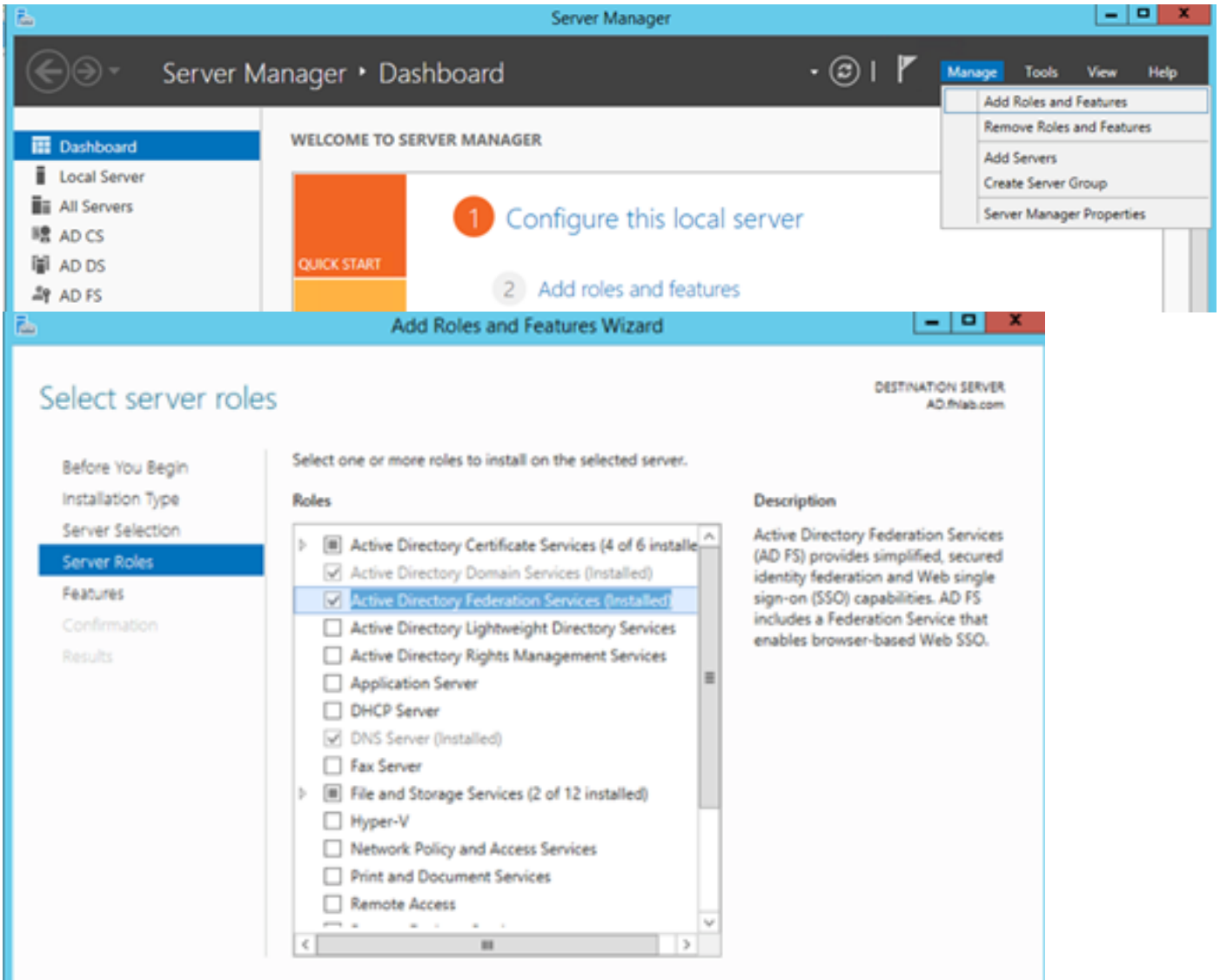
새 사이트 바인딩을 추가하고 **HTTPS**를 유형으로 선택합니다.SSL 인증서의 경우 AD 서버와 동일한 FQDN을 가져야 하는 서버 인증서를 선택합니다.



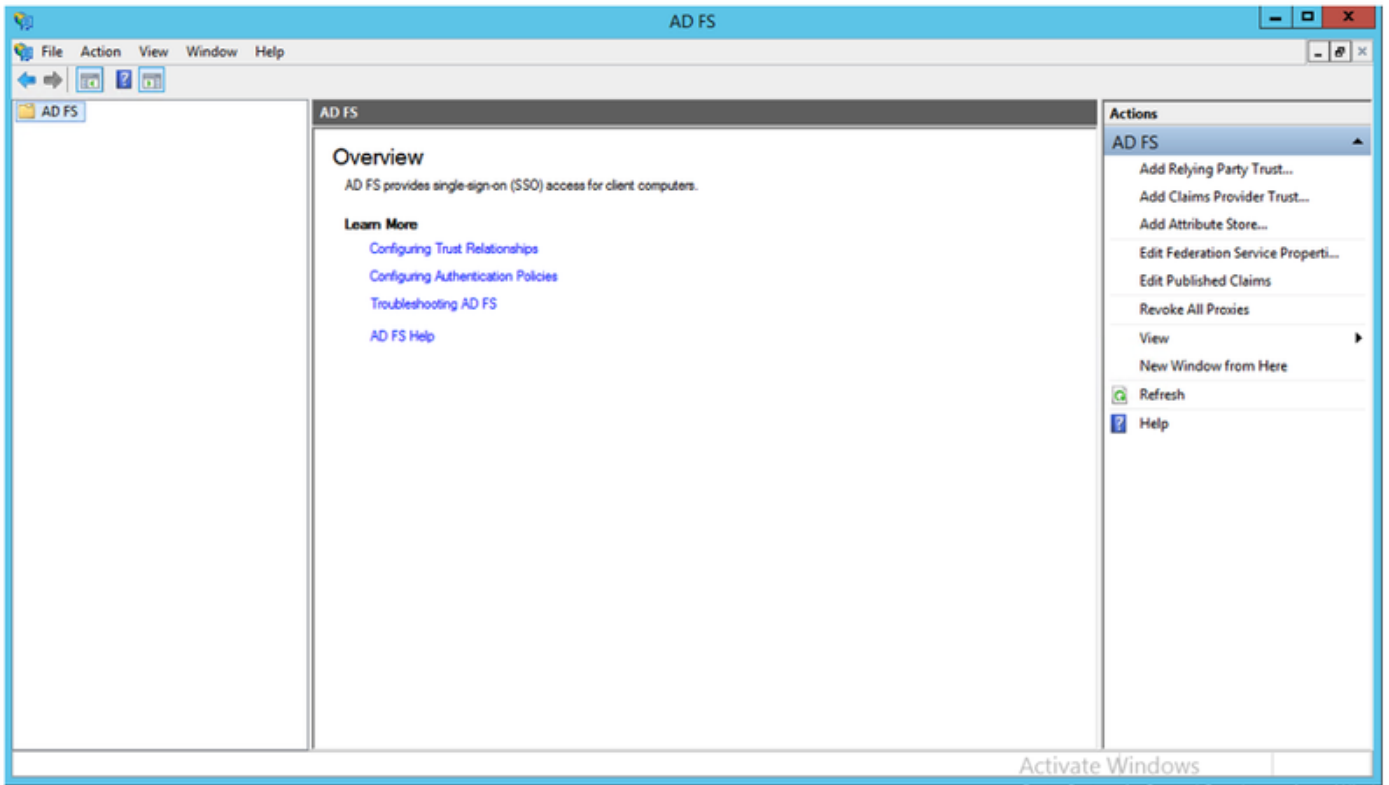
모든 필수 구성 요소 역할이 환경에 설치되어 있으므로 이제 ADFS3 Active Directory Federation Services(Windows Server 2012)를 설치할 수 있습니다.

Server Role(서버 역할)의 경우 **Server Manager(서버 관리자) > Manage(관리) > Add Server Roles and Features(서버 역할 및 기능 추가)**로 이동한 다음 **Active Directory Federation Services(Active**

Directory Federation Services)를 선택합니다. 이 IDP를 고객 네트워크 내 프라이빗 LAN에 설치하는 경우 선택합니다.



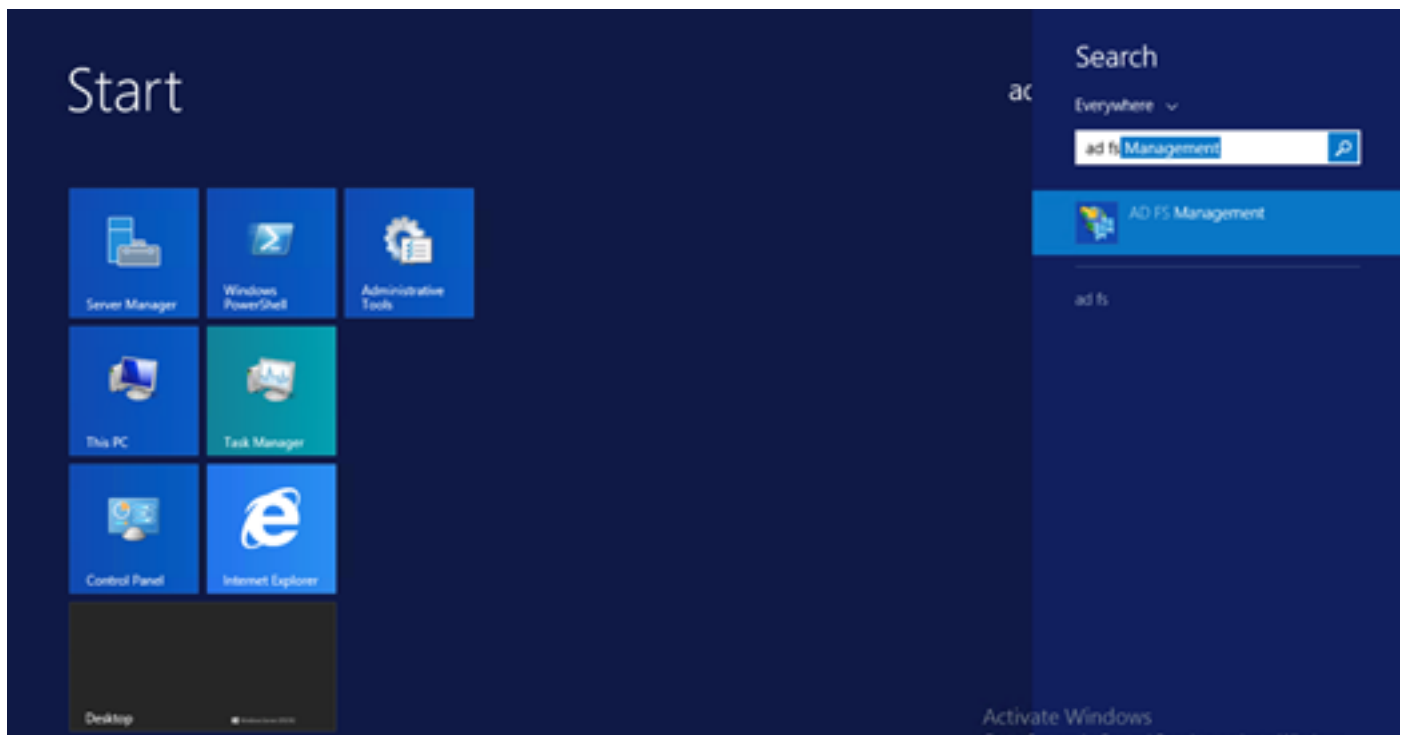
설치가 완료되면 작업 표시줄이나 시작 메뉴에서 열 수 있습니다.



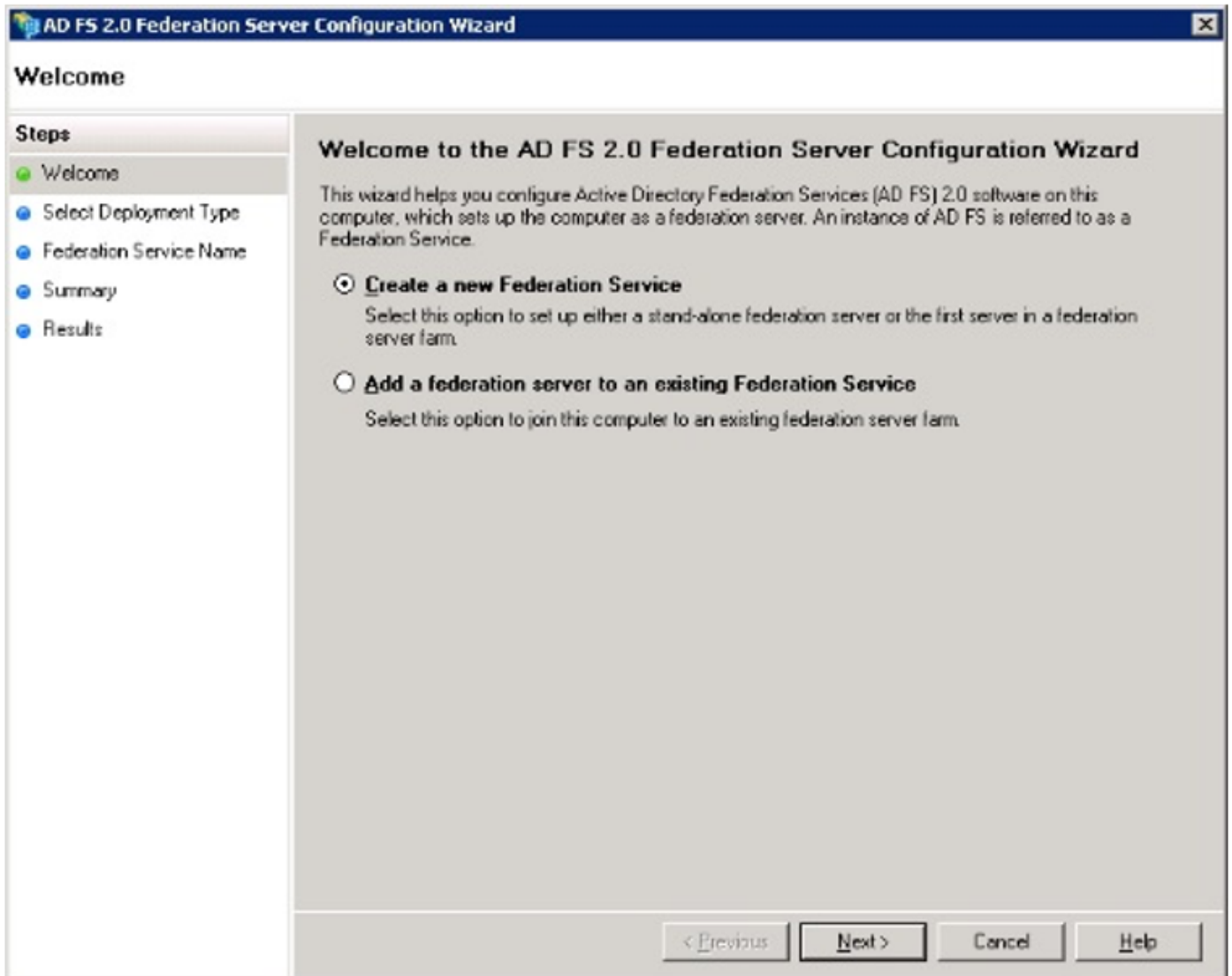
ADFS3 초기 컨피그레이션

이 섹션은 새로운 독립 실행형 페더레이션 서버 설치로 이동하지만 도메인 컨트롤러에 설치하는 데 사용할 수도 있습니다

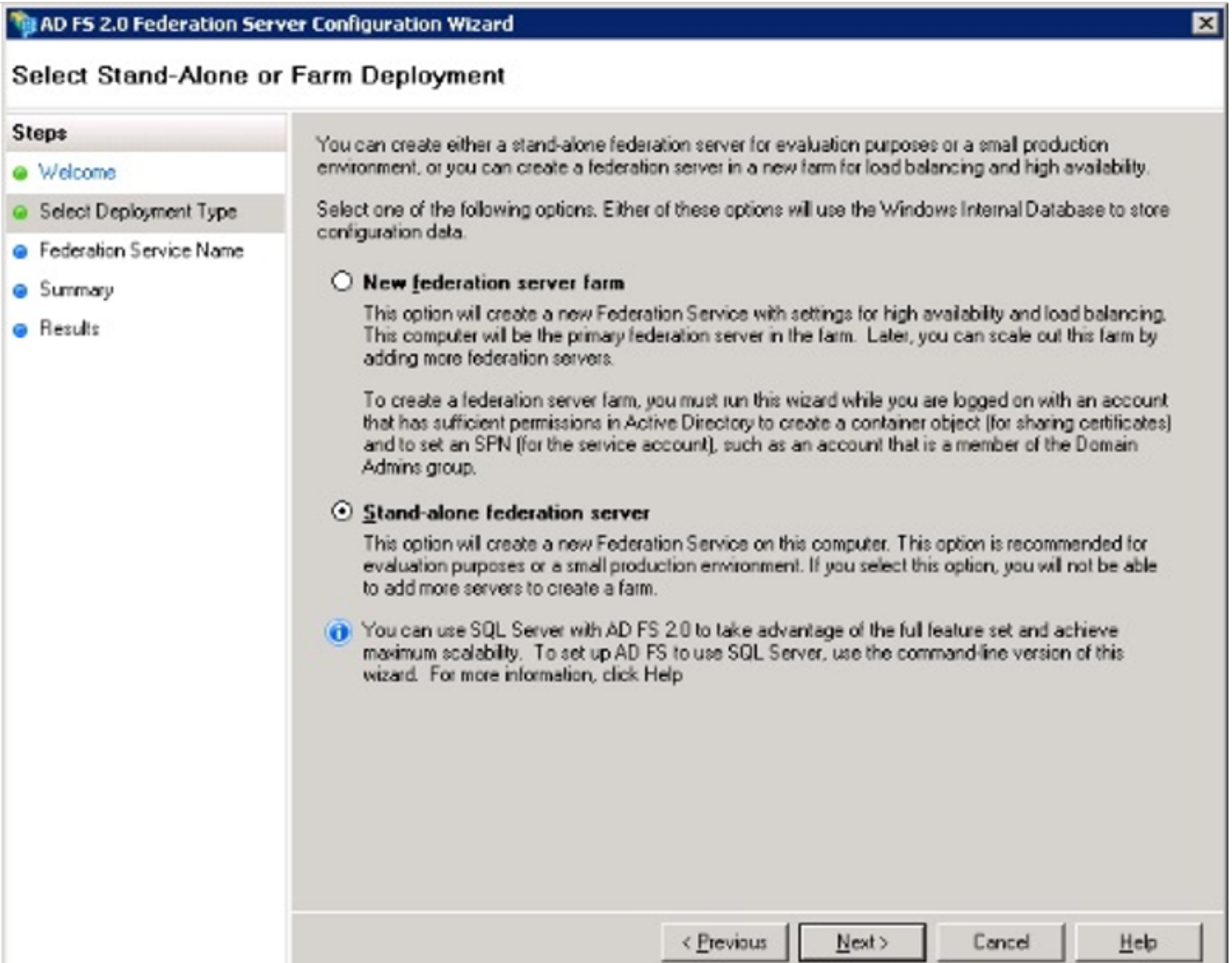
이미지에 표시된 대로 ADFS 관리 콘솔을 실행하려면 **Windows**를 선택하고 **AD FS Management**를 입력합니다.



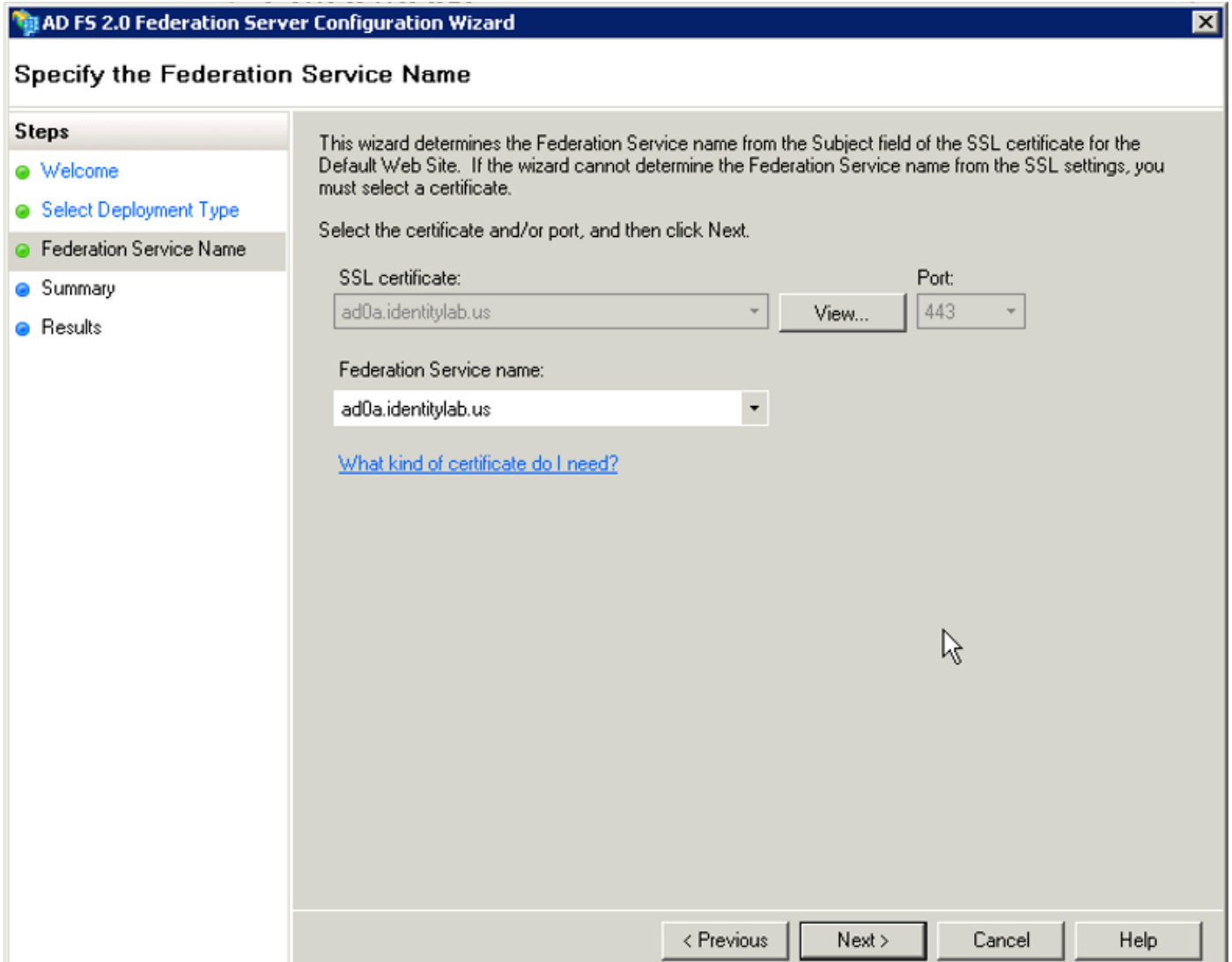
ADFS 서버 컨피그레이션을 시작하려면 **AD FS 3.0 Federation Server Configuration Wizard** 옵션을 선택합니다. 이러한 스크린샷은 AD FS 3에서 동일한 단계를 나타냅니다.



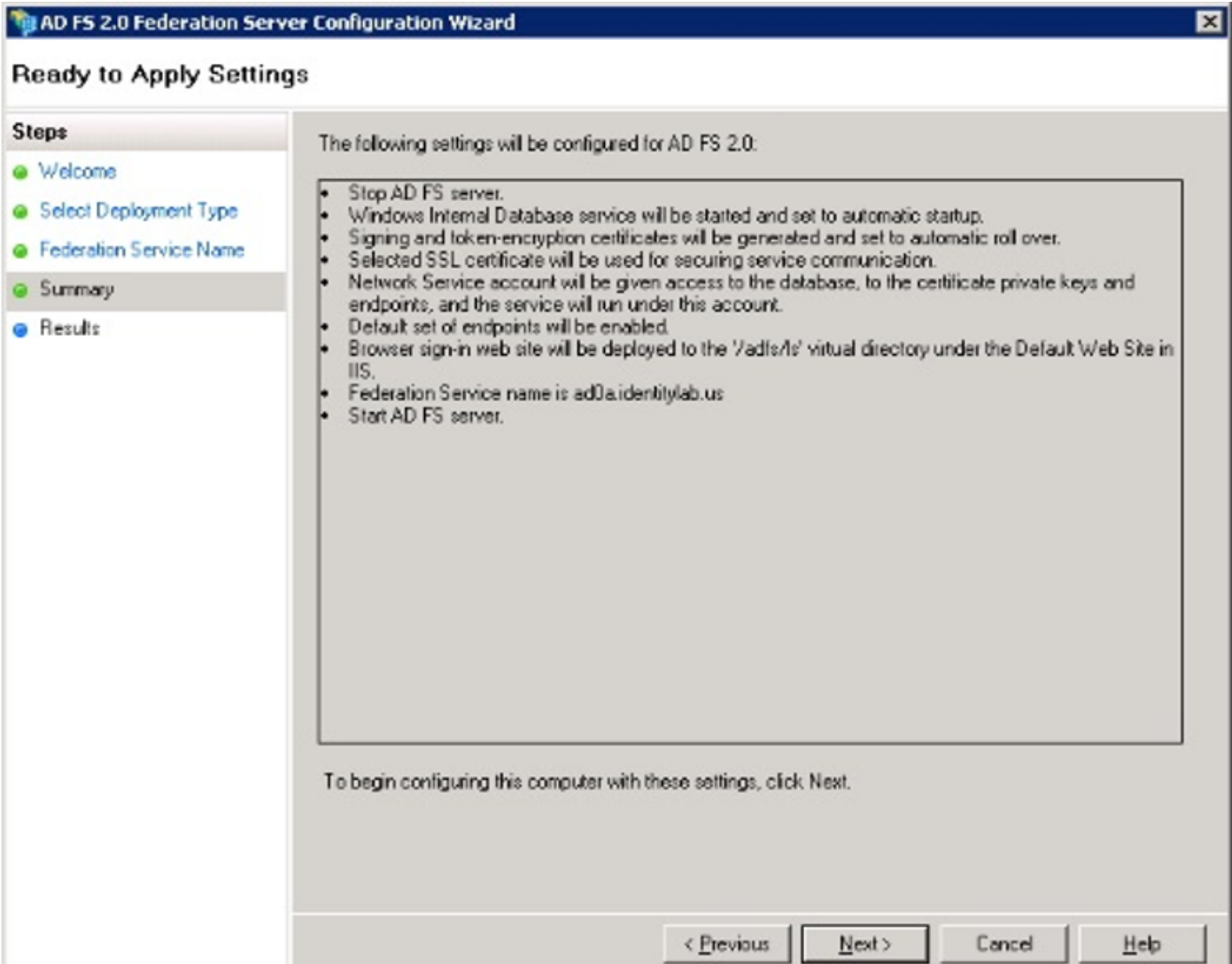
Create a new Federation Service(새 페더레이션 서비스 생성)를 선택하고 Next(다음)를 클릭합니다.



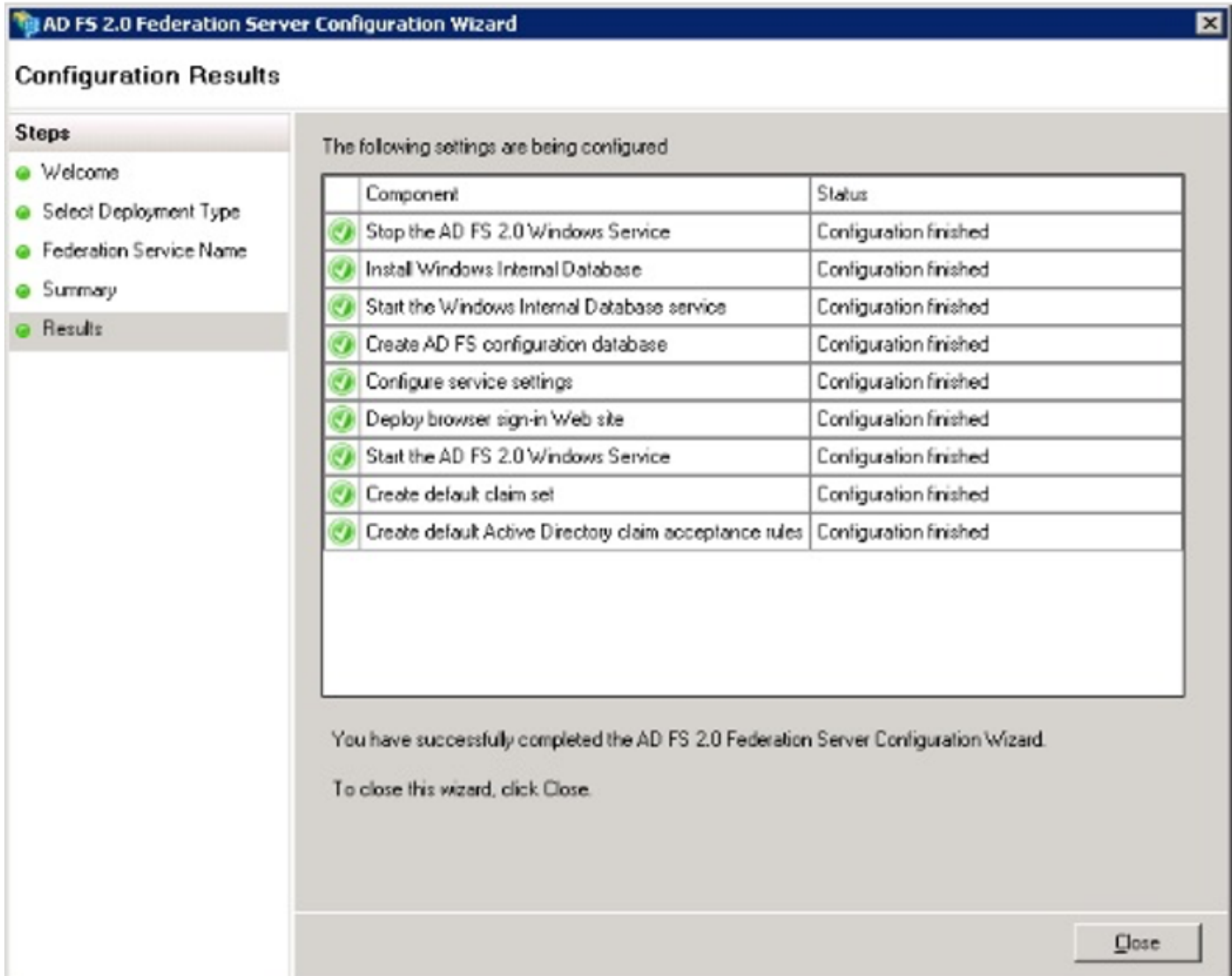
[독립 실행형 페더레이션 서버]를 선택하고 이미지에 표시된 대로 다음을 클릭합니다.



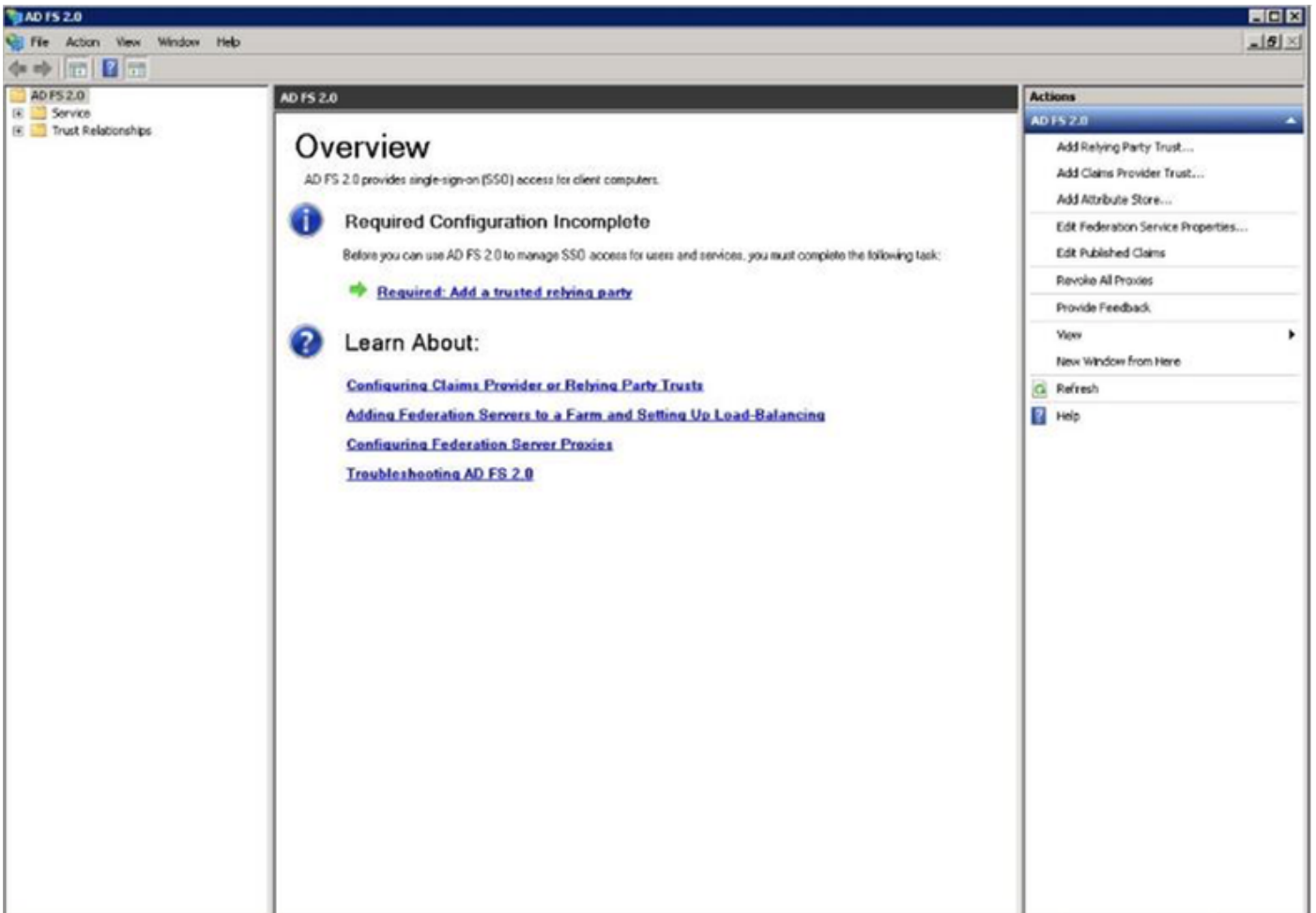
SSL 인증서의 목록에서 자체 서명 인증서를 선택합니다. 페더레이션 서비스 이름이 자동으로 채워집니다. Next(다음)를 클릭합니다.



설정을 검토하고 Next(다음)를 클릭하여 설정을 적용합니다.



모든 구성 요소가 성공적으로 완료되었는지 확인하고 **Close(닫기)**를 클릭하여 마법사를 종료하고 기본 관리 콘솔로 돌아갑니다. 몇 분 정도 걸릴 수 있습니다.



이제 ADFS가 IdP(Identity Provider)로 효과적으로 활성화되고 구성됩니다. 다음으로, CUCM을 신뢰할 수 있는 신뢰 파트너로 추가해야 합니다. 이 작업을 수행하려면 먼저 CUCM Administration에서 일부 컨피그레이션을 수행해야 합니다.



ADFS를 사용하여 CUCM에서 SSO 구성

LDAP 컨피그레이션

클러스터는 Active Directory와 LDAP로 통합되어야 하며, LDAP 인증을 구성한 후에 더 진행해야 합니다. 이미지에 표시된 대로 **System(시스템) 탭 > LDAP System(LDAP 시스템)**으로 이동합니다.

LDAP System Configuration

Status

-  Please Delete All LDAP Directories Before Making Changes on This Page
-  Please Disable LDAP Authentication Before Making Changes on This Page

LDAP System Information

Enable Synchronizing from LDAP Server

LDAP Server Type


LDAP Attribute for User ID

그런 다음 System(시스템) 탭 > LDAP Directory(LDAP 디렉토리)로 이동합니다.

LDAP Directory

 Save  Delete  Copy  Perform Full Sync Now  Add New

Status

 Status: Ready

LDAP Directory Information

LDAP Configuration Name*

LDAP Manager Distinguished Name*

LDAP Password*

Confirm Password*

LDAP User Search Base*

LDAP Custom Filter for Users

Synchronize* Users Only Users and Groups

LDAP Custom Filter for Groups

LDAP Directory Synchronization Schedule

Perform Sync Just Once

Perform a Re-sync Every*

Next Re-sync Time (YYYY-MM-DD hh:mm)*

Standard User Fields To Be Synchronized			
Cisco Unified Communications Manager User Fields	LDAP Attribute	Cisco Unified Communications Manager User Fields	LDAP Attribute
User ID	sAMAccountName	First Name	givenName
Middle Name	middleName	Last Name	sn
Manager ID	manager	Department	department
Phone Number	telephoneNumber	Mail ID	mail
Title	title	Home Number	homephone
Mobile Number	mobile	Pager Number	pager
Directory URI	mail	Display Name	displayName

LDAP Server Information

Host Name or IP Address for Server* LDAP Port* Use TLS

Active Directory 사용자가 CUCM과 동기화된 후 LDAP 인증을 구성해야 합니다.

The screenshot shows the Cisco Unified CM Administration web interface. The page title is "Cisco Unified CM Administration" and the sub-header is "LDAP Authentication". The status is "Ready". Under "LDAP Authentication for End Users", the "Use LDAP Authentication for End Users" checkbox is checked. The "LDAP Manager Distinguished Name" is set to "fhlab/Administrator". The "LDAP Password" and "Confirm Password" fields are masked with asterisks. The "LDAP User Search Base" is set to "cn=users,dc=fhlab,dc=com". Below this, the "LDAP Server Information" section is visible, showing the host name "10.89.228.226" and LDAP port "389".

CUCM의 최종 사용자는 최종 사용자 프로필에 특정 액세스 제어 그룹을 할당해야 합니다. ACG는 표준 CCM 슈퍼 유저입니다. 환경이 준비되면 사용자가 SSO를 테스트하는 데 사용됩니다.

End User Configuration Related Links: [Back to Find List Users](#)

Confirm MLPP Password
 MLPP Precedence Authorization Level

CAPF Information

Associated CAPF Profiles [View Details](#)

Permissions Information

Groups:

- Standard CCM End Users
- Standard CCM Super Users**
- Standard CTI Allow Control of All Devices
- Standard CTI Enabled

[View Details](#)

Roles:

- Standard AXL API Access
- Standard Admin Rep Tool Admin
- Standard CCM Admin Users
- Standard CCM End Users
- Standard CCMADMIN Administration

[View Details](#)

Conference Now Information

Enable End User to Host Conference Now
 Meeting Number
 Attendees Access Code

CUCM 메타데이터

이 섹션에는 CUCM 게시자에 대한 프로세스가 표시됩니다.

첫 번째 작업은 URL로 이동해야 하는 CUCM 메타데이터를 가져오는 것입니다. <https://<CUCM Pub FQDN>:8443/ssosp/ws/config/metadata/sp> 또는 **System 탭 > SAML Single Sign-on**에서 다운로드 할 수 있습니다. 노드 또는 Cluster Wide 별로 수행할 수 있습니다. 이 클러스터 전체에서 수행하는 것이 좋습니다.

System > Call Routing > Media Resources > ... > Device > User Manager > ... > SAML Administration

SAML Single Sign-On

SSO Mode

Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)
 Per node (One metadata file per node)

Status

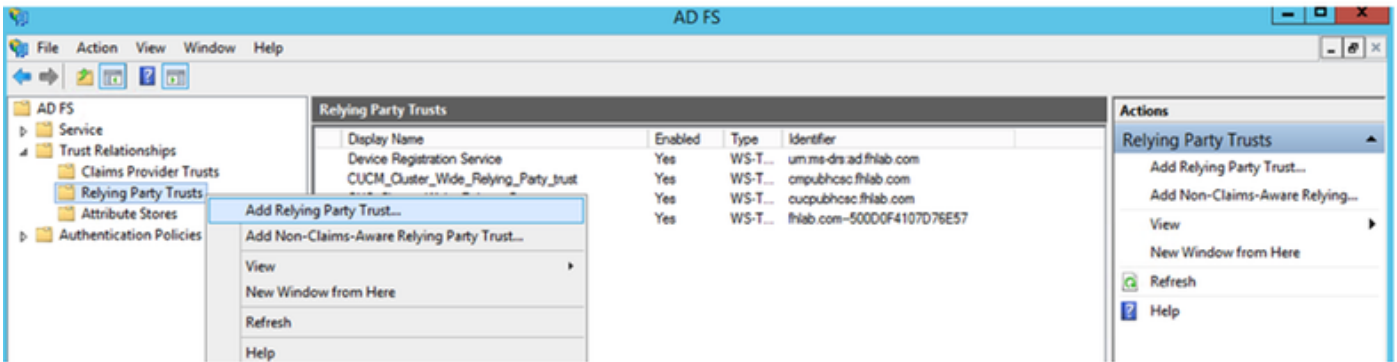
- RTMT is enabled for SSO. You can change SSO for RTMT [here](#).
- SAML SSO enabled

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cmpubhcsc.fhlab.com	SAML	N/A	April 20, 2020 2:00:57 PM PDT	File	April 18, 2020 8:05:38 PM PDT	Passed - April 20, 2020 2:02:15 PM PDT <input type="button" value="Run SSO Test..."/>
cmsubhcsc.fhlab.com	SAML	IdP	April 20, 2020 2:00:57 PM PDT	File	April 18, 2020 8:05:37 PM PDT	Passed - April 20, 2020 1:49:45 PM PDT <input type="button" value="Run SSO Test..."/>
imppubhcsc.fhlab.com	SAML	IdP	April 20, 2020 2:00:57 PM PDT	File	April 18, 2020 8:05:37 PM PDT	Passed - May 24, 2020 12:02:56 PM PDT <input type="button" value="Run SSO Test..."/>
impsubhcsc.fhlab.com	SAML	IdP	April 20, 2020 2:00:57 PM PDT	File	April 18, 2020 8:05:37 PM PDT	Passed - May 24, 2020 12:03:26 PM PDT <input type="button" value="Run SSO Test..."/>

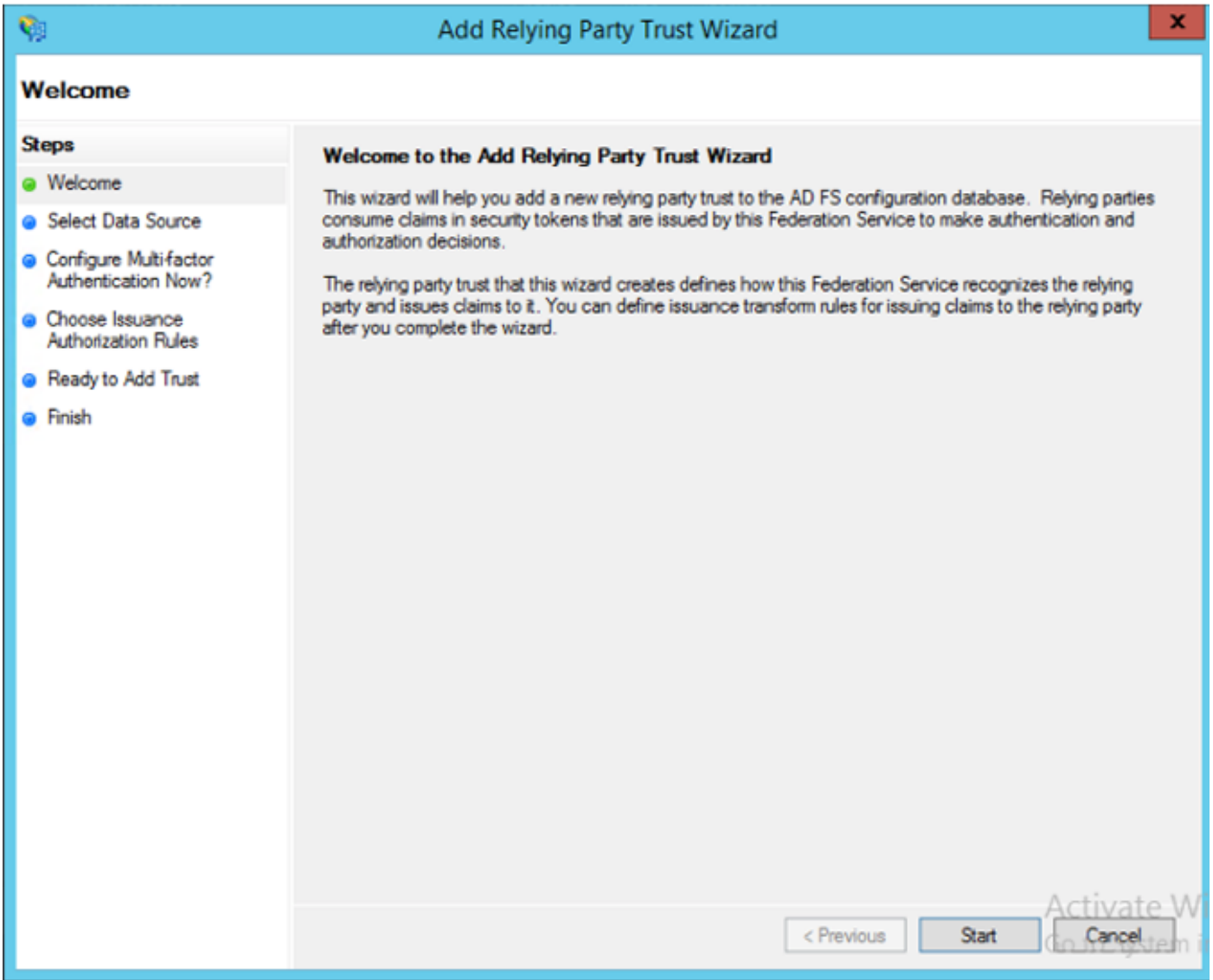
다음에 필요한 sp_cucm0a.xml과 같은 의미 있는 이름으로 데이터를 로컬에 저장합니다.

ADFS 신뢰 당사자 구성

AD FS 3.0 관리 콘솔로 다시 전환합니다.

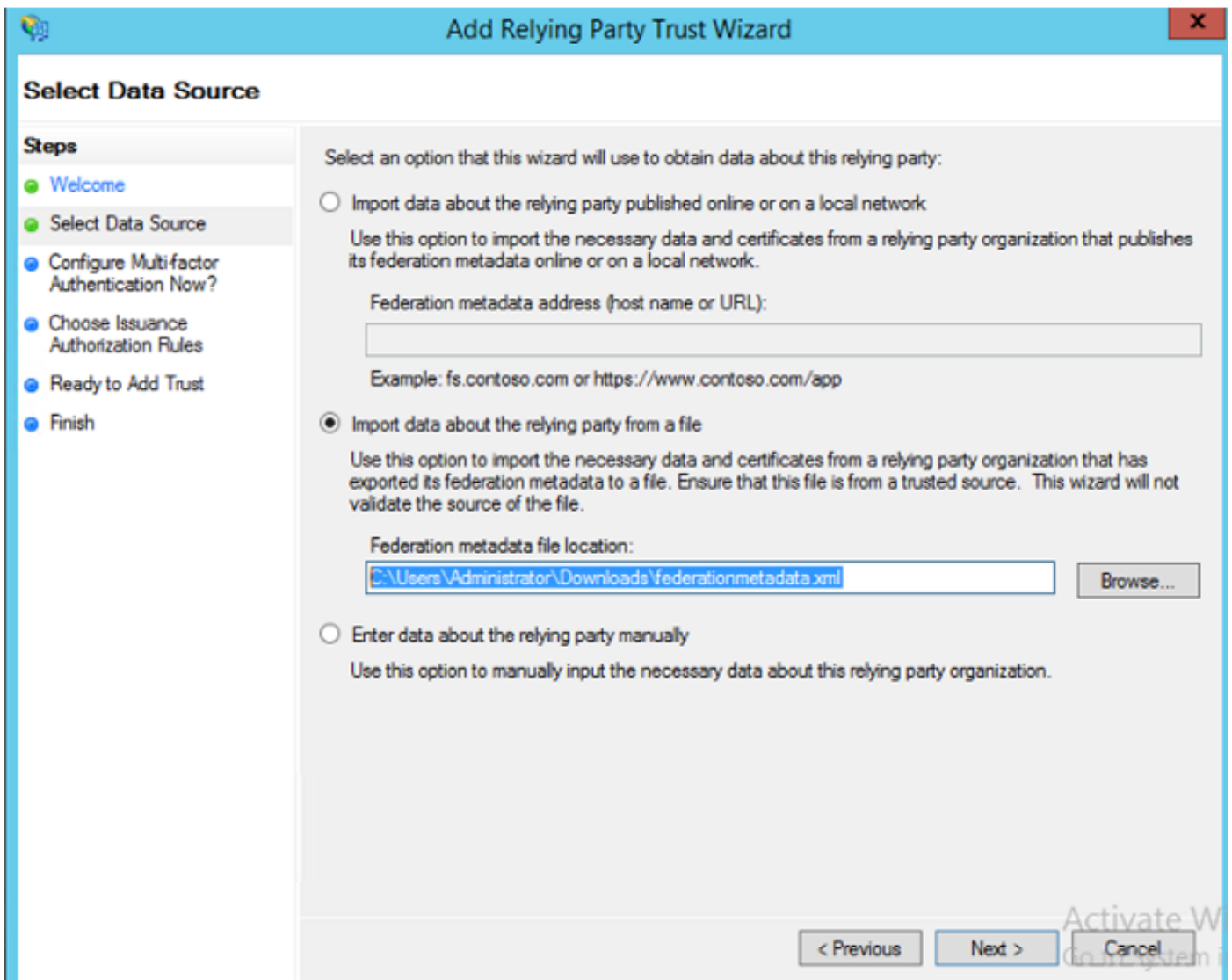


Add Relying Party Trust Wizard를 클릭합니다.

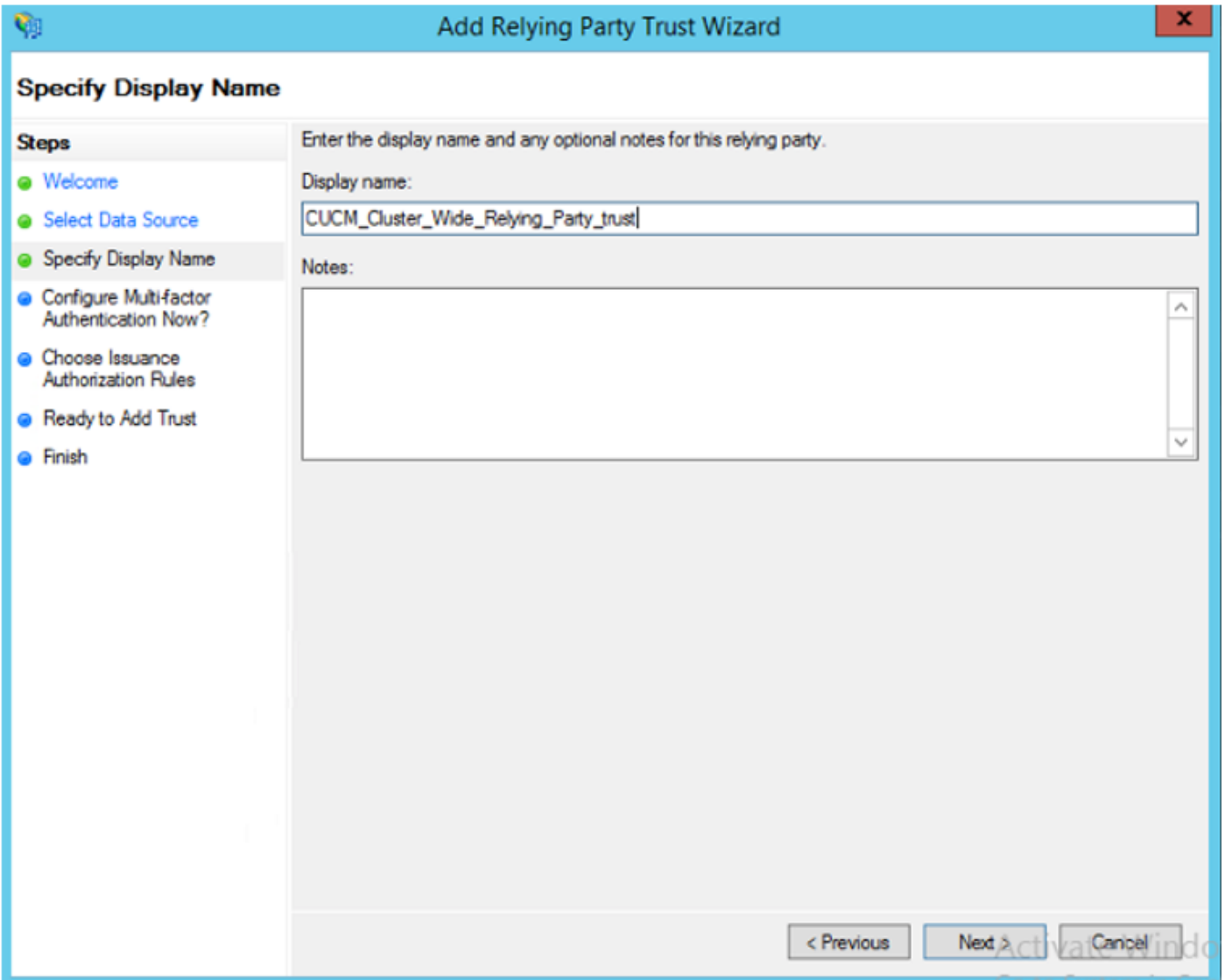


Start(시작)를 클릭하여 계속합니다.

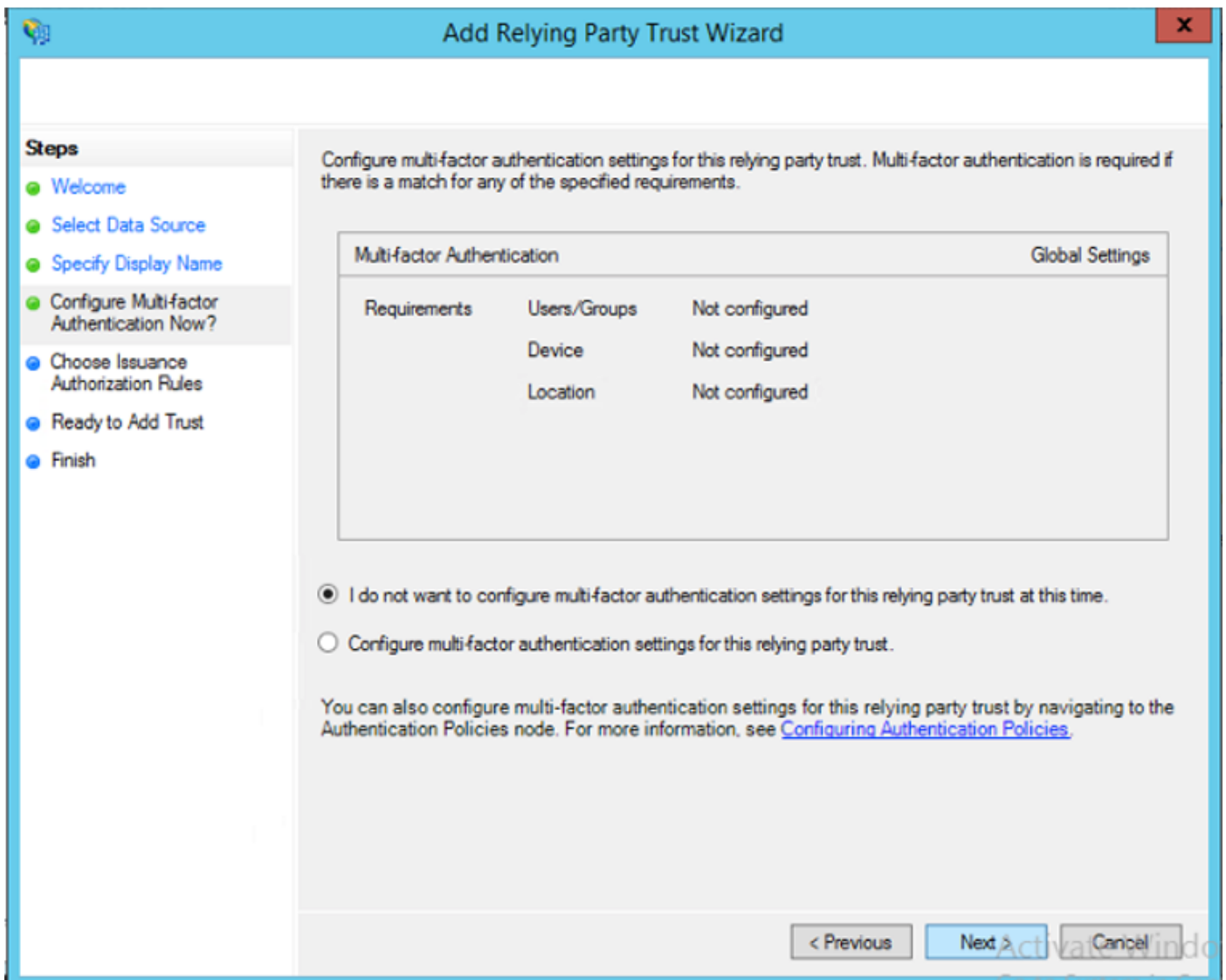
이전에 저장한 federationmetadata.xml 메타데이터 XML 파일을 선택하고 다음을 클릭합니다.



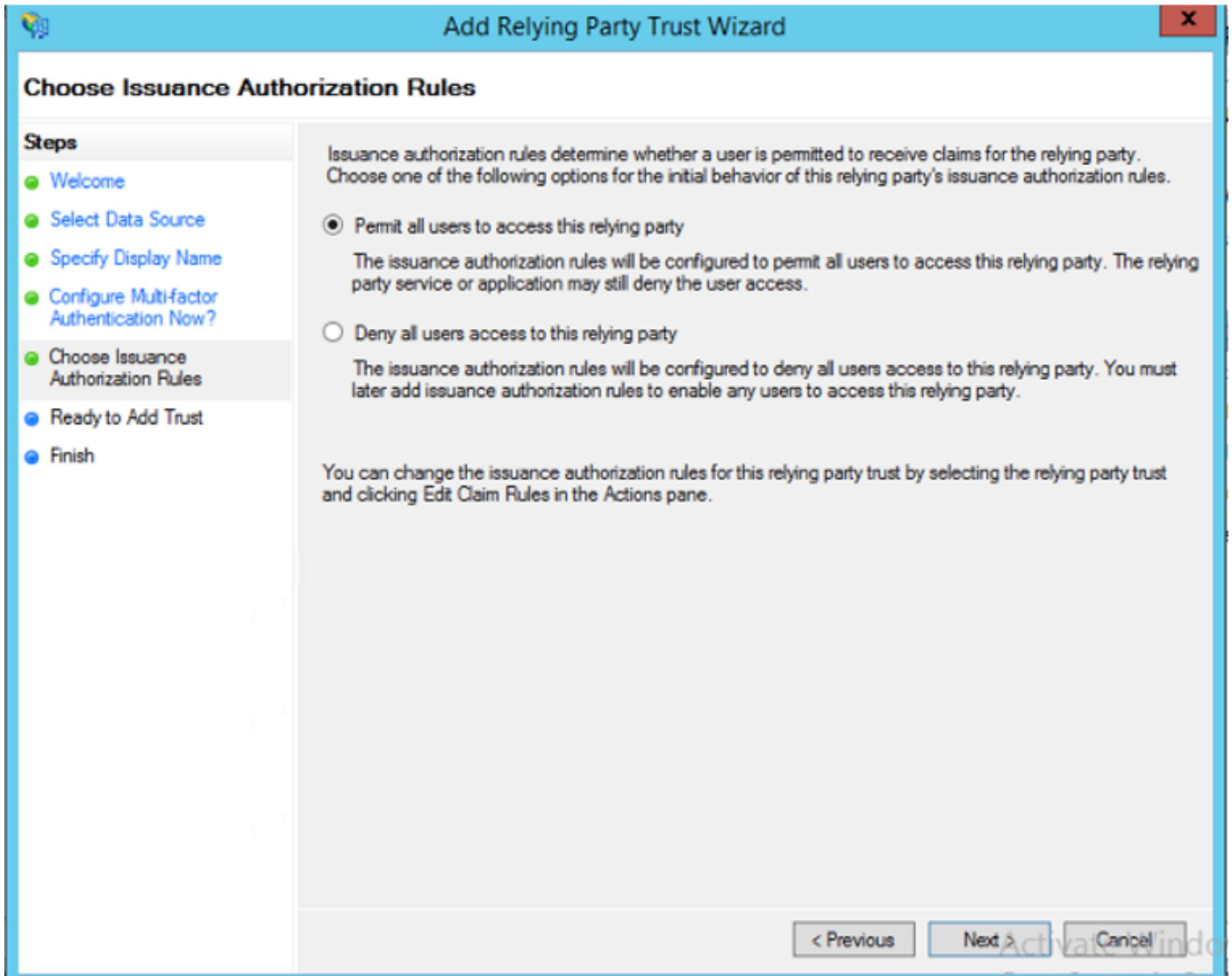
CUCM_Cluster_Wide_Relying_Party_trust를 표시 이름으로 사용하고 Next를 클릭합니다.



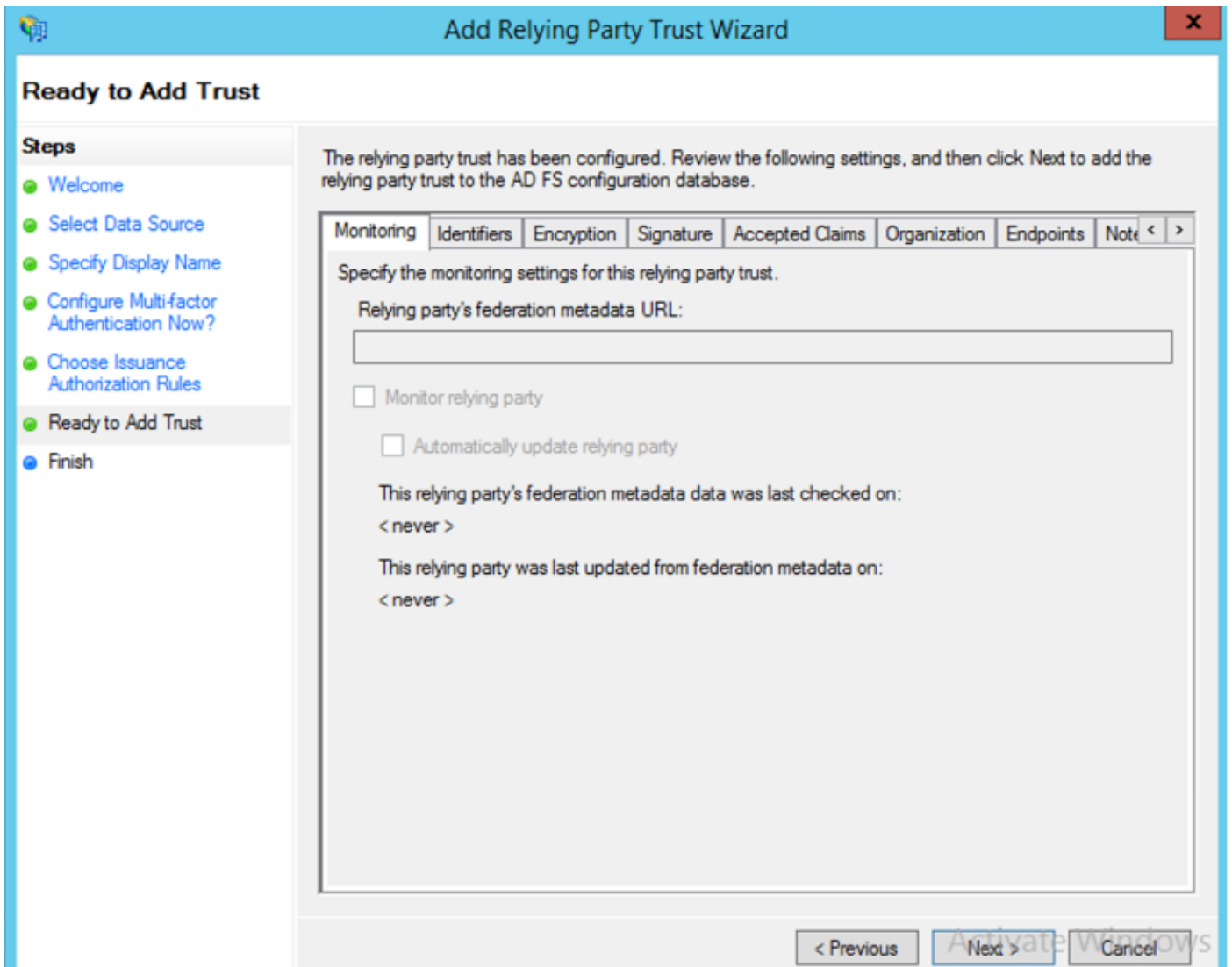
첫 번째 옵션을 선택하고 다음을 클릭합니다.



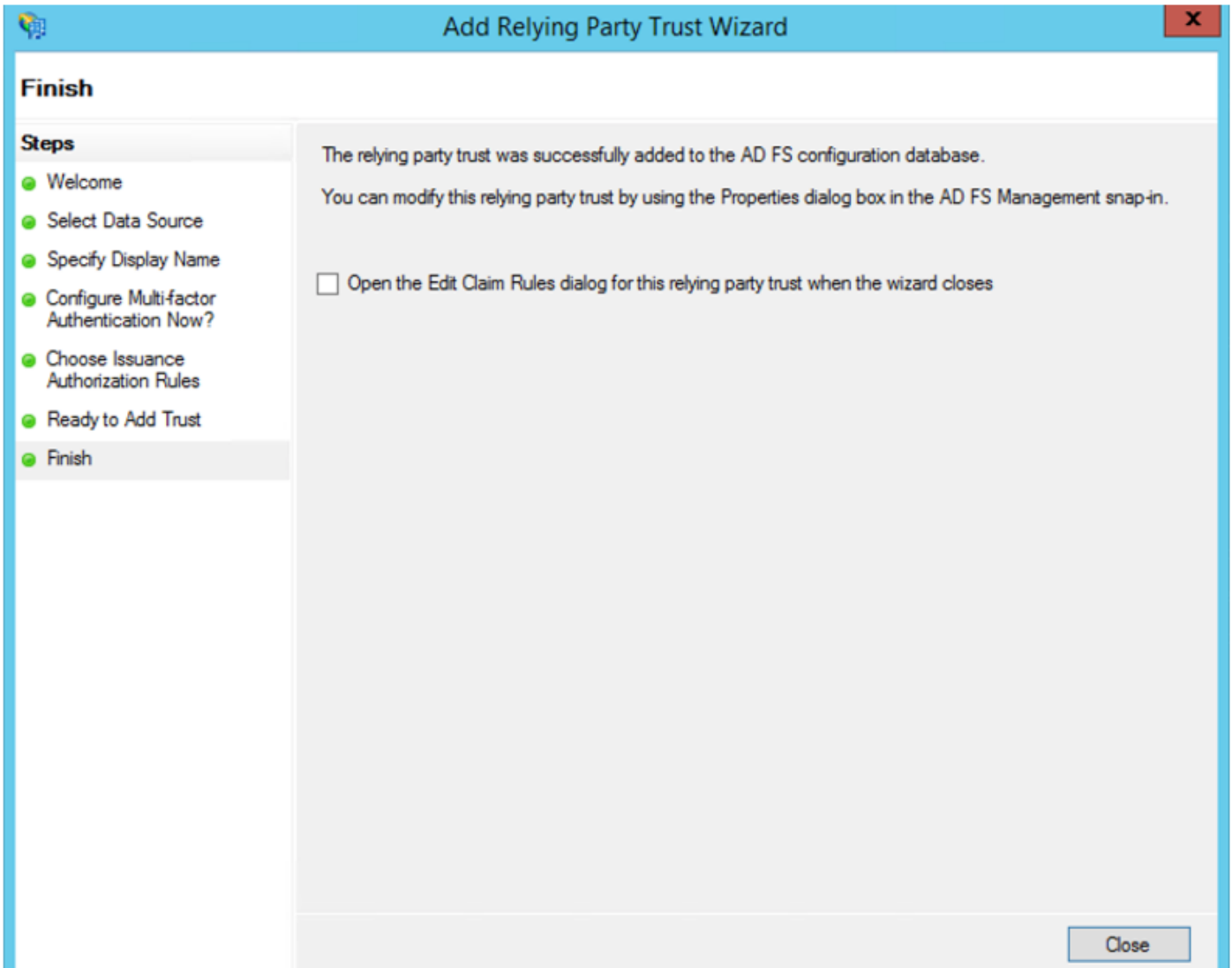
Permit all users to access this relying party(모든 사용자가 이 신뢰 당사자에 액세스하도록 허용)를 선택하고 이미지에 표시된 대로 Next(다음)를 클릭합니다.



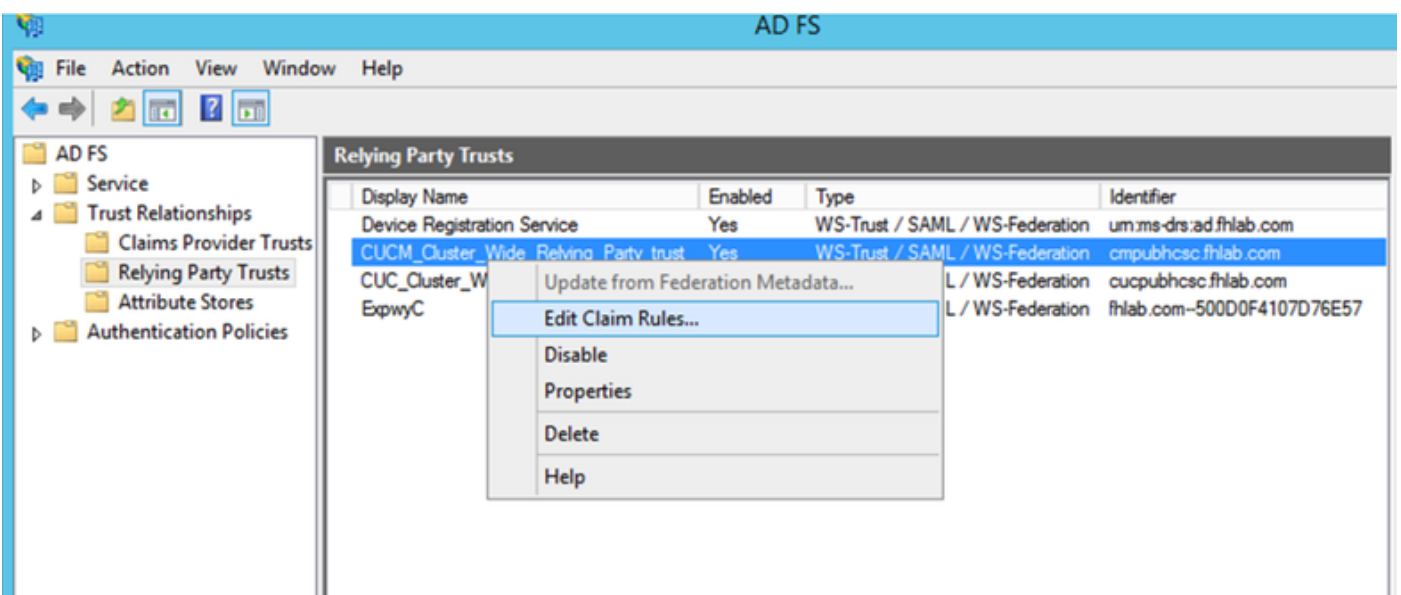
컨피그레이션을 검토하고 이미지에 표시된 대로 **Next**를 클릭합니다.



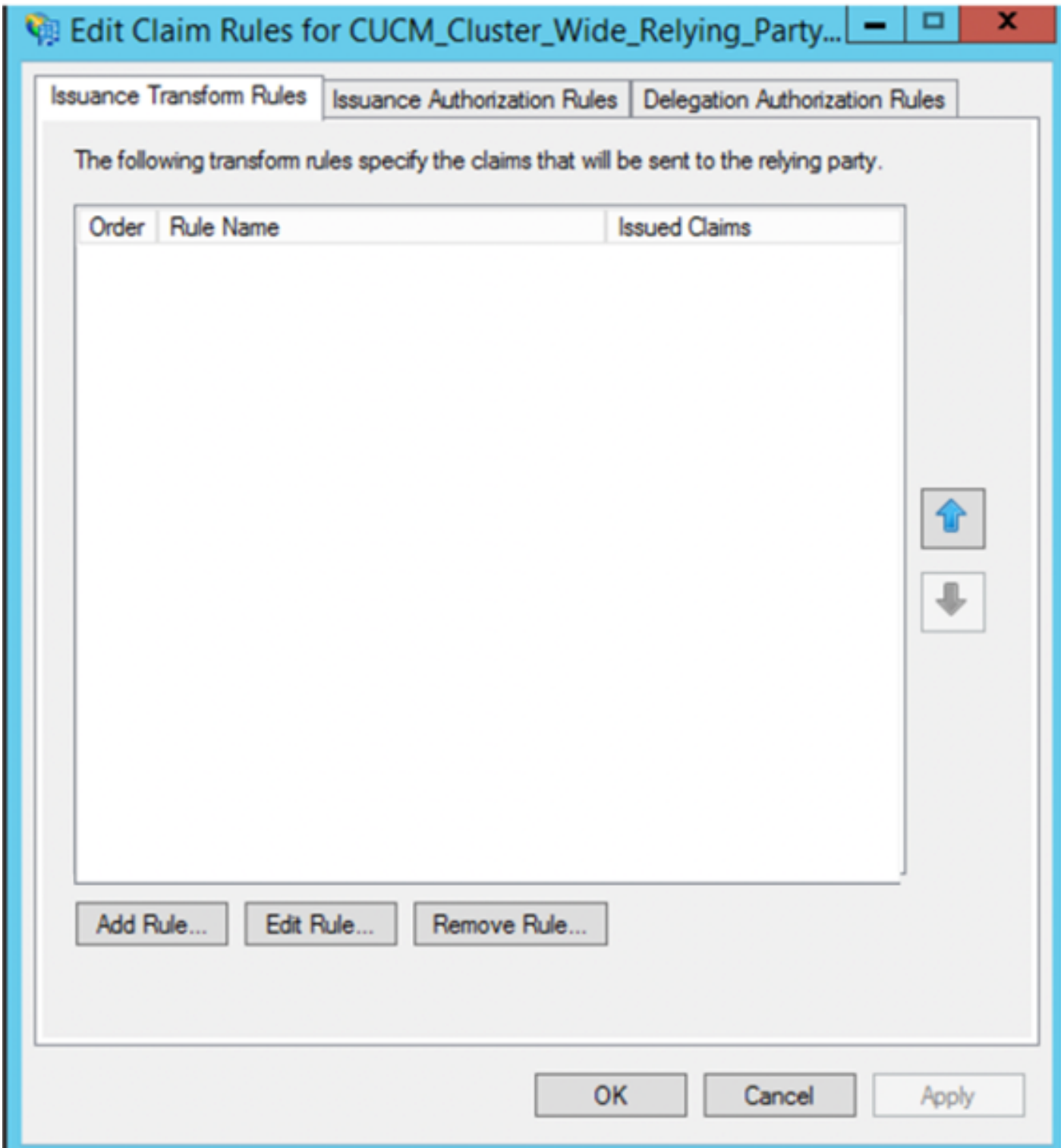
확인란의 선택을 취소하고 닫기를 클릭합니다.



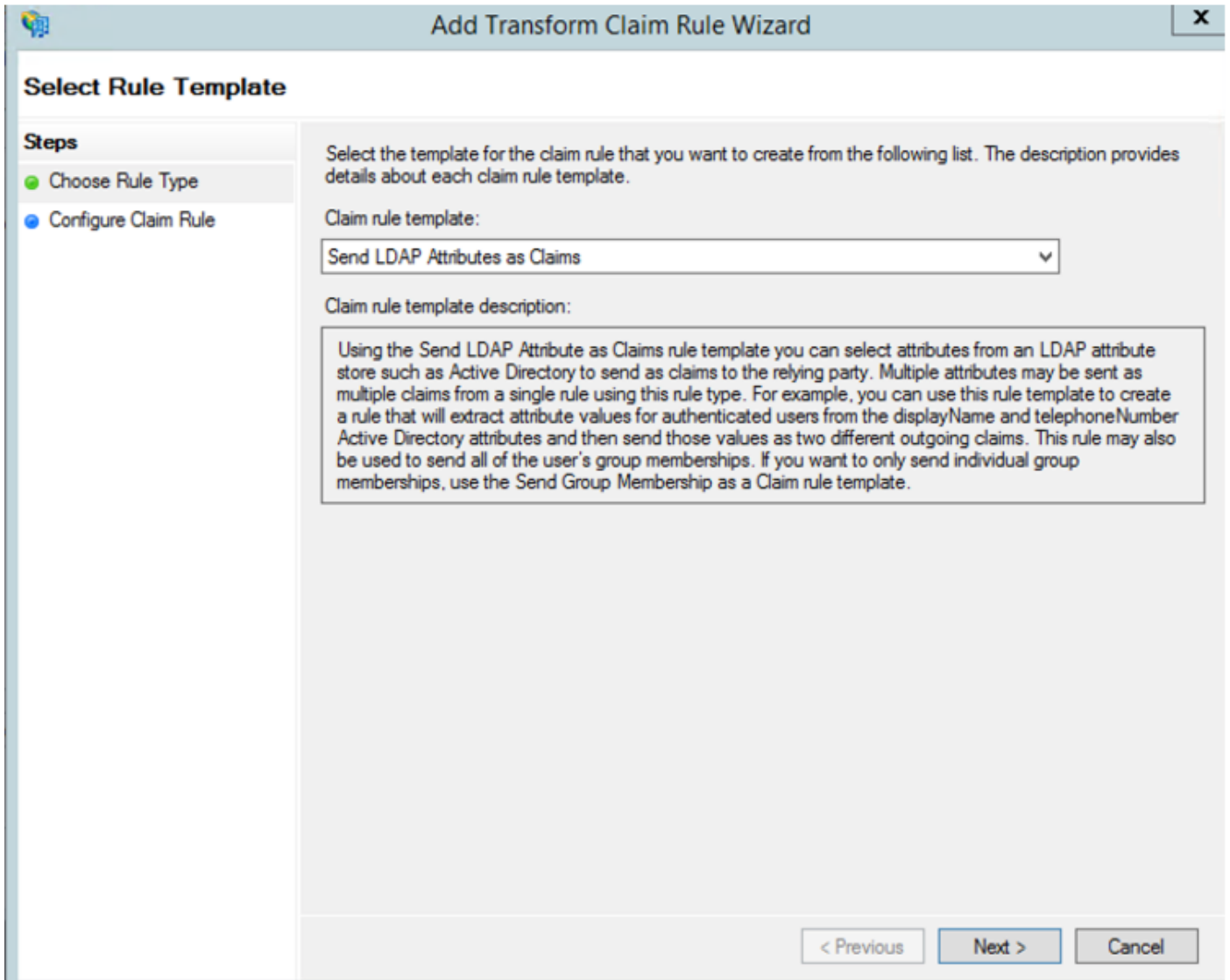
보조 마우스 버튼을 사용하여 이미지에 표시된 대로 방금 생성한 **Relying Party Trust**(당사자 신뢰 신뢰 신뢰)와 **Edit Claim Rules**(클레임 규칙 수정) 컨피그레이션을 선택합니다.



이미지에 표시된 대로 **Add Rule**을 클릭합니다.



Send LDAP Attributes as Claims(LDAP 특성을 클레임으로 보내기)를 선택하고 Next(다음)를 클릭합니다.



다음 매개변수를 구성합니다.

클레임 규칙 이름:이름 ID

특성 저장소:Active Directory(드롭다운 메뉴 화살표를 두 번 클릭)

LDAP 특성:SAM 계정 이름

발송 클레임 유형:uid

FINISH/OK를 클릭하여 계속합니다.

uid는 소문자는 아니며 드롭다운 메뉴에 없습니다.입력합니다.

Edit Rule - NameID ✕

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

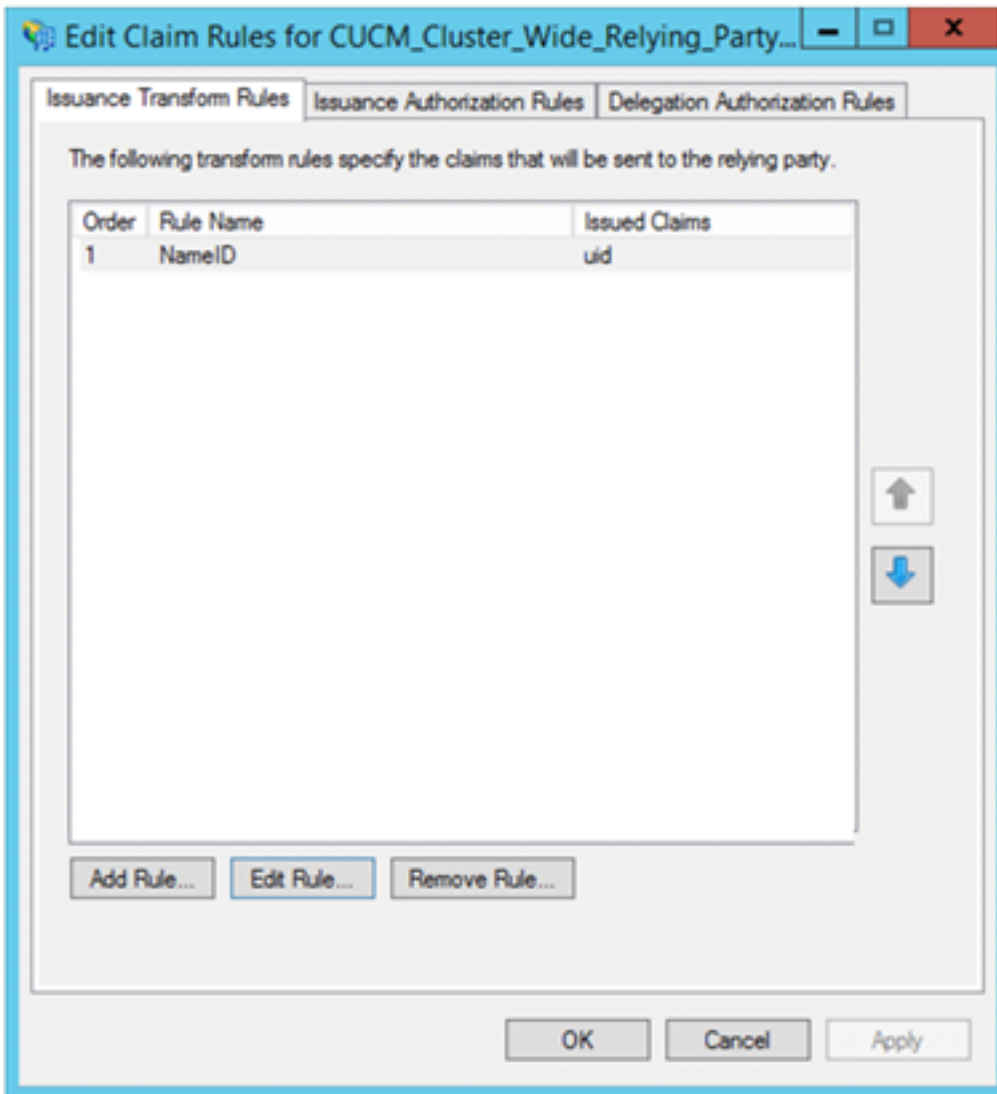
Attribute store:

Mapping of LDAP attributes to outgoing claim types:

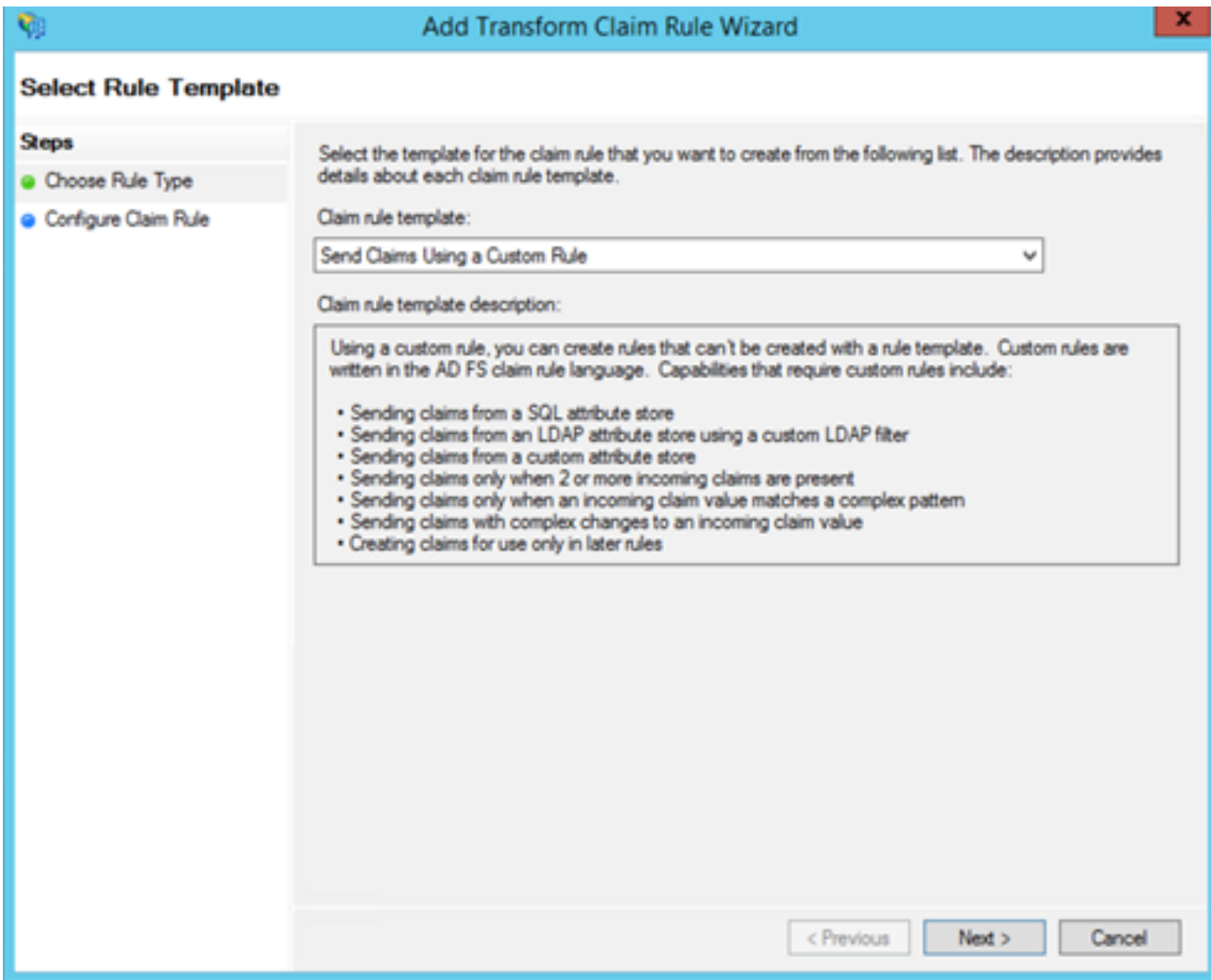
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name	uid
*		

Activate

다른 규칙을 추가하려면 Add Rule을 다시 클릭합니다.



Send Claims Using a Custom Rule을 선택하고 Next를 클릭합니다.



Cluster_Side_Claim_Rule이라는 사용자 지정 규칙을 생성합니다.

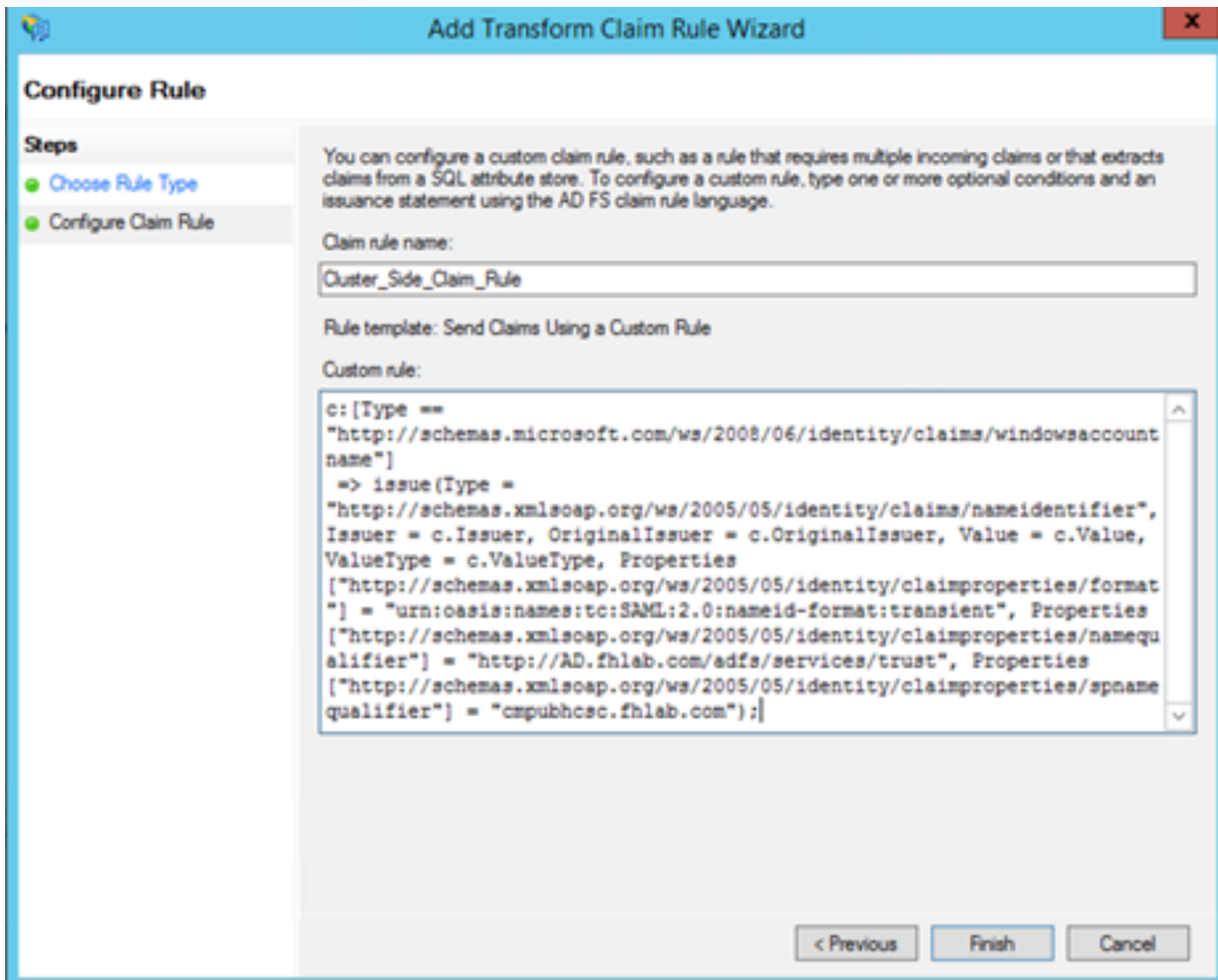
여기에서 바로 규칙 창에 이 텍스트를 복사하여 붙여넣습니다. 텍스트 편집기에서 편집하면 다음표가 변경되고 SSO를 테스트할 때 규칙이 실패합니다.

```
c:[Type ==
```

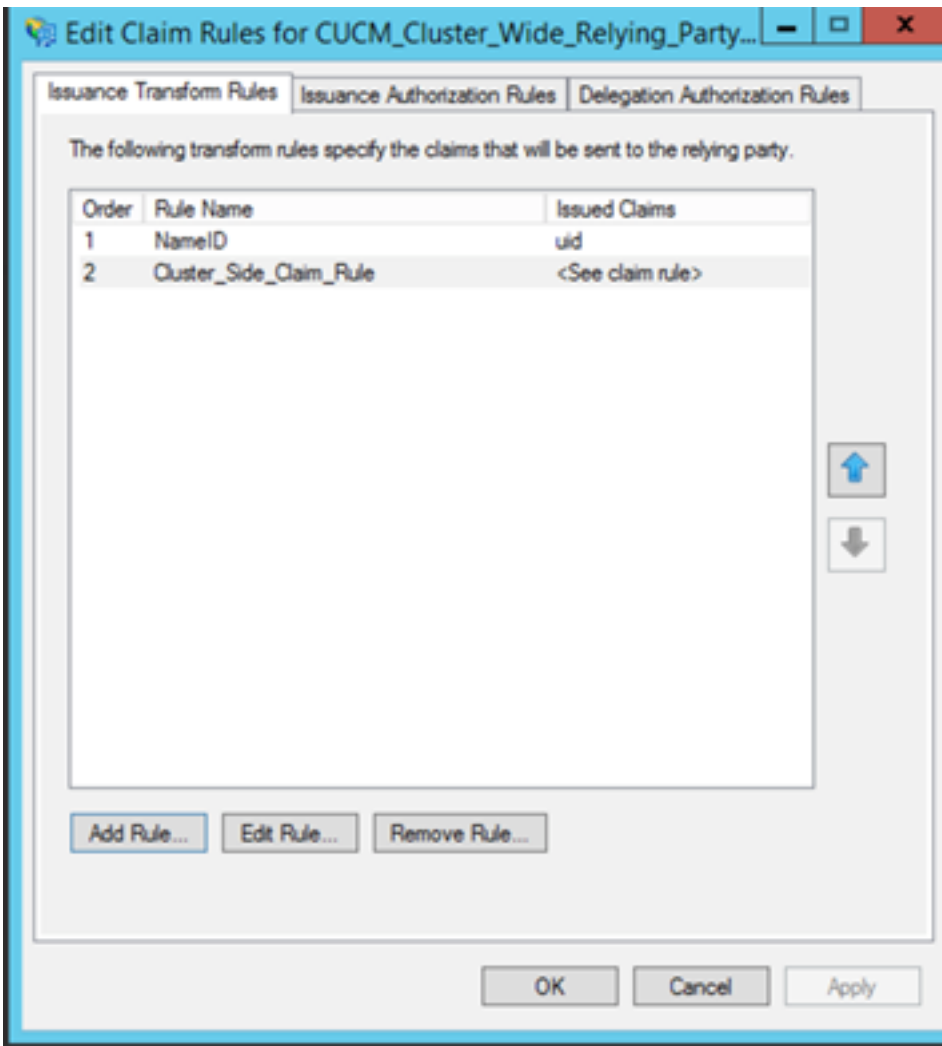
```
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]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

```
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://AD.fhlab.com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"cmpubhsc.fhlab.com");
```

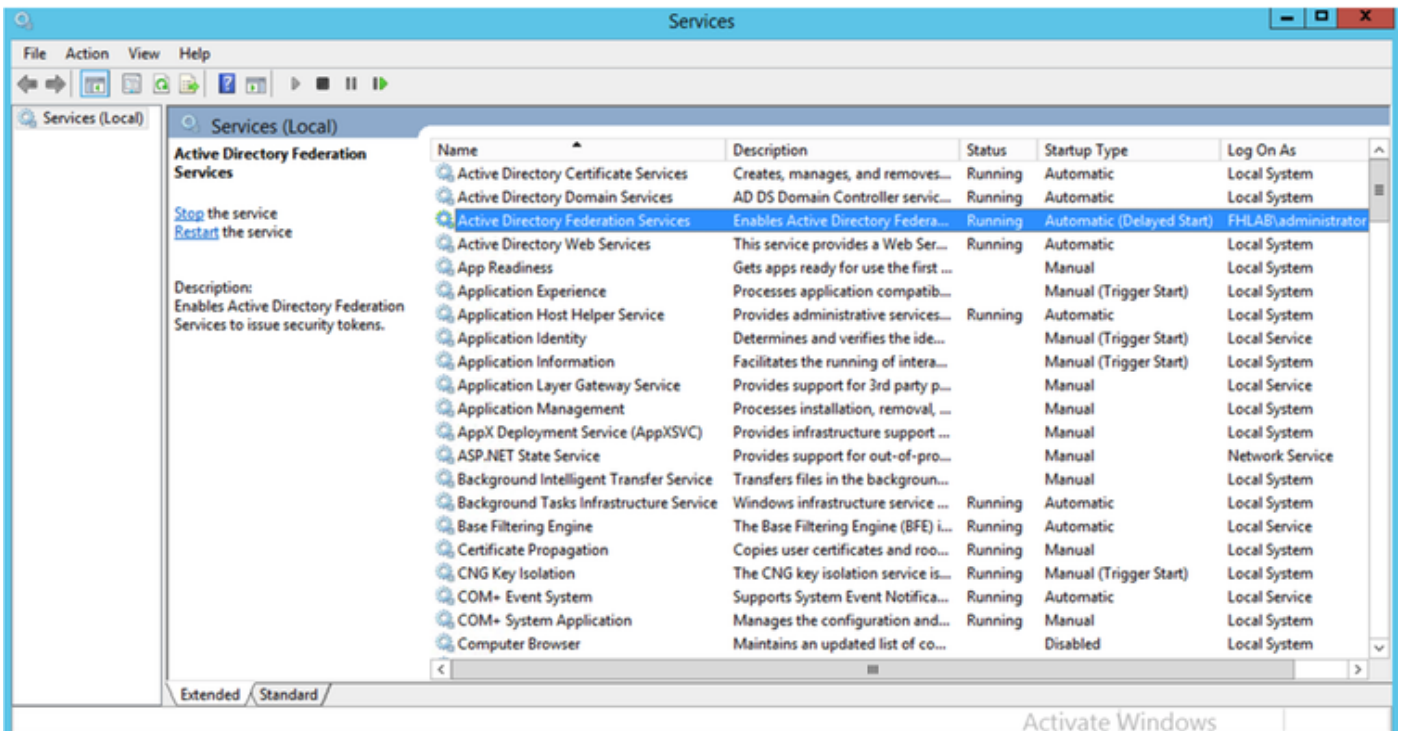
Finish를 클릭하여 계속합니다.



이제 ADFS에 두 개의 규칙이 정의되어야 합니다. Apply(적용) 및 OK(확인)를 클릭하여 규칙 창을 닫습니다.



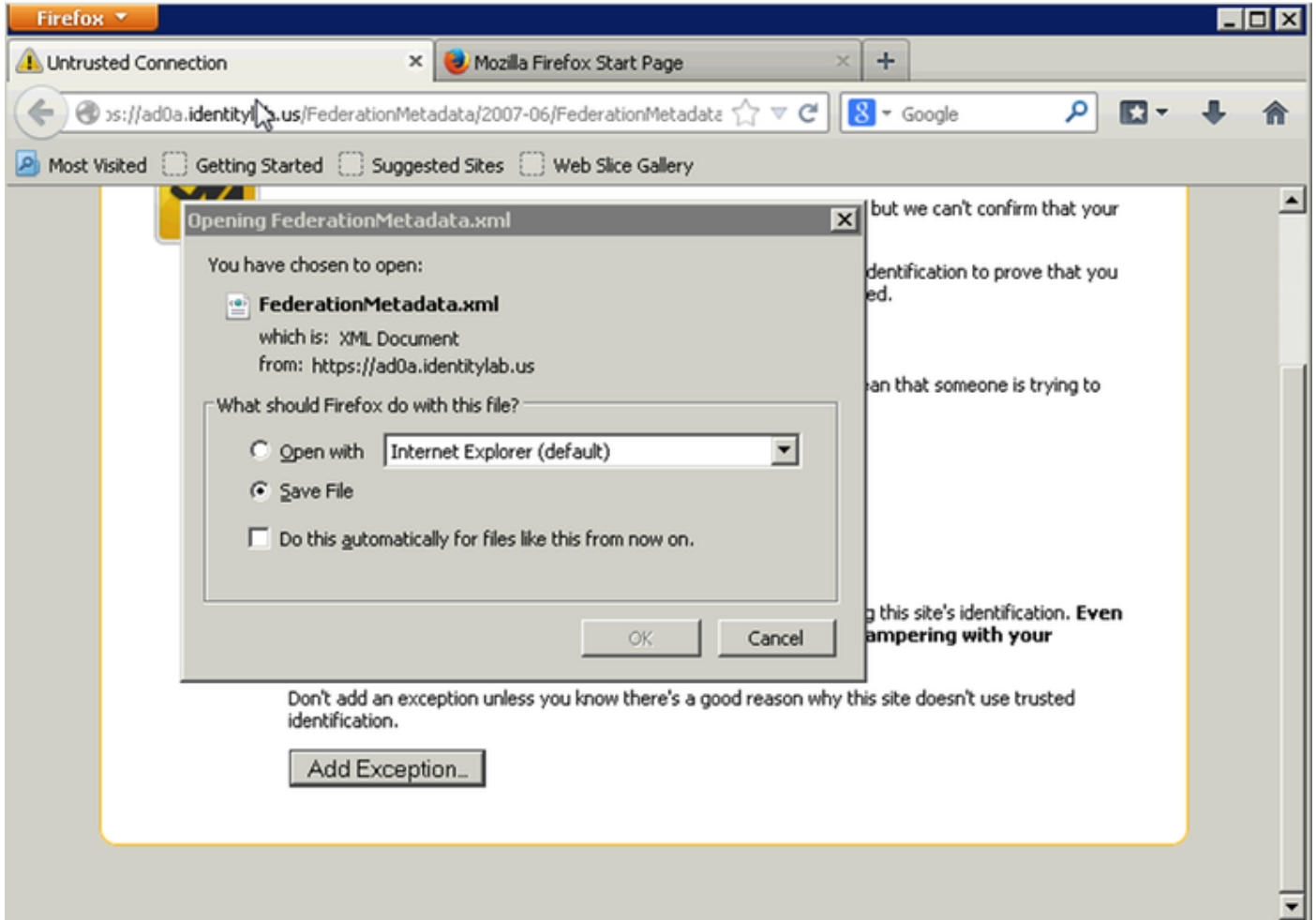
이제 CUCM이 ADFS에 신뢰할 수 있는 신뢰 당사자로 추가되었습니다.



계속하기 전에 ADFS 서비스를 다시 시작하십시오. 시작 메뉴 > 관리 도구 > 서비스로 이동합니다.

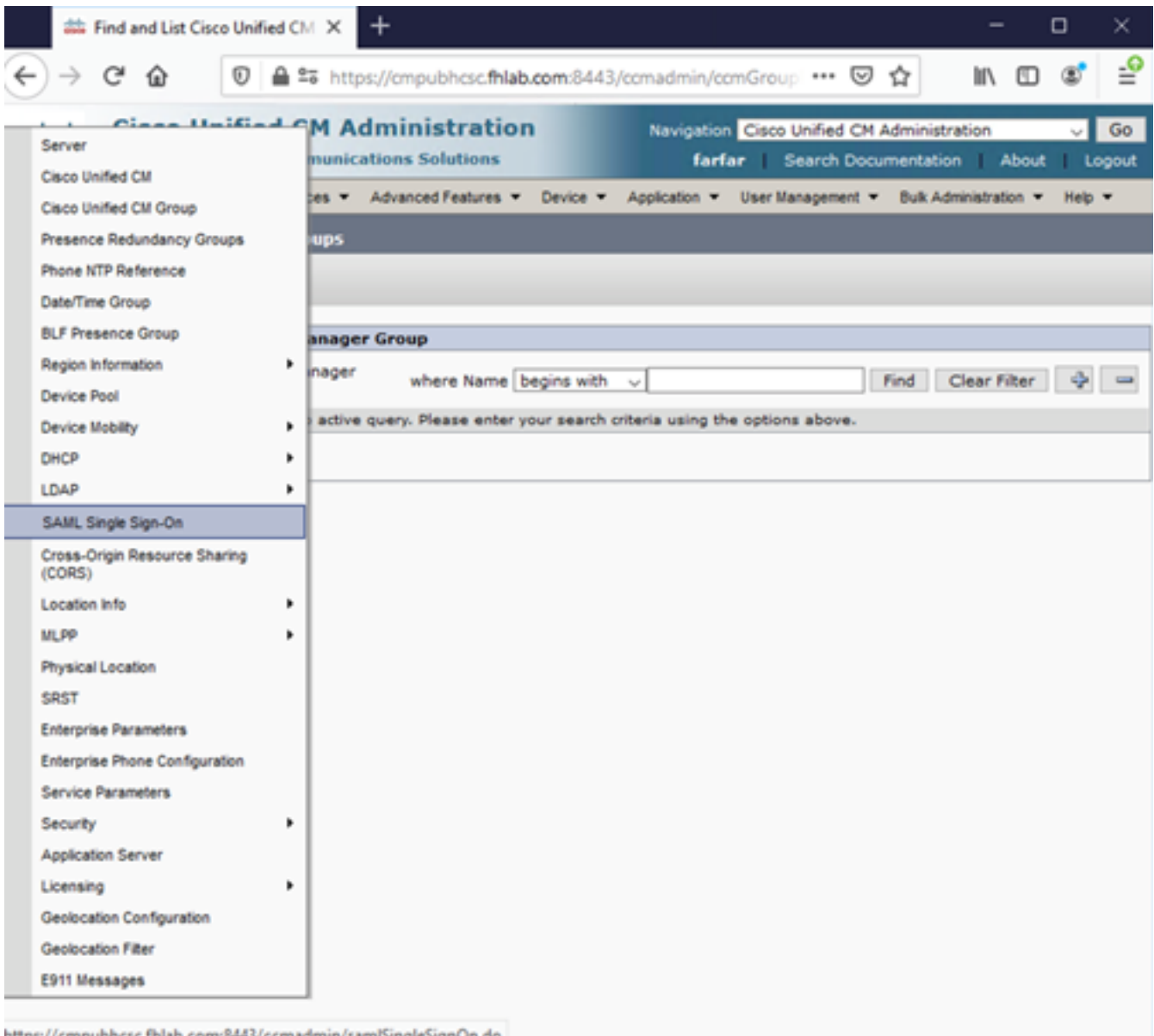
IDP 메타데이터

IdP에 대한 정보를 CUCM에 제공해야 합니다. 이 정보는 XML 메타데이터를 사용하여 교환됩니다. ADFS가 설치된 서버에서 이 단계를 수행해야 합니다.



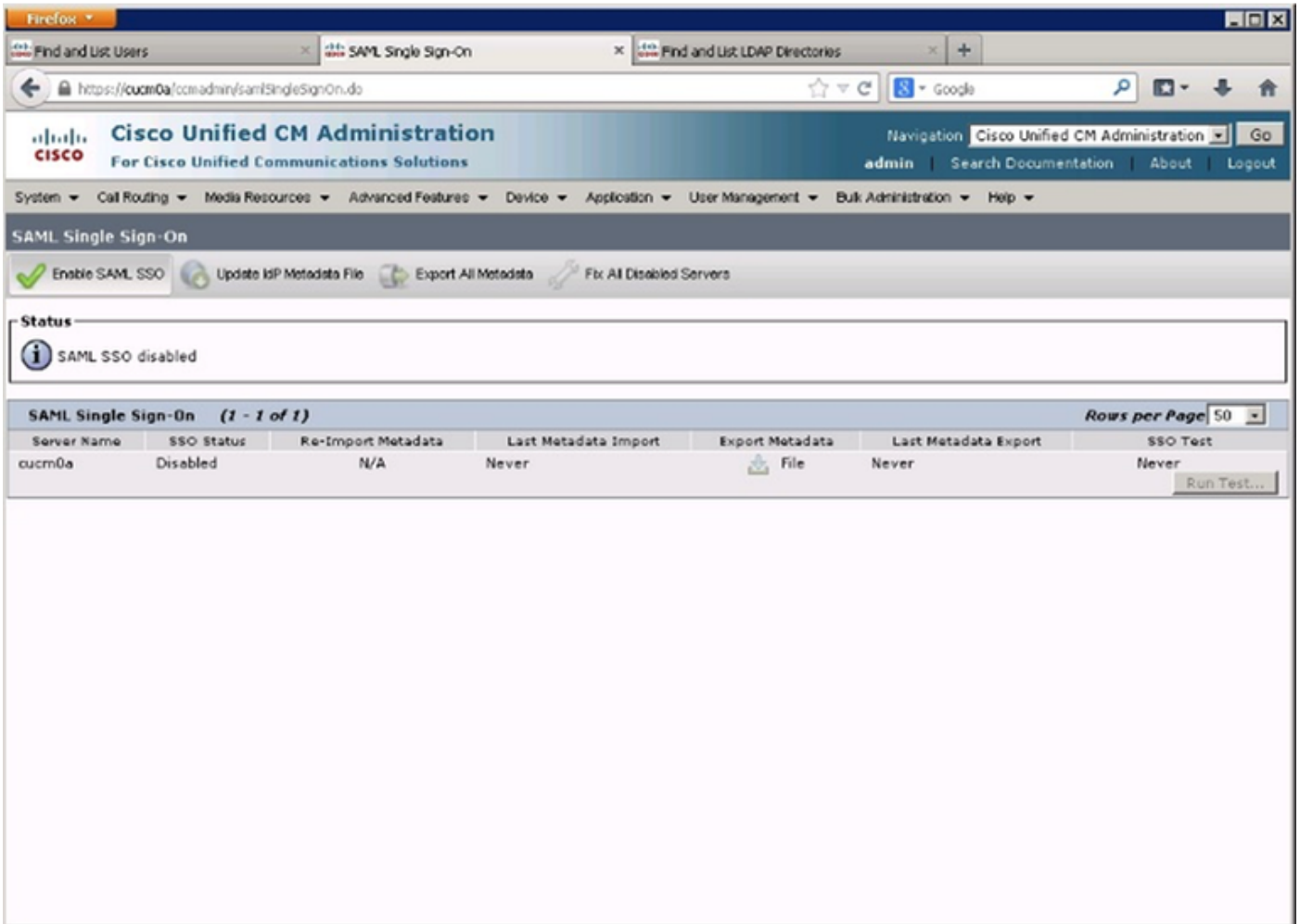
먼저 Firefox 브라우저를 사용하여 AD FS(IdP)에 연결하여 XML 메타데이터를 다운로드해야 합니다. <https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>으로 브라우저를 열고 메타데이터를 로컬 폴더에 저장합니다.

이제 CUCM 컨피그레이션으로 이동하여 Menu(시스템 메뉴) > SAML Single Sign-On 메뉴로 이동합니다.



<https://cmpublicsc.fhlab.com:8443/ccmadmin/samlSingleSignOn.do>

CUCM Administration(CUCM 관리)으로 돌아가 SYSTEM(시스템) > SAML Single Sign-On을 선택합니다.



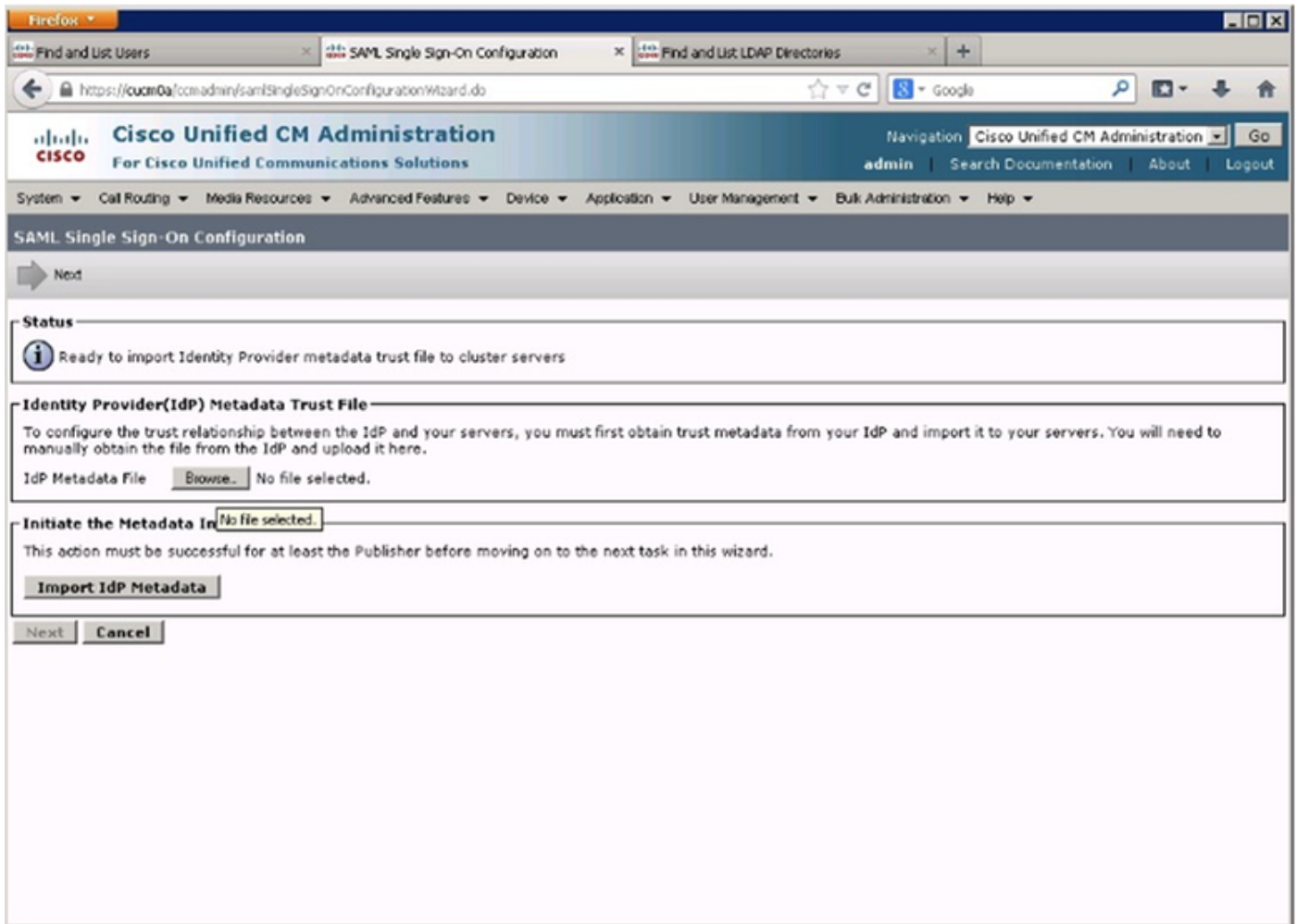
Enable SAML SSO(SAML SSO 활성화)를 선택합니다.

경고를 승인하려면 Continue(계속)를 클릭합니다.

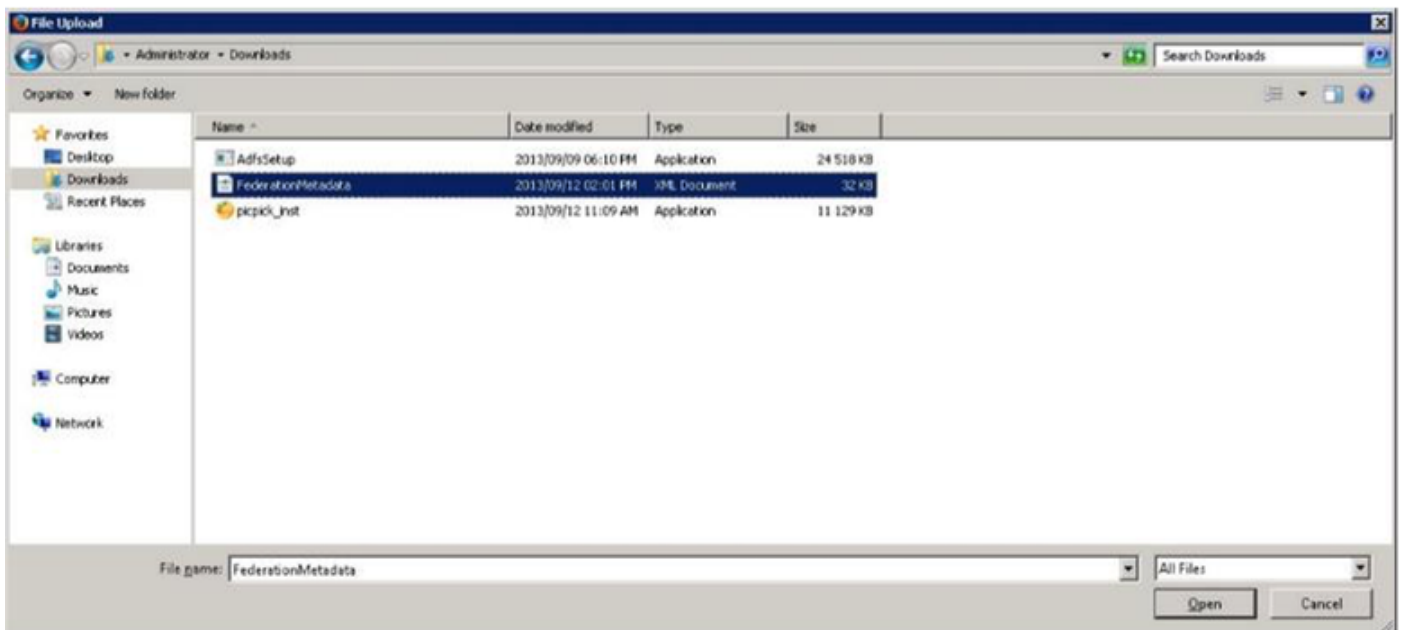


SSO 화면에서 **찾아보기..**를 클릭하여 이전에 저장한 FederationMetadata.xml 메타데이터 XML 파

일을 이미지에 표시된 대로 가져옵니다.



XML 파일을 선택하고 열기를 클릭하여 다운로드(Downloads) 아래의 즐겨찾기(Favorites)에서 CUCM에 업로드합니다.



업로드한 후 Import IdP Metadata(IdP 메타데이터 가져오기)를 클릭하여 IdP 정보를 CUCM으로 가져옵니다. 가져오기에 성공했는지 확인하고 Next(다음)를 클릭하여 계속합니다.

SAML Single Sign-On Configuration - Windows Internet Explorer

Navigation Cisco Unified CM Administration Go

admin | Search Documentation | About | Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

SAML Single Sign-On Configuration

Next

Status

✓ Import succeeded for all servers

Identity Provider(IdP) Metadata Trust File

To configure the trust relationship between the IdP and your servers, you must first obtain trust metadata from your IdP and import it to your servers. You will need to manually obtain the file from the IdP and upload it here.

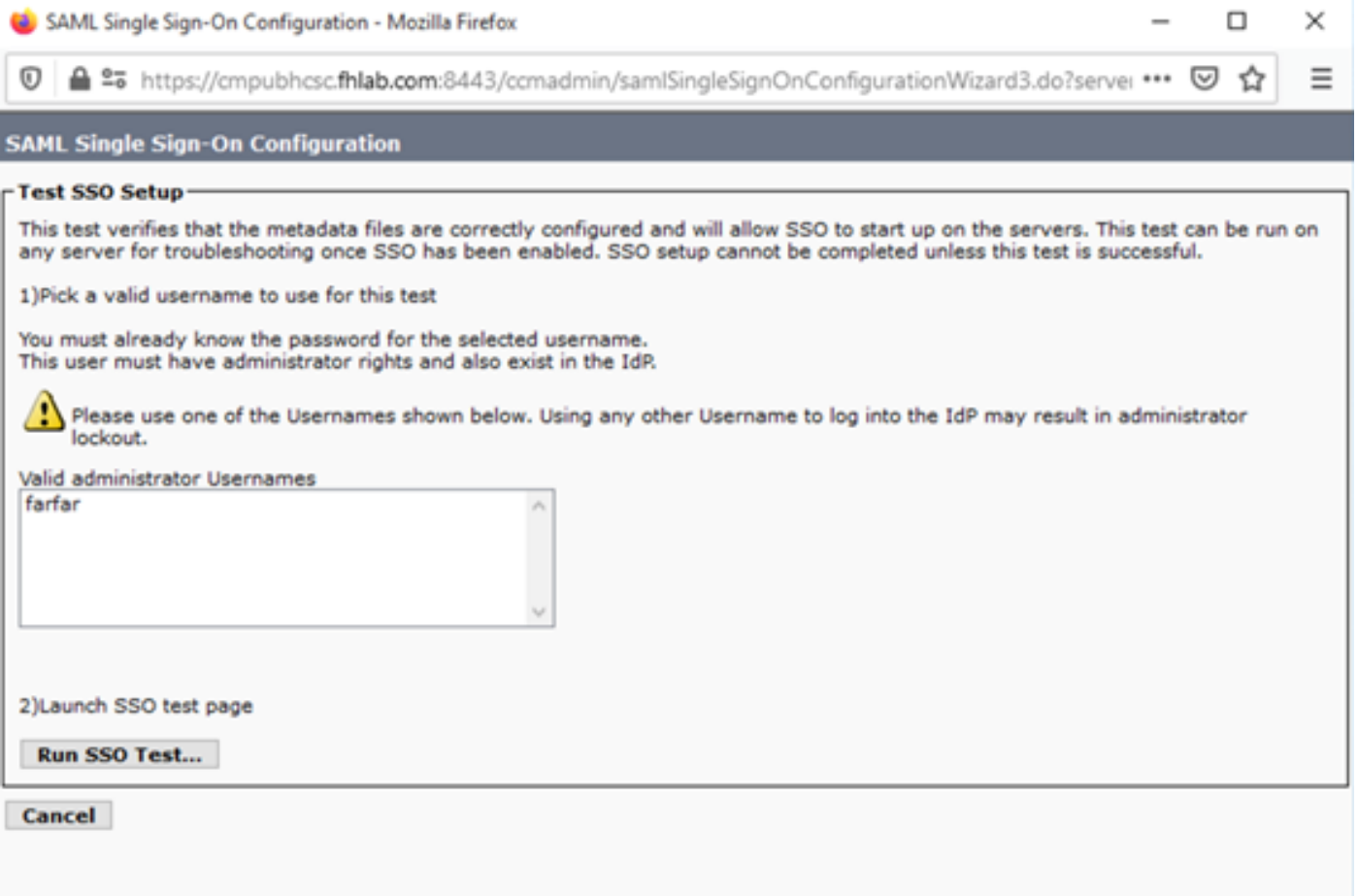
IdP Metadata File Browse...

Initiate the Metadata Import

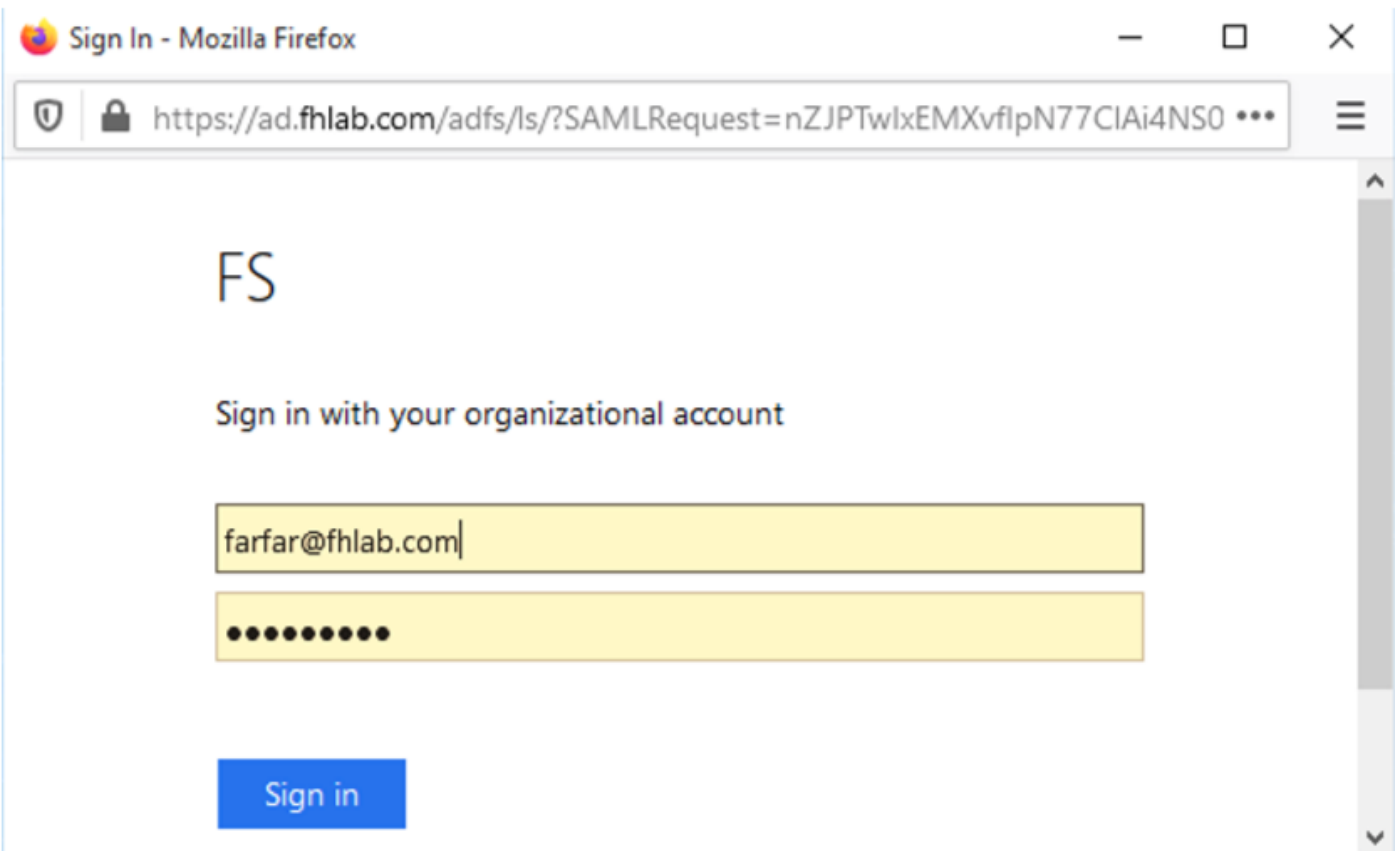
This action must be successful for at least the Publisher before moving on to the next task in this wizard.

✓ Import succeeded for all servers

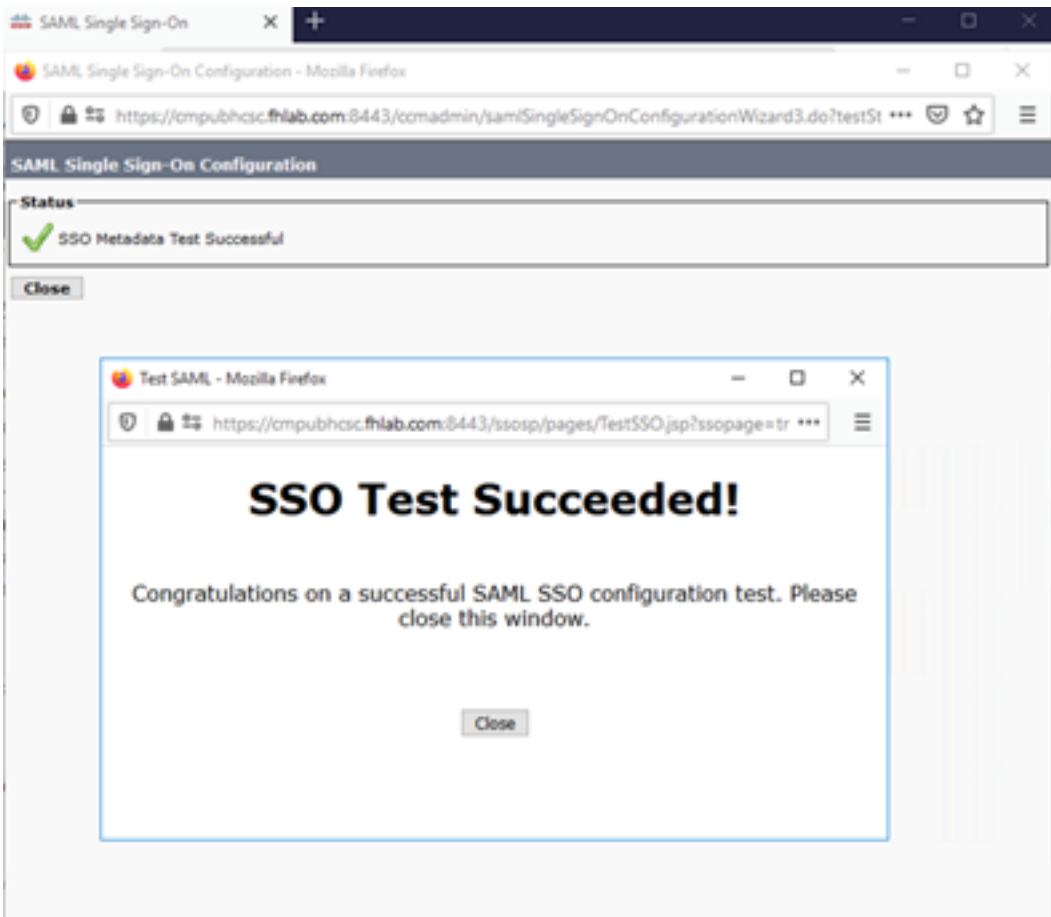
Standard CCM Super Users(표준 CCM 슈퍼 사용자)에 속하는 사용자를 선택하고 RUN SSO TEST(SSO 테스트 실행)를 클릭합니다.



사용자 인증 대화 상자가 표시되면 적절한 사용자 이름과 비밀번호를 사용하여 로그인합니다.



모든 것이 올바르게 구성된 경우 SSO Test Succeeded!(SSO 테스트 성공!)라는 메시지가 표시됩니다.



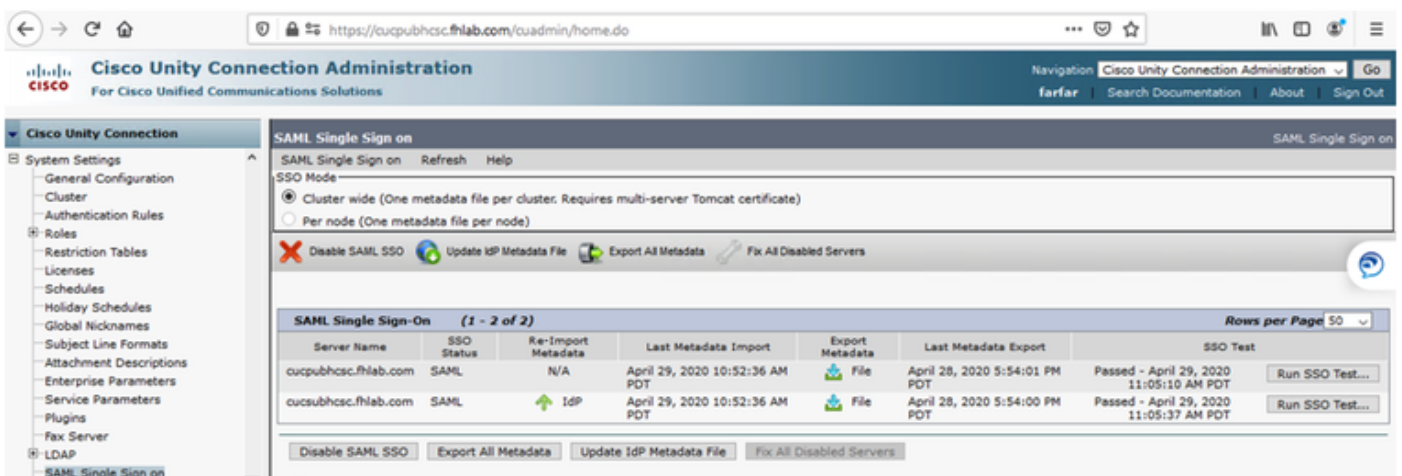
CLOSE(닫기) 및 FINISH(마침)를 클릭하여 계속합니다.

이제 ADFS를 사용하여 CUCM에서 SSO를 활성화하는 기본 컨피그레이션 작업을 완료했습니다.

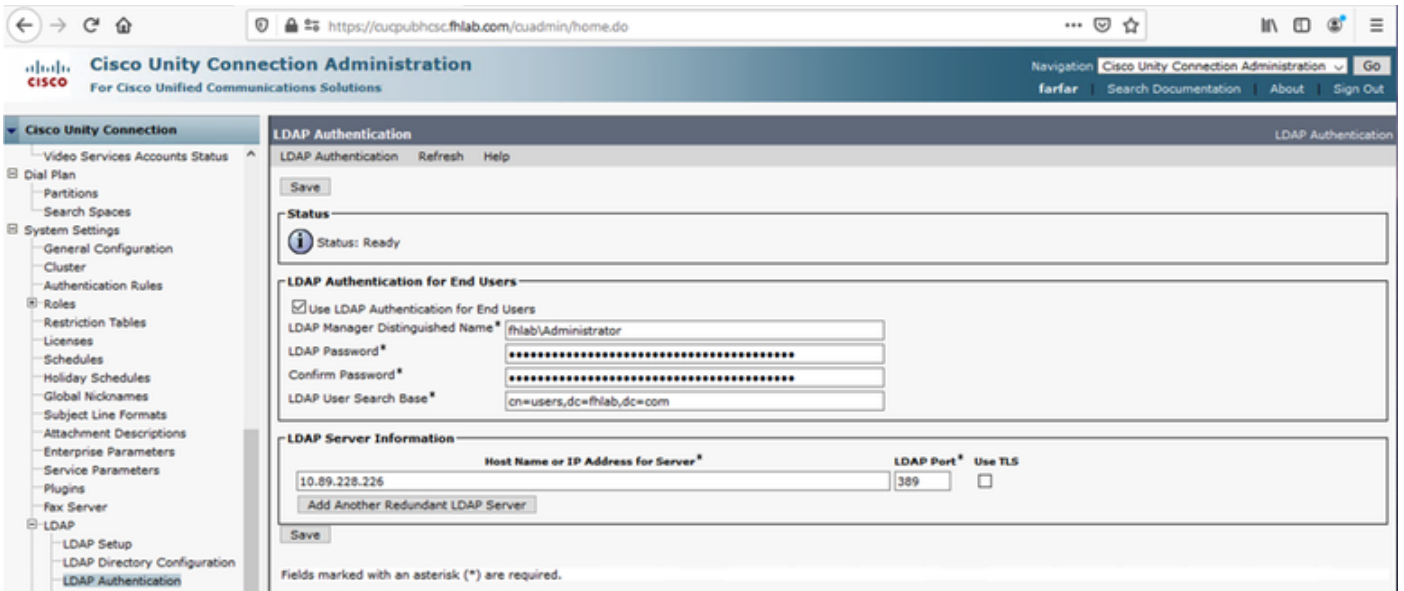
CUC에서 SSO 구성

Unity Connection에서 SSO를 활성화하려면 동일한 프로세스를 따를 수 있습니다.

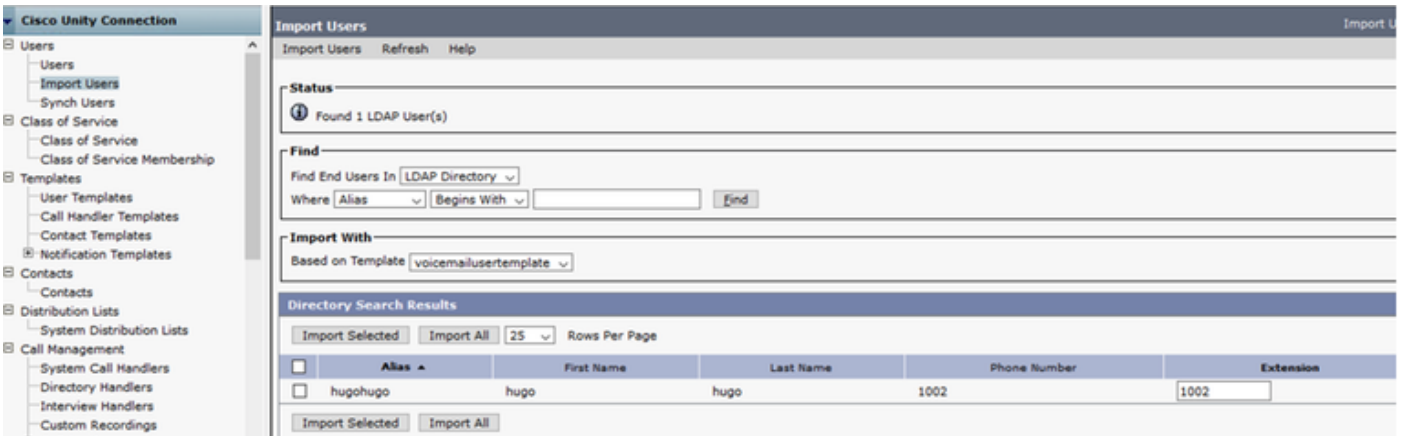
CUC와 LDAP 통합



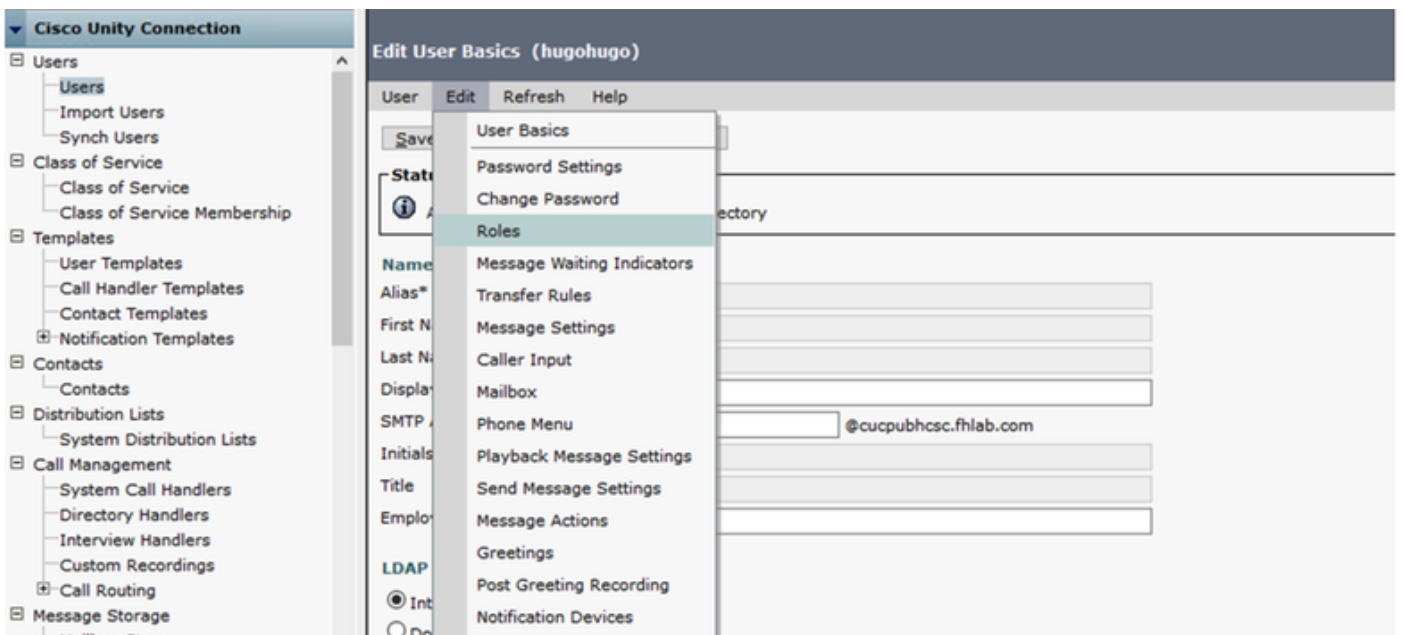
LDAP 인증을 구성합니다.



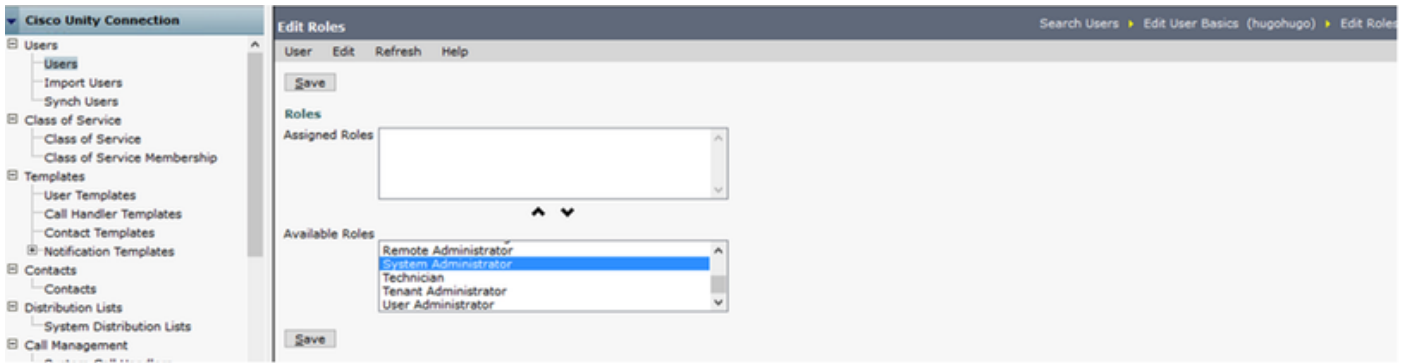
음성 메일이 할당될 LDAP에서 사용자 및 SSO 테스트를 위해 서비스될 사용자를 가져옵니다.



이미지에 표시된 대로 Users(사용자) > Edit(편집) > Roles(역할)로 이동합니다.

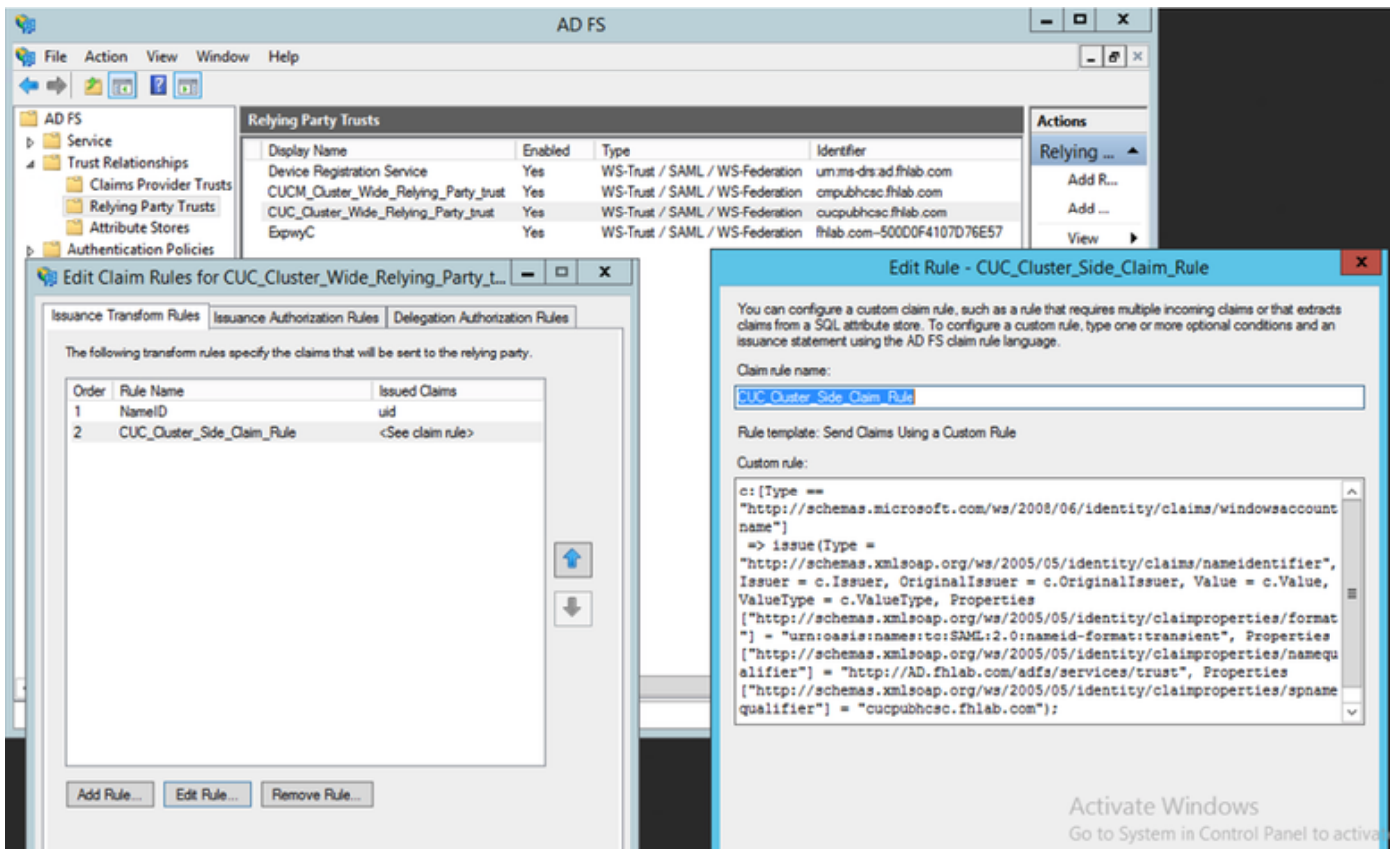


테스트 사용자에게 시스템 관리자의 역할을 할당합니다.

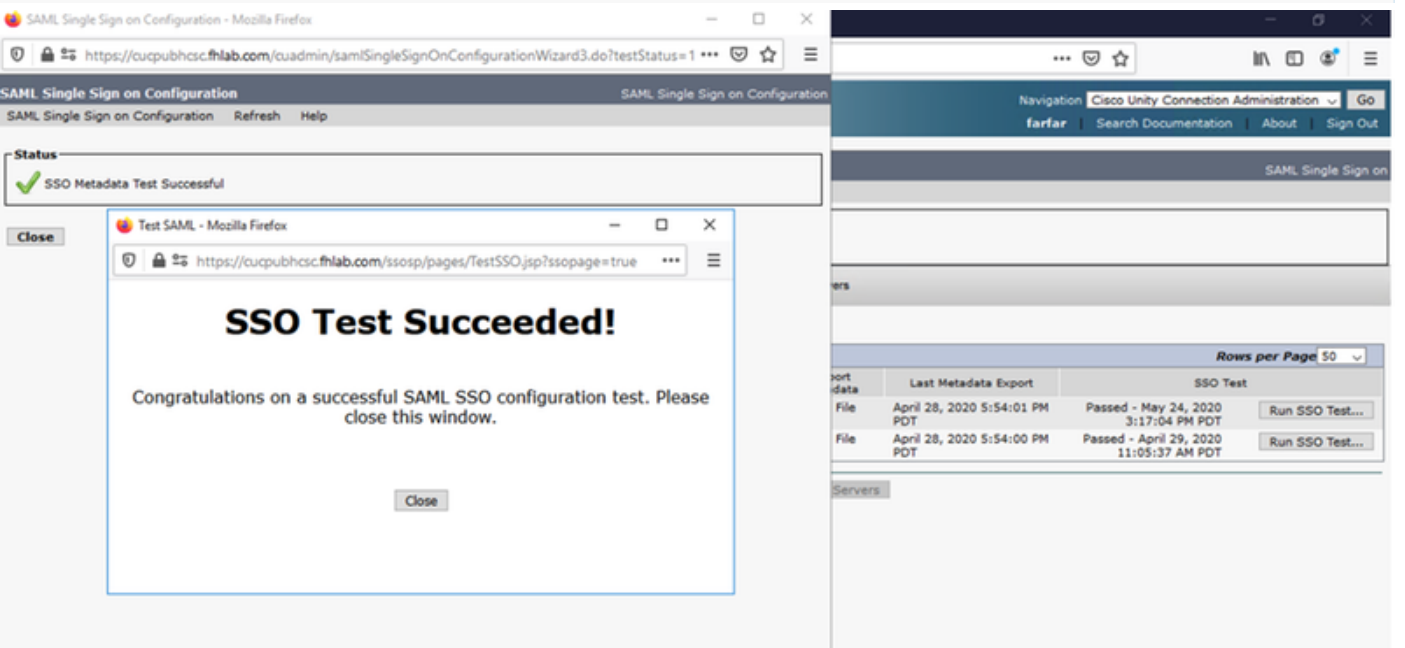
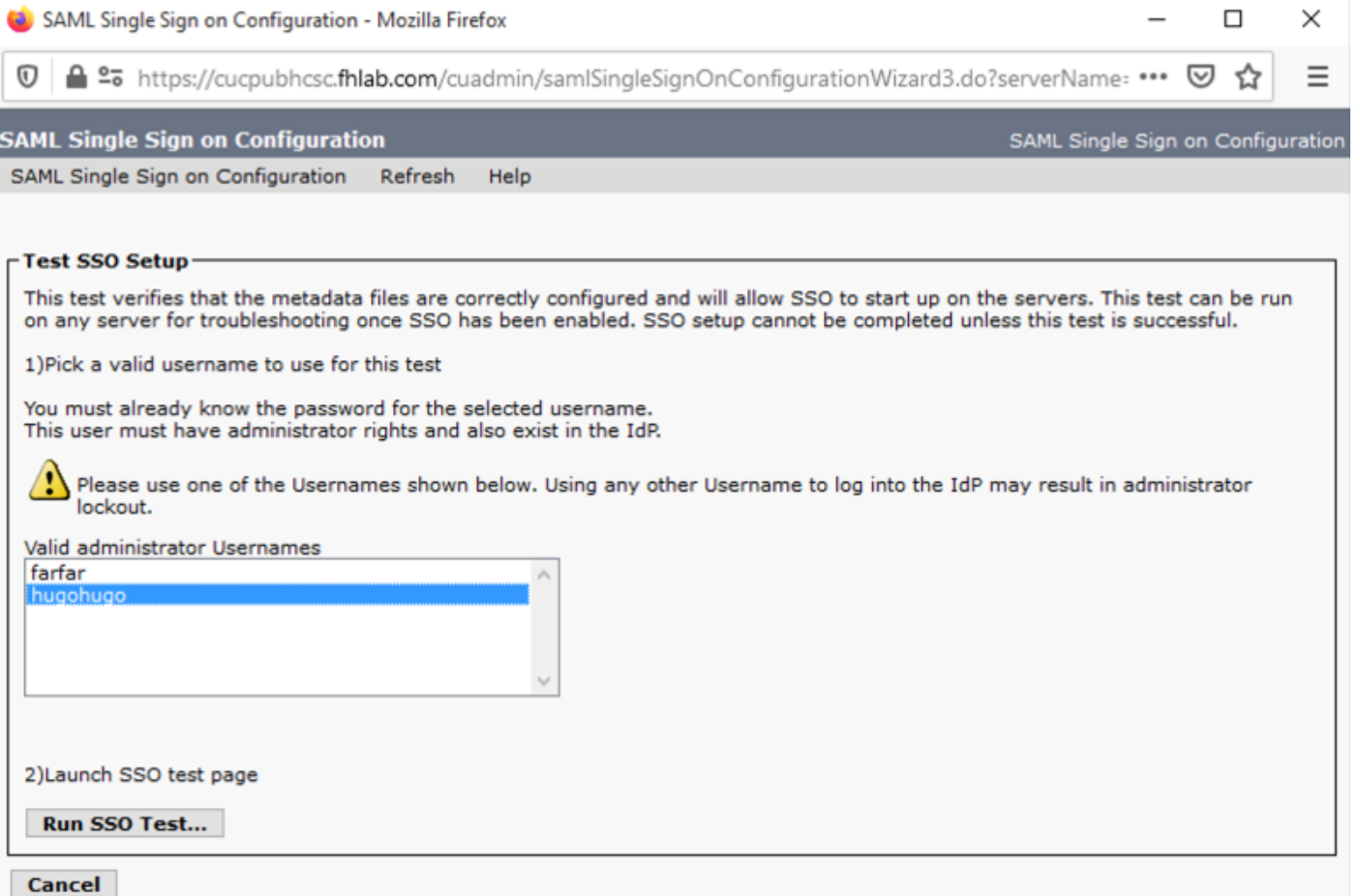


CUC 메타데이터

이제 CUC 메타데이터를 다운로드하고, CUC에 대해 RelyingPartyTrust를 생성하고, CUC 메타데이터를 업로드하고, ADFS 3.0에서 AD FS에서 규칙을 생성했어야 합니다.



SAML Single Sign-On으로 이동하고 Enable SAML SSO로 이동합니다.



Expressway에서 SSO 구성

Expressway C로 메타데이터 가져오기

https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml으로 브라우저를 열고 메타데이터를 로컬 폴더에 저장합니다.

Configuration(컨피그레이션) > Unified Communications > IDP에 업로드합니다.

Expressway C에서 메타데이터 내보내기

configuration(컨피그레이션) -> Unified Communications -> IDP -> Export SAML Data(SAML 데이터 내보내기)로 이동합니다.

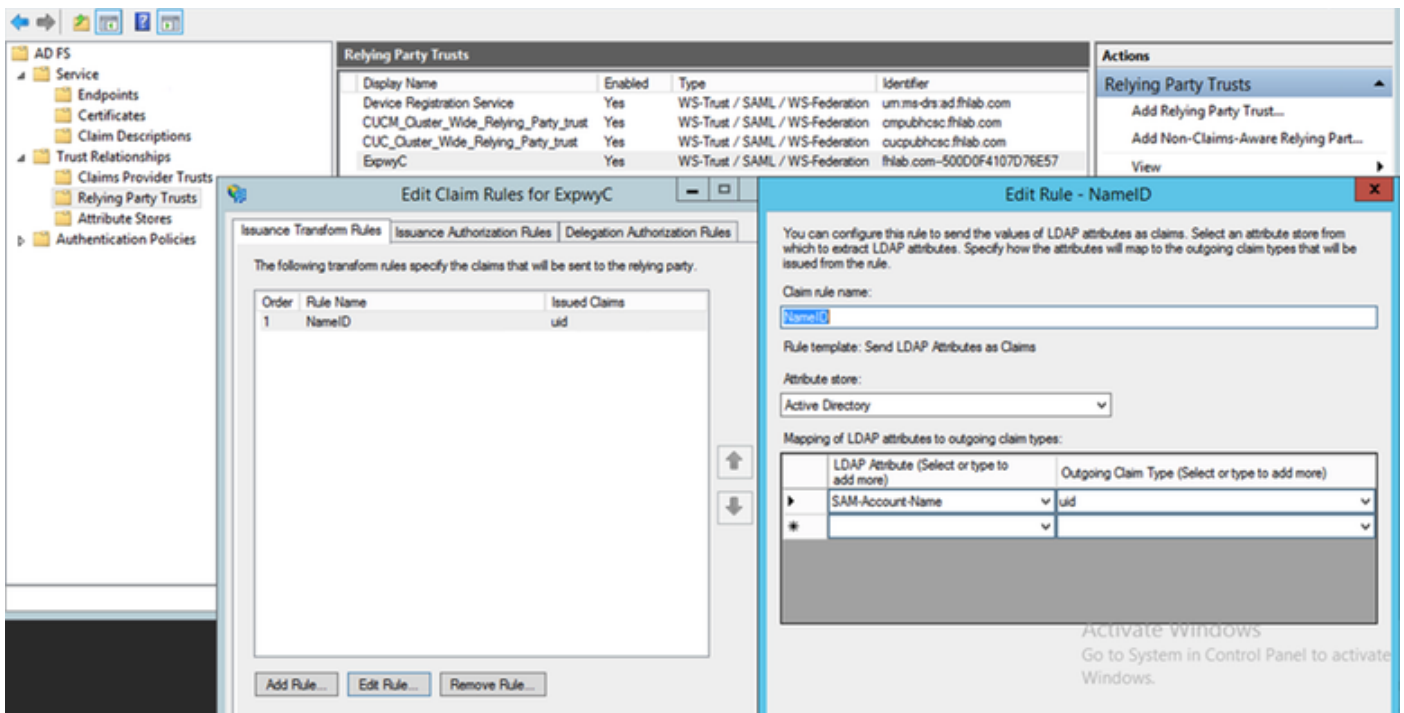
클러스터 모드에서는 SAML에 포함된 자체 서명 인증서(수명이 긴 인증서)를 사용합니다.

메타데이터 및 SAML 요청 서명에 사용

- 클러스터 전체 모드에서 단일 클러스터 전체 메타데이터 파일을 다운로드하려면 Download(다운로드)를 클릭합니다.
- 피어별 모드에서 개별 피어에 대한 메타데이터 파일을 다운로드하려면 피어 옆에 있는 Download를 클릭합니다..zip 파일로 모두 내보내려면 Download All을 클릭합니다.

Cisco Expressway-E에 대한 당사자 Trust 추가

먼저 Expressway-Es에 대한 당사자 트러스트를 만든 다음 ID를 UID 특성으로 보낼 클레임 규칙을 추가합니다.

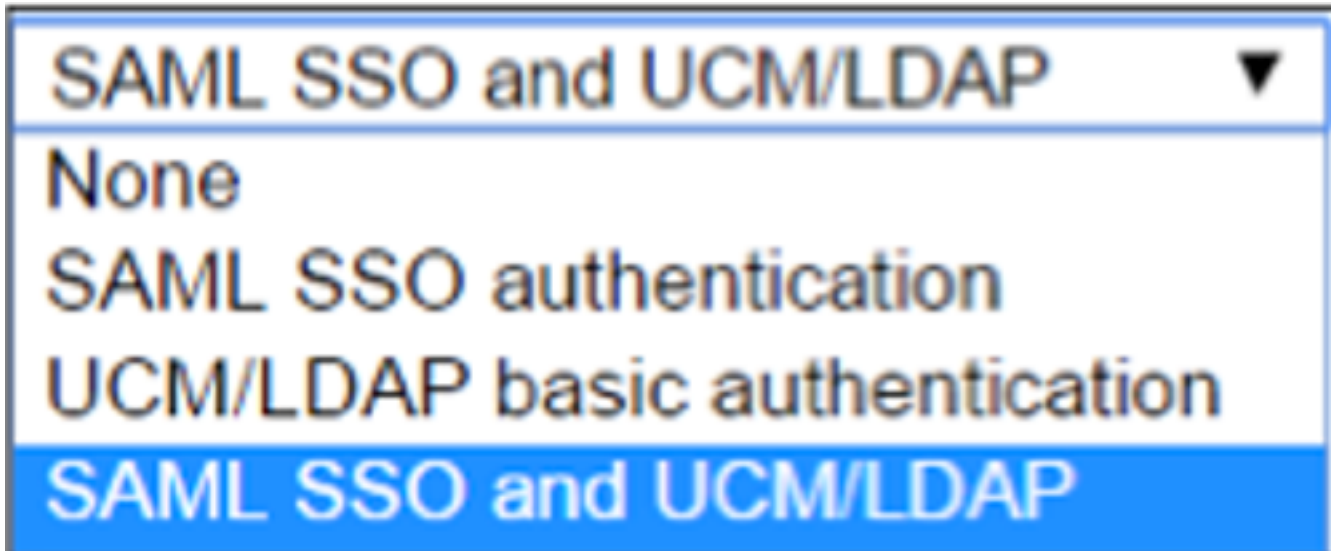


새로 고침 로그인에 있는 OAuth

Cisco CUCM Enterprise Parameters(Cisco CUCM 엔터프라이즈 매개변수)에서 Refresh(새로 고침) 로그인 플로우 매개변수가 활성화된 OAuth를 확인합니다.Cisco Unified CM Administration(Cisco Unified CM 관리) > Enterprise Parameters(엔터프라이즈 매개변수) > SSO 및 OAuth Configuration(SSO 및 OAuth 컨피그레이션)으로 이동합니다.

SSO and OAuth Configuration		
OAuth Token Expiry Timer (minutes) *	60	60
OAuth Refresh Token Expiry Timer (days) *	60	60
Redirect URIs for Third Party SSO Client		
SSO Login Behavior for iOS *	Use embedded browser (WebView)	Use embedded browser (WebView)
OAuth with Refresh Login Flow *	Enabled	Disabled
Use SSO for RTMT *	True	True

인증 경로



- 인증 경로가 "SAML SSO 인증"으로 설정된 경우 SSO가 활성화된 Unified CM 클러스터를 사용하는 Jabber 클라이언트만 이 Expressway에서 MRA를 사용할 수 있습니다. 이는 SSO 전용 컨피그레이션입니다.
- 모든 IP 전화, 모든 TelePresence 엔드포인트 및 SSO에 대해 구성되지 않은 Unified CM 클러스터에 속한 Jabber 클라이언트에 대한 Expressway MRA를 지원하려면 인증 경로가 UCM/LDAP 인증을 포함해야 합니다.
- 하나 이상의 Unified CM 클러스터가 Jabber SSO를 지원하는 경우 "SAML SSO 및 UCM/LDAP"를 선택하여 SSO 및 기본 인증을 모두 허용합니다.

SSO 아키텍처

SAML은 XML 기반 개방형 표준 데이터 형식으로서 관리자가 정의된 Cisco 협업 애플리케이션 세트에 로그인한 후 해당 애플리케이션 중 하나에 원활하게 액세스할 수 있도록 합니다. SAML SSO는 SAML 2.0 프로토콜을 사용하여 Cisco 협업 솔루션에 대해 도메인 간 및 제품 간 Single Sign-On을 제공합니다.

온프레미스 로그인 흐름

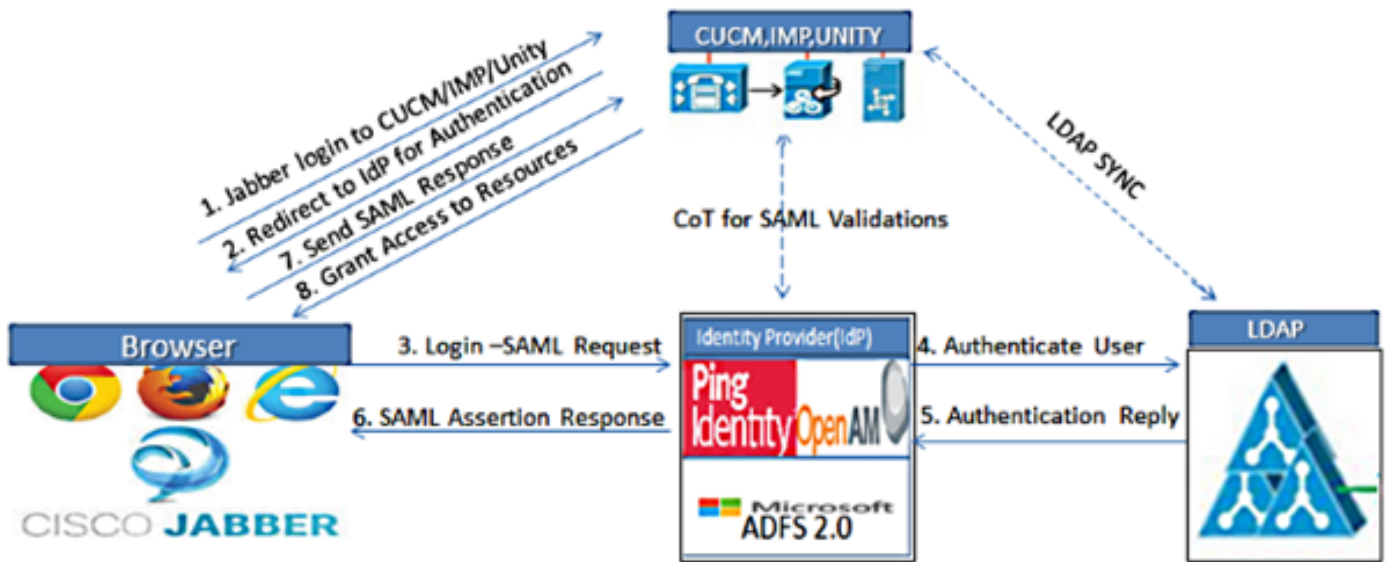
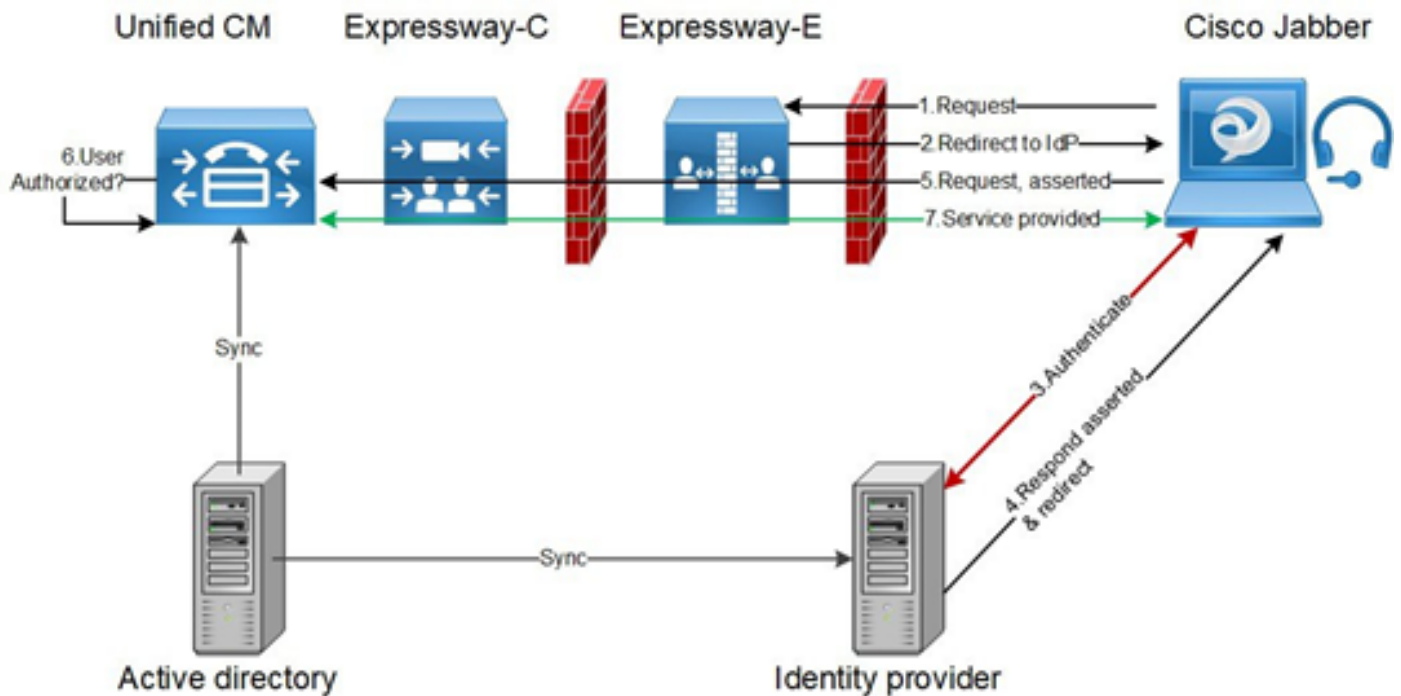


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

MRA 로그인 흐름



OAuth

OAuth는 권한 부여를 지원하는 표준입니다. 사용자를 인증하려면 먼저 사용자를 인증해야 합니다. 권한 부여 코드 부여 흐름은 클라이언트가 리소스에 액세스하기 위해 토큰을 가져오고 새로 고치는 방법(Unified CM, IM&P, Unity 및 Expressway 서비스)을 제공합니다. 이 흐름은 리디렉션을 기반으로 하므로 클라이언트가 사용자가 제어하는 HTTP 사용자 에이전트(웹 브라우저)와 상호 작용할 수 있어야 합니다. 클라이언트는 HTTPS를 사용하여 권한 부여 서버에 초기 요청을 합니다. OAuth 서버는 사용자를 인증 서비스로 리디렉션합니다. SAML SSO가 활성화된 경우 Unified CM 또는 외부 IdP에서 실행될 수 있습니다. 사용 중인 인증 방법에 따라 최종 사용자에게 웹 페이지 보기가 나타나 자신을 인증할 수 있습니다.(Kerberos 인증은 웹 페이지를 표시하지 않는 예입니다.) 암시적 부여 흐름과 달리, 성공적인 인증 코드 부여 프로우는 OAuth 서버에서 웹 브라우저에

"Authorization Code"를 발급하게 됩니다. 이 코드는 일회성 단기간 고유 코드로, 웹 브라우저에서 클라이언트로 다시 전달됩니다. 클라이언트는 이 "권한 부여 코드"를 사전 공유 암호와 함께 권한 부여 서버에 제공하고, Exchange에서 "액세스 토큰" 및 "토큰 새로 고침"을 수신합니다. 이 단계에서 사용된 클라이언트 암호는 권한 부여 서비스에서 등록 및 인증된 클라이언트만 사용하도록 제한할 수 있습니다. 토큰은 다음과 같은 용도로 사용됩니다.

토큰 액세스/새로 고침

액세스 토큰: 이 토큰은 권한 부여 서버에서 발급됩니다. 클라이언트는 해당 서버의 보호된 리소스에 액세스해야 할 때 리소스 서버에 토큰을 제공합니다. 리소스 서버에서 토큰을 확인하고 토큰을 사용하여 연결을 신뢰할 수 있습니다. (Cisco 액세스 토큰은 기본적으로 수명 60분으로 설정)

토큰 새로 고침: 이 토큰은 권한 부여 서버에서 다시 발급됩니다. 클라이언트는 액세스 토큰이 만료되었거나 만료될 때 클라이언트 암호와 함께 이 토큰을 권한 부여 서버에 제공합니다. 새로 고침 토큰이 여전히 유효한 경우 권한 부여 서버는 다른 인증 없이 새 액세스 토큰을 발급합니다. (Cisco Refresh 토큰은 기본적으로 60일의 수명을 갖습니다.) 새로 고침 토큰이 만료된 경우 새 토큰을 얻으려면 새 전체 OAuth 권한 부여 코드 부여 흐름을 시작해야 합니다.

OAuth 권한 부여 코드 권한 부여 플로우가 더 좋음

암시적 부여 흐름에서 액세스 토큰은 HTTP 사용자 에이전트(브라우저)를 통해 Jabber 클라이언트에 전달됩니다. 권한 부여 코드 부여 흐름에서 액세스 토큰은 권한 부여 서버와 Jabber 클라이언트 간에 직접 교환됩니다. 시간 제한 고유 권한 부여 코드를 사용하여 권한 부여 서버에서 토큰을 요청합니다. 액세스 토큰의 직접 교환은 더 안전하며 위험 노출을 줄입니다.

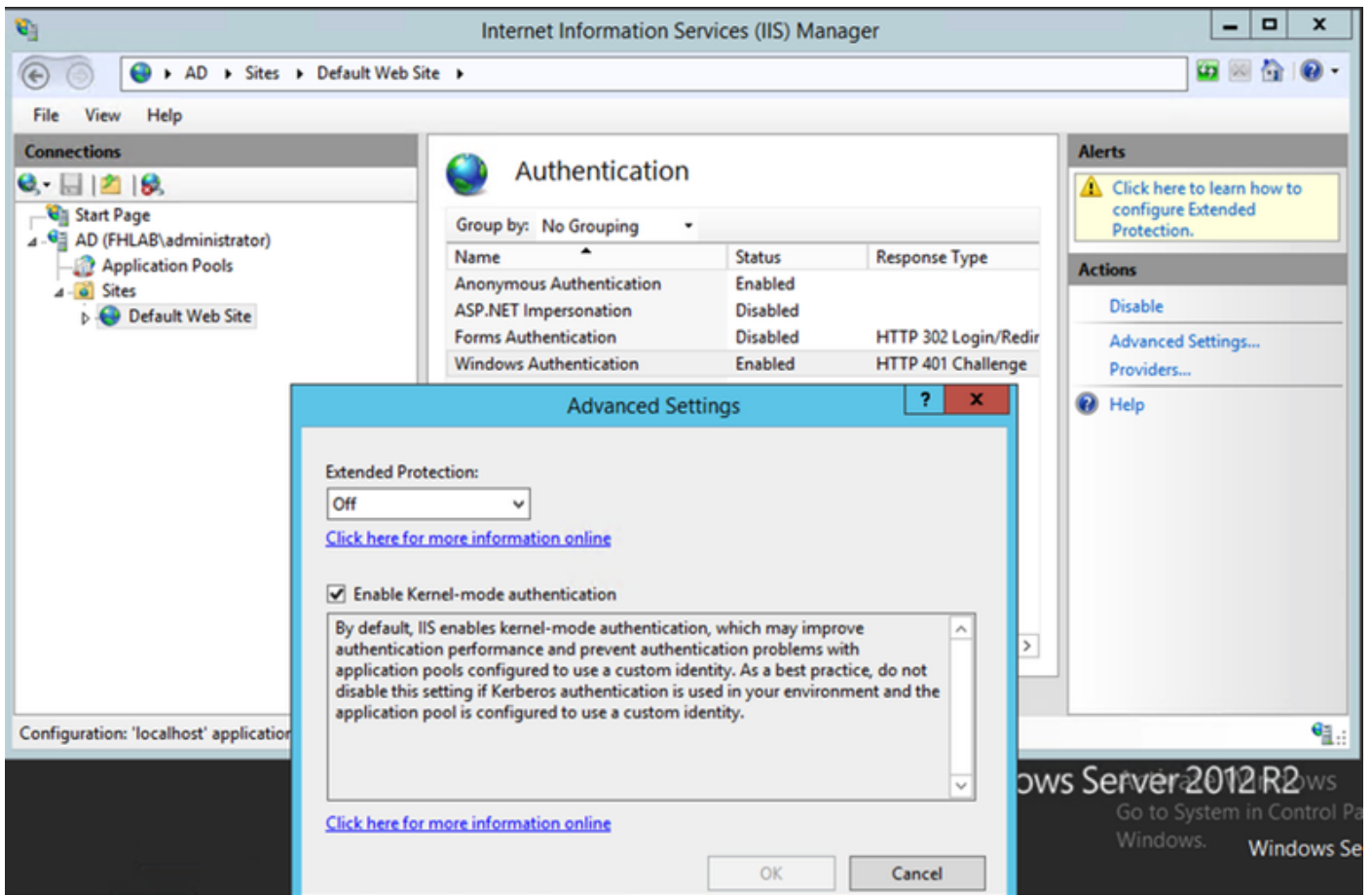
OAuth 권한 부여 코드 권한 부여 흐름은 새로 고침 토큰 사용을 지원합니다. 따라서 최종 사용자는 자주 재인증할 필요가 없으므로(기본적으로 60일) 더 나은 환경을 제공할 수 있습니다.

Kerberos 구성

Windows 인증 선택

IIS(인터넷 정보 서비스) 관리자 > 사이트 > 기본 웹 사이트 > 인증 > Windows 인증 > 고급 설정.

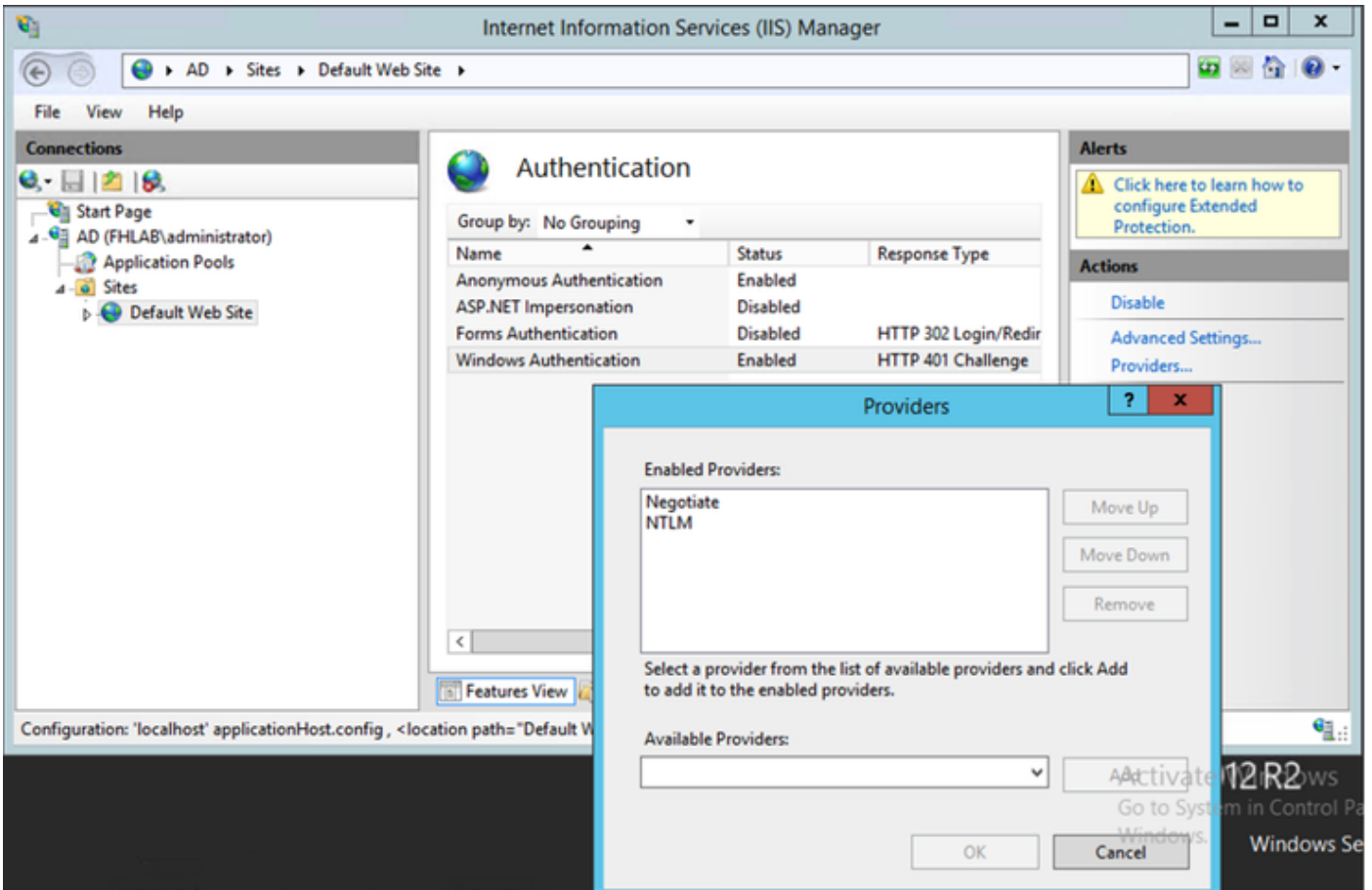
1. Enable Kernel-mode authentication(커널 모드 인증 활성화)을 선택 취소합니다.
2. 확장된 보호가 해제되어 있는지 확인합니다.



ADFS는 Kerberos NTLM을 모두 지원합니다.

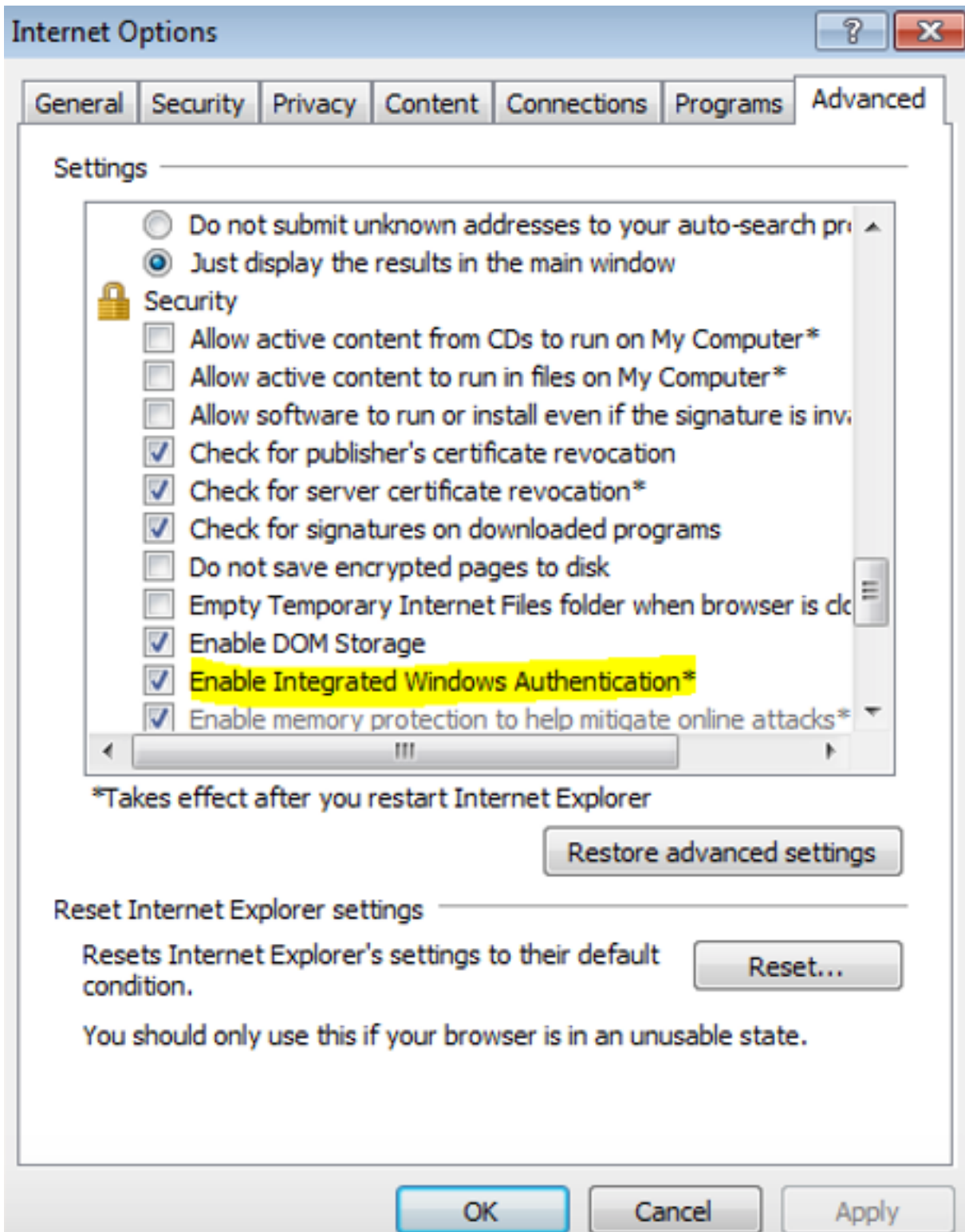
모든 비 Windows 클라이언트는 Kerberos를 사용할 수 없고 NTLM을 사용할 수 없으므로 AD FS 버전 3.0이 Kerberos 프로토콜과 NTLM(NT LAN Manager) 프로토콜을 모두 지원하는지 확인하십시오.

오른쪽 창에서 Providers(공급자)를 선택하고 Enabled Providers(활성화된 공급자) 아래에 Negotiate(협상) 및 NTLM이 있는지 확인합니다.



Microsoft Internet Explorer 구성

Internet Explorer > Advanced > Enable Integrated Windows Authentication(통합 Windows 인증 활성화)이 선택되어 있는지 확인합니다.



Security(보안) > Intranet zones(인트라넷 영역) > Sites(사이트)에서 ADFS URL 추가

