

使用CUCM和AD FS 2.0配置單點登入

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[在Windows伺服器上下載並安裝AD FS 2.0](#)

[在Windows伺服器上配置AD FS 2.0](#)

[將Idp後設資料匯入CUCM /下載CUCM後設資料](#)

[將CUCM後設資料匯入AD FS 2.0伺服器並建立宣告規則](#)

[在CUCM上完成SSO啟用並運行SSO測試](#)

[疑難排解](#)

[將SSO日誌設定為調試](#)

[查詢聯合身份驗證服務名稱](#)

[無點證書和聯合身份驗證服務名稱](#)

[CUCM和IDP伺服器之間的時間不同步](#)

[相關資訊](#)

簡介

本文檔介紹如何在Cisco Unified Communications Manager和Active Directory聯合身份驗證服務上配置單一登入(SSO)。

必要條件

需求

思科建議您瞭解以下主題：

- 思科整合通訊管理員(CUCM)
- Active Directory聯合身份驗證服務(AD FS)的基本知識

要在您的實驗環境中啟用SSO，您需要以下配置：

- 安裝了AD FS的Windows伺服器。
- 配置了LDAP同步的CUCM。
- 已選擇標準CCM超級使用者角色的終端使用者。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 採用AD FS 2.0的Windows伺服器
- CUCM 10.5.2

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。

背景資訊

提供了在Windows Server 2008 R2上安裝AD FS 2.0的過程。這些步驟也適用於Windows Server 2016上的AD FS 3.0。

在Windows伺服器上下載並安裝AD FS 2.0

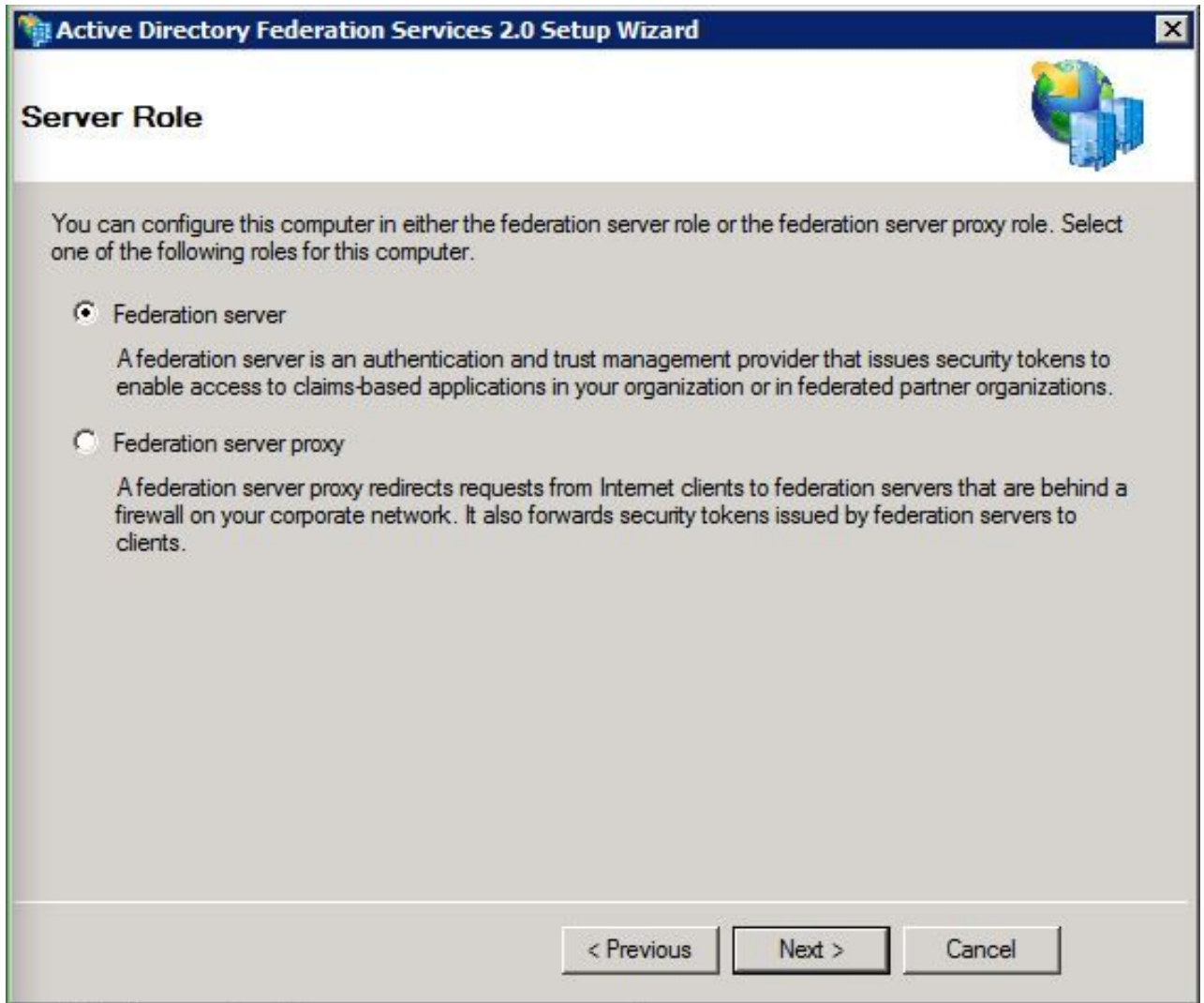
步驟 1. 導覽至[Download AD FS 2.0](#)。

步驟 2. 確保根據Windows Server選擇適當的下載。

步驟 3. 將下載的檔案移動到Windows伺服器。

步驟 4. 繼續安裝：

步驟 5. 出現提示時，選擇Federation Server:



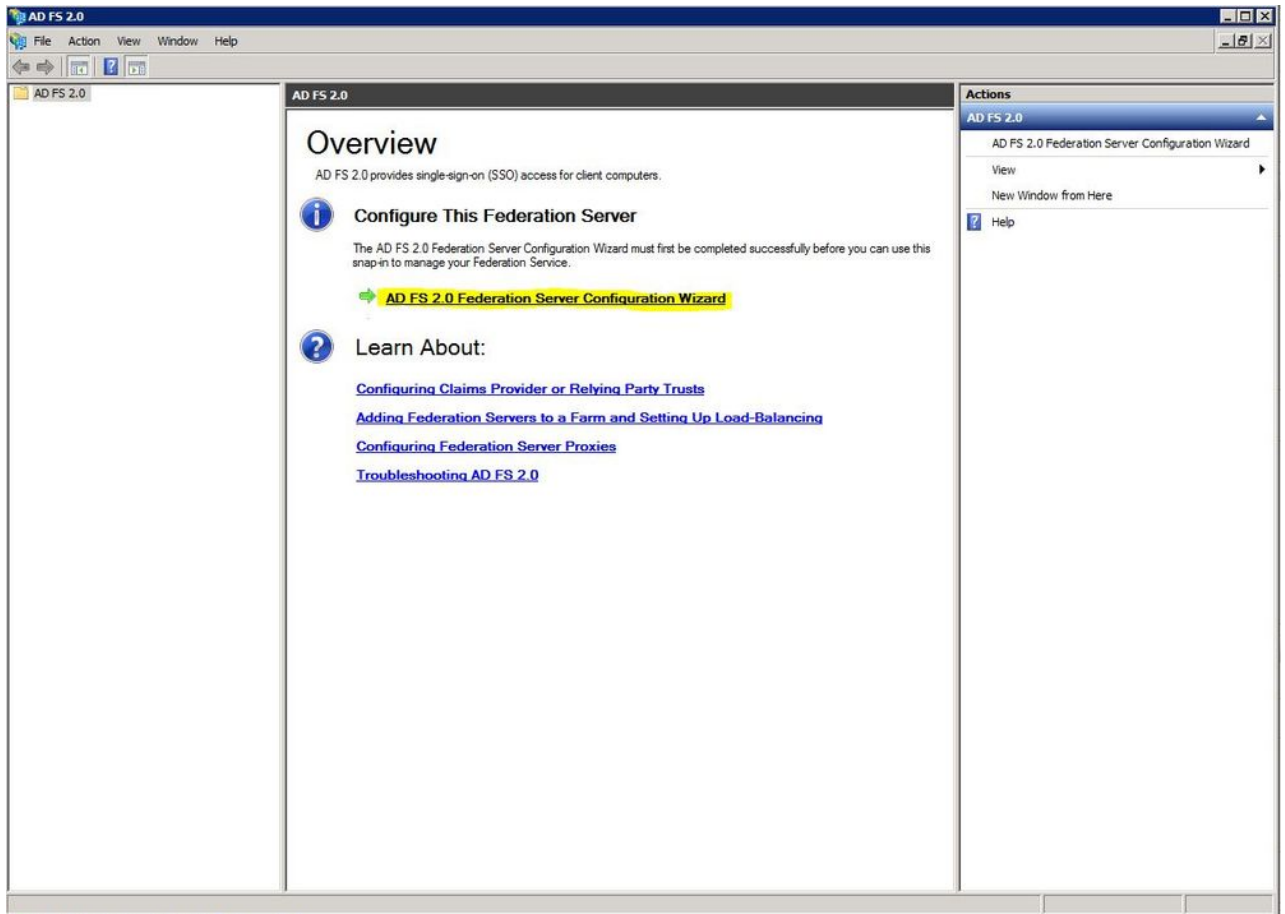
步驟6.自動安裝某些依賴項 — 完成後，按一下完成。

現在您的伺服器上已安裝AD FS 2.0，您需要新增一些配置。

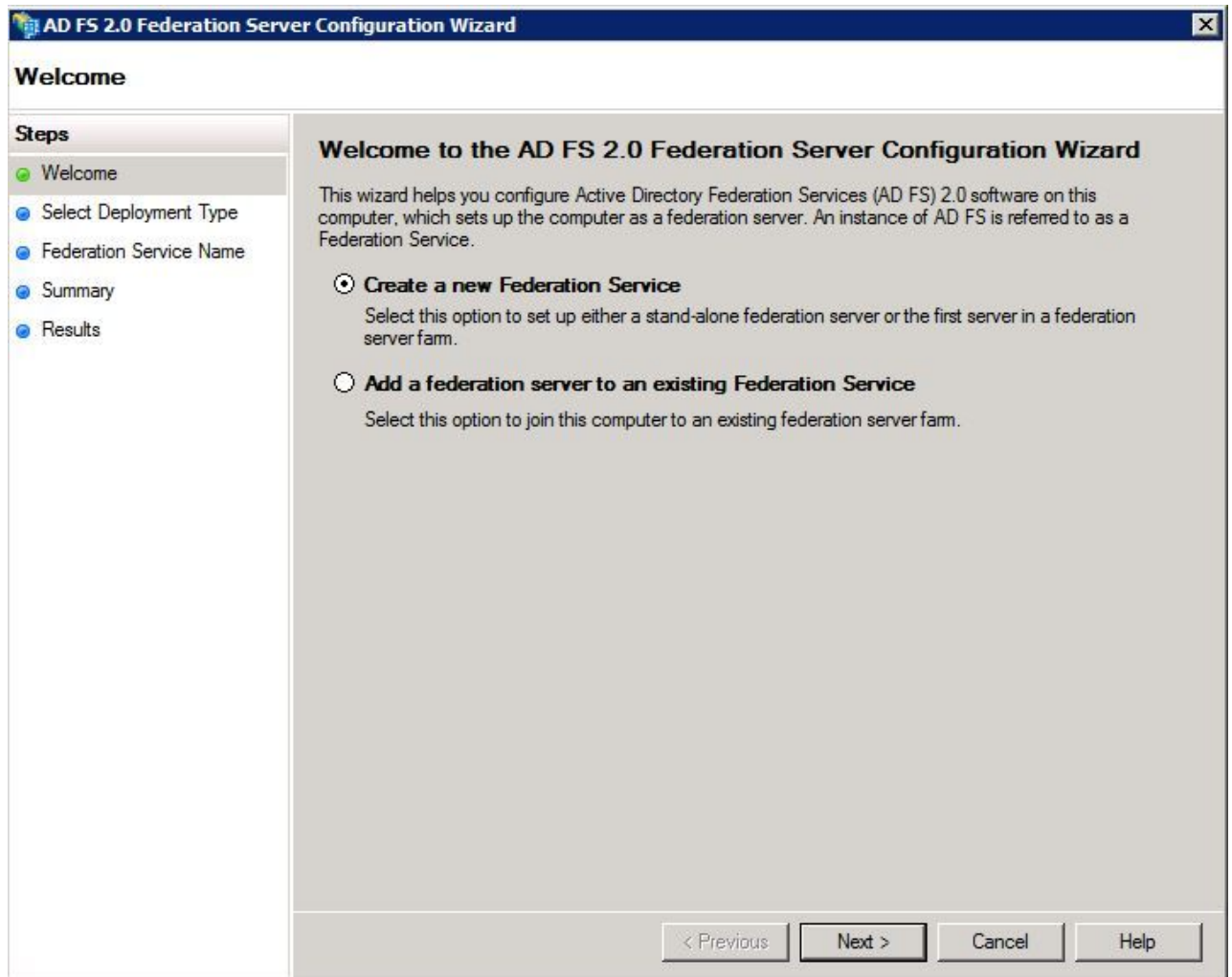
在Windows伺服器上配置AD FS 2.0

步驟 1.如果在安裝後沒有自動開啟AD FS 2.0視窗，可以按一下Start並搜尋AD FS 2.0管理以手動開啟該視窗。

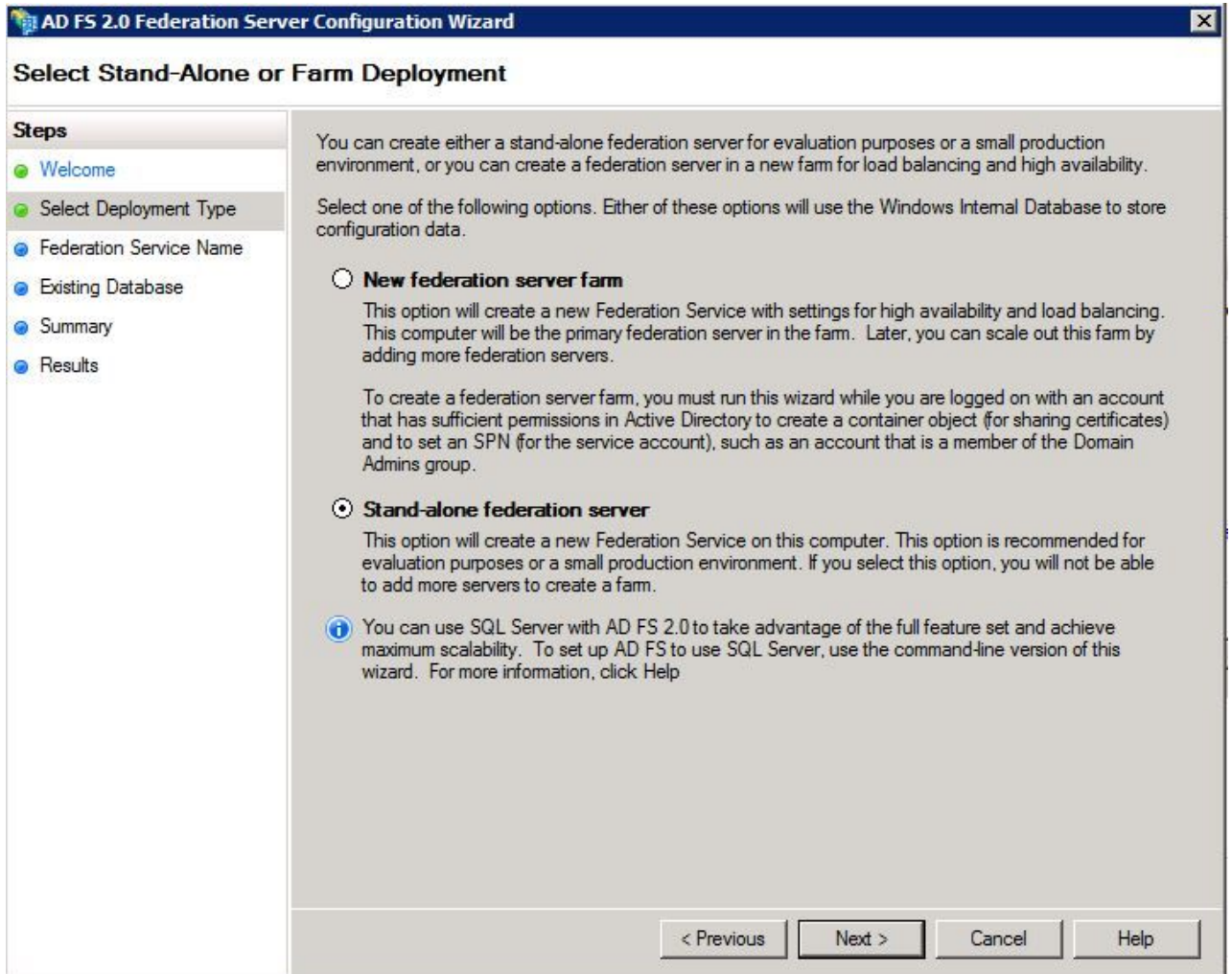
步驟 2.選擇AD FS 2.0 Federation Server Configuration Wizard。



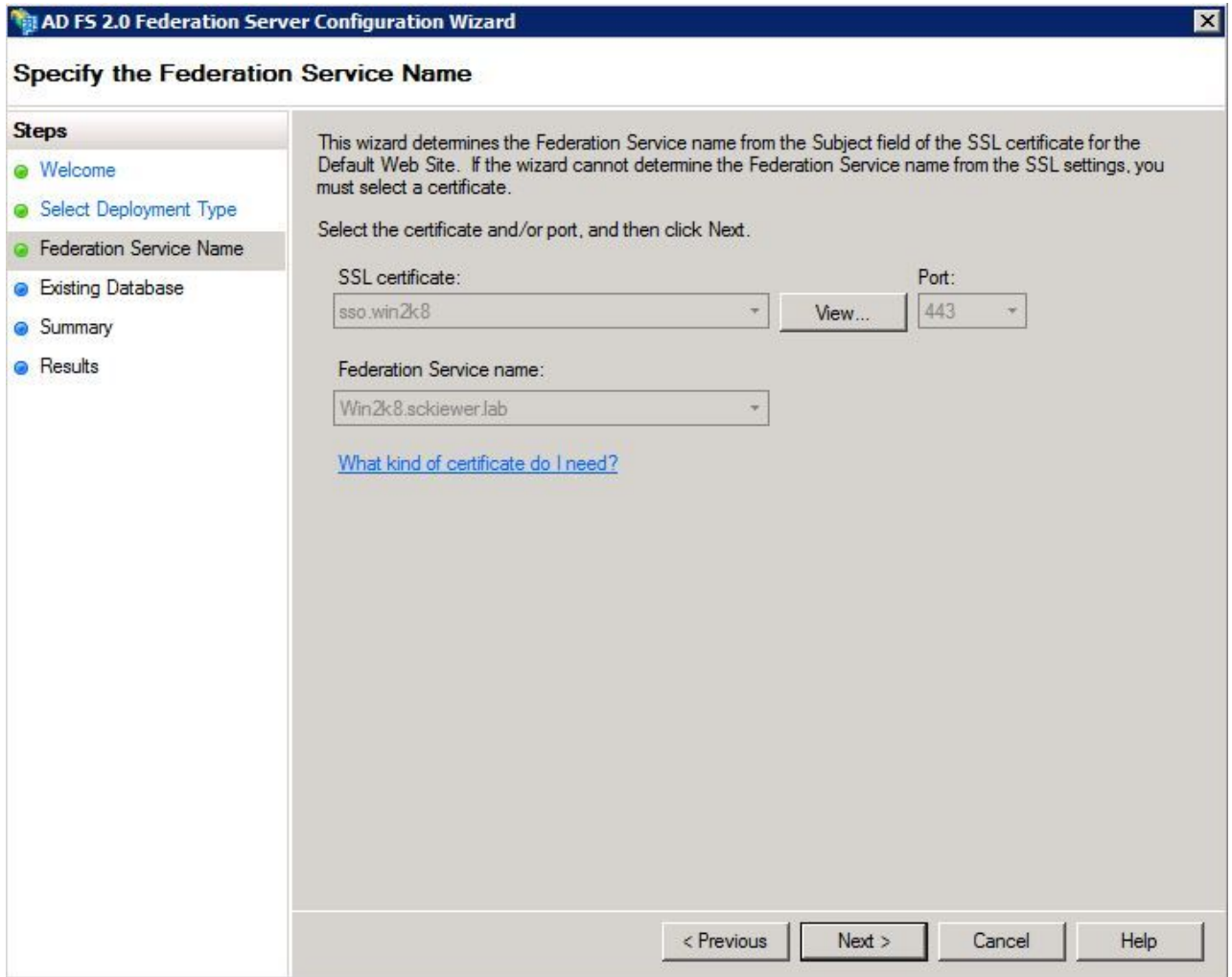
步驟3. 下一步，按一下建立新的聯合身份驗證服務。



步驟 4.對於大多數環境，獨立聯合伺服器就足夠了。



步驟 5.接下來，系統會要求您選擇憑證。只要伺服器有證書，此欄位就會自動填充。



步驟 6.如果伺服器上已經有一個AD FS資料庫，則需要將其刪除才能繼續。

步驟 7.最後，您將進入一個摘要螢幕，您可以在其中按一下下一步。

將Idp後設資料匯入CUCM /下載CUCM後設資料

步驟 1.使用您的Windows伺服器主機名/FQDN更新URL並從AD FS伺服器下載後設資料 — <https://hostname/federationmetadata/2007-06/federationmetadata.xml>

步驟 2.導覽至Cisco Unified CM Administration > System > SAML Single Sign-On。

步驟 3.按一下Enable SAML SSO。

步驟 4.如果收到有關Web伺服器連線的警報，請按一下Continue。

步驟 5.接下來，CUCM會指示您從IdP下載後設資料檔案。在此方案中，您的AD FS伺服器是IdP，您在第1步中下載了後設資料，因此按一下下一步。

步驟 6.按一下Browse > Select the .xml from Step 1 > Import IdP Metadata。

步驟 7.有一條消息表明匯入成功：

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

SAML Single Sign-On Configuration

Next

Status

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

步驟 8.按「Next」（下一步）。

步驟 9.現在您已將IdP後設資料匯入CUCM，因此需要將CUCM的後設資料匯入IdP。

步驟 10.按一下下載信任後設資料檔案。

步驟 11.按「Next」（下一步）。

步驟 12.將.zip檔案移動到Windows Server並將內容解壓到資料夾中。

將CUCM後設資料匯入AD FS 2.0伺服器並建立宣告規則

步驟 1.按一下Start並搜尋AD FS 2.0 Management。

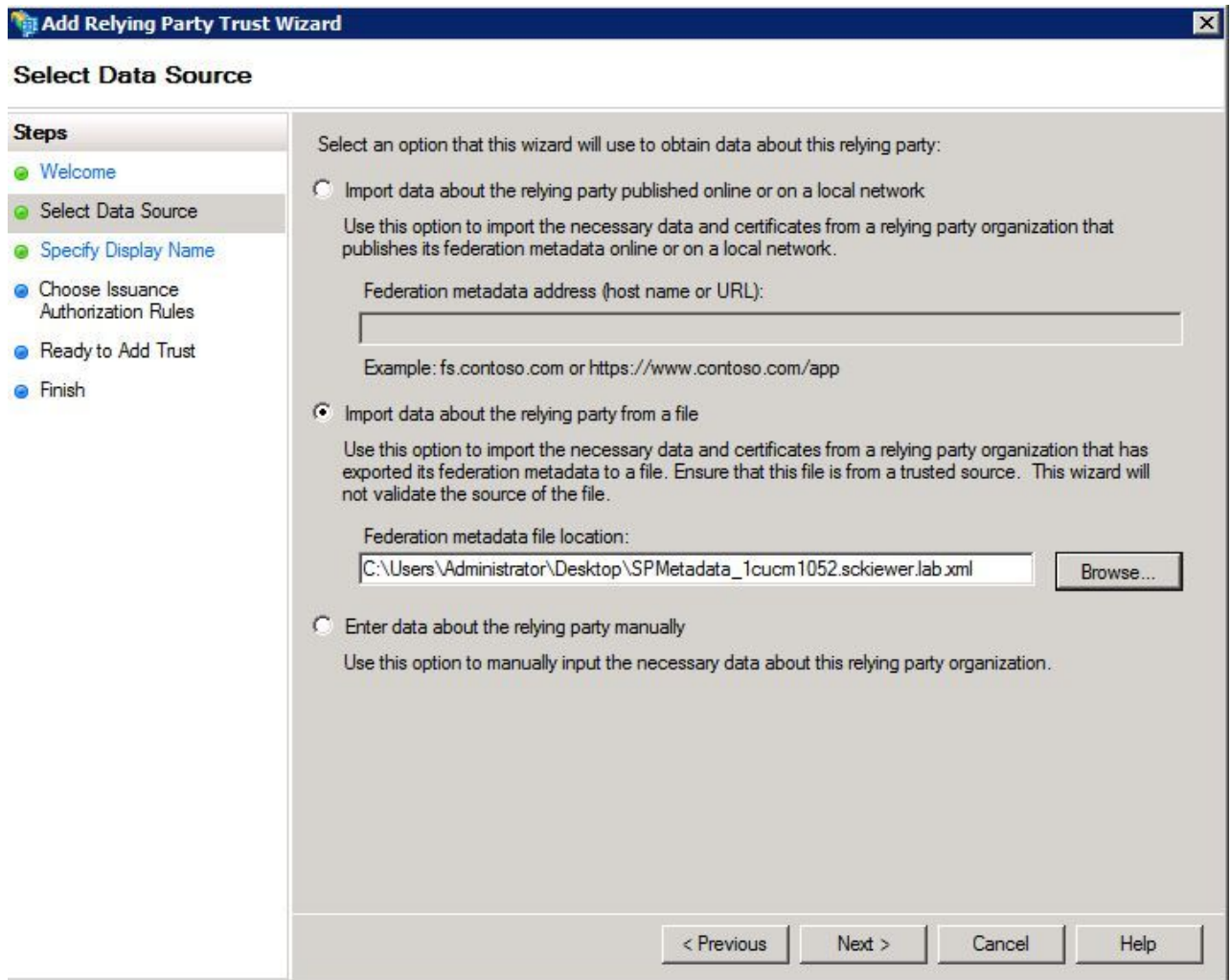
步驟 2.按一下Required: Add a trusted relisting party。

註：如果您沒有看到此選項，您需要關閉視窗並重新開啟它。

步驟 3.開啟Add Relisting Party Trust Wizard後，單擊Start。

步驟 4.在此，您需要匯入在步驟12中抽取的XML檔案。選擇Import data about the relisting party from a file，瀏覽到資料夾檔案，然後為發佈者選擇XML。

注意：對於要使用SSO的任何Unified Collaboration伺服器，請使用上述步驟。



步驟 5.按「Next」(下一步)。

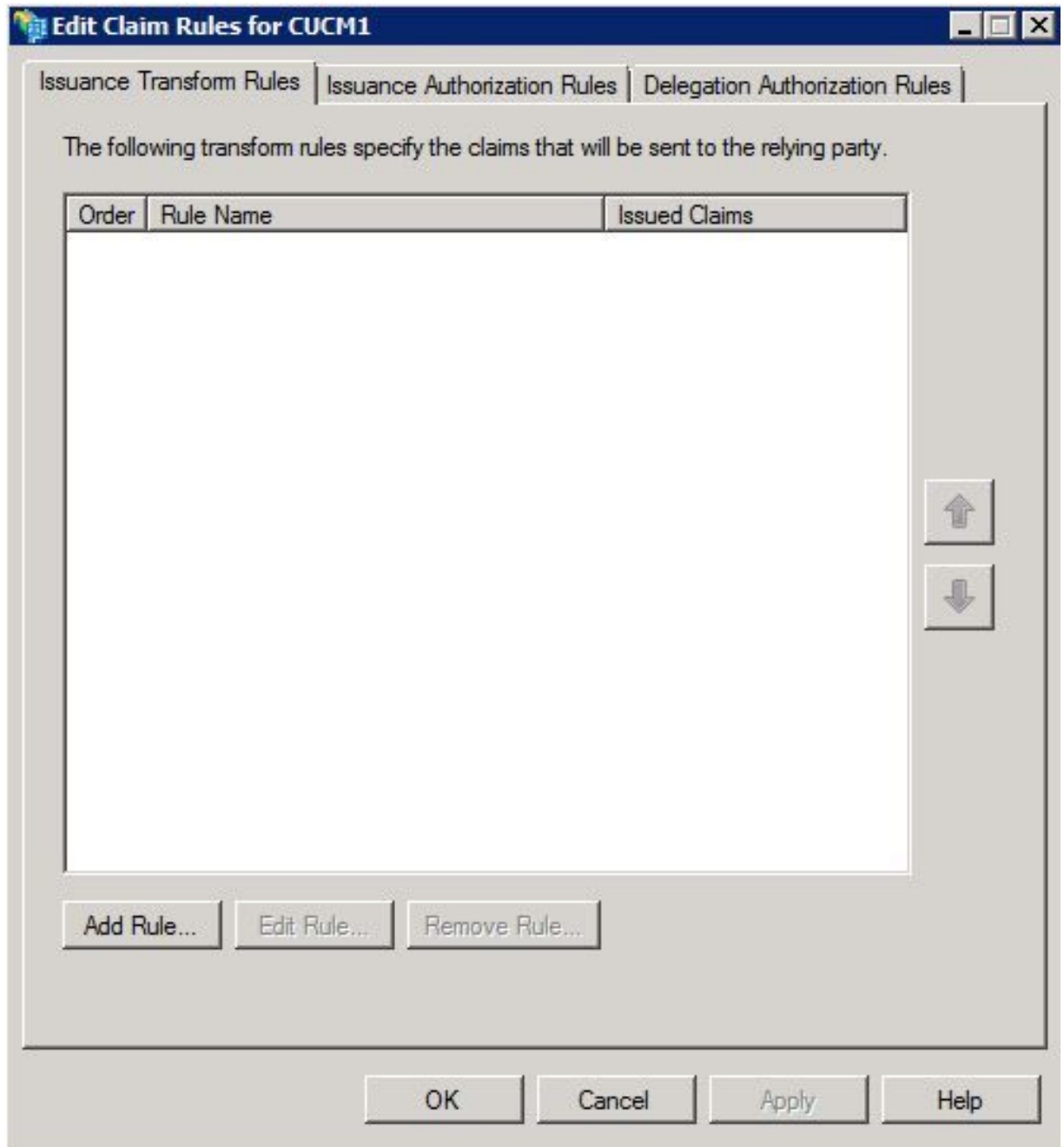
步驟 6.編輯顯示名稱，然後按一下下一步。

步驟 7.選擇Permit all users to access this relisting party，然後按一下Next。

步驟 8.再次按一下Next。

步驟 9.在此螢幕上，確保選中嚮導關閉時已為此信賴方信任開啟「編輯宣告規則」對話框，然後按一下「關閉」。

步驟 10.此時將開啟「編輯宣告規則」視窗：



步驟 11.在此視窗中，按一下Add Rule。


步驟 12.對於宣告規則模板，選擇Send LDAP Attributes as Claims，然後按一下Next。

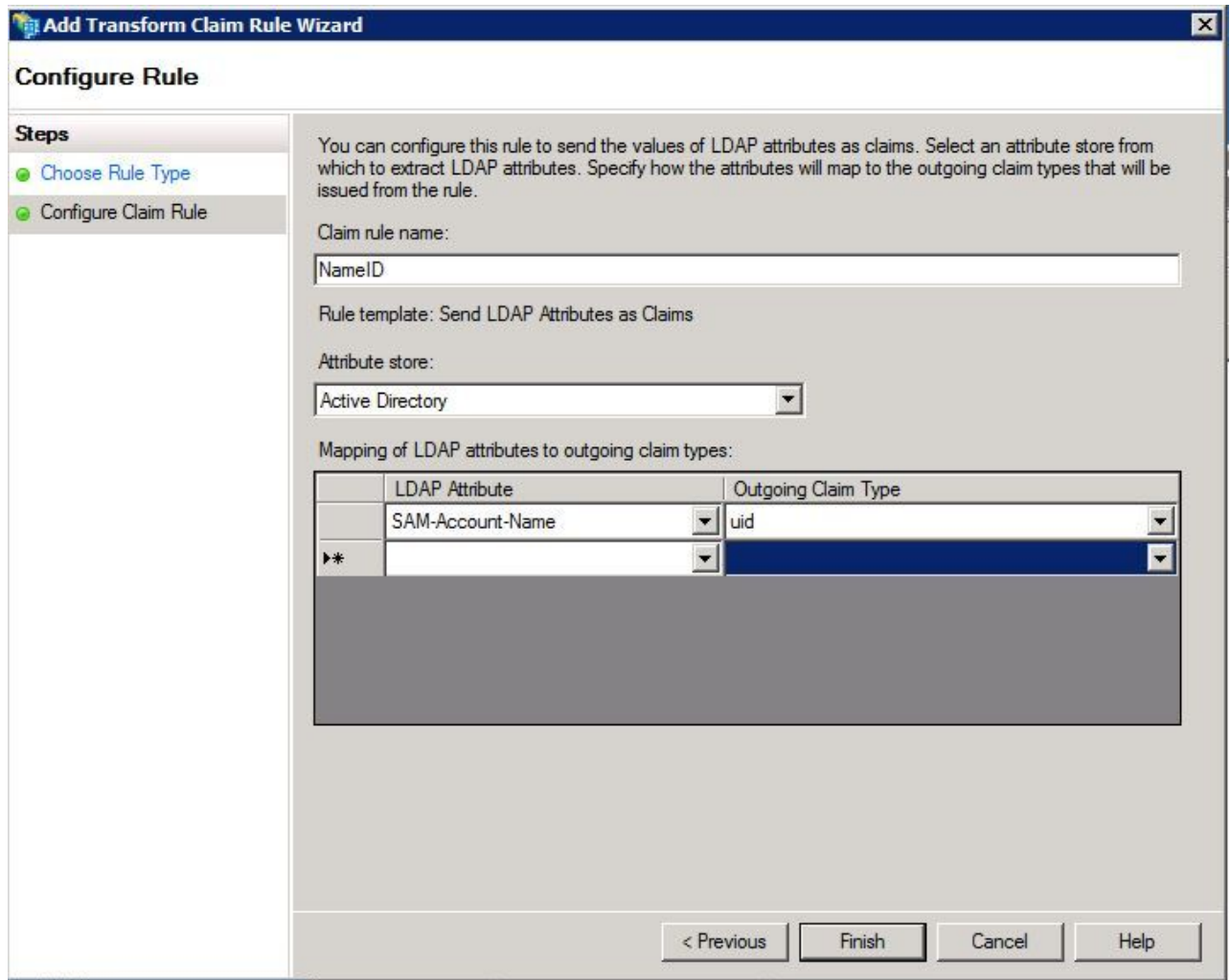
步驟 13.在下一頁上，輸入NameID作為索賠規則名稱。

步驟 14.為屬性儲存選擇Active Directory。

步驟 15.為LDAP Attribute選擇SAM-Account-Name。

步驟 16.輸入uid作為傳出宣告型別。

 註:uid不是下拉選單中的選項 — 必須手動輸入它。



步驟 17.按一下「Finish」（結束）。

步驟 18.第一條規則現在已完成。再次按一下Add Rule。


步驟 19.選擇Send Claims Using a Custom Rule。

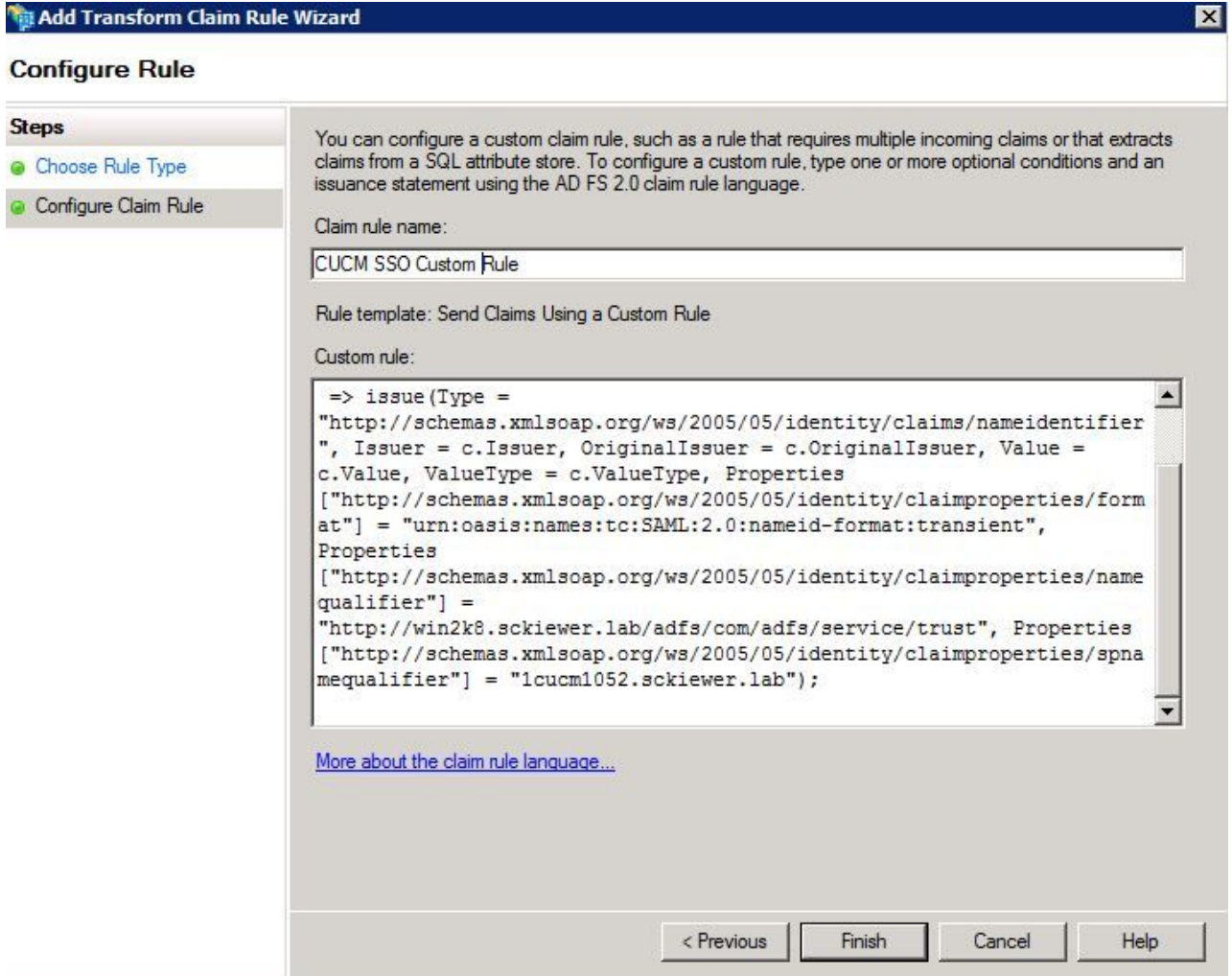
步驟 20.輸入申請規則名稱。

步驟 21.在Custom rule欄位中，貼上以下文本：

```
c:[鍵入 == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=>問題(型別 = "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/claimperities/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient", 屬性
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimperities/namequalifier"] =
"http://ADFS\_FEDERATION\_SERVICE\_NAME/com/adfs/service/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimperities/spnamequalifier"] =
"CUCM_ENTITY_ID");
```

步驟 22.確保將AD_FS_SERVICE_NAME和CUCM_ENTITY_ID更改為相應的值。

 註：如果您不確定AD FS服務名稱，可以按照步驟查詢它。 CUCM實體ID可以從CUCM後設資料檔案中的第一行提取。 檔案第一行上有一個entityID，如下所示，entityID=1cucm1052.sckiewer.lab。您需要在索賠規則的相應部分輸入帶下劃線的值。



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language.

Claim rule name: CUCM SSO Custom Rule

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
=> 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://win2k8.sckiewer.lab/adfs/com/adfs/service/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "1cucm1052.sckiewer.lab");
```

[More about the claim rule language...](#)

< Previous Finish Cancel Help

步驟 23.按一下「Finish」（結束）。

步驟 24.按一下「OK」（確定）。


 注意：對於要使用SSO的任何Unified Collaboration伺服器，都需要宣告規則。

在CUCM上完成SSO啟用並運行SSO測試


步驟 1.現在，AD FS伺服器已完全配置，您可以返回到CUCM。

步驟 2.您在最終配置頁面上關閉：

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 a

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

sckiewer

2) Launch SSO test page

步驟 3. 選擇已選擇「標準CCM超級使用者」角色的終端使用者，然後按一下運行SSO測試.....

步驟 4. 確保您的瀏覽器允許彈出視窗，並在提示中輸入您的憑據。



步驟 5. 在彈出視窗中按一下Close，然後按一下Finish。

步驟 6. 在短暫重新啟動Web應用程式後，啟用SSO。

疑難排解

將SSO日誌設定為調試

要將SSO日誌設定為調試，必須在CUCM的CLI中運行此命令：set samltrace level debug

可以從RTMT下載SSO日誌。日誌集的名稱為Cisco SSO。

查詢聯合身份驗證服務名稱

要查詢聯合身份驗證服務名稱，請按一下Start並搜尋AD FS 2.0 Management。

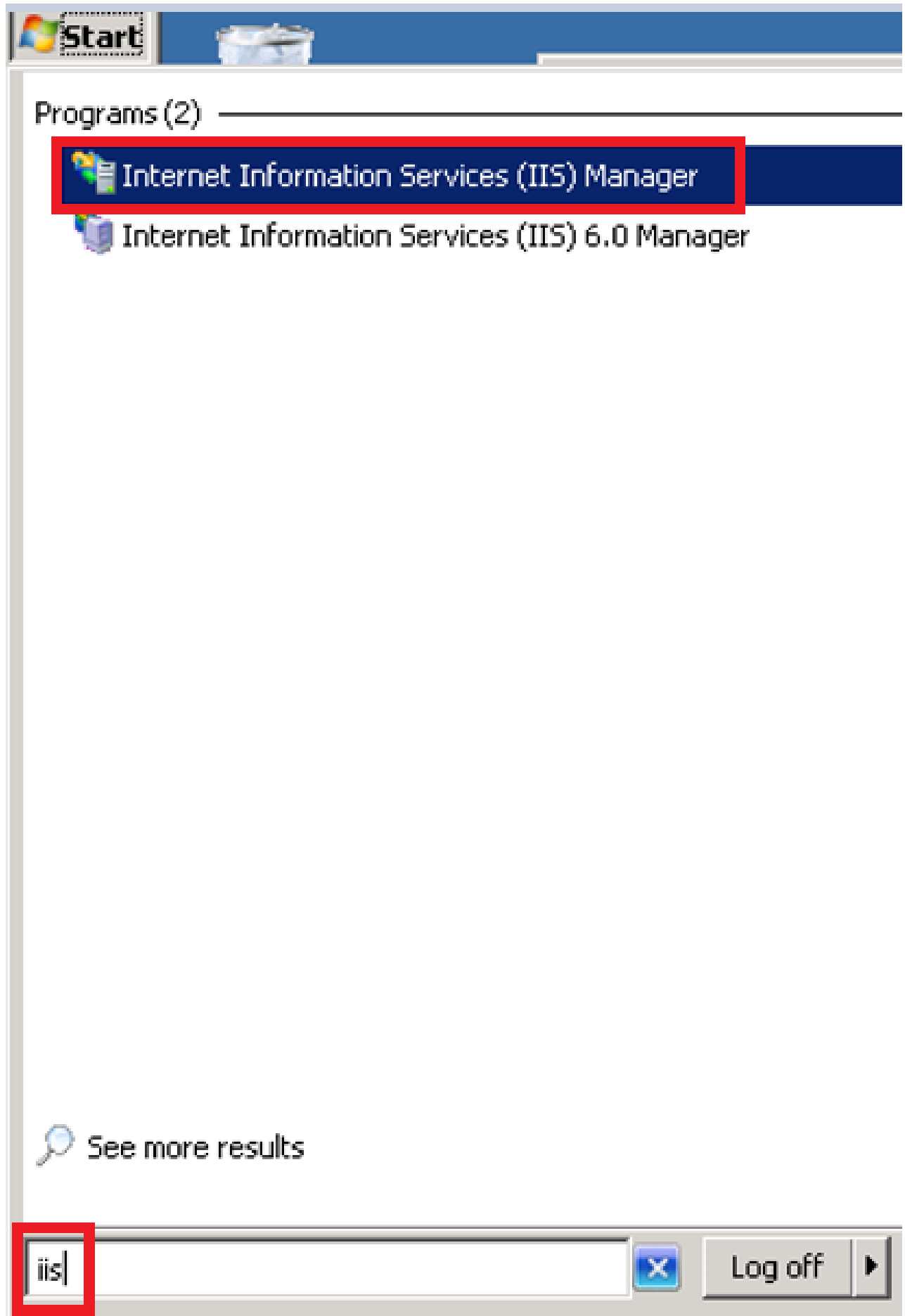
- 按一下「編輯聯盟服務屬性.....」
- 在「常規」頁籤上，查詢聯合身份驗證服務名稱

無點證書和聯合身份驗證服務名稱

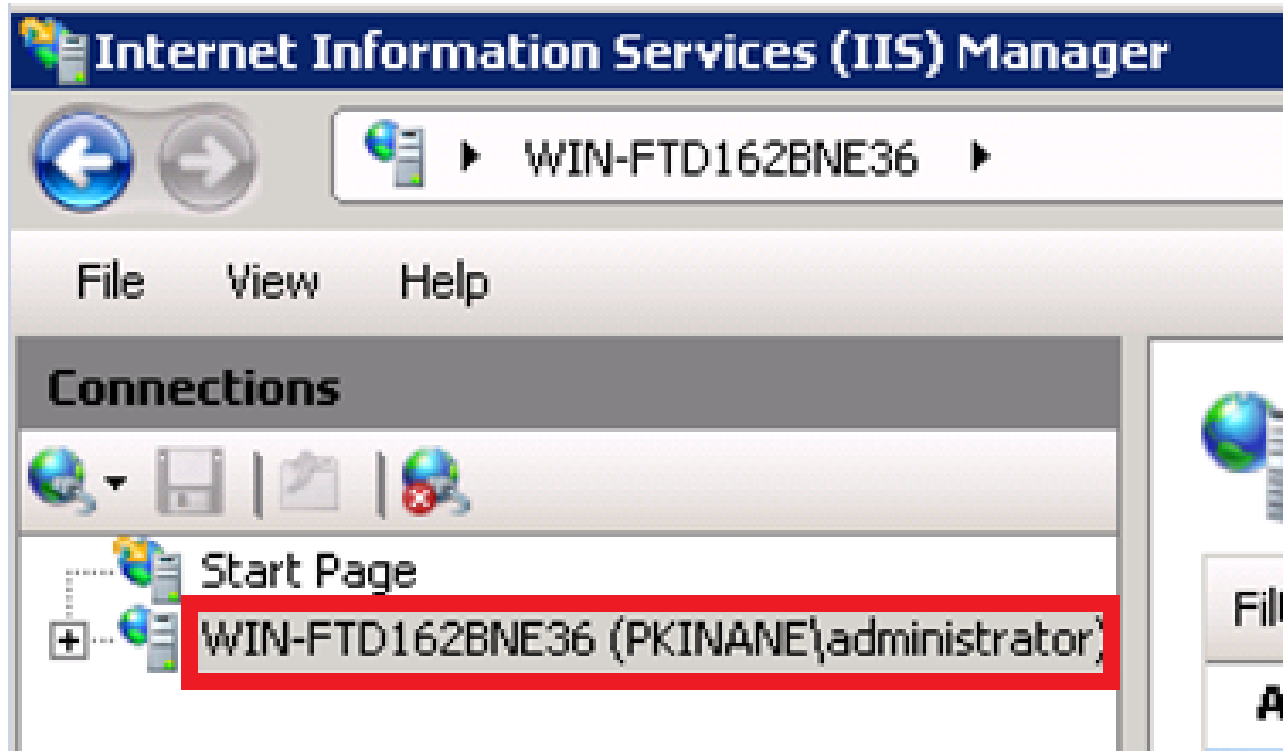
如果在AD FS配置嚮導中收到此錯誤消息，則需要建立新證書。

所選證書不能用於確定聯合身份驗證服務名稱，因為所選證書具有無點（短名稱）使用者名稱。請選擇沒有無點（短名稱）使用者名稱的其他證書，然後重試。

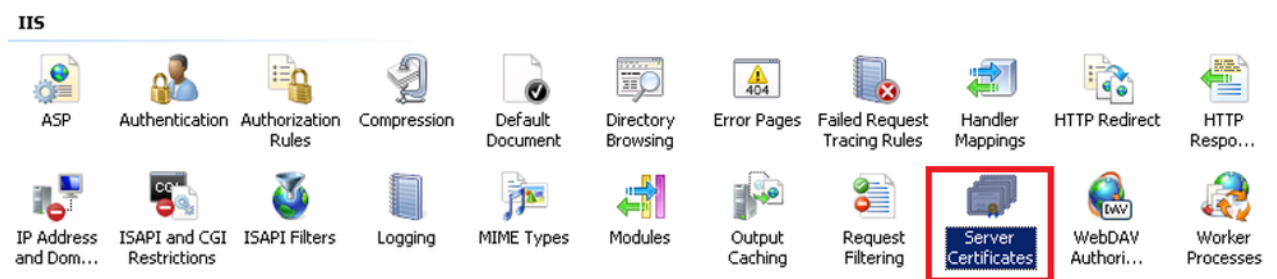
步驟 1.按一下「開始」並搜尋iis，然後開啟「Internet資訊服務(IIS)管理器」



步驟 2. 按一下伺服器的名稱。



步驟 3.按一下「伺服器證書」。



步驟 4.點選Create Self-Signed Certificate。

Actions

Import...

Create Certificate Request...

Complete Certificate Request...

Create Domain Certificate...

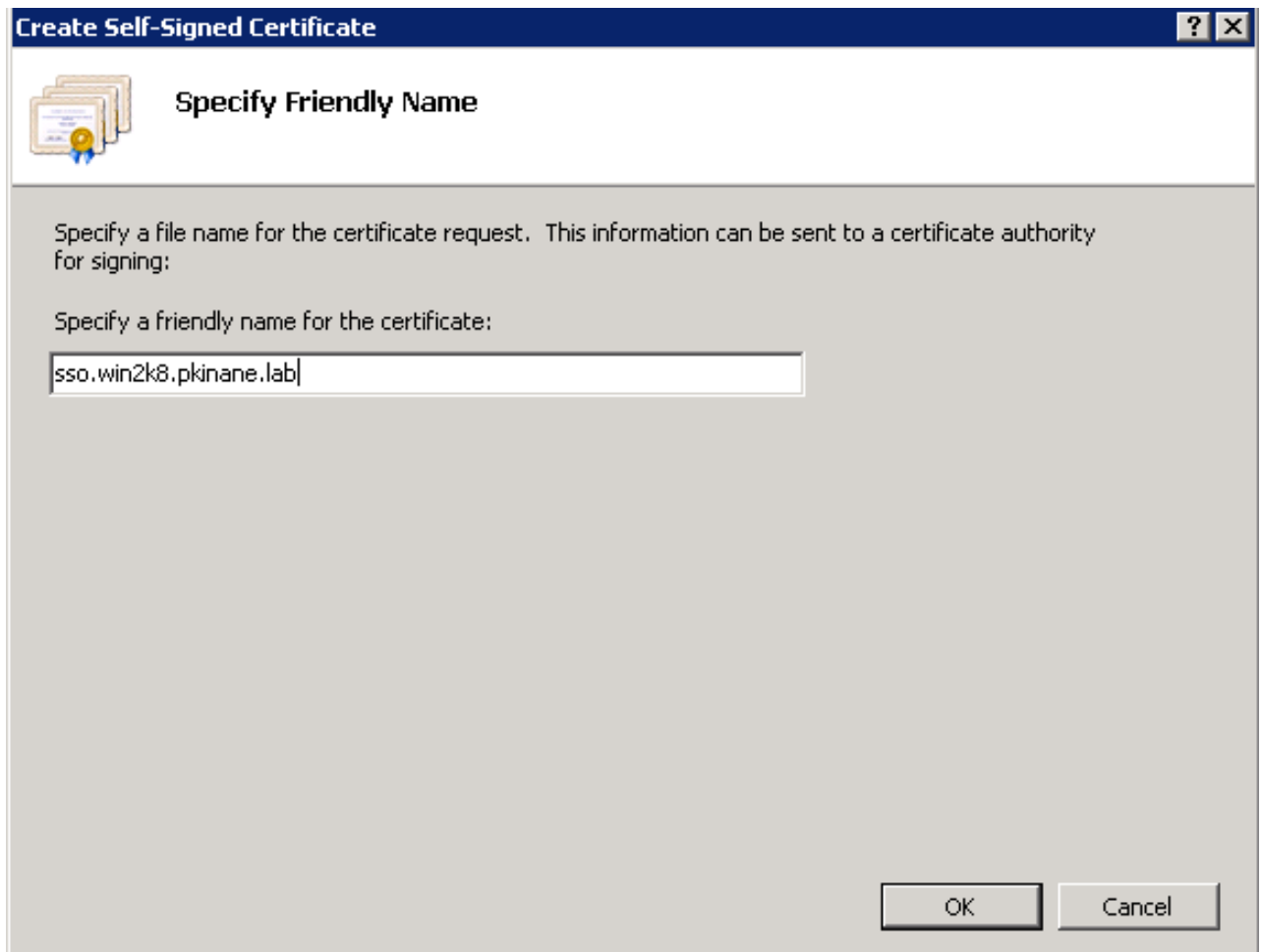
Create Self-Signed Certificate...



Help

Online Help

步驟 5.輸入您想要用作證書別名的名稱。



CUCM和IDP伺服器之間的時間不同步

如果在從CUCM運行SSO測試時收到此錯誤，則需要將Windows伺服器配置為使用與CUCM相同的NTP伺服器。

無效的SAML響應。當Cisco Unified Communications Manager和IDP伺服器之間的時間不同步時，可能會造成這種情況。請驗證兩台伺服器上的NTP配置。從CLI運行「utils ntp status」以檢查Cisco Unified Communications Manager上的此狀態。

在Windows Server指定了正確的NTP伺服器後，您需要執行另一個SSO測試並檢視問題是否仍然存在。在某些情況下，有必要歪曲宣告的有效期。關於這一過程的更多詳細資訊。

相關資訊

- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。