ADFS 3.0을 사용하여 Cisco Unified Communications Manager에서 SAML SSO 구성

목차

<u>소</u>개 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 로그인이 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 <u>NTLM을 모두 지원합니다.</u> 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)

<u>IE에 추가하는 사이트</u> <u>동기화 중단 문제</u> <u>토큰 취소</u> <u>부트스트랩 파일</u> 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 디바 이스는 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 이 름으로 확인하는 DNS 레코드 유형).

A 레코드

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



포인터(PTR) 레코드

🍰 DNS	Name	Туре	Data	Timestamp
A D	(same as parent folder)	Start of Authority (SOA)	[14], ad.fhlab.com., hostmaster.fhlab.co	static
4 🎬 Forward Lookup Zones	(same as parent folder)	Name Server (NS)	ad.fhlab.com.	static
[] _msdcs.fhlab.com	10.89.228.144	Pointer (PTR)	expwyc.fhlab.com.	static
⊿ 🛐 fhlab.com	10.89.228.145	Pointer (PTR)	expwye.fhlab.com.	static
▷ [] _msdcs	10.89.228.146	Pointer (PTR)	cmpubhcsc.fhlab.com.	static
i _sites	10.89.228.147	Pointer (PTR)	cmsubhcsc.fhlab.com.	static
þ 🛄 _tcp	10.89.228.148	Pointer (PTR)	imppubhcsc.fhlab.com.	static
þ 🛄 _udp	10.89.228.150	Pointer (PTR)	impsubhcsc.fhlab.com.	static
DomainUnsZones	10.89.228.151	Pointer (PTR)	cucpubhcsc.fhlab.com.	static
A ForestUnsZones	10.89.228.153	Pointer (PTR)	cucsubhcsc.fhlab.com.	static
psites	10.89.228.154	Pointer (PTR)	win10.fhlab.com.	5/12/2020 10:00:00 AM
Reverse Lookup Zones	10.89.228.226	Pointer (PTR)	ad.fhlab.com.	5/12/2020 11:00:00 AM
228.89.10.in-addr.arp	10.89.228.227	Pointer (PTR)	win10ext.fhlab.com.	5/7/2020 4:00:00 PM

Jabber Discovery Services에 SRV 레코드가 있어야 함

â, DNS	Name	Type	Data		Timestamp	
A AD	_cisco-uds	Service Location (SRV)	[0][0][8443] cmsubhcsc.fhl	ab.com.	static	
a 🚞 Forward Lookup Zones	cisco-uds	Service Location (SRV)	[0][0][8443] cmpubhcsc.fhl	ab.com.	static	
[] _msdcs.fhlab.com	cuplogin	Service Location (SRV)	[0][0][8443] impsubhcsc.fh	lab.com.	static	
⊿ 👸 fhlab.com	cuplogin	Service Location (SRV)	[0][0][8443] imppubhcsc.fh	lab.com.	static	
D [] _msdcs	99	Service Location (SRV)	[0][100][3268] ad.fhlab.com	.	5/12/2020 10:00:00 AM	
bsites	kerberos	Service Location (SRV)	[0][100][88] ad.fhlab.com.		5/12/2020 10:00:00 AM	
tcp	kpasswd	Service Location (SRV)	[0][100][464] ad.fhlab.com.		5/12/2020 10:00:00 AM	
budp	Idap	Service Location (SRV)	[0][100][389] ad.fhlab.com			
DomainUnszones					_cisco-uds Properti	es 🦹 🔭
b Sites				Service Location	n (SRV) Security	
tcp					under a second	
a 🧾 Reverse Lookup Zones				Domain:	fhlab.com	
228.89.10.in-addr.arp						
Trust Points				Service:	_cisco-uds	~
Conditional Forwarders				Protocol:	top	~
Global Logs						
				Priority:	0	
				Weight:	0	
					0.440	
				Port number:	8443	
				Host offering th	his service:	
				cmpublicsc.fh	lab.com.	
	1					

• 루트 CA(인증서가 엔터프라이즈 CA 서명)

웹 서버 인증서 템플릿을 기반으로 인증서 템플릿을 만들어야 합니다. 이 템플릿은 복제되고 이름 이 변경되며, Extensions(확장) 탭에서 Application Policies(애플리케이션 정책)가 수정되어 클라이 언트 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.

Certificate Templates (AD.fhlab.	Template Display Name	Schem	Version Versi Int A Actions	
	CEP Encryption	1	Properties of New Template	 Ø
	ClientServerAuth	2		
	Code Signing	1	Subject Name Server Issuance Requirements	strative Tools P
	Computer 2	1	Compatibility General Request Handling Cryptography Key Atlestation	alization Delicion Extension
	Cross Certification Authority	2	Superseded Templates Extensions Security Edit Ap	oplication Policies Extension
	Directory Email Replication	2	To modify an extension, select it, and then click Edit. An applicat	tion policy defines how a certificate can be
	Domain Controller	1	used.	
	Domain Controller Authentication	2	Extensions included in this template:	
	EFS Recovery Agent	1	Application Policies Application	policies:
	Enrollment Agent	1	Basic Constraints Client Aut	hentication
	Enrollment Agent (Computer)	1	Certificate Template Information Server Au	thentication
	Exchange Enrollment Agent (Offline requ	1	Subscription States	
	Exchange Signature Only	1	Key Usage	
	Exchange User	1		
	@ IPSec	1		
	IPSec (Offline request)	1	Ede	
	Kerberos Authentication	2		
	Key Recovery Agent	2	Description of Application Policies:	Add Edit Remove
	OCSP Response Signing	3	Server Authentication	
	RAS and IAS Server	2	Client Authentication	is extension critical
	Root Certification Authority	1		

CSR에 서명할 수 있도록 생성된 템플릿을 발행해야 합니다.

File Action View Help		
🗢 🧼 🙋 🙆 👔		
E Certification Authority (Local)	Name	Intended Purpose
🔺 🛃 fhlab-AD-CA	ClientServerAuth	Server Authentication, Client Authentic
Revoked Certificates	Directory Email Replication	Directory Service Email Replication
Issued Certificates	Domain Controller Authentication	Client Authentication, Server Authentic
Pending Requests	Kerberos Authentication	Client Authentication, Server Authentic
Failed Requests	EFS Recovery Agent	File Recovery
Certificate Te Manag	ge	Encrypting File System
New	Certificate Template	to Issue ication

CA 인증서 웹에서 이전에 생성한 템플릿을 선택합니다.

Microsoft Active Directory Certificate Services -- fhlab-AD-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external sour Web server) in the Saved Request box.

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	8V8mW7/9kjhqfnpeBzAN++tol62BjnvqaT85tMM LA0dphF6LrurUeY2KLvMLmK1ft7aSy483yCsm0v1 OWGPZoLb3bS80ziW7fqEFWSaCq567DMOQ6Fk2t5N 10y/Ip6oDzTdE29w2p8rK3YxccbypovSt0ijIirh AV/Gjnz0 END CERTIFICATE REQUEST				
Certificate Templ	ate:				
Certificate Templ	ate:				
Certificate Templ	ato: ✓ User Basic EFS				
Certificate Templ	ate: ✓ User Basic EFS Administrator				
Certificate Templ	ate: ✓ User Basic EFS Administrator EFS Recovery Agent				
Certificate Templ	ate: ✓ User Basic EFS Administrator EFS Recovery Agent Web Server				
Certificate Templ Additional Attribu Attributes:	ate: V User Basic EFS Administrator EFS Recovery Agent Web Server Subordinate Certification Authority				

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

Generate Certificate Signing F	Request	
🔋 Generate 🖳 Close		
-		
-Status-		
Warning: Generating a r	new CSR for a specific certificate type will overwrite the exis	ting CSR for that type
- Generate Certificate Signing	g Request	
Certificate Purpose**	tomcat 🗸	
Distribution*	Multi-server(SAN)	
Common Name*	cmpubhcsc-ms.fhlab.com	
Subject Alternate Names (S	SANs)	
Auto-populated Domains	cmpubhcsc.fhlab.com cmsubhcsc.fhlab.com imppubhcsc.fhlab.com impsubhcsc.fhlab.com	
Parent Domain	fhlab.com	
Other Domains		Browse No file selected.
		Please import .TXT file only. For more information please refer to the notes in the Help Section
	~	E Add
Key Type**	RSA	
Key Length*	2048	
Hash Algorithm*	SHA256	
Generate Close		

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

Cisco Unified Operating System Administration For Cisco Unified Communications Solutions						Nav	ipation Cisco Unified OS Administration 🗸	Go Logout
Show . Settings	Security Software Upgrades	• Services • Help	-					
Certificate List								
Generate Self	signed 🙃 Upload Certificate/Certifica	te chain 🛐 Genera	te CSR					
0		40						
1 7 records fo	ound							1
Certificate List	t (1-7 of 7)						Rows per Page 50	~
Find Certificate Li	ist where Certificate v begin	ns with v torncat		Find Clear Filter	4 -			
Contificate *	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description	
tomcat	cmpubhcsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/18/2022	Certificate Signed by fhlab-AD-CA	
tomcat-ECDSA	cmoubhcsc-EC.thlab.com	Self-signed	EC	cmpubhcsc.thiab.com	cmpubhcsc-EC.thlab.com	04/02/2025	Self-signed certificate generated by system	
tomcat-trust	imppublicsc-EC.fhlab.com	Self-signed	EC	imppublicsc.fhlab.com	imppublicsc-EC.fhlab.com	04/02/2025	Trust Certificate	
tomcat-trust	cmsubhcsc-EC.fhlab.com	Self-signed	EC	cmsubhcsc.fhlab.com	cmsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate	
tomcat-trust	impsubhcsc-EC.fhlab.com	Self-signed	EC	impsubhcsc.fhlab.com	impsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate	
Instant Instant	emashhara EC falsh com	Eall signed	80	consultations (black com	consultance EC faish com	04/03/3035	Tout Cadificate	
tomcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate	
Generate Self-	signed Upload Certificate/Certifi	icate chain Gene	rate CSR					
-								
								_
Certificate List	t (1-6of6)						Rows per Page	50 .
Find Certificate Li	st where Certificate v begin	ns with $\ \lor$ torncat		Find Clear Filter	4 -			
Contificate *	Common Name	Type	Key Typ	Distribution	Issued By	Expiration	Description	
tomcat	cucoubhcsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/28/2022	Certificate Signed by fhlab-AD-CA	
								i
tomcat-trust	INIAD-AD-CA	Self-signed	RSA	misb-AD-CA	INIAB-AD-CA	04/18/2025	Signed Certificate	
torritory trans	Sandara and South and	Call signed	50	new block Clab and	and the State	04/02/2025	Text e Adjuste Windows	
tomcat-crust	cucsuphose-cC.Ihiab.com	Ser-signed	EC.	cucsubnese.miab.com	cucsubnese-EC.Miab.com	04/02/2025	Trust Certificate IC WITGOWS	5
comcat-crust	cucevoncec-EC.Thiab.com	Ser-signed	EC.	cucpublicsc.mlab.com	cucpuonosc-EC.Iniab.com	04/02/2025	must certriterettings to activate Window	-
Generate Self-	signed Upload Certificate/Certifi	icate chain Gene	rate CSR		-			

• 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.

<u>ia</u>	Server Manager	_ _ X
Server Ma	anager • Dashboard 🛛 - 🗐 🏲	Manage Tools View Help Add Roles and Features
Dashboard	WELCOME TO SERVER MANAGER	Remove Roles and Features Add Servers
AD CS	1 Configure this local server	Create Server Group Server Manager Properties
■ AD DS 과 AD FS 叠 DNS ■ File and Storage Services ▷ 률 IIS	QUICK START 2 Add roles and features 3 Add other servers to manage WHAT'S NEW 4 Create a server group	
	LEARN MORE	Hide
	ROLES AND SERVER GROUPS Roles: 6 Server groups: 1 Servers total: 1	
	Image: AD CS Image: Image	D FS 1

Active Directory 인증서 서비스 역할을 선택합니다.

b	Add Roles and Features Wizard	_ _ X
Select server roles		DESTINATION SERVER AD:fniab.com
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select one or more roles to install on the selected server. Roles	Description Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
	Fax Server Methods and Access Services Print and Document Services	< Previous Next > Install Cancel

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

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

구축에 따라 엔터프라이즈 또는 독립형 을 선택할 수 있습니다.

Add Roles Wizard		×
Specify Setup Ty	pe	
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results	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.	
	More about the differences between enterprise and standalone setup	
	< Previous Next > Instal Cancel	

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.NET을 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 수행됩 니다.



바인딩 편집을 선택합니다.



새 사이트 바인딩을 추가하고 HTTPS를 유형으로 선택합니다.SSL 인증서의 경우 AD 서버와 동일 한 FQDN을 가져야 하는 서버 인증서를 선택합니다.

e j			Intern	et Information	n Services (IIS) Manager	
💽 💿 💊 🕨 🖌 AD 🕨	Sites + D	efault Web Site	•			
File View Help						
Connections				Site	Bindings	? X
Start Page AD (FHLAB\admini Application Poc Sites Sites Default Web	Type http https	Host Name Type: https Host name: Require S SSL certifical fhlab-AD-C Not selected fhlab-AD-C AD.fhlab.col	Port 80 442 I Server Name te: A I A m	IP Address * Edit P address: All Unassigned	Binding Informa t Site Binding V 443	Add Fdit ? X

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 설치하 는 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 Windows를 선택하고 AD FS Management를 입력합니다.



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

AD FS 2.0 Federation Ser	ver Configuration Wizard	×
Welcome		
Steps Welcome Select Deployment Type Federation Service Name Summary Results	 Welcome to the AD FS 2.0 Federation Server Configuration Wizard This visard helps you configure Active Directory Federation Services (AD FS) 2.0 software on this computer, which sets up the computer as a federation server. An instance of AD FS is referred to as a Federation Service. C freate a new Federation Service Select this option to set up either a stand-alone federation server or the first server in a federation server farm. Add a federation server to an existing Federation Service Select this option to join this computer to an existing federation server farm. 	
	< <u>Previous</u> Cancel <u>H</u> elp	

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

AD FS 2.0 Federation Ser	ver Configuration Wizard	Ľ
Select Stand-Alone or	Farm Deployment	
Step:	You can create either a stand-alone federation server for evaluation purposes or a small production environment, or you can create a federation server in a new farm for load balancing and high availability.	
 Select Deployment Type 	Select one of the following options. Either of these options will use the Windows Internal Database to store configuration data.	
 Federation Service Name Summary Results 	 New federation server fam. This option will create a new Federation Service with settings for high availability and load balancing. This computer will be the primary federation server in the fam. Later, you can scale out this fam by adding more federation servers. To create a federation server fam, you must run this wizard while you are logged on with an account that has sufficient permissions in Active Directory to create a container object [for sharing certificates] and to set an SFN [for the service account], such as an account that is a member of the Domain Admins group. C Stand-alone federation server This option will create a new Federation Service on this computer. This option is recommended for evaluation purposes or a small production errormment. If you select this option, you will not be able to add more servers to create a fam. You can use SQL Server with AD FS 2.0 to take advantage of the full feature set and achieve maximum scalability. To set up AD FS to use SQL Server, use the command-line version of this wizard. For more information, click Help. 	
독립 실행형 페더레이	션 서버]를 선택하고 이미지에 표시된 대로 다음 을 클릭합니다.	

Specify the Federation Service Name Steps • Welcome • Select Deployment Type • Federation Service Name • Summay • Results • Federation Service name: • adDa identitylab.us • What kind of certificate do 1 need? • What kind of certificate do 1 need? • What kind of certificate do 1 need? • Previous Next • Previous Next • Steps Cancel • Help This wized details details	MAD FS 2.0 Federation Serv	ver Configuration Wizard
Steps This wizad determines the Federation Service name from the Subject field of the SSL certificate for the Default Web Site. If the wizad cannot determine the Federation Service name from the SSL settings, you must select a certificate. Select Deployment Type Federation Service Name Summary Results Federation Service name: adda.identitylab.us adda.identitylab.us what kind of certificate doil need? What kind of certificate doil need? SSL DISAMON Next> Cancel Help SSL DISAMON Next> Cancel Help SSL DISAMON Next/CFS) = a = 1 = 1 urb.	Specify the Federation	n Service Name
< Previous Next> Cancel Help SSL 인증서의 목록에서 자체 서명 인증서를 선택합니다.페더레이션 서비스 이름이 자동으로 채워 집니다.Next(다음)를 클릭합니다.	Steps Welcome Select Deployment Type Federation Service Name Summary Results	This wizard determines the Federation Service name from the Subject field of the SSL certificate for the Default Web Site. If the wizard cannot determine the Federation Service name from the SSL settings, you must select a certificate and/or port, and then click Next. Select the certificate and/or port, and then click Next. SSL certificate: Port: ad0a.identitylab.us Federation Service name: ad0a.identitylab.us What kind of certificate do I need?
		ß
	SSL 인증서의 목록에서 진니다 Next(다음)를 클	<pre></pre>

aD FS 2.0 Federation Ser	ver Configuration Wizard	×
Ready to Apply Settin	gs	
Steps Welcome Select Deployment Type Federation Service Name Summary Results	 The following settings will be configured for AD FS 2.0: Stop AD FS server. Windows Internal Database service will be started and set to automatic startup. Signing and token-encryption certificates will be generated and set to automatic roll over. Selected SSL certificate will be used for securing service communication. Network Service account will be given access to the database, to the certificate private keys and endpoints, and the service will run under this account. Default set of endpoints will be enabled. Browser sign-in web site will be deployed to the Vadfs/Is' virtual directory under the Default Web Site in IIS. Federation Service name is adDatidentitylab.us Start AD FS server. 	
	To begin configuring this computer with these settings, click Next.	
	< <u>Previous</u> <u>N</u> ext> Cancel <u>H</u> elp	

설정을 검토하고 Next(다음)를 클릭하여 설정을 적용합니다.

Paderation Serv	ver Configuration Wizard	2
Configuration Results		
Steps	The following settings are being configured	
 Welcome Select Deployment Type Federation Service Name Summary Results 	Component Install Windows Internal Database Install Windows Internal Database <td< th=""><th>Status Configuration finished Server Configuration Wizard.</th></td<>	Status Configuration finished Server Configuration Wizard.
		Dose
모든 구성 요소가 성공	적으로 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 신 뢰할 수 있는 신뢰 파트너로 추가해야 합니다.이 작업을 수행하려면 먼저 CUCM Administration에 서 일부 컨피그레이션을 수행해야 합니다.

ADFS를 사용하여 CUCM에서 SSO 구성

LDAP 컨피그레이션

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

LDAP System Configuration

Status							
Status							
(i) Please Delete All LDAP	i Please Delete All LDAP Directories Before Making Changes on This Page						
i Please Disable LDAP A	Please Disable LDAP Authentication Before Making Changes on This Page						
LDAP System Informatio	n						
Enable Synchronizing from the second seco	om LDAP Server						
LDAP Server Type	Microsoft Active Directory						
LDAP Attribute for User ID	sAMAccountName						

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	Status Status: Ready							
LDAP Directory Information								
LDAP Configuration Name*	LDAP1							
LDAP Manager Distinguished Name*	fhlab\administrator							
LDAP Password*								
Confirm Password*								
LDAP User Search Base* c	n=users,dc=fhlab,dc=com							
LDAP Custom Filter for Users	< None >							
Synchronize*	 Users Only							
LDAP Custom Filter for Groups	< None >							
LDAP Directory Synchronization So	chedule							
Perform Sync Just Once								
Perform a Re-sync Every*	7 DAY ᅌ							
Next Re-sync Time (YYYY-MM-DD hh:r	mm)* 2020-05-24 00:00							

Г	Standard User Fields To Be Synchronized —			
l	Cisco Unified Communications Manager User Fields	LDAP Attribute	Cisco Unified Communications Manager	r User Fields LDAP Attribute
l	User ID	sAMAccountName	First Name	givenName
l	Middle Name	middleName 😌	Last Name	sn
l	Manager ID	manager	Department	department
l	Phone Number	telephoneNumber 🖸	Mail ID	mail
l	Title	title	Home Number	homephone
l	Mobile Number	mobile	Pager Number	pager
	Directory URI	mail	Display Name	displayName
	LDAP Server Information – Host Name or IP Addre	ss for Server [*]	LDAP Port* U	se TLS
	10.89.228.226		389	
	Add Another Red	undant LDAP Server		

Save Delete

Copy

Perform Full Sync Now Add New

Active Directory 사용자가 CUCM과 동기화된 후 LDAP 인증을 구성해야 합니다.

		Cieco	. 11	nifie	I CM	Ad	min	istr	atio																	Marcha	tion .	Cierro		Ead C	N Ada	inistrati			Go
	isco	Encle		aified		Au	in the second	istre Feluti	atio																	navig	stion	Cisco	o Unir	ned C	MAG	ninistrat	on they	, i	00
_		For Cis	000	nimea	ommu	ncat	ions :	FOILUTIN	ons					_	_	_	_	_	_	_	_		_				artar		Sear	nah De	cume	ncation	ADOU	<u>ا</u> ا	Logout
Sys	em 🕶	Call Routing	•	Media Re	sources	• /	Advano	ed Feat	ures *	Dev	ice +	App	sication .	* (User Ma	agement		Bulk	Administ	ration	•	Help •	•												
LD/	P Aut	henticatio	m																																
	Save																																		
r St	tus-																							 	 										
G) Stat	us: Ready																																	
																		_						 	 										
L ro	AP Au	thenticati	on fo	or End	Jsers-																														
	Use L	DAP Authen	ticat	ion for B	ind Use	\$																													
LD	AP Mar	nager Distin	nguisl	hed Nan	10 [*] fhl	b\Ad	minist	ator]																			
LD	AP Pas	sword*			•••	••••	•••••	•••••					••••]																			
Co	nfirm I	Password*											••••			1																			
LD	AP Use	r Search B	ase"		cn	usen	a,dc=f	hlab,do	c=com							j																			
-10	AP Se	rver Infor	mati	on			_			_	_	_						_										_							
					Host N	me o	IP A	ddress	for Se	rver*						LDA	P Por	۰.	Use TLS																
	0.89.2	28.226					_			_	_	_				389																			
1	Add A	nother Red	lunda	nt LDAP	Server]																													

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

End Use	er Configuration			Re	lated Links: B	ack to Find List Users	✓ G0
Sav	ve 🗙 Delete 🕂 Add New						
Confirm	n MLPP Password						1
MLPP Pr	recedence Authorization Level	Default		~]		
- CAPF Information							
Associa	ted CAPF Profiles			^			
				View Details	2		
Permis	sions Information						
Groups	Standard CCM End Users Standard CCM Super Users	^			c Control Crow	-	
	Standard CTI Allow Control of Standard CTI Enabled	All Devices		Remove from	n Access Control	p ol Group	
Delec		~	View Details				
Roles	Standard AXL API Access Standard Admin Rep Tool Adm	nin					
	Standard CCM Admin Users Standard CCM End Users	tration					
	Standard CCHADHIN Adminis	tration	View Details				
Confer	ence Now Information						
L Enal Meeting	ble End User to Host Conference Number 1001	e Now					
Attende	es Access Code						
Save	Delete Add New						

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-on에서 다운로드 할 수 있습니다.노드 또는 Cluster Wide별로 수행할 수 있습니다.이 클러스터 전체에서 수행하는 것 이 좋습니다.

yotem * Cas Houding * Moda Hestoricha								
SAML Single Sign-On								
ISO Mode								
Cluster wide (One me	Ø Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)							
) Per node (One metadata file per node)								
🗙 Disable SAML SSO 🧯	Export All Metada	ta 🔞 Update kdP Metadi	ata File 🧳 Fix All Disabled Servers					
Status								
Aatus								
A start is suchied for	eeo var en ek	and the state have						
RTMT is enabled for	SSO. You can cha	ange SSO for RTMT here	L					
RTMT is enabled for SAML SSO enabled	SSO. You can chi	inge SSO for RTMT here	L.					
RTMT is enabled for SAML SSO enabled	SSO. You can che	inge SSO for RTMT <u>here</u>	L					
RTMT is enabled for SAML SSO enabled SAML Single Sign-On	\$\$0. You can che (1 - 4 of 4)	inge SSO for RTMT <u>hers</u>	L				Rows per Page 50 v	
RTMT is enabled for SAML SSO enabled SAML Single Sign-On Server Name	SSO. You can che (1 - 4 of 4) SSO Status	nge SSO for RTMT <u>herr</u> Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test	Rows per Page 50	
RTMT is enabled for SAML SSO enabled SAML Single Sign-On Server Name cmpubhcsc.fhlab.com	SSO. You can che (1 - 4 of 4) SSO Status SAML	Re-Import Metadata	Last Metadata Import April 20, 2020 2:00:57 PM PDT	Export Metadata	Lest Metadata Export April 18, 2020 8:05:38 PM PDT	SSO Teat Passed - April 20, 2020 20215 PM PDT	Rows per Page 50 V	
RTHT is enabled for SAML SSO enabled SAML Single Sign-On Server Name cmpubhcsc.fhlab.com cmsubhcsc.fhlab.com	SSO. You can che (1 - 4 of 4) SSO Status SAML SAML	Re-Import Metadata N/A M	Last Metadata Import April 20, 2020 2:00:57 PM PDT April 20, 2020 2:00:57 PM PDT	Export Metadata Die File Die	Last Metadeta Export April 18, 2020 8:05:38 PM PDT April 18, 2020 8:05:37 PM PDT	850 Teat Passed - April 20, 2020 2:02:15 P4 PDT Passed - April 20, 2020 1:49:45 P44 PDT	Rows per Page 50 Run SSO Test Run SSO Test	
RTHT is enabled for SAML SSO enabled SAML SSO enabled SAML Single Sign-On Server Name cmpubhcsc.fhlab.com mppubhcsc.fhlab.com	SSO. You can chu (1 - 4 of 4) SSO Status SAML SAML SAML	Re-Import Metadata N/A M IdP IdP	Last Metadata Import April 20, 2020 2:00:57 PM PDT April 20, 2020 2:00:57 PM PDT April 20, 2020 2:00:57 PM PDT	Export Metadata	Last Metadata Export April 18, 2020 8:05:38 PM PDT April 18, 2020 8:05:37 PM PDT April 18, 2020 8:05:37 PM PDT	SSO Test Passed - April 20, 2020 2:02:15 PM PDT Passed - April 20, 2020 1:49:45 PM PDT Passed - May 24, 2020 12:02:56 PM PDT	Rows per Page 50 Run SSO Test Run SSO Test 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.

\$	Add Relying Party Trust Wizard
Welcome	
 Steps Welcome Select Data Source Configure Multi factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish 	<section-header><text><text><text></text></text></text></section-header>

Start(시작)를 클릭하여 계속합니다.

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

\$	Add Relying Party Trust Wizard
Select Data Source	
 Steps Welcome Select Data Source Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish 	Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata address (host name or URL): Federation metadata address (host name or URL): Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Filter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.

CUCM_**Cluster_Wide_Relying_Party_trust를** 표시 이름으로 사용하고 **Next**를 클릭합니다.

\$	Add Relying Party Trust Wizard	x
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
 Welcome 	Display name:	
Select Data Source	CUCM_Cluster_Wide_Relying_Party_trust	
Specify Display Name	Notes:	
Configure Multi-factor Authentication Now?		^
 Choose Issuance Authorization Rules 		
 Ready to Add Trust 		
 Finish 		\square
	< Previous Next A ct Va Canibel	ndo

첫 번째 옵션을 선택하고 **다음**을 클릭합니다.

\$	Add Relying Party Trust Wizard
Steps Welcome	Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.
 Select Data Source Specify Display Name 	Multi-factor Authentication Global Settings
Configure Multi-factor Authentication Now?	Requirements Users/Groups Not configured
Choose Issuance Authorization Rules	Location Not configured
 Ready to Add Trust Finish 	
	 I do not want to configure multifactor authentication settings for this relying party trust at this time. Configure multifactor authentication settings for this relying party trust.
	You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u> .
	< Previous Next A ct Cancel in d

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

\$	Add Relying Party Trust Wizard
Choose Issuance Autho	prization Rules
Steps	Issuance authorization rules determine whether a user is permitted to receive claims for the relying party.
Welcome	Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.
Select Data Source	 Permit all users to access this relying party
Specify Display Name	The issuance authorization rules will be configured to permit all users to access this relying party. The relying
Configure Multi-factor Authentication Now?	Deny all users access to this relying party
 Choose Issuance Authorization Rules 	The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.
 Ready to Add Trust 	
• Finish	You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.
	< Previous Next & ct ValCangel indo

컨피그레이션을 검토하고 이미지에 표시된 대로 Next를 클릭합니다.

\$	Add Relying Party Trust Wizard
Ready to Add Trust	
Ready to Add Trust Steps • Welcome • Select Data Source • Specify Display Name • Configure Multi-factor Authentication Now? • Choose Issuance Authorization Rules • Ready to Add Trust • Finish	The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.
	< Previous ANext > ate Vicancel > S

확인란의 선택을 취소하고 **닫기**를 클릭합니다.

\$	Add Relying Party Trust Wizard
Finish	
Steps Velcome Select Data Source Specify Display Name Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in. Open the Edit Claim Rules dialog for this relying party trust when the wizard closes
	Close

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.

V		AD	FS	
🗌 File Action View Windo	w Help			
🗢 🄿 🙍 🖬 🖬 🖬				
AD FS	Relying Party Trusts			
Service	Display Name	Enabled	Туре	Identifier
Claims Provider Trusts	Device Registration Servic	e Yes	WS-Trust / SAML / WS-Federation	um:ms-drs:ad.fhlab.com
 Relying Party Trusts Attribute Stores Authentication Policies 	CUC_Cluster_W Up ExpwyC Ed Dis Prr De He	date from Federation Meta date from Federation Meta t Claim Rules able operties lete	L / WS-Federation	cucpublicse fhlab.com fhlab.com-500D0F4107D76E57

이미지에 표시된 대로 Add Rule을 클릭합니다.

Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party	• X
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization R	ules
The following transform rules specify the claims that will be sent to the relying party.	
Order Rule Name Issued Claims	
	+
Add Rule Edit Rule Remove Rule	
OK Cancel	Apply

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

Select Rule Template Steps • Choose Rule Type • Configure Claim Rule Claim rule template Caim rule template Caim rule template Claim rule template description: Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to creat a rule that will extract attribute values for authenticated users from the displayName and telephoneNumt Active Directory attributes and then send those values as two different outgoing claims. This rule may all be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.	
Steps Select the template for the claim rule that you want to create from the following list. The description provide details about each claim rule template. Configure Claim Rule Claim rule template: Send LDAP Attributes as Claims Image: Claim rule template description: Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attributes as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to creat a rule that will extract attribute soft attribute soft on and the send those values as two different outgoing claims. This rule may all be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.	
e Choose Rule Type details about each claim rule template. e Configure Claim Rule Claim rule template: Send LDAP Attributes as Claims Claim rule template description: Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to creat a rule that will extract attributes and then send those values as two different outgoing claims. This rule may al be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.	s
 Configure Claim Rule Claim rule template: Send LDAP Attributes as Claims Claim rule template description: Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to creat a rule that will extract attribute values for authenticated users from the displayName and telephoneNumb Active Directory attributes and then send those values as two different outgoing claims. This rule may all be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template. 	
Send LDAP Attributes as Claims v Claim rule template description: Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to creat a rule that will extract attribute values for authenticated users from the displayName and telephoneNumb Active Directory attributes and then send those values as two different outgoing claims. This rule may all be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.	
Claim rule template description: Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to crea a rule that will extract attribute values for authenticated users from the displayName and telephoneNumt Active Directory attributes and then send those values as two different outgoing claims. This rule may all be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.	
Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to creat a rule that will extract attribute values for authenticated users from the displayName and telephoneNumt Active Directory attributes and then send those values as two different outgoing claims. This rule may all be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.	
Convision Next > Convi	

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 Ru	ule - NameID 🛛 🗙
You car which to issued f	n configure this rule to send the values of L o extract LDAP attributes. Specify how the rom the rule.	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be
Claim ru	le name:	
Namel	0	
Rule ter	mplate: Send LDAP Attributes as Claims	
Attribute	e store:	
Active	Directory	¥
Mappin	g of LDAP attributes to outgoing claim type	5:
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
•	SAM-Account-Name V	vid 🗸 🗸 Vila
*	~	×
View I	Rule Language	OK Cancel

다른 규칙**을** 추가하려면 Add Rule을 다시 클릭합니다.

🧐 Edit Clai	m Rules for CUCM_Clu	ster_Wide	e_Relying_Party	- 🗆 X
Issuance Tran	sform Rules Issuance Author	ization Rules	Delegation Authoriza	tion Rules
The followin	ng transform rules specify the cla	aims that will	be sent to the relying p	arty.
Order R	ule Name		Issued Claims	
1 N	amelD		uid	
				T
				*
Add Rule	Edit Rule Remov	ve Rule		
L				
		0	K Cancel	Apply

Send **Claims Using a Custom Rule을 선택하고 Next**를 클릭합니다.

Q	Add Transform Claim Rule Wizard
Select Rule Template	,
Steps	Select the template for the claim rule that you want to create from the following list. The description provides
Choose Rule Type	details about each claim rule template.
Configure Claim Rule	Claim rule template:
	Send Claims Using a Custom Rule 🗸
	Claim rule template description:
	Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include: Sending claims from a SQL attribute store Sending claims from a custom attribute store using a custom LDAP filter Sending claims only when 2 or more incoming claims are present Sending claims only when an incoming claim value matches a complex pattern Sending claims for use only in later rules Creating claims for use only in later rules
	< Previous Next > Cancel

Cluster_Side_Claim_Rule이라는 사용자 지정 규칙을 생성합니다.

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

c:[Type ==

"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
<pre>=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",</pre>
<pre>Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,</pre>
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =</pre>
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties[" <u>http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier</u> "]
= "http:// <adfs fqdn="">/adfs/com/adfs/services/trust",</adfs>
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =</pre>
" <cucm fqdn="" pub="">");</cucm>
c:[Type == " <u>http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname</u> "]
<pre>=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",</pre>
<pre>Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,</pre>
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =</pre>
"urn:oasis:names:tc:SAMI.:2 0:nameid-format:transient"
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] = "http://AD.fhlab.com/adfs/services/trust",</pre>
<pre>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"] =</pre>

Finish를 클릭하여 계속합니다.

%	Add Transform Claim Rule Wizard
Configure Rule	
Steps Configure Claim Rule	<pre>You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language. Caim rule name: Custom_Side_Claim_Rule Rule template: Send Claims Using a Custom Rule Custom rule (:[Type == " "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount name"] => issue(Type = "http://schemas.miscosof.com/ws/2005/05/identity/claims/windowsaccount name"] => issue(Type = "http://schemas.miscoso.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties ["http://schemas.miscosp.org/ws/2005/05/identity/claimproperties/format "] = "nurcoasis:names:tc:SAML:2.0:nameid-format:transient", Properties ["http://schemas.miscosp.org/ws/2005/05/identity/claimproperties/format "] = "nutp://schemas.miscosp.org/ws/2005/05/identity/</pre>
	< Previous Pinish Cancel

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

IDP 메타데이터

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

9		Service	5				x
File Action View	Help						
🗢 🔿 📅 🔯 🤄	2 🕞 🛛 🖬 🕨 🖬 🕪						
Services (Local)	Services (Local)						
	Active Directory Federation	Name A	Description	Status	Startup Type	Log On As	^
	Services	Active Directory Certificate Services	Creates, manages, and removes	Running	Automatic	Local System	=
	Stop the service	Active Directory Enderation Services	Foobles Active Directory Federa	Running	Automatic (Delayed Start)	EHLAR\administra	
	Restart the service	Active Directory Web Services	This service provides a Web Ser-	Running	Automatic	Local System	-
		App Readiness	Gets apps ready for use the first		Manual	Local System	
	Description:	Application Experience	Processes application compatib		Manual (Trigger Start)	Local System	
	Enables Active Directory Federation	Application Host Helper Service	Provides administrative services	Running	Automatic	Local System	
	Services to issue security tokens.	Application Identity	Determines and verifies the ide		Manual (Trigger Start)	Local Service	
		Application Information	Facilitates the running of intera		Manual (Trigger Start)	Local System	
		Application Layer Gateway Service	Provides support for 3rd party p		Manual	Local Service	
		Application Management	Processes installation, removal,		Manual	Local System	
		AppX Deployment Service (AppXSVC)	Provides infrastructure support		Manual	Local System	
		CASP.NET State Service	Provides support for out-of-pro		Manual	Network Service	
		Background Intelligent Transfer Service	Transfers files in the backgroun		Manual	Local System	
		Background Tasks Infrastructure Service	Windows infrastructure service	Running	Automatic	Local System	
		😘 Base Filtering Engine	The Base Filtering Engine (BFE) i	Running	Automatic	Local Service	
		Certificate Propagation	Copies user certificates and roo	Running	Manual	Local System	
		CNG Key Isolation	The CNG key isolation service is	Running	Manual (Trigger Start)	Local System	
		COM+ Event System	Supports System Event Notifica	Running	Automatic	Local Service	
		G COM+ System Application	Manages the configuration and	Running	Manual	Local System	
		Computer Browser	Maintains an updated list of co		Disabled	Local System	¥
		< l					>
	Extended Standard						
				1	Activate Windows		

_____ 이제 CUCM이 ADFS에 신뢰할 수 있는 신뢰 당사자로 추가되었습니다.

🎨 Edit C	laim Rules fo	or CUCM_	Cluster_Wid	de_Relyi	ng_Party	-		×
Issuance	Transform Rules	Issuance Au	thorization Ruk	s Delega	tion Authoriza	tion R	ules	
The foll	owing transform n	les specify th	e claims that w	I be sent to	the relying pa	aty.		
Order	Rule Name			Issued Cla	aims			
1	NameID			uid				
2	Ouster_Side_O	laim_Rule		<see clair<="" td=""><td>m rule></td><td></td><td></td><td></td></see>	m rule>			
Add I	Rule Edit F	Rule	emove Rule]			•	
			(ок [Cancel		App	у

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

Firefox 🔻		
👍 Untrusted Connection 🛛 🗙 🧶 Mozilla Firefox Start Page 🔗	+	
🗲 🕲 ɔs://ad0a.identity 💫.us/FederationMetadata/2007-06/FederationMetadata 🏠 🔻 C	8 - Google 🔎 🔣 -	+ 🏦
Most Visited Getting Started Suggested Sites Web Slice Gallery		
Opening FederationMetadata.xml	but we can't confirm that your	<u> </u>
You have chosen to open: FederationMetadata.xml	dentification to prove that you ed.	
which is: XML Document from: https://ad0a.identitylab.us What should Firefox do with this file? © Qpen with Internet Explorer (default) © Save File Do this gutomatically for files like this from now on. OK Cancel	an that someone is trying to g this site's identification. Even ampering with your	
Don't add an exception unless you know there's a good reason why identification. Add Exception.	this site doesn't use trusted	
		-

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

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

🗱 Find and List Cisc	Unified CM × +	- c	ı ×
← → ♂ ☆	🛛 🖴 😂 https://cmpubhcsc.fhlab.com:8443/ccmadmin/ccmGroup 🚥 🖂 🟠	lii\ 🖸	\$ ₽
Server Cisco Unified CM Cisco Unified CM Group Presence Redundancy Group Phone NTP Reference Date/Time Group BLF Presence Group Region Information Device Pool Device Mobility DHCP	Administration Navigation Cisco Unified CM Administr nunications Solutions farfar Search Documentation res • Advanced Features • Device • Application • User Management • Buk Ad ps ups anager Group nager where Name begins with v Find • active query. Please enter your search criteria using the options above.	ration on About ministration •	Go Logout Help •
LDAP SAML Single Sign-On	•		
SAML Single Sign-On Cross-Origin Resource Sha (CORS) Location Info MLPP Physical Location SRST Enterprise Parameters Enterprise Phone Configura Service Parameters Security Application Server Licensing Geolocation Configuration Geolocation Filter E911 Messages	ing		

https://cmpubhcsc.fhlab.com/8443/ccmadmin/sam/SingleSignOn.do

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

Firefox *						_ 🗆 🗙
End and List Users	× SAML Single Sign-On	× to Find	and List LDAP Directories	× +		
+ A https://cucm0a/comadmin	(samlSingleSignOn.do		습 =	C Scogle	۰ 🗅 ۹	+ #
Cisco Unifi Cisco Unifi	ied CM Administrations ed Communications Solutions	on		Navigation Cisco Unifie admin Search Docume	d CM Administration Intation About	Go Logout
System - Call Routing - Med	is Resources + Advanced Features		User Management 👻 Bu	k Administration 👻 Help 👻		
SAML Single Sign-On						
🥜 Enable SAML SSO 🚷 Up	date IdP Metodata File 👔 Export A	Metadata 🧳 Fix All Disabled S	iervers			
Status						
() SAML SSO disabled						
SAML Single Sign-On (2	1 - 1 of 1)				Rows per Page	50 💌
Server Name SSO Stati cucm0a Disabled	us Re-Import Metadata N/A	Last Metadata Import Never	Export Metadata	Last Metadata Export Never	SSO Tes Never	n Test

Enable SAML SSO(SAML SSO 활성화)를 선택합니다.

경고를 승인하려면 Continue(계속)를 클릭합니다.

😺 Reset Warning - Mozilla Firefox 📃 🗆 🗙
Https://cucmDa/ccmadmin/genericDialogWindow.do?windowtitlekey=genericdialogwindow.windowtitle.ssoenable
Web server connections will be restarted Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again. Continue Cancel

일을 이미지에 표시된 대로 가져옵니다.

Firefox *			
🕮 Find and List Users × 🕮 SAML Single Sign-On Configuration × 🛤 Find and List LDAP Directories	× +		
← ▲ https://cum0a/comadmin/samlSingleSignOnConfigurationWzard.do ☆ ▼ €	Scogle	۶ 🖬 -	+ +
CISCO Unified CM Administration For Cisco Unified Communications Solutions	Navigation Cisco Unified CM A dmin Search Documentatio	dministration	Go Logout
System 👻 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻 Bulk A	dministration 👻 Help 👻		
SAML Single Sign-On Configuration			
Next			
Status Ready to import Identity Provider metadata trust file to cluster 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 Id manually obtain the file from the IdP and upload it here. IdP Metadata File Bowne No file selected. Initiate the Metadata In/No file selected. This action must be successful for at least the Publisher before moving on to the next task in this wizard. Import IdP Metadata Next Cancel	IP and import it to your servers.	You will need	to

XML 파일을 선택하고 **열기**를 클릭하여 다운로드(Downloads) 아래의 즐겨찾기(Favorites)에서 CUCM에 업로드합니다.

😧 File Upload					
😗 🖓 - Adminis	strator - Downloads				Search Downloads
Organize • New folder)# • 🖬 9
* Favortes	Name *	Date modified	Type	Size	
E Desktop	AdfsSetup	2013/09/09 06:10 PM	Application	24 518 KB	
S Downloads	🖆 FederationMetadata	2013/09/12 02:01 PM	3ML Document	32 KB	
2 Recent Places	pkpkk_hst	2013/09/12 11:09 AM	Application	11 129 88	
Documents Documents Music Pictures Videos Computer Network					
File	e game: FederationMetadata				All Files
					<u>Q</u> pen Cancel

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

🥰 SAML Single Sign-On Configuration - Windows Internet Explorer 📃 🖸 🔀
🚱 🕘 💌 🎑 https://10.1.1.100/ccmadmin/s 🔎 💌 😢 🖅 🏼 🧭 SAML Single Sign-On Configu 🗙 👘 🏠 🔅
CISCO Unified CM Administration Navigation Cisco Unified CM Administration Cisco Unified CM Ad
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
SAML Single Sign-On Configuration
Next
Status V 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 C:\Users\bbanks\Downloads\FederationMetadata.xml 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 IdP Metadata Import succeeded for all servers Next Cancel

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

i SAML Single Sign-On Configuration - Mozilla Firefox	-	(\times
🛛 🖨 📽 https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOnConfigurationWizard3.do?serve	fi ***	⊌	☆	≡
SAML Single Sign-On Configuration				
Test SSO Setup				
This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is such	s test ccessfi	can b ul.	be run	on
1)Pick a valid username to use for this test				
You must already know the password for the selected username. This user must have administrator rights and also exist in the IdP.				
Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in a lockout.	dmini	strate	or	
Valid administrator Usernames				
farfar				
2)Launch SSO test page				
Run SSO Test				
Cancel				

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

ڬ Sign In - Mozilla Firefox		-		\times
🛛 🔒 https://ad.fhlab.co	m/adfs/ls/?SAMLRequest=nZJPTwlx	EMXvflpN77ClAi	4NS0 •••	≡
				^
FS				
Sign in with y	our organizational account			
farfar@fhlab.	com			
••••••				
Sign in				*

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

€ → ሮ ŵ	🛛 🔒 😂 https://cucput	hese.fhlab.co	m/cuadmin/home	•	· 🛛 🕁	III\ 🗊	8		
Cisco Unity C For Cisco Unified C	Connection Administ	ration				Naviga farfa	ion Cisco Unity Connection A Search Documentation	dministration	1 ↓ Ge Sign O
Cisco Unity Connection	SAML Single Sign on							SAML SI	ngle Sign
General Configuration - Cluster - Authentication Rules Roles - Roles - Restriction Tables - Licenses - Schedules - Holiday Schedules	Cluster wide (One m Per node (One meti Disable SAML SSO II	SD Mode © Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate) Per node (One metadata file per node) Comparison of the server server and the server serve							6
Global Nicknames Subject Line Formats	Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Te	it .	
	cucpubhcsc.fhlab.com	N/A	April 29, 2020 10:52:36 AM PDT	📩 file	April 28, 2020 5:54:01 PM PDT	Passed - April 29, 2020 11:05:10 AM PDT	Run SS	O Test	
Service Parameters cucsubhcsc.fhlab.com SAML IP IdP April 29, 2020 10:52:36 AM April 28, 2020 5:54:00 PM Passed - April 29, 2020 Run SSO PDT 11:05:37 AM PDT Run SSO									O Test
Fax Server B-LDAP SAML Single Sign on	Disable SAML SSO	Export All I	Metadata Updi	ate IdP Metadata File Fix All 0	isabled Server	5			

LDAP 인증을 구성합니다.

← → ♂ ☆	D ≜ ≅ https://cucpubhcscfhlab.com/cuadmin/home.do								
Cisco Unity Con For Cisco Unified Comm	nection Administration munications Solutions	Navigation Cisco Unity Connection Administration 🗸 Go farfar Search Documentation About Sign Out							
Cisco Unity Connection	LDAP Authentication	LDAP Authentication							
Cluster Unity Connection Video Services Accounts Status Dial Plan Partitions Search Spaces System Settings General Configuration Cluster Authentication Rules Reles Reles Reles Status Schedules Holiday Schedules	LOAP Authentication Refresh Help Save Status Status UaP Authentication for End Users UaP Authentication for End Users LDAP Manager Distinguished Name* fhlab/Administrator LDAP Password* Confirm Password* LDAP User Search Base* Cn=users,dc=fhlab,dc=com								
Attachment Descriptions Enterprise Parameters Service Parameters Plugins Fax Server LDAP LDAP Setup LDAP Setup LDAP Authentication	LDAP Server Information Host Name or IP Address for Server [®] LDAP Por 10.89-228-226 Add Another Redundant LDAP Server Save Fields marked with an asterisk (*) are required.	4 [*] υ‱π.5] □							

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

Cisco Unity Connection	Import Users				Import U
E Users ^	Import Users Refresh Help				
Users Import Users	- Status				
Synch Users	0				
Class of Service	Found 1 LDAP User(s)				
Class of Service	Find				
Class of Service Membership	Find End Users In LDAP Directory				
i remplates		-	1		
Oser remplates	Where Alias V Begins Wi	th v	Eind		
Call Handler Templates					
Contact Templates	[Import With				
Notification Templates	Based on Template voicemailuser	template 🗸			
🗄 Contacts					
Contacts	Directory Search Results				
Distribution Lists	birectory search kesuits				
System Distribution Lists	Import Selected Import All	25 V Rows Per Page			
Call Management					
System Call Handlers	Alias A	First Name	Last Name	Phone Number	Extension
Directory Handlers	hugohugo	hugo	hugo	1002	1002
Interview Handlers		· · · · · · · · · · · · · · · · · · ·			
Custom Recordings	Import Selected Import All				

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

Cisco Unity Connection	c.de i	licer Dacies (hugehuge)		
Users	^ Eal(User Basics (hugonugo)		
Users	User	r Edit Refresh Help		
Import Users		Liser Basics	1.	
Synch Users	<u>S</u> a	ave Oser Dasies	-	
E Class of Service	_ Sta	ate Password Settings		
Class of Service		Change Password		
Class of Service Membership Templates		Roles	ectory	
User Templates	Nam	me Message Waiting Indicators	1	
Call Handler Templates	Alias	s* Transfer Rules		
Contact Templates	First	N Message Settings		
Notification Templates		Message Settings		
Contacts	Last	Caller Input		
Contacts	Disp	Mailbox		
Distribution Lists	SMT	P Phone Menu	@cucpubhcsc.fhlab.com	
System Distribution Lists	Initia	als Playback Message Settings		
Call Management	Title	Sand Massaga Sattings		
Directory Handlers		Send Message Settings		
- Interview Handlers	Emp	Message Actions		
Custom Recordings		Greetings		
E-Call Routing	LOA	Post Greeting Recording		
Message Storage	•	Int Notification Devices		
Mailboy Stores	0	Do		

테스트 사용자에게 시스템 관리자의 역할을 할당합니다.



CUC 메타데이터

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

-								A	D FS	5				_ 🗆 X	
9	File	Action	Niew	Wine	dow	Help								- 8 ×	
+	nþ	2	2												
1	AD F	s			Re	elying Party Trus	ts							Actions	
Þ	<u> </u>	ervice				Display Name		Enabled	5	Туре	_		Identifier	Relying 🔺	
1	-	rust Rel	ationship or Provide	s e Teurs		Device Registratio	in Service	Yes		WS-Trust /	SAML	/WS-Federation	um:ms-drs:ad.fhlab.com	Add R	
		Relyi	ng Party T	rusts	1	CUCM_Ouster_W	ide_Relying_Party_trust	Yes		WS-Trust /	SAML	/WS-Federation	cmpublicsc fhlab.com	Add	
	1	Attrit	oute Store	s		EpwyC	e_redeng_rend_reak	Yes	1	WS-Trust /	SAML	/WS-Federation	Phab.com-500D0F4107D76E57	View	
Þ	<u> </u>	Authenti	cation Po	licies		Charles Wide	Dataina Data t	_ 0	1 .	x			Edit Rule - CUC	Cluster Side Clair	m_Rule X
	99 E	dit Cla	im kule	stor	CUC,	_Cluster_wide	_Kelying_Party_t(-			-		-
ш	Issu	ance Tra	nsform Ru	les Is	suance	e Authorization Rule	B Delegation Authorizat	on Rules	1	_		You can cor claims from a	figure a custom claim rule, such as a s SQL attribute store. To configure a c	rule that requires multiple custom rule, type one or	e incoming claims or that extracts more optional conditions and an
ш	Т	he follow	ing transfo	m rules	specif	fy the claims that wi	I be sent to the relying pa	ty.				issuance sta	tement using the AD FS claim rule lan	guage.	
	Г	Order	R de Name				Issued Claims					Claim rule na	me:		
		1 1	VameID				uid	-				CUC_Duste	r_Side_Claim_Rule		
		2 (CUC_Clust	er_Side	_Claim	Rule	<see claim="" rule=""></see>					Rule templat	e: Send Claims Using a Custom Rule		
ш												Custom rule:			
ш												c: [Type			<u>^</u>
												"http://	schemas.microsoft.com/ws/	2008/06/identity	/claims/windowsaccount
									•			=> 1350	e(Type =		
									•			"http://	schemas.xmlsoap.org/ws/20 c.Issuer, OriginalIssuer	<pre>= c.OriginalIss</pre>	laims/nameidentifier", uer, Value = c.Value,
									\$			ValueTyp	e = c.ValueType, Properti	83	
									-			["http://	/schemas.xmlsoap.org/ws/2 n:oasis:names:tc:SAML:2.0	nameid-format:t:	claimproperties/format ransient", Properties
ш												["http:/	/schemas.xmlsoap.org/ws/2	005/05/identity/	claimproperties/namegu
н												alifier"] = "http://AD.fhlab.com/ /schemas.xmlsoap.org/ws/2	adfs/services/tro 005/05/identity/	ust", Properties
н												qualifie	r"] = "cucpubhcsc.fhlab.c	om");	~
-															
	L														
	[Add Ru	e E	dt Rule		Remove Rule]							Activate	Windows
														Go to Such	am in Control Panel to active
															en in control Panel to activa

SAML Single Sign-On으로 이동하고 Enable SAML SSO로 이동합니다.

i SAML S	Single Sign on Configuration - Mozilla Firefox		-		\times
0 🔒	https://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnCon	figurationWizard3.do?serverName=	··· 6	J ↔	≡
SAML Sin	gle Sign on Configuration	SAML Single	Sign or	n Config	uration
SAML Sing	gle Sign on Configuration Refresh Help				
Test SS	O Setup	w SSO to start up on the servers. This	e test c	an he ri	
on any s	erver for troubleshooting once SSO has been enabled. SSO setup ca	nnot be completed unless this test is	succes	sful.	
1)Pick a	valid username to use for this test				
You mus This use	t already know the password for the selected username. r must have administrator rights and also exist in the IdP.				
	ase use one of the Usernames shown below. Using any other Userna kout.	me to log into the IdP may result in a	dminis	trator	
Valid ad	ninistrator Usernames				
farfar hugohu	go^				
	~				
2)Launcl	n SSO test page				
Run S	S0 Test				
Cancel					
SAML Single Si	gn on Configuration - Mozilla Firefox - 🛛 -	×		- 0	- ×
SAML Single Sid	non Configuration	= ···· 영업			• =
SAML Single Sign	on Configuration Refresh Help	farfar Search Docu	mentation A	About	Sign Out
Status	iata Test Successful			SAML Sir	ngle Sign on
Close	🍯 Test SAML - Mozilia Firefox — 🗆 🗙				
	O				
	SSO Test Succeeded!	**			
	bbo rest succeducu.		Roy	ws per Page	50 v
	Congratulations on a successful SAML SSO configuration test. Please	file April 28, 2020 5:54:01 PM Passed - May	SSO Ter 24, 2020	Run SSI	D Test
	close this window.	PDT 3:17:04 File April 28, 2020 5:54:00 PM Passed - April PDT 11:05:37	29, 2020 AM PDT	Run SSG	D Test
	Close	Servers			
	,				

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 데이 터 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(다 운로드)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.

🗢 🏟 🖄 📰 📓 🗊						
aD FS	Relying Party Trusts					Actions
AD FS Service Endpoints Cetificates Claim Descriptions Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies	Relying Party Trusts Display Name Ducker Registration Service CUCM_Cluster_Wide_Relying_Party_trust Display Name Decode CUC_Cluster_Wide_Relying_Party_trust Display Name Edit Claim Rules for Expw Transform Rules Issuance Authorization Rules Issuance Authorization Rules Deleg owing transform rules specify the claims that will be sent Rule Name Rule Name Issued (NameID uid	Enabled Yes Yes Yes yC gation Author to the relying Daims	Type WS-Trust / SAI WS-Trust / SAI WS-Trust / SAI US-Trust / SAI Lation Rules party.	AL / WS-Federation AL / WS-Federation AL / WS-Federation You can configu which to extract issued from the issued from the Claim rule name: Storetic Rule template: S Attribute store: Active Directory Mapping of LDA Badd m B SAM-A #	Identifier umms-dra.ad.fhlab.com corpubhosc.fhlab.com cucpubhosc.fhlab.com Ihlab.com-50000F4107076E57 Edit Ru re this rule to send the values of LI LDAP attributes. Specify how the I ule. Find LDAP Attributes as Claims P attributes to outgoing claim typer Attributes to outgoing claim typer Attributes to outgoing claim typer Attributes (select or type to re) v	Actions Relying Party Trusts Add Relying Party Trust Add Non-Claims-Aware Relying Part View Ide - NameID X DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be Outgoing Claim Type (Select or type to add more) ud v
Add F	Nule Edt Rule Remove Rule					Activate Windows Go to System in Control Panel to activate Windows.

새로 고침 로그인이 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

SAML SSO and UCM/LDAP ▼ None SAML SSO authentication UCM/LDAP basic authentication SAML SSO and UCM/LDAP

- 인증 경로가 "SAML SSO 인증"으로 설정된 경우 SSO가 활성화된 Unified CM 클러스터를 사용 하는 Jabber 클라이언트만 이 Expressway에서 MRA를 사용할 수 있습니다.이는 SSO 전용 컨 피그레이션입니다.
- 모든 IP 전화, 모든 TelePresence 엔드포인트 및 SSO에 대해 구성되지 않은 Unified CM 클러 스터에 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 세 트에 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 고치 는 방법(Unified CM, IM&P, Unity 및 Expressway 서비스)을 제공합니다. 이 흐름은 리디렉션을 기 반으로 하므로 클라이언트가 사용자가 제어하는 HTTP 사용자 에이전트(웹 브라우저)와 상호 작용 할 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 보 기가 나타나 자신을 인증할 수 있습니다.(Kerberos 인증은 웹 페이지를 표시하지 않는 예입니다.) 암시적 부여 흐름과 달리, 성공적인 인증 코드 부여 플로우는 OAuth 서버에서 웹 브라우저에 "Authorization Code"를 발급하게 됩니다.이 코드는 일회성 단기간 고유 코드로, 웹 브라우저에서 클 라이언트로 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 사용 된 클라이언트 암호는 권한 부여 서비스에서 등록 및 인증 된 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 사용 하여 연결을 신뢰할 수 있습니다.(Cisco 액세스 토큰은 기본적으로 수명 60분으로 설정)

토큰 새로 고침:이 토큰은 권한 부여 서버에서 다시 발급됩니다.클라이언트는 액세스 토큰이 만료 되었거나 만료될 때 클라이언트 암호와 함께 이 토큰을 권한 부여 서버에 제공합니다.새로 고침 토 큰이 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 얻 으려면 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 클라이언트 에 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 요청 합니다.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 버 전 3.0이 Kerberos 프로토콜과 NTLM(NT LAN Manager) 프로토콜을 모두 지원하는지 확인하십시 오.

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

Nanager								
€ Sites ► Default Web Sites	e >				0 🖂 🔂 10 -			
File View Help								
Connections				Alerts				
Q, - 🔒 🖄 🔗	Authentication			Click here to	learn how to			
Start Page	Group by: No Grouping			Protection.	tended			
- Application Pools	Name	Status	Response Type	Actions				
⊿ - 🙆 Sites	Anonymous Authentication	Enabled		Disable				
Default Web Site	Forms Authentication	Disabled	HTTP 302 Login/Redir	Advanced Se	ttings			
	Windows Authentication	Enabled	HTTP 401 Challenge	Providers				
			Providers	? X				
	Enable	d Providers:						
	Negot	iate		Move Up				
				Move Down				
				Remove				
	< Select	a provider from the	list of available providers and	click Add				
	Features View 📓 to add	it to the enabled pr	oviders.	CIICK AGO				
Configuration: 'localhost' applicationHost.config , <loca< th=""><td>ation path="Default W</td><td>le Providers</td><td></td><td></td><td>•<u>1.</u>;</td></loca<>	ation path="Default W	le Providers			• <u>1.</u> ;			
			~	Addition	12.D0			
				Go to Svs	m in Control P			
				Windows.	Windows Se			
			OK	Cancel				

Microsoft Internet Explorer 구성

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

Internet O	ptions					? <mark>×</mark>		
General	Security	Privacy	Content	Connection	s Programs	Advanced		
Setting	s ———							
	 Do not submit unknown addresses to your auto-search provide a security Allow active content from CDs to run on My Computer* Allow active content to run in files on My Computer* Allow software to run or install even if the signature is involved to check for publisher's certificate revocation Check for server certificate revocation* Check for signatures on downloaded programs Do not save encrypted pages to disk Empty Temporary Internet Files folder when browser is clc Enable DOM Storage Enable Integrated Windows Authentication* 							
₹	kes effect a	fter vou	restart Inte	ernet Explore	Þr	•		
*Takes effect after you restart Internet Explorer Restore advanced settings Resets Internet Explorer settings to their default condition. You should only use this if your browser is in an unusable state.								
			OK		Cancel	Apply		

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