

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](#)

[Siti da aggiungere a IE](#)

[Problema non sincronizzato](#)

[Revoca un token](#)

[File bootstrap](#)

[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,

expwyc, expwye, impubhcsc e imsubhcsc.

The screenshot shows the DNS console with the following structure:

- DNS
 - AD
 - Forward Lookup Zones
 - _msdcs.fhlab.com
 - fhlab.com (selected)
 - _msdcs
 - _sites
 - _tcp
 - _udp
 - DomainDnsZones
 - ForestDnsZones
 - Reverse Lookup Zones
 - 228.89.10.in-addr.arp
 - Trust Points
 - Conditional Forwarders
 - Global Logs

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

Record puntatore (PTR)

The screenshot shows the DNS console with the following structure:

- DNS
 - AD
 - Forward Lookup Zones
 - _msdcs.fhlab.com
 - fhlab.com (selected)
 - _msdcs
 - _sites
 - _tcp
 - _udp
 - DomainDnsZones
 - ForestDnsZones
 - _sites
 - _tcp
 - Reverse Lookup Zones
 - 228.89.10.in-addr.arp

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

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

Name	Type	Data	Timestamp
_cisco-uds	Service Location (SRV)	[0][0][8443] cmsubhcsc.fhlab.com.	static
_cisco-uds	Service Location (SRV)	[0][0][8443] cmpubhcsc.fhlab.com.	static
_cuplogin	Service Location (SRV)	[0][0][8443] impsubhcsc.fhlab.com.	static
_cuplogin	Service Location (SRV)	[0][0][8443] imppubhcsc.fhlab.com.	static
_gc	Service Location (SRV)	[0][100][3268] ad.fhlab.com.	5/12/2020 10:00:00 AM
_kerberos	Service Location (SRV)	[0][100][88] ad.fhlab.com.	5/12/2020 10:00:00 AM
_kpasswd	Service Location (SRV)	[0][100][464] ad.fhlab.com.	5/12/2020 10:00:00 AM
_ldap	Service Location (SRV)	[0][100][389] ad.fhlab.com.	5/12/2020 10:00:00 AM

_cisco-uds Properties

Service Location (SRV) Security

Domain: fhlab.com

Service: _cisco-uds

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 8443

Host offering this service: cmpubhcsc.fhlab.com.

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

È necessario 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.

Template Display Name	Schema Version
CEP Encryption	1
ClientServerAuth	2
Code Signing	1
Computer	1
Cross Certification Authority	2
Directory Email Replication	2
Domain Controller	1
Domain Controller Authentication	2
EFS Recovery Agent	1
Enrollment Agent	1
Enrollment Agent (Computer)	1
Exchange Enrollment Agent (Offline requ...	1
Exchange Signature Only	1
Exchange User	1
IPSec	1
IPSec (Offline request)	1
Kerberos Authentication	2
Key Recovery Agent	2
OCSP Response Signing	3
RAS and IAS Server	2
Root Certification Authority	1

Properties of New Template

Subject Name Server Issuance Requirements

Compatibility General Request Handling Cryptography Key Attestation

Superseded Templates Extensions Security

To modify an extension, select it, and then click Edit.

Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

- Server Authentication
- Client Authentication

Edit Application Policies Extension

An application policy defines how a certificate can be used.

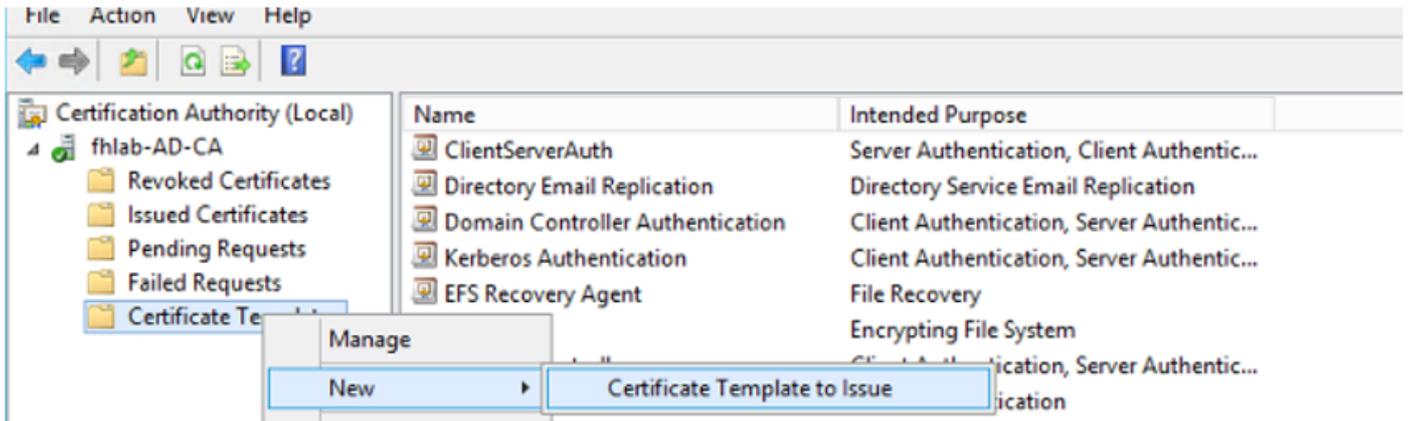
Application policies:

- Client Authentication
- Server Authentication

Add... Edit... Remove

Make this extension critical

È necessario 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 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 source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```

8V8mWY/9kjhgfnpeBzAAW++to1GzBjnvqaT8StWN
LA0dphF6LrurUeY2KLvMLmK1ft7aSy483yCsm0v1
OWQFzoLb3bS80ziW7fQEPWSaCg567DMOQ8PkZt5N
10y/Ip6oDzTdZE9w2p8rK3YxcbyfovStOijIirh
AM/GjnzQ
-----END CERTIFICATE REQUEST-----

```

Certificate Template:

Additional Attributes:

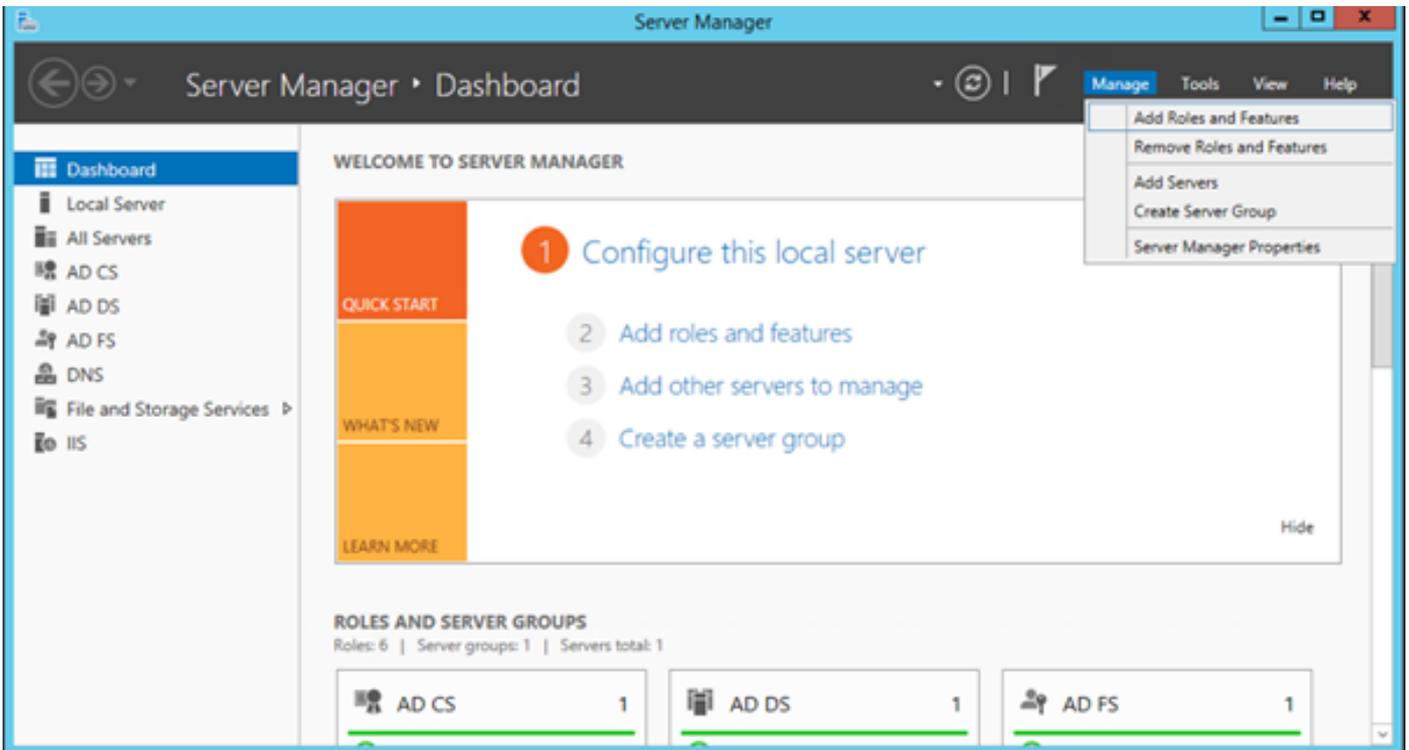
- User
- Basic EFS
- Administrator
- EFS Recovery Agent
- Web Server
- Subordinate Certification Authority
- ClientServerAuth

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

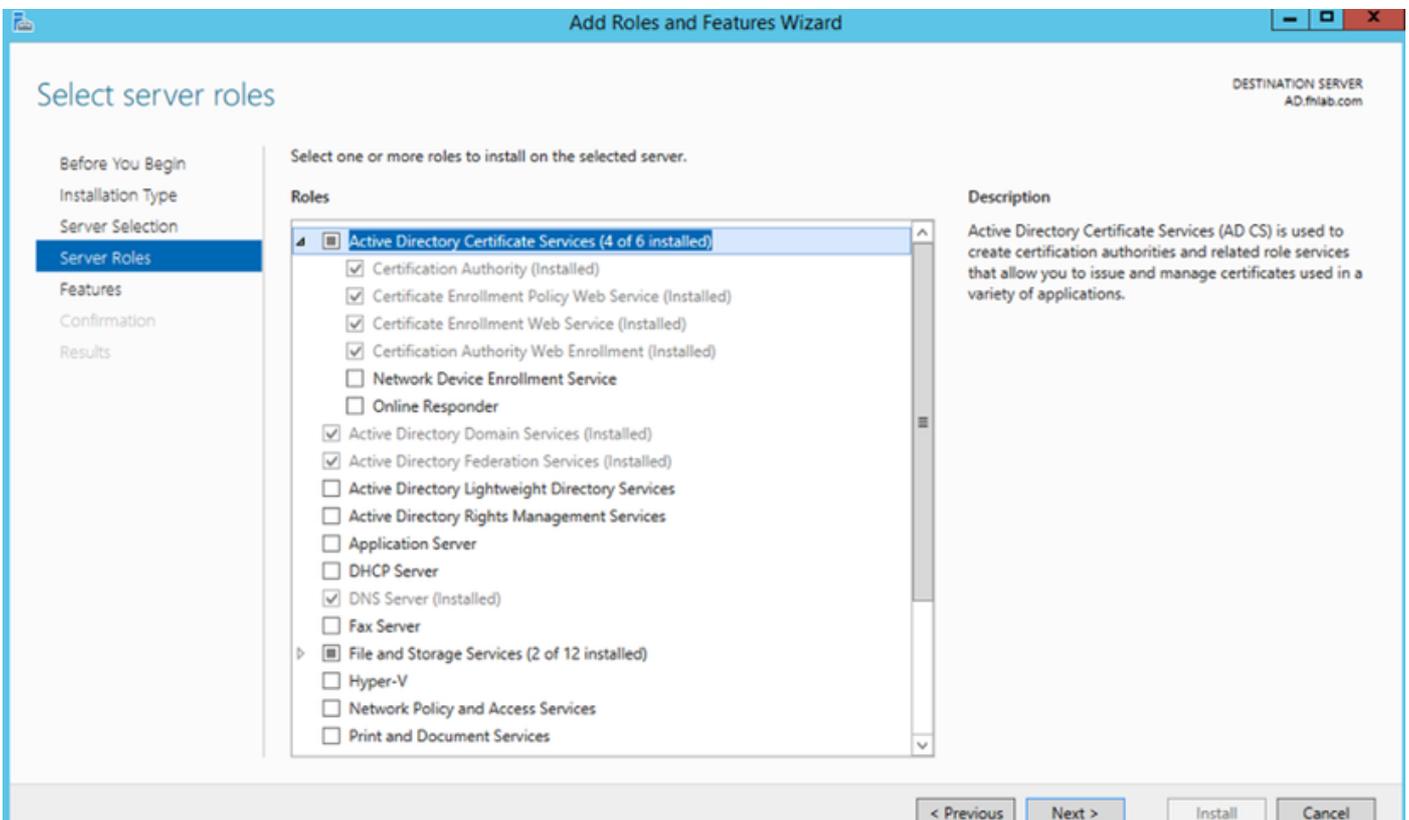
Dopo l'installazione di Windows 2012 R2 con DNS, innalzare il server a controller di dominio.

La prossima operazione sarà installare Servizi certificati Microsoft.

Passare a Server Manager e aggiungere un nuovo ruolo:



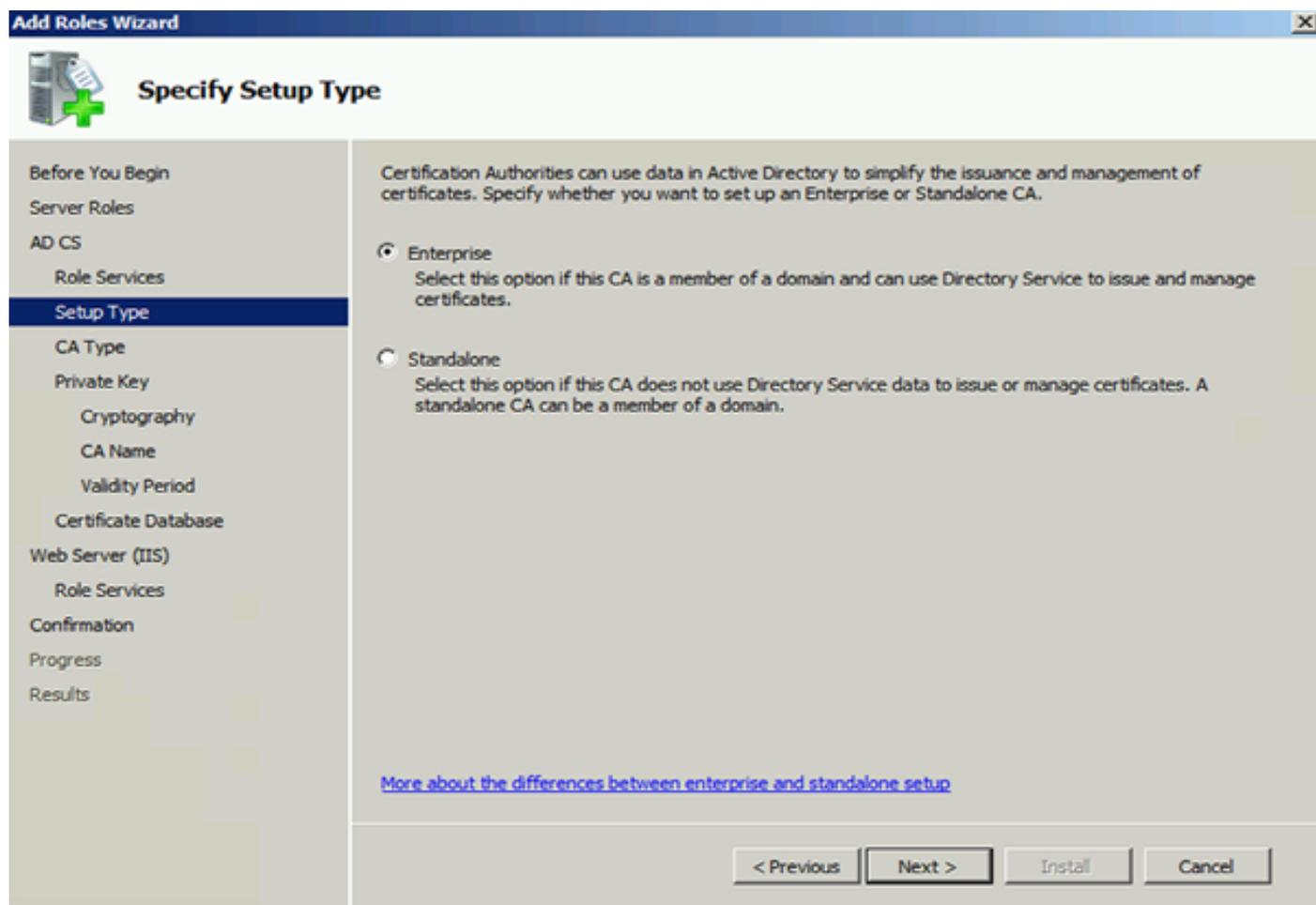
Selezionare il ruolo **Servizi certificati Active Directory**.



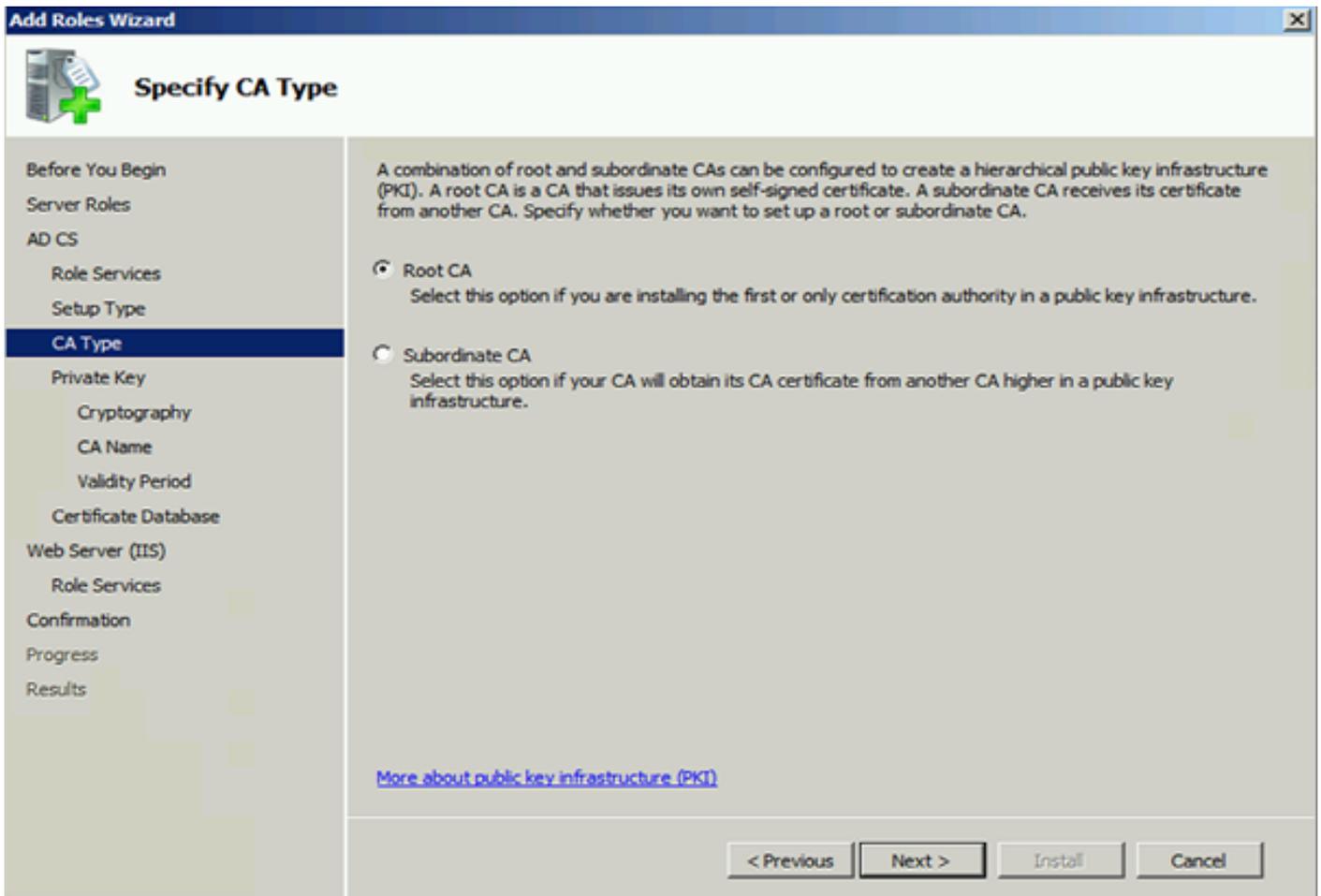
E distribuire questi servizi - Servizio Web di informazioni sulle registrazioni di certificati di Autorità di certificazione. Dopo aver installato questi due ruoli, configurarli e quindi installare **Servizio Web di registrazione certificati** e **Registrazione Web Autorità di certificazione**. Configurarle.

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

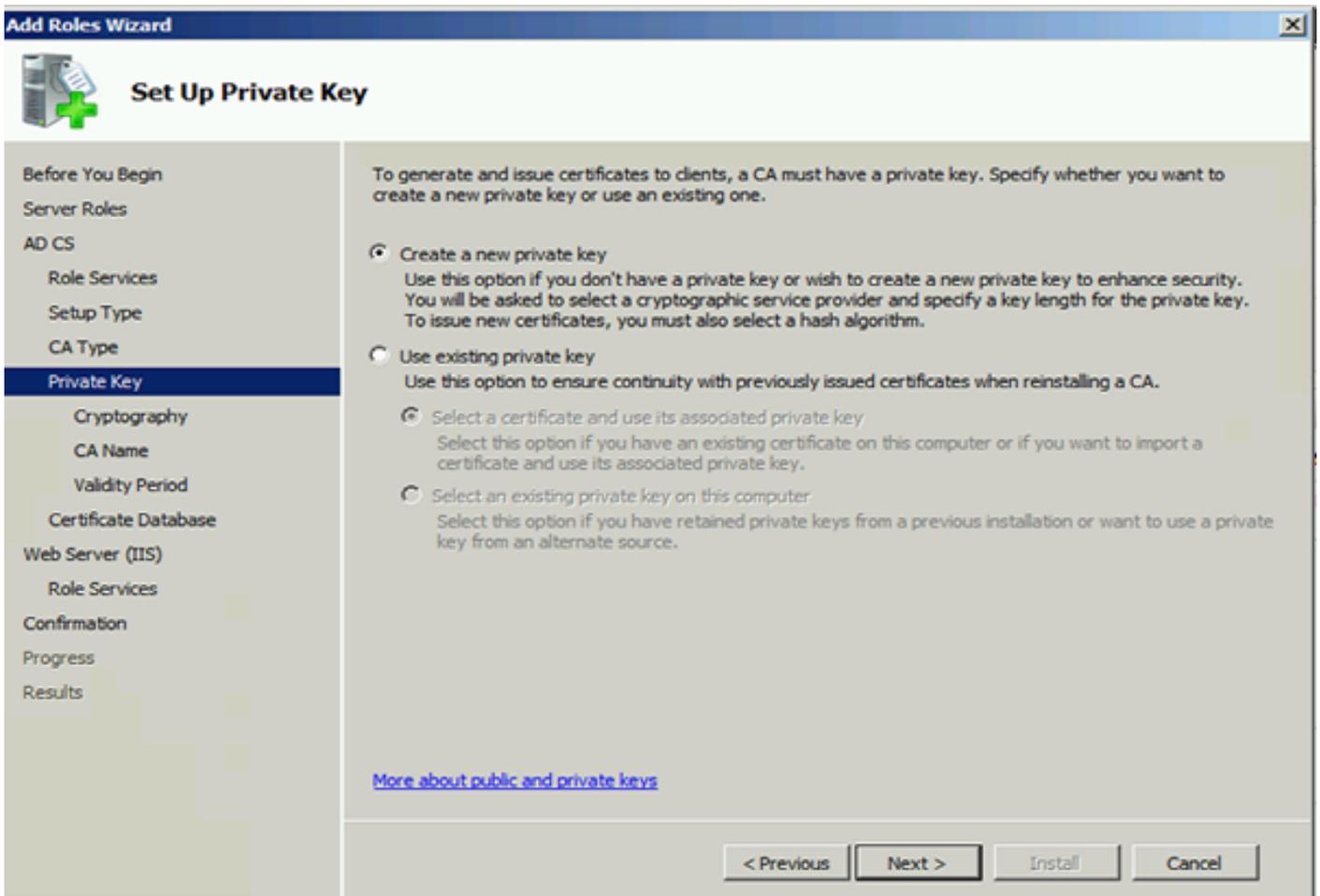
A seconda della distribuzione, è possibile selezionare Enterprise o Standalone.



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

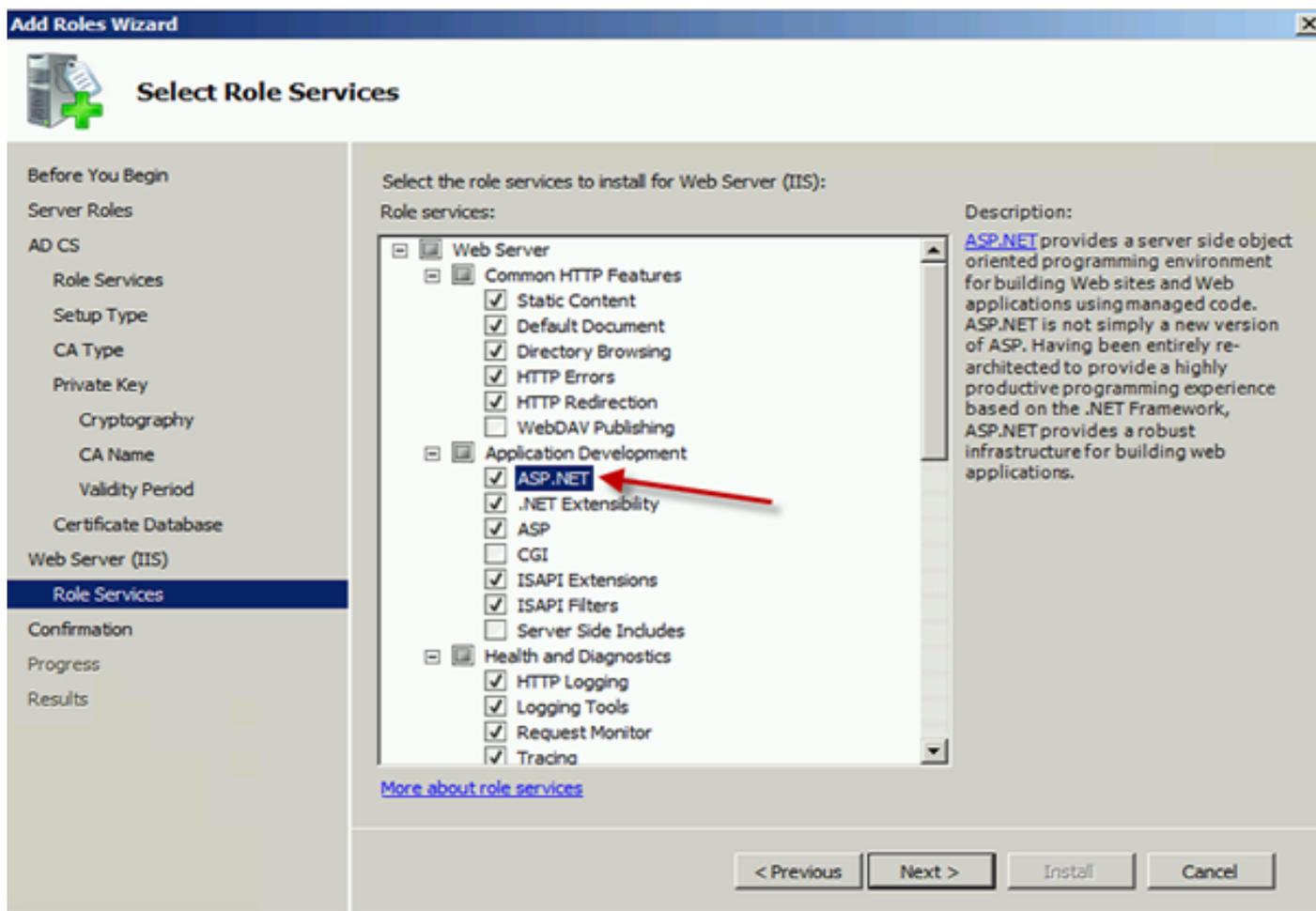


Il passaggio successivo consiste nella creazione di una chiave privata per la CA.

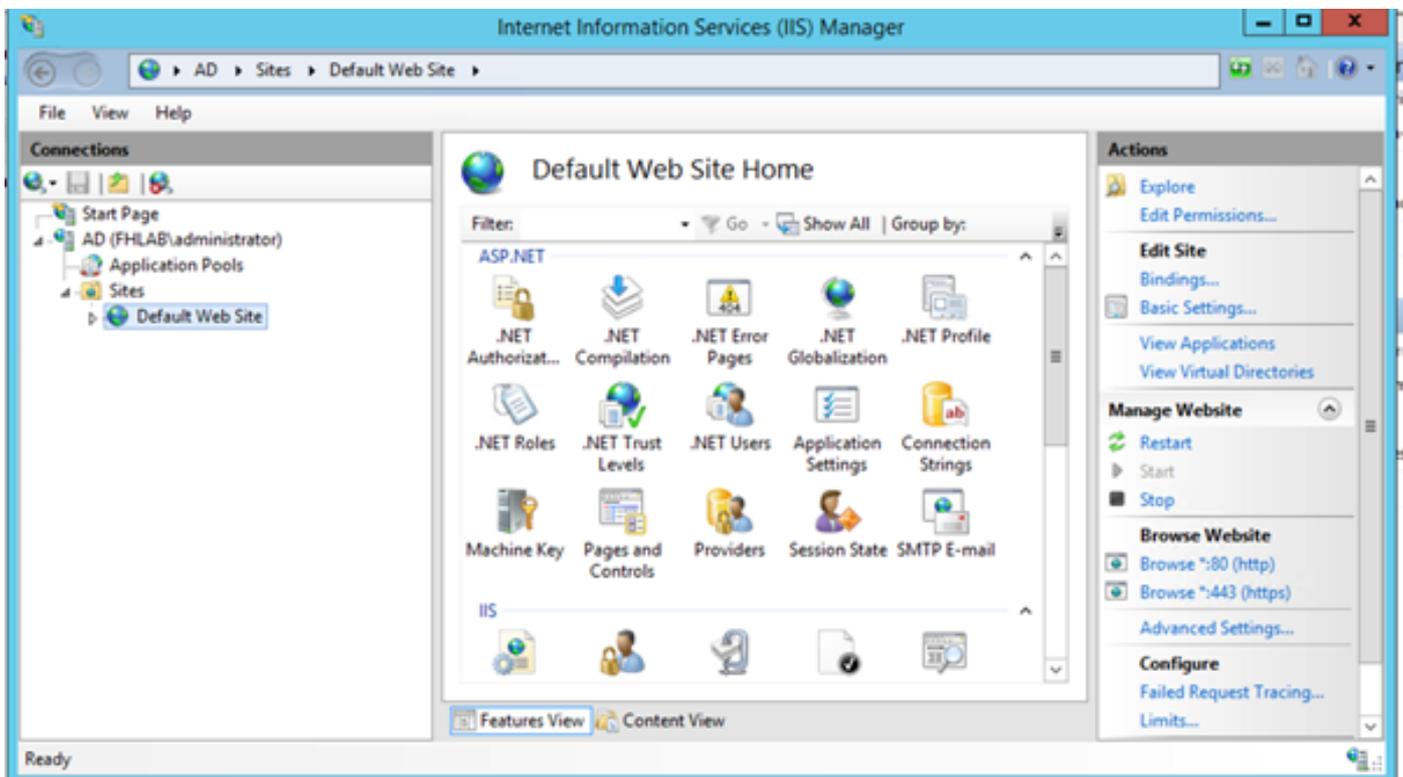


Questo passaggio è necessario solo se si installa ADFS3 in un Windows Server 2012 separato.

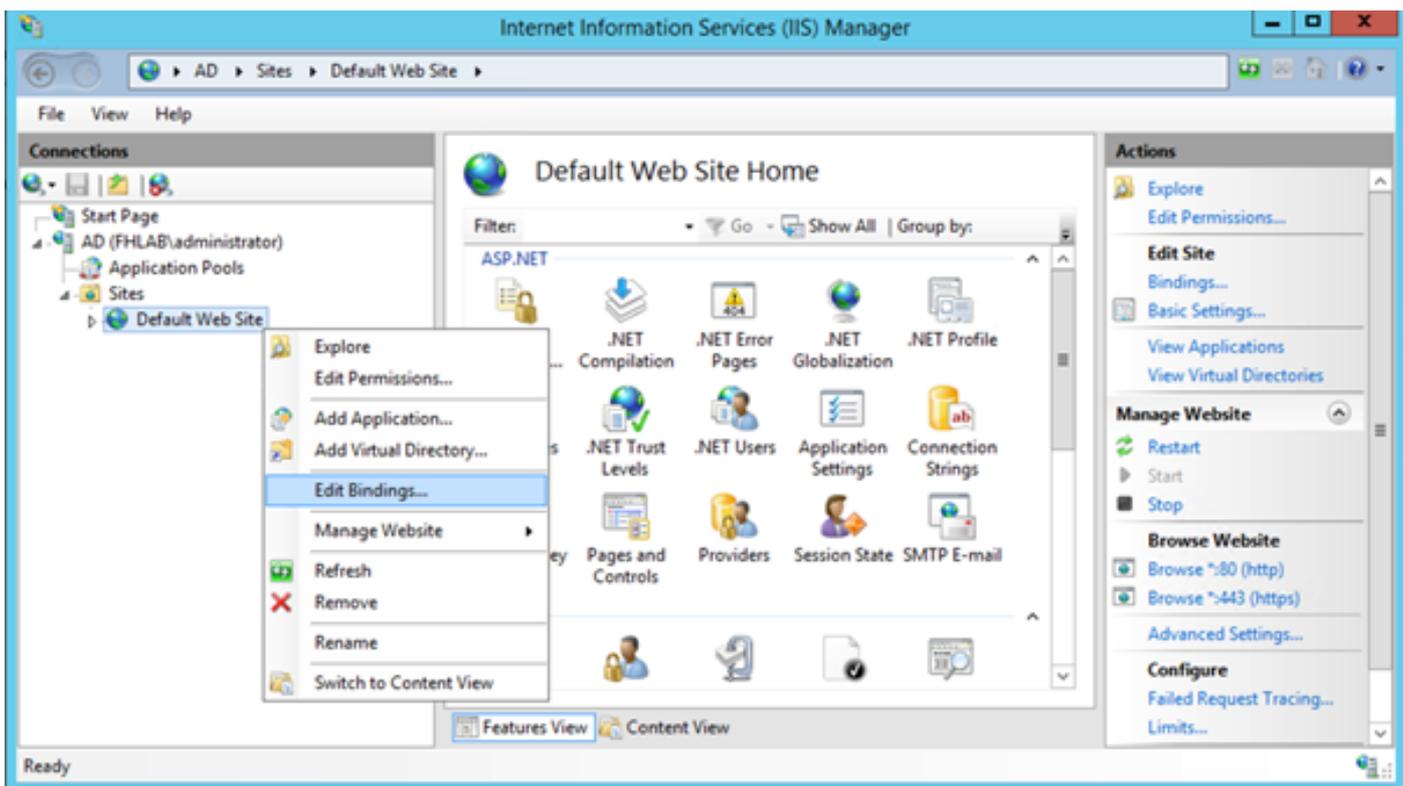
Dopo aver configurato la CA, è necessario configurare i servizi ruolo per IIS. Questa operazione è necessaria per la registrazione Web sulla CA. Per la maggior parte delle distribuzioni ADFS, è necessario un ruolo aggiuntivo in IIS, fare clic su **ASP.NET** in Sviluppo applicazioni.



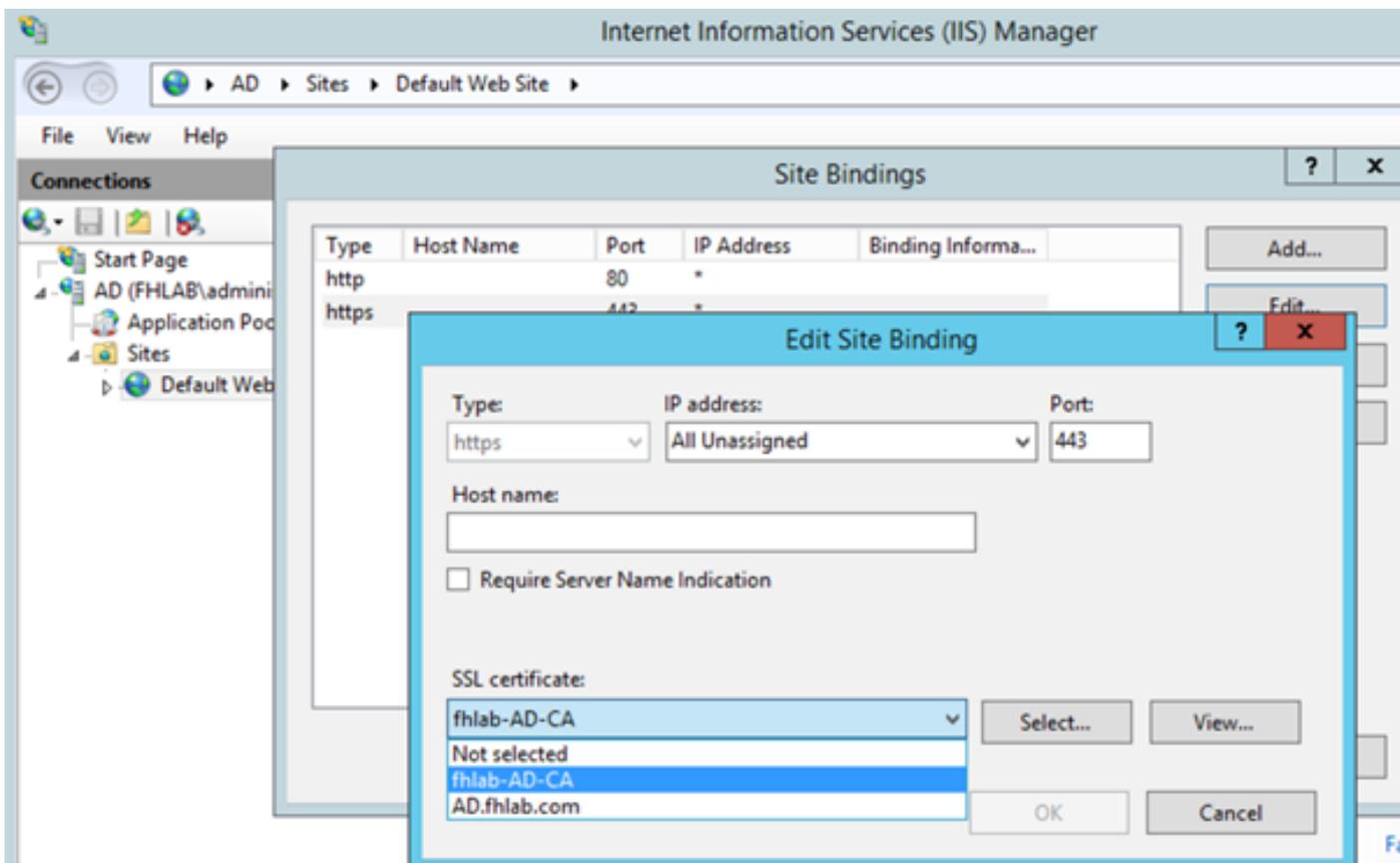
In Server Manager fare clic su **Server Web > IIS**, quindi fare clic con il pulsante destro del mouse su **Sito Web predefinito**. È necessario modificare il binding per consentire anche HTTPS oltre a HTTP. Questa operazione viene eseguita per supportare HTTPS.



Selezionare **Modifica associazioni**.

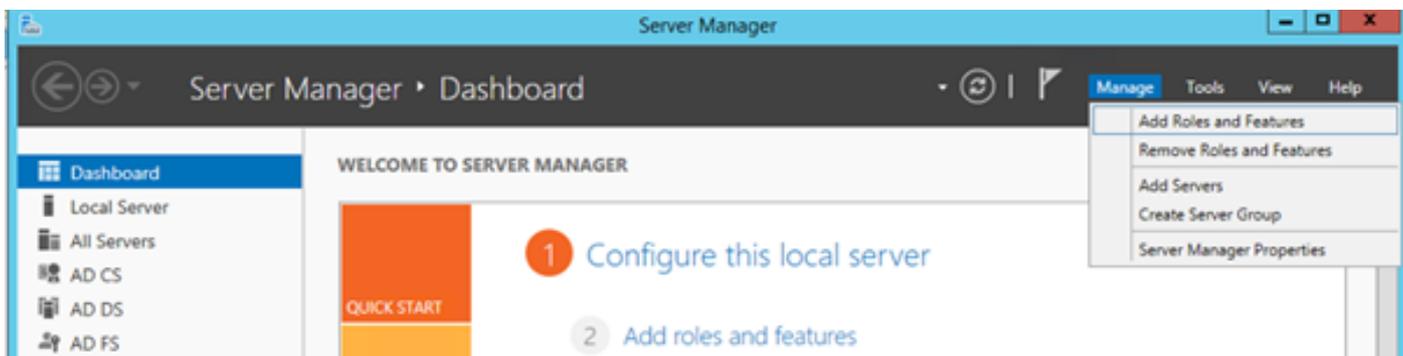


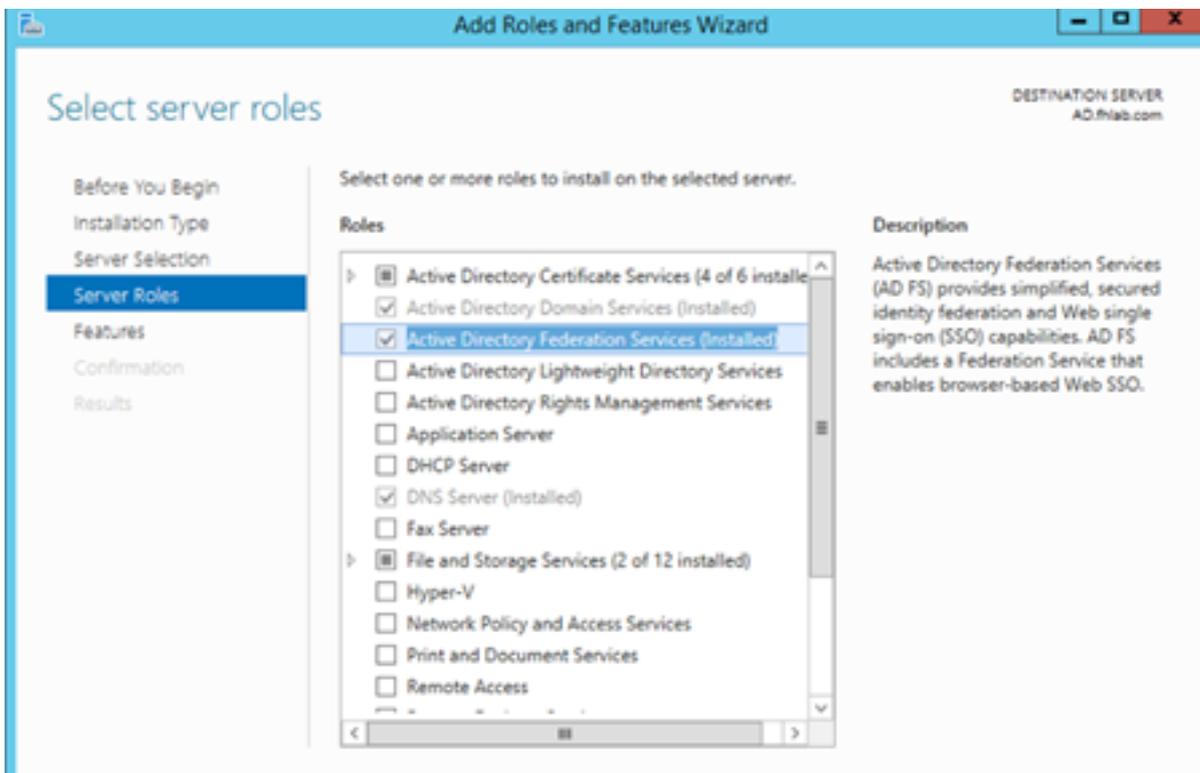
Aggiungere una nuova associazione sito e selezionare **HTTPS** come tipo. Per il certificato SSL, selezionare il certificato server che deve avere lo stesso FQDN del server AD.



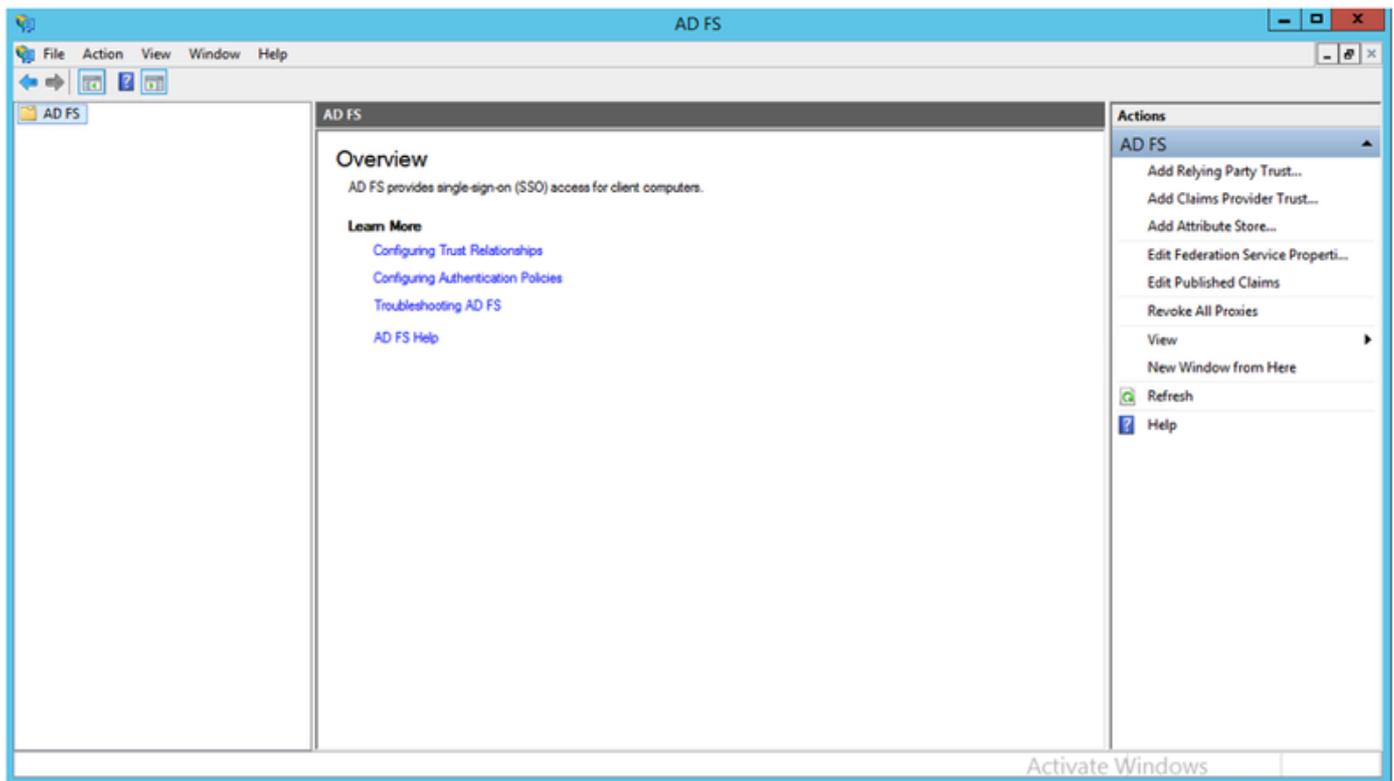
Tutti i ruoli prerequisiti sono installati nell'ambiente, quindi è possibile procedere con l'installazione di ADFS3 Active Directory Federation Services (in Windows Server 2012).

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.





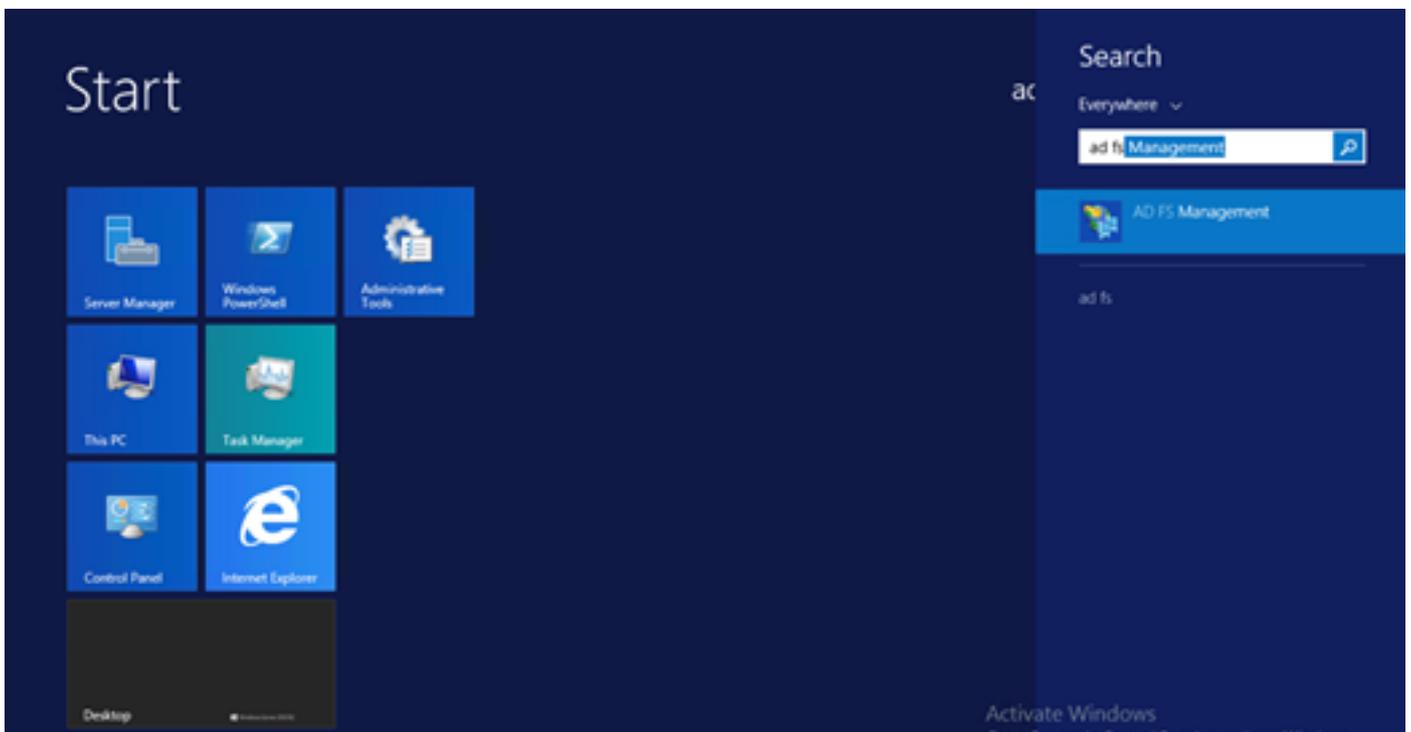
Al termine dell'installazione, sarà possibile aprirla dalla barra delle applicazioni o dal menu Start.



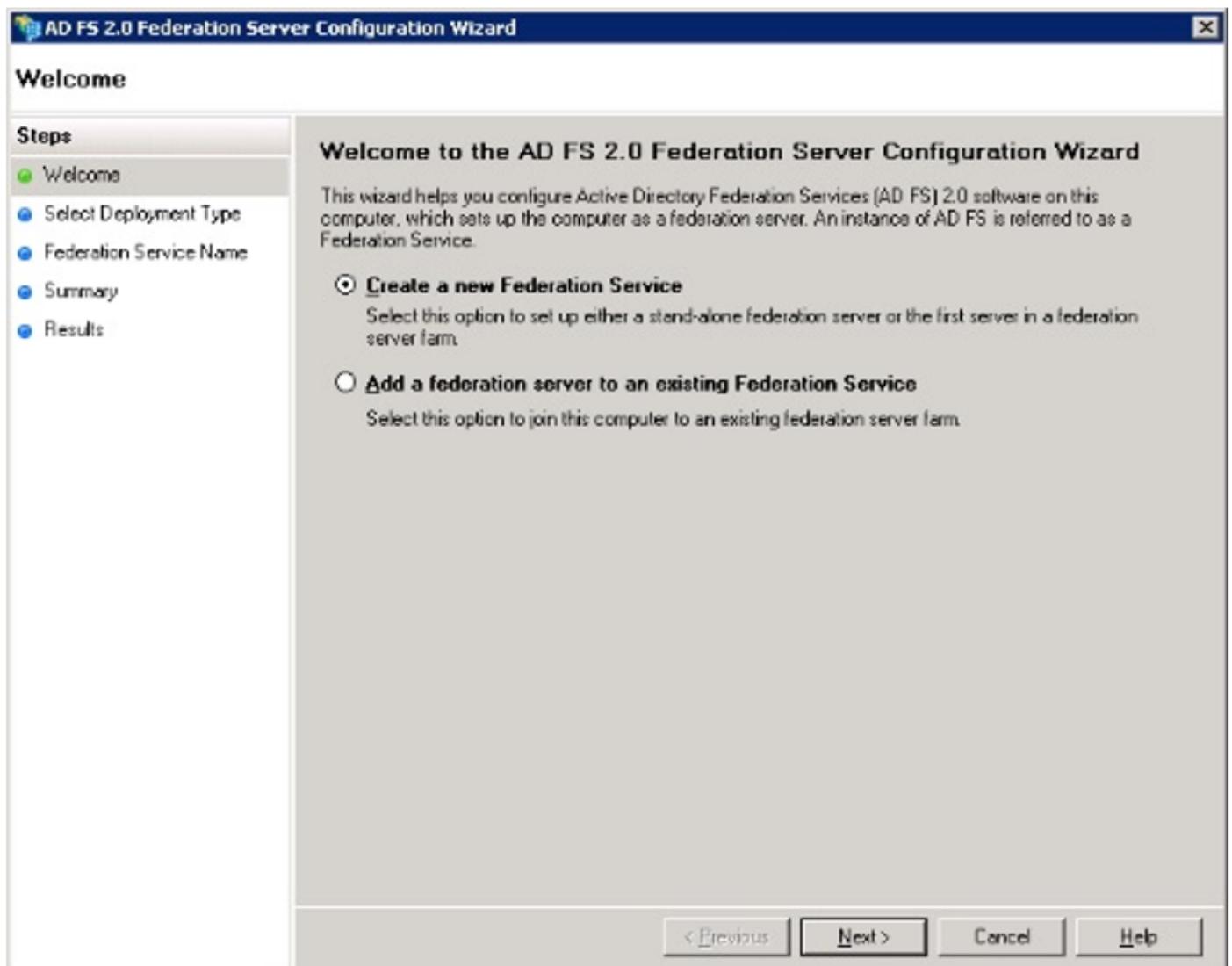
Configurazione iniziale di ADFS3

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

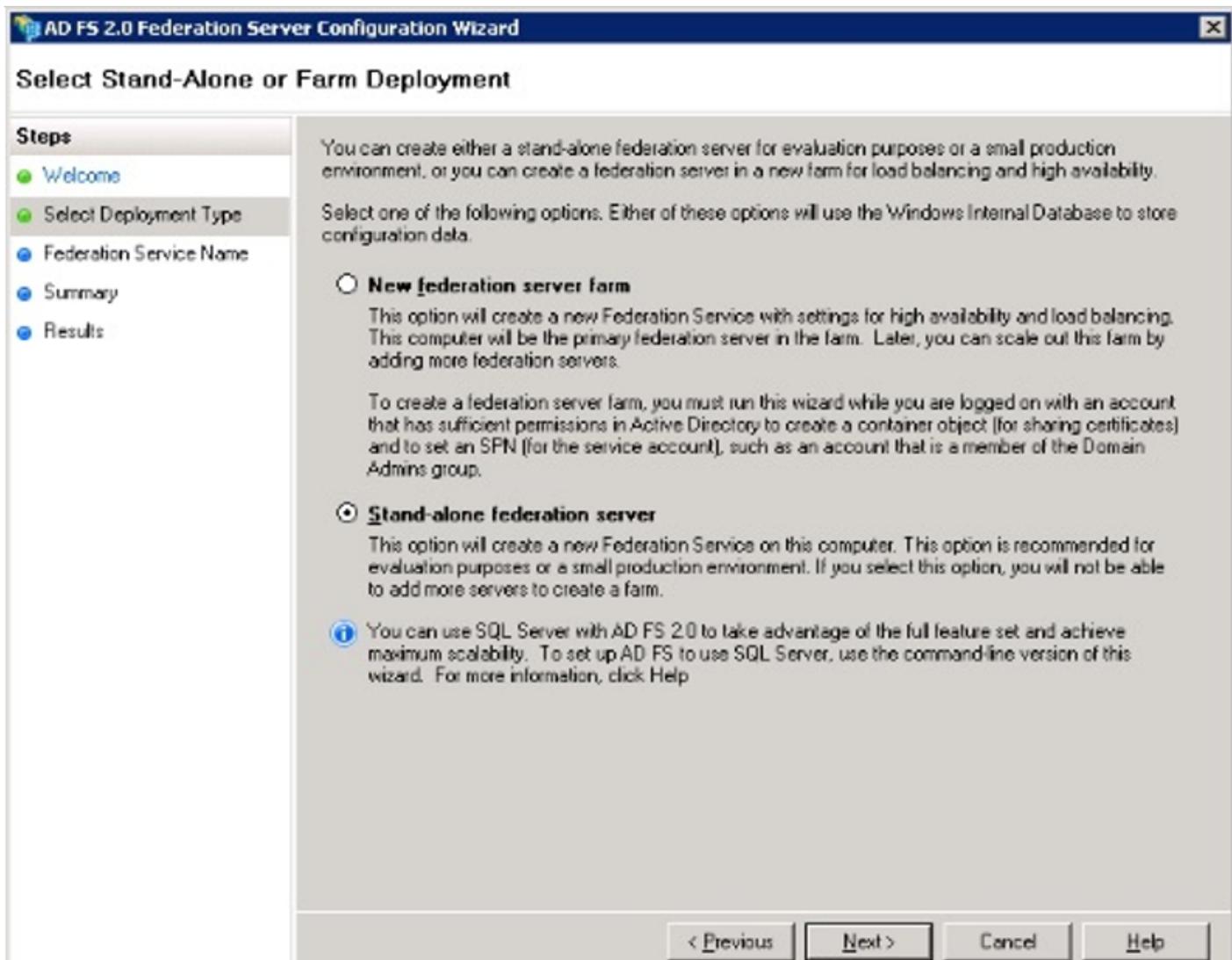
Selezionare **Windows** e digitare **Gestione ADFS** per avviare la console Gestione ADFS, come illustrato nell'immagine.



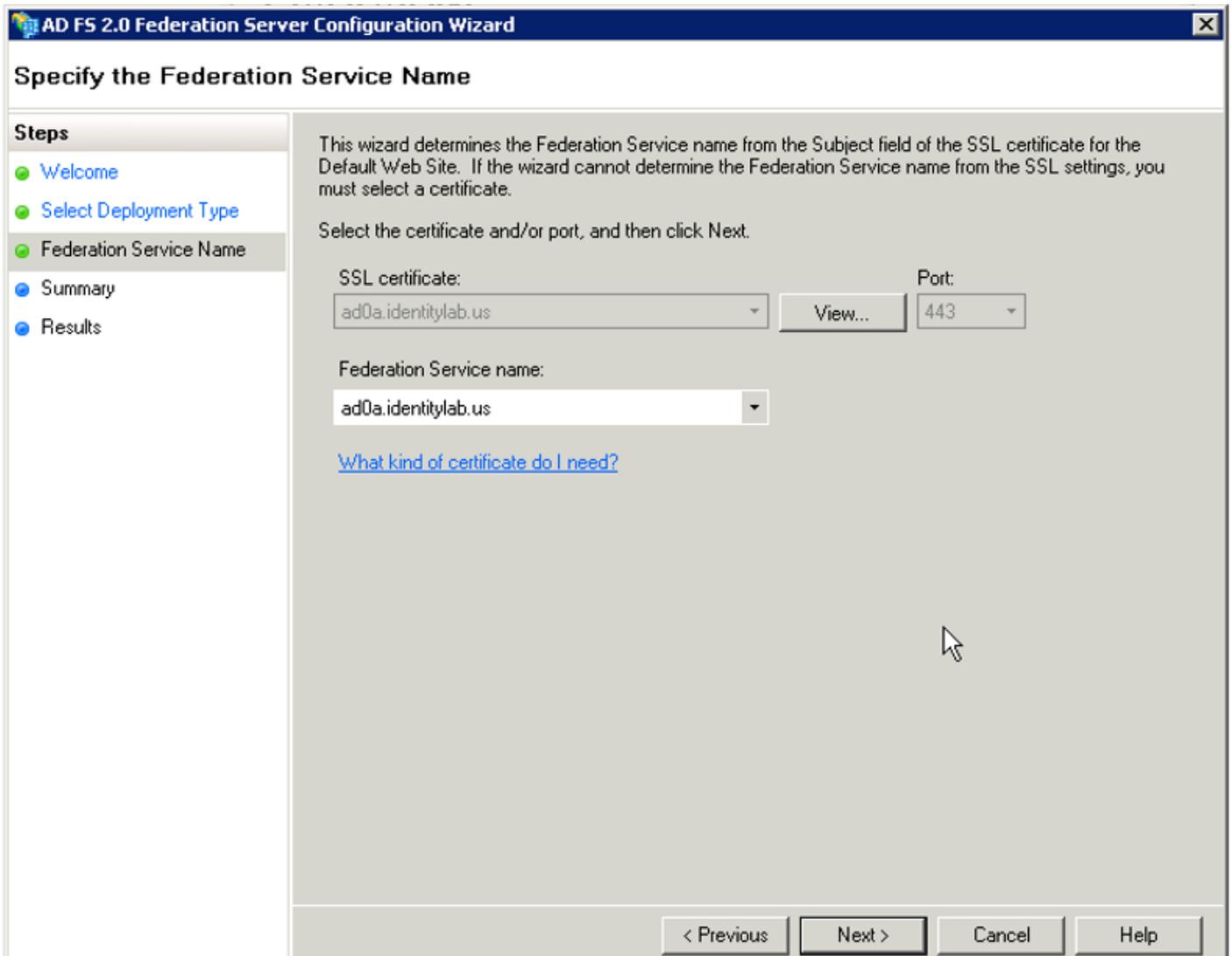
Selezionare l'opzione **Configurazione guidata server federativo ADFS 3.0** per avviare la configurazione del server ADFS. Questi screenshot rappresentano gli stessi passaggi in ADFS 3.



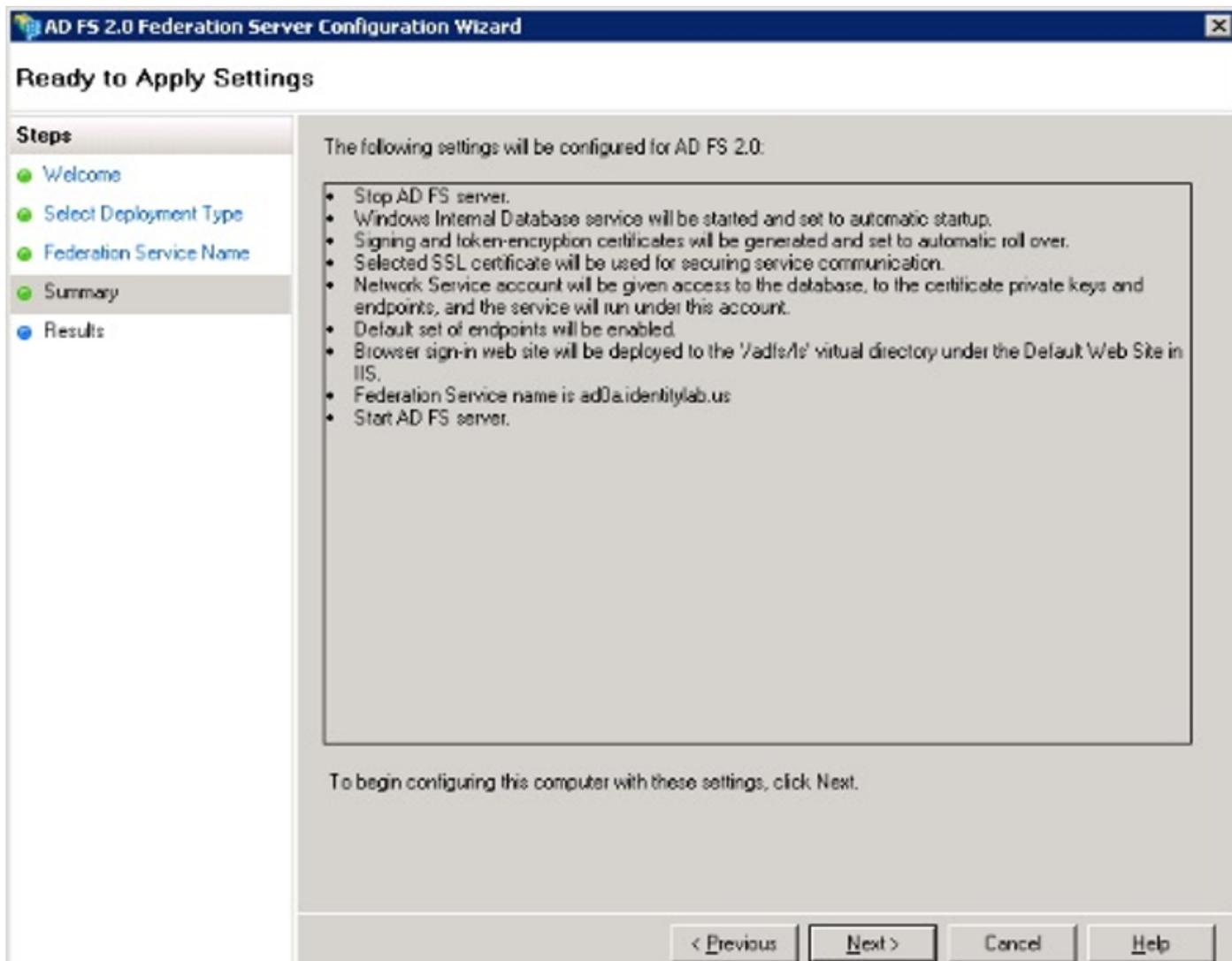
Selezionare Crea nuovo **servizio federativo** e fare clic su **Avanti**.



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



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



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

AD FS 2.0 Federation Server Configuration Wizard

Configuration Results

Steps

- Welcome
- Select Deployment Type
- Federation Service Name
- Summary
- Results**

The following settings are being configured

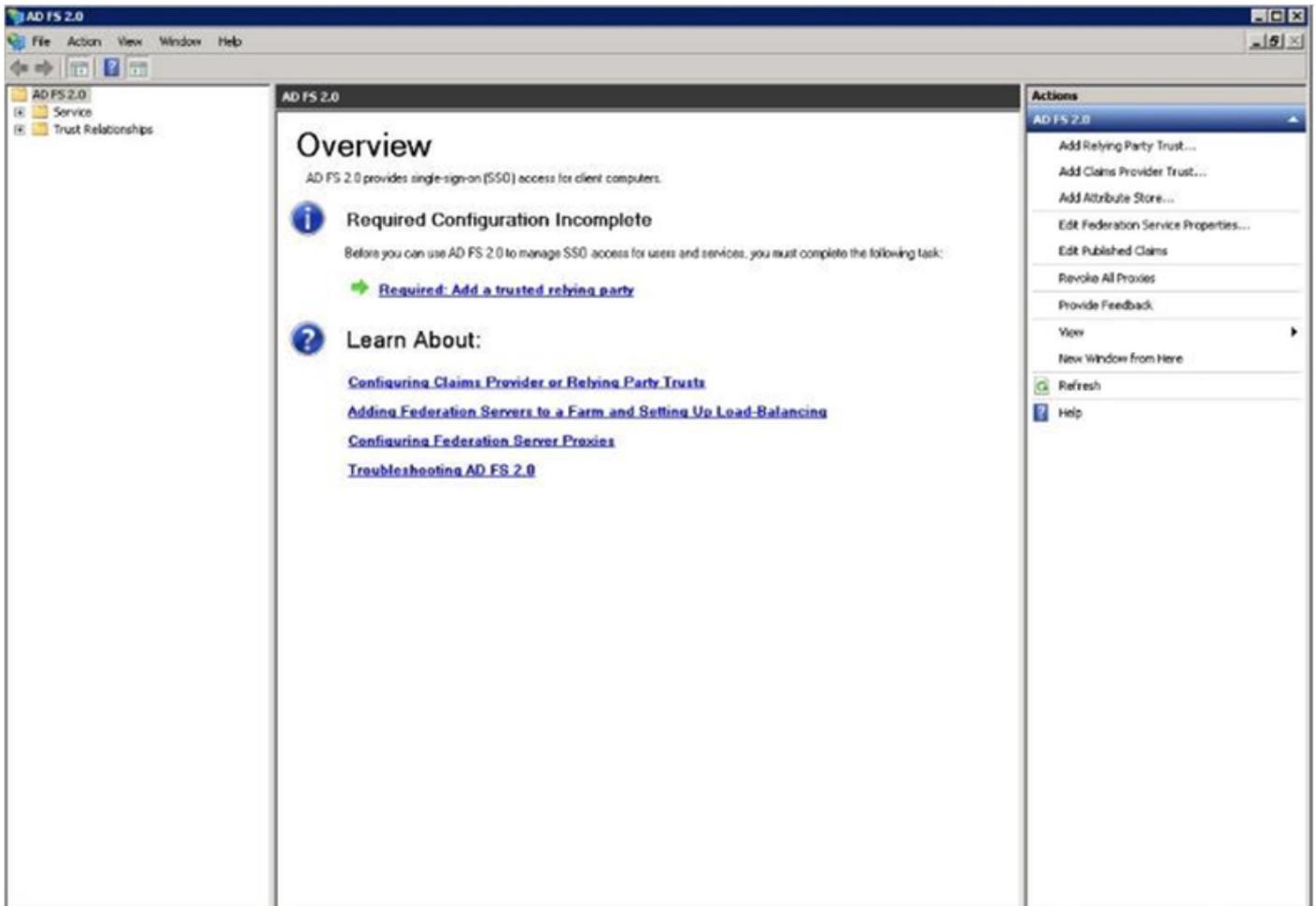
Component	Status
Stop the AD FS 2.0 Windows Service	Configuration finished
Install Windows Internal Database	Configuration finished
Start the Windows Internal Database service	Configuration finished
Create AD FS configuration database	Configuration finished
Configure service settings	Configuration finished
Deploy browser sign-in Web site	Configuration finished
Start the AD FS 2.0 Windows Service	Configuration finished
Create default claim set	Configuration finished
Create default Active Directory claim acceptance rules	Configuration finished

You have successfully completed the AD FS 2.0 Federation Server Configuration Wizard.

To close this wizard, click Close.

Close

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



Please Delete All LDAP Directories Before Making Changes on This Page



Please Disable LDAP Authentication Before Making Changes on This Page

LDAP System Information

Enable Synchronizing from LDAP Server

LDAP Server Type

LDAP Attribute for User ID

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*

LDAP Manager Distinguished Name*

LDAP Password*

Confirm Password*

LDAP User Search Base*

LDAP Custom Filter for Users

Synchronize* Users Only Users and Groups

LDAP Custom Filter for Groups

LDAP Directory Synchronization Schedule

Perform Sync Just Once

Perform a Re-sync Every*

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

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

LDAP Server Information

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

[Add Another Redundant LDAP Server](#)

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

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | farfar | Search Documentation | About | Logout

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

LDAP Authentication

Status
Status: Ready

LDAP Authentication for End Users

Use LDAP Authentication for End Users

LDAP Manager Distinguished Name*

LDAP Password*

Confirm Password*

LDAP User Search Base*

LDAP Server Information

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

[Add Another Redundant LDAP Server](#)

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

Confirm MLPP Password
 MLPP Precedence Authorization Level

CAPF Information

Associated CAPF Profiles [View Details](#)

Permissions Information

Groups:

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

[View Details](#)

Roles:

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

[View Details](#)

Conference Now Information

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

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.

System > Call Routing > Media Resources > ... > Device > User Manager > ... > Administration > SAML Single Sign-On

SAML Single Sign-On

SSO Mode

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

Status

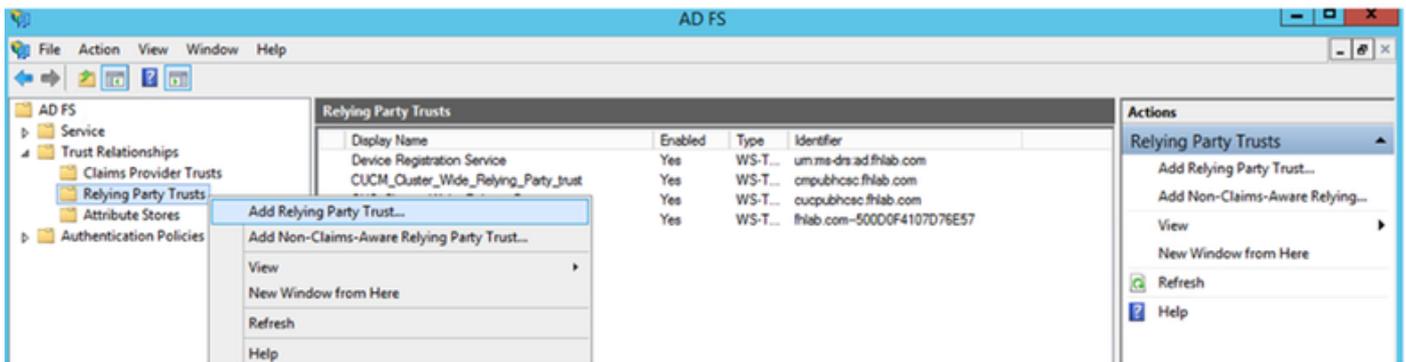
- RTMT is enabled for SSO. You can change SSO for RTMT [here](#).
- SAML SSO enabled

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

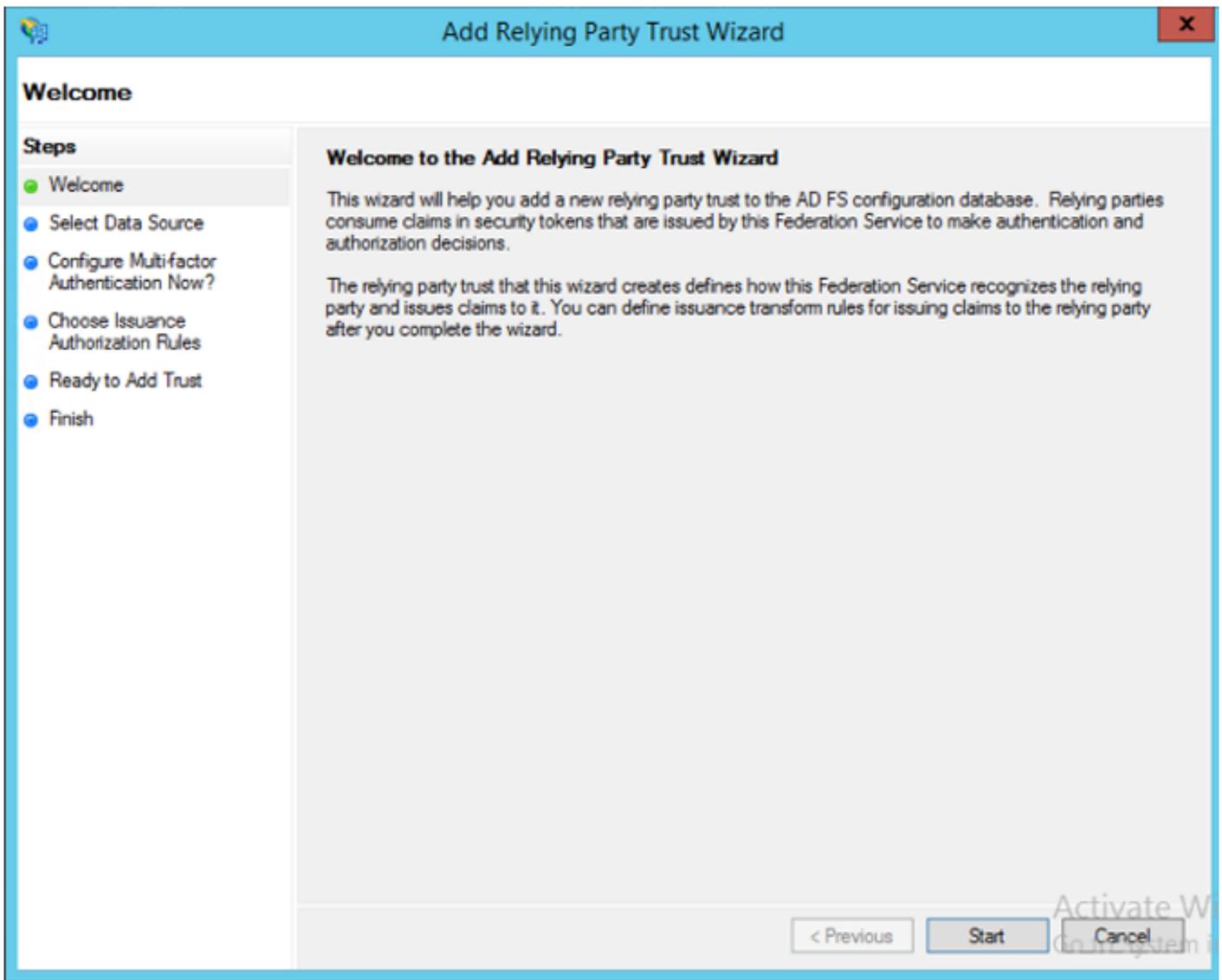
Salvare i dati localmente con un nome significativo, ad esempio `sp_cucm0a.xml`, che sarà necessario utilizzare in seguito.

Configura componente ADFS

Tornare alla console di gestione di AD FS 3.0.

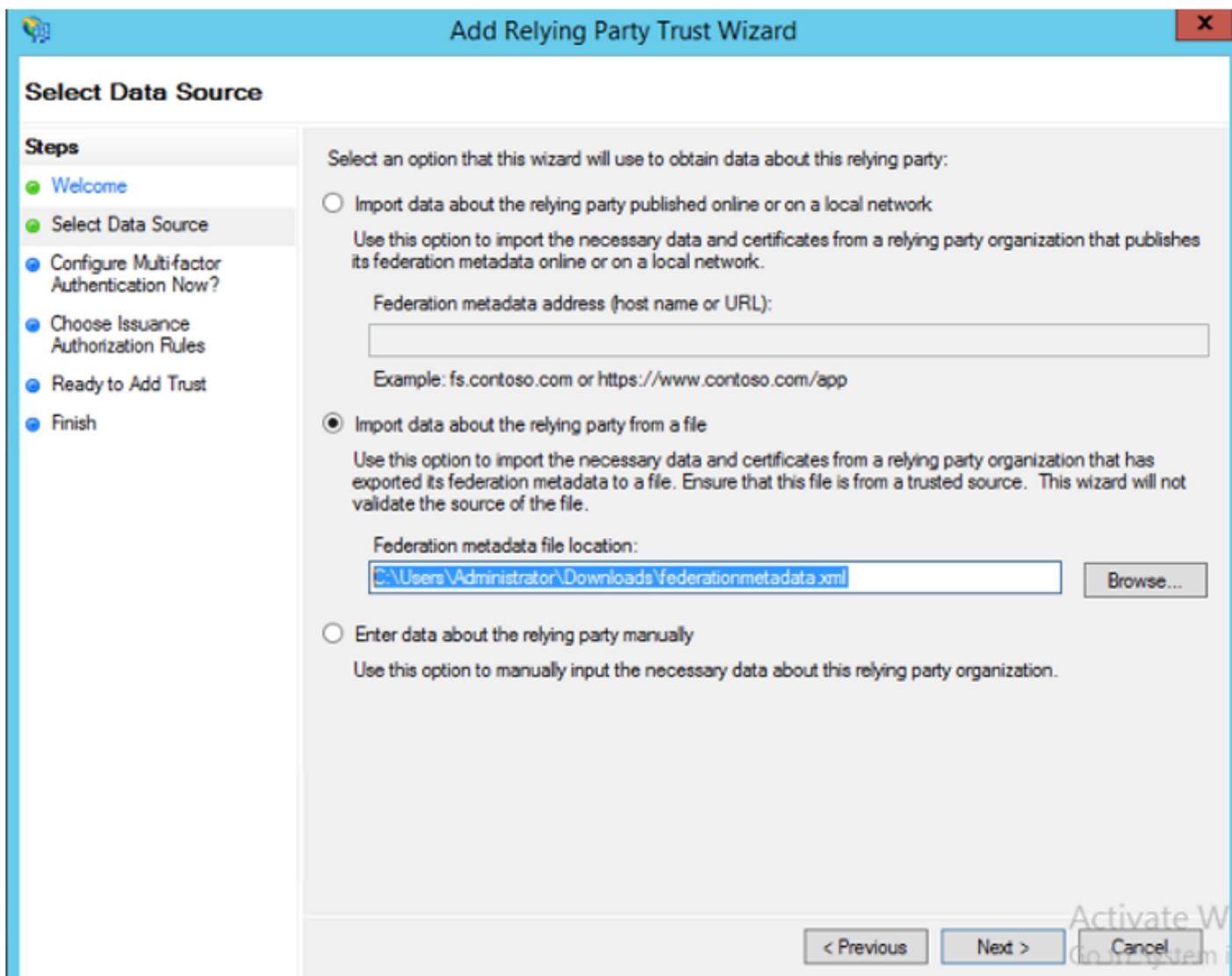


Fare clic su **Aggiunta guidata attendibilità componente**.



Fare clic su **Start** per continuare.

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



Utilizzare CUCM_Cluster_Wide_Relying_Party_trust come nome visualizzato e fare clic su **Avanti**.

Add Relying Party Trust Wizard

Specify Display Name

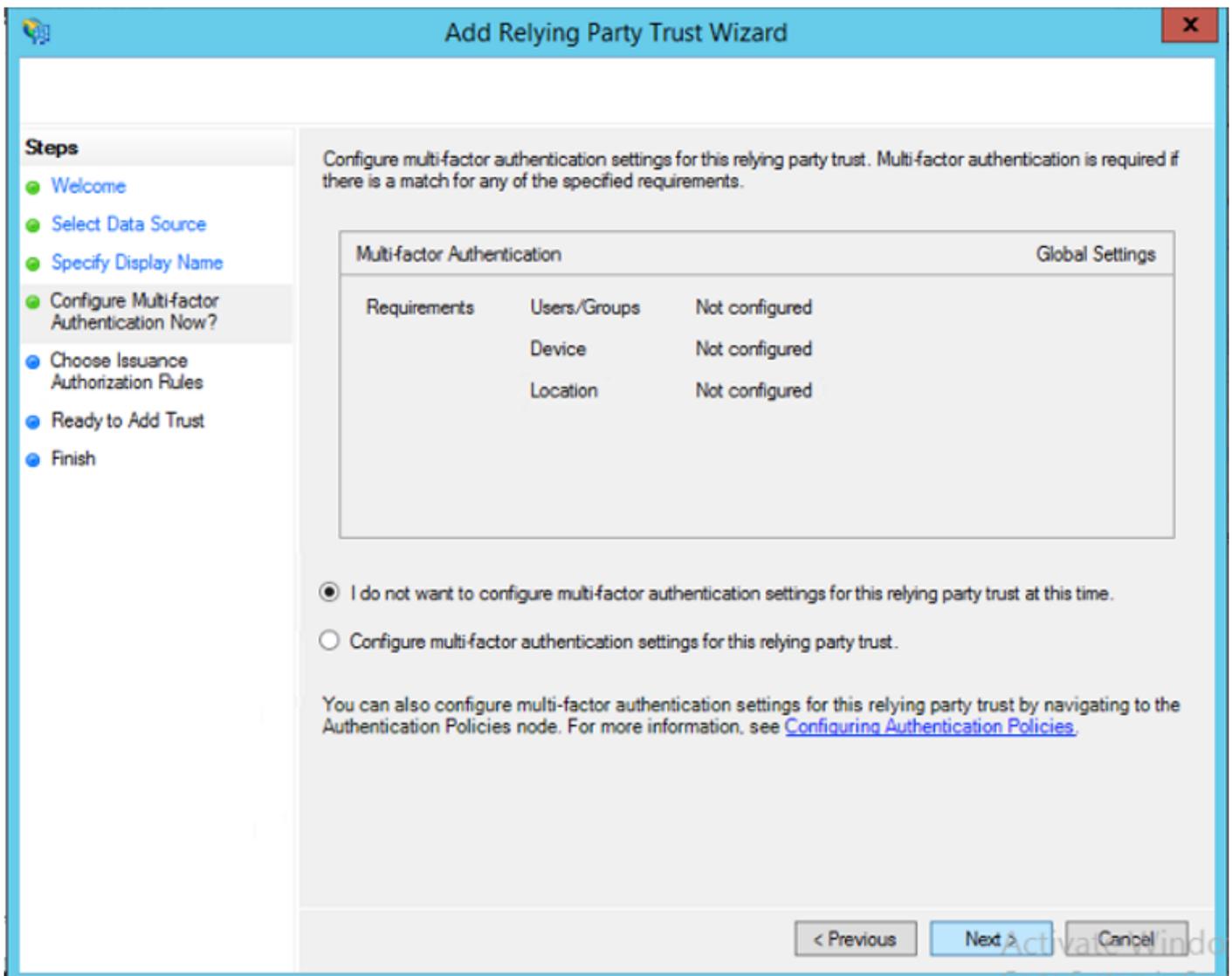
Enter the display name and any optional notes for this relying party.

Display name:

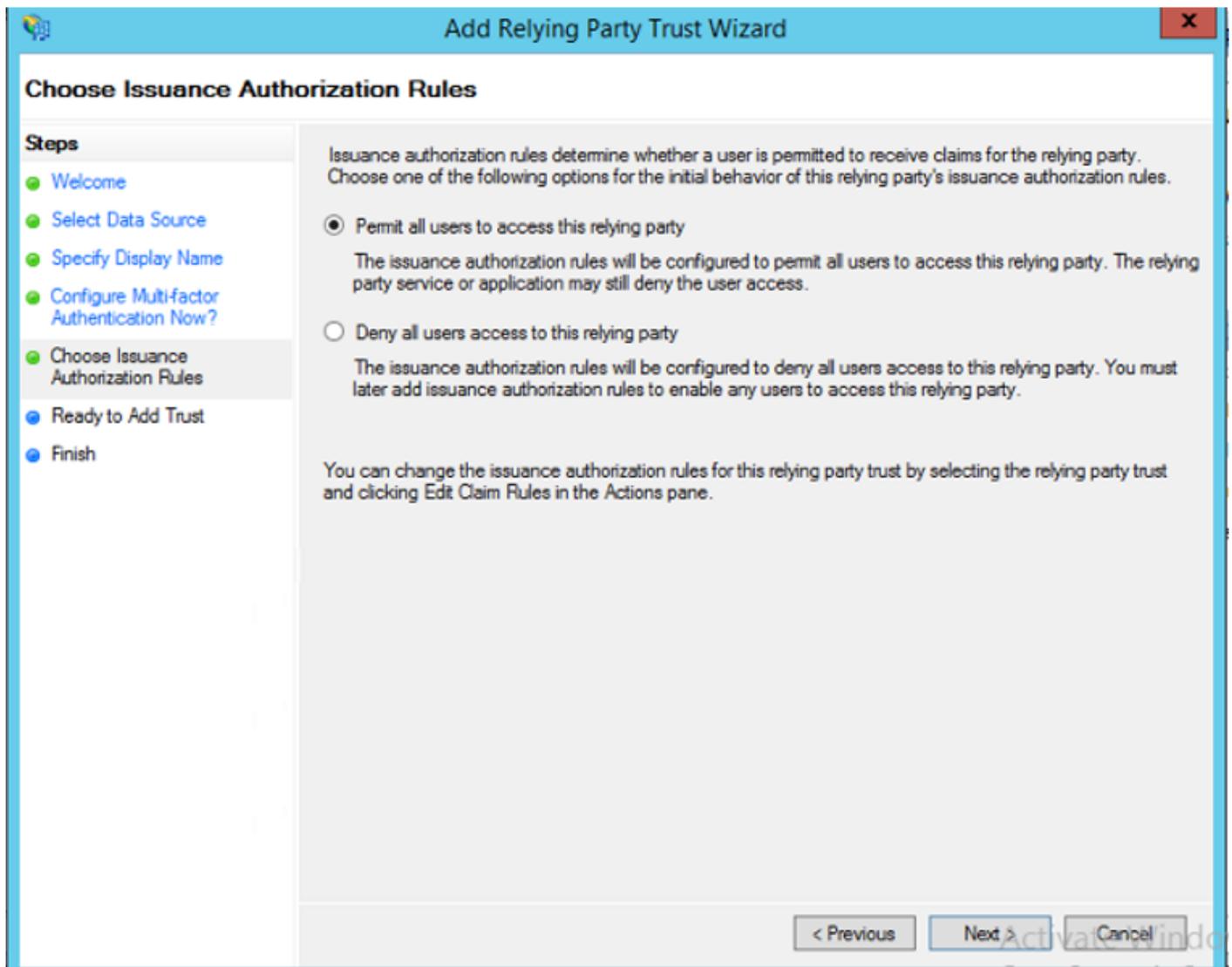
Notes:

< Previous Next > Cancel

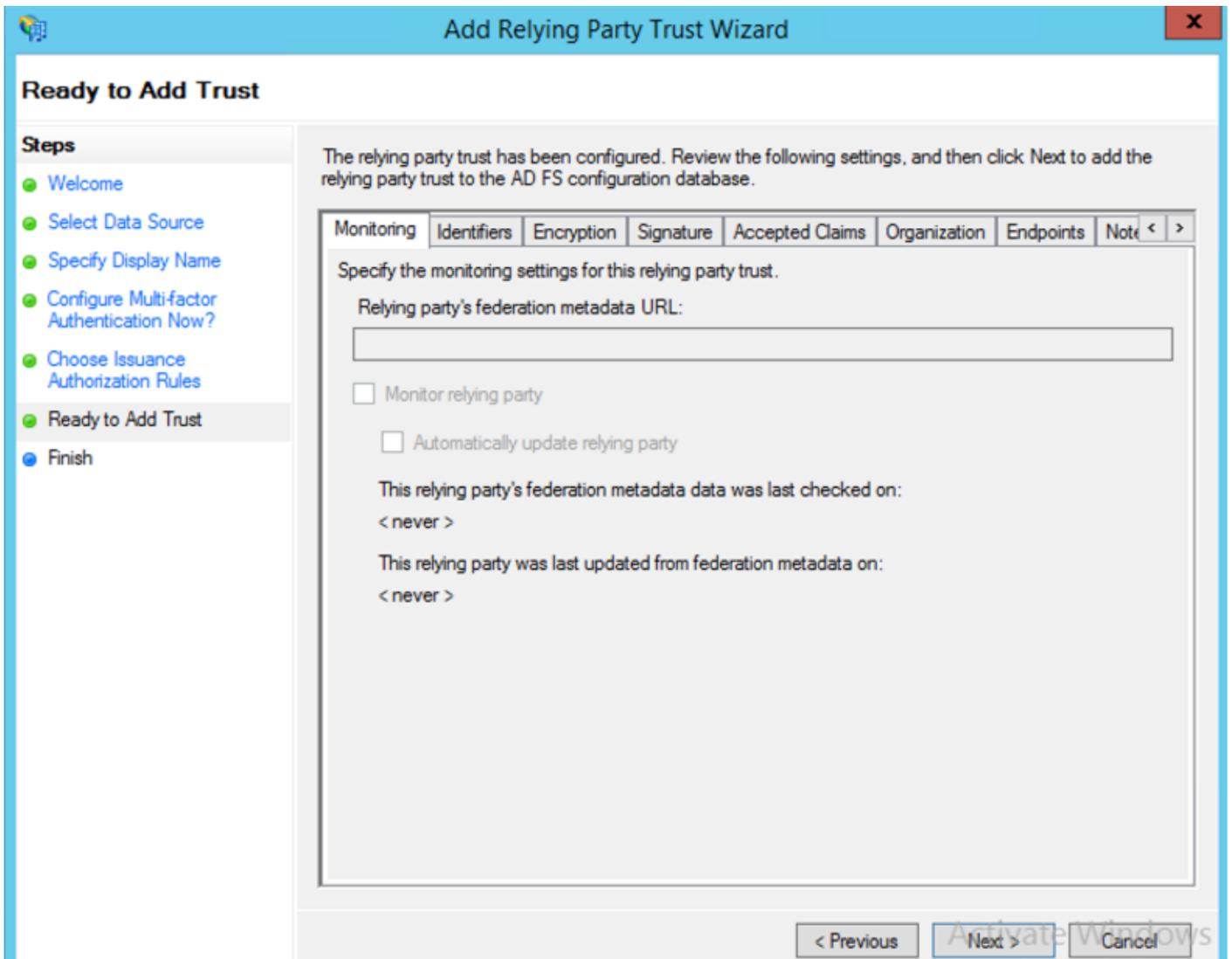
Selezionare la prima opzione e fare clic su **Avanti**.



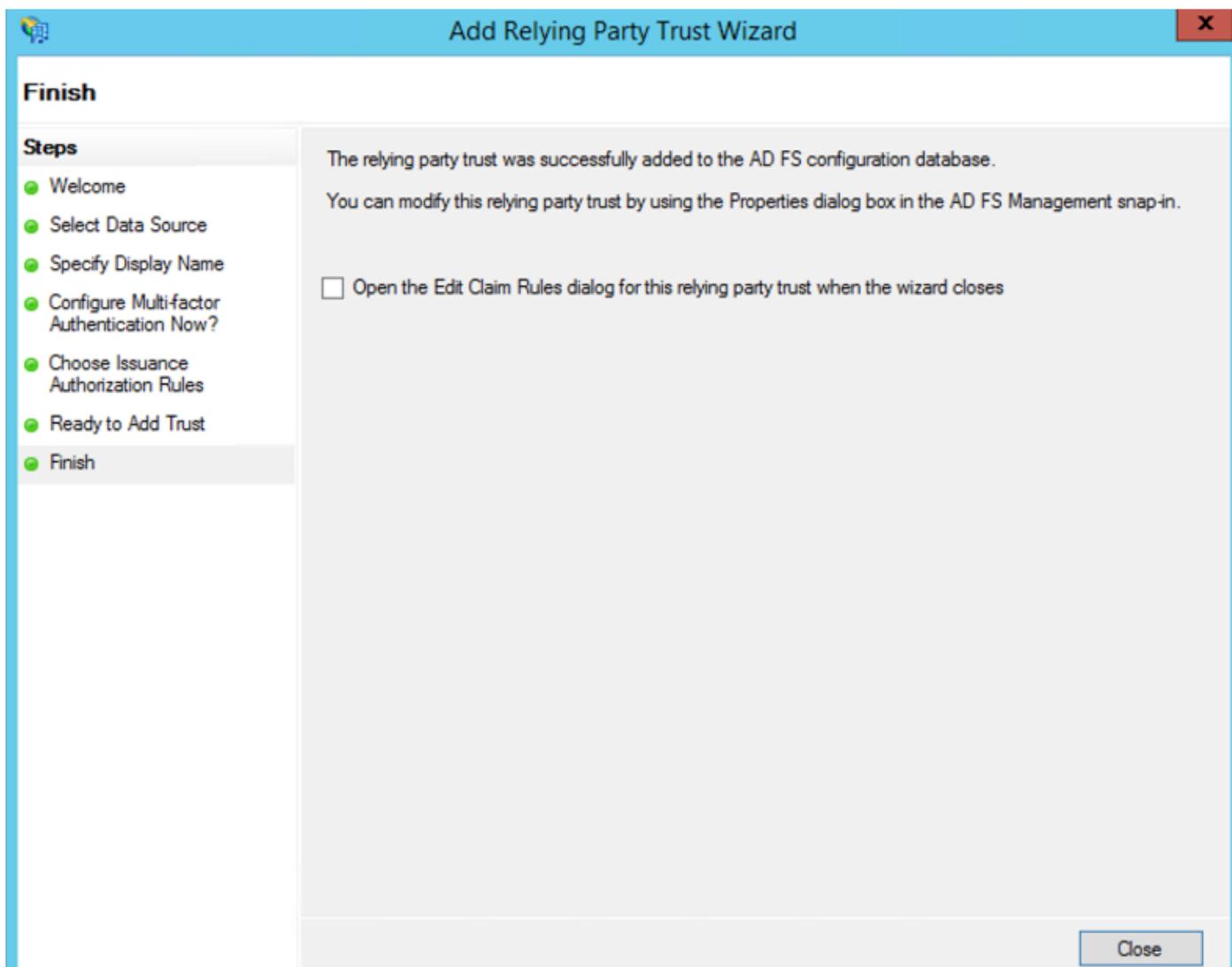
Selezionare **Permetti a tutti gli utenti di accedere a questo componente** e fare clic su **Avanti**, come mostrato nell'immagine.



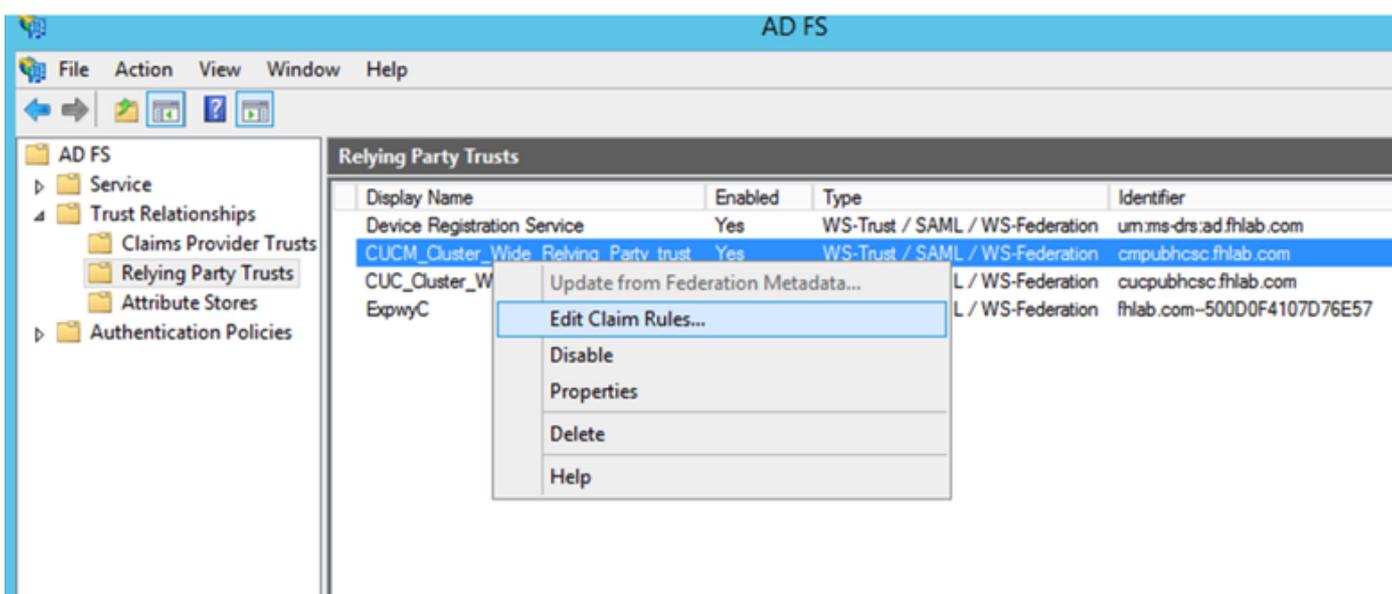
Esaminare la configurazione e fare clic su **Next** (Avanti), come mostrato nell'immagine.



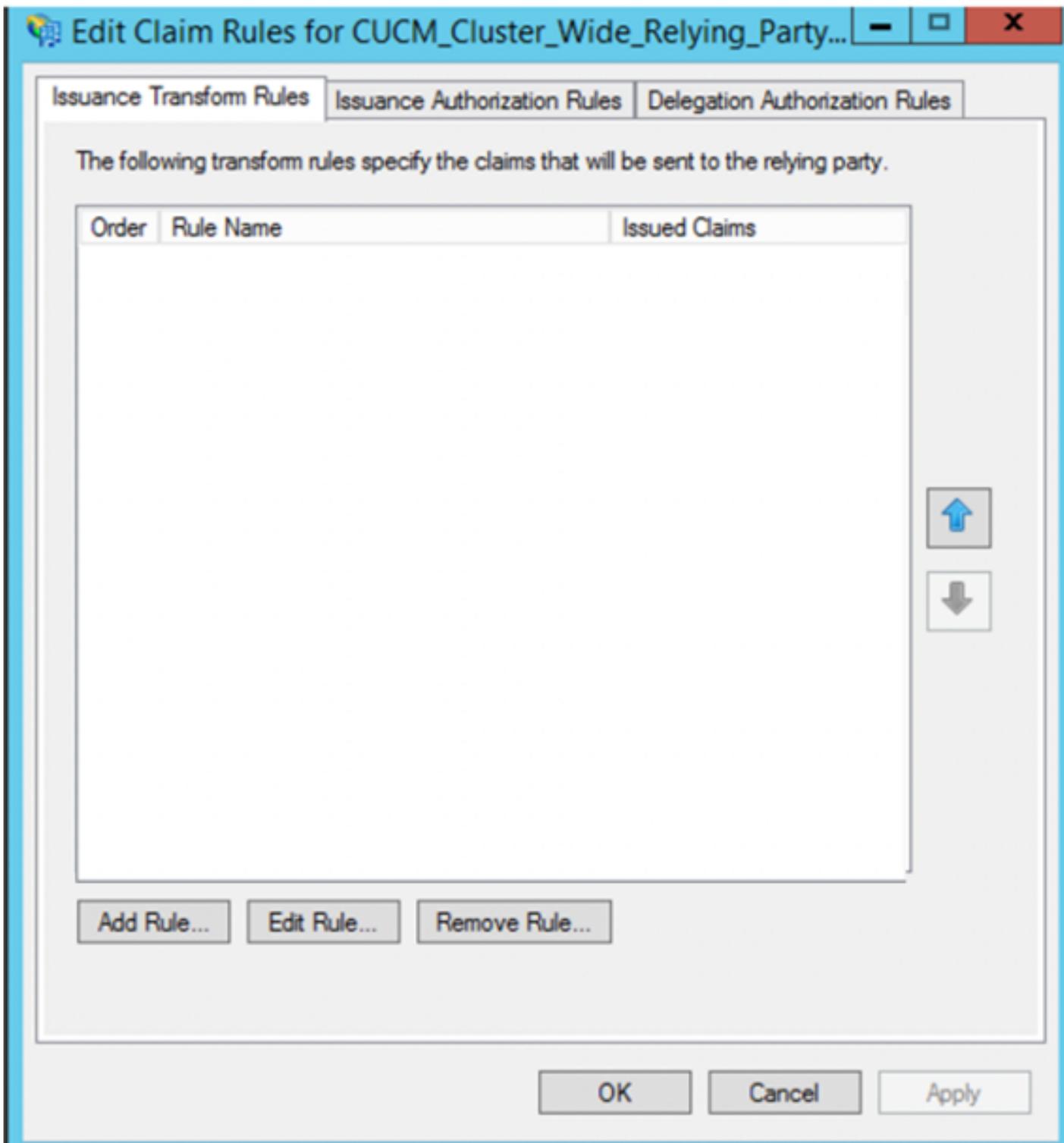
Deselezionare la casella e fare clic su **Chiudi**.



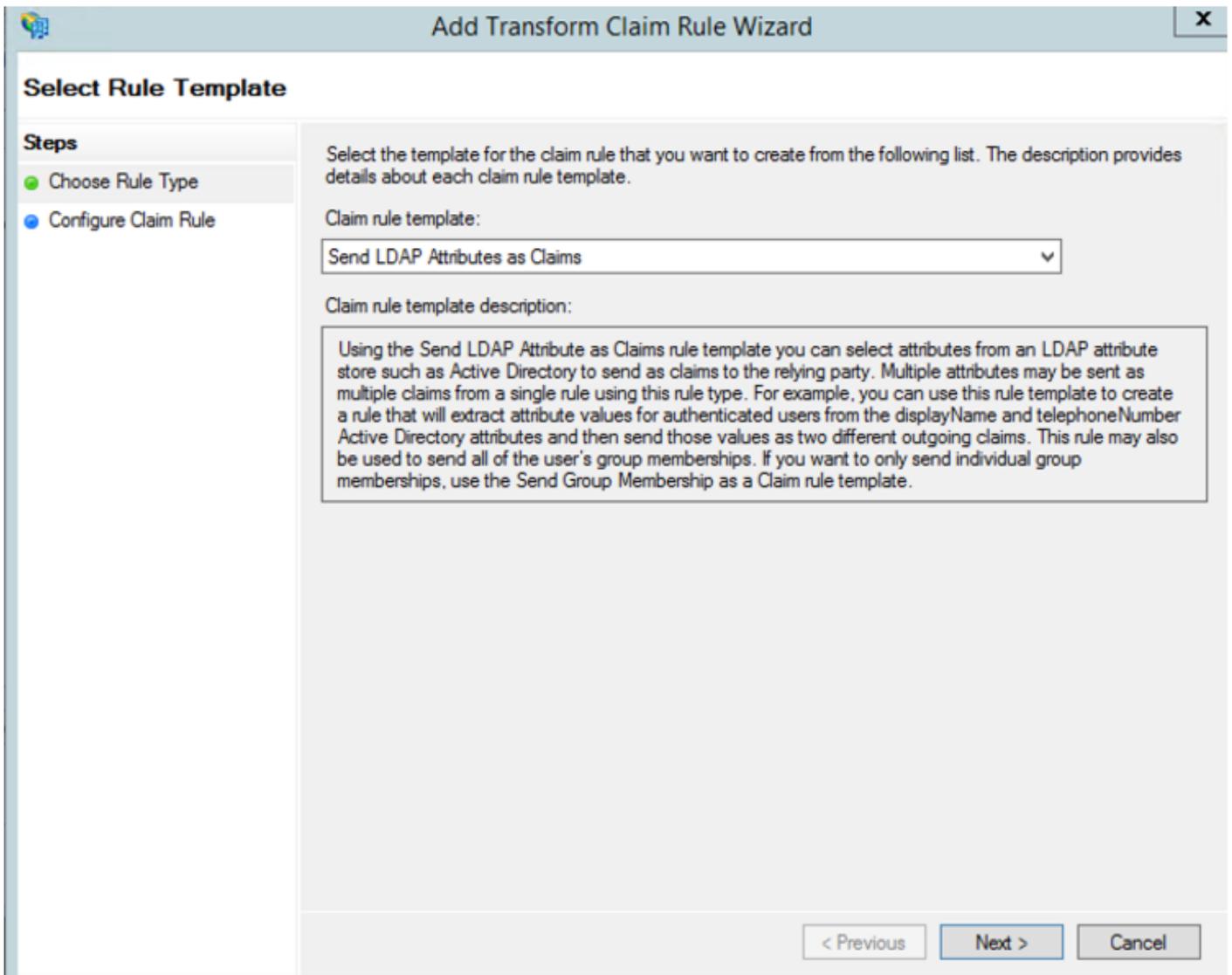
Con il pulsante secondario del mouse, selezionare l'**attendibilità componente** appena creata e **modificare** la configurazione **delle regole attestazione** come mostrato nell'immagine.



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



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



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 Rule - NameID

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

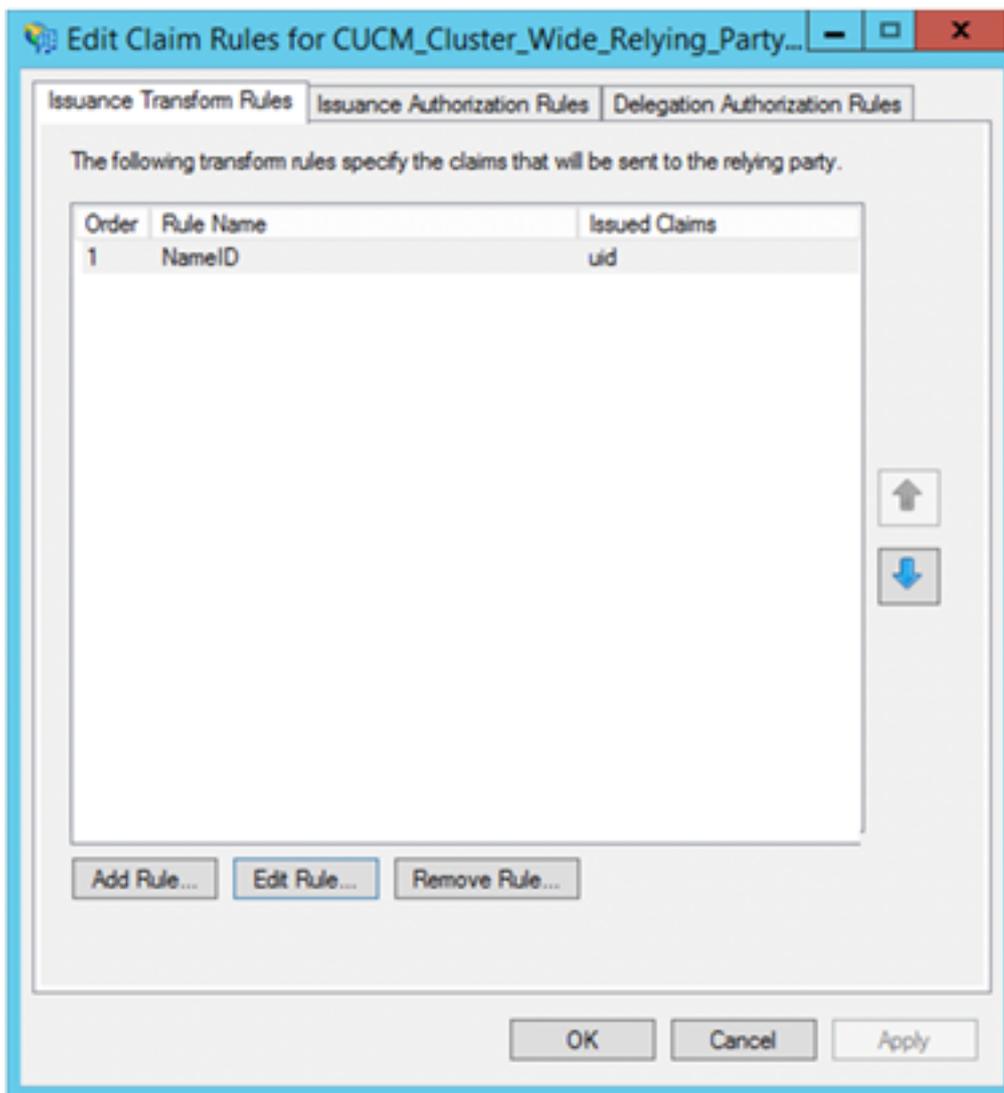
Rule template: Send LDAP Attributes as Claims

Attribute store:

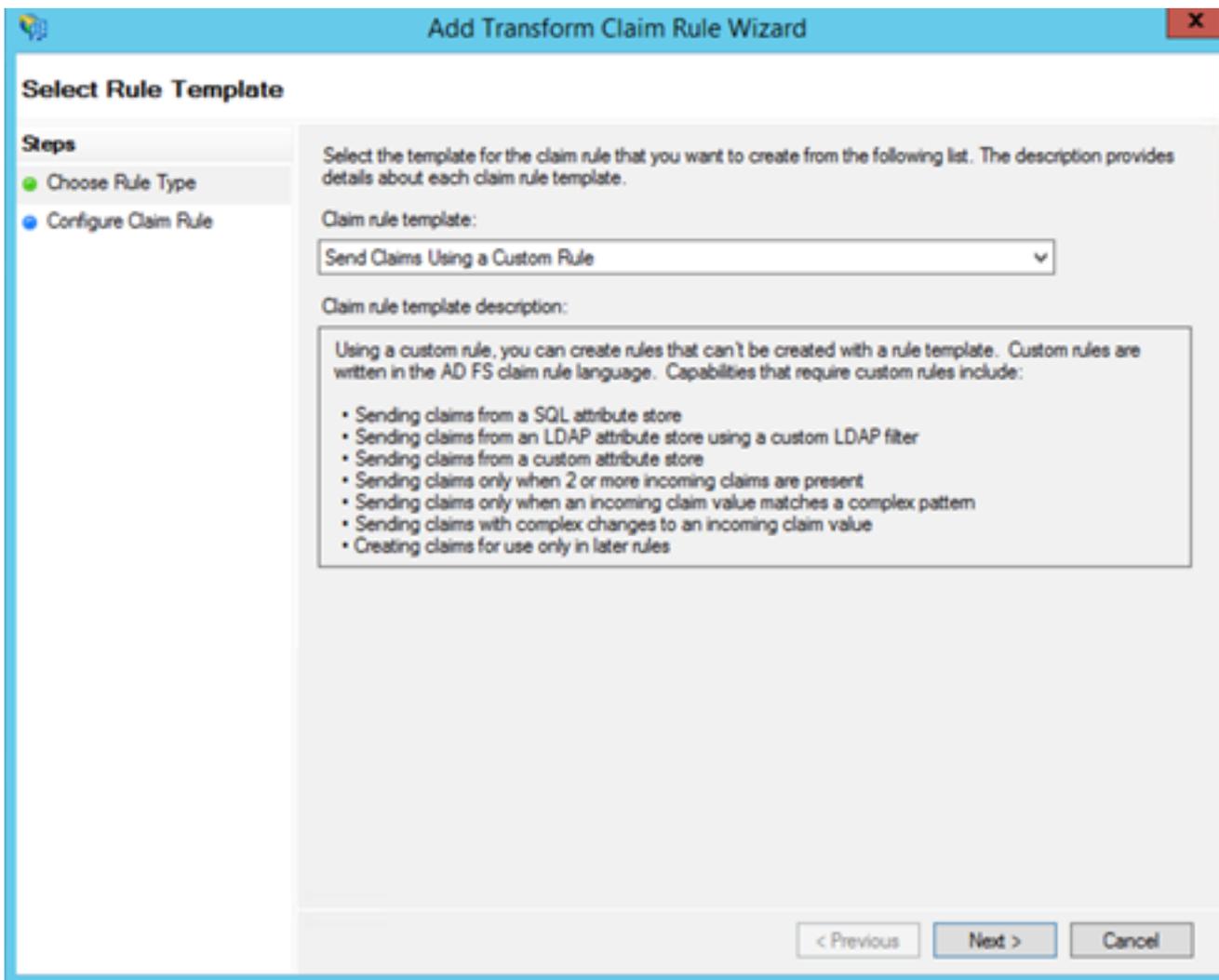
Mapping of LDAP attributes to outgoing claim types:

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

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



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



Creare una regola personalizzata denominata Cluster_Side_Claim_Rule.

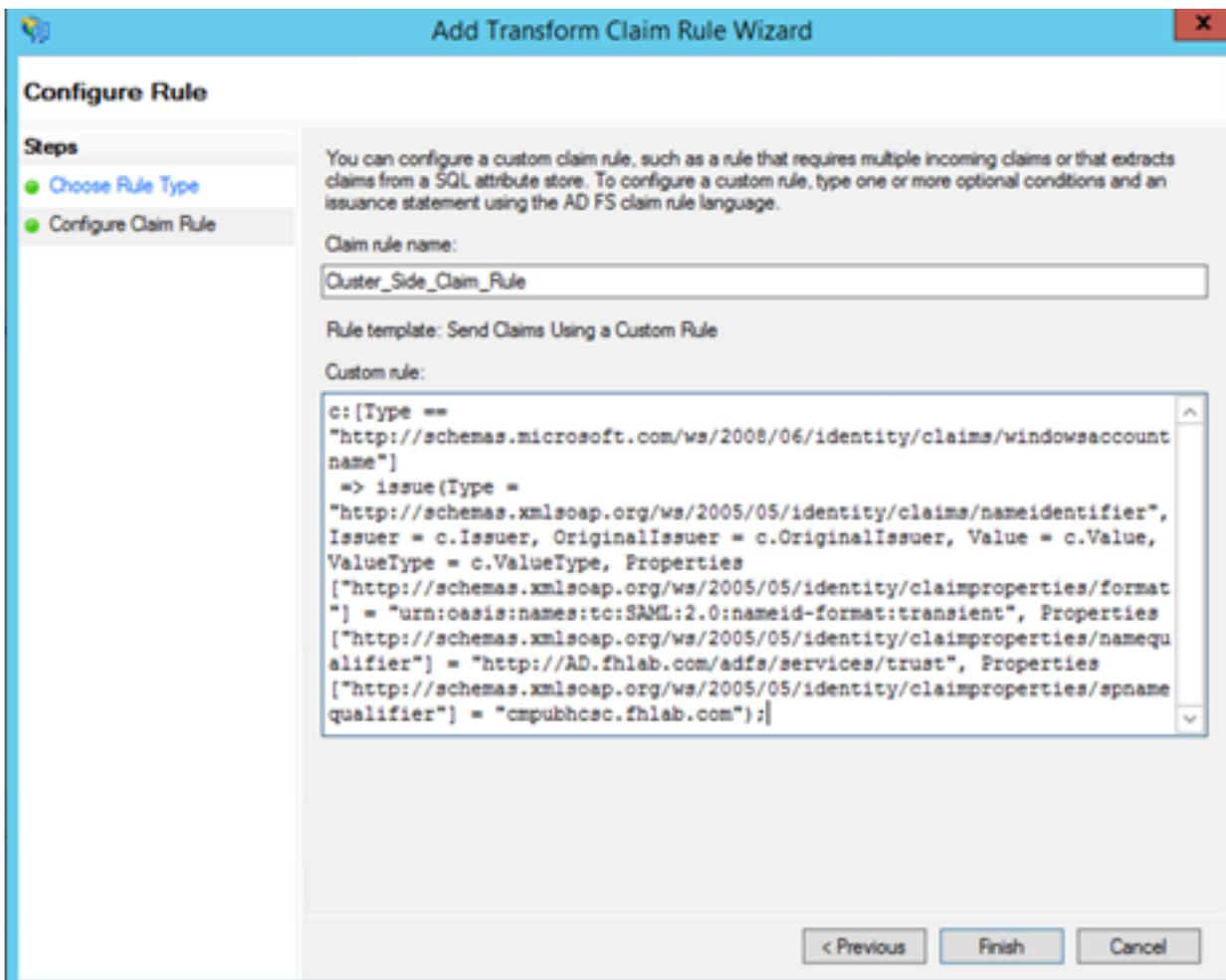
Copiare e incollare il testo nella finestra della regola direttamente da qui. A volte, le virgolette vengono modificate se modificate in un editor di testo e questo renderà la regola errata quando si esegue il test SSO:

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

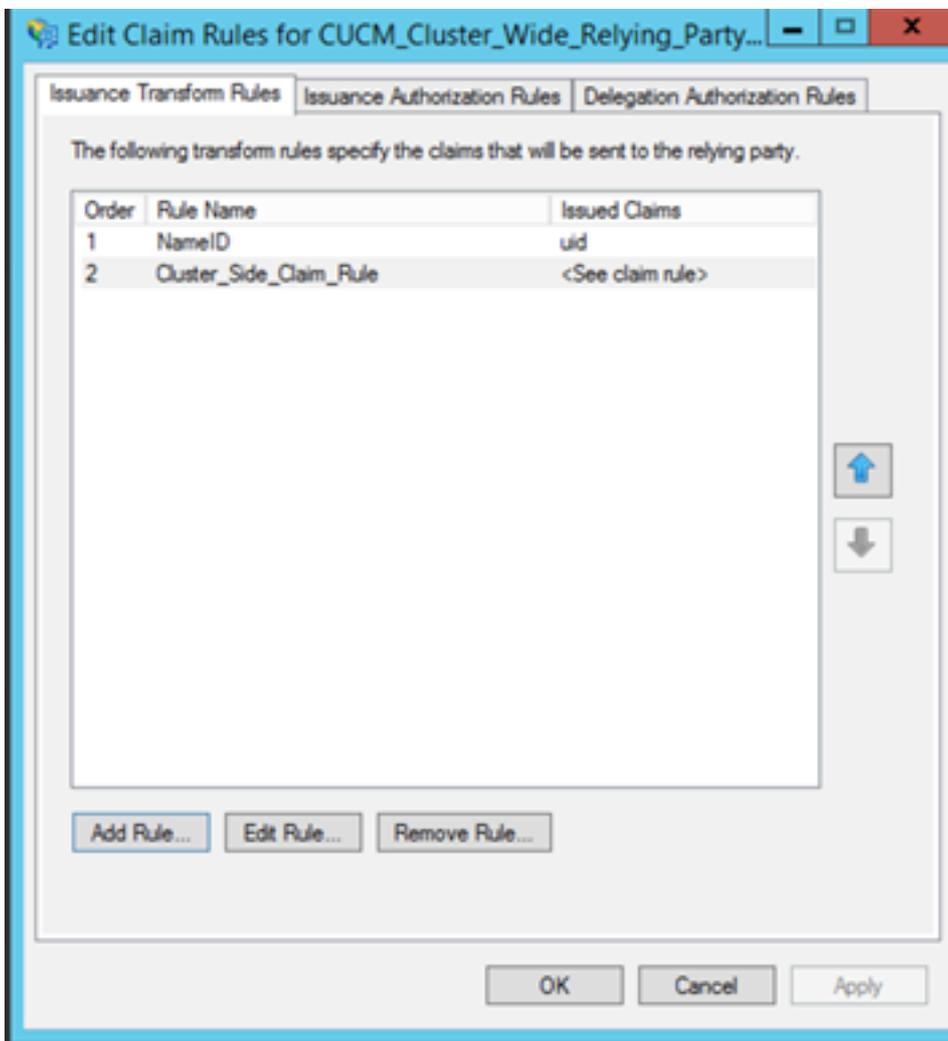
```
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]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

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

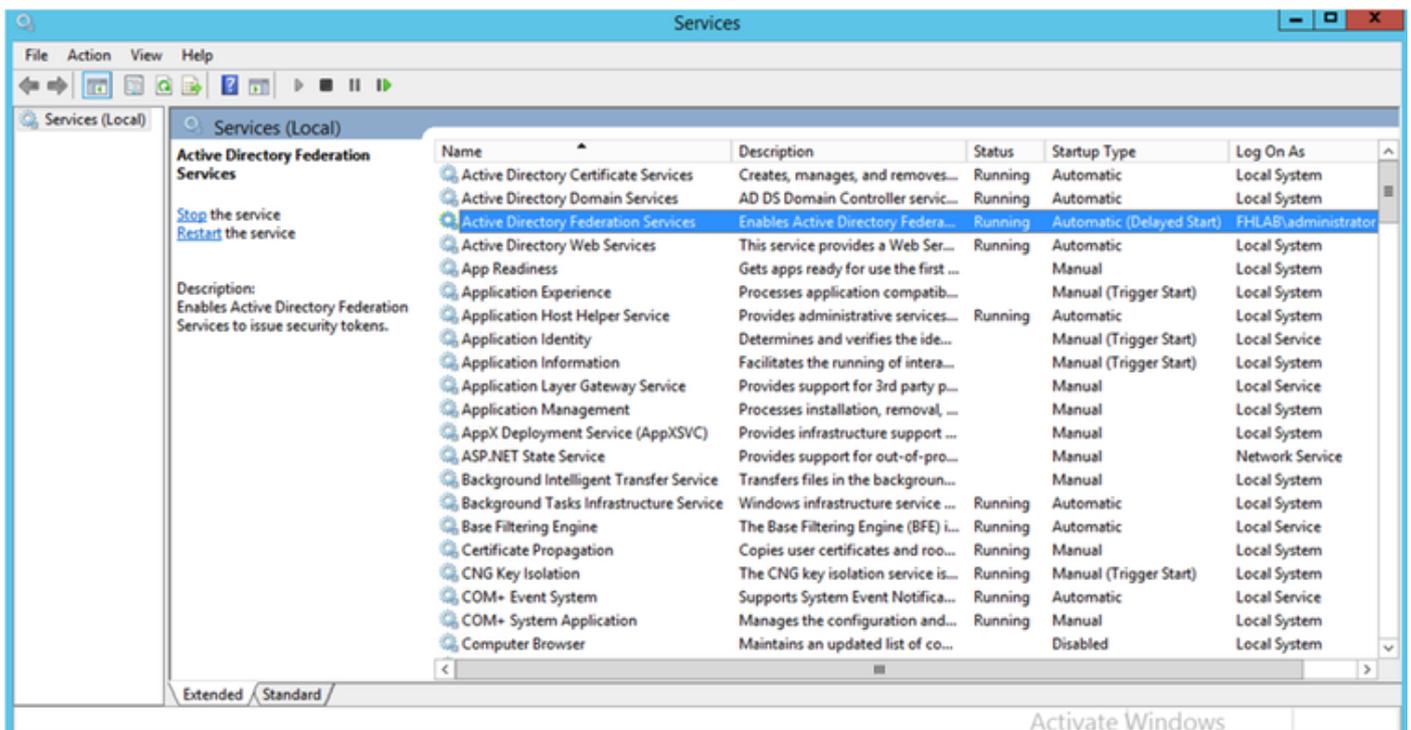
Fare clic su **Fine** per continuare.



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



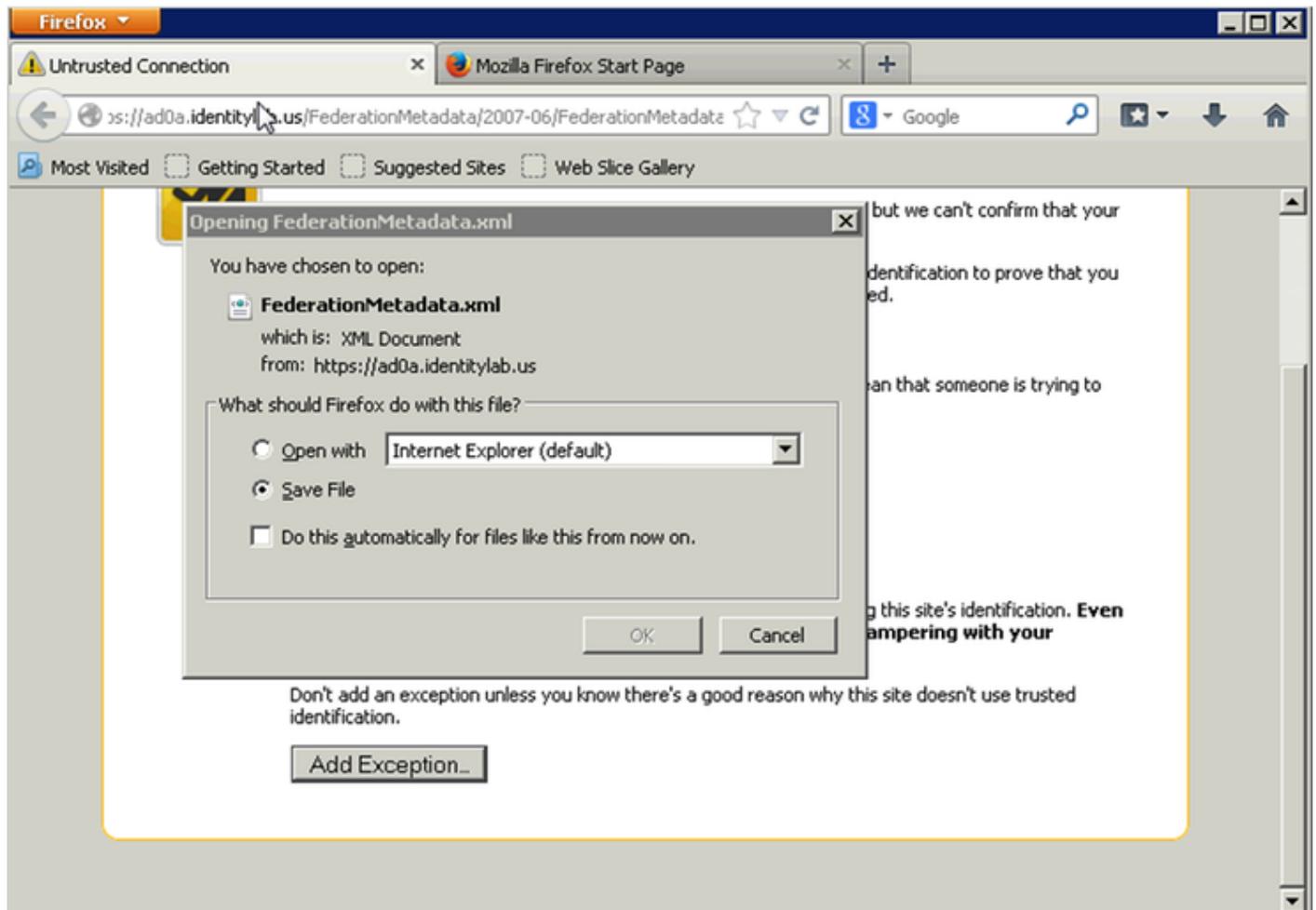
CUCM è stato aggiunto come componente attendibile ad ADFS.



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

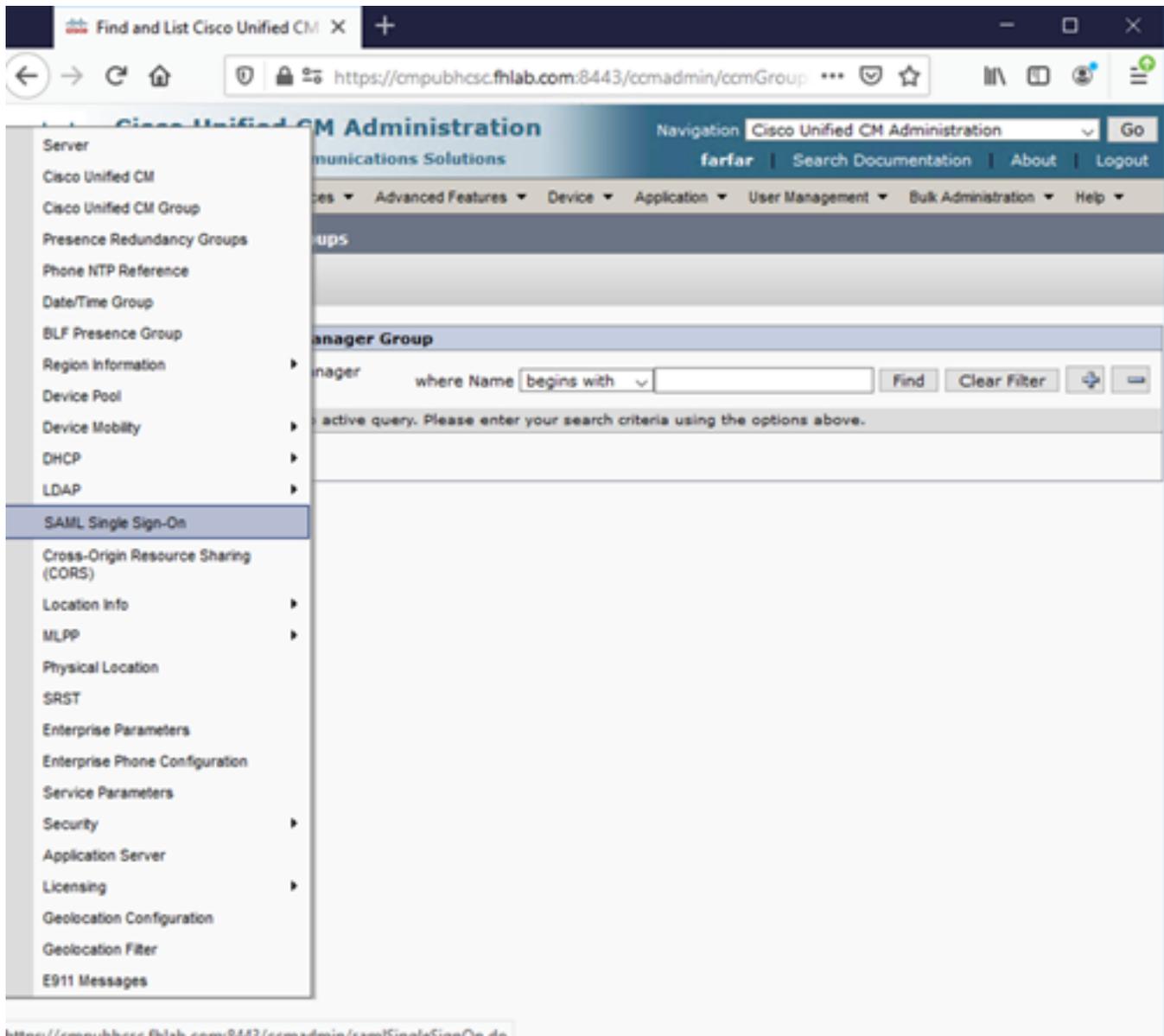
Metadati IDP

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.



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.**



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

The screenshot shows the Cisco Unified CM Administration interface for SAML Single Sign-On. At the top, there are navigation tabs for 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The main heading is 'SAML Single Sign-On'. Below this, there are several action buttons: 'Enable SAML SSO' (with a green checkmark), 'Update IDP Metadata File', 'Export All Metadata', and 'Fix All Disabled Servers'. A 'Status' section indicates 'SAML SSO disabled'. Below the status, there is a table with the following data:

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cucm0a	Disabled	N/A	Never	File	Never	Never

At the bottom right of the table, there is a 'Run Test...' button.

Selezionare **Abilita SSO SAML**.

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

The screenshot shows a 'Reset Warning' dialog box in Mozilla Firefox. The title bar reads 'Reset Warning - Mozilla Firefox'. The URL in the address bar is 'https://cucm0a/ccmadmin/genericDialogWindow.do?windowTitleKey=genericDialogWindow.windowTitle.ssoenable'. The main content of the dialog is as follows:

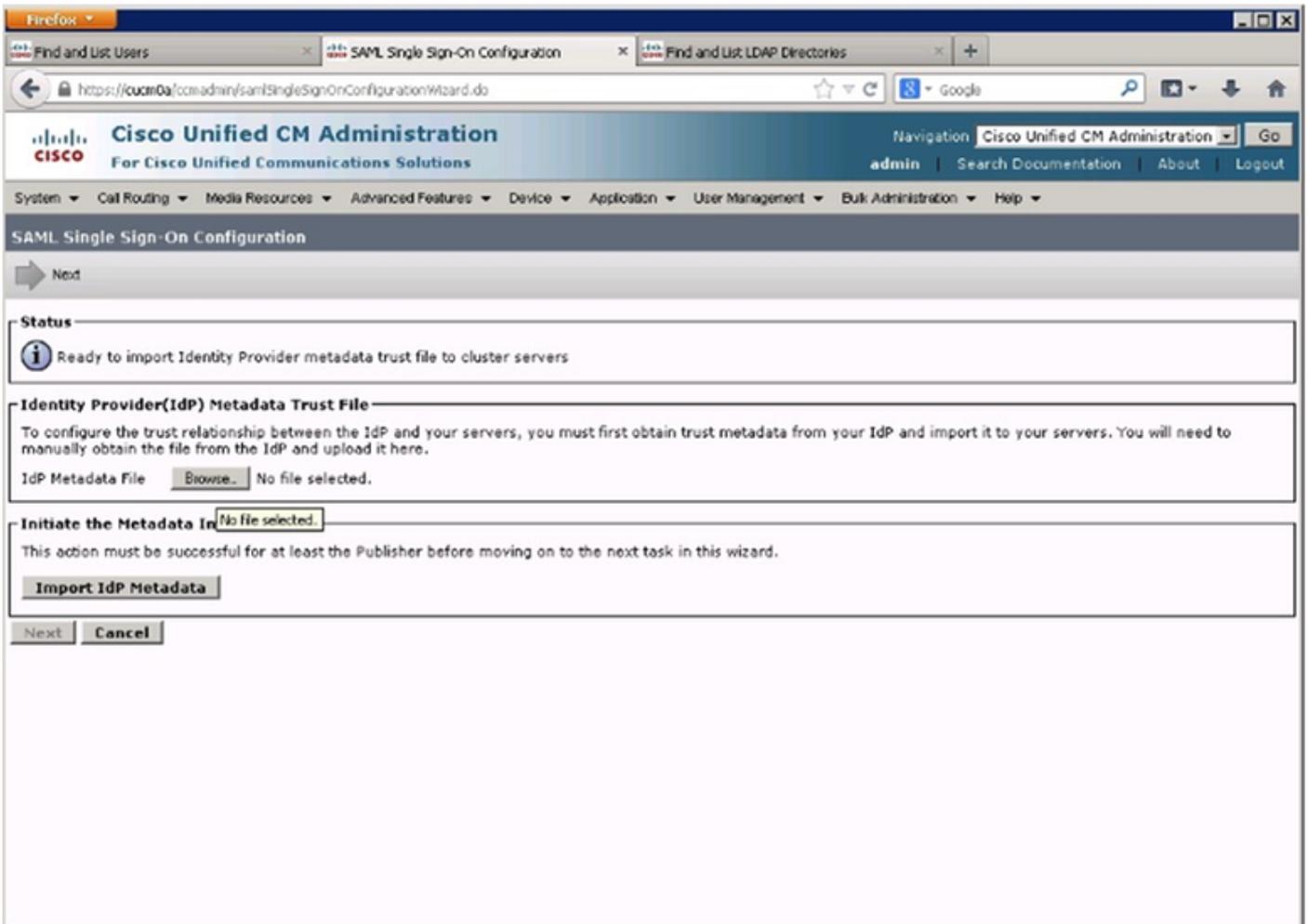
Web server connections will be restarted

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 in again.

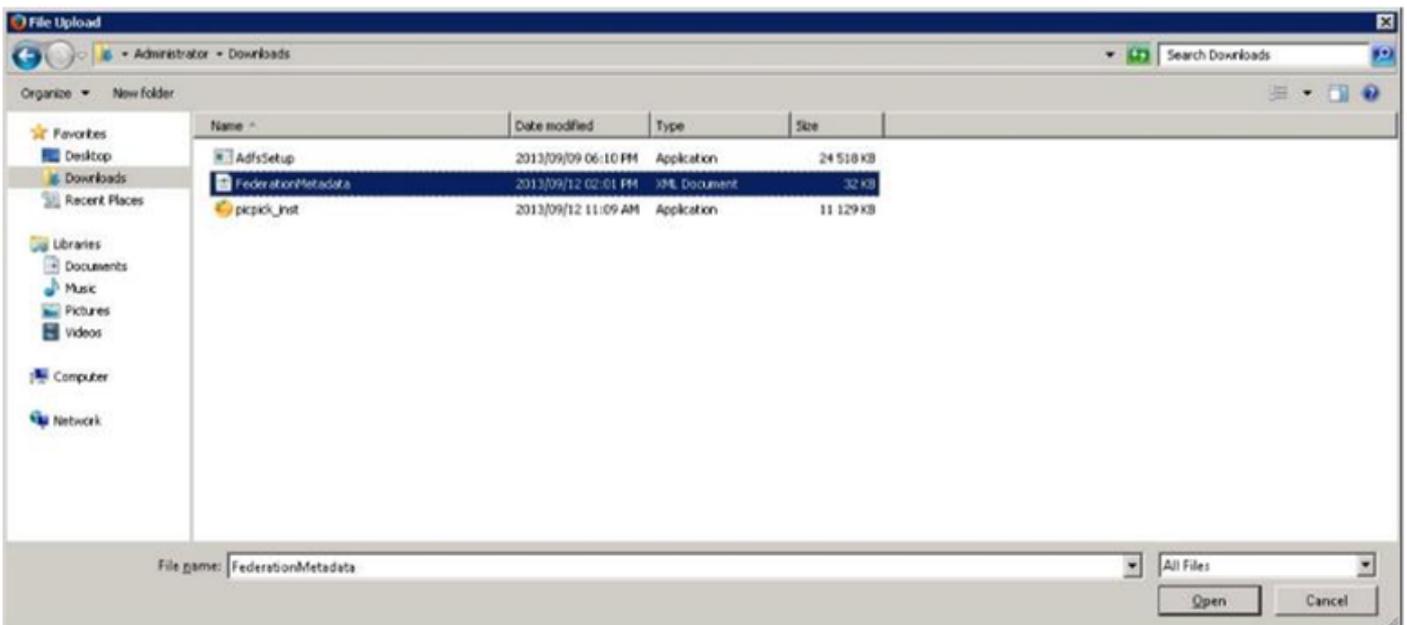
At the bottom right, there are two buttons: 'Continue' and 'Cancel'.

Nella schermata SSO e fare clic su **Sfoggia..** per importare il file XML di metadati

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



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



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

Navigation Cisco Unified CM Administration Go

admin | Search Documentation | About | Logout

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

SAML Single Sign-On Configuration

Next

Status

✓ Import succeeded for all servers

Identity Provider(IdP) Metadata Trust File

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

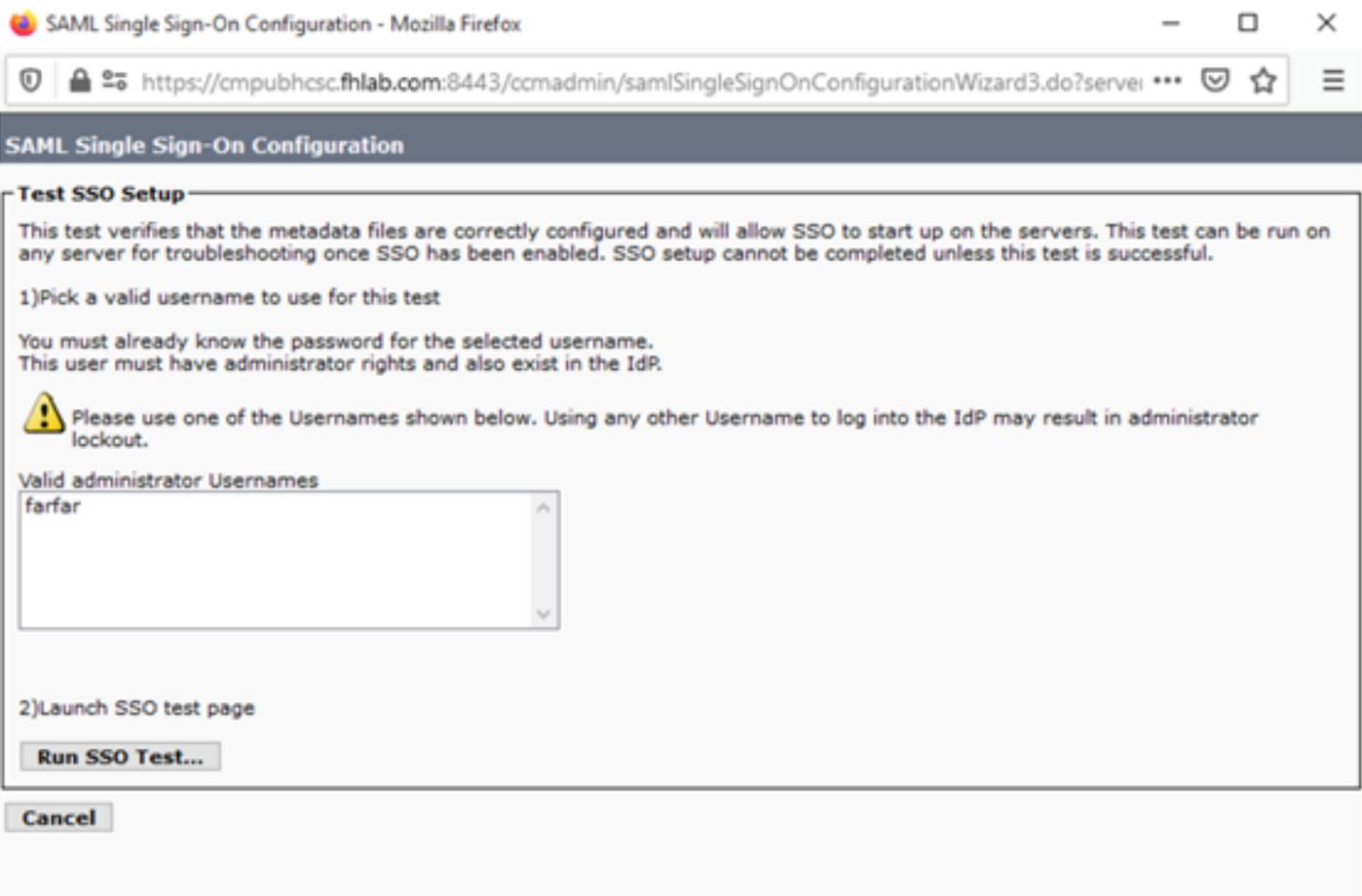
IdP Metadata File Browse...

Initiate the Metadata Import

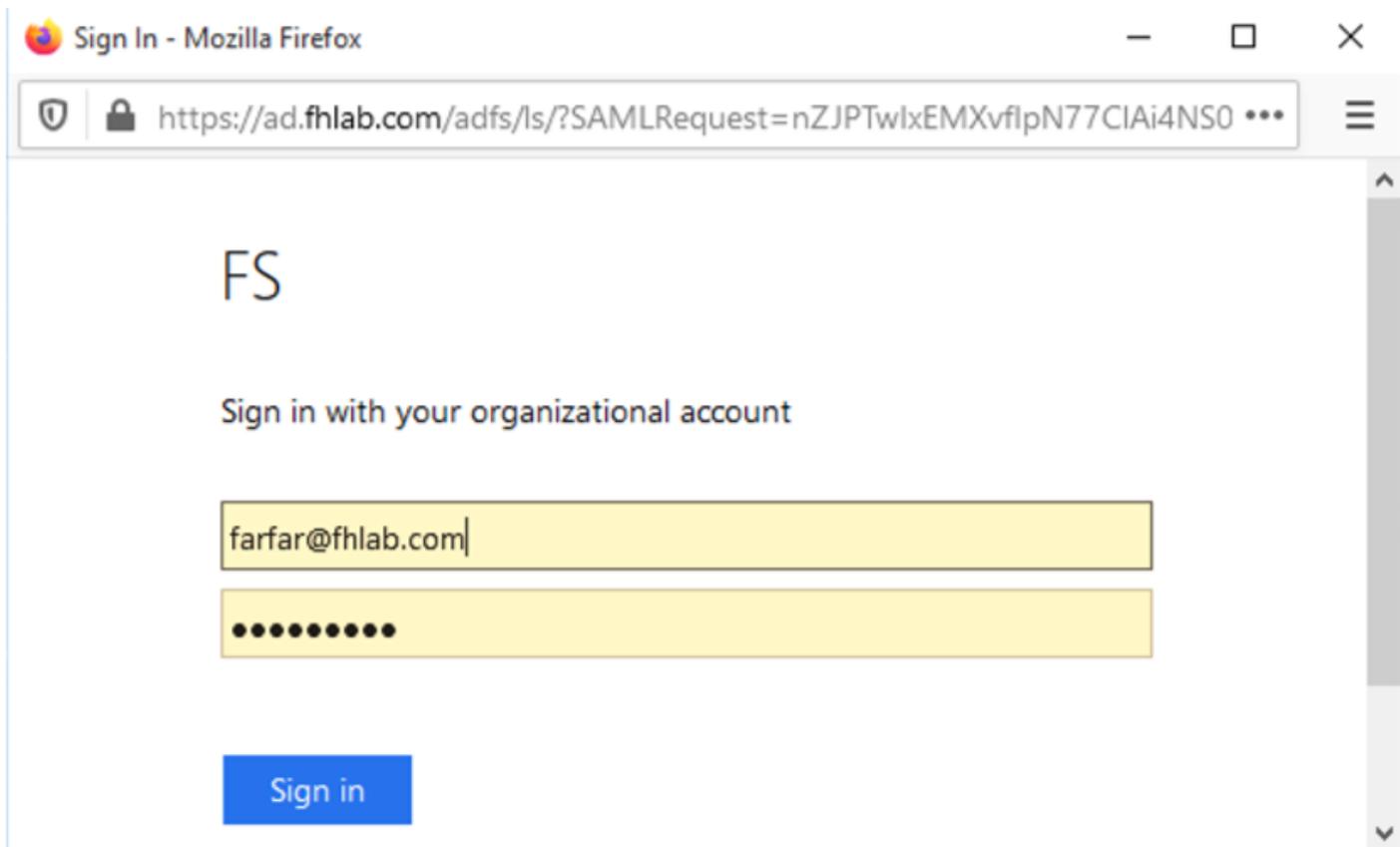
This action must be successful for at least the Publisher before moving on to the next task in this wizard.

✓ Import succeeded for all servers

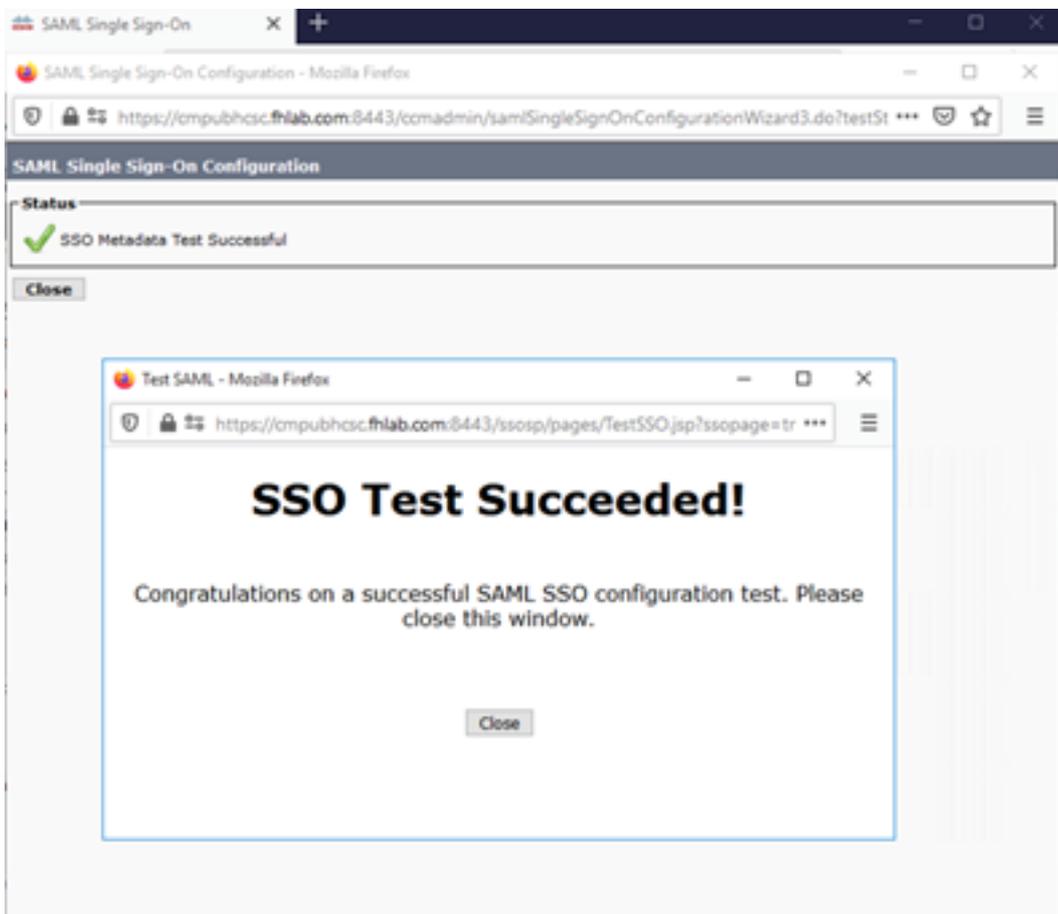
Selezionare l'utente appartenente agli utenti privilegiati CCM standard e fare clic su ESEGUI TEST SSO.



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



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



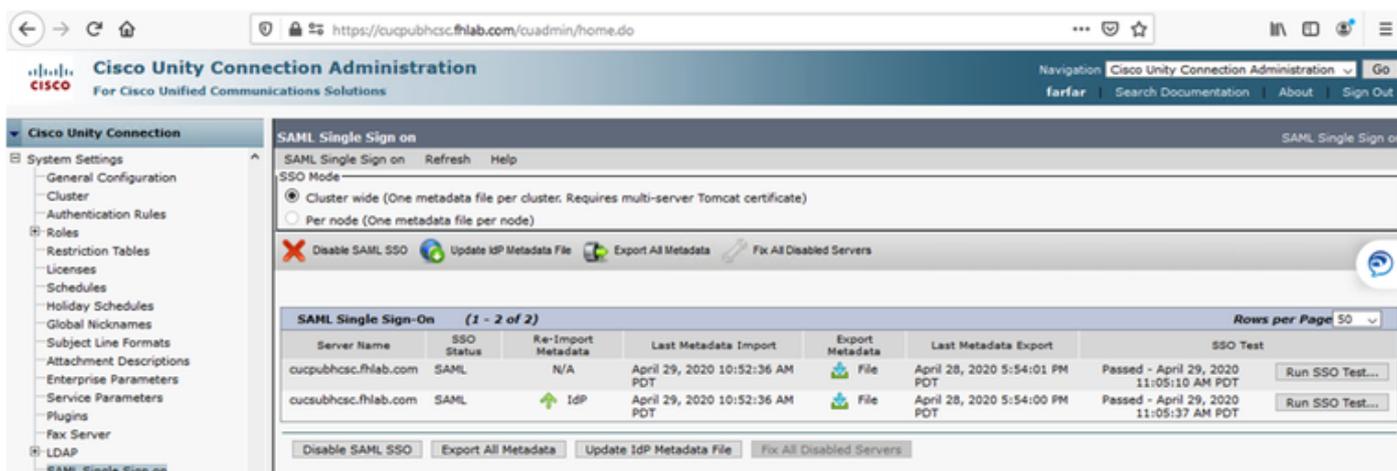
Fare clic su CLOSE e FINISH per continuare.

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

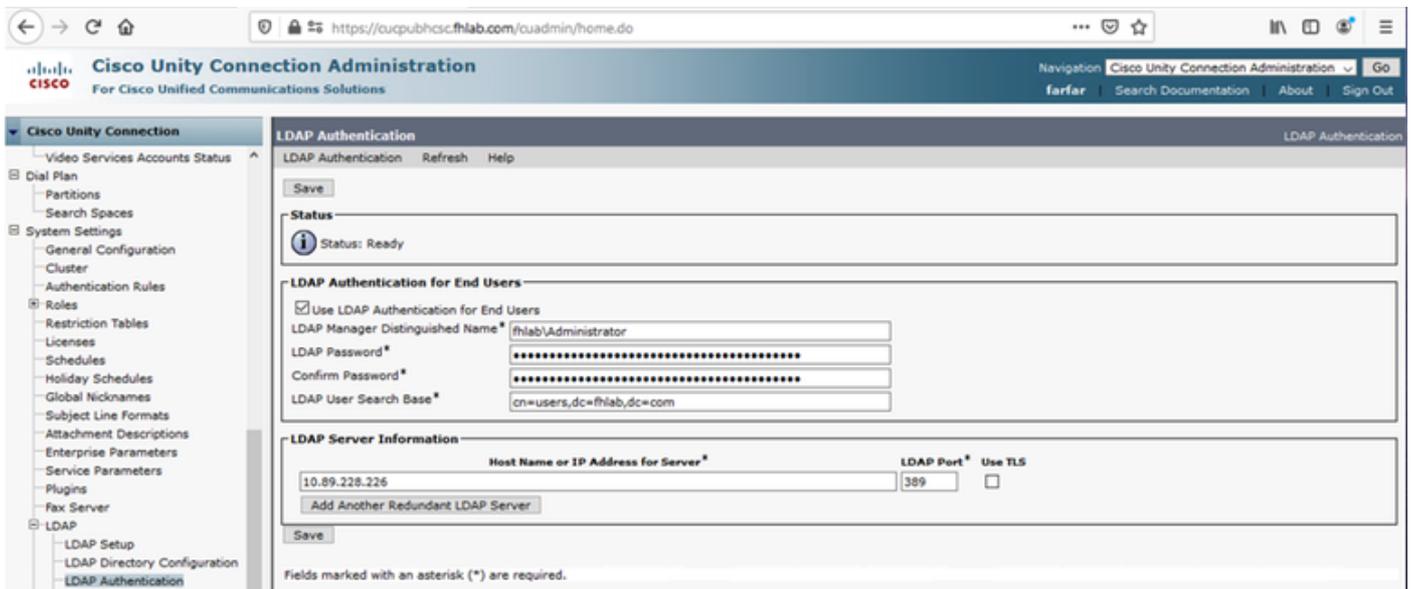
Configura SSO su CUC

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

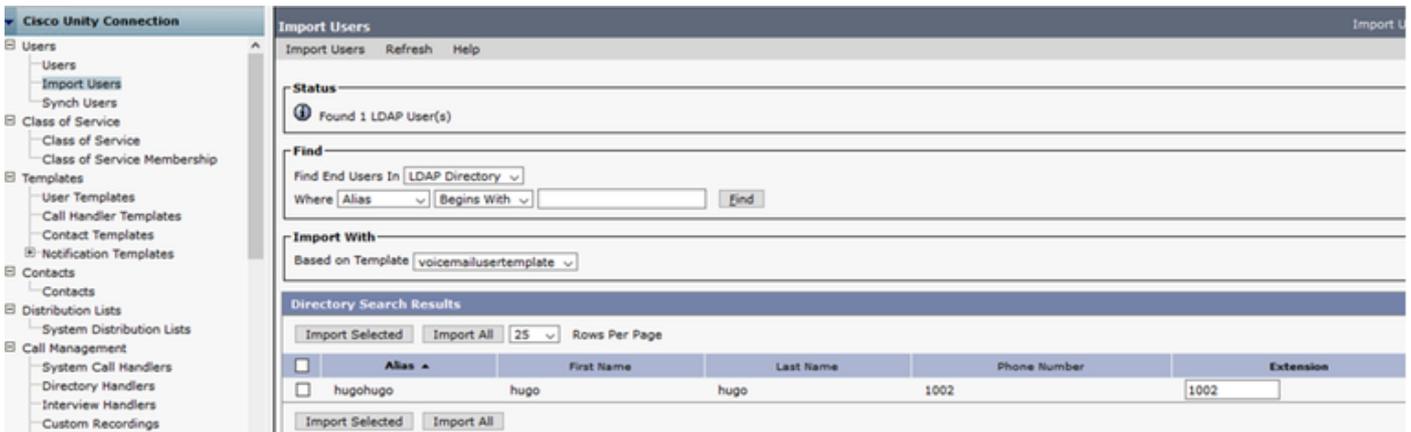
Integrazione LDAP con CUC.



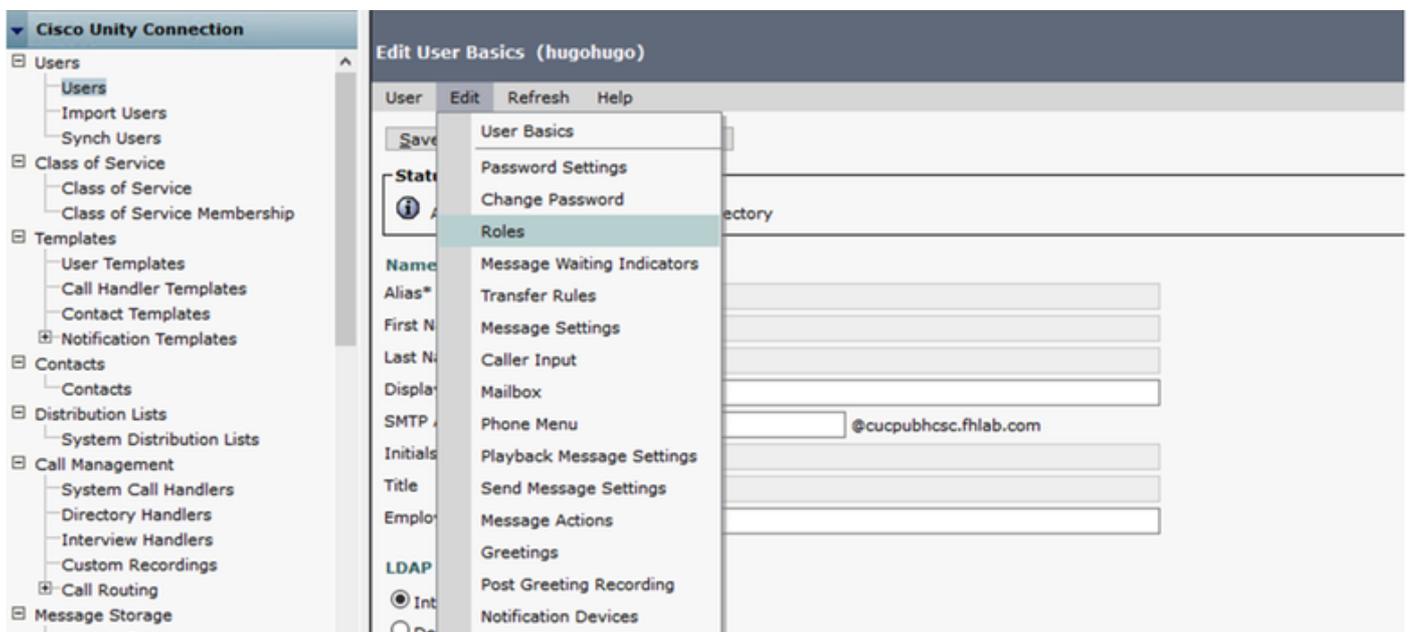
Configurare l'autenticazione LDAP.



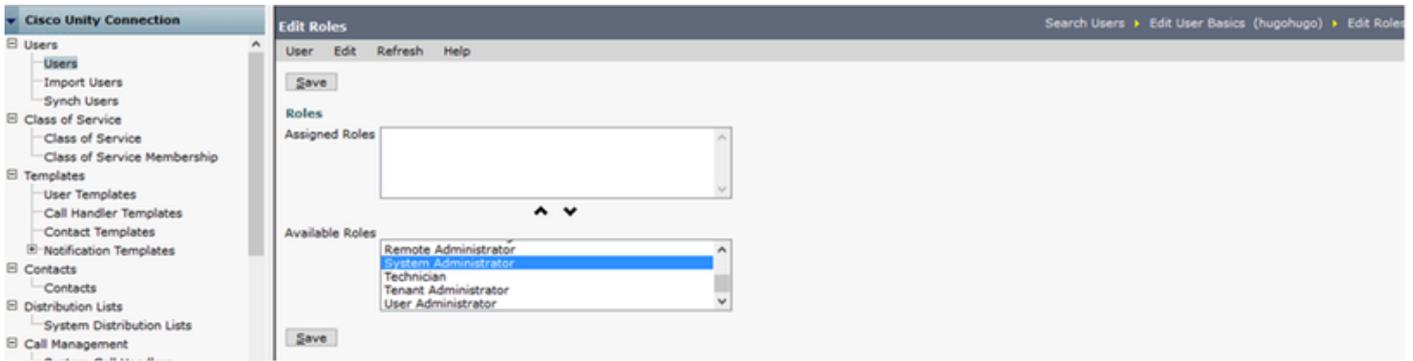
Importare gli utenti da LDAP a cui verranno assegnati i messaggi vocali e l'utente che verrà utilizzato per il test dell'SSO.



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

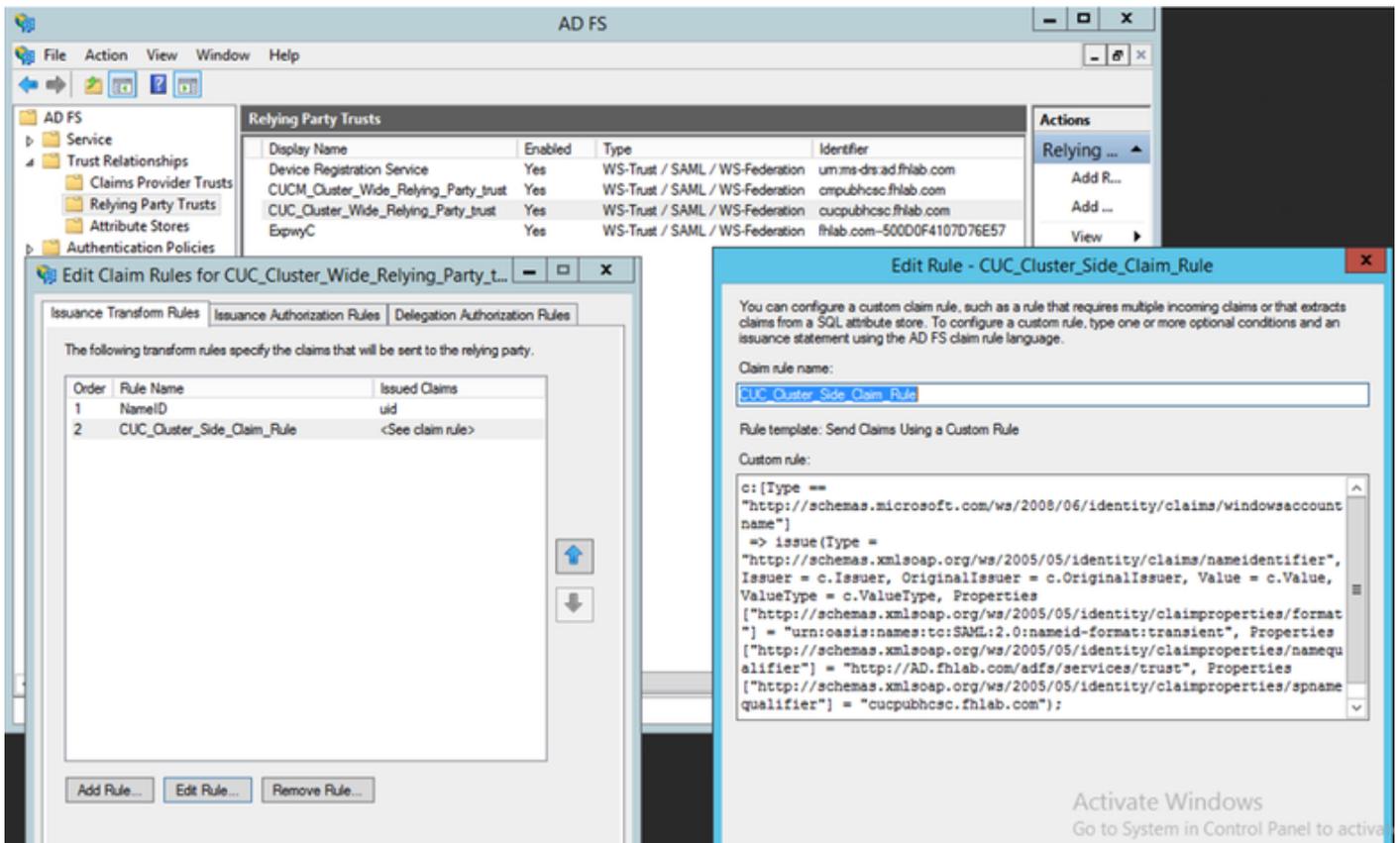


Assegnare all'utente che esegue il test il ruolo di amministratore di sistema.



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 Single Sign on Configuration - Mozilla Firefox

https://cucpubhsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?serverName: ...

SAML Single Sign on Configuration

SAML Single Sign on Configuration Refresh Help

Test SSO Setup

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be run on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is successful.

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 administrator lockout.

Valid administrator Usernames

- farfar
- hugohugo

2) Launch SSO test page

Run SSO Test...

Cancel

SAML Single Sign on Configuration - Mozilla Firefox

https://cucpubhsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?testStatus=1 ...

SAML Single Sign on Configuration

SAML Single Sign on Configuration Refresh Help

Status

SSO Metadata Test Successful

Test SAML - Mozilla Firefox

https://cucpubhsc.fhlab.com/ssosp/pages/TestSSO.jsp?ssopage=true

SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test. Please close this window.

Close

Navigation Cisco Unity Connection Administration Go

farfar Search Documentation About Sign Out

SAML Single Sign on

Rows per Page 50

port data	Last Metadata Export	SSO Test
File	April 28, 2020 5:54:01 PM PDT	Passed - May 24, 2020 3:17:04 PM PDT Run SSO Test...
File	April 28, 2020 5:54:00 PM PDT	Passed - April 29, 2020 11:05:37 AM PDT Run SSO Test...

Servers

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.

The screenshot displays the Cisco Expressway configuration interface. On the left, a tree view shows the navigation path: AD FS > Trust Relationships > Relying Party Trusts. The main area is divided into two panes. The top pane, titled 'Relying Party Trusts', contains a table with the following data:

Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-Trust / SAML / WS-Federation	um.ms-drs.ad.fhlab.com
CUCM_Cluster_Wide_Relying_Party_trust	Yes	WS-Trust / SAML / WS-Federation	cmpubhcsc.fhlab.com
CUC_Cluster_Wide_Relying_Party_trust	Yes	WS-Trust / SAML / WS-Federation	cucpubhcsc.fhlab.com
ExpwyC	Yes	WS-Trust / SAML / WS-Federation	fhlab.com-500D0F4107D76E57

The bottom pane, titled 'Edit Rule - NameID', shows the configuration for a claim rule. The 'Claim rule name' is 'NameID'. The 'Rule template' is 'Send LDAP Attributes as Claims'. The 'Attribute store' is 'Active Directory'. The 'Mapping of LDAP attributes to outgoing claim types' table is as follows:

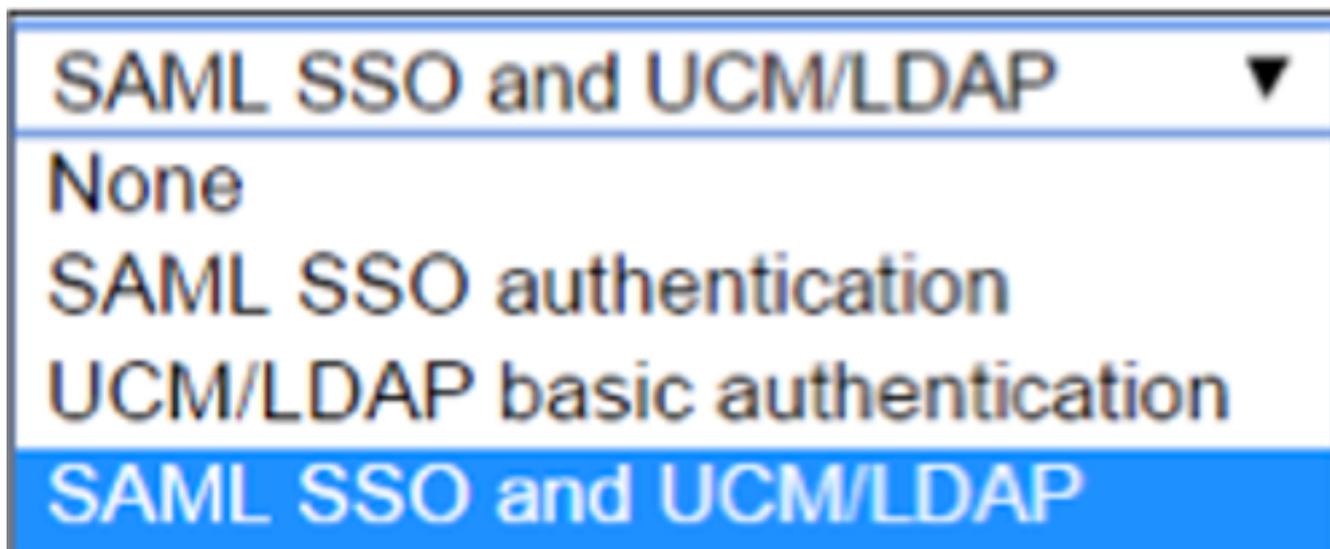
LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
SAM-Account-Name	uid
*	*

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		
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

Percorso di autenticazione



- 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

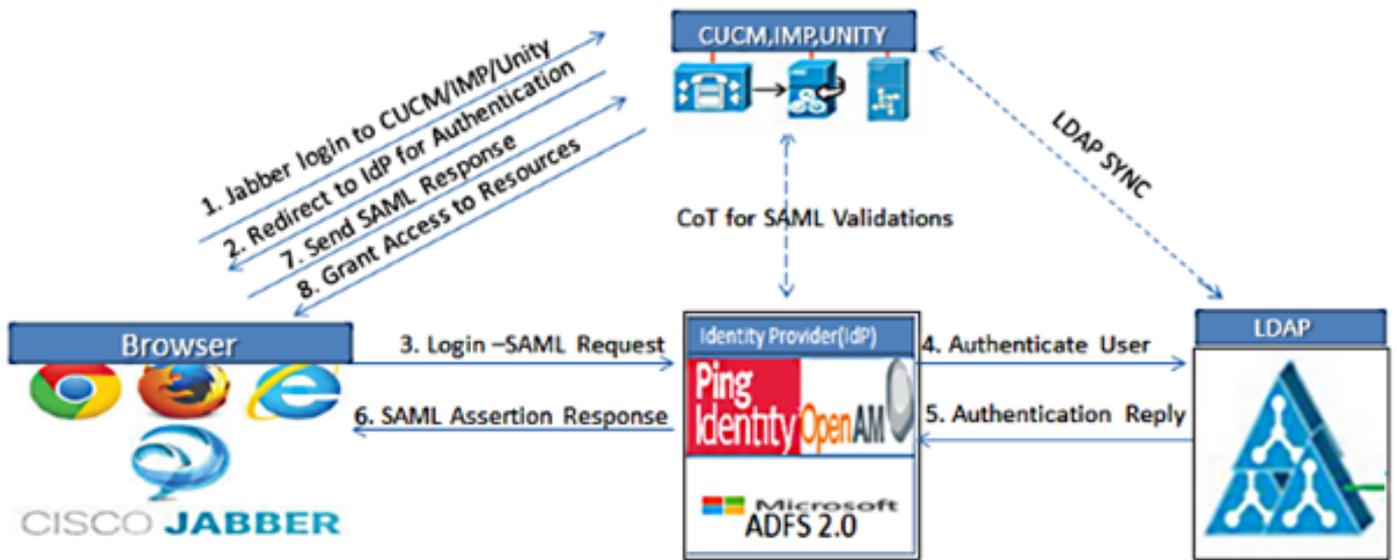
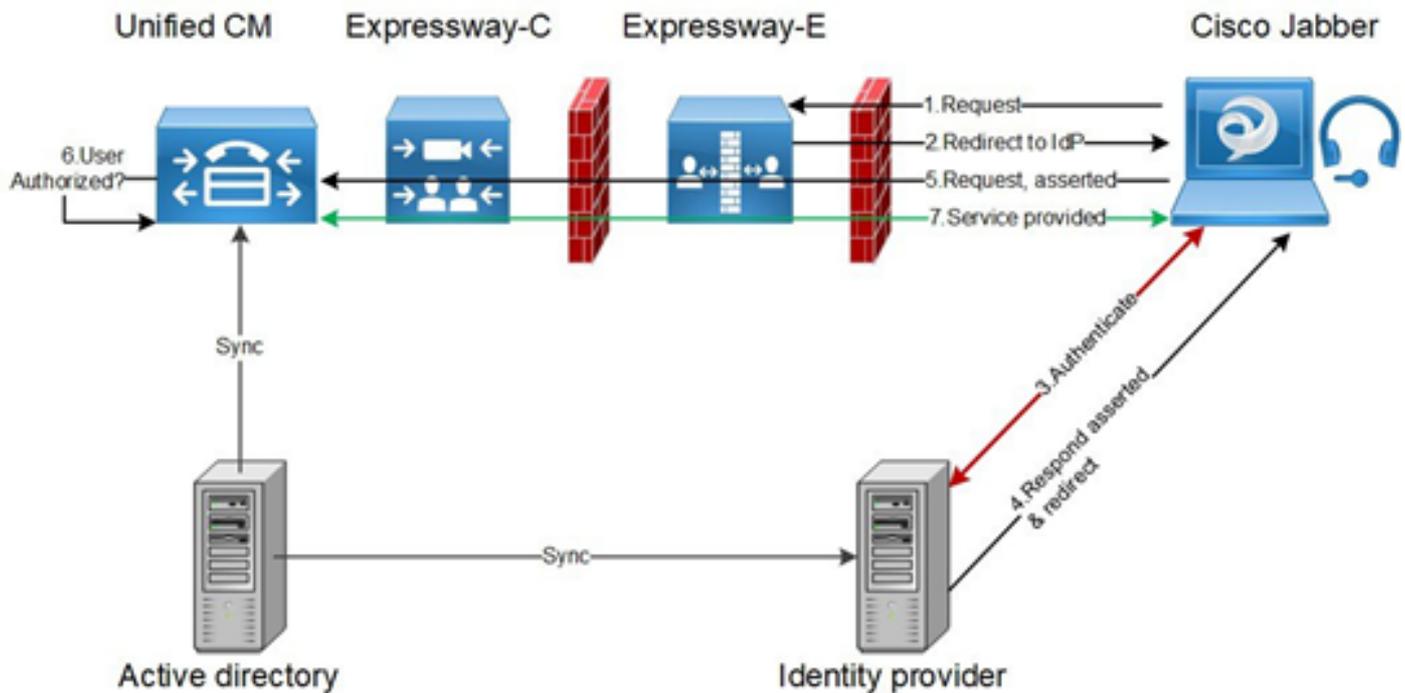


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

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.

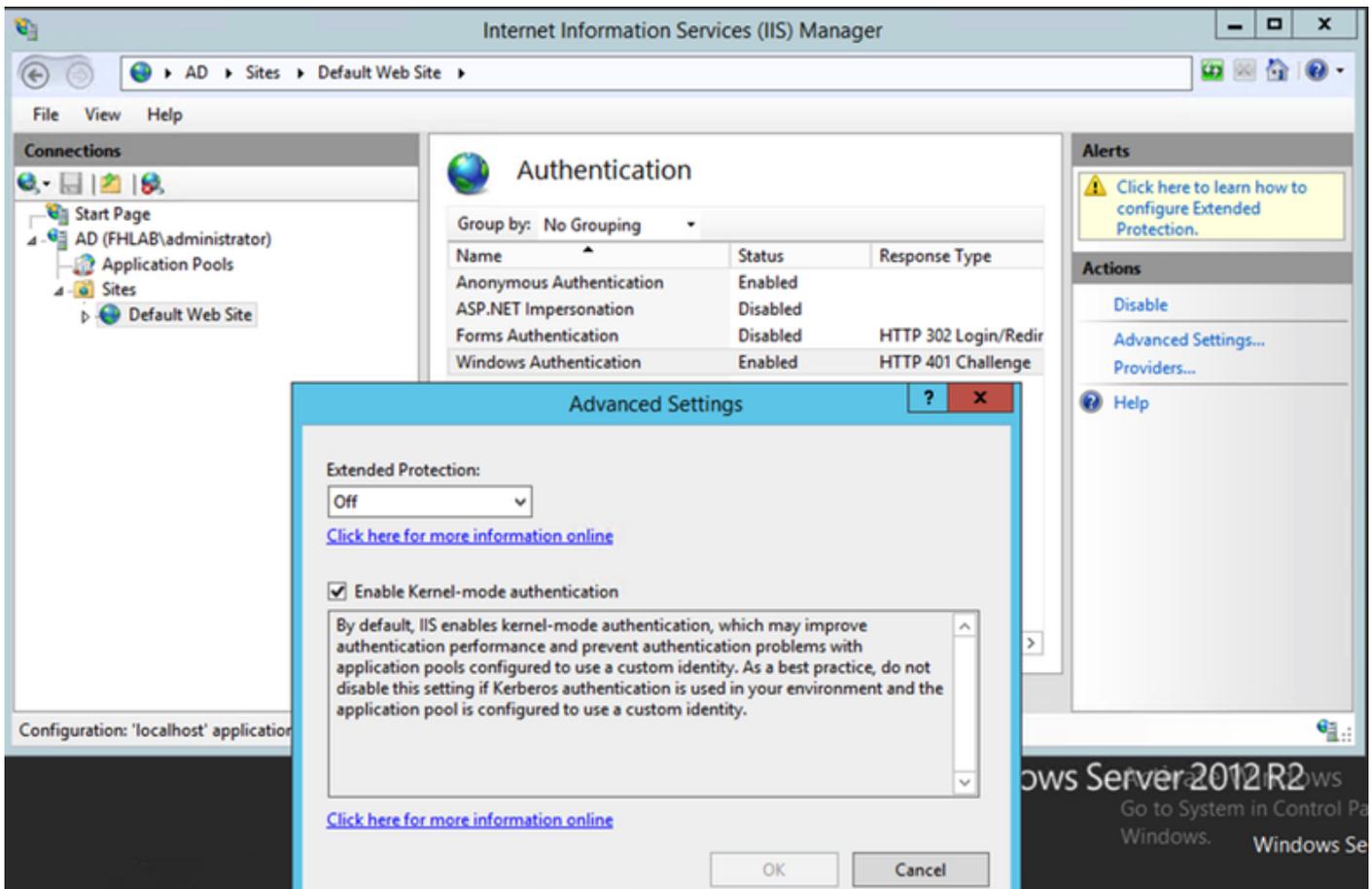
Il flusso di concessione del codice di autorizzazione OAuth supporta l'utilizzo dei token di aggiornamento. In questo modo l'utente finale può beneficiare di un'esperienza migliore, poiché non deve eseguire la nuova autenticazione con la stessa frequenza (per impostazione predefinita 60 giorni)

Configura Kerberos

Seleziona autenticazione di Windows

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

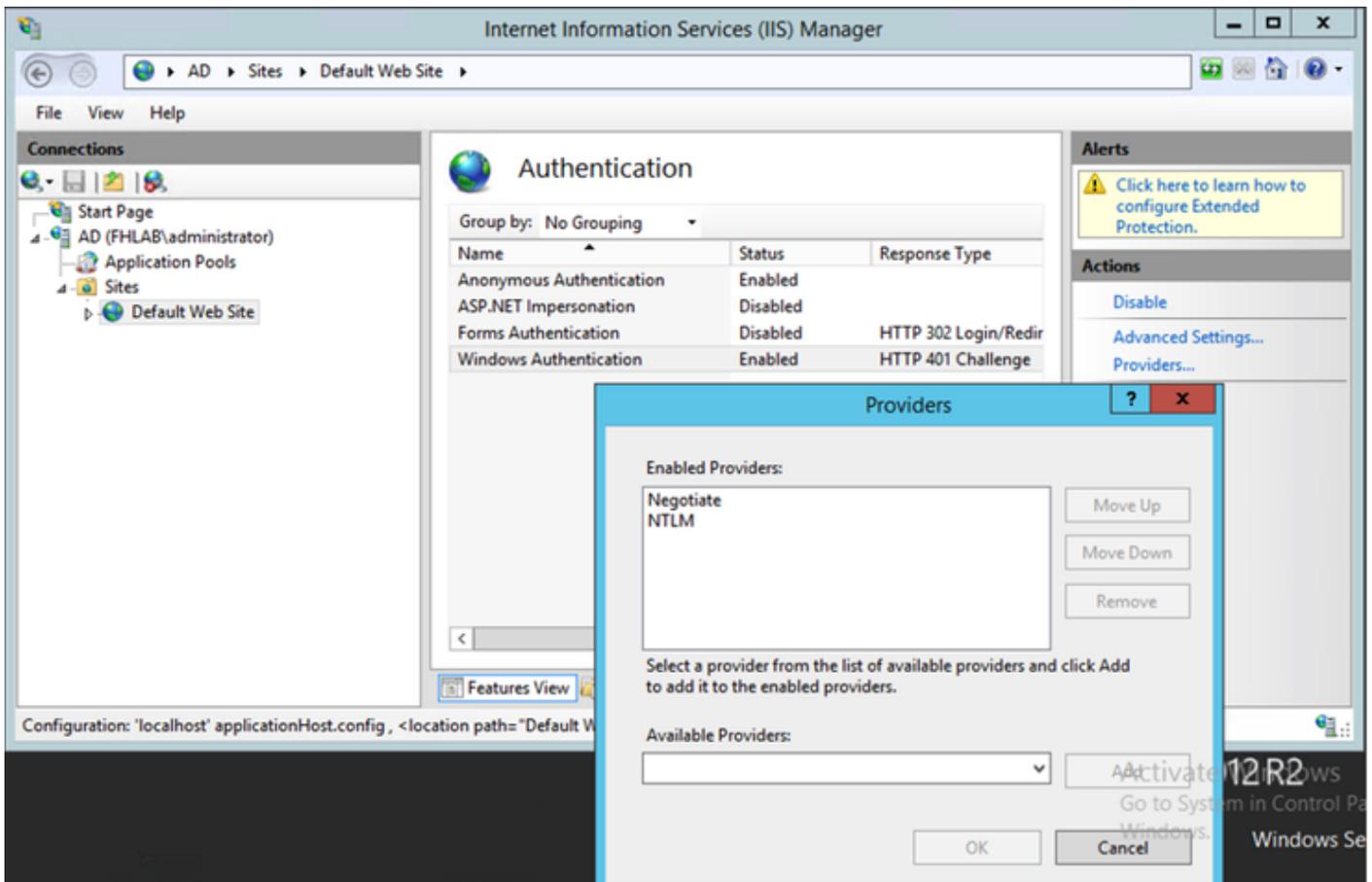
1. Deselezionare Attiva autenticazione in modalità kernel.
2. Assicurarsi che la protezione estesa sia disattivata.



ADFS supporta sia Kerberos che NTLM

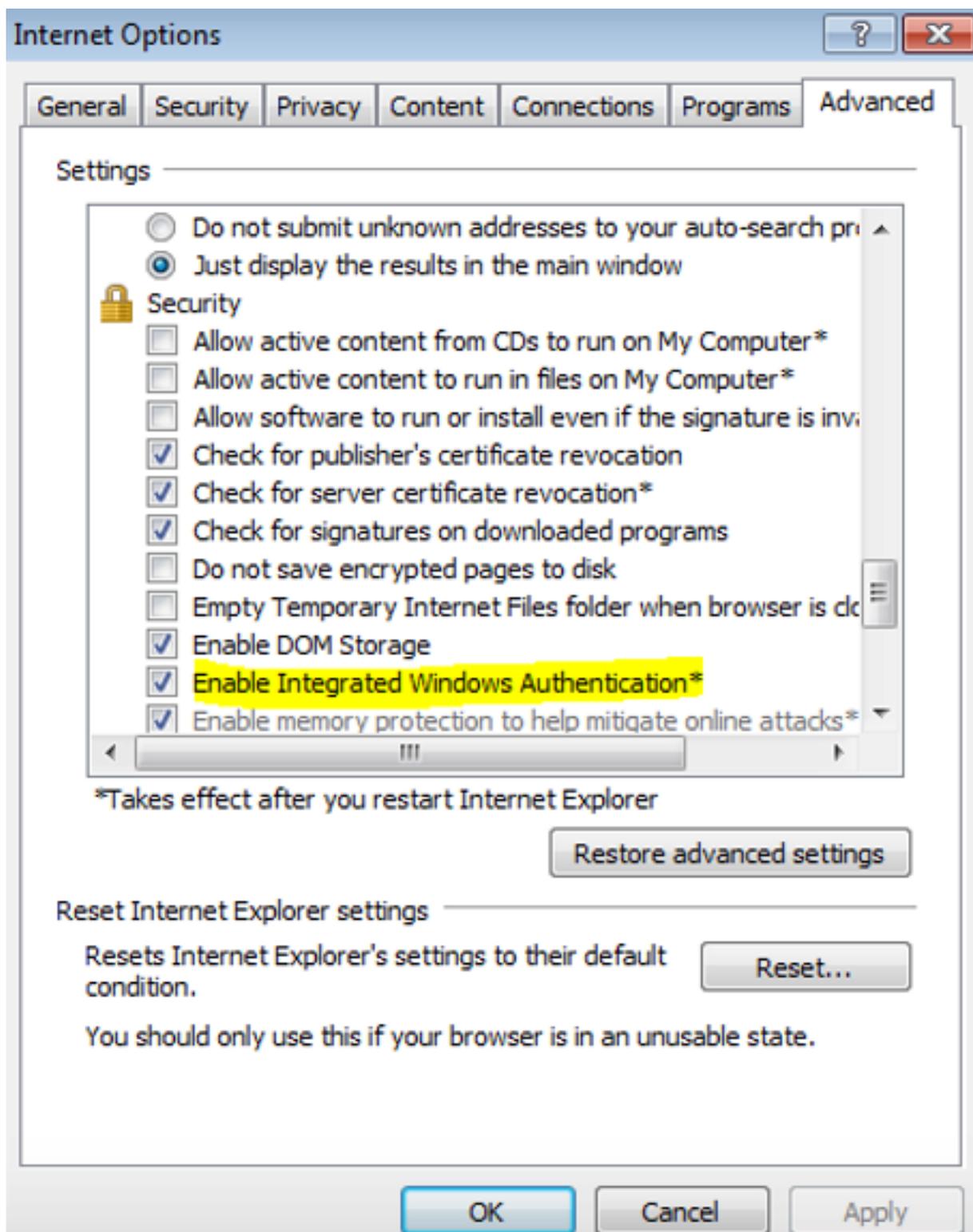
Verificare che AD FS versione 3.0 supporti sia il protocollo Kerberos che il protocollo NTLM (NT LAN Manager), poiché tutti i client non Windows non possono utilizzare Kerberos e si basano su NTLM.

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



Configurare Microsoft Internet Explorer

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



Aggiungi URL ADFS in Protezione > Aree Intranet > Siti

