

Cisco Unified SAML SSO نيوكت ADFS 3.0 مادختساب Communications Manager

تايوتحمل

[عمدقمل](#)

[ةيساسأل تابلطمل](#)

[تابلطمل](#)

[عمدختسمل تانوكمل](#)

[نيوكتل نم قب سمل ققحتل](#)

[A تالجس](#)

[\(PTR\) رشؤمل تالجس](#)

[Jabber فاشتك تامدخ ناكم في SRV تالجس رفوت مزلي](#)

[ADFS3 ل ةيلوال ةئيهتل](#)

[ADFS مادختساب CUCM ل ع SSO نيوكت](#)

[LDAP نيوكت](#)

[ةيلوال CUCM تانايب](#)

[ADFS دامتعا ةهج نيوكت](#)

[ايلخاد ني درشمل فيرعت تانايب](#)

[CUC ل ع SSO نيوكت](#)

[CUC فيرعت تانايب](#)

[Expressway ل ع SSO نيوكت](#)

[Expressway C ل فيرعتل تانايب داريتسا](#)

[Expressway C نم فيرعتل تانايب ريصت](#)

[Cisco Expressway-E ل دامتعالا فرط ةقث ةفاضل](#)

[لوخدلا ليجست شي دحت عم OAuth](#)

[ةقداصلمل راسم](#)

[SSO ةينب](#)

[يلحمل لوخدلا ليجست قفدت](#)

[MRA ل لوخدلا ليجست قفدت](#)

[ثوا](#)

[زيممل شي دحتل/لوصول زمر](#)

[لض فأ OAuth ليوخت دوكنم قفدت](#)

[Kerberos نيوكت](#)

[Windows ةقداصلم دي دحت](#)

[Kerberos NTLM نم الك ADFS معدت](#)

[Microsoft Internet Explorer نيوكت](#)

[عق او مل > ت نارتنا قطانم > ني مائل تحت ADFS URL ناونع ةفاضل](#)

[اب قوئومل عق او مل > نامأل ل Unity و IMP و CUCM تافيضم عامسأ ةفاضل](#)

[مدختسمل ةقداصلم](#)

[SSO في Jabber ل لوخدلا ليجست](#)

[اهجالص او عاخال فاشكتسا](#)

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

[IE إلى أفضال عقاوملا](#)

[قنمازتم ريغ قلكشم](#)

[زيمم زمرا لاطبا](#)

[فلم bootstrap](#)

[بب سب SSO لشف MSIS7066](#)

ةمدقملا

Active Directory داخا ةمدخ مادختساب يداحألا لوخدلا ليجست نيوكا تاوطخ دنن سمل اذه فصوي Windows 2012 R2 مادختساب (ADFS 3.0) Cisco Unified Communications Manager (CUCM)، و Cisco Unity Connection (CUC)، Expressway تاختنم و. دنن سمل اذه في اضيأ Kerberos.

ةيساسألا تابلطتملا

تابلطتملا

Windows تاختنم و (SSO) يداحألا لوخدلا ليجستب ةفرعم كيدل نوكت نأب Cisco في صوت.

ةمدختسمل تانوكملا

ةيلال ةيدامل تانوكملا و اجماربلا تارادصا إلى دنن سمل اذه في ةدراولا تامولعمل دننست:

- CUCM 11.5
- CUC 11,5
- Expressway 12
- Windows 2012 R2 Server ةيلال راودألا عم:
 - Active Directory تاداهش تامدخ
 - Active Directory داخا تامدخ

ةصاخ ةيلمعم ةئييب في ةدوجوملا ةزهجال نم دنن سمل اذه في ةدراولا تامولعمل عاشنإ مت ت ناك اذا. (فيضارتفا) حوسمم نيوكا دنن سمل اذه في ةمدختسمل ةزهجال عيمج تادب رمايال لم تحملا ريثأتلل كمهف نم دكأتف، ليغشتلا دي قكتكبش.

نيوكتلا نم قبسمل ققحتلا

ةئييبلا في لعفلاب ةدوجوم نوكت نأ إلى هذه مداخالا راودأ جاتحت، ADFS3 تيبتت لب ق.

DNS و لاجملاب مكحتلا ةدحو:

موقوي يذلا DNS لفس عون) اهب صاخالا رشؤملا لفس عم تالفسك مداوخال عيمج ةفاضل بجي (فيضملا مسا و لاجم إلى IP ناوئع لخب

A تالفس

و cucpubhcsc و cmsubhcsc و cmpubhcsc ةفيضملا ةزهجال ةفاضل تمت. fhlab.com في و cucsubhcsc و expwyc و expwye و impubhcsc و imsubhcsc.

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

رشفؤملا تالچس (PTR)

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

Jabber فاشتك تالچس رشفؤملا تالچس (SRV)

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

• (سؤم لل CA نم ةقوم تاداهش لل نوكت نأ ضارت فاب) رذجل ال CA
 مداخ ةداهش بلق " راركت متي و ،" بي و مداخ ةداهش بلق " ل اذانت سا " ةداهش بلق " عاشن ا مزلي
 ةفاضاب " قي بطلل جهن " ل يدعت متي ، " تاقحلم " بي و بطلل ةمالع يفو ، هتي مست ةداعاو ، " بي و
 (CUCM و ةي ل ادل تاداهش لل ةي قوتل بلق لل اذه مزلي . " لي م عل ةقداصم قي بطلل جهن " و
 تابلط ةي قوت اضيأ ي ل ادل ال CA ل نكمي ةي لمعم ةئي بي يف (Expressway Core و IMP و CUC و
 Expressway E (CSR) تاداهش ةي قوت

CSR. ةي قوت لعل ارداق نوكل هؤاشن ا مت يذلا بلق لل رادصا بجي

اقبس م هؤاشن إ مت يذلا بلال قلدح ،قدصملا عجرملا ةداهش بيوي ع

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 (Web server) in the Saved Request box.

Saved Request:

```
8V8mWY/9kjhgfnpeBzAAW++to1GzBjnvqaT8StWM
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
LA0dphF6LrurUeY2KLvMLmK1ft7aSy483yCsm0v1
OWQFz0Lb3bS80ziW7fQEFWSaCg567DMQ8FkZt5N
10y/1p60dzTdZE9w2p8rK3YxcbygovSt0iJiirh
AM/GjnzQ
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Additional Attributes:

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

نوئي نأ بجي .CA ةطساوب اهعيقوتو CUC Multi-Server CSR و IMP و CUCM ءاشن إ بجي TOMCAT. وه ةداهشلا نم ضرغل

Generate Certificate Signing Request

Generate Close

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing 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

+ Add

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

Generate Close

Tomcat. إ قءوملا ةداهشلاو Tomcat Trust إ قءوملا ةداهش ليحت بجي

Cisco Unified Operating System Administration

Navigation Cisco Unified OS Administration osadmin Search Documentation About Logout

Show Settings Security Software Upgrades Services Help

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

7 records found

Certificate List (1 - 7 of 7) Rows per Page 50

Find Certificate List where Certificate begins with tomcat Find Clear Filter

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat	cmouubhsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/18/2022	Certificate Signed by fhlab-AD-CA
tomcat-ECDSA	cmouubhsc-EC.fhlab.com	Self-signed	EC	cmouubhsc.fhlab.com	cmouubhsc-EC.fhlab.com	04/02/2025	Self-signed certificate generated by system
tomcat-trust	cmouubhsc-EC.fhlab.com	Self-signed	EC	cmouubhsc.fhlab.com	cmouubhsc-EC.fhlab.com	04/02/2025	Trust Certificate
tomcat-trust	cmouubhsc-EC.fhlab.com	Self-signed	EC	cmouubhsc.fhlab.com	cmouubhsc-EC.fhlab.com	04/02/2025	Trust Certificate
tomcat-trust	cmouubhsc-EC.fhlab.com	Self-signed	EC	cmouubhsc.fhlab.com	cmouubhsc-EC.fhlab.com	04/02/2025	Trust Certificate
tomcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

Certificate List (1 - 6 of 6) Rows per Page 50

Find Certificate List where Certificate begins with tomcat Find Clear Filter

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat	cucubhsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/28/2022	Certificate Signed by fhlab-AD-CA
tomcat-ECDSA	cucubhsc-EC.fhlab.com	Self-signed	EC	cucubhsc.fhlab.com	cucubhsc-EC.fhlab.com	04/02/2025	Self-signed certificate generated by system
tomcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate
tomcat-trust	cmouubhsc-EC.fhlab.com	Self-signed	EC	cmouubhsc.fhlab.com	cmouubhsc-EC.fhlab.com	04/02/2025	Trust Certificate
tomcat-trust	cucubhsc-EC.fhlab.com	Self-signed	EC	cucubhsc.fhlab.com	cucubhsc-EC.fhlab.com	04/02/2025	Trust Certificate

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

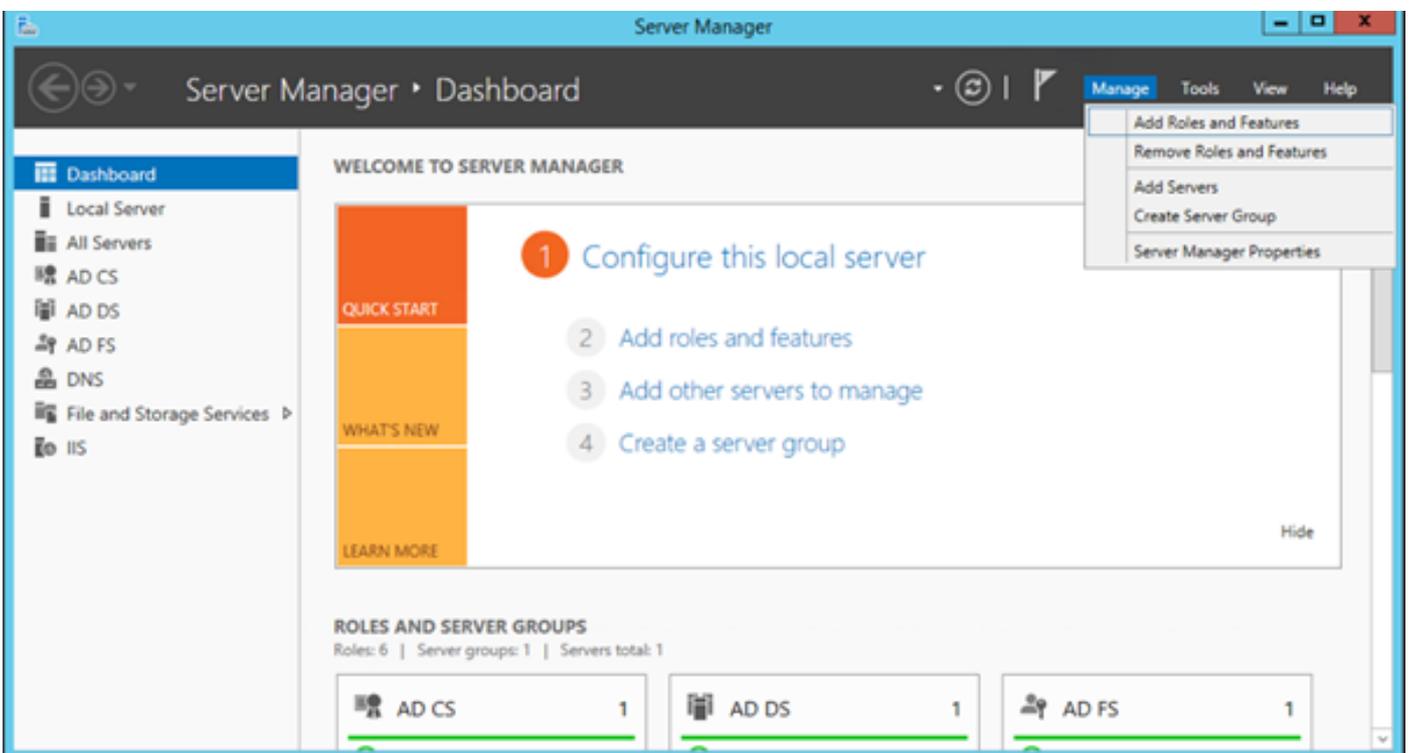
- IIS

موقف، الإو. راودال هذه تيبثت لال خ نم مسقلا اذ ذيفنت متيس، حاسم كانه نكت مل اذاو Microsoft نم ADFS3 ليزنت إلى إرشابم لقتنا م مسقلا اذ يطختب

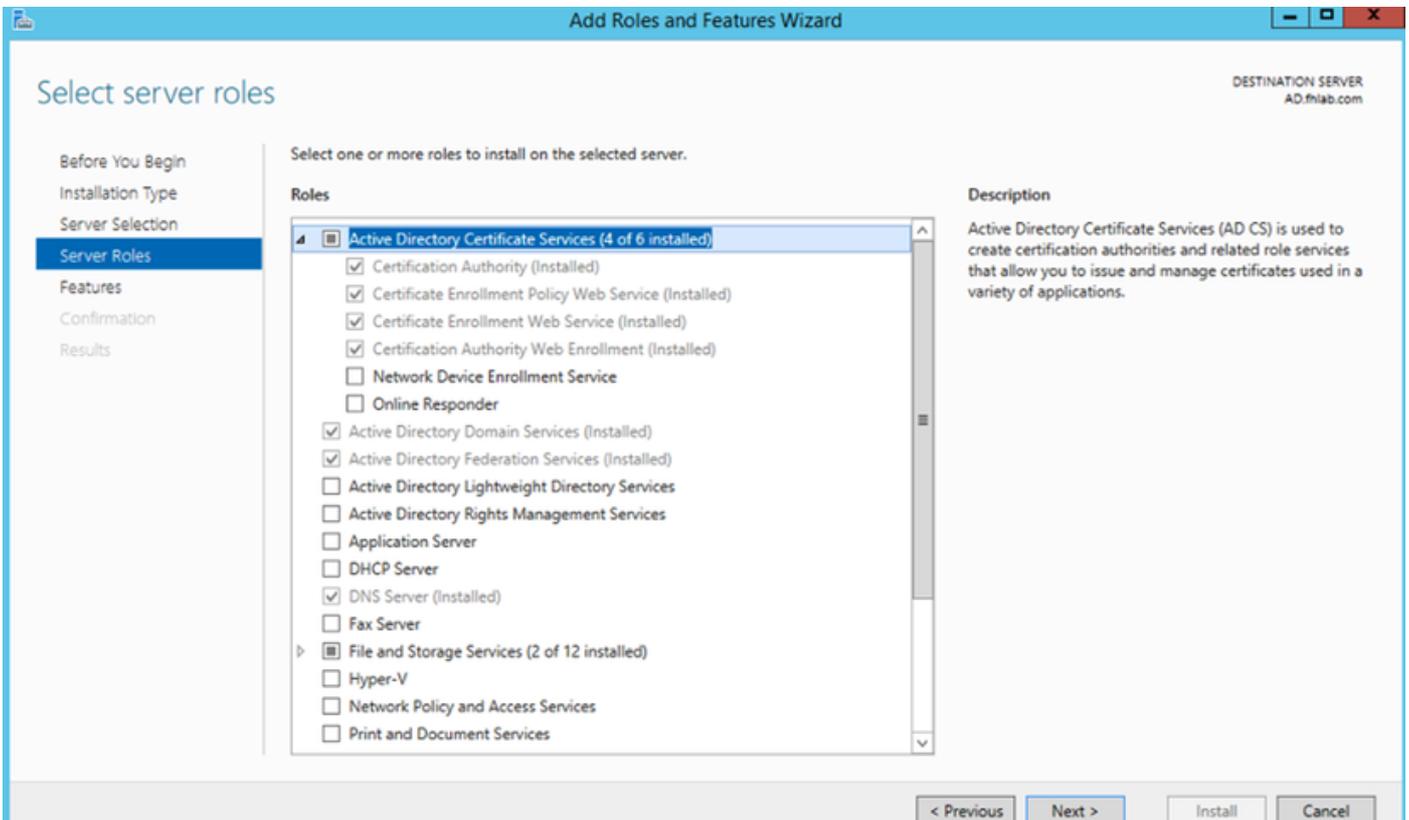
لاجل م كحت ةدحو إلى مداخل ةيقرتب مق، DNS مادختساب Windows 2012 R2 تيبثت دعب

Microsoft Certificate Services تيبثت يه ةيلاتل ةمهمل نوكتس

اديح ارود فضاو مداوخلل ةرادا إلى لقتنا:



Active Directory. تاداهش تامدخ رود ددح



تثبيت دعب. الؤا قءصم ال عجرم ال اءاءش لئجسء ءه نل بؤ و ءمءء - ءامءء ال هءه رشن ب مق بؤ و لئجسء و ءءاءش ال لئجسء بؤ و ءمءء ءبءء ب مق مء امه نؤكء ب مق، نؤرءء ال نؤءه مهنؤكء ب مق. قءصم ال عجرم ال

"قءصم ال عجرم ال" ءبءء ءن ع، IIS لءم، روءل ءؤفءاء ءازؤم و ءامءء ءفءاء مءؤس امك

اهءءب ءمءءق وؤ ءسؤم ءؤءء كنكمؤ، كب ءصءء ال رشن ال ءؤلم ع ءل اءانءس



Specify Setup 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

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.

- Enterprise
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.
- Standalone
Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.

[More about the differences between enterprise and standalone setup](#)

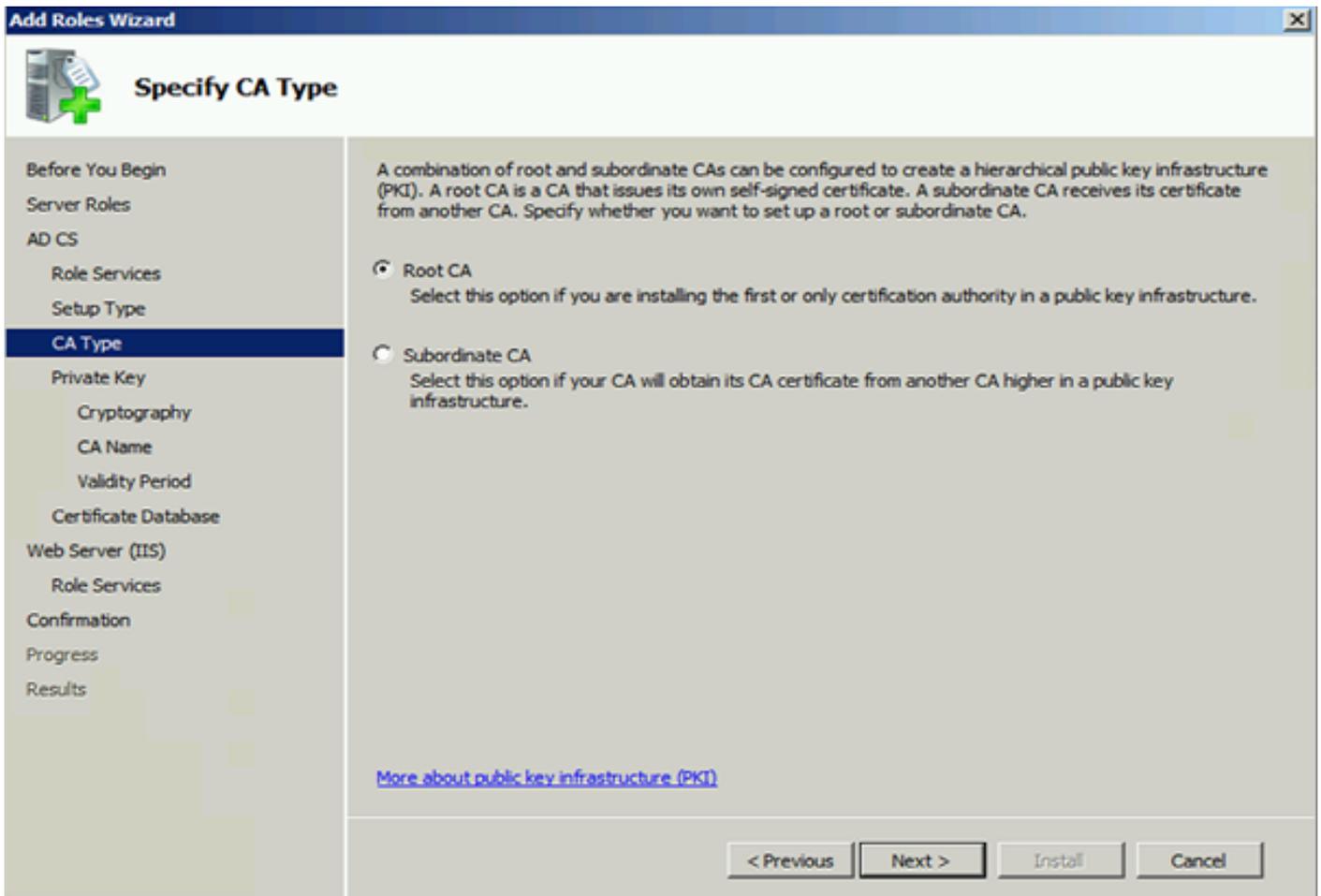
< Previous

Next >

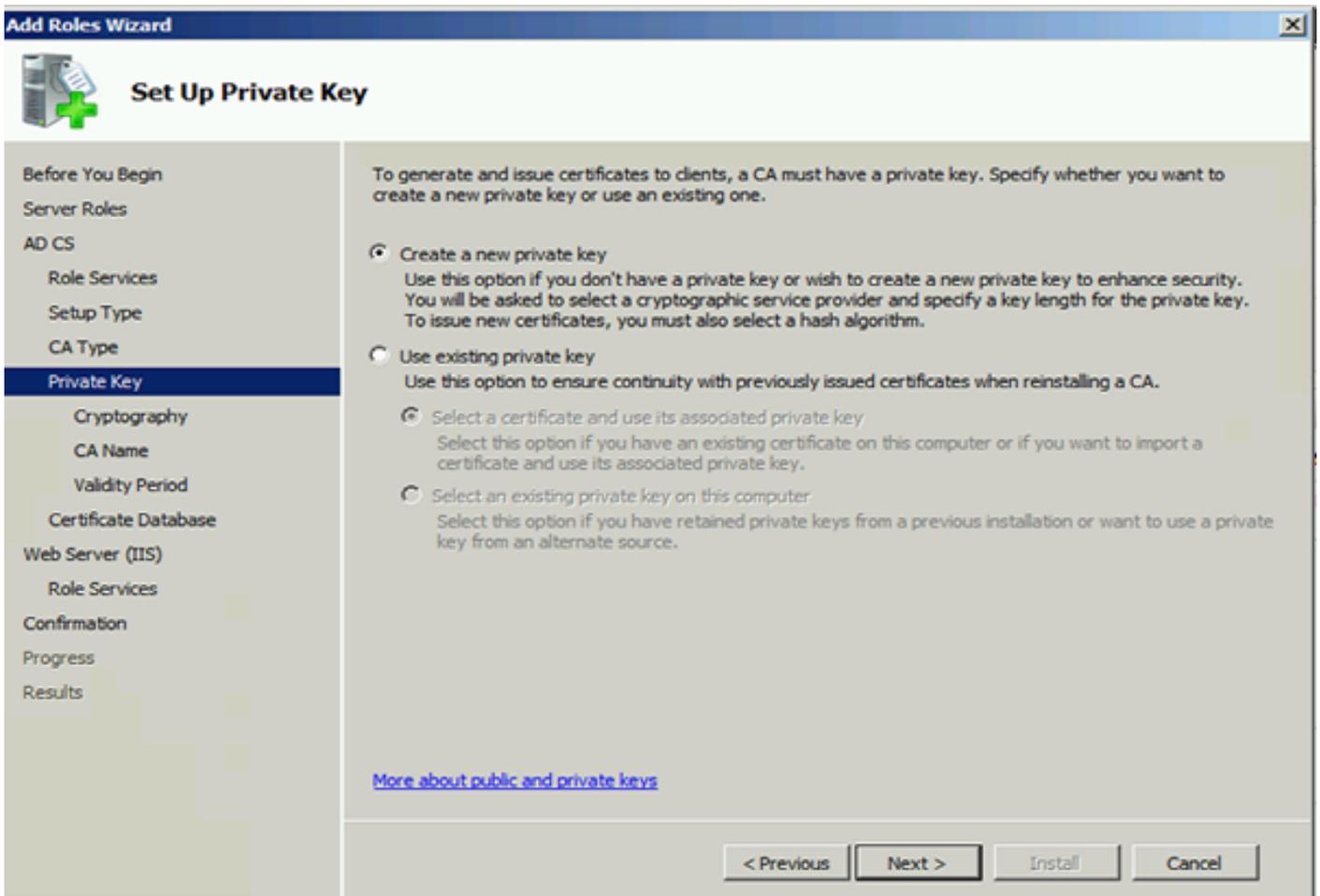
Install

Cancel

قدصملا عجرملا وأ رذجال قدصملا عجرملا ديدحت كنكمي، قدصملا عجرملا عونل ةبسنلاب عجرملا ددحف، ةسسؤملا يف لعفلاب ليغشتلا ديق رخأ قدصم عجرم كانه نكي مل اذا. عباتلا رذجال قدصملا.

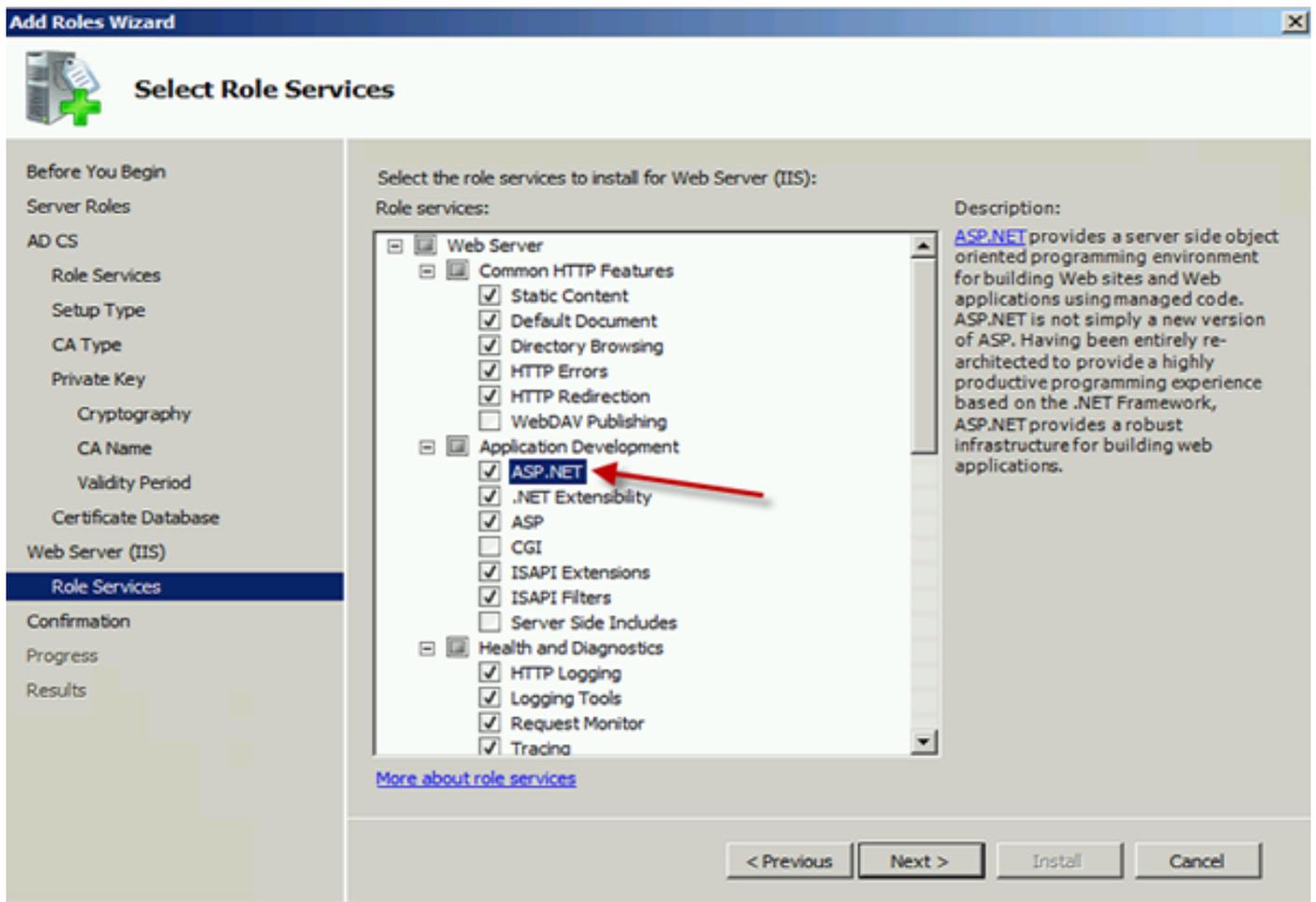


ك. صاخال CA ل صاخال حاتفم ءاشن إ يف ةلالال ةوطخال ل ثمتت

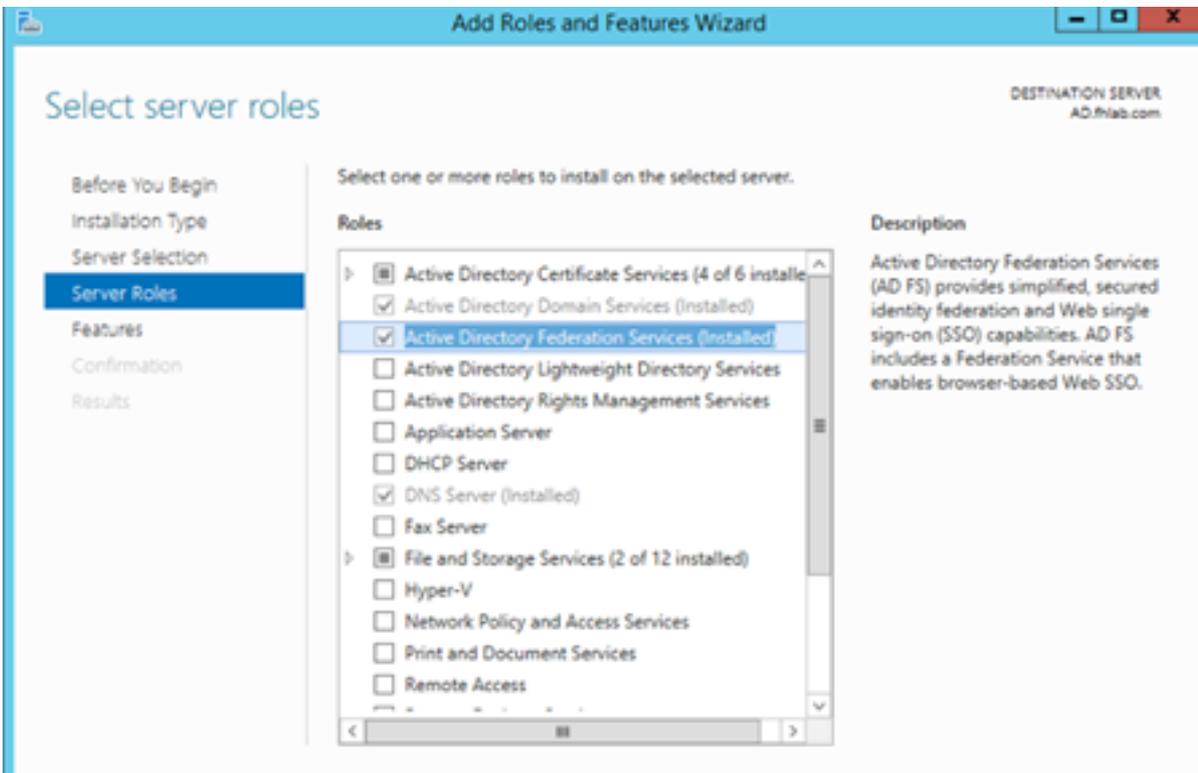


Windows Server 2012 لى ADFS3 تىبثت ب تمق اذا ال ةبولطم ةوطخال هذه نوكت ال

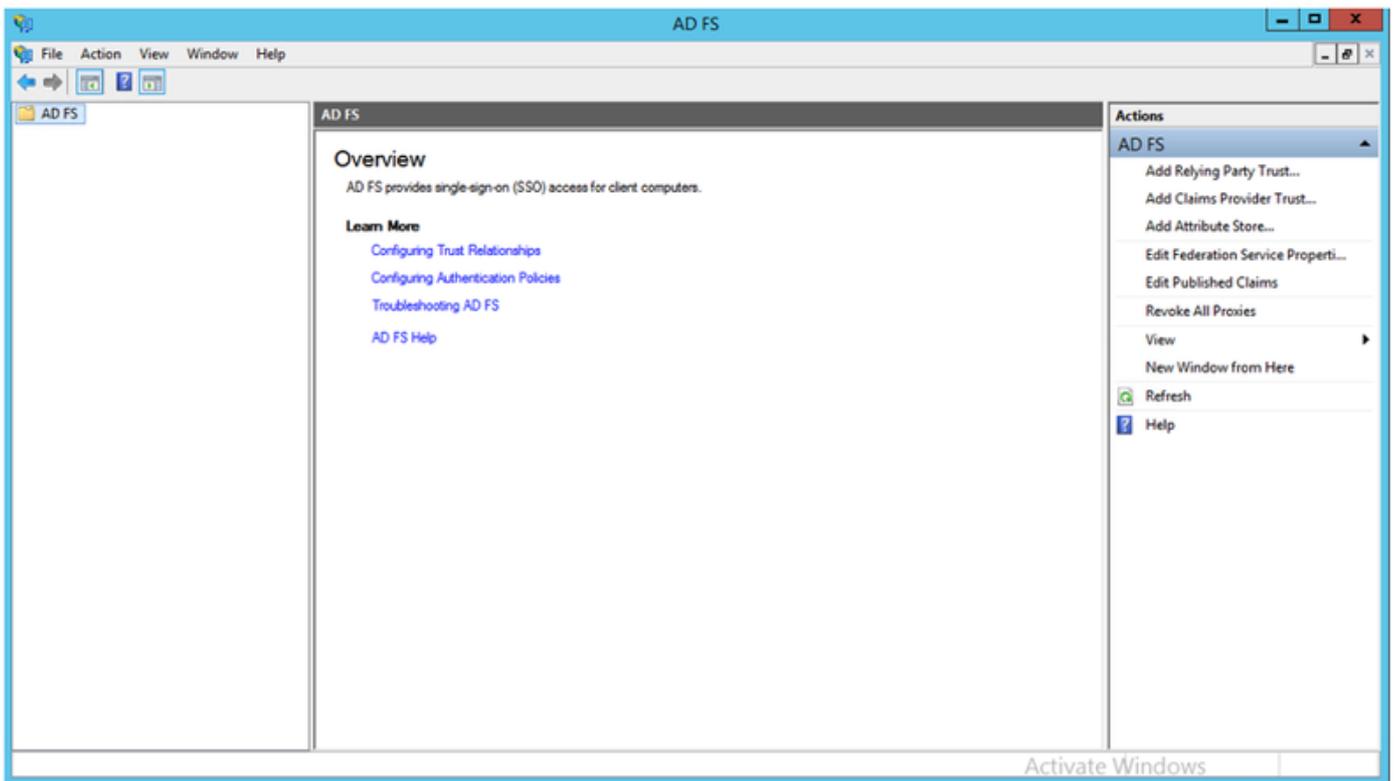
بېوولای لېجسټل ږوررض اذه. IIS ل Role Services نېوکت مزلي، CA نېوکت دعب. لصفنم رقنا، IIS ږي فاضا رود کانه، ADFS رشن تاي لعم مظعمل ةبس نلاب. قدصم لاجرم لاي ږي بولطم لاي قيبطت لاي ريوطت نمض ASP.NET قوف.



بېولای عقوم قوف نمي الای سوام لای رزب رقنا م، IIS > بېولا مداخ قوف رقنا، "مداوخل ةرادا" ږي متي و. HTTP لای ةفاض لای اب HTTPS ب اضي احم س لای قيبطت لاي ربيغت بجي. ږي ضار ت فالای HTTPS م عدل ک لذب ماي ق لای.



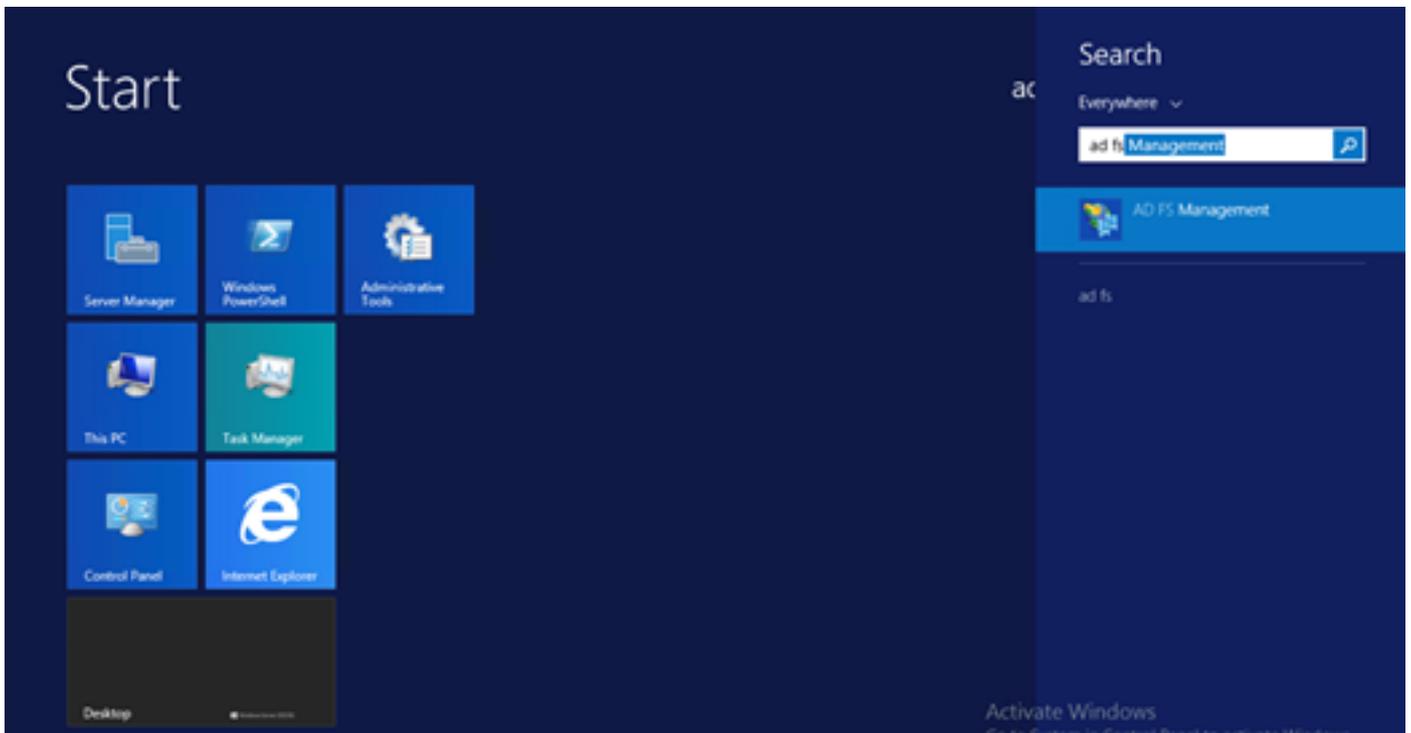
"أدب" عمئاق ل ن م وأ ماهم ل طيرش ن م هحتف كنكمي ، تيبتت ل لامتكا ل درجمب



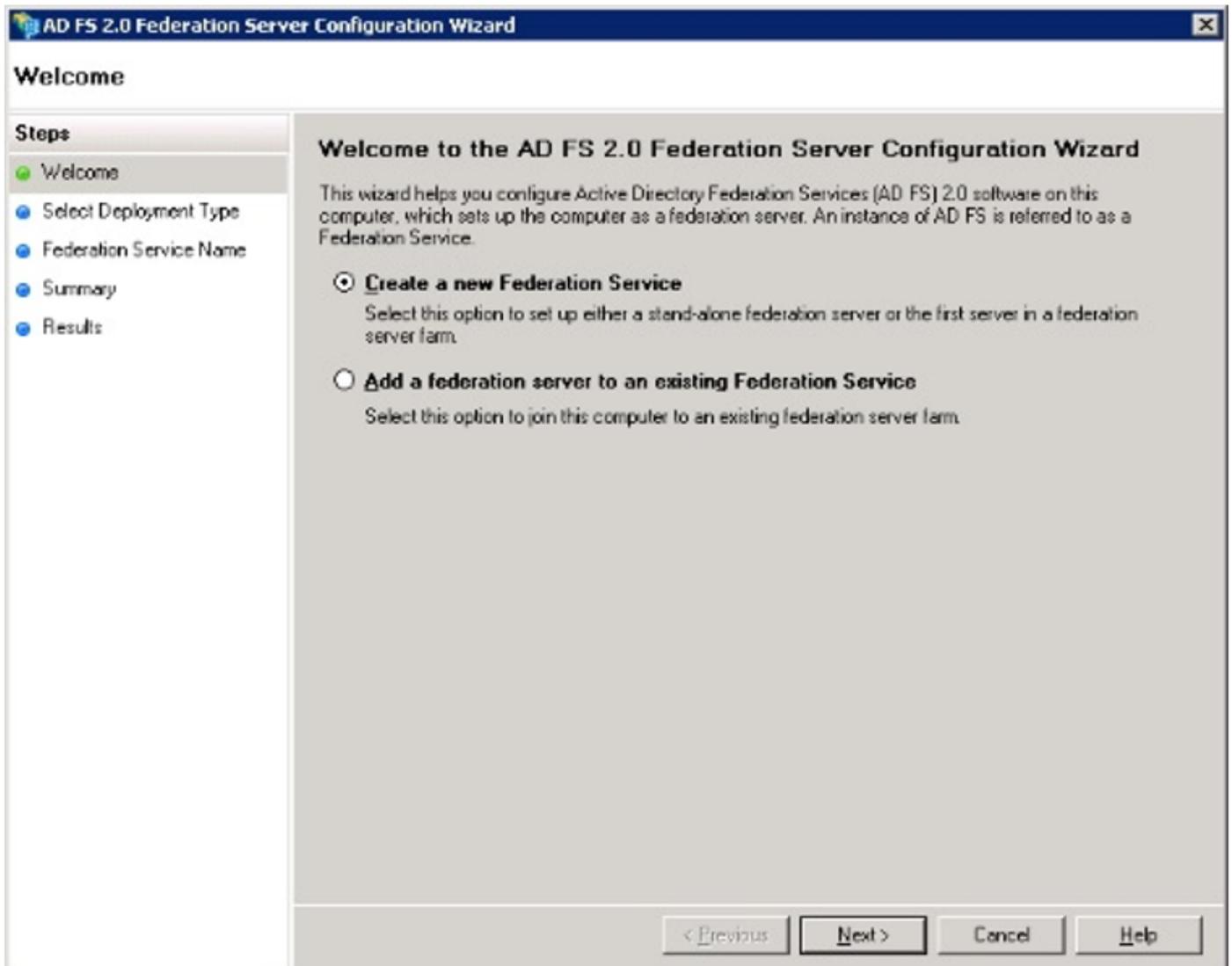
ADFS3 ل ةي ل و أ ل ةئي هت ل ل

هم ادختسا نكمي نكلو ، ديدج لقتسم داحتا م داخ تيبتت ل ل الخ ن م مسقلا اذ ذيفنت متيس ل
 لاجم ل اب مكحت ةدحو ل ع هت تيبتت ل اضيأ

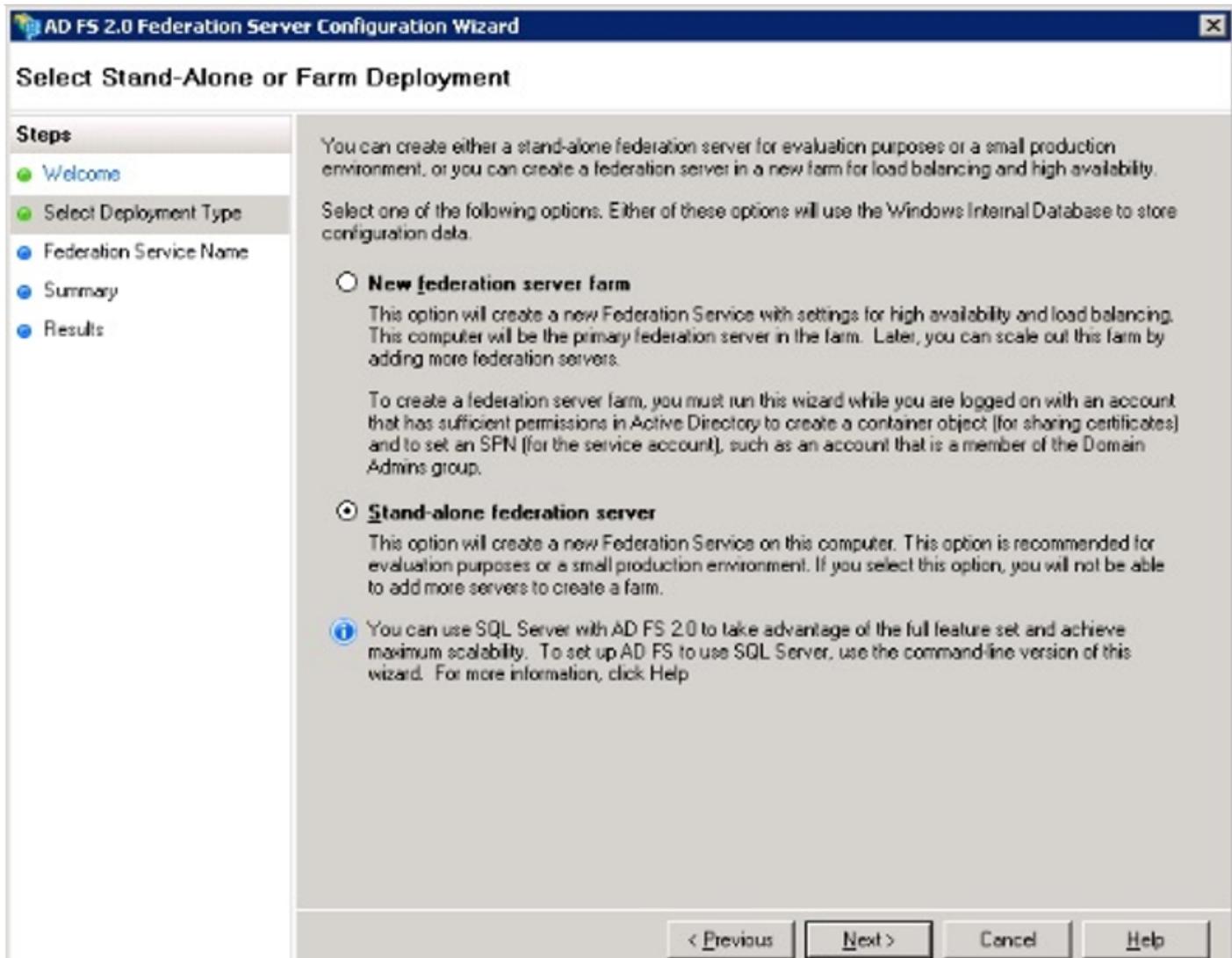
يف حضورم وه امك ADFS ةرادا مكحت ةدحو ل ل يغشت ل AD FS Management بتكا و Windows ددح
 ةروصل ل ل.



لثمت .كب صاخلل ADFS م داخ نيوكت ءدبل AD FS 3.0 داخ تالال م داخ نيوكت جلا عم را يخ ددح AD FS 3. ف تاوطخال لس فن هذ ة شاشللا تا طؤل



يللال قوف رقناو ءديج داخ تالال م داخ نيوكت جلا عم را يخ ددح



ةروصلال يف حضوم وه امك يلاتال قوف رقناو لقتسملا داحتالا مداخ ددح

AD FS 2.0 Federation Server Configuration Wizard

Specify the Federation Service Name

Steps

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

This wizard determines the Federation Service name from the Subject field of the SSL certificate for the Default Web Site. If the wizard cannot determine the Federation Service name from the SSL settings, you must select a certificate.

Select the certificate and/or port, and then click Next.

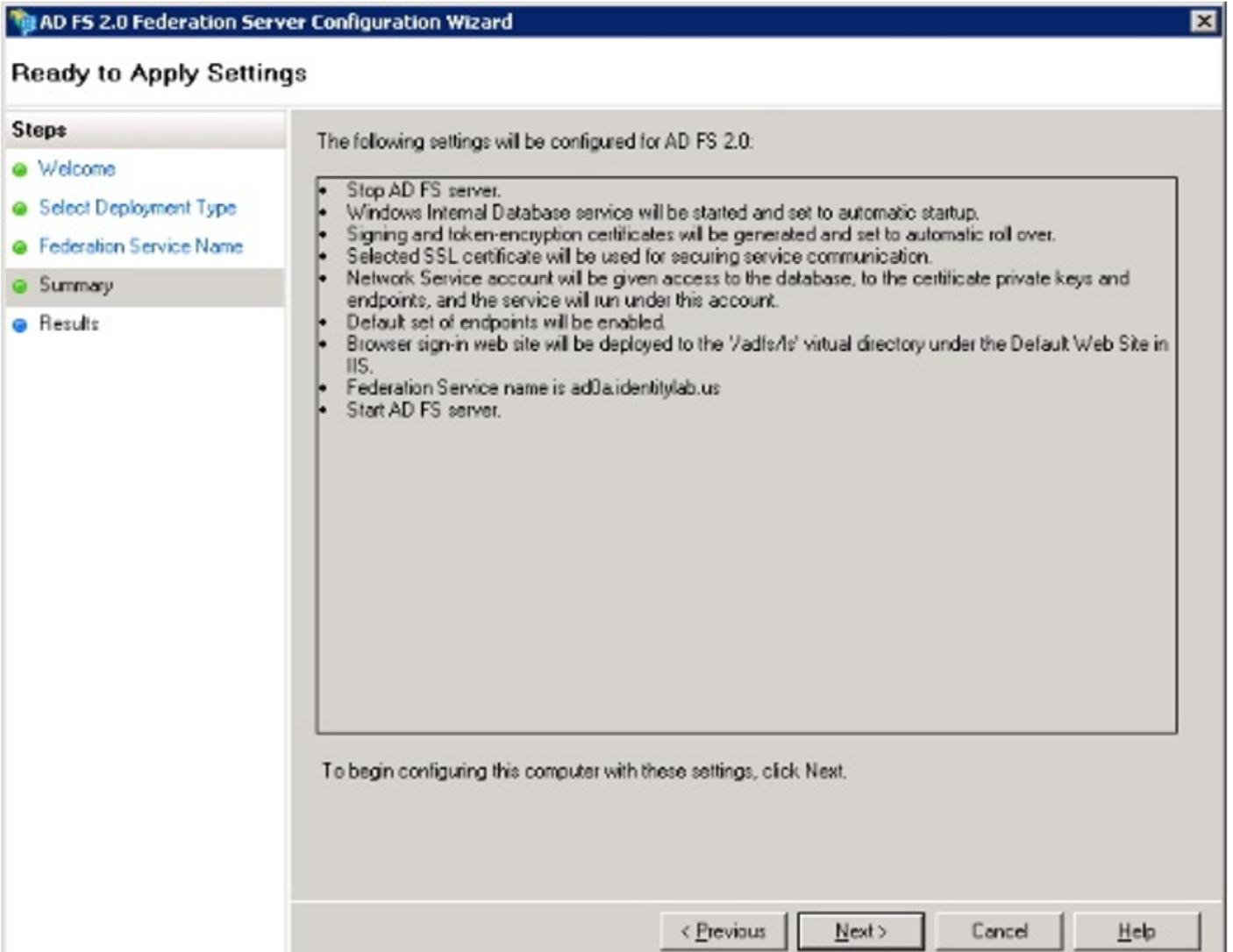
SSL certificate: ad0a.identitylab.us Port: 443

Federation Service name: ad0a.identitylab.us

[What kind of certificate do I need?](#)

< Previous **Next >** Cancel Help

داحاتالال ةمدخ مسا علم متيس . ةمئاقلا نم ايتاذ ةعقووملا ةداهشلا ددح ، SSL ةداهش تحت
داحاتالال (يلااتلا) Next قوف رونا . ايئاقلا



دادع | ةيلمعلا تقبط in order to كذ دعب ةقطقو دادع | ةيلمعلا تعجار

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

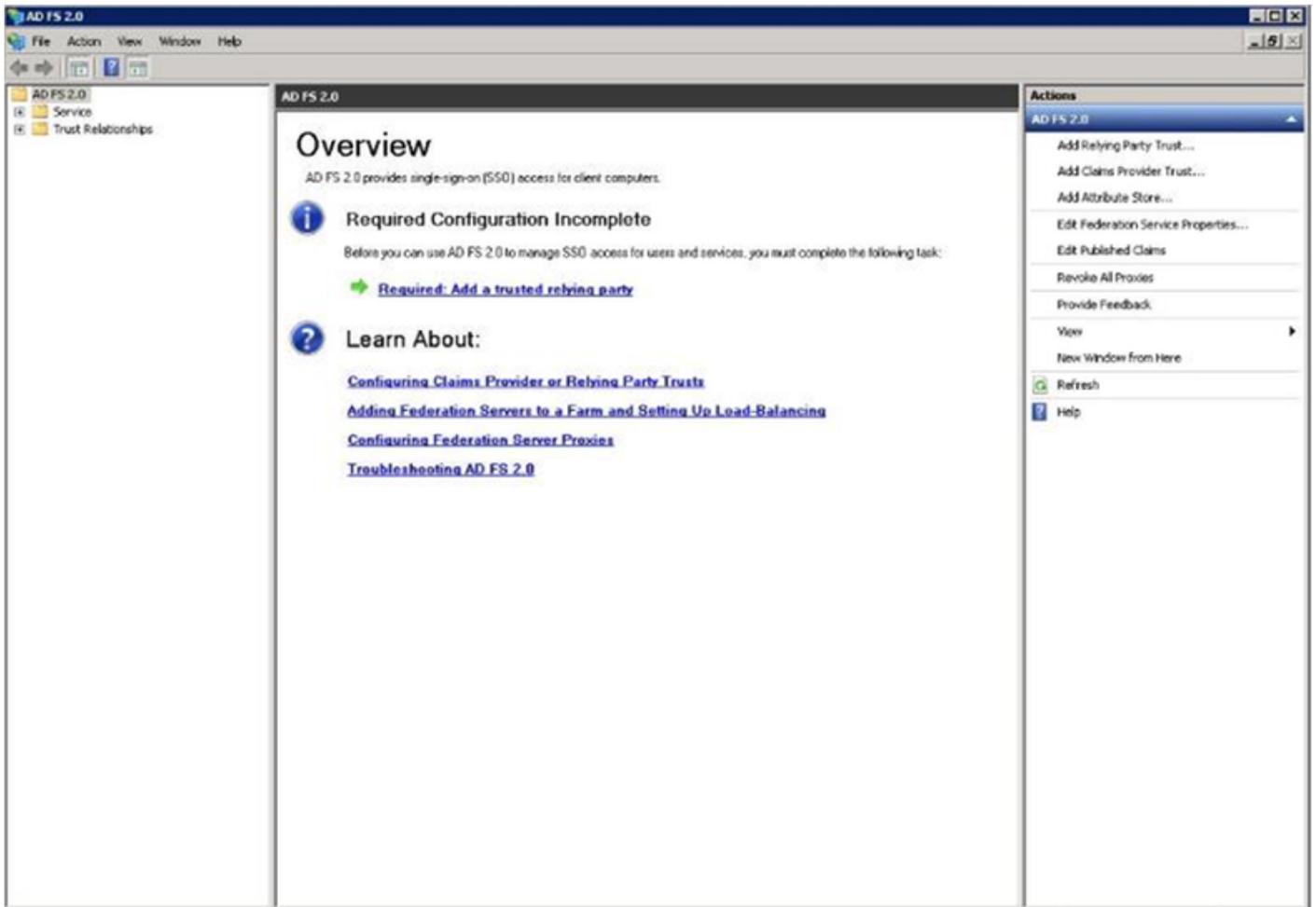
Component	Status
Stop the AD FS 2.0 Windows Service	Configuration finished
Install Windows Internal Database	Configuration finished
Start the Windows Internal Database service	Configuration finished
Create AD FS configuration database	Configuration finished
Configure service settings	Configuration finished
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

ة دحو ىل ءو ج رل او ج ل ا ع م ل ا ء ا ه ن ا ل ق ا ل غ ء ق و ف ر ق ن ا و ح ا ج ن ب ت ا ن و ك م ل ا ء ف ا ك ل ا م ت ك ا ن م د ك ا ت ق ئ ا ق د ع ض ب ك ل ل ذ ق ر غ ت س ي د ق . ء ي س ي ر ل ل ا ء ر ا د ا ل ا م ك ح ت ل ل



ىل اچاتحت ،كلذ دع ب (IdP) ةي وه رفومك لاعف لكش ب هنيوكتو ADFS نيكمت نأل امتي
ىل الواچاتحت ،كلذب مايقلا نم نكمتت نأل بق . هب قوٹوم دامتعا كيرشك CUCM ةفاضل
CUCM ةرادا ي ف نيوكتال ضعب

ADFS مادختساب CUCM ىلع SSO نيوكت

LDAP نيوكت

لبق LDAP ةقداصم نيوكت مزليو Active Directory ةمدخ عم LDAP عم ةومجملا ماظن جم دبجي
حضورم وه امك LDAP System > "ماظنلا" بيوبتلا ةمالع ىل لقتنا . رخأ ناكم يا ىل لاقتنال
ةروصلال ف

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

Microsoft Active Directory



LDAP Attribute for User ID

sAMAccountName



LDAP لي دد > "ماظنللا" بي وبتللا ةمالة لى لى لقتنا ،مث

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*

Users Only Users and Groups

LDAP Custom Filter for Groups

< None >

LDAP Directory Synchronization 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 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](#)

LDAP قوڊداصم نى وكت مزلي، CUCM عم Active Directory مې دختسم ەنمازم دعب

The screenshot shows the Cisco Unified CM Administration web interface. The main heading is "LDAP Authentication". Below it, there is a "Status" section showing "Status: Ready". The "LDAP Authentication for End Users" section is expanded, showing the following configuration:

- Use LDAP Authentication for End Users
- LDAP Manager Distinguished Name*: rhlab/Administrator
- LDAP Password*: [Redacted]
- Confirm Password*: [Redacted]
- LDAP User Search Base*: cn=users,dc=rhlab,dc=com

Below this, the "LDAP Server Information" section is also visible, showing the same configuration as the first screenshot: Host Name or IP Address for Server* (10.89.228.226), LDAP Port* (389), and Use TLS (unchecked).

فللم لوصولا في مكحتال تاعومجم ضعب نبيعت الى CUCM في فئاهنلا مدختسملا جاتحي متيس. لمعتسم ربوس CCM ةيسايق يه ACG. هب صاخلا فئاهنلا مدختسملا فيرعت ةزهاج ةئيبلا نوكت امدنع SSO رابتخال مدختسملا مادختسا.

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

ةيلوأل CUCM تانايب

CUCM. رشانل ةيللمعال مسقلا اذه رهظيس

لىل ضارعتسالا لىل جاتحت كلذل، CUCM فيرعت تانايب لىل لوصحلل يه لىل وأل ةمهمل اهلپزنت نكمي وأ <https://<CUCM Pub FQDN>:8443/SSOSP/ws/config/metadata/sp> ناونع لىل وأ ةدقع لكل كلذب مايقلا نكمي. يداحأ SAML لوخذ لىلجست > ماظنلل بىوبت ةمالع نم اذه ةومجمل ماظن ضرع ءارچا لصفى. ةومجمل ماظن لىوتسم

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

SAML Single Sign-On

SSO Mode

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

Status

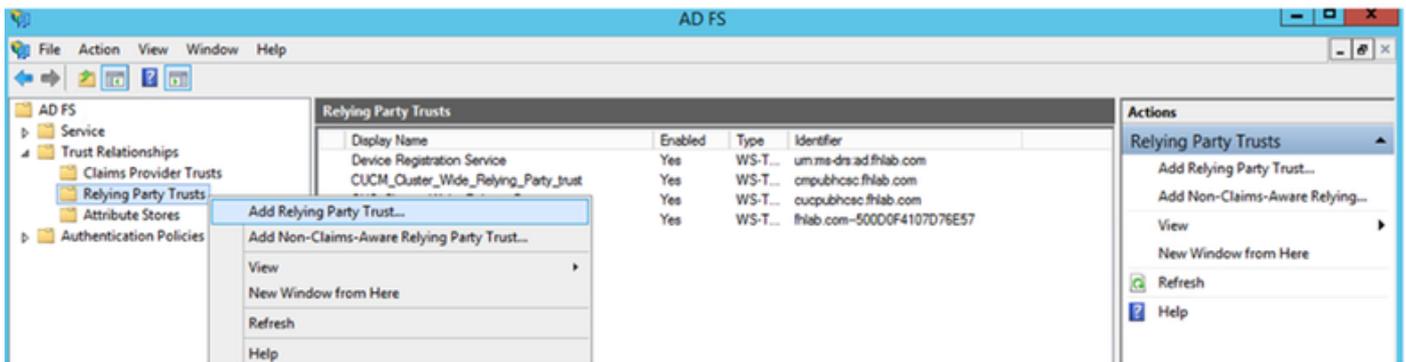
RTMT is enabled for SSO. You can change SSO for RTMT [here](#).
 SAML SSO enabled

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cmpubhcsc.fhlab.com	SAML	N/A	April 20, 2020 2:00:57 PM PDT	<input type="button" value="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	<input type="button" value="IDP"/>	April 20, 2020 2:00:57 PM PDT	<input type="button" value="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	<input type="button" value="IDP"/>	April 20, 2020 2:00:57 PM PDT	<input type="button" value="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	<input type="button" value="IDP"/>	April 20, 2020 2:00:57 PM PDT	<input type="button" value="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..."/>

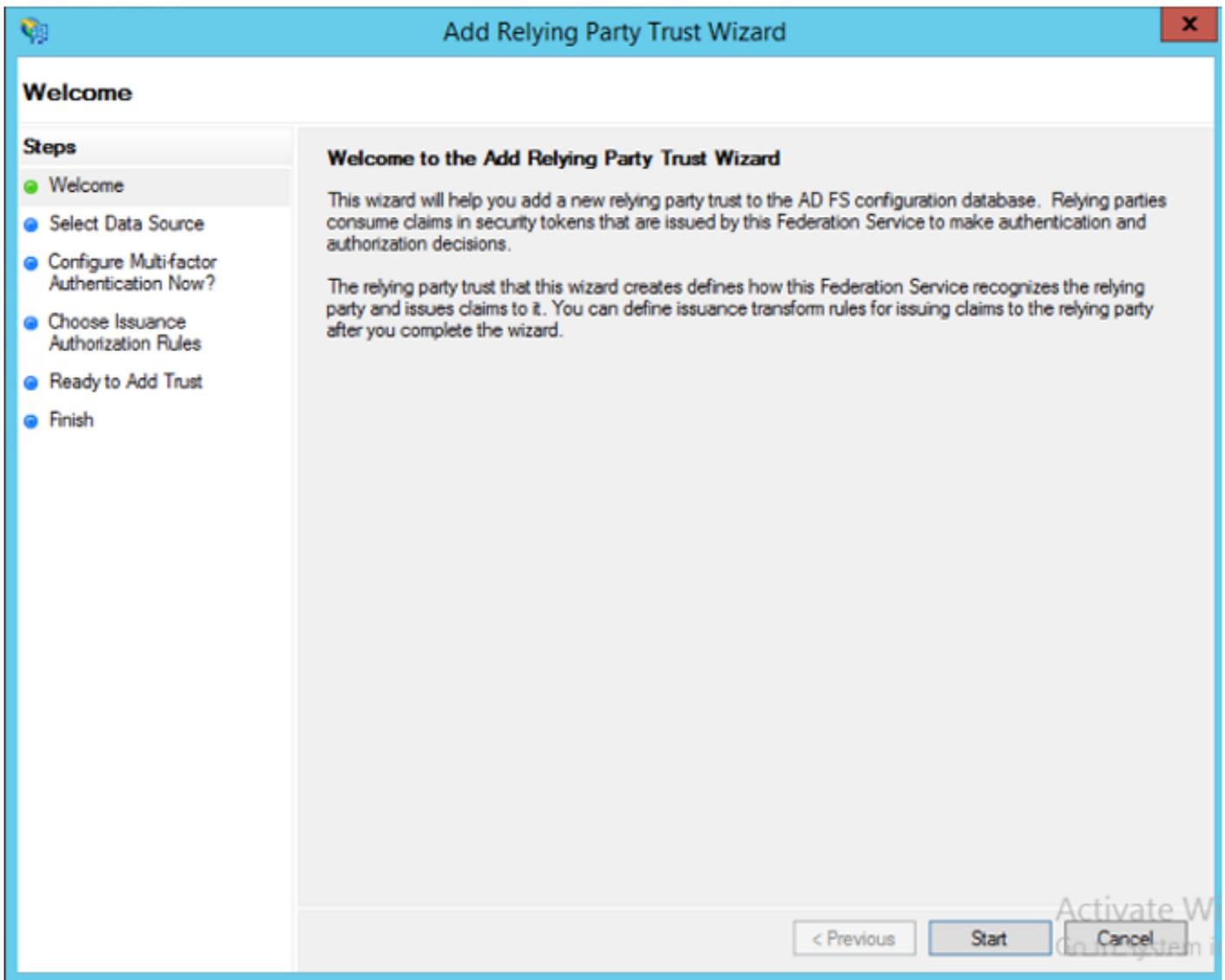
كلذ دعب هلىل جاتحتسو، sp_cucm0a.xml لثم لىنعم يذ مساب ايللم تانايبلا ظفح

ADFS ةامتعا ةهچ نيوكت

AD FS 3.0 ةرادا مكحت ةدحو لىل ءوچرلا

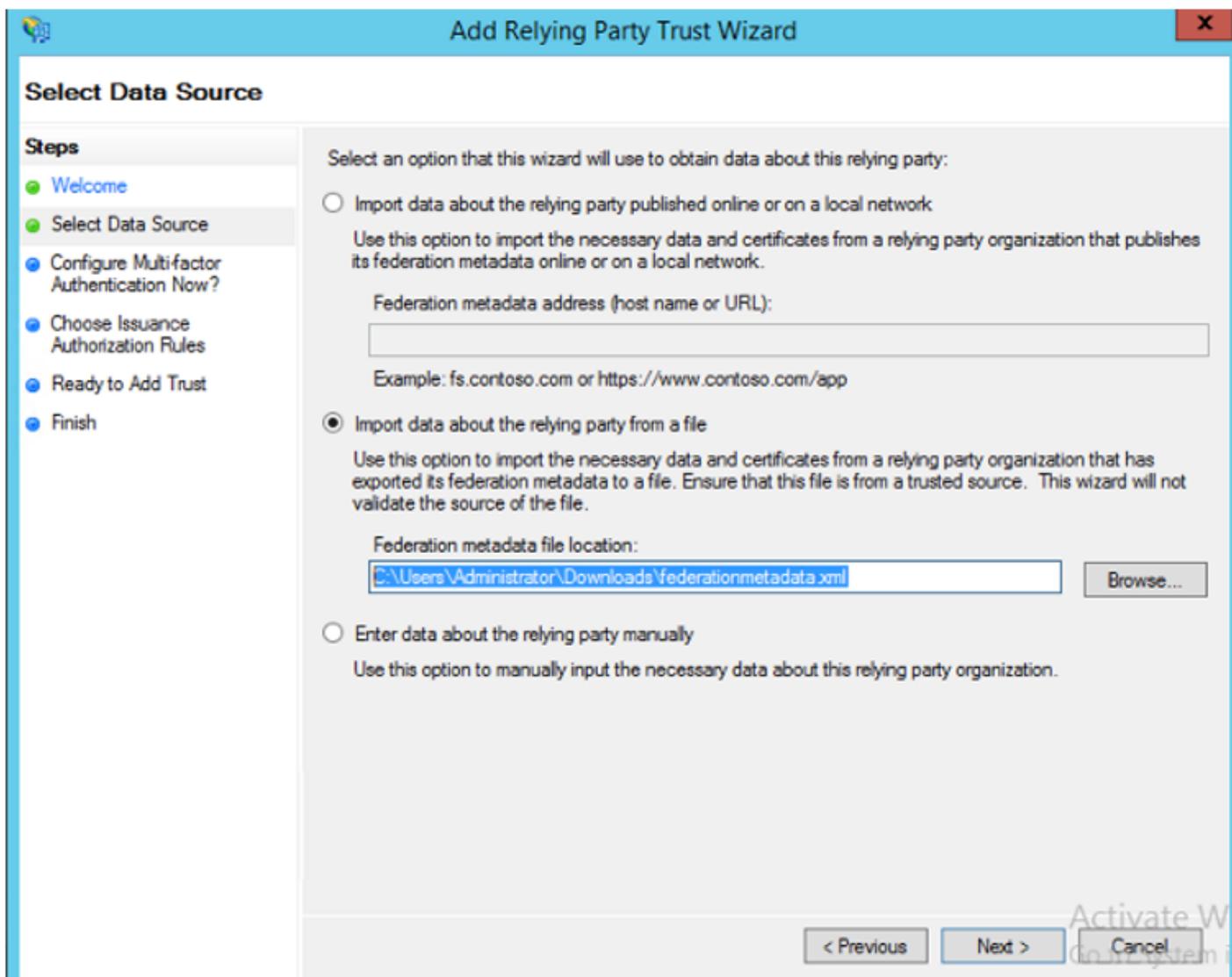


لعمل الفرطال عقث ةفاضل جلام قوف رونا



ةعبات ملل ءب قوف رونا

رونا واقباس اهظفحب تمق يتل Federationmetadata.xml فيرعت تانايل XML فلم دح
يللاتل



قوف رقن او ضرع لا مساك CUCM_CLUSTER_WIDE_RELIVING_PARTY_TRUST مدختسأ
يلاتلا

Add Relying Party Trust Wizard

Specify Display Name

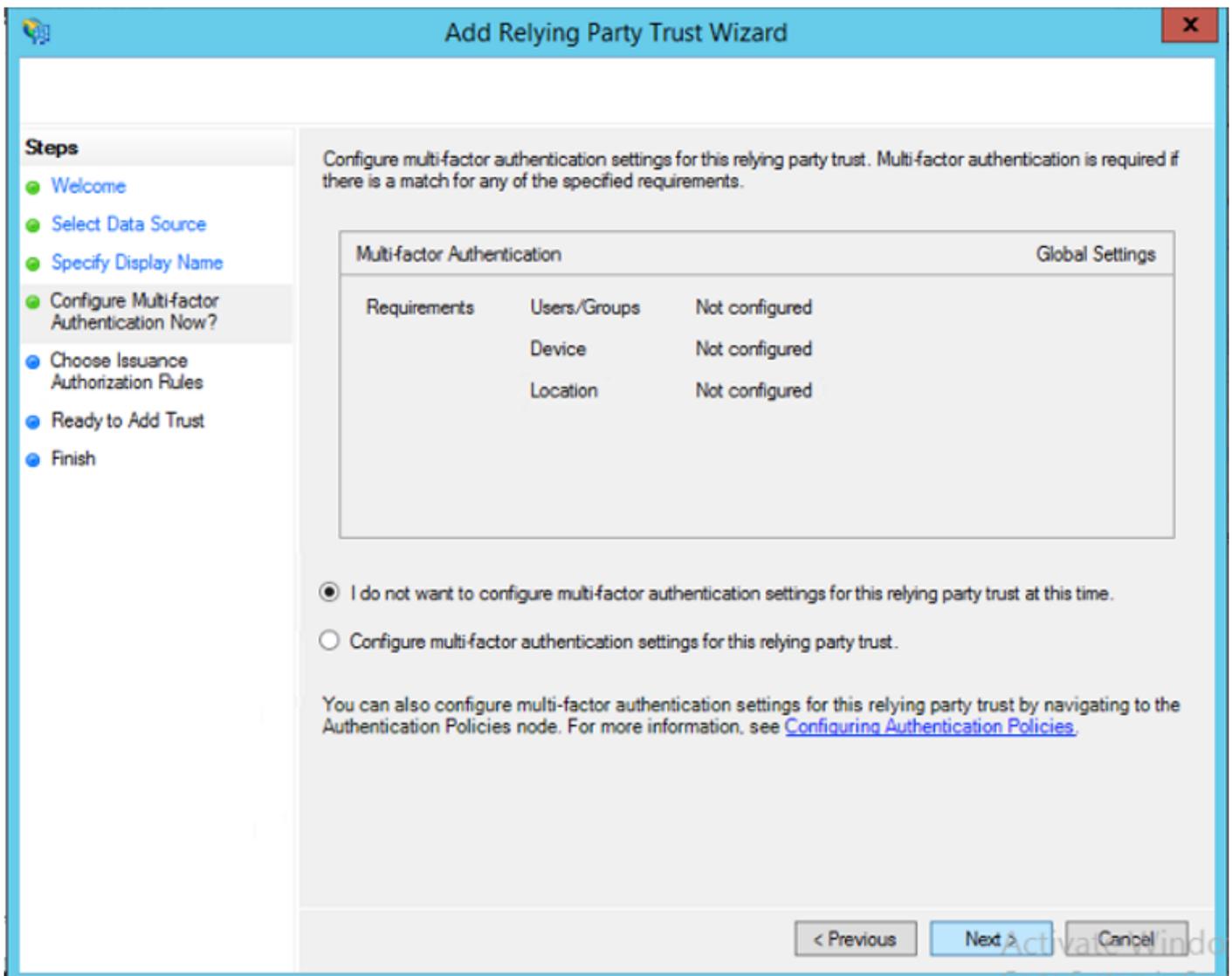
Enter the display name and any optional notes for this relying party.

Display name:

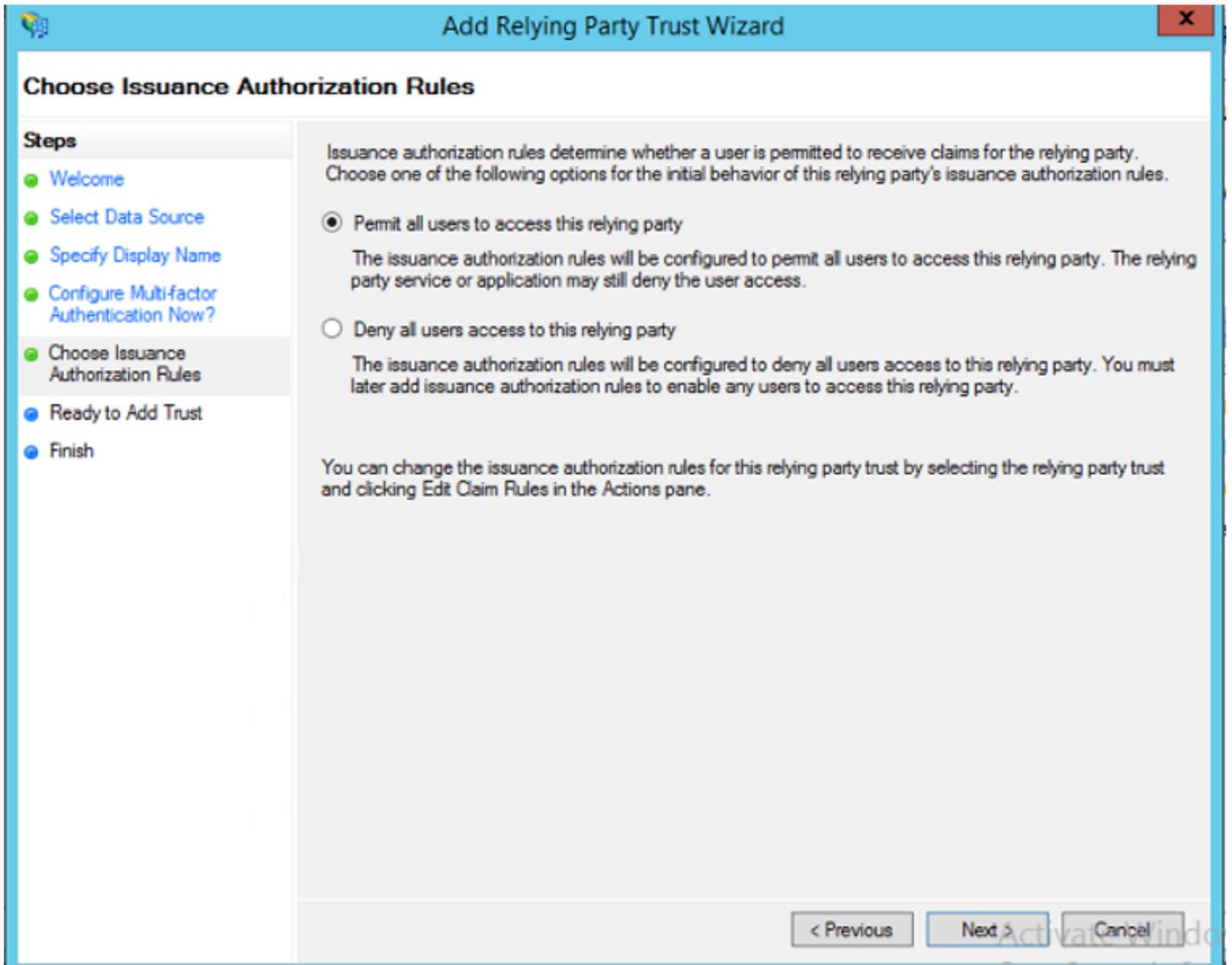
Notes:

< Previous Next > Cancel

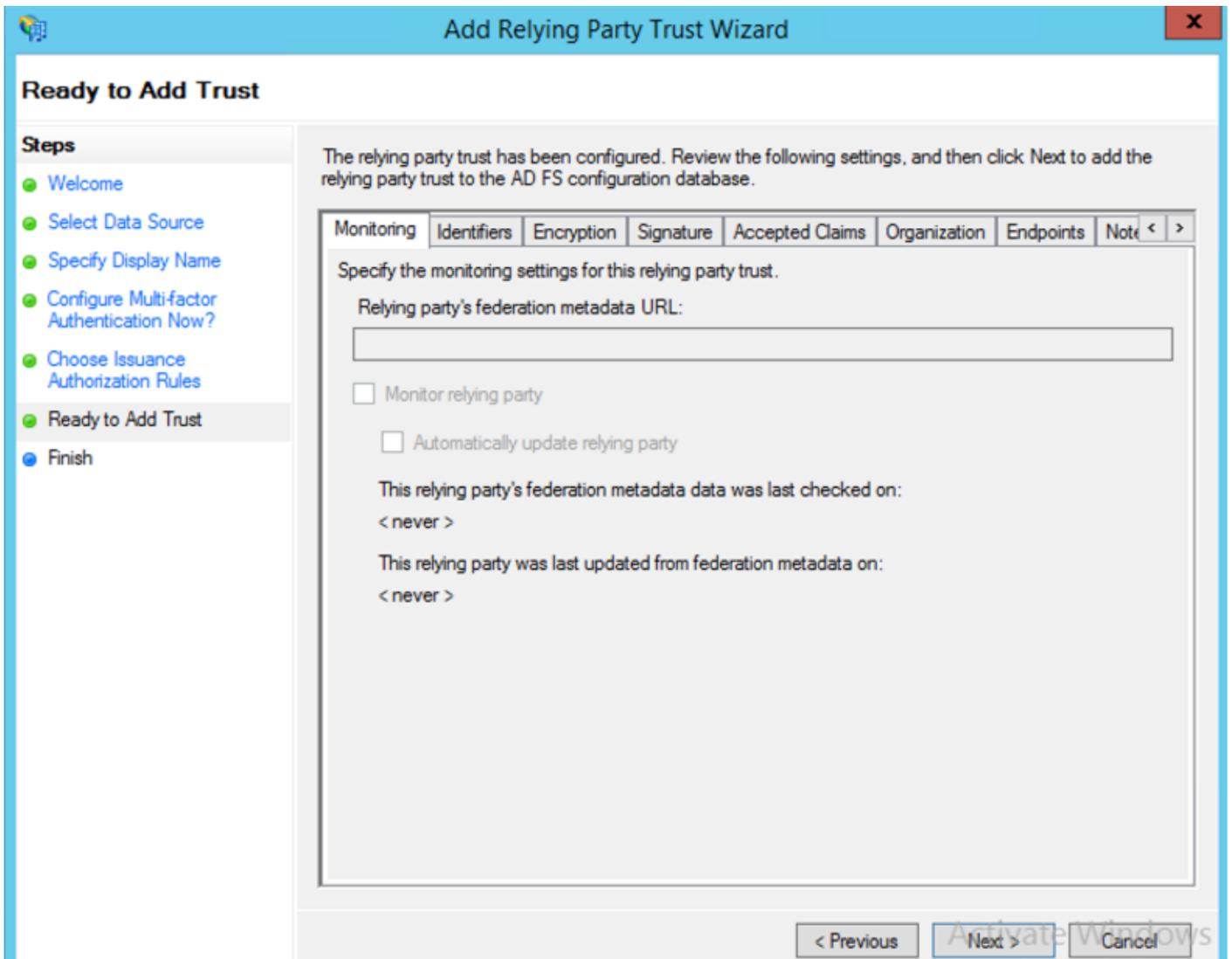
يہاں رکنوں اور لوگوں کو داخل کرنے کے لیے



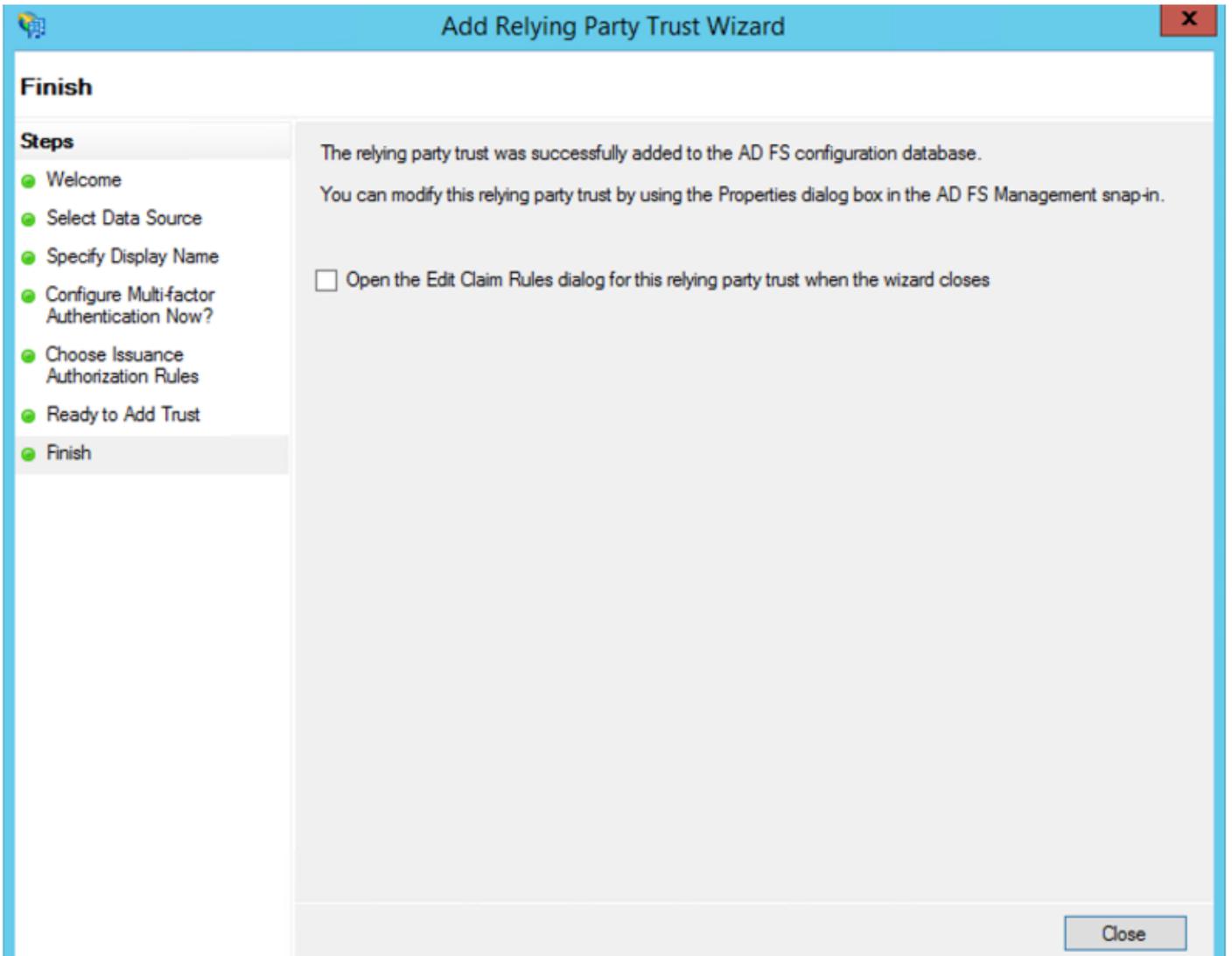
وه امك يلات ال قوف رقناو هذه دامت عالاه جى لى لوصول اب نيم دختسم ال عيم جى ل حامس ال ددح
ةروصل ال ي ف حضوم.



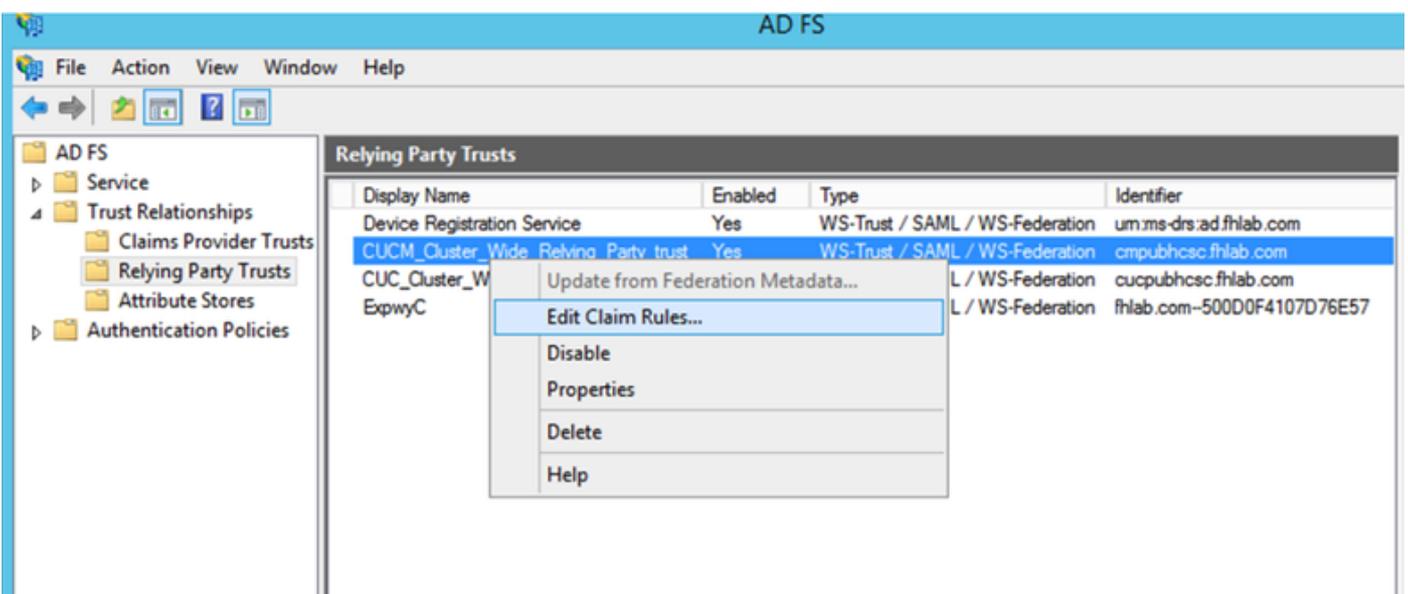
ةروضلا يف حضوم وه امك يلاتلا قوف رقناو نيوكتلا عجار.



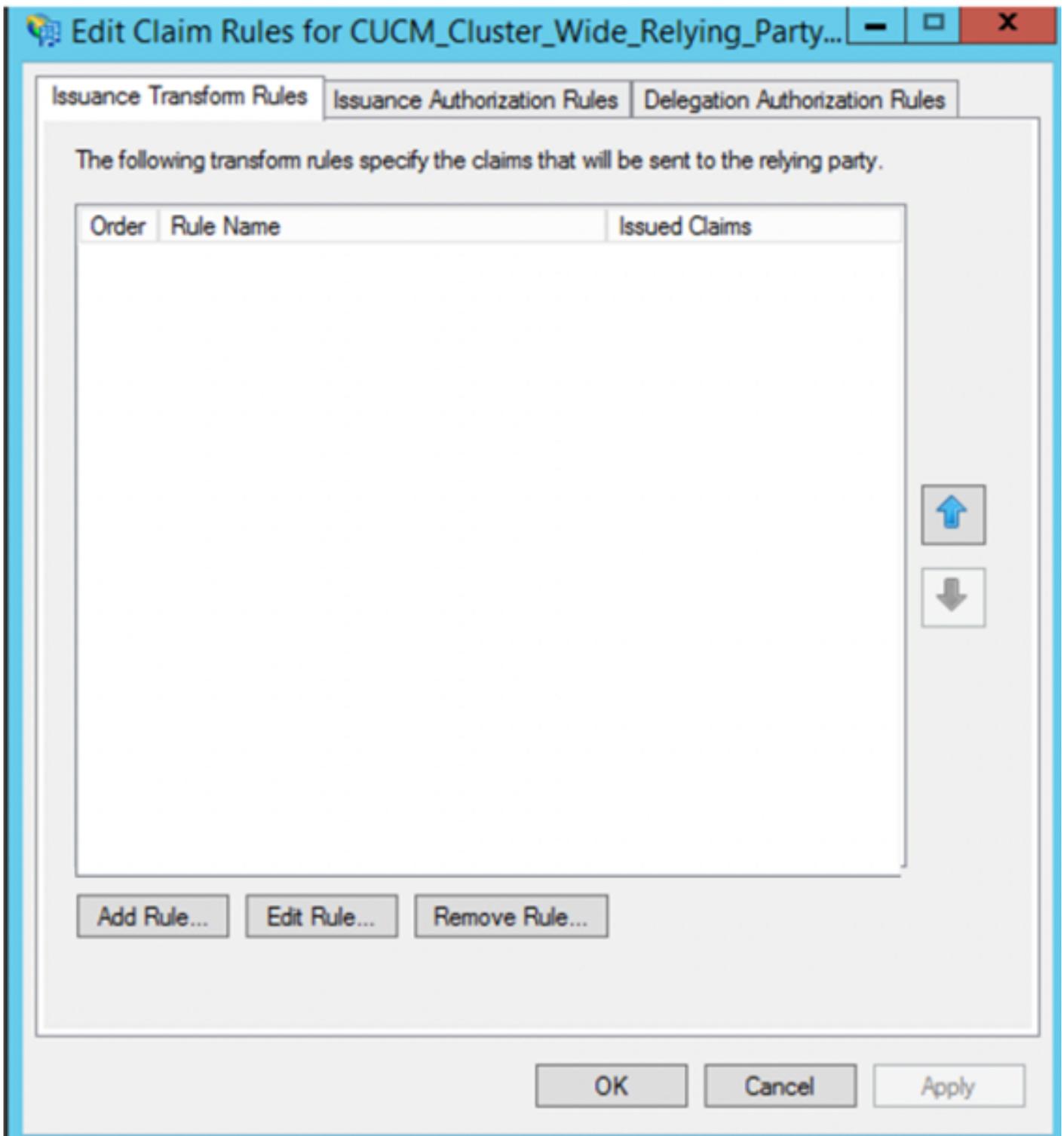
"قالغا قوف رقناو عبرم لا ديحت اءاغل اب مق



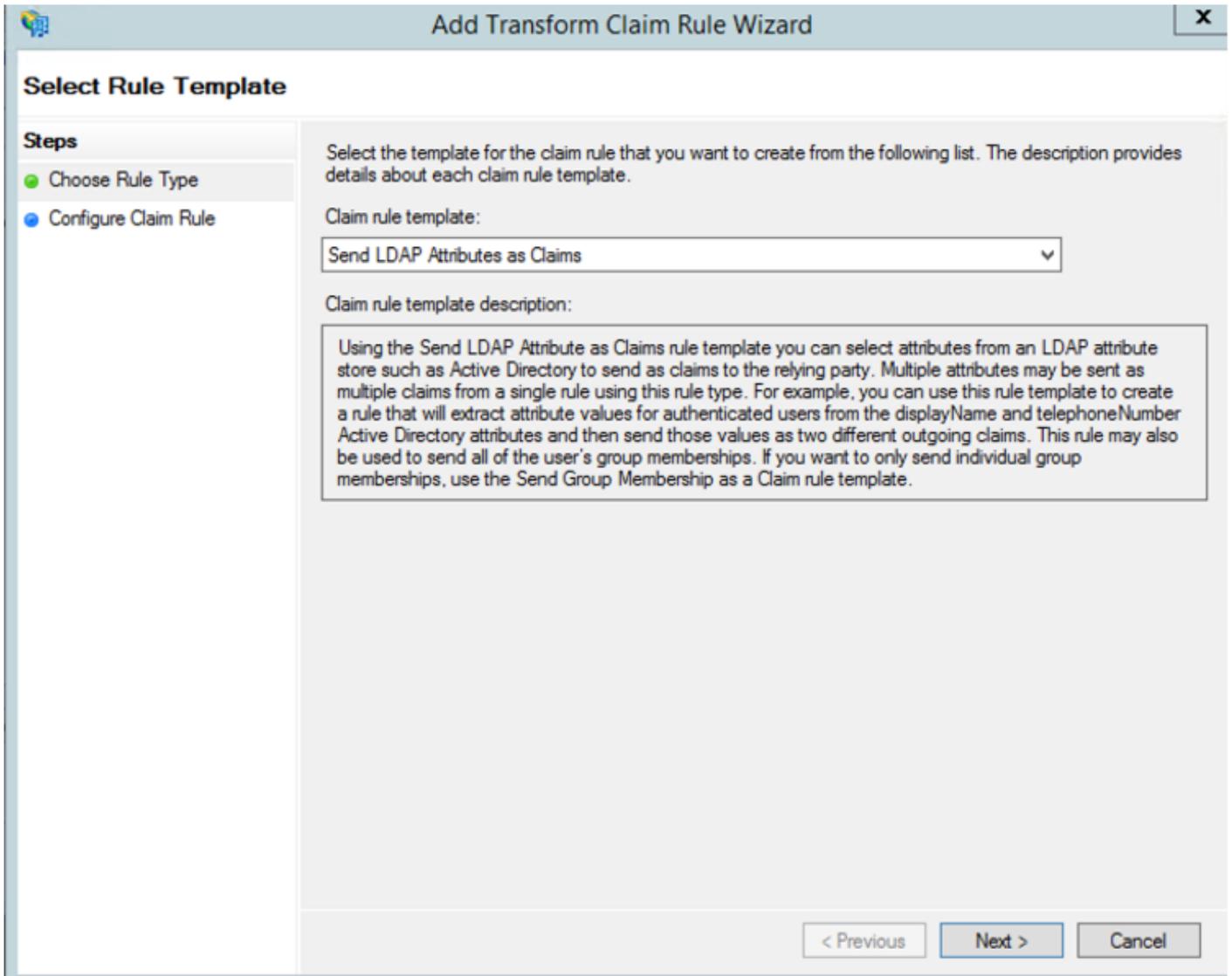
نيوكت ريرحت واهئاشناب تمق يتلا دامت عالاهج ةقث ددح، يونالثا سواملا رزم ادختساب ةروصلال يف حضوم وه امك تابلالاطملا دعاوق.



ةروصلال يف حضوم وه امك ريرطست ةفاضل قوف رقنا.



كلذ دع ب رقن او تابل لاطمك LDAP تامس لاسرا ددح.



تامل عمل هذه نيوكت:

NameID: ةبل اطل م ا ةد ا ق م سا

(ةلدسنملا ةمئاقلا مهس قوف اچودزم ارقن رقنا) Active Directory: تامسلل نزم

LDAP: SAM-account-name ةمس

uid: ةرداصل ةبل اطل م ا عون

ةعباتم لل قفاوم/ءاهن| قوف رقنا

ةمئاقلا يف لعفلاب دوجوم ريغ من اولقأ ةلاح يف سئل ديرفلل فرع م ا نأ ةطحال م ا اچرلا اذه بكتا. ةلدسنملا

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:

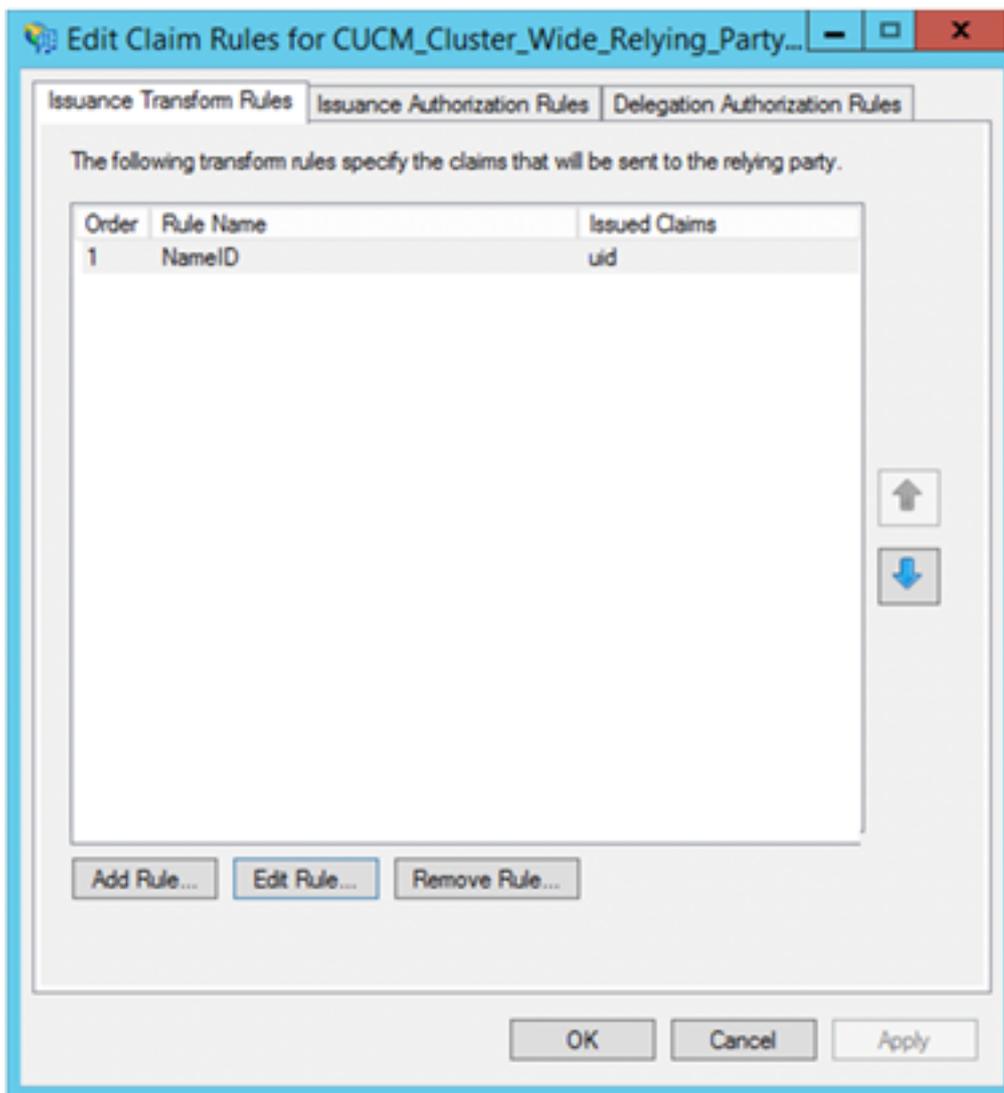
Rule template: Send LDAP Attributes as Claims

Attribute store:

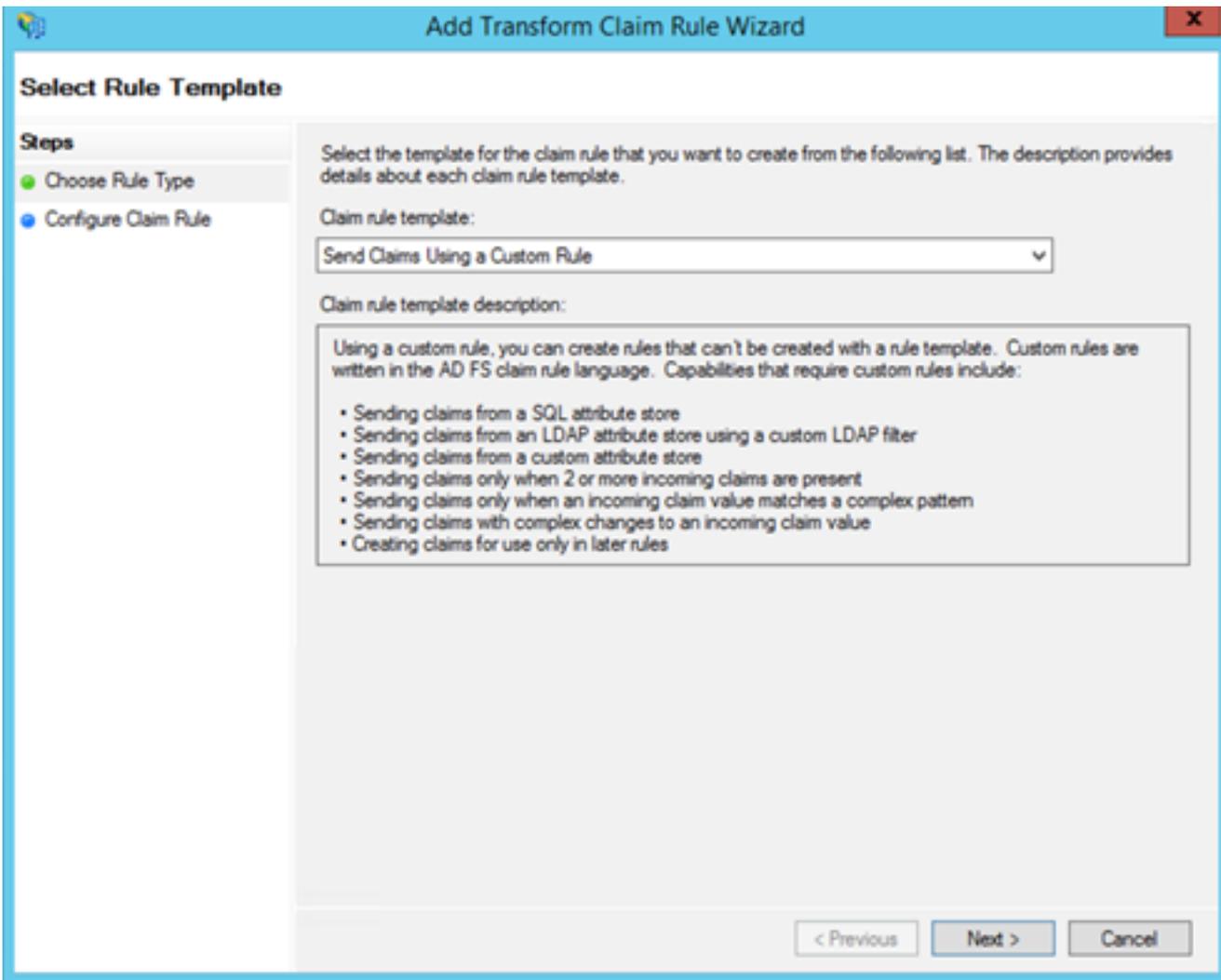
Mapping of LDAP attributes to outgoing claim types:

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

يرخأ ةدعاق ةفاضل يرخأ ةرم ةدعاق ةفاضل قوف رونا.



يُملأ قوف رقناو ةصصخم ةدعاق مادختساب تابلاطم لاسرا ددح.



قوالب قواعد تحويل الادعاءات CLUSTER_SIDE_CLAIM_RULE. يمكن استخدامها لإنشاء قواعد ادعاءات مخصصة.

يتم استخدامها لإنشاء قواعد ادعاءات مخصصة، والتي لا يمكن إنشاؤها باستخدام قوالب الادعاءات. يمكن كتابة قواعد الادعاءات المخصصة بلغة قواعد الادعاءات لـ AD FS. تشمل القدرات التي تتطلب قواعد الادعاءات المخصصة ما يلي:

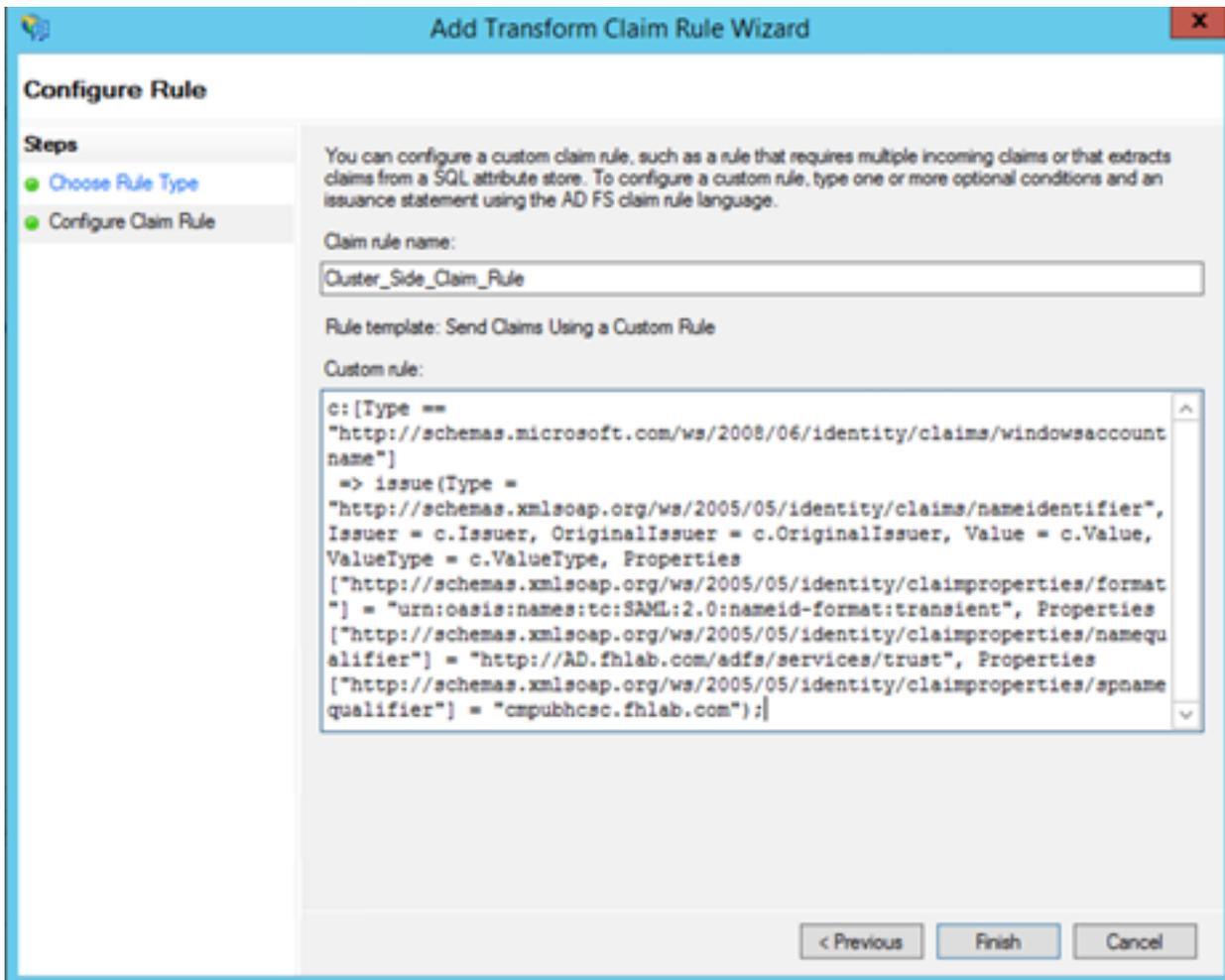
- إرسال الادعاءات من متجر السمات SQL
- إرسال الادعاءات من متجر السمات LDAP باستخدام مرشح LDAP مخصص
- إرسال الادعاءات من متجر السمات المخصص
- إرسال الادعاءات فقط عندما يكون هناك ادعاءات متداخلة أو أكثر
- إرسال الادعاءات فقط عندما يتطابق قيمة الادعاءات الواردة مع نمط معقد
- إرسال الادعاءات مع تغييرات معقدة على قيمة الادعاءات الواردة
- إنشاء الادعاءات لاستخدامها فقط في قواعد الادعاءات اللاحقة

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

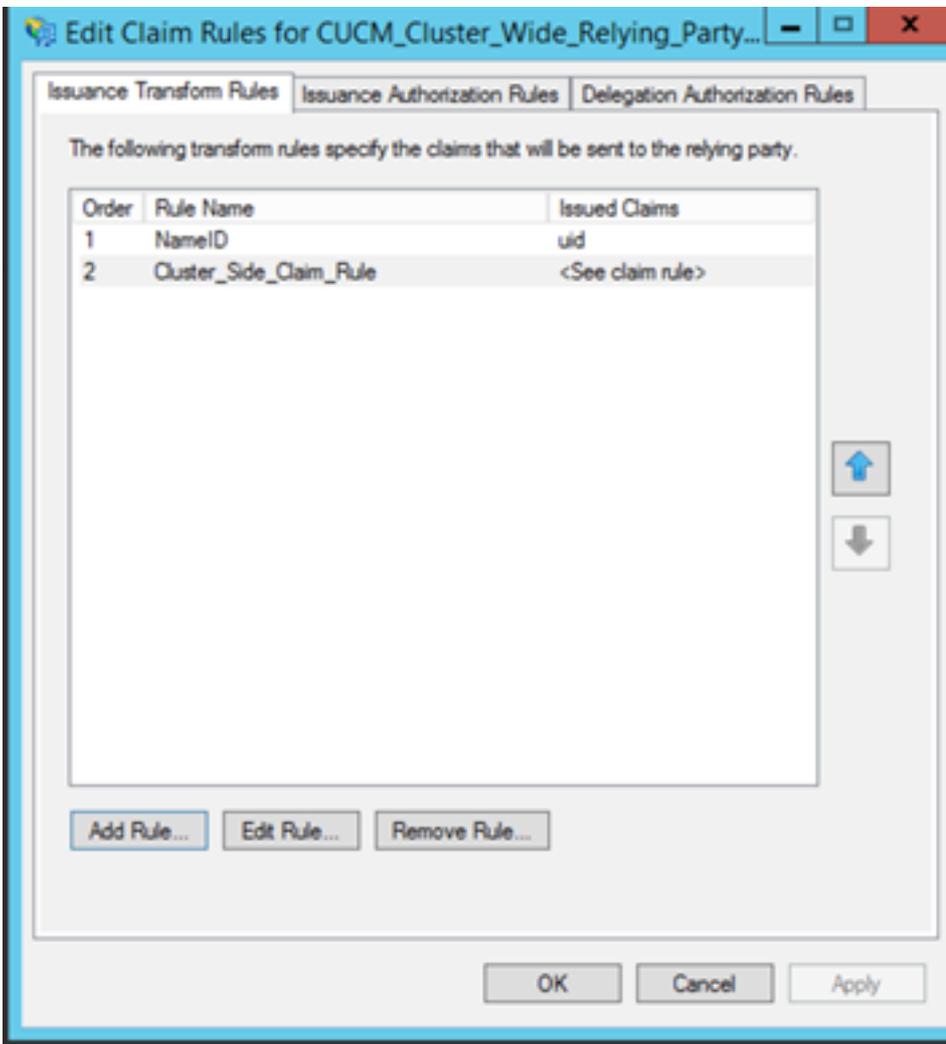
```
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"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");
```

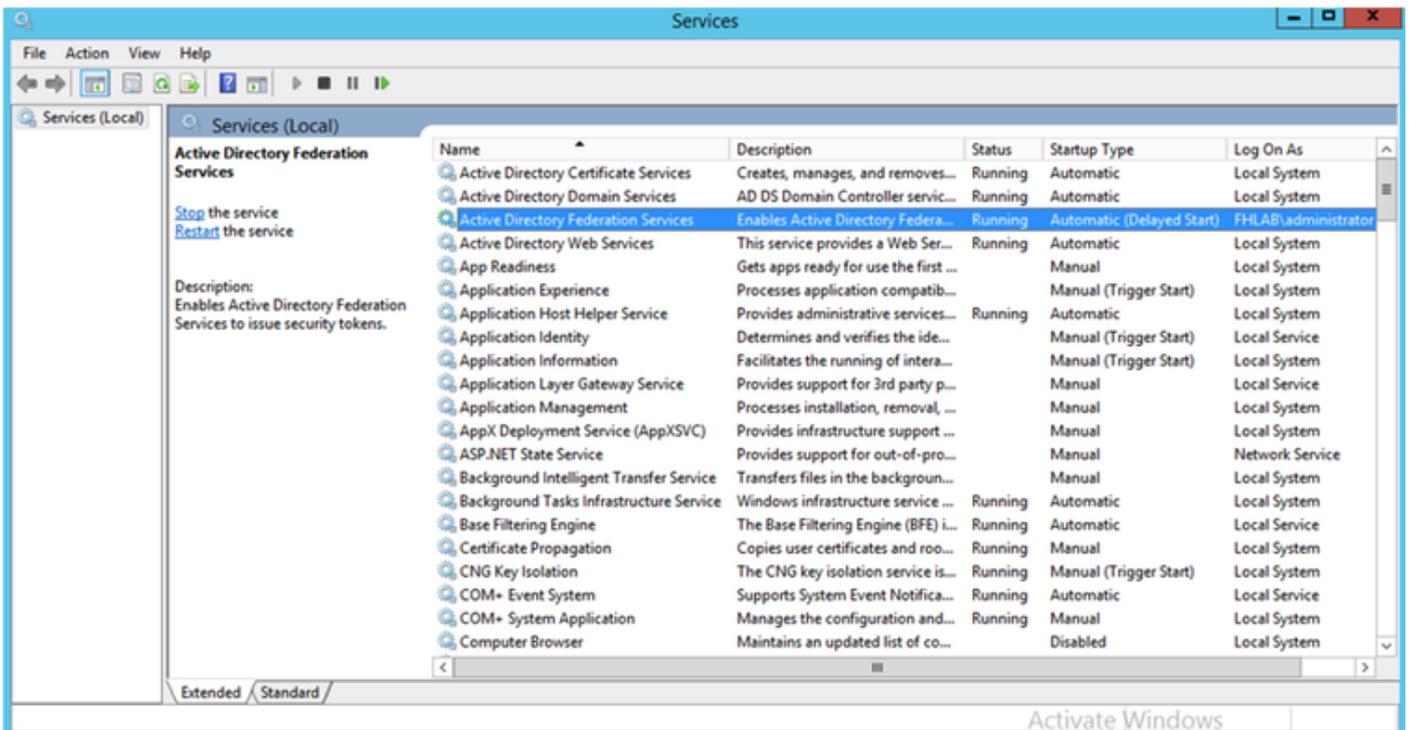
قوالب قواعد تحويل الادعاءات "عاشق" قوالب قواعد تحويل الادعاءات.



قال غإل ق ف او م و ق ي ب ط ت ق و ف ر ق ن ا . ADFS ل ع ن ي ف ر ع م ن ي ت د ع ا ق ن آ ل ا ك ي د ل ن و ك ي ن أ ب ح ي د ع ا و ق ل ا ة ذ ف ا ن .



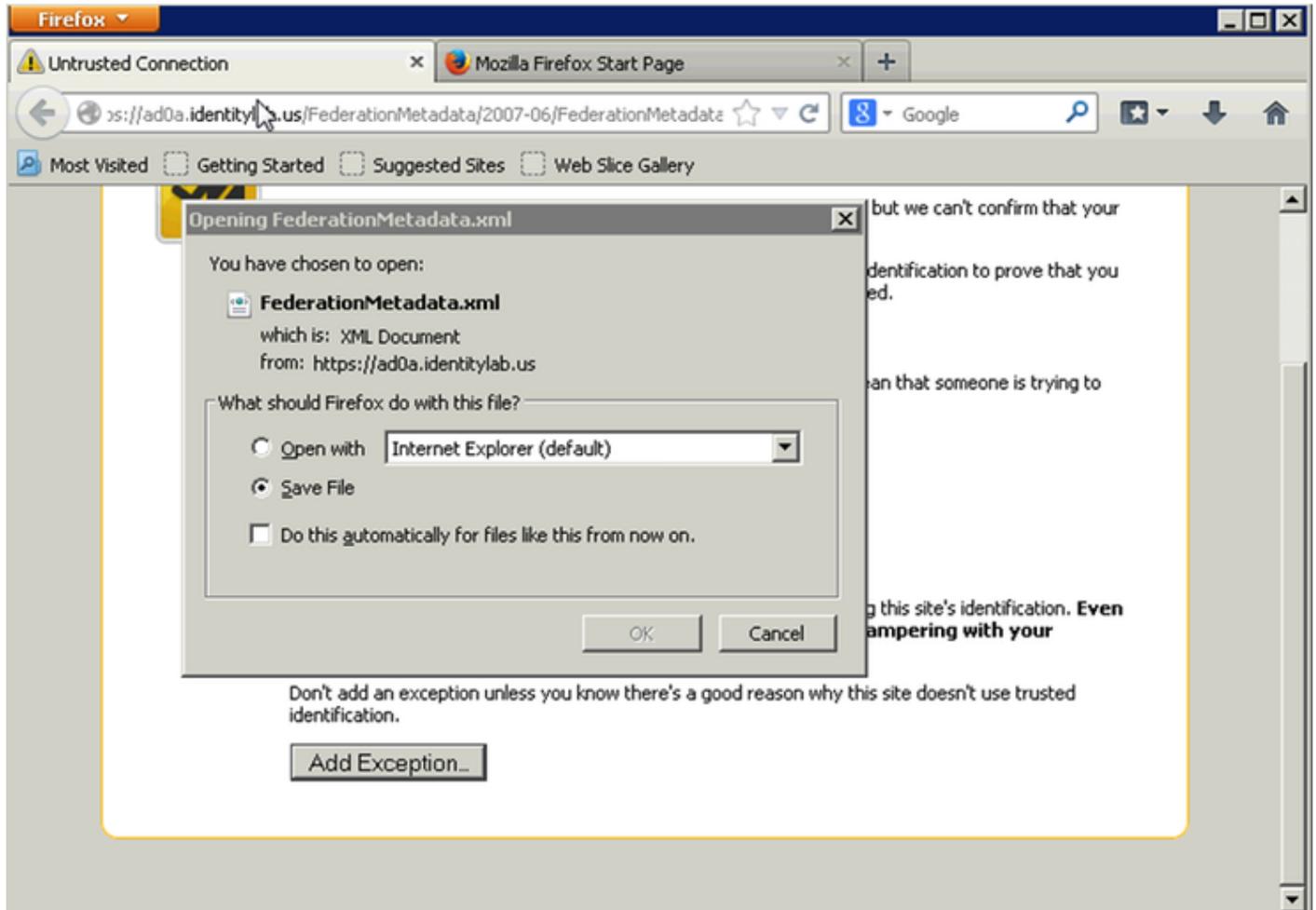
ADFS إلى اهاب قوتوم دامتعا ههك نألا حاجناب CUCM ةفاضلا تمت



تامدخ > ةيراد ا تاودأ > ادبا ةمئاق إلى لقتنا ADFS. ةمدخ ليغشت ةداع ا عاجرلا، ةعباتملا لبق

ايلخاد ني درشملا فيرعت تانايب

مادختساب تامولعمل هذه لدابت متي. انب صاخلا IDp لوح تامولعمل م CUCM ديوزت ىل اجاتحت
ADFS. تىبثت متي شيح مداخل ال ىل ع ووطخل هذه ذيفنت نم دكأت XML فيرعت تانايب



XML تانايب لىزن تل Firefox ح فرصتم مادختساب (IDp) ADFS ب لاصتال ال اجاتحت، الوأ
ىل اجاتحت فى ا ح فرصتم ح فى ا https://<ADFS FQDN>/FederationMetadata/2007-
06/FederationMetadata.xml واطفح او

SAML يداخال لوخدلا لىجست عمئاق > ماظنلا عمئاق ىل CUCM نيوكت ىل لقتنا، نألا

The screenshot shows the Cisco Unified CM Administration web interface. The browser address bar displays the URL: <https://cmpublicsc.fhlab.com:8443/ccadmin/ccmGroup>. The page title is "Cisco Unified CM Administration". A navigation menu is open on the left side, listing various configuration options. The "SAML Single Sign-On" option is highlighted. The main content area shows a search filter for "Manager Group" with a dropdown menu set to "begins with". Below the search bar, there is a message: "No active query. Please enter your search criteria using the options above." The URL at the bottom of the screenshot is <https://cmpublicsc.fhlab.com:8443/ccadmin/samlSingleSignOn.do>.

- Server
- Cisco Unified CM
- Cisco Unified CM Group
- Presence Redundancy Groups
- Phone NTP Reference
- Date/Time Group
- BLF Presence Group
- Region Information
- Device Pool
- Device Mobility
- DHCP
- LDAP
- SAML Single Sign-On**
- Cross-Origin Resource Sharing (CORS)
- Location Info
- MLPP
- Physical Location
- SRST
- Enterprise Parameters
- Enterprise Phone Configuration
- Service Parameters
- Security
- Application Server
- Licensing
- Geolocation Configuration
- Geolocation Filter
- E911 Messages

SAML يداخ ل وخذ ليجست > ماظنلا ددحو CUCM قراذ اىل لقتنا

The screenshot shows the Cisco Unified CM Administration interface for SAML Single Sign-On. The status is '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

دخول SAML SSO.

رابطه را در آدرس بار وارد کنید و دکمه Run Test را بزنید.

The screenshot shows a 'Reset Warning' dialog box with the following text:

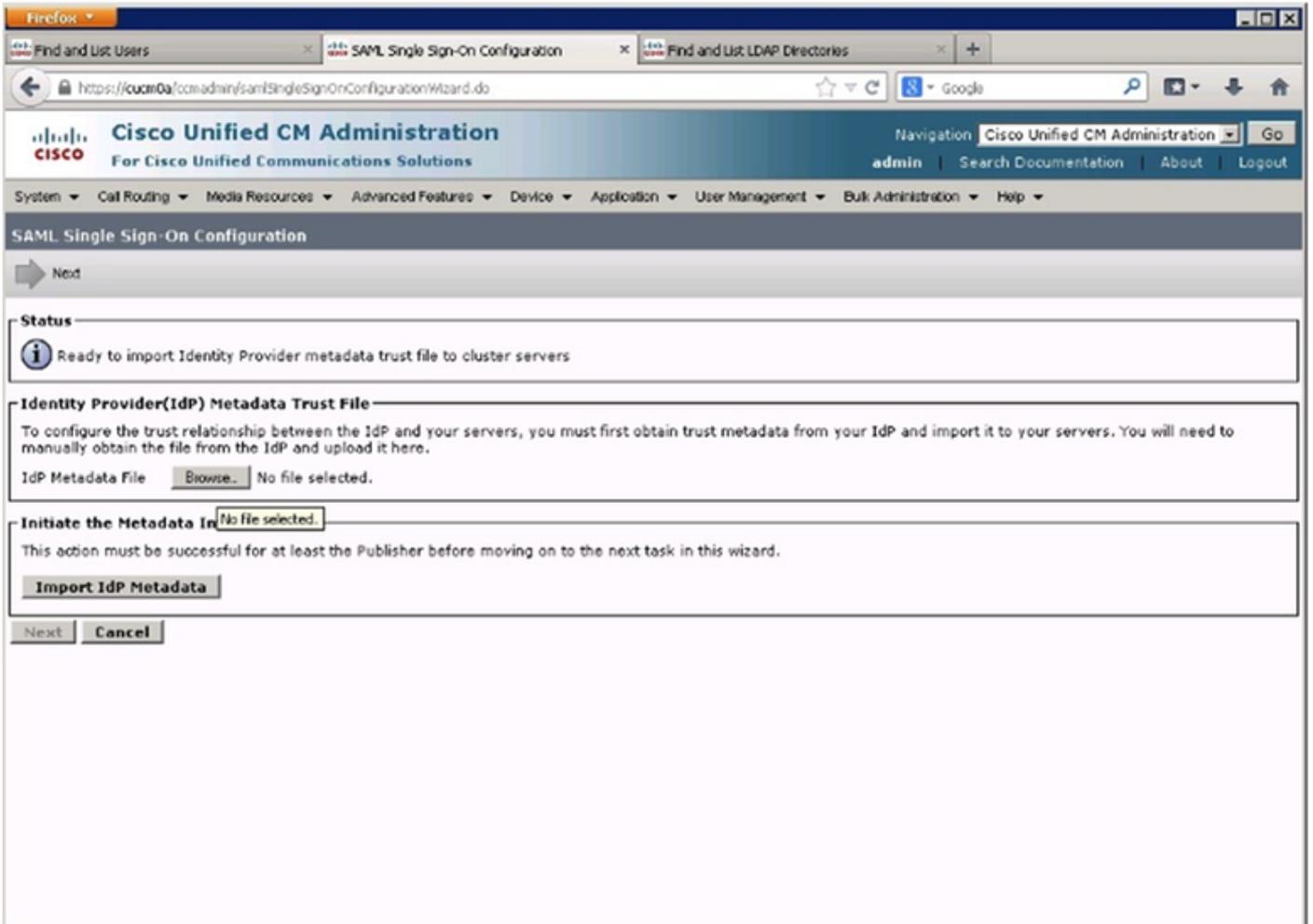
Web server connections will be restarted

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.

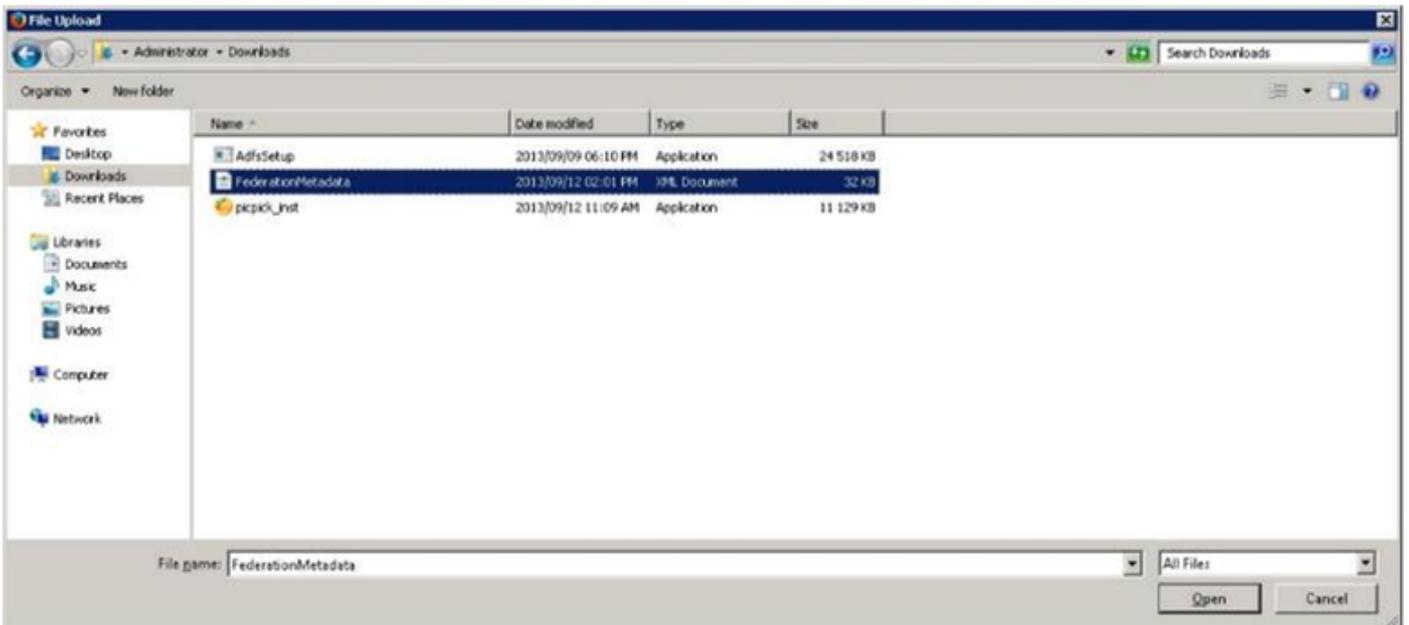
Buttons: Continue, Cancel

فهرست اتانای XML فلم داریت سال.. ضارعت س | لعل روناو SSO ةشاش لعل

ةروصلال ي ف حضورم وه امك اق بس م اهظ ف ح ب تم ق ي ت ل ال FederationMetadata.xml



ةلض فلم ل نمض تال ي ز ن ت ل ال نم CUCM ل ال ه ل ي م ح ت ل ح ت ف ق و ف ر ق ن و XML فلم د د ح



ل ال CUCM ل ال IdP تاملول عم دار ي ت س ال IdP ف ي ر ع ت تاناي ب دار ي ت س ل ل ع ر ق ن ا ، ه ل ي م ح ت در ج م ب ة ع ب ا ت م ل ل " ي ل ا ت ل ا " ق و ف ر ق ن و دار ي ت س ال ا ح ا ن نم د ك ا ت

SAML Single Sign-On Configuration - Windows Internet Explorer

Navigation Cisco Unified CM Administration 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

قوف رقناو ني سايقلا نيزيتملا CCM يمدختسم لىا يمتني يذلا مدختسملا دح "SSO" رابتخا ليغشت.

SAML Single Sign-On Configuration - Mozilla Firefox

https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOnConfigurationWizard3.do?servei ...

SAML Single Sign-On Configuration

Test SSO Setup

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This 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

2) Launch SSO test page

ةم لك و مدخت س م ل م س ا ب ل و خ د ل ا ل ي ج س ت ب م ق م د خ ت س م ل ا ة ق د ا ص م ر ا و ج ع ب ر م ع م ه م ي د ق ت د ن ع ن ي م ا ل م ل ر و ر م ل .

Sign In - Mozilla Firefox

https://ad.fhlab.com/adfs/ls/?SAMLRequest=nZJPTwIxEMXvflpN77CIAi4NS0 ...

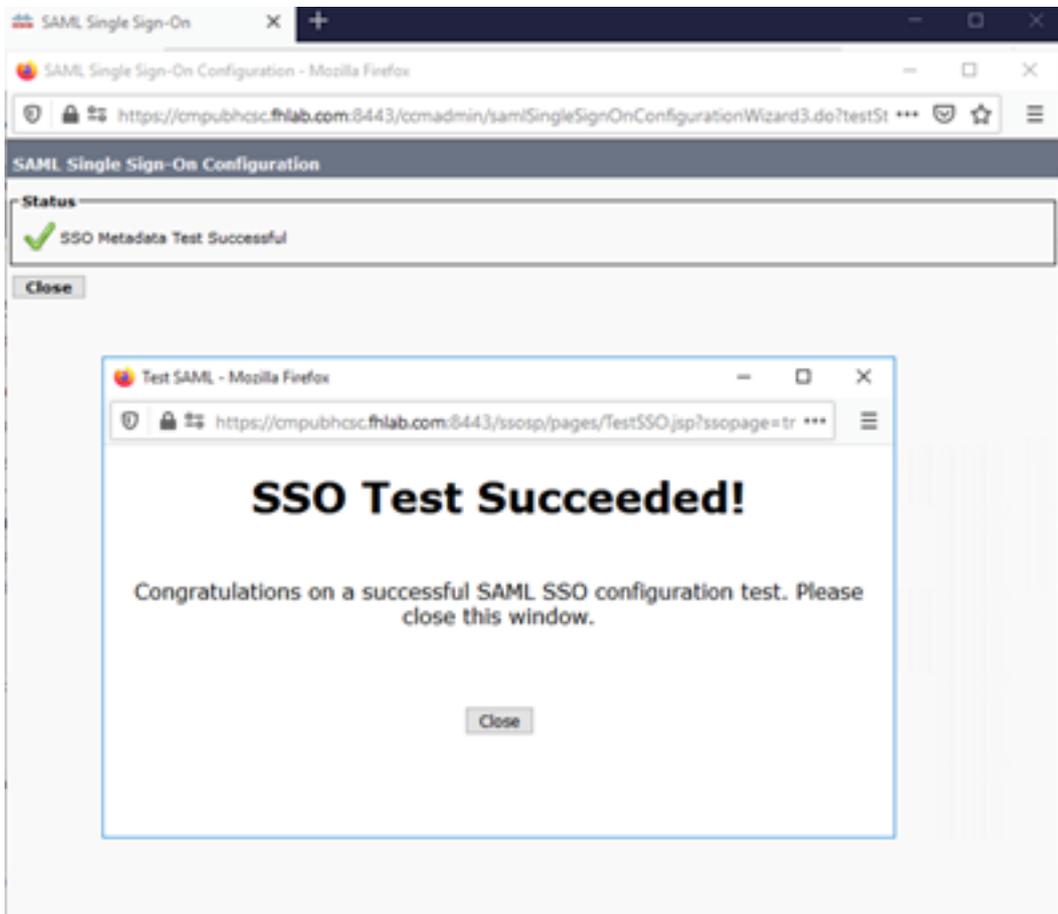
FS

Sign in with your organizational account

farfar@fhlab.com

.....

SSO! ر ا ب ت خ ! ح ا ج ن ل و ق ت ة ل ا س ر ر ت ن ا ب ج ي ، ح ي ح ص ل ك ش ب ع ي ش ل ك ن ي و ك ت م ت ا ذ ا



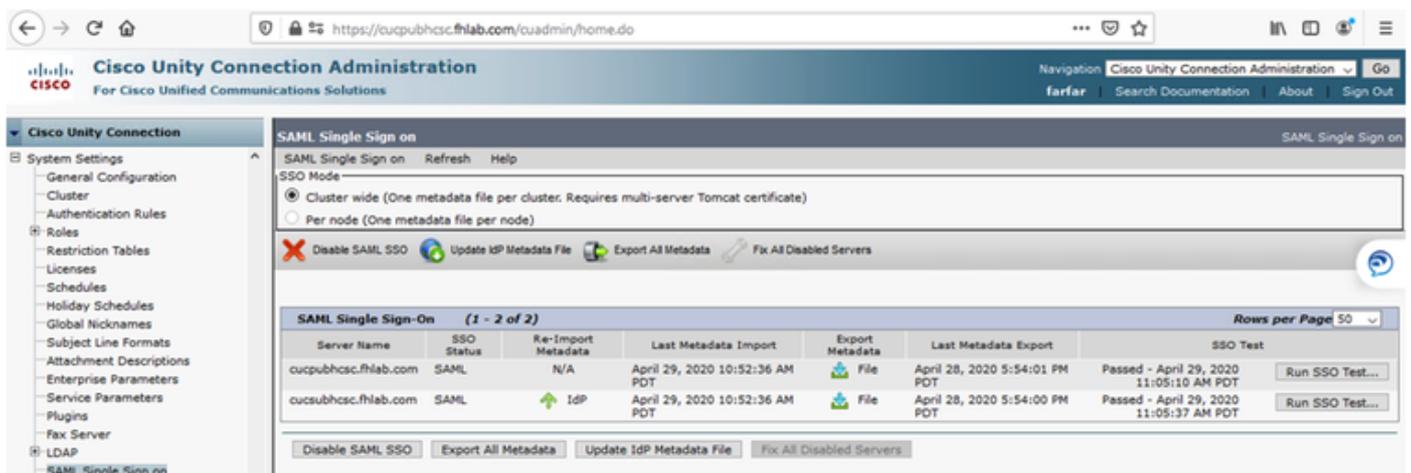
ةعبات ملل "ءاهن" و "قالغ" قوف رونا

ADFS مادختساب CUCM ىلع SSO نيكمتل حاجنب ةيساسأل نيوكتل ما هم لامك نأل امت

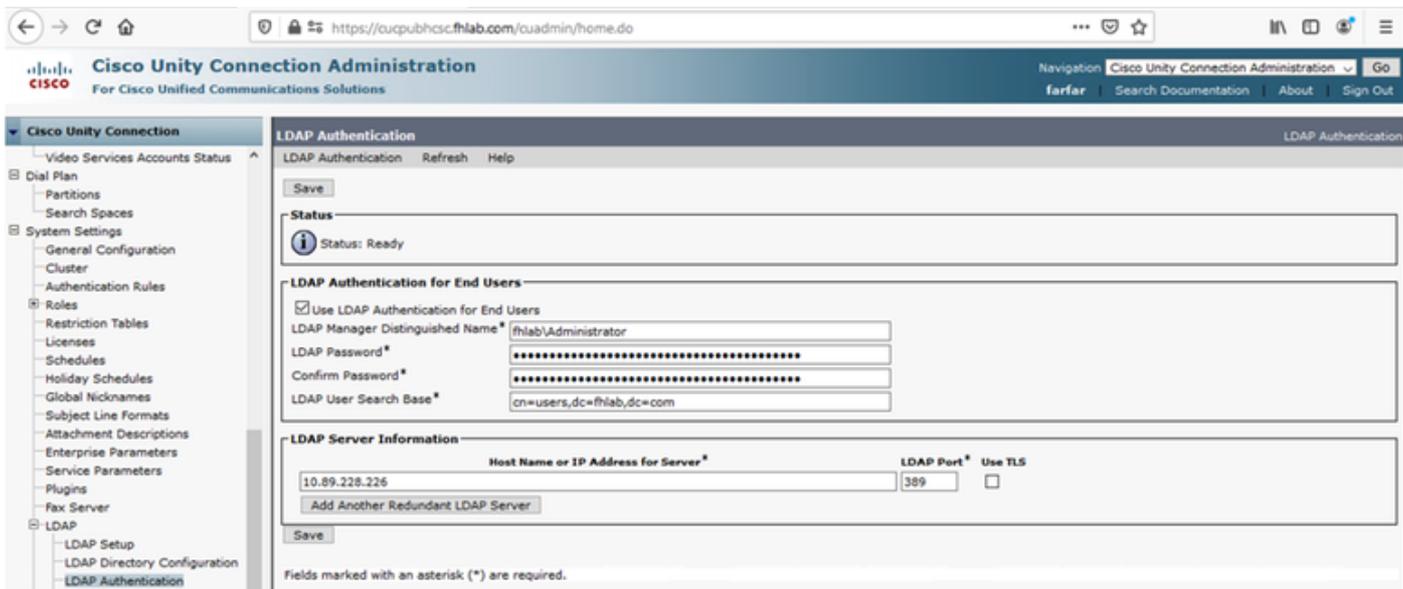
CUC ىلع SSO نيوكت

Unity Connection في SSO نيكمتل ةيلعمل لسفن عابتا نكمي

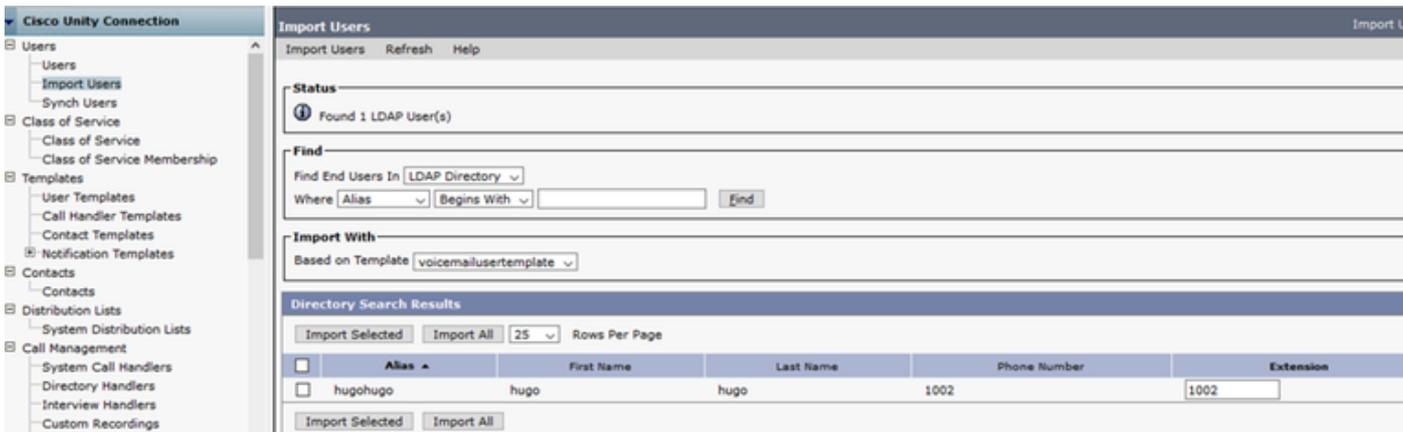
CUC عم LDAP جمدم



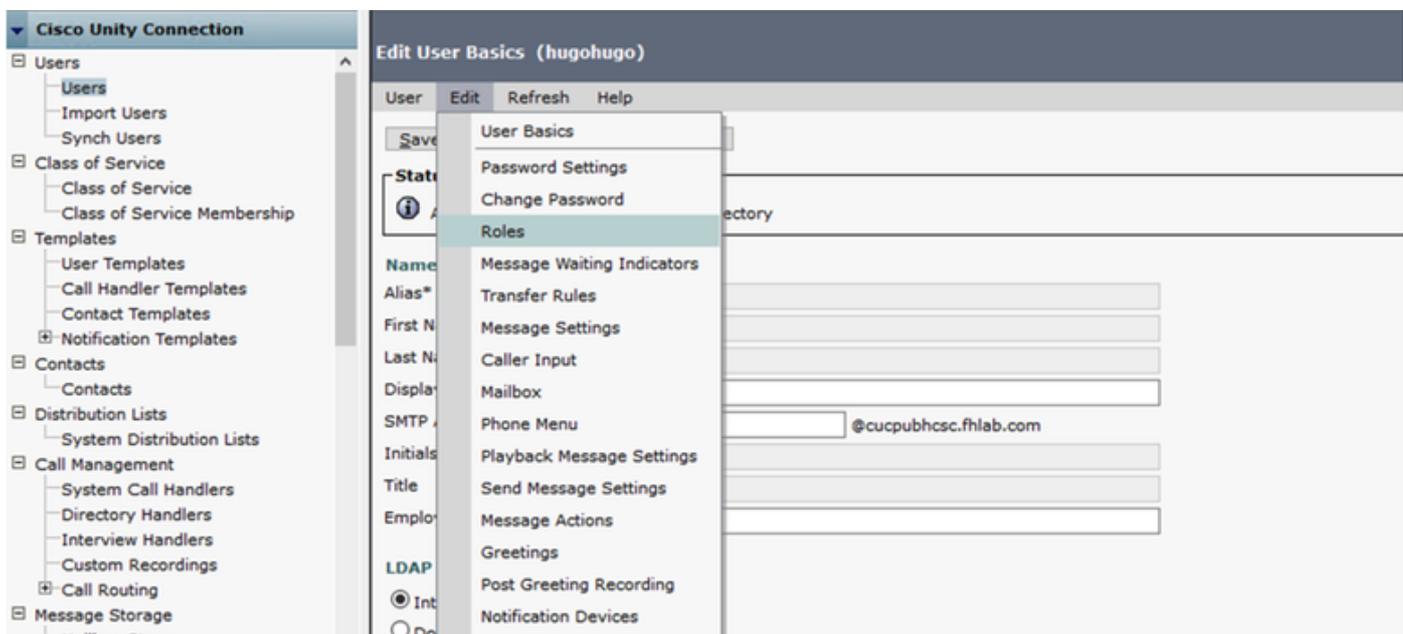
LDAP ةقداصم نيوكت



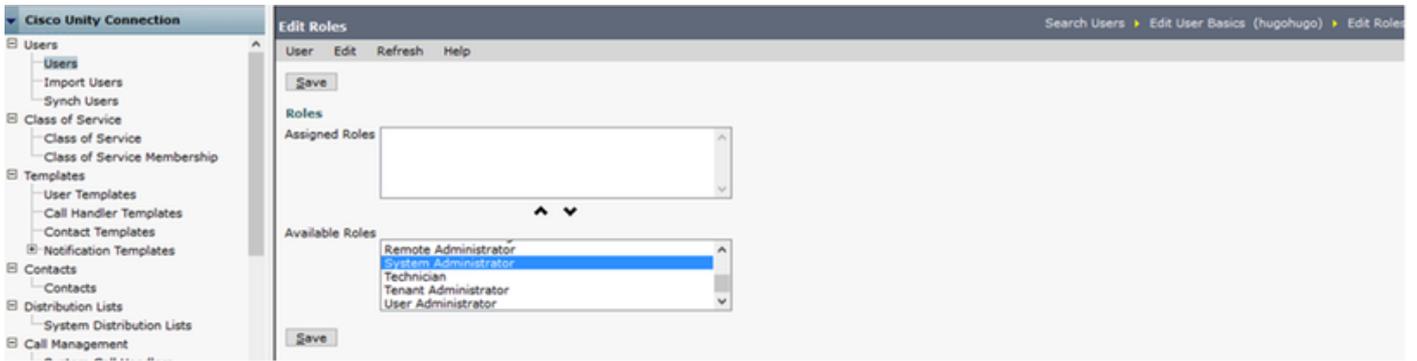
مدخست سمل ك لذك و هل يت واصل دي ربل ني عت متي س ي ذل LDAP نم ني مدخست سمل ا داري ت س ل SSO رابت خ ل ع لم عي س ي ذل



ة روصل ي ف حضورم وه امك راودأ > ريرحت > ني مدخست سمل ا ل ق ت نا

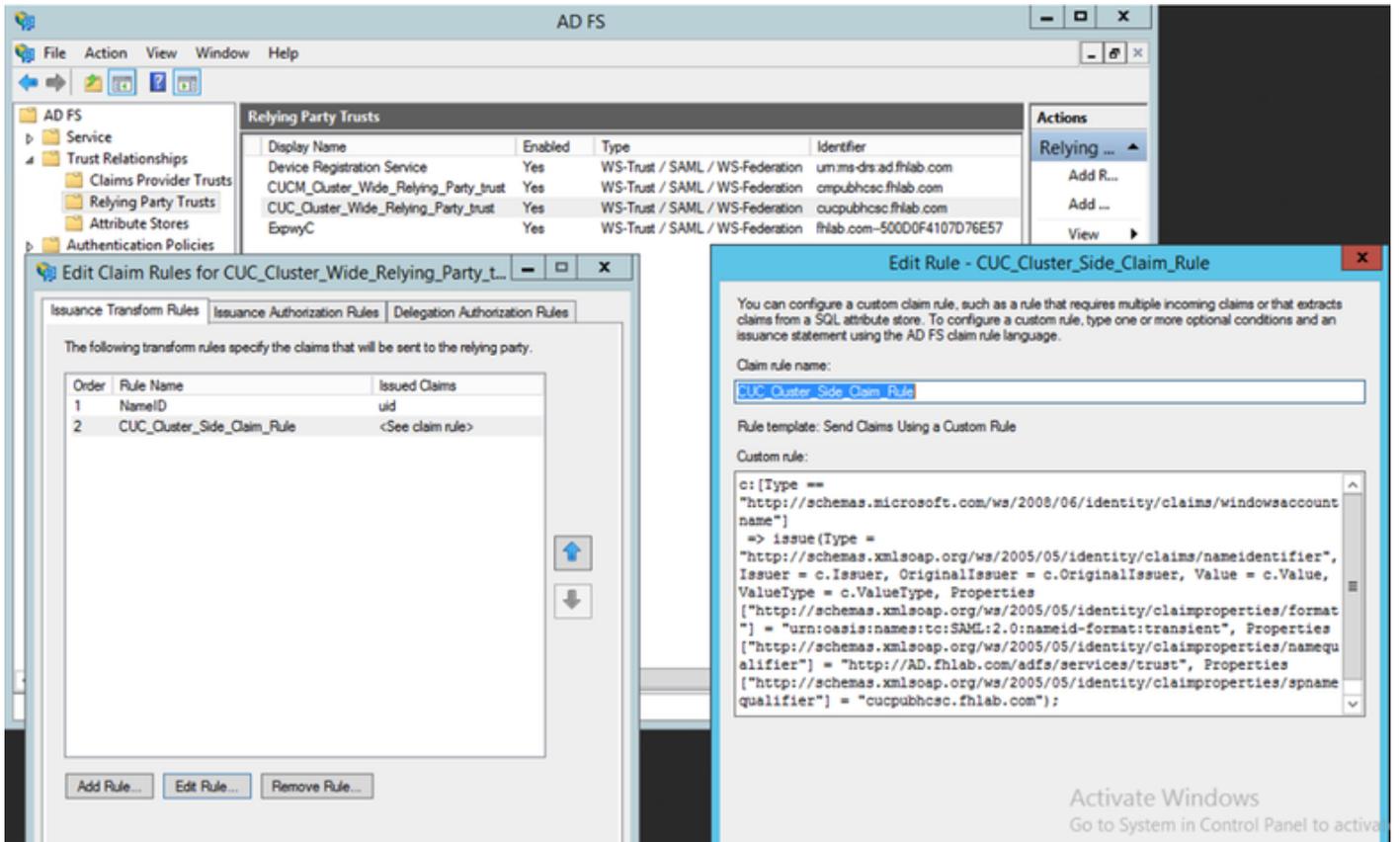


رابت خ ال ا مدخست سمل ا مظن ل ل لوؤسم رود ني عت



CUC فيرعت تانايب

CUC ل RelyingPartyTrust ءاشن او، CUC فيرعت تانايب ليزن تبت تمق دق نوكت نأ بجي AD FS 3.0 لىل ءاوق ءاشن او CUC فيرعت تانايب لىمحت و



SSO نىمكتب مقو SAML ل يداخال لوخدلا لىجست لىل لقتنا

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
- huqohuqo

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

Expressway SSO نيوكت

Expressway C لى فيرعتل تانايب داريتسا

لى حفصتم حتفا <https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml> لى حفصتم حتفا

IDP > ةدومل تالاصتالا > نيوكتل لى لىمحتلا

Expressway C نم فيرعتل تانايب ري دصت

SAML تانايب ري دصت -> IDP -> ةدحومل تالاصتال -> نيوكتل لىل لقتنا

يف ةنمضم (ليوط يضا رتفا رمع تاذ) ايتاذ ةعقوم ةداهش ةعومجمل ماظن عضو مدختسي SAML

SAML تابلط عيقوتل ةمدختسمل او ةيولوال تانايبلا

- وتسم لىل داخا ةي فصولا تانايبلا فلم ليزنتل، ةضيرعل ةعومجمل ماظن عضو ي ف ليزنت قوف رقنا، ةعومجمل
- ليزنت قوف رقنا، يدرف ريظنل فيرعتل تانايب فلم ليزنتل، ريظن لك عضو ي ف لىل ليزنت رقنا، zip. فلم ي ف لىل ري دصت. ريظنل راوجب

Cisco Expressway-E ل دامتعالا فرط ةقث ةفاضل

لاسرال ةبللاطم ةدعاق فضا مث Expressway-Es تامسل لوعمل فرطال ةقث عاشناب مق، الوأ UID ةمسك ةيولال

The screenshot displays the Cisco Expressway configuration interface. On the left, a tree view shows the configuration hierarchy: AD FS > Service > 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-ds.ad.fhlab.com
CUCM_Cluster_Wide_Relying_Party_trust	Yes	WS-Trust / SAML / WS-Federation	cmpubhcsc.fhlab.com
CUCM_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. It includes a table for 'Issuance Transform Rules' with the following data:

Order	Rule Name	Issued Claims
1	NameID	uid

The 'Edit Rule - NameID' pane also shows the 'Rule template: Send LDAP Attributes as Claims' and the 'Mapping of LDAP attributes to outgoing claim types' table:

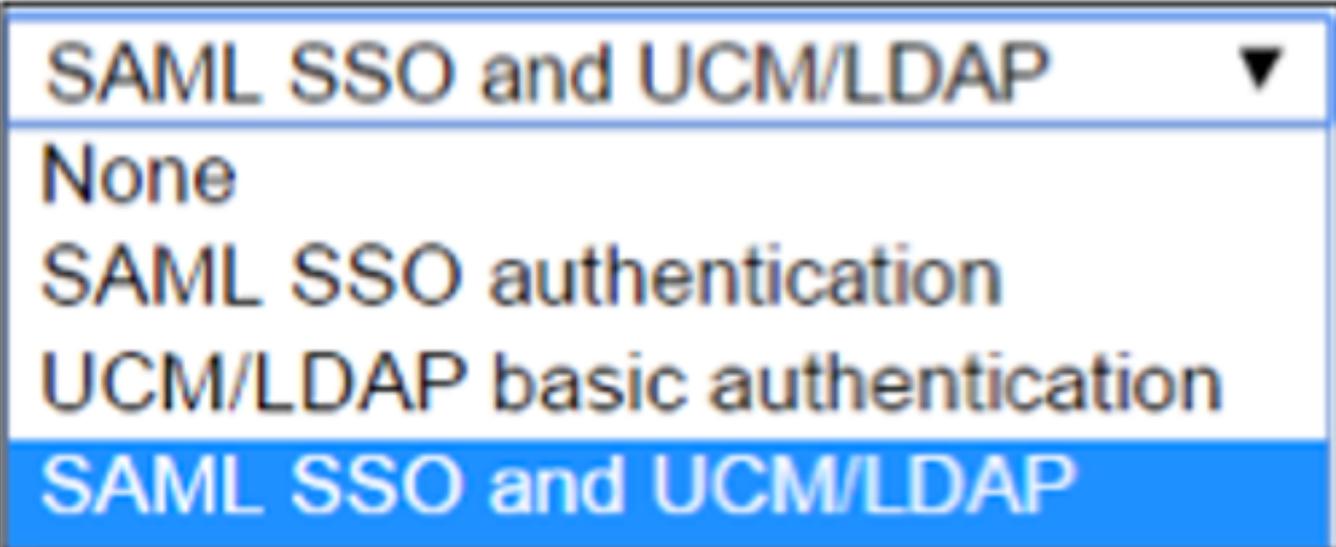
LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
SAM-Account-Name	uid
*	

لوخدلا ليجست شي دحت عم OAuth

قفتت ةملم عم مادختساب OAuth ني كمت نم ققحت، Cisco CUCM Enterprise تاملم عم ي نيوكت > ةسسؤملا تاملم عم > Cisco Unified CM ةرادل لىل لقتنا. شي دحتل لىل لوخدلا ليجست SSO و OAuth.

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

ةقداصملا راسم



- ءالمع ىوس نكمتي نلف ، "SAML SSO ةقداصم" ىلع ةقداصملا راسم نييعت مت اذا مراه م ادختسا نم SSO نيكمت مت يتلا ةدحوملا CM ةومجم نومدختسي نيذلا Jabber طوق SSO نيوكت اذه .عيرسلا قيرطلا اذه ىلع .
- TelePresence ماظنل ةياهنلا طاقن عيمجو IP فتاوه عيمجل MRA ExpressWay معد بلطتي ةقداصملا راسم SSO ل ةنوكملا ريغ ةدحوملا CM ةومجم ىلى ني ددحم Jabber ءالمع يا ةقداصملا UCM/LDAP ةقداصم ني مضتل .
- "SAML ةدحف ، Jabber SSO قيبطت معدت ةدحوملا CM تاعومجم نم رثكأ وأ ةدحاو تناك اذا ةقداصملاو ةساسلا ةقداصملا نم لكب حامسلا ل "UCM/LDAP و SSO .

ةسسو ةينب

نم ةددم ةومجم ىلى لوصول ني لوؤسملل حيتي XML ىلع مئاق تانايب قيسنت وه SAML تاقببطلل هذه دحا ىلى لوخدلا ليجست دعب ةسالسب Cisco نم نواعتل تاقببطلت جت نمل او لاجملا ربع يداح لوخد ليجست مي دقتل SAML 2.0 لوكوتورب SAML SSO مدختسي Cisco نم نواعتل لولحل .

يلحملا لوخدلا ليجست قفدت

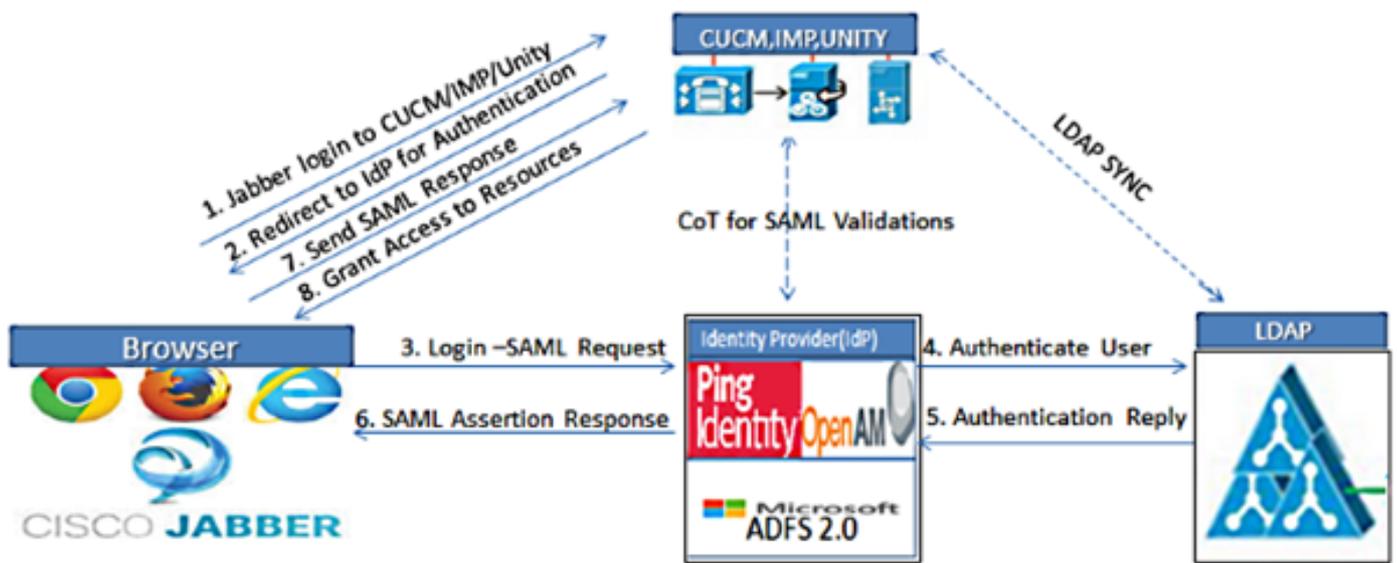
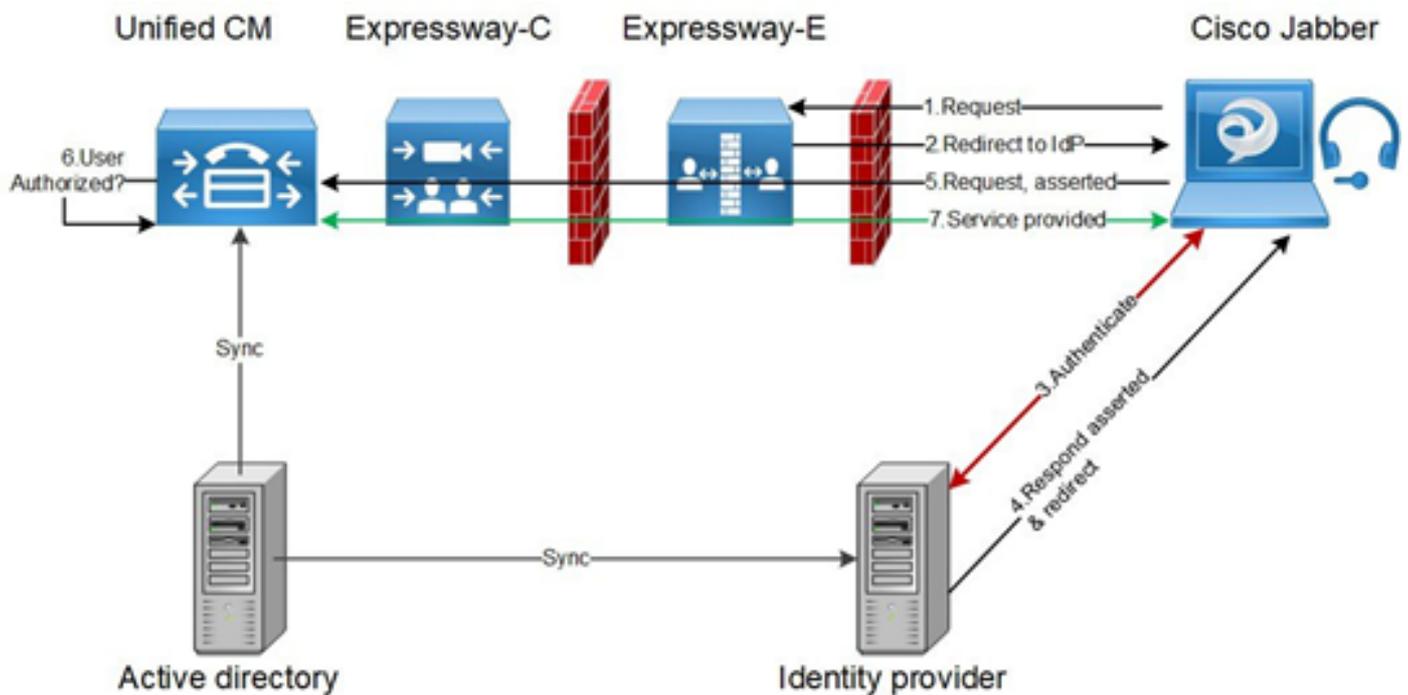


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

MRA إلى لوخدلا ليحست قفدت



ثوأ

زمرحنم قفدت رفوي .هليوخت لبق مدختسمل ا قداصم بجي .ليوختل م عدي رايعم وه OAuth إلى لوصولل ةزي ممل زومرلا شيدحتو لوصولل قح إلى لوصولل لقي م عملل قيرط ليوختل ا ةداغ إلى ااضيأ قفدتل اذه دن تساي .(Unified CM، IM&P، Unity و Expressway Services) ام دروم HTTP مدختسم ليوكتو عم لعافتل إلى لع ارداق ليوختل نوكتي نأ بلطتي يلاتلابلو هيحوتل ا مي دقتب ليوختل موقيس .مدختسمل ا ةطساوب هي ف مكحتل ا متي يذلا (بيولا ضرعتسم) إلى مدختسمل ا هيحوت ةداغاب OAuth مداغ موقاي .HTTPS مداغ تساب ليوختل ا مداغ إلى يلوأ بلط إلى بيو ةحفص ضرع مي دقت نوكتي ، ةمدختسمل ا ةقداصم ل قيرط بسح إلى لع . ةحفص ضرعي ال لاثم يه Kerberos ةقداصم) .هسفن إلى لع ةقداصم ل ليوختل ا ممدختسمل ا

مداوخ مايق ىل حجانلا ةقداصملا دوك حنم قفدت يدؤيس ،ينمضلا حنملا قفدت فالخ ب .) بي و رمعل ريصقو مادختسالا يداخ ديرف زمر اذه .بيولا ضرعتسمل "ليوختلا زمر" رادصاب OAuth مداخل اذه "ليوختلا زمر" ليمعلا رفوي .ليمعلا ىل بيولا ضرعتسم نم كلذ دعب هريرم متي شيوختلا زمر" و "زيمملا لوصولا زمر" لباقملا يف ملتسي و اقبس م كرتشم رس عم ليوختلا ىل مادختسالا ديوخت ليوختلا ةمدخل ووطخلا هذه يف مدختسمل ليمعلا رس حيتي . "زيمملا ةيلاتلا ضارغالل ةزيمملا تامالعل مادختسا متي . طقف ني قداصملا او نيلجسمل اعالمل

زيمملا شيوختلا/لوصولا زمر

ليمعلا مدقي .ليوختلا مداخ ةطساوب زيمملا زمرلا اذه رادصاب متي :لوصولل زيمملا زمرلا مداخل كلذ ىل ةيمملا دراوملا ىل لوصولا ىل جاتحي امدنع دراوملا مداخل زيمملا زمرلا .زيمملا زمرلا مادختساب تالاصتاب قثي و زيمملا زمرلا ءحص نم ققحتلا دراوملا مداخل نكمي .(ةقيقد 60 غلبت ةايح ةرتفل ةيضارتفالا هي Cisco نم لوصولل ةزيمملا زومرلا)

مدقي .ليوختلا مداخ ةطساوب ىرخأ ةرم زيمملا زمرلا اذه رادصاب مت :شيوختلل زيمملا زمرلا زيمملا زمرلا ةيخالص ءهتنا دنع ليمعلا رس عم ليوختلا مداخ ىل زيمملا زمرلا اذه ليمعلا مداخ ردصي سف ،خالص لازي ال شيوختلل زيمملا زمرلا ناك اذا .هتيخالص ءهتنا و لوصولل ةزيمملا شيوختلا زومر نوكت . ىرخأ ةقداصم ىل ةجالل نود لوصولل ديوج زيمملا زمر ليوختلا ،شيوختلل زيمملا زمرلا ةيخالص تهتنا اذا .(اموي 60 غلبت ةايح ةرتفل ةيضارتفا Cisco نم ةديج ةزيمملا زومر ىل لوصولل ديوج لىمك OAuth ليوخت زمر حنم قفدت ادب بجي ف

لضفأ OAuth ليوخت دوك حنم قفدت

ليكو ربع Jabber ليمع ىل لوصولل زيمملا زمرلا ريرم متي ،ينمضلا ءحنملا قفدت يف زيمملا لوصولا زمر لدابت متي ،ليوختلا دوك حنم قفدت يف .(ضرعتسمل) HTTP مدختسم ليوختلا مداخ نم زيمملا زمرلا بلط متي .Jabber ليمعو ليوختلا مداخ ني ب ءرشابم لوصولل زيمملا زمرلل رشابملا لدابتلا اذه نوكتي و .اي نمز ددحم ديرف ليوخت زمر مادختساب رطاخملل ضرعتلا للقي و انام ارتكأ .

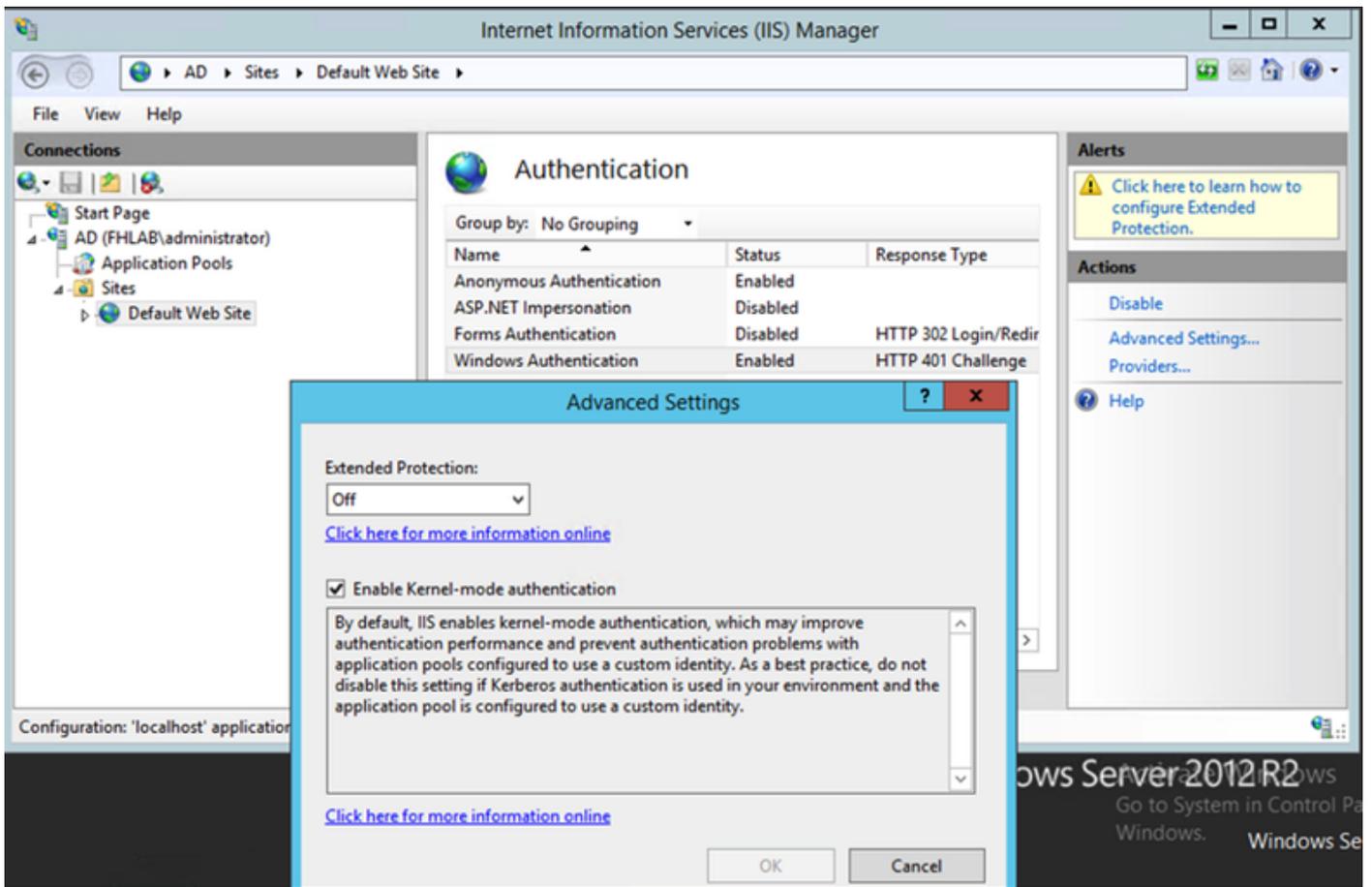
رمال اذه رفوي .ةزيمملا شيوختلا زومر مادختسا OAuth ليوخت زمر ءحنم قفدت معددي رركتم لكشب ةقداصملا ءداع ىل جاتحي ال هنا شيح لصفأ ءبرجت يئاهنلا مدختسمل لل .(اموي 60 يضارتفا لكشب)

Kerberos نيوكت

Windows ةقداصم ديوخت

> ةقداصملا > يضارتفالا بيولا عقوم > عقاوملا > (IIS) تترنتنالا تامولعم تامدخ ءرادا > ءمدقمت تاداع | > Windows ةقداصم

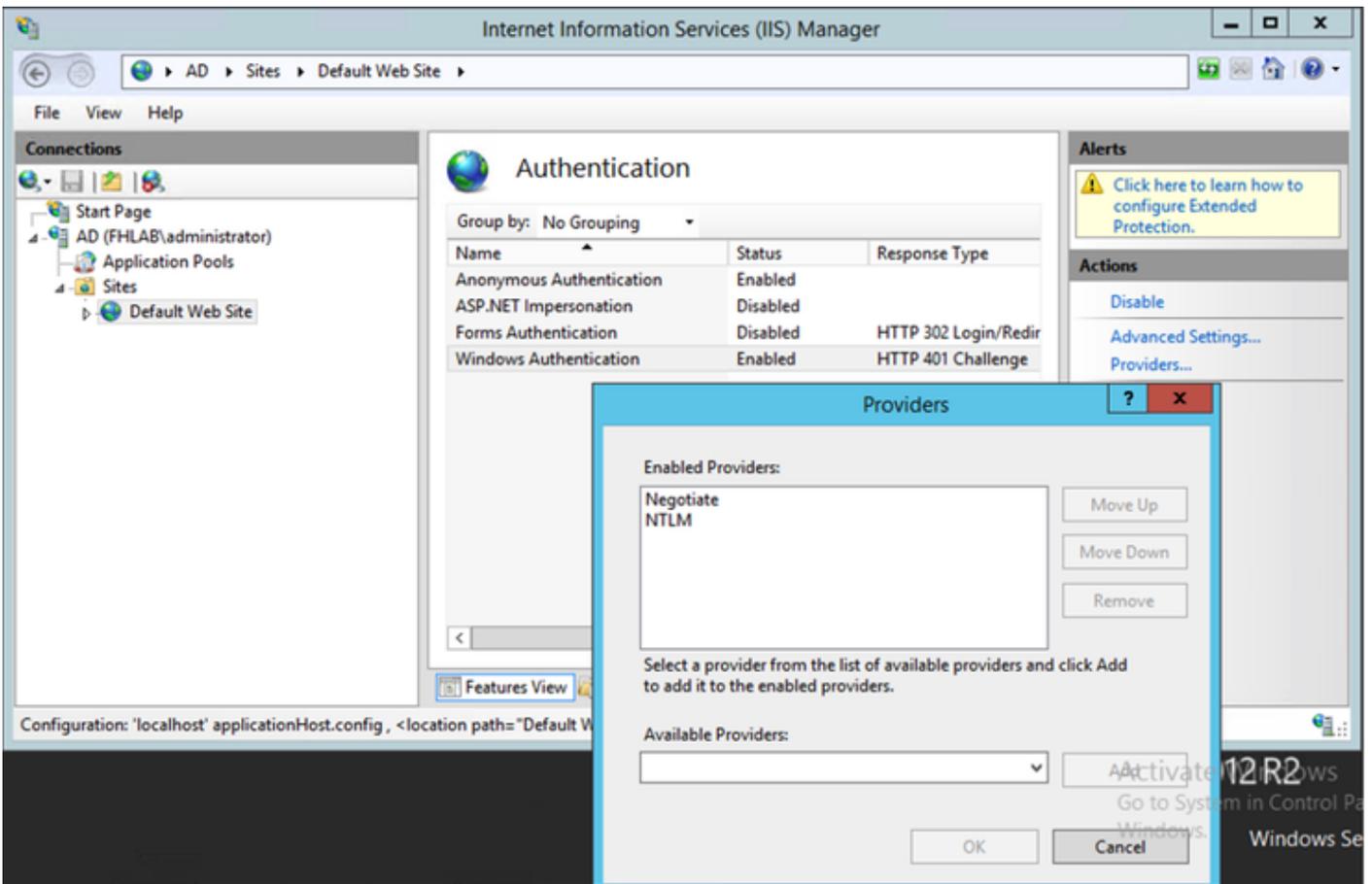
1. kernel عضو ةقداصم نيكمت ديوخت ءاغلل مق .
2. ءسسوملا ءياملل ليغشت فاقيا نم دكأت .



معدت Kerberos NTLM نم الك ADFS مع دت

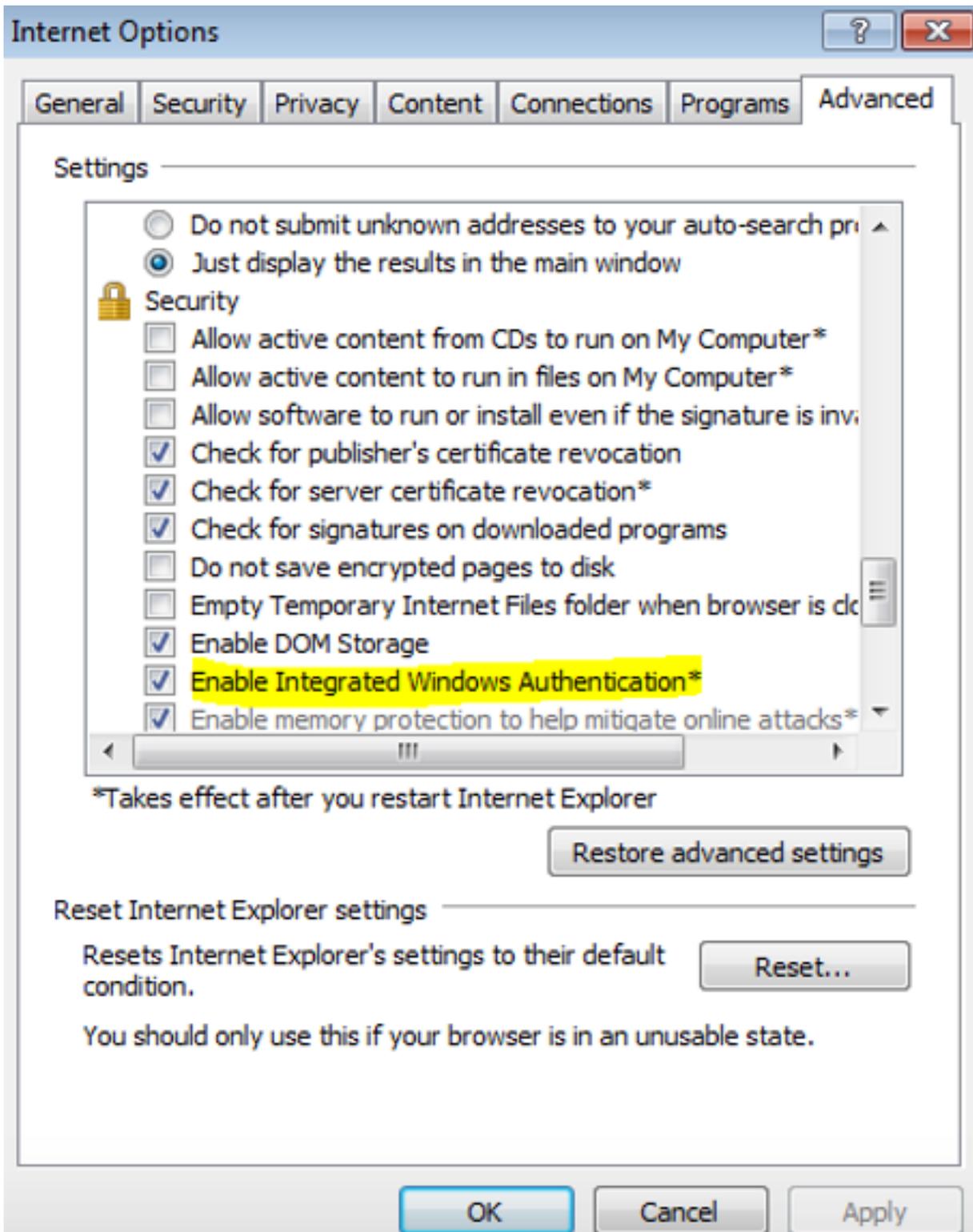
LAN ةكبش ري دم لوكوتورب و Kerberos لوكوتورب نم الك مع دت 3.0 رادصل ال AD FS نأ نم دكأت لى لع دامت عال او Kerberos مادختسا مه نكمي ال Windows فالخب عال مع ال عي مج نأل NTLM (NTLM).

م نى ذل نى رومل نم ض NTLM و Negotiate دوجو نم دكأت و نى رومل دح ، نى أال اعزل لى ف مهنى كمت:



Microsoft Internet Explorer نيوكت

Windows. لة لم اکت المة قد اصم المة نيوکتم > مدقتم > Internet Explorer نم ققحت المة نم دکأت



عق اوملا > ت نارتنل ق طانم > نيمأتلا تحت ADFS URL ناو نع ة فاضلا

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء نأ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل ة مچرت ل ض ف أن ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ئ ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن إ ل ا دن تسمل ا