在ECE中配置代理和分割槽管理的SSO並對其進行故障排除

目錄

簡介

本檔案說明在ECE解決方案中為代理程式與分割區管理員設定單一登入(SSO)所需的步驟。

必要條件

需求

思科建議您瞭解以下主題：

思科套裝客服中心企業版(PCCE)

Cisco Unified Contact Center Enterprise (UCCE)

企業版聊天與電子郵件(ECE)

Microsoft Active Directory

採用元件

本文中的資訊係根據以下軟體和硬體版本：

UCCE版本：12.6(1)

ECE版本：12.6(1)

Windows Server 2016上的Microsoft Active Directory Federation Service (ADFS)

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

企業聊天和電子郵件(ECE)控制檯可以在Finesse外部訪問，但是，必須啟用SSO以允許座席和主管透過Finesse登入到ECE。

也可以為新的分割槽管理員配置Single Sign-On。這可確保登入思科管理員案頭的新使用者有權訪問企業聊天和電子郵件管理控制檯。

單一登入需要注意的重要事項：

- 設定單一登入系統的程式必須由分割區使用者在分割區層級對安全性節點執行，並採取必要動作：檢視應用程式安全性與管理應用程式安全性。
- 啟用了SSO後，主管和管理員若要登入到「代理控制檯」以外的控制檯，必須在分割槽設定中提供有效的應用程式外部URL。有關詳細資訊，請參閱一般分割槽設定。
- 需要Java Keystore (JKS)證書來配置SSO，以允許具有管理員或主管角色的使用者使用其SSO登入憑據登入到Finesse之外的ECE分割槽1。請諮詢您的IT部門以獲取JKS證書。
- Cisco IDS的安全套接字層(SSL)證書必須導入到安裝中的所有應用伺服器。要獲取必要的SSL證書檔案，請與您的IT部門或Cisco IDS支援部門聯絡。
- Unified CCE的DB伺服器歸類區分大小寫。從使用者資訊終端URL返回的宣告中的使用者名稱和Unified CCE中的使用者名稱必須相同。如果不相同，則無法辨識登入為單一登入代理，並且ECE無法將代理可用性傳送到Unified CCE。
- 為Cisco IDS配置SSO將影響已在Unified CCE中配置為單點登入的使用者。確保在ECE中為SSO啟用的使用者在Unified CCE中配置為SSO。有關詳細資訊，請諮詢您的Unified CCE管理員。

附註：

- 確保在ECE中為SSO啟用的使用者在Unified CCE中配置為SSO。
- 本檔案指定在單一AD FS部署中設定ECE信賴零件信任的步驟，其中資源同盟伺服器和帳戶同盟伺服器安裝在同一部機器上。
- 對於Split AD FS部署，請導航到相應版本的ECE安裝及設定指南。

設定步驟

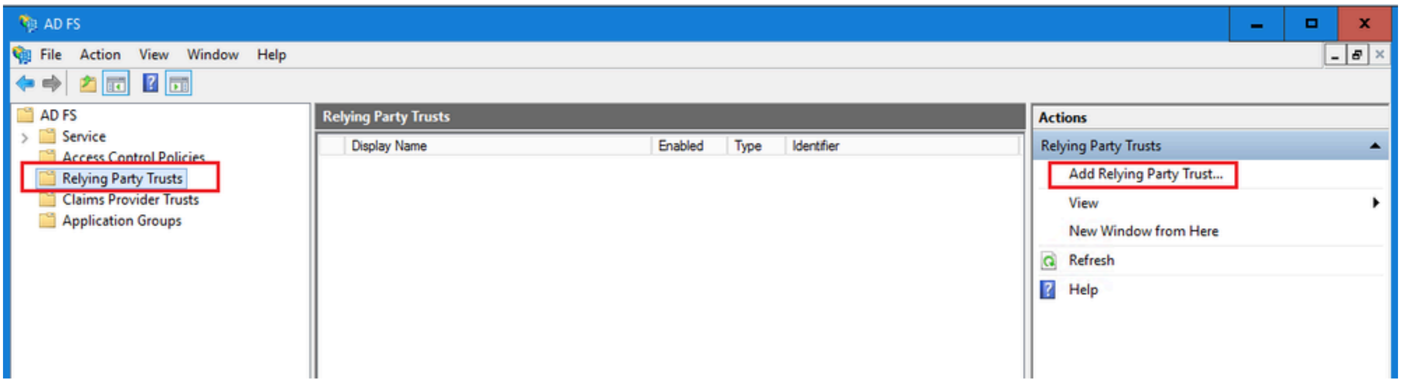
為ECE配置信賴方信任

步驟 1

打開AD FS管理控制檯，然後導航到AD FS >信任關係>信賴方信任。

步驟 2

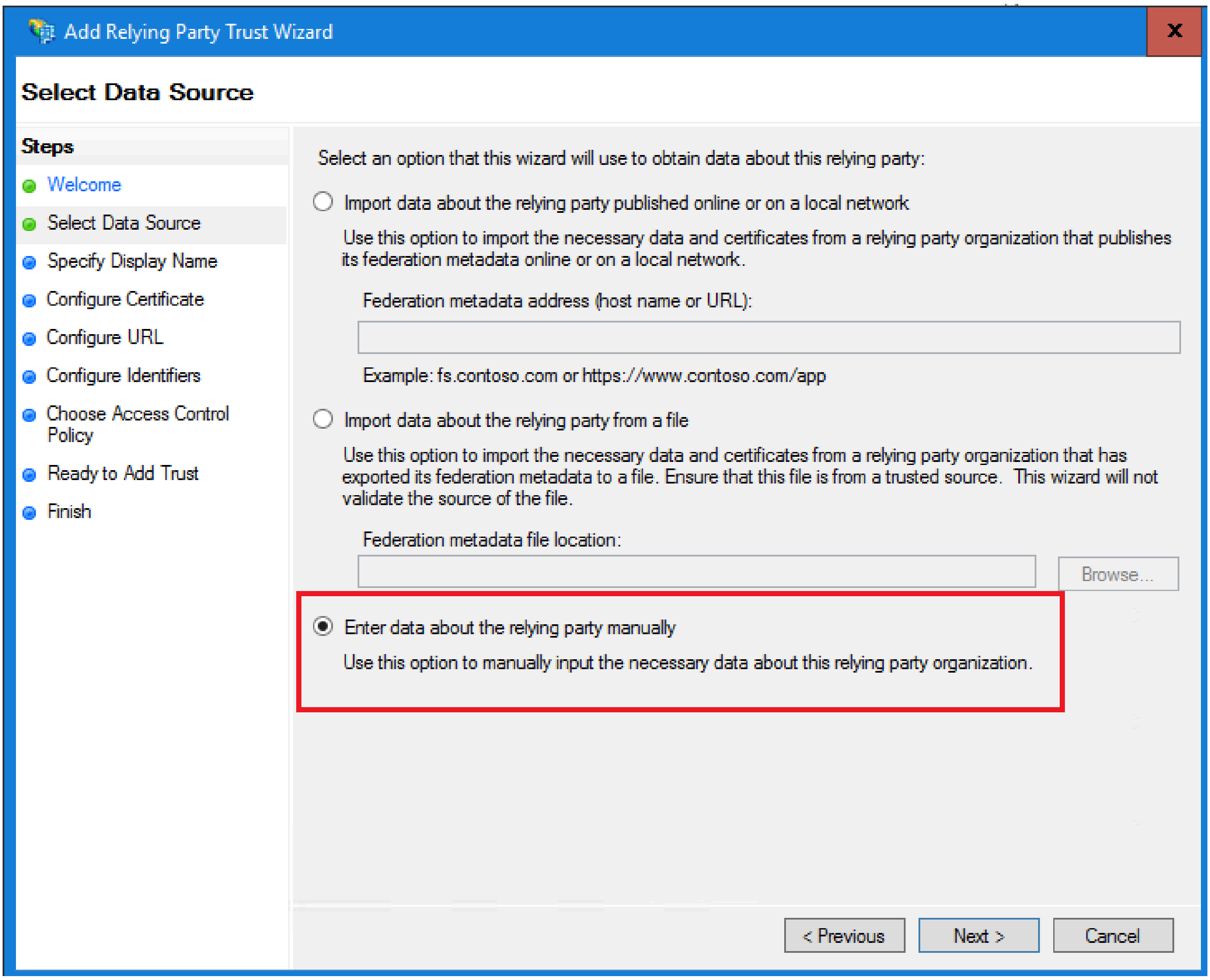
在Actions部分中，按一下Add Reliing Party Trust...



步驟 3

在「增加信賴方信任」嚮導中，按一下「開始」並完成以下步驟：

a.在「選擇資料來源」頁中，選擇手動輸入有關回複方的資料選項，然後按一下下一步。



Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

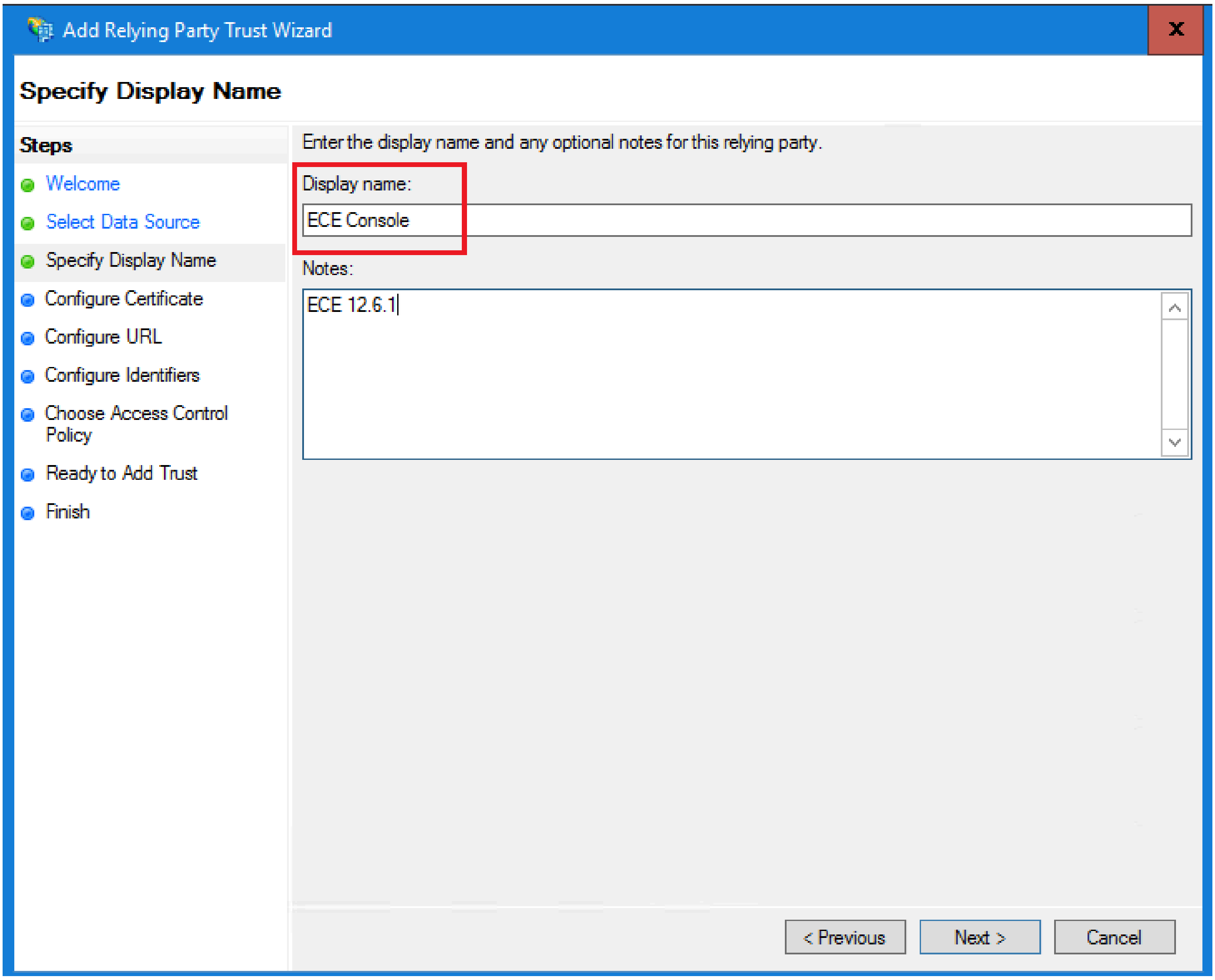
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

● Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

b.在「指定顯示名稱」頁面中，提供信賴方的顯示名稱。按一下「下一步」



Enter the display name and any optional notes for this relying party.

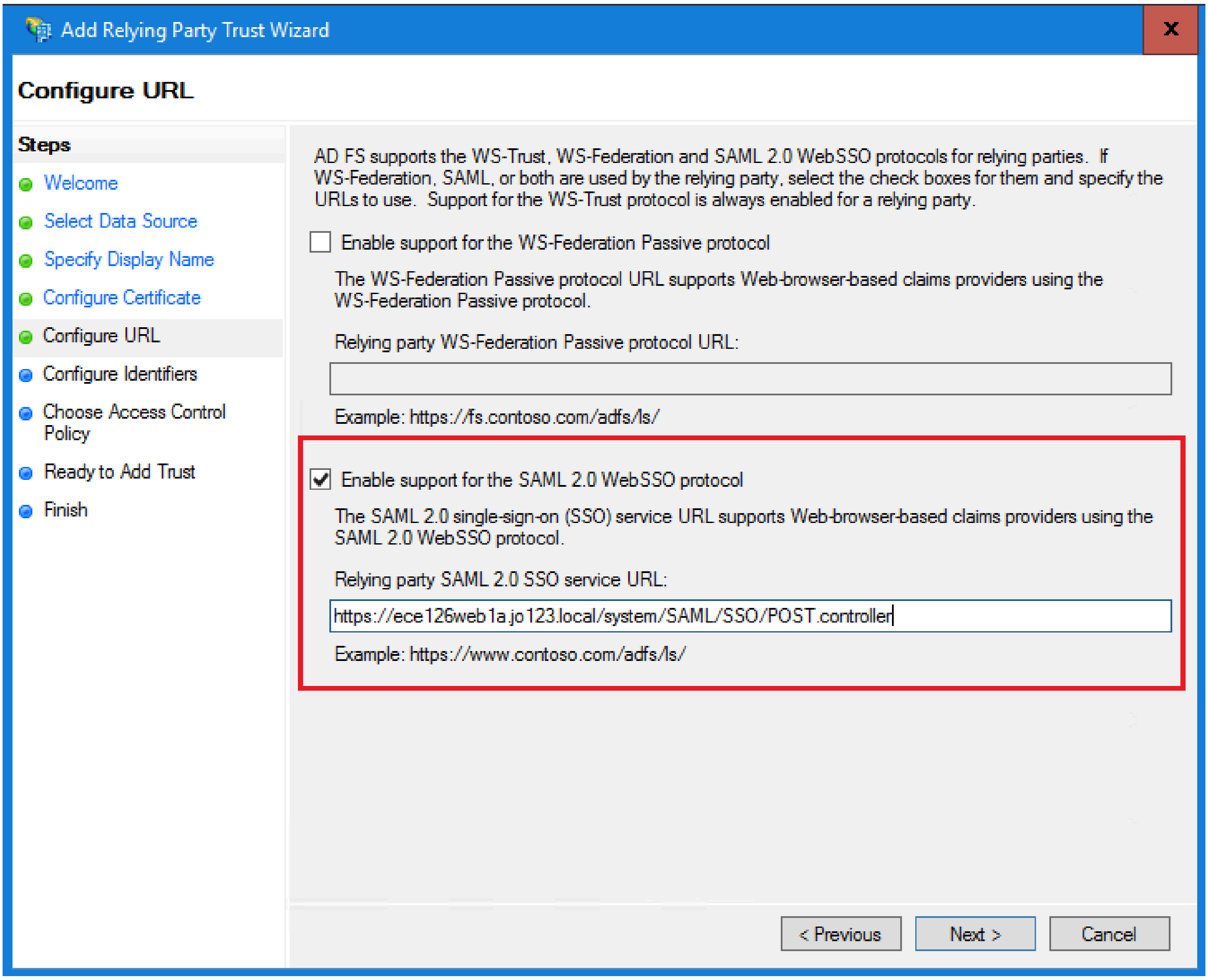
Display name: ECE Console

Notes: ECE 12.6.1

c.在「配置URL」頁中：

i.選擇Enable support for the SAML 2.0 Web SSO protocol選項。

ii.在信賴方SAML 2.0 SSO伺服器URL欄位中，提供以下格式的URL：https://<Web-Server-Or-Load-Balancer-FQDN>/system/SAML/SSO/POST.controller



Configure URL

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☑ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

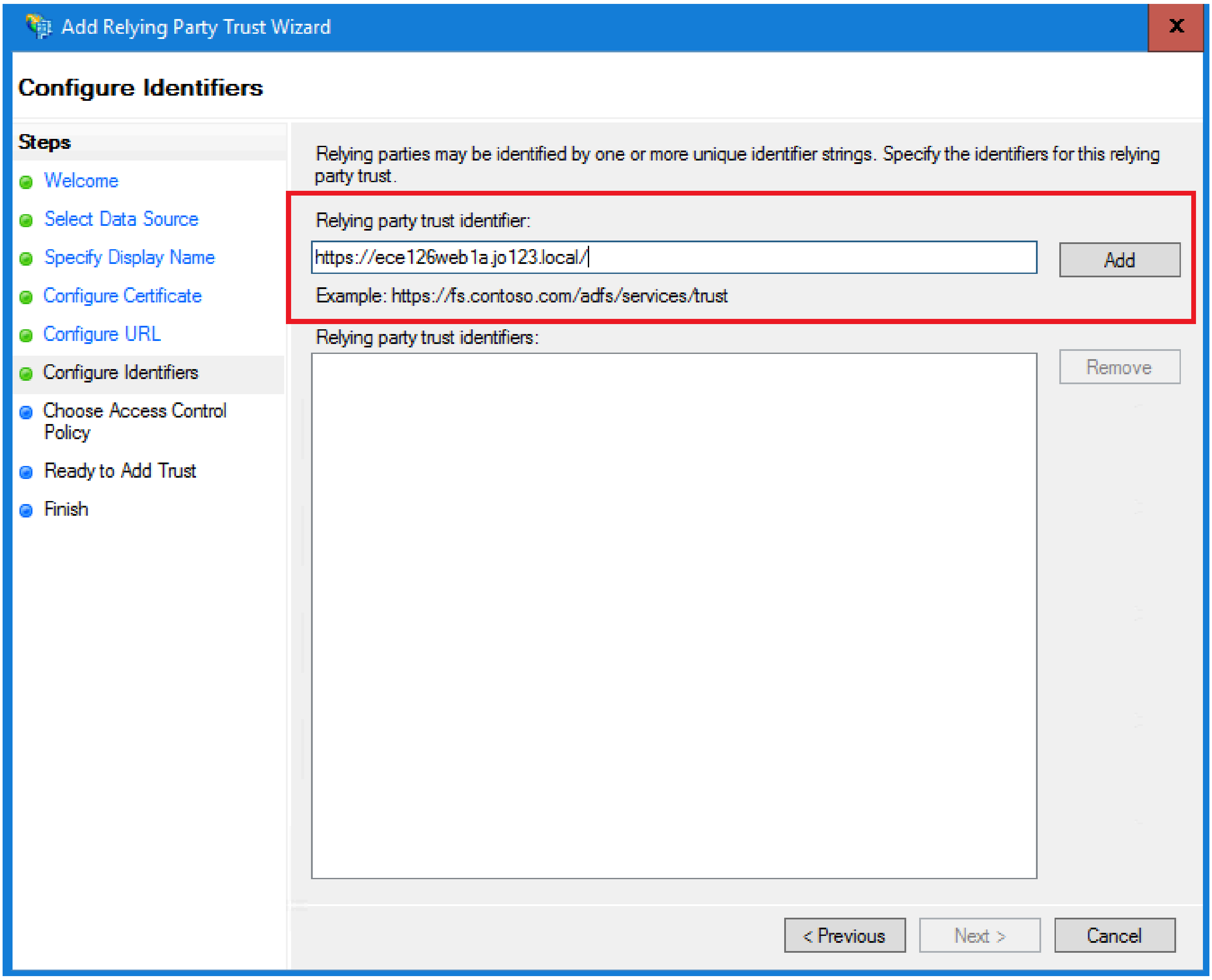
Relying party SAML 2.0 SSO service URL:

https://ece126web1a.jo123.local/system/SAML/SSO/POST.controller

Example: https://www.contoso.com/adfs/ls/

d.在「配置識別符號」頁中，提供信賴方信任識別符號，然後按一下「增加」。

- 值的格式必須為：https://<Web-Server-Or-Load-Balancer-FQDN>/



Add Relying Party Trust Wizard

Configure Identifiers

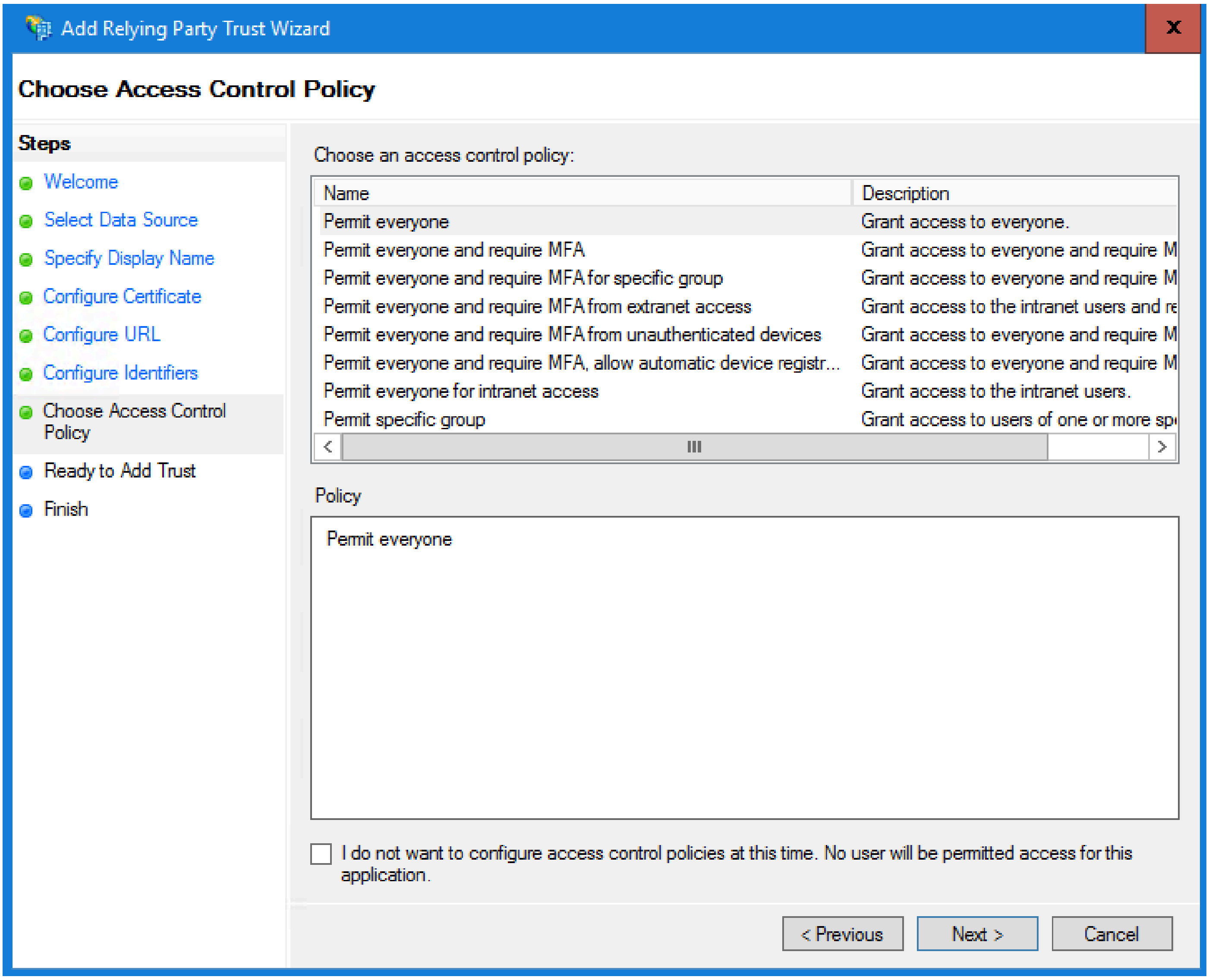
Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier: https://ece126web1a.jo123.local/

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

e.在Choose Access Control Policy頁中，按一下具有預設值「Permit everyone」策略的「next」。



Choose Access Control Policy

Choose an access control policy:

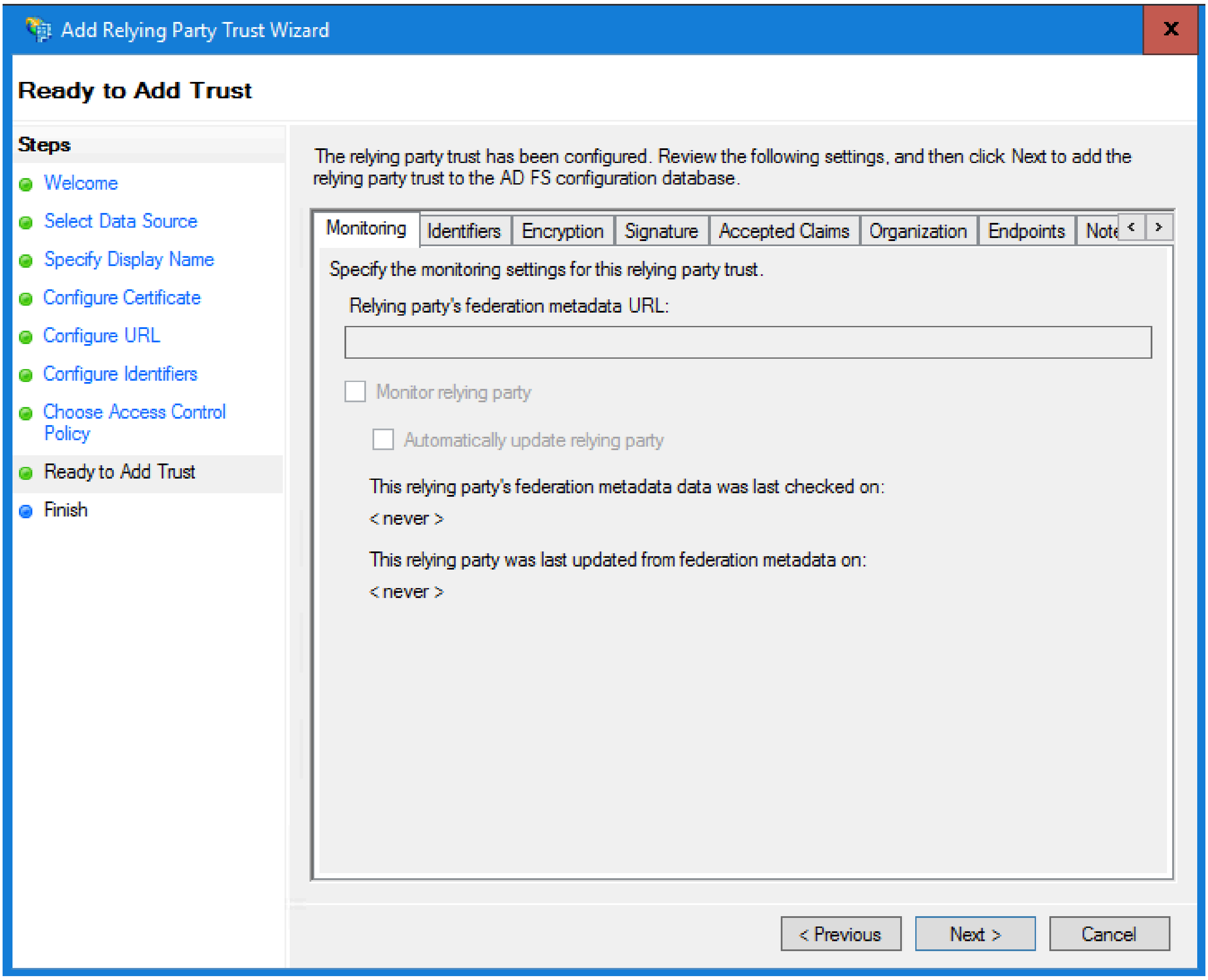
Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require M
Permit everyone and require MFA for specific group	Grant access to everyone and require M
Permit everyone and require MFA from extranet access	Grant access to the intranet users and re
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require M
Permit everyone and require MFA, allow automatic device registr...	Grant access to everyone and require M
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more sp

Policy

Permit everyone

□ I do not want to configure access control policies at this time. No user will be permitted access for this application.

f.在「準備增加信任」頁中，按一下「下一步」。



The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

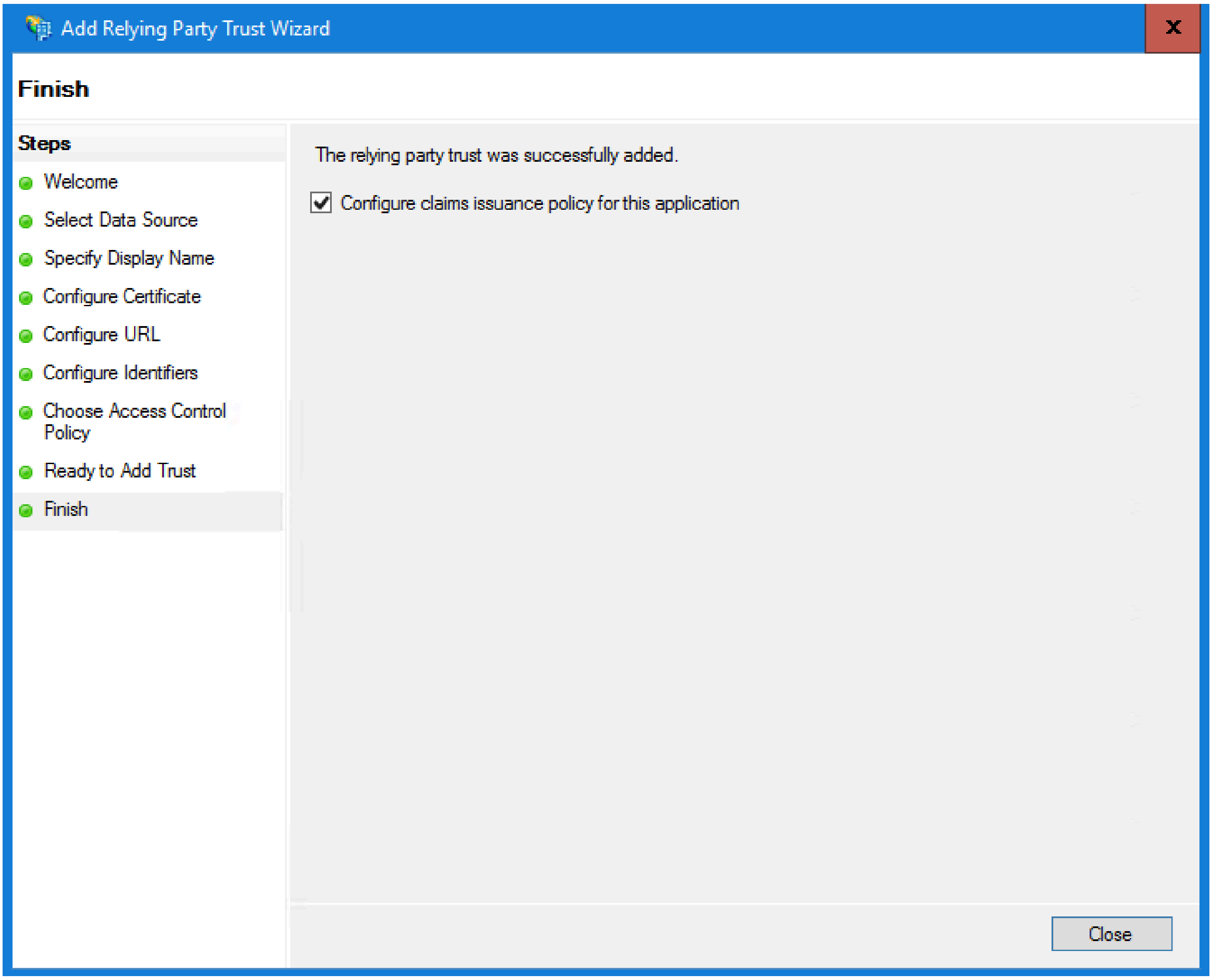
□ Monitor relying party

□ Automatically update relying party

This relying party's federation metadata data was last checked on:
< never >

This relying party was last updated from federation metadata on:
< never >

g.成功增加信賴方信任後，點選Close。

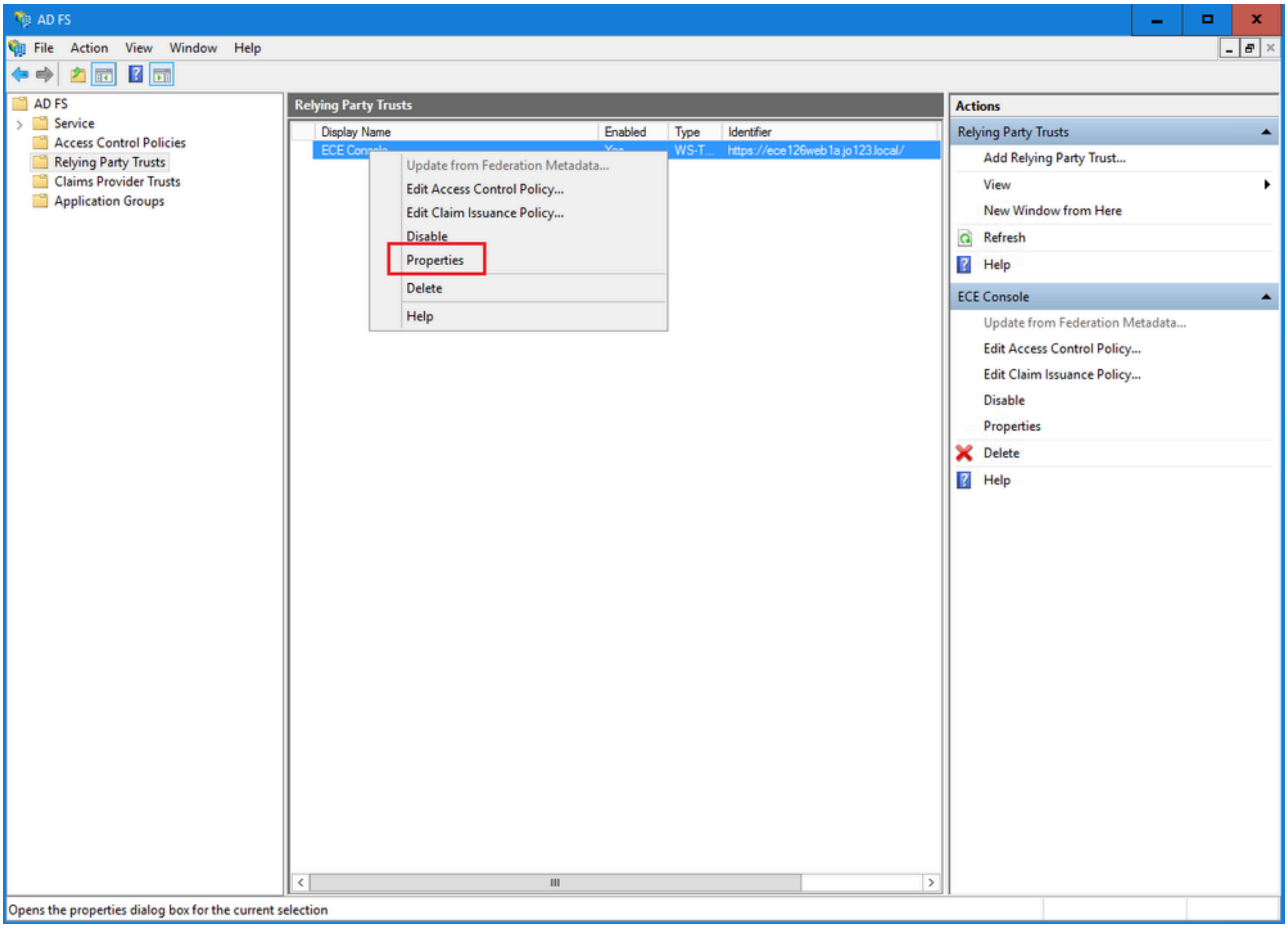


The relying party trust was successfully added.

☑ Configure claims issuance policy for this application

步驟 4

在信賴提供方信任清單中，選擇為ECE建立的信賴方信任，並在「操作」部分中按一下屬性。

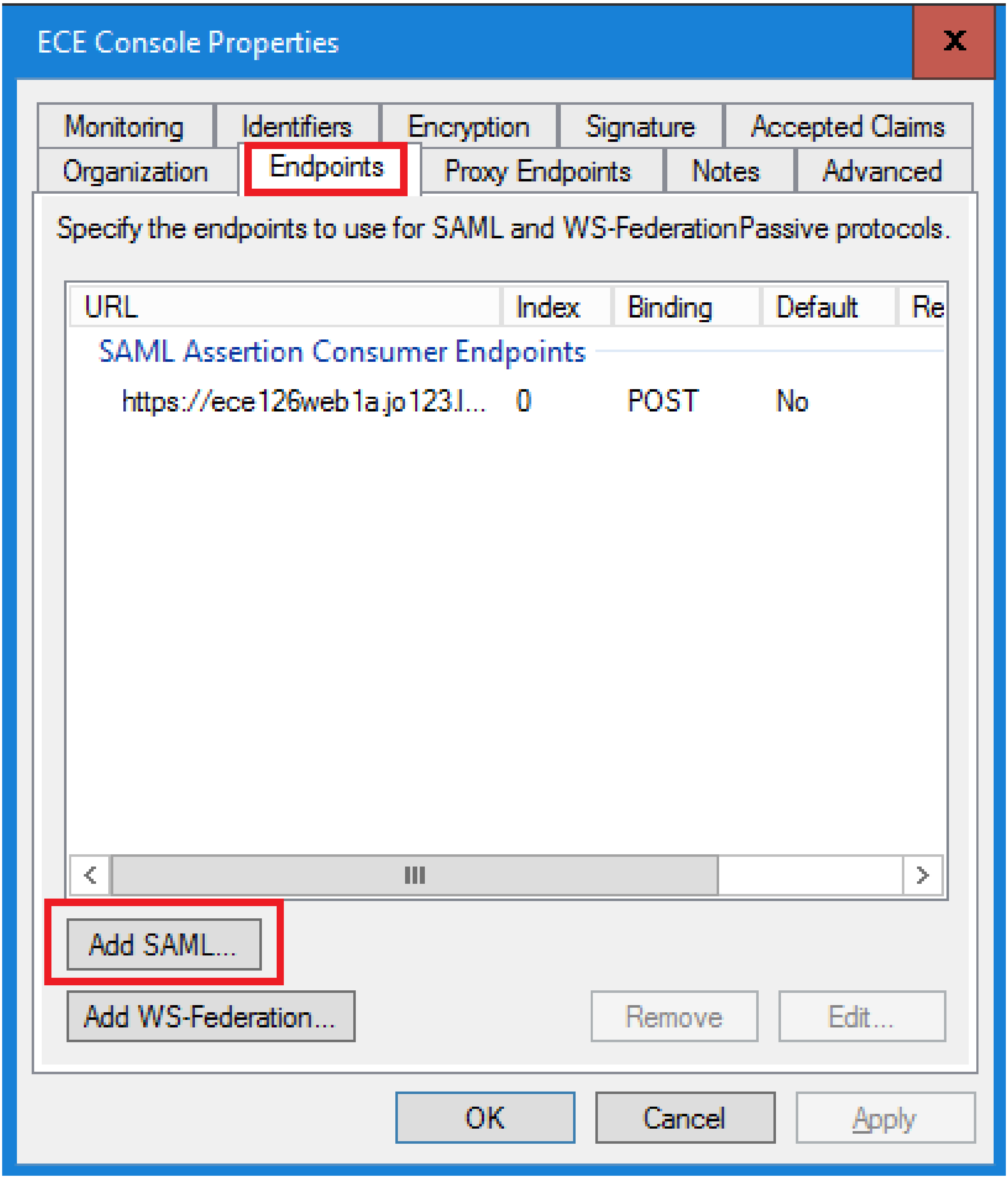


Display Name	Enabled	Type	Identifier
ECE Console	Yes	WS-T...	https://ece126web1a.jo123.local/

Opens the properties dialog box for the current selection

步驟 5

在「屬性」窗口中，導航到終端頁籤，然後按一下增加SAML..按鈕



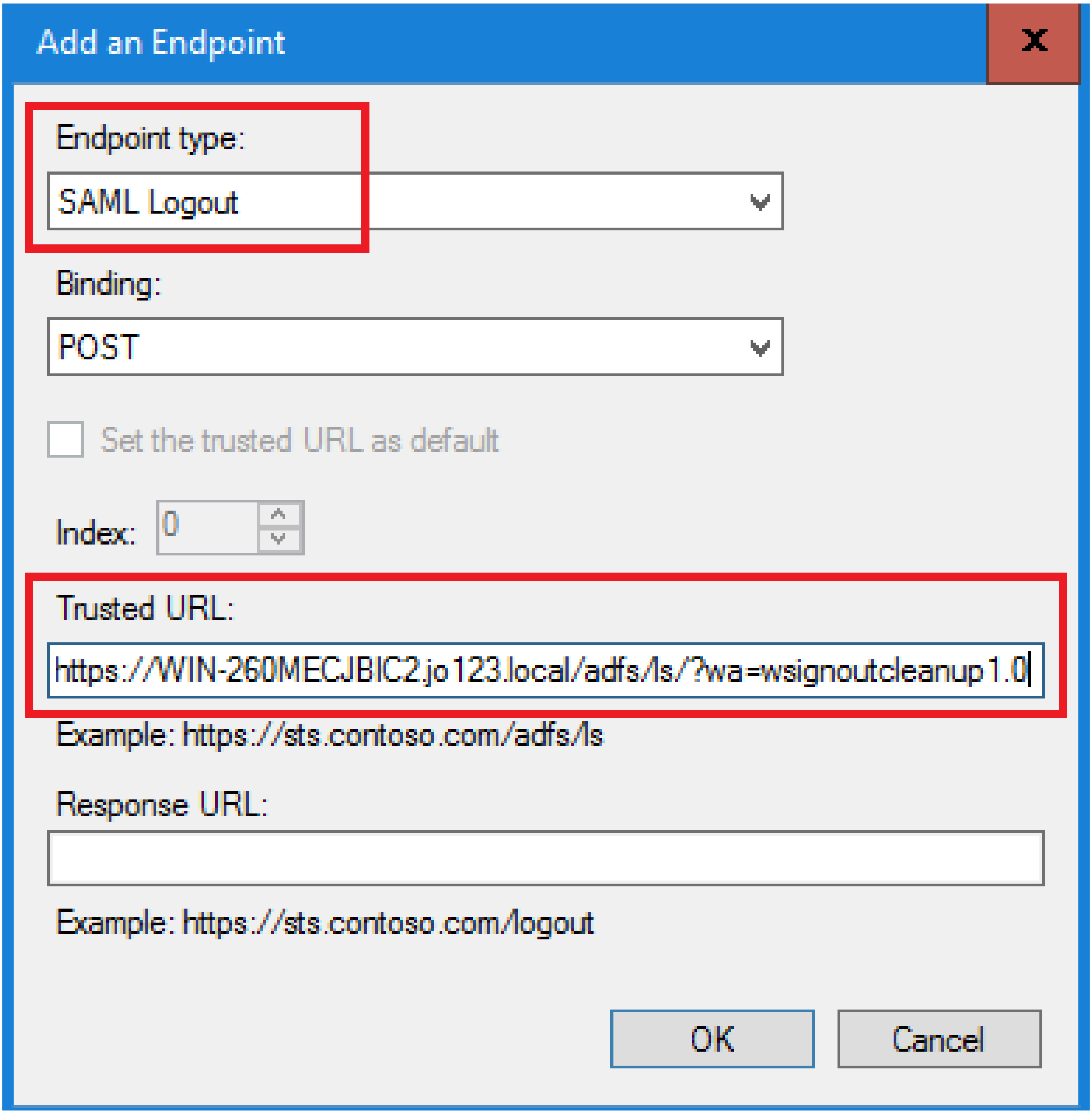
Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://ece126web1a.jo123.l...	0	POST	No	

步驟 6

在Add an Endpoint窗口中，按照說明進行配置：

1. 選擇Endpoint type作為SAML Logout。
2. 將受信任的URL指定為https://<ADFS-server-FQDN>/adfs/ls/ ? wa=wsignoutcleanup1.0
3. 按一下「OK」（確定）。



Add an Endpoint

Endpoint type:

SAML Logout

Binding:

POST

□ Set the trusted URL as default

Index: 0

Trusted URL:

https://WIN-260MECJBIC2.jo123.local/adfs/ls/?wa=wsignoutcleanup1.0

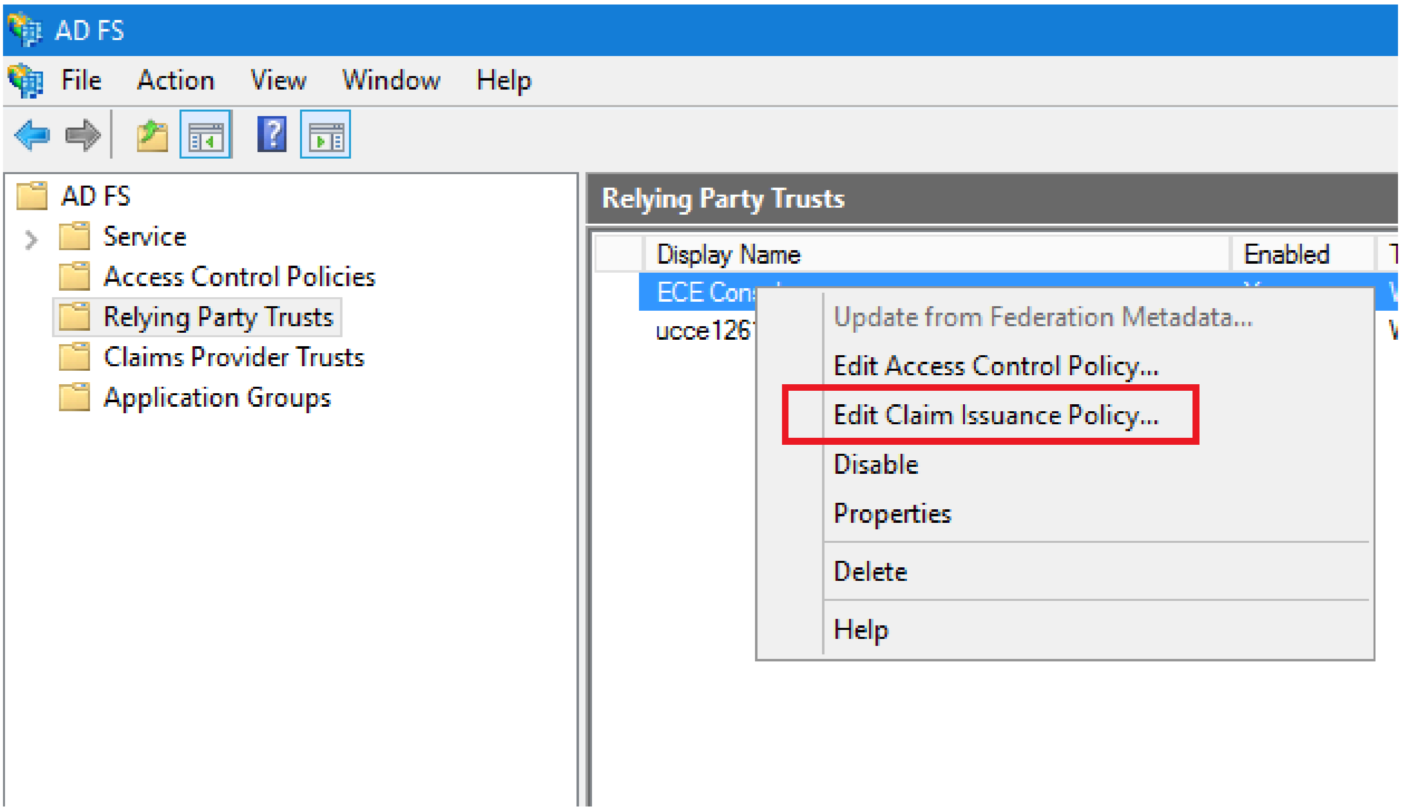
Example: https://sts.contoso.com/adfs/ls

Response URL:

Example: https://sts.contoso.com/logout

步驟 7

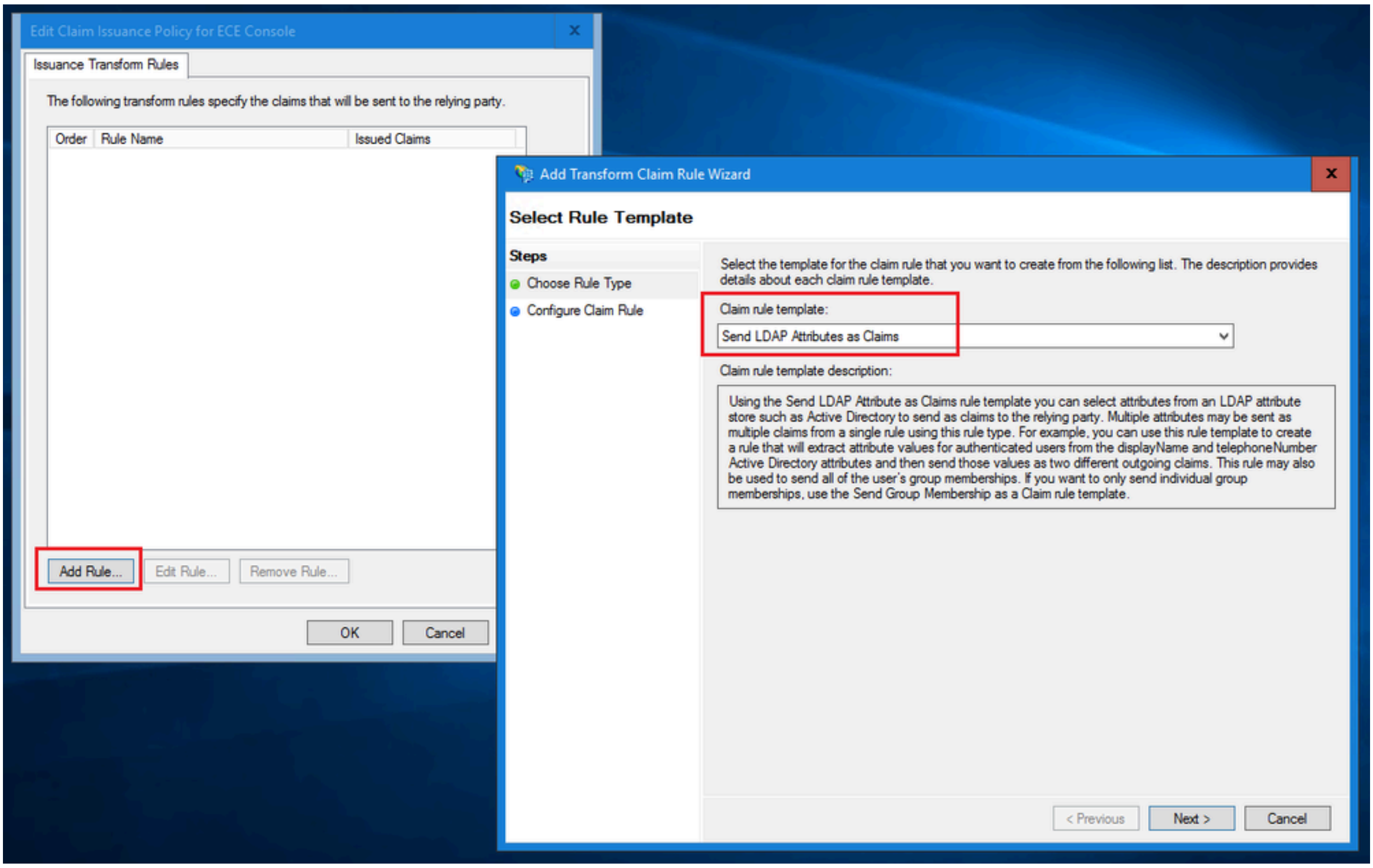
在「信賴提供商信任」清單中，選擇為ECE建立的信任，並在「操作」部分中按一下編輯索賠保險單。



步驟 8

在「編輯索賠保險單」窗口的「頒發轉換規則」頁籤下，按一下增加規則……按鈕並進行配置，如下所示：

a.在「選擇規則型別」頁中，從下拉選單中選擇將LDAP屬性作為宣告傳送，然後按一下「下一步」。



The following transform rules specify the claims that will be sent to the relying party.

Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

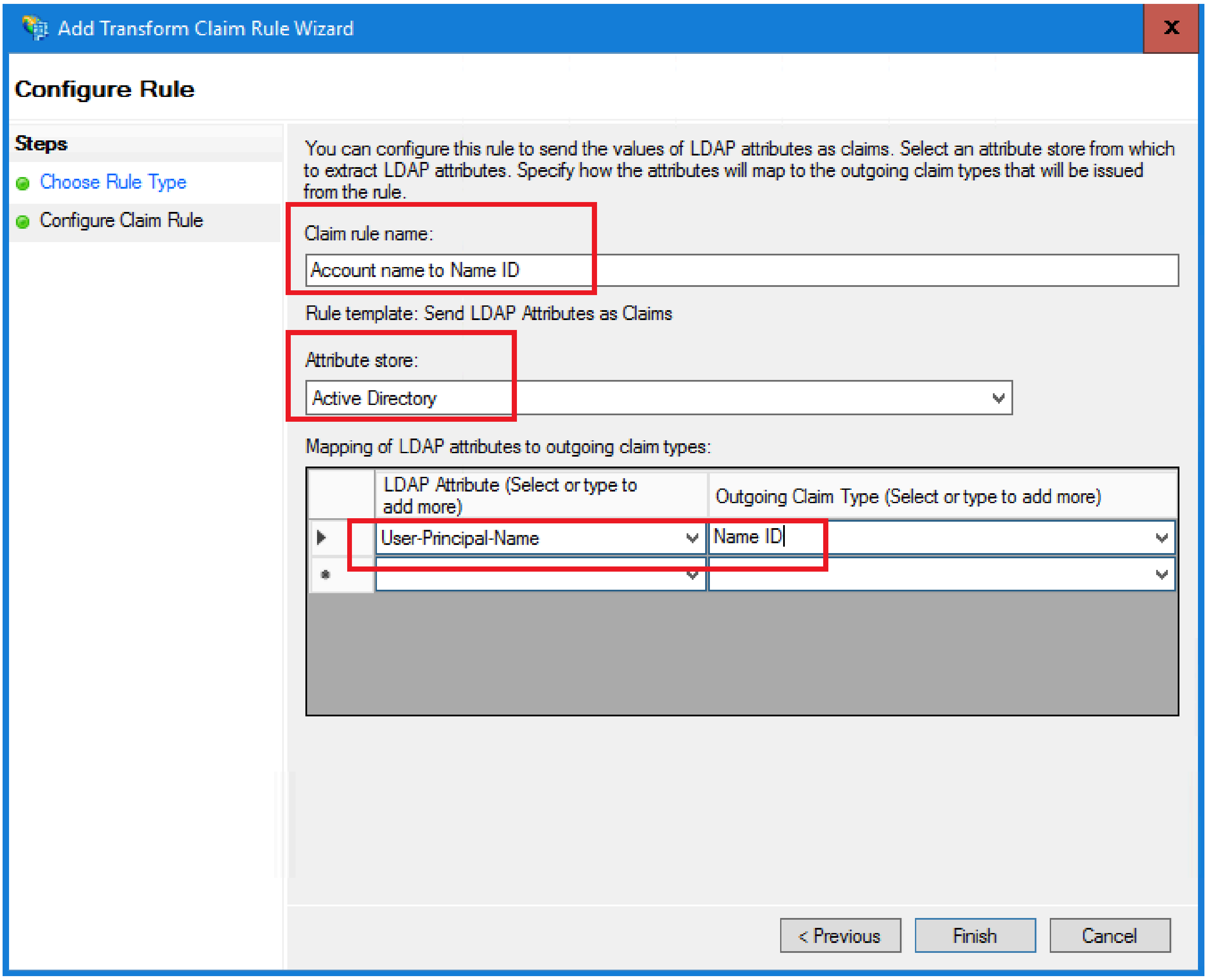
Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

b.在「設定宣告規則」頁面中：

1. 提供宣告規則名稱並選擇屬性儲存。
2. 定義LDAP屬性與傳出宣告型別的對應。

- 選擇Name ID作為傳出宣告型別名稱。
- 按一下「完成」返回「編輯索賠保險單」視窗，然後按一下「確定」。



Configure 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:

Account name to Name ID

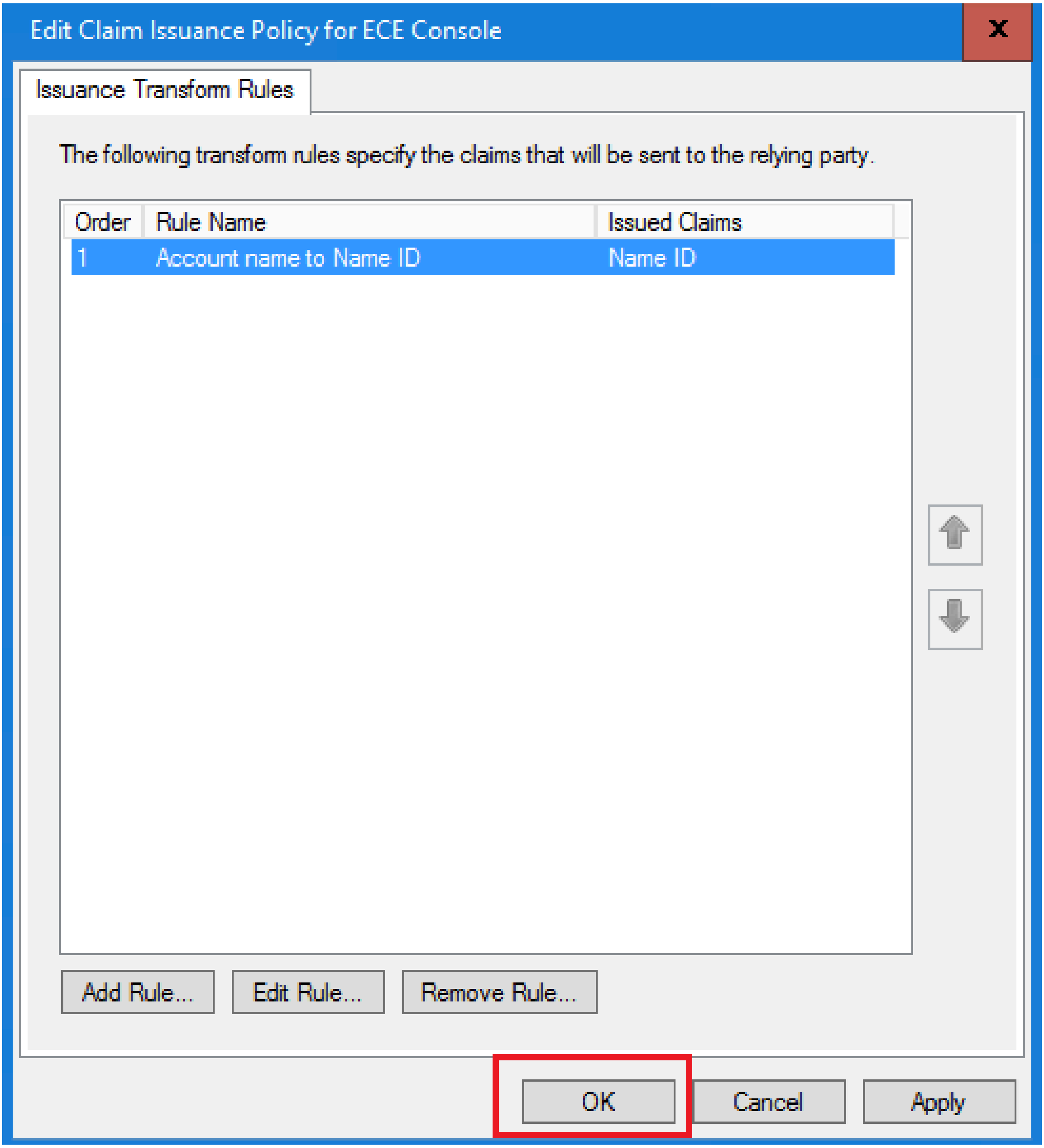
Rule template: Send LDAP Attributes as Claims

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)
▶	User-Principal-Name	Name ID
*		



The following transform rules specify the claims that will be sent to the relying party.

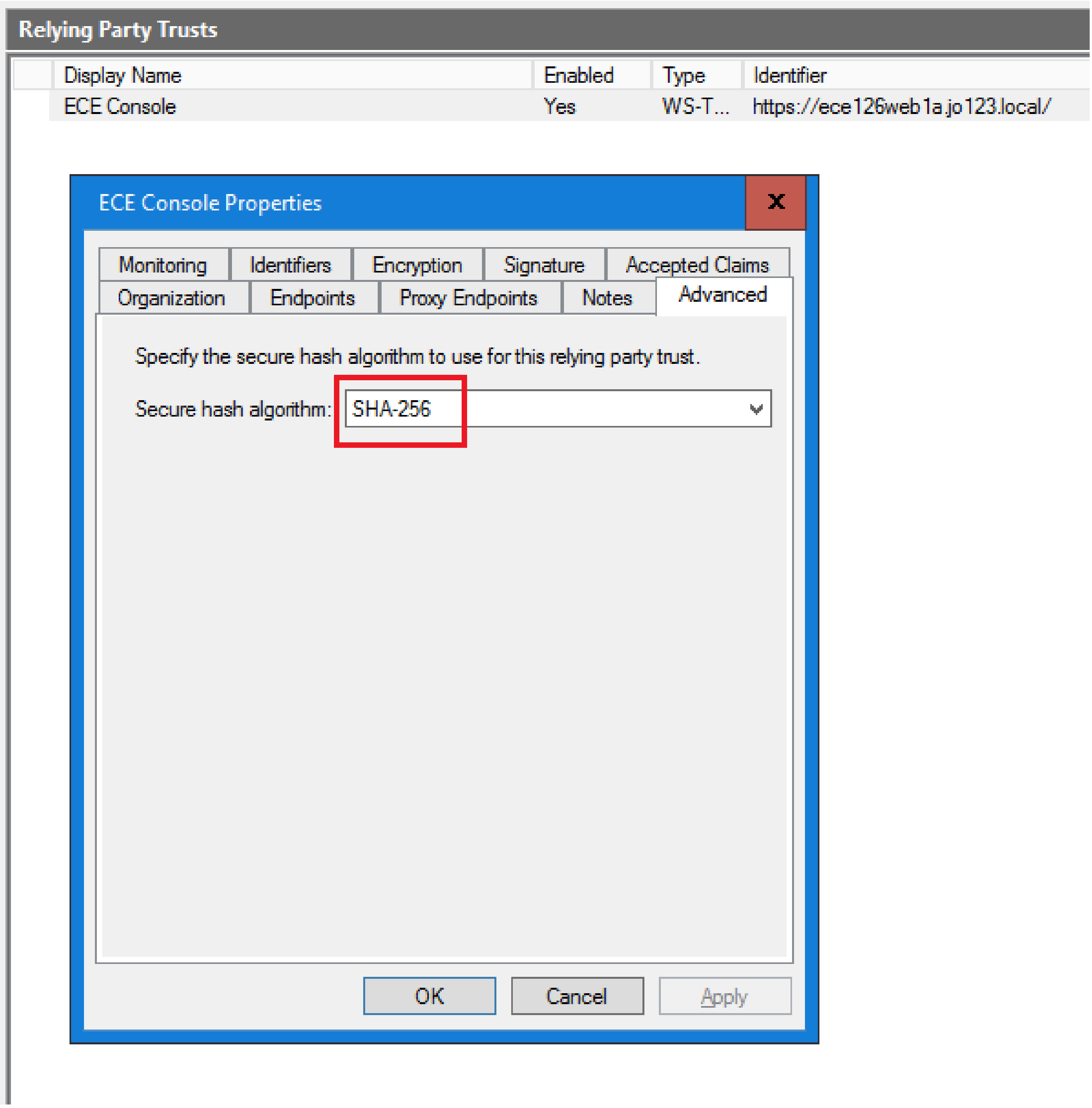
Order	Rule Name	Issued Claims
1	Account name to Name ID	Name ID

步驟 9

在「信賴提供者信任」清單中，連按兩下您建立的ECE信賴方信任。

在打開的「屬性」窗口中，轉至「高級」頁籤，將「安全雜湊演算法」設定為SHA-1或SHA-256。按一下「確定」以關閉視窗。

註：此值必須與ECE中SSO配置下的「服務提供商」設定的「簽名演算法」值匹配



Relying Party Trusts

Display Name	Enabled	Type	Identifier
ECE Console	Yes	WS-T...	https://ece126web1a.jo123.local/

ECE Console Properties

Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-256

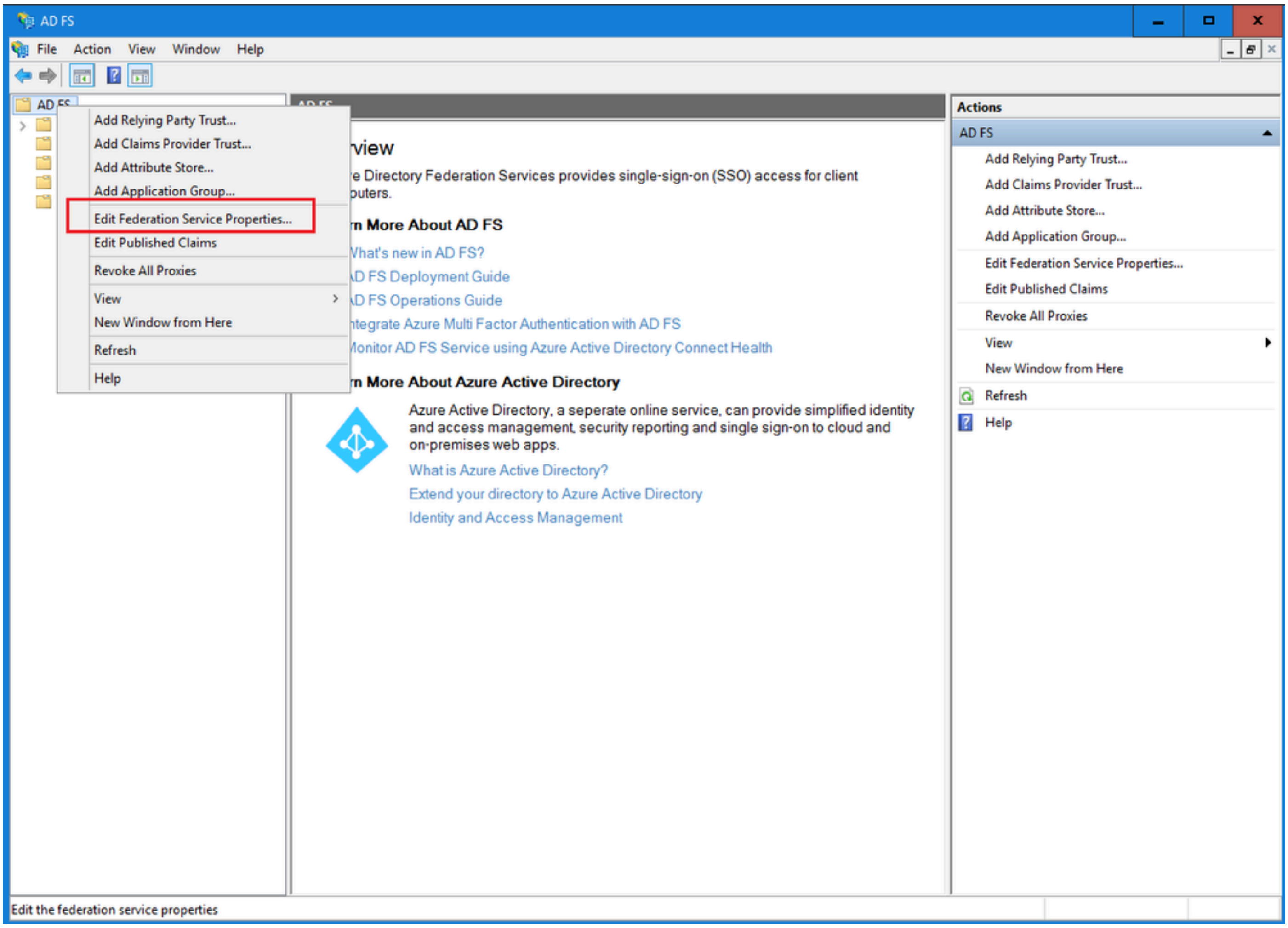
步驟 10

驗證並記下Federation Service Identifier值。

- 在AD FS管理控制檯中，選擇並按一下右鍵AD FS >「編輯聯合身份驗證服務屬性」>「常規」頁籤>「聯合身份驗證服務識別符號」

附註：

- 必須完全按照在ECE的SSO配置下為身份提供程式配置「實體ID」值的方式增加此值。
- 使用http://並不表示ADFS不安全，這只是識別符號。



view

e Directory Federation Services provides single-sign-on (SSO) access for client puters.

n More About AD FS

Vhat's new in AD FS?

D FS Deployment Guide

D FS Operations Guide

ntegrate Azure Multi Factor Authentication with AD FS

Monitor AD FS Service using Azure Active Directory Connect Health

n More About Azure Active Directory

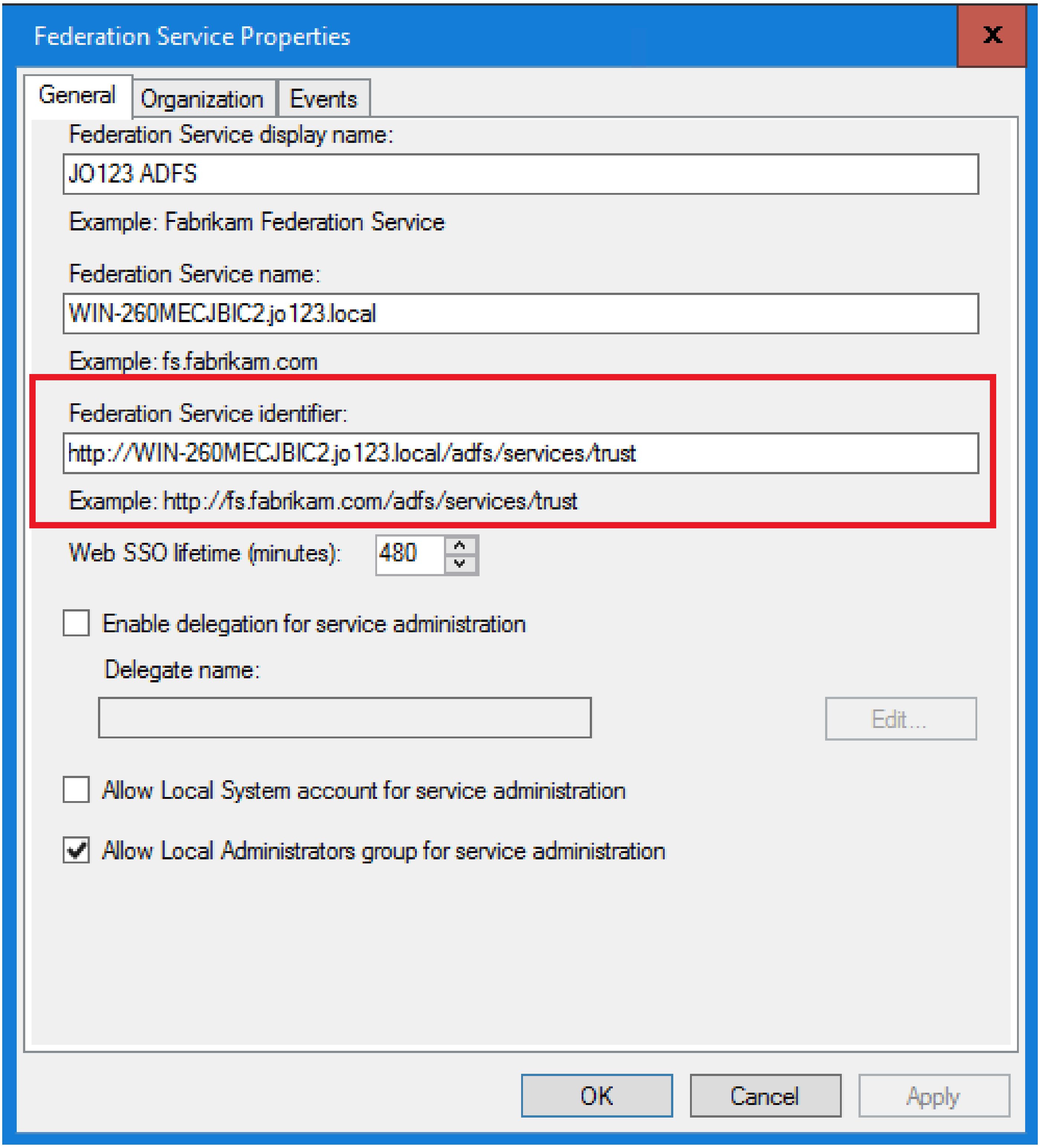
Azure Active Directory, a seperate online service, can provide simplified identity and access management, security reporting and single sign-on to cloud and on-premises web apps.

What is Azure Active Directory?

Extend your directory to Azure Active Directory

Identity and Access Management

Edit the federation service properties



Federation Service Properties

Federation Service display name:

JO123 ADFS

Example: Fabrikam Federation Service

Federation Service name:

WIN-260MECJBIC2.jo123.local

Example: fs.fabrikam.com

Federation Service identifier:

http://WIN-260MECJBIC2.jo123.local/adfs/services/trust

Example: http://fs.fabrikam.com/adfs/services/trust

Web SSO lifetime (minutes): 480

□ Enable delegation for service administration

Delegate name:

□ Allow Local System account for service administration

☑ Allow Local Administrators group for service administration

設定辨識提供者

步驟 11

需要Java Keystore (JKS)證書來配置SSO，以允許具有管理員或主管角色的使用者使用其SSO登入憑據登入到Finesse外部的ECE分割槽。

如果您要設定SSO，以允許具有管理員或主管角色的使用者使用其SSO登入證明資料登入Finesse以外的ECE分割區，則Java Keystore (JKS)憑證必須轉換成公用金鑰憑證，並在為ECE在

IdP伺服器上建立的信賴方信任中設定。

請諮詢您的IT部門以獲取JKS證書。

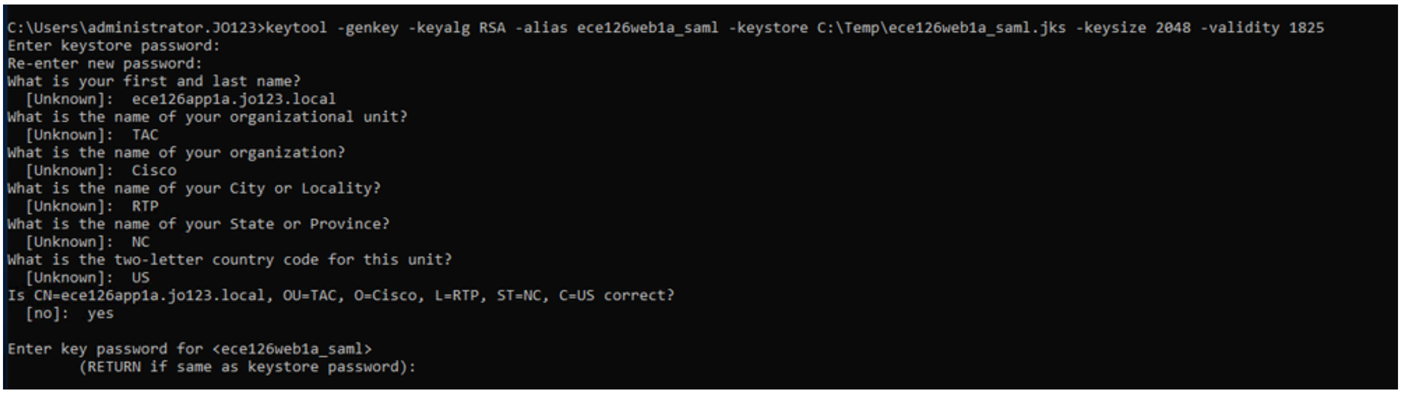
注意：這些步驟適用於使用ADFS作為身份提供者的系統。其他辨識提供者可以使用不同的方法來設定公開金鑰憑證。

以下示例說明如何在實驗中生成JKS檔案：

a.生成JKS：

```
keytool -genkey -keyalg RSA -alias ece126web1a_saml -keystore C:\Temp\ece126web1a_saml.jks -keysize 204
```

註：此處輸入的金鑰庫密碼、別名和金鑰密碼用於在ECE的SSO配置下配置「服務提供商」配置。



```
C:\Users\administrator.JO123>keytool -genkey -keyalg RSA -alias ece126web1a_saml -keystore C:\Temp\ece126web1a_saml.jks -keysize 2048 -validity 1825
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  ece126app1a.jo123.local
What is the name of your organizational unit?
  [Unknown]:  TAC
What is the name of your organization?
  [Unknown]:  Cisco
What is the name of your City or Locality?
  [Unknown]:  RTP
What is the name of your State or Province?
  [Unknown]:  NC
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=ece126app1a.jo123.local, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US correct?
  [no]:  yes

Enter key password for <ece126web1a_saml>
        (RETURN if same as keystore password):
```

b.匯出憑證：

此keytool命令將檔名ece126web1a_saml.crt的.crt格式的證書檔案導出到C:\Temp目錄中。

```
keytool -exportcert -alias ece126web1a_saml -keystore C:\Temp\ece126web1a_saml.jks -rfc -file C:\Temp\e
```

步驟 12

設定辨識提供者

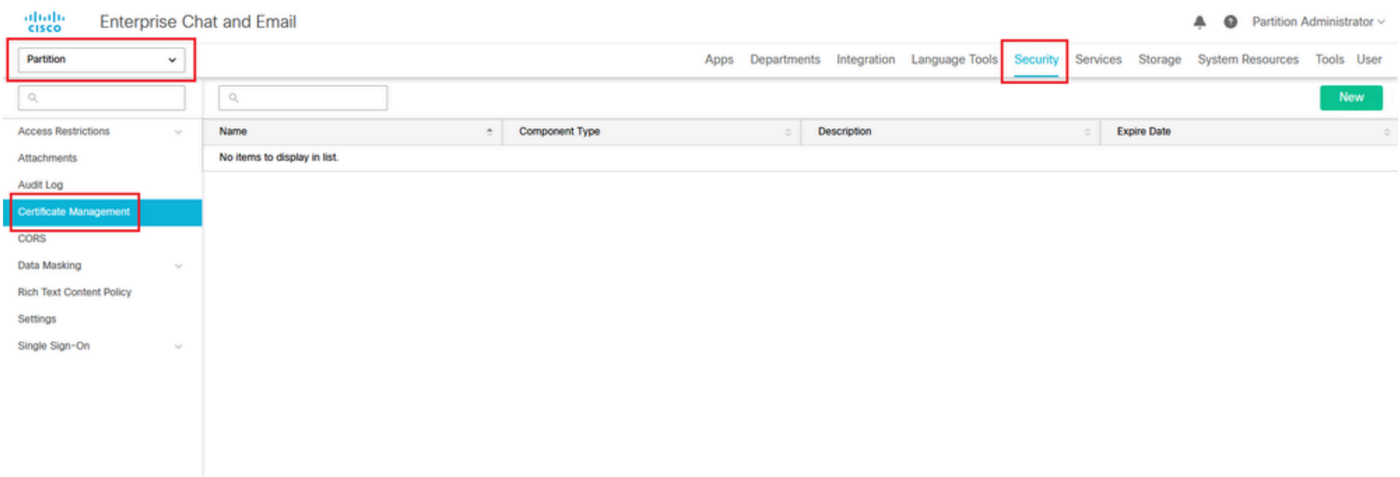
1. 在AD FS管理控制檯上，選擇並按一下右鍵為ECE建立的信賴方信任。
2. 打開信任的「屬性」窗口，然後在「簽名」頁籤下按一下「增加」按鈕。
3. 增加公共證書（上一步生成的.crt檔案），然後按一下「確定」。

建立與匯入憑證

步驟 13

在將SSO配置為使用Cisco IDS進行代理的單點登入之前，必須將Cisco IdS伺服器的Tomcat證書導入到應用程式中。

a.在ECE管理控制檯的分割槽級別選單下，按一下安全選項，然後從左側選單中選擇證書管理。

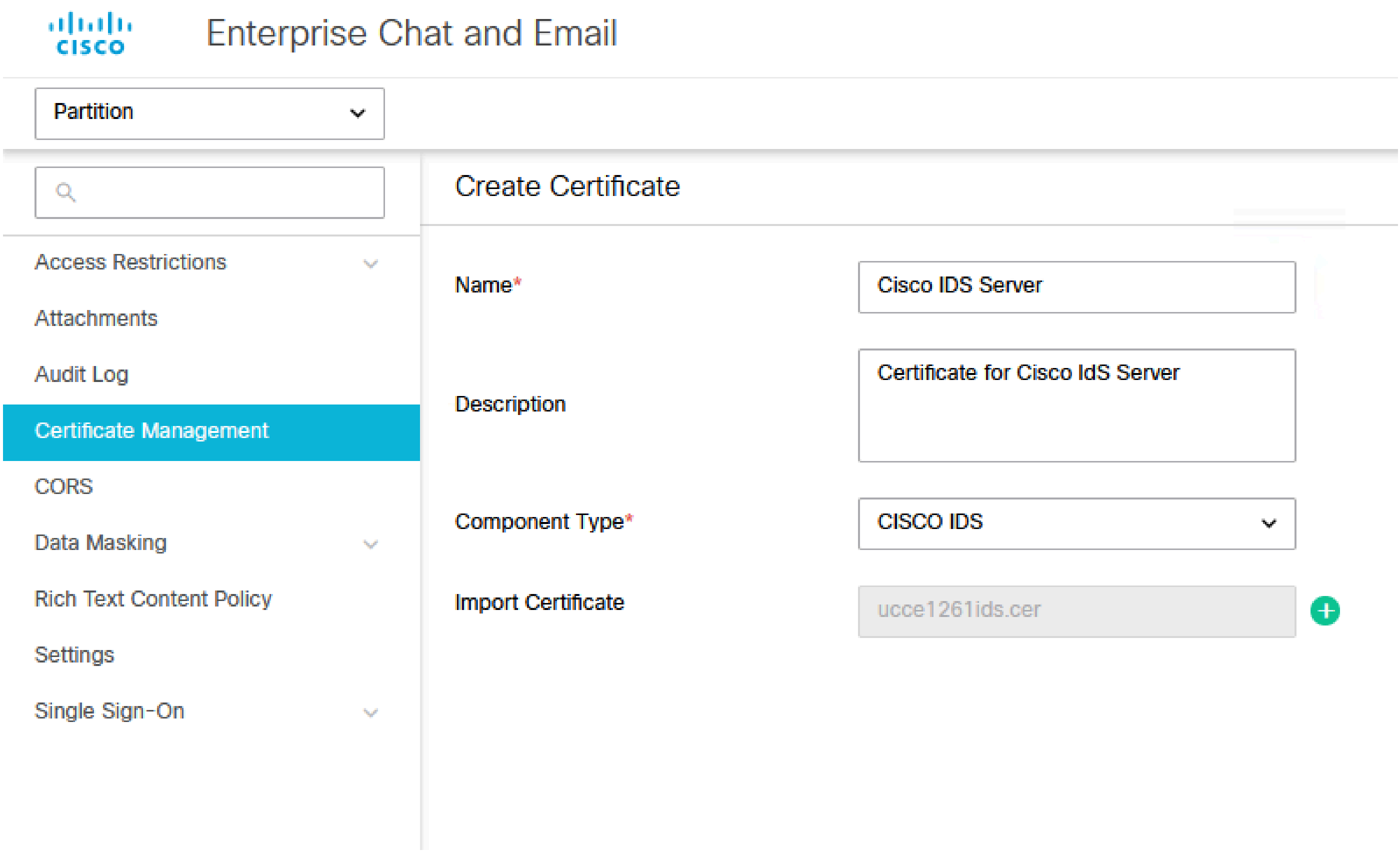


Name	Component Type	Description	Expire Date
No items to display in list.			

b.在證書管理空間中，按一下「新建」按鈕並輸入相應的詳細資訊：

- 名稱：輸入憑證的名稱。
- 描述：新增憑證的描述。
- 元件型別：選擇CISCO IDS。
- 匯入憑證：若要匯入憑證，請按一下搜尋並新增按鈕，然後輸入要求的詳細資訊：
- 憑證檔案：按一下「瀏覽」按鈕，然後選取您要匯入的憑證。憑證只能以.pem、.der（二進位）或.cer/cert格式匯入。
- 別名：提供憑證的別名。

c.按一下「儲存」



Name* Cisco IDS Server

Description Certificate for Cisco IdS Server

Component Type* CISCO IDS

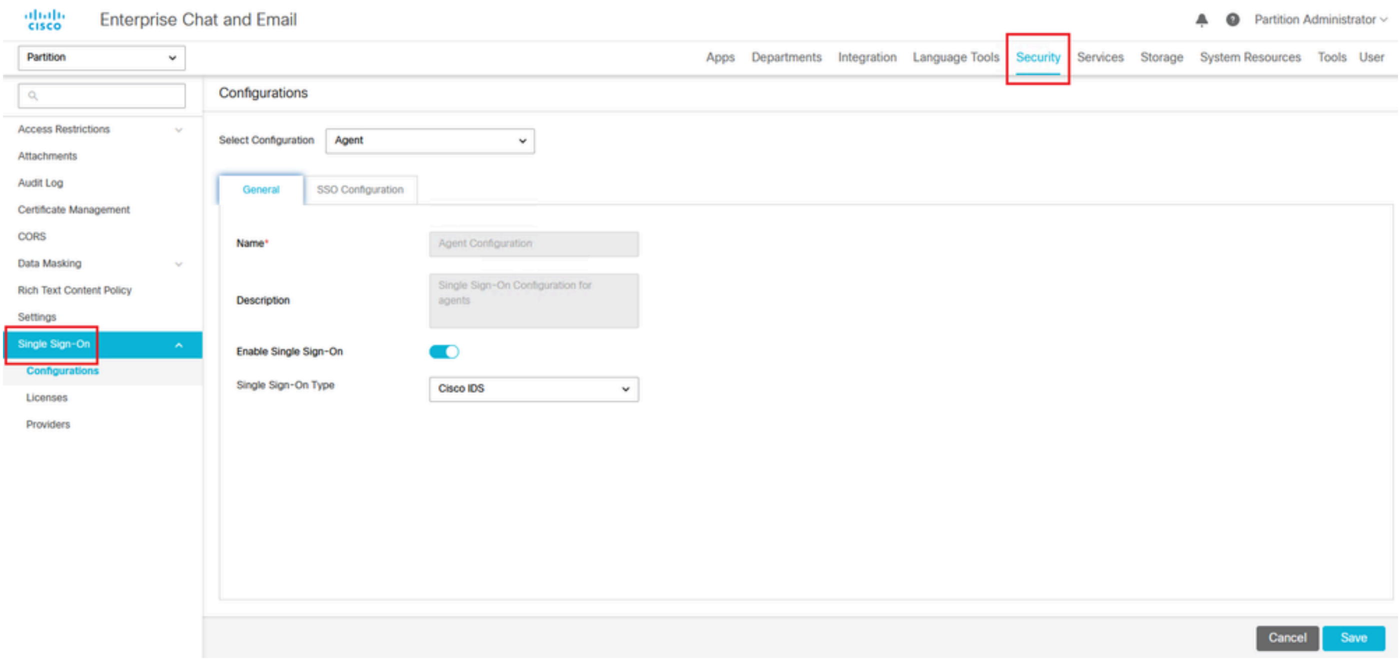
Import Certificate ucce1261ids.cer

設定代理程式單一登入

步驟 14

1. 在ECE管理控制檯的分割槽級別選單下，按一下「Security」選項，然後從左側選單中選擇Single Sign-On > Configurations。
2. 在Select Configuration下拉選單中，選擇Agent，並在General頁籤下設定配置：

- 啟用單一登入：按一下切換按鈕以啟用SSO。
- Single Sign-On Type：選擇Cisco IDS。



Select Configuration: Agent

Name*: Agent Configuration

Description: Single Sign-On Configuration for agents

Enable Single Sign-On: ●

Single Sign-On Type: Cisco IDS

步驟 15

按一下SSO Configuration頁籤並提供配置詳細資訊：

a. OpenID連線提供程式

主要使用者資訊端點URL

- 主Cisco IDS伺服器的使用者資訊終端URL。
- 此URL驗證使用者令牌/使用者資訊API。
- 其格式為：https://cisco-ids-1:8553/ids/v1/oauth/userinfo，其中cisco-ids-1表示主Cisco IDS伺服器的完全限定域名(FQDN)。

使用者辨識宣告名稱

- 使用者資訊終端URL返回的宣告的名稱，用於標識統一CCE或封裝CCE中的使用者名稱。
- 統一或封裝CCE中的宣告名稱和使用者名稱必須匹配。
- 這是響應持有者令牌驗證而獲得的宣告之一。
- 如果Unified或Packaged CCE中的代理使用者名稱與使用者主體名稱匹配，請提供「upn」作為User Identity Claim name欄位的值。
- 如果Unified或Packaged CCE中的代理使用者名稱與SAM Account Name匹配，請提供「sub」作為User Identity Claim name欄位的值。

次要使用者資訊端點URL

- Cisco IDS伺服器的輔助使用者資訊終端URL。
- 其格式為：https://cisco-ids-2:8553/ids/v1/oauth/userinfo，其中cisco-ids-2表示輔助Cisco IDS伺服器的完全限定域名(FQDN)。

使用者資訊端點URL方法

- ECE用來對使用者資訊終端URL進行承載令牌驗證呼叫的HTTP方法。

- 從顯示的選項清單中選取POST（在此選取POST以符合IDS伺服器的方法）。

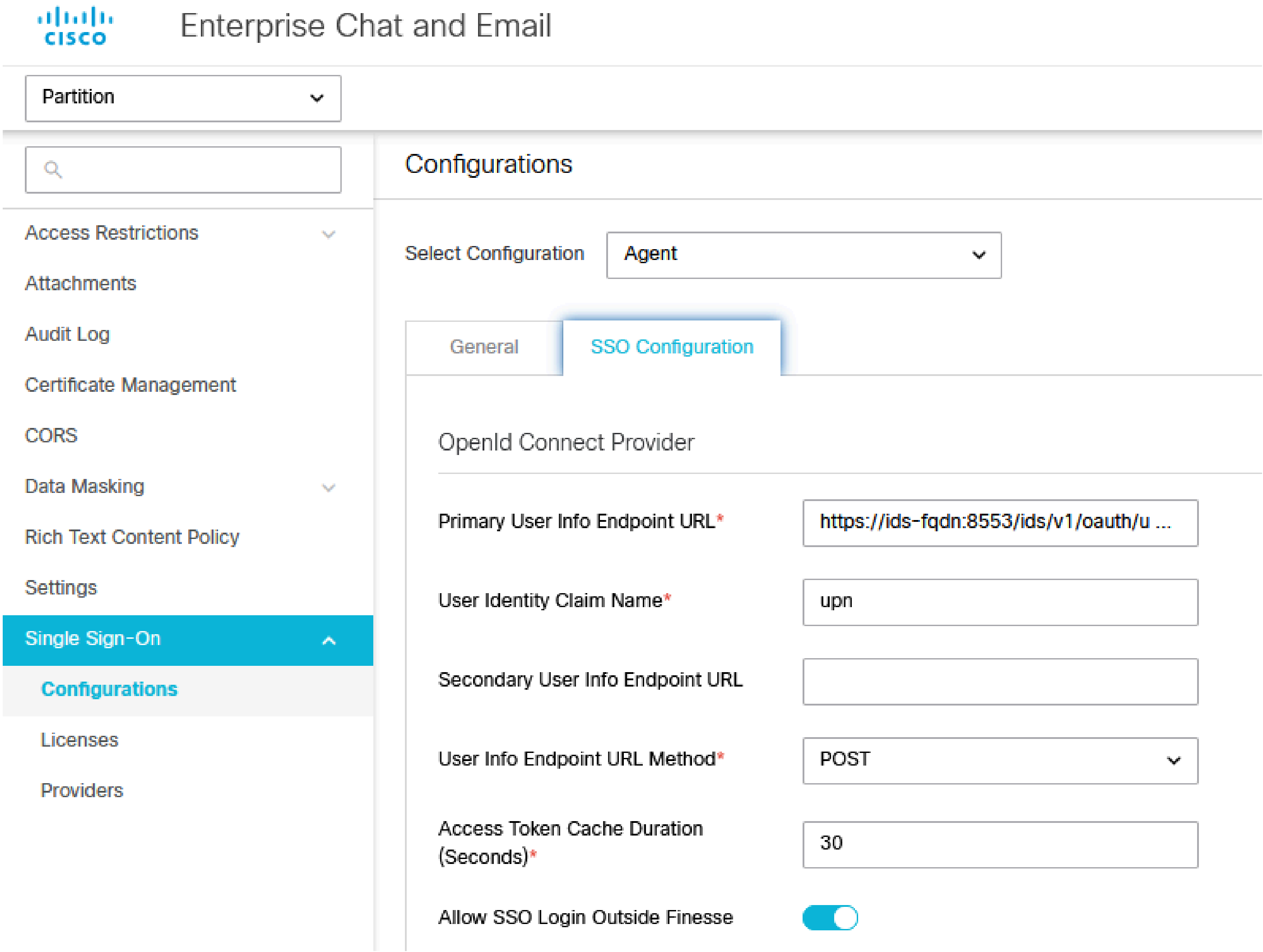
POST：將資料傳送到指定終端的Cisco IDS伺服器的方法。

存取權杖快取持續時間（秒）

- 必須在ECE中快取承載令牌的持續時間（秒）。
- 驗證呼叫成功的持有者記號只會儲存在快取中。（最小值：1；最大值30）

允許SSO在Finesse外部登入

- 如果您希望允許具有管理員或主管角色的使用者使用其SSO登入憑據登入到Finesse外部的ECE分割槽，請按一下此切換按鈕。
- 如果啟用，則必須在[辨識提供者]和[服務提供者]區段下提供資訊。
- 這要求您的IdP配置允許共用的IdP伺服器。



Configurations

Select Configuration: Agent

OpenId Connect Provider

Primary User Info Endpoint URL*: https://ids-fqdn:8553/ids/v1/oauth/u ...

User Identity Claim Name*: upn

Secondary User Info Endpoint URL:

User Info Endpoint URL Method*: POST

Access Token Cache Duration (Seconds)*: 30

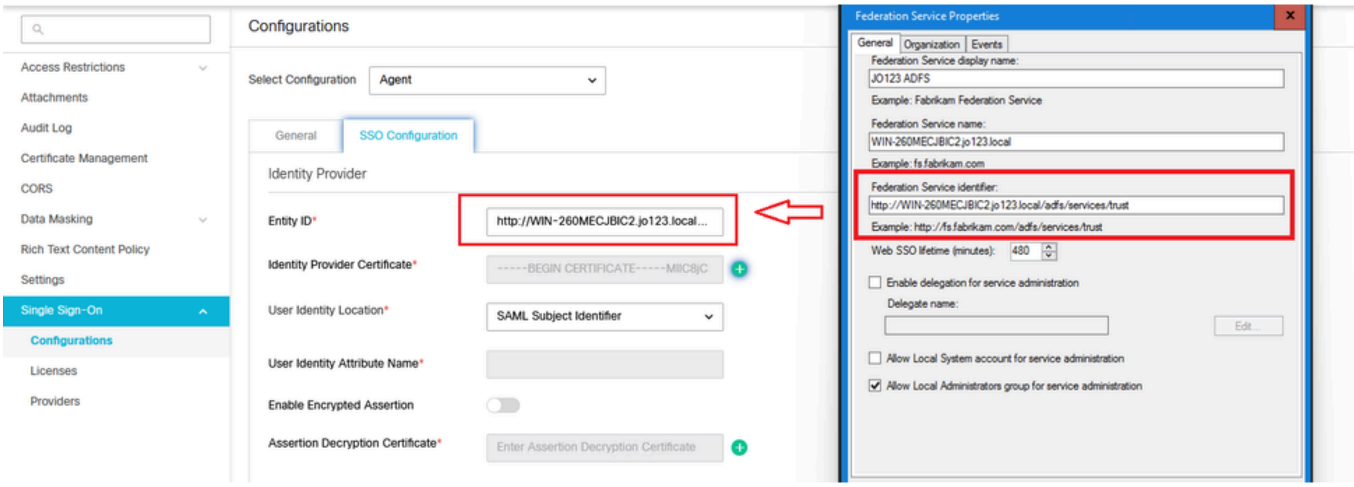
Allow SSO Login Outside Finesse: On

b.身份提供者

實體ID

- IdP伺服器的實體ID。

注意：此值必須與AD FS管理控制檯中的「聯合身份驗證服務識別符號」值完全匹配。



Configurations

Select Configuration: Agent

General | SSO Configuration

Identity Provider

Entity ID*: http://WIN-260MECJBIC2.jo123.local...

Identity Provider Certificate*: -----BEGIN CERTIFICATE-----MIIC8jC

User Identity Location*: SAML Subject Identifier

User Identity Attribute Name*:

Enable Encrypted Assertion

Assertion Decryption Certificate*: Enter Assertion Decryption Certificate

Federation Service Properties

General | Organization | Events

Federation Service display name: JO123 ADFS

Example: Fabrikam Federation Service

Federation Service name: WIN-260MECJBIC2.jo123.local

Example: fs.fabrikam.com

Federation Service identifier: http://WIN-260MECJBIC2.jo123.local/adfs/services/trust

Example: http://fs.fabrikam.com/adfs/services/trust

Web SSO lifetime (minutes): 480

□ Enable delegation for service administration

Delegate name:

Edit...

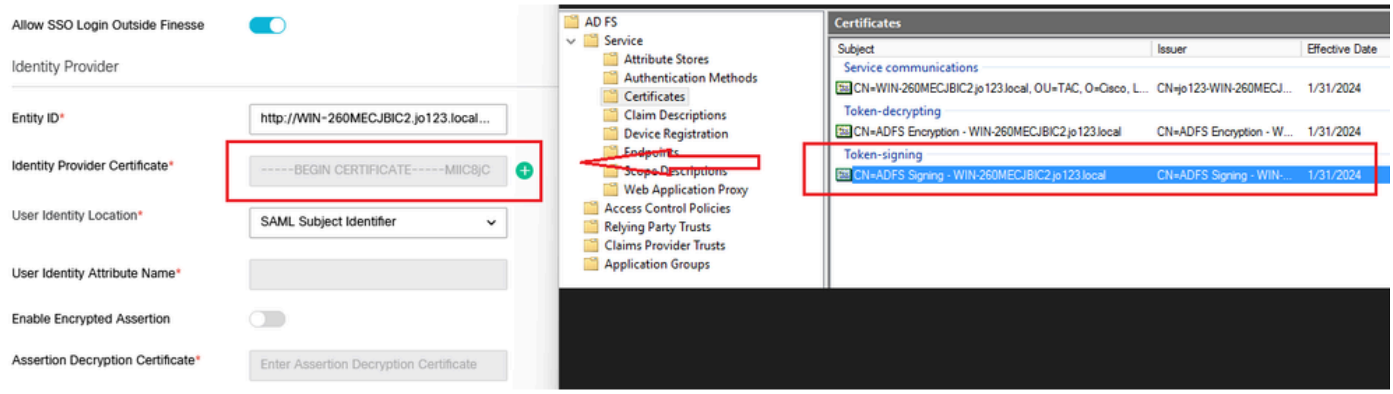
□ Allow Local System account for service administration

☑ Allow Local Administrators group for service administration

辨識提供者憑證

- 公開金鑰憑證。

- 憑證必須以「-----BEGIN CERTIFICATE-----」開頭，以「-----END CERTIFICATE-----」結尾
- 這是AD FS管理控制檯>服務>證書>令牌簽名中的令牌簽名證書。



Allow SSO Login Outside Finesse: on

Identity Provider

Entity ID*	http://WIN-260MECJBIC2.jo123.local...
Identity Provider Certificate*	-----BEGIN CERTIFICATE-----MIIC8jC
User Identity Location*	SAML Subject Identifier
User Identity Attribute Name*	
Enable Encrypted Assertion	off
Assertion Decryption Certificate*	Enter Assertion Decryption Certificate

Certificates

Subject	Issuer	Effective Date
Service communications		
CN=WIN-260MECJBIC2.jo123.local, OU=TAC, O=Cisco, L...	CN=jo123-WIN-260MECJ...	1/31/2024
Token-decrypting		
CN=ADFS Encryption - WIN-260MECJBIC2.jo123.local	CN=ADFS Encryption - W...	1/31/2024
Token-signing		
CN=ADFS Signing - WIN-260MECJBIC2.jo123.local	CN=ADFS Signing - WIN-...	1/31/2024

使用者身份位置

- 選擇SAML Subject Identifier，將證書中的標識位置設定為預設SAML使用者識別符號，如SAML宣告中的主題（例如，<saml：Subject>中的使用者名稱）。
- 選擇SAML Attribute以將身份位置分配給證書中的特定屬性，例如email.address。在User Identity Attribute Name欄位中提供屬性。

使用者身份辨識屬性名稱

- 僅當使用者ID位置值是SAML屬性時適用。
- 這可以在SAML斷言中調整，並用於為使用者的身份驗證選擇其他屬性，例如電子郵件地址。
- 它也可以用來建立具有SAML屬性的新使用者。
- 例如，如果使用者是透過email.address屬性中提供的值辨識的，而提供的電子郵件地址值與系統中的任何使用者都不匹配，則會使用提供的SAML屬性建立新使用者。

啟用加密宣告（可選）

- 如果您要啟用具有Identity Provider的加密宣告以進行主控台登入，請按一下[切換]按鈕，將值設定為[啟用]。
- 否則，將該值設定為「停用」。

宣告解密憑證

如果Enable encrypted assertion設定為Enabled，請按一下Search and Add按鈕，並確認您更改證書的選擇。

在Assertion Decryption Certificate窗口中提供詳細資訊：

- Java Keystore檔案：提供Java Keystore檔案的檔案路徑。此檔案採用.jks格式，包含系統訪問由身份提供程式保護的檔案所需的解密金鑰。
- 別名：解密金鑰的唯一辨識碼。
- 金鑰儲存庫密碼：存取Java金鑰儲存庫檔案所需的密碼。
- 金鑰密碼：存取別名的解密金鑰所需的密碼。

註：這必須與AD FS管理控制檯上配置的ECE信賴方信任的「加密」頁籤中的證書匹配。

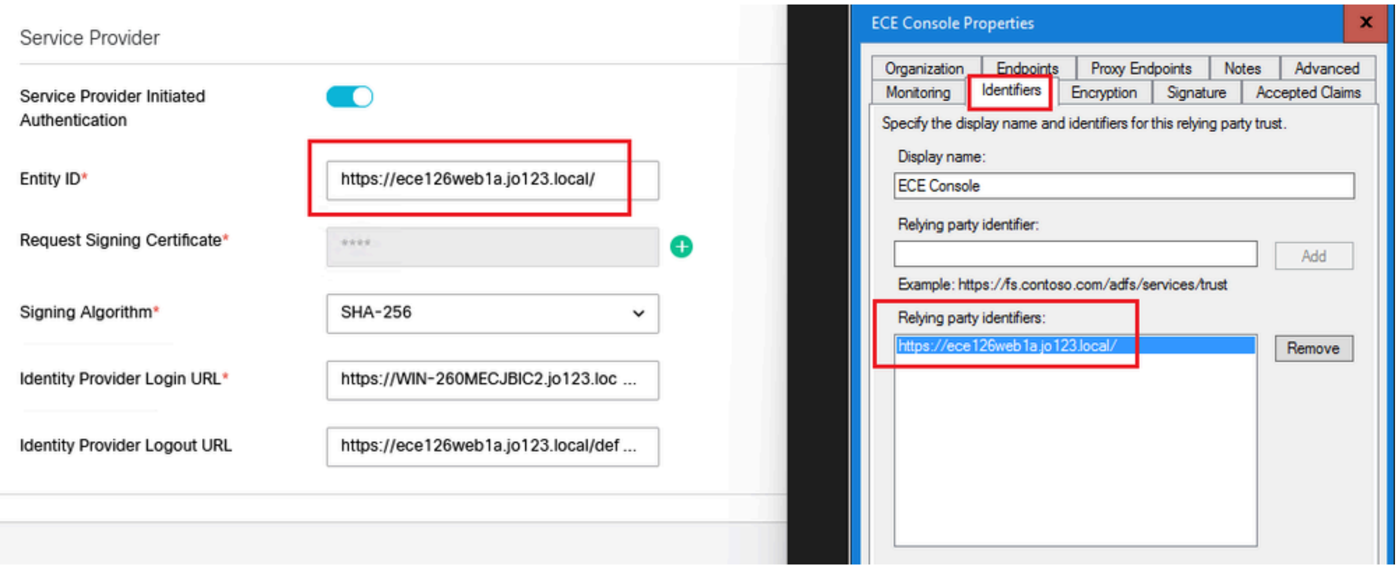
c.服務提供商

服務提供者啟動的驗證

- 將切換按鈕設定為「啟用」。

實體ID

- 提供ECE應用程式的外部URL。



Service Provider

Service Provider Initiated Authentication

Entity ID*: https://ece126web1a.jo123.local/

Request Signing Certificate*: ****

Signing Algorithm*: SHA-256

Identity Provider Login URL*: https://WIN-260MECJBIC2.jo123.loc ...

Identity Provider Logout URL: https://ece126web1a.jo123.local/def ...

ECE Console Properties

Specify the display name and identifiers for this relying party trust.

Display name: ECE Console

Relying party identifier:

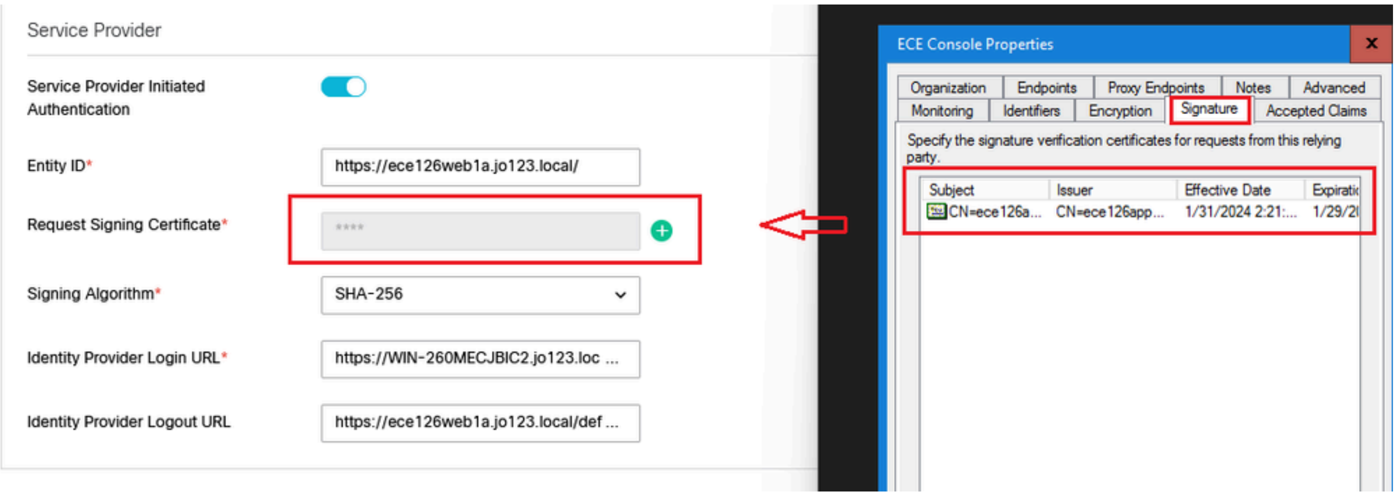
Example: https://fs.contoso.com/adfs/services/trust

Relying party identifiers: https://ece126web1a.jo123.local/

要求簽署憑證

- 需要Java Keystore (JKS)證書才能提供必要的資訊。
- 使用步驟11中生成的別名和金鑰庫/金鑰密碼上傳.jks檔案。

註：這必須匹配上傳到AD FS管理控制檯上配置的ECE信賴方信任的「簽名」頁籤的證書。



Service Provider

Service Provider Initiated Authentication

Entity ID*	https://ece126web1a.jo123.local/
Request Signing Certificate*	****
Signing Algorithm*	SHA-256
Identity Provider Login URL*	https://WIN-260MECJBIC2.jo123.loc ...
Identity Provider Logout URL	https://ece126web1a.jo123.local/def ...

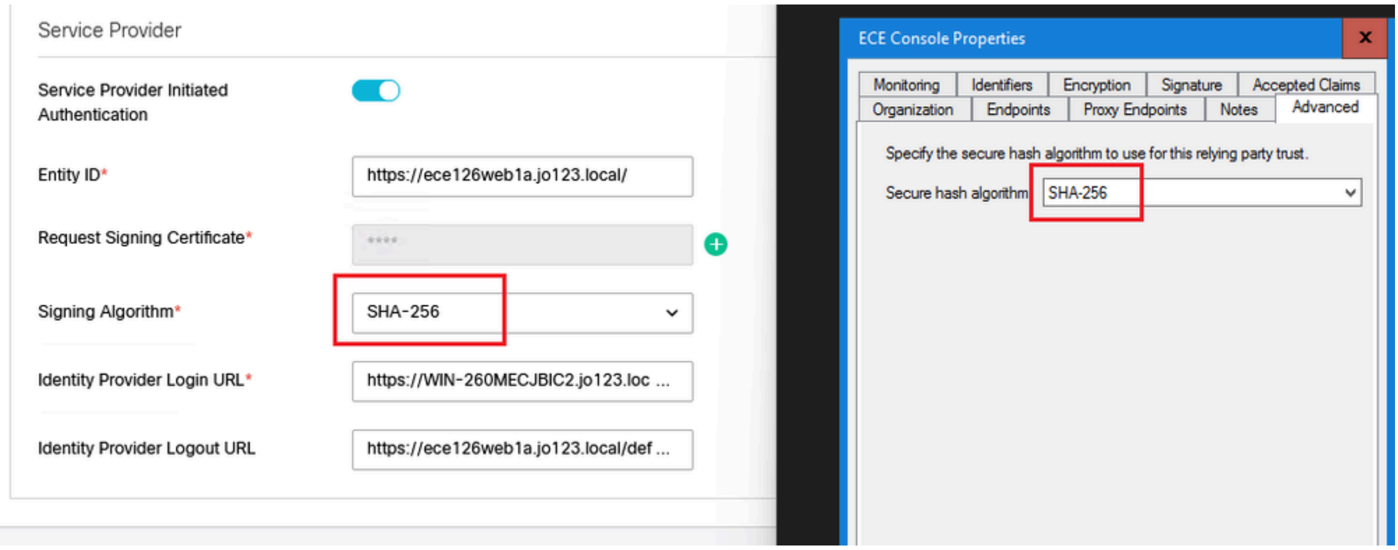
ECE Console Properties

Specify the signature verification certificates for requests from this relying party.

Subject	Issuer	Effective Date	Expiratio
CN=ece126a...	CN=ece126app...	1/31/2024 2:21:...	1/29/2

簽署演演算法

- 設定服務提供者的簽署演演算法。
- 如果使用ADFS，該值必須與在「高級」頁籤下為ECE建立的信賴方信任中選定的演算法匹配。



Service Provider

Service Provider Initiated Authentication

Entity ID*: https://ece126web1a.jo123.local/

Request Signing Certificate*: ****

Signing Algorithm*: SHA-256

Identity Provider Login URL*: https://WIN-260MECJBIC2.jo123.loc ...

Identity Provider Logout URL: https://ece126web1a.jo123.local/def ...

ECE Console Properties

Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-256

辨識提供者登入URL

- SAML身份驗證的URL。
- 例如，對於ADFS，應為http://<ADFS>/adfs/ls。

辨識提供者登出URL

- 登出時使用者重新導向的URL。這是選擇性的，可以是任何URL。
- 例如，在SSO註銷後，可以將代理重定向到https://www.cisco.com或任何其他URL。

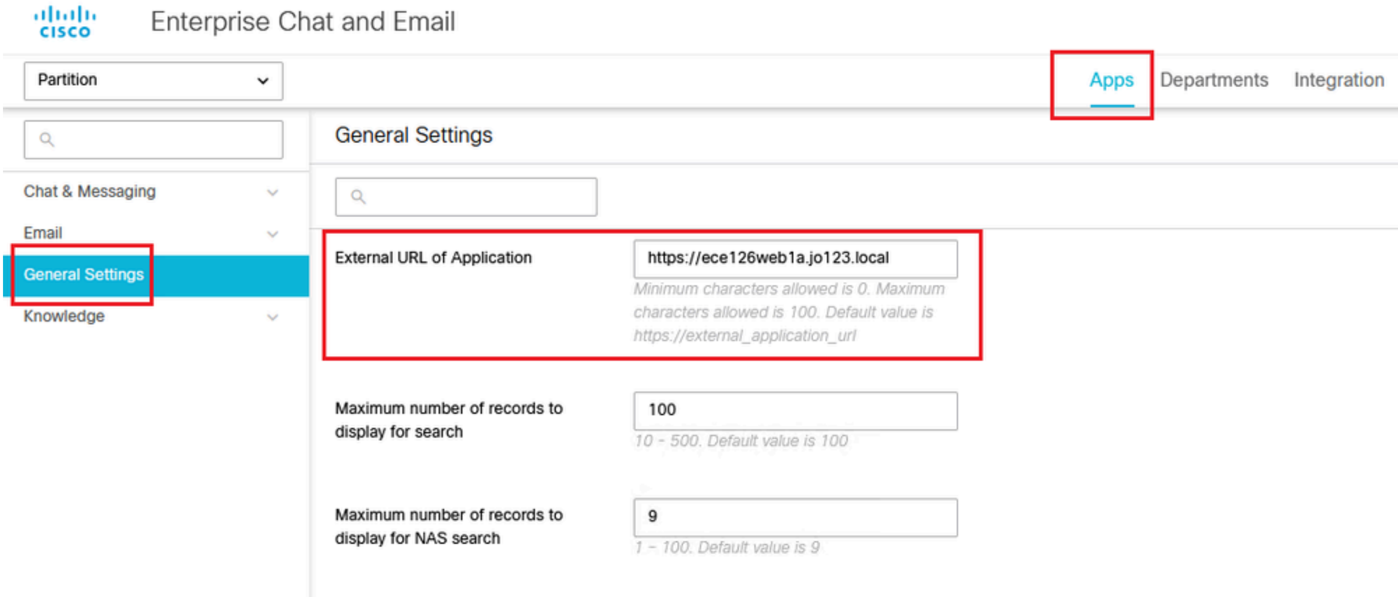
步驟 16

按一下儲存

在分割槽設定中設定Web伺服器/LB URL

步驟 17

確保在「Partition settings」下輸入了正確的Web Server/LB URL >選擇Apps頁籤，然後導航到General Settings > External URL of the Application


Enterprise Chat and Email

General Settings

External URL of Application: https://ece126web1a.jo123.local

Minimum characters allowed is 0. Maximum characters allowed is 100. Default value is https://external_application_url

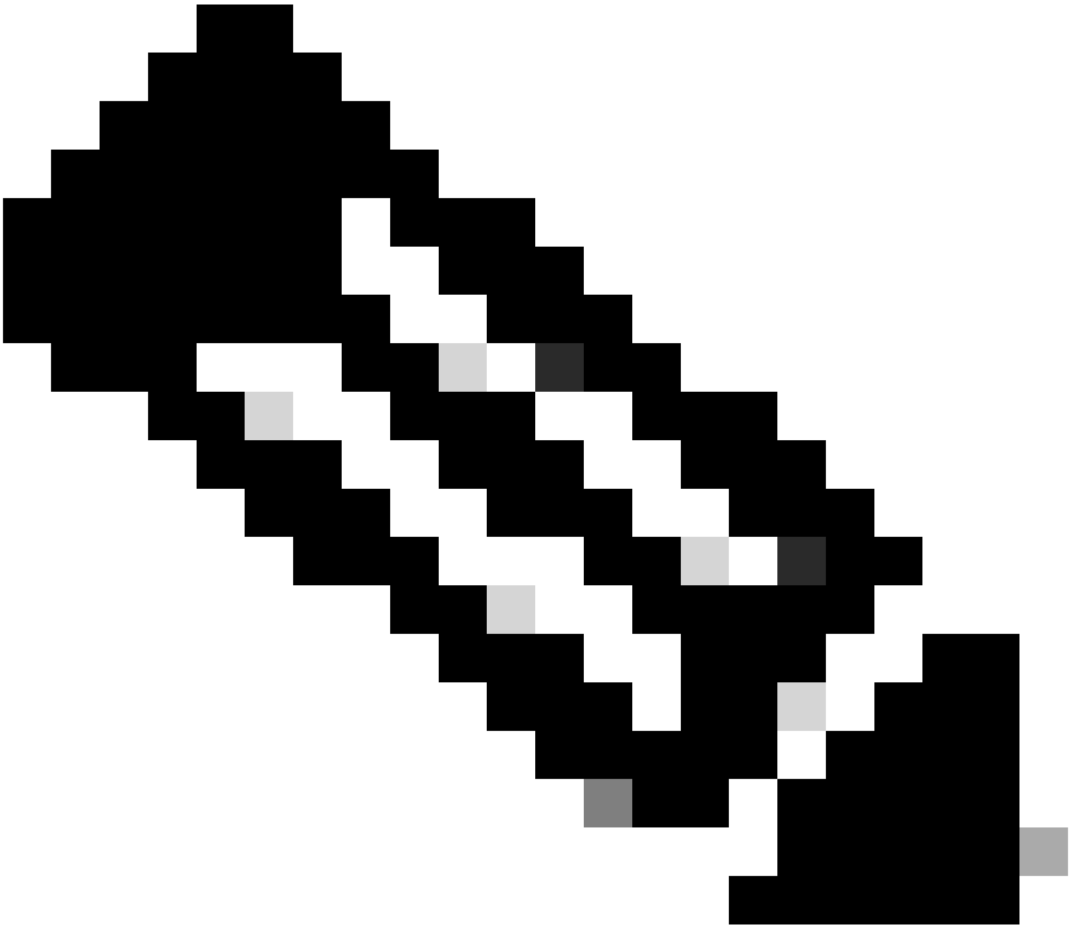
Maximum number of records to display for search: 100

10 - 500. Default value is 100

Maximum number of records to display for NAS search: 9

1 - 100. Default value is 9

為分割槽管理員配置SSO



附註：

- 此步驟僅適用於PCCE。
- 這是在CCE管理WEB介面https:///cceadmin中訪問的ECE小工具。

步驟 18

設定分割區管理員的SSO

1. 在ECE管理控制檯分割槽級別選單下，按一下「Security（安全）」選項，然後從左側選單中選擇「Single Sign-On（單一登入）」>「Configurations（配置）」。
2. 在選擇配置下拉選單中，選擇分割槽管理員，然後輸入配置詳細資訊：

LDAP URL

- LDAP伺服器的URL。
- 這可以是LDAP伺服器的網域控制站URL (例如，ldap://LDAP_server:389)或通用類別目錄URL (例如，ldap://LDAP_server:3268)。
- 如果使用LDAP查詢配置ECE，則透過CCE管理控制檯訪問ECE時，可以自動將分割槽增加到系統。
- 但是，在單個林中具有多個域或配置了備用UPN的Active Directory部署中，不能使用具有標準LDAP埠389和636的域控制器URL。
- LDAP整合可以配置為使用帶有埠3268和3269的全局目錄URL。

基礎

注意：最佳做法是使用全局目錄URL。 如果不使用GC，則ApplicationServer日誌中會出現以下錯誤。

- LDAP身份驗證時出現異常<@> javax.naming.PartialResultException：未處理的連續參照；剩餘名稱 'DC=example，DC=com'

DN屬性

- 包含使用者登入名稱的DN屬性。
- 例如，userPrincipalName。

基礎

- 為Base指定的值被應用程式用作搜尋庫。
- Search base是在LDAP目錄樹中搜尋的開始位置。
- 例如，DC=mycompany， DC=com。

LDAP搜尋的DN

- 如果您的LDAP系統不允許匿名連結，請提供在LDAP目錄樹狀結構上具有搜尋許可權的使用者辨別名稱(DN)。
- 如果LDAP伺服器允許匿名繫結，請將此欄位留空。

密碼

- 如果您的LDAP系統不允許匿名連結，請提供在LDAP目錄樹狀結構上具有搜尋許可權的使用者密碼。
- 如果LDAP伺服器允許匿名繫結，請將此欄位留空。

步驟 19

按一下儲存

現在完成ECE中代理和分割槽管理員的單一登入配置。

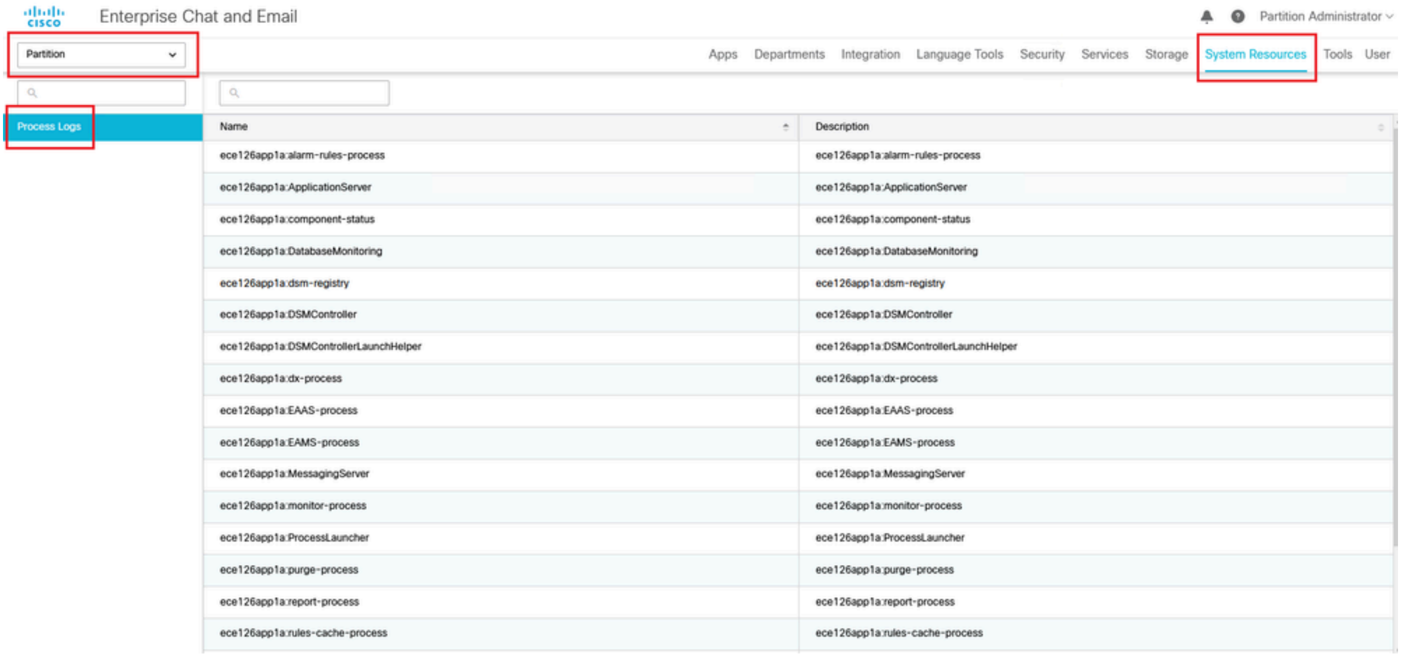
疑難排解

設定追蹤層級

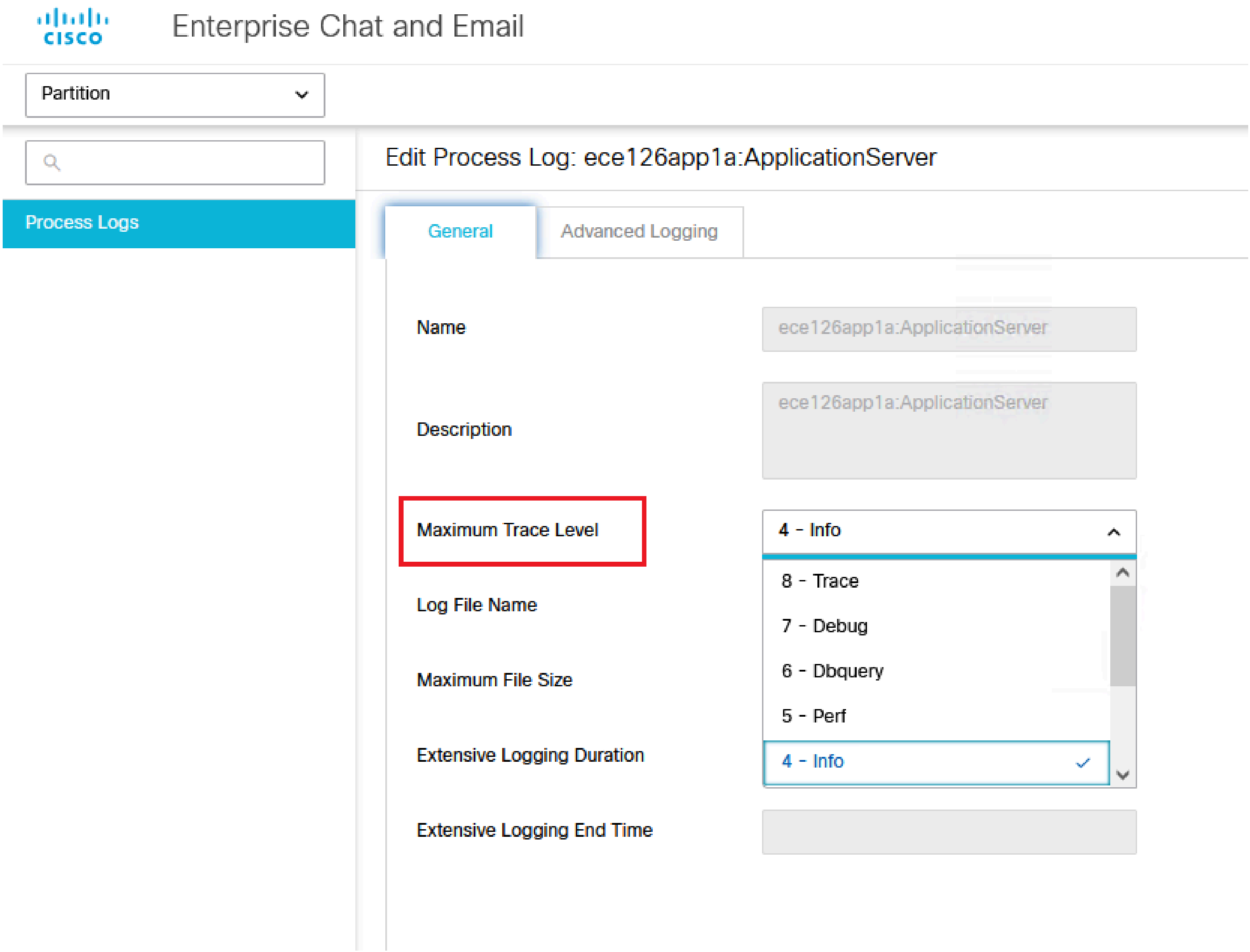
1. 在ECE管理控制檯的分割槽級選單下，按一下System Resources選項，然後從左側選單中選擇Process Logs。
2. 從進程清單中選擇ApplicationServer進程>從「最大跟蹤級別」下拉選單設定所需的跟蹤級別。

附註：

- 要排除初始設定或重新配置期間的SSO登入錯誤，請將ApplicationServer進程跟蹤設定為第7級。
- 在重現錯誤後，將跟蹤級別設定回預設級別4，以避免覆蓋日誌。



Name	Description
ece126app1a:alarm-rules-process	ece126app1a:alarm-rules-process
ece126app1a:ApplicationServer	ece126app1a:ApplicationServer
ece126app1a:component-status	ece126app1a:component-status
ece126app1a:DatabaseMonitoring	ece126app1a:DatabaseMonitoring
ece126app1a:dsm-registry	ece126app1a:dsm-registry
ece126app1a:DSMController	ece126app1a:DSMController
ece126app1a:DSMControllerLaunchHelper	ece126app1a:DSMControllerLaunchHelper
ece126app1a:dx-process	ece126app1a:dx-process
ece126app1a:EAAS-process	ece126app1a:EAAS-process
ece126app1a:EAMS-process	ece126app1a:EAMS-process
ece126app1a:MessagingServer	ece126app1a:MessagingServer
ece126app1a:monitor-process	ece126app1a:monitor-process
ece126app1a:ProcessLauncher	ece126app1a:ProcessLauncher
ece126app1a:purge-process	ece126app1a:purge-process
ece126app1a:report-process	ece126app1a:report-process
ece126app1a:rules-cache-process	ece126app1a:rules-cache-process



Edit Process Log: ece126app1a:ApplicationServer

Name	ece126app1a:ApplicationServer
Description	ece126app1a:ApplicationServer
Maximum Trace Level	4 - Info
Log File Name	
Maximum File Size	
Extensive Logging Duration	
Extensive Logging End Time	

疑難排解案例1

錯誤

- 錯誤碼： 500
- 錯誤描述：應用程式此時無法登入使用者，因為辨識提供者登入失敗。

日誌分析

- IdP登入失敗- <samlp：Status><samlp：StatusCode Value="urn：oasis：names：tc：SAML：2.0：status：Responder" /></samlp：Status>
- 此處，狀態「響應方」表示AD FS端存在一些問題-在本例中，主要是在ECE管理控制檯（SSO配置>服務提供商）上載入的「請求簽名證書」，以及在「簽名」頁籤下上傳到ECE信賴方信任的證書。
- 這是使用Java Keystore檔案產生的憑證。

應用程式伺服器記錄-追蹤層級7：

<#root>

```
unmarshallAndValidateResponse:


2022-09-21 18:18:15.002 GMT+0000 <@> ERROR <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID
2022-09-21 18:18:15.002 GMT+0000 <@> INFO <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID:


L10N_USER_STATUS_CODE_ERROR:


2022-09-21 18:18:15.002 GMT+0000 <@> ERROR <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.unmarshallAndValidateResponse(SAML2_0
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Han
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Han
at com.egain.platform.module.security.sso.handler.OpenIDConnect_Handler.validateReqWithAttributes(OpenI
at com.egain.platform.module.security.sso.admin.SSOAdministrator.validateRequestWithAttributes(SSOAdmin
at com.egain.platform.module.security.sso.controller.SSOControllerServlet.doPost(SSOControllerServlet.j
.
.
.
.
at java.lang.Thread.run(Thread.java:834) ~[?:?]



errorCode=500&errorString=The application is not able to login the user at this time as Identity Provide


2022-09-21 18:18:15.003 GMT+0000 <@> DEBUG <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID
2022-09-21 18:18:15.003 GMT+0000 <@> DEBUG <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID
```

解析

- 請參閱「配置代理Single Sign-On -服務提供商」部分中的請求簽名證書配置。
- 確保將在步驟11中生成的Java Keystore .jks檔案上傳到ECE管理控制檯上的「Request Signing certificate」欄位，該欄位位於SSO Configuration > Select Configuration 'Agent' > 'SSO Configuration' tab > Service Provider > Request Signing certificate下。
- 確保在ECE信賴方信任的「簽名」頁籤下上載.crt檔案(第12步)。

疑難排解案例2

錯誤

- 錯誤碼： 400
- 錯誤描述： SAML回應語彙基元無效：簽章驗證失敗。

日誌分析

- 此錯誤表示ADFS上的「令牌簽名證書」與ECE SSO配置上的「身份提供程式證書」證書不匹配。

應用程式伺服器記錄-追蹤層級7：

<#root>

```
Entering 'validateSSOCertificate' and validating the saml response against certificate:


2022-10-07 15:27:34.523 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.520 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.521 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.521 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.521 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.523 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
.....
-----END CERTIFICATE----- <@>
2022-10-07 15:27:34.523 GMT+0000 <@> INFO <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID:

Error: Could not parse certificate: java.io.IOException: Incomplete data:


2022-10-07 15:27:34.523 GMT+0000 <@> ERROR <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.524 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.525 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.525 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID

Signature validation failed:


2022-10-07 15:27:34.525 GMT+0000 <@> ERROR <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.525 GMT+0000 <@> INFO <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID:
2022-10-07 15:27:34.525 GMT+0000 <@> ERROR <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.525 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
```

解析

- 在記錄程式碼片段'無法剖析憑證： java.io.IOException： Incomplete data'中看到的錯誤，表示未正確輸入'辨識提供者憑證'內容
- 要解決此問題：在AS FS Management > AD FS > Service > Certificates > Token-Signing > Export this certificate > open in a text editor > copy all contents > paste under 'Identity

provider certificate' fixed in the SSO configuration > Save。

- 請參閱「配置代理單一登入-身份提供程式」部分下的「身份提供程式證書」配置(步驟15)。

疑難排解案例3

錯誤

- 錯誤代碼：401-114
- 錯誤說明：在SAML屬性中找不到使用者標識。

日誌分析

應用程式伺服器記錄-追蹤層級7：

<#root>

getSSODataFromSAMLToken:

```
2024-02-01 01:44:32.081 GMT+0000 <@> ERROR <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
2024-02-01 01:44:32.081 GMT+0000 <@> TRACE <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
```

L10N_USER_IDENTIFIER_NOT_FOUND_IN_ATTRIBUTE:

```
2024-02-01 01:44:32.081 GMT+0000 <@> ERROR <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
com.egain.platform.module.security.sso.exception.SSOLoginException: null
 at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.getSSODataFromSAMLToken(SAML2_0_Hand
 at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.unmarshallAndValidateResponse(SAML2_
 at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Ha
 at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Ha
 at com.egain.platform.module.security.sso.handler.OpenIDConnect_Handler.validateReqWithAttributes(Open
 at com.egain.platform.module.security.sso.admin.SSOAdministrator.validateRequestWithAttributes(SSOAdmi
 at com.egain.platform.module.security.sso.controller.SSOControllerServlet.doPost(SSOControllerServlet.
.
.
.
 at java.lang.Thread.run(Thread.java:830) [?:?]
```

errorCode=401-114&errorString=User Identity not found in SAML attribute: 'upn':

```
2024-02-01 01:44:32.083 GMT+0000 <@> DEBUG <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
2024-02-01 01:44:32.083 GMT+0000 <@> TRACE <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
```

解析

- 此錯誤表示「使用者身份位置」和「使用者身份屬性名稱」欄位中存在配置問題/不匹配。
- 在ECE管理控制檯中的「Single Sign-On」>「Configurations」>下拉選單中，選擇「Agent」

>「SSO Configuration」頁籤>「Identify Provider」(第15步)，檢查並更正使用者身份位置和使用者身份屬性名稱。

相關資訊

在開始任何歐洲經委會安裝或整合之前，您必須仔細審查這些主要檔案。這不是一份全面的歐洲經委會檔案清單。

附註：

- 大多數歐洲經委會檔案有兩個版本。請確保下載並使用適用於PCCE的版本。文檔標題在版本號後為Packaged Contact Center Enterprise或（用於PCCE）或（用於UCCE和PCCE）。
- 在進行任何安裝、升級或整合之前，確保檢視思科企業聊天和電子郵件文檔的開始頁面以瞭解任何更新。
- https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html

ECE版本12.6(1)

- 企業版聊天與電子郵件管理員指南

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）。