

# Configurar e Solucionar Problemas de SSO para Agentes e Administrador de Partição no ECE

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configuration Steps](#)

[Configurando Confiança da Terceira Parte Confiável para ECE](#)

[Configurando um provedor de identidade](#)

[Criando e Importando Certificados](#)

[Configuração do Logon Único do Agente](#)

[Defina o URL do servidor Web/LB nas configurações de partição](#)

[Configurando SSO para Administradores de Partição](#)

[Troubleshooting](#)

[Definindo o nível de rastreamento](#)

[Cenário de Identificação e Solução de Problemas 1](#)

[Erro](#)

[Análise de log](#)

[Resolução](#)

[Cenário de Identificação e Solução de Problemas 2](#)

[Erro](#)

[Análise de log](#)

[Resolução](#)

[Cenário de Identificação e Solução de Problemas 3](#)

[Erro](#)

[Análise de log](#)

[Resolução](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve as etapas necessárias para configurar o Logon Único (SSO) para Agentes e Administradores de Partição em uma solução ECE.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

Cisco Packaged Contact Center Enterprise (PCCE)

Cisco Unified Contact Center Enterprise (UCCE)

E-mail e bate-papo corporativo (ECE)

Microsoft Ative Directory

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

Versão UCCE: 12.6(1)

Versão ECE: 12.6(1)

Serviço de Federação do Microsoft Ative Directory (ADFS) no Windows Server 2016

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

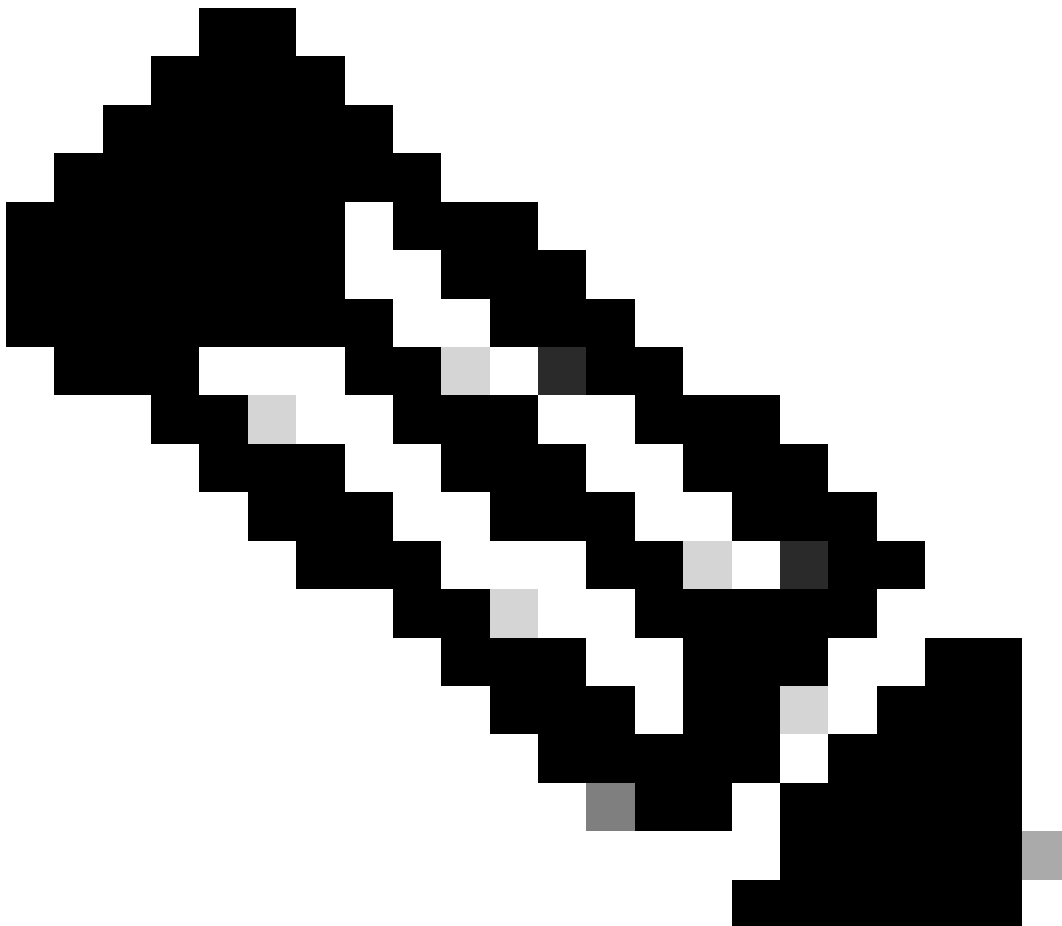
Os consoles ECE (Enterprise Chat and Email) podem ser acessados fora do Finesse; no entanto, o SSO deve ser habilitado para permitir que agentes e supervisores façam login no ECE por meio do Finesse.

O Logon Único também pode ser configurado para novos administradores de partição. Isso garante que os novos usuários que efetuarem login na área de trabalho do Administrador da Cisco tenham acesso ao Enterprise Chat and Email Administration Console.

Aspectos importantes a serem observados sobre o Logon Único:

- O processo de configuração de um sistema para logon único deve ser executado para o nó de segurança no nível de partição por um usuário da partição com as ações necessárias: Exibir segurança do aplicativo e Gerenciar segurança do aplicativo.
- Para que os supervisores e administradores efetuem login nos consoles que não sejam o Console do agente, uma vez que o SSO esteja habilitado, você deverá fornecer um URL Externo válido do Aplicativo nas configurações de partição. Consulte Configurações gerais de partição para obter mais informações.
- Um certificado JKS (Java Keystore) é necessário para configurar o SSO para permitir que usuários com funções de administrador ou supervisor entrem na partição 1 do ECE fora do Finesse usando suas credenciais de login do SSO. Consulte seu departamento de TI para receber o certificado JKS.

- Um certificado SSL (Secure Sockets Layer) do Cisco IDS deve ser importado para todos os servidores de aplicativos em uma instalação. Para obter o arquivo de certificado SSL necessário, entre em contato com o departamento de TI ou o suporte Cisco IDS.
  - O agrupamento do servidor de banco de dados para o Unified CCE diferencia maiúsculas de minúsculas. O nome de usuário na declaração retornada da URL do ponto de extremidade de informações do usuário e o nome de usuário no Unified CCE devem ser iguais. Se não forem iguais, os agentes de logon único não serão reconhecidos como conectados e a ECE não poderá enviar a disponibilidade do agente para o Unified CCE.
  - A configuração do SSO para Cisco IDS afeta os usuários que foram configurados no Unified CCE para Logon Único. Verifique se os usuários que você deseja habilitar para SSO no ECE estão configurados para SSO no Unified CCE. Consulte o administrador do Unified CCE para obter mais informações.
- 



Note:

- Verifique se os usuários que você deseja habilitar para SSO no ECE estão configurados para SSO no Unified CCE.
  - Este documento especifica as etapas para configurar a Relying Part Trust for ECE
-

em uma Única Implantação do AD FS em que o Servidor de Federação de Recursos e o Servidor de Federação de Contas estão instalados na mesma máquina.

- Para uma implantação do AD FS Dividido, navegue até o guia de Instalação e Configuração ECE para a respectiva versão.

## Configuration Steps

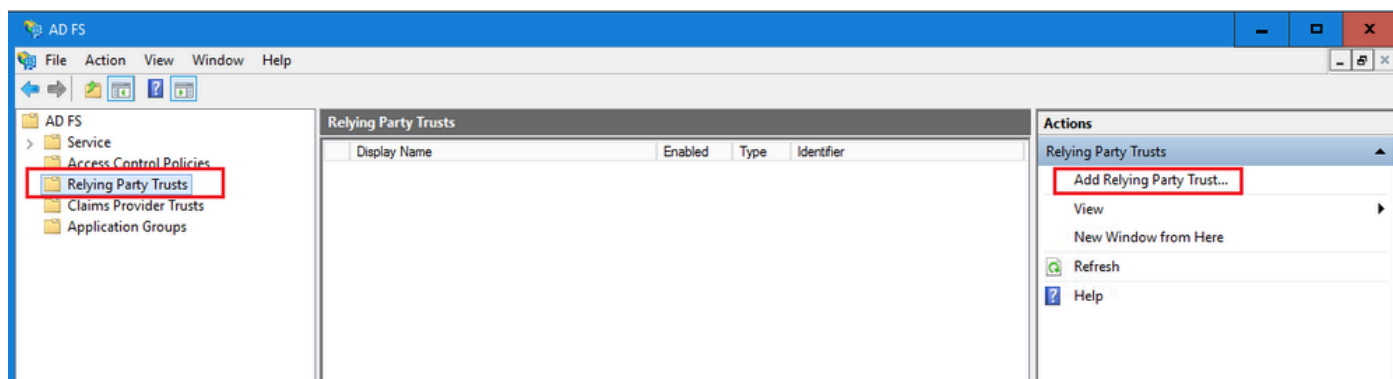
### Configurando Confiança da Terceira Parte Confiável para ECE

#### Passo 1

Abra o console de Gerenciamento do AD FS e navegue para AD FS > Relações de Confiança > Confiança da Terceira Parte Confiável.

#### Passo 2

Na seção Ações, clique em Adicionar objeto de confiança de terceira parte confiável...



#### Etapa 3

No assistente para Adicionar Objeto de Confiança de Terceira Parte Confiável, clique em Iniciar e conclua as próximas etapas:

- a. Na página Selecionar Origem de Dados, selecione a opção Inserir dados sobre a parte de resposta manualmente e clique em Próximo.

Add Relying Party Trust Wizard

## Select Data Source

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

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.

< Previous   Next >   Cancel

b. Na página Especificar Nome para Exibição, forneça um nome para Exibição para a terceira parte confiável. Clique em Next

The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Specify Display Name' step. The window title is 'Add Relying Party Trust Wizard'. The main heading is 'Specify Display Name'. Below the heading, there is a 'Steps' list on the left and a main configuration area on the right. The 'Steps' list includes: Welcome, Select Data Source, Specify Display Name (current step), Configure Certificate, Configure URL, Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main configuration area contains the instruction 'Enter the display name and any optional notes for this relying party.' There is a 'Display name:' label followed by a text box containing 'ECE Console'. Below this is a 'Notes:' label followed by a text area containing 'ECE 12.6.1'. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

**Add Relying Party Trust Wizard**

### Specify Display Name

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

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Display name:  
ECE Console

Notes:  
ECE 12.6.1

< Previous   Next >   Cancel

c. Na página Configurar URL:

i. Selecione a opção Ativar suporte para o protocolo SSO da Web SAML 2.0.

ii. No campo URL do servidor SSO SAML 2.0 da Terceira Parte Confiável, forneça o URL no formato: `https://<Web-Server-Or-Load-Balancer-FQDN>/system/SAML/SSO/POST.controller`

**Add Relying Party Trust Wizard**

### Configure URL

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL**
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

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.

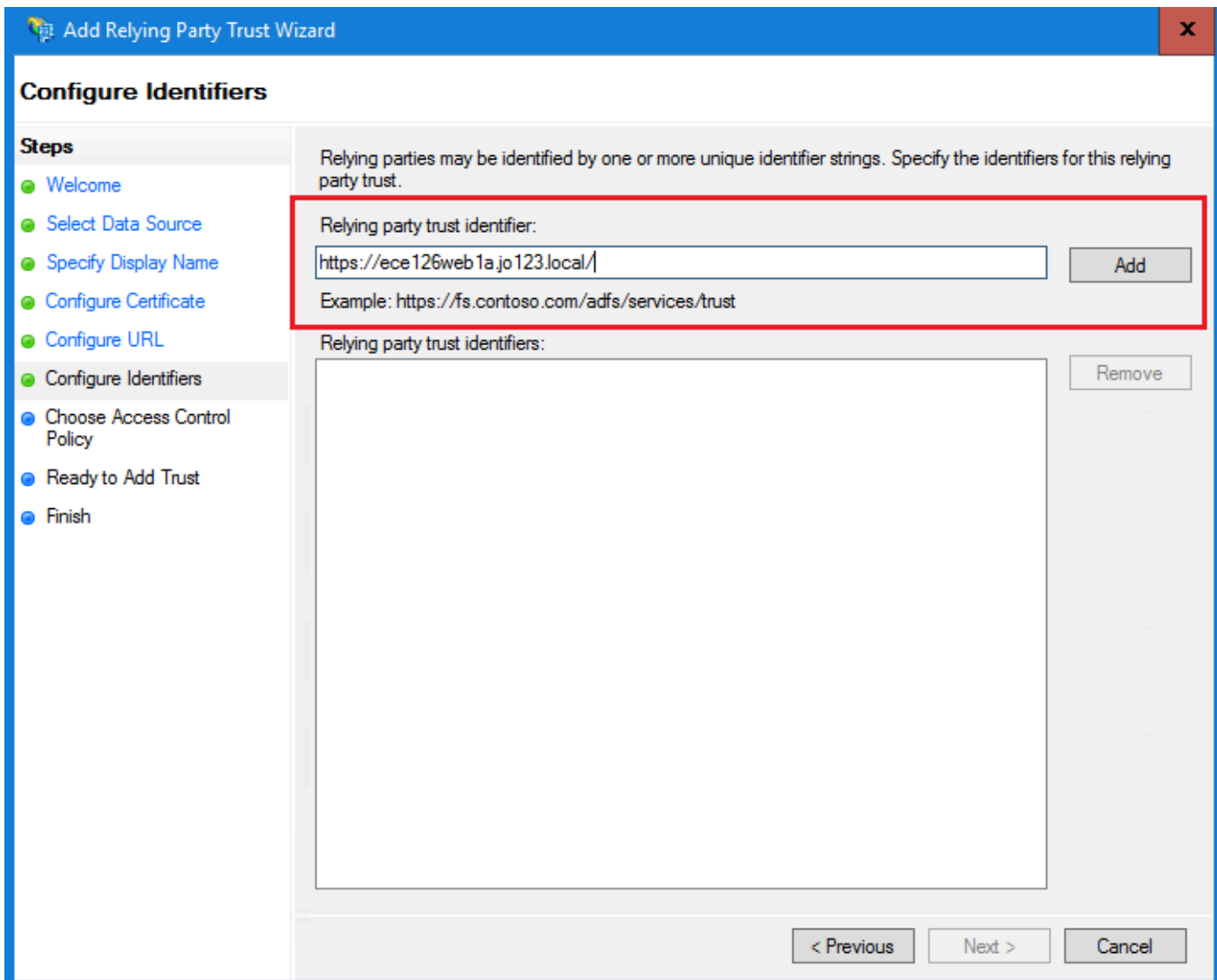
Relying party SAML 2.0 SSO service URL:

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

< Previous    Next >    Cancel

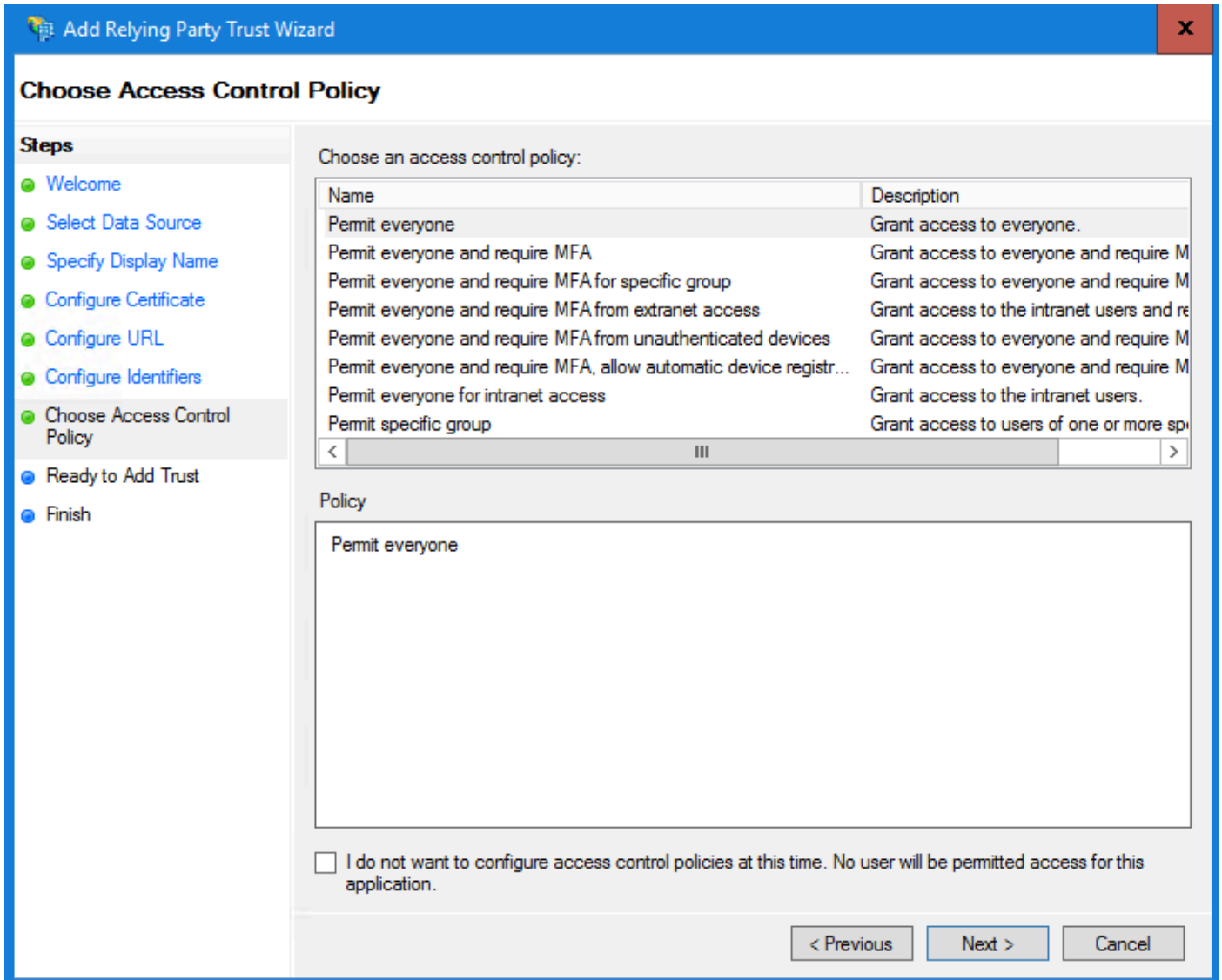
d. Na página Configurar Identificadores, forneça o identificador do objeto de confiança da terceira parte confiável e clique em Adicionar.

- O valor deve estar no formato: <https://<Web-Server-Or-Load-Balancer-FQDN>/>

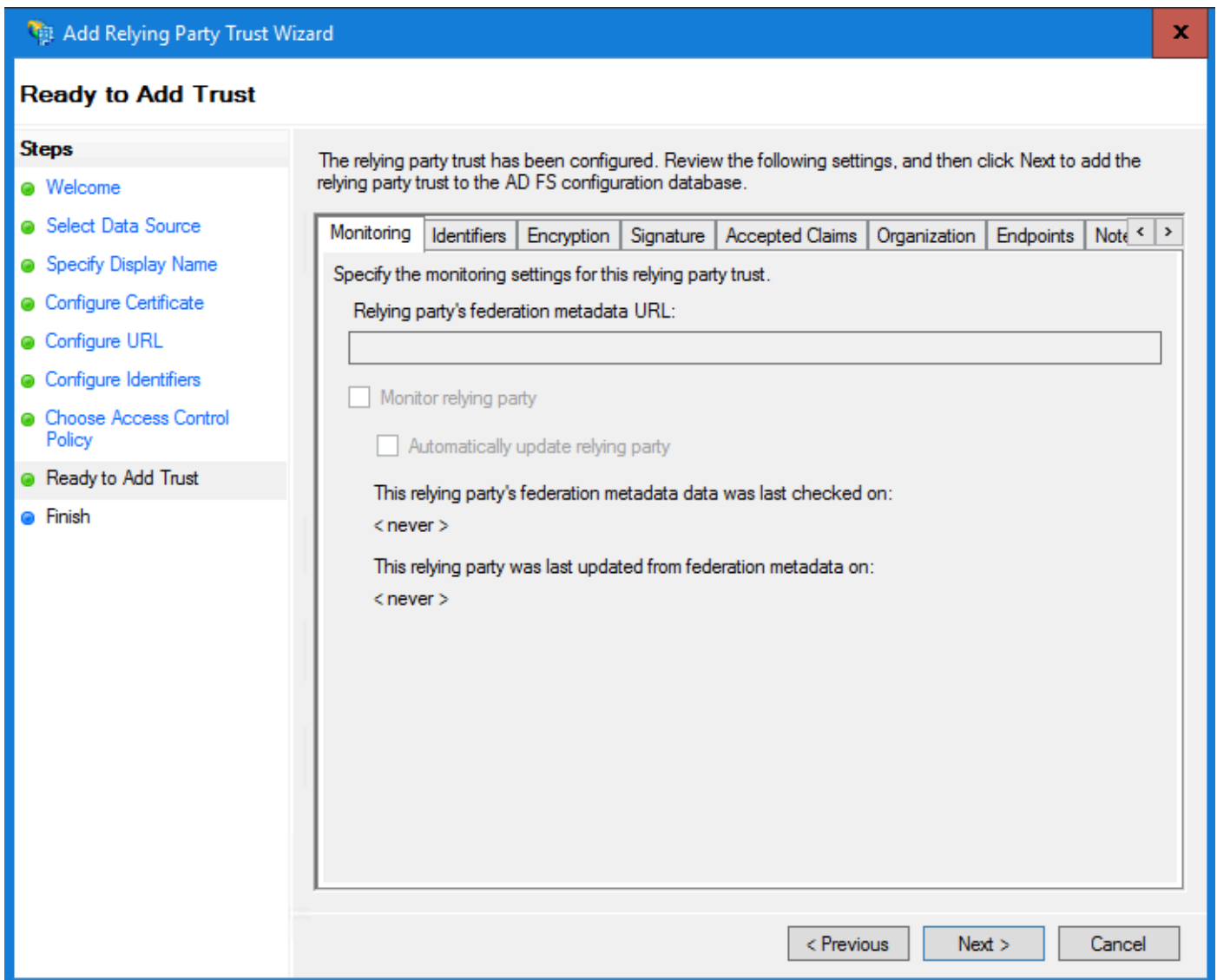


e. Na página Escolher política de controle de acesso, clique em próximo com o valor padrão da política 'Permitir todos'.

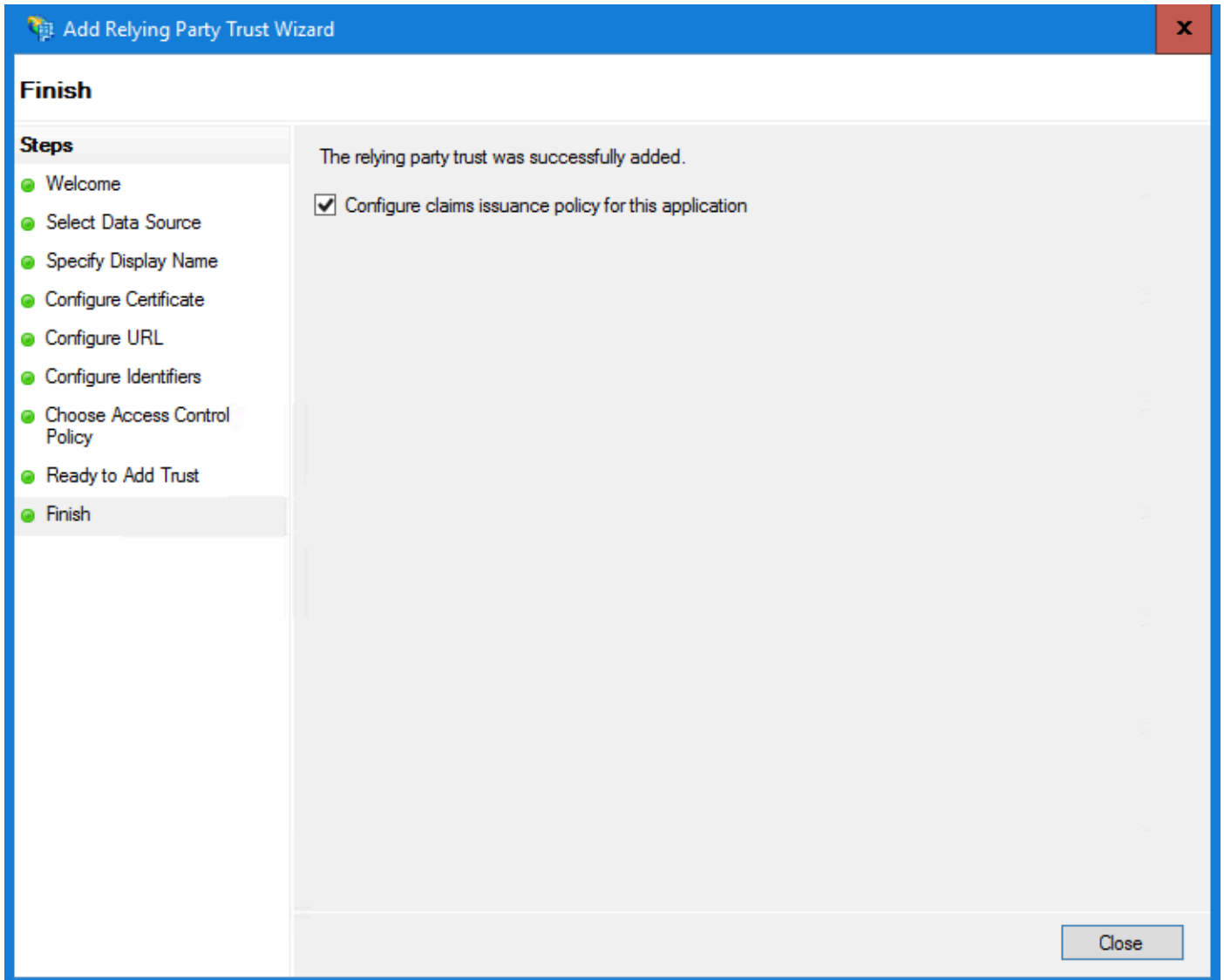




f. Na página Ready to Add Trust, clique em Next.

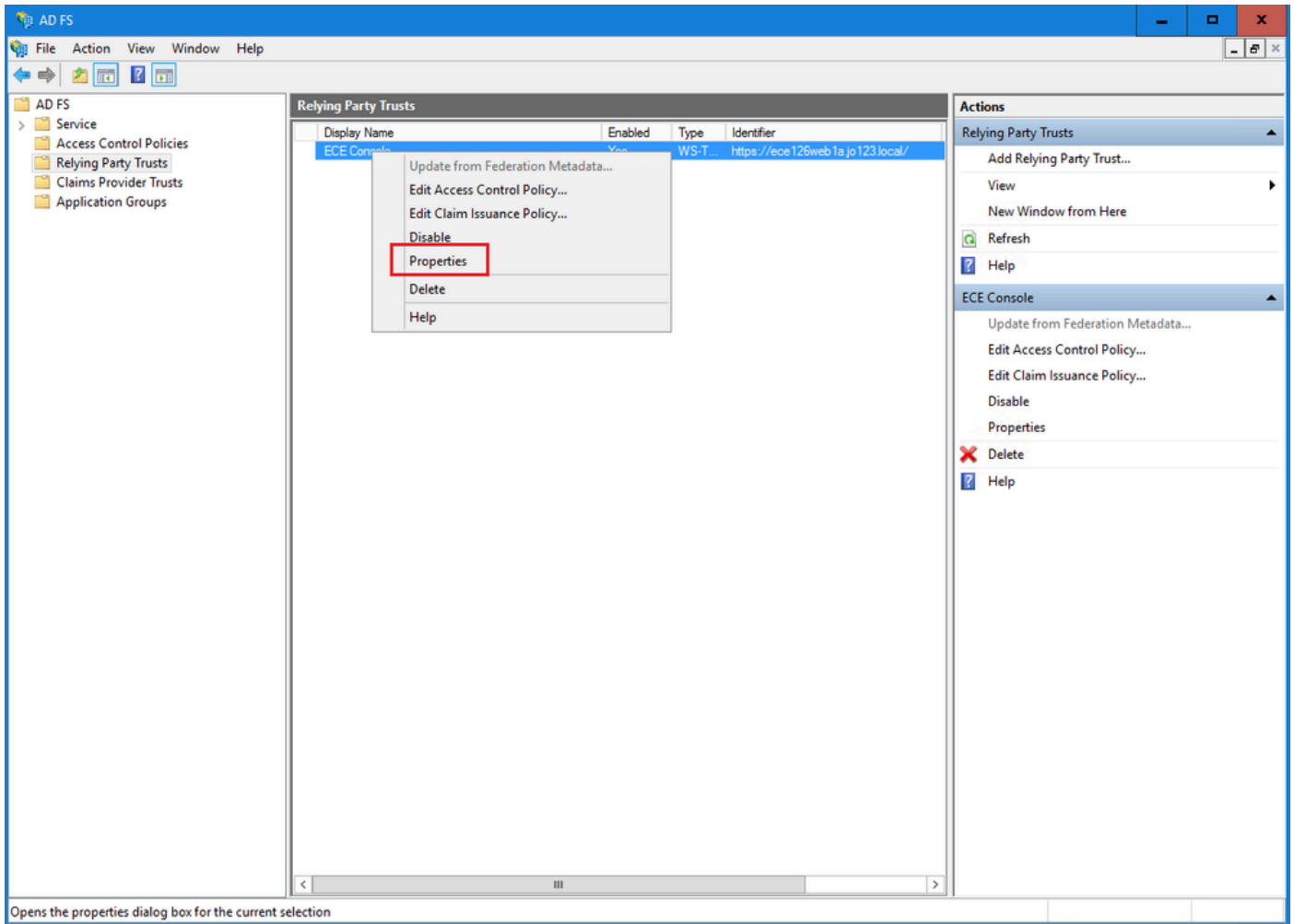


g. Depois que o objeto de confiança de terceira parte confiável for adicionado com êxito, clique em Fechar.



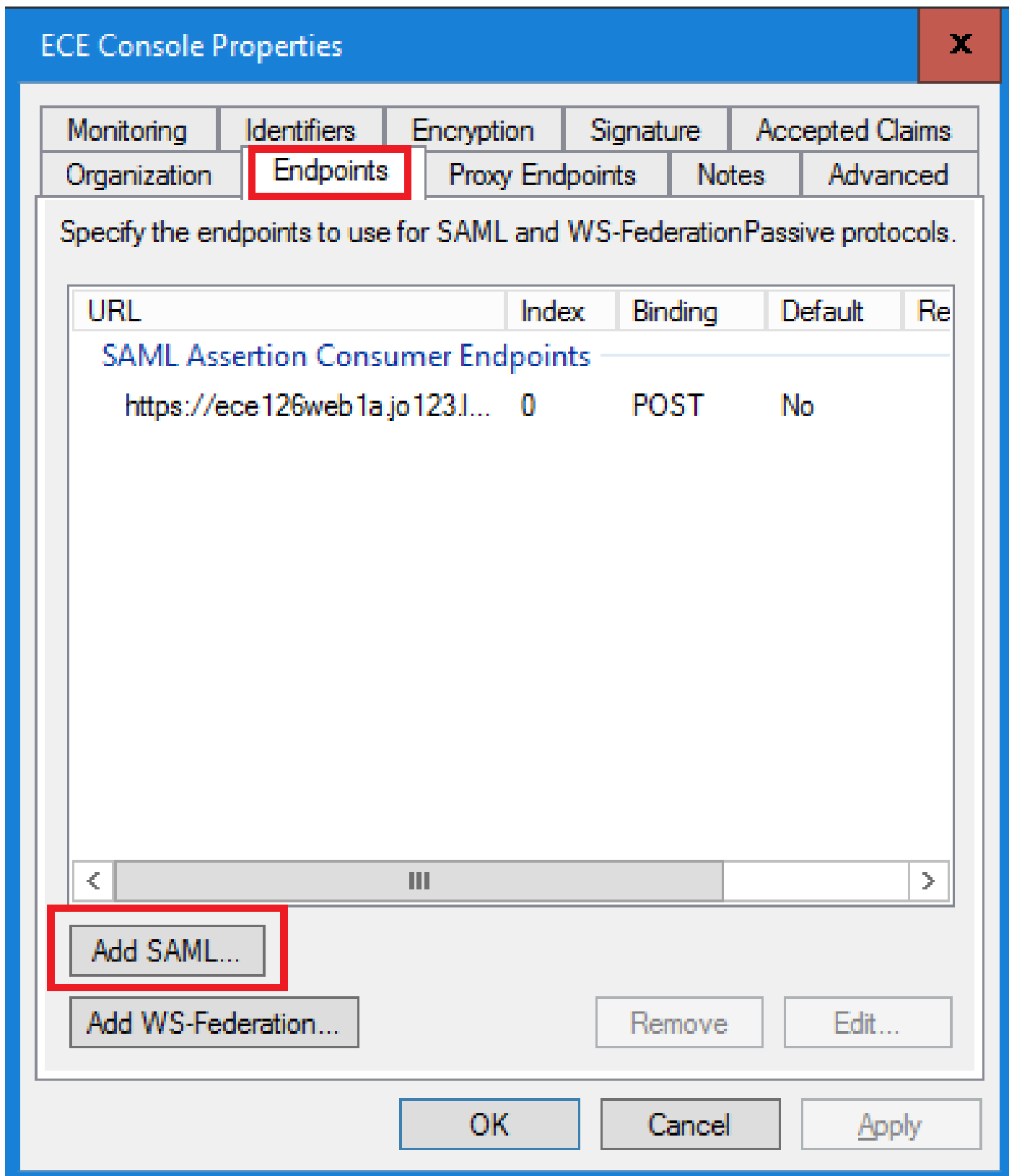
#### Passo 4

Na lista Confiança do Provedor Confiável, selecione a confiança da Terceira Parte Confiável criada para ECE e, na seção Ações, clique em Propriedades.



## Etapa 5

Na janela Propriedades, navegue até a guia Endpoints e clique no botão Adicionar SAML...



Etapa 6

Na janela Add an Endpoint, configure conforme observado:

1. Selecione o tipo de endpoint como logout SAML.
2. Especifique a URL Confiável como `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`

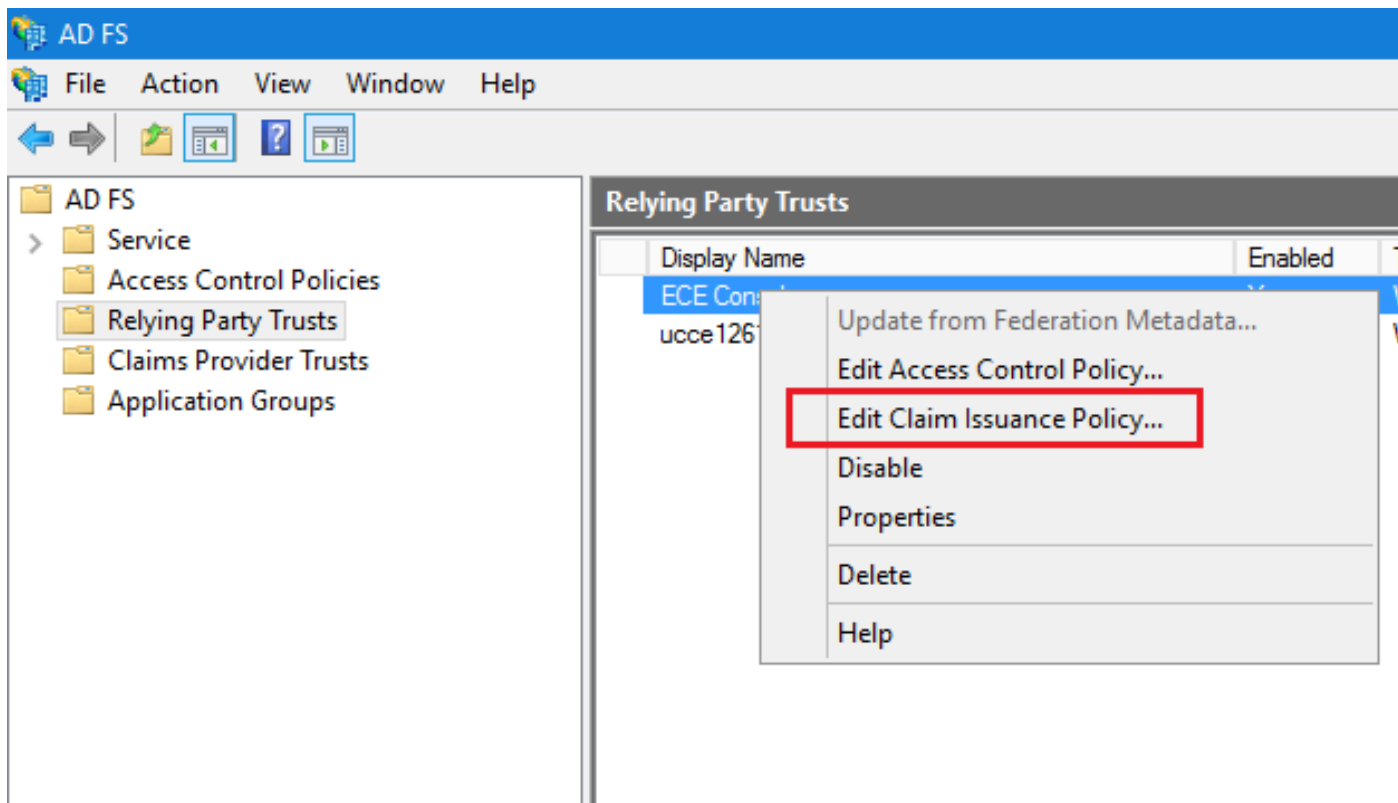
Response URL:

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

OK Cancel

#### Etapa 7

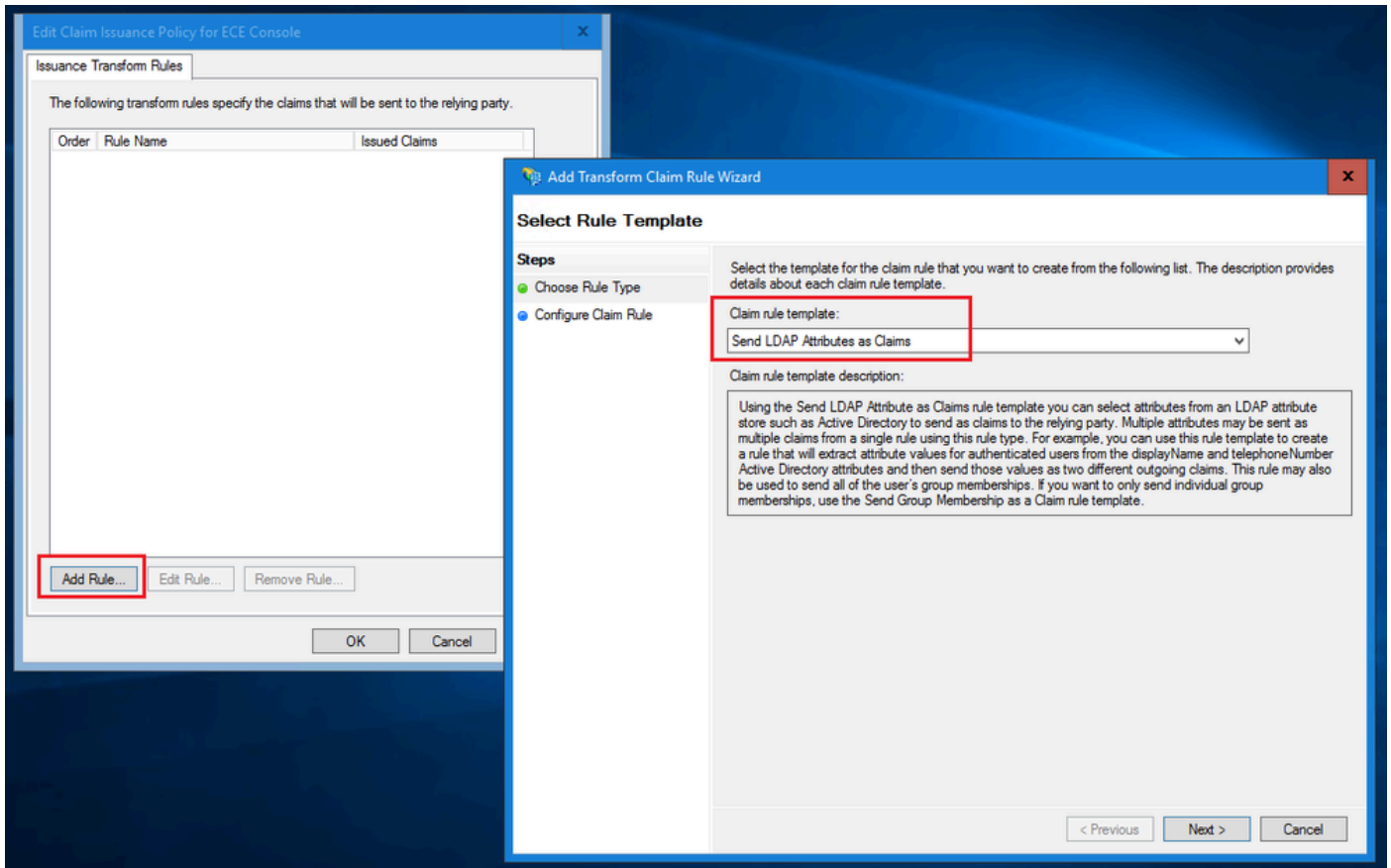
Na lista Confiança do provedor confiável, selecione a confiança criada para ECE e, na seção Ações, clique em Editar política de seguro de reivindicação.



## Passo 8

Na janela Editar política de seguro de reivindicação, na guia Regras de transformação de emissão, clique no botão Adicionar regra... e configure conforme mostrado:

a. Na página Escolher tipo de regra, selecione Enviar atributos LDAP como reivindicações no menu suspenso e clique em Avançar.



b. Na página Configurar Regra de Reivindicação:

1. Forneça o nome da regra de Declaração e selecione o armazenamento de Atributos.
  2. Defina o mapeamento do atributo LDAP e o tipo de declaração de saída.
- Selecione ID do Nome como o nome do tipo de declaração de saída.
  - Clique em Concluir para voltar à janela Editar Política de Seguro de Reivindicação e clique em OK.



## 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

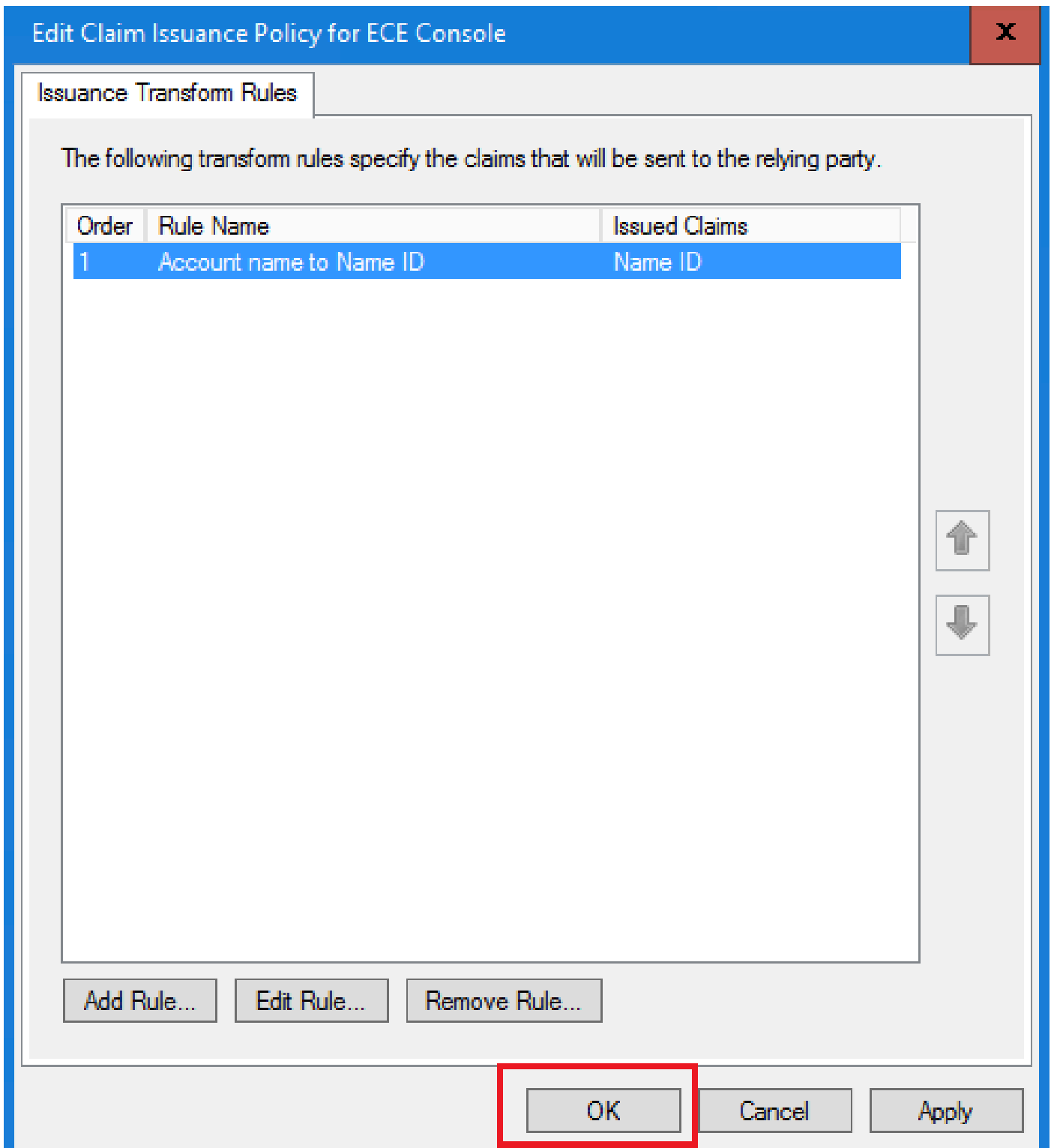
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	Name ID
*		

< Previous

Finish

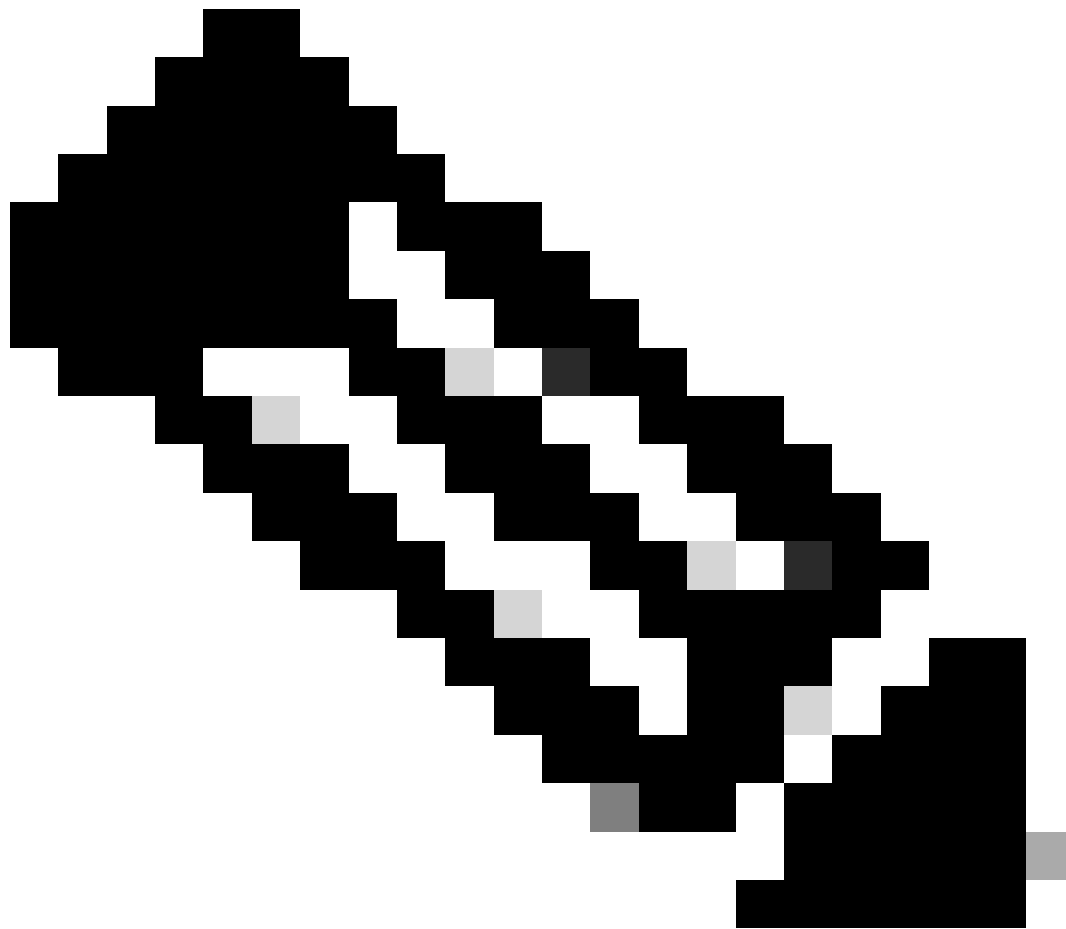
Cancel



### Passo 9

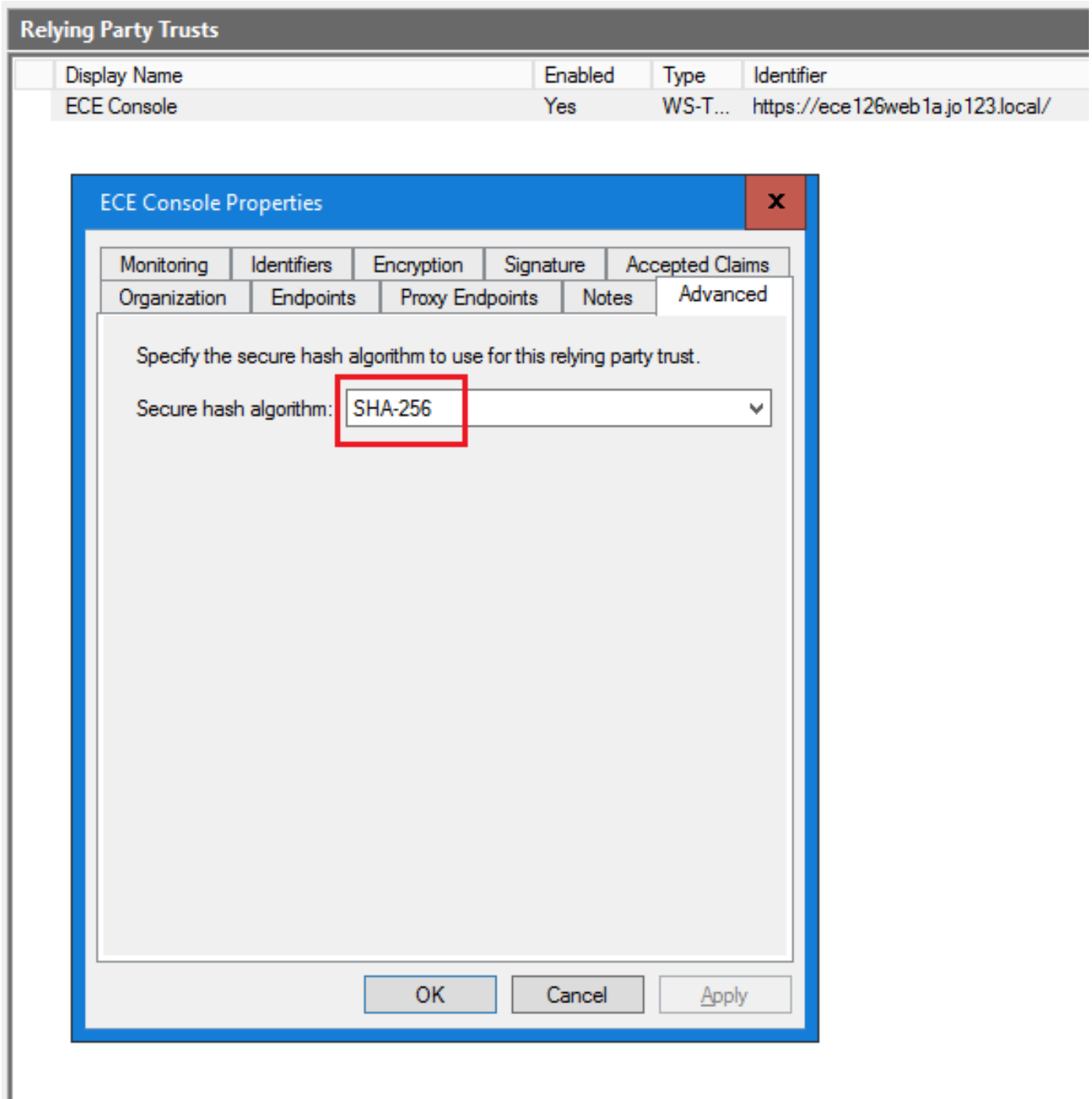
Na lista Confianças do provedor confiável, clique duas vezes no objeto de confiança da terceira parte confiável ECE que você criou.

Na janela Propriedades que será aberta, vá até a guia Avançado e defina o algoritmo de hash seguro como SHA-1 ou SHA-256. Clique em OK para fechar a janela.



Observação: este valor deve corresponder ao valor 'Signing algorithm' definido para o 'Service Provider' em SSO Configurations in ECE

---



## Passo 10

Verifique e anote o valor do Identificador do Serviço de Federação.

- No console Gerenciamento do AD FS, selecione e clique com o botão direito do mouse em AD FS > Editar Propriedades do Serviço de Federação > guia Geral > Identificador do Serviço de Federação



Note:

- Este valor deve ser adicionado exatamente como está ao configurar o valor de 'ID da entidade' para Provedor de identidade em Configurações de SSO em ECE.
  - O uso de `http://` NÃO significa que o ADFS não seja seguro; esse é apenas um identificador.
-

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 information about AD FS, including a 'view' section, a 'More About AD FS' section with links like 'What's new in AD FS?', 'AD FS Deployment Guide', and 'AD FS Operations Guide', and a 'More About Azure Active Directory' section with a blue diamond icon and text describing Azure Active Directory. The right-hand pane, titled 'Actions', lists the same menu items as the context menu. At the bottom of the window, a status bar displays the text 'Edit the federation service properties'.

The image shows a Windows dialog box titled "Federation Service Properties" with a blue header and a red close button in the top right corner. The dialog has three tabs: "General", "Organization", and "Events". The "General" tab is selected. The fields are as follows:

- Federation Service display name:** Text box containing "JO123 ADFS". Below it, an example: "Example: Fabrikam Federation Service".
- Federation Service name:** Text box containing "WIN-260MECJBIC2.jo123.local". Below it, an example: "Example: fs.fabrikam.com".
- Federation Service identifier:** Text box containing "http://WIN-260MECJBIC2.jo123.local/adfs/services/trust". Below it, an example: "Example: http://fs.fabrikam.com/adfs/services/trust". This section is highlighted with a red border.
- Web SSO lifetime (minutes):** Spin box set to "480".
- Enable delegation for service administration**  
    **Delegate name:** Text box (empty) and "Edit..." button.
- Allow Local System account for service administration**
- Allow Local Administrators group for service administration**

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

## Configurando um provedor de identidade

### Passo 11

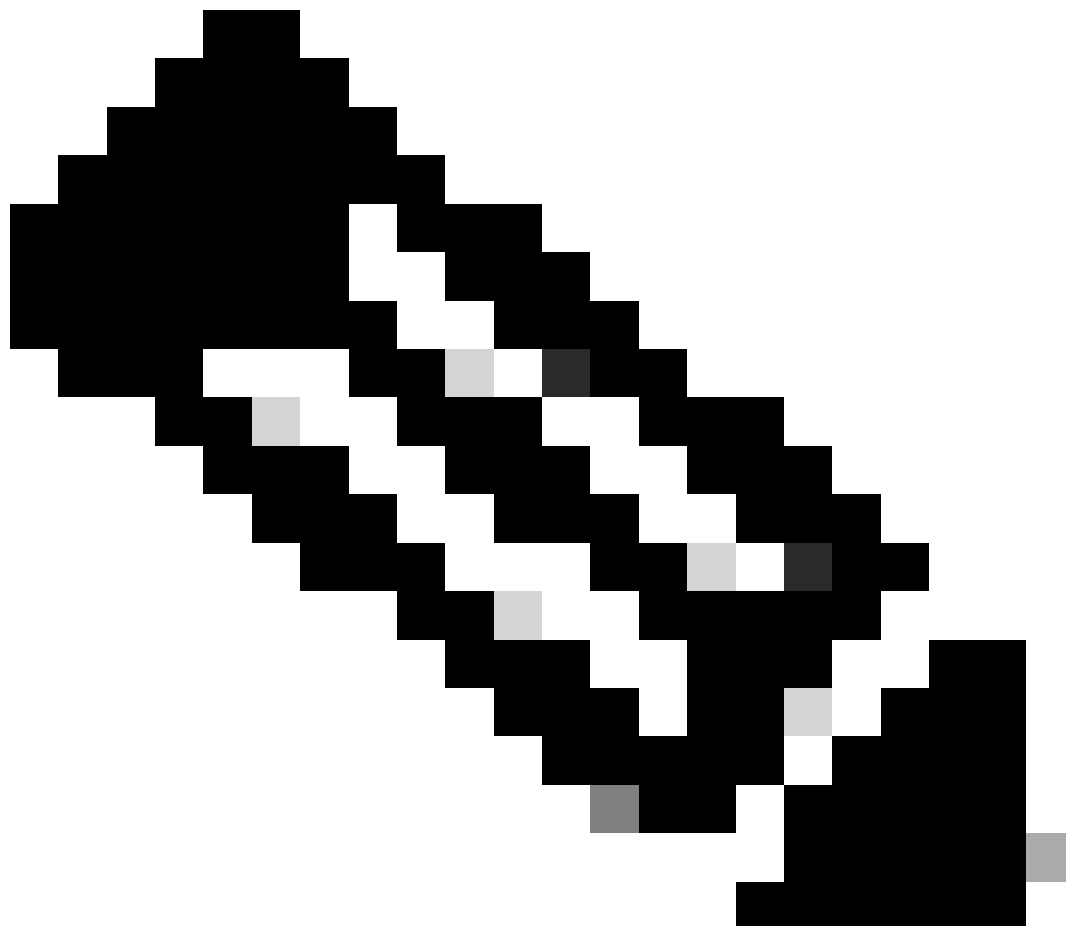
Um certificado JKS (Java Keystore) é necessário para configurar o SSO para permitir que usuários com funções de administrador ou supervisor entrem na partição ECE fora do Finesse usando suas credenciais de login do SSO.

Se você quiser configurar o SSO para permitir que usuários com funções de administrador ou

supervisor entrem na partição ECE fora do Finesse usando suas credenciais de login do SSO, o certificado JKS (Java Keystore) deve ser convertido em certificado de chave pública e configurado na Confiança da Terceira Parte Confiável criada no servidor IdP para ECE.

Consulte seu departamento de TI para receber o certificado JKS.

---



Observação: essas etapas são aplicáveis a sistemas que usam o ADFS como o provedor de identidade. Outros provedores de identidade podem ter métodos diferentes para configurar o certificado de chave pública.

---

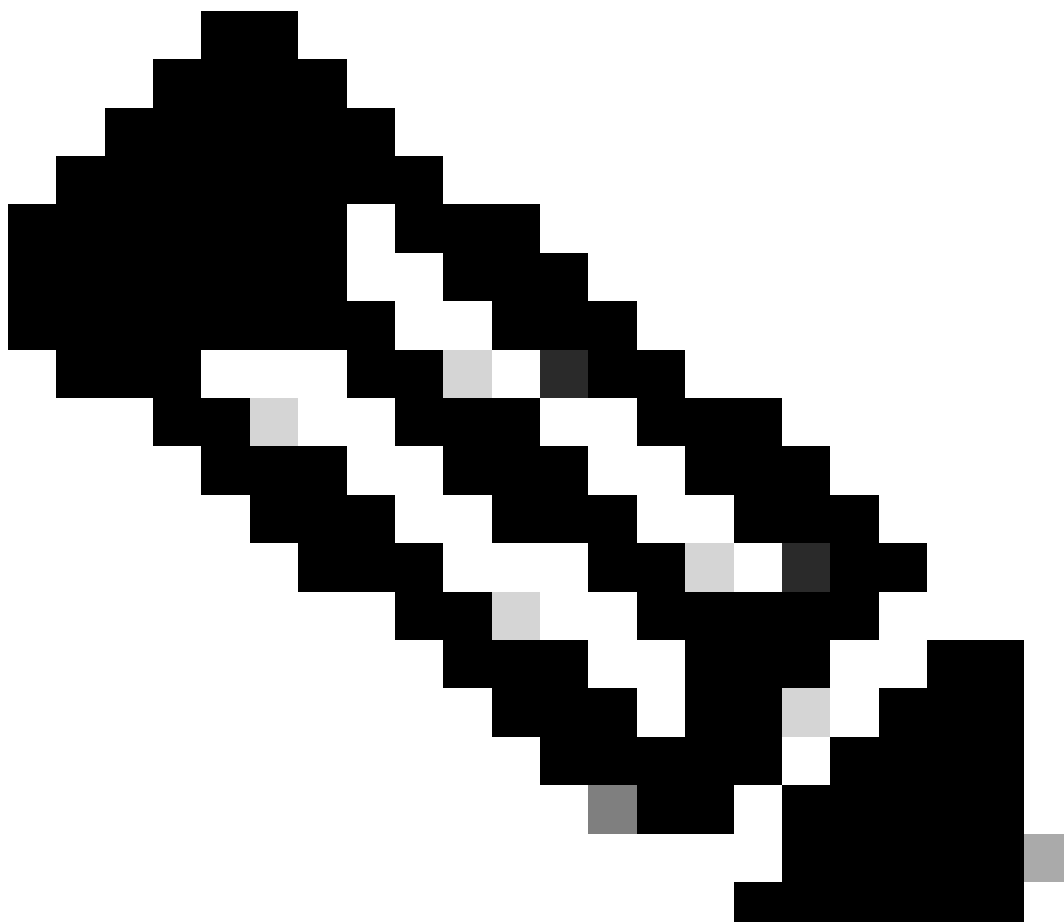
Aqui está um exemplo de como um arquivo JKS foi gerado no laboratório:

a. Gerar JKS:

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



---



Observação: a senha do armazenamento de chaves, o nome do alias e a senha da chave inseridos aqui são usados durante a configuração da configuração do 'Provedor de serviços' em Configurações de SSO no ECE.

---

```
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. Exportar o certificado:

Este comando keytool exporta o arquivo de certificado no formato .crt com o nome de arquivo

ece126web1a\_saml.crt para o diretório C:\Temp.

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

## Etapa 12

### Configurando um provedor de identidade

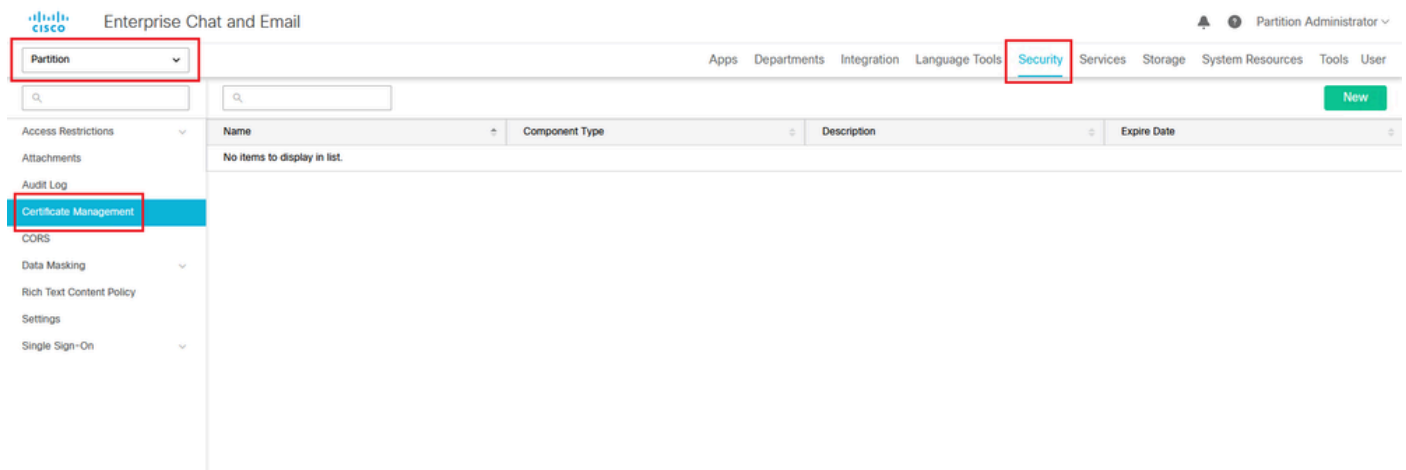
1. No console Gerenciamento do AD FS, selecione e clique com o botão direito do mouse na Terceira Parte Confiável criada para ECE.
2. Abra a janela Propriedades da relação de confiança e, na guia Assinatura, clique no botão Adicionar.
3. Adicione o certificado público (arquivo .crt gerado na etapa anterior) e clique em OK.

## Criando e Importando Certificados

### Passo 13

Antes de configurar o SSO para usar o Cisco IDS para Logon Único para Agentes, o certificado Tomcat do servidor Cisco IdS deve ser importado para o aplicativo.

- a. No console de administração ECE, em menu de nível de partição, clique na opção Security e selecione Certificate Management no menu à esquerda.



- b. No espaço Gerenciamento de Certificados, clique no botão Novo e insira os detalhes apropriados:

- Nome: digite um nome para o certificado.
- Descrição: adicione uma descrição para o certificado.
- Tipo de componente: selecione CISCO IDS.
- Importar certificado: para importar o certificado, clique no botão Pesquisar e adicionar e insira os detalhes solicitados:
- Arquivo de certificado: clique no botão Procurar e selecione o certificado que deseja importar. Os certificados só podem ser importados nos formatos .pem, .der (BINÁRIO) ou

.cer/cert.

- Nome do Apelido: forneça um apelido para o seu certificado.

### c. Clique em Salvar

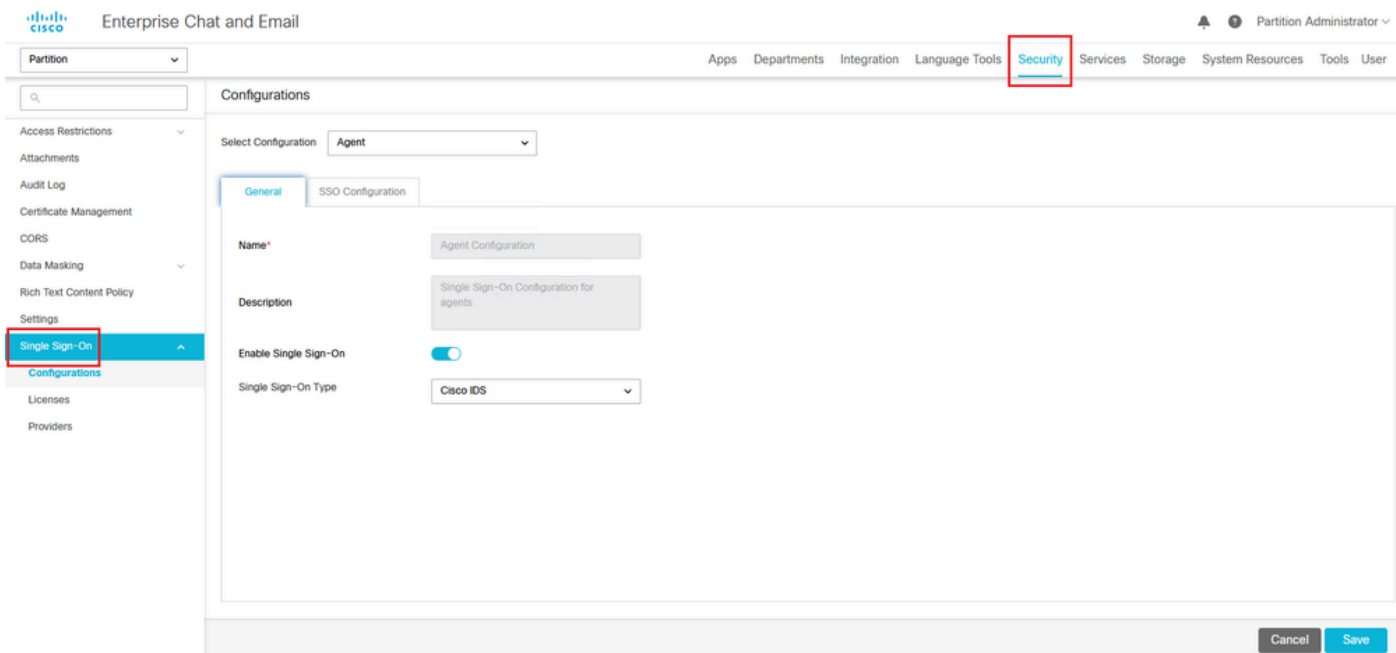
The screenshot shows the Cisco Enterprise Chat and Email configuration page. At the top left is the Cisco logo and the page title "Enterprise Chat and Email". Below the logo is a "Partition" dropdown menu. A search bar is located on the left side of the main content area. A navigation sidebar on the left contains the following items: "Access Restrictions", "Attachments", "Audit Log", "Certificate Management" (highlighted in blue), "CORS", "Data Masking", "Rich Text Content Policy", "Settings", and "Single Sign-On". The main content area is titled "Create Certificate" and contains the following fields:

- Name\***: Cisco IDS Server
- Description**: Certificate for Cisco IdS Server
- Component Type\***: CISCO IDS (dropdown menu)
- Import Certificate**: ucce1261ids.cer (with a green plus icon to the right)

## Configuração do Logon Único do Agente

### Passo 14

1. No console de administração ECE, em menu de nível de partição, clique na opção Security e selecione Single Sign-On > Configurations no menu à esquerda.
2. No menu suspenso Selecionar configuração, selecione Agente e defina a configuração na guia Geral:
  - Ativar Signon Único: Clique no botão Alternar para ativar o SSO.
  - Tipo de logon único: selecione Cisco IDS.



## Etapa 15

Clique na guia Configuração de SSO e forneça os detalhes da configuração:

### a. Provedor do OpenID Connect

#### URL do Ponto de Extremidade de Informações do Usuário Primário

- A URL do ponto final de informações do usuário do servidor Cisco IDS principal.
- Esta URL valida a API de token do usuário/Informações do usuário.
- Ele está no formato: <https://cisco-ids-1:8553/ids/v1/oauth/userinfo>, onde cisco-ids-1 indica o Fully Qualified Domain Name (FQDN) do servidor Cisco IDS primário.

#### Nome da Declaração de Identidade do Usuário

- O nome da declaração retornado pela URL do ponto de extremidade de informações do usuário, que identifica o nome de usuário no Unified ou no Packaged CCE.
- O nome da declaração e o nome de usuário no Unified CCE ou no Packaged CCE devem corresponder.
- Esta é uma das asserções obtidas em resposta à validação do token do Portador.
- Se o nome de usuário dos agentes no Unified CCE ou no Packaged CCE corresponder ao Nome UPN, forneça "upn" como o valor do campo Nome da declaração de identidade do usuário.
- Se o nome de usuário dos agentes no Unified CCE ou no Packaged CCE corresponder ao nome da conta SAM, forneça "sub" como o valor do campo Nome da reivindicação de identidade do usuário.

#### URL do Ponto de Extremidade de Informações do Usuário Secundário

- A URL do ponto final de informações do usuário secundário do servidor Cisco IDS.
- Ele está no formato: <https://cisco-ids-2:8553/ids/v1/oauth/userinfo>, onde cisco-ids-2 indica o Fully Qualified Domain Name (FQDN) do servidor Cisco IDS secundário.

## Método de URL do Ponto de Extremidade de Informações do Usuário

- O método HTTP usado por ECE para fazer chamadas de validação de token de Portador para a URL do Ponto de Extremidade de Informações do Usuário.
- Selecione POST na lista de opções apresentada (o POST é selecionado aqui para corresponder ao método do servidor IDS).

POST: método usado para enviar dados ao servidor Cisco IDS no endpoint especificado.

## Duração do Cache de Token de Acesso (Segundos)

- A duração, em segundos, para a qual um token de Portador deve ser armazenado em cache em ECE.
- Os tokens de portador para os quais as chamadas de validação são bem-sucedidas são armazenados apenas em caches. (Valor mínimo: 1; valor máximo: 30)

## Permitir login de SSO fora do Finesse

- Clique neste botão de alternância se desejar permitir que usuários com funções de administrador ou supervisor entrem na partição ECE fora do Finesse usando suas credenciais de login SSO.
- Se ativado, as informações nas seções Provedor de identidade e Provedor de serviços devem ser fornecidas.
- Isso exige que sua configuração de IdP permita um servidor IdP compartilhado.



Partition

---

## Configurations

Select Configuration

General **SSO Configuration**

### OpenId Connect Provider

Primary User Info Endpoint URL*	<input type="text" value="https://ids-fqdn:8553/ids/v1/oauth/u ..."/>
User Identity Claim Name*	<input type="text" value="upn"/>
Secondary User Info Endpoint URL	<input type="text" value=""/>
User Info Endpoint URL Method*	<input type="text" value="POST"/>
Access Token Cache Duration (Seconds)*	<input type="text" value="30"/>
Allow SSO Login Outside Finesse	<input checked="" type="checkbox"/>

## b. Provedor de identidade

### ID da entidade

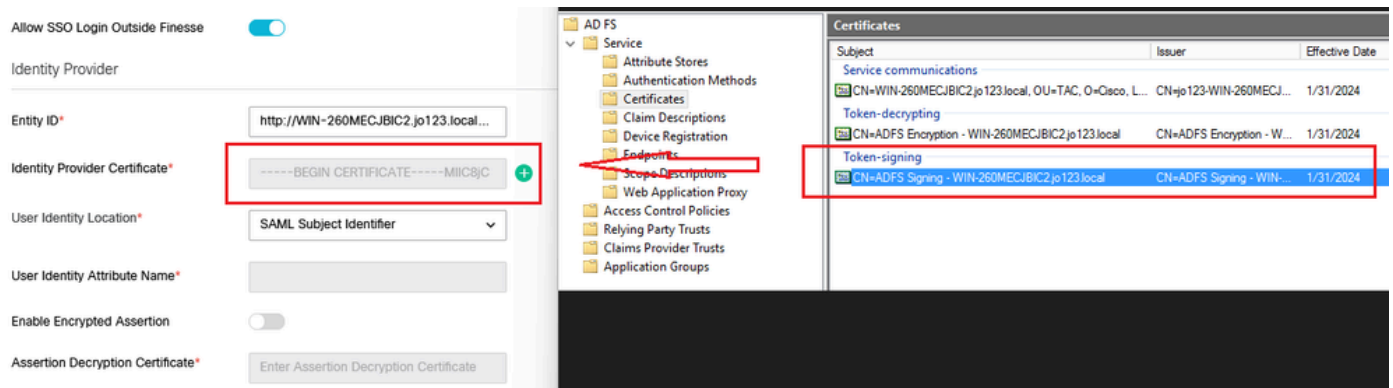
- ID da entidade do servidor IdP.

Observação: este valor deve corresponder exatamente ao valor do 'Identificador do Serviço de Federação' no console de Gerenciamento do AD FS.

The screenshot displays the AD FS Management console. On the left, a navigation pane shows 'Single Sign-On' selected, with 'Configurations' expanded. The main area shows the 'Configurations' page for the 'Agent' configuration, with the 'SSO Configuration' tab active. Under the 'Identity Provider' section, the 'Entity ID\*' field is highlighted with a red box and contains the value 'http://WIN-260MECJBIC2.jo123.local...'. A red arrow points from this field to the 'Federation Service Properties' dialog box on the right. In this dialog, the 'Federation Service Identifier' field is also highlighted with a red box and contains the value 'http://WIN-260MECJBIC2.jo123.local/adfs/services/trust'. Other fields in the dialog include 'Federation Service display name' (JO123 ADFS), 'Federation Service name' (WIN-260MECJBIC2.jo123.local), and 'Web SSO lifetime (minutes)' (480). There are also checkboxes for 'Enable delegation for service administration', 'Allow Local System account for service administration', and 'Allow Local Administrators group for service administration'.

Certificado do provedor de identidade

- O certificado de chave pública.
- O certificado deve começar com "-----BEGIN CERTIFICATE-----" e terminar com "-----END CERTIFICATE-----"
- Este é o certificado de assinatura de token no Console de Gerenciamento do AD FS > Serviço > Certificados > Assinatura de token.



## Local da Identidade do Usuário

- Selecione SAML Subject Identifier para definir o local da identidade no certificado para o identificador de assunto SAML padrão, como no assunto na asserção SAML, por exemplo, o nome de usuário no <saml:Subject>.
- Selecione SAML Attribute para atribuir o local da identidade a um atributo específico no certificado, por exemplo, email.address. Forneça o atributo no campo Nome do atributo de identidade do usuário.

## Nome do Atributo de Identidade do Usuário

- Aplicável somente quando o valor Local da ID de usuário é um atributo SAML.
- Isso pode ser ajustado dentro da asserção SAML e usado para selecionar um atributo diferente para a autenticação de usuários, como um endereço de e-mail.
- Ele também pode ser usado para criar novos usuários com um Atributo SAML.
- Por exemplo, se um usuário for identificado pelo valor fornecido no atributo email.address e o valor do endereço de email fornecido não corresponder a nenhum usuário no sistema, um novo usuário será criado com os atributos SAML fornecidos.

## Habilitar Asserção Criptografada (Opcional)

- Se quiser habilitar a asserção criptografada com o Provedor de identidade para logon no console, clique no botão Alternar para definir o valor como Habilitado.
- Caso contrário, defina o valor como Disabled (Desativado).

## Certificado de Descriptografia de Asserção

Se a opção Ativar asserção criptografada estiver definida como Ativada, clique no botão Pesquisar e adicionar e confirme a opção de alterar o certificado.

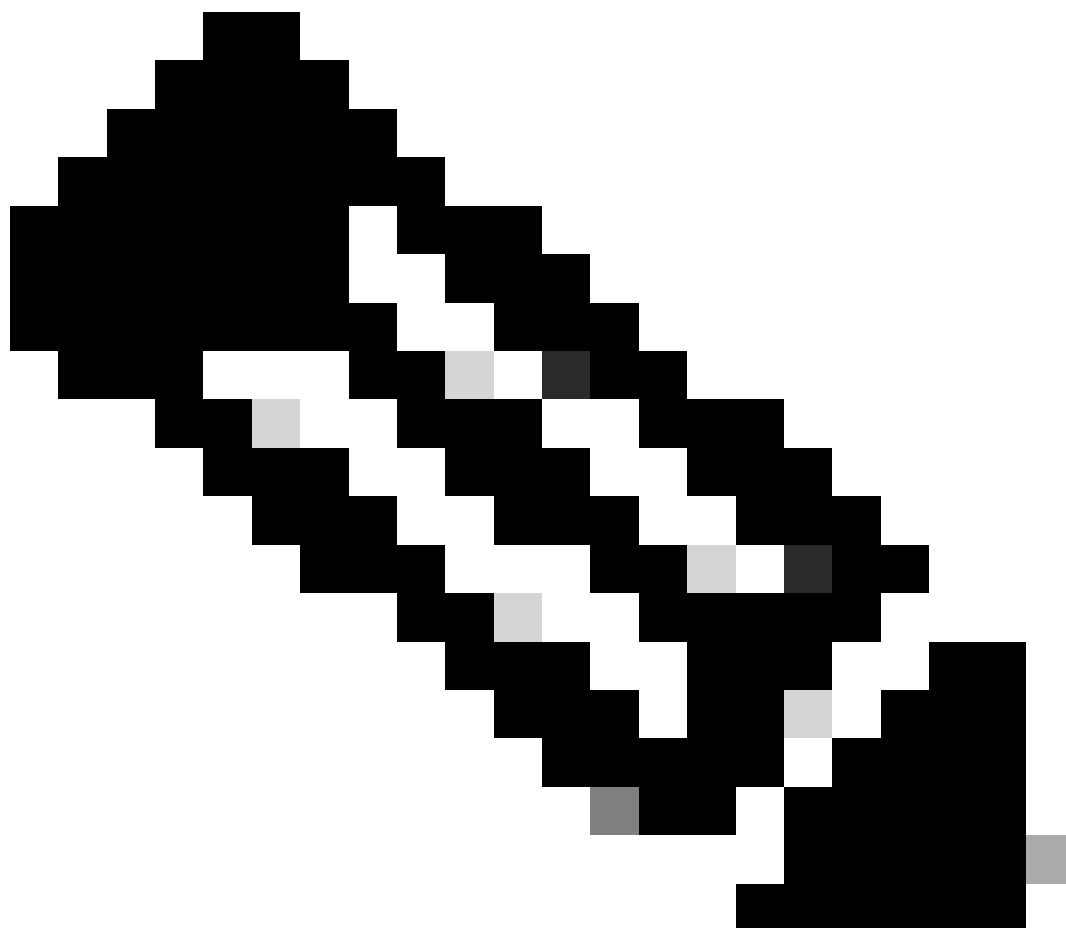
Forneça os detalhes na janela Certificado de Descriptografia de Asserção:

- Arquivo de armazenamento de chaves Java: forneça o caminho do arquivo de



armazenamento de chaves Java. Esse arquivo está no formato .jks e contém a chave de criptografia de que o sistema precisa para acessar arquivos protegidos pelo provedor de identidade.

- Nome do Apelido: O identificador exclusivo da chave de criptografia.
  - Senha da área de armazenamento de chaves: a senha necessária para acessar o arquivo de área de armazenamento de chaves Java.
  - Senha da Chave: A senha necessária para acessar a chave de criptografia do Alias.
- 



Observação: isso precisa corresponder ao certificado na guia 'Criptografia' da Terceira Parte Confiável ECE configurada no console de Gerenciamento do AD FS.

---

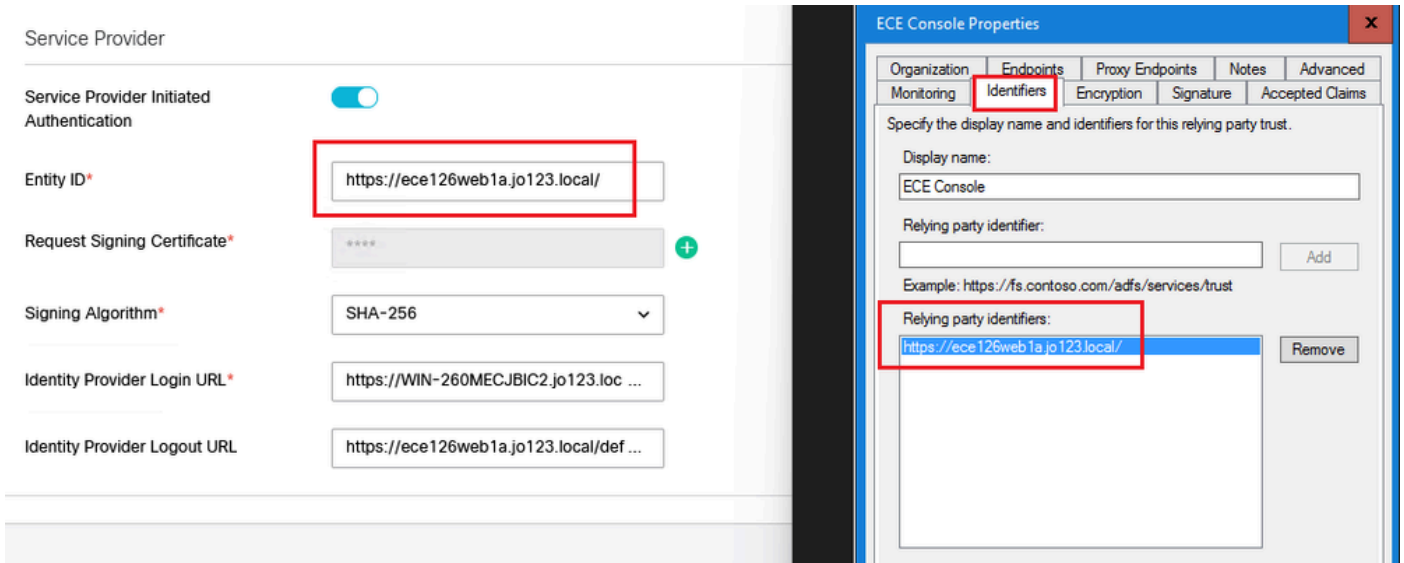
### c. Provedor de serviços

#### Autenticação Iniciada pelo Provedor de Serviços

- Defina o botão de alternância como Ativado.

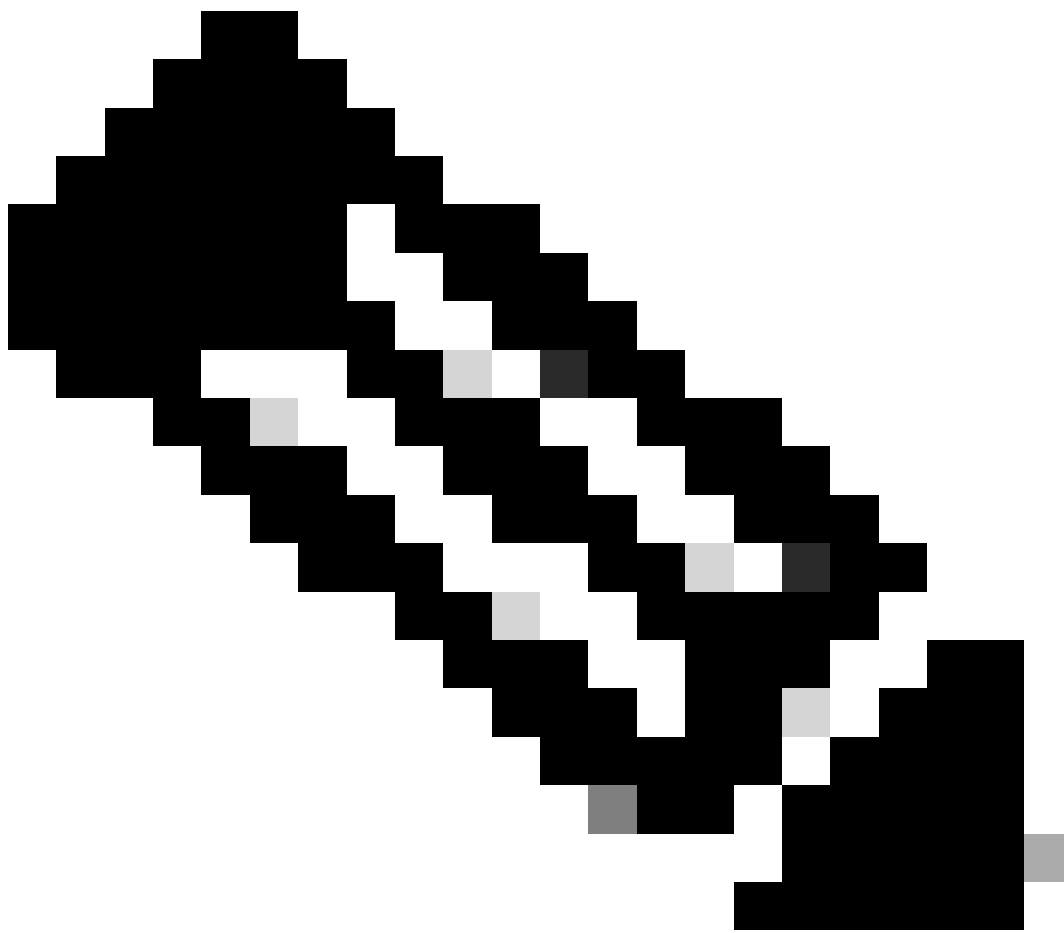
#### ID da entidade

- Forneça o URL externo do aplicativo ECE.



### Solicitar certificado de assinatura

- Um certificado JKS (Java Keystore) é necessário para fornecer as informações necessárias.
- Carregue o arquivo .jks usando o nome do alias e a senha da chave/armazenamento de chaves gerados na etapa 11.



Observação: isso precisa corresponder ao certificado carregado na guia 'Assinatura' do Objeto de Confiança de Terceira Parte Confiável ECE configurado no console de Gerenciamento do AD FS.

Service Provider

Service Provider Initiated Authentication

Entity ID\*

Request Signing Certificate\*

Signing Algorithm\*

Identity Provider Login URL\*

Identity Provider Logout URL

ECE Console Properties

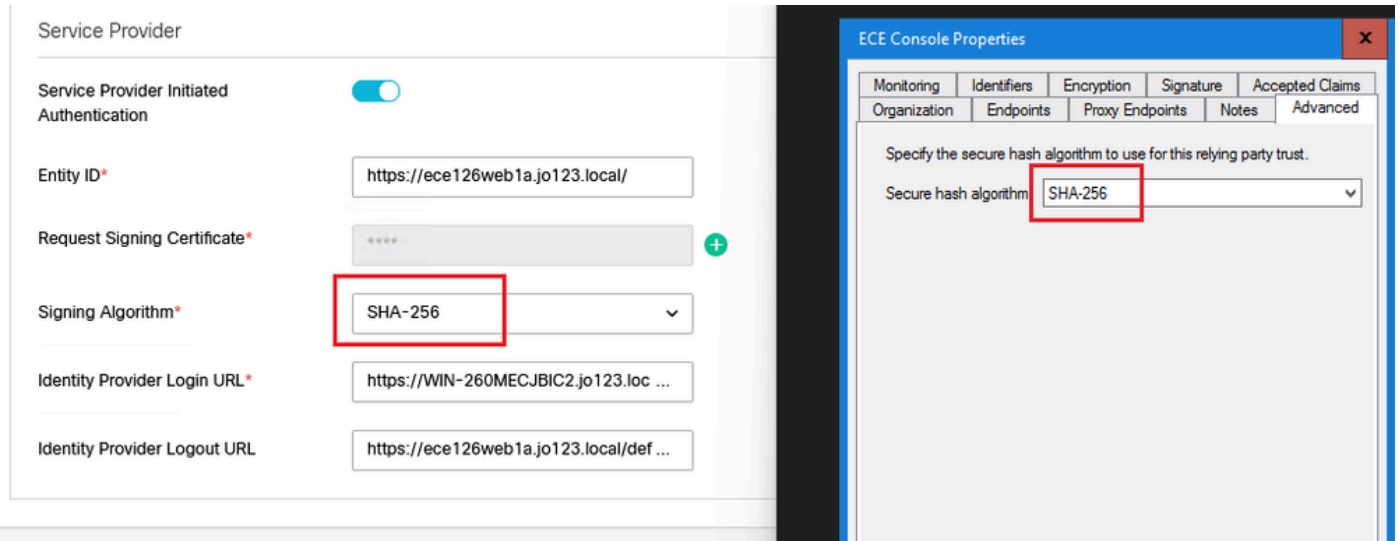
Organization Endpoints Proxy Endpoints Notes Advanced  
Monitoring Identifiers Encryption **Signature** Accepted Claims

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:...	1/29/20...

## Algoritmo de assinatura

- Defina o algoritmo de assinatura para o provedor de serviços.
- Se estiver usando ADFS, esse valor deverá corresponder ao algoritmo selecionado no objeto de confiança de terceira parte confiável criado para ECE na guia Avançado.



## URL de Logon do Provedor de Identidade

- A URL para autenticação SAML.
- Por exemplo, para ADFS, seria <http://<ADFS>/adfs/ls>.

## URL de Logout do Provedor de Identidade

- A URL para a qual os usuários são redirecionados ao fazer logoff. Isso é opcional e pode ser qualquer URL.
- Por exemplo, os agentes podem ser redirecionados para <https://www.cisco.com> ou qualquer outro URL após o logout do SSO.

## Passo 16

Clique em Salvar

Defina o URL do servidor Web/LB nas configurações de partição

## Etapa 17

Verifique se o URL correto do servidor Web/LB foi inserido em Configurações da partição > selecione a guia Aplicativos e navegue para Configurações gerais > URL externa do aplicativo



Partition  Apps Departments Integration

General Settings

Chat & Messaging

Email

**General Settings**

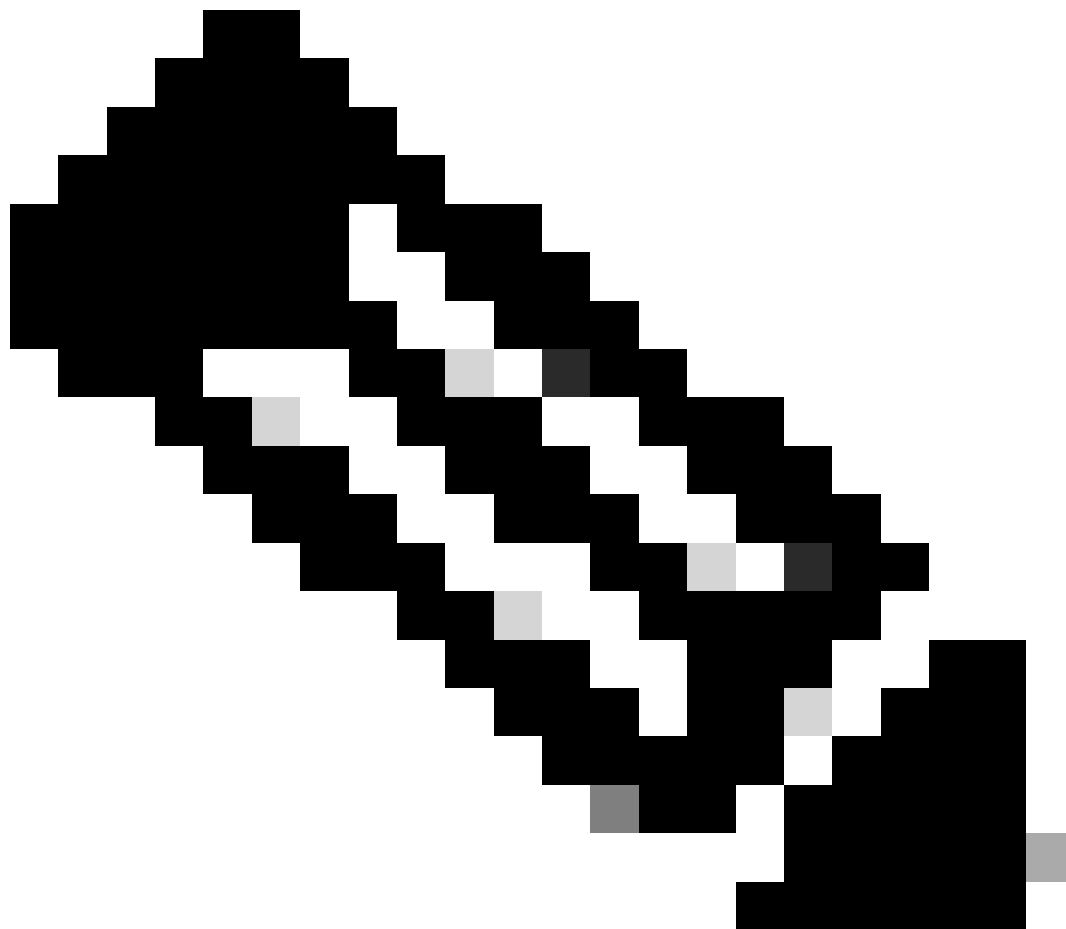
Knowledge

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

## Configurando SSO para Administradores de Partição



---

Note:

- Esta etapa se aplica somente ao PCCE.
- Isso é para o gadget ECE acessado na interface da WEB de administração do CCE <https://cceadmin>.

---

## Etapa 18

Para configurar o SSO para o Administrador de Partição

1. No console de administração ECE, em menu de nível de partição, clique na opção Security e selecione Single Sign-On > Configurations no menu à esquerda.
2. No menu suspenso Selecionar configuração, selecione Administradores de partição e insira os detalhes de configuração:

### URL LDAP

- A URL do servidor LDAP.
- Pode ser o URL do controlador de domínio (por exemplo, `ldap://LDAP_server:389`) ou o URL do catálogo global (por exemplo, `ldap://LDAP_server:3268`) do servidor LDAP.
- A partição pode ser adicionada automaticamente ao sistema quando o ECE é acessado por meio do Console de administração do CCE se o ECE estiver configurado com consulta LDAP.
- No entanto, em implantações do Active Directory com vários domínios em uma única floresta ou onde UPNs alternativos estão configurados, a URL do controlador de domínio com as portas LDAP padrão de 389 e 636 não deve ser usada.
- A integração LDAP pode ser configurada para usar o URL do catálogo global com as portas 3268 e 3269.



Observação: é uma prática recomendada usar o URL do Catálogo Global. Se você não usar um GC, um erro nos logs do ApplicationServer será mostrado a seguir.

- Exceção na autenticação LDAP <@>  
javax.naming.PartialResultException: Referência(s) de continuidade não processada(s); nome restante 'DC=example,DC=com'

---

#### atributo de DN

- O atributo do DN que contém o nome de login do usuário.
- Por exemplo, userPrincipalName.

#### Base

- O valor especificado para Base é usado pelo aplicativo como a base de pesquisa.
- Base de pesquisa é o local inicial para pesquisa na árvore de diretórios LDAP.
- Por exemplo, DC=minha empresa, DC=com.

## DN para pesquisa LDAP

- Se o seu sistema LDAP não permitir associação anônima, forneça o DN (Distinguished Name - Nome Distinto) de um usuário que tenha permissões de pesquisa na árvore de diretórios LDAP.
- Se o servidor LDAP permitir associação anônima, deixe este campo em branco.

## Senha

- Se o seu sistema LDAP não permitir associação anônima, forneça a senha de um usuário que tenha permissões de pesquisa na árvore de diretórios LDAP.
- Se o servidor LDAP permitir associação anônima, deixe este campo em branco.

## Etapa 19

### Clique em Salvar

Isso agora conclui a configuração de Logon Único para Agentes e Administradores de Partição no ECE.

# Troubleshooting

## Definindo o nível de rastreamento

1. No console de administração ECE, em menu de nível de partição, clique na opção System Resources e selecione Process Logs no menu à esquerda.
2. Na lista de processos, selecione o processo ApplicationServer > defina o nível de rastreamento desejado no menu suspenso 'Maximum Trace Level'.





Note:

- Para solucionar os erros de login do SSO durante a instalação inicial ou a reconfiguração, defina o rastreamento do processo do Servidor de Aplicativos para o nível 7.
  - Quando o erro for reproduzido, defina o nível de rastreamento de volta ao nível padrão 4, para evitar a substituição dos logs.
-

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

Process Logs

### Edit Process Log: ece126app1a:ApplicationServer

General | Advanced Logging

Name: ece126app1a:ApplicationServer

Description: ece126app1a:ApplicationServer

**Maximum Trace Level**: 4 - Info

Log File Name:

Maximum File Size:

Extensive Logging Duration:

Extensive Logging End Time:

4 - Info ✓

## Cenário de Identificação e Solução de Problemas 1

Erro

- Código do erro: 500
- Descrição do erro: o aplicativo não pode fazer login no usuário neste momento, pois houve falha no login do Provedor de identidade.

## Análise de log

- Falha no login do IdP - `<samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder" /></samlp:Status>`
- Aqui, o status "Respondente" indica que há algum problema no lado do AD FS - neste caso, principalmente com o "Solicitar certificado de assinatura" carregado no console de administração ECE (Configuração SSO > Provedor de serviços) e o certificado carregado para o ECE Relying Party Trust na guia 'Assinatura'.
- Este é o certificado que é gerado usando o arquivo de armazenamento de chaves Java.

## Logs do servidor de aplicativos - nível de rastreamento 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:
```

## Resolução

- Consulte a configuração "Solicitar Certificado de Autenticação" na seção "Configurando o Logon Único do Agente - Provedor de Serviços".
- Certifique-se de que o arquivo .jks do armazenamento de chaves Java gerado na Etapa 11

esteja carregado no campo "Solicitar certificado de assinatura" no console de administração ECE em Configuração de SSO > Selecione a configuração 'Agente' > guia 'Configuração de SSO' > Provedor de serviços > Solicitar certificado de assinatura.

- Verifique se o arquivo .crt está carregado na guia 'Signature' (Assinatura) do ECE Relying Party Trust (Etapa 12).

## Cenário de Identificação e Solução de Problemas 2

### Erro

- Código do erro: 400
- Descrição do Erro: token de Resposta SAML inválido: falha na validação de assinatura.

### Análise de log

- Este erro indica que há uma incompatibilidade no certificado entre o 'Certificado de assinatura de token' no ADFS e o 'Certificado do provedor de identidade' na Configuração SSO ECE.

Logs do servidor de aplicativos - nível de rastreamento 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:
```

## Resolução

- O erro visto no trecho de log, 'Não foi possível analisar o certificado: java.io.IOException: Dados incompletos', indica que o conteúdo 'Certificado do Provedor de Identidade' não foi inserido corretamente
- Para resolver isso: no AS FS Management > AD FS > Service > Certificates > Token-Signing > Export this certificate > abra em um editor de texto > copie todo o conteúdo > cole em 'Identity provider certificate' arquivado na configuração do SSO > Save.
- Consulte a configuração do "Certificado do Provedor de Identidade" na seção "Configuração do logon único do Agente - Provedor de Identidade" (Etapa 15).

## Cenário de Identificação e Solução de Problemas 3

### Erro

- Código do erro: 401-114
- Descrição do erro: identidade do usuário não encontrada no atributo SAML.

### Análise de log

#### Logs do servidor de aplicativos - nível de rastreamento 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:110)  
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Handler.java:120)  
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.OpenIDConnect_Handler.validateReqWithAttributes(OpenIDConnect_Handler.java:140)  
at com.egain.platform.module.security.sso.admin.SSOAdministrator.validateRequestWithAttributes(SSOAdministrator.java:150)  
at com.egain.platform.module.security.sso.controller.SSOControllerServlet.doPost(SSOControllerServlet.java:160)  
.  
.  
.  
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 <@>

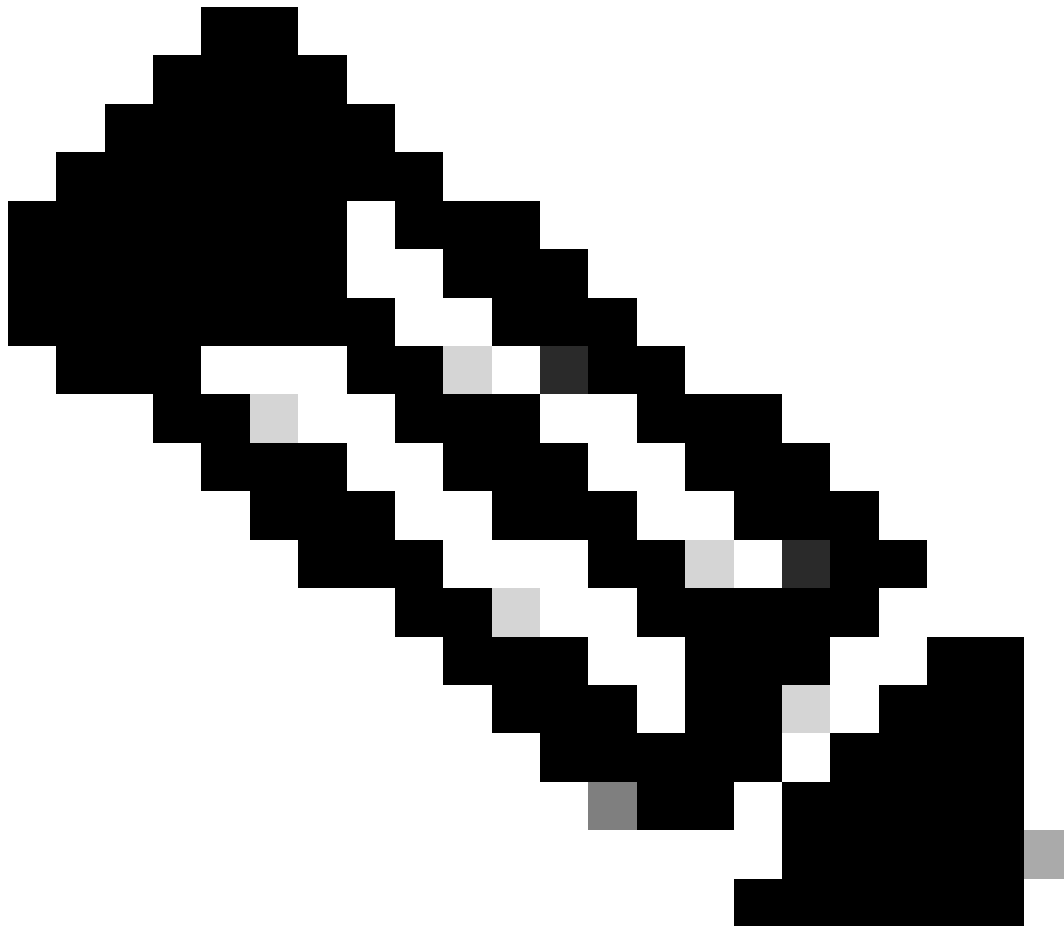
## Resolução

- Este erro indica um problema/incompatibilidade de configuração nos campos 'User Identity Location' e 'User Identity Attribute Name'.
- Verifique e corrija o 'User Identity Location' e o 'User Identity Attribute Name' no console de administração ECE, em Single Sign-On > Configurations > no menu suspenso Select Configuration, selecione Agent > guia SSO Configuration > Identify Provider (Etapa 15).

## Informações Relacionadas

Estes são os documentos principais que você deve revisar cuidadosamente antes de iniciar qualquer instalação ou integração ECE. Esta não é uma lista completa de documentos ECE.

---



---

Note:

- A maioria dos documentos ECE tem duas versões. Certifique-se de fazer o download e usar as versões que são para o PCCE. O título do documento é para o Packaged Contact Center Enterprise ou (para PCCE) ou (para UCCE e PCCE) após o número da versão.
  - Verifique a página inicial da documentação do Cisco Enterprise Chat and Email para obter atualizações antes de qualquer instalação, atualização ou integração.
  - <https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html>
- 

ECE versão 12.6(1)

- [Guia do administrador de e-mail e bate-papo corporativo](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.