# Configurazione di SAML SSO su Cisco Unified Communications Manager con ADFS 3.0

# Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Controllo preliminare della configurazione **Record A** Record puntatore (PTR) I record SRV devono essere installati per i servizi di rilevamento Jabber Configurazione iniziale di ADFS3 Configurare SSO su CUCM con ADFS **Configurazione LDAP** Metadati CUCM Configura componente ADFS Metadati IDP Configura SSO su CUC Metadati CUC Configura SSO su Expressway Importa metadati in Expressway C Esporta metadati da Expressway C Aggiungi un trust della relying party per Cisco Expressway-E OAuth con accesso aggiornato Percorso di autenticazione Architettura SSO Flusso di login in locale Flusso di accesso MRA OAuth Token di accesso/aggiornamento Il flusso di concessione del codice di autorizzazione OAuth è migliore **Configura Kerberos** Seleziona autenticazione di Windows ADFS supporta sia Kerberos che NTLM Configurare Microsoft Internet Explorer Aggiungi URL ADFS in Protezione > Aree Intranet > Siti Aggiungi nomi host CUCM, IMP e Unity a Protezione > Siti attendibili Autenticazione utente SSO accesso Jabber Risoluzione dei problemi Internet Explorer

<u>Siti da aggiungere a IE</u> <u>Problema non sincronizzato</u> <u>Revoca un token</u> <u>File bootstrap</u> Errore SSO dovuto a MSIS7066

# Introduzione

In questo documento viene descritto come configurare Single Sign-On con Active Directory Federation Service (ADFS 3.0) con l'utilizzo di Windows 2012 R2 su prodotti Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (CUC) ed Expressway. In questo documento sono inoltre illustrati i passaggi per configurare Kerberos.

# Prerequisiti

# Requisiti

Cisco raccomanda la conoscenza dei prodotti Single Sign-On (SSO) e Windows.

# Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CUCM 11.5
- CUC 11.5
- Expressway 12
- Server Windows 2012 R2 con questi ruoli:
  - Servizi certificati Active Directory
  - Active Directory Federation Services

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Controllo preliminare della configurazione

Prima di installare ADFS3, è necessario che questi ruoli server esistano già nell'ambiente:

·Controller di dominio e DNS

•Tutti i server devono essere aggiunti come record A insieme al relativo record puntatore (un tipo di record DNS che risolve un indirizzo IP in un dominio o un nome host)

# **Record A**

In fhlab.com. sono stati aggiunti gli host cmpubhcsc, cmsubhcsc, cucpubhcsc, cucsubhcsc,



# Record puntatore (PTR)

A DNS	Name	Туре	Data	Timestamp
⊿ AD	(same as parent folder)	Start of Authority (SOA)	[14], ad.fhlab.com., hostmaster.fhlab.co	static
a 📋 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
D udp	10.89.228.150	Pointer (PTR)	impsubhcsc.fhlab.com.	static
DomainDnsZones	10.89.228.151	Pointer (PTR)	cucpubhcsc.fhlab.com.	static
A PorestUnsZones	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
Peverre Lookup Zoper	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

I record SRV devono essere installati per i servizi di rilevamento Jabber

L DNS	Name	Туре	Data	Т	imestamp	
a 🗎 AD	cisco-uds	Service Location (SRV)	[0][0][8443] cmsubhcsc.fhl	ab.com. st	tatic	
a 🔛 Forward Lookup Zones	cisco-uds	Service Location (SRV)	[0][0][8443] cmpubhcsc.fh	lab.com. st	tatic	
[] _msdcs.fhlab.com	cuplogin	Service Location (SRV)	[0][0][8443] impsubhcsc.fh	lab.com. st	tatic	
⊿ 👸 fhlab.com	cuplogin	Service Location (SRV)	[0][0][8443] imppubhcsc.fh	lab.com. st	tatic	
D [] _msdcs	gc	Service Location (SRV)	[0][100][3268] ad.fhlab.com	n. 5/	/12/2020 10:00:00 AM	
b iii _sites	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	
þudp	_Idap	Service Location (SRV)	[0][100][389] ad.fhlab.com			
DomainDnsZones					_cisco-uds Properties	? X
A ForestUnsZones						
psites				Service Location	(SRV) Security	
_tcp				Demain	Polah com	
229 90 10 in addr arm				Domain:	1100.0011	
Taust Points				Service:	cisco-uds	~
Conditional Forwarders						
b Fill Global Logs				Protocol:	_tcp	~
				Priority:	0	
				Weight:	0	
				Post ou mbar:	8443	
				Port noniber.		
				Host offering this	service:	
				cmpubhcsc.fhla	b.com.	

 CA radice (supponendo che i certificati siano firmati dall'autorità di certificazione dell'organizzazione)

Ènecessario creare un modello di certificato basato sul modello di certificato del server Web, il primo viene duplicato, rinominato e nella scheda Estensioni i Criteri di applicazione vengono modificati aggiungendo un criterio di applicazione per l'autenticazione client. Questo modello è necessario per firmare tutti i certificati interni (CUCM, CUC, IMP ed Expressway Core) in un ambiente LAB. La CA interna può inoltre firmare le richieste di firma del certificato (CSR) di Expressway E.



Ènecessario emettere il modello creato per poter firmare CSR.



Nel sito Web del certificato CA selezionare il modello creato in precedenza.

Microsoft Active	Directory Certificate Services fhlab-AD-CA	
Submit a Cert	tificate Request or Renewal Request	
To submit a sa Web server) in	ved request to the CA, paste a base-64-encoded Cl the Saved Request box.	CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external sour
Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	8V8mWY/9kjhqfnpeBzAAW++tolGzBjnvqaT8StWM LA0dphF6LrurU0eY2KLwKLmKlft7aSy483yCsm0v1 OWQPZoLb3bS80ziW7fgEFWSaCg567DMOQ8Fkzt5N lOy/Ip6oDzTdZE9w2p8rK3YxccbypovSt0ijIirh AM/Gjnz0 END CERTIFICATE REQUEST	
Certificate Templ	late:	
Additional Attribu	✓ User Basic EFS 4 Administrator EFS Recovery Agent Web Server	
Additional Attributes:	✓ User Basic EFS Administrator EFS Recovery Agent Web Server	

Subordinate Certification Authority

CUCM, IMP e CUC Multi-Server CSR devono essere generati e firmati dalla CA. Lo scopo del certificato deve essere tomcat.

Generate Certificate Signing	Request	
🖳 Generate 🛛 🖳 Close		
Status		
Warning: Generating a	new CSR for a specific certificate type will overwrite the	e existing CSR for that type
Generate Certificate Signin	g Request	
Certificate Purpose**	tomcat 🗸	
Distribution*	Multi-server(SAN)	
Common Name*	cmpubhcsc-ms.fhlab.com	
Subject Alternate Names (	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
Key Type** Key Length* Hash Algorithm*	RSA 2048	Add

Il certificato radice CA deve essere caricato in Tomcat Trust e il certificato firmato in Tomcat.

cisco For C	co Unified Operating	System Ad	ministra	tion		Navi	oation Cisco Unified OS Administration  V sadmin Search Documentation About Log
Show - Settings	<ul> <li>Security          <ul> <li>Software Upgrades</li> </ul> </li> </ul>	• Services • Hel	, <del>v</del>				
ertificate List							
Al Committe Cart of	En links Contraction	u data 🛐 carro	4.000				
Oenerate Sen-s	igned 20 option Certificate/Certifica	te chan 60 Gener	INE COK				
<ol> <li>7 records fou</li> </ol>	und						
-							
Certificate List	(1 - 7 of 7)						Rows per Page 50 🗸
Find Certificate Lis	t where Certificate v begin	ns with           torncat		Find Clear Filter	4 -		
Carl Barde A	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
lomcat	cmoubhcsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/18/2022	Certificate Signed by fhlab-AD-CA
omcat-ECDSA	cmoubhcsc-EC.mlab.com	Self-signed	EC	cmpubhcsc.thlab.com	cmpubhcsc-EC.thlab.com	04/02/2025	Self-signed certificate generated by system
omcat-trust	imppublicsc-EC.fhlab.com	Self-signed	EC	imppublicsc.fhlab.com	imppublicsc-EC.fhlab.com	04/02/2025	Trust Certificate
omcat-trust	cmsubhcsc-EC.fhlab.com	Self-signed	EC	cmsubhcsc.fhlab.com	cmsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
omcat-trust	impsubhcsc-EC.fhlab.com	Self-signed	EC	impsubhcsc.fhlab.com	impsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
amost tourt	emashhara 20 filsh com	Eall signed	50	come debases (black come	consultance EC faish com	04/03/3035	Tool Cadificate
omcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate
Generate Self-si	igned Upload Certificate/Certifi	icate chain Gene	rate CSR				
-							
Certificate List	(1 - 6 of 6)						Rows per Page 50
Find Certificate Lis	t where Certificate v begin	ns with $\sim$ torncet		Find Clear Filter	ф —		
Contificate *	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
omcat	cucpublicsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/28/2022	Certificate Signed by fhlab-AD-CA
		A		and the second state and			and the second sec
omcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate
	The second s	CH Agrico	1000	Here server (own)	ITTO AD CA		- A chinete Mindours
omcat-trust	cucsubhcsc-EC.fhlab.com	Self-signed	EC	cucsubhcsc.fhlab.com	cucsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate Le VVIII GOWS

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

• IIS

In caso contrario, la sezione procederà all'installazione di questi ruoli. In caso contrario, ignorare questa sezione e procedere direttamente al download di ADFS3 da Microsoft.

Dopo l'installazione di Windows 2012 R2 con DNS, innalzare il server a controller di dominio.

La prossima operazione sarà installare Servizi certificati Microsoft.

Passare a Server Manager e aggiungere un nuovo ruolo:



Selezionare il ruolo Servizi certificati Active Directory.

2	Add Roles and Features Wizard	<b>_</b> X
Select server rol	es	DESTINATION SERVER AD.fnlab.com
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection	Active Directory Certificate Services (4 of 6 installed)	<ul> <li>Active Directory Certificate Services (AD CS) is used to</li> </ul>
Server Roles	Certification Authority (Installed)	create certification authorities and related role services
Features	Certificate Enrollment Policy Web Service (Installed)	variety of applications.
Confirmation	Certificate Enrollment Web Service (Installed)	
Results	Certification Authority Web Enrollment (Installed)	
	Network Device Enrollment Service	
	Online Responder	
	Active Directory Domain Services (Installed)	=
	✓ Active Directory Federation Services (Installed)	
	Active Directory Lightweight Directory Services	
	Active Directory Rights Management Services	
	Application Server	
	DHCP Server	
	✓ DNS Server (Installed)	
	Fax Server	
	File and Storage Services (2 of 12 installed)	
	Hyper-V	
	Network Policy and Access Services	
	Print and Document Services	~
		( Depring   Next)
		< Previous Next > Install Cancel

E distribuire questi servizi - Servizio Web di informazioni sulle registrazioni di certificati di Autorità di certificazione. Dopo aver installato questi due ruoli, configurarli e quindi installare **Servizio Web di registrazione certificati** e **Registrazione Web Autorità di certificazione**. Configurarle.

Quando si installa l'Autorità di certificazione, verranno inoltre aggiunti i servizi ruolo e le funzionalità aggiuntivi necessari, ad esempio IIS.

A seconda della distribuzione, è possibile selezionare Enterprise o Standalone.

Add Roles Wizard		×
Specify Setup Ty	ре	
Before You Begin Server Roles AD CS Role Services Setup Type CA Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Veb 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	

Per Tipo CA, è possibile selezionare CA radice o CA subordinata. Se nell'organizzazione non sono già in esecuzione altre CA, selezionare **CA radice**.

Add Roles Wizard		×
Specify CA Type		
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	<ul> <li>A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKQ). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.</li> <li>Root CA Select this option if you are installing the first or only certification authority in a public key infrastructure.</li> <li>Subordinate CA Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.</li> </ul>	
	More about public key infrastructure (PKI)	
	< Previous Next > Install Cancel	

Il passaggio successivo consiste nella creazione di una chiave privata per la CA.



Questo passaggio è necessario solo se si installa ADFS3 in un Windows Server 2012 separato.

Dopo aver configurato la CA, è necessario configurare i servizi ruolo per IIS. Questa operazione è necessaria per la registrazione Web sulla CA. Per la maggior parte delle distribuzioni ADFS, è necessario un ruolo aggiuntivo in IIS, fare clic su **ASP.NET** in Sviluppo applicazioni.



In Server Manager fare clic su **Server Web > IIS**, quindi fare clic con il pulsante destro del mouse su **Sito Web predefinito**. È necessario modificare il binding per consentire anche HTTPS oltre a HTTP. Questa operazione viene eseguita per supportare HTTPS.



Selezionare Modifica associazioni.

<i>8</i> ]	Interne	t Informatio	n Services	(IIS) Manage	er		- 0 X
🕞 🕒 🖌 AD 🔸 Sites 🔸 Default Web Si	te 🕨						📅 🖂 🔂 i 🕖 •
File View Help							
Connections	0.0	four de la de la de	Cite He				Actions
🔍 • 🔜 🖄 😣	e De	erault web	Site Ho	me			🔉 Explore
Start Page	Filter		- 7 Go -	Show All	Group by:		Edit Permissions
AD (FHLAB\administrator)	ASP.NET					A A	Edit Site
A - 😺 Sites	- E		404	9	Ę.		Bindings Basic Settings
Explore Edit Permissions		.NET Compilation	NET Error Pages	.NET Globalization	.NET Profile		View Applications View Virtual Directories
Add Application		- internet - 1	- <u>6</u> 2	鮰	ab		Manage Website
Add Virtual Direc	tory s	.NET Trust	.NET Users	Application	Connection		🗢 Restart
Edit Bindings		E CEVED	<b>e</b>	ettings	Junings		Start
Manage Website	•		10K	8÷			Browse Website
2 Refresh	9	/ Pages and Controls	Providers	Session State	SMTP E-mail		Browse *:80 (http)
× Remove							Browse *:443 (https)
Rename			A				Advanced Settings
Switch to Conter	nt View		P	0	11 <u>1</u> 2	v	Configure
	Features Vi	iew 💦 Conten	t View				Limits
Ready							• <u>1.</u> ;

Aggiungere una nuova associazione sito e selezionare **HTTPS** come tipo. Per il certificato SSL, selezionare il certificato server che deve avere lo stesso FQDN del server AD.

<b>e</b> j			Intern	et Information	n Services (IIS) Manage	er -
🛞 💿 😜 🖌 AD 🕨	Sites 🕨 I	Default Web Site	•			
File View Help						
Connections				Site	Bindings	? X
<ul> <li>Start Page</li> <li>AD (FHLAB\admini</li> <li>Application Poc</li> <li>Sites</li> <li>Default Web</li> </ul>	Type http https	Host Name Type: https Host name: Require S SSL certifica fhlab-AD-Co Not selected fhlab-AD-Co AD.fhlab.com	Port 80 442 I v ierver Name te: A I A m	IP Address * Edit P address: All Unassigned * Indication	Binding Informa t Site Binding Por 443	Add  Fdit  X  Cancel FX

Tutti i ruoli prerequisiti sono installati nell'ambiente, quindi è possibile procedere con l'installazione di ADFS3 Active Directory Federation Services (in Windows Server 2012).

Per il ruolo Server, passare a Server Manager > Gestisci > Aggiungi ruoli server e funzionalità e quindi selezionare Active Directory Federation Services se si installa l'IDP nella rete del cliente, nella LAN privata.

i.	Server Manager	- <b>-</b> X
<b>€</b> ∋•	Server Manager • Dashboard • 🕑 I 🚩	Manage Tools View Help
Dashboard	WELCOME TO SERVER MANAGER	Add Roles and Features Remove Roles and Features Add Servers
Local Server	Configure this local server	Create Server Group Server Manager Properties
III AD CS III AD DS 과 AD FS	QUICK START 2 Add roles and features	

	Add Roles and Features Wizard	_ 0
elect server roles		DESTINATION SERVER AD filab.com
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection	La Martine Directory Castificate Services (A of 6 installs A	Active Directory Federation Services
Server Roles	Active Directory Certificate Services (4 of 6 Installe	(AD FS) provides simplified, secured
Features	Active Directory Domain Services (Installed)	identity federation and Web single sign-on (SSO) capabilities, AD FS
	Active Directory Lightweight Directory Services	includes a Federation Service that
	Active Directory Biphts Management Services	enables browser-based Web SSO.
	Application Server	
	DHCP Server	
	DNS Server (Installed)	
	Fax Server	
	File and Storage Services (2 of 12 installed)	
	Hyper-V	
	Network Policy and Access Services	
	Print and Document Services	
	Remote Access	
	V	
	< II >	

Al termine dell'installazione, sarà possibile aprirla dalla barra delle applicazioni o dal menu Start.

<b>9</b> 0	AD FS	_ <b>_</b> X
Sile Action View Window Help		- 8 ×
AD FS	AD FS	Actions
ADIS	AD FS provides single-sign on (SSO) access for client computers. Learn More Configuring Trust Relationships Configuring Authentication Policies Troubleshooting AD FS AD FS Help	Actions AD FS Add Relying Party Trust Add Claims Provider Trust Add Attribute Store Edit Federation Service Properti Edit Published Claims Revoke All Proxies View New Window from Here Refresh Help
	Activate	Windows

# Configurazione iniziale di ADFS3

Questa sezione consente di installare un nuovo server federativo autonomo, ma può essere utilizzata anche per installarlo in un controller di dominio

Selezionare **Windows** e digitare **Gestione ADFS** per avviare la console Gestione ADFS, come illustrato nell'immagine.



Selezionare l'opzione **Configurazione guidata server federativo ADFS 3.0** per avviare la configurazione del server ADFS. Questi screenshot rappresentano gli stessi passaggi in ADFS 3.

p AD FS 2.0 Federation Ser	ver Configuration Wizard
Welcome	
Steps	Welcome to the AD FS 2.0 Federation Server Configuration Wizard
<ul> <li>Welcome</li> <li>Select Deployment Type</li> <li>Federation Service Name</li> <li>Summary</li> <li>Results</li> </ul>	This wixed 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. <b>O fracte a new Federation Service</b> Belet this option to set up either a stand-alone federation server or the first server in a federation server farm. <b>O Ad a federation server to an existing Federation Service</b> Belet this option to join this computer to an existing federation server farm.
	< <u>Previous</u> <u>Next&gt;</u> Cancel <u>H</u> elp

Selezionare Crea nuovo servizio federativo e fare clic su Avanti.

AD FS 2.0 Federation Ser	ver Configuration Wizard
Select Stand-Alone or	r Farm Deployment
Step*	You can create either a stand-alone federation server for evaluation purposes or a small production
Welcome	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	O New federation server farm
Results	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 farm. Later, you can scale out this farm by adding more federation servers.
	To create a federation server farm, 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 SPN (for the service account), such as an account that is a member of the Domain Admins group.
	⊙ 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 environment. If you select this option, you will not be able to add more servers to create a farm.
	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
	< Previous Next > Cancel Help

Selezionare Server federativo autonomo e fare clic su Avanti, come illustrato nell'immagine.

M AD FS 2.0 Federation Serve	er Configuration Wizard		×
Specify the Federation	Service Name		
Steps  Welcome Select Deployment Type Federation Service Name	This wizard determines the Federation Service name fr Default Web Site. If the wizard cannot determine the f must select a certificate. Select the certificate and/or port, and then click Next. SSL certificate:	rom the Subject field of the SSL certificate for the Federation Service name from the SSL settings, you Port:	
<ul> <li>Summary</li> <li>Results</li> </ul>	ad0a.identitylab.us         Federation Service name:         ad0a.identitylab.us         what kind of certificate do I need?	<ul> <li>View</li> <li>443 *</li> </ul>	
	< Previo	Lς us Next> Cancel Help	

In Certificato SSL selezionare il certificato autofirmato dall'elenco. Il nome del servizio federativo verrà popolato automaticamente. Fare clic su **Next** (Avanti).

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

Verificare le impostazioni e fare clic su **Avanti** per applicarle.

Step:	The following settings are being contigured		
<ul> <li>Welcome</li> <li>Select Deployment Type</li> <li>Federation Service Name</li> <li>Summary</li> <li>Results</li> </ul>	Component         Install Windows Internal Database         Install Windows Internal Database <td< th=""><th>Status         Configuration finished         Nonfiguration finished         Configuration finished</th><th></th></td<>	Status         Configuration finished         Nonfiguration finished         Configuration finished	

Verificare che tutti i componenti siano stati completati correttamente e fare clic su **Chiudi** per terminare la procedura guidata e tornare alla console di gestione principale. L'operazione potrebbe richiedere alcuni minuti.



ADFS è ora effettivamente abilitato e configurato come provider di identità (IdP). Successivamente, è necessario aggiungere CUCM come Relying Partner attendibile. Prima di eseguire questa operazione, è necessario eseguire alcune operazioni di configurazione in Amministrazione CUCM.

# Configurare SSO su CUCM con ADFS

# **Configurazione LDAP**

Il cluster deve essere integrato con LDAP con Active Directory e prima di procedere è necessario configurare l'autenticazione LDAP. Passare alla **scheda Sistema > Sistema LDAP** come mostrato nell'immagine.

# LDAP System Configuration

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

Quindi, passare alla **scheda Sistema > LDAP Directory**.

LDAP Directory	
🔚 Save 🗙 Delete 🗋 Copy 🕻	Perform Full Sync Now 🕂 Add New
Status Status: Ready	
LDAP Directory Information	
LDAP Configuration Name*	LDAP1
LDAP Manager Distinguished Name*	fhlab\administrator
LDAP Password*	•••••
Confirm Password*	•••••
LDAP User Search Base*	cn=users,dc=fhlab,dc=com
LDAP Custom Filter for Users	< None >
Synchronize*	<ul> <li>Users Only O Users and Groups</li> </ul>
LDAP Custom Filter for Groups	< None >
LDAP Directory Synchronization S	Schedule
Perform Sync Just Once	
Perform a Re-sync Every*	7 DAY 🗢
Next Re-sync Time (YYYY-MM-DD hh:	:mm)* 2020-05-24 00:00

Standard User Fields To Be Synchronized					
Cisco Unified Communications Manager User Fields	LDAP Attribute	Cisco Unified C	communications Ma	nager 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	r		homephone
Mobile Number	mobile	Pager Number	r		pager
Directory URI	mail 🖸	Display Name			displayName
LDAP Server Information – Host Name or IP Addre	ss for Server <sup>*</sup>		LDAP Port*	Use TLS	
10.89.228.226			389		
Add Another Red	undant LDAP Server				
Save Delete Co	Dy Derform Full Sync Now Add New				

Dopo la sincronizzazione degli utenti di Active Directory con CUCM, è necessario configurare l'autenticazione LDAP.

cis	0	Cisco L	Unified Con		dministra	tion								Navigation	Cisc	o Unified CM Ad	iministratic	n Abert	✓ Go
System	÷	Call Routing *	Media Resou	urces *	Advanced Featur	es v D	evice +	Application •	User Mar	agement 🕶	Bulk Administration	• Help ▼	-			See of Secon			
LDAP	Aut	hentication																	
🔒 s	ave																		
- Statu																			
1	Statu	s: Ready																	
LDAP	Aut	hentication	for End Use	ers —															
Øu:	e LC	AP Authentica	ation for End	Users															
LDAP	Man	ager Distingui	ished Name*	fhlab\4	dministrator					]									
LDAP	Pasi	*browd		•••••		•••••		•••••		]									
Confi	rm P	assword*		•••••		•••••	•••••	•••••		]									
LDAP	User	r Search Base		cn=use	rs,dc=fhlab,dc=	com				]									
LDAP	Ser	ver Informa	tion																
			Но	ost Name	or IP Address f	or Serve				LDAP Por	" Use TLS								
10.4	19.22	28.226								389									
Ad	Id Ar	other Redund	ant LDAP Se	erver															

Un utente finale in CUCM deve disporre di determinati gruppi di controllo di accesso assegnati al proprio profilo utente finale. ACG è una versione standard di CCM Super Users. L'utente verrà utilizzato per eseguire il test dell'SSO quando l'ambiente è pronto.

End Use	er Configuration				Related Links: Ba	ck to Find List Users	√ Go
Sav	e 🗙 Delete 🕂 Add Ne	w					
Confirm MLPP Pr	n MLPP Password recedence Authorization Lev	el Default			~		
CAPF I	nformation						
Associa	ted CAPF Profiles			∧ ✓ <u>View D</u>	etails		
Permis	sions Information						
Groups	Standard CCM End Users Standard CCM Super Users Standard CTI Allow Contro Standard CTI Enabled Standard AXL API Access Standard Admin Rep Tool A Standard CCM Admin User Standard CCM End Users Standard CCMADMIN Adm	Admin s inistration	View Details	Add to A Remove	ccess Control Group from Access Contro	) I Group	
Conference Enable Meeting Attende	ence Now Information — ble End User to Host Conference Number 1001 es Access Code	ence Now			]		
Save	Delete Add New						

### Metadati CUCM

In questa sezione viene illustrato il processo per l'editore CUCM.

La prima attività consiste nell'ottenere i metadati CUCM, in modo da poter individuare l'URL; https://<CUCM Pub FQDN>:8443/ssosp/ws/config/metadata/sp o può essere scaricato dalla scheda Sistema > SAML Single Sign-On. Questa operazione può essere eseguita per nodo o a livello di cluster. Preferibile eseguire questa operazione a livello di cluster.

SAML Single Sign-On							
SSO Mode							
Cluster wide (One met	tadata file per clu	ster. Requires multi-serv	ver Tomcat certificate)				
O Per node (One metada	ata file per node)						
🗙 Disable SAML SSO 🕃	Export All Metadal	a 🔞 Update kdP Metada	ata File 🥜 Fix All Disabled Servers				
RTMT is enabled for     SAML SSO enabled	SSO. You can cha	nge SSO for RTMT <u>here</u>	ь.				Pour our Page 50
RTMT is enabled for     SAML SSO enabled  SAML Single Sign-On Server Name	SSO. You can cha (1 - 4 of 4) SSO Status	nge SSO for RTMT here	Last Matadata Import	Evnort Metadata	Last Metadata Export	550 Test	Rows per Page 50
RTMT is enabled for     SAML SSO enabled  SAML Single Sign-On Server Name cmpubhcsc.fhlab.com	SSO. You can cha (1 - 4 of 4) SSO Status SAML	nge SSO for RTMT <u>here</u> Re-Import Metadata N/A	Last Metadata Import April 20, 2020 2:00:57 PM PDT	Export Metadata	Last Metadata Export April 18, 2020 8:05:38 PM PDT	SSO Test Passed - April 20, 2020 2:02:15 PM PDT	Rows per Page 50 V
RTHT is enabled for     SAML SSO enabled      SAML Signe Sign-On     Server Name cmpubhcsc.fhlab.com cmsubhcsc.fhlab.com	SSO. You can cha (1 - 4 of 4) SSO Status SAML SAML	nge SSO for RTMT here Re-Import Metadata N/A IdP	Last Metadata Import April 20, 2020 2:00:57 PM PDT April 20, 2020 2:00:57 PM PDT	Export Metadata	Last Metadeta Export April 18, 2020 8:05:38 PM PDT April 18, 2020 8:05:37 PM PDT	550 Test Passed - April 20, 2020 2:02:15 PM PDT Passed - April 20, 2020 1:49:45 PM 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     imppubhcsc.fhlab.com	SSO. You can cha (1 - 4 of 4) SSO Status SAML SAML SAML	Re-Import Metadata N/A 1dP 1dP	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 File File File File	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

Salvare i dati localmente con un nome significativo, ad esempio sp\_cucm0a.xml, che sarà necessario utilizzare in seguito.

### Configura componente ADFS

Tornare alla console di gestione di AD FS 3.0.



Fare clic su Aggiunta guidata attendibilità componente.

<b>\$</b>	Add Relying Party Trust Wizard
Welcome	
<ul> <li>Steps</li> <li>Welcome</li> <li>Select Data Source</li> <li>Configure Multi factor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	<section-header>         Welcome to the Add Relying Party Trust Wizard         This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and autorization decisions.         The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party error uses for issuing claims to the relying party atter you complete the wizard.</section-header>

Fare clic su Start per continuare.

Selezionare il file XML di metadati **federationmedatada.xml** salvato in precedenza e fare clic su **Avanti**.

<b>\$</b>	Add Relying Party Trust Wizard
Select Data Source	
<ul> <li>Steps</li> <li>Welcome</li> <li>Select Data Source</li> <li>Configure Multifactor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	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 online or on a local network.         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:         Exture data about the relying party manually         Use this option to manually input the necessary data about this relying party organization.
	< Previous Next > Cancel em i

Utilizzare **CUCM\_Cluster\_Wide\_Relying\_Party\_trust** come nome visualizzato e fare clic su **Avanti**.

<b>\$</b>	Add Relying Party Trust Wizard	¢
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
<ul> <li>Welcome</li> </ul>	Display name:	
Select Data Source	CUCM_Cluster_Wide_Relying_Party_trust	
Specify Display Name	Notes:	
Configure Multi-factor Authentication Now?		]
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
<ul> <li>Ready to Add Trust</li> </ul>		_
<ul> <li>Finish</li> </ul>		1
	< Previous Next A ctive (Caripel/in)	de

Selezionare la prima opzione e fare clic su Avanti.

<b>\$</b>	Add Relying Party Trust Wizard	x	
Steps	Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is require	dif	
<ul> <li>Welcome</li> </ul>	there is a match for any of the specified requirements.		
Select Data Source	Midifactor Aitheotication (Global		
Specify Display Name	Mathactor Adhenication Global Settings	-	
Configure Multi-factor Authentication Now?	Requirements Users/Groups Not configured		
Choose Issuance     Authorization Bules	Device Not configured		
Ready to Add Trust	Location Not contigured		
<ul> <li>Finish</li> </ul>			
	<ul> <li>I do not want to configure multifactor authentication settings for this relying party trust at this time.</li> <li>Configure multifactor authentication settings for this relying party trust.</li> <li>You can also configure multifactor authentication settings for this relying party trust by navigating to Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u>.</li> </ul>	the	
	< Previous Next > Ct Va (Caricel	inde	

Selezionare **Permetti a tutti gli utenti di accedere a questo componente** e fare clic su **Avanti**, come mostrato nell'immagine.

<b>\$</b>	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	<ul> <li>Permit all users to access this relying party</li> </ul>		
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?	Denvial users access to this relying party		
<ul> <li>Choose Issuance Authorization Rules</li> </ul>	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.		
<ul> <li>Ready to Add Trust</li> </ul>			
<ul> <li>Finish</li> </ul>	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 Va (Canbel in do		

Esaminare la configurazione e fare clic su Next (Avanti), come mostrato nell'immagine.

<b>\$</b>	Add Relying Party Trust Wizard
Ready to Add Trust	
<ul> <li>Steps</li> <li>Welcome</li> <li>Select Data Source</li> <li>Specify Display Name</li> <li>Configure Multi-factor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	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 Avext yate Weater Vicancel V

Deselezionare la casella e fare clic su Chiudi.

<b>\$</b> 1	Add Relying Party Trust Wizard
Finish	
<ul> <li>Steps</li> <li>Welcome</li> <li>Select Data Source</li> <li>Specify Display Name</li> <li>Configure Multi-factor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	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

Con il pulsante secondario del mouse, selezionare l'**attendibilità componente** appena creata e **modificare la** configurazione **delle regole attestazione** come mostrato nell'immagine.

<b>V</b>		AD FS		
💱 File Action View Windo	w Help			
📔 AD FS	Relying Party Trusts			
<ul> <li>Service</li> <li>Trust Relationships</li> <li>Claims Provider Trusts</li> <li>Relying Party Trusts</li> <li>Attribute Stores</li> <li>Authentication Policies</li> </ul>	Display Name Device Registration Service CUCM_Cluster_Wide Relving Party trust CUC_Cluster_W ExpwyC Edit Claim Rules Disable Properties Delete Help	Enabled Type Yes WS-Trust / SAI Yes WS-Trust / SAI deration Metadata	ML / WS-Federation L / WS-Federation L / WS-Federation L / WS-Federation	Identifier um:ms-drs:ad.fhlab.com cmpublicsc.fhlab.com cucpublicsc.fhlab.com fhlab.com-500D0F4107D76E57

Fare clic su Add Rule (Aggiungi regola) come mostrato nell'immagine.

👒 Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party 💻 🗖 🗙
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules
The following transform rules specify the claims that will be sent to the relying party.
Order Rule Name Issued Claims
Add Rule Edit Rule Remove Rule
OK Canal Andr
UK Cancel Apply

Selezionare Invia attributi LDAP come attestazioni e fare clic su Avanti.

<b>\$</b>	Add Transform Claim Rule Wizard	X
Select 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	s
Choose Rule Type		
<ul> <li>Contigure Claim Rule</li> </ul>	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 create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumbe Active Directory attributes and then send those values as two different outgoing claims. This rule may also 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.	н аг о
	< Previous Next > Cancel	

Configurare i seguenti parametri:

Nome regola attestazione: IDNome

Archivio attributi: Active Directory (fare doppio clic sulla freccia del menu a discesa)

Attributo LDAP: Nome-Account-SAM

Tipo attestazione in uscita: uid

Fare clic su **FINISH/OK** per continuare.

Si noti che l'UID non è in lettere minuscole e non esiste già nel menu a discesa. Digitalo.

	Edit R	ule - NamelD				
You ca which t issued t	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 ssued from the rule.					
Claim n	ule name:					
Namel	0					
Rule te	mplate: Send LDAP Attributes as Claims					
Attribut	e store:					
Active	Directory	×				
Mappin	g of LDAP attributes to outgoing claim type	s:				
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)				
•	SAM-Account-Name V	vid 🗸 🗸 vi				
*	~	×				
View	Rule Language	OK Cancel				
		Activat				

Per aggiungere un'altra regola, fare nuovamente clic su Aggiungi regola.

🎙 Edit C	laim Rules for	CUCM_Clust	er_Wid	e_Relying_Party.	_	• X	
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules							
The foll	owing transform rule	s specify the clair	ns that will	be sent to the relying ;	party.		
Order	Rule Name			Issued Claims			
1	NameID			uid			
						-	
Add F	Rule Edit Rul	e Remove	Rule				
			0	K Cancel		Apply	

Selezionare Invia attestazioni utilizzando una regola personalizzata e fare clic su Avanti.

<b>\$</b>	Add Transform Claim Rule Wizard
Select Rule Template	
Steps Ghoose Rule Type Configure Claim Rule	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template. Claim rule template:
	<ul> <li>✓</li> <li>✓</li> <li>✓</li> <li>Claim rule template description:</li> <li>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:</li> <li>Sending claims from a SQL attribute store</li> <li>Sending claims from a custom attribute store using a custom LDAP filter</li> <li>Sending claims only when 2 or more incoming claims are present</li> <li>Sending claims only when an incoming claim value matches a complex pattern</li> <li>Sending claims for use only in later rules</li> <li>Oreating claims for use only in later rules</li> </ul>
	< Previous Next > Cancel

Creare una regola personalizzata denominata Cluster\_Side\_Claim\_Rule.

Copiare e incollare il testo nella finestra della regola direttamente da qui. A volte, le virgolette vengono modificate se modificate in un editor di testo e questo renderà la regola errata quando si esegue il test SSO:

c:[Type ==

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

"cmpubhcsc.fhlab.com");

### Fare clic su **Fine** per continuare.

<b>%</b>	Add Transform Claim Rule Wizard	×
Configure Rule		
Configure Rule Steps Coorse Rule Type Configure Claim Rule	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. Claim rule name: Custor_Side_Claim_Rule Rule template: Send Claims Using a Custom Rule Custom rule: c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount name"] => 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 ] = "urrocasis:namestrc:SML:2.0:nameid=formatites.com/templates.c	^
	<pre>["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequ alifier"] = "http://AD.fhlab.com/adfs/services/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spname qualifier"] = "cmpubhcsc.fhlab.com");]</pre>	~

In ADFS dovrebbero essere definite due regole. Fare clic su **Apply** (Applica), quindi su **OK** per chiudere la finestra delle regole.

🎭 Edit C	laim Rules f	or CUCM_Clust	ter_Wide	e_Relying_Party	- 🗆 X
Issuance '	Transform Rules	Issuance Authoriz	ation Rules	Delegation Authorizatio	n Rules
The folk	owing transform n	les specify the clair	ns that will	be sent to the relying part	у.
Order	Rule Name			Issued Claims	
2	Ouster_Side_O	laim_Rule		<see claim="" rule=""></see>	
Add F	Rule Edt f	Sule	e Rule		•
			0	K Cancel	Apply

CUCM è stato aggiunto come componente attendibile ad ADFS.

9		Service	5				x
File Action View	Help						
💠 🔿 🔝 🖸	2 🕞 🛛 🖬 🕨 🖬 🕪						
Services (Local)	Services (Local)						
	Active Directory Federation	Name	Description	Status	Startup Type	Log On As	^
	Services	Active Directory Certificate Services	Creates, manages, and removes	Running	Automatic	Local System	
		Active Directory Domain Services	AD DS Domain Controller servic	Running	Automatic	Local System	=
	Stop the service	😘 Active Directory Federation Services	Enables Active Directory Federa	Running	Automatic (Delayed Start)	FHLAB\administra	tor
	Including 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	
	Services to issue security tokens.	Application Host Helper Service	Provides administrative services	Running	Automatic	Local System	
		C 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	
		C ASP.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	
		G 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	¥
		<					>
	Extended Standard						
				ļ	Activate Windows		
				A	Activate Windows		

Prima di continuare, riavviare il servizio ADFS. Selezionare Menu Start > Strumenti di amministrazione > Servizi.

## Metadati IDP

Devi fornire a CUCM informazioni sul nostro IdP. Queste informazioni vengono scambiate utilizzando metadati XML. Assicurarsi di eseguire questa operazione sul server in cui è installato ADFS.

Firefox 🔺	
🔔 Untrusted Connection 🛛 🗙 🧶 Mozilla Firefox Start Page 🛛 🗙	+
< 🕙 >s://ad0a.identity 🐎.us/FederationMetadata/2007-06/FederationMetadata 🏠 🔻 😋 💽	- Google 🔎 🖸 - 🦊 🏫
Most Visited Getting Started Suggested Sites Web Slice Gallery	
Opening FederationMetadata.xml	but we can't confirm that your
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? © Open with Internet Explorer (default) © Save File Do this gutomatically for files like this from now on.	an that someone is trying to
OK Cancel Don't add an exception unless you know there's a good reason why the identification. Add Exception	s site doesn't use trusted
	-

Innanzitutto, è necessario connettersi ad ADFS (IdP) utilizzando un browser Firefox per scaricare i metadati XML. Aprire un browser in https://<FQDN ADFS>/FederationMetadata/2007-06/FederationMetadata.xml e SALVARE i metadati in una cartella locale.

Passare alla configurazione CUCM dal **menu** di sistema **> SAML Single Sign-On**.

https://cmpubhcsc.fhlab.com:8443/ccmadmin/samISingleSignOn.do

Tornare alla pagina Amministrazione CUCM e selezionare **SYSTEM > SAML Single Sign-On** (SISTEMA > Single Sign-On SAML).

Firefox *							_ [ ] X
🕮 Find and List User	s	× SAML Single Sign-Cr	×	End and List LDAP Directories	× +		
+ A https://cu	cm0a/comadmin/samiSi	ngleSignOn.do		습 v	C' Scogle	۶ 🖬 -	+ #
cisco For	Cisco Unified Co	CM Administrations	on		Navigation Cisco Unifie admin Search Docum	d CM Administratio entation About	n 💌 Go Logout
System - Cal Ro	uting 👻 Media Reso	urces 👻 Advanced Features	- Device - Applicatio	on 👻 User Management 👻 B	ulk Administration 👻 Help 👻		
SAML Single Si	jn-On						
SAML S	ISO 🔥 Update kil	P Metadata File 👔 Export A	Metadata 🧳 Fix All Dis	sabled Servers			
- Status							
(i) SAML SSO	disabled						
SAML Single S	ign-On (1 - 1 a	of 1)				Rows per Pag	e 50 💌
Server Name	SSO Status	Re-Import Metadata	Last Metadata Imp	ort Export Metadata	Last Metadata Export	SSO TO	est
cucmua	Disabled	ny A	Never	ine rite	Never	Rever	un Test

Selezionare Abilita SSO SAML.

Per confermare l'avviso, fare clic su Continue (Continua).

😔 Reset Warning - Mozilla Firefox 📃 🔲	×
Https://cucmDa/ccmadmin/genericDialogWindow.do?windowtitlekey=genericdialogwindow.windowtitle.ssoenable	2
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	

FederationMetadata.xml salvato in precedenza, come mostrato nell'immagine.

Firefox *						- (D ×
Find and List Users	× SAML Single Sign-On Configuration	× Find and List LDAP Directories	× +			
+ https://cucm0a/comadmin/	samlSingleSignOnConfigurationWizard.do	 	S - Google	۹ (	<b>0- 1</b>	F 🕆
cisco Unifie	ed CM Administration	ad	Navigation Cisco Ur Imin Search Doo	ified CM Administ umentation A	ration 💌	Go Logout
System 👻 Call Routing 👻 Media	a Resources - Advanced Features - Device - A	Application 👻 User Management 👻 Bulk Ad	ininistration 👻 Help 👻			
SAML Single Sign-On Confi	guration					
Next						
Status Ready to import Identity Identity Provider(IdP) Met To configure the trust relation manually obtain the file from I IdP Metadata File Browse. Initiate the Metadata In <sup>11</sup> / <sub>20</sub> This action must be successful Import IdP Metadata Next Cancel	Provider metadata trust file to cluster servers adata Trust File ship between the IdP and your servers, you must the IdP and upload it here. No file selected. <u>He selected</u> I for at least the Publisher before moving on to th	t first obtain trust metadata from your Id e next task in this wizard.	P and import it to you	r servers. You wil	need to	

Selezionare il file XML e fare clic su Apri per caricarlo in CUCM dal menu Download in Preferiti.

😨 File Upload					X
G · Admiris	trator - Downloads				• 🗱 Search Downloads 🗾
Organize - New folder					ji • 🗊 0
* Favortes	Name +	Date modified	Туре	Size	
E Desktop	AdfsSetup	2013/09/09 06:10 FM	Application	24 518 KB	
B Downloads	🖆 FederationMetadata	2013/09/12 02:01 PM	194L Document	32 K8	
2 Recent Places	Spicpick_inst	2013/09/12 11:09 AM	Application	11 129 KB	
Ubraries Documents Music Pictures Videos Computer Metwork					
File	e game: FederationMetadata				All Files

Una volta caricati, fare clic su Importa metadati IdP per importare le informazioni IdP in CUCM. Confermare che l'importazione è riuscita e fare clic su Avanti per continuare.

SAML Single Sign-On Configuration - Windows Internet Explorer		_ 🗆 🗵				
🚱 💿 🗢 🎯 https://10.1.1.100/ccmadmin/s 🔎 💌 😵 Ce 🖻 😏 🁔	🌀 SAML Single Sign-On Configu 🗙 🔛	☆ 🕸				
CISCO Cisco Unified CM Administration For Cisco Unified Communications Solutions	Navigation Cisco Unified CM Administration	Go Logout				
System   Call Routing   Media Resources   Advanced Features   Help	Device      Application      User Management      Bulk Administration	stration 👻				
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, to your servers. You will need to manually obtain the file from the IdP	, you must first obtain trust metadata from your IdP and imp P and upload it here.	iort it				
IdP Metadata File C:\Users\bbanks\Downloads\FederationMetadata	ta.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						

Selezionare l'utente appartenente agli utenti privilegiati CCM standard e fare clic su ESEGUI TEST SSO.

🍅 SAML Single Sign-On Configuration - Mozilla Firefox	-		נ	×
🛛 🖨 📽 https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOnConfigurationWizard3.do?serve	••••	. ⊡	☆	≡
SAML Single Sign-On Configuration				
Test SS0 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 suc	s test ( cessfu	can be Jl.	e run o	n
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	strato	r	
Valid administrator Usernames				
2)Launch SSO test page				
Run SSO Test				
Cancel				

Quando viene visualizzata una finestra di dialogo di autenticazione utente, effettuare il login con il nome utente e la password appropriati.

ۏ Sign lı	n - Mozilla Firefox	-		$\times$
0	https://ad. <b>fhlab.com</b> /adfs/ls/?SAMLRequest=nZJPTwlxEMXvflpN77	CIAi4N	SO •••	≡
				^
	FS			
	Sign in with your organizational account			
	farfar@fhlab.com			
	•••••			
	Sign in			
				~

Se tutto è stato configurato correttamente, dovrebbe essere visualizzato un messaggio che indica che il test SSO è riuscito.



Fare clic su CLOSE e FINISH per continuare.

Le attività di configurazione di base per l'abilitazione dell'SSO su CUCM tramite ADFS sono state completate.

# Configura SSO su CUC

Èpossibile seguire lo stesso processo per abilitare l'SSO in Unity Connection.

Integrazione LDAP con CUC.



Configurare l'autenticazione LDAP.

(←) → ♂ ŵ	🛛 🖨 🕾 https://cucpubhcsc.fhlab.com	m/cuadmin/home.do		··· 🖂 🕁	li\ ⊡ 📽 ≡
cisco Unity Con For Cisco Unified Com	nection Administration			Navigation Cisco Unity Conn farfar Search Docume	ection Administration 🤟 Go ntation   About   Sign Out
Cisco Unity Connection	LDAP Authentication				LDAP Authentication
Cicco Unity Connection     Video Services Accounts Status     Dial Plan     Partitions     Search Spaces     System Settings     General Configuration     Cluster     Authentication Rules     Restriction Tables     Schedules     Schedules     Holiday Schedules     Global Nicknames	▲ LDAP Authentication Refresh Hel     Save     Status     Status     Status: Ready     LDAP Authentication for End Use     DAP Authentication for End Use     LDAP Authentication for End     LDAP Manager Distinguished Name*     LDAP Dassword*     LDAP User Search Base*	p Users (fhlab\Administrator (			
Attachment Descriptions Enterprise Parameters Service Parameters Plugins Plugins Plugins DAP UDAP Setup UDAP Setup UDAP Directory Configuration UDAP Authentication	LDAP Server Information     Ho     10.89.228.226     Add Another Redundant LDAP Se     Save     Fields marked with an asterisk (*) and	st Name or IP Address for Server <sup>®</sup>	LDAP Port* Use TLS		

Importare gli utenti da LDAP a cui verranno assegnati i messaggi vocali e l'utente che verrà utilizzato per il test dell'SSO.

Cisco Unity Connection	Import Users				Import U			
E Users	Import Users Refresh Help	vort Users Refresh Help						
Users								
Import Users	Status							
Synch Users	( Frank Links Links)							
Class of Service	Pound I LUAP User(s)							
Class of Service	c Find							
Class of Service Membership								
E Templates	Find End Users In LDAP Directory							
User Templates	Where Alias v Begins Wi	th v	Eind					
Call Handler Templates								
Contact Templates	Import With							
<ul> <li>Notification Templates</li> </ul>	Based on Template voicemailuser	template 🗸						
🗄 Contacts								
Contacts	Directory Search Results							
Distribution Lists								
System Distribution Lists	Import Selected Import All	25 V Rows Per Page						
Call Management	C Altra i	End No	to at Research	Alter a March and	E A volta			
System Call Handlers		First Name	Last Name	Phone Number	Extension			
Directory Handlers	hugohugo	hugohugo hugo hugo 1002 1002						
Interview Handlers	Terrated and Income							
Custom Recordings	Import Selected Import All	1						

### Passare a **Utenti > Modifica > Ruoli** come mostrato nell'immagine.

<ul> <li>Cisco Unity Connection</li> </ul>			
E Users	Edit Use	er Basics (hugohugo)	
Users	User	Edit Refresh Help	
-Import Users			
Synch Users	Save	User Basics	
Class of Service	- State	Password Settings	
Class of Service	5.64	Change Password	
Class of Service Membership	0 4	change rassilora	ectory
Templates		Roles	
User Templates	Name	Message Waiting Indicators	
Call Handler Templates	Alias*	Transfer Rules	
Contact Templates	First N	Massage Cattings	
Notification Templates		Message Settings	
Contacts	Last N	Caller Input	
Contacts	Displa	Mailbox	
Distribution Lists	SMTP	Phone Menu	@cucoubhosc fblab.com
System Distribution Lists	Tableta		eccpublicaci nabicum
Call Management	Initials	Playback Message Settings	
System Call Handlers	Title	Send Message Settings	
Directory Handlers	Employ	Message Actions	
		Greatings	
Custom Recordings	LDAP	Greetings	
Call Routing		Post Greeting Recording	
Message Storage	3 Inc	Notification Devices	
Mailhow Stores	O Do		

Assegnare all'utente che esegue il test il ruolo di amministratore di sistema.

Cisco Unity Connection	Edit Roles	Search Users + Edit User Basics (hugohugo) + Edit Role
E Users	User Edit Refresh Help	
Users		
-Import Users	Save	
Synch Users		
Class of Service	Roles	
Class of Service	Assigned Roles	
Class of Service Membership		
Templates		
User Templates	M	
Call Handler Templates	A V	
Contact Templates	Available Roles	
Notification Templates	Remote Administrator	
E Contacts	System Administrator	
Contacts	Technican Tenant Administrator	
Distribution Lists	User Administrator V	
System Distribution Lists		
E Call Management	Save	

# Metadati CUC

A questo punto è necessario scaricare i metadati CUC, creare RelyingPartyTrust per CUC e caricare i metadati CUC e creare le regole in ADFS 3.0



Andare a SAML Single Sign-On e abilitare SAML SSO.

👛 saml :	_		$\times$				
0	https://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?serverName=	e	7 ☆	≡			
SAML Sin	gle Sign on Configuration SAML Single S	Sign or	) Config	uration			
SAML Sin	gle Sign on Configuration Refresh Help						
<ul> <li>Test SSO Setup</li> <li>This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This te on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is such 1)Pick a valid username to use for this test</li> <li>You must already know the password for the selected username. This user must have administrator rights and also exist in the IdP.</li> <li>Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator.</li> </ul>							
Valid adi farfar hugohu 2)Launci <b>Run S</b>	Valid administrator Usernames farfar hugohugo 2)Launch SSO test page Run SSO Test						
	na conferencia e Marilla Finder		- 0	L X			
🕑 🚔 🖙 http	se of computation - Mobiles Filefox			° ^ ⊛' ≡			
SAML Single Sig SAML Single Sig	n on Configuration SAML Single Sign on Configuration Navigation Cisco Unity Co on Configuration Refresh Help fartar Search Docur	nnection Ac	dministration	Go Sign Out			
Status			SAML Sin	gle Sign on			
	Test SAML - Mozilla Firefox						
Close	© ≜ ⅔ https://cucpubhcscfhlab.com/ssosp/pages/TestSSO.jsp?ssopage=true ····						
		Row	s per Page	50 v			
	Congratulations on a successful SAML SSO configuration test. Please close this window. File April 28, 2020 5:54:00 PM Passed - May 2 PDT PDT PASSED - April 28, 2020 5:54:00 PM Passed - April 2 PDT 11:05:37	SSO Test 4, 2020 PM PDT 9, 2020 AM PDT	Run SSC	Test			
	Close						

# Configura SSO su Expressway

### Importa metadati in Expressway C

Aprire un browser in https://<FQDN ADFS>/FederationMetadata/2007-06/FederationMetadata.xml e SALVARE i metadati in una cartella locale

Caricare in **Configuration > Unified Communications > IDP**.

# Esporta metadati da Expressway C

Andare alla configurazione -> Unified Communications -> IDP -> Export SAML Data (Esporta dati SAML)

La modalità cluster utilizza un certificato autofirmato (con durata prolungata) incluso nel SAML

metadati e utilizzati per firmare le richieste SAML

- In modalità cluster, per scaricare il file di metadati a livello di cluster singolo, fare clic su Scarica
- In modalità peer, per scaricare il file di metadati per un singolo peer, fare clic su Scarica accanto al peer. Per esportare tutto in un file zip, fare clic su Scarica tutto.

### Aggiungi un trust della relying party per Cisco Expressway-E

Creare innanzitutto i trust della relying party per Expressway-E e quindi aggiungere una regola attestazione per inviare l'identità come attributo UID.



### OAuth con accesso aggiornato

In Cisco CUCM Enterprise Parameters, Verificare OAuth con il parametro Aggiorna flusso di accesso è abilitato. Andare a Cisco Unified CM Administration > Enterprise Parameters > SSO and OAuth Configuration.

	-SSO and OAuth Configuration		
I	550 and oracle configuration		
I	OAuth Token Expiry Timer (minutes) *	60	60
	OAuth Refresh Token Expiry Timer (days) *	60	60
	Redirect URIs for Third Party SSO Client		
I	SSO Login Behavior for iOS *	Use embedded browser (WebView)	Use embedded browser (WebView)
l	OAuth with Refresh Login Flow *	Enabled	Disabled
	Use SSO for RTMT *	True 🗸	True
ι			

# Percorso di autenticazione

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

- Se il percorso di autenticazione è impostato su "Autenticazione SSO SAML", solo i client Jabber che utilizzano un cluster Unified CM abilitato a SSO saranno in grado di utilizzare MRA in questo Expressway. Si tratta di una configurazione SSO only.
- Il supporto MRA di Expressway per tutti i telefoni IP, tutti gli endpoint TelePresence e qualsiasi client Jabber ospitato in un cluster Unified CM non configurato per SSO richiederà che il percorso di autenticazione includa l'autenticazione UCM/LDAP.
- Se uno o più cluster MCM unificato supportano SSO Jabber, selezionare "SAML SSO and UCM/LDAP" per consentire sia l'autenticazione SSO che l'autenticazione di base.

# Architettura SSO

SAML è un formato di dati basato su XML basato su standard aperti che consente agli amministratori di accedere senza problemi a un set definito di applicazioni di collaborazione Cisco dopo aver eseguito l'accesso a una di tali applicazioni. SAML SSO utilizza il protocollo SAML 2.0 per offrire Single Sign-On tra domini e prodotti diversi per le soluzioni di collaborazione Cisco.

# Flusso di login in locale



Figure :SAML Single sign SSO Call Flow for Collaboration Servers



### Flusso di accesso MRA

# OAuth

OAuth è uno standard che supporta l'autorizzazione. Per poter essere autorizzati, gli utenti devono essere autenticati. Il flusso di concessione del codice di autorizzazione fornisce a un client un metodo per ottenere l'accesso e aggiornare i token per accedere a una risorsa (servizi Unified CM, IM&P, Unity ed Expressway). Questo flusso è basato anche sul reindirizzamento e pertanto richiede che il client sia in grado di interagire con un agente utente HTTP (browser Web) controllato dall'utente. Il client invierà una richiesta iniziale al server di autorizzazione utilizzando HTTPS. Il server OAuth reindirizza l'utente a un servizio di autenticazione. Questa operazione può essere eseguita su Unified CM o un IdP esterno se SAML SSO è abilitato. A seconda del metodo di autenticazione utilizzato, è possibile che all'utente finale venga visualizzata una pagina Web per

autenticarsi. L'autenticazione Kerberos è un esempio che non consente di visualizzare una pagina Web. A differenza del flusso di concessione implicito, un flusso di concessione del codice di autenticazione riuscito farà sì che i server OAuth emettano un "codice di autorizzazione" al browser Web. Si tratta di un codice univoco monouso di breve durata che viene quindi passato dal browser Web al client. Il client fornisce questo "codice di autorizzazione" al server di autorizzazione insieme a un segreto già condiviso e riceve in cambio un "token di accesso" e un "token di aggiornamento". Il segreto client utilizzato in questo passaggio consente al servizio di autorizzazione di limitare l'utilizzo ai soli client registrati e autenticati. I token vengono utilizzati per i seguenti scopi:

### Token di accesso/aggiornamento

Token di accesso: Token rilasciato dal server di autorizzazione. Il client presenta il token a un server delle risorse quando deve accedere alle risorse protette su tale server. Il server delle risorse è in grado di convalidare il token e considera attendibili le connessioni che utilizzano il token. (la durata predefinita dei token di accesso Cisco è di 60 minuti)

Token di aggiornamento: Questo token viene nuovamente rilasciato dal server di autorizzazione. Il client presenta questo token al server di autorizzazione insieme al segreto client quando il token di accesso è scaduto o sta per scadere. Se il token di aggiornamento è ancora valido, il server di autorizzazione rilascerà un nuovo token di accesso senza richiedere un'altra autenticazione. Per impostazione predefinita, i token di aggiornamento Cisco hanno una durata di 60 giorni. Se il token di aggiornamento è scaduto, è necessario avviare un nuovo flusso di concessione del codice di autorizzazione OAuth completo per ottenere nuovi token.

### Il flusso di concessione del codice di autorizzazione OAuth è migliore

Nel flusso di concessione implicito, il token di accesso viene passato al client Jabber tramite un agente utente HTTP (browser). Nel flusso di concessione del codice di autorizzazione, il token di accesso viene scambiato direttamente tra il server di autorizzazione e il client Jabber. Il token viene richiesto dal server di autorizzazione utilizzando un codice di autorizzazione univoco con limiti di tempo. Questo scambio diretto del token di accesso è più sicuro e riduce l'esposizione al rischio.

Il flusso di concessione del codice di autorizzazione OAuth supporta l'utilizzo dei token di aggiornamento. In questo modo l'utente finale può beneficiare di un'esperienza migliore, poiché non deve eseguire la nuova autenticazione con la stessa frequenza (per impostazione predefinita 60 giorni)

# **Configura Kerberos**

### Seleziona autenticazione di Windows

Gestione Internet Information Services (IIS) > Siti > Sito Web predefinito > Autenticazione > Autenticazione di Windows > Impostazioni avanzate.

- 1. Deselezionare Attiva autenticazione in modalità kernel.
- 2. Assicurarsi che la protezione estesa sia disattivata.



# ADFS supporta sia Kerberos che NTLM

Verificare che AD FS versione 3.0 supporti sia il protocollo Kerberos che il protocollo NTLM (NT LAN Manager), poiché tutti i client non Windows non possono utilizzare Kerberos e si basano su NTLM.

Nel riquadro di destra, selezionare Provider e assicurarsi che Negotiate e NTLM siano presenti in Provider abilitati:

<b>V</b> 3	Internet Information Se	ervices (IIS) Man	ager		- 🗆 X
€ Sites ► Default Web Sites	e <b>&gt;</b>				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	

# Configurare Microsoft Internet Explorer

Verificare che Internet Explorer > Avanzate > Abilita autenticazione integrata di Windows sia selezionato.

Internet (	Options						? <b>X</b>	
General	Security	Privacy	Content	Connec	tions Pr	ograms	Advanced	
Setting	js ———						]	
	<ul> <li>Do not submit unknown addresses to your auto-search pro</li> <li>Just display the results in the main window</li> <li>Security</li> <li>Allow active content from CDs to run on My Computer*</li> <li>Allow active content to run in files on My Computer*</li> <li>Allow software to run or install even if the signature is invi</li> <li>Check for publisher's certificate revocation</li> <li>Check for server certificate revocation*</li> <li>Check for signatures on downloaded programs</li> <li>Do not save encrypted pages to disk</li> <li>Empty Temporary Internet Files folder when browser is ck</li> <li>Enable DOM Storage</li> <li>Enable Integrated Windows Authentication*</li> </ul>							
•							•	
*Takes effect after you restart Internet Explorer Restore advanced settings Resets Internet Explorer settings to their default Reset You should only use this if your browser is in an unusable state.								
			OK		Cance		Apply	

Aggiungi URL ADFS in Protezione > Aree Intranet > Siti