用於SAML SSO的AD FS 2.0版設定配置示例

目錄

簡介

本文說明如何配置Active Directory聯合身份驗證服務(AD FS)版本2.0，以便為思科合作產品(如Cisco Unified Communications Manager(CUCM)、Cisco Unity Connection(UCXN)、CUCM IM and Presence和Cisco Prime Collaboration)啟用安全斷言標籤語言(SAML)單一登入(SSO)。

必要條件

需求

必須安裝和測試AD FS 2.0版。

> **注意**：本安裝指南基於實驗室設定，假設AD FS 2.0版僅用於帶有Cisco Collaboration產品的SAML SSO。如果其他業務關鍵型應用程式使用它，則必須根據官方Microsoft文檔進行必要的自定義。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- AD FS版本2.0
- Microsoft Internet Explorer 10
- CUCM版本10.5

- Cisco IM和狀態伺服器版本10.5
- UCXN版本10.5
- Cisco Prime合作布建10.5

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

下載AD FS 2.0版身份提供程式(IdP)後設資料

若要下載IdP後設資料，請在瀏覽器上運行此連結：https://<ADFS的FQDN>/FederationMetadata/2007-06/FederationMetadata.xml。

下載合作伙服器(SP)後設資料

CUCM IM和狀態服務

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

Unity Connection

開啟Web瀏覽器，以管理員身份登入UCXN，然後導航至**系統設定>SAML單一登入**。

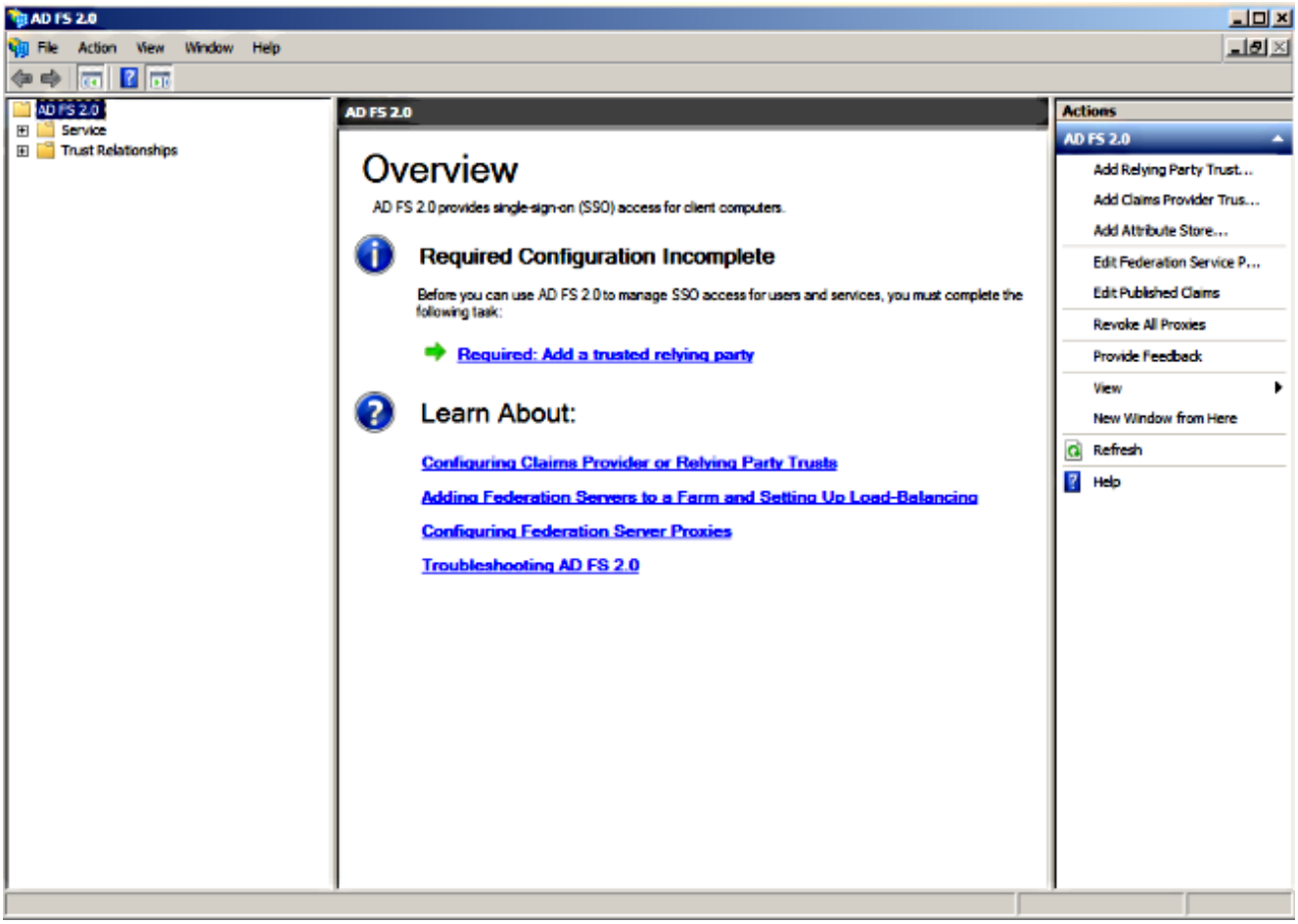
Cisco Prime Collaboration Provisioning

開啟Web瀏覽器，以globaladmin身份登入到Prime Collaboration Assurance，然後導航到**Administration > System Setup > Single Sign On**。

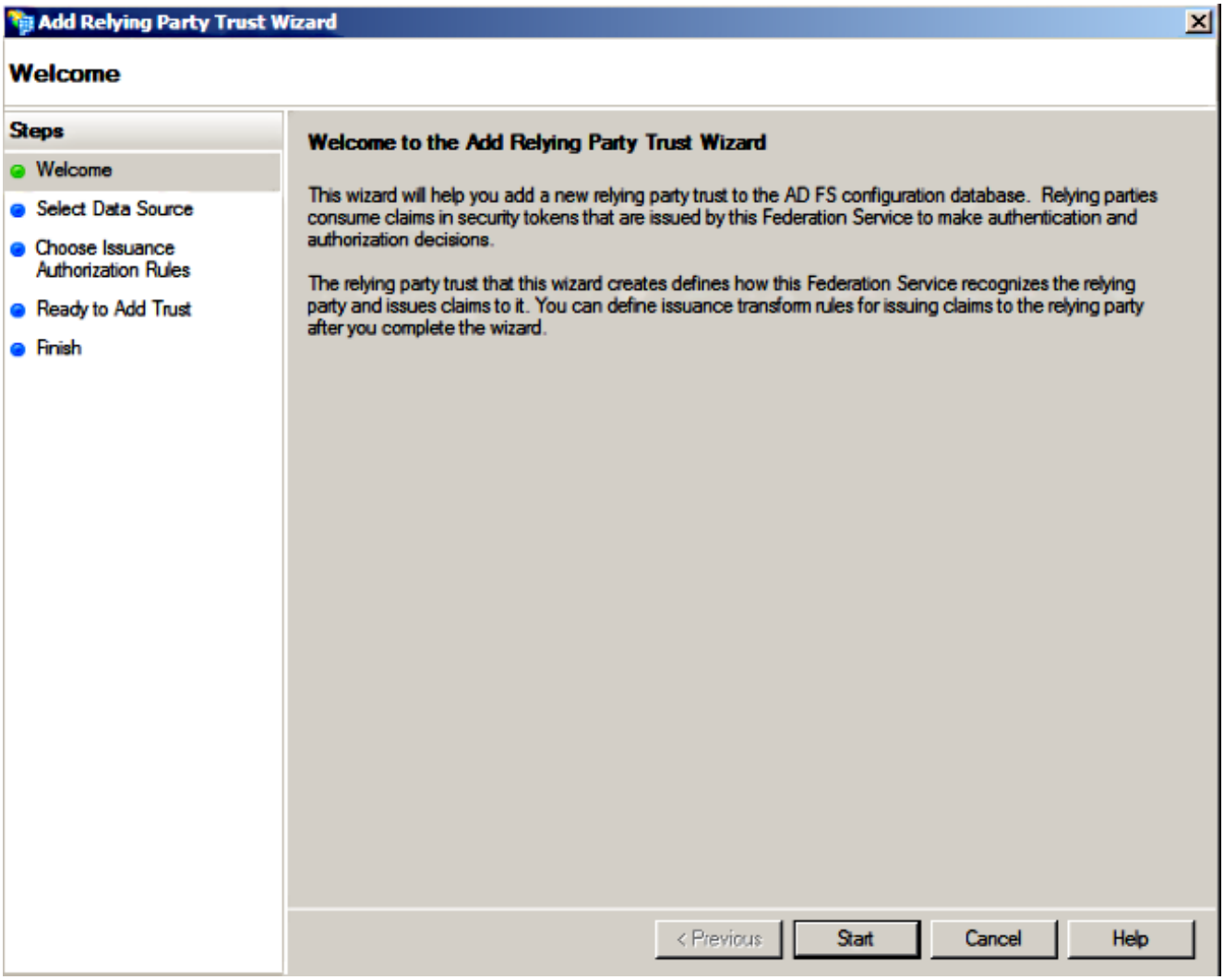
將CUCM新增為信賴方信任

1. 登入到AD FS伺服器並從Microsoft Windows程式選單啟動AD FS版**本2**.0。

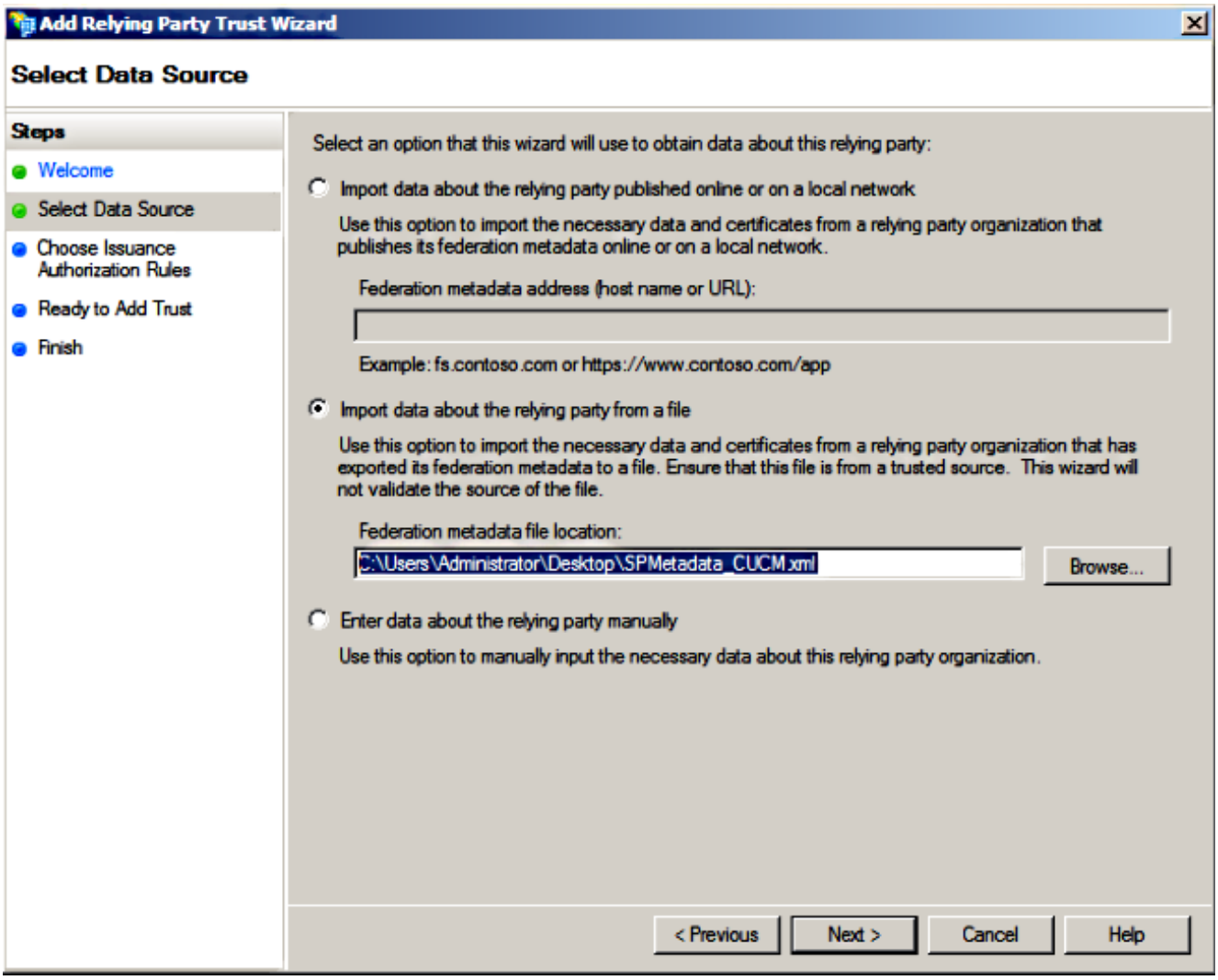
2. 選擇**新增信賴方信任**。


AD FS 2.0
File Action View Window Help
AD FS 2.0
Service
Trust Relationships
AD FS 2.0
Overview
AD FS 2.0 provides single-sign-on (SSO) access for client computers.
Required Configuration Incomplete
Before you can use AD FS 2.0 to manage SSO access for users and services, you must complete the following task:
Required: Add a trusted relying party
Learn About:
Configuring Claims Provider or Relying Party Trusts
Adding Federation Servers to a Farm and Setting Up Load-Balancing
Configuring Federation Server Proxies
Troubleshooting AD FS 2.0
Actions
AD FS 2.0
Add Relying Party Trust...
Add Claims Provider Trus...
Add Attribute Store...
Edit Federation Service P...
Edit Published Claims
Revoke All Proxies
Provide Feedback
View
New Window from Here
Refresh
Help

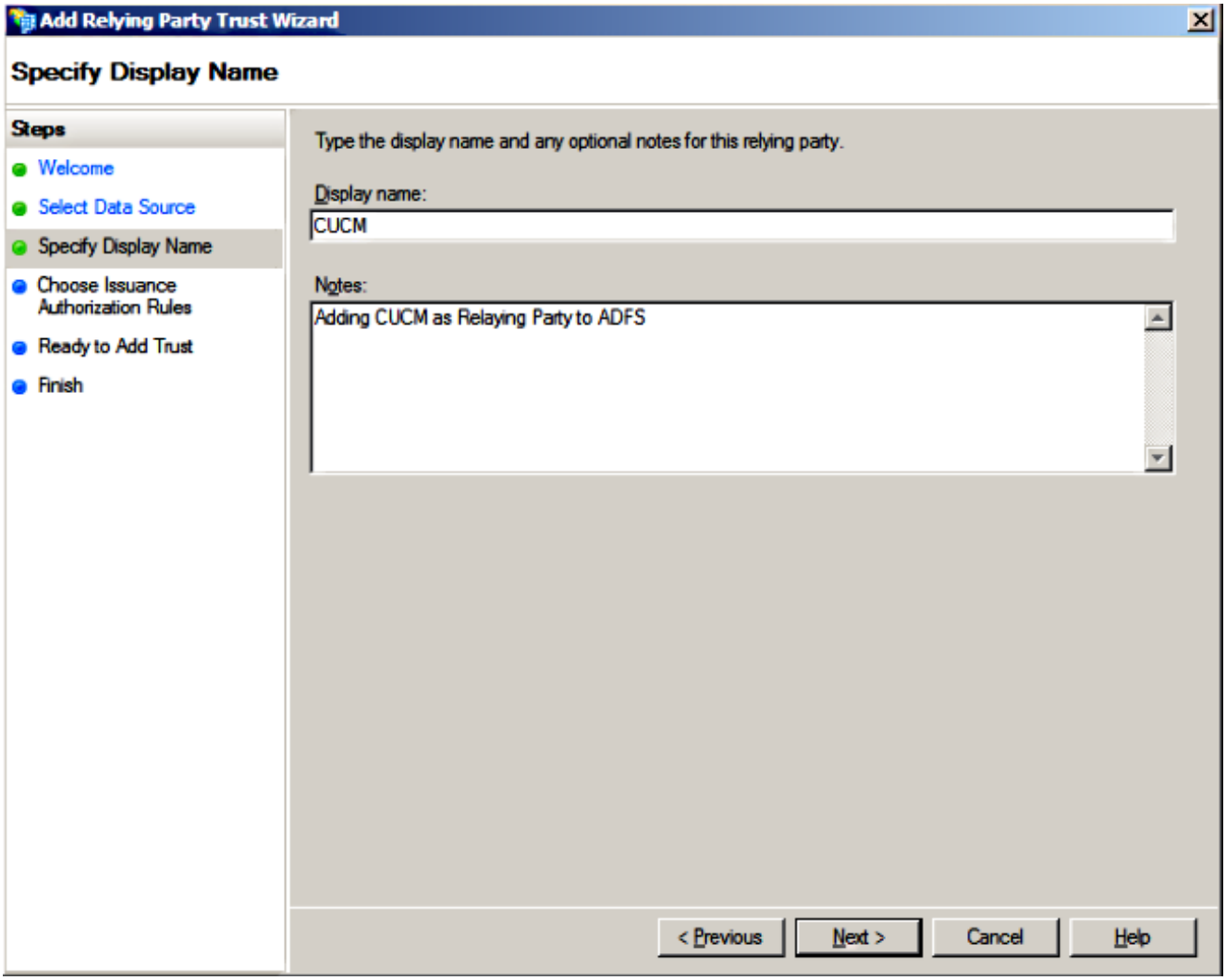
3. 按一下「Start」。



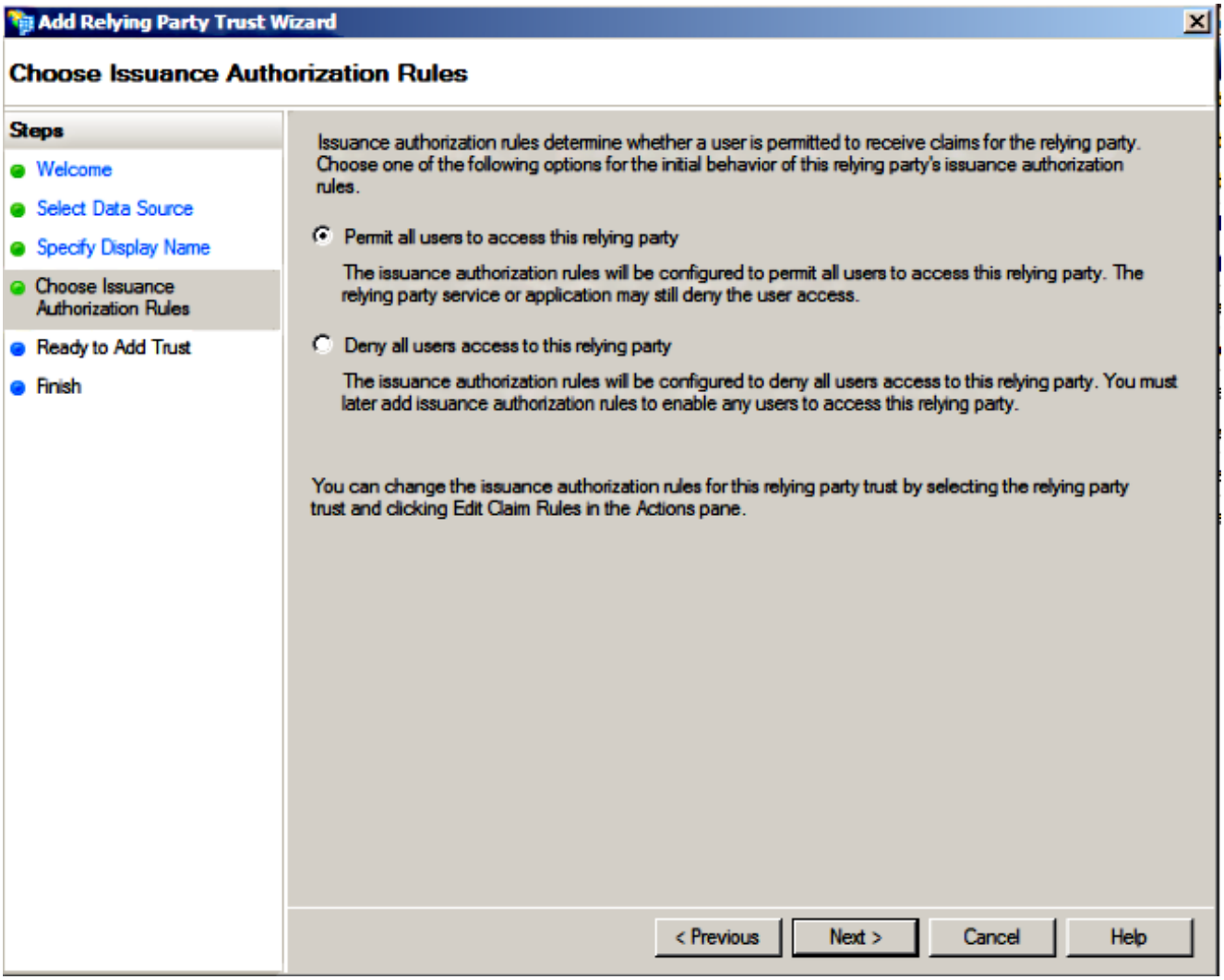
4. 選擇**Import data about the relisting party from a file**選項，選擇之前從CUCM下載的**SPMetadata_CUCM.xml**後設資料檔案，然後按一下**Next**。



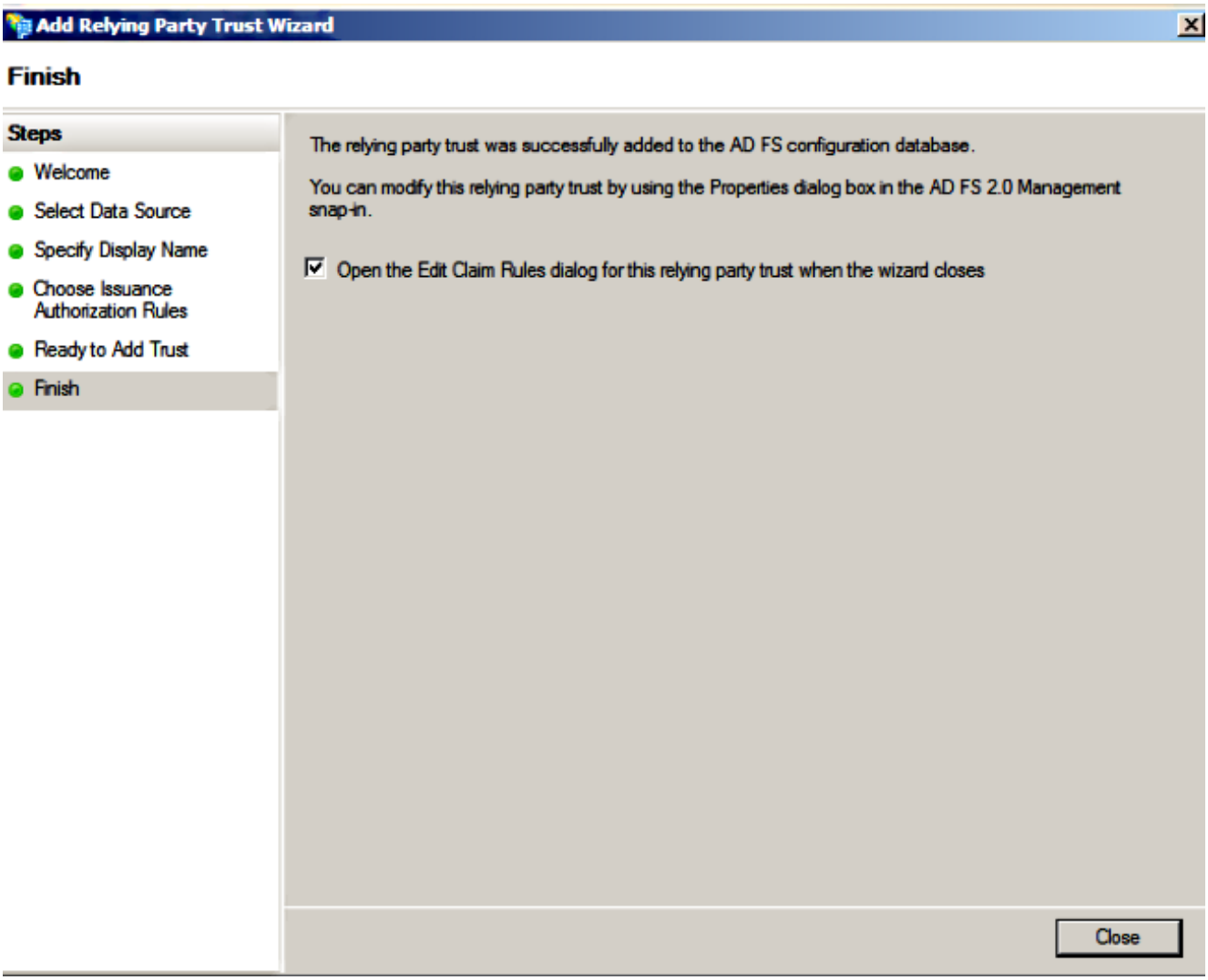
5. 輸入**顯示名稱**，然後按一下**下一步**。



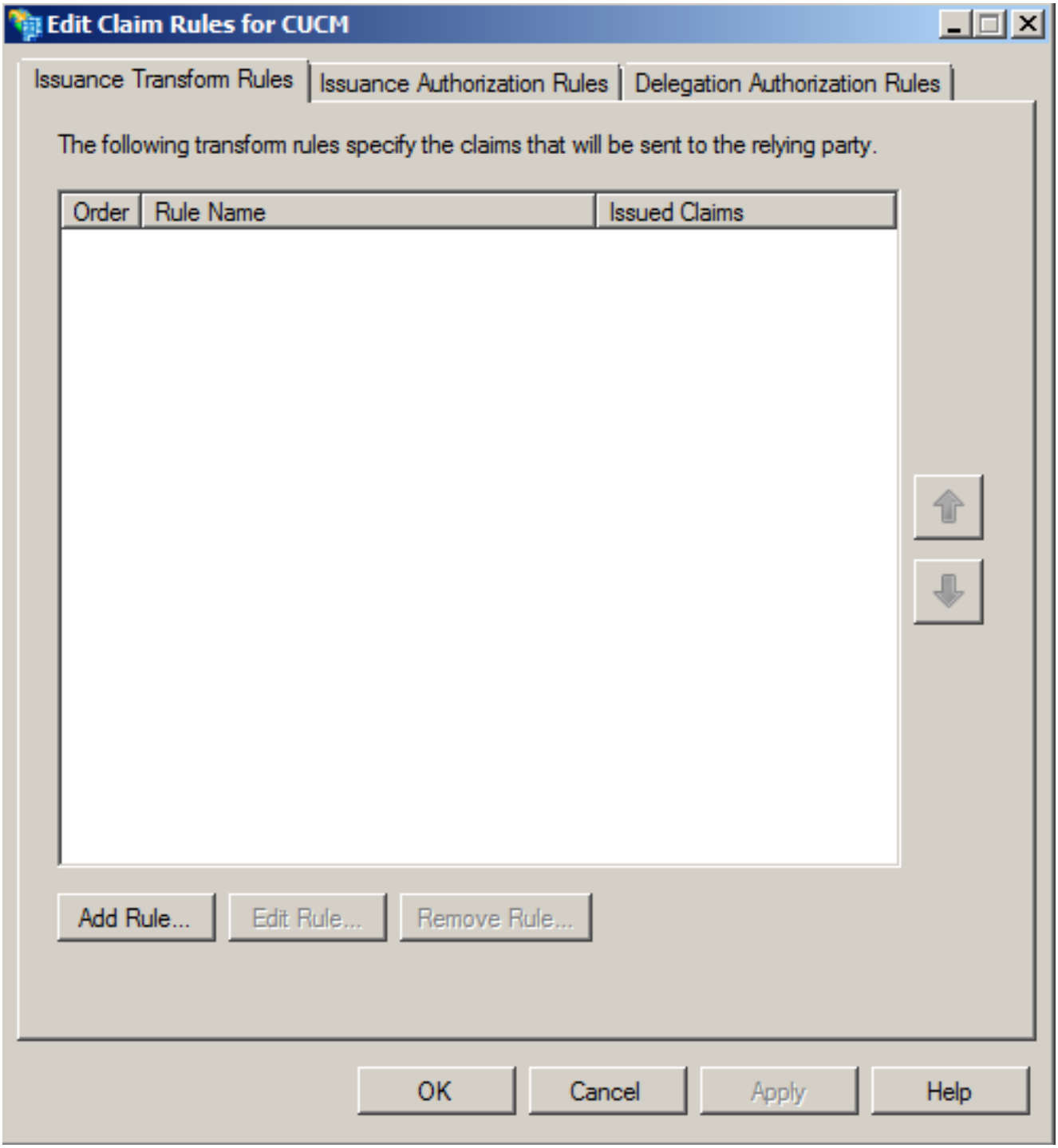
6. 選擇**允許所有使用者訪問此信賴方**，然後按一下**下一步。**



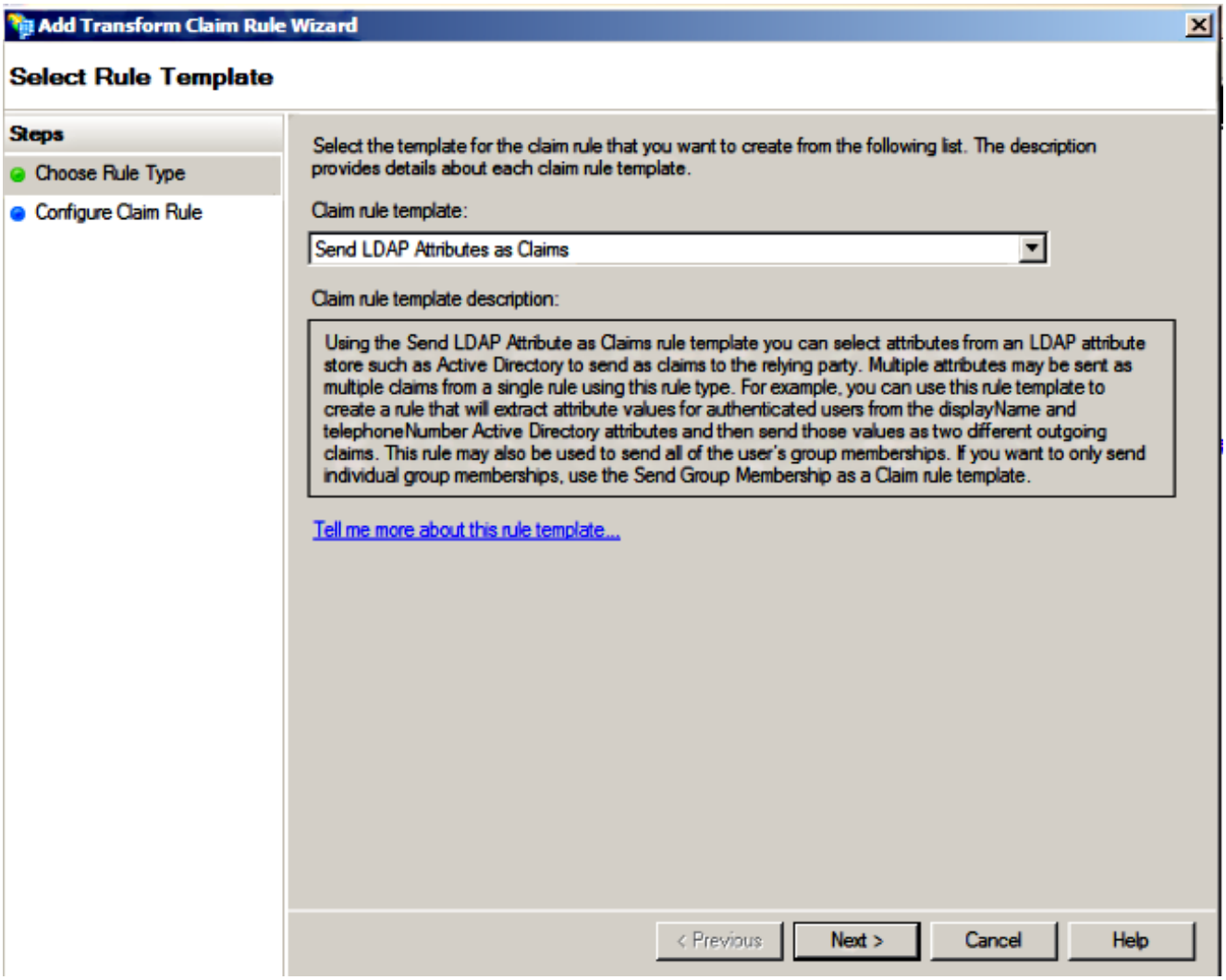
7. 選擇嚮導關閉時為信賴方信任開啟「編輯宣告規則」對話方塊，然後單擊「關閉」。



8. 按一下「Add Rule」。

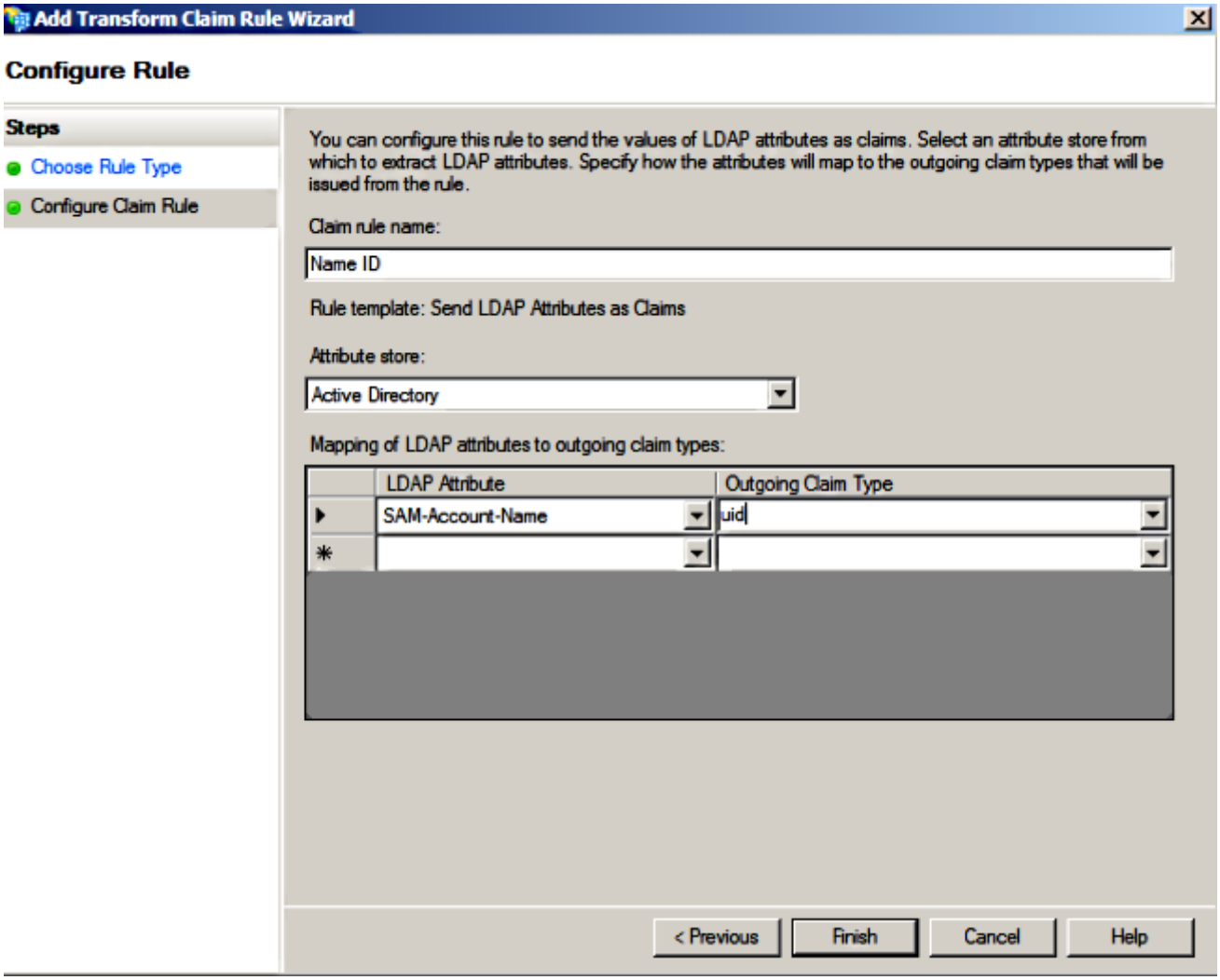


9. 按一下**Next**，預設宣告規則模板設定為**Send LDAP Attributes as Claims**。

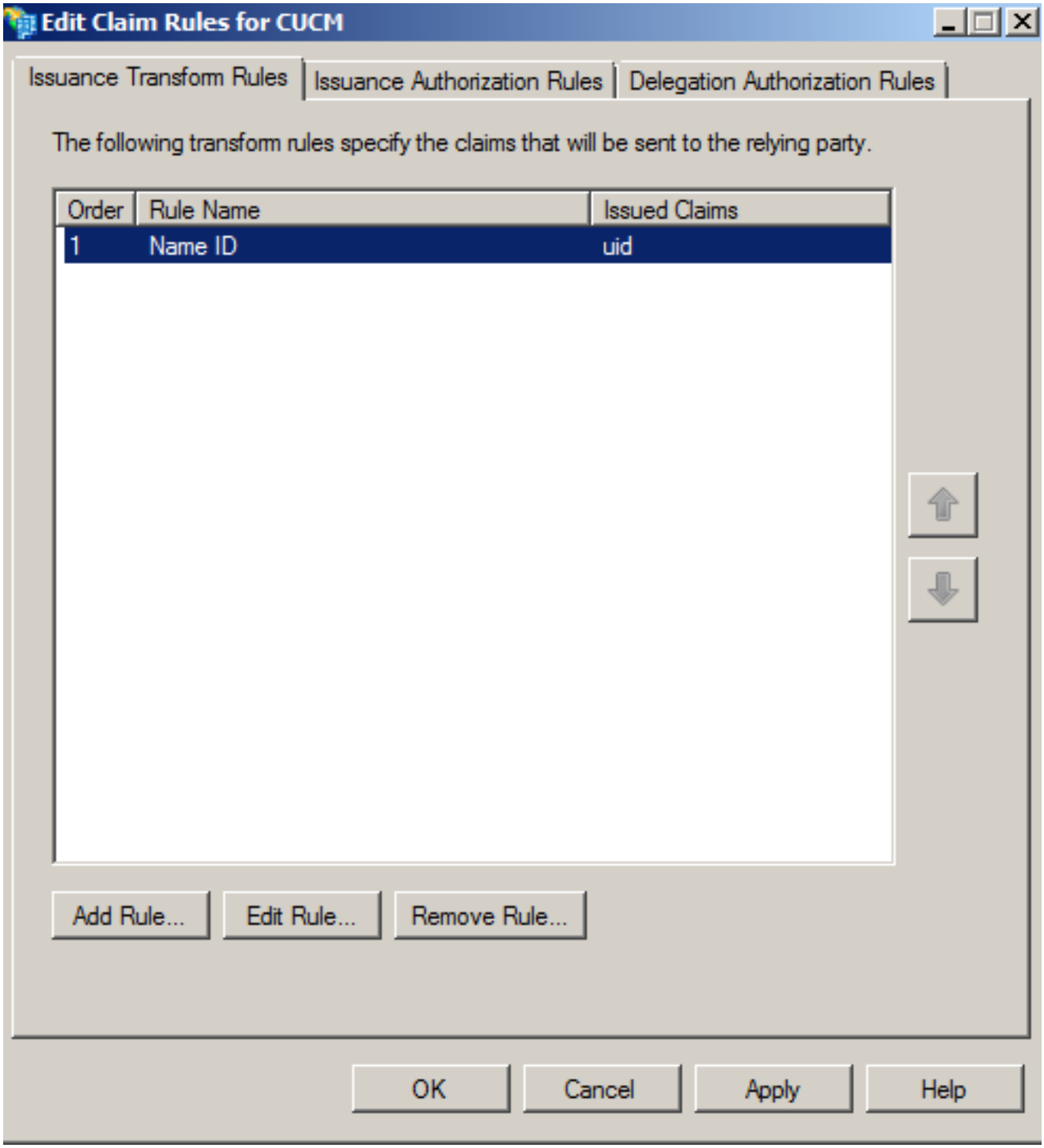


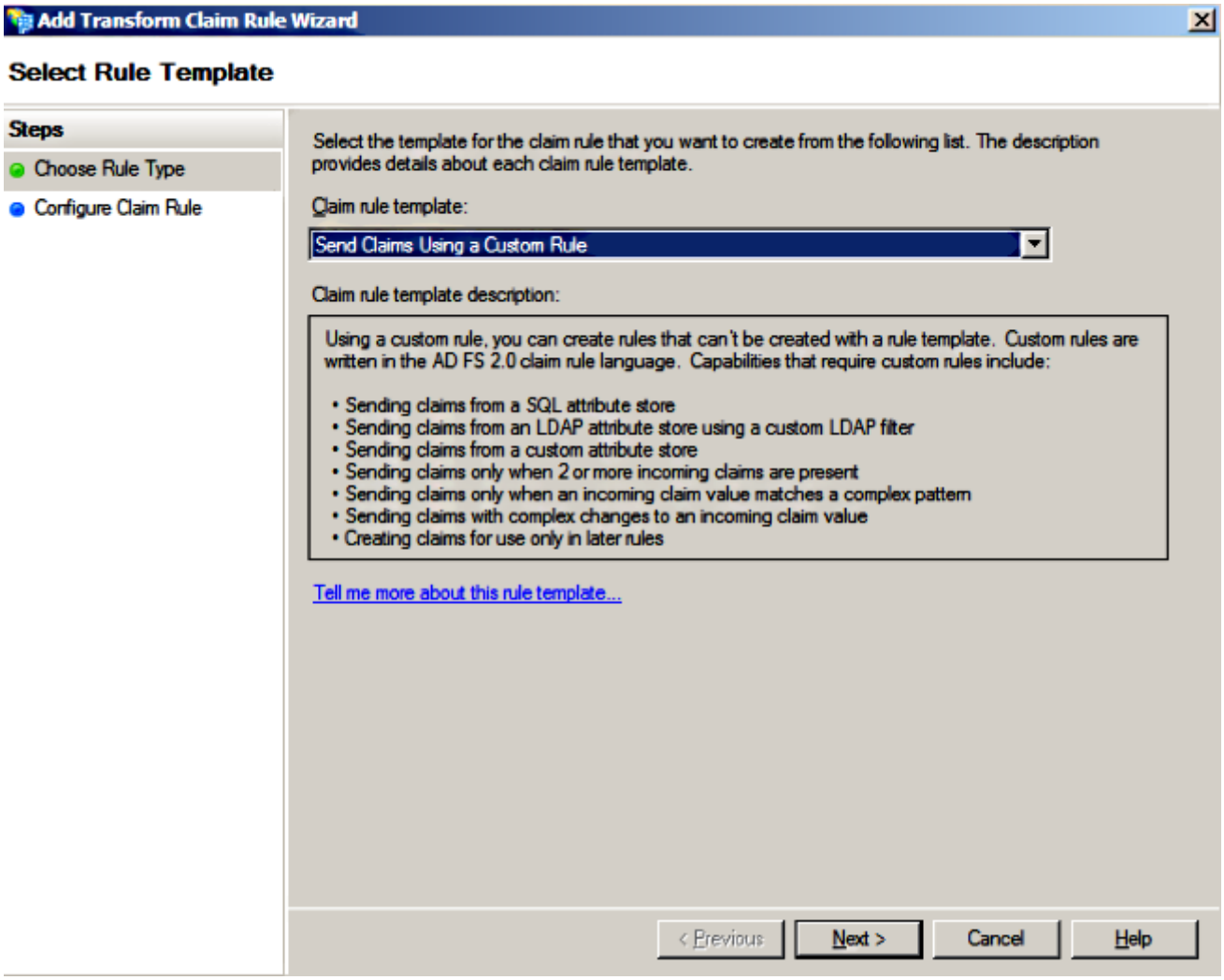
10. 在Configure Rule中，輸入宣告規則名稱，選擇**Active Directory**作為屬性儲存，配置**LDAP Attribute**和**Outgoing Claim Type**（如下圖所示），然後按一下**Finish**。

附註：
— 輕型目錄訪問協定(LDAP)屬性應與CUCM上的目錄同步屬性匹配。
- 「uid」應使用小寫。



11. 按一下**Add Rule**，選擇**Send Claims Using a Custom Rule**作為宣告規則模板，然後按一下**Next**。

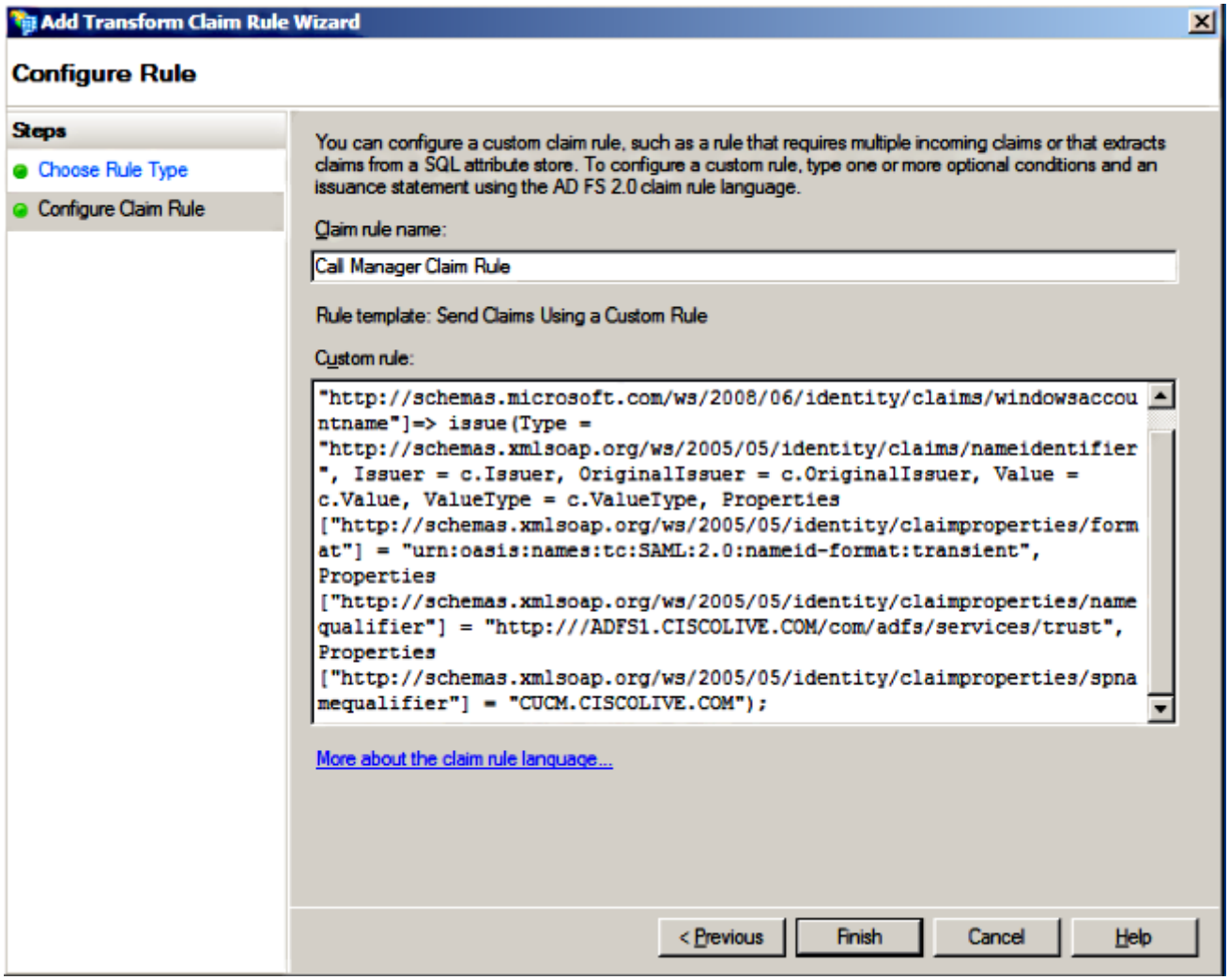

Edit Claim Rules for CUCM
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
The following transform rules specify the claims that will be sent to the relying party.
Order
Rule Name
Issued Claims
1
Name ID
uid
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply
Help



12. 輸入宣告規則名稱的名稱，並在Custom rule下提供的空格中複製以下語法：

```
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>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier
"] = "<FQDN of CUCM>");
```

(附註： 如果複製並貼上來自這些示例的文本，請注意某些字處理軟體將用UNICODE版本("")替換ASCII引號(")。UNICODE版本將導致宣告規則失敗。)



附註：
— 在此示例中，CUCM和ADFS完全限定域名(FQDN)預填充了實驗CUCM和AD FS，必須對其進行修改以匹配您的環境。
- CUCM/ADFS的FQDN區分大小寫，必須與後設資料檔案匹配。

13. 按一下「**Finish**」（結束）。

14. 按一下「**Apply**」，然後「**OK**」。

15. 從**Services.msc**重新啟動AD FS版本2.0服務。

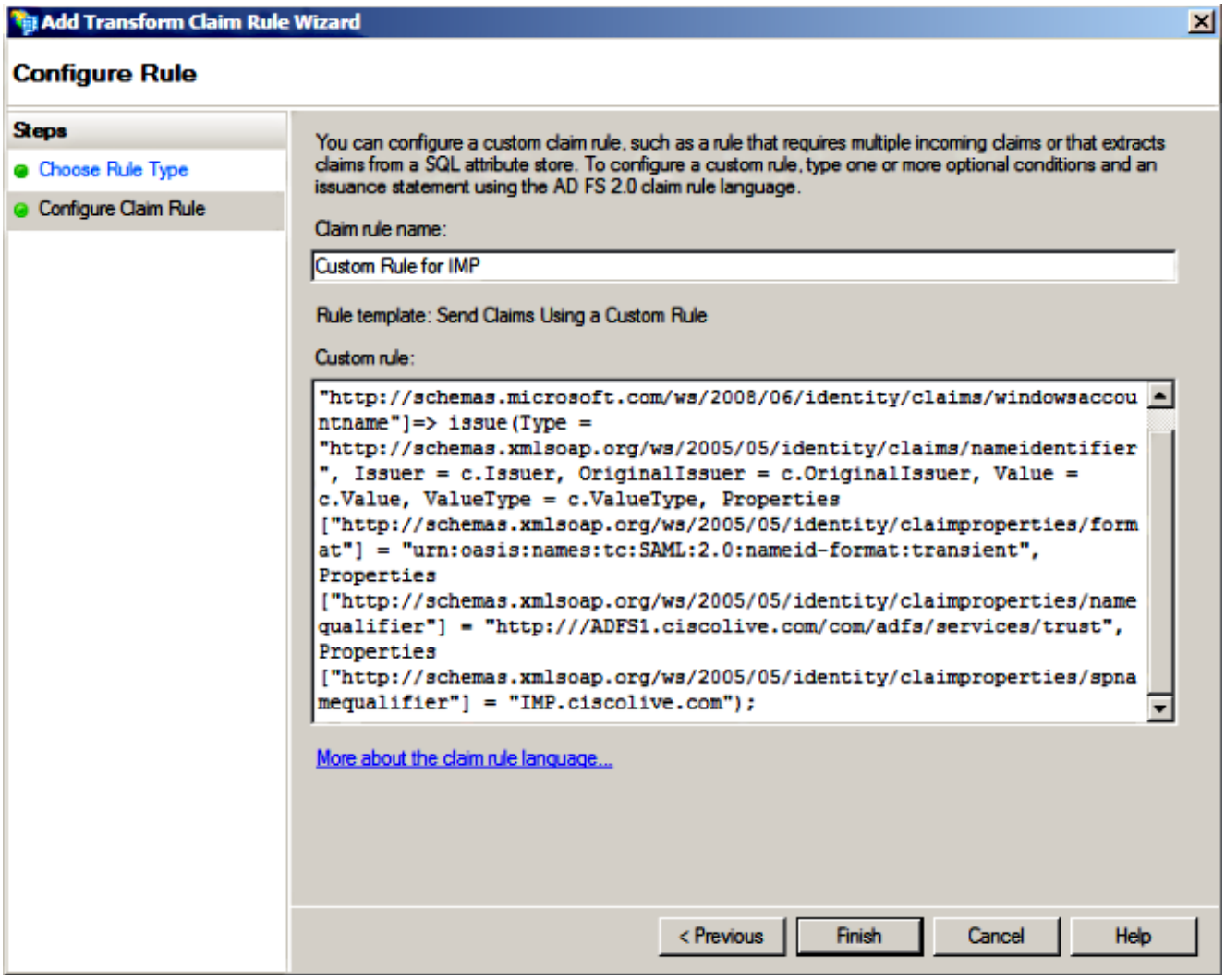
將CUCM IM和線上狀態新增為信賴方信任

1. 按照**將CUCM新增為信賴方信任**的說明，重複步驟1至11，然後繼續執行步驟2。

2. 輸入宣告規則名稱的名稱，並在Custom rule下提供的空格中複製以下語法：

```
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>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of IMP>");
```



請注意，本示例中的IM and Presence和AD FS FQDN預填充了實驗IM and Presence和AD FS，必須對其進行修改以匹配您的環境。

3. 按一下「**Finish**」（結束）。

4. 按一下「**Apply**」，然後「**OK**」。

5. 從**Services**.msc重新啟動AD FS版本2.0**服務**。

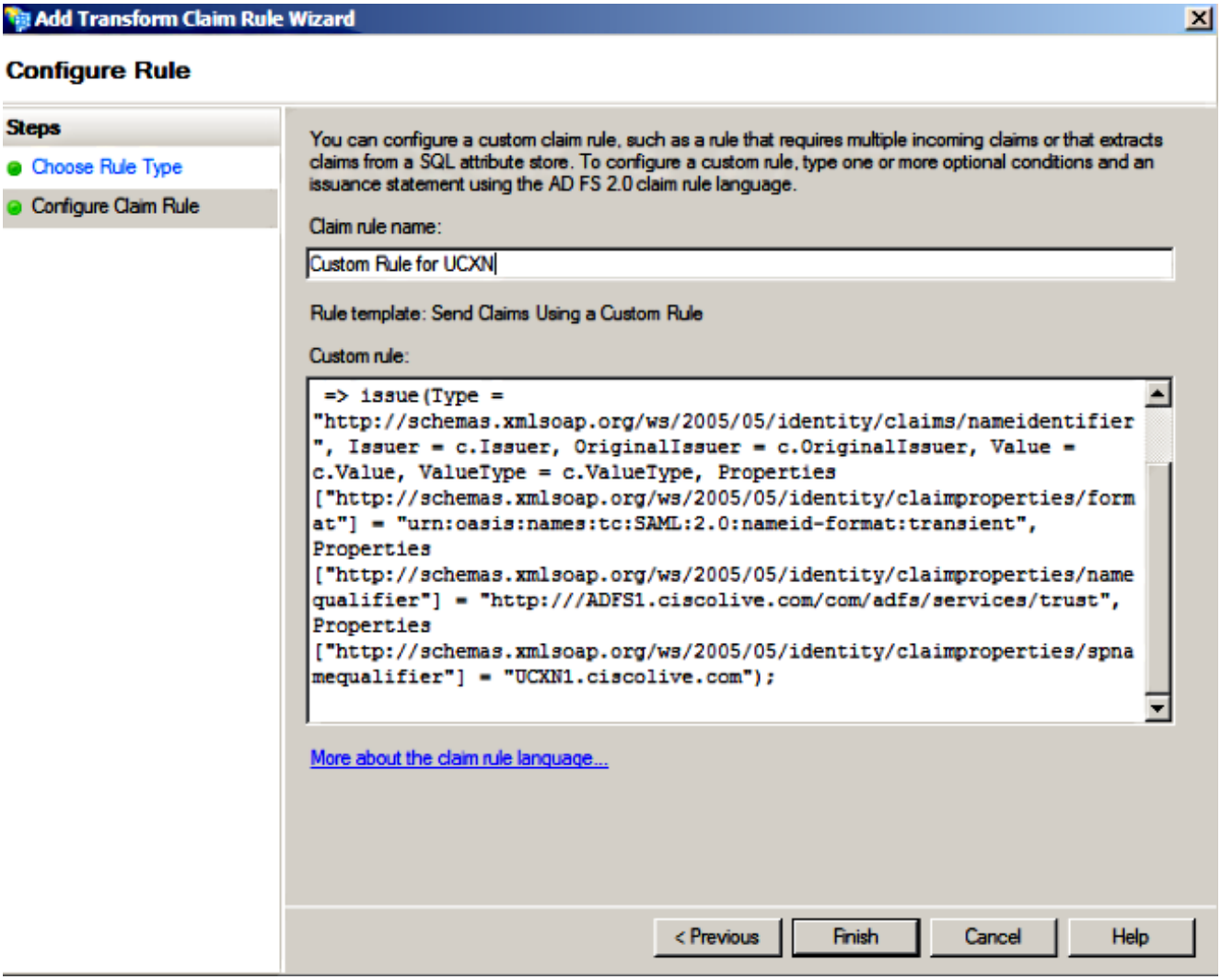
將UCXN新增為信賴方信任

1. 按照**將CUCM新增為信賴方信任**的說明，重複步驟1至12，然後繼續執行步驟2。

2. 為宣告規則名稱輸入一個名稱，並在自定義規則下提供的空白處復制以下語法:

```
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>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of UCXN>");
```



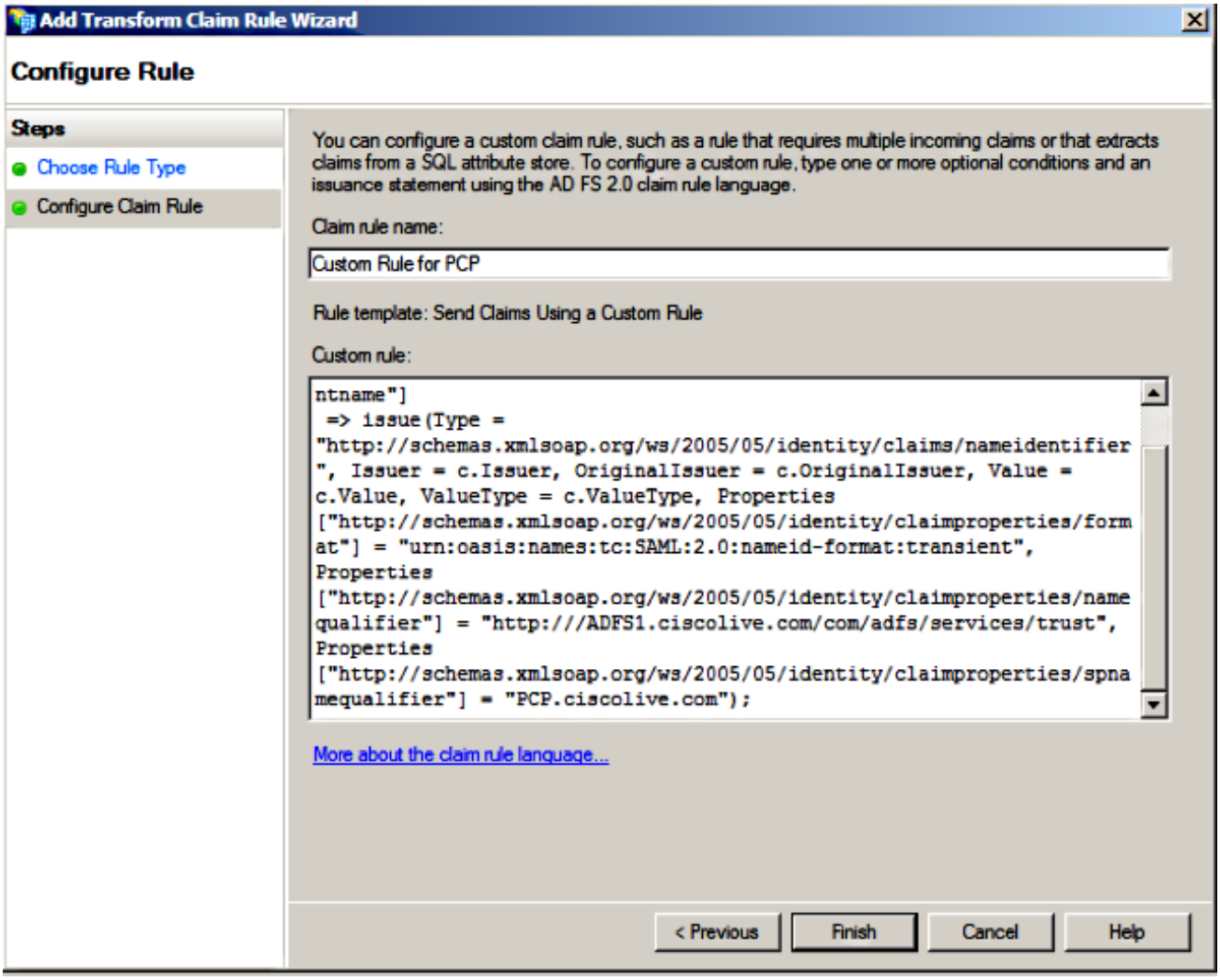
請注意，在此示例中，UCXN和AD FS FQDN預填充了實驗UCXN和ADFS，必須對其進行修改才能與您的環境匹配。

3. 按一下「**Finish**」（結束）。
4. 按一下「**Apply**」，然後「**OK**」。
5. 從**Services**.msc重新啟動AD FS版本2.0**服務。**

將Cisco Prime合作調配新增為信賴方信任

1. 按照**將CUCM新增為信賴方信任**的說明，重複步驟1至12，然後繼續執行步驟2。
2. 輸入宣告規則名稱的名稱，並在Custom rule下提供的空白處復制以下語法：

```
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>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of PCP>");
```



請注意，Prime Provisioning和AD FS FQDN已預填充本示例中的實驗室Prime Collaboration Provisioning(PCP)和AD FS，必須對其進行修改才能與您的環境匹配。

3. 按一下「**Finish**」（結束）。
4. 按一下「**Apply**」，然後「**OK**」。
5. 從**Services.msc**重新啟動AD FS版本2.0服務。

設定AD FS版本2.0後，繼續啟用思科合作產品上的SAML SSO。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

AD FS將診斷資料記錄到系統事件日誌。 從AD FS伺服器上的伺服器管理器開啟**Diagnostics -> Event Viewer -> Applications and Services -> AD FS 2.0 -> Admin**

查詢AD FS活動記錄的錯誤