

# 在ECE中为代理和分区管理配置SSO并对其进行故障排除

## 目录

---

### [简介](#)

### [先决条件](#)

#### [要求](#)

#### [使用的组件](#)

### [背景信息](#)

### [配置步骤](#)

#### [为ECE配置信赖方信任](#)

#### [配置身份提供程序](#)

#### [创建和导入证书](#)

#### [配置代理单一登录](#)

#### [在分区设置中设置Web服务器/LB URL](#)

#### [为分区管理员配置SSO](#)

### [故障排除](#)

#### [设置跟踪级别](#)

#### [故障排除场景1](#)

##### [Error](#)

##### [日志分析](#)

##### [分辨率](#)

#### [故障排除场景2](#)

##### [Error](#)

##### [日志分析](#)

##### [分辨率](#)

#### [故障排除场景3](#)

##### [Error](#)

##### [日志分析](#)

##### [分辨率](#)

### [相关信息](#)

---

## 简介

本文档介绍在ECE解决方案中为代理和分区管理员配置单一登录(SSO)所需的步骤。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

思科套装联系中心企业版(PCCE)

思科统一联系中心企业版(UCCE)

企业聊天和电子邮件(ECE)

Microsoft Active Directory

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

UCCE版本：12.6(1)

ECE版本：12.6(1)

Windows Server 2016上的Microsoft Active Directory联合身份验证服务(ADFS)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

可以在Finesse外部访问企业聊天和邮件(ECE)控制台，但是，必须启用SSO以允许座席和主管通过Finesse登录到ECE。

还可以为新分区管理员配置单一登录。这可确保登录到Cisco Administrator桌面的新用户有权访问企业聊天和电子邮件管理控制台。

有关单点登录的重要注意事项：

- 分区用户必须在分区级别对安全节点执行为单点登录配置系统的过程，执行必要的操作：查看应用安全和管理应用安全。
- 为了使管理引擎和管理员能够登录代理控制台以外的控制台，一旦启用SSO，您必须在分区设置中提供应用的有效外部URL。有关详细信息，请参阅常规分区设置。
- 配置SSO需要Java密钥库(JKS)证书，以允许具有管理员或主管角色的用户使用其SSO登录凭证登录到Finesse外部的ECE的分区1。请咨询您的IT部门以接收JKS证书。
- 在安装过程中，必须将思科IDS的安全套接字层(SSL)证书导入到所有应用服务器。要获取必要的SSL证书文件，请联系您的IT部门或思科IDS支持。
- Unified CCE的数据库服务器归类区分大小写。从用户信息终端URL返回的声明中的用户名和Unified CCE中的用户名必须相同。如果座席不相同，则单点登录座席无法识别为已登录，并且ECE无法将座席可用性发送到Unified CCE。
- 为Cisco IDS配置SSO会影响已在Unified CCE中配置单点登录的用户。确保在Unified CCE中为您希望在ECE中启用SSO的用户配置为SSO。有关详细信息，请咨询您的Unified CCE管理员。

---

注意：

- 确保在Unified CCE中为您希望在ECE中启用SSO的用户配置为SSO。
- 本文档指定在单一AD FS部署中为ECE配置信赖部件信任的步骤，其中资源联合服务器和帐户联合服务器安装在同一台计算机上。
- 对于拆分AD FS部署，请导航至相应版本的ECE安装和配置指南。

---

## 配置步骤

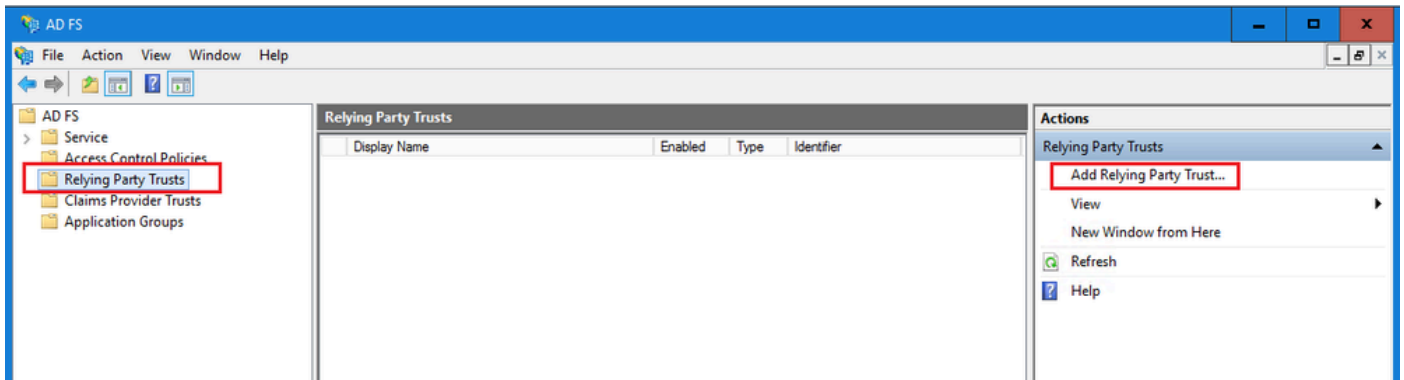
### 为ECE配置信赖方信任

#### 第 1 步

打开AD FS管理控制台并导航到AD FS >“信任关系”>“信赖方信任”。

#### 步骤 2

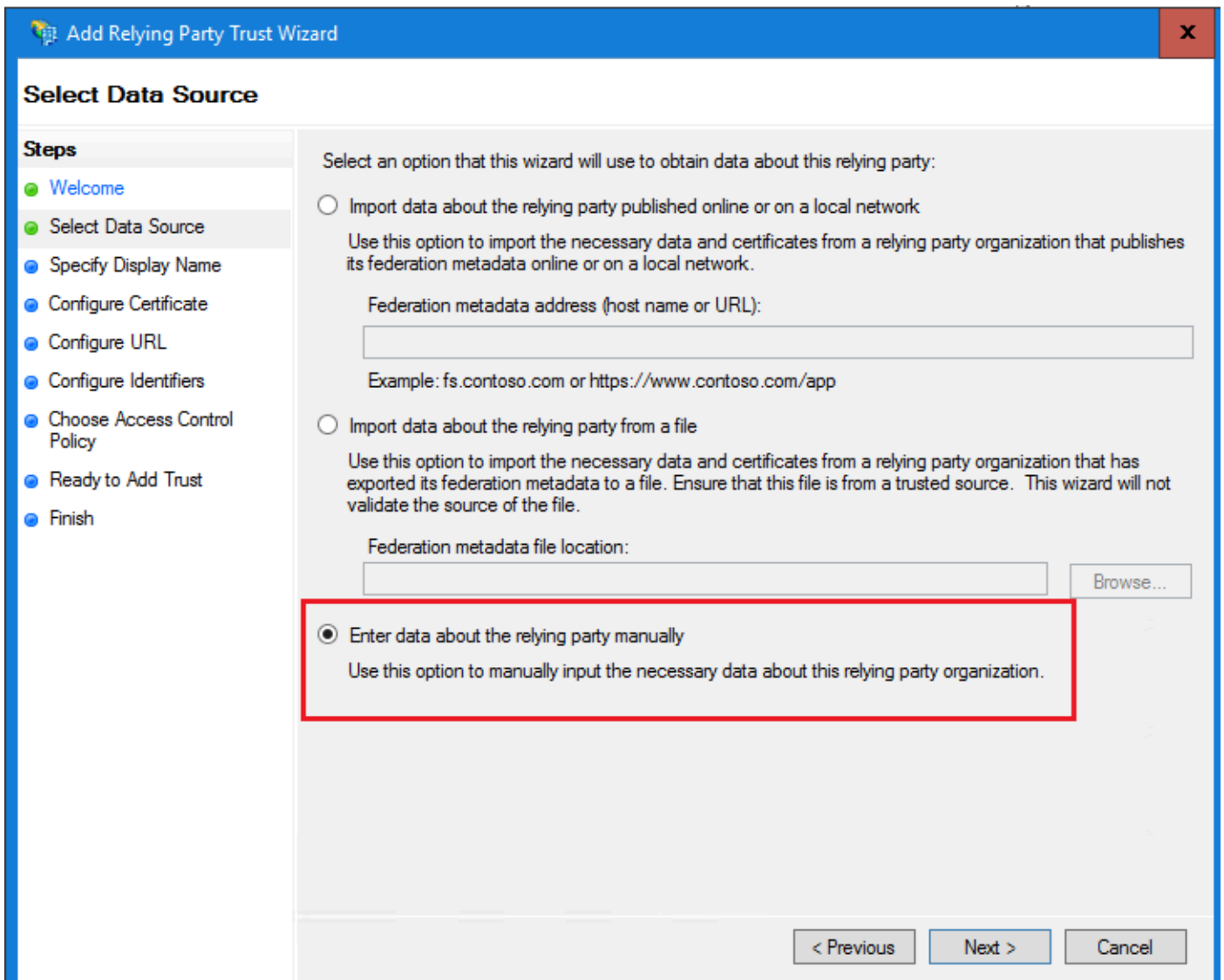
在“操作”部分中，单击添加信赖方信任。



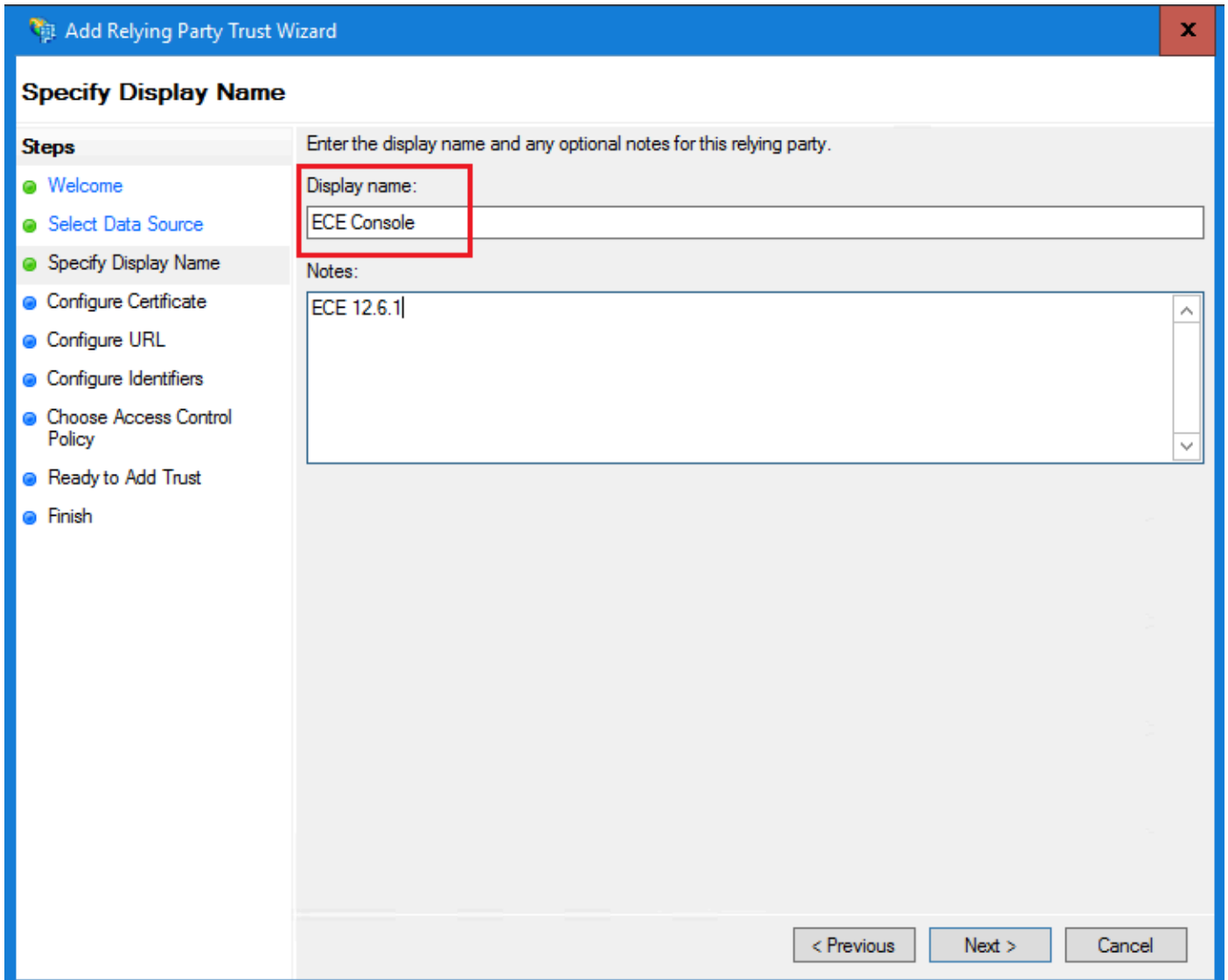
### 步骤 3

在“添加信赖方信任”向导中，单击“开始”并完成以下步骤：

a. 在“选择数据源”页中，选择手动输入关于应答方的数据选项，然后单击“下一步”。



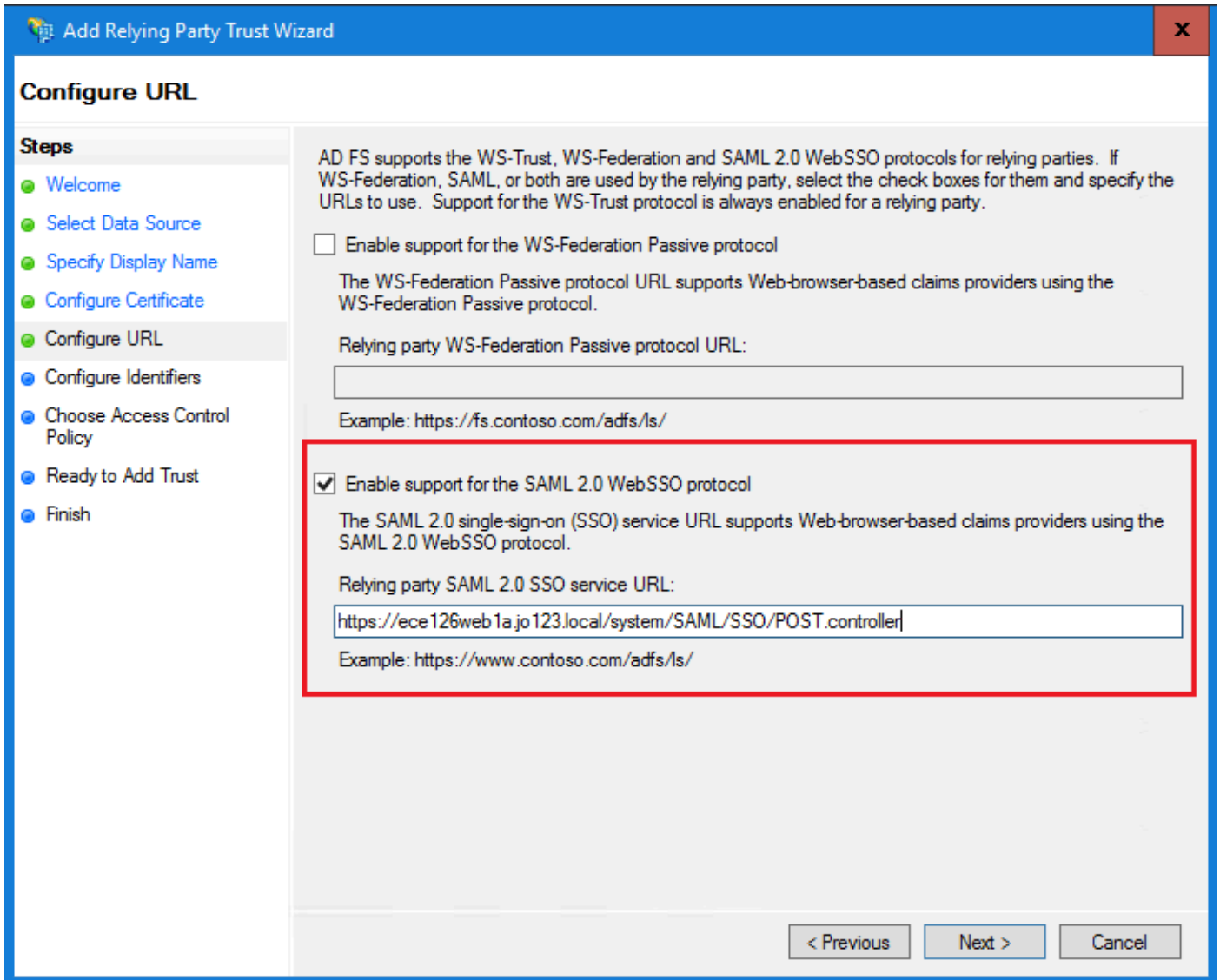
b. 在“指定显示名称”页中，为信赖方提供显示名称。单击“下一步”



c.在Configure URL ( 配置URL ) 页面中：

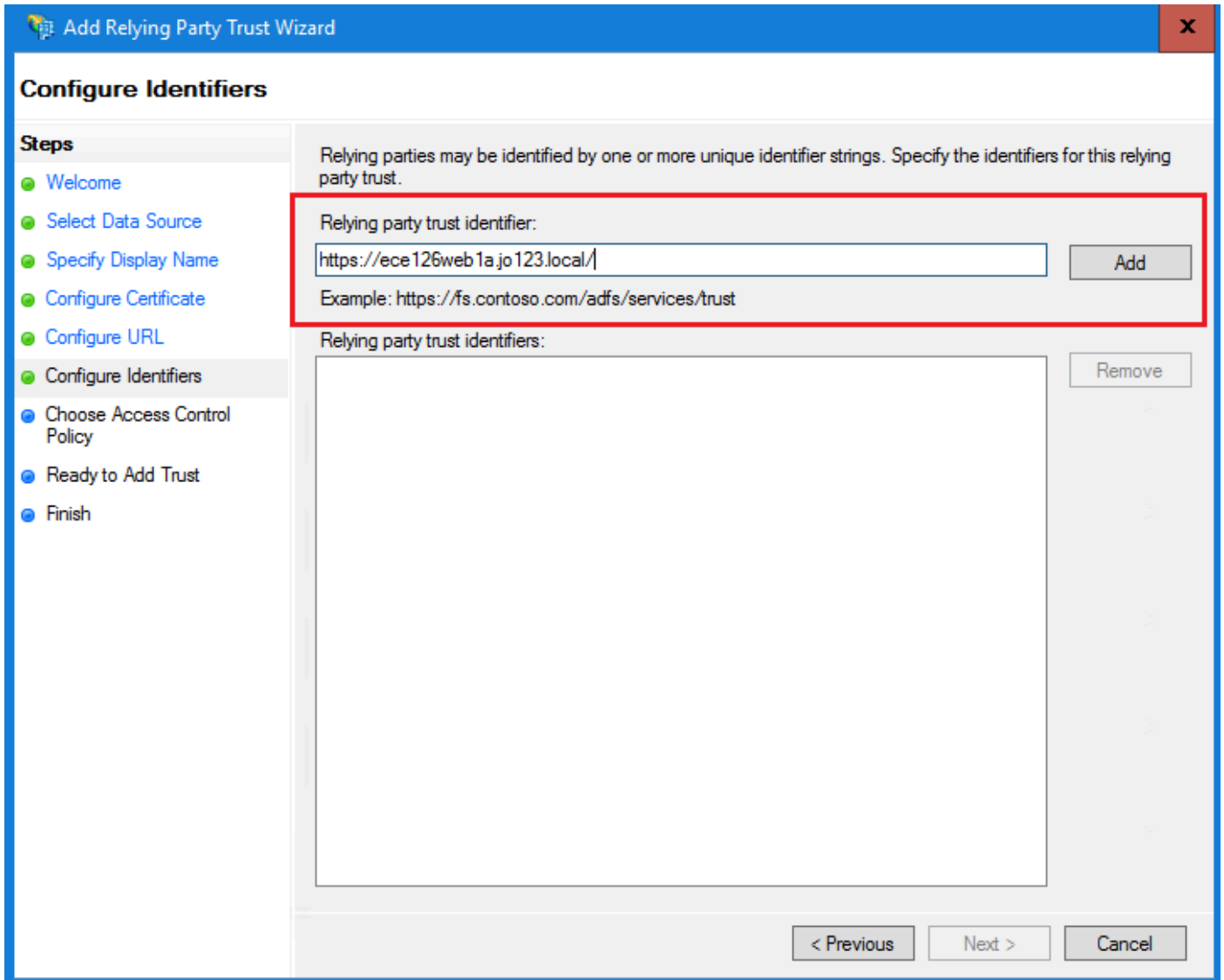
i.选择Enable support for the SAML 2.0 Web SSO protocol选项。

ii.在信赖方SAML 2.0 SSO服务器URL字段中，按照以下格式提供URL：`https://<Web-Server-Or-Load-Balancer-FQDN>/system/SAML/SSO/POST.controller`

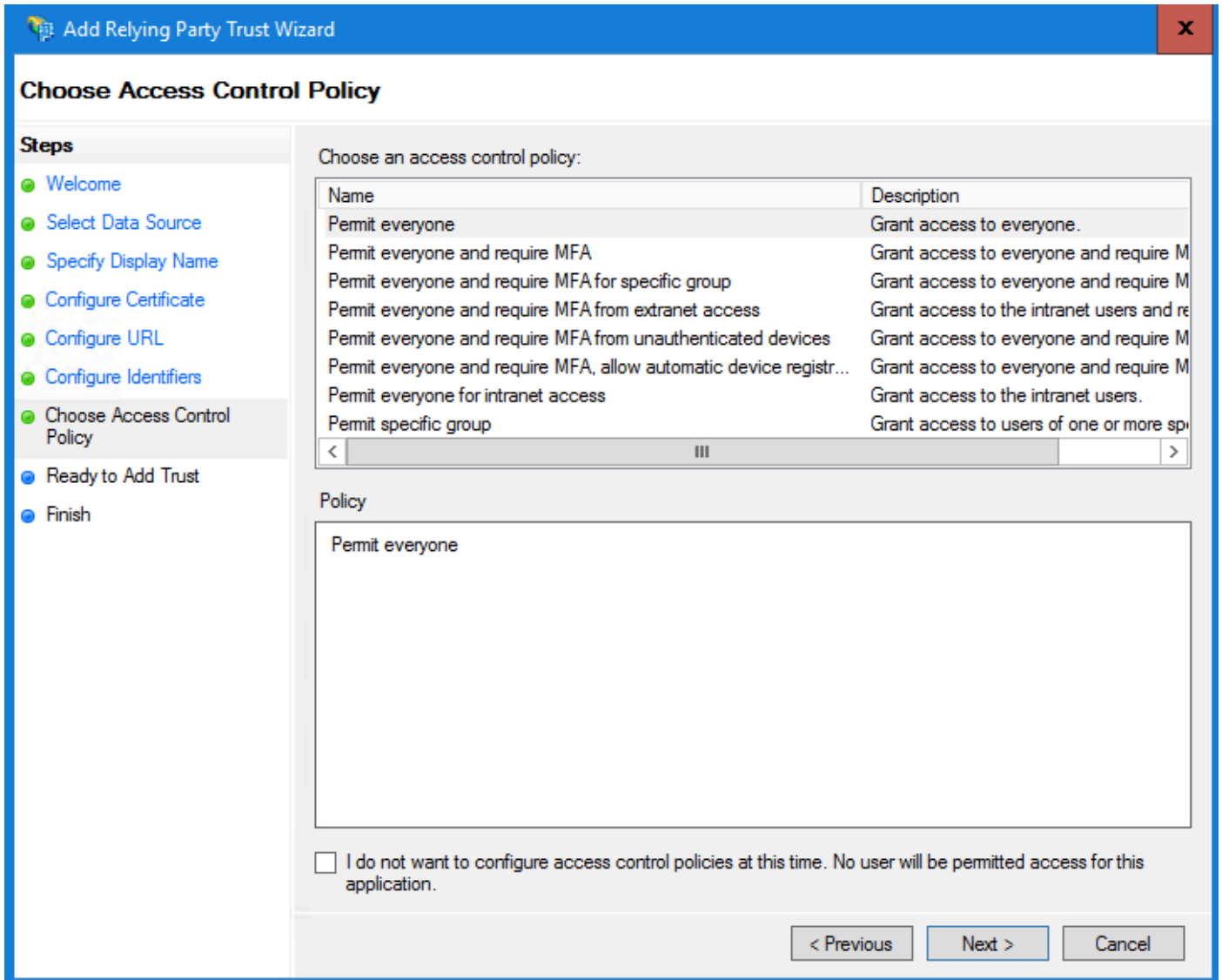


d.在“配置标识符”页上，提供信赖方信任标识符，然后单击“添加”。

- 值必须采用以下格式：`https:// <Web-Server-Or-Load-Balancer-FQDN>/`

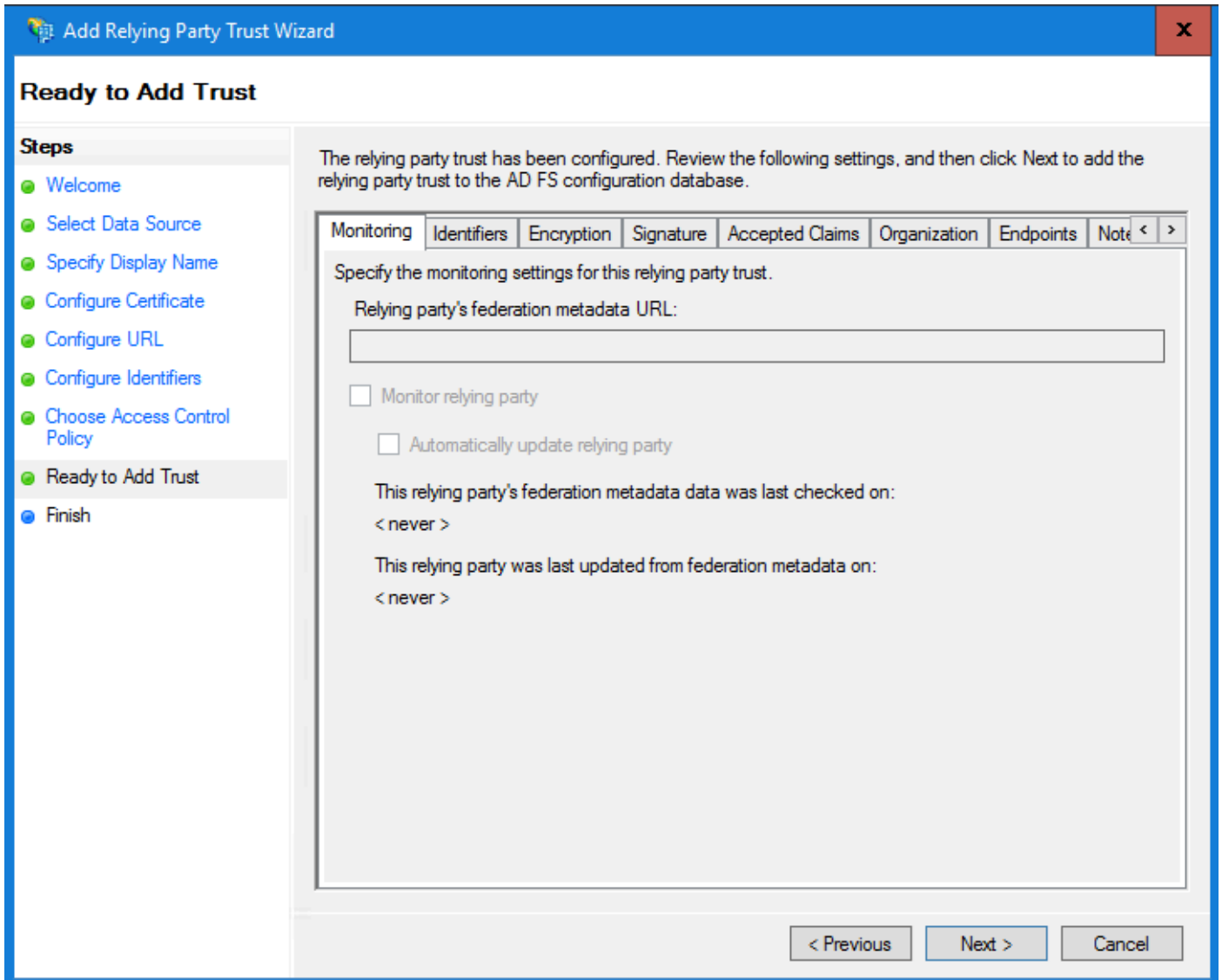


e. 在 Choose Access Control Policy 页中，单击具有默认值“Permit everyone”策略的“next”。

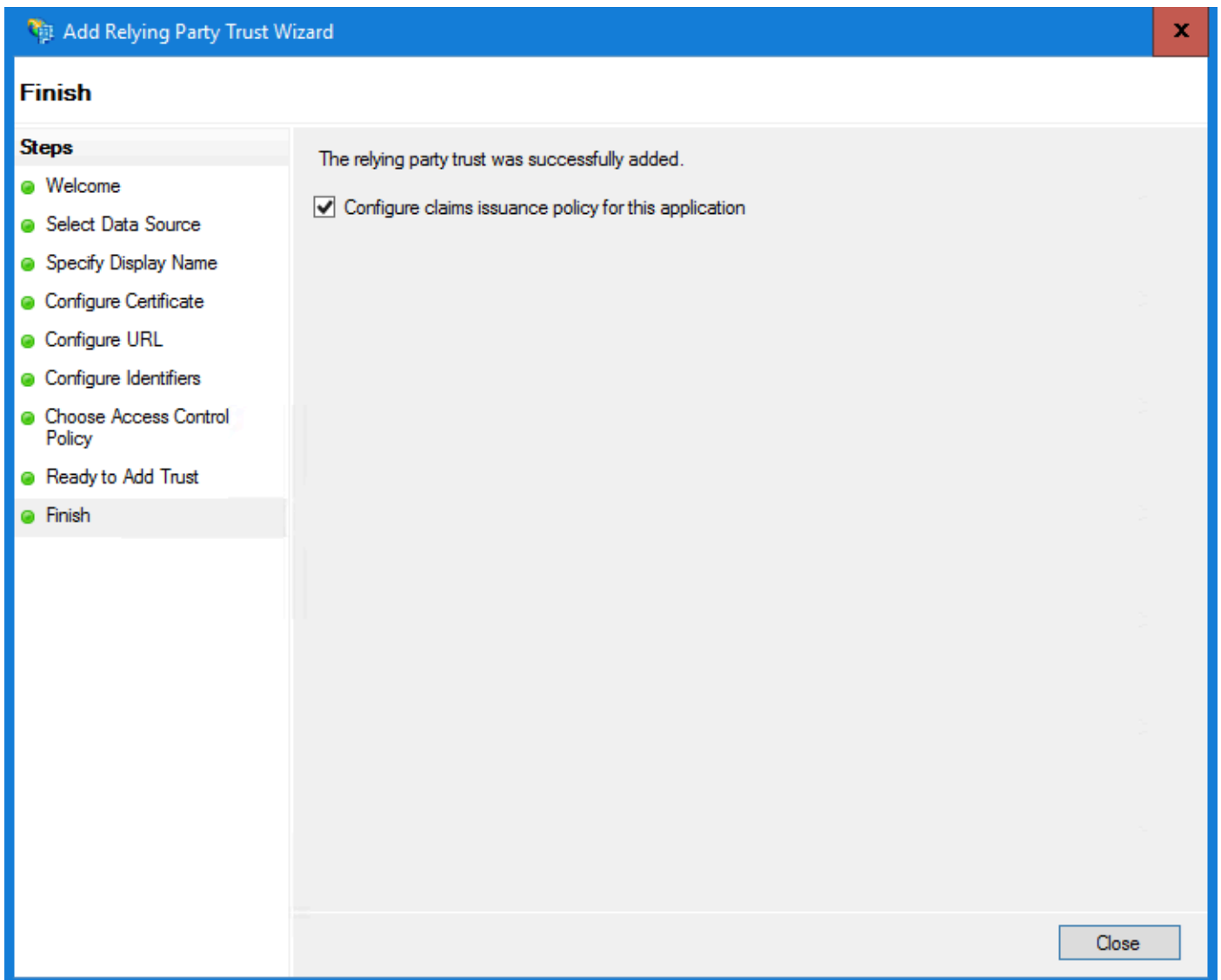


f. 在“准备添加信任”页中，单击“下一步”。



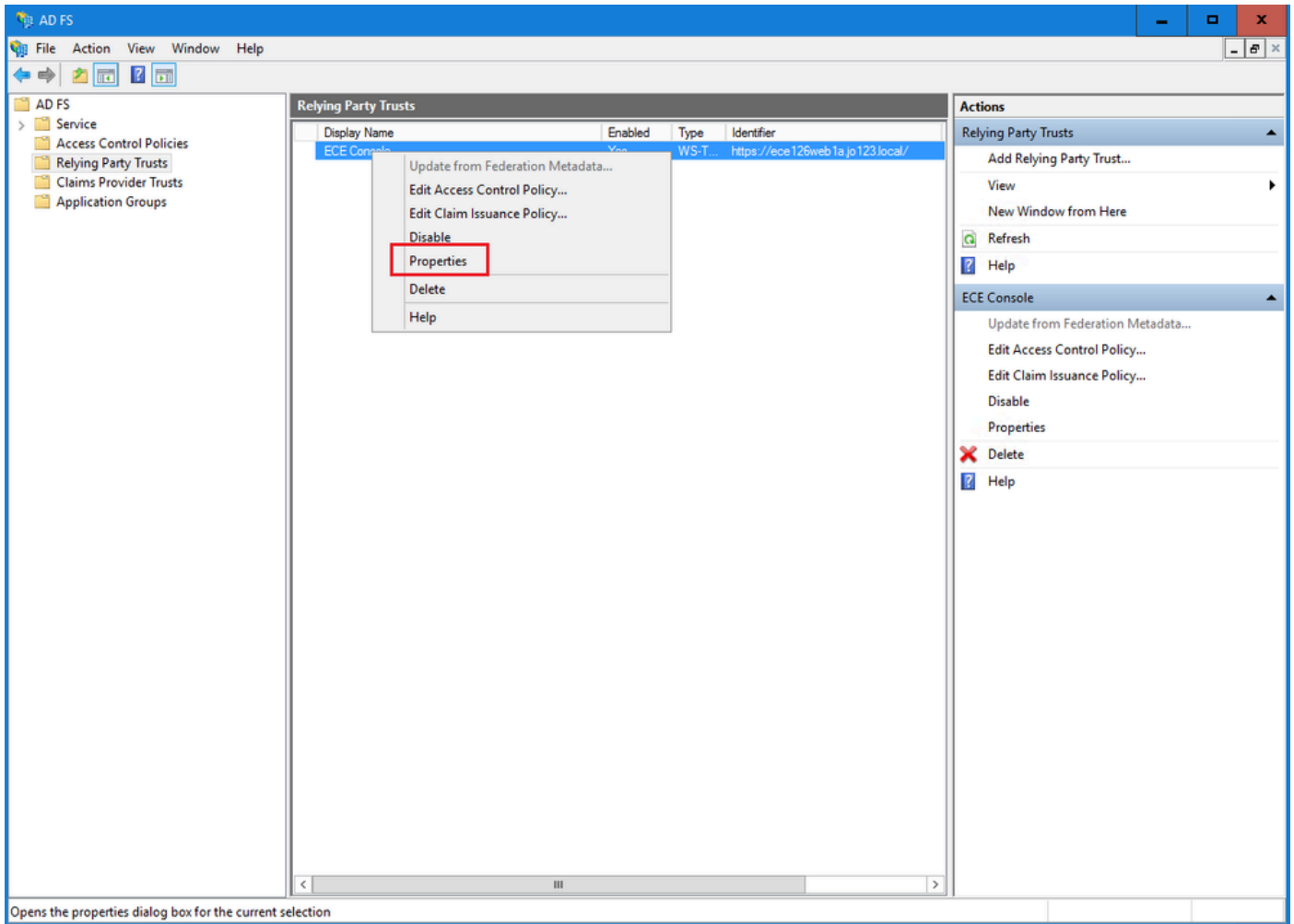


g.成功添加信赖方信任后，点击“关闭”。



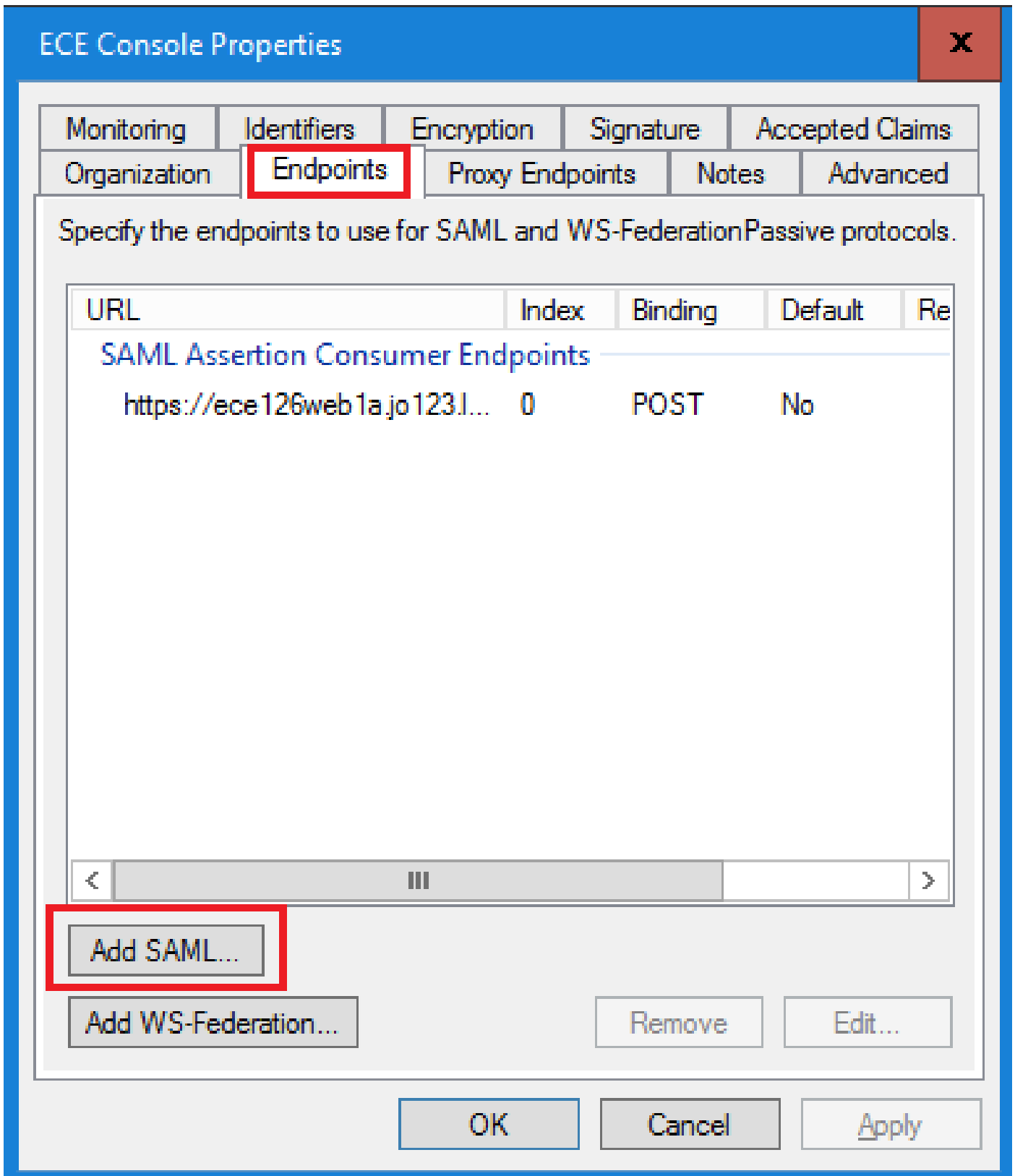
#### 步骤 4

在信赖提供程序信任列表中，选择为ECE创建的信赖方信任，并在“操作”部分中单击属性。



## 步骤 5

在“属性”窗口中，导航到终端选项卡，然后单击添加SAML..按钮



#### 步骤 6

在Add an Endpoint窗口中，按照说明进行配置：

1. 选择SAML Logout作为终端类型。
2. 将受信任URL指定为https://<ADFS-server-FQDN>/adfs/ls/?wa=wsignoutcleanup1.0
3. Click OK.

**Add an Endpoint** X

Endpoint type:  
SAML Logout

Binding:  
POST

Set the trusted URL as default

Index: 0

Trusted URL:  
`https://WIN-260MECJBIC2.jo123.local/adfs/ls/?wa=wsignoutcleanup.1.0`

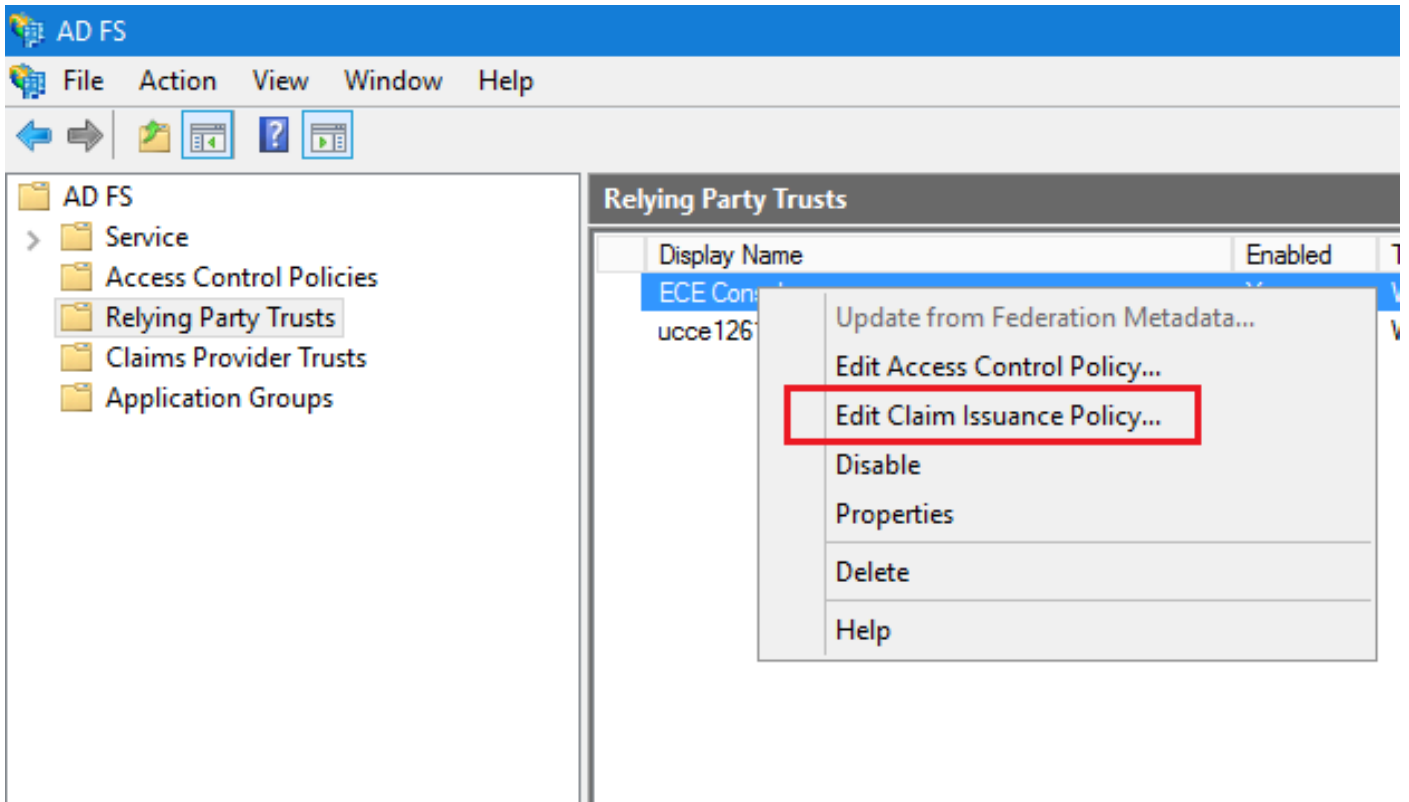
Example: `https://sts.contoso.com/adfs/ls`

Response URL:

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

### 步骤 7

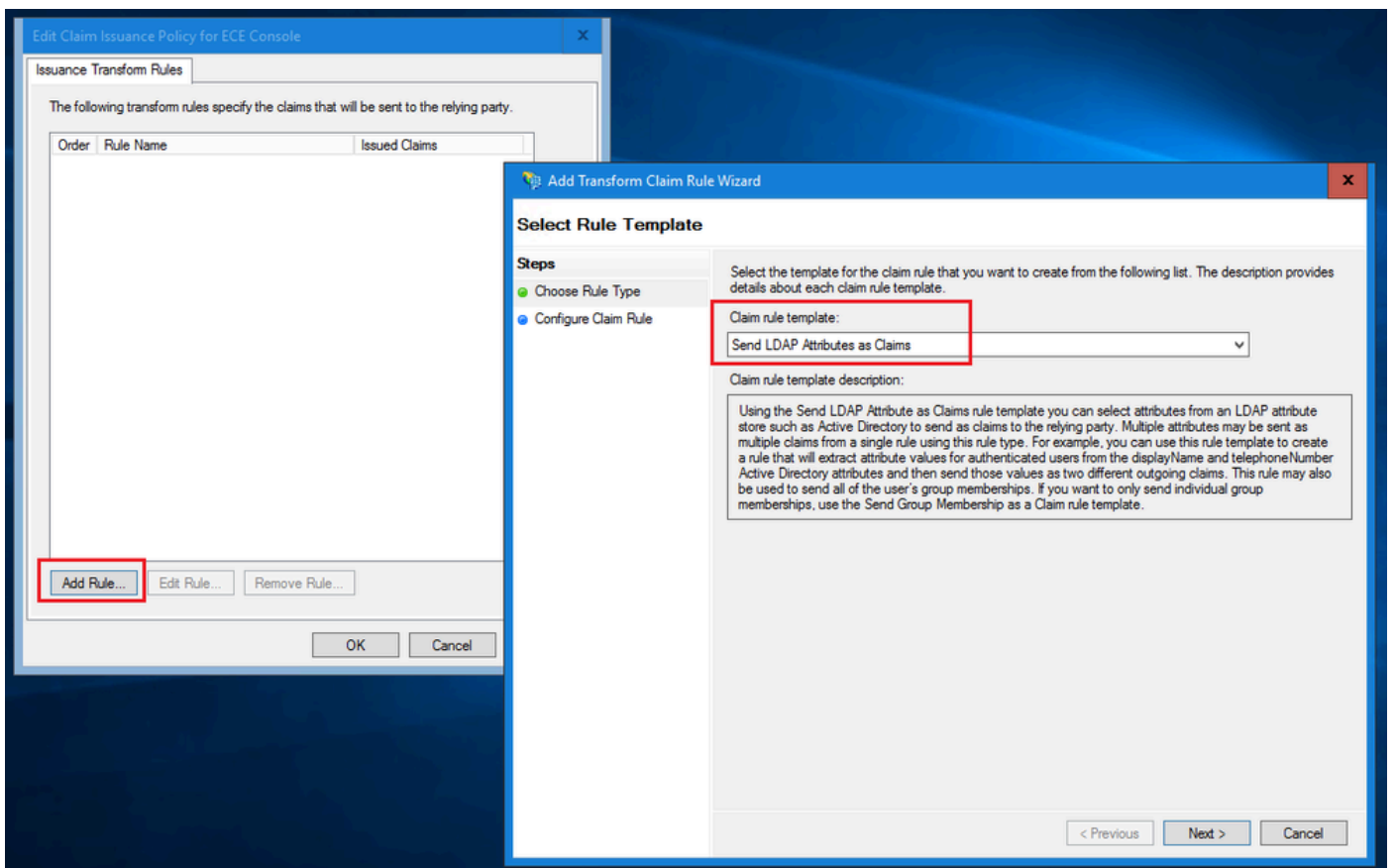
在“信赖提供商信任”列表中，选择为ECE创建的信任，并在“操作”部分中点击编辑索赔保险单。



## 步骤 8

在“Edit Claim Issuance Policy”窗口的“Issuance Transform Rules”选项卡下，单击Add Rule...按钮并进行如下配置：

a. 在“选择规则类型”页中，从下拉菜单中选择将LDAP属性作为声明发送，然后单击“下一步”。



b.在“配置声明规则”页中：

1. 提供声明规则名称并选择属性存储。
  2. 定义LDAP属性和传出声明类型的映射。
- 选择Name ID作为传出声明类型名称。
  - 点击Finish返回Edit Claim Insurance Policy窗口，然后点击OK。

**Add Transform Claim Rule Wizard** [Close]

### 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:  
Account name to Name ID

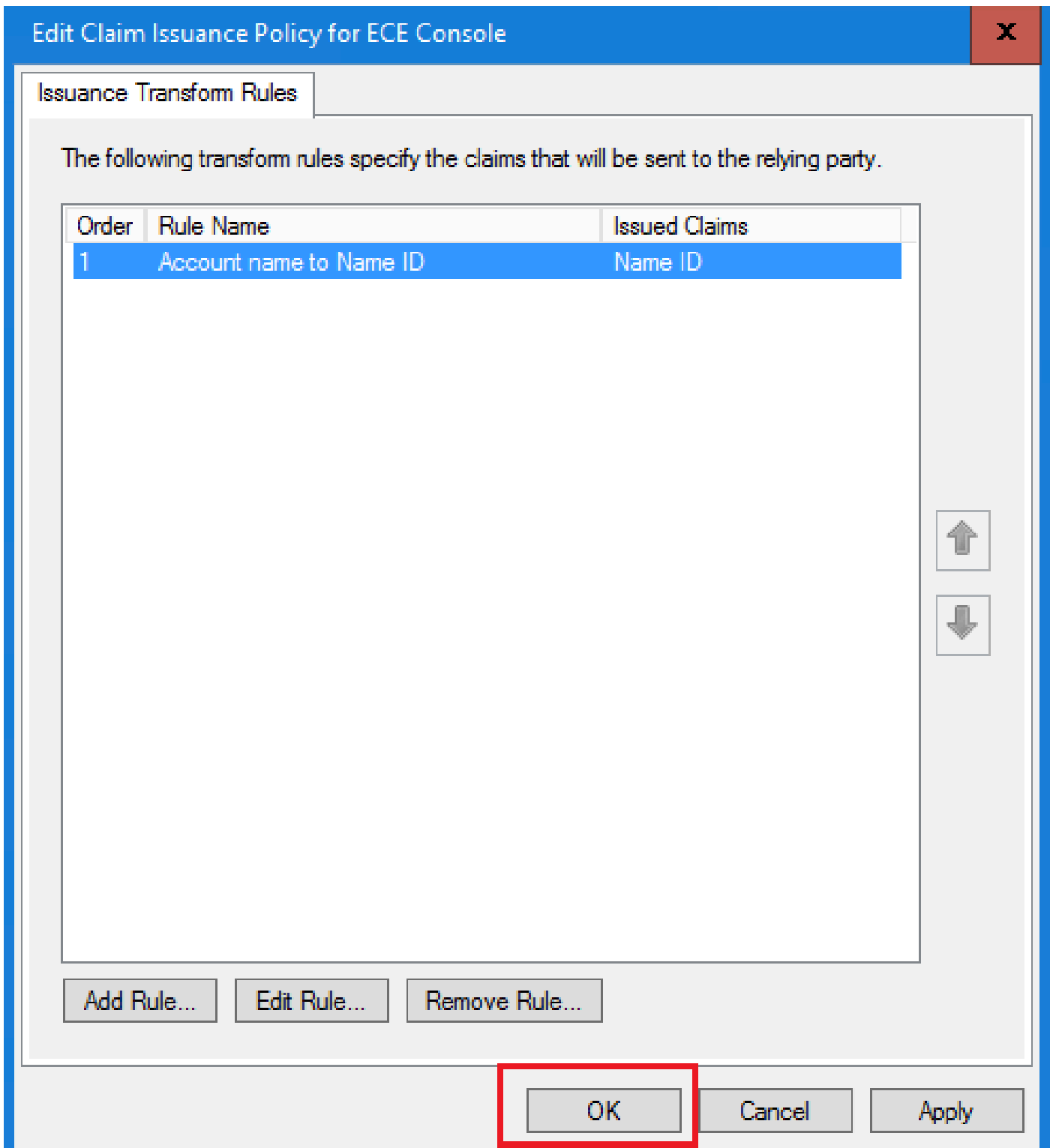
Rule template: Send LDAP Attributes as Claims

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
*		

< Previous   Finish   Cancel

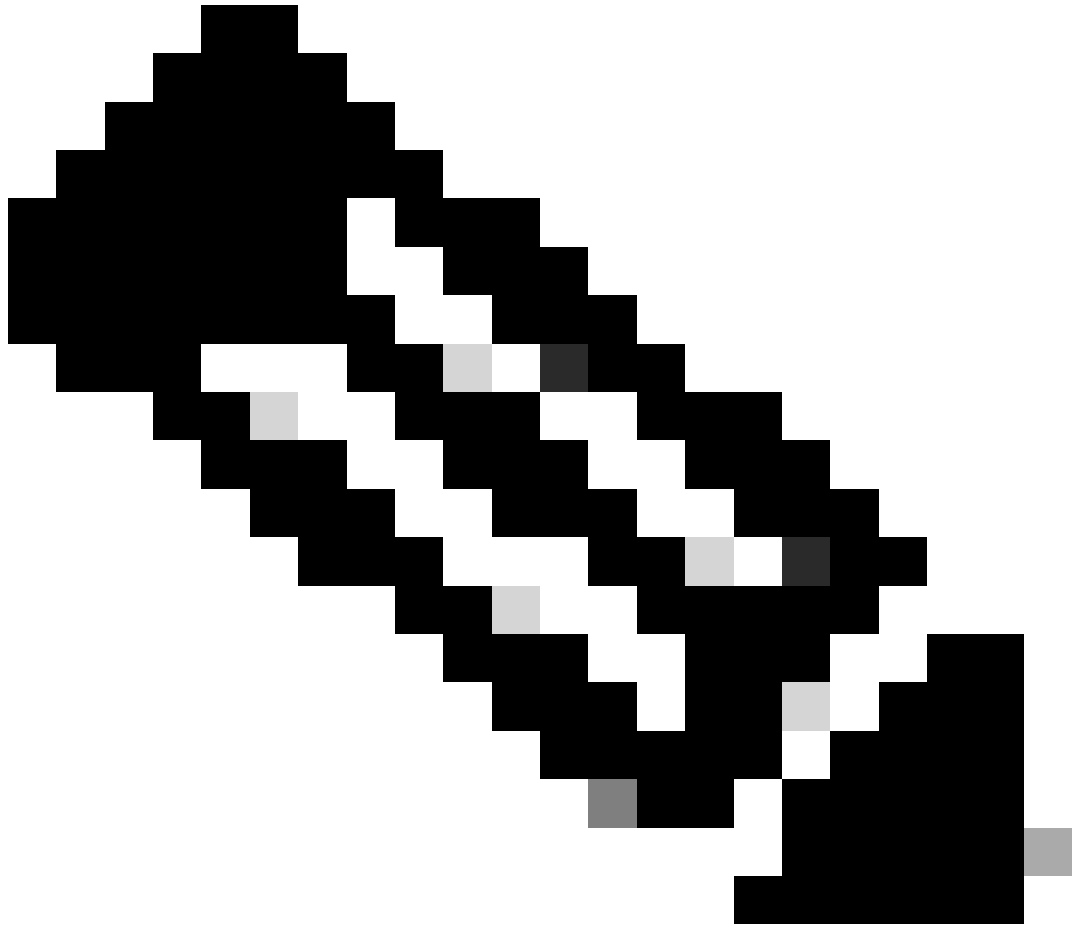


### 步骤 9

在Relying Provider Trusts列表中，双击您创建的ECE信赖方信任。

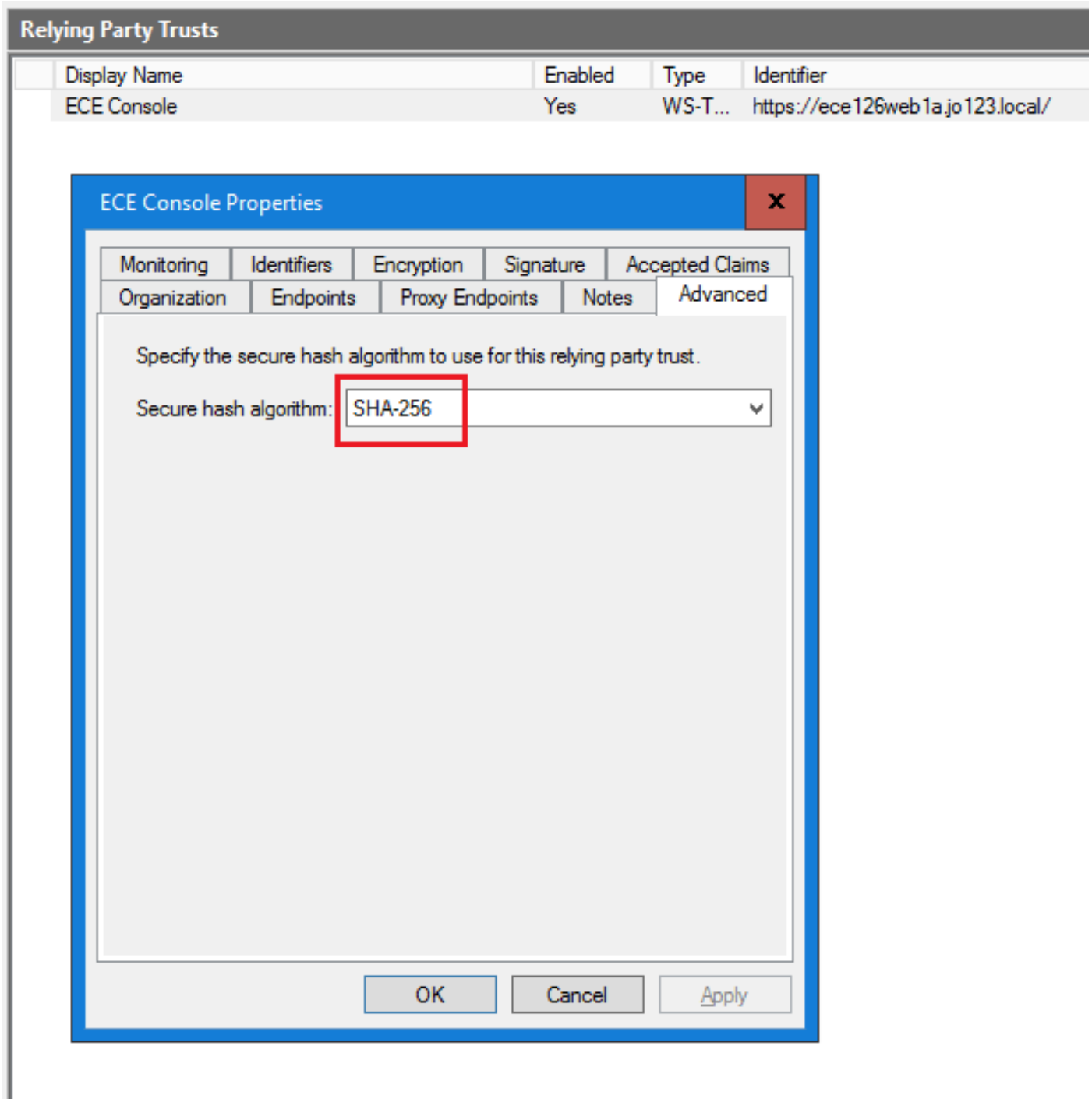
在打开的“属性”窗口中，转到“高级”选项卡，将“安全散列算法”设置为SHA-1或SHA-256。请单击“确定”关闭窗口。





注意：此值必须与ECE中“SSO配置”下的“服务提供商”设置的“签名算法”值匹配

---



## 步骤 10

验证并记下联合身份验证服务标识符值。

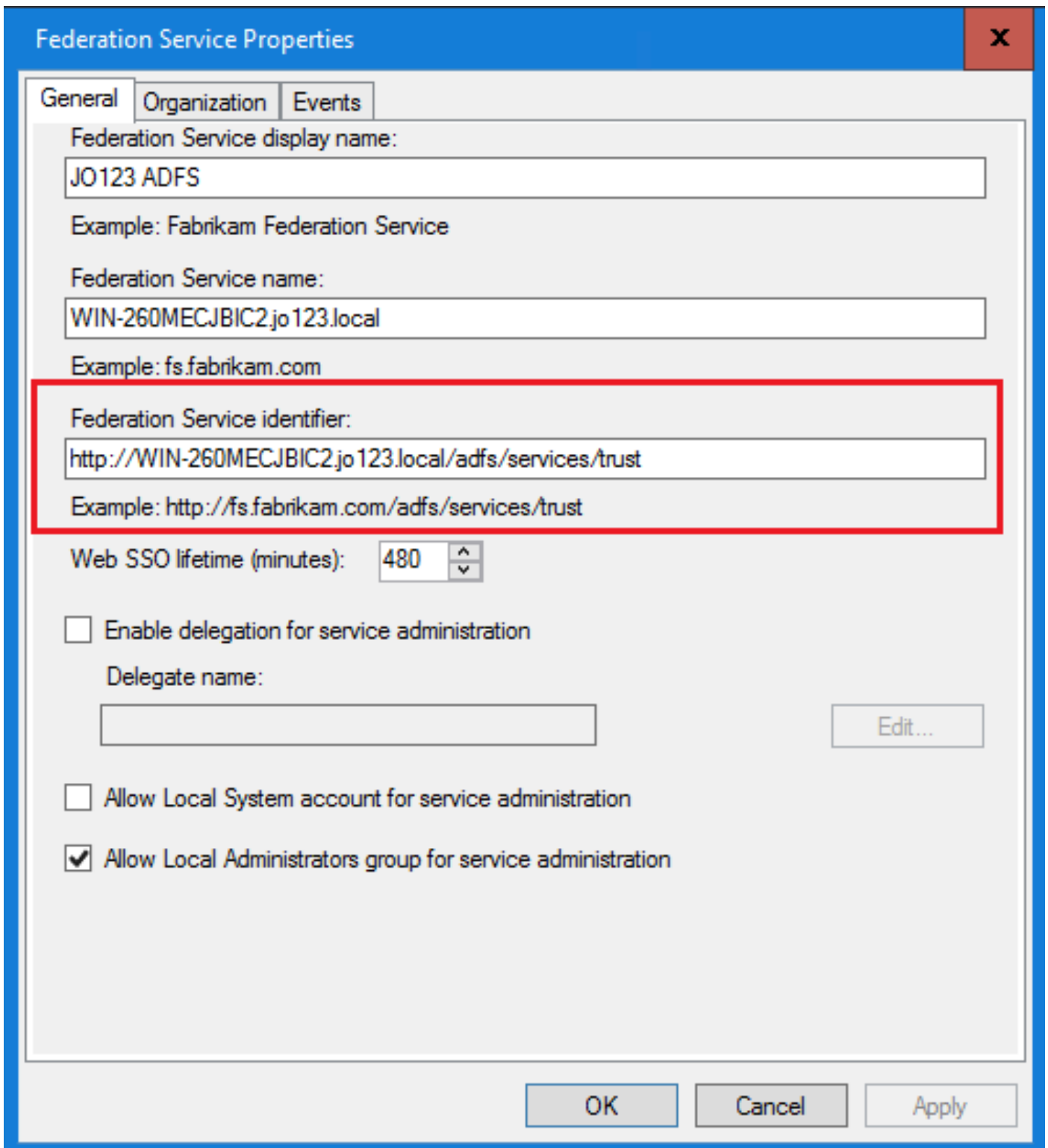
- 在AD FS管理控制台中，选择并右键单击AD FS >编辑联合身份验证服务属性>常规选项卡>联合身份验证服务标识符



注意：

- 必须完全按照在ECE中的SSO配置下为身份提供程序配置“实体ID”值的方式添加此值。
  - 使用http://并不意味着ADFS不安全，它只是一个标识符。
-

The screenshot shows the AD FS console interface. The top menu bar includes 'File', 'Action', 'View', 'Window', and 'Help'. The left-hand navigation pane shows a tree view with 'AD FS' selected. A context menu is open over the 'AD FS' node, with the option 'Edit Federation Service Properties...' highlighted by a red rectangular box. Other menu items include 'Add Relying Party Trust...', 'Add Claims Provider Trust...', 'Add Attribute Store...', 'Add Application Group...', 'Edit Published Claims', 'Revoke All Proxies', 'View', 'New Window from Here', 'Refresh', and 'Help'. The main content area displays a 'view' section with introductory text about Directory Federation Services and links for 'More About AD FS' and 'More About Azure Active Directory'. The right-hand 'Actions' pane lists the same menu items as the context menu. At the bottom of the console, a status bar displays the text 'Edit the federation service properties'.



## 配置身份提供程序

### 步骤 11

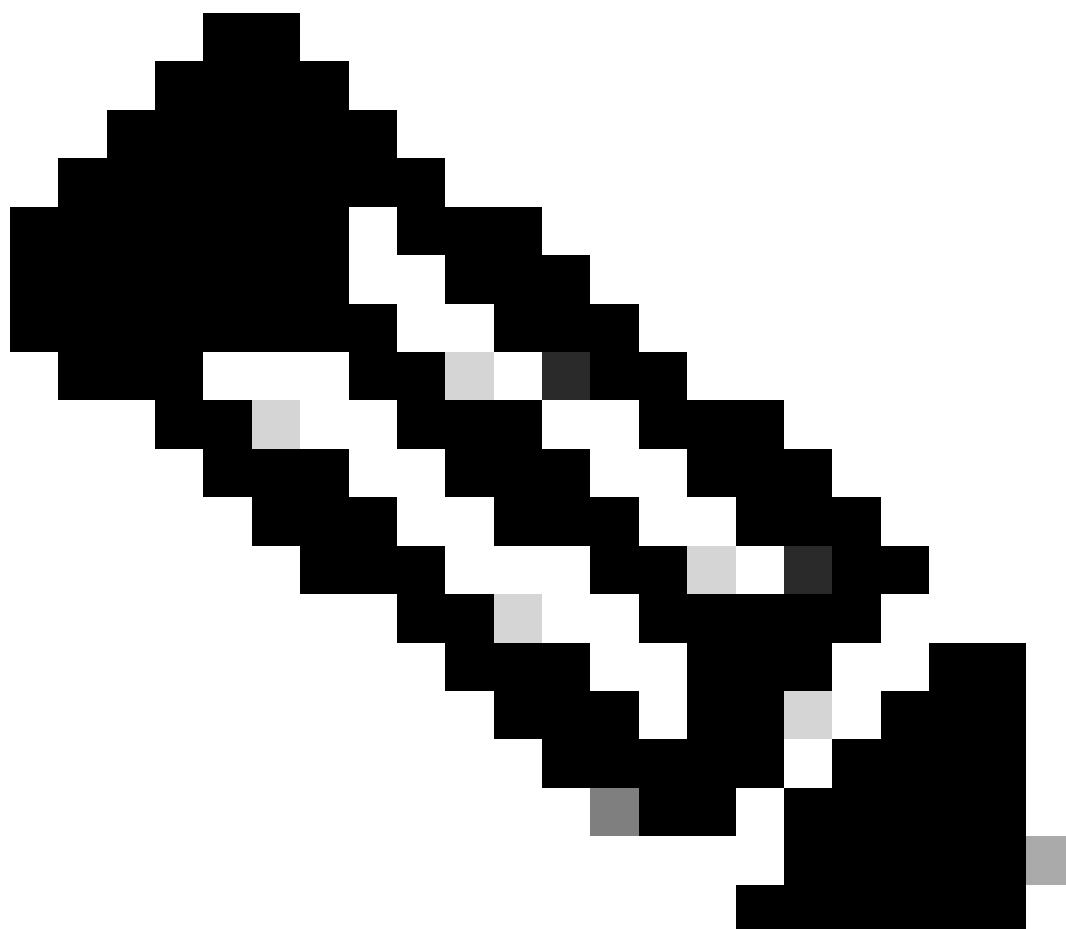
配置SSO需要Java密钥库(JKS)证书，以允许具有管理员或主管角色的用户使用其SSO登录凭证登录到Finesse外部的ECE分区。

如果要将SSO配置为允许具有管理员或主管角色的用户使用其SSO登录凭证登录到Finesse外部的ECE分区，则必须将Java密钥库(JKS)证书转换为公钥证书，并在为ECE在IdP服务器上创建的信赖

方信任中对其进行配置。

请咨询您的IT部门以接收JKS证书。

---



注意：这些步骤适用于使用ADFS作为身份提供程序的系统。其他身份提供程序可以使用不同的方法来配置公钥证书。

---

以下示例展示了如何在实验中生成JKS文件：

a.生成JKS：

```
keytool -genkey -keyalg RSA -alias ece126web1a_saml -keystore C:\Temp\ece126web1a_saml.jks -keysize 2048
```

---

注意：此处输入的密钥库密码、别名和密钥密码用于在ECE的“SSO配置”下配置“服务提供商”配置。

```
C:\Users\administrator.J0123>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.导出证书：

此keytool命令将file name为ece126web1a\_saml.crt的.crt格式的证书文件导出到C:\Temp目录中。

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

## 步骤 12

### 配置身份提供程序

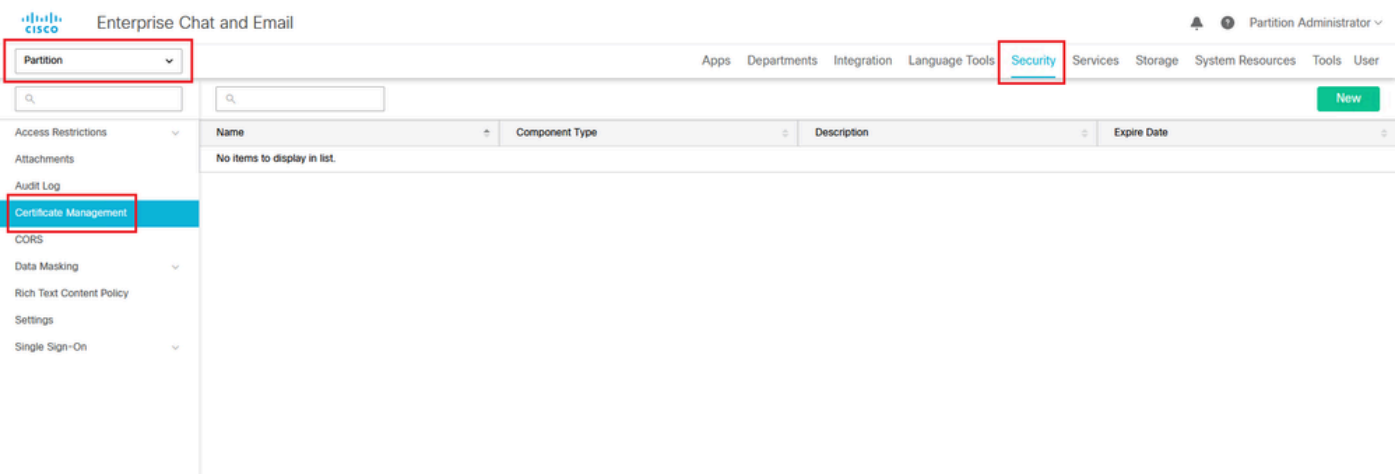
1. 在AD FS管理控制台上，选择并右键单击为ECE创建的信赖方信任。
2. 打开信任的“属性”窗口，然后在“签名”选项卡下单击“添加”按钮。
3. 添加公共证书（在上一步中生成的.crt文件），然后单击OK。

## 创建和导入证书

### 步骤 13

在将SSO配置为使用Cisco IDS进行代理的单点登录之前，必须将Cisco IdS服务器的Tomcat证书导入到应用中。

a.在ECE管理控制台的分区级菜单下，单击Security选项，然后从左侧菜单中选择Certificate Management。



b.在证书管理空间中，单击“新建”按钮并输入相应的详细信息：

- Name：键入证书的名称。
- Description：为证书添加说明。
- Component Type：选择CISCO IDS。
- 导入证书(Import Certificate)：要导入证书，请点击搜索和添加(Search and Add)按钮并输入请求的详细信息：
- 证书文件(Certificate file)：点击浏览(Browse)按钮并选择您要导入的证书。只能以.pem、.der (BINARY)或.cer/cert格式导入证书。
- Alias Name：为您的证书提供别名。

c.单击“保存”



Partition ▼

### Create Certificate

- Access Restrictions ▼
- Attachments
- Audit Log
- Certificate Management
- CORS
- Data Masking ▼
- Rich Text Content Policy
- Settings
- Single Sign-On ▼

**Name\***

**Description**

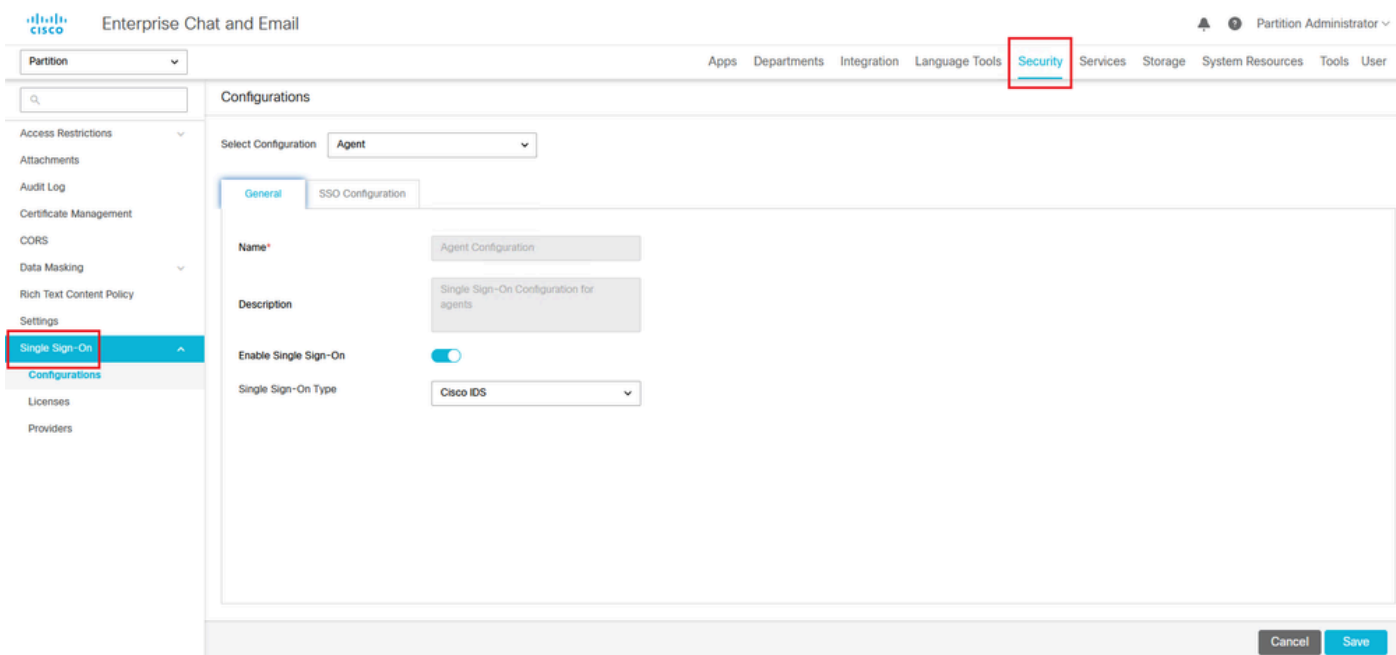
**Component Type\***  ▼

**Import Certificate**  +

## 配置代理单一登录

### 步骤 14

1. 在ECE管理控制台的分区级菜单下，单击“Security”选项，然后从左侧菜单中选择Single Sign-On > Configurations。
2. 在Select Configuration下拉列表中，选择Agent并在General选项卡下设置配置：
  - 启用单点登录：点击切换按钮以启用SSO。
  - Single Sign-On Type：选择Cisco IDS。



## 步骤 15

点击SSO配置选项卡并提供配置详细信息：

### a. OpenID Connect提供程序

#### 主要用户信息终端URL

- 主Cisco IDS服务器的用户信息终端URL。
- 此URL验证用户令牌/用户信息API。
- 其格式为：<https://cisco-ids-1:8553/ids/v1/oauth/userinfo>，其中cisco-ids-1表示主Cisco IDS服务器的完全限定域名(FQDN)。

#### 用户身份声明名称

- 由用户信息终端URL返回的声明的名称，用于标识统一或打包CCE中的用户名。
- Unified或Packaged CCE中的声明名称和用户名必须匹配。
- 这是响应承载令牌验证获得的声明之一。
- 如果Unified或Packaged CCE中代理的用户名与User Principal Name匹配，请提供“upn”作为User Identity Claim name字段的值。
- 如果Unified或Packaged CCE中代理的用户名与SAM帐户名称匹配，请提供“sub”作为User Identity Claim name字段的值。

#### 辅助用户信息终端URL (Secondary User Info Endpoint URL)

- Cisco IDS服务器的辅助用户Info Endpoint URL。
- 其格式为：<https://cisco-ids-2:8553/ids/v1/oauth/userinfo>，其中cisco-ids-2表示辅助Cisco IDS服务器的完全限定域名(FQDN)。

#### 用户信息终端URL方法

- ECE用于对用户信息终端URL进行承载令牌验证调用的HTTP方法。

- 从显示的选项列表中选择POST（此处选择POST以匹配IDS服务器的方法）。

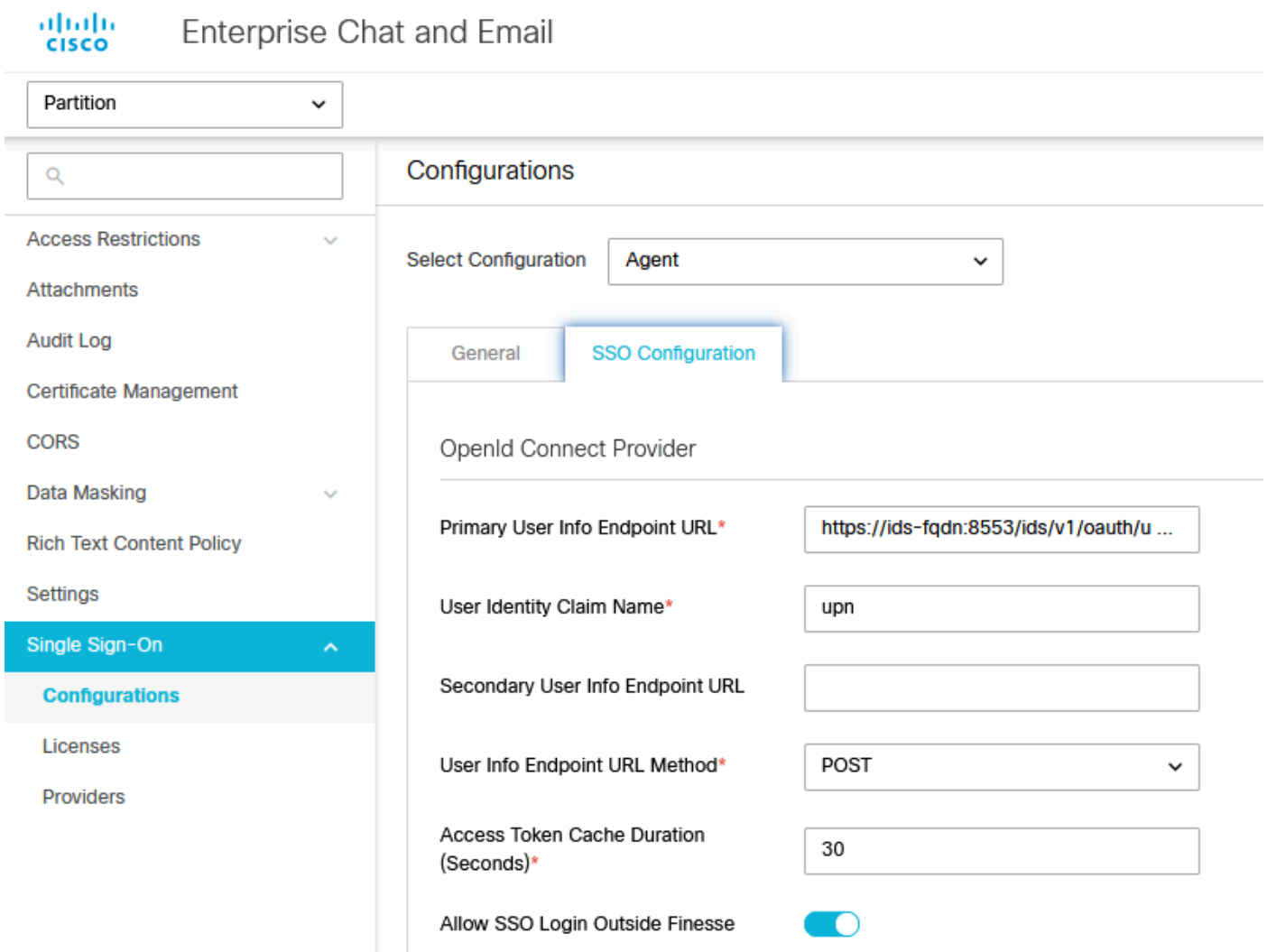
POST：用于发送数据到指定终端上的Cisco IDS服务器的方法。

访问令牌缓存持续时间（秒）

- 必须在ECE中缓存承载令牌的持续时间（秒）。
- 验证调用成功的承载令牌仅存储在缓存中。（最小值：1；最大值：30）

允许SSO在Finesse外部登录

- 如果您希望允许具有管理员或主管角色的用户使用其SSO登录凭证登录Finesse外部的ECE分区，请单击此切换按钮。
- 如果启用，则必须提供“身份提供程序”和“服务提供程序”部分下的信息。
- 这要求您的IdP配置允许共享IdP服务器。



**Enterprise Chat and Email**

Partition

Configurations

Select Configuration: Agent

General | **SSO Configuration**

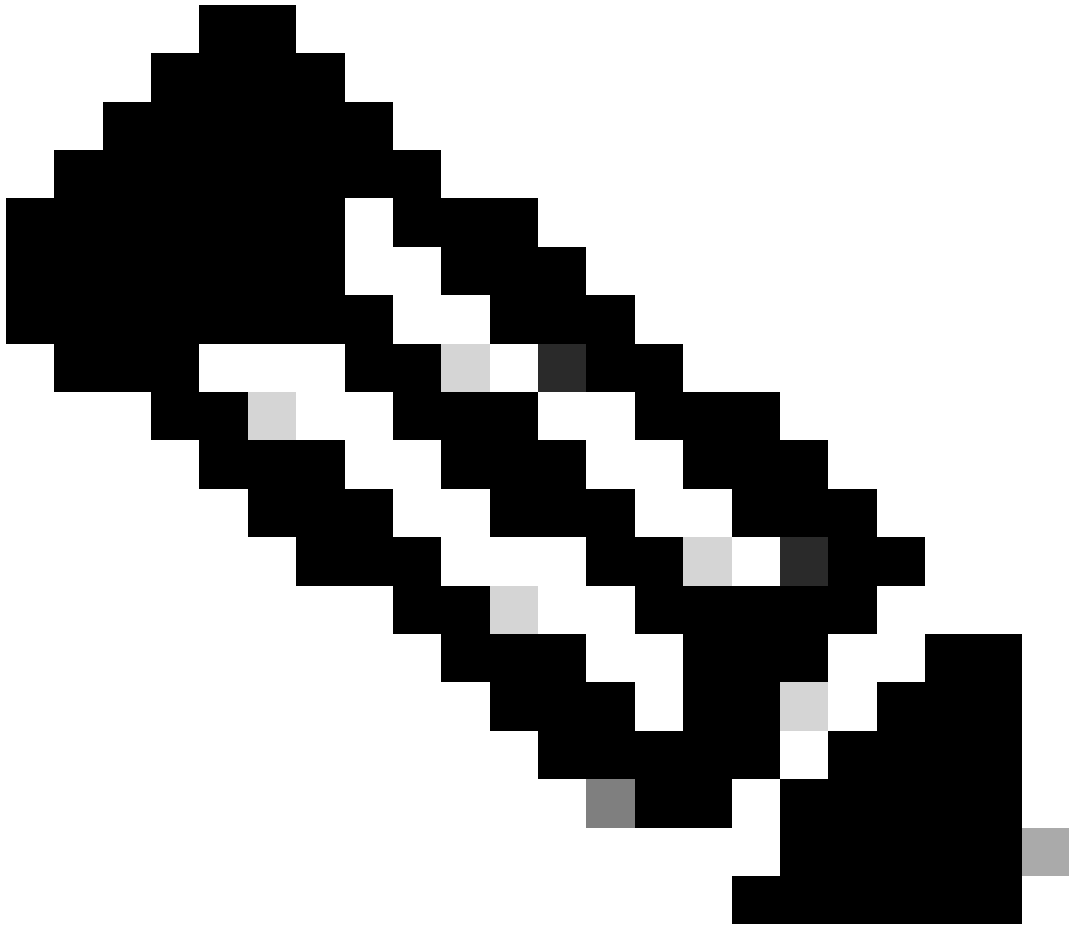
OpenId Connect Provider

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	<input checked="" type="checkbox"/>

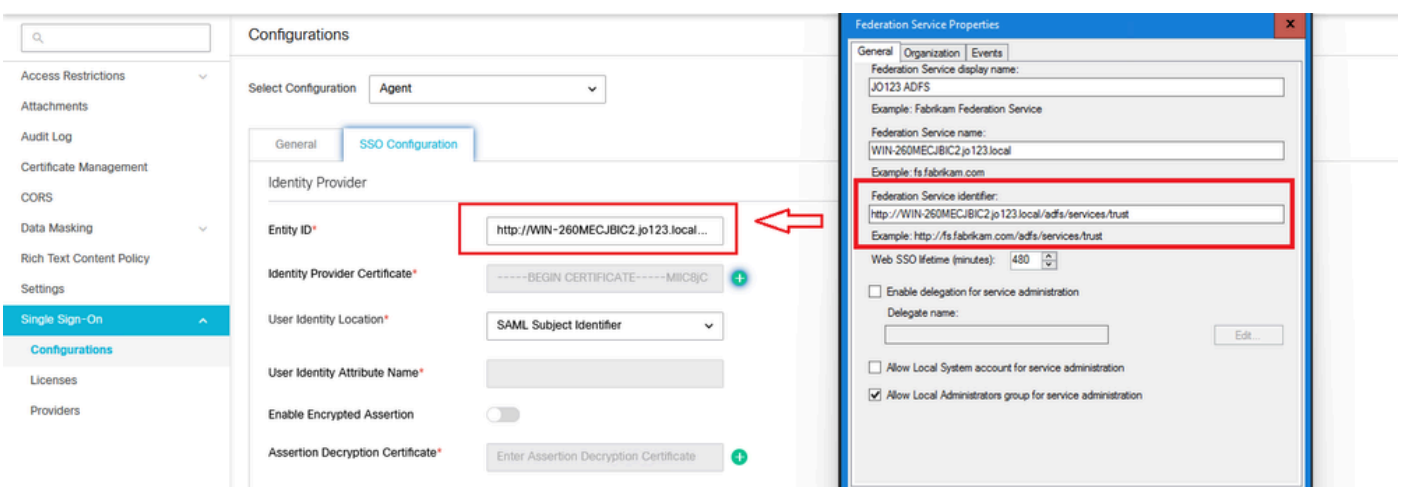
## b. 身份提供者

实体Id

- IdP服务器的实体ID。



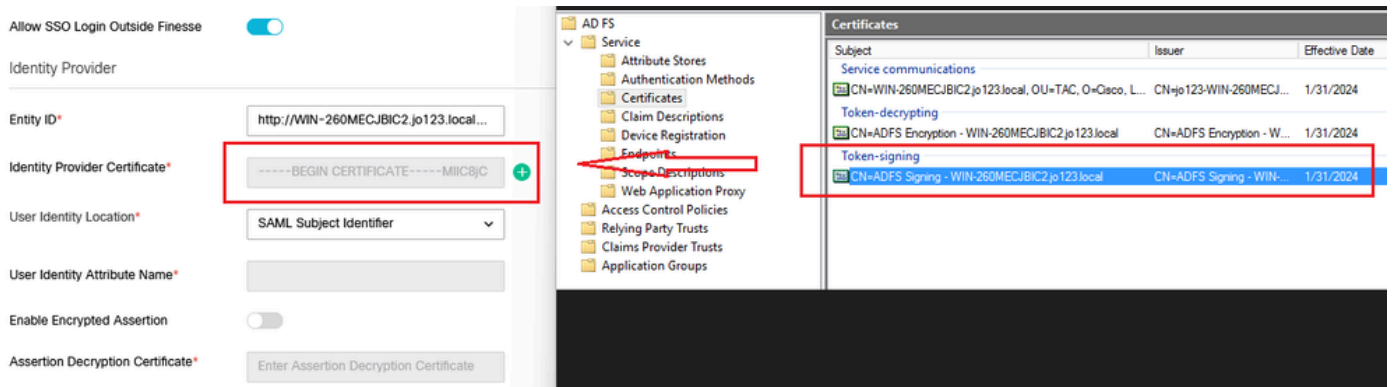
注意：此值必须与AD FS管理控制台中的“联合身份验证服务标识符”值完全匹配。



## 身份提供程序证书

- 公钥证书。

- 证书必须以“-----BEGIN CERTIFICATE-----”开头，以“-----END CERTIFICATE-----”结尾
- 这是位于AD FS管理控制台>服务>证书>令牌签名中的令牌签名证书。



## 用户身份位置

- 选择SAML Subject Identifier，将证书中的标识位置设置为默认SAML主题标识符，如SAML断言中的主题，如<saml: Subject>中的用户名。
- 选择SAML Attribute以将身份位置分配给证书中的特定属性，例如email.address。在User Identity Attribute Name字段中提供属性。

## 用户身份属性名称

- 仅当User ID Location值是SAML属性时适用。
- 这可以在SAML断言中调整，并用于为用户身份验证选择其他属性，例如邮件地址。
- 它还可以用于创建具有SAML属性的新用户。
- 例如，如果通过email.address属性中提供的值识别用户，并且提供的电子邮件地址值与系统中的任何用户都不匹配，则会使用提供的SAML属性创建新用户。

## 启用加密断言（可选）

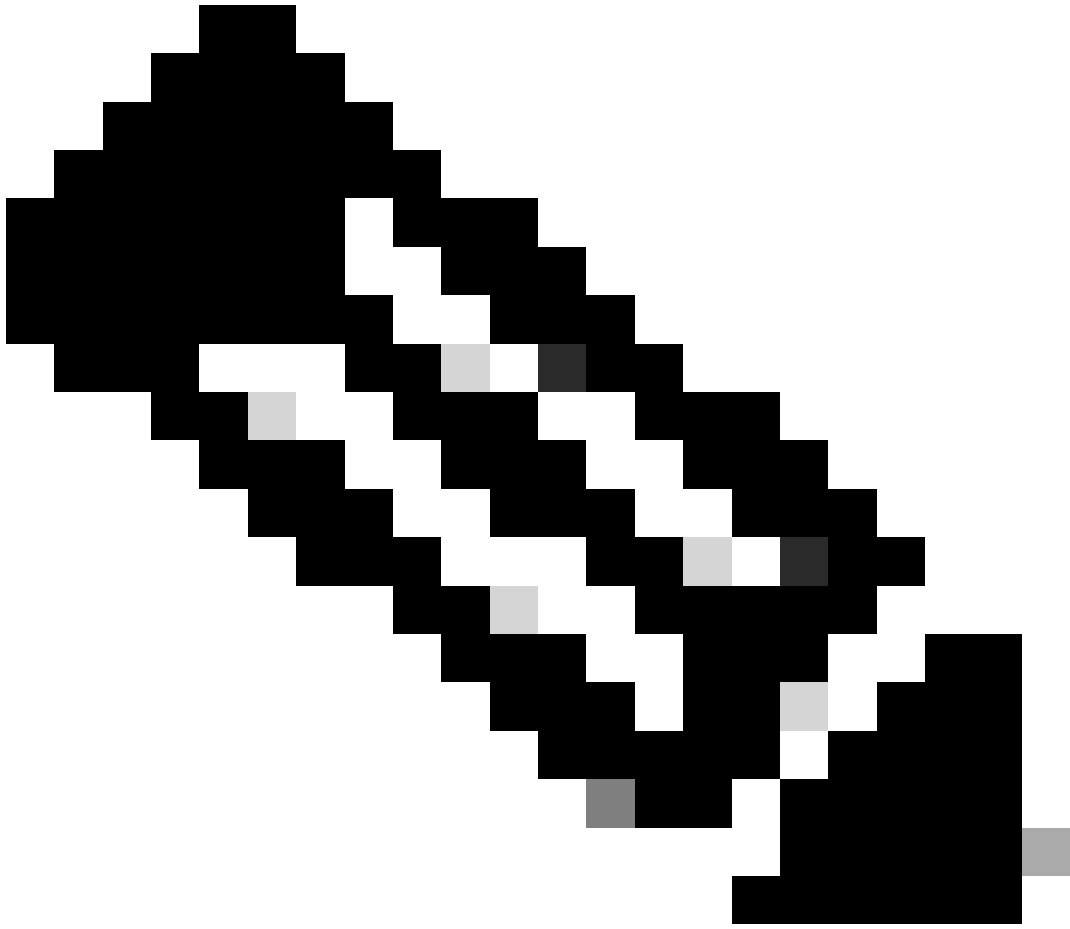
- 如果您希望通过身份提供者控制台登录启用加密断言，请点击Toggle按钮将值设置为Enabled。
- 否则，将该值设置为Disabled。

## 断言解密证书

如果Enable encrypted assertion设置为Enabled，请点击Search and Add按钮，并确认您更改证书的选择。

在Assertion Decryption Certificate窗口中提供详细信息：

- Java Keystore File：提供Java Keystore File的文件路径。此文件为.jks格式，包含系统访问由身份提供程序保护的证书所需的解密密钥。
- Alias Name：解密密钥的唯一标识符。
- 密钥库密码：访问Java密钥库文件所需的密码。
- 密钥密码：访问别名的解密密钥所需的密码。



注意：这需要与AD FS管理控制台上已配置的ECE信赖方信任的“加密”选项卡中的证书匹配。

---

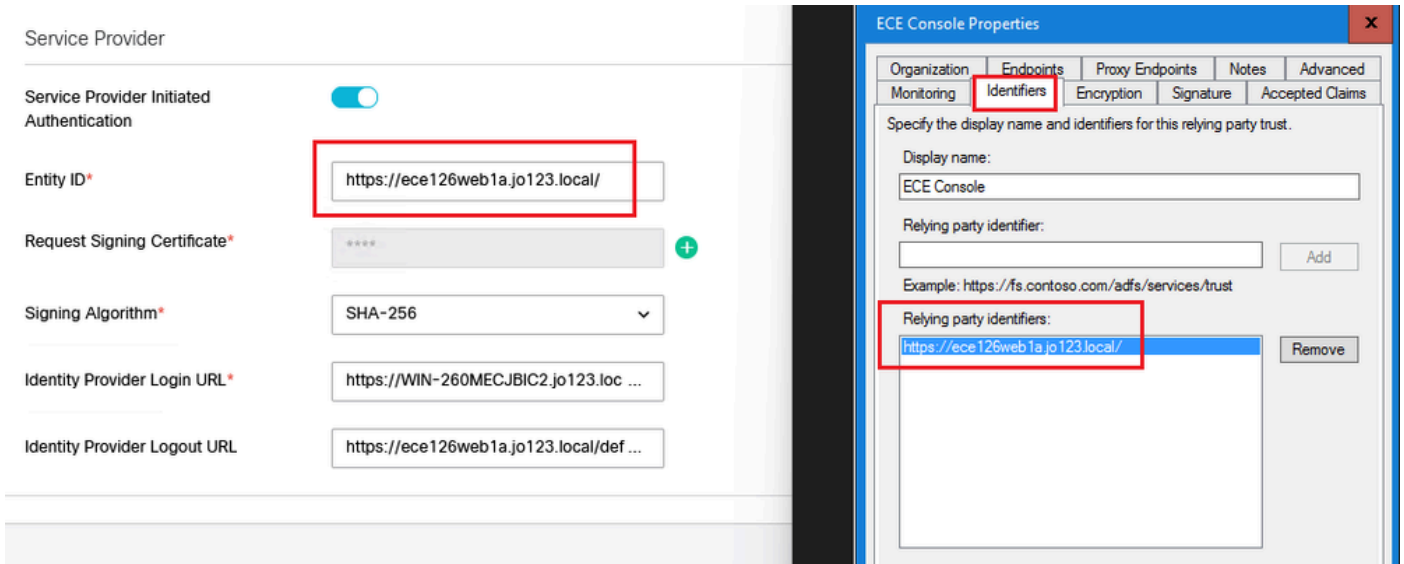
### c. 服务提供商

服务提供商发起的身份验证

- 将切换按钮设置为“启用”。

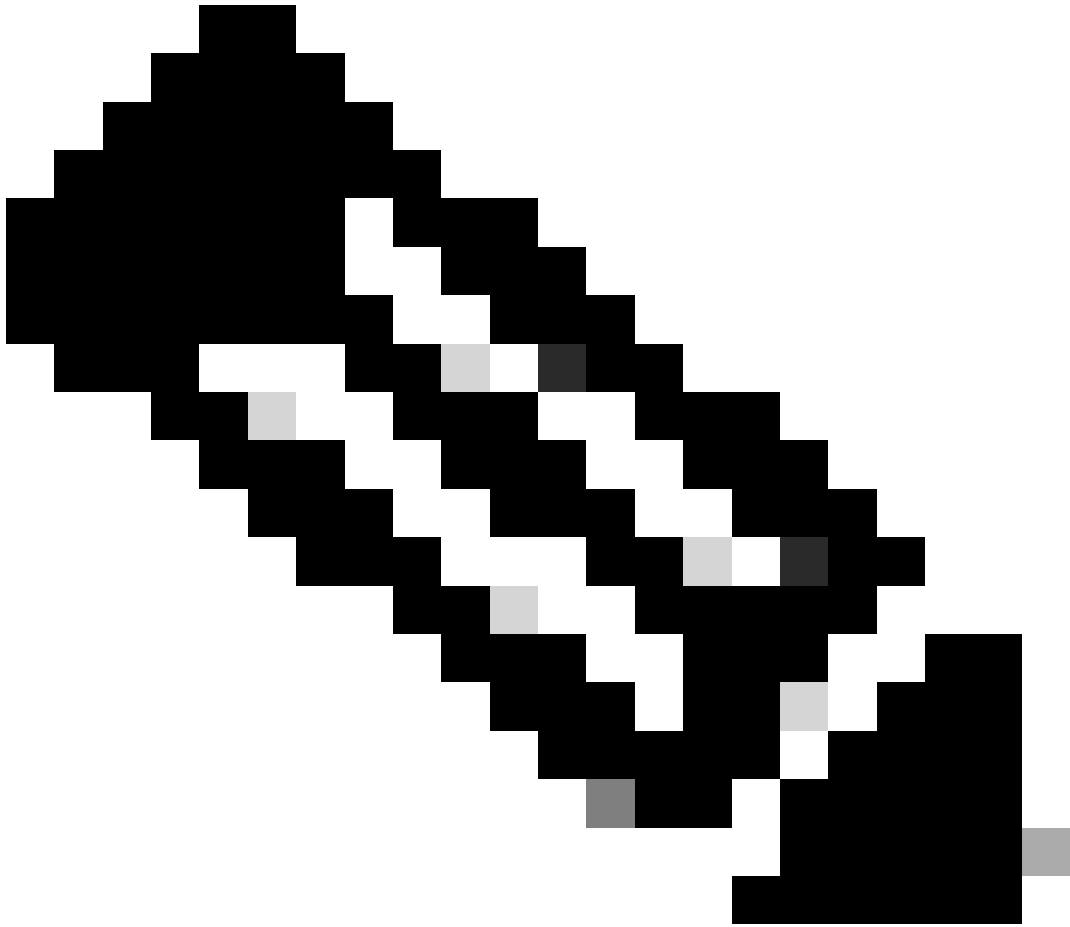
实体Id

- 提供ECE应用程序的外部URL。



## 请求签名证书

- 需要Java密钥库(JKS)证书才能提供必要的信息。
- 使用步骤11中生成的别名和密钥库/密钥密码上传.jks文件。



注意：这必须与上传到AD FS管理控制台上已配置的ECE信赖方信任的“签名”选项卡的证书匹配。

Service Provider

Service Provider Initiated Authentication

Entity ID\*

Request Signing Certificate\*  +

Signing Algorithm\*

Identity Provider Login URL\*

Identity Provider Logout URL

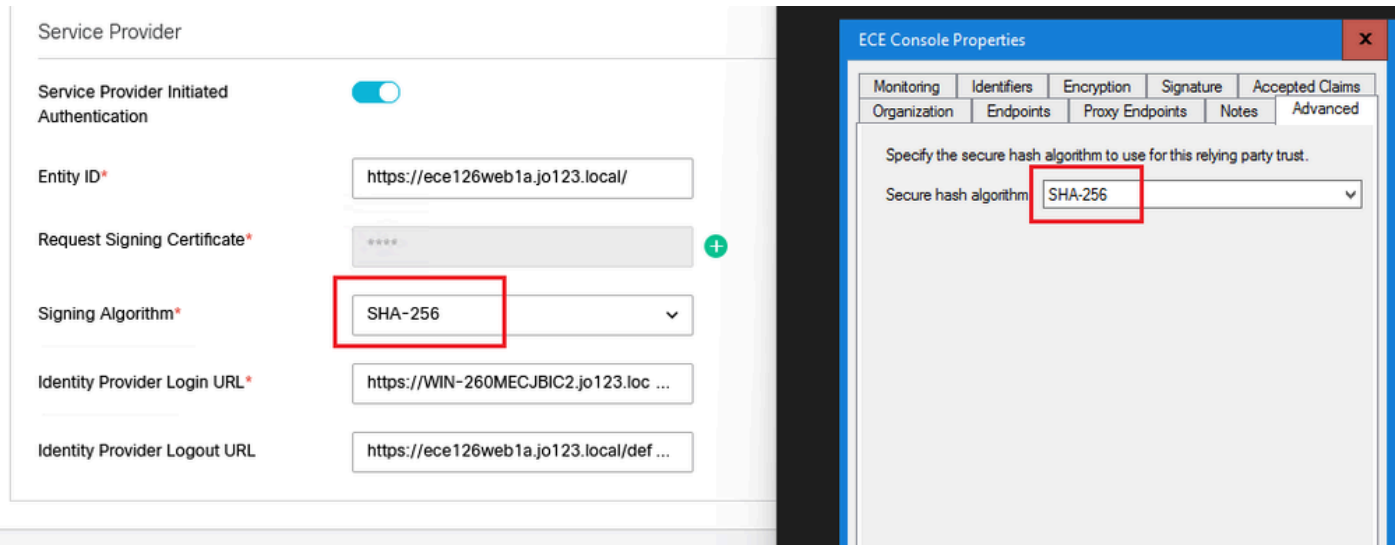
ECE Console Properties

Organization	Endpoints	Proxy Endpoints	Notes	Advanced
Monitoring	Identifiers	Encryption	Signature	Accepted Claims
Specify the signature verification certificates for requests from this relying party.				
Subject	Issuer	Effective Date	Expiration	
CN=ece126a...	CN=ece126app...	1/31/2024 2:21:...	1/29/21...	

签名算法



- 设置服务提供商的签名算法。
- 如果使用ADFS，该值必须与“高级”选项卡下为ECE创建的信赖方信任中选择的算法匹配。



### 标识提供程序登录URL

- SAML身份验证的URL。
- 例如，对于ADFS，应为 <http://<ADFS>/adfs/ls>。

### 标识提供程序注销URL

- 注销时将用户重定向到的URL。这是可选的，可以是任何URL。
- 例如，在SSO注销后，可以将代理重定向到 <https://www.cisco.com> 或任何其他URL。

### 步骤 16

点击保存

### 在分区设置中设置Web服务器/LB URL

### 步骤 17

确保在“Partition settings”下输入正确的Web Server/LB URL >选择Apps选项卡，然后导航到 General Settings > External URL of the Application



Partition  Apps Departments Integration

General Settings

Chat & Messaging

Email

**General Settings**

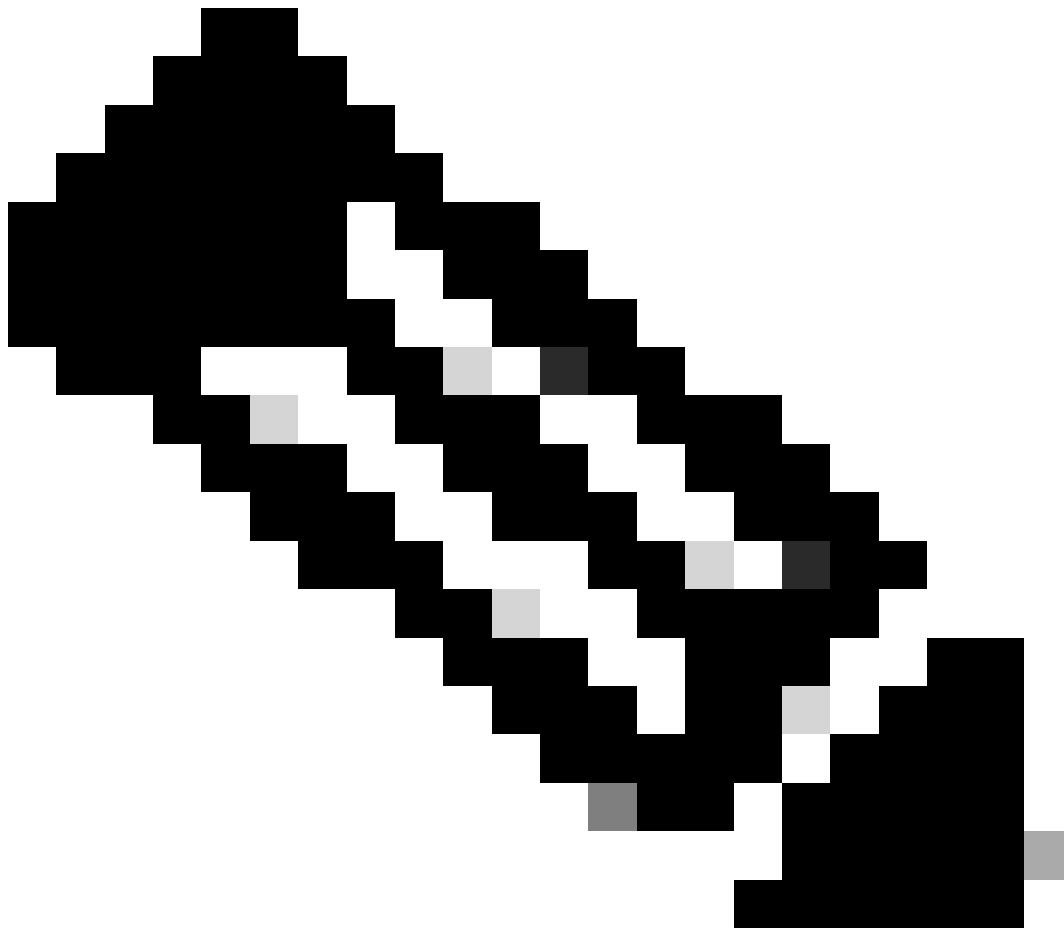
Knowledge

External URL of Application   
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   
10 - 500. Default value is 100

Maximum number of records to display for NAS search   
1 - 100. Default value is 9

## 为分区管理员配置SSO



---

注意：

- 此步骤仅适用于PCCE。
- 这是用于在CCE管理网络界面<https://cceadmin>中访问的ECE小工具。

---

## 步骤 18

### 为分区管理员配置SSO

1. 在ECE管理控制台的分区级菜单下，点击Security选项，然后从左侧菜单中选择Single Sign-On > Configurations。
2. 在选择配置下拉列表中，选择分区管理员，然后输入配置详细信息：

#### LDAP URL

- LDAP服务器的URL。
- 这可以是LDAP服务器的域控制器URL(例如，`ldap://LDAP_server:389`)或全局目录URL(例如，`ldap://LDAP_server:3268`)。
- 如果ECE配置了LDAP查找，则通过CCE管理控制台访问ECE时，可以自动将分区添加到系统中。
- 但是，在单个林中具有多个域或配置了备用UPN的Active Directory部署中，不得使用具有标准LDAP端口389和636的域控制器URL。
- LDAP集成可以配置为使用端口3268和3269的全局目录URL。

---

注意：最佳做法是使用全局目录URL。如果不使用GC，则ApplicationServer日志中的错误如下。

- LDAP身份验证中发生异常<@>  
javax.naming.PartialResultException：未处理的连续引用；剩余名称  
“DC=example，DC=com”

---

## DN属性

- 包含用户登录名的DN的属性。
- 例如，userPrincipalName。

## 基础

- 为Base指定的值由应用程序用作搜索库。
- Search base是在LDAP目录树中搜索的开始位置。
- 例如，DC=mycompany，DC=com。

## 用于LDAP搜索的DN

- 如果LDAP系统不允许匿名绑定，请提供在LDAP目录树上具有搜索权限的用户的可分辨名称(DN)。
- 如果LDAP服务器允许匿名绑定，请将此字段留空。

## 密码

- 如果LDAP系统不允许匿名绑定，请提供在LDAP目录树上具有搜索权限的用户的密码。
- 如果LDAP服务器允许匿名绑定，请将此字段留空。

## 步骤 19

### 点击保存

现在即可完成ECE中代理和分区管理员的单点登录配置。

## 故障排除

### 设置跟踪级别

1. 在ECE管理控制台的分区级菜单下，单击System Resources选项，然后从左侧菜单中选择Process Logs。
2. 从进程列表中选择ApplicationServer进程>从“Maximum Trace Level”下拉菜单设置所需的跟踪级别。



注意：

- 要排除初始设置或重新配置期间的SSO登录错误，请将ApplicationServer进程跟踪设置为级别7。
  - 重现错误后，请将跟踪级别重新设置为默认级别4，以避免覆盖日志。
-

Enterprise Chat and Email

Partition Administrator

Partition

Apps Departments Integration Language Tools Security Services Storage System Resources Tools User

Process Logs

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

Enterprise Chat and Email

Partition

Edit Process Log: ece126app1a:ApplicationServer

Process Logs

General Advanced Logging

Name ece126app1a:ApplicationServer

Description ece126app1a:ApplicationServer

Maximum Trace Level 4 - Info

Log File Name

Maximum File Size

Extensive Logging Duration 4 - Info

Extensive Logging End Time

## 故障排除场景1

Error

- 错误代码：500
- 错误说明：应用程序此时无法登录用户，因为身份提供程序登录失败。

## 日志分析

- IdP登录失败- <samlp : Status><samlp : StatusCode Value="urn : oasis : names : tc : SAML : 2.0 : status : Responder" /></samlp : Status>
- 此处，状态“Responder”表示AD FS端存在一些问题-在这种情况下，主要是通过ECE管理控制台（SSO配置>服务提供商）上传的“请求签名证书”，以及通过“签名”选项卡上传到ECE信赖方信任的证书。
- 这是使用Java密钥库文件生成的证书。

## 应用服务器日志-跟踪级别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_Handler.java:100)
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Handler.java:100)
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Handler.java:100)
at com.egain.platform.module.security.sso.handler.OpenIDConnect_Handler.validateReqWithAttributes(OpenIDConnect_Handler.java:100)
at com.egain.platform.module.security.sso.admin.SSOAdministrator.validateRequestWithAttributes(SSOAdministrator.java:100)
at com.egain.platform.module.security.sso.controller.SSOControllerServlet.doPost(SSOControllerServlet.java:100)
.
.
.
.
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 Provider is not available.
```

```
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:
```

## 分辨率

- 请参阅“配置代理单一登录-服务提供商”部分中的请求签名证书配置。
- 确保将步骤11中生成的Java Keystore .jks文件上传到ECE管理控制台上的“Request Signing certificate”字段，该字段位于“SSO Configuration”>“Select Configuration 'Agent'”>“SSO Configuration”选项卡>“Service Provider”>“Request Signing certificate”下。
- 确保在ECE信赖方信任的“签名”(Signature)选项卡下上传.crt文件(第12步)。



## 故障排除场景2

### Error

- 错误代码：400
- 错误说明：SAML响应令牌无效：签名验证失败。

### 日志分析

- 此错误表明ADFS上的“令牌签名证书”和ECE SSO配置上的“身份提供程序证书”之间的证书不匹配。

### 应用服务器日志-跟踪级别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:
```

### 分辨率

- 日志代码片段中看到的错误“无法解析证书：java.io.IOException：数据不完整”表明“身份提供程序证书”内容未正确输入
- 要解决此问题：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。

- 请参阅“配置代理单一登录-身份提供程序”部分中的“身份提供程序证书”配置(步骤15)。

## 故障排除场景3

### Error

- 错误代码：401-114
- 错误说明：在SAML属性中找不到用户身份。

### 日志分析

应用服务器日志-跟踪级别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_Handler.java:100)
    at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.unmarshallAndValidateResponse(SAML2_0_Handler.java:115)
    at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Handler.java:130)
    at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Handler.java:145)
    at com.egain.platform.module.security.sso.handler.OpenIDConnect_Handler.validateReqWithAttributes(OpenIDConnect_Handler.java:100)
    at com.egain.platform.module.security.sso.admin.SSOAdministrator.validateRequestWithAttributes(SSOAdministrator.java:100)
    at com.egain.platform.module.security.sso.controller.SSOControllerServlet.doPost(SSOControllerServlet.java:100)
    at javax.servlet.http.HttpServlet.doPost(HttpServlet.java:156)
    at org.apache.catalina.core.StandardWrapper.doPost(StandardWrapper.java:165)
    at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:369)
    at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:103)
    at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:146)
    at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:93)
    at org.apache.catalina.valves.AccessLogValve.invoke(AccessLogValve.java:559)
    at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:327)
    at org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:908)
    at org.apache.coyote.AbstractProtocol.handleAbstract(AbstractProtocol.java:899)
    at org.apache.coyote.http11.Http11Protocol.handle(Http11Protocol.java:57)
    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 <@>
```

### 分辨率

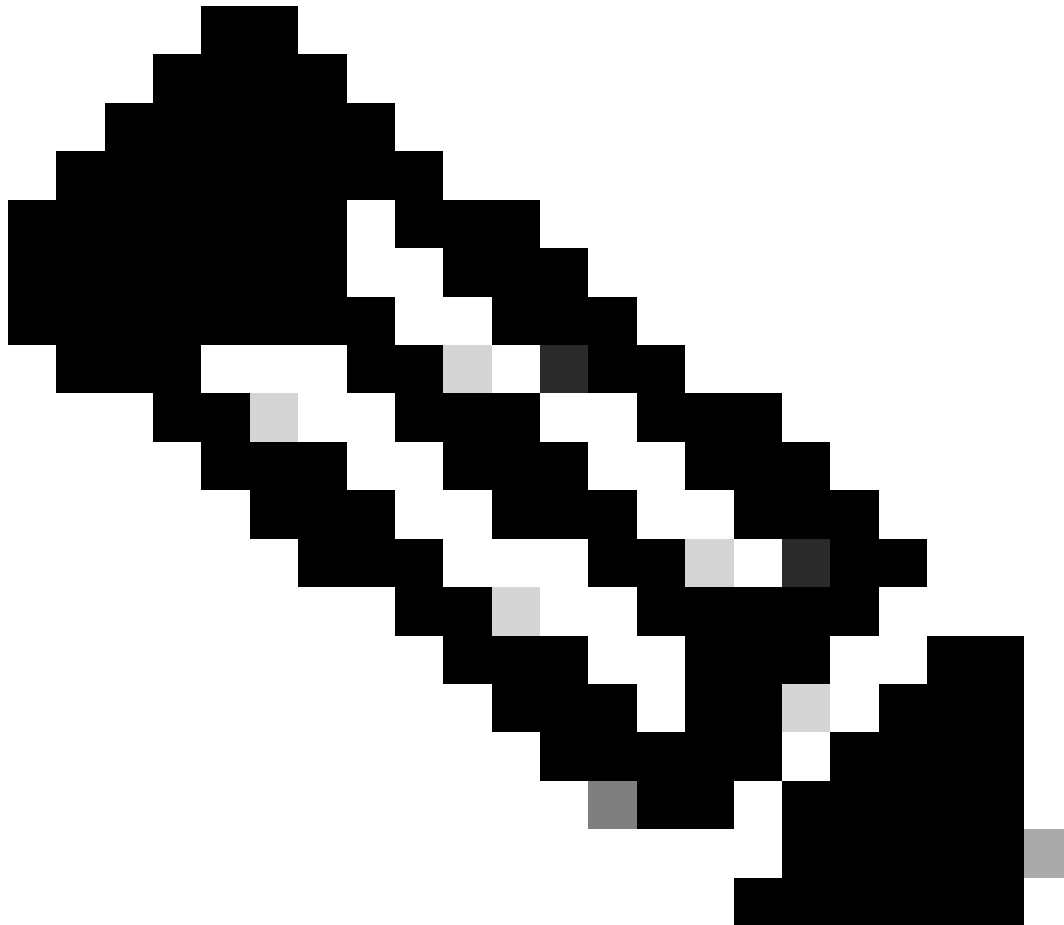
- 此错误表示“用户身份位置”(User Identity Location)和“用户身份属性名称”(User Identity Attribute Name)字段中存在配置问题/不匹配。

- 在ECE管理控制台中的“用户身份位置”和“用户身份属性名称”检查并更正，在“选择配置”下拉菜单中的“单一登录”>“配置”下，选择“代理”>“SSO配置”选项卡>“标识提供程序”(第15步)。

## 相关信息

这些是您在开始安装或整合欧洲经委会之前必须仔细审查的重要文件。这不是一份欧洲经委会文件的综合清单。

---



注意：

- 大多数欧洲经委会文件有两个版本。请确保下载并使用适用于PCCE的版本。文档标题在版本号后为Packaged Contact Center Enterprise或（用于PCCE）或（用于UCCE和PCCE）。
  - 在安装、升级或集成之前，确保您查看思科企业聊天和电子邮件文档的开始页面以了解任何更新。
  - <https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html>
-

ECE版本12.6(1)

- [企业聊天和电子邮件管理员指南](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。