

為ESA和SMA配置使用AD FS的SAML SSO外部身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[適用於SAML的ADFS IDP配置步驟](#)

[配置信賴方信任](#)

[方法A:通過匯入SP後設資料建立信賴方信任](#)

[配置信賴方信任終結點\(僅限群集\)](#)

[頒發轉換規則—宣告](#)

[下載IdP後設資料並將其上傳到ESA](#)

[驗證](#)

[相關資訊](#)


簡介

本文檔介紹如何將Active Directory聯合身份驗證服務配置為SAML身份提供程式，以便在Cisco ESA和SMA上進行外部身份驗證。

必要條件

本文檔提供了工程師無法以其他方式看到的第三方應用程式的檢視。

- 針對思科郵件安全裝置(ESA)和安全管理裝置(SMA)的最新版本，使用Active Directory聯合身份驗證服務(AD FS)2012和2016進行安全宣告標籤語言(SAML)外部身份驗證的配置步驟。
- 不包括專門部署特定配置的基本實驗室步驟。
- 與生產部署不同的實驗室環境的工作示例。

 **注意：**在此過程之前完成服務提供商(SP)配置。請參閱。

需求

- Microsoft Active Directory聯合身份驗證服務(AD FS)2012或2016
- 思科電子郵件安全裝置(ESA)和安全管理裝置(SMA)最新版本。

採用元件

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。

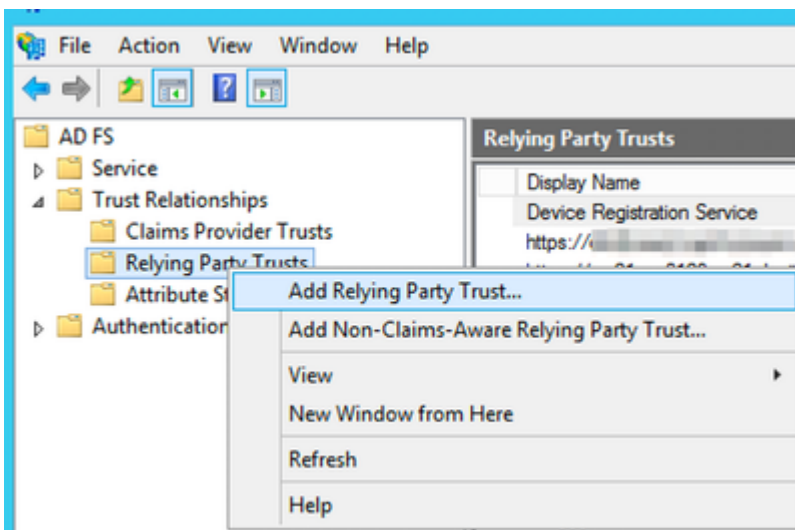
適用於SAML的ADFS IDP配置步驟

配置信賴方信任

使用兩個選項之一在AD FS中建立信賴方信任。

方法A:通過匯入SP後設資料建立信賴方信任

1. 從管理工具中開啟AD FS管理控制檯。
2. 在AD FS管理控制檯中，展開Trusted Relationships，按一下右鍵Relying Party Trusts，然後選擇Add Relying Party Trust。



新增信賴方信任

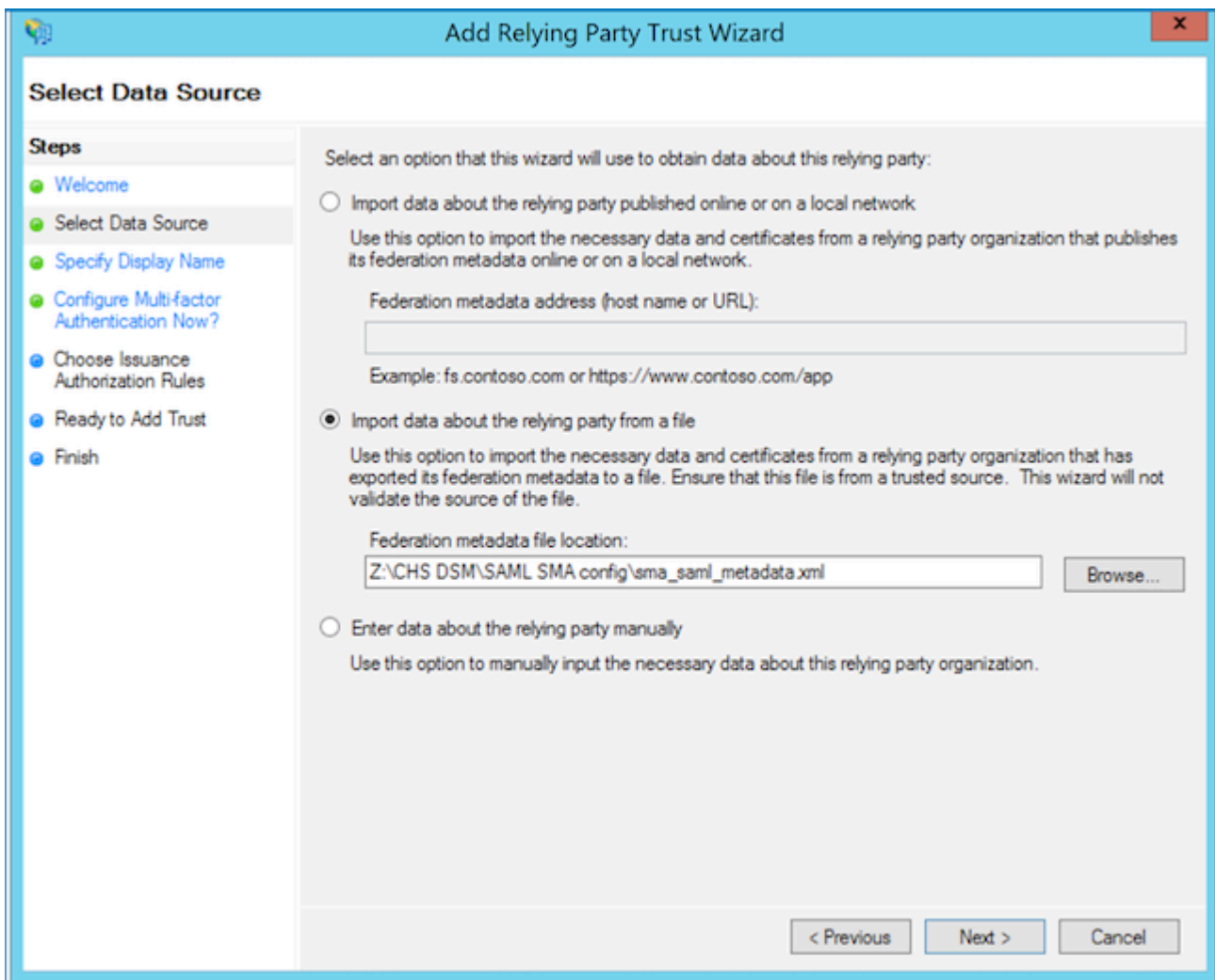
 提示：[Microsoft信賴方信任](#)

使用以下兩個選項之一繼續操作：

- 選項 A：從檔案匯入有關信賴方的資料。上傳ESA或SMA服務提供商(SP)metadata.xml檔案。
- 選項 B：手動輸入有關信賴方的資料。該選項指導您完成手動配置。

選項 A：從檔案匯入有關信賴方的資料。上傳ESA或SMA服務提供商(SP)metadata.xml檔案。

1. 選擇選項以從檔案匯入有關信賴方的資料，然後選擇下一步。



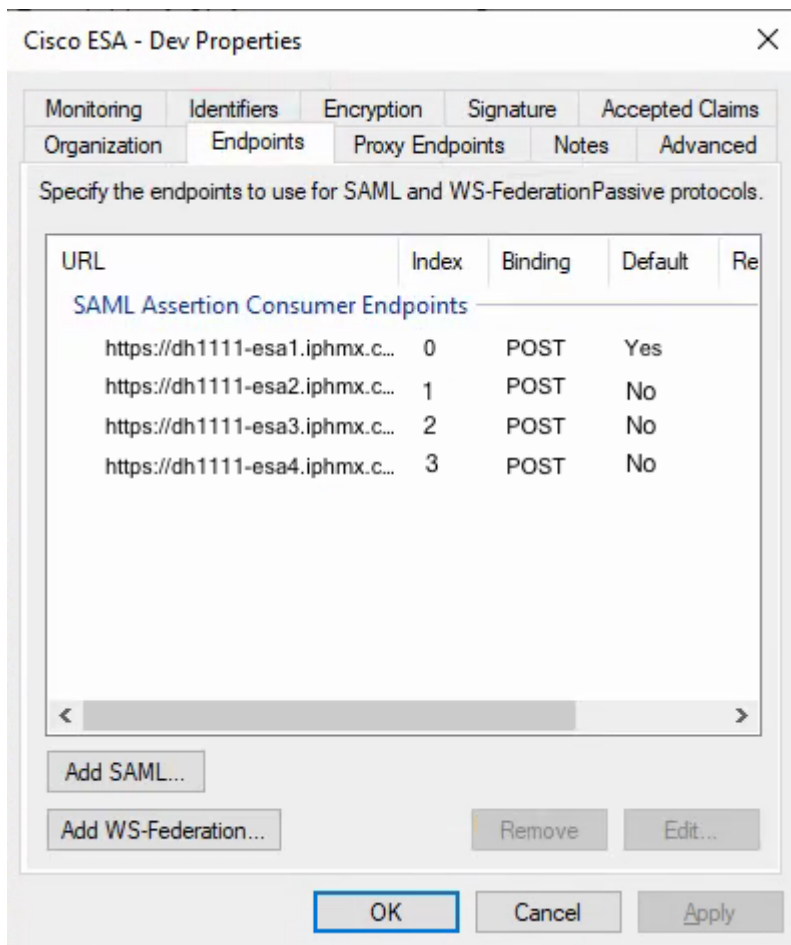
匯入ESA/SMA後設資料檔案

- 指定顯示名稱以標識此信賴方信任，然後選擇Next兩次。
- 對於頒發授權規則，請選擇Permit all users，然後選擇Next。
- 在Ready to Add Trust頁面上，接受預設設定，然後選擇Next。
- 選擇完成。這將開啟信賴方信任的「編輯宣告規則」對話方塊，該對話方塊在Issuance Transform Rules - Claims中介紹。

信賴方信任屬性 — 終端

僅當集群中存在多個ESA時才執行此步驟。

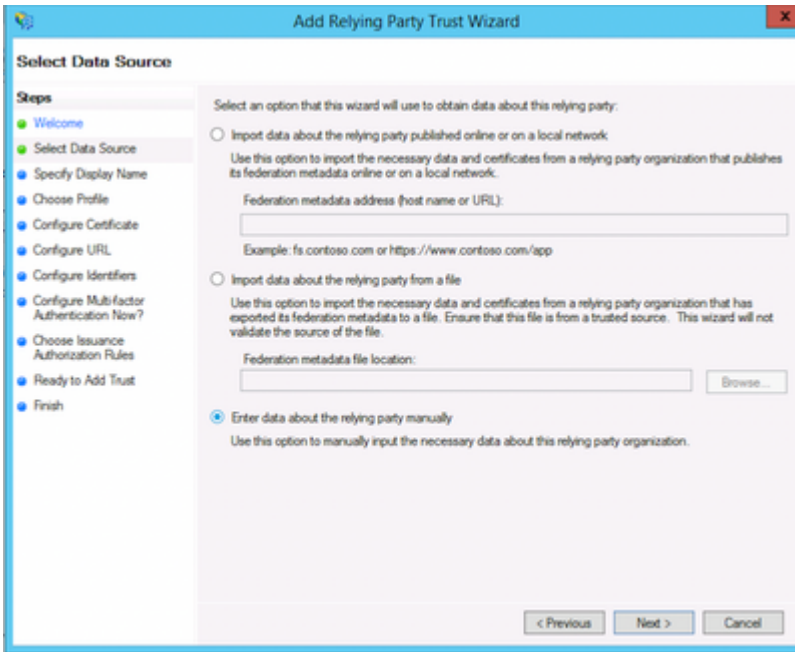
1. 開啟信賴方信任屬性>終結點。
2. 新增每個ESA可訪問URL地址，然後選擇OK。
3. 索引值從0開始計數，即0、1、2和3。
4. 僅將一個條目設定為Default = Yes。
5. 將剩餘條目設定為Default = No。



信賴方信任屬性 — 終端

選項 B：手動輸入有關信賴方的資料。該選項指導您完成手動配置。

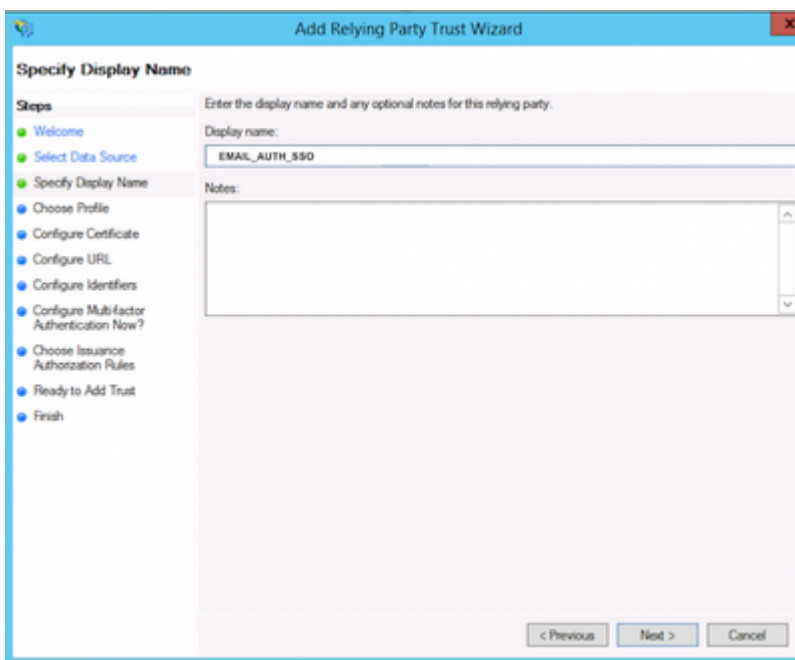
1. 選擇手動輸入有關信賴方的資料。



手動新增信賴方

 提示：顯示名稱是您選擇用於標識ESA或SMA SAML信賴方信任的名稱。

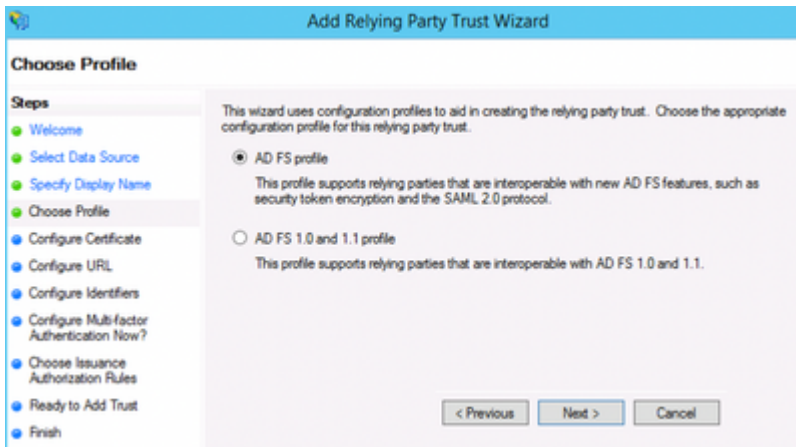
1. 輸入服務提供商的顯示名稱，例如ESA_SP。



為服務提供者配置檔案建立名稱

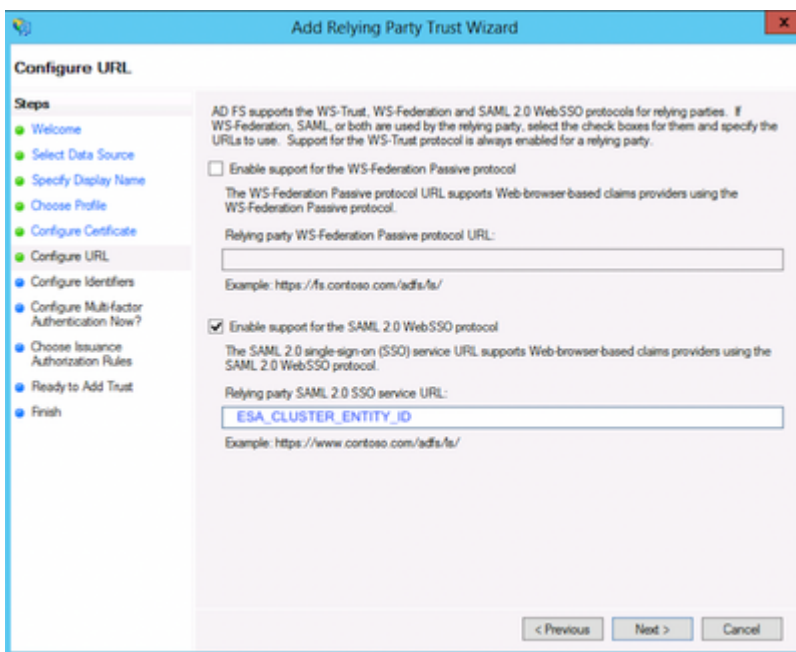
 提示：[理賠規則與發行轉換規則的作用](#)

1. 選擇配置檔案選項AD FS配置檔案。



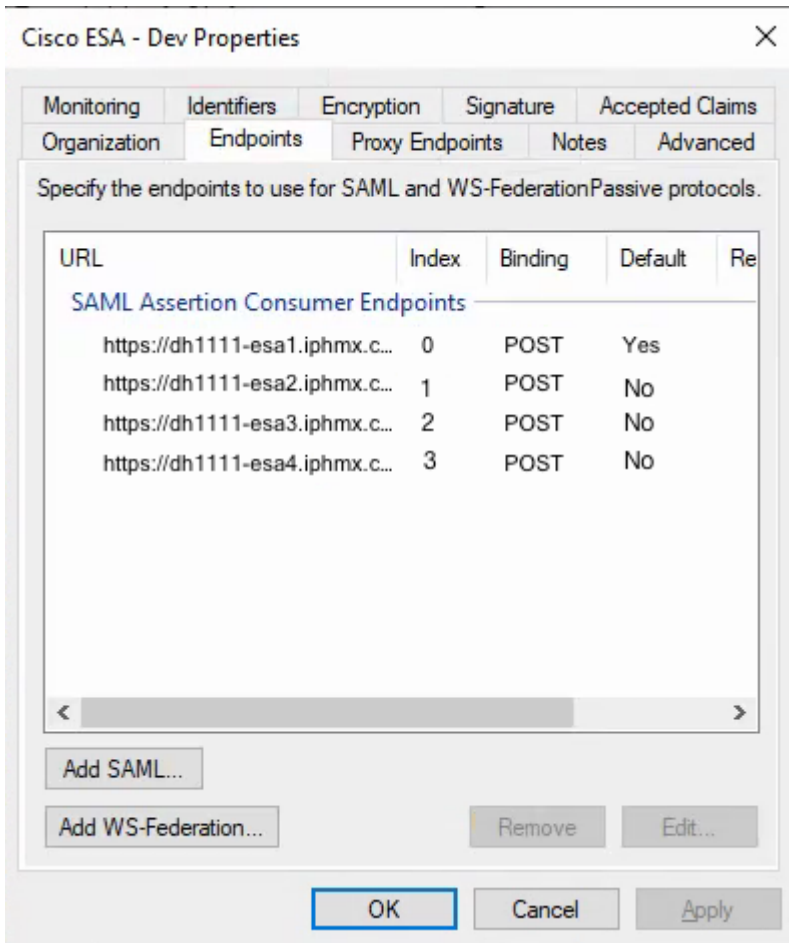
使用SAML 2.0的AD FS配置檔案選項

1. 從ESA服務提供商(SP)配置載入公共證書。
2. 對於Configure URL，選擇Enable support for the SAML 2.0 single-sign-on(SSO)。
3. 輸入具有SP配置檔案實體ID值的信賴方SAML 2.0 SSO服務URL。



頒發授權規則 — 允許所有使用者

1. 對於頒發授權規則，請選擇允許所有使用者訪問此信賴方。



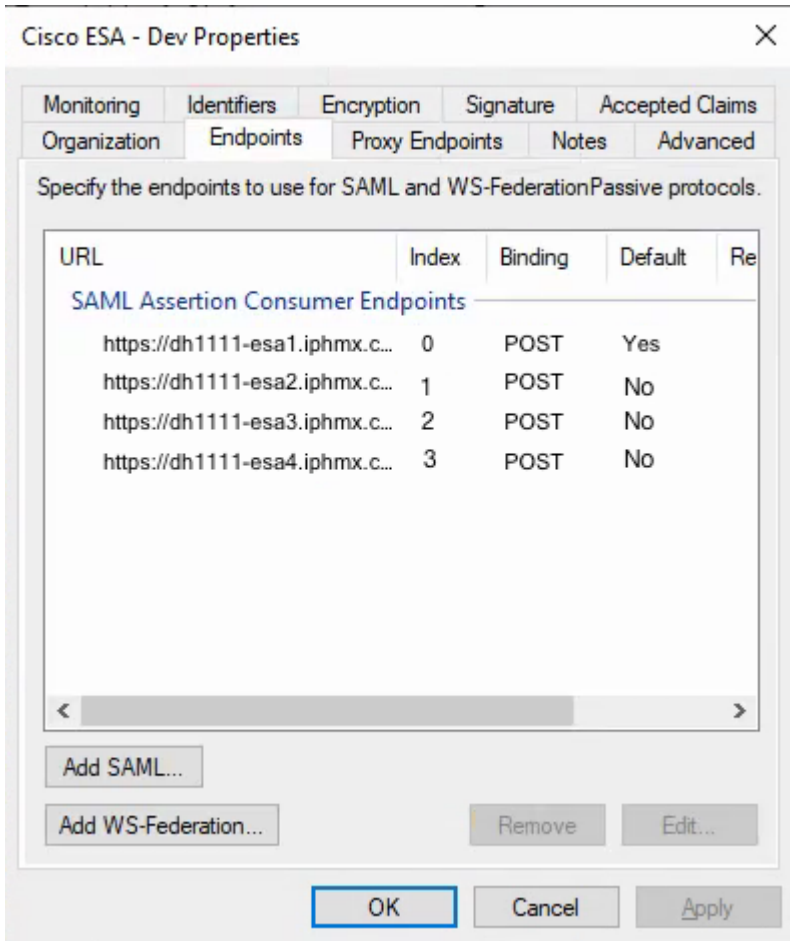
選擇頒發授權規則

1. 選擇下一步以移動到「完成」頁。

配置信賴方信任終結點 (僅限群集)

僅當集群中存在多個ESA時才執行此步驟。

1. 開啟信賴方信任屬性>終結點。
2. 新增每個ESA可訪問URL地址，然後按一下OK。
3. 設定從0開始的終結點索引值 (例如0、1、2、3)。
4. 僅將一個端點設定為Default = Yes。將剩餘終端設定為Default =否

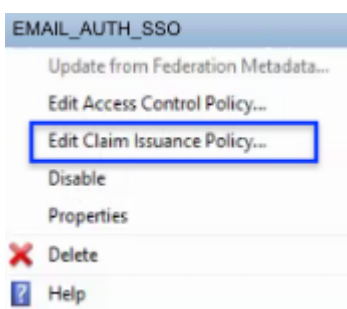


頒發授權規則 — 允許所有使用者

- 完成步驟將啟動「Issuance Transform Rules」中涵蓋的信賴方信任的「Edit Claim Rules」對話方塊。

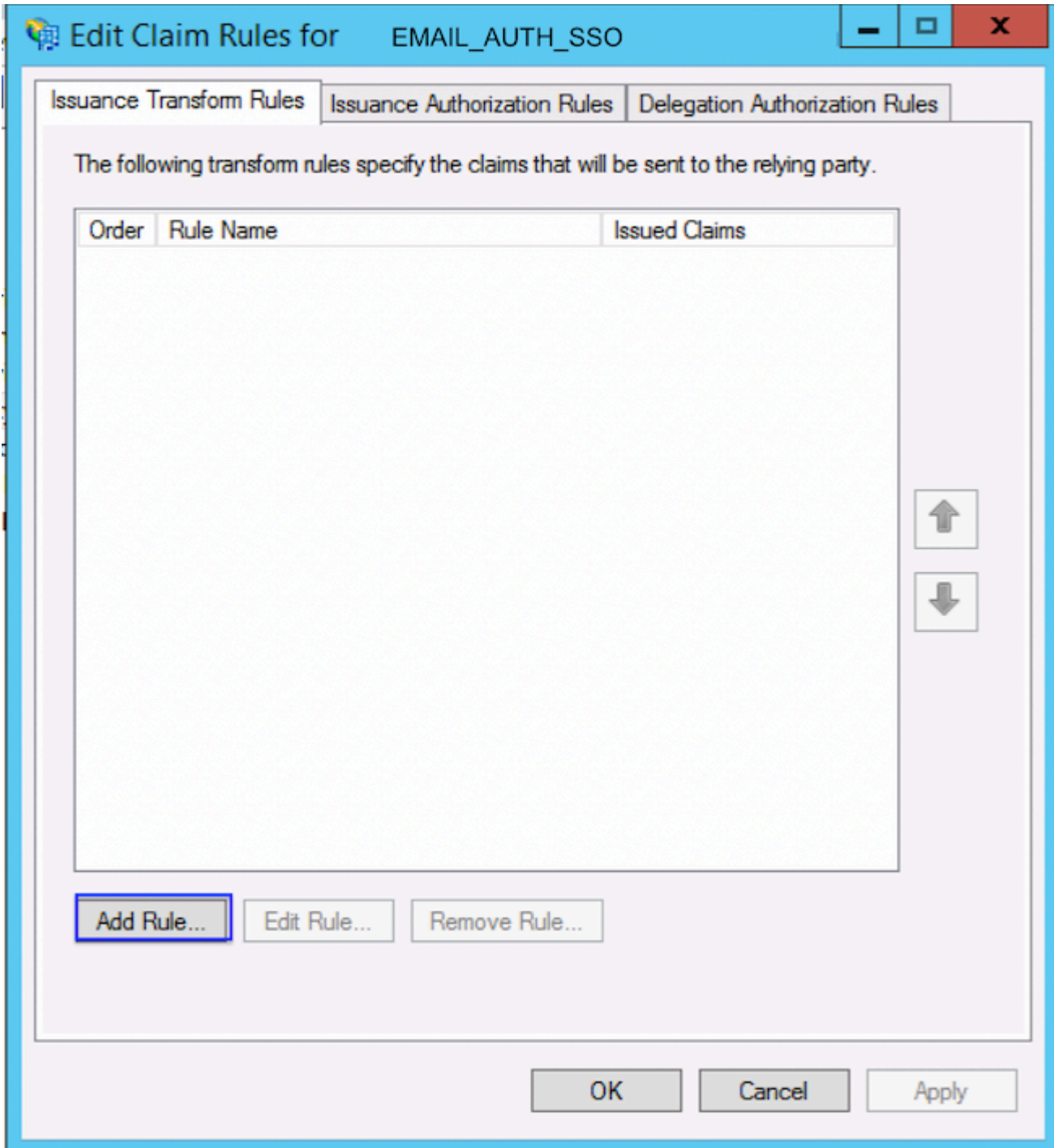
頒發轉換規則 — 宣告

- 選擇Edit Claims Issuance Policy。



編輯宣告頒發策略


- 選擇Add Rule。



新增頒發轉換規則

此處顯示的值是允許ESA在外部身份驗證設定中填充組名稱的通用值。

 提示：對映中的值可能因管理員首選項而異。

 提示：在列出的示例中，手動輸入傳出宣告類型memberOf和userPrincipalName。從下拉選單中選擇Name ID。

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

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:
LDAP

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

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)
▶	E-Mail-Addresses	Name ID
*	Token-Groups - Unqualified Names	memberOf
*	User-Principal-Name	userPrincipalName


< Previous Finish Cancel

轉換宣告規則

- 選擇完成。

下載IdP後設資料並將其上傳到ESA

完成信賴方信任和宣告規則配置後，匯出身份提供方(IdP)元數據並將其上傳到ESA。

 **注意：**重新啟動AD FS服務可能會中斷活動身份驗證會話。如果需要，在維護時段執行此步驟。

- 如果需要，請重新啟動AD FS服務。
- 運行以下命令：

```
net stop adfssrv
net start adfssrv
```

- 從此URL下載後設資料檔案：

<https://myserver.domain.com/FederationMetadata/2007-06/FederationMetadata.xml>

- 完成並返回ESA群集。

驗證

1. 在ESA或SMA中，確認IdP後設資料匯入成功完成。
2. 使用SAML單一登入(SSO)測試管理登入。
3. 驗證是否收到預期的組宣告，以及角色對映是否按預期填充到外部身份驗證配置中。

相關資訊

- [Cisco Email Security Appliance - 一般使用者指南](#)
- [思科內容安全管理裝置 — 最終使用手冊](#)

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）。