

Versão 2.0 AD FS Setup para o exemplo de configuração de SAML SSO

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Transfira Metadados do provedor de identidade da versão 2.0 AD FS \(IdP\)](#)

[Transfira Metadados do Collaboration Server \(SP\)](#)

[CUCM IM e serviço de presença](#)

[Conexão de unidade](#)

[Abastecimento da Colaboração da primeira de Cisco](#)

[Adicionar CUCM como a confiança de confiança do partido](#)

[Adicionar CUCM IM e presença como a confiança de confiança do partido](#)

[Adicionar UCXN como a confiança de confiança do partido](#)

[Adicionar o abastecimento principal da Colaboração de Cisco como a confiança de confiança do partido](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar a versão 2.0 do serviço de federação do diretório ativo (AD FS) a fim de permitir o uso da linguagem de marcação de afirmação de Segurança (SAML) escolhendo Sinal-em (SSO) para os produtos de colaboração do Cisco como o gerente das comunicações unificadas do Cisco (CUCM), o Cisco Unity Connection (UCXN), o CUCM IM e a presença, e a Colaboração principal do Cisco.

Pré-requisitos

Requisitos

A versão 2.0 AD FS deve ser instalada e testada.

Caution: Este Guia de Instalação é baseado em uma instalação de laboratório e a versão 2.0 AD FS é suposta para ser usada somente para SAML SSO com produtos de colaboração do Cisco. Caso que é usada por outros aplicativos business-critical, a seguir a personalização necessária deve ser feita conforme a documentação Microsoft oficial.

[Componentes Utilizados](#)

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

- Versão 2.0 AD FS
- Microsoft Internet explorer 10
- Versão 10.5 CUCM
- Cisco IM e versão de servidor 10.5 da presença
- Versão 10.5 UCXN
- Abastecimento 10.5 da Colaboração da prima de Cisco

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Transfira Metadata do fornecedor da identidade da versão 2.0 AD FS (IdP)

A fim transferir metadata de IdP, execute este link em você navegador: [https:// <FQDN de ADFS>/FederationMetadata/2007-06/FederationMetadata.xml](https://<FQDN de ADFS>/FederationMetadata/2007-06/FederationMetadata.xml).

Metadata do Collaboration Server da transferência (SP)

CUCM IM e serviço da presença

Abra um navegador da Web, log em CUCM como o administrador, e navegue ao **sistema > sinal de SAML** ao único sobre.

Conexão de unidade

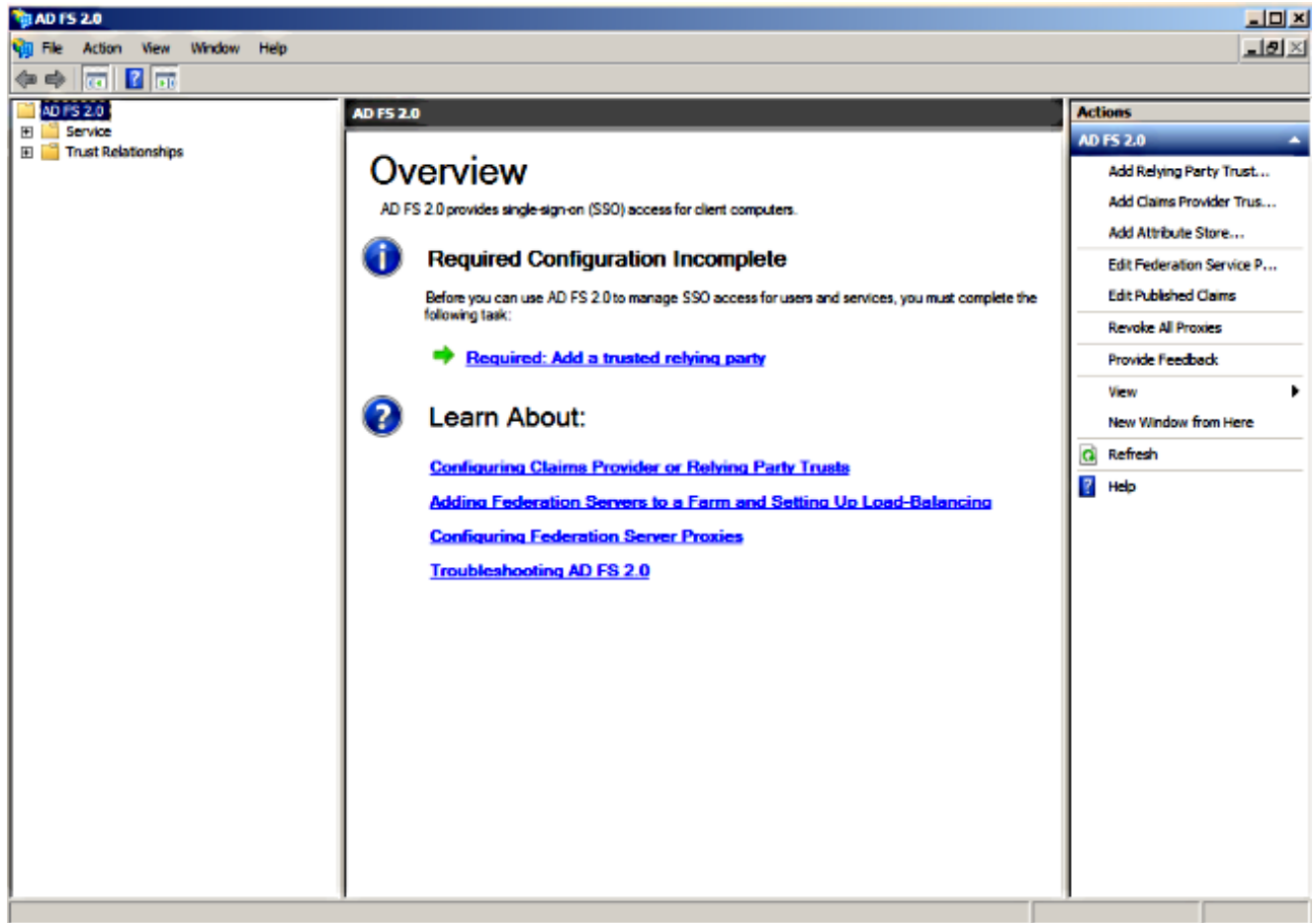
Abra um navegador da Web, log em UCXN como o administrador, e navegue às **configurações de sistema > sinal de SAML** ao único sobre.

Abastecimento da Colaboração da prima de Cisco

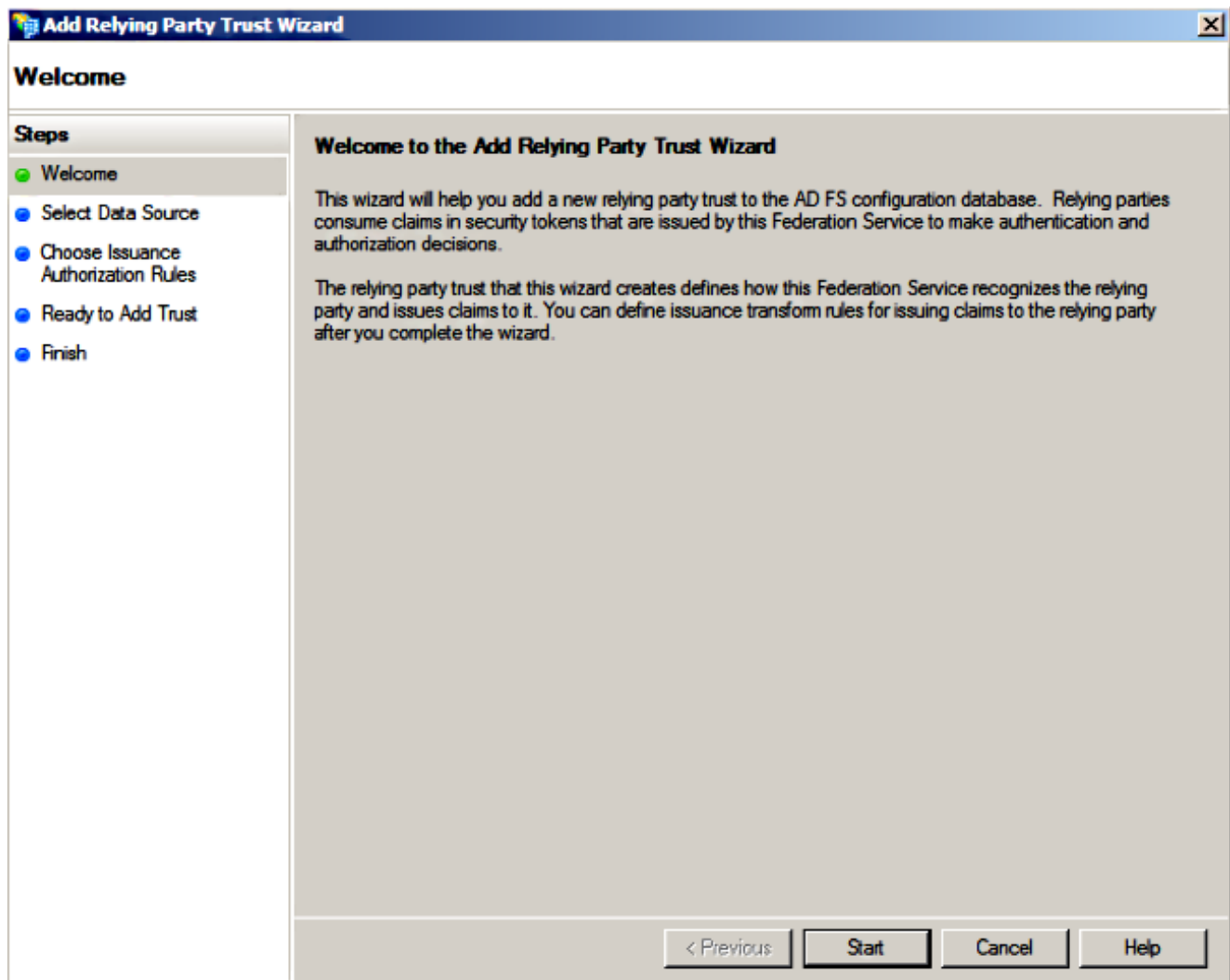
Abra um navegador da Web, log no credenciais principal da Colaboração como o globaladmin, e navegue à **administração > ao sistema Setup > único sinal** sobre.

Adicionar CUCM como a confiança de confiança do partido

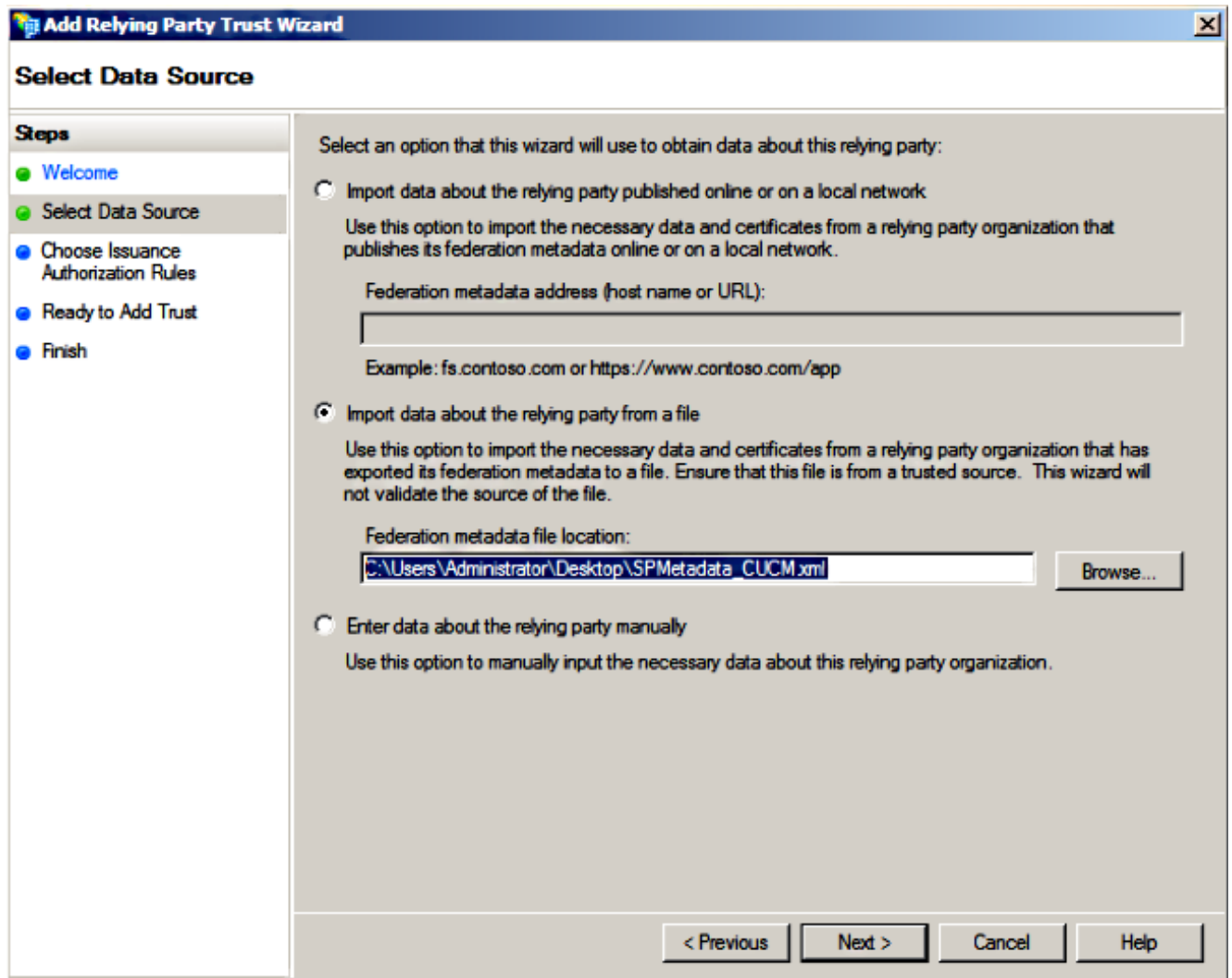
1. O log na versão 2.0 do server e do lançamento AD FS AD FS de Microsoft Windows programa o menu.
2. Seleto **adicionar a confiança de confiança do partido**.



3. Clique em Iniciar.



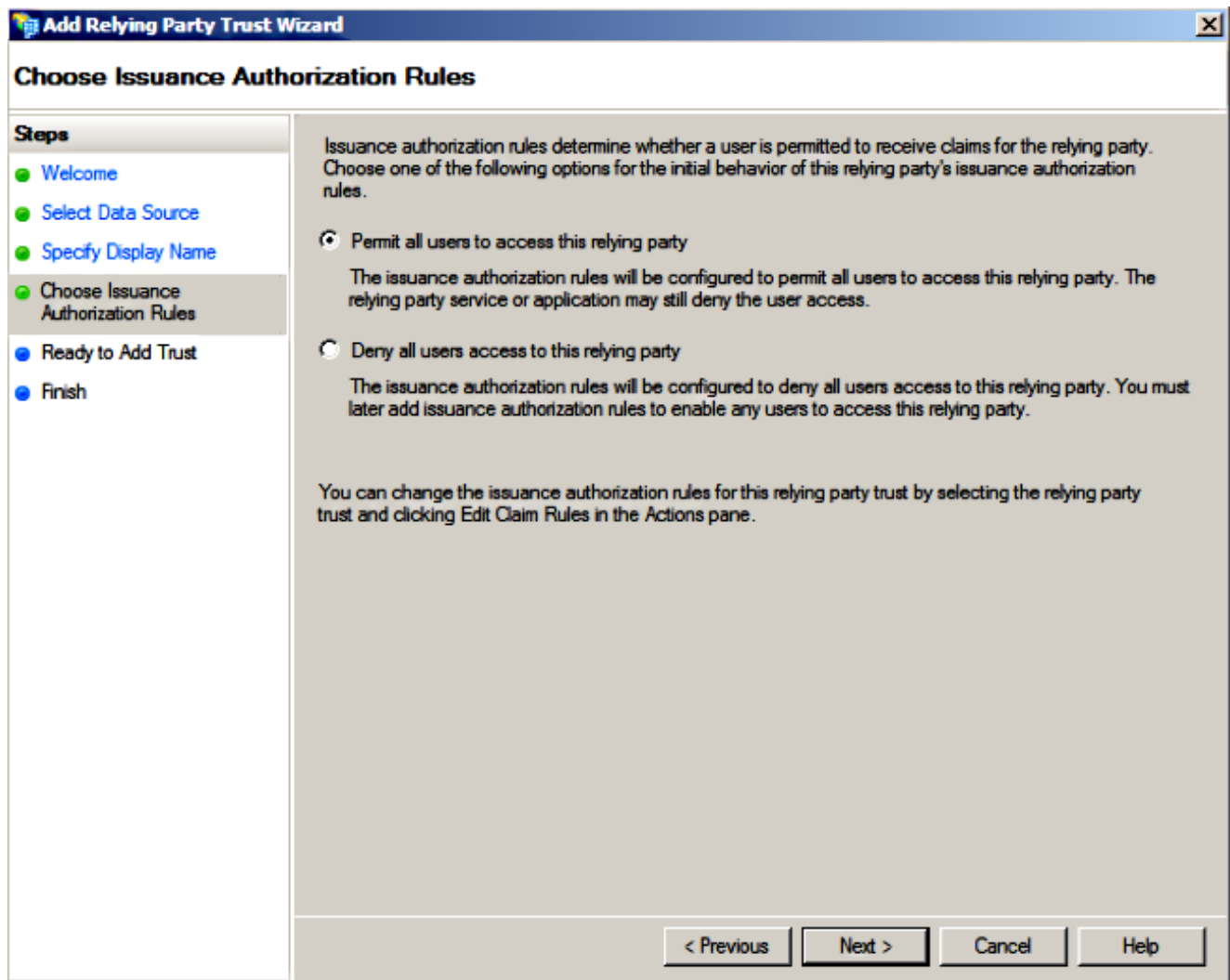
4. Selecione os dados da importação sobre o partido de confiança de uma opção de arquivo, escolha o arquivo dos metadata `SPMetadata_CUCM.xml` que você transferiu de CUCM mais cedo, e clique-o em seguida.



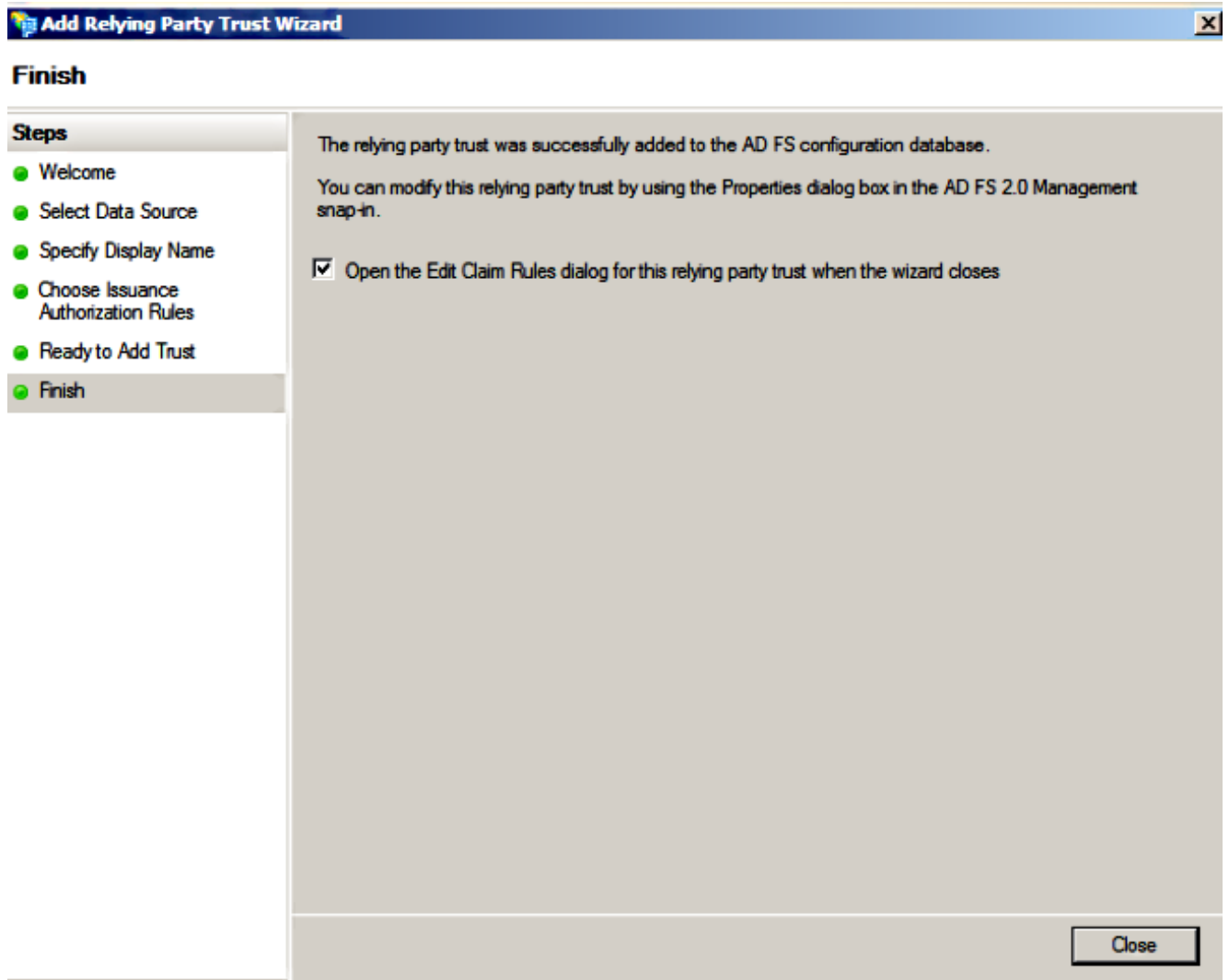
5. Dê entrada com o nome do indicador e clique-o em seguida.

The image shows a Windows-style dialog box titled "Add Relying Party Trust Wizard". The main title bar is blue with the text "Add Relying Party Trust Wizard" and a close button (X) on the right. Below the title bar, the dialog is titled "Specify Display Name". On the left side, there is a "Steps" pane with a list of steps: "Welcome", "Select Data Source", "Specify Display Name" (which is highlighted in grey), "Choose Issuance Authorization Rules", "Ready to Add Trust", and "Finish". The main area of the dialog contains the instruction "Type the display name and any optional notes for this relying party." Below this, there is a "Display name:" label followed by a text input field containing the text "CUCM". Underneath the input field is a "Notes:" label followed by a text area containing the text "Adding CUCM as Relaying Party to ADFS". At the bottom of the dialog, there are four buttons: "< Previous", "Next >", "Cancel", and "Help".

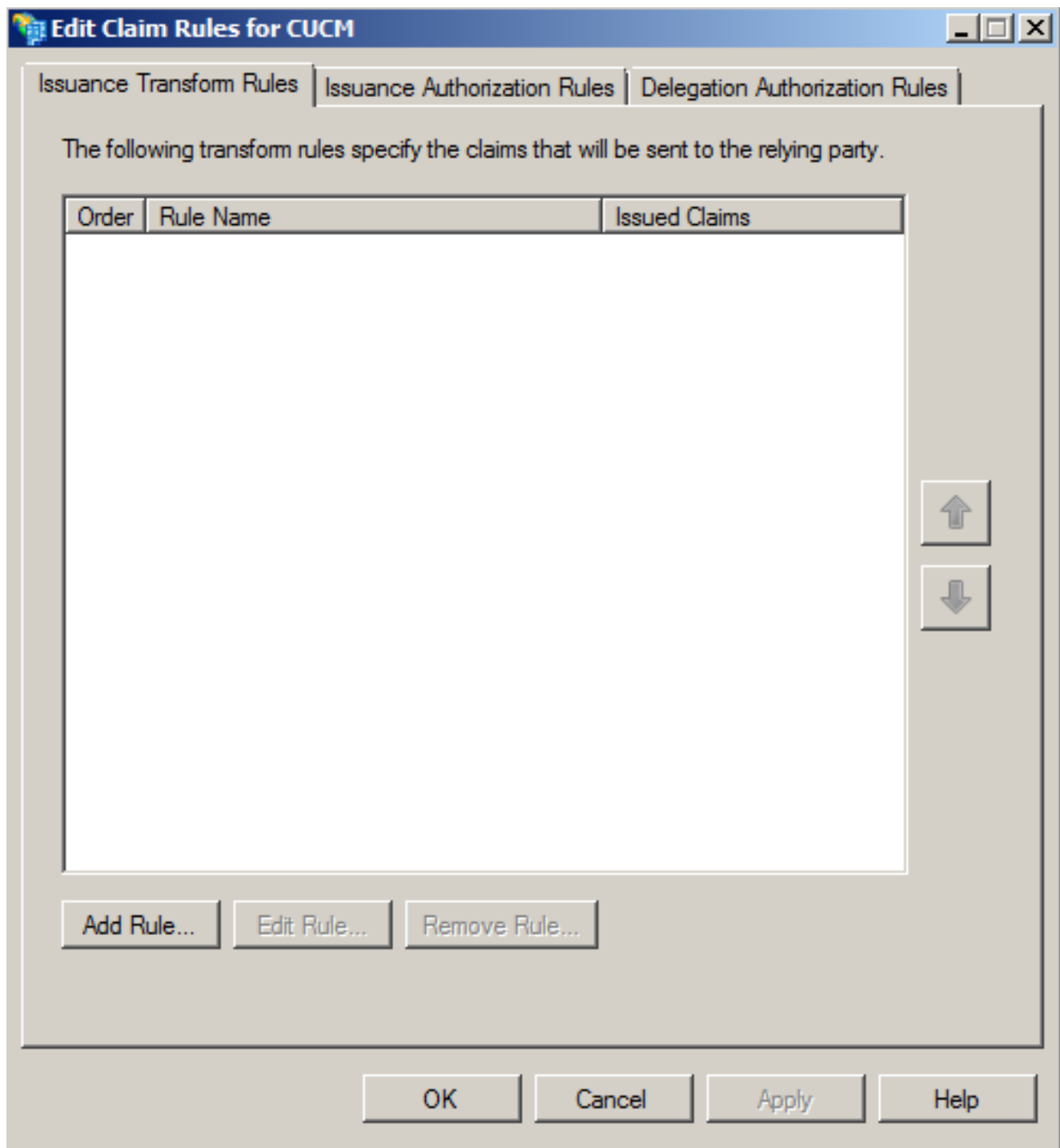
6. Escolha a licença todos os usuários para alcançar este partido de confiança e para clicá-lo em seguida.



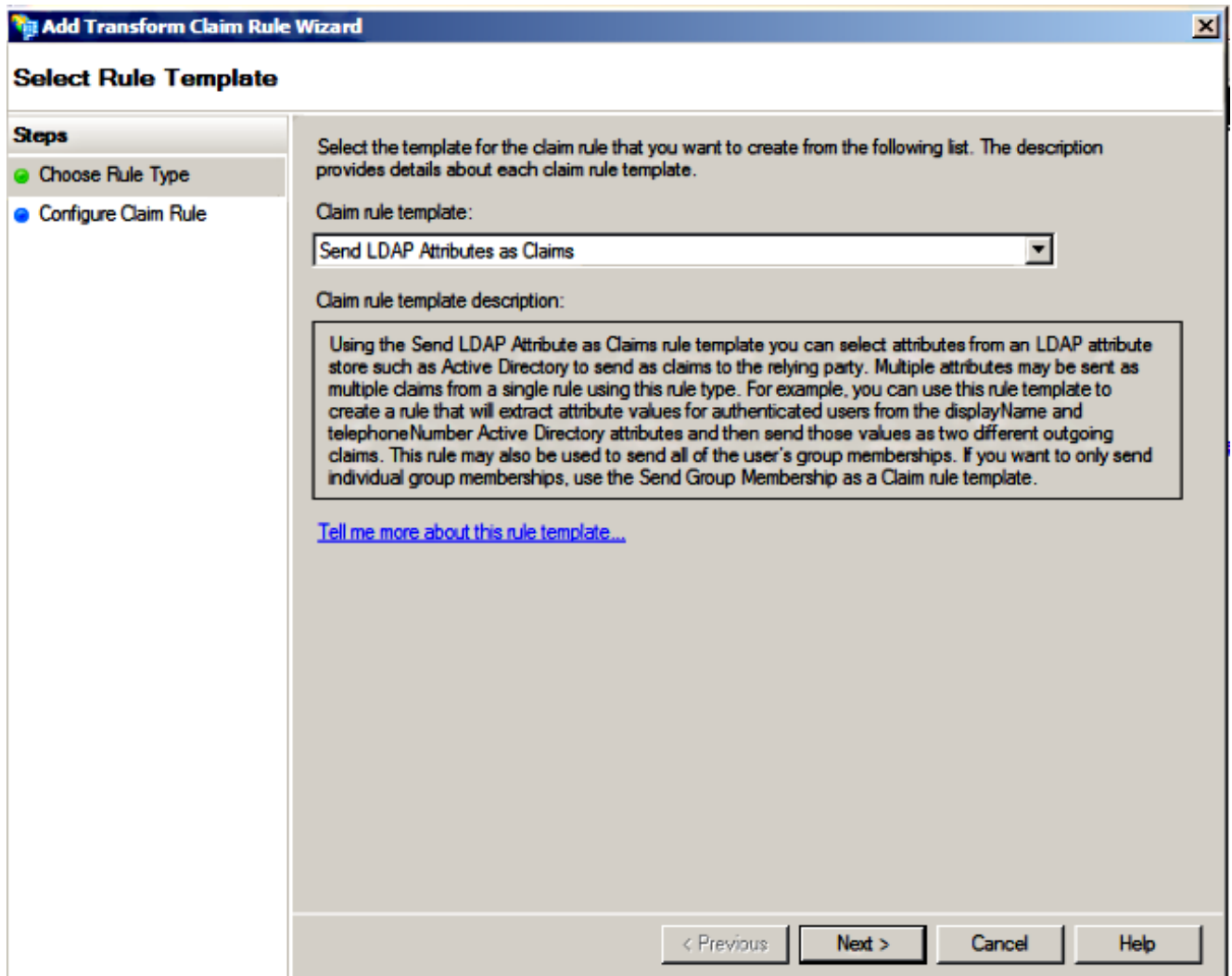
7. Selecione **aberto** o diálogo das regras da reivindicação da edição para a confiança de confiança do partido do thee quando o assistente se fecha e clique-o **perto**.



8. O clique adiciona a regra.



9. Clique **em seguida** com grupo do molde da regra da reivindicação do padrão **para enviar atributos LDAP como reivindicações**.



10. Em configurar a regra, dê entrada com o nome da regra da reivindicação, **diretório ativo** selete como a loja do atributo, configura o **atributo LDAP** e **tipo que parte da reivindicação** segundo as indicações desta imagem, e clique o **revestimento**.

Note:

- O atributo do Lightweight Directory Access Protocol (LDAP) deve combinar o atributo da sincronização do diretório em CUCM.
- o "uid" deve estar na caixa baixa.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
Name ID

Rule template: Send LDAP Attributes as Claims

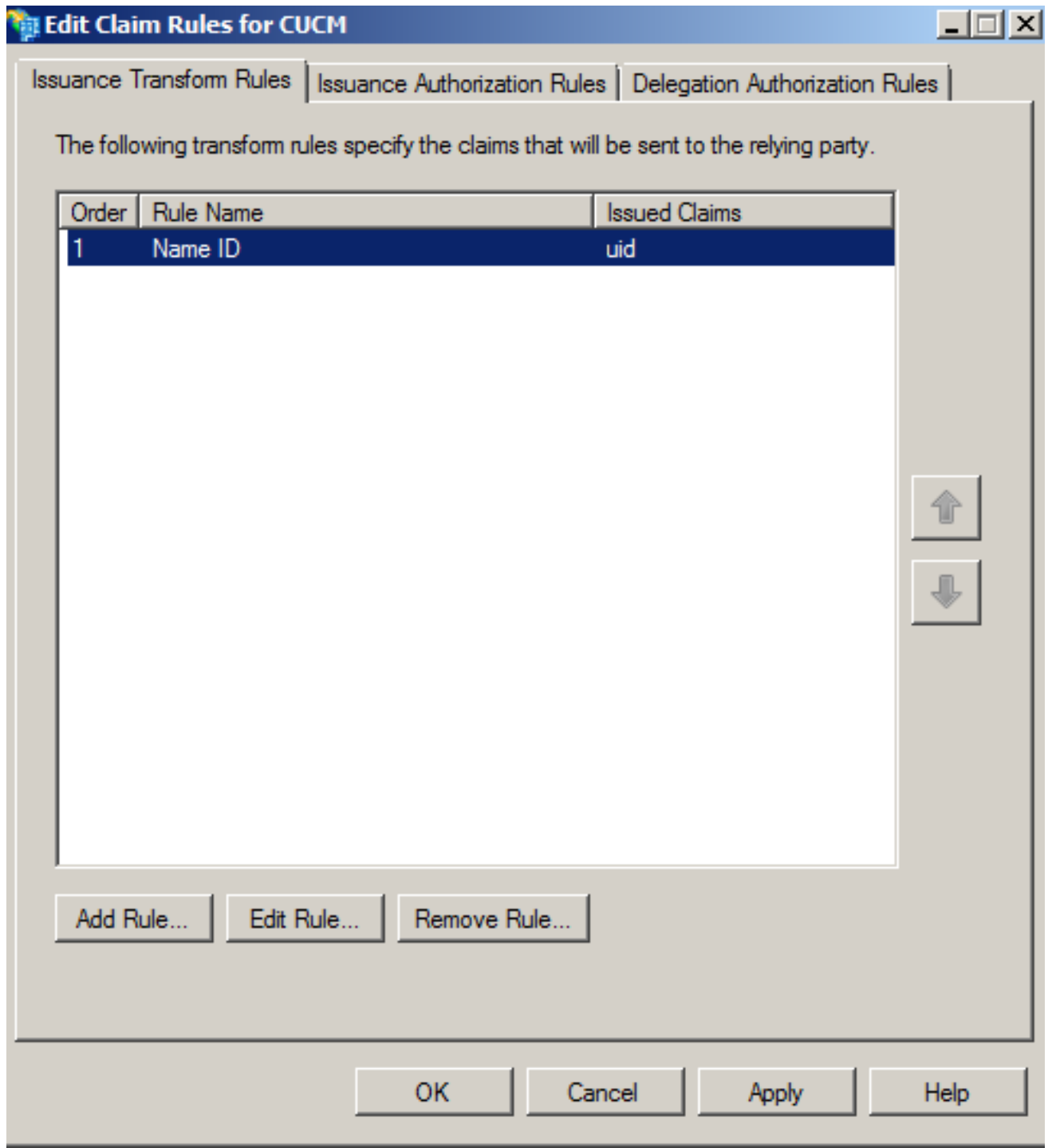
Attribute store:
Active Directory

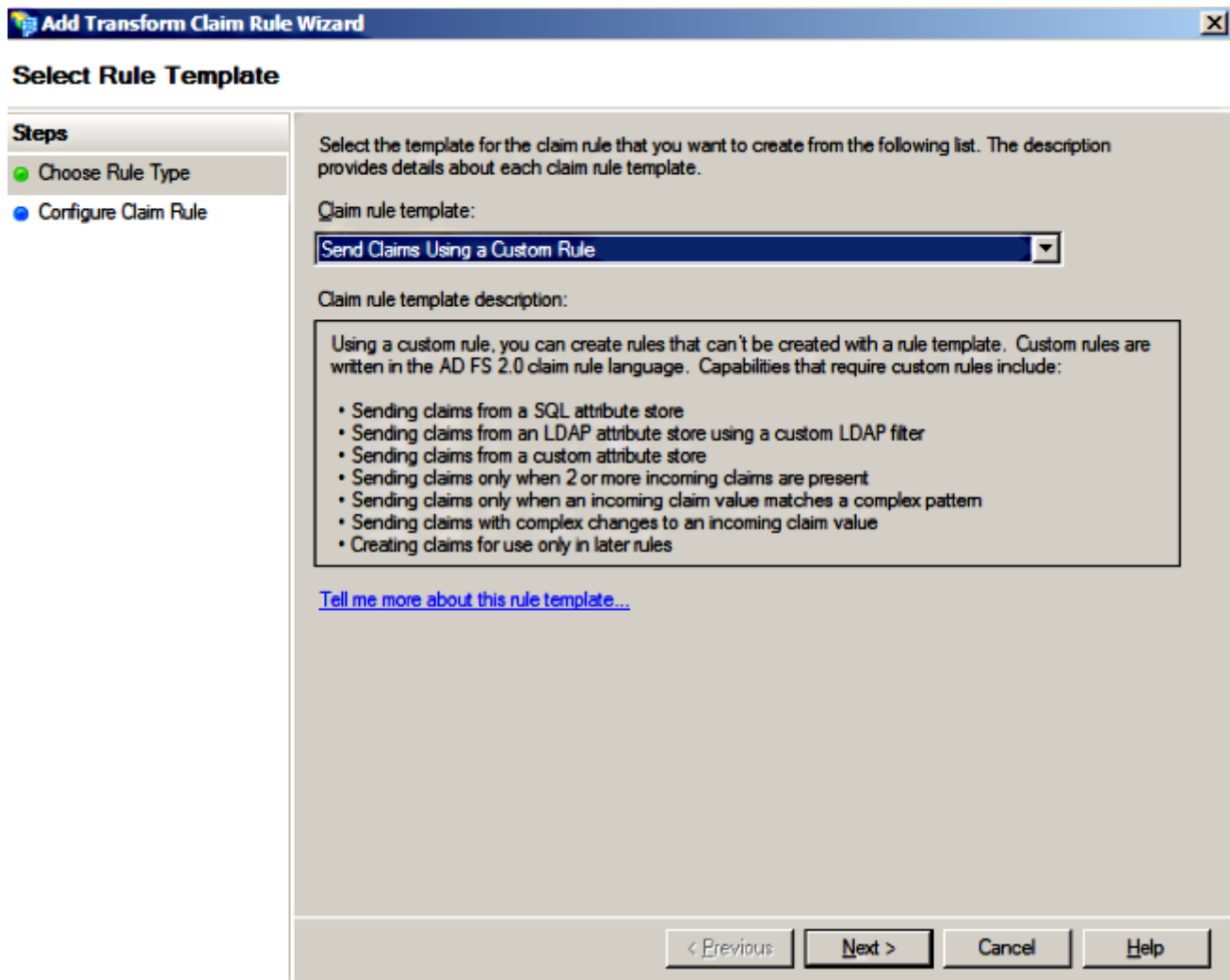
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
▶	SAM-Account-Name	uid
*		

< Previous Finish Cancel Help

11. O clique adiciona a regra, seleta envie reivindicações usando uma regulamentação aduaneira enquanto o molde da regra da reivindicação, e as clique em seguida.

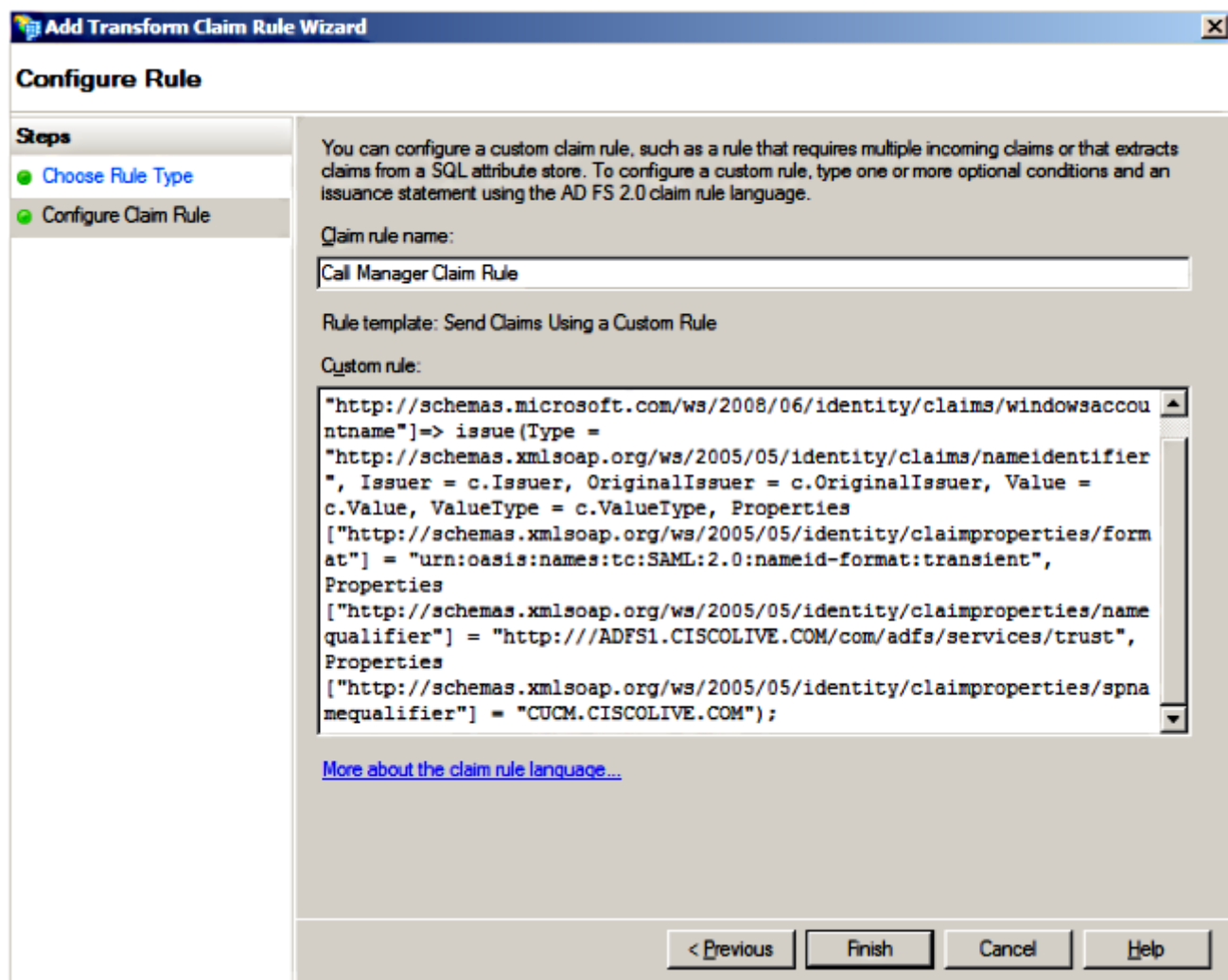




12. Dê entrada com um nome para o nome da regra da reivindicação e copie esta sintaxe no espaço dado sob a regulamentação aduaneira:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
= "http://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier
"] = "<FQDN of CUCM>");
```

(NOTA: Se você copia e cola o texto destes exemplos, esteja ciente que algum software do processamento de texto substituirá a cotação ASCII - identificar (") por meio das versões de UNICODE ("). As versões de UNICODE farão com que a regra da reivindicação falhe.)



Note:

- O nome de domínio totalmente qualificado CUCM e ADFS (FQDN) prepopulated com o laboratório CUCM e AD FS neste exemplo e deve ser alterado para combinar seu ambiente.
- o FQDN de CUCM/ADFS é diferenciando maiúsculas e minúsculas e deve combinar com os arquivos dos metadata.

13. Clique em Finish.

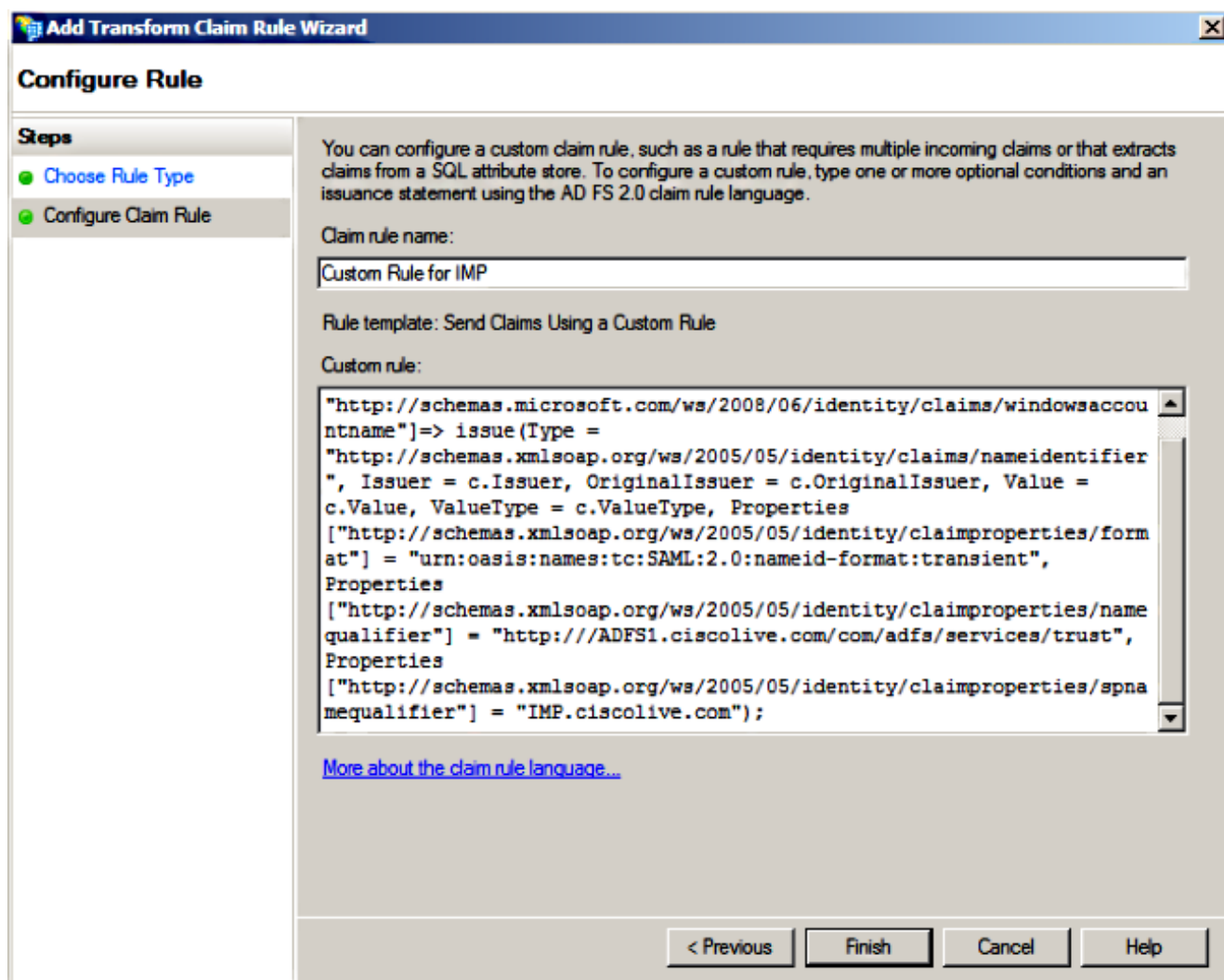
14. O clique **aplica-se** e **APROVA-SE** então.

15. Reinicie o serviço da versão 2.0 AD FS de **Services.msc**.

Adicionar CUCM IM e presença como a confiança de confiança do partido

1. Repita etapas 1 11 como descritos para Add CUCM como a confiança de confiança do **partido** e continue a etapa 2.
2. Dê entrada com um nome para o nome da regra da reivindicação e copie esta sintaxe no espaço dado sob a regulamentação aduaneira:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
= "http://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of IMP>");
```



Observe que IM e a presença e o FQDN AD FS prepopulated com o laboratório IM e a presença e o AD FS neste exemplo e devem ser alterados para combinar seu ambiente.

3. Clique em Finish.
4. O clique **aplica-se** e **APROVA-SE** então.
5. Reinicie o serviço da versão 2.0 AD FS de **Services.msc**.

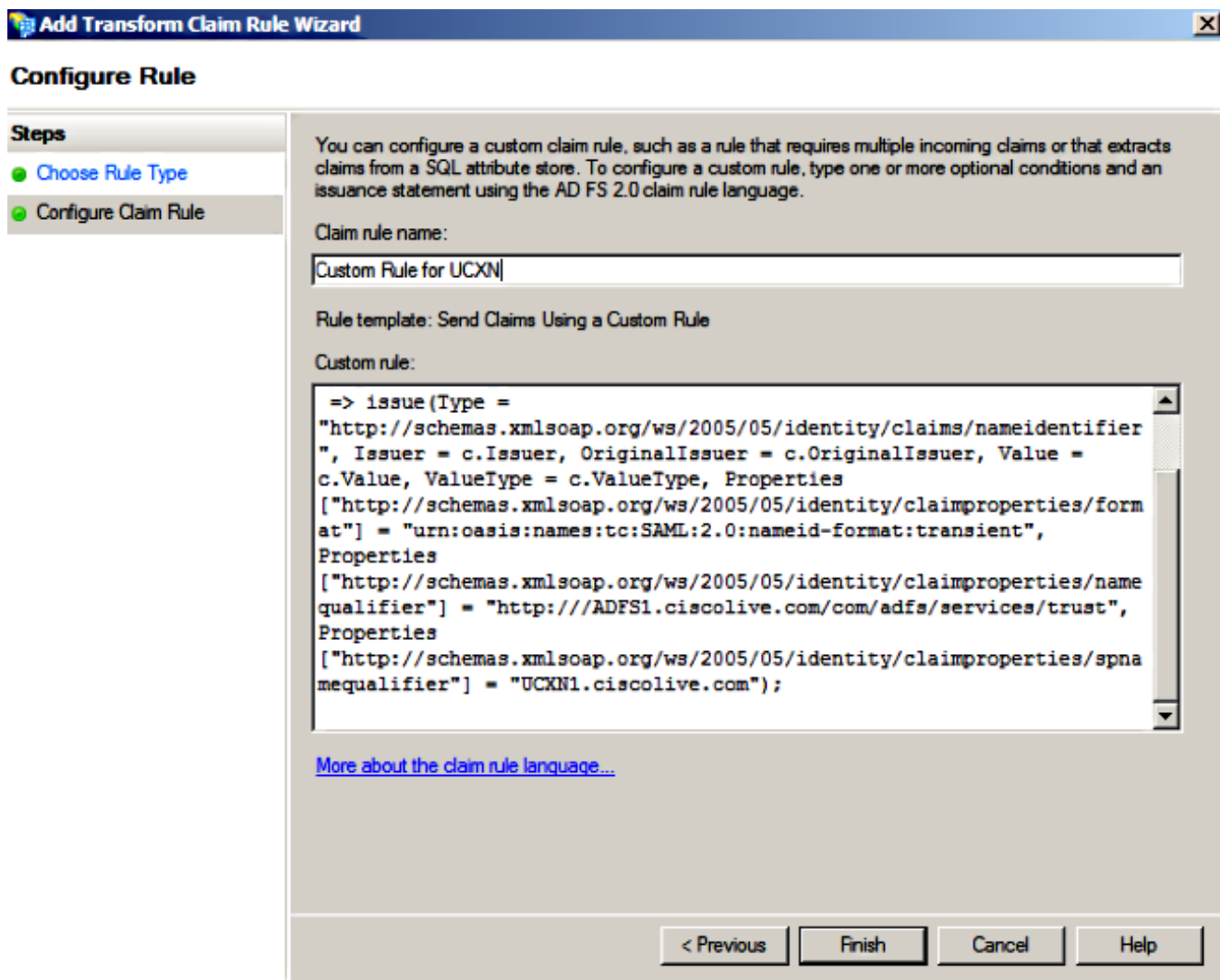
Adicionar UCXN como a confiança de confiança do partido

1. Repita etapas 1 12 como descritos para Add CUCM como a confiança de confiança do

partido e continue a etapa 2.

2. Dê entrada com um nome para o nome da regra da reivindicação e copie esta sintaxe no espaço dado sob a regulamentação aduaneira:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
= "http://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of UCXN>");
```



Observe que o FQDN UCXN e AD FS prepopulated com o laboratório UCXN e ADFS neste exemplo e deve ser alterado para combinar seu ambiente.

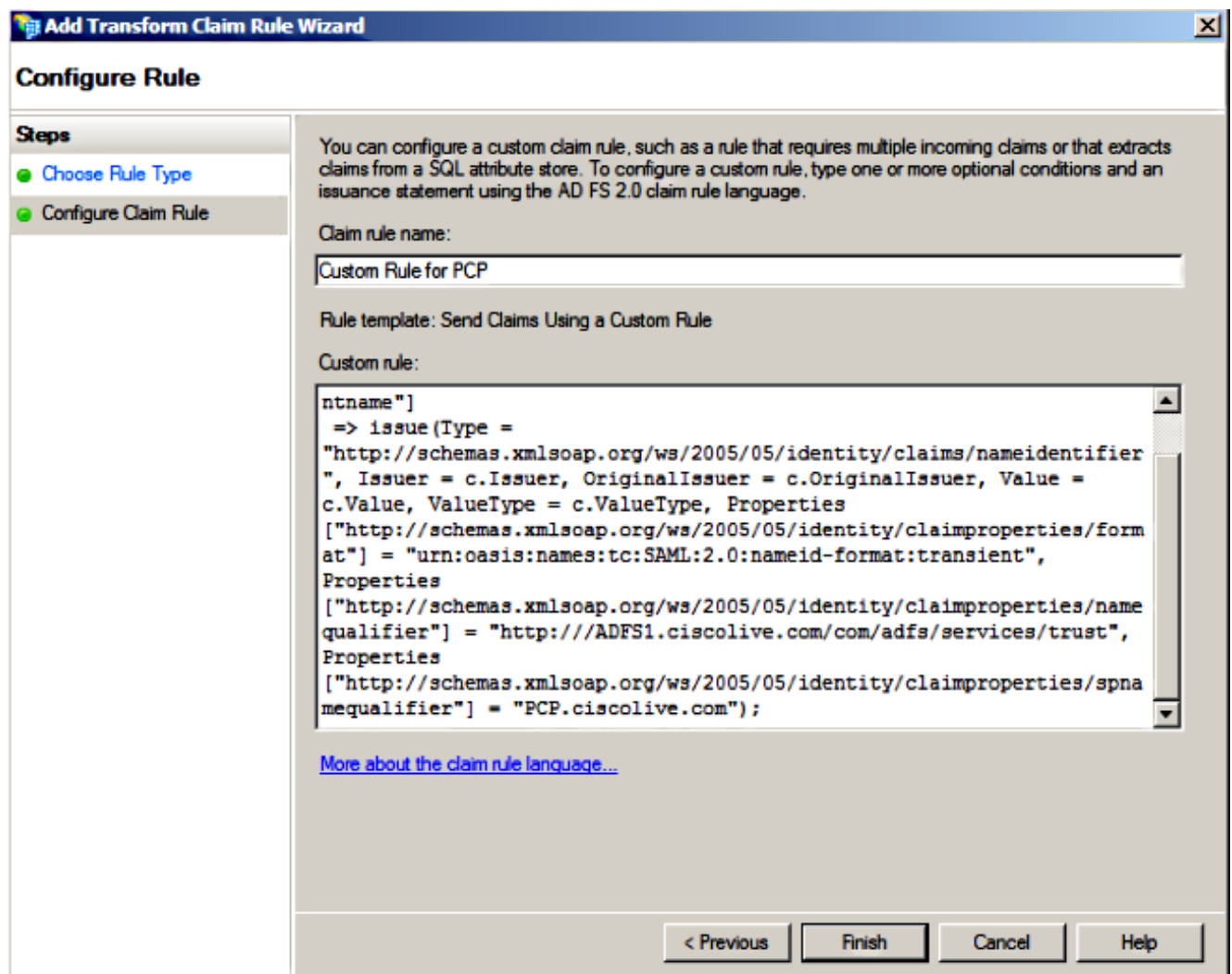
3. Clique em Finish.
4. O clique aplica-se e APROVA-SE então.

5. Reinicie o serviço da versão 2.0 AD FS de **Services.msc**.

Adicionar o abastecimento principal da Colaboração de Cisco como a confiança de confiança do partido

1. Repita etapas 1 12 como descritos para **Add CUCM como a confiança de confiança do partido** e continue a etapa 2.
2. Dê entrada com um nome para o nome da regra da reivindicação e copie esta sintaxe no espaço dado sob a regulamentação aduaneira:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
= "http://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of PCP>");
```



Observe que o abastecimento da prima e o FQDN AD FS prepopulated com o

abastecimento da Colaboração da prima do laboratório (PCP) e o AD FS deste exemplo e devem ser alterados para combinar seu ambiente.

3. Clique em Finish.
4. O clique **aplica-se** e **APROVA-SE** então.
5. Reinicie o serviço da versão 2.0 AD FS de **Services.msc**.

Uma vez que você estabelece a versão 2.0 AD FS, continue permitir SAML SSO no Produtos da colaboração do Cisco.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

O AD FS registra dados de diagnóstico ao log de evento do sistema. Do gerenciador do servidor no server AD FS abra **diagnósticos -> visualizador de eventos -> aplicativos e serviços -> AD FS 2.0 -> Admin**

Procure os erros registrados para a atividade AD FS

Level	Date and Time	Source	Event ID	Task Category
Information	6/28/2016 11:18:12 AM	AD FS 2.0	337	None
Information	6/28/2016 11:18:12 AM	AD FS 2.0	336	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	390	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	386	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	399	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	157	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	156	None
Information	6/27/2016 11:18:02 PM	AD FS 2.0	337	None
Information	6/27/2016 11:18:02 PM	AD FS 2.0	336	None
Information	6/27/2016 8:12:59 PM	AD FS 2.0	388	None
Error	6/27/2016 8:12:11 PM	AD FS 2.0	364	None
Error	6/27/2016 8:12:11 PM	AD FS 2.0	321	None
Information	6/27/2016 8:12:10 PM	AD FS 2.0	251	None
Information	6/27/2016 8:11:59 PM	AD FS 2.0	100	None

Event 321, AD FS 2.0

General | Details

The SAML authentication request had a NameID Policy that could not be satisfied.
Requestor: ciscouc-105-imps1.ciscouc.org
Name identifier format: urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Log Name: AD FS 2.0/Admin
Source: AD FS 2.0 Logged: 6/27/2016 8:12:11 PM
Event ID: 321 Task Category: None