

# 使用AD FS版本2.0為每個群集配置單個SAML IdP連線/協定

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[步驟1.從CUCM匯出SP後設資料](#)

[步驟2.從AD FS下載IDP後設資料](#)

[步驟3.設定IdP](#)

[步驟4.啟用SAML SSO](#)

[驗證](#)

[疑難排解](#)

## 簡介

本文檔介紹如何使用Active Directory聯合身份驗證服務(AD FS)為每個群集配置單一安全斷言標籤語言(SAML)身份提供程式(IdP)連線/協定。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Cisco Unified Communications Manager(CUCM)11.5或更高版本
- Cisco Unified Communications Manager IM and Presence版本11.5或更高版本
- Active Directory聯合身份驗證服務版本2.0

### 採用元件

本檔案中的資訊是根據以下軟體版本：

- 作為IdP的Active Directory聯合身份驗證服務版本2.0
- 思科整合通訊管理員版本11.5
- Cisco IM和狀態伺服器版本11.5

## 背景資訊

對於SAML SSO，需要在服務提供商(SP)和IdP之間形成一個信任圈。當交換信任（後設資料）時

，此信任作為SSO啟用的一部分建立。從CUCM下載後設資料並將其上傳到IdP，同樣，從IdP下載後設資料並將其上傳到CUCM。

在CUCM 11.5之前的版本中，始發節點生成後設資料檔案，同時從集群中的其他節點收集後設資料檔案。它將所有後設資料檔案新增到單個zip檔案，然後呈現給管理員。管理員必須解壓縮此檔案並在IdP上預配每個檔案。例如，8個節點群集的8個後設資料檔案。

每個集群的單個SAML IdP連線/協定功能是從11.5引入的。作為此功能的一部分，CUCM為集群中的所有CUCM和IMP節點生成單個服務提供商後設資料檔案。後設資料檔案的新名稱格式為  
<hostname>-single-agreement.xml

基本上，一個節點建立後設資料並將其推送到群集中的其他SP節點。這可實現輕鬆的配置、維護和管理。例如，8節點群集有1個後設資料檔案。

群集範圍的後設資料檔案使用Multiserver tomcat證書，該證書確保群集中所有節點使用的金鑰對相同。後設資料檔案還包含群集中每個節點的斷言使用者服務(ACS)URL清單。

CUCM和Cisco IM and Presence版本11.5支援SSO模式、**群集範圍**（每個集群一個後設資料檔案）和每個節點（現有模型）。

本文檔介紹如何使用AD FS 2.0配置SAML SSO的群集範圍模式。

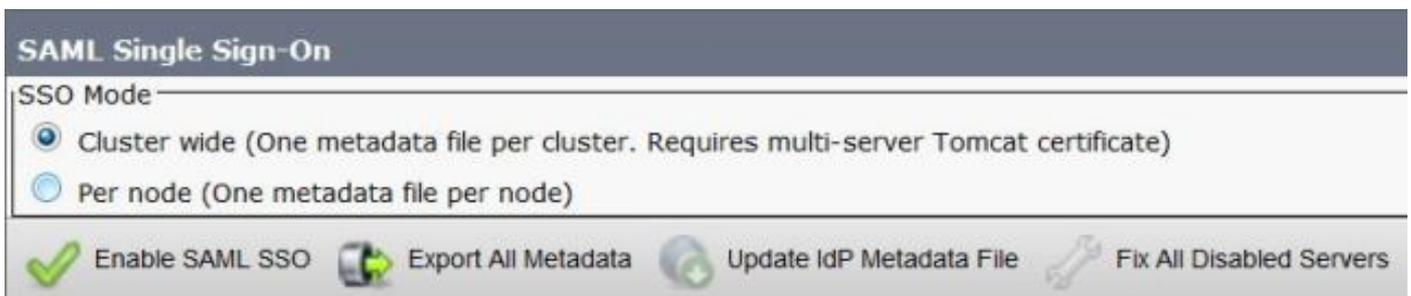
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 設定

### 步驟1.從CUCM匯出SP後設資料

開啟Web瀏覽器，以管理員身份登入到CUCM，然後導覽至System > SAML Single Sign On。

預設情況下，Cluster Wide單選按鈕處於選中狀態。按一下匯出所有後設資料。以名稱 <hostname>-single-agreement.xml向管理員顯示的後設資料資料檔案



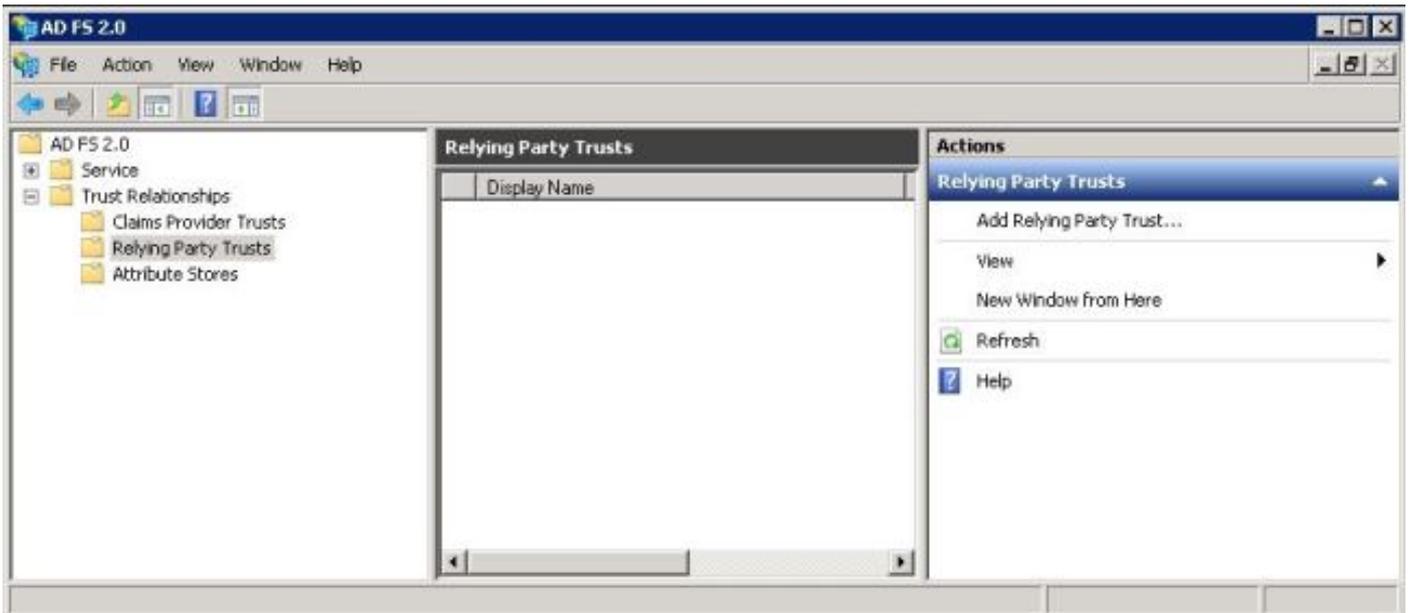
### 步驟2.從AD FS下載IDP後設資料

要下載IdP後設資料，請參閱連結[https:// <ADFS的FQDN>/federationmetadata/2007-06/federationmetadata.xml](https://<ADFS的FQDN>/federationmetadata/2007-06/federationmetadata.xml)

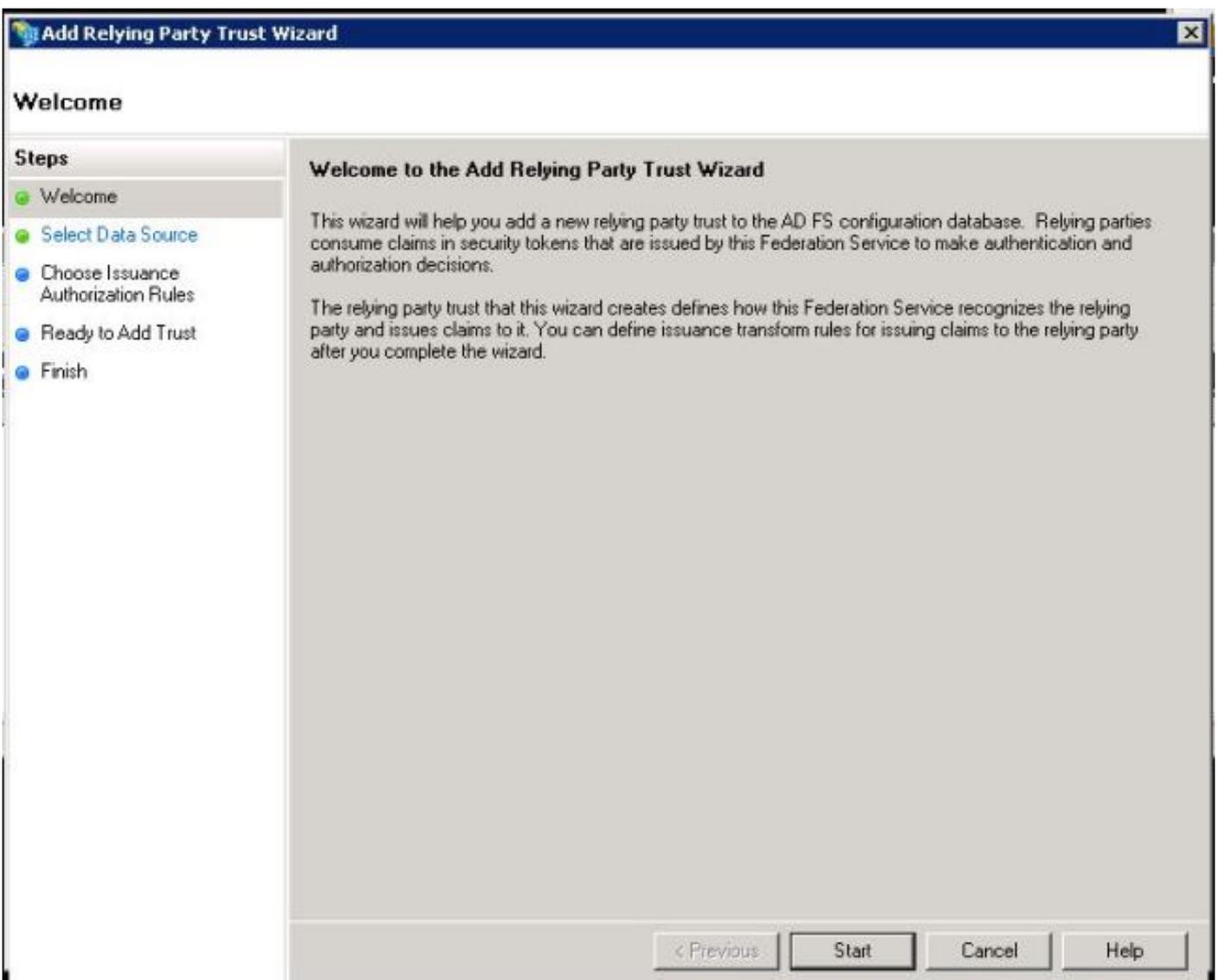
### 步驟3.設定IdP

如圖所示，導航到AD FS 2.0 Management/Trust Relationship Ships/Reliding Party trust。按一下新

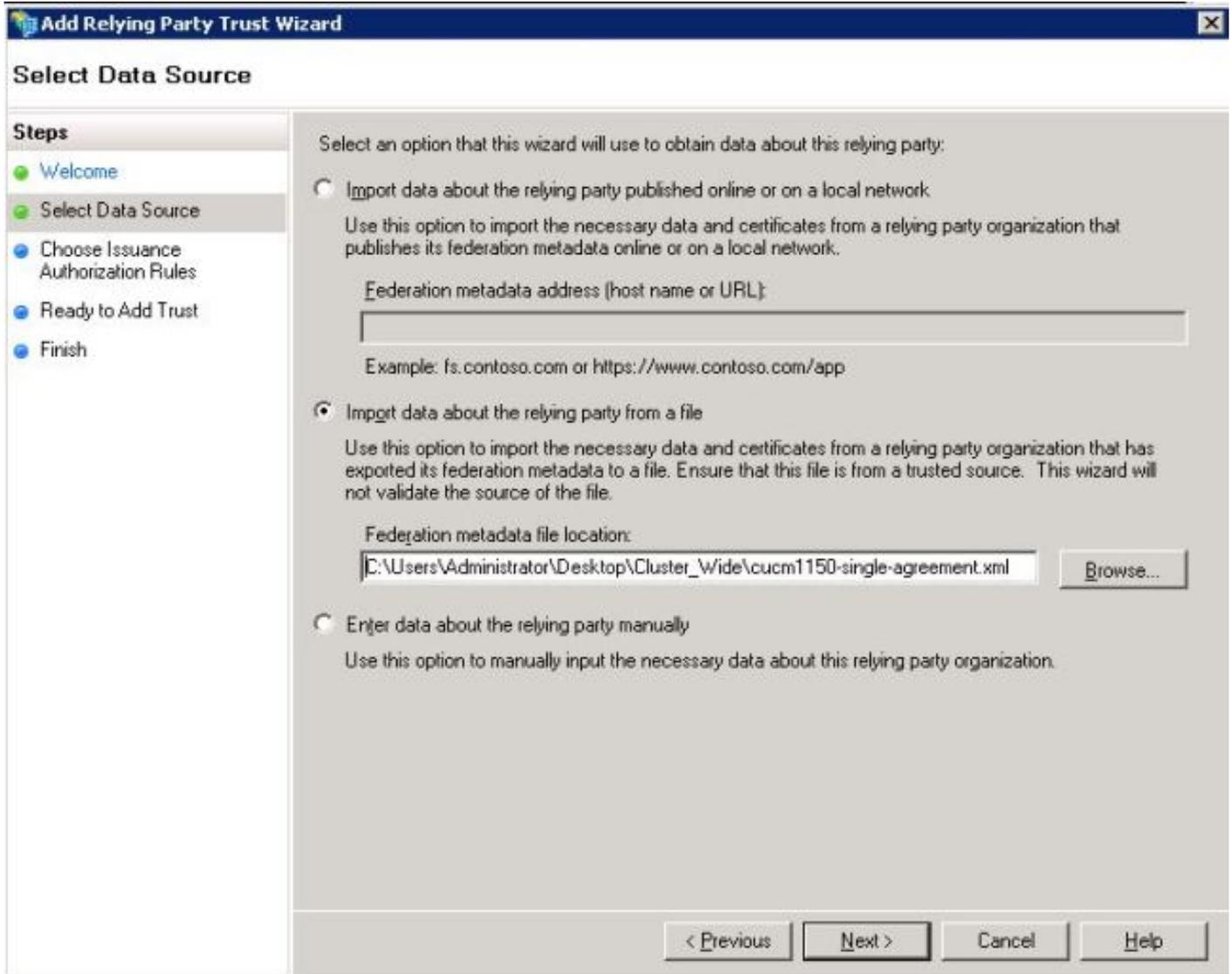
增信賴方信任。



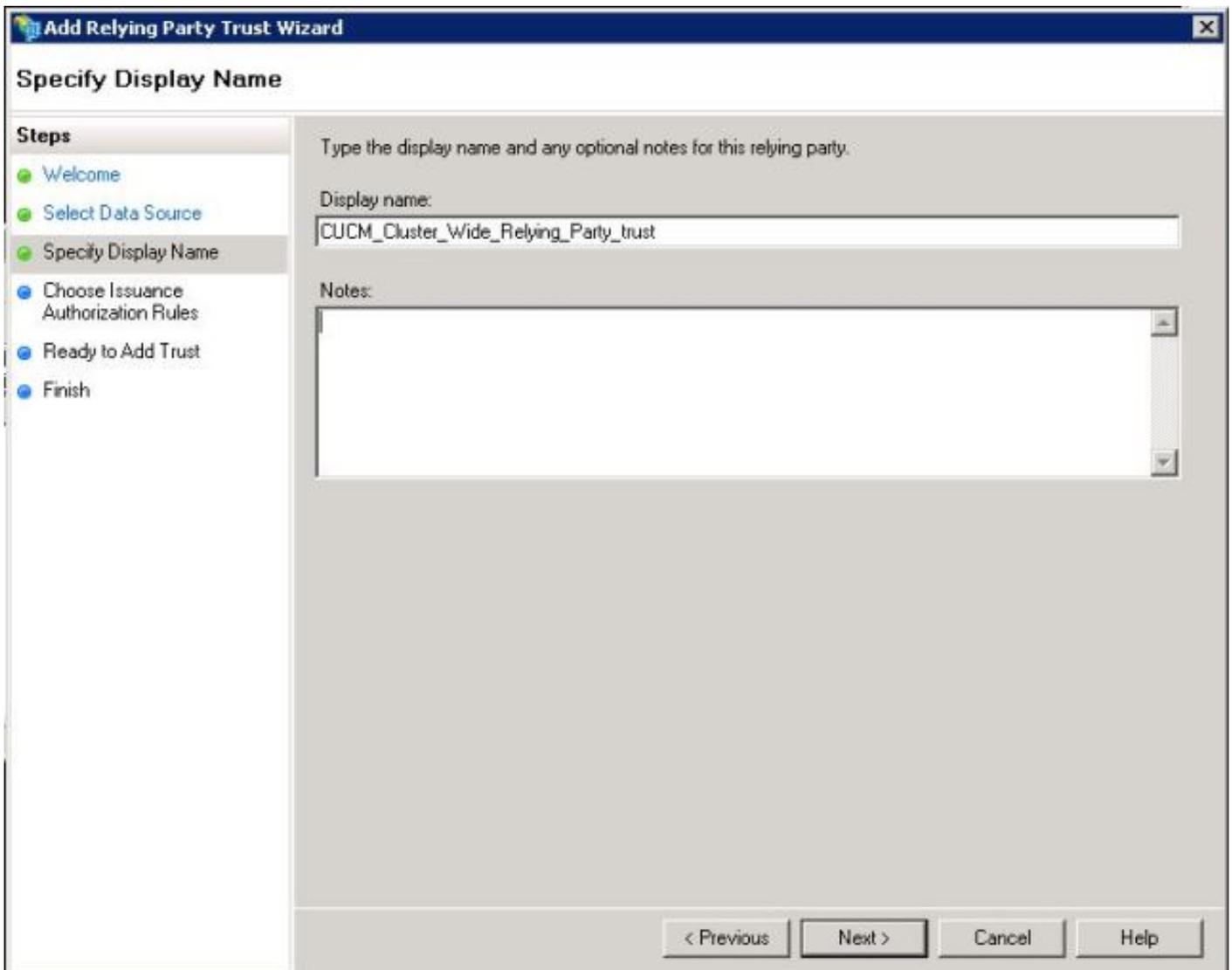
將開啟「新增信賴方信任嚮導」（如圖所示），然後按一下「開始」。



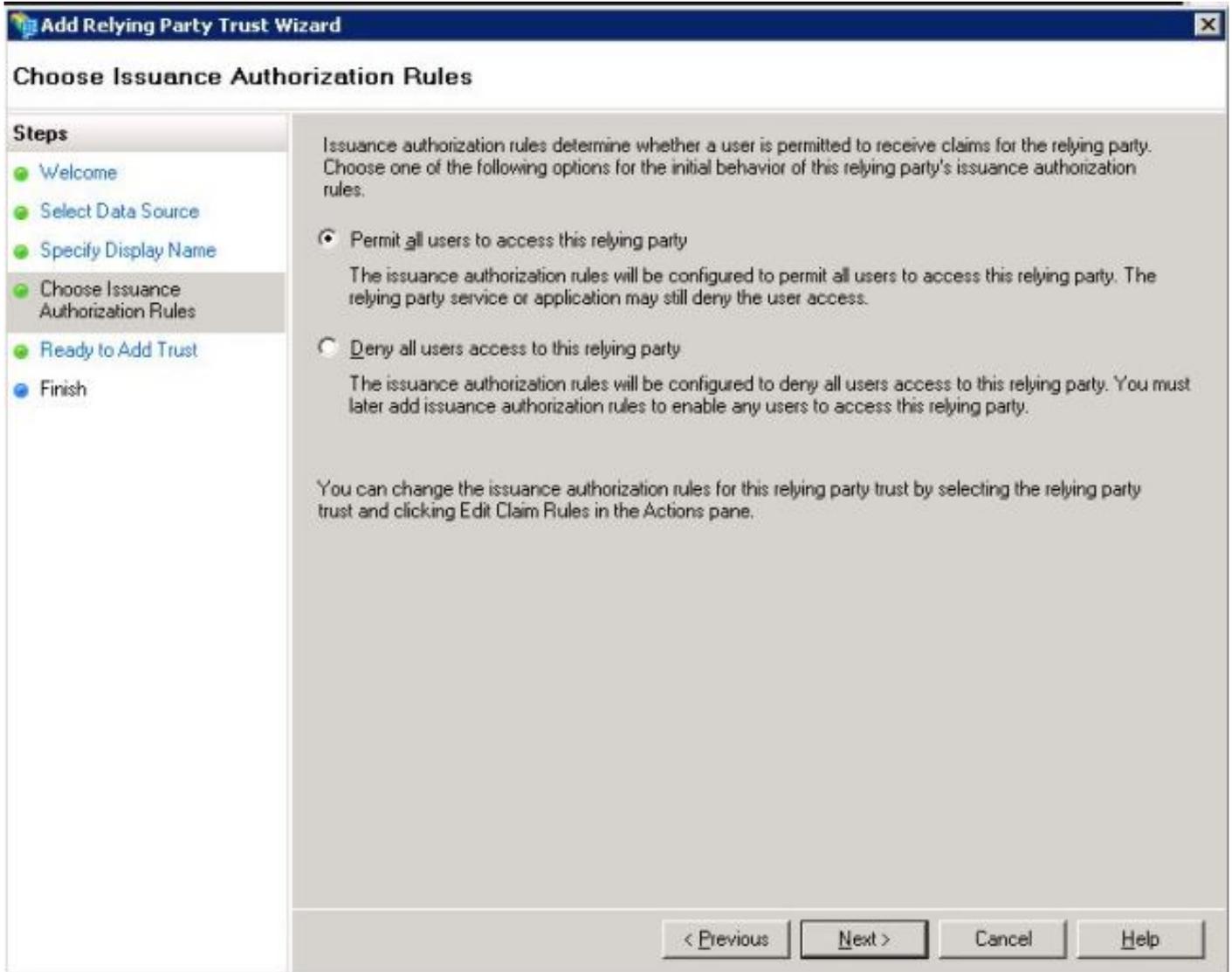
從檔案中按一下有關信賴方的匯入資料。瀏覽從CUCM SAML SSO配置頁下載的SP後設資料。然後按一下「Next」，如下圖所示：



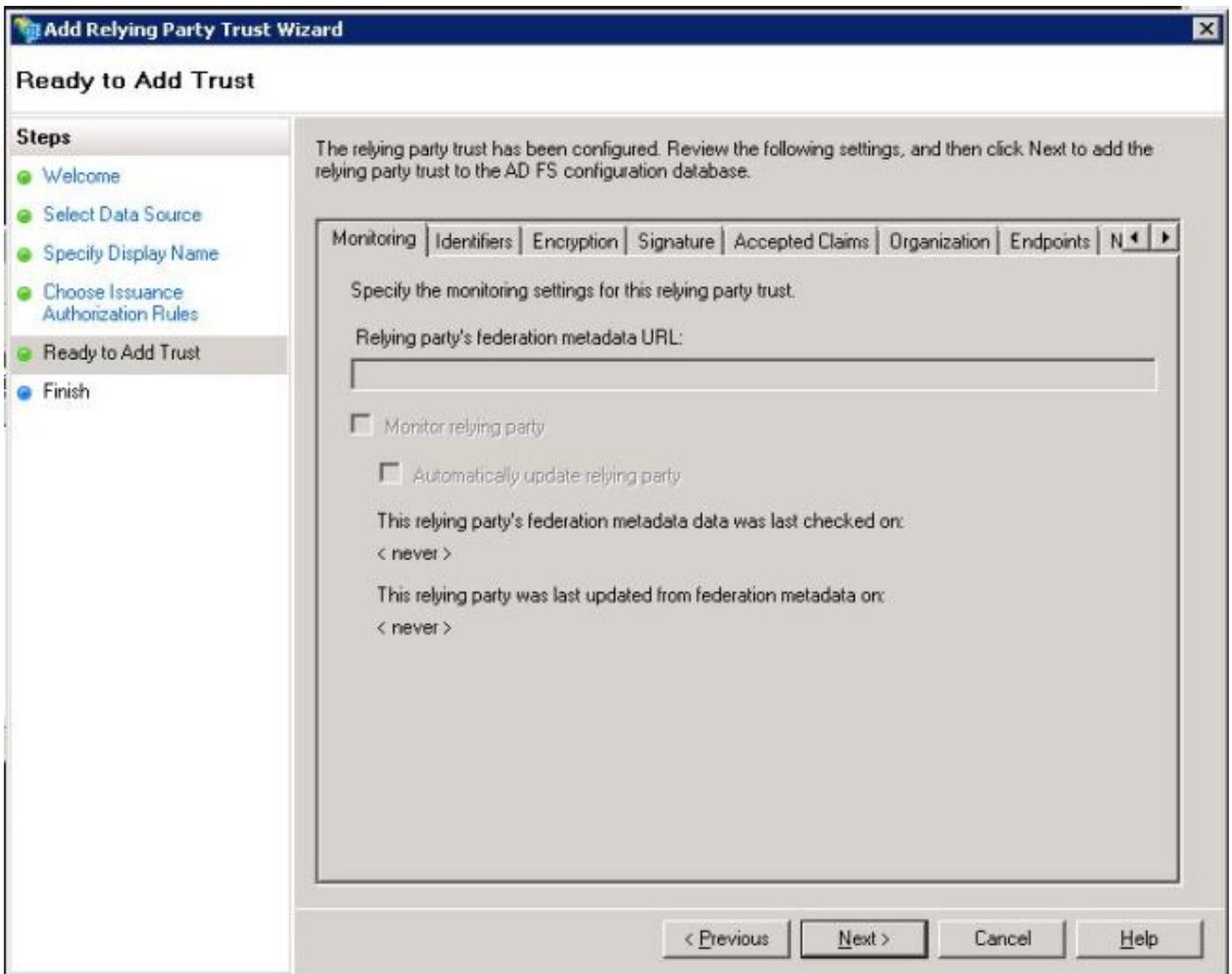
鍵入信賴方的顯示名稱和任何可選註釋。按一下「Next」，如下圖所示：



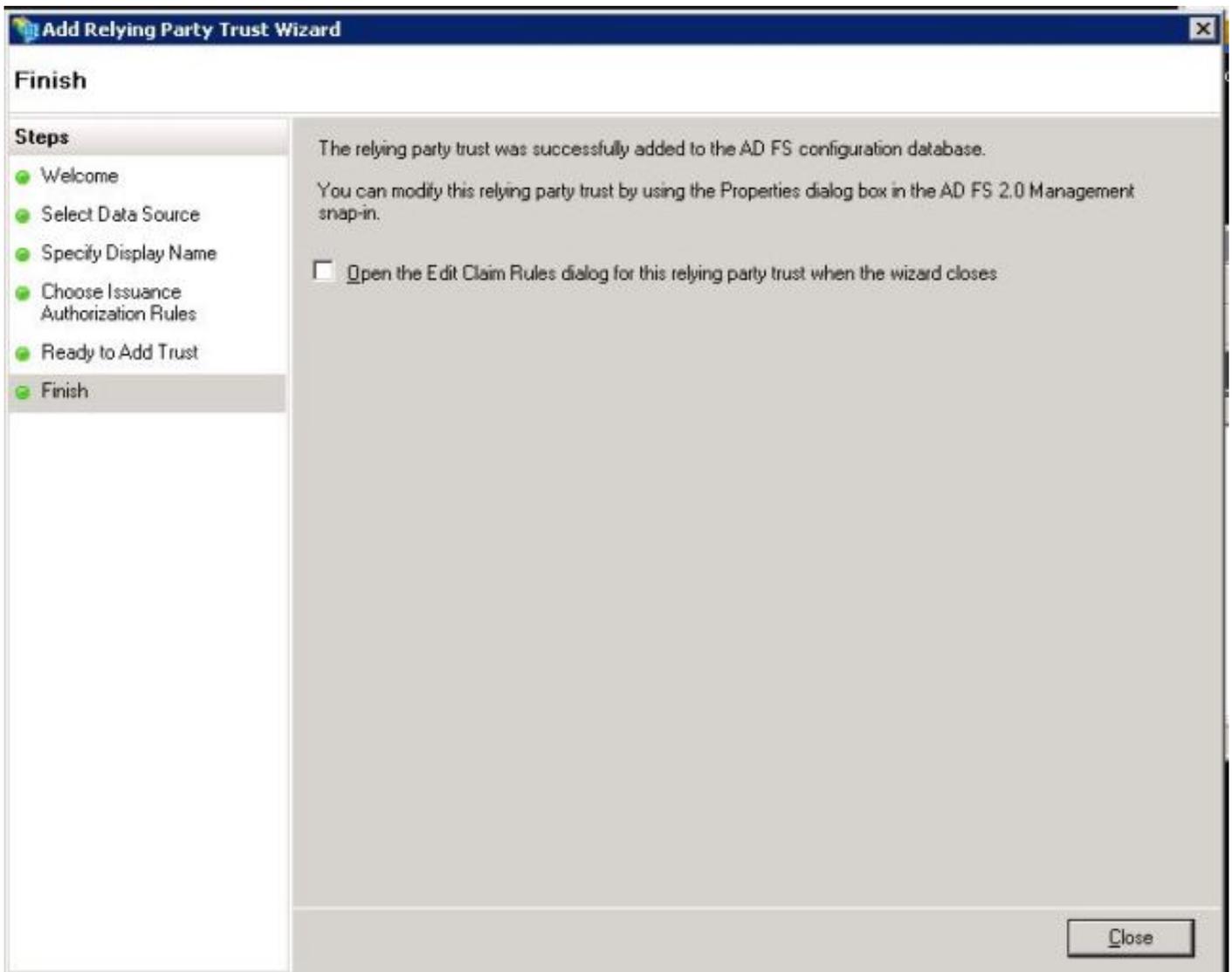
選擇允許所有使用者訪問此信賴方以允許所有使用者訪問此信賴方，然後按一下下一步，如下圖所示：



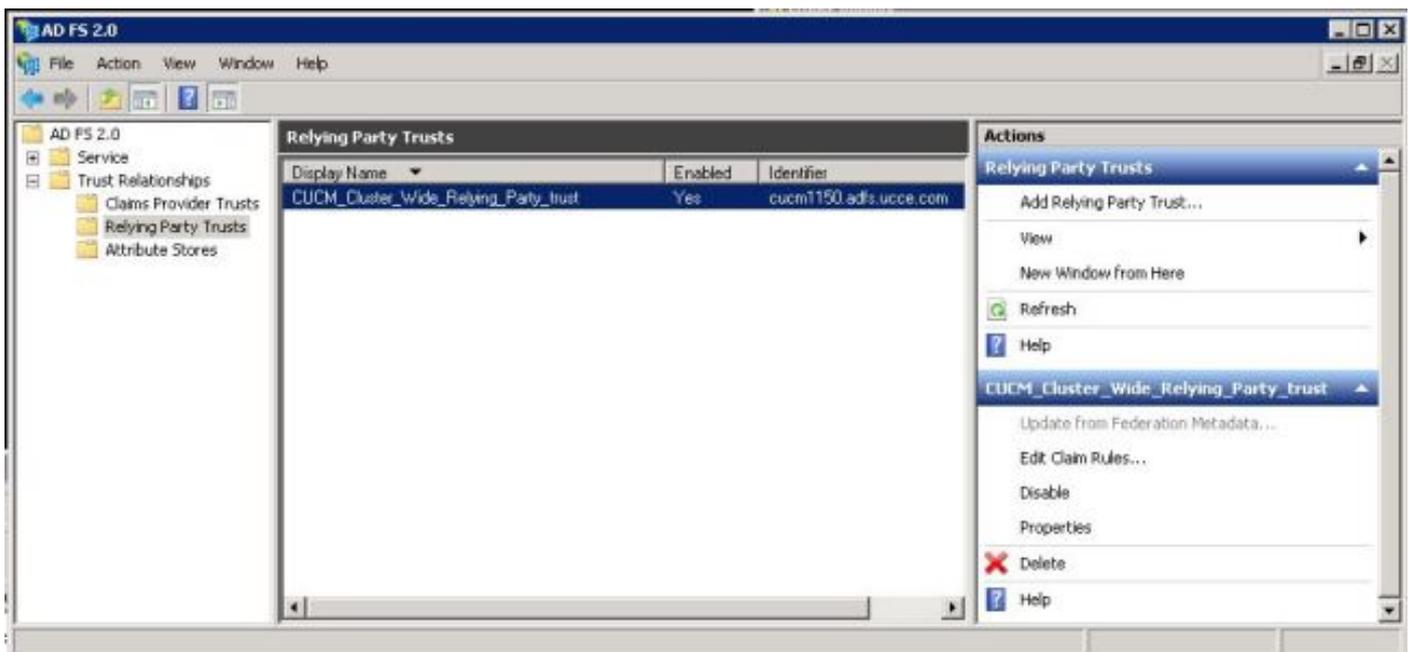
在Ready to Add Trust頁面下，您可以檢視已配置的信賴方信任的設定。現在按一下Next，如下圖所示：



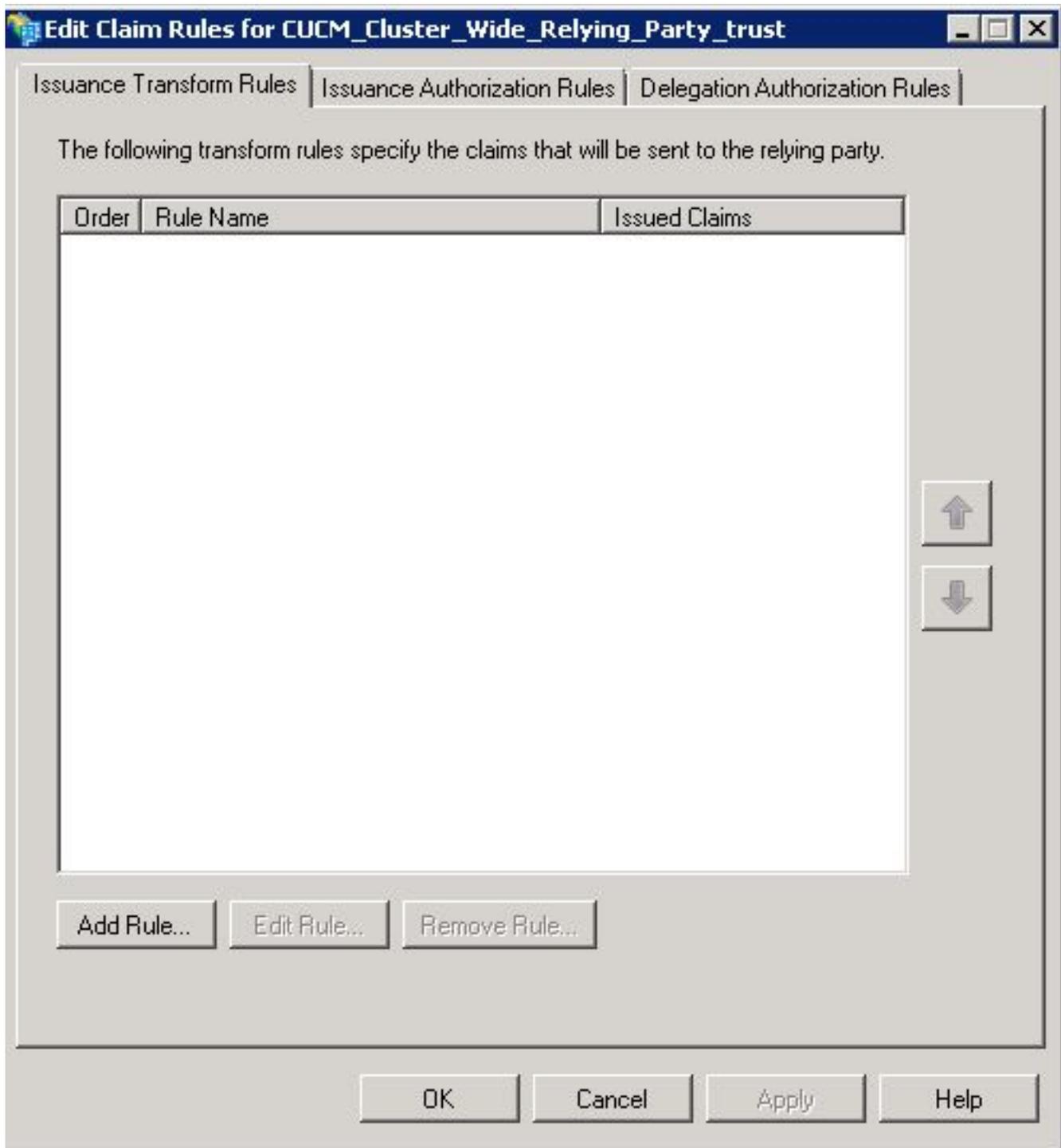
完成頁確認信賴方信任已成功新增到AD FS配置資料庫。取消選中該框並按一下**Close**，如下圖所示：



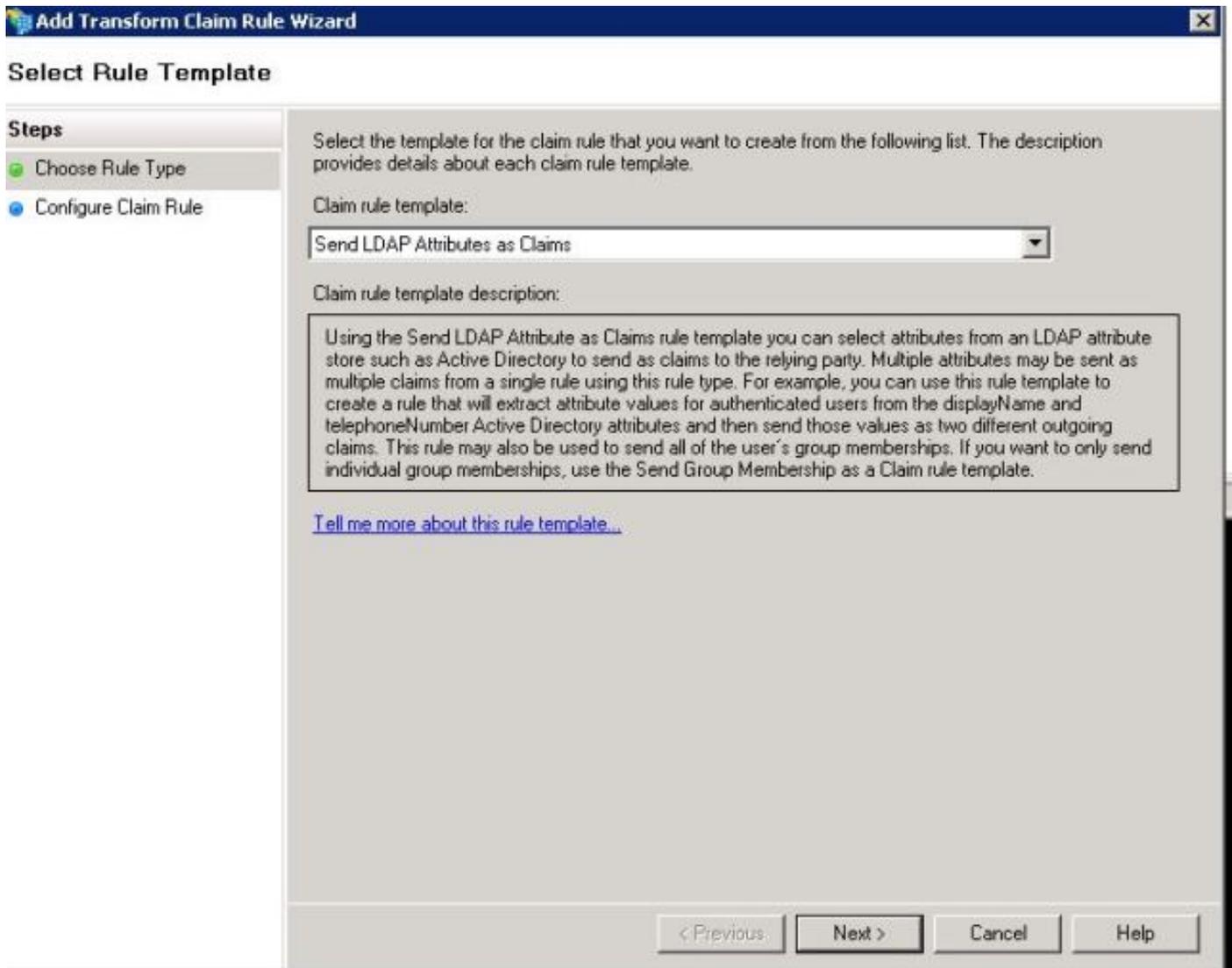
按一下右鍵信賴方信任，然後按一下編輯宣告規則，如下圖所示：



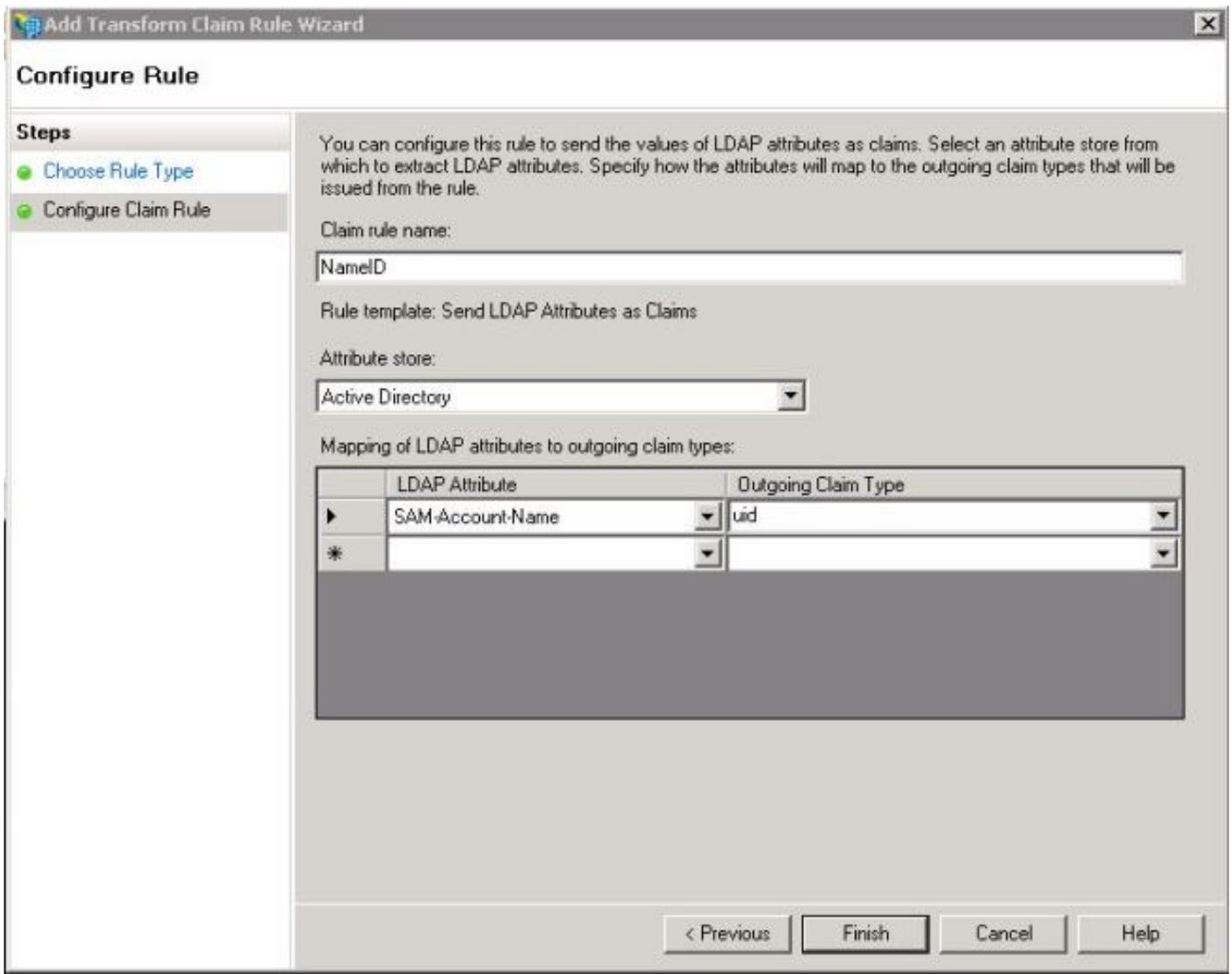
現在，按一下「Add Rule」，如下圖所示：



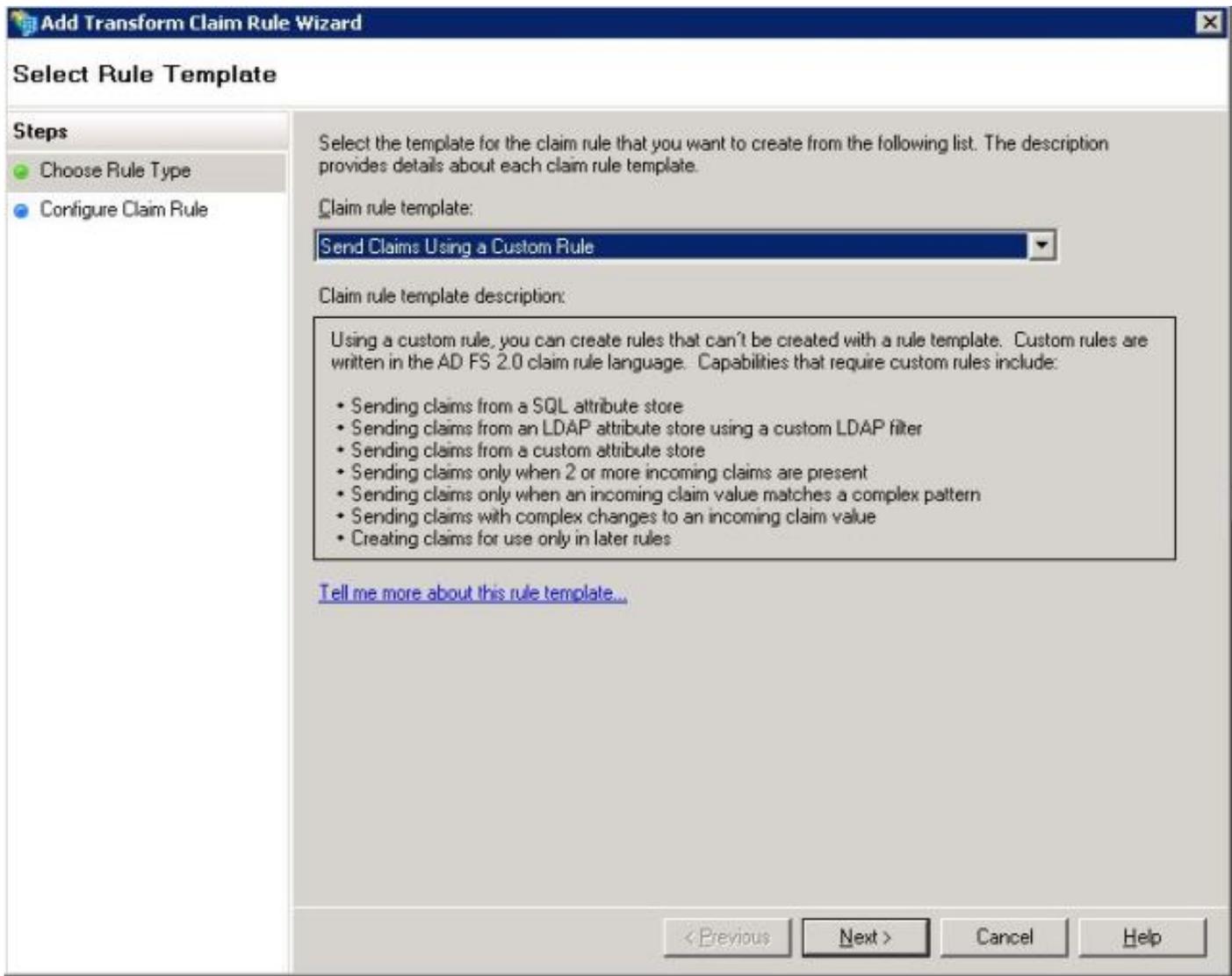
開啟Add Transform Claim Rule後，使用預設宣告規則模板Send LDAP Attributes as Claims按一下Next，如下圖所示：



按一下「**Configure Claim Rule**」，如下圖所示。LDAP屬性必須與CUCM中LDAP目錄配置中的LDAP屬性匹配。以uid身份管理傳出宣告型別。按一下「**Finish**」，如下圖所示：



為信賴方新增自定義規則。按一下**Add rule**。選擇**Send Claims using a Custom Rule**，然後按一下**Next**，如下圖所示：

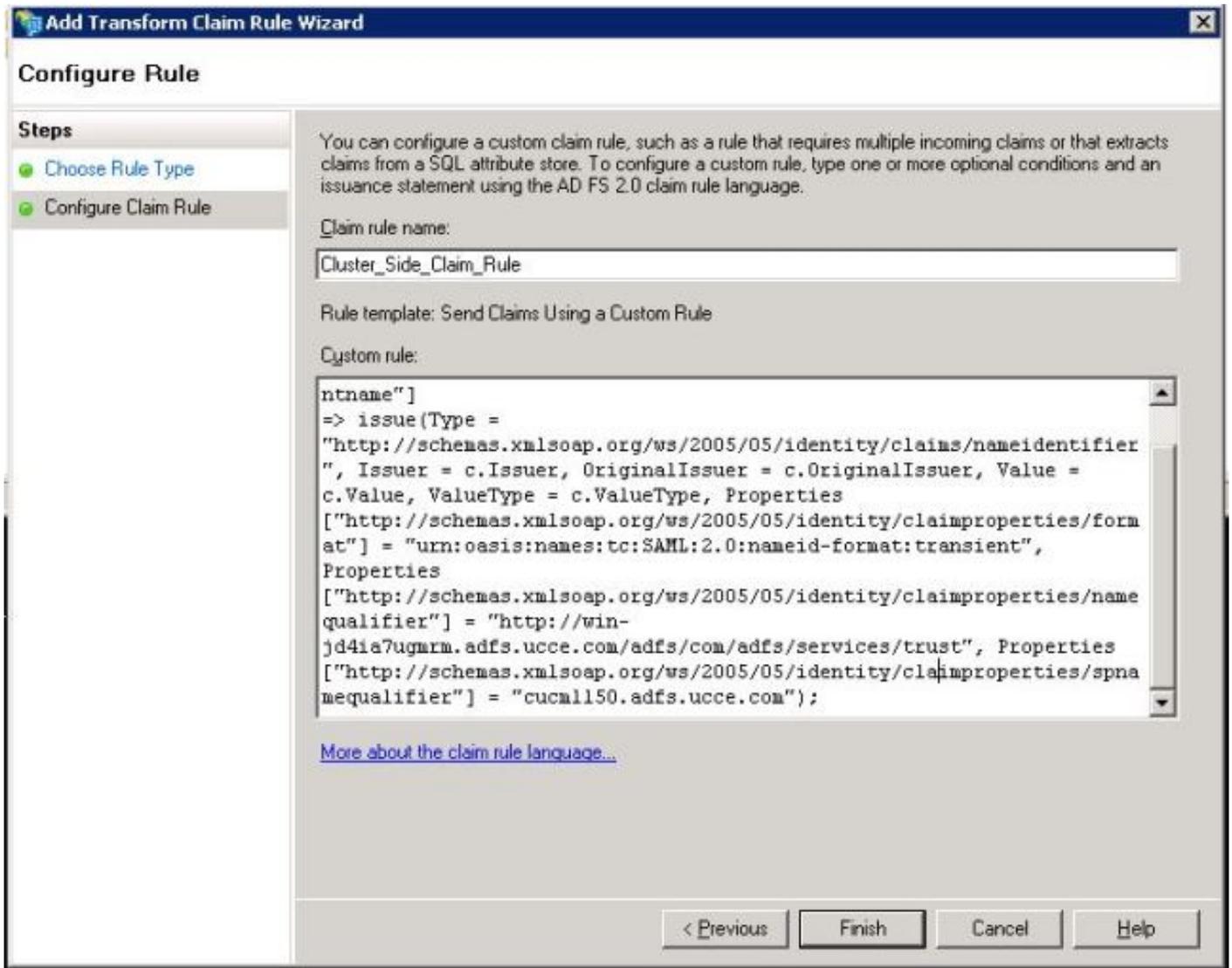


在配置宣告規則中，在嚮導的Custom Rule欄位中鍵入Claim Rule Name，然後複製給定和過去的宣告規則，修改宣告規則中的namequalifier和spname限定符。按一下「Finish」，如下圖所示：

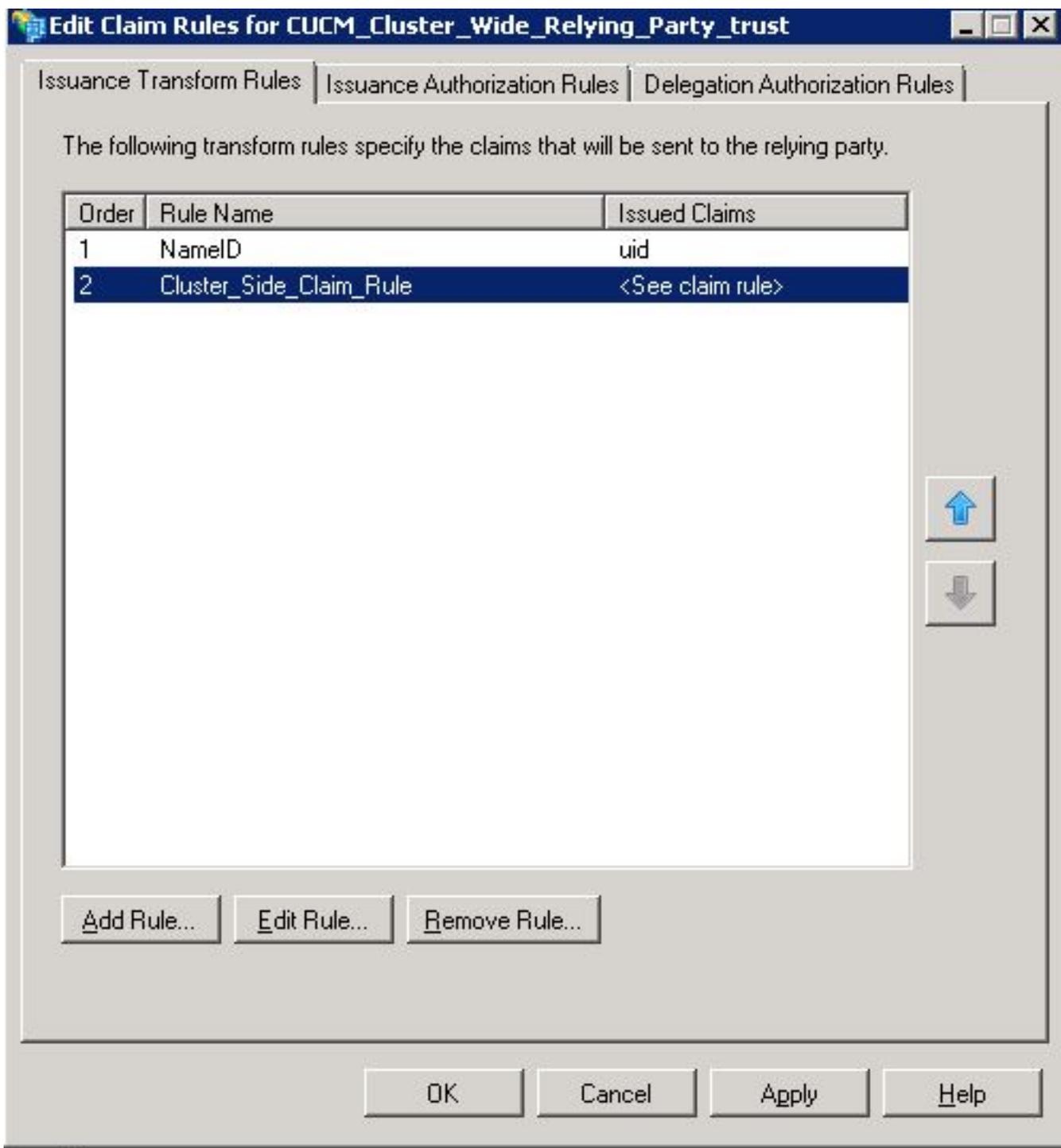
### 報銷申請規則：

```
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://<FQDN of ADFS>/adfs/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"<Entity ID in the SP Metadata>");
```

Entity ID = Open the SP metadata and check the Entity ID. Basically, its the CUCM Publisher's FQDN.



如圖所示，按一下Apply，然後OK。



#### 步驟4.啟用SAML SSO

開啟Web瀏覽器，以管理員身份登入CUCM，然後導覽至System > SAML Single Sign On。

預設情況下，Cluster Wide單選按鈕處於選中狀態。按一下「Enable Saml SSO」，如下圖所示：

## 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)

 Enable SAML SSO  Export All Metadata  Update IdP Metadata File  Fix All Disabled Servers

如圖所示，彈出視窗將通知Web伺服器重新啟動警告以及根據idp選擇群集範圍的SAML SSO或每節點SAML SSO的資訊。按一下「**Continue**」（繼續）。

### 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.

### Click "Export All Metadata" button

If the server metadata has not already been uploaded to the IdP, it can be done before running the wizard. You can obtain the server metadata by clicking the "Export All Metadata" button on the main page. Then go to the IdP and upload the file.

If IDP is provisioned with cluster-wide SP metadata, you need to enable cluster-wide SAML SSO. If IDP is provisioned with per-node SP metadata, you need to enable per-node SAML SSO.

Continue

Cancel

啟用群集範圍的SSO的條件是：必須已經部署多伺服器tomcat證書。按一下「**Test for Multi-Server tomcat Certificate**」，如下圖所示：

## SAML Single Sign-On Configuration

 Next

### Status

 Status: Ready

### Test for Multi-Server tomcat certificate

The criteria for enabling clusterwide SSO is that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below steps:

- 1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
- 2) Click on Generate CSR
- 3) Select Certificate Purpose as Tomcat
- 4) Select Distribution as "Multi-Server"
- 5) Click Generate
- 6) Download the CSR and get it signed from the CA of your choice
- 7) Once the certificate is issued by the CA, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
- 8) Restart Tomcat service on all the nodes in the cluster
- 9) Restart TFTP service on all the TFTP nodes in the cluster

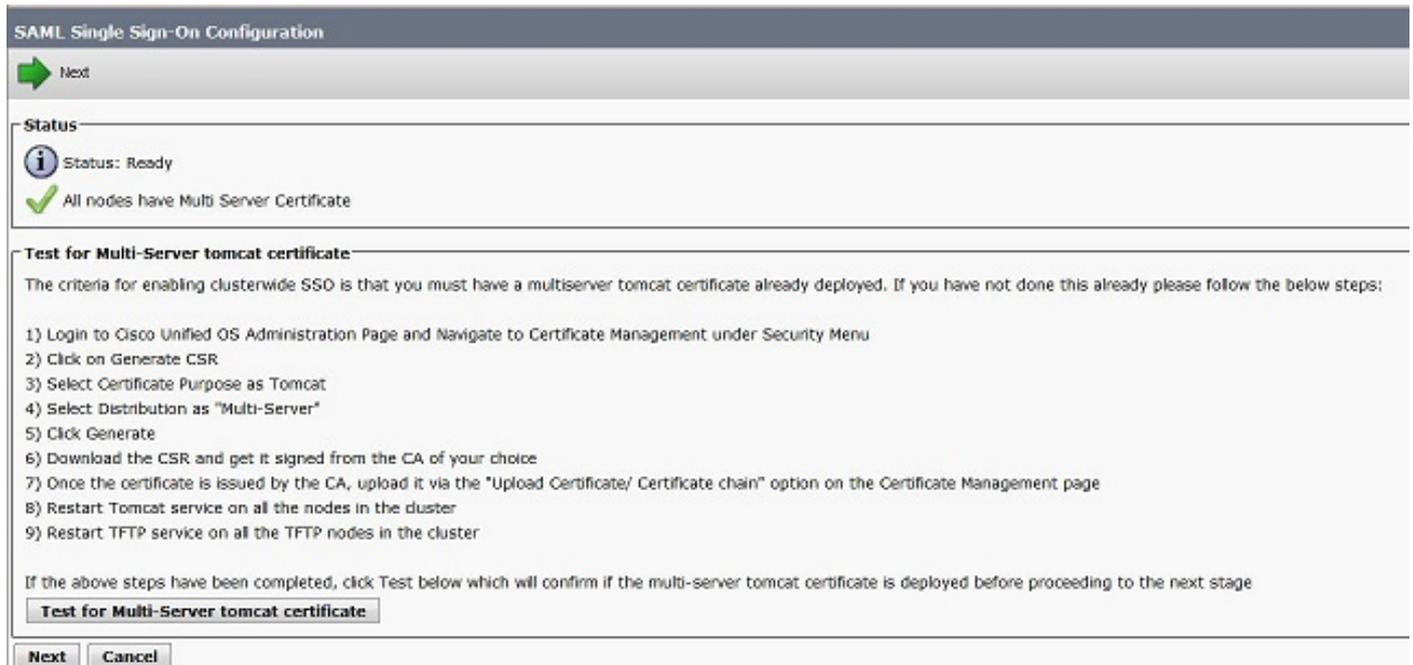
If the above steps have been completed, click Test below which will confirm if the multi-server tomcat certificate is deployed before proceeding to the next stage

**Test for Multi-Server tomcat certificate**

Next

Cancel

確認後，所有節點都具有多伺服器證書(Multi Server Certificate)將顯示**所有節點都具有多伺服器證書(All Nodes have Multi Server Certificate)**，然後按一下下一步，如下圖所示：



SAML Single Sign-On Configuration

Next

**Status**

 Status: Ready

 All nodes have Multi Server Certificate

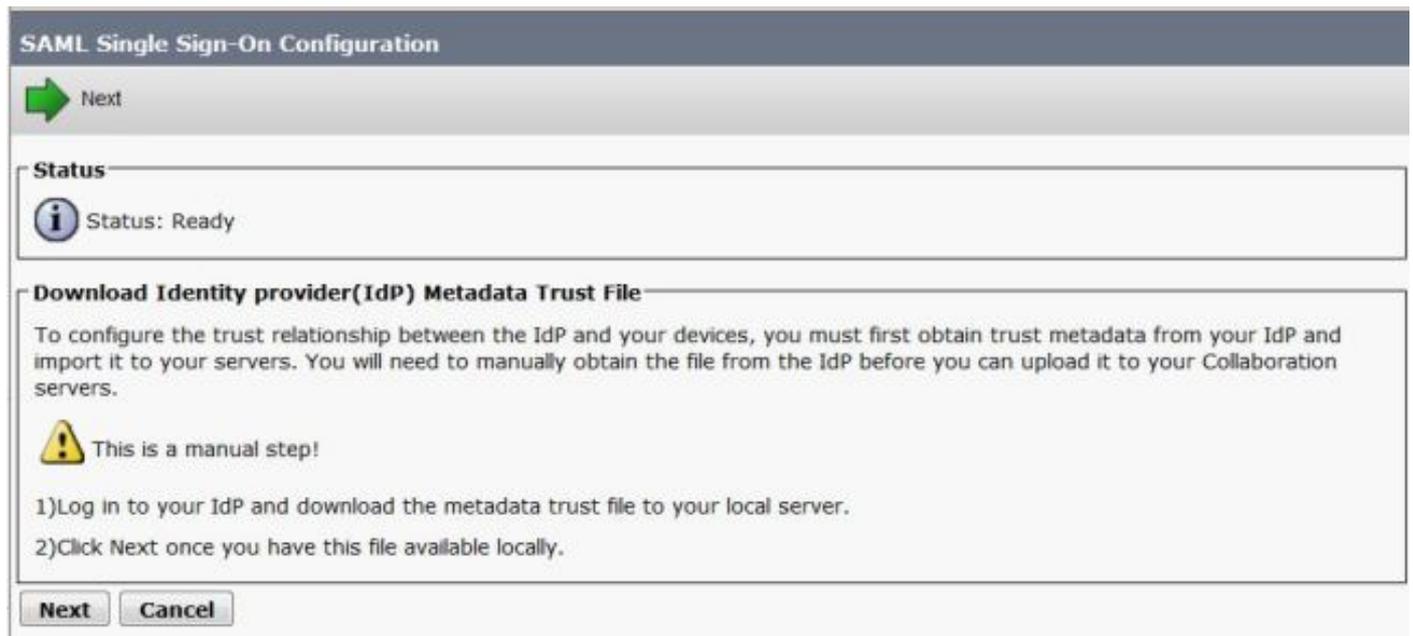
**Test for Multi-Server tomcat certificate**

The criteria for enabling clusterwide SSO is that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below steps:

- 1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
- 2) Click on Generate CSR
- 3) Select Certificate Purpose as Tomcat
- 4) Select Distribution as "Multi-Server"
- 5) Click Generate
- 6) Download the CSR and get it signed from the CA of your choice
- 7) Once the certificate is issued by the CA, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
- 8) Restart Tomcat service on all the nodes in the cluster
- 9) Restart TFTP service on all the TFTP nodes in the cluster

If the above steps have been completed, click Test below which will confirm if the multi-server tomcat certificate is deployed before proceeding to the next stage

如圖所示，按一下下一步。



SAML Single Sign-On Configuration

Next

**Status**

 Status: Ready

**Download Identity provider(IdP) Metadata Trust File**

To configure the trust relationship between the IdP and your devices, 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 before you can upload it to your Collaboration servers.

 This is a manual step!

- 1)Log in to your IdP and download the metadata trust file to your local server.
- 2)Click Next once you have this file available locally.

瀏覽並選擇下載的IdP後設資料。按一下「Import IdP Metadata」，如下圖所示：

**SAML Single Sign-On Configuration**

Next

**Status**

- Status: Ready
- Ready to import Identity Provider metadata trust file to cluster servers

**Import the IdP Metadata Trust File**

This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.

1) Select the IdP Metadata Trust File

federationmetadata.xml

2) Import this file to the Collaboration servers

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

此頁確認所有伺服器的匯入成功，然後按一下下一步，如下圖所示：

**SAML Single Sign-On Configuration**

Next

**Status**

- Status: Ready
- Import succeeded for all servers

**Import the IdP Metadata Trust File**

This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.

1) Select the IdP Metadata Trust File

No file selected.

2) Import this file to the Collaboration servers

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

如圖所示，按一下下一步，因為已從初始SAML SSO配置頁匯出SP後設資料。

### SAML Single Sign-On Configuration

← Back    Next →

**Status**

-  Status: Ready
-  If Admin has already uploaded the server metadata to IdP then skip the steps below and click Next. Otherwise follow the steps below to upload the server metadata to IdP
-  IdP Metadata has been imported to servers in this cluster

**Download Server Metadata and install on the IdP**

Download the metadata trust file from Collaboration servers and manually install it on the IdP server to complete SSO setup.

1)Download the server metadata trust files to local storage

**Download Trust Metadata File**

 This is a manual step!

2)Log in to your IdP and upload the server metadata trust file.

3)Click Next once you have installed the server metadata on the IdP.

**Back**    **Next**    **Cancel**

CUCM必須與LDAP目錄同步。嚮導顯示了LDAP目錄中配置的有效管理員使用者。選擇使用者並按一下**運行SSO測試**，如下圖所示：

### SAML Single Sign-On Configuration

← Back

**Status**

 The server metadata file must be installed on the IdP before this test is run.

**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

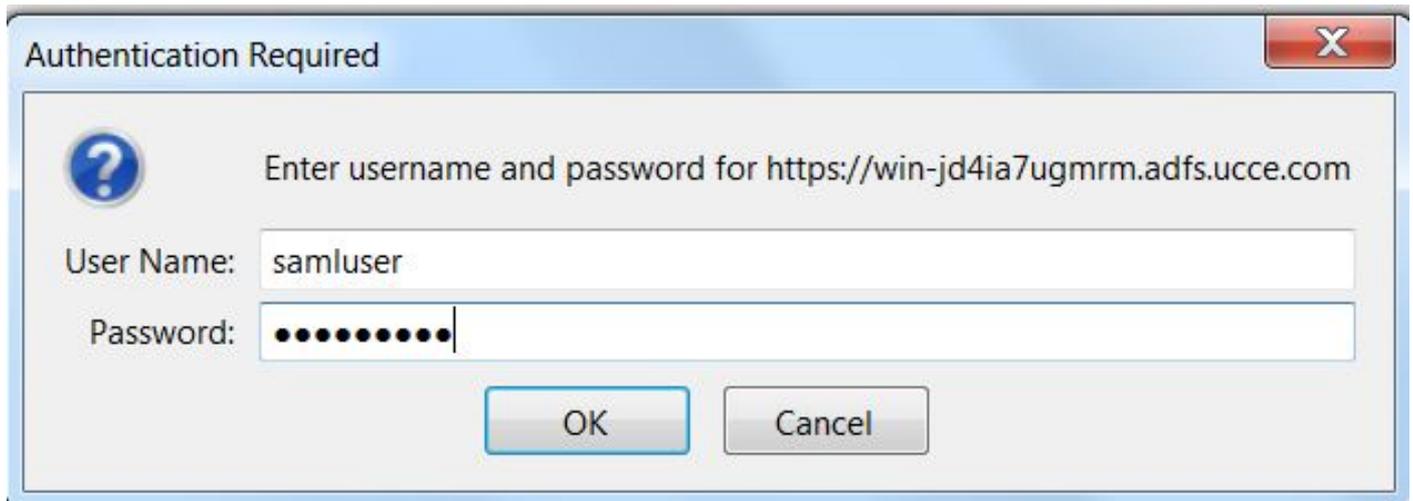
samluser

2)Launch SSO test page

**Run SSO Test...**

**Back**    **Cancel**

如圖所示，提示後輸入使用者ID和各自的密碼。



Authentication Required

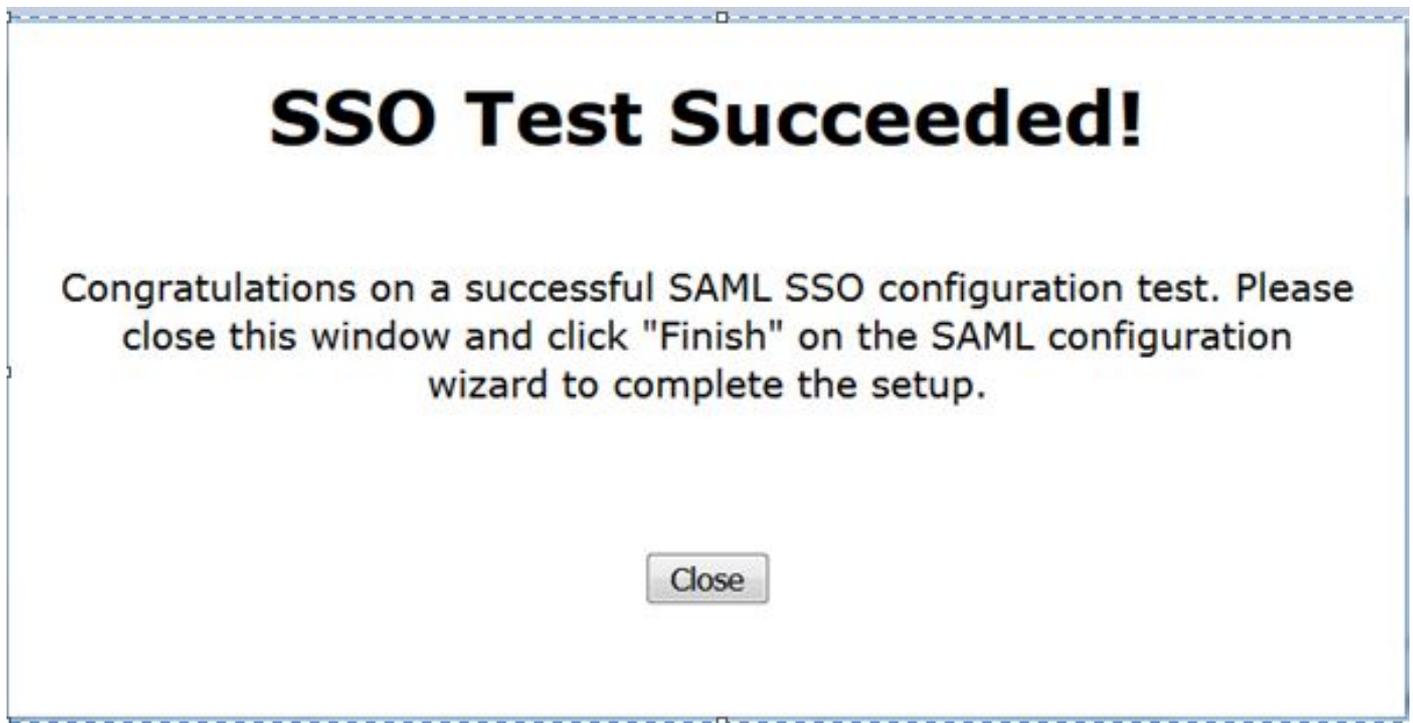
Enter username and password for https://win-jd4ia7ugmrm.adfs.uce.com

User Name:

Password:

OK Cancel

如圖所示彈出可確認測試已成功。



**SSO Test Succeeded!**

Congratulations on a successful SAML SSO configuration test. Please close this window and click "Finish" on the SAML configuration wizard to complete the setup.

Close

如圖所示，按一下**Finish**即可完成啟用SSO的組態。

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administra

### SAML Single Sign-On Configuration

← Back → Finish

**Status**

✓ SSO Metadata Test Successful

**Ready to Enable SSO**

Clicking "Finish" will complete enabling SSO on all the servers in this cluster. There will be a short delay while the applications are being updated.

To verify the SSO status of each server, check the main SSO Configuration page.  
Additional testing and manual uploads may be performed from the main page if necessary.

Back Finish Cancel

圖中所示的頁面確認SAML SSO啟用進程已在所有伺服器上啟動。

### SAML Single Sign-On Configuration

**Status**

✓ SAML SSO enablement process initiated on all servers.  
There will be a short delay while the applications are being updated on each server.  
To verify the SSO status of each server, check the main SSO Configuration page.

註銷並使用SAML SSO憑據重新登入到CUCM。導航到System >SAML Single Sign On。按一下群集中其他節點的運行SSO測試，如下圖所示：

### 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)

✗ Disable SAML SSO Export All Metadata Update IdP Metadata File Fix All Disabled Servers

**Status**

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

SAML SSO enabled

SAML Single Sign-On (1 - 3 of 3)							Rows per Page 50 ▾
Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test	
cucm1150.adfs.ucce.com	SAML	N/A	June 21, 2016 9:28:39 PM IST	File	June 21, 2016 7:46:56 PM IST	Passed - June 21, 2016 9:29:14 PM IST	
cucm1150sub.adfs.ucce.com	SAML	IdP	June 21, 2016 9:28:39 PM IST	File	June 21, 2016 7:46:56 PM IST	Never	
imp115.adfs.ucce.com	SAML	IdP	June 21, 2016 9:28:39 PM IST	File	June 21, 2016 7:46:56 PM IST	Never	

## 驗證

使用本節內容，確認您的組態是否正常運作。

確認已啟用SAML SSO的節點的SSO測試成功。導航到System >SAML Single Sign On。成功的SSO測試顯示「通過」狀態。

**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)

Disable SAML SSO Export All Metadata Update IdP Metadata File Fix All Disabled Servers

**Status**

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

SAML SSO enabled

**SAML Single Sign-On (1 - 3 of 3)** Rows per Page 50

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cucm1150.adfs.ucce.com	SAML	N/A	June 20, 2016 9:57:30 AM IST	File	June 20, 2016 10:06:27 PM IST	Passed - June 20, 2016 9:59:02 PM IST
cucm1150sub.adfs.ucce.com	SAML	IdP	June 20, 2016 10:15:46 PM IST	File	June 20, 2016 10:06:26 PM IST	Passed - June 20, 2016 10:11:39 PM IST
imp115.adfs.ucce.com	SAML	IdP	June 20, 2016 10:15:46 PM IST	File	June 20, 2016 10:06:26 PM IST	Passed - June 20, 2016 10:12:40 PM IST

啟用SAML SSO後，CUCM登入頁面將列出已安裝應用程式和平台應用程式，如下圖所示。

## Installed Applications

- Cisco Unified Communications Manager
  - Recovery URL to bypass Single Sign On (SSO)
- Cisco Unified Communications Self Care Portal
- Cisco Prime License Manager
- Cisco Unified Reporting
- Cisco Unified Serviceability

## Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

啟用SAML SSO後，系統會為IM and Presence登入頁列出已安裝應用程式和平台應用程式，如下圖所示：

## Installed Applications

- Cisco Unified Communications Manager IM and Presence
  - Recovery URL to bypass Single Sign On (SSO)
- Cisco Unified Reporting
- Cisco Unified Serviceability

## Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

若要將SSO日誌設定為調試，請使用命令**set samltrace level DEBUG**

使用RTMT或使用CLI從**activelog /tomcat/logs/ssosp/log4j/\*.log**位置收集SSO日誌。

SSO日誌的示例顯示了生成的後設資料並傳送到其他節點

```
2016-05-28 14:59:34,026 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call GET API to generate Clusterwide SP Metadata in the Local node.
2016-05-28 14:59:47,184 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call to post the generated SP Metadata to other nodes
2016-05-28 14:59:47,185 INFO [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Begin:postClusterWideSPMetaData
2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Nodes [cucm1150, cucm1150sub.adfs.ucce.com]
2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post ClusterWideSPMetadata to the cucm1150
2016-05-28 14:59:47,187 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post ClusterWideSPMetadata to the cucm1150sub.adfs.ucce.com
```