

在帶有ADFS 3.0的Cisco Unified Communications Manager上配置SAML SSO

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[組態預先檢查](#)

[A記錄](#)

[指標\(PTR\)記錄](#)

[需要為Jabber Discovery Services保留SRV記錄](#)

[ADFS3初始配置](#)

[使用ADFS在CUCM上配置SSO](#)

[LDAP配置](#)

[CUCM後設資料](#)

[配置ADFS信賴方](#)

[IDP後設資料](#)

[在CUC上配置SSO](#)

[CUC後設資料](#)

[在Expressway上配置SSO](#)

[將後設資料匯入到Expressway C](#)

[從Expressway C匯出後設資料](#)

[為Cisco Expressway-E新增信賴方信任](#)

[使用刷新登入的OAuth](#)

[驗證路徑](#)

[SSO架構](#)

[本地登入流程](#)

[MRA登入流](#)

[OAuth](#)

[存取/刷新權杖](#)

[OAuth授權代碼授權流程更好](#)

[配置Kerberos](#)

[選擇Windows身份驗證](#)

[ADFS同時支援Kerberos NTLM](#)

[配置Microsoft Internet Explorer](#)

[在Security > Intranet zones > Sites下新增ADFS URL](#)

[將CUCM、IMP和Unity主機名新增到Security > Trusted Sites](#)

[使用者驗證](#)

[SSO中的Jabber登入](#)

[疑難排解](#)

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

[站點新增到IE](#)

[不同步問題](#)

[撤銷令牌](#)

[載入程式檔案](#)

[由於MSIS7066而導致SSO失敗](#)

簡介

本文檔介紹在Cisco Unified Communication Manage(CUCM)、Cisco Unity Connection(CUC)和Expressway產品上使用Windows 2012 R2使用Active Directory聯合身份驗證服務(ADFS 3.0)配置單一登入的步驟。本文還包括配置Kerberos的步驟。

必要條件

需求

思科建議您瞭解一次登入(SSO)和Windows產品。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CUCM 11.5
- CUC 11.5
- Expressway 12
- 具有以下角色的Windows 2012 R2 Server:
 - Active Directory證書服務
 - Active Directory聯合身份驗證服務

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

組態預先檢查

安裝ADFS3之前，環境中需要已經存在這些伺服器角色：

·域控制器和DNS

·所有伺服器必須作為A記錄與其指標記錄（將IP地址解析為域或主機名的一種DNS記錄）一起新增

A記錄

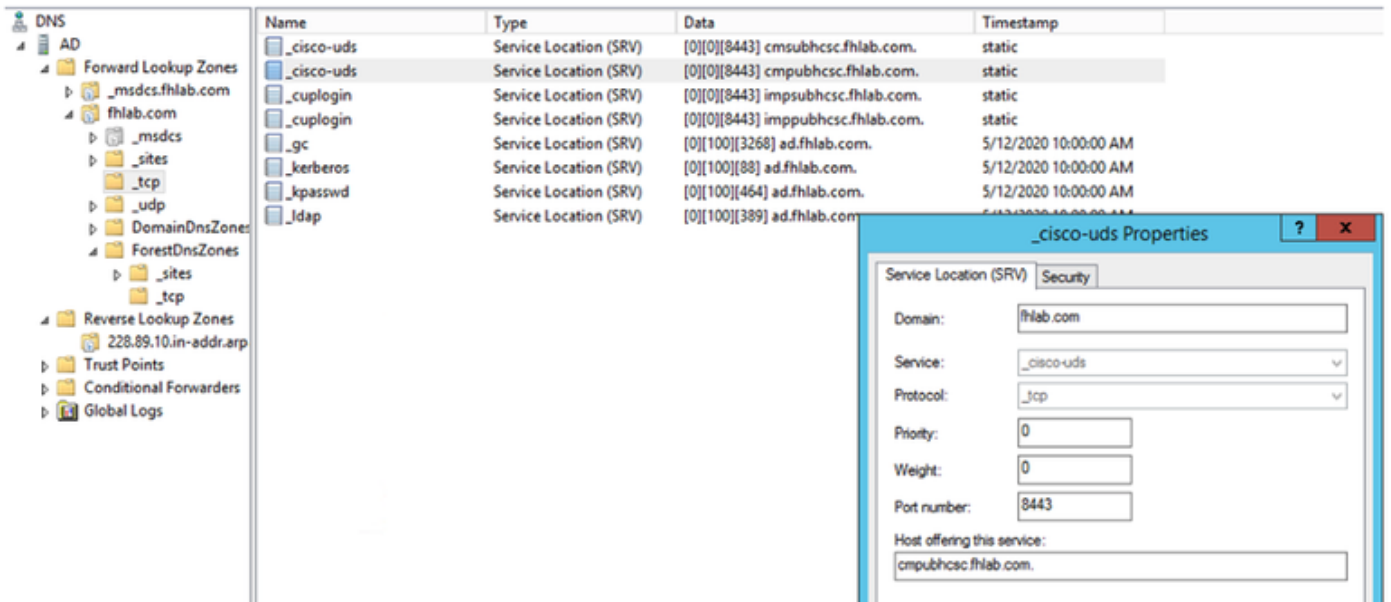
在fhlab.com。已新增主機cmpubhcsc、cmsubhcsc、cucpubhcsc、cucsubhcsc、expwyc、expwye、impubhcsc和imsubhcsc。

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)

指標(PTR)記錄

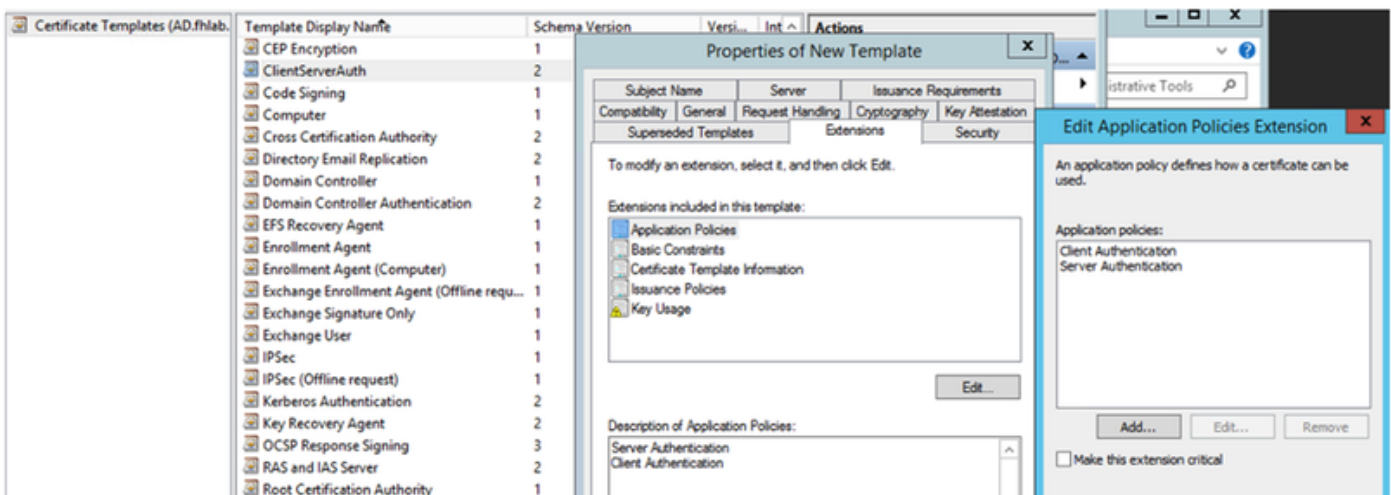
Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[14], ad.fhlab.com, hostmaster.fhlab.co...	static
(same as parent folder)	Name Server (NS)	ad.fhlab.com.	static
10.89.228.144	Pointer (PTR)	expwyc.fhlab.com.	static
10.89.228.145	Pointer (PTR)	expwye.fhlab.com.	static
10.89.228.146	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

需要為Jabber Discovery Services保留SRV記錄

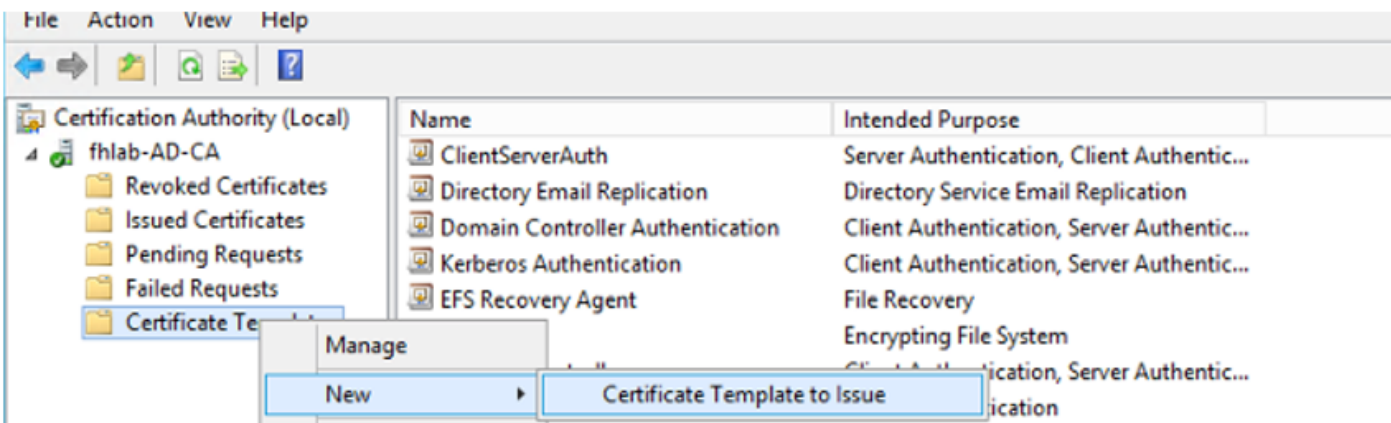


- 根CA (假設證書由企業CA簽署)

需要基於Web伺服器證書模板建立證書模板，複製證書模板，重新命名證書模板，並在「擴展」頁籤上修改應用程式策略，新增客戶端身份驗證應用程式策略。在實驗室環境中簽署所有內部證書 (CUCM、CUC、IMP和Expressway核心) 時需要使用此模板。內部CA還可以簽署Expressway E證書簽名請求(CSR)。



需要頒發建立的模板才能簽署CSR。



在CA證書Web上，選擇以前建立的模板。

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:

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

```
8V8mWY/9kjhgfnpeBzAAW++to1GzBjnvqaT8StWM  
LA0dphF6LrurUeY2KLvMLmK1ft7aSy483yCsm0v1  
OWQFzoLb3bS80ziW7fQEFWSaCg567DMOQ8FkZt5N  
10y/Ip6oDzTdZE9w2p8rK3YxcbygovStOijIirh  
AM/GjnzQ  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Additional Attributes:

Attributes:

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

CUCM、IMP和CUC多伺服器CSR必須生成並由CA簽名。證書用途必須為tomcat。

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

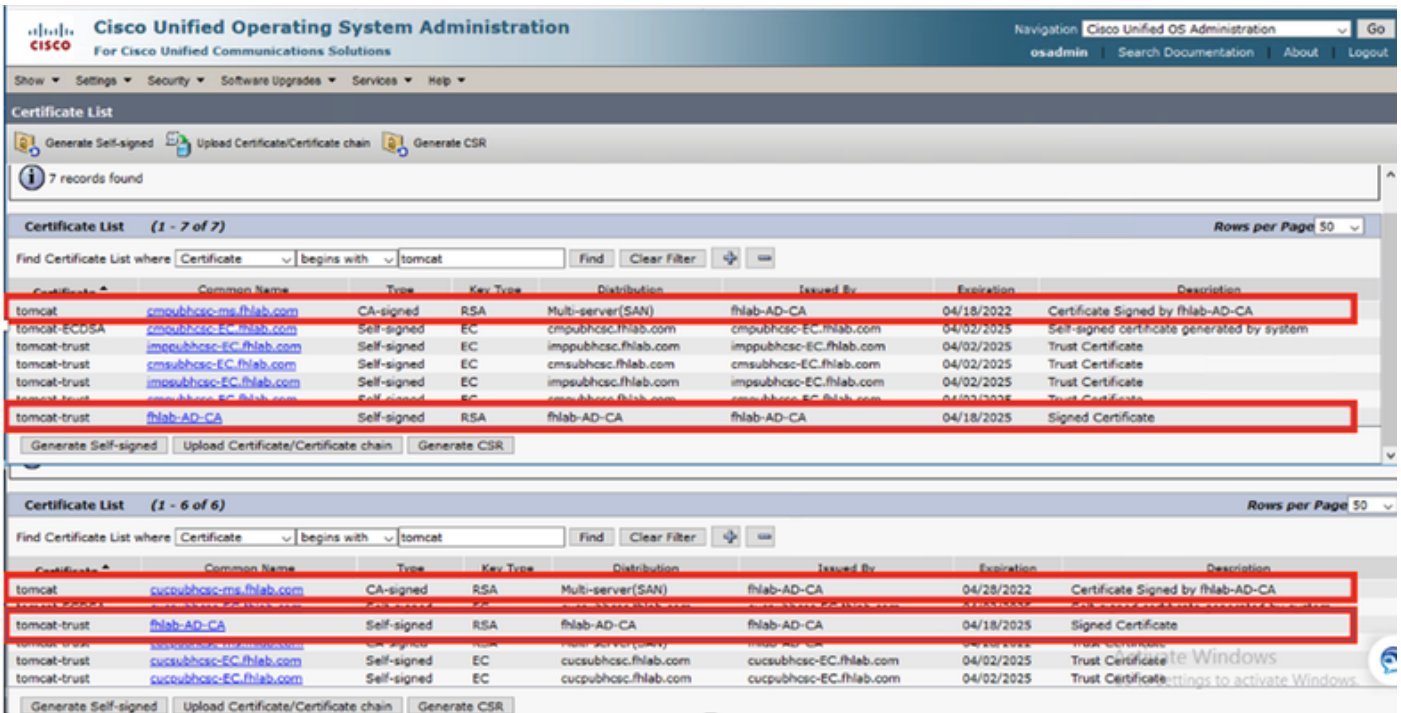
Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

Generate Close

必須將CA根證書上傳到Tomcat信任，並將簽名證書上傳到tomcat。



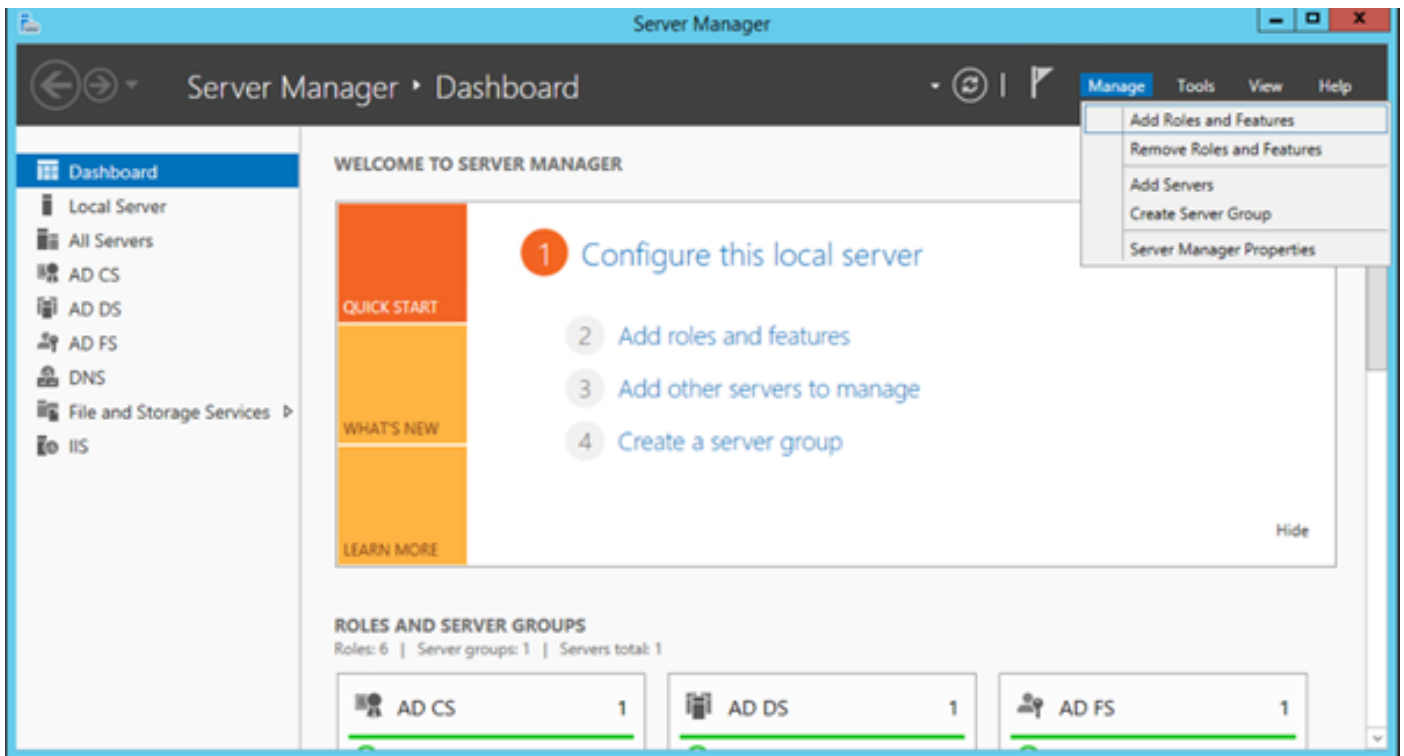
- IIS

如果沒有，本節將介紹這些角色的安裝。否則，請跳過此部分，直接從Microsoft下載ADFS3。

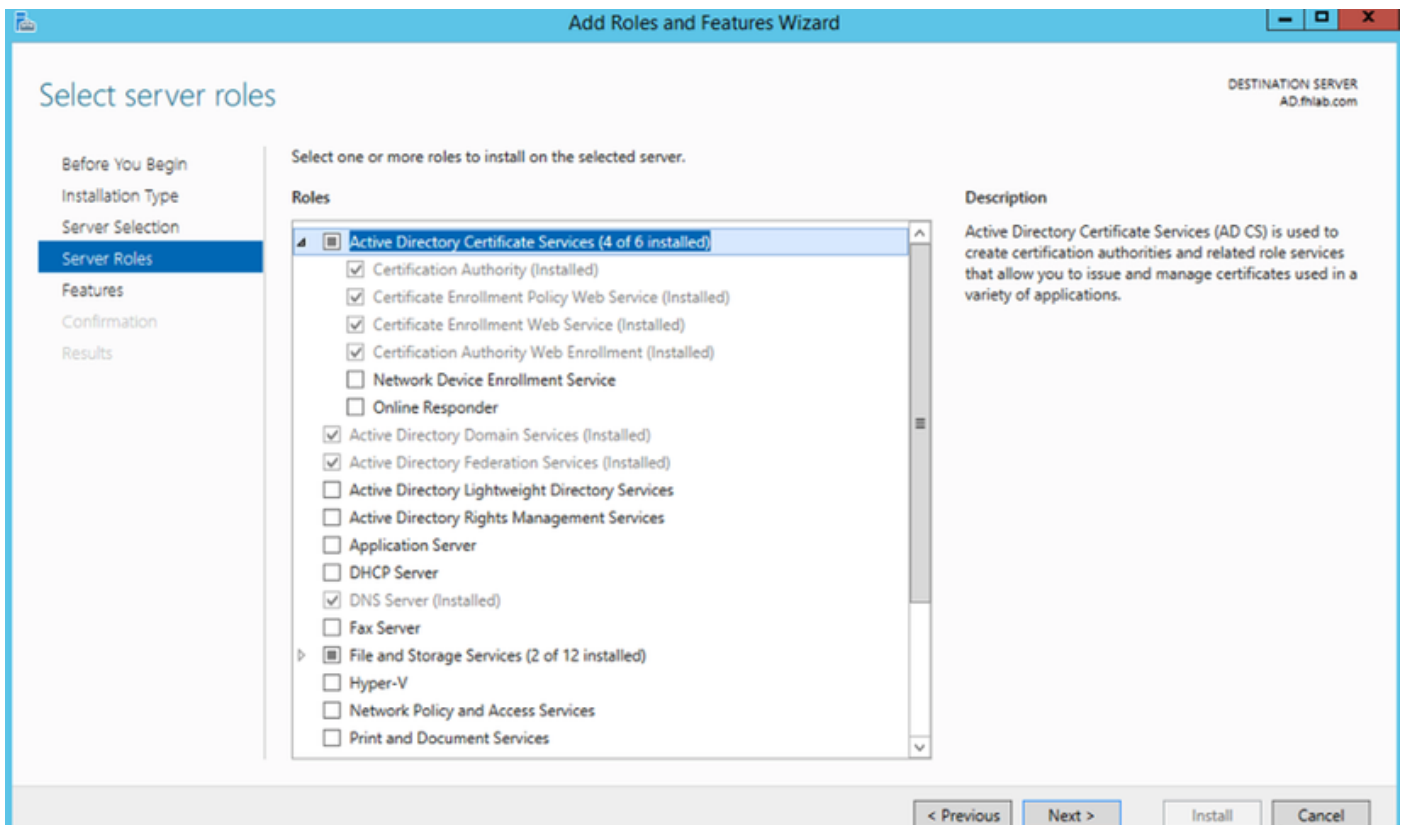
安裝帶有DNS的Windows 2012 R2後，將伺服器升級為域控制器。

下一個任務是安裝Microsoft證書服務。

導航到伺服器管理器並新增新角色：



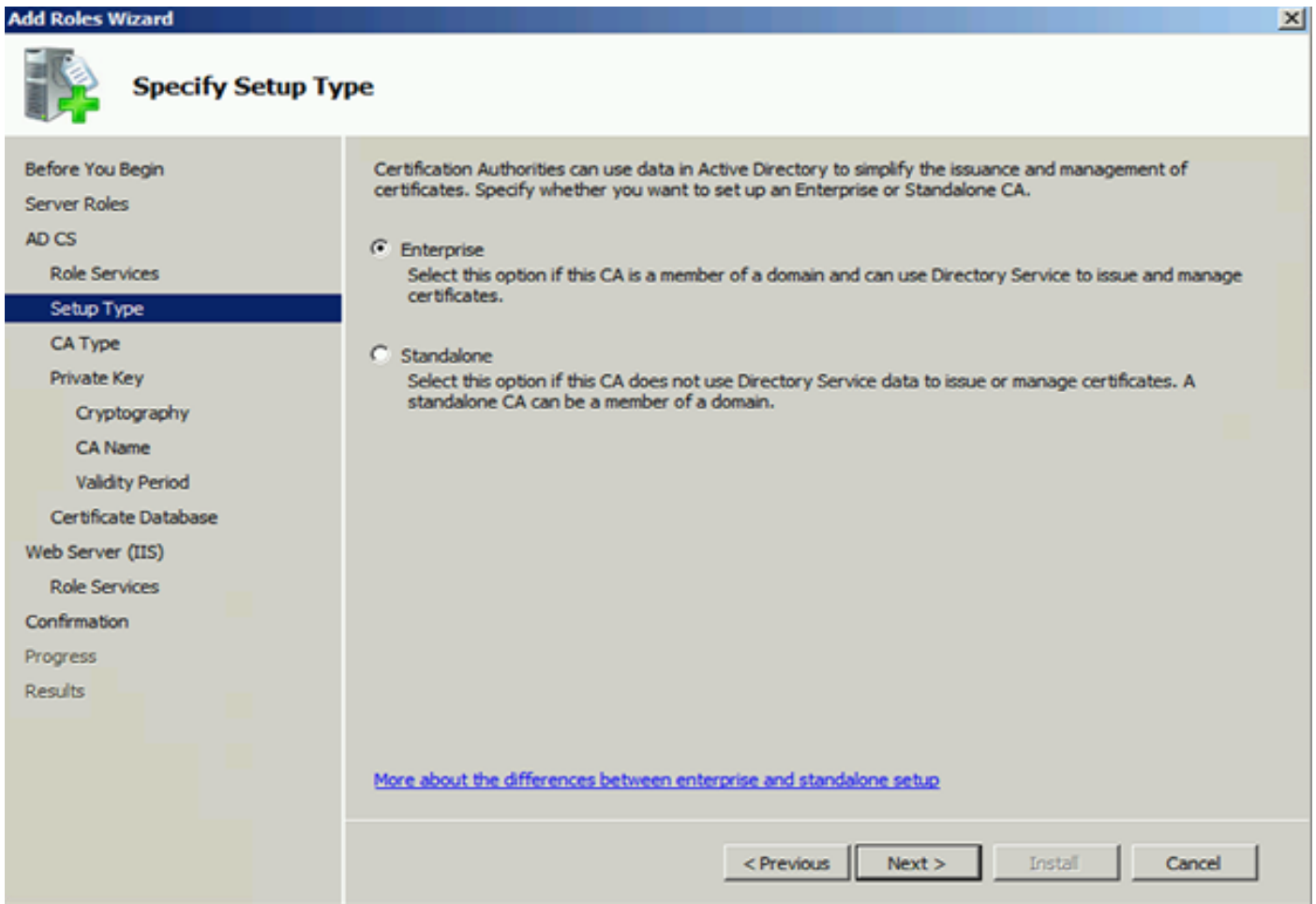
選擇Active Directory證書服務角色。



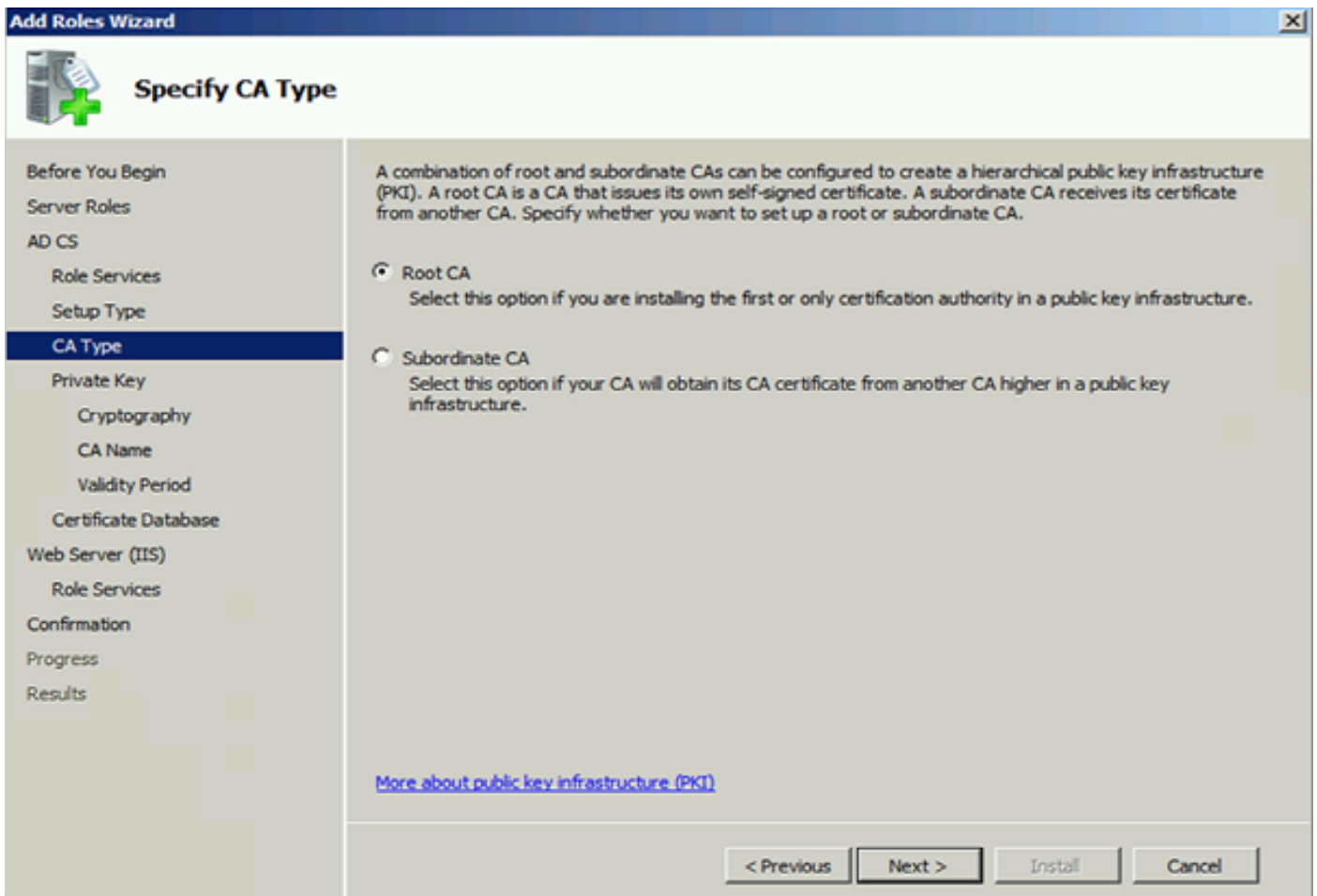
並首先部署這些服務 — 證書頒發機構證書註冊策略Web服務。安裝這兩個角色後，請對其進行配置，然後安裝證書註冊Web服務和證書頒發機構Web註冊。配置它們。

安裝證書頒發機構後，還會新增所需的其它角色服務和功能，例如IIS。

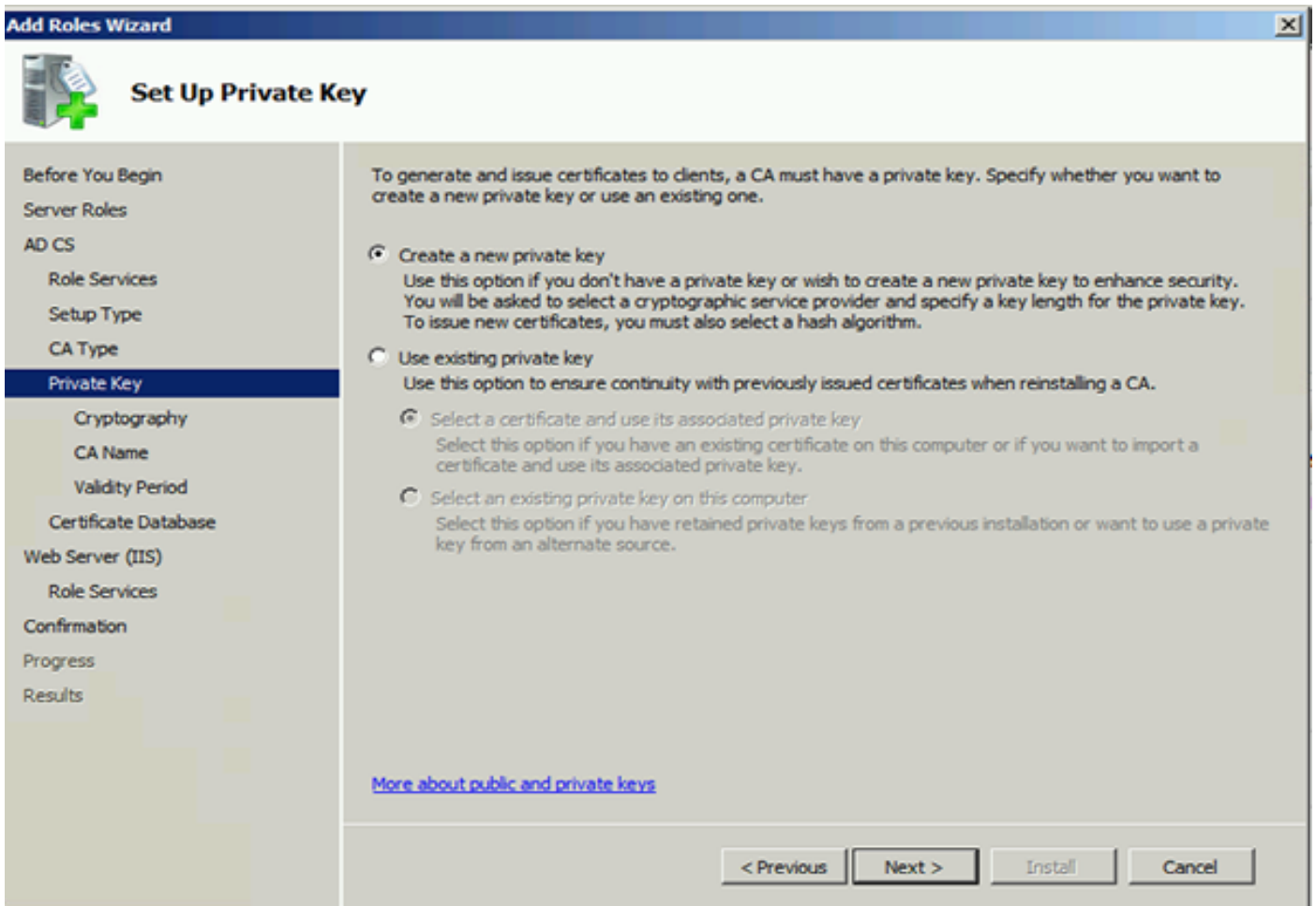
根據您的部署，您可以選擇企業或獨立。



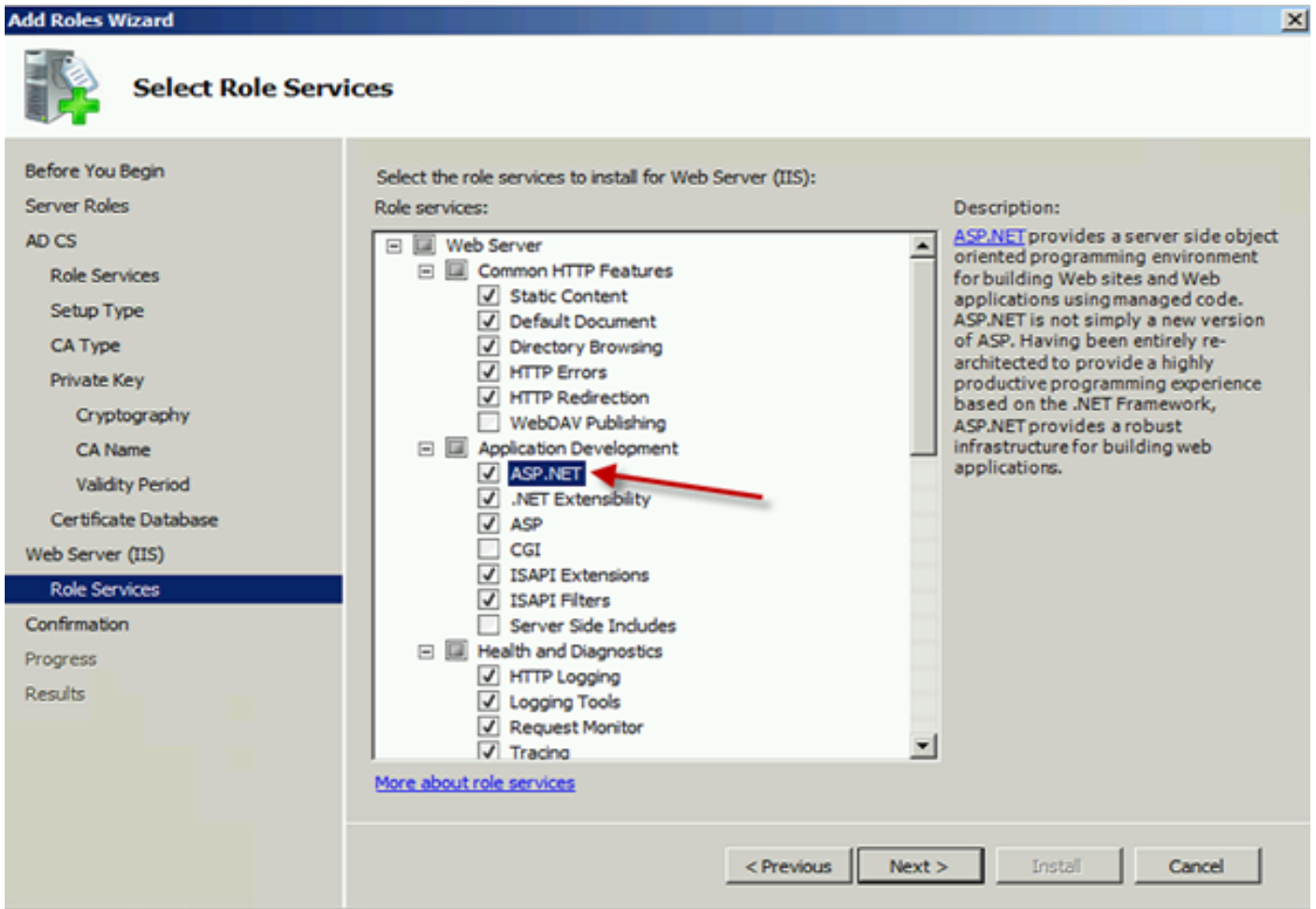
對於CA型別，您可以選擇根CA或從屬CA。如果組織中沒有其他CA正在運行，請選擇根CA。



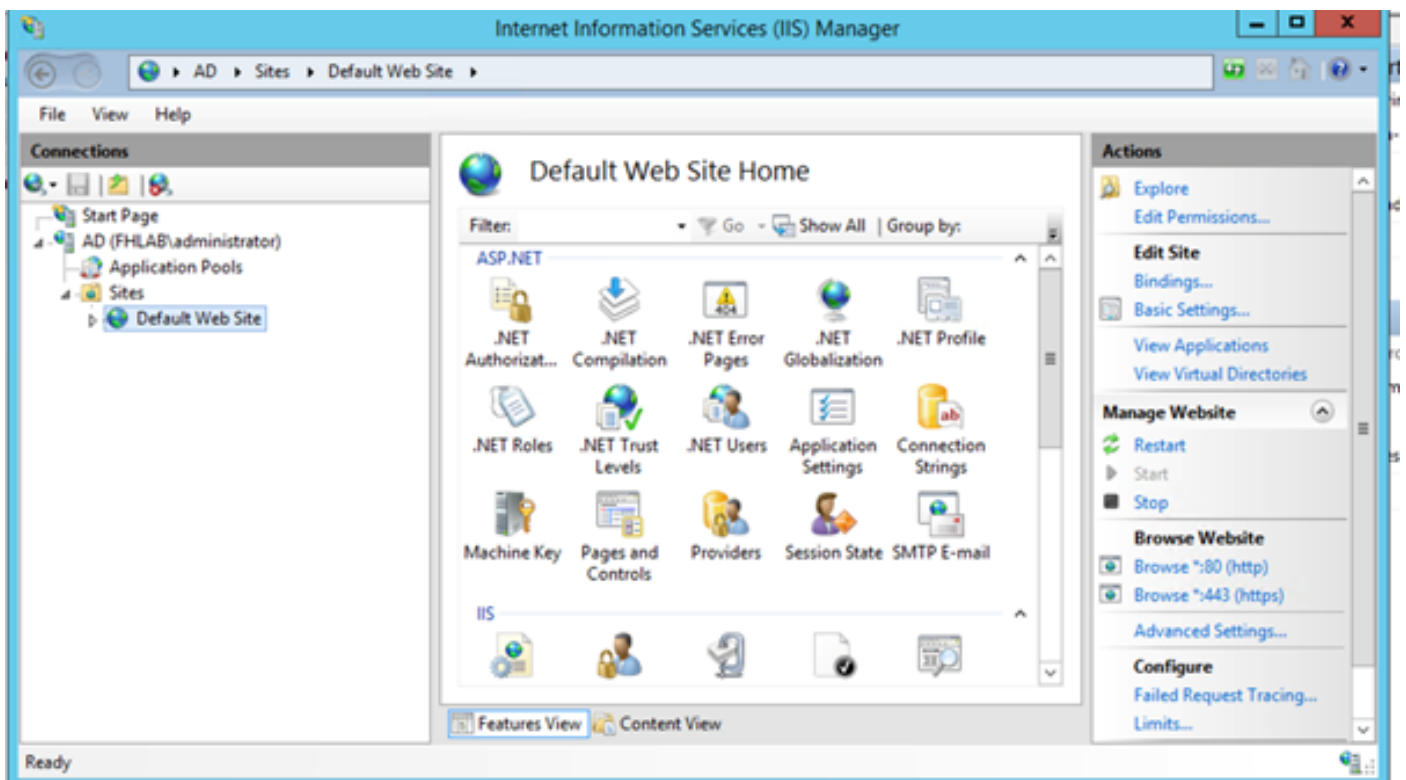
下一步是為您的CA建立私鑰。



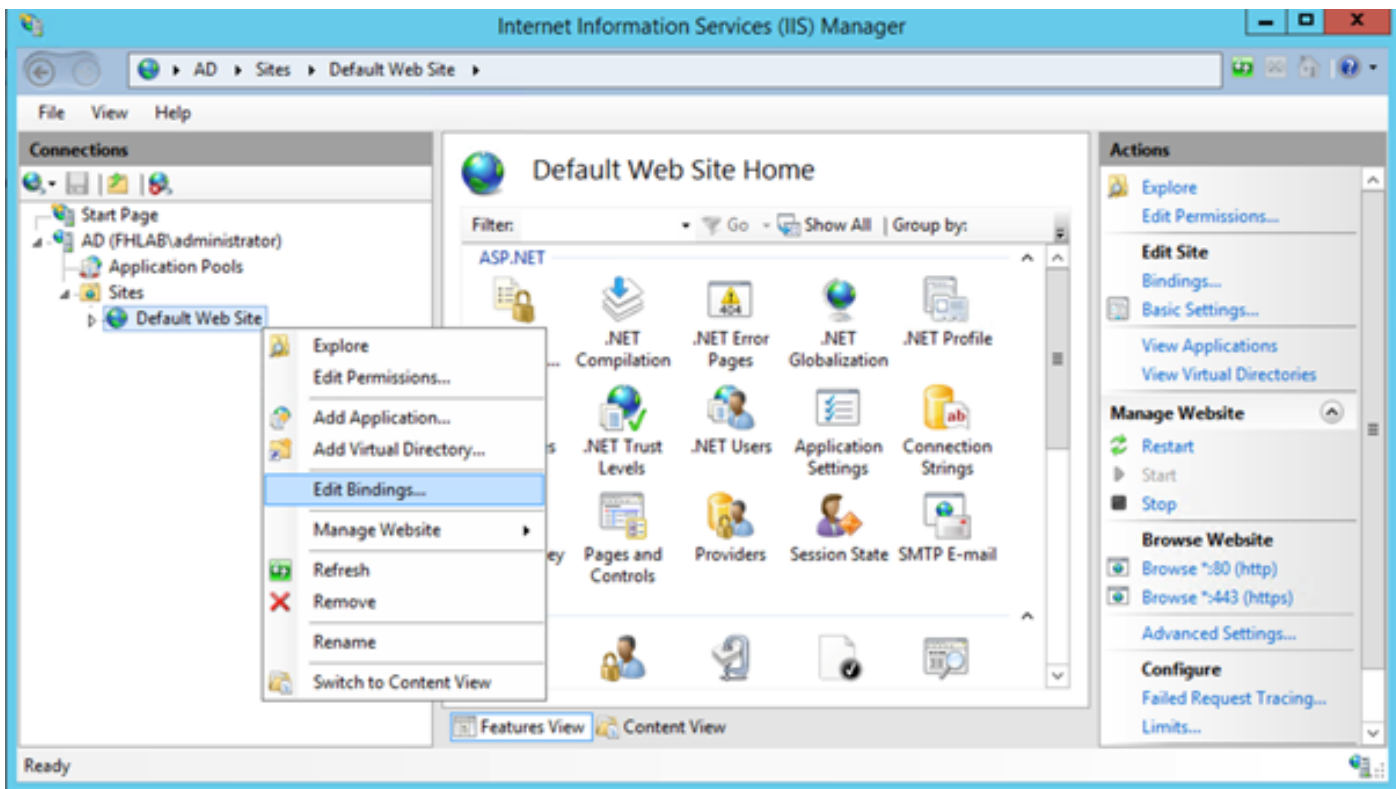
只有在單獨的Windows Server 2012上安裝ADFS3時，才需要執行此步驟。配置CA後，需要配置IIS的角色服務。這是在CA上進行Web註冊所必需的。對於大多數ADFS部署，在IIS中需要額外的角色，請按一下「應用程式開發」下的**ASP.NET**。



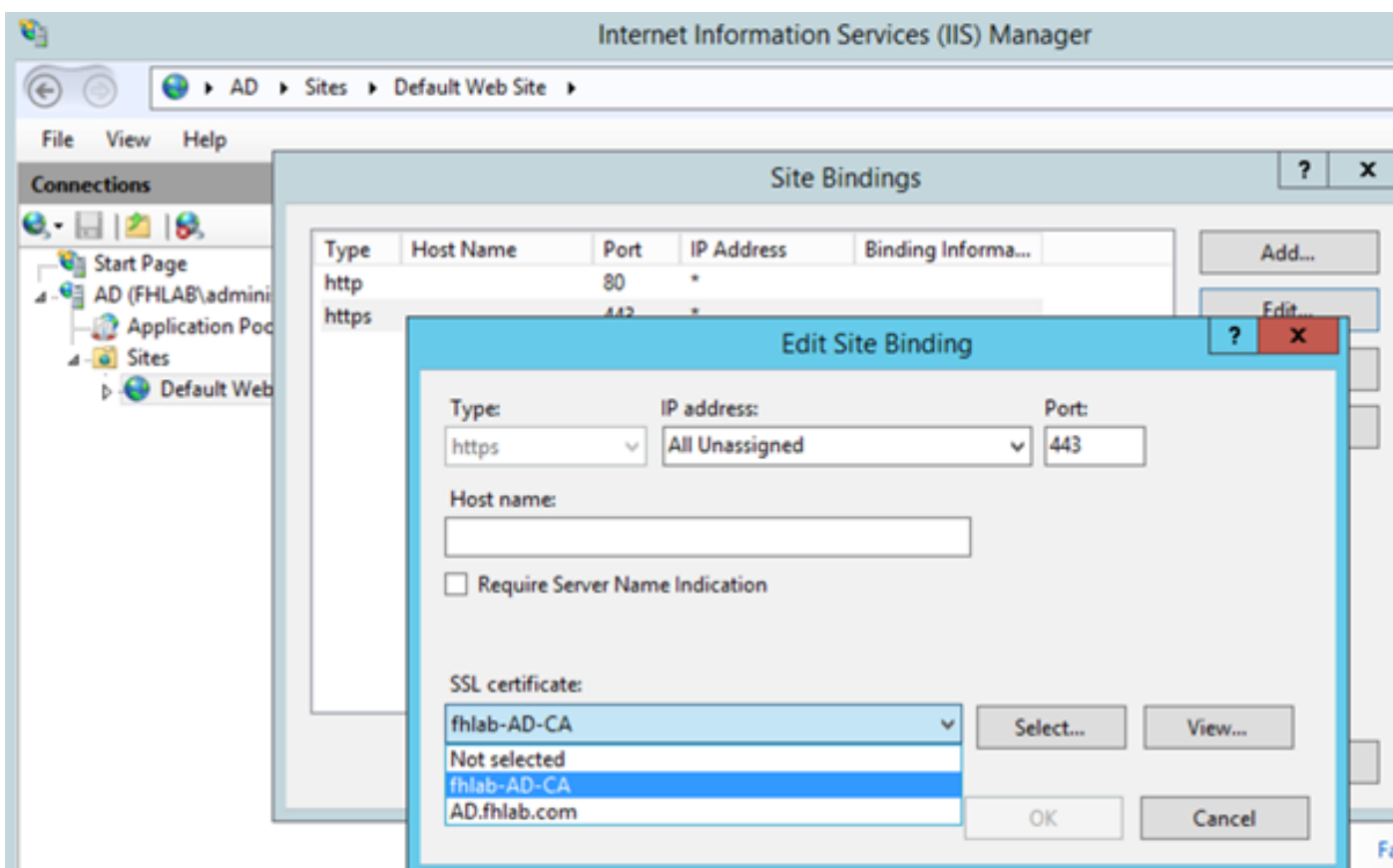
在伺服器管理器中，按一下**Web Server > IIS**，然後按一下右鍵**Default Web Site**。除了HTTP外，還需要更改繫結以允許HTTPS。這麼做是為了支援HTTPS。



選擇**編輯繫結**。

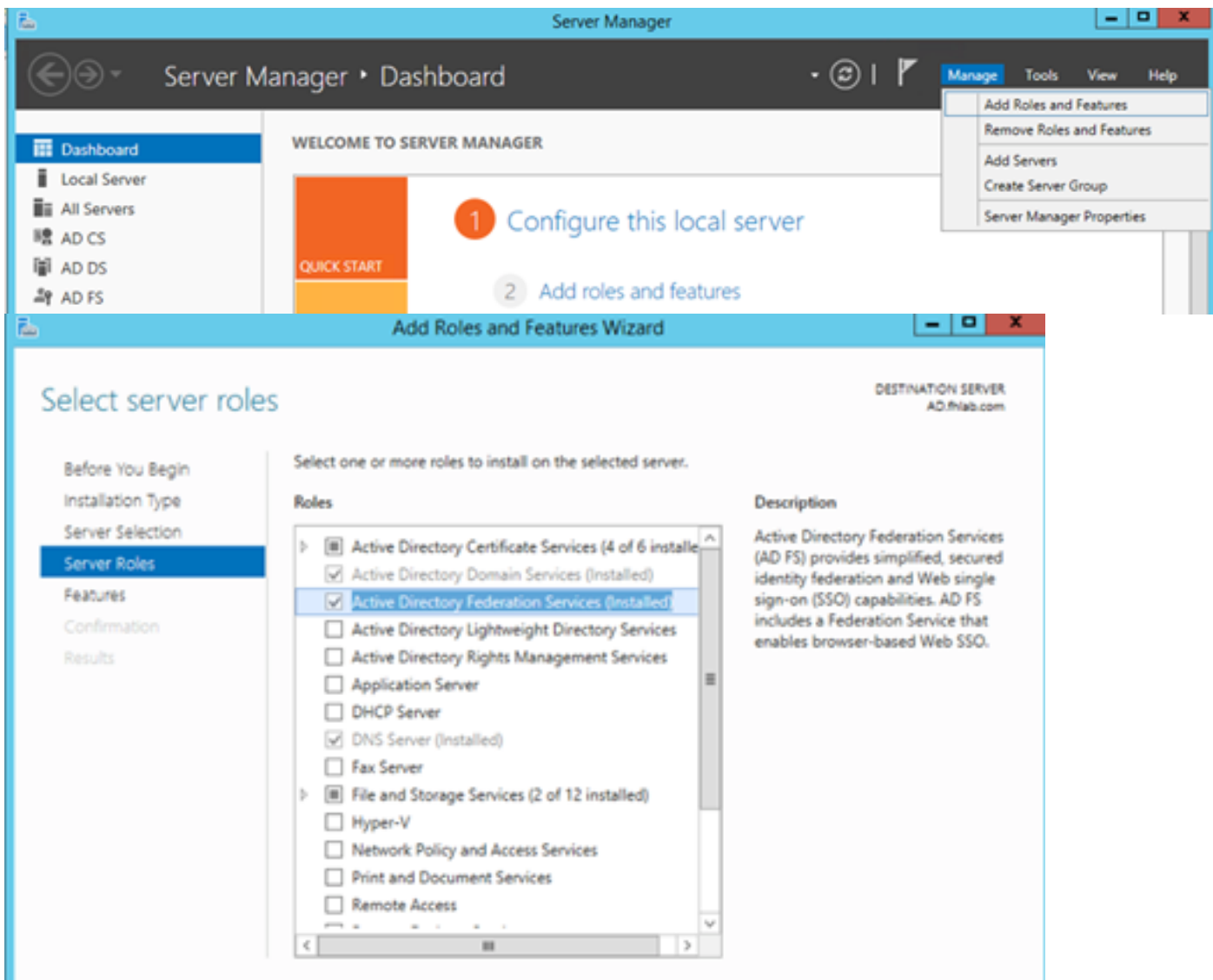


新增新的站點繫結並選擇HTTPS作為型別。對於SSL證書，選擇應與AD伺服器具有相同FQDN的伺服器證書。

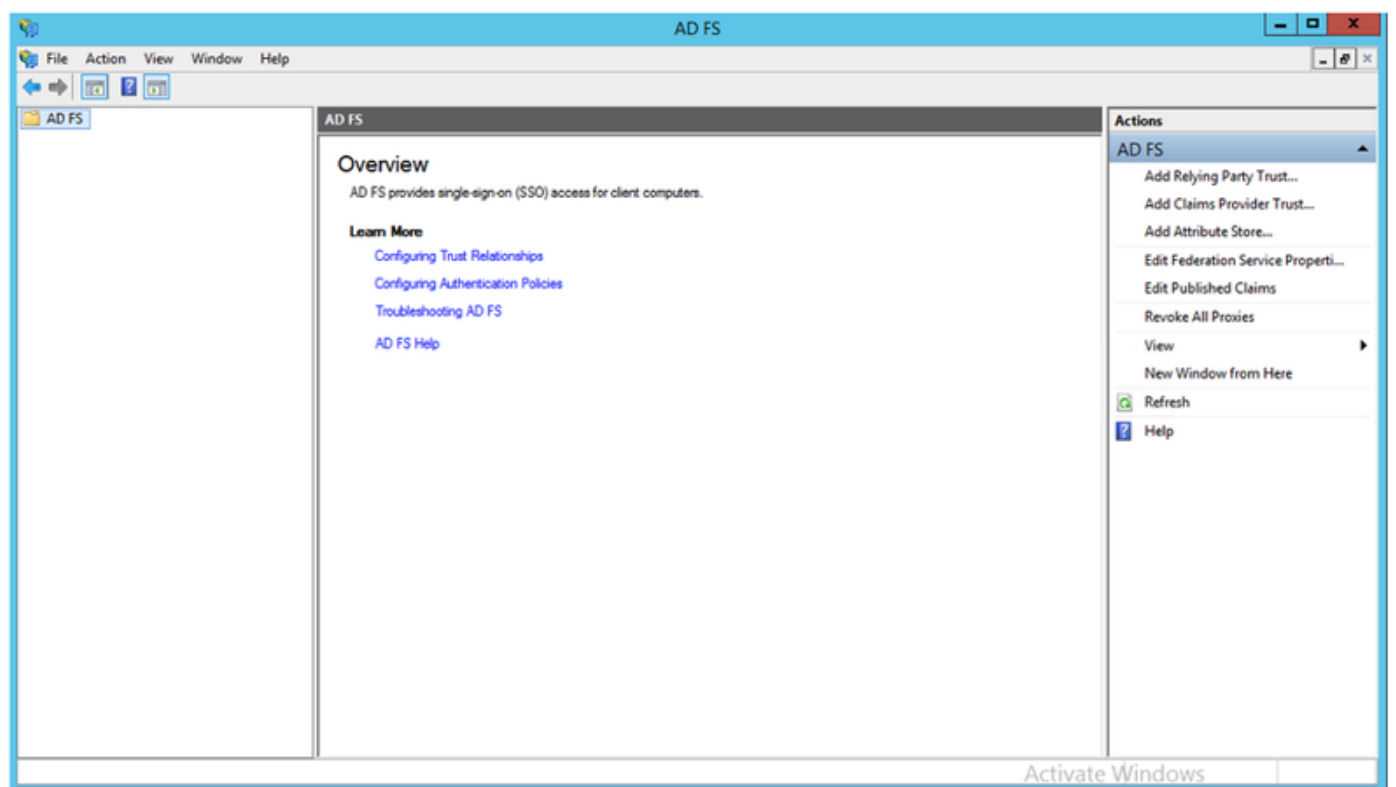


所有必備角色都安裝在環境中，因此現在您可以繼續安裝ADFS3 Active Directory聯合身份驗證服務（在Windows Server 2012上）。

對於伺服器角色，導航到**Server Manager > Manage > Add Server Roles and Features**，然後在專用LAN上在客戶網路中安裝IDP時選擇**Active Directory Federation Services**。



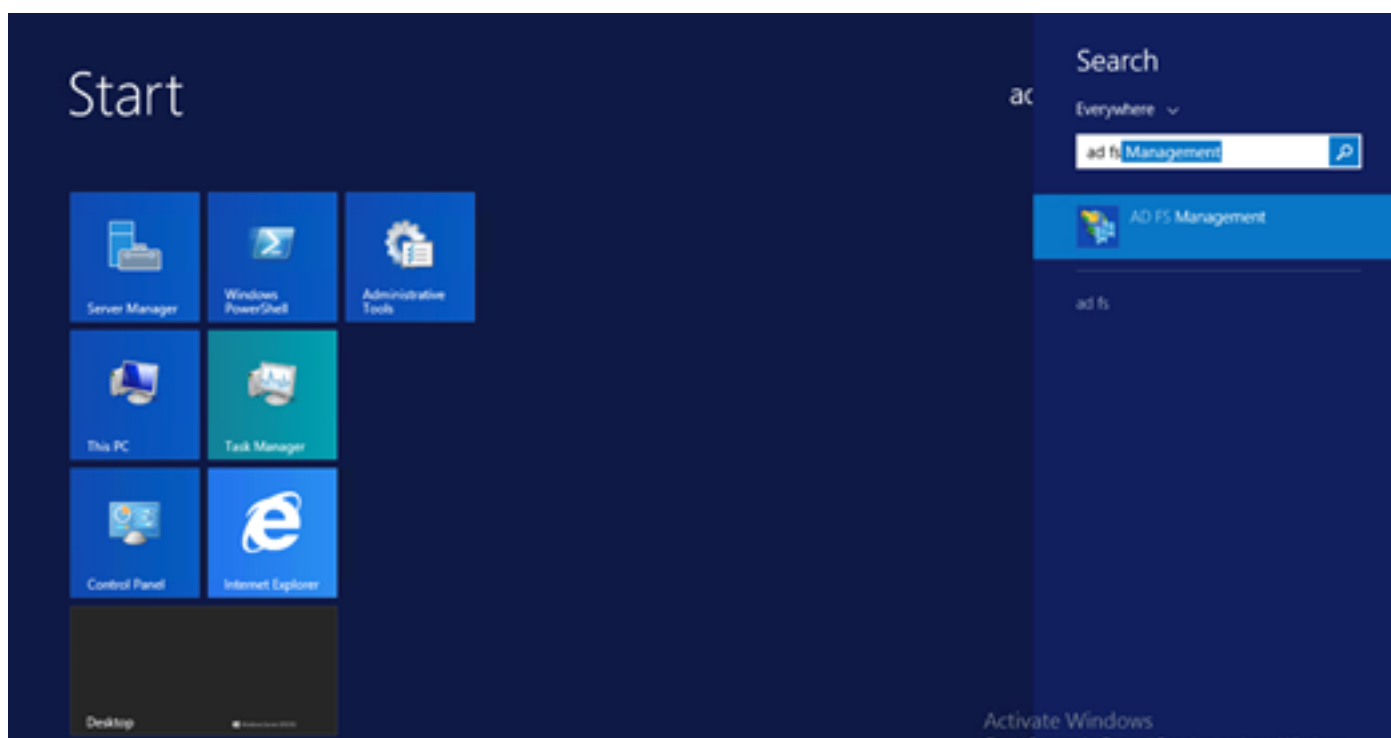
安裝完成後，您可以從工作列或「開始」選單開啟它。



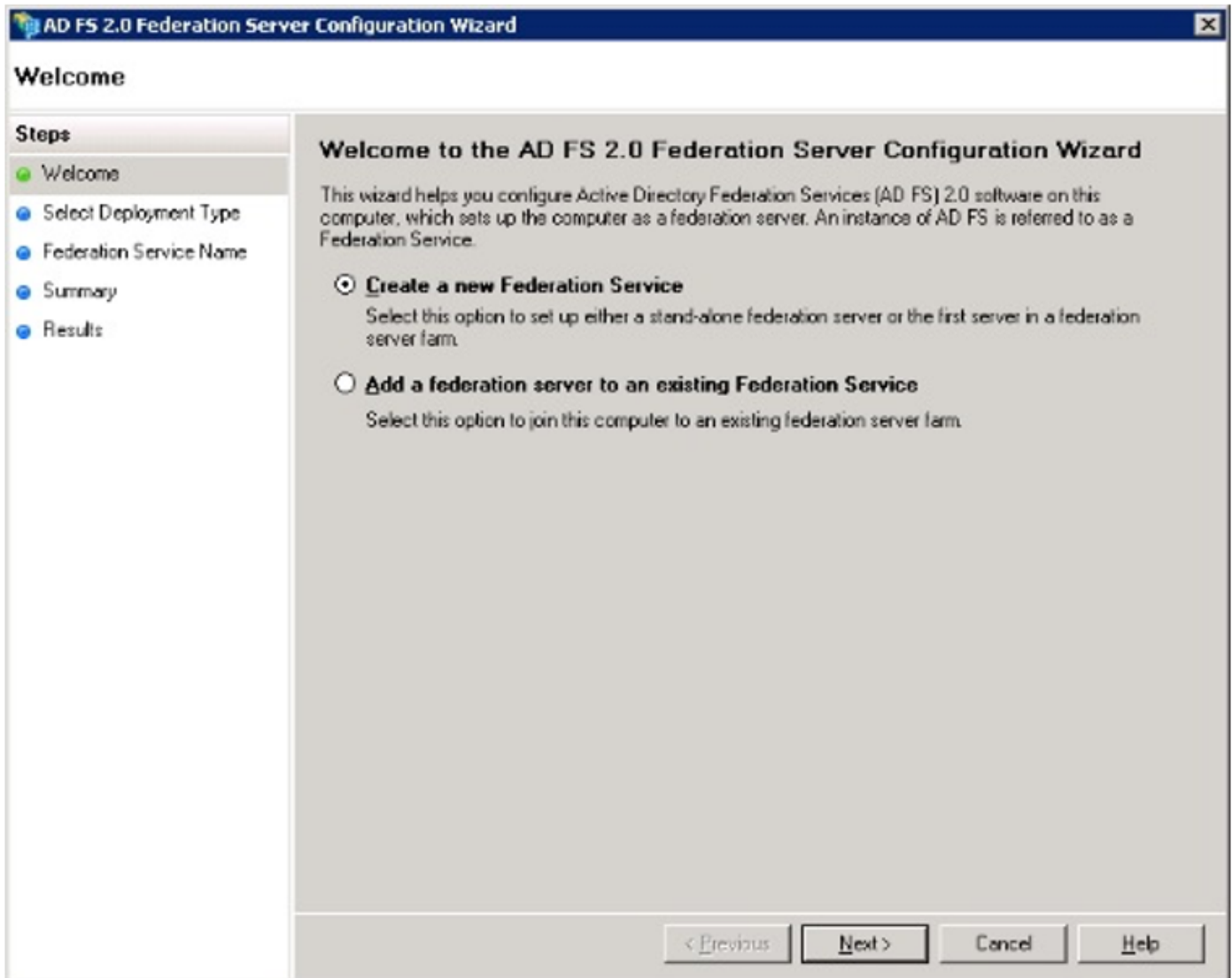
ADFS3初始配置

本節將介紹如何安裝新的獨立聯合伺服器，但也可以將其安裝在域控制器上

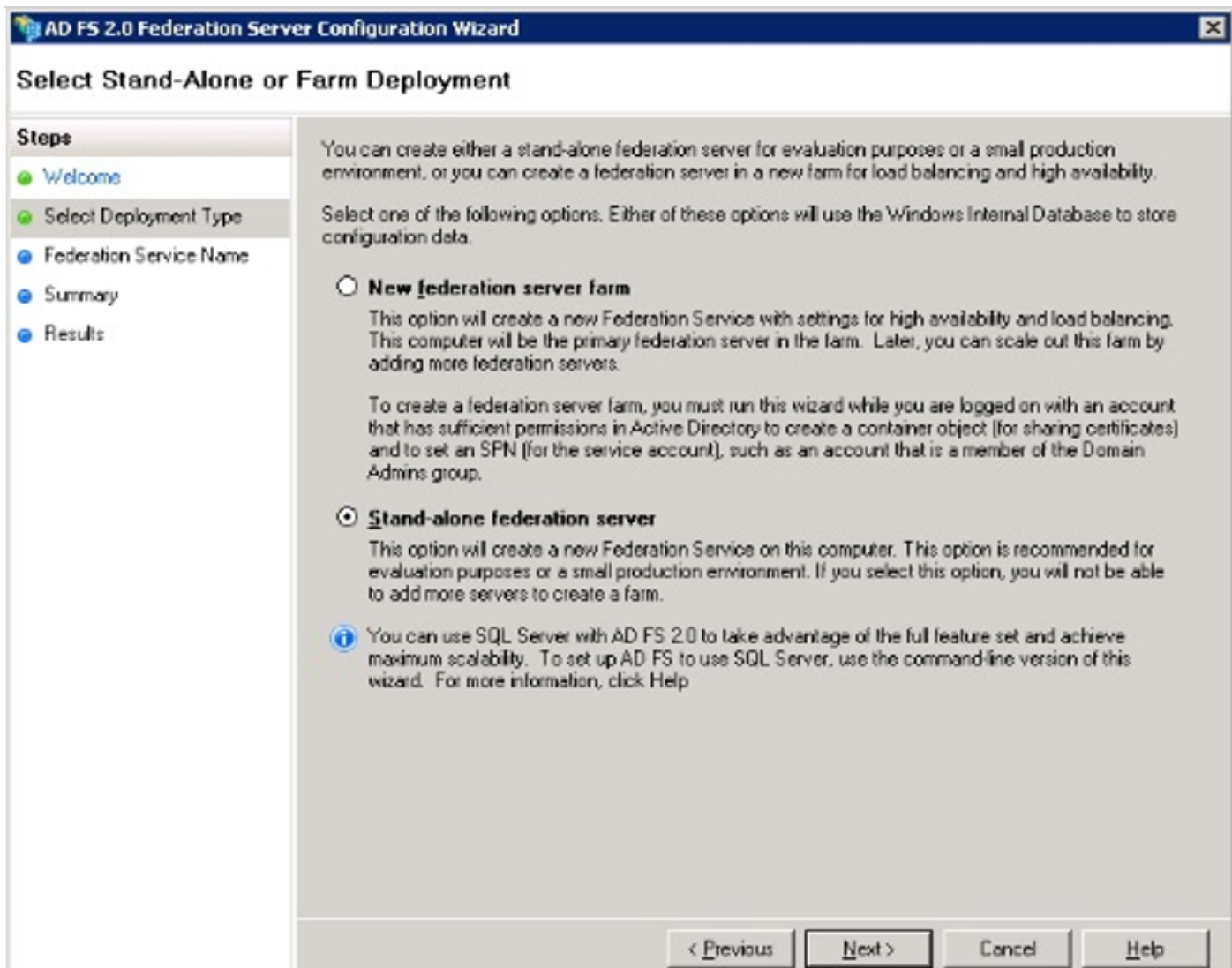
選擇Windows並鍵入AD FS Management以啟動ADFS管理控制檯，如下圖所示。



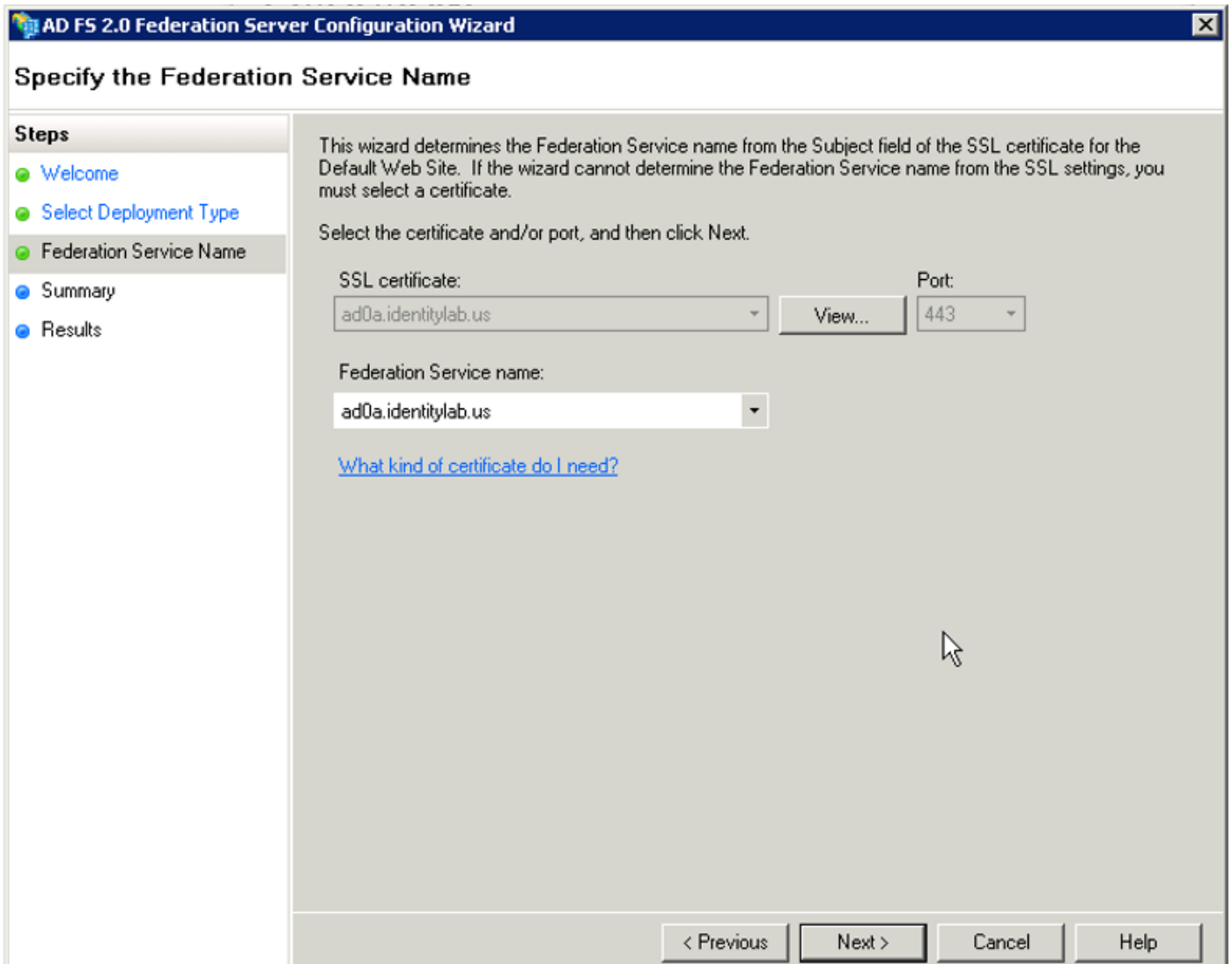
選擇AD FS 3.0 Federation Server Configuration Wizard選項以啟動ADFS伺服器配置。這些截圖與AD FS 3中的步驟相同。



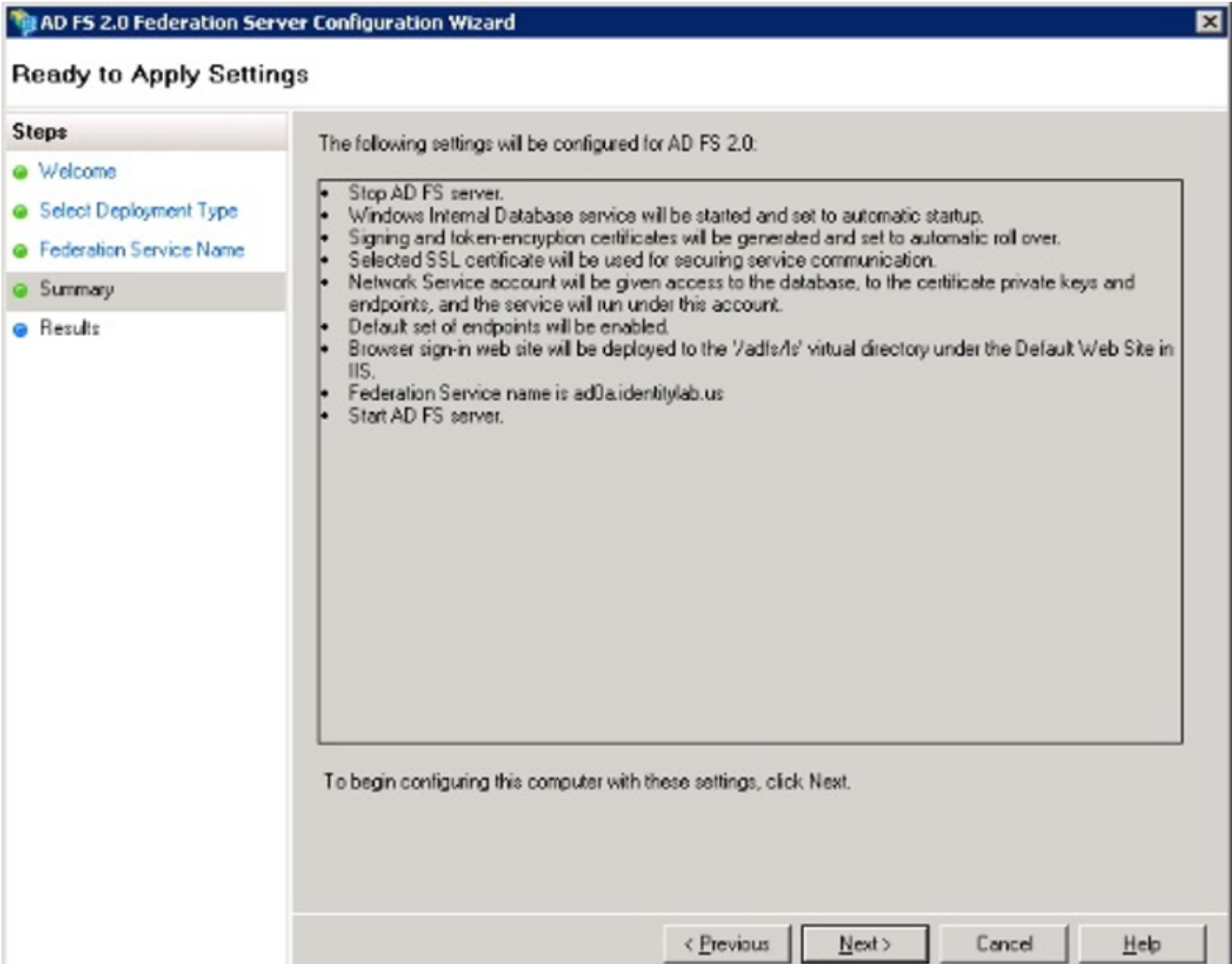
選擇Create a new Federation Service並單擊Next。



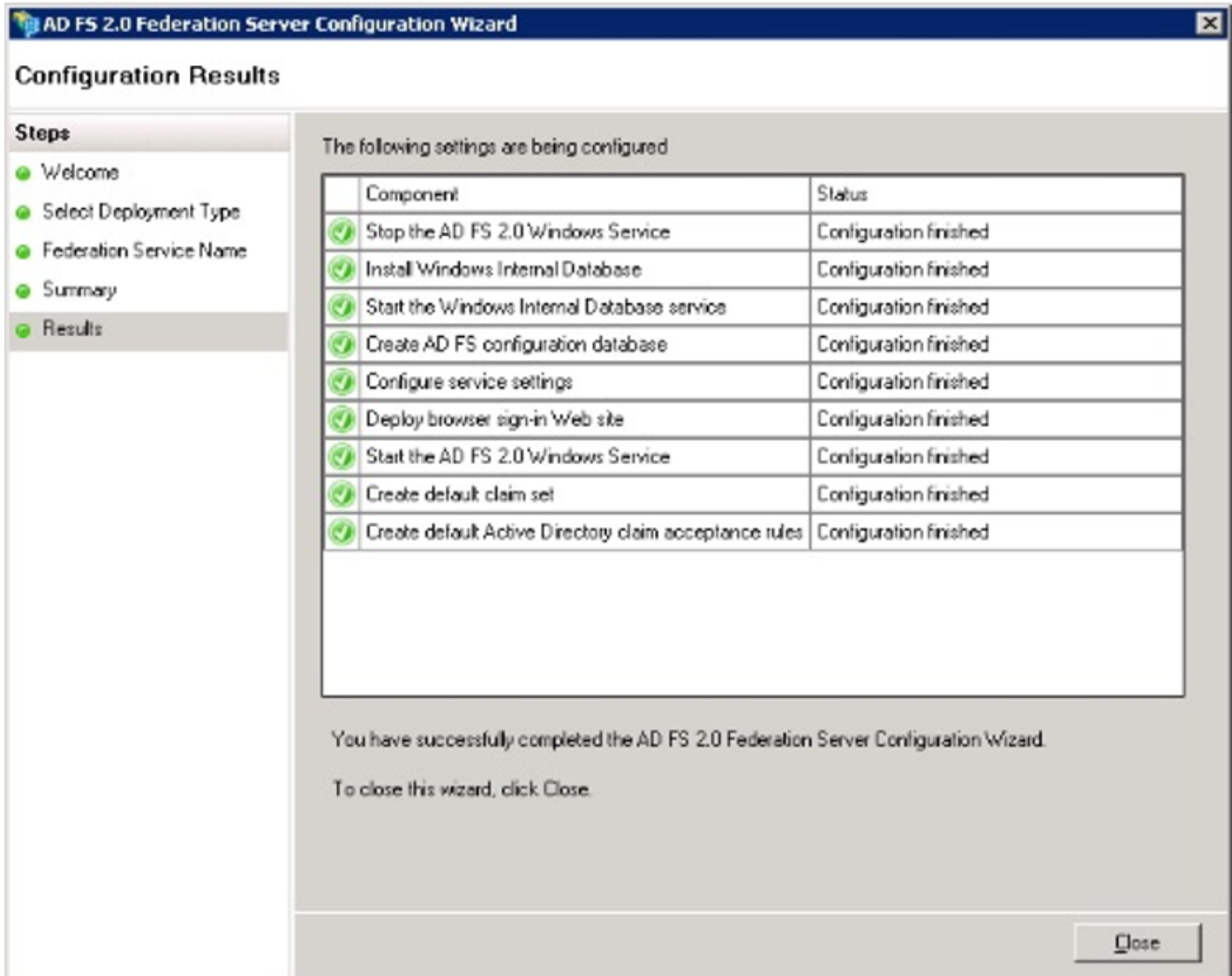
選擇Standalone Federation Server並按一下Next，如下圖所示。



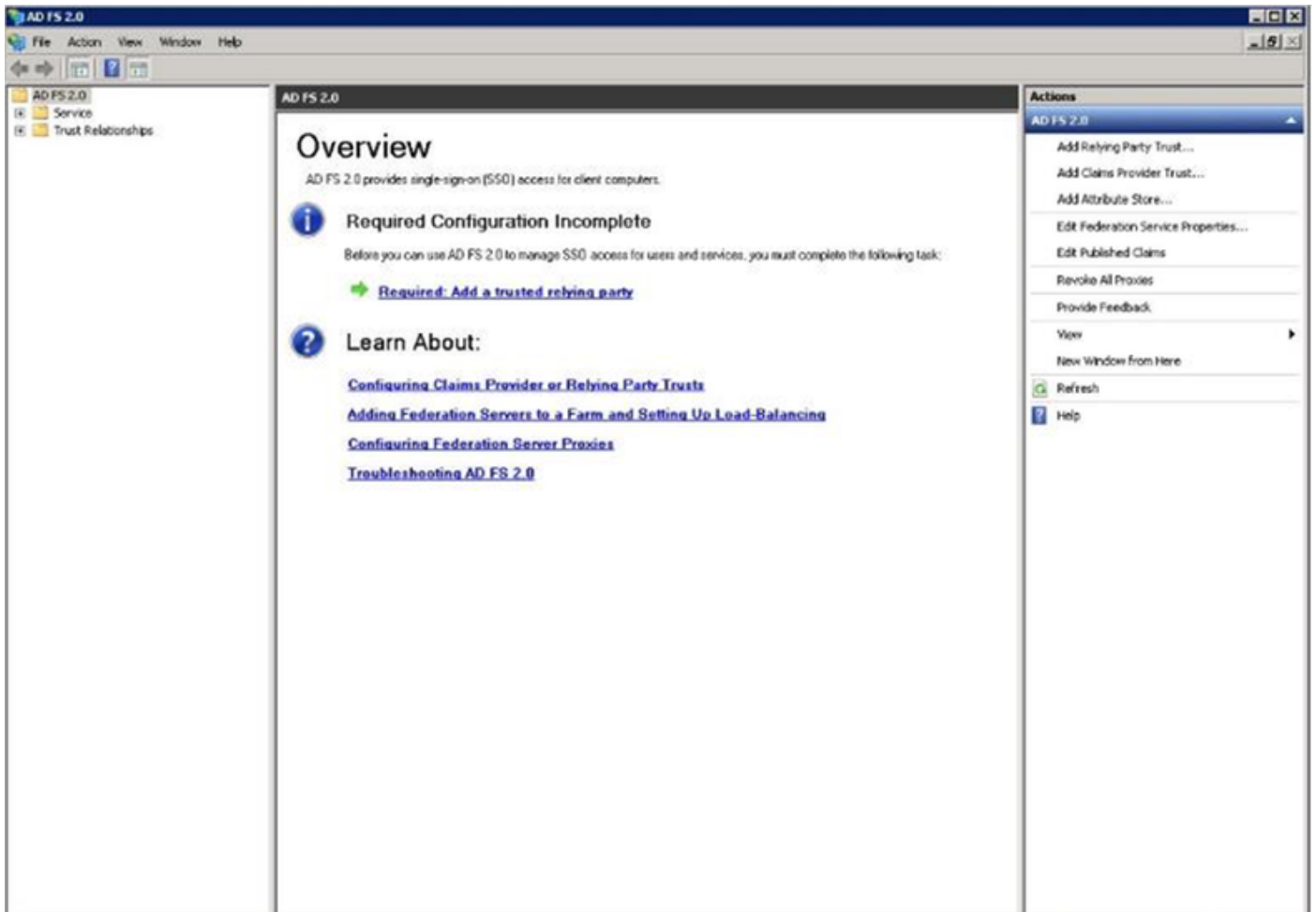
在SSL certificate下，從清單中選擇自簽名證書。聯合身份驗證服務名稱將自動填充。按「Next」（下一步）。



檢查設定並按一下下一步以應用設定。



確認所有元件已成功完成，然後按一下關閉以結束嚮導並返回主管理控制檯。這可能需要幾分鐘時間。



ADFS現在已有效地啟用並配置為身份提供程式(IdP)。接下來，您需要將CUCM新增為可信賴合作夥伴。在執行此操作之前，您需要先在CUCM管理中執行一些配置。



使用ADFS在CUCM上配置SSO

LDAP配置

群集需要與Active Directory進行LDAP整合，並且需要在進一步之前配置LDAP身份驗證。導覽至System索引標籤> LDAP System，如下圖所示。

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:

然後，導航到System頁籤 > LDAP目錄。

LDAP Directory

Save Delete Copy Perform Full Sync Now Add New

Status

Status: Ready

LDAP Directory Information

LDAP Configuration Name*

LDAP Manager Distinguished Name*

LDAP Password*

Confirm Password*

LDAP User Search Base*

LDAP Custom Filter for Users

Synchronize* Users Only Users and Groups

LDAP Custom Filter for Groups

LDAP Directory Synchronization Schedule

Perform Sync Just Once

Perform a Re-sync Every*

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

Standard User Fields To Be Synchronized

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

LDAP Server Information

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

Save

Active Directory使用者與CUCM同步後，需要配置LDAP身份驗證。

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

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

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

LDAP Authentication

Save

Status
Status: Ready

LDAP Authentication for End Users

Use LDAP Authentication for End Users
 LDAP Manager Distinguished Name* fhlab\Administrator
 LDAP Password*
 Confirm Password*
 LDAP User Search Base* cn=users,dc=fhlab,dc=com

LDAP Server Information

Host Name or IP Address for Server* 10.89.228.226 LDAP Port* 389 Use TLS
 Add Another Redundant LDAP Server

CUCM中的終端使用者需要為其終端使用者配置檔案分配特定的訪問控制組。ACG是標準CCM超級使用者。當環境準備就緒時，將使用使用者測試SSO。

End User Configuration Related Links: Back to Find List Users Go

Save Delete Add New

Confirm MLPP Password
 MLPP Precedence Authorization Level Default

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
 Add to Access Control Group
 Remove from Access Control Group

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

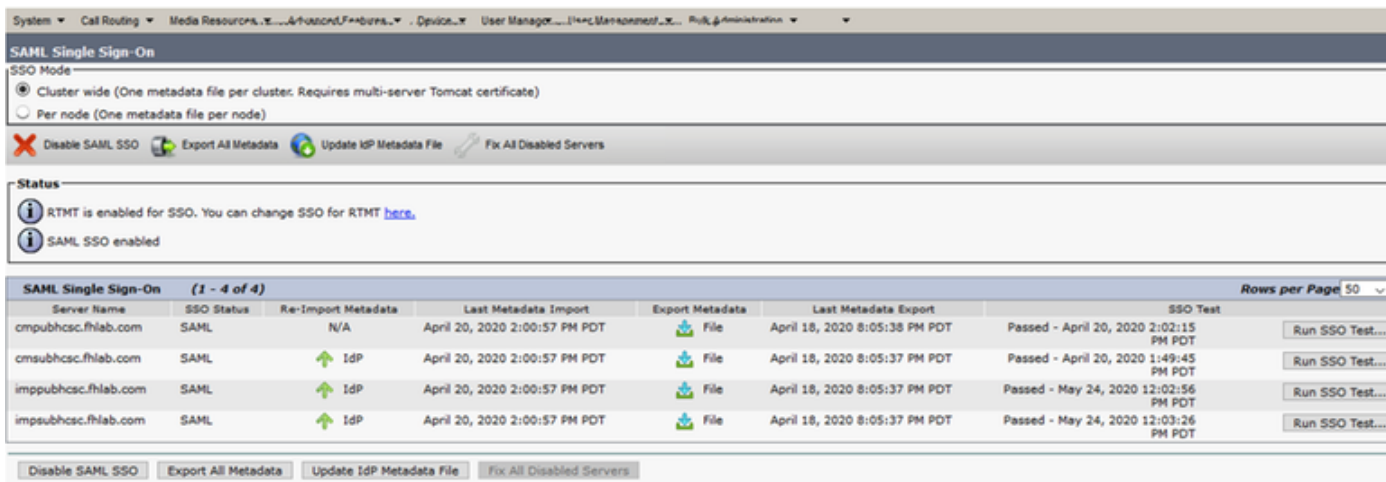
Enable End User to Host Conference Now
 Meeting Number 1001
 Attendees Access Code

Save Delete Add New

CUCM後設資料

本節將介紹CUCM Publisher的流程。

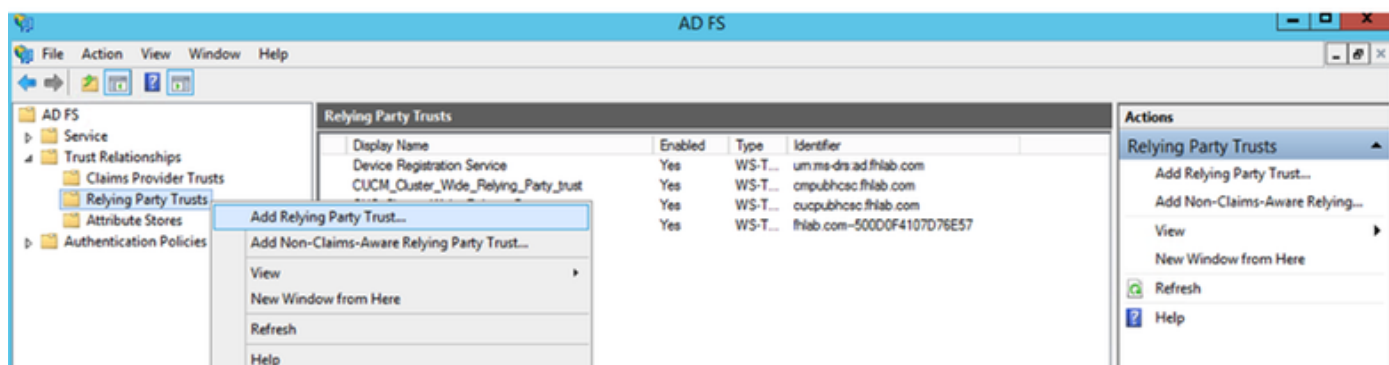
第一個任務是獲取CUCM後設資料，為此您需要瀏覽到URL;https://<CUCM Pub FQDN>:8443/ssosp/ws/config/metadata/sp，或者可以從「System (系統)」頁籤> SAML單一登入下載。這可以按節點或集群範圍完成。最好在群集範圍內執行此操作。



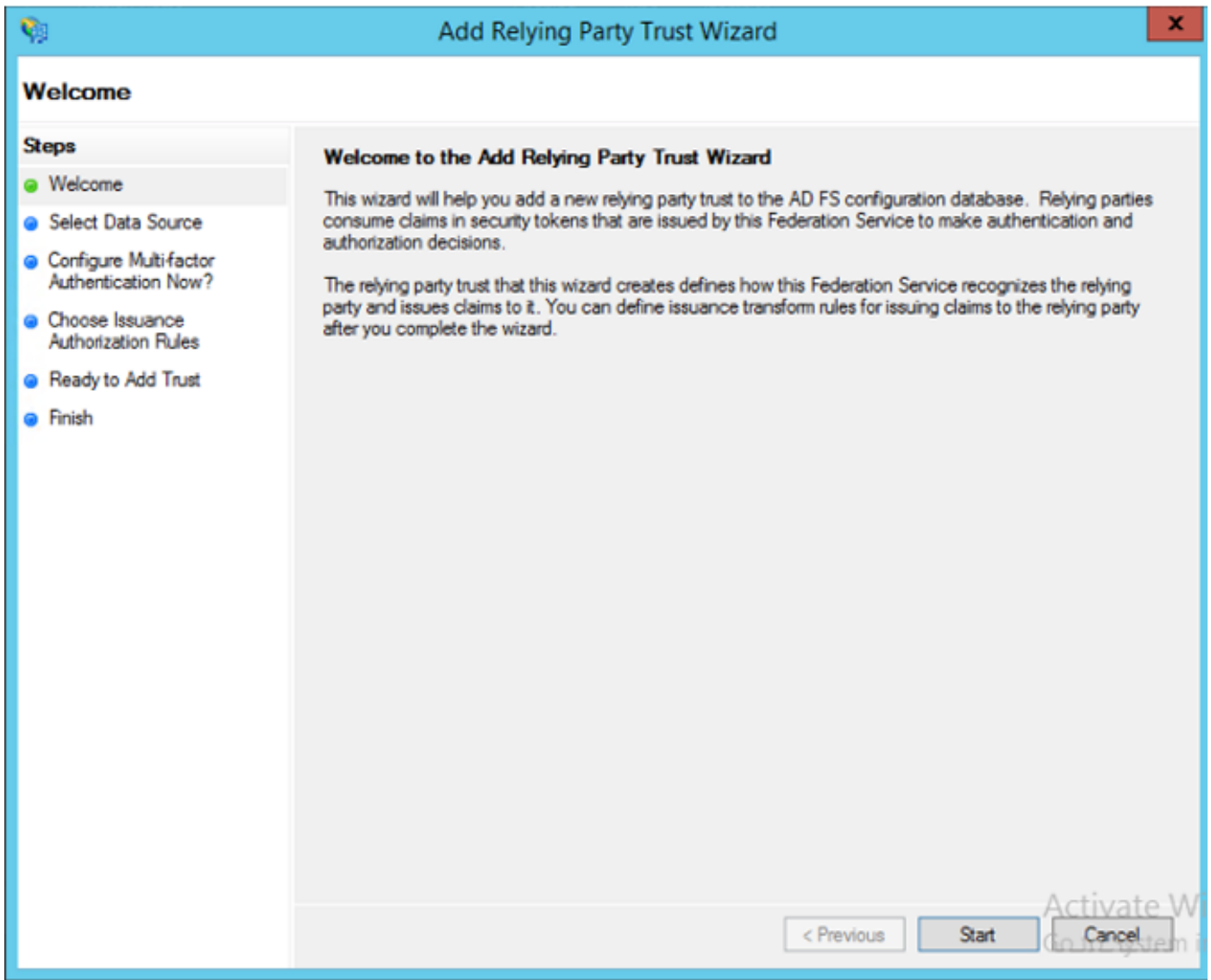
使用有意義的名稱 (如sp_cucm0a.xml) 在本地儲存資料，之後您將需要該名稱。

配置ADFS信賴方

回到AD FS 3.0管理控制檯。

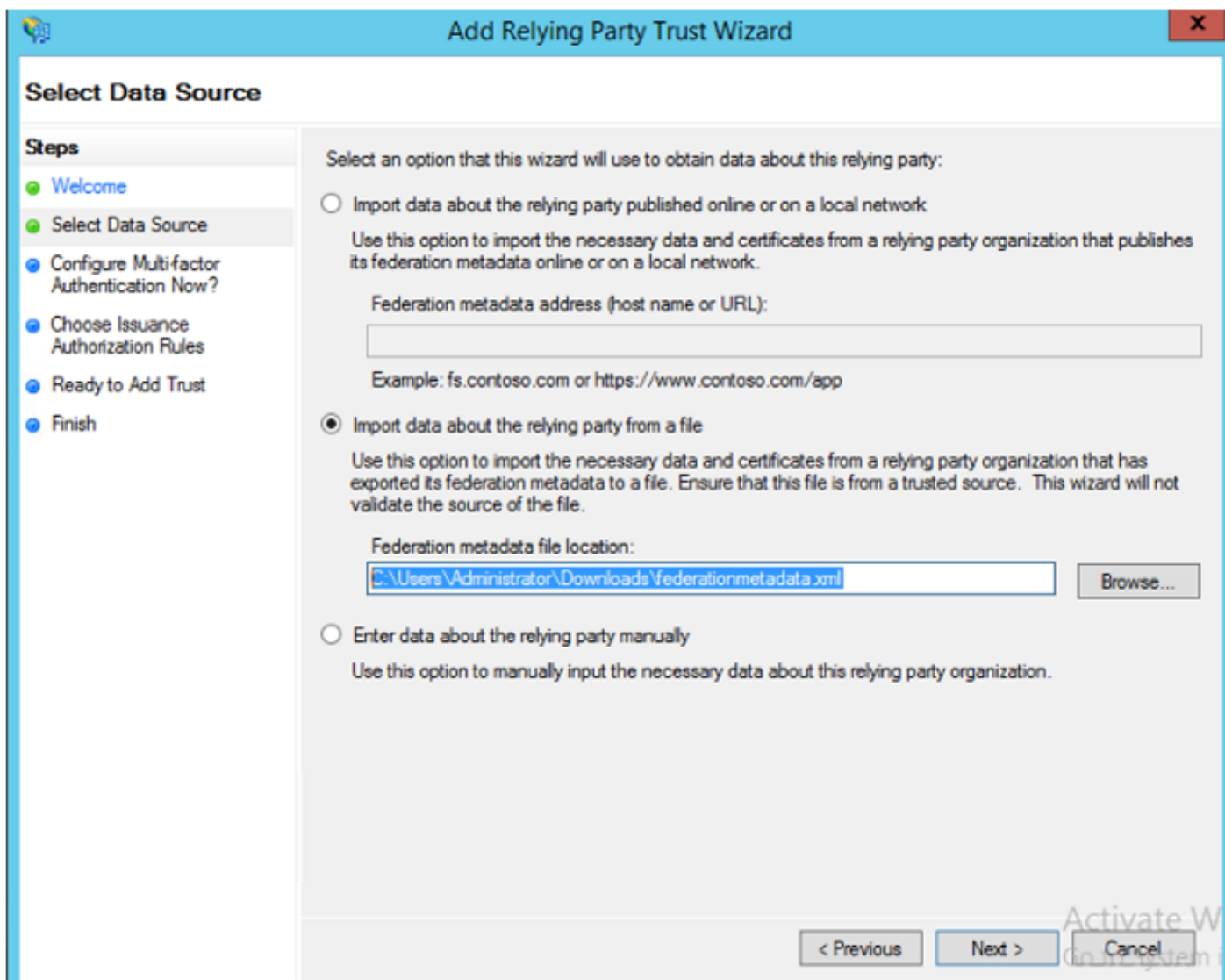


按一下**新增信賴方信任嚮導**。

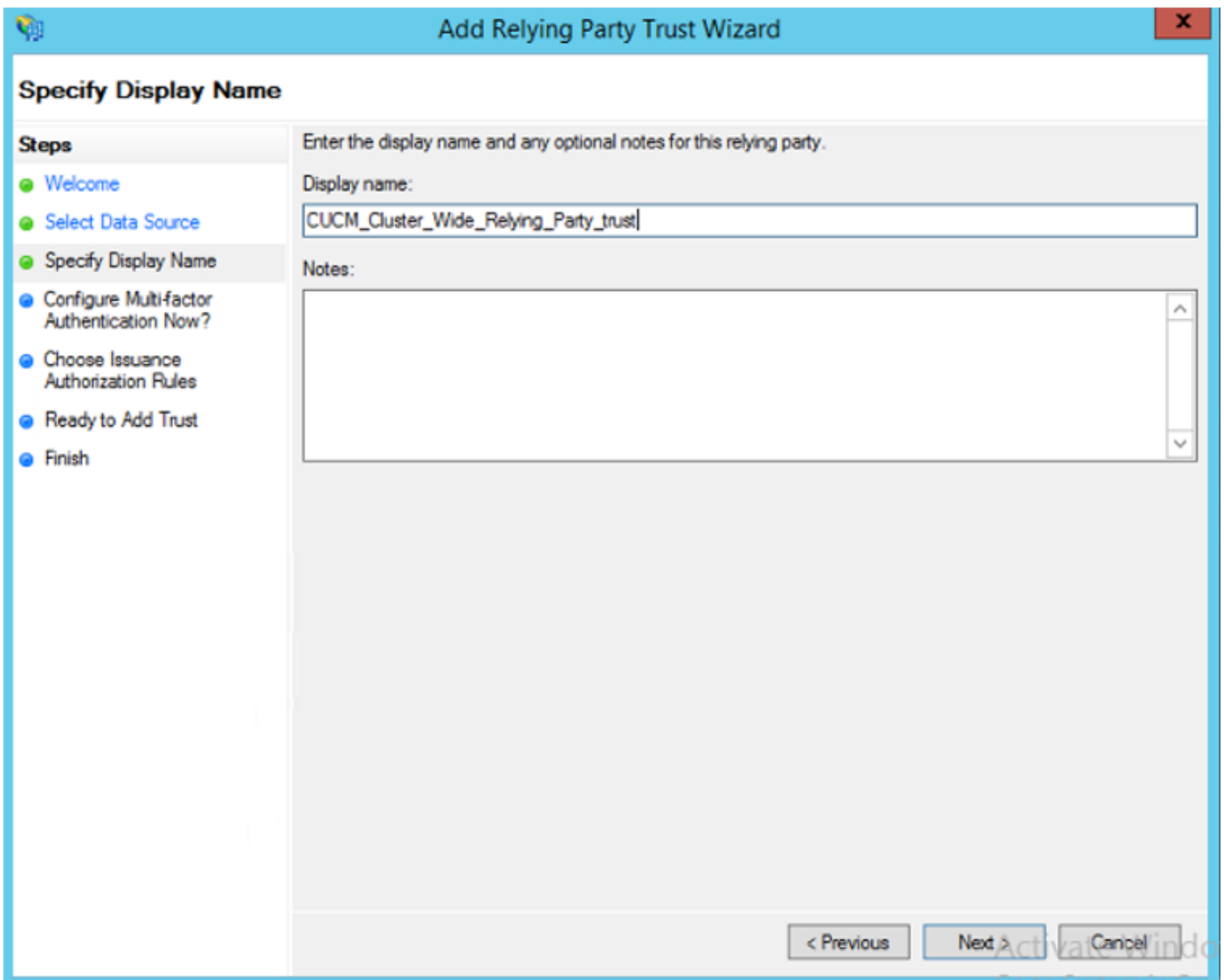


按一下**Start**繼續。

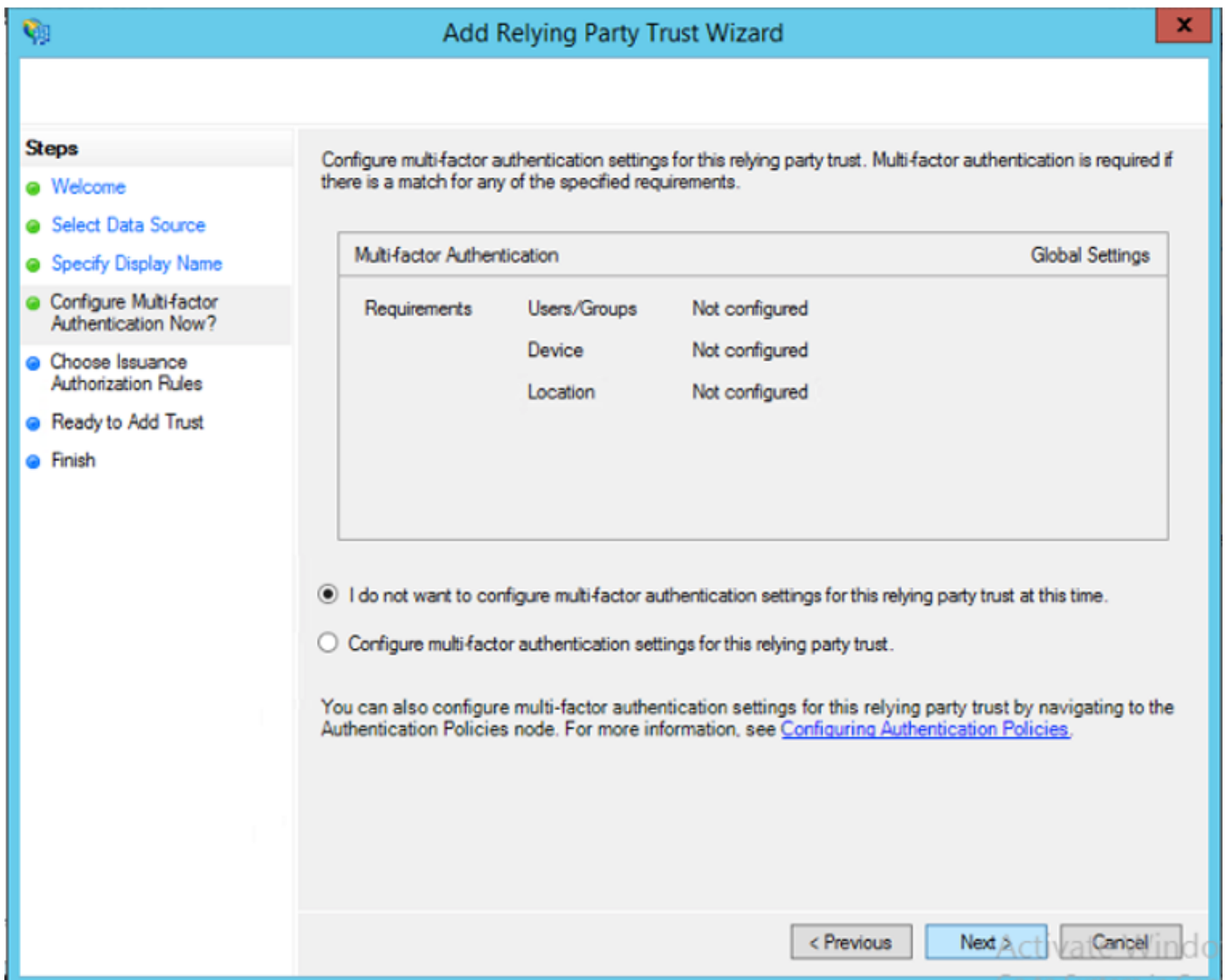
選擇之前儲存的**federationmetadata.xml**元資料XML檔案，然後按一下下一步。



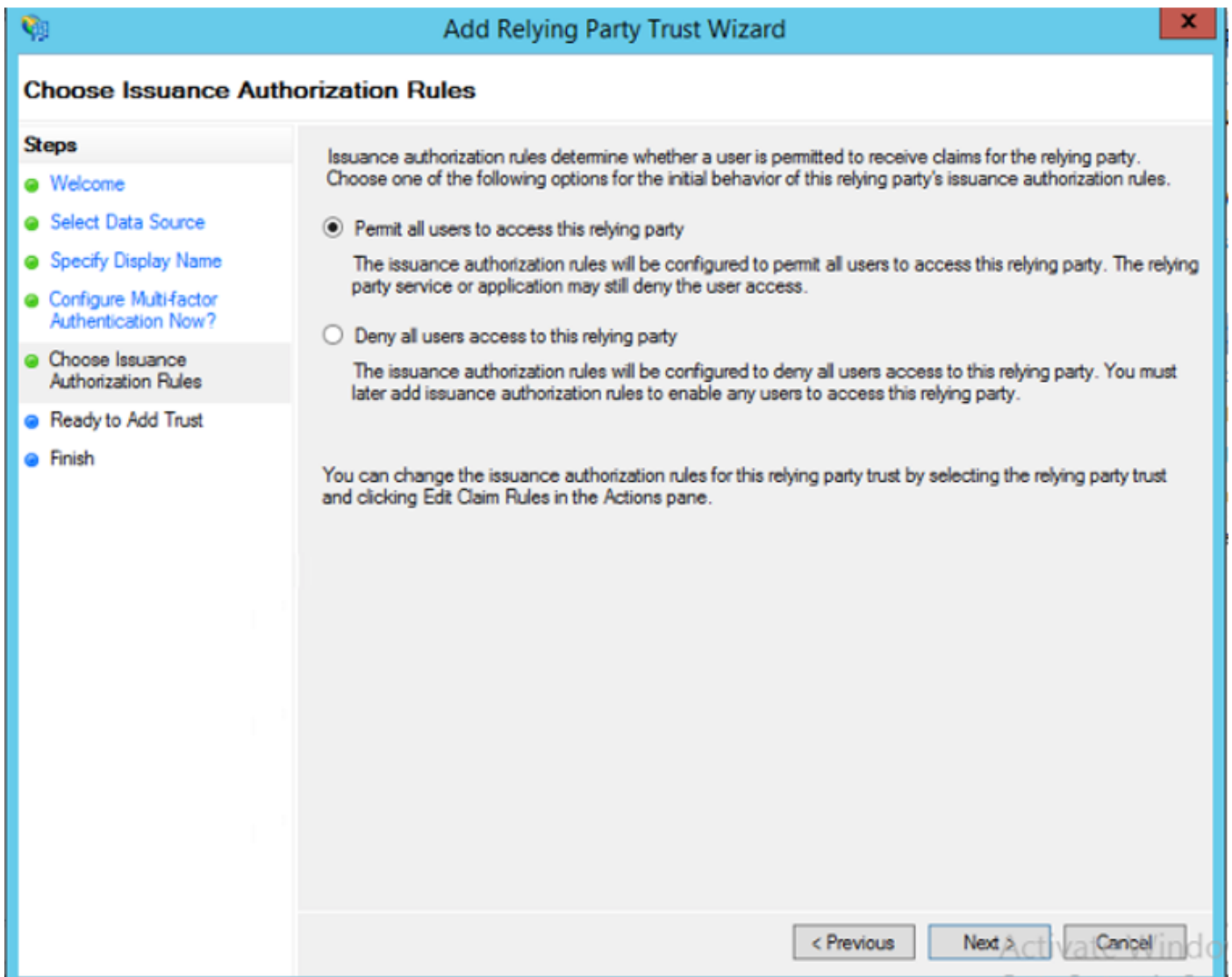
使用CUCM_Cluster_Wide_Reliking_Party_trust作為顯示名稱，然後按一下下一步。



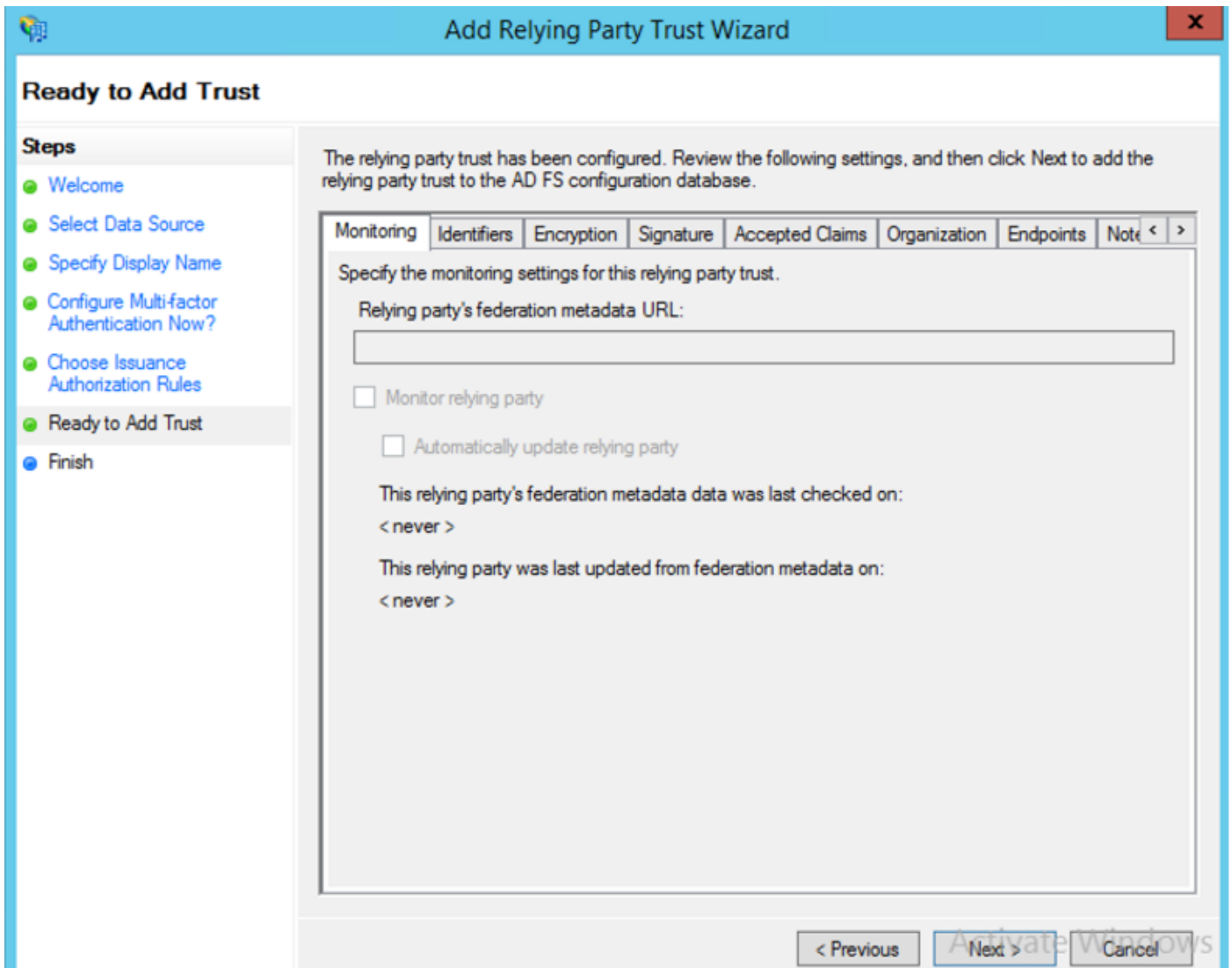
選擇第一個選項，然後按一下下一步。



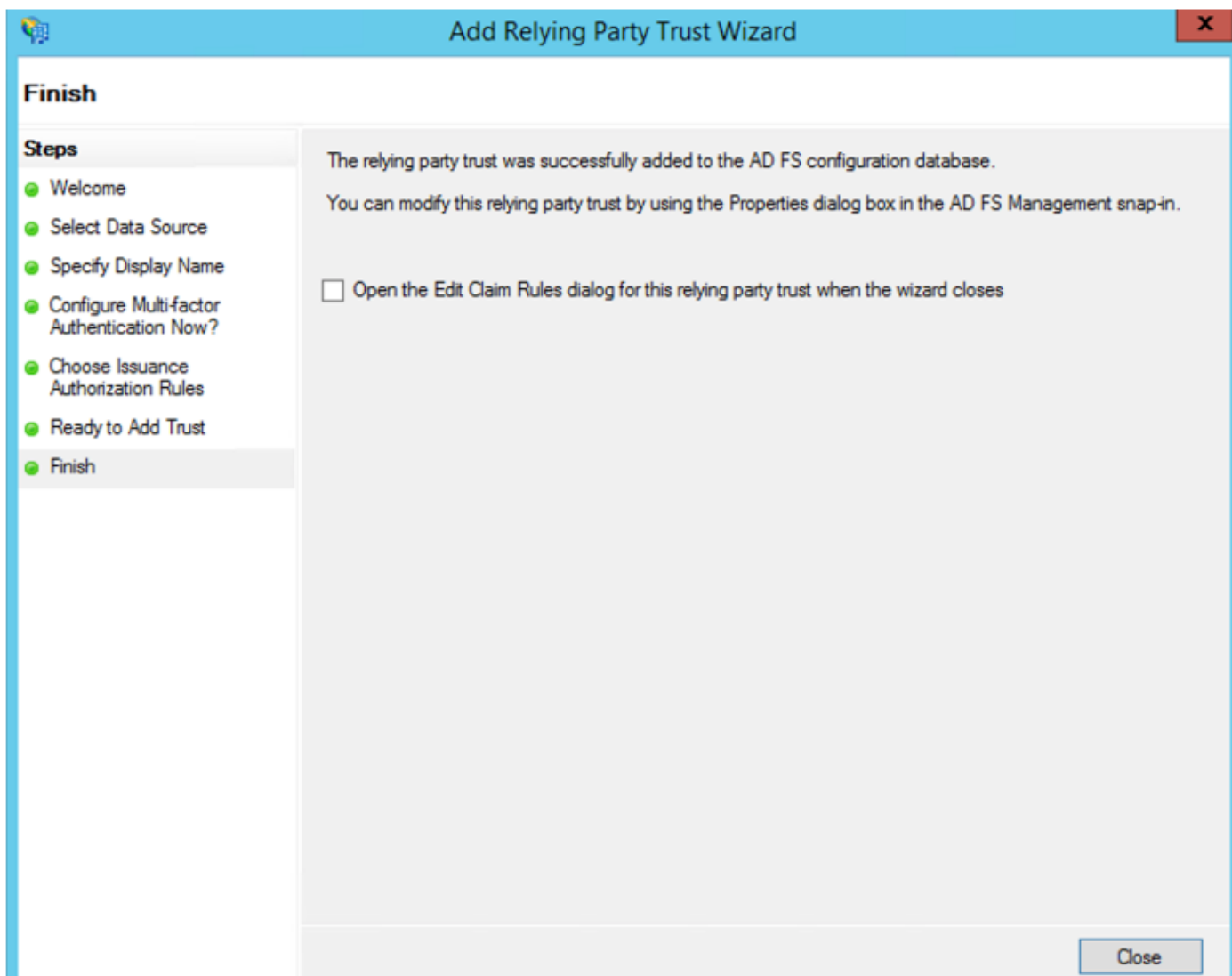
選擇允許所有使用者訪問此信賴方，然後按一下下一步，如下圖所示。



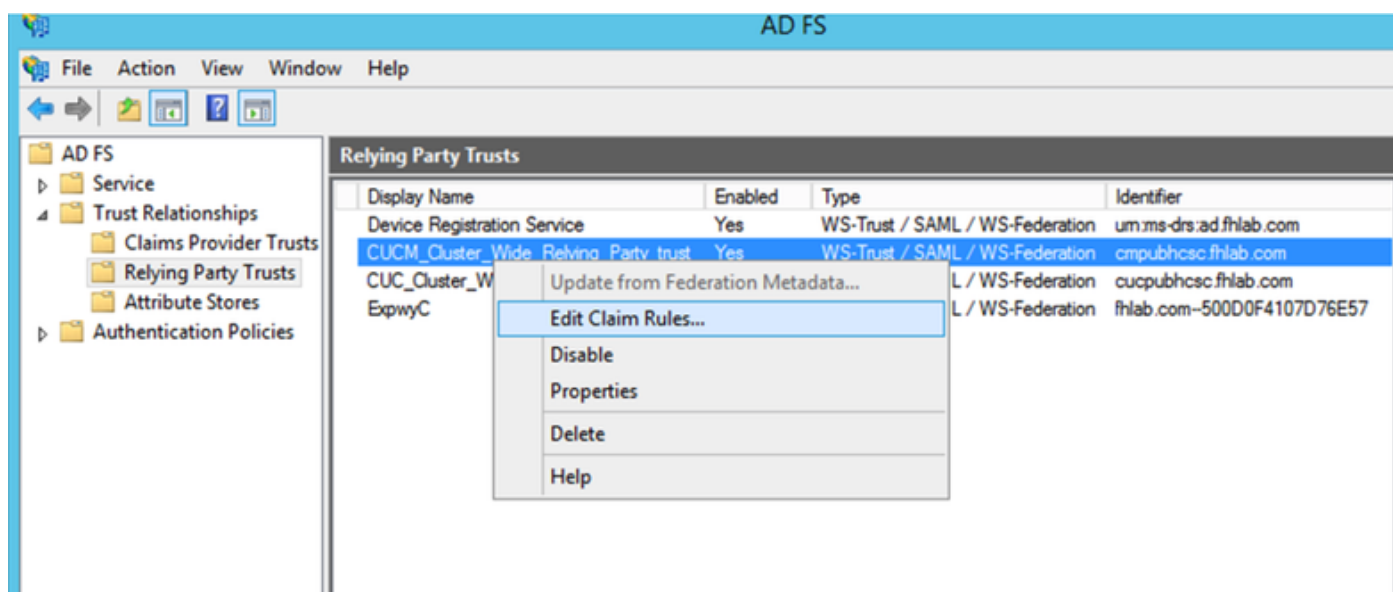
檢視設定，然後按一下**Next**，如下圖所示。



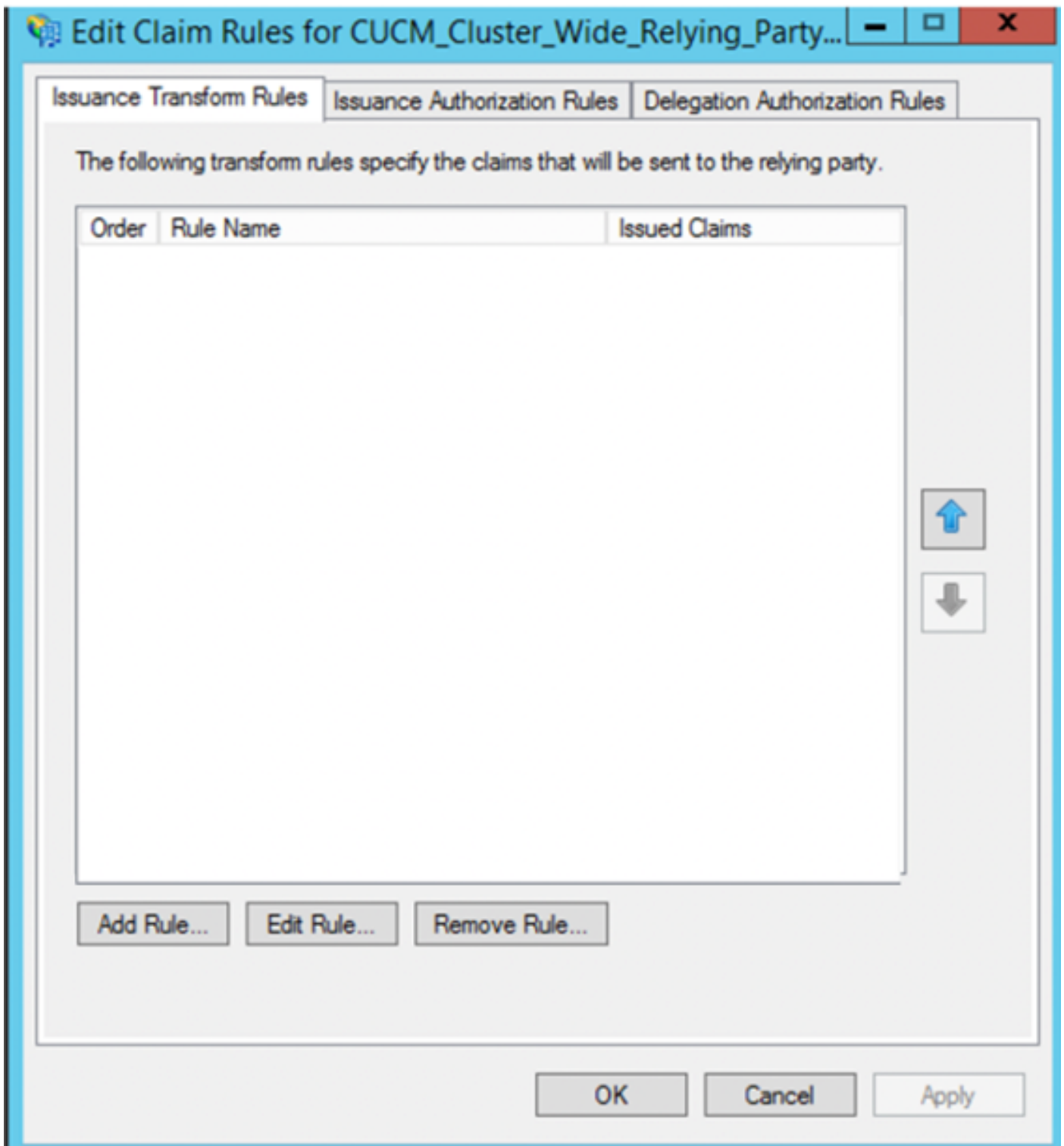
取消選中該框並按一下**Close**。



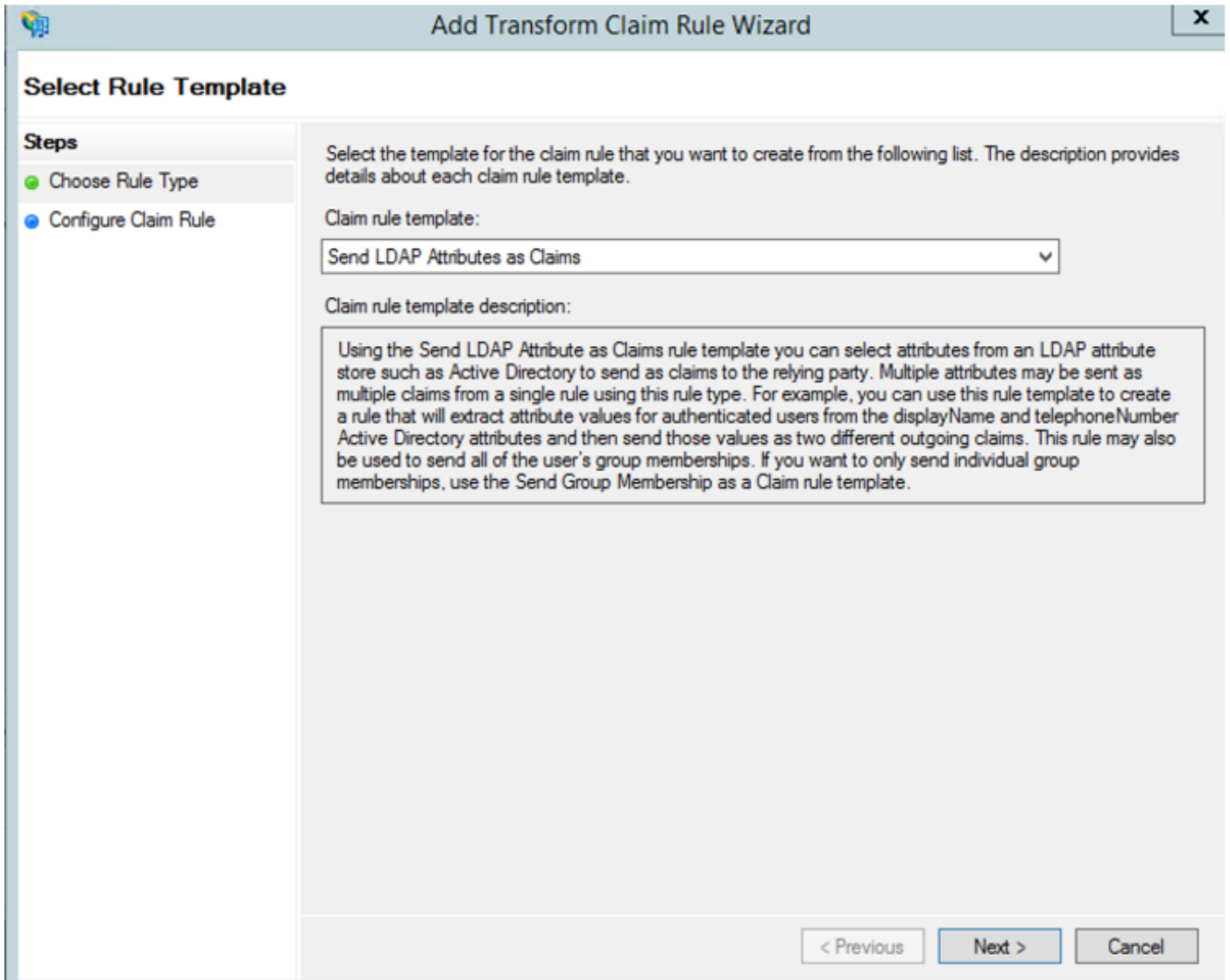
使用滑鼠輔助按鍵選擇剛建立的信賴方信任和「編輯宣告規則」配置，如下圖所示。



按一下「Add Rule」，如下圖所示。



選擇Send LDAP Attributes as Claims，然後按一下Next。



配置以下引數：

宣告規則名稱：名稱ID

屬性儲存：Active Directory (按兩下下拉選單箭頭)

LDAP屬性：SAM-Account-Name

傳出宣告型別：uid

按一下FINISH/OK繼續。

請注意，uid大小寫不小，並且不在下拉選單中。打出來。

Edit Rule - NameID [X]

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

Claim rule name:

Rule template: Send LDAP Attributes as Claims

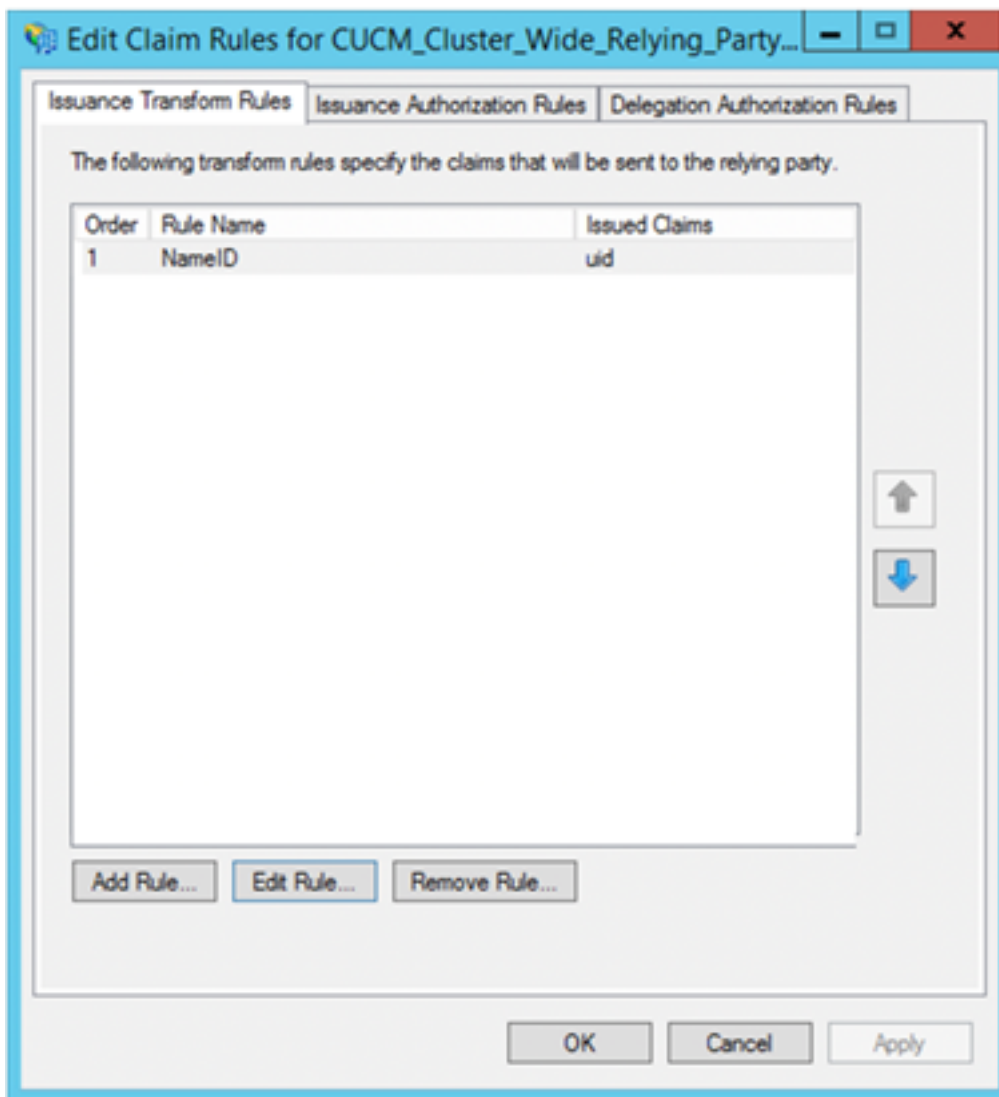
Attribute store:

Mapping of LDAP attributes to outgoing claim types:

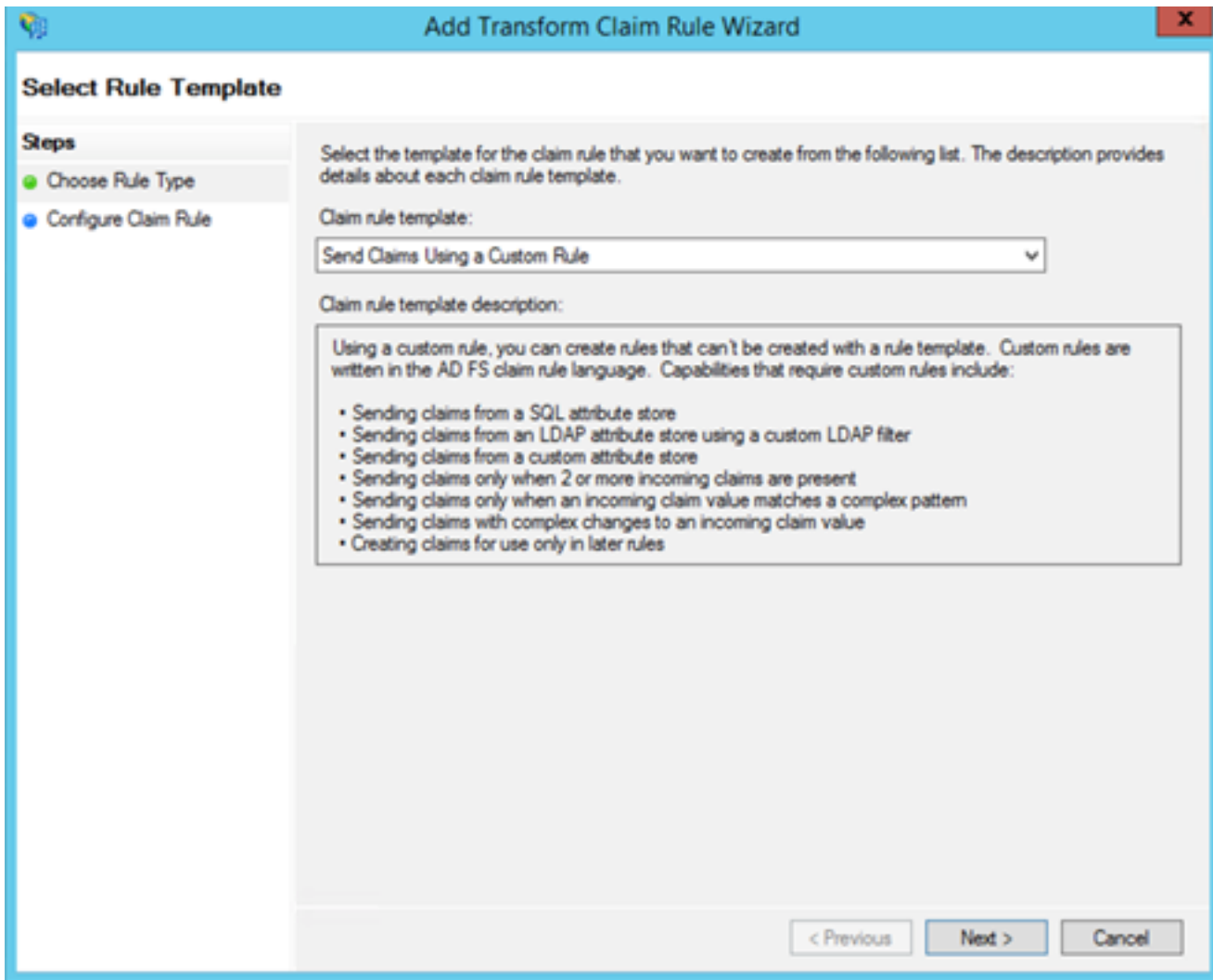
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name	uid
*		

Activate

再次按一下**Add Rule**以新增其他規則。



選擇Send Claims Using a Custom Rule，然後按一下Next。



建立名為Cluster_Side_Claim_Rule的自定義規則。

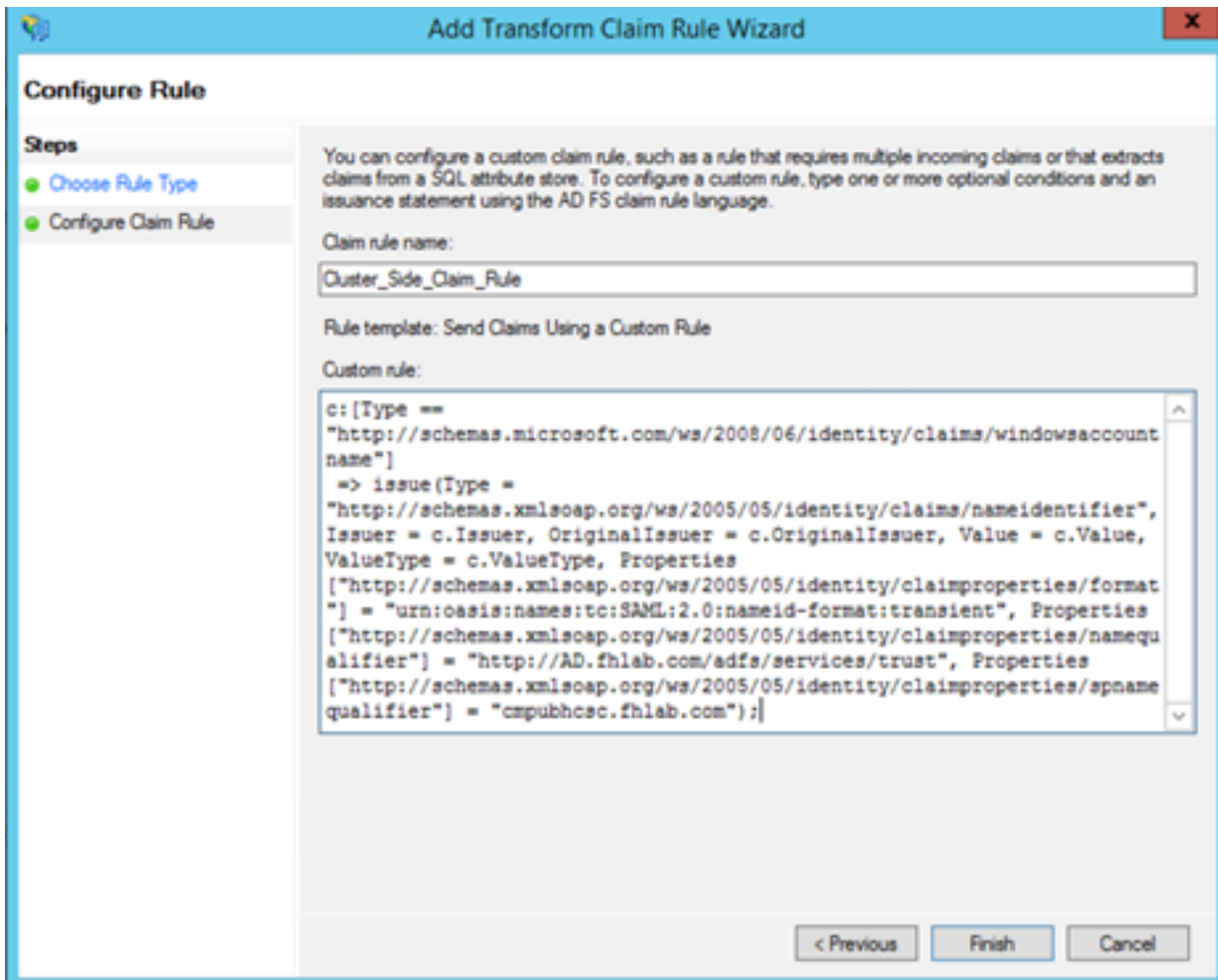
從此處直接在規則視窗中複製並貼上此文本。有時，如果在文本編輯器中編輯引號，則會發生更改，這會導致測試SSO時規則失敗：

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

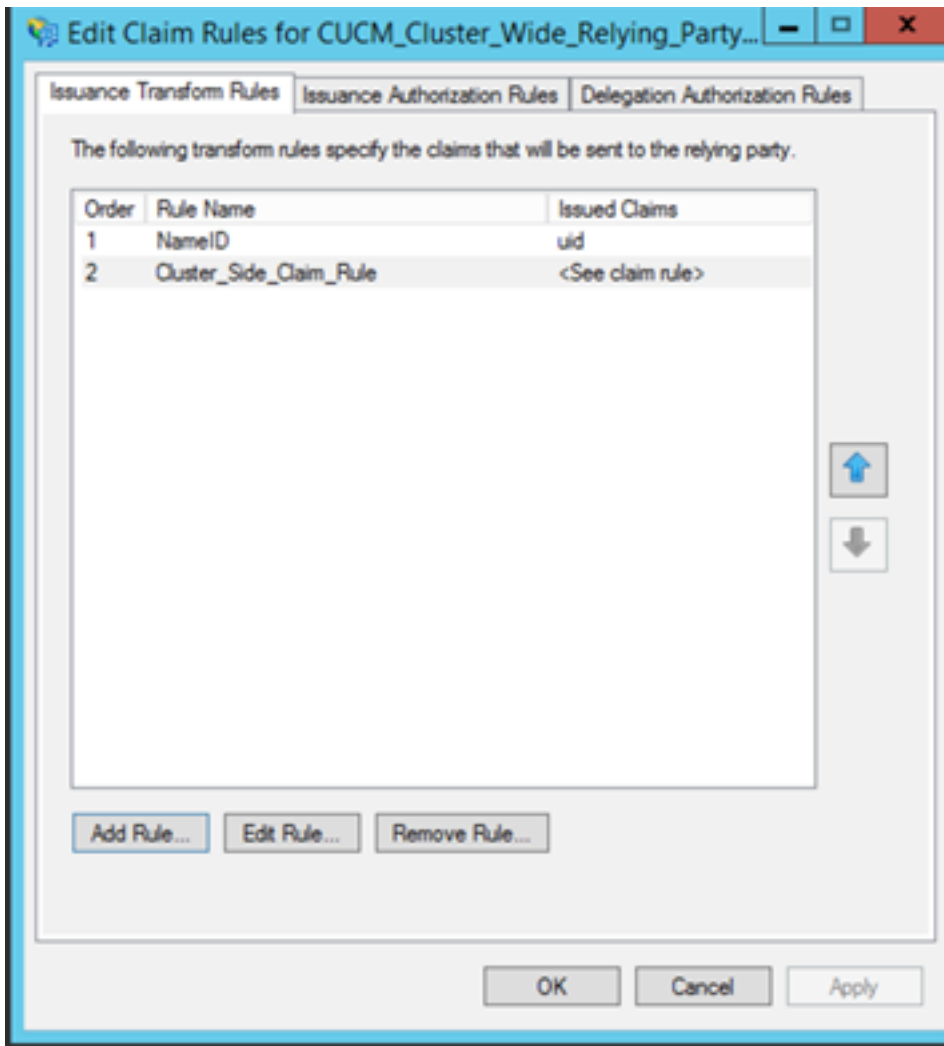
```
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]  
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",  
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,  
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]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

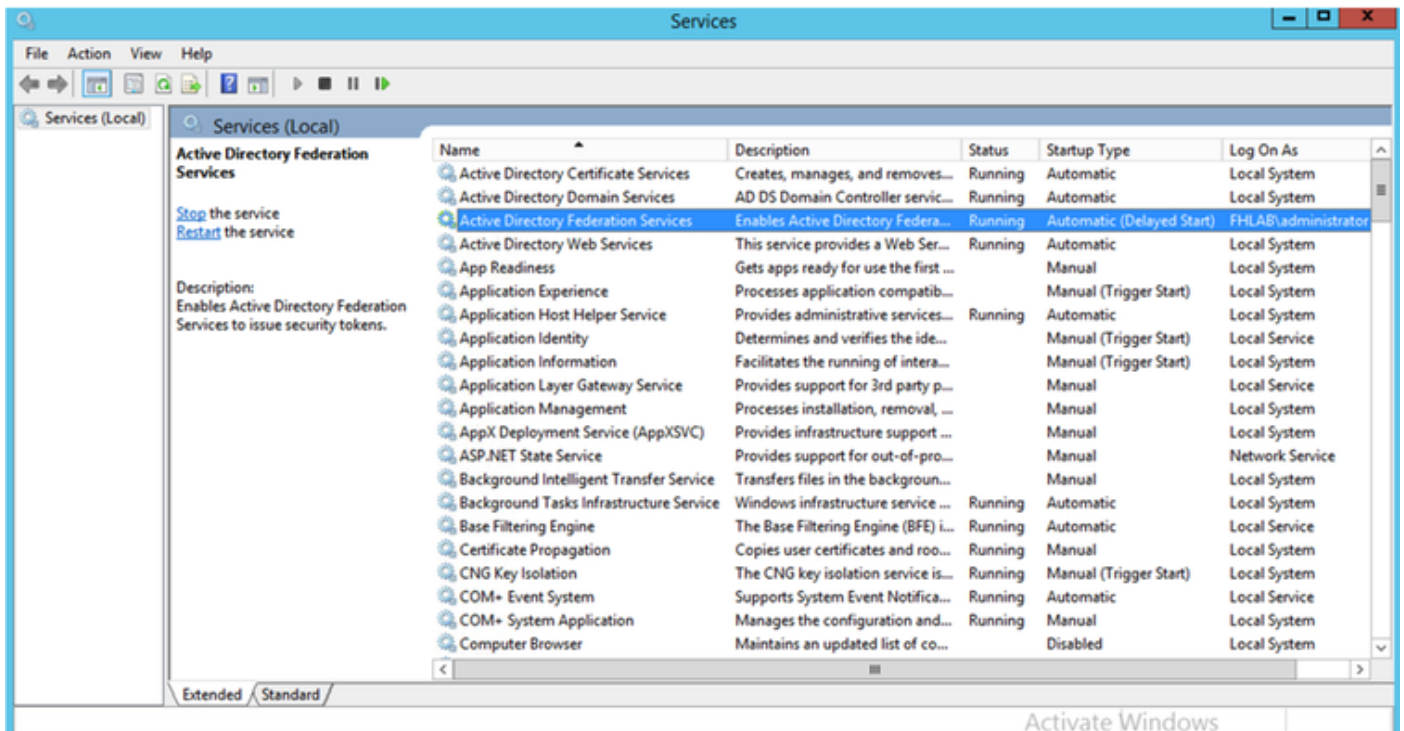
按一下Finish以繼續。



現在，您應該在ADFS上定義兩個規則。按一下Apply和OK關閉規則視窗。



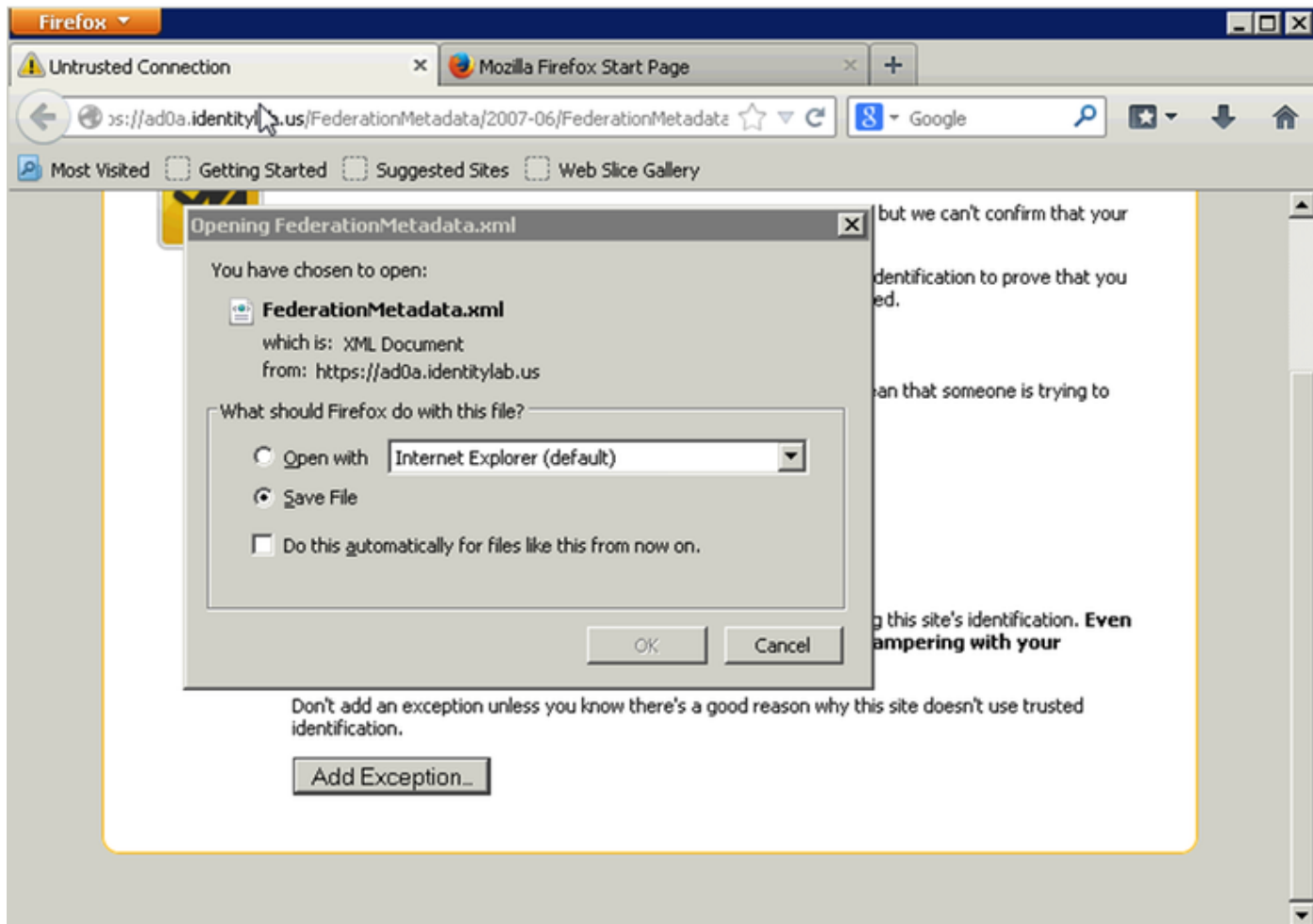
CUCM現在已成功新增為ADFS的受信任信賴方。



繼續之前，請重新啟動ADFS服務。導航到開始選單>管理工具>服務。

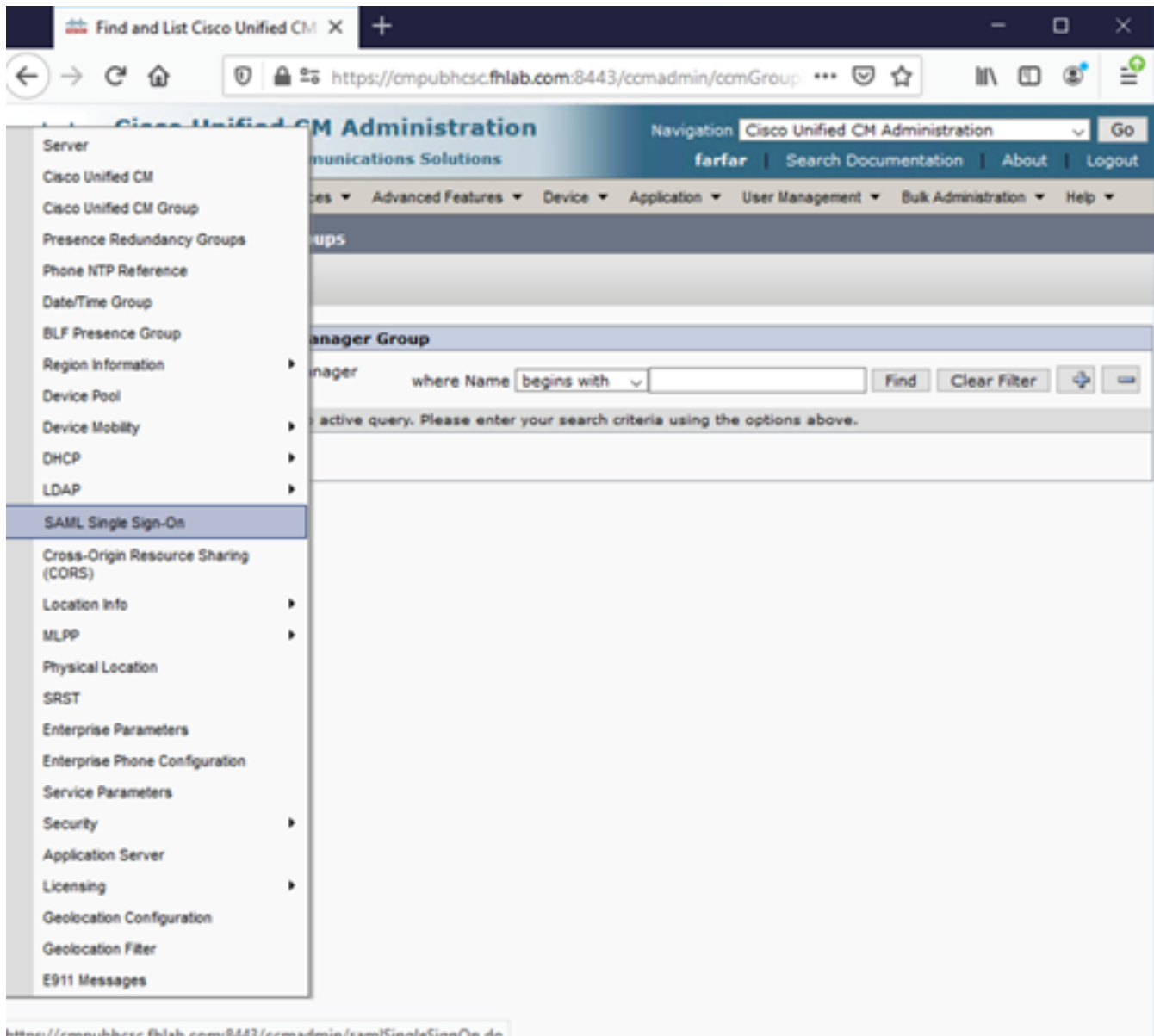
IDP後設資料

您需要向CUCM提供有關我們的IdP的資訊。使用XML後設資料交換此資訊。確保在安裝ADFS的伺服器上執行此步驟。

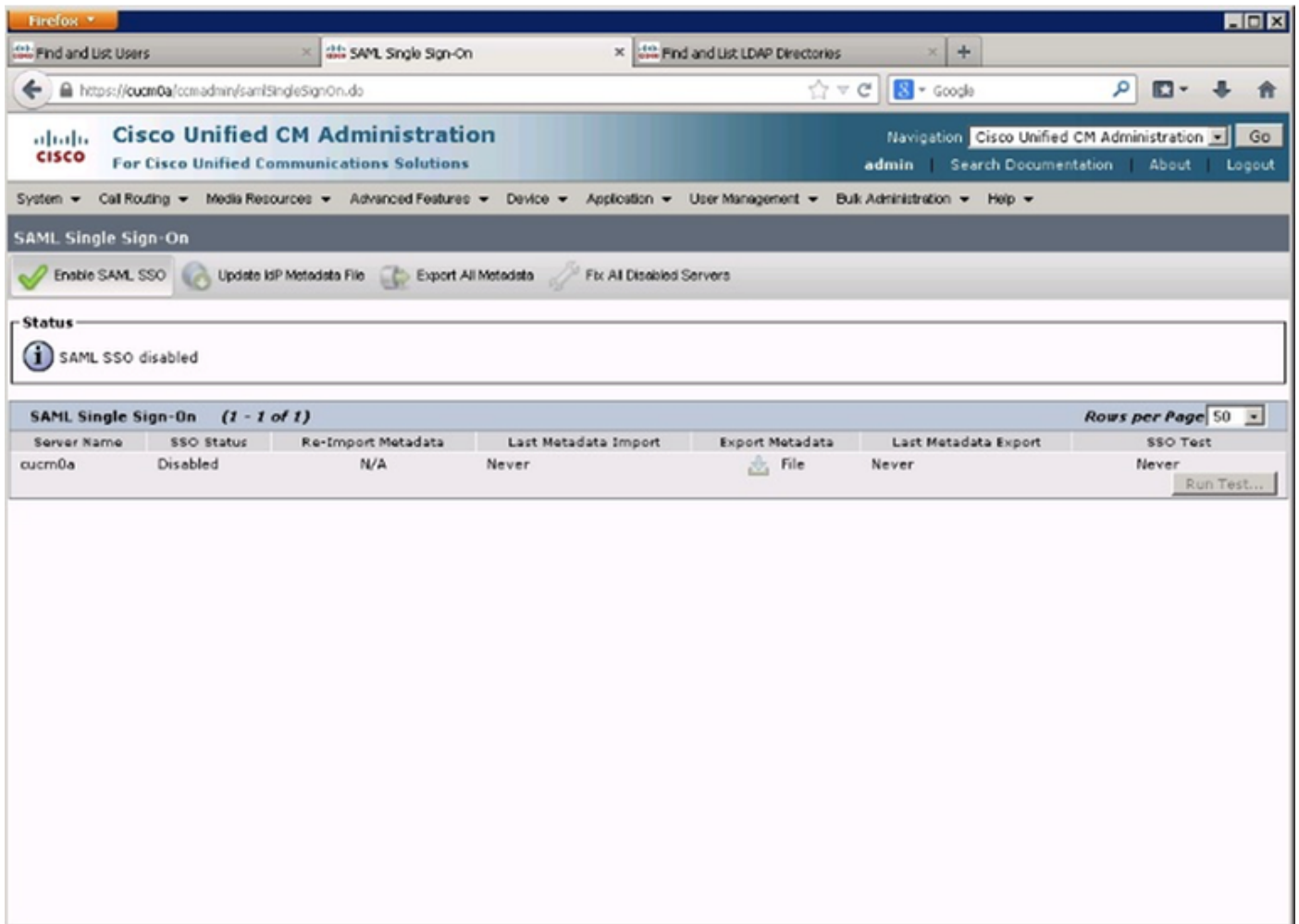


首先，您需要使用Firefox瀏覽器連線到ADFS(IdP)以下載XML後設資料。開啟瀏覽器到 <https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>，並將後設資料儲存到本地資料夾。

現在，導航至CUCM配置至system Menu > SAML Single Sign-On選單。



切换回CUCM管理並選擇SYSTEM > SAML Single Sign-On。



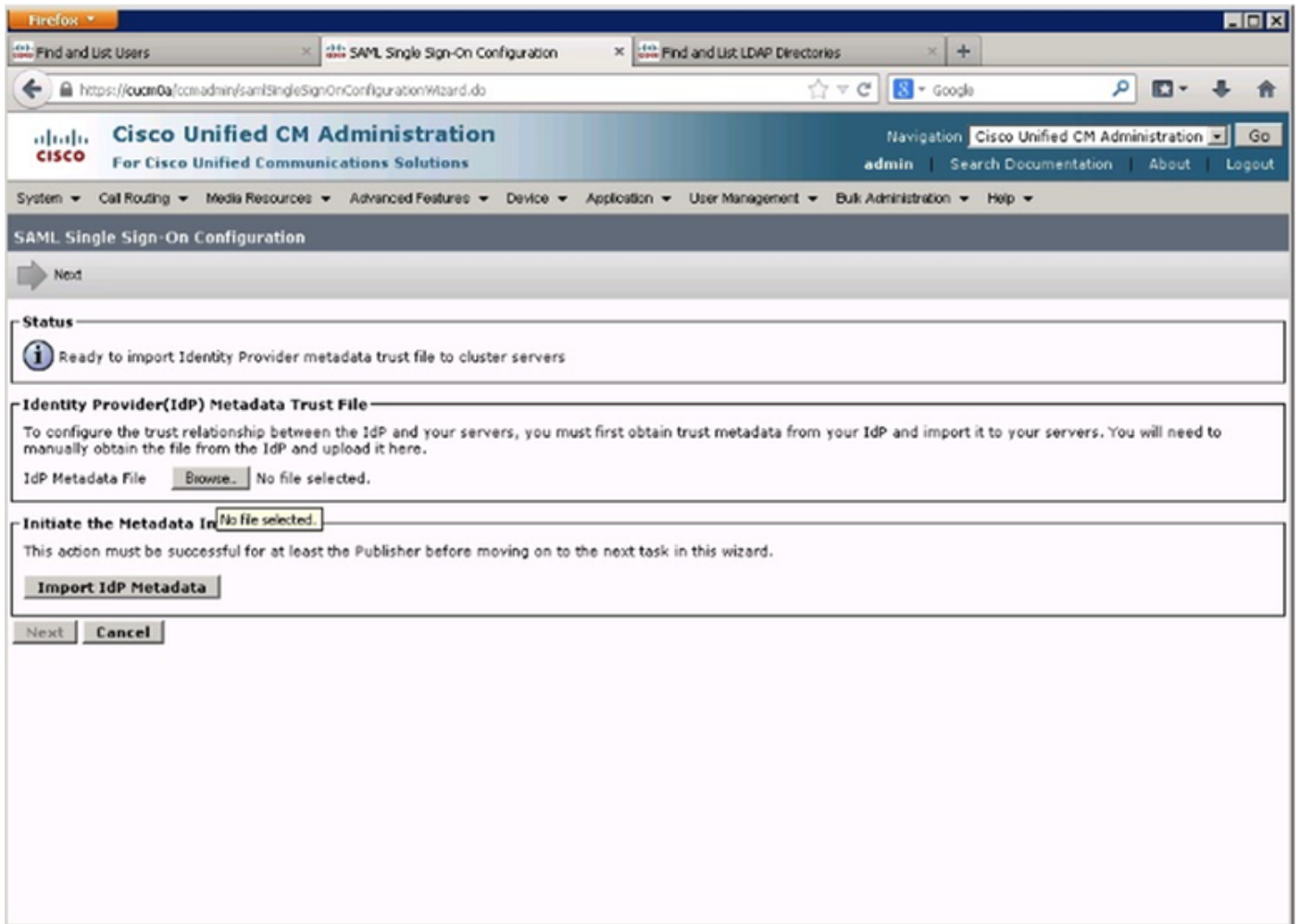
選擇啟用SAML SSO。

按一下「Continue」以確認警告。

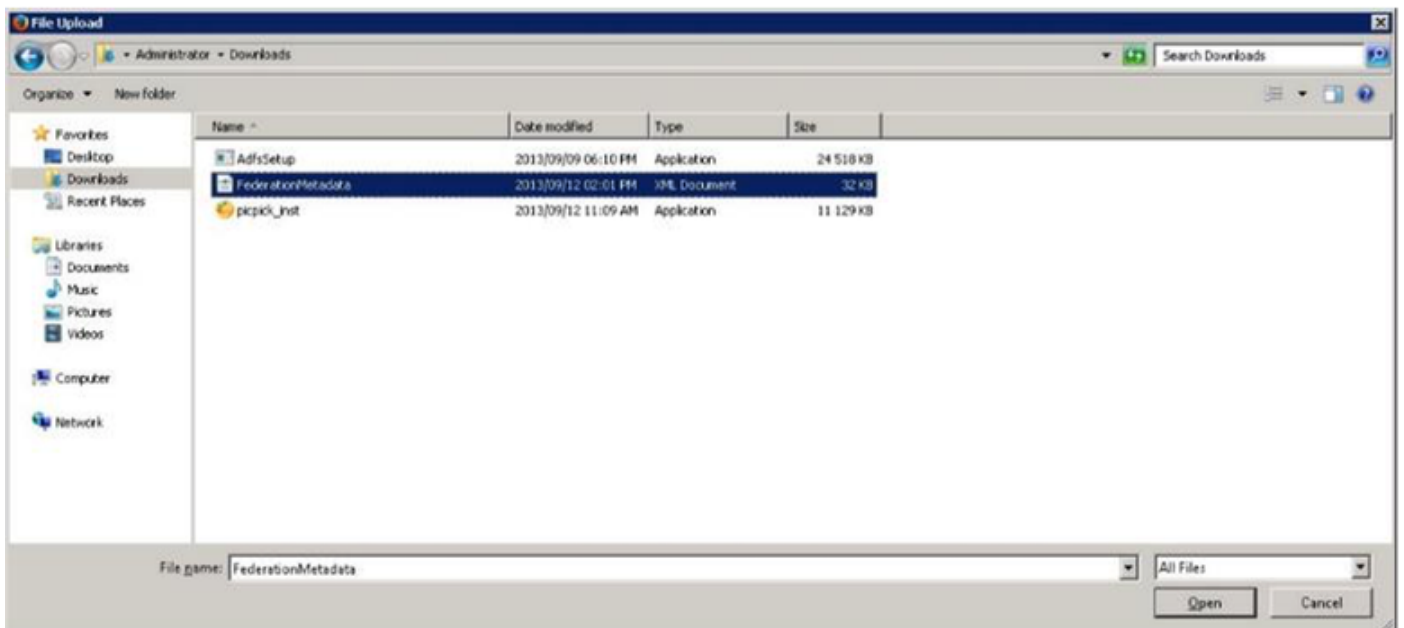


在SSO螢幕上，按一下Browse..以匯入之前儲存的FederationMetadata.xml後設資料XML檔案，如

下圖所示。



選擇XML檔案，然後按一下**開啟**，以便從「收藏夾」下的「下載」中將其上載到CUCM。



上傳後，點選Import IdP Metadata將IdP資訊匯入CUCM。確認匯入成功，然後按一下「下一步」繼續。

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

選擇屬於「標準CCM超級使用者」的使用者，然後按一下「運行SSO測試」。

SAML Single Sign-On Configuration - Mozilla Firefox

https://cmpubhcsc.fhlab.com:8443/ccadmin/samlSingleSignOnConfigurationWizard3.do?server...


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

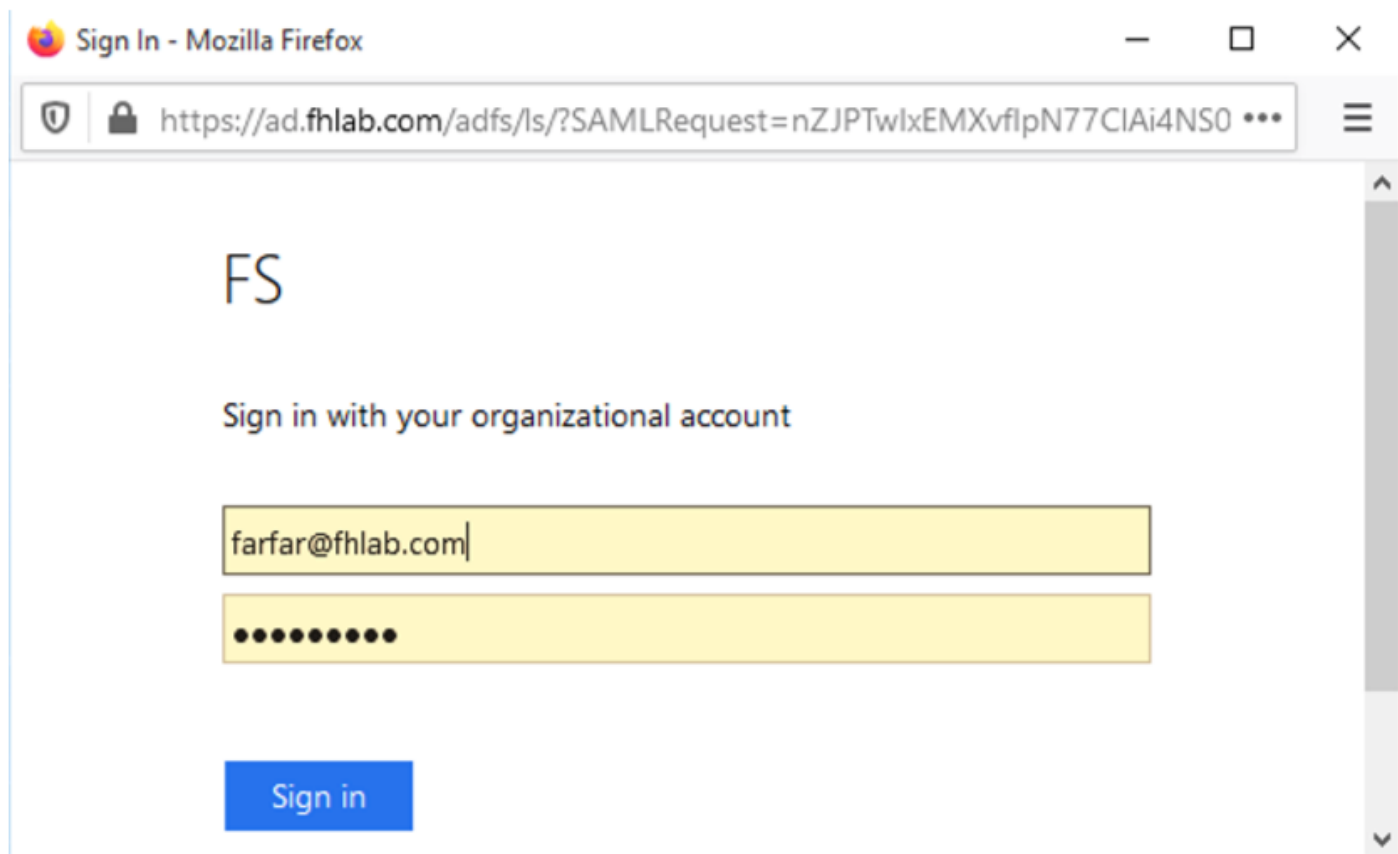
You must already know the password for the selected username. This user must have administrator rights and also exist in the IdP.

 Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

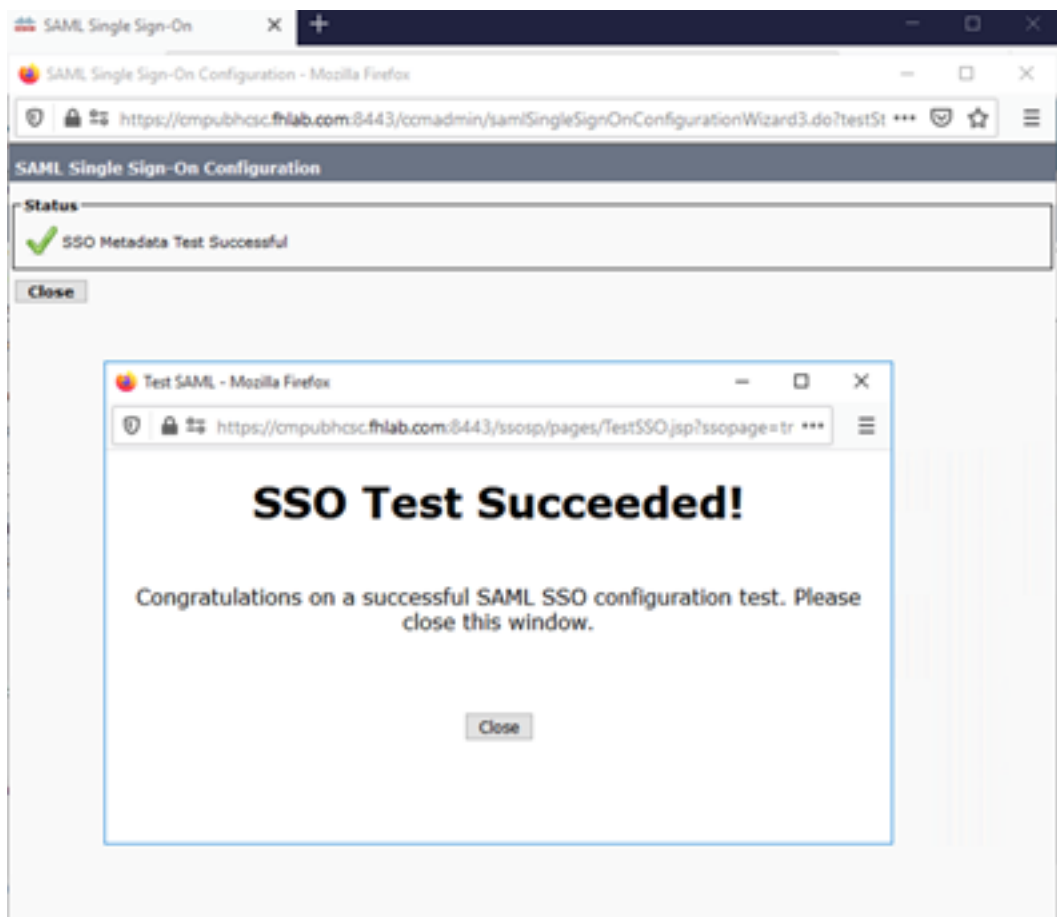
Valid administrator Usernames

2) Launch SSO test page

出現使用者身份驗證對話方塊時，使用相應的使用者名稱和密碼登入。



如果所有配置都正確，您應該會看到一條消息，指示SSO測試成功！



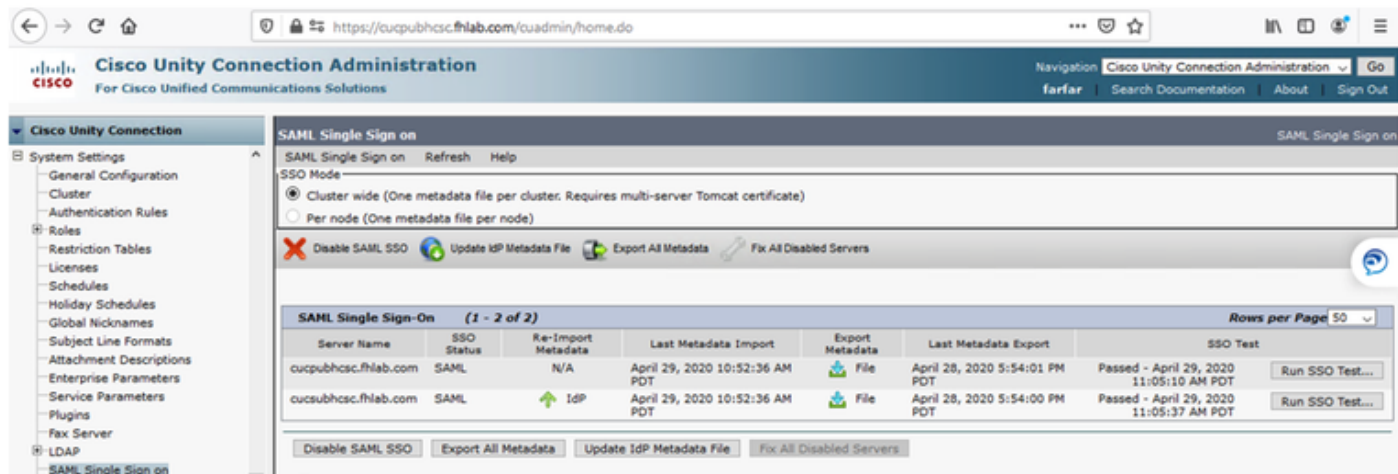
按一下「關閉」和「完成」繼續。

我們現在已成功完成使用ADFS在CUCM上啟用SSO的基本配置任務。

在CUC上配置SSO

在Unity Connection中啟用SSO的過程相同。

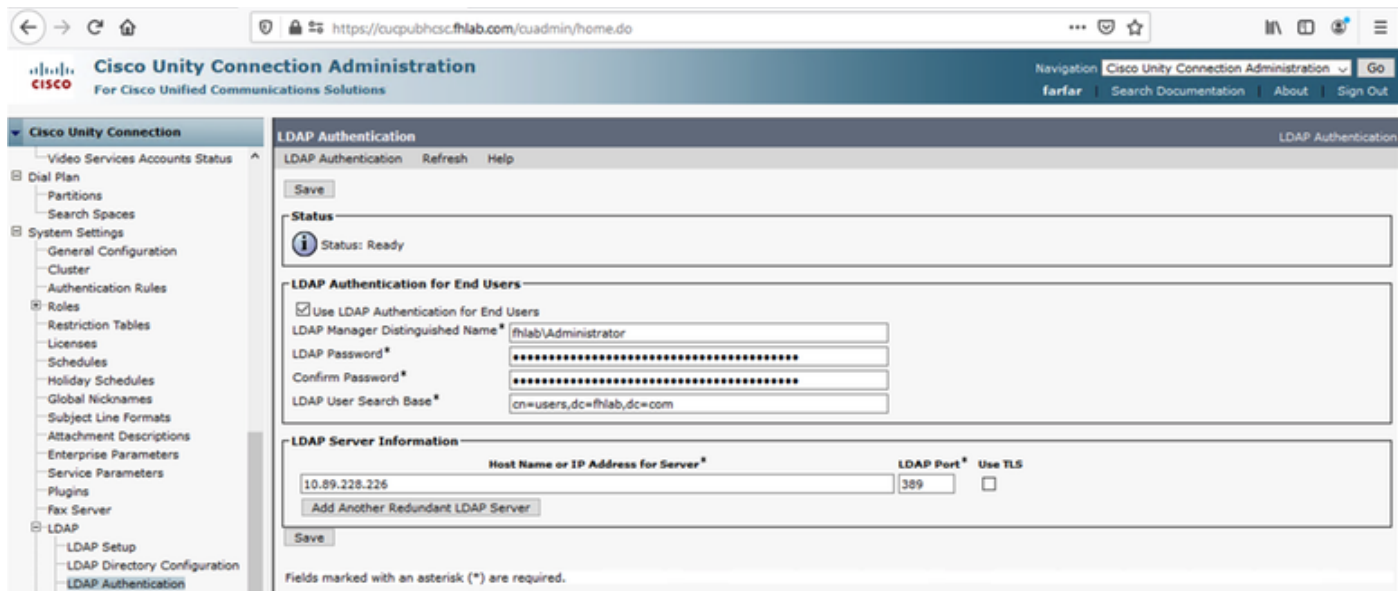
LDAP與CUC整合。



The screenshot displays the Cisco Unity Connection Administration web interface. The left sidebar shows the navigation menu with 'SAML Single Sign on' selected. The main content area is titled 'SAML Single Sign on' and includes a 'SSO Mode' section with two radio buttons: 'Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)' (selected) and 'Per node (One metadata file per node)'. Below this are buttons for 'Disable SAML SSO', 'Update IdP Metadata File', 'Export All Metadata', and 'Fix All Disabled Servers'. A table titled 'SAML Single Sign-On (1 - 2 of 2)' shows the configuration for two servers:

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cucpubhsc.fhlab.com	SAML	N/A	April 29, 2020 10:52:36 AM PDT	File	April 28, 2020 5:54:01 PM PDT	Passed - April 29, 2020 11:05:10 AM PDT
cucsubhsc.fhlab.com	SAML	IdP	April 29, 2020 10:52:36 AM PDT	File	April 28, 2020 5:54:00 PM PDT	Passed - April 29, 2020 11:05:37 AM PDT

配置LDAP身份驗證。



The screenshot displays the Cisco Unity Connection Administration web interface for LDAP Authentication. The left sidebar shows the navigation menu with 'LDAP Authentication' selected. The main content area is titled 'LDAP Authentication' and includes a 'Status' section showing 'Ready'. Below this is the 'LDAP Authentication for End Users' section with the following fields:

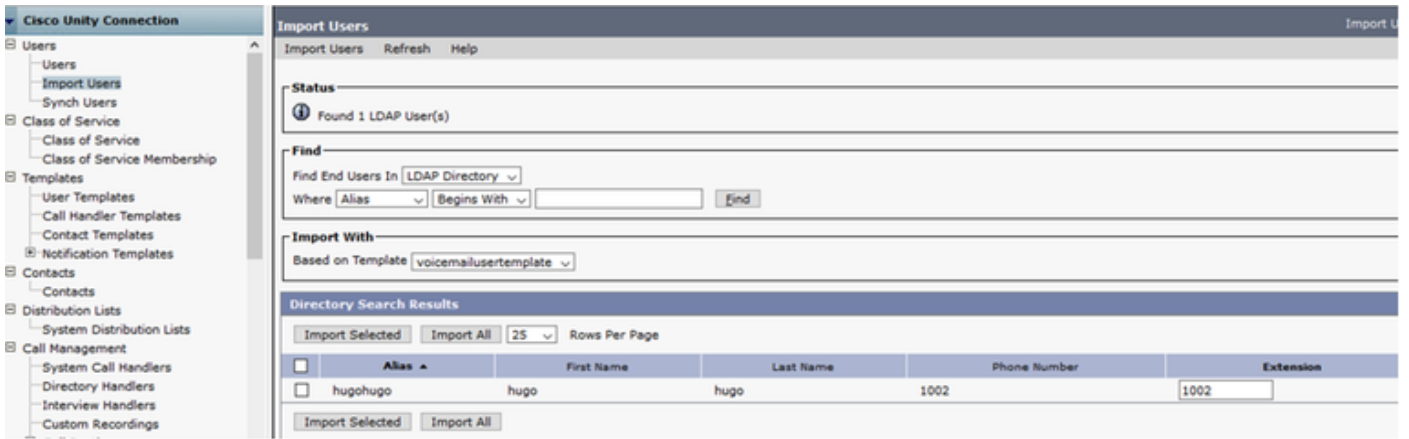
- Use LDAP Authentication for End Users
- LDAP Manager Distinguished Name*: fhlab\Administrator
- LDAP Password*: [Redacted]
- Confirm Password*: [Redacted]
- LDAP User Search Base*: cn=users,dc=fhlab,dc=com

The 'LDAP Server Information' section includes:

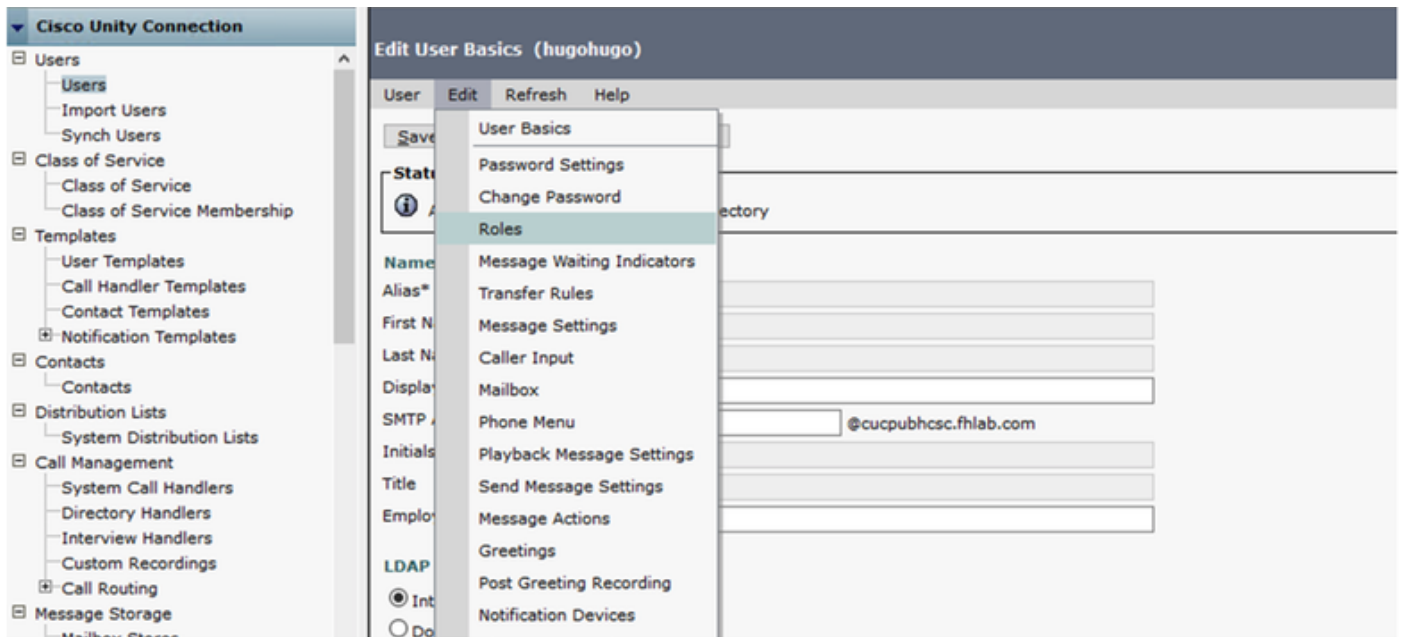
- Host Name or IP Address for Server*: 10.89.228.226
- LDAP Port*: 389
- Use TLS:

Buttons for 'Save' and 'Add Another Redundant LDAP Server' are visible. A note at the bottom states: 'Fields marked with an asterisk (*) are required.'

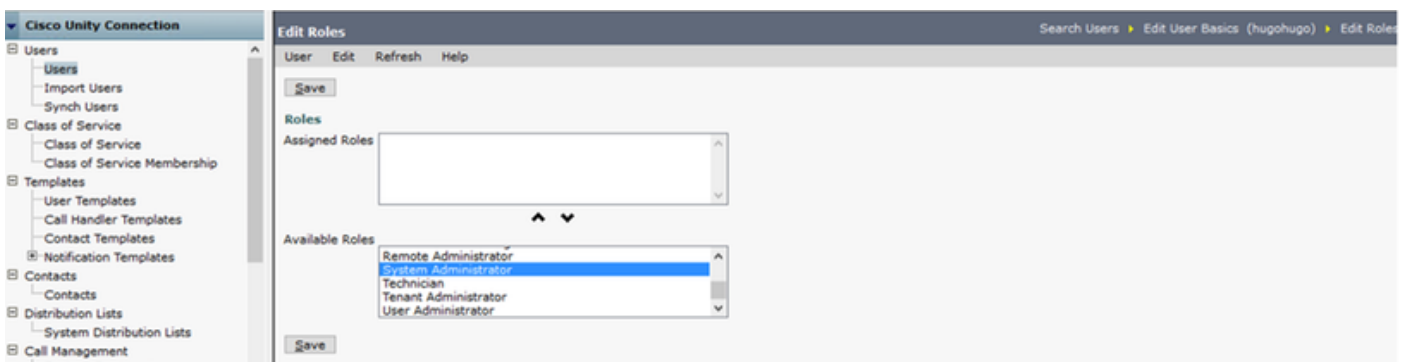
從LDAP匯入將分配語音郵件的使用者以及將用於測試SSO的使用者。



導覽至Users > Edit > Roles，如下圖所示。

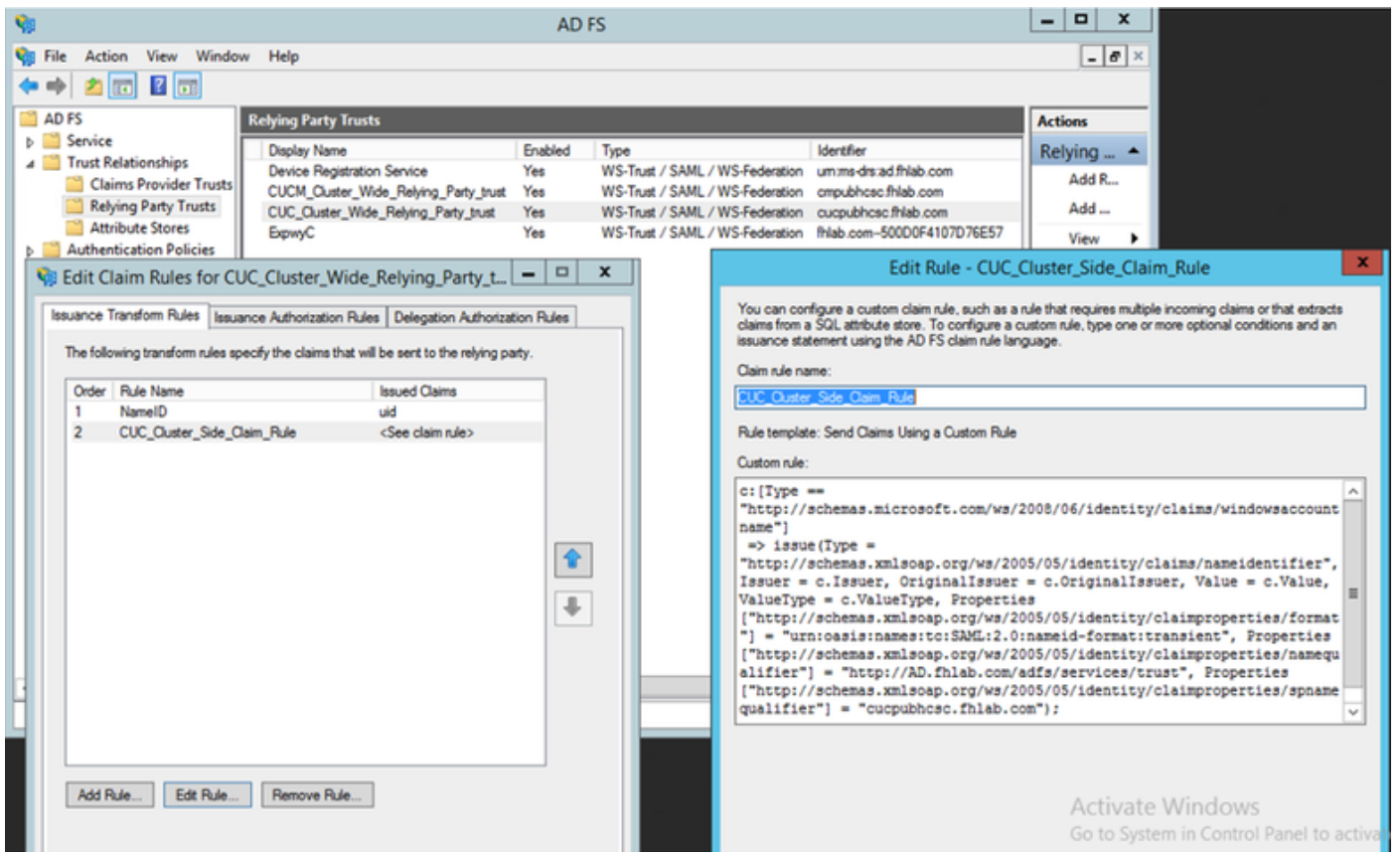


為測試使用者分配系統管理員角色。

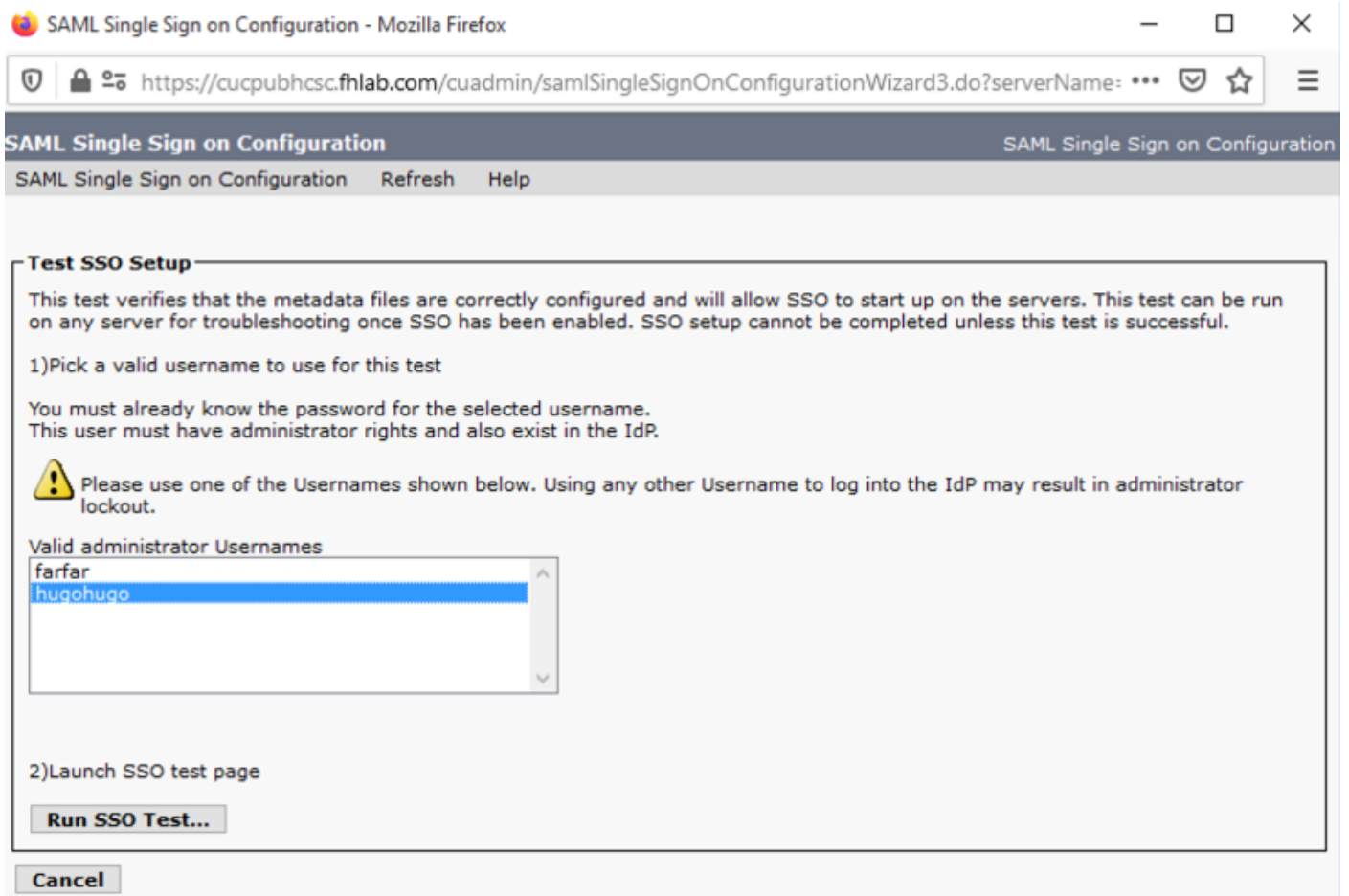


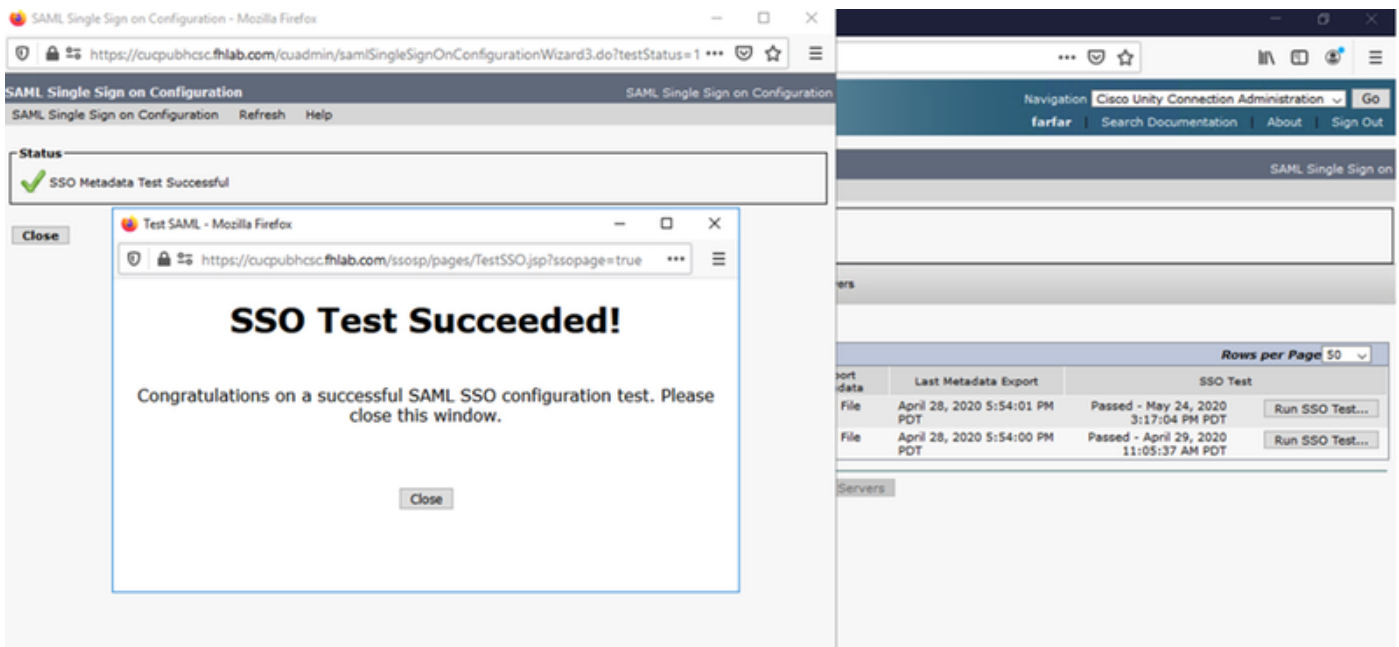
CUC後設資料

現在，您應該已經下載了CUC後設資料，為CUC建立了ReliingPartyTrust並上載了CUC後設資料，並在ADFS 3.0上建立了規則I AD FS



轉到SAML單一登入並啟用SAML SSO。





在Expressway上配置SSO

將後設資料匯入到Expressway C

開啟瀏覽器到<https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>，並將後設資料儲存到本地資料夾

上傳到Configuration > Unified Communications > IDP。

從Expressway C匯出後設資料

轉到配置 — > 統一通訊 — > IDP->匯出SAML資料

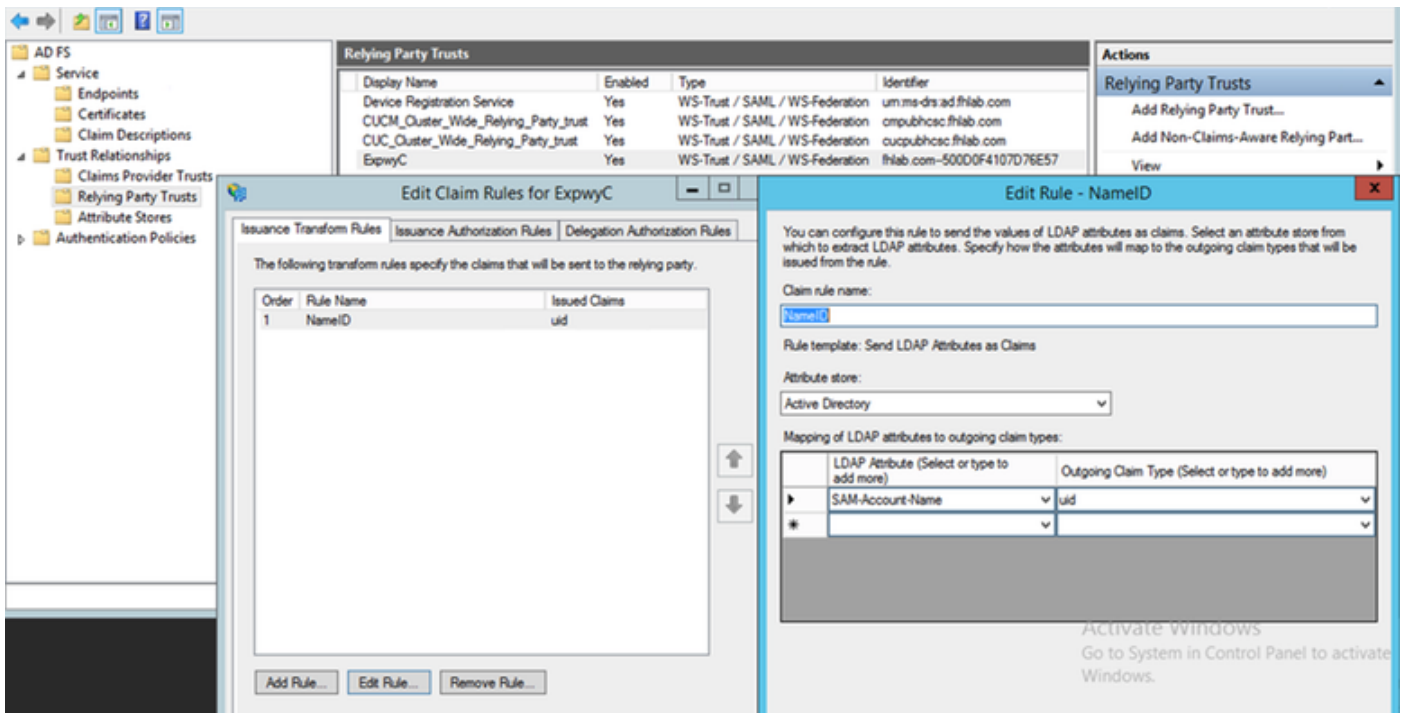
群集模式使用包含在SAML中的自簽名證書 (壽命長)

用於對SAML請求進行簽名的後設資料

- 在群集範圍模式下，要下載單個群集範圍後設資料檔案，請按一下「下載」
- 在每對等體模式下，要下載單個對等體的後設資料檔案，請按一下該對等體旁邊的Download。要全部匯出到.zip檔案，請按一下「全部下載」。

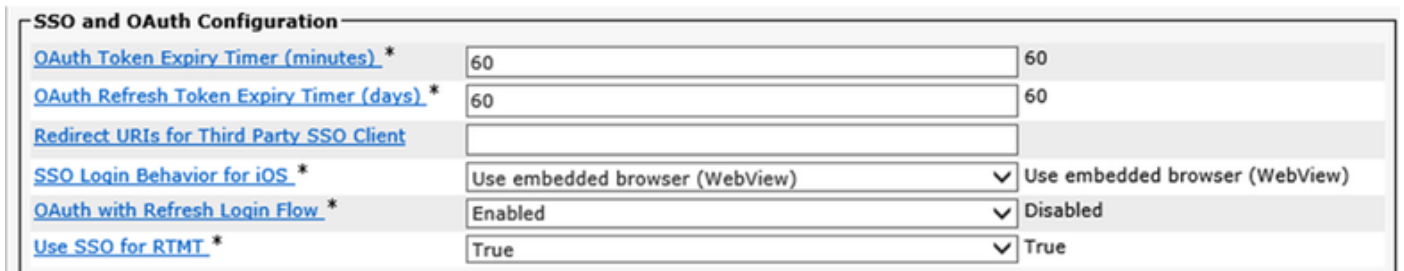
為Cisco Expressway-E新增信賴方信任

首先，為Expressway-Es建立信賴方信任，然後新增宣告規則以傳送標識作為UID屬性。

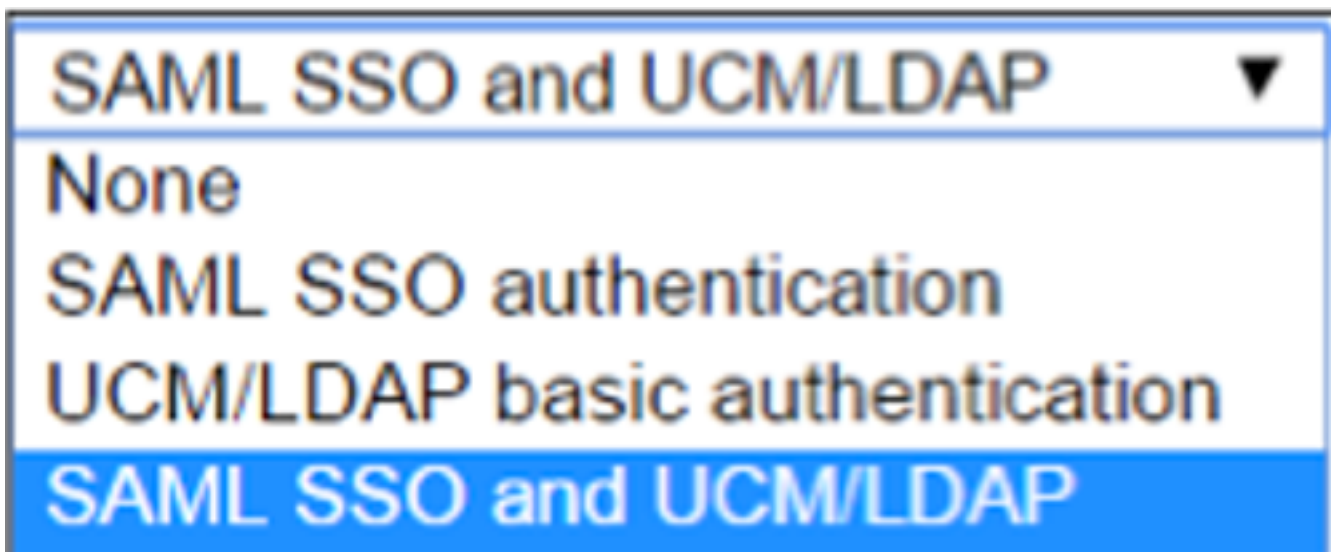


使用刷新登入的OAuth

在Cisco CUCM Enterprise Parameters中，啟用Verify OAuth with Refresh login flow引數。轉到Cisco Unified CM管理>企業引數>SSO和OAuth配置。



驗證路徑



- 如果身份驗證路徑設定為「SAML SSO身份驗證」，則只有使用啟用了SSO的Unified CM集群的Jabber客戶端才能在此Expressway上使用MRA。這是僅SSO配置。

- 對於所有IP電話、所有網真終端和駐留在未配置SSO的Unified CM集群上的任何Jabber客戶端，Expressway MRA支援都需要身份驗證路徑以包括UCM/LDAP身份驗證。
- 如果有一個或多個Unified CM集群支援Jabber SSO，請選擇「SAML SSO和UCM/LDAP」以允許SSO和基本身份驗證。

SSO架構

SAML是基於XML的開放式標準資料格式，使管理員能夠在登入到其中某個應用程式後無縫訪問一組已定義的思科合作應用程式。SAML SSO使用SAML 2.0協定為思科合作解決方案提供跨域和跨產品單點登入。

本地登入流程

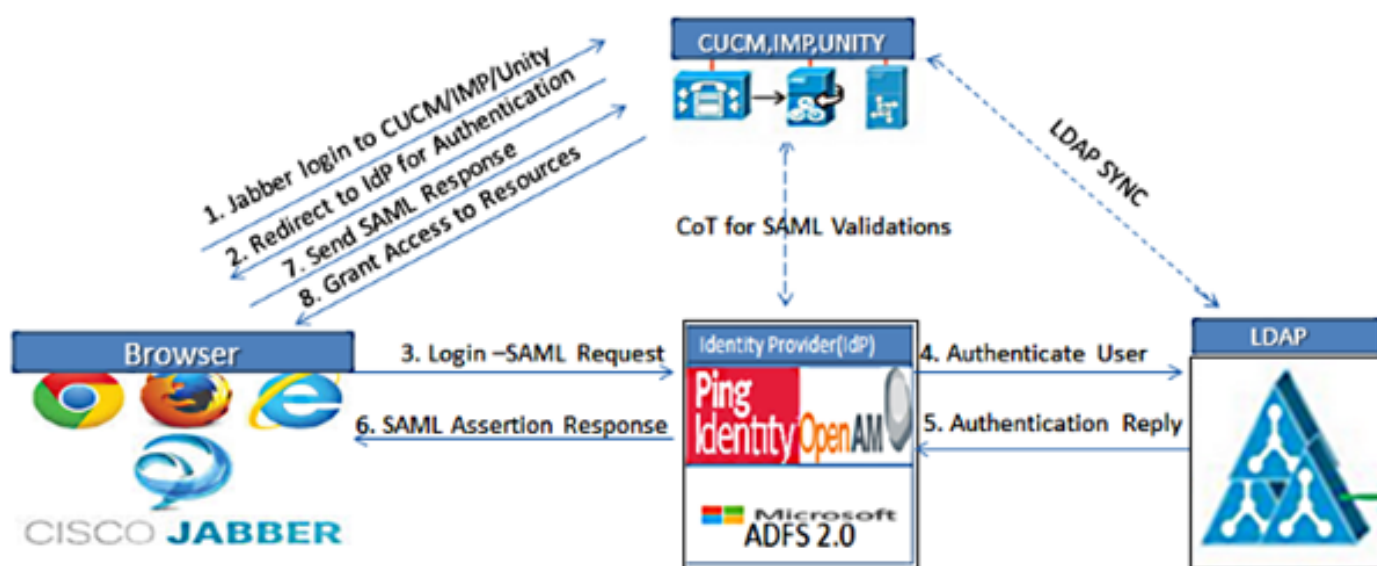
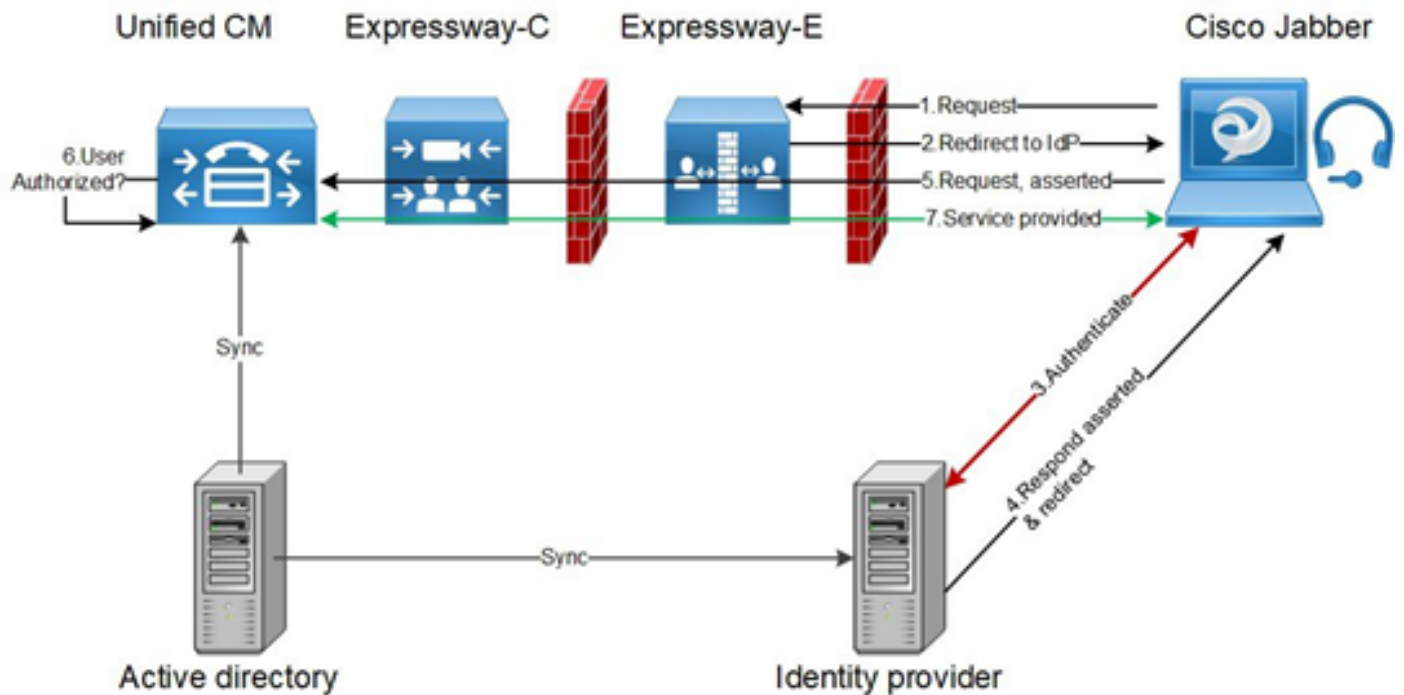


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

MRA登入流



OAuth

OAuth是一個支援授權的標準。使用者必須經過驗證才能獲得授權。授權碼授權流程為客戶端提供獲取訪問權杖和刷新權杖以訪問資源（Unified CM、IM&P、Unity和Expressway服務）的方法。此流程也基於重定向，因此需要客戶端能夠與使用者控制的HTTP使用者代理（Web瀏覽器）互動。客戶端將使用HTTPS向授權伺服器發出初始請求。OAuth伺服器將使用者重定向到身份驗證服務。如果啟用SAML SSO，則此操作可能在Unified CM或外部IdP上運行。根據所使用的認證方法，網頁檢視可能呈現給終端使用者以認證其自身。（Kerberos驗證是不顯示網頁的範例。）與隱式授予流程不同，成功的身份驗證代碼授予流程將導致OAuth伺服器向Web瀏覽器發出「授權碼」。這是一個一次性使用的短暫唯一代碼，然後從Web瀏覽器傳回客戶端。使用者端將這個「授權碼」與預先共用密碼一起提供到授權伺服器，並交換接收「存取權杖」和「刷新權杖」。在此步驟中使用的客戶端密碼使授權服務可以將使用限制為僅註冊和經過身份驗證的客戶端。令牌用於以下用途：

存取/刷新權杖

訪問令牌：此令牌由授權伺服器頒發。當客戶端需要訪問資源伺服器上的受保護資源時，向資源伺服器呈現令牌。資源伺服器能夠驗證該令牌並信任使用該令牌的連線。（思科訪問令牌的生存時間預設為60分鐘）

刷新令牌：授權伺服器再次發出此令牌。當訪問令牌已過期或即將過期時，客戶端將此令牌與客戶端金鑰一起提供給授權伺服器。如果刷新令牌仍然有效，則授權伺服器將頒發新的訪問令牌，而無需其他身份驗證。（思科刷新令牌的生存期預設為60天）。如果刷新令牌已過期，則必須啟動新的完整OAuth授權代碼授予流程以獲取新令牌。

OAuth授權代碼授權流程更好

在隱式授予流程中，訪問令牌通過HTTP使用者代理（瀏覽器）傳遞到Jabber客戶端。在授權碼授權流程中，訪問令牌直接在授權伺服器和Jabber客戶端之間交換。使用時間限制的唯一授權碼從授權伺服器請求令牌。這種直接交換訪問令牌更加安全並且減少了風險。

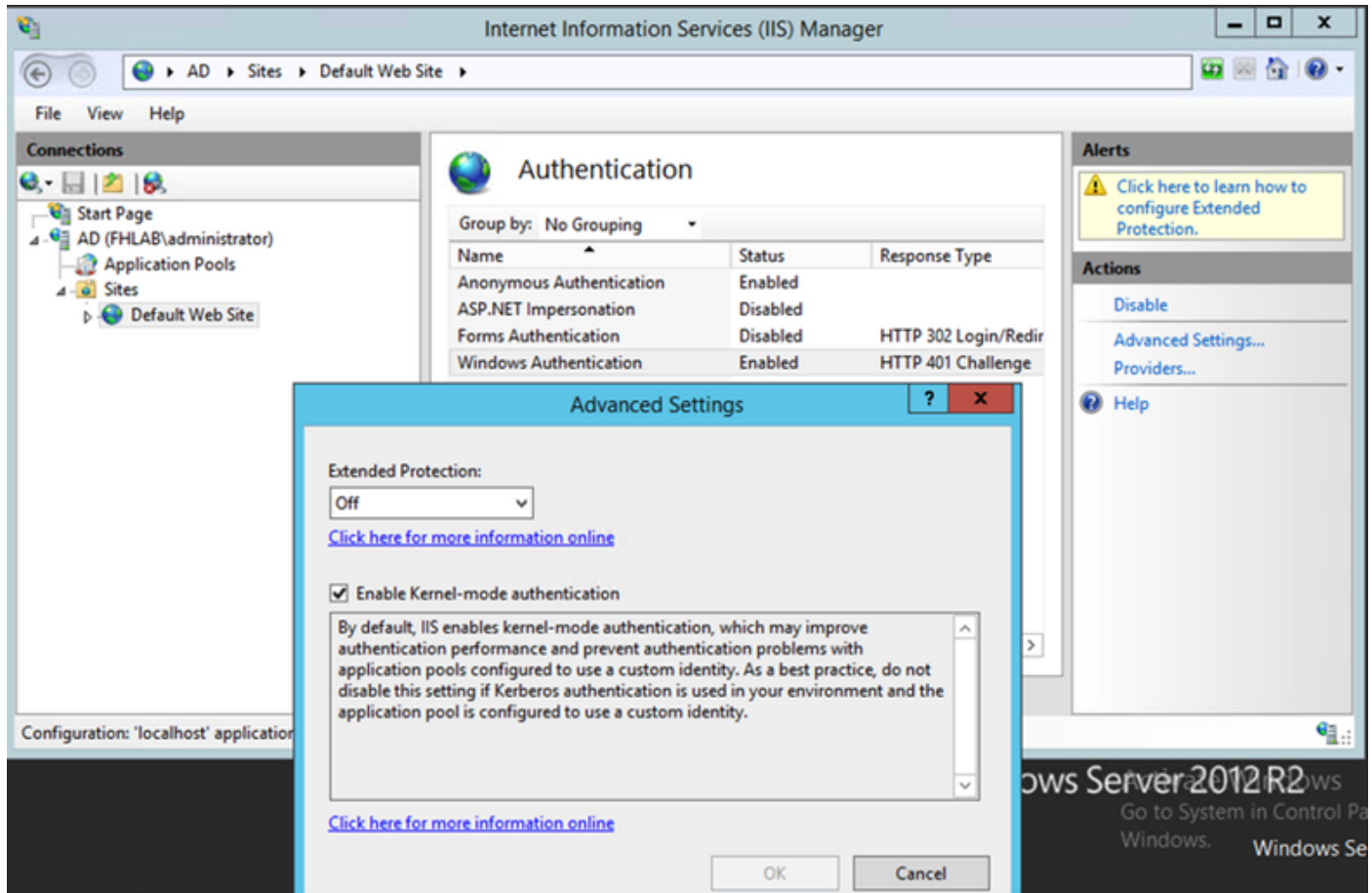
OAuth授權代碼授予流程支援使用刷新令牌。這可以為終端使用者提供更好的體驗，因為他們不需要頻繁地重新進行身份驗證（預設情況下為60天）

配置Kerberos

選擇Windows身份驗證

Internet資訊服務(IIS)管理器>站點>預設網站>身份驗證> Windows身份驗證>高級設定。

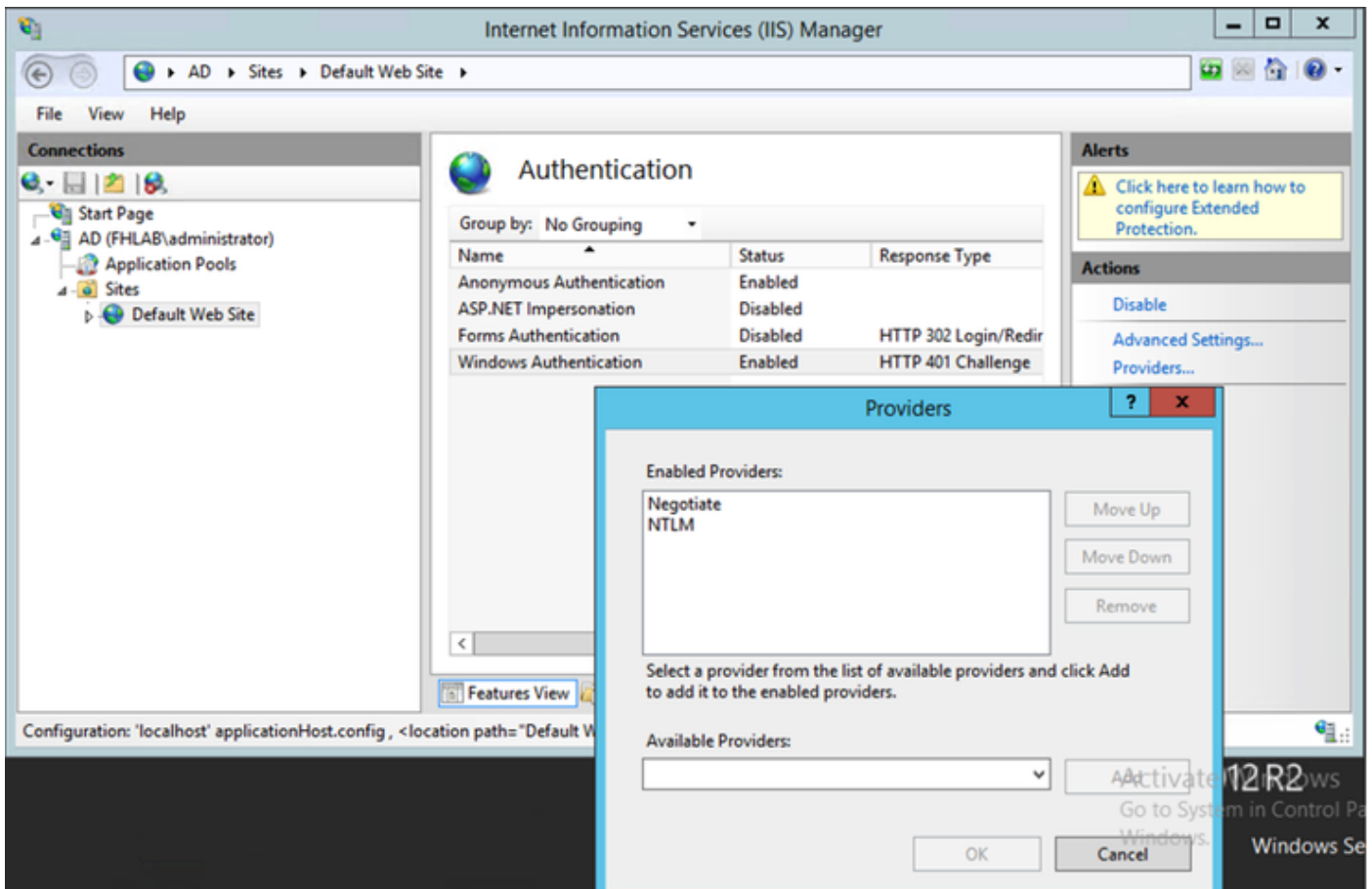
1. 取消選中Enable Kernel-mode authentication。
2. 確保已關閉擴展保護。



ADFS同時支援Kerberos NTLM

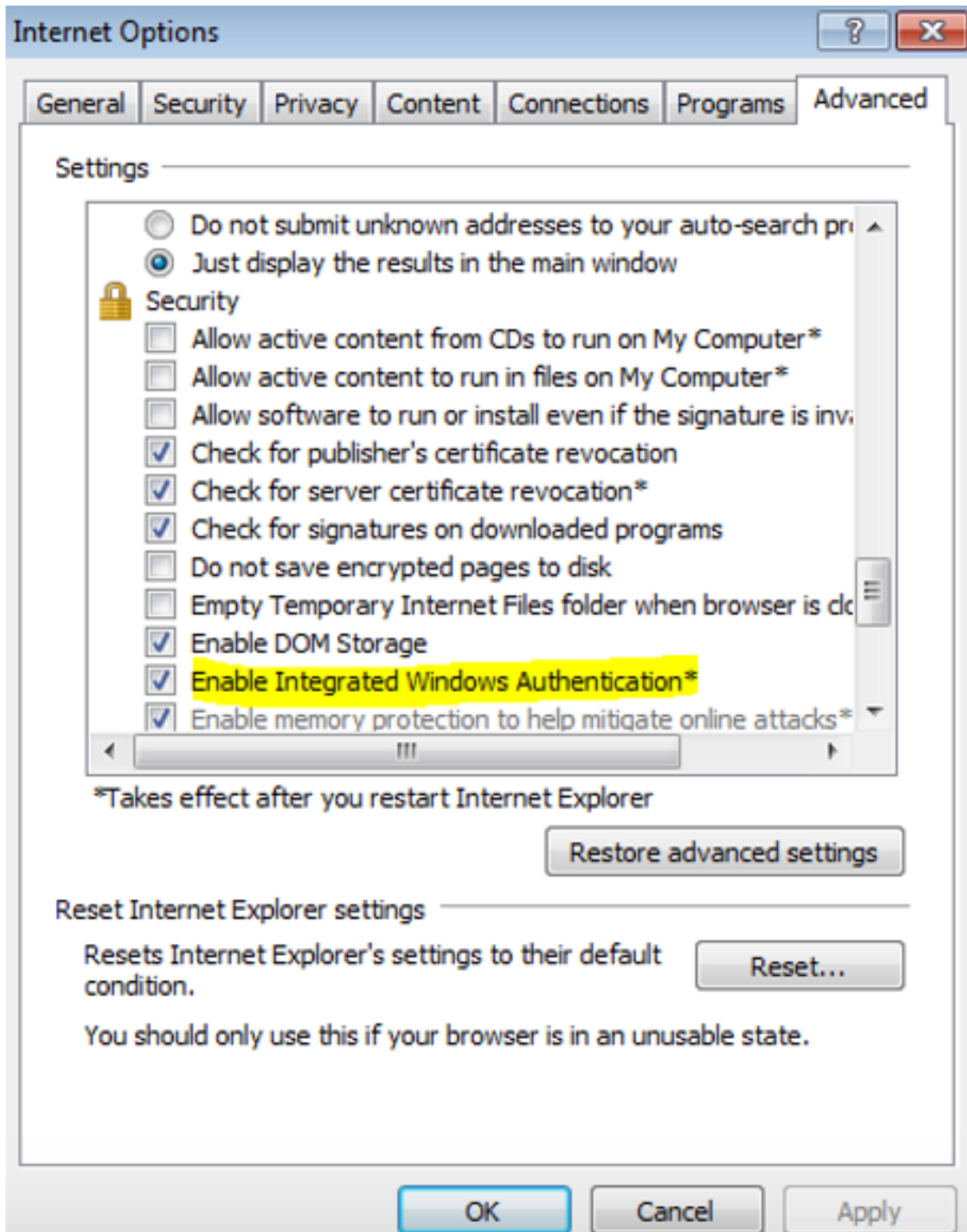
確保AD FS版本3.0同時支援Kerberos協定和NT LAN Manager(NTLM)協定，因為所有非Windows客戶端都不能使用Kerberos並依賴NTLM。

在右窗格中，選擇Providers (提供程式)，並確保Negotiate and NTLM出現在Enabled Providers (已啟用提供程式) 下：



配置Microsoft Internet Explorer

確保選中Internet Explorer > Advanced > Enable Integrated Windows Authentication。



在Security > Intranet zones > Sites下新增ADFS URL

