Configurar Conexão/Contrato de IdP de SAML Única por Cluster com AD FS Versão 2.0

Contents

Introduction

Este documento descreve como configurar a conexão/o contrato do Provedor de Identidade (IdP) do SAML (Single Security Assertion Markup Language) por cluster com o AD FS (Ative Diretory Federation Service).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Communications Manager (CUCM) 11.5 ou posterior
- Cisco Unified Communications Manager IM and Presence versão 11.5 ou posterior
- Ative Diretory Federation Service versão 2.0

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Ative Diretory Federation Service versão 2.0 como IdP
- Cisco Unified Communications Manager versão 11.5
- Cisco IM and Presence Server versão 11.5

Informações de Apoio

Para o SSO SAML, precisa ser um círculo de confiança entre o provedor de serviços (SP) e o IdP. Essa confiança é criada como parte do SSO Enablement, quando a confiança (metadados) é trocada. Baixe os Metadados do CUCM e faça o upload para o IdP, faça o download dos metadados do IdP e faça o upload para o CUCM.

Antes do CUCM 11.5, o nó de origem gera o arquivo de metadados, além de coletar os arquivos de metadados de outros nós no cluster. Ele adiciona todos os arquivos de metadados a um único arquivo zip e apresenta ao administrador. O administrador precisa descompactar esse arquivo e provisionar cada arquivo no IdP. Por exemplo, 8 arquivos de metadados para um cluster de 8 nós.

Um único contrato/conexão de IdP SAML por recurso de cluster é apresentado a partir de 11.5. Como parte desse recurso, o CUCM gera um único arquivo de metadados do provedor de serviços para todos os nós CUCM e IMP no cluster. O novo formato de nome para o arquivo de metadados é **<hostname>-single-agreement.xml**

Basicamente, um nó cria os Metadados e os envia para outros nós de SP no cluster. Isso facilita o provisionamento, a manutenção e o gerenciamento. Por exemplo, 1 arquivo de metadados para um cluster de 8 nós.

O arquivo de metadados do cluster wide usa o certificado de tomcat de multiservidor que garante que o par de chaves seja usado para todos os nós no cluster. O arquivo de metadados também tem uma lista de urls do Serviço de consumidor de asserção (ACS) para cada nó no cluster.

CUCM e Cisco IM and Presence versão 11.5 Suporta os Modos SSO, **em todo o cluster** (um arquivo de metadados por cluster) e por nó (modelo existente).

Este documento descreve como configurar o modo de cluster-wide do SSO SAML com AD FS 2.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Etapa 1. Exportar metadados SP do CUCM

Abra um navegador da Web, faça login no CUCM como administrador e navegue **paraSystem > SAML Single Sign On (Sistema > Logon único SAML).**

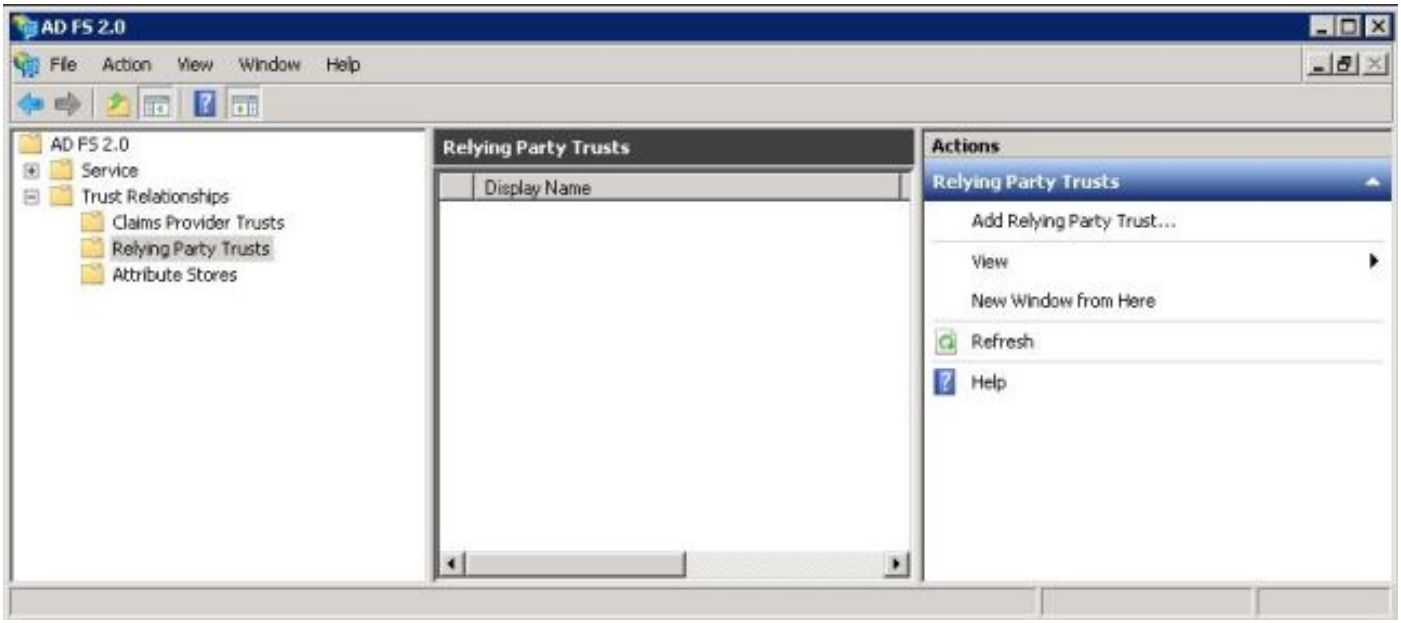
Por padrão, o botão de opção **Cluster Wide** está selecionado. Clique em **Exportar todos os metadados.** O arquivo de dados de metadados apresentado ao administrador no nome **<hostname>-single-agreement.xml**

Etapa 2. Transferir metadados IDP do AD FS

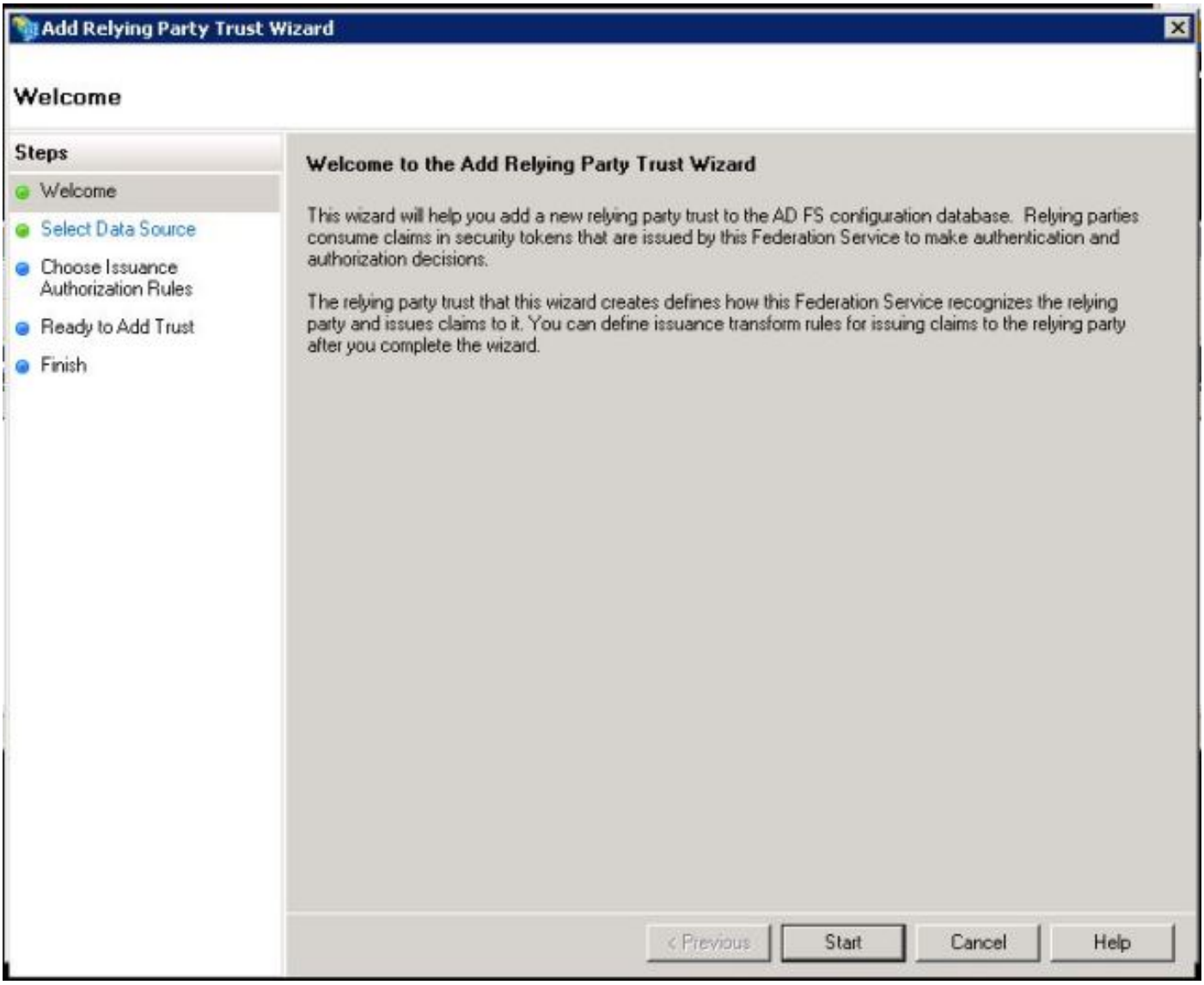
Para fazer o download dos metadados IdP, consulte o link https:// <FQDN do ADFS>/federationmetadata/2007-06/federationmetadata.xml

Etapa 3. Provisionar IdP

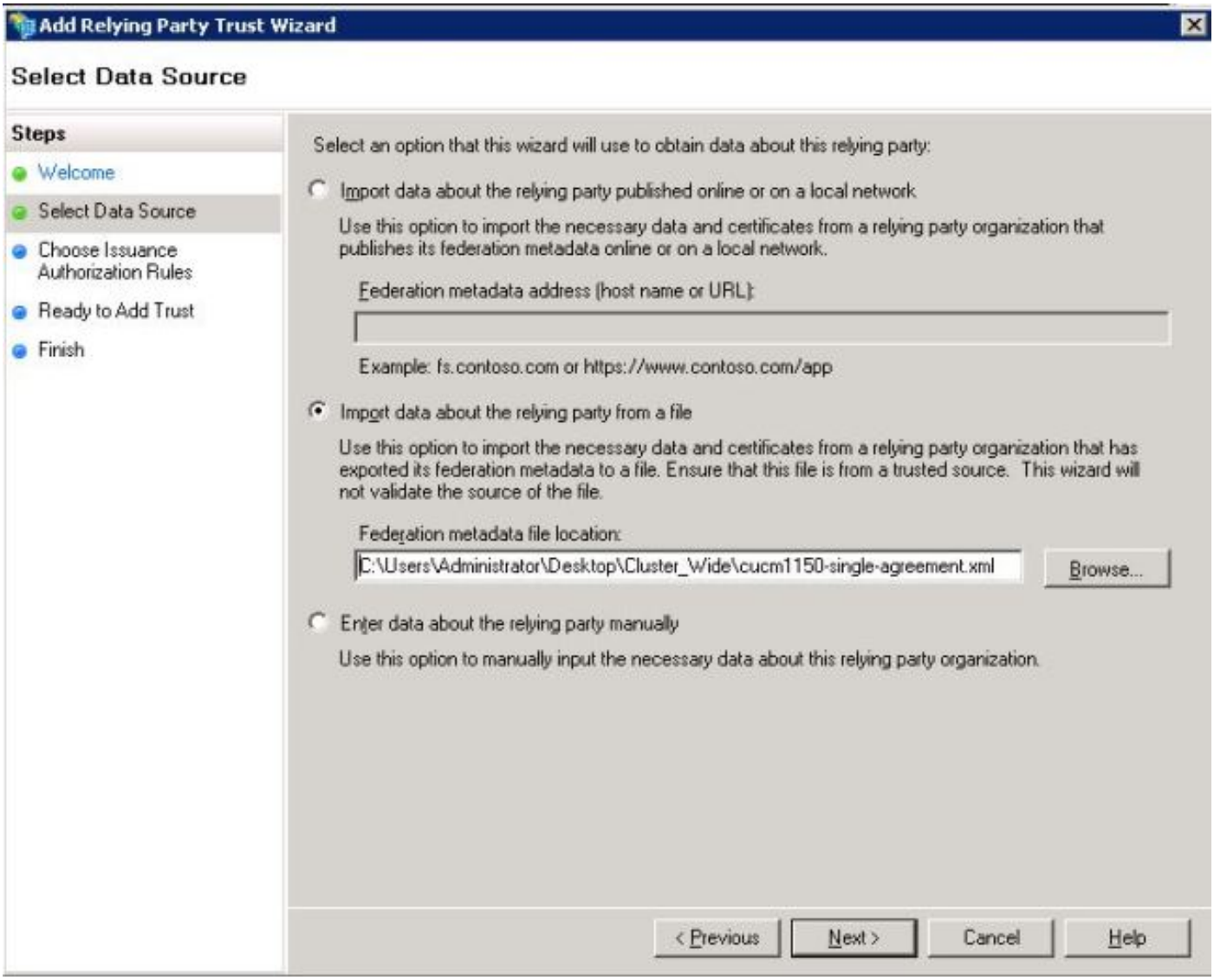
Como mostrado na imagem, navegue para **Gerenciamento do AD FS 2.0 / Confiança de Confiança / Envio de Relação de Confiança do AD FS 2.0**. Clique em **Adicionar confiança de terceira parte confiável**.



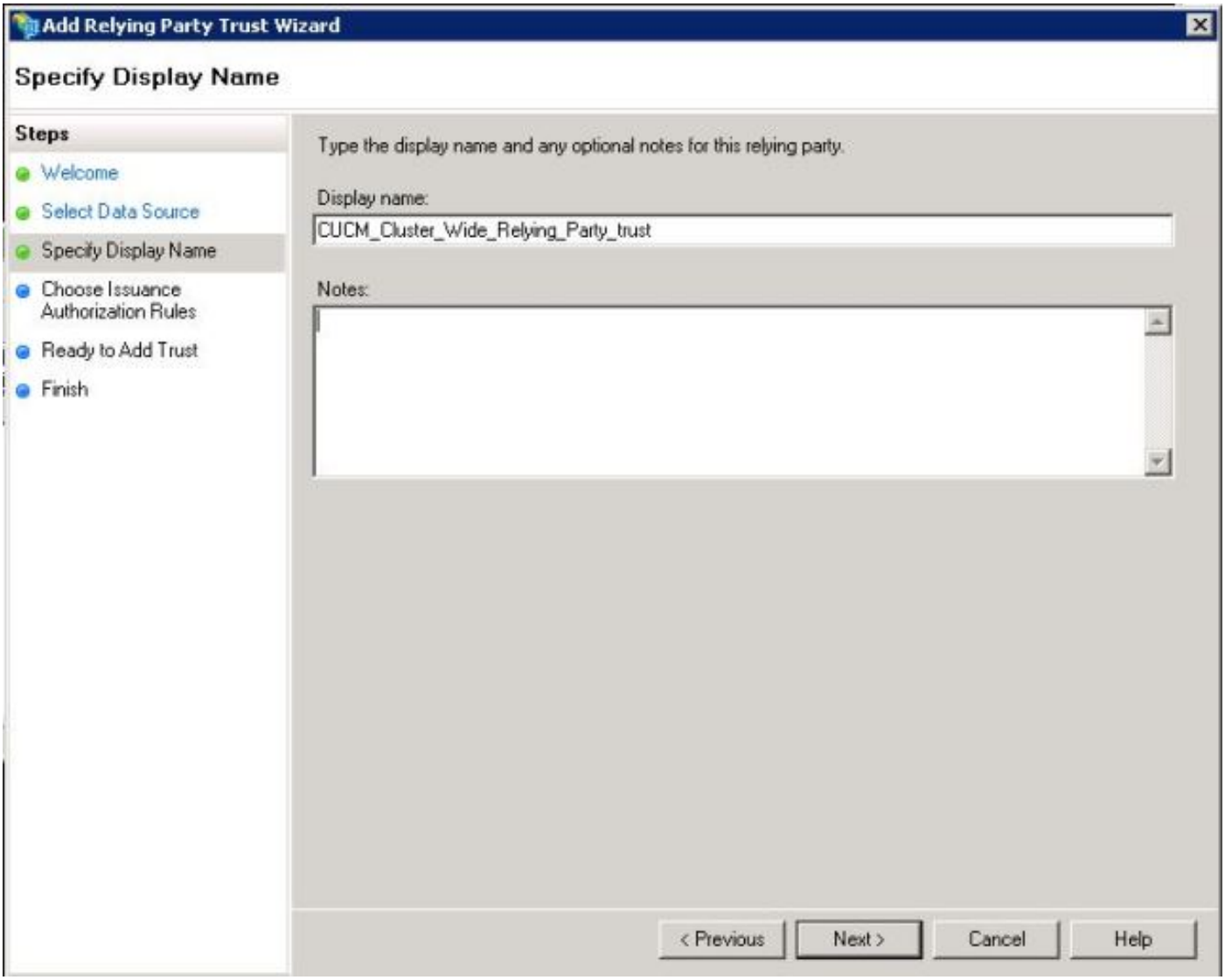
O Assistente para Adicionar Confiança de Terceiros Confiantes é aberto conforme mostrado na imagem e, agora, clique em **Iniciar**.



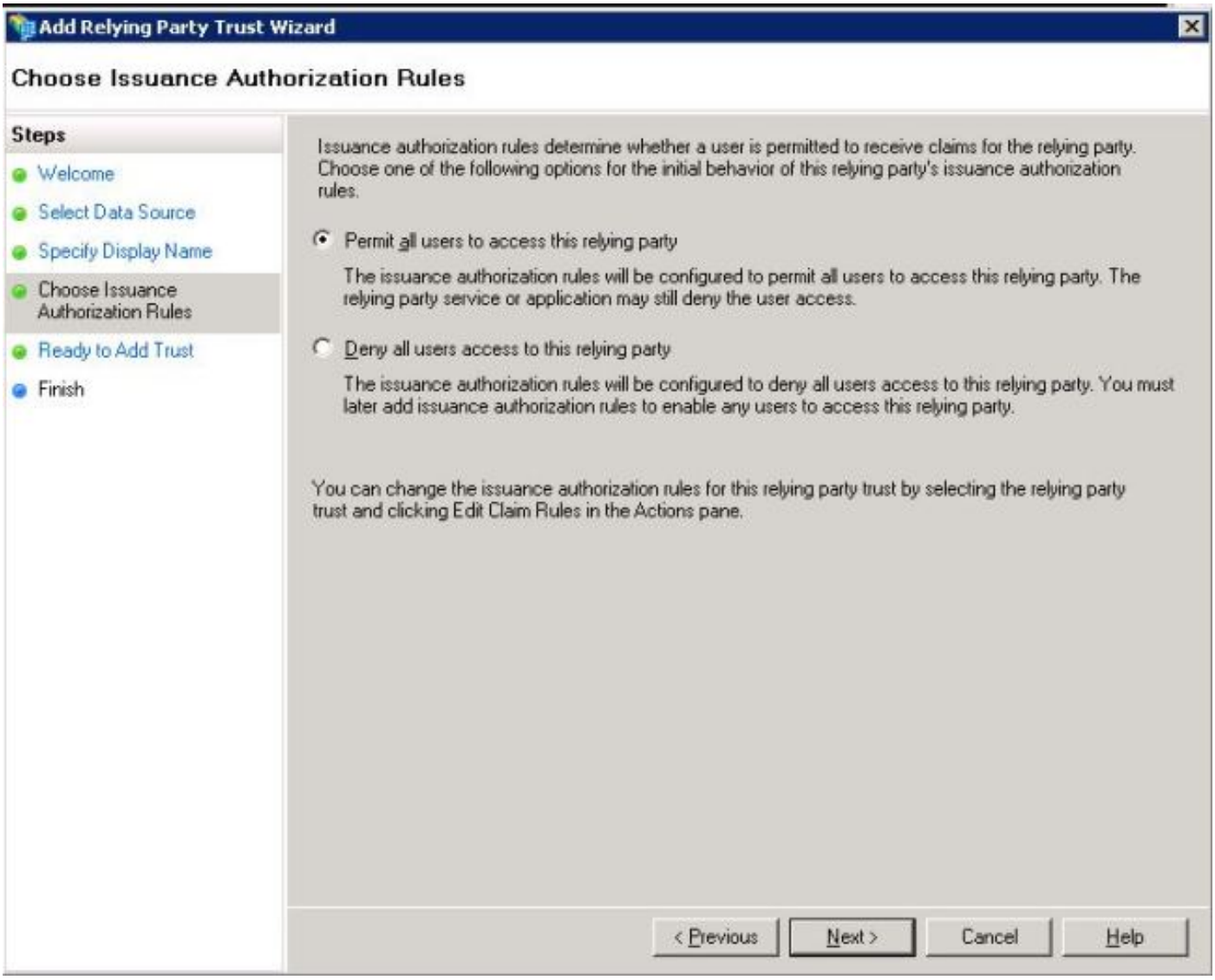
Clique nos dados de importação sobre a terceira parte confiável de um arquivo. Navegue pelos metadados SP baixados da página de configuração SSO do CUCM SAML. Em seguida, clique em **Avançar**, conforme mostrado na imagem:



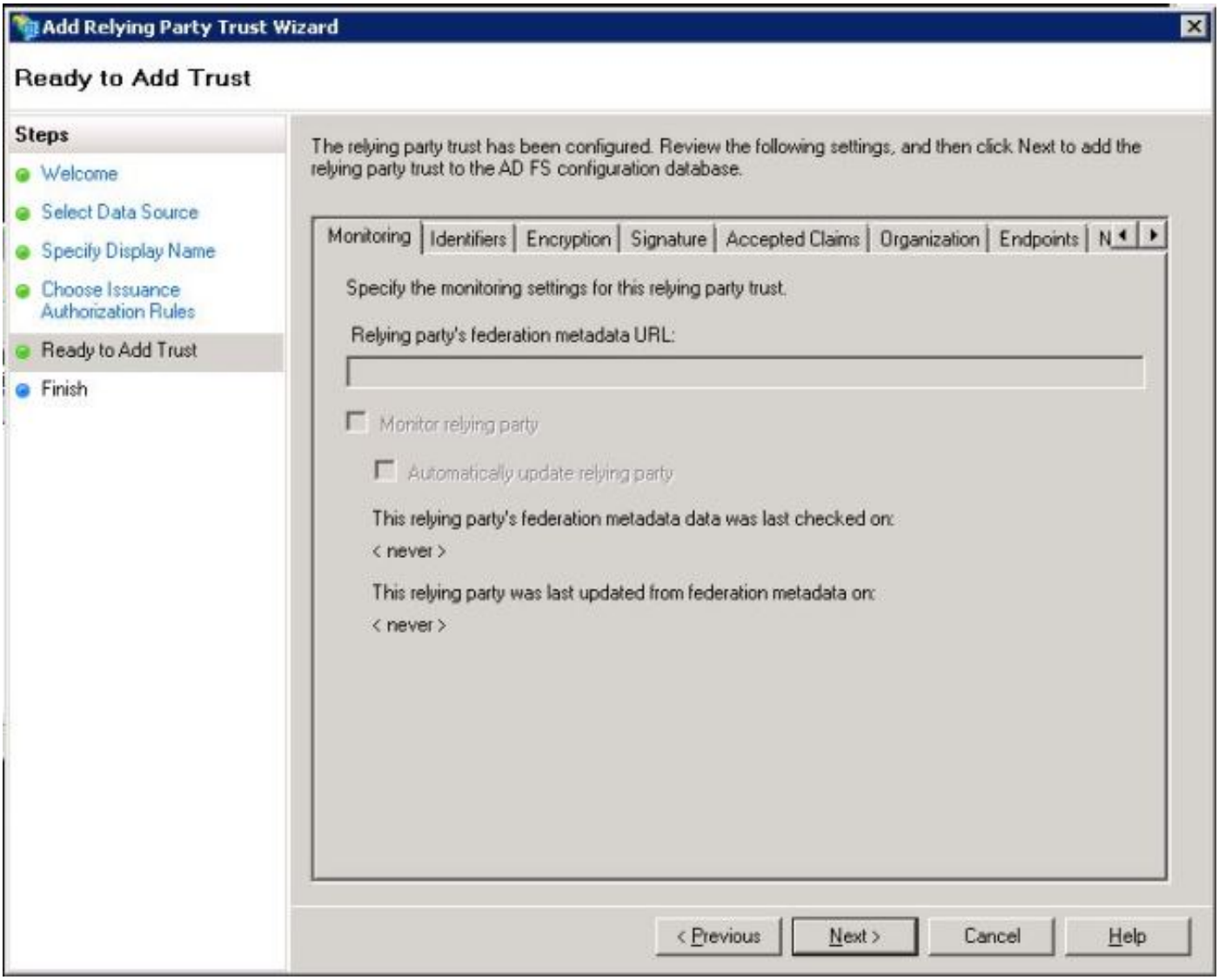
Digite o nome de exibição e todas as notas opcionais para a terceira parte confiável. Clique em **Avançar**, conforme mostrado na imagem:



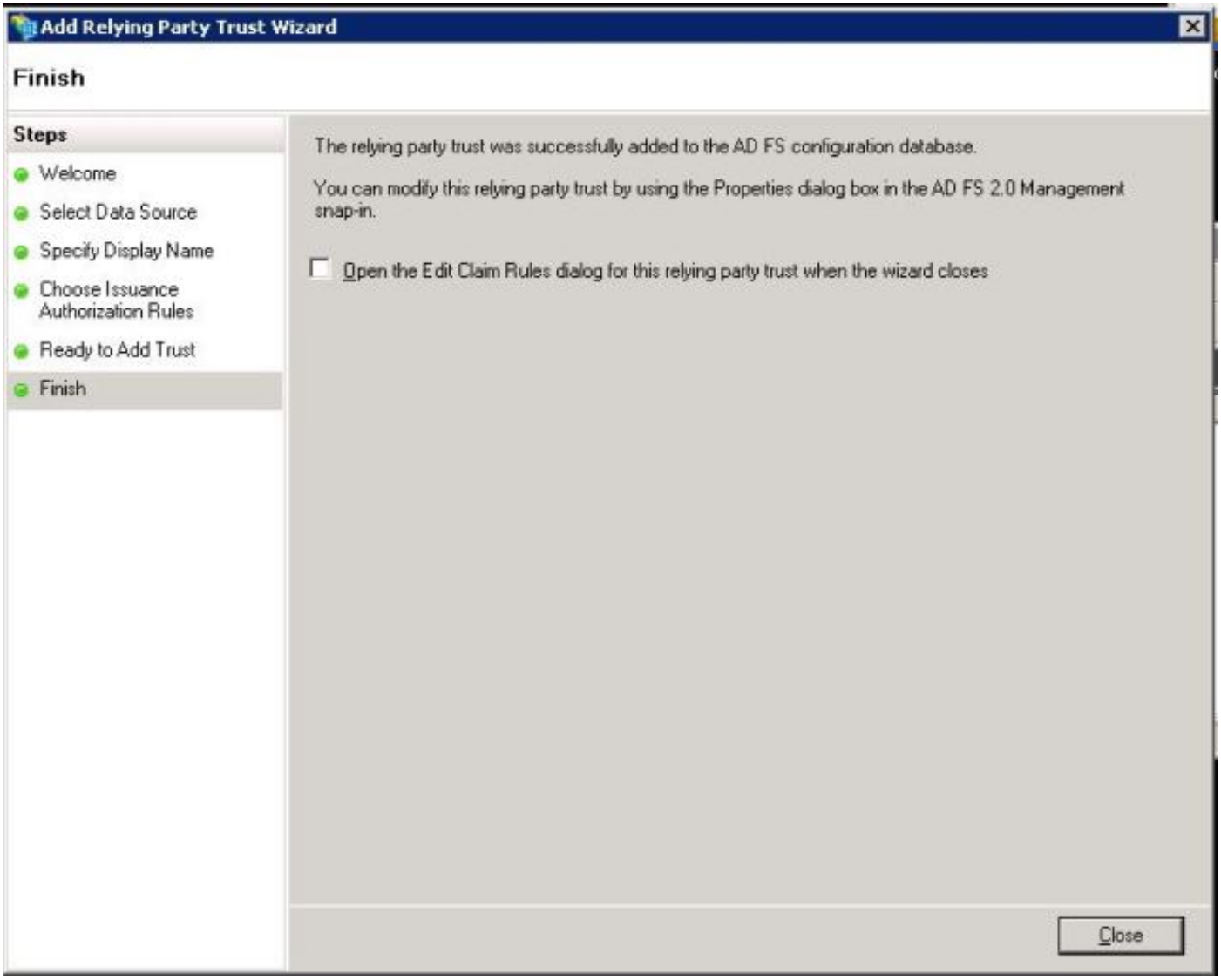
Selecione **Permitir que todos os usuários acessem esta terceira parte confiável** para permitir que todos os usuários acessem esta terceira parte confiável e clique em **Avançar**, como mostrado na imagem:



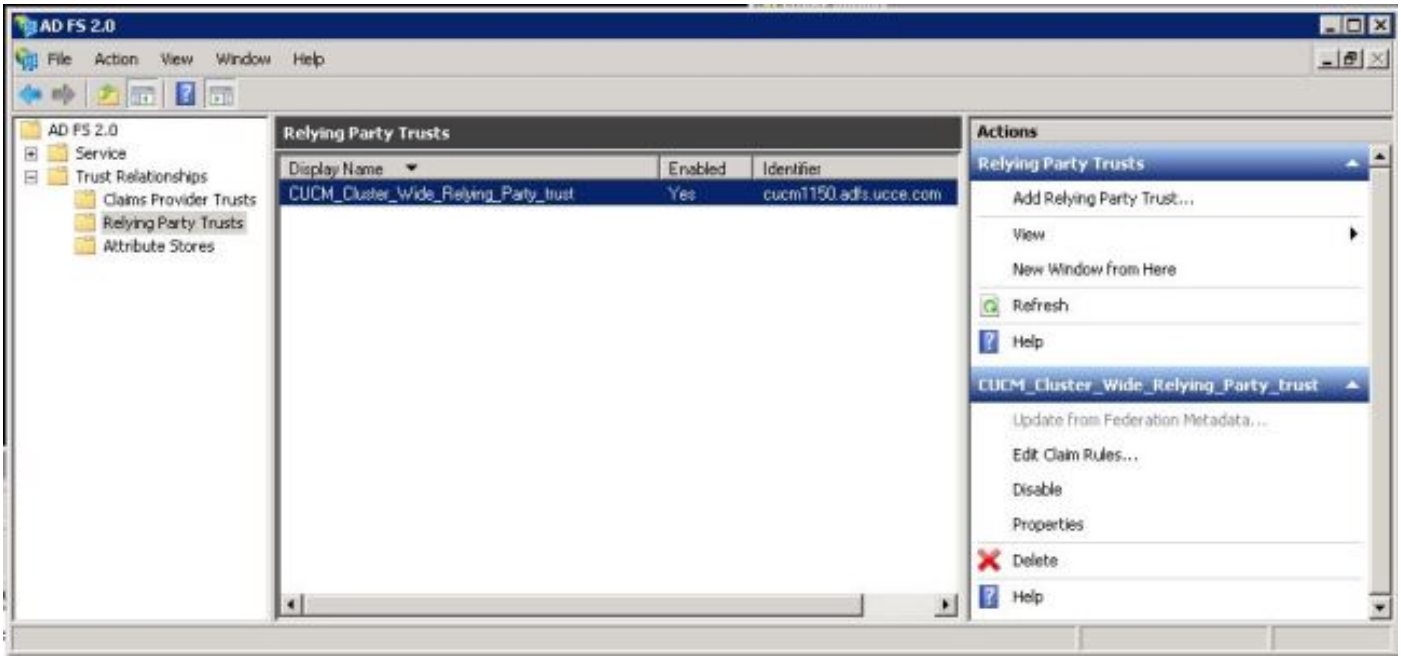
Na página **Pronto para adicionar confiança**, você pode revisar as configurações para a Confiança da terceira parte confiável, que foi configurada. Agora clique em **Next**, como mostrado na imagem:



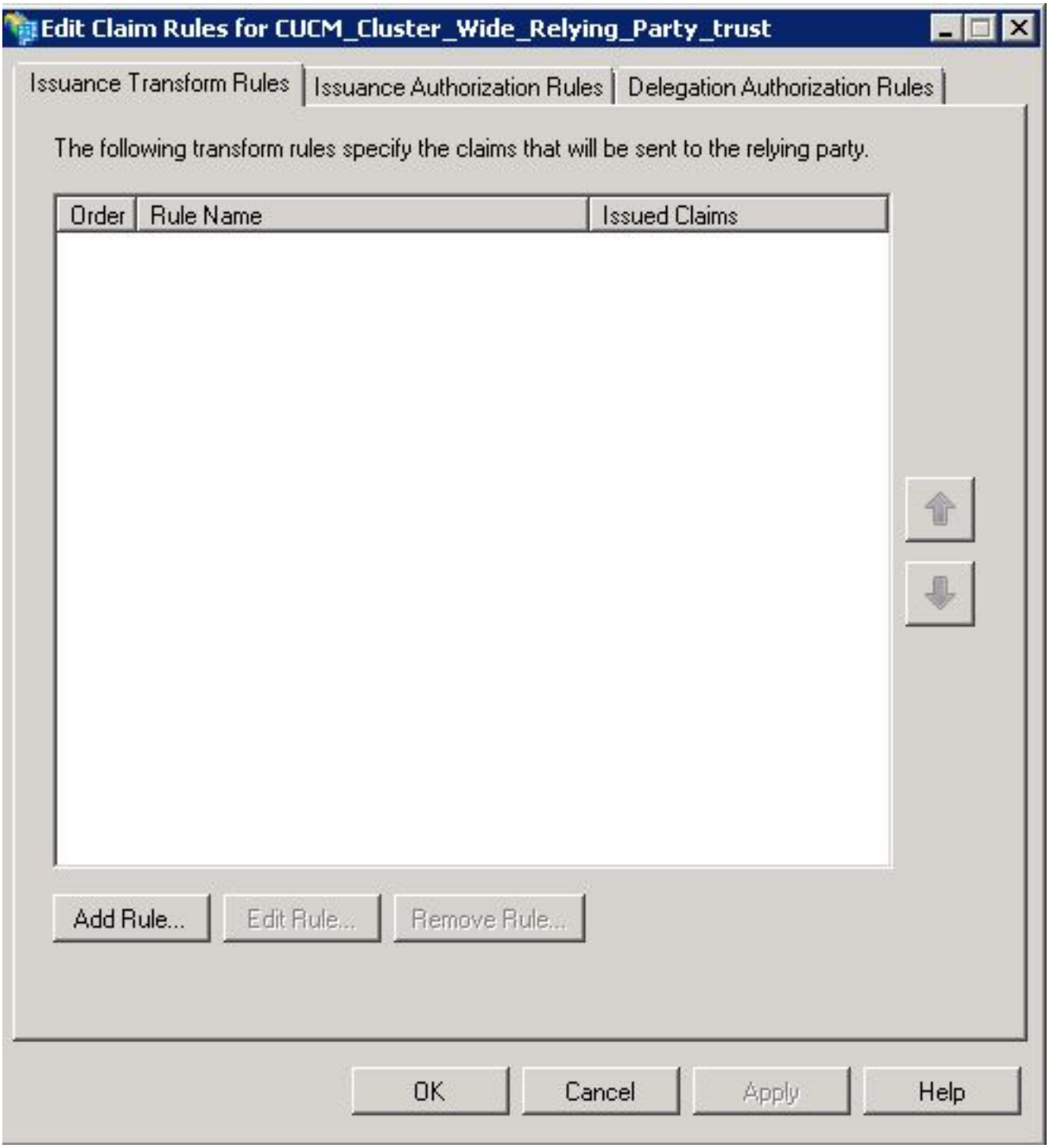
A página Concluir confirma que a confiança da terceira parte confiável foi adicionada com êxito ao banco de dados de configuração do AD FS. Desmarque a caixa e clique em **Fechar**, como mostrado na imagem:



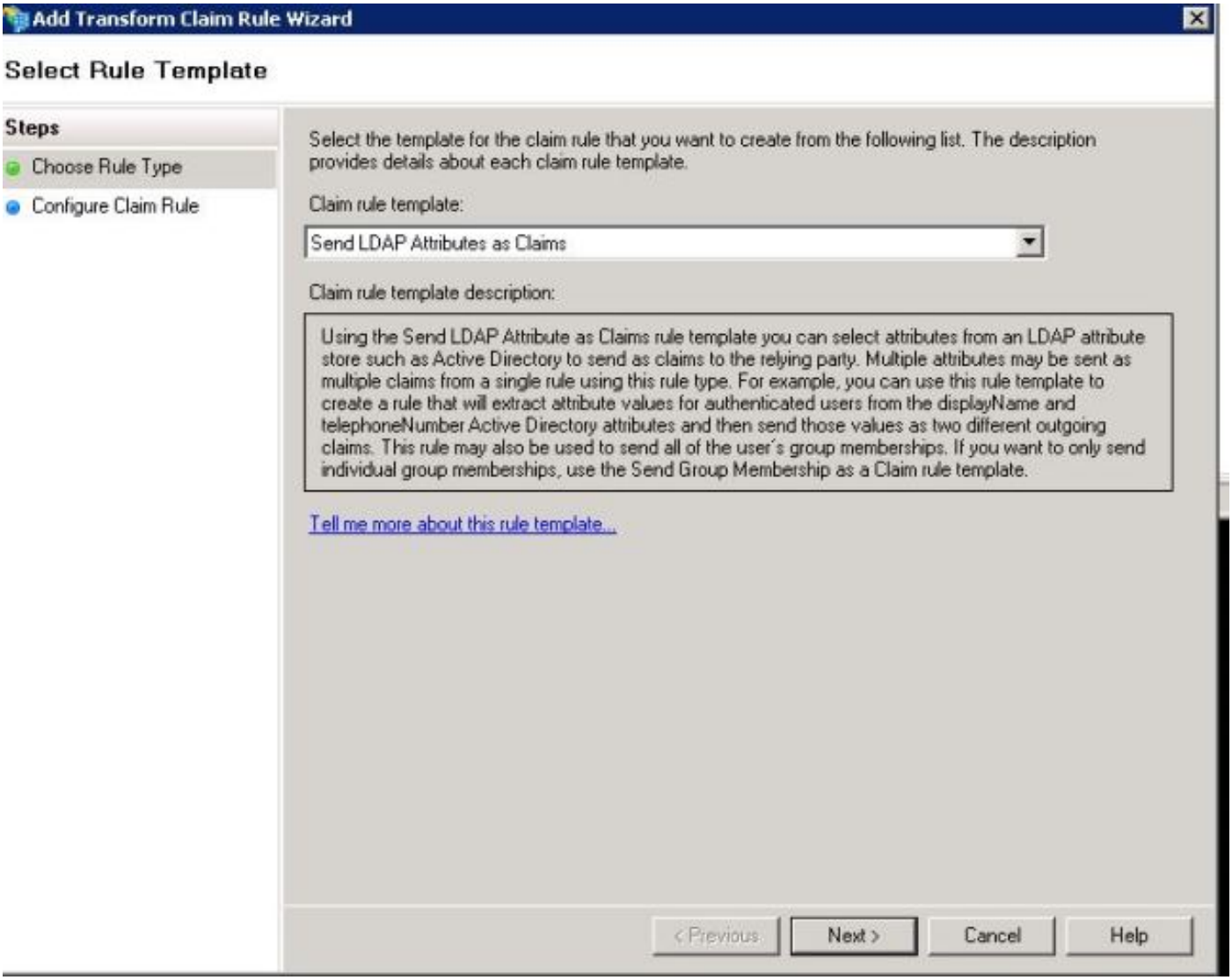
Clique com o botão direito do mouse em **Confianças de terceira parte** e clique em **Editar regras de reivindicação**, conforme mostrado na imagem:



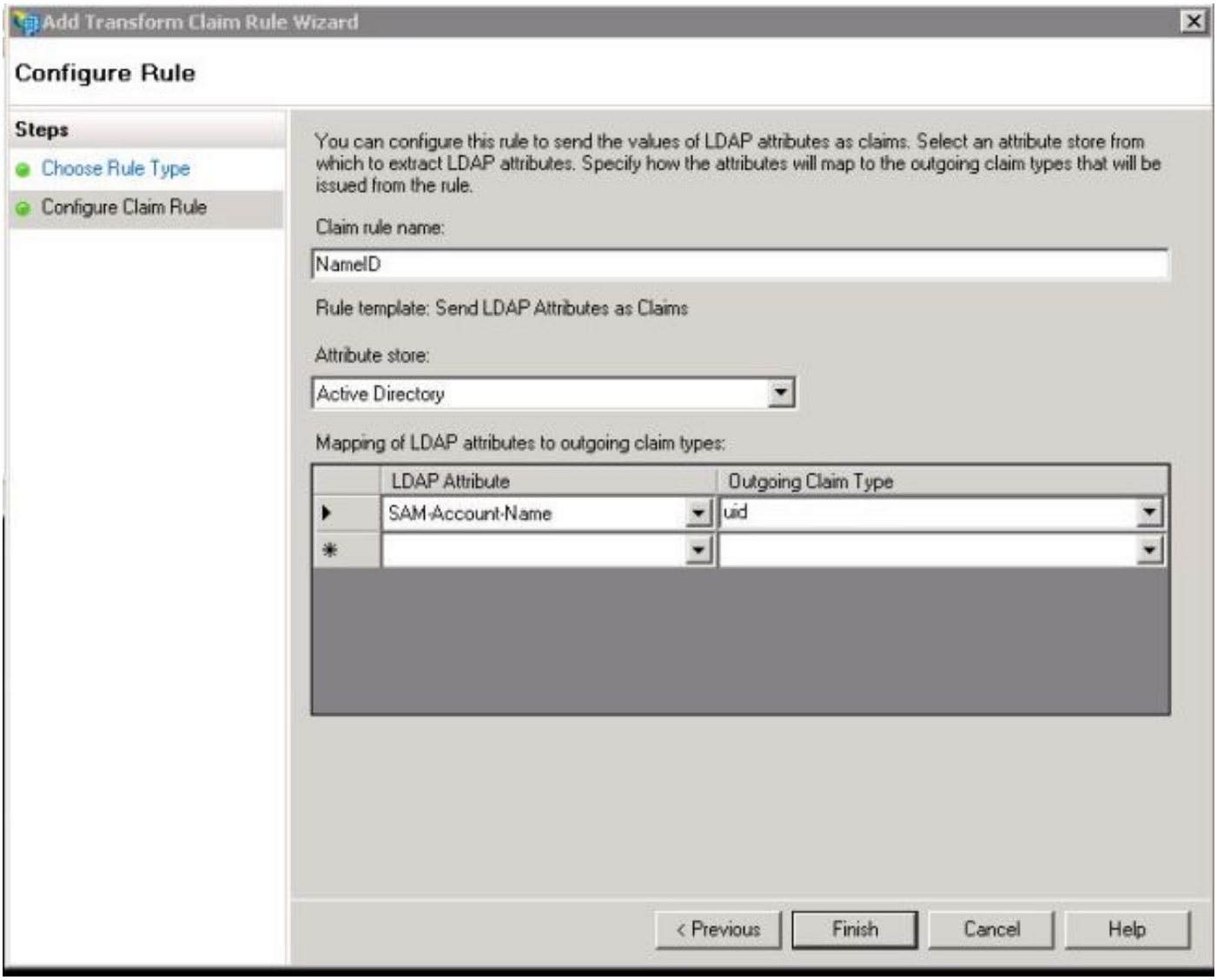
Agora clique em **Add Rule**., como mostrado na imagem:



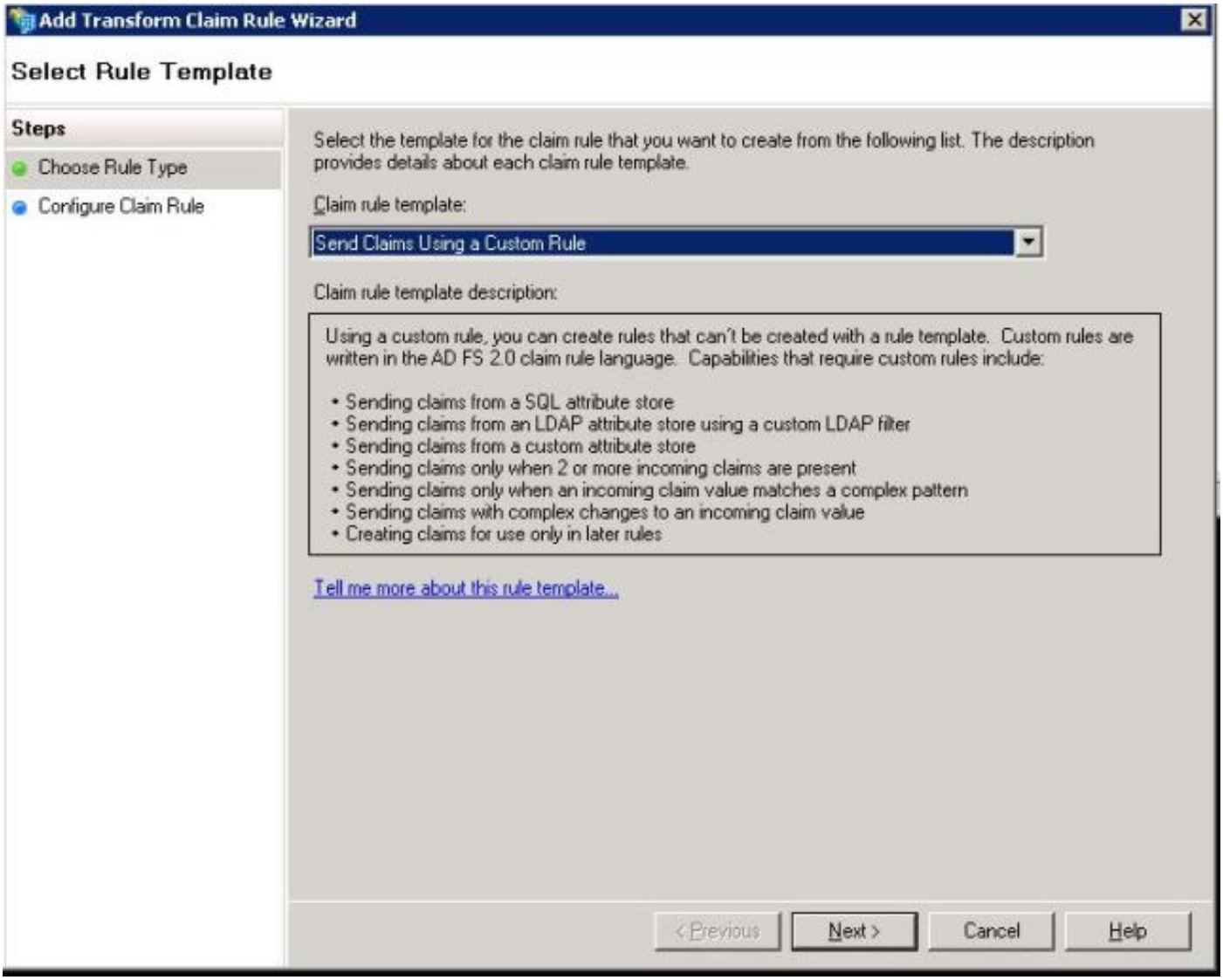
Quando a **opção Add Transform Claim Rule** for aberta, clique em **Next** com o modelo de regra de reivindicação padrão **Send LDAP Attributes as Claims**, como mostrado na imagem:



Clique em **Configure Claim Rule** conforme mostrado nesta imagem. O atributo LDAP deve corresponder ao atributo LDAP na configuração do diretório LDAP no CUCM. Gerenciar o tipo de declaração de saída como **uid**. Clique em **Concluir**, conforme mostrado na imagem:



Adicione a regra personalizada para a terceira parte confiável. Clique em **Adicionar regra**. Selecione **Enviar reivindicações usando uma regra personalizada** e clique em **Avançar,** conforme mostrado na imagem:



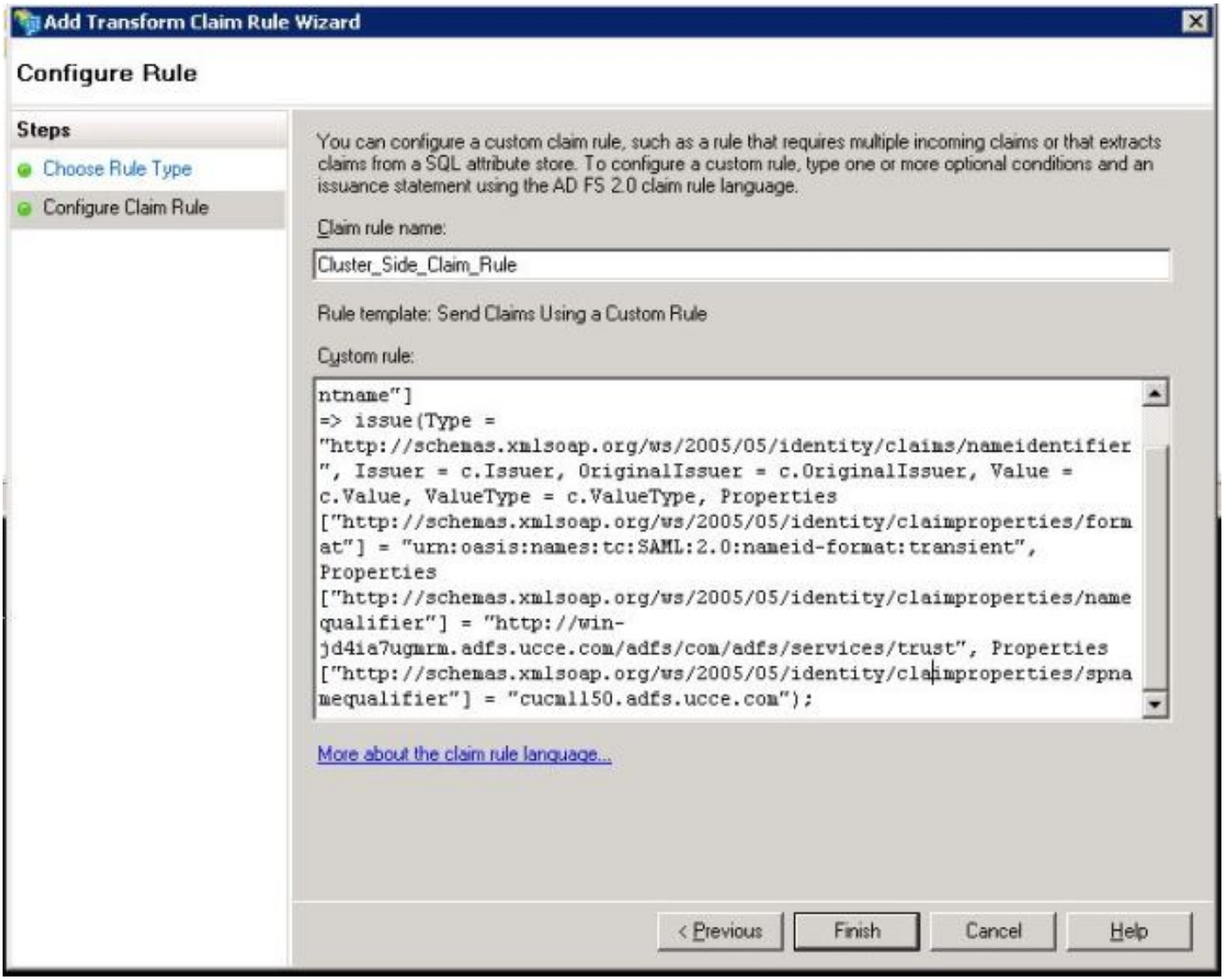
Em Configurar regra de Reivindicação, digite um Nome da regra de Reivindicação e, em seguida, Copie a regra de reivindicação fornecida e passada no campo Regra personalizada do assistente que modifica o qualificador de nome e qualificador de nome de nome na regra de Reivindicação. Clique em **Concluir**, conforme mostrado na imagem:

Regra de solicitação:

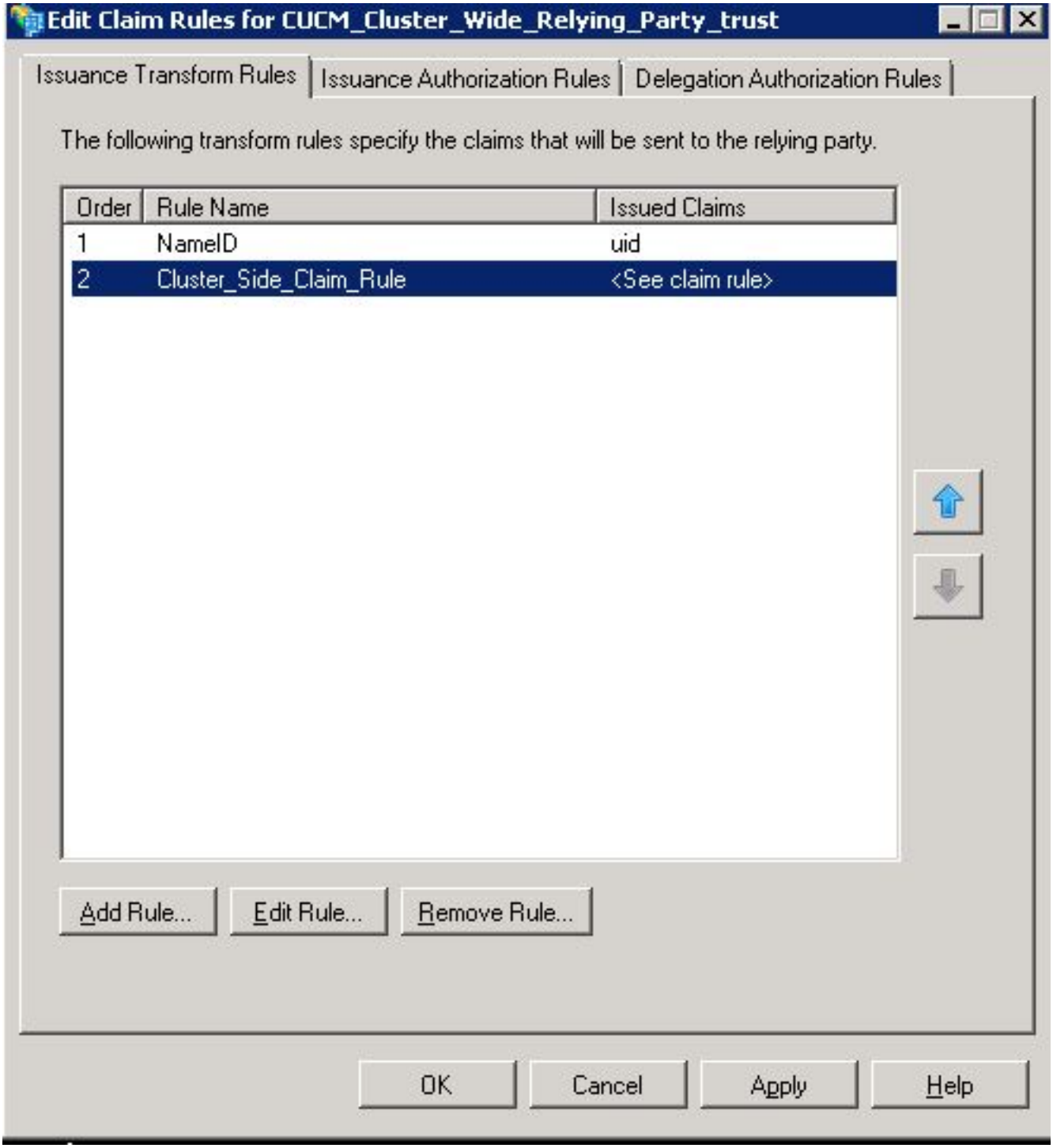
```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]

=> 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>/adfs/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"<Entity ID in the SP Metadata>");
```

```
Entity ID = Open the SP metadata and check the Entity ID. Basically, its the CUCM Publisher's
FQDN.
```



Como mostrado na imagem, clique em **Apply** e em **OK**.

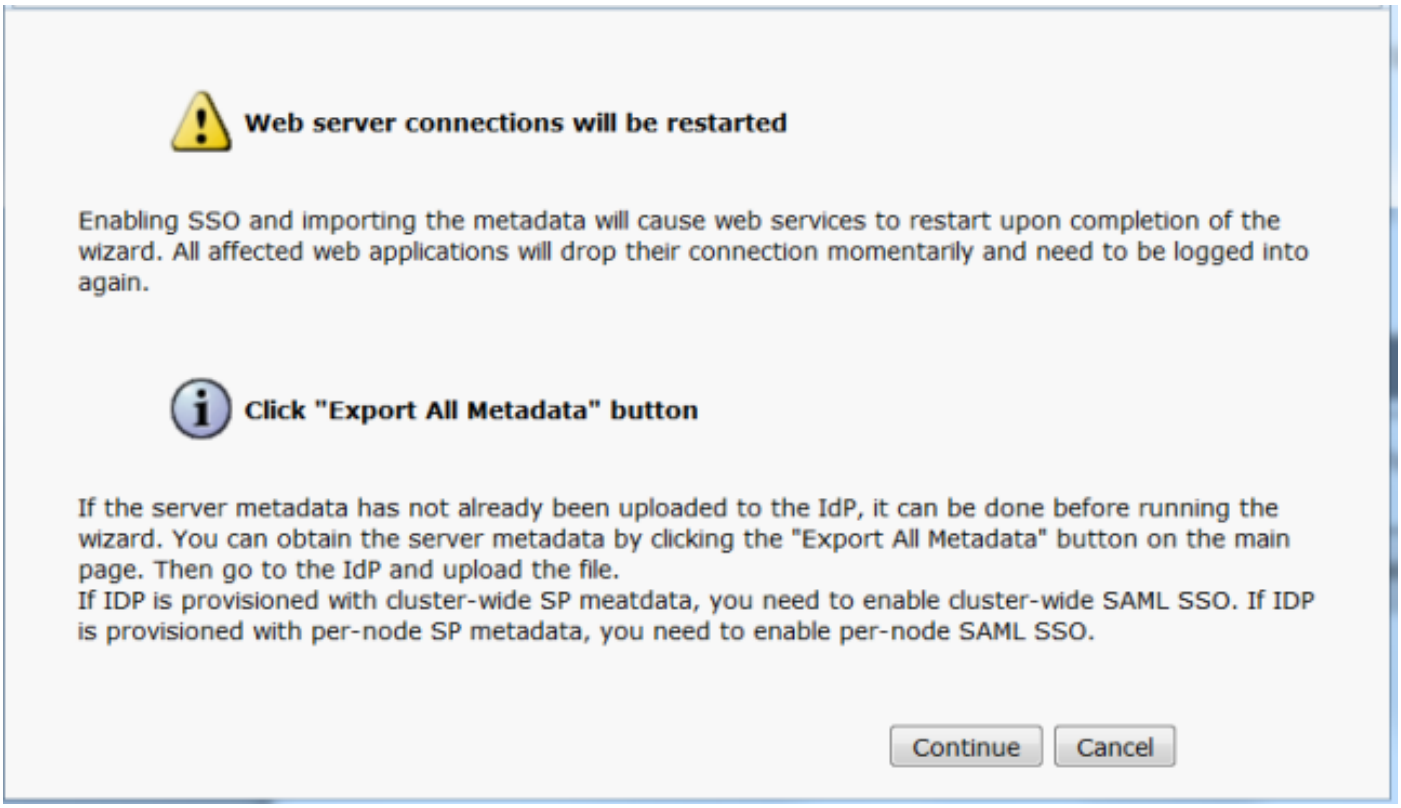


Etapa 4. Ativar SSO SAML

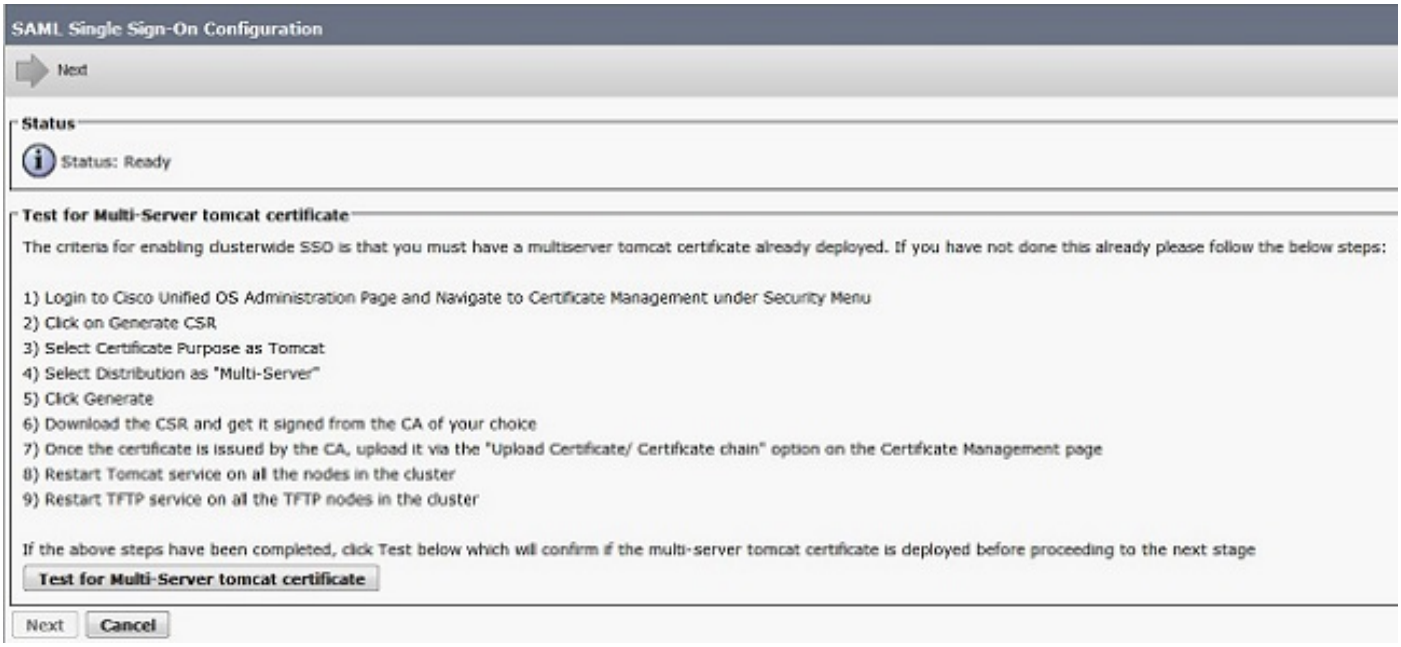
Abra um navegador da Web, faça login no CUCM como administrador e navegue **paraSystem >SAML Single Sign On**.

Por padrão, o botão de opção **Cluster Wide** está selecionado. Clique em **Enable Saml SSO**, conforme mostrado na imagem:

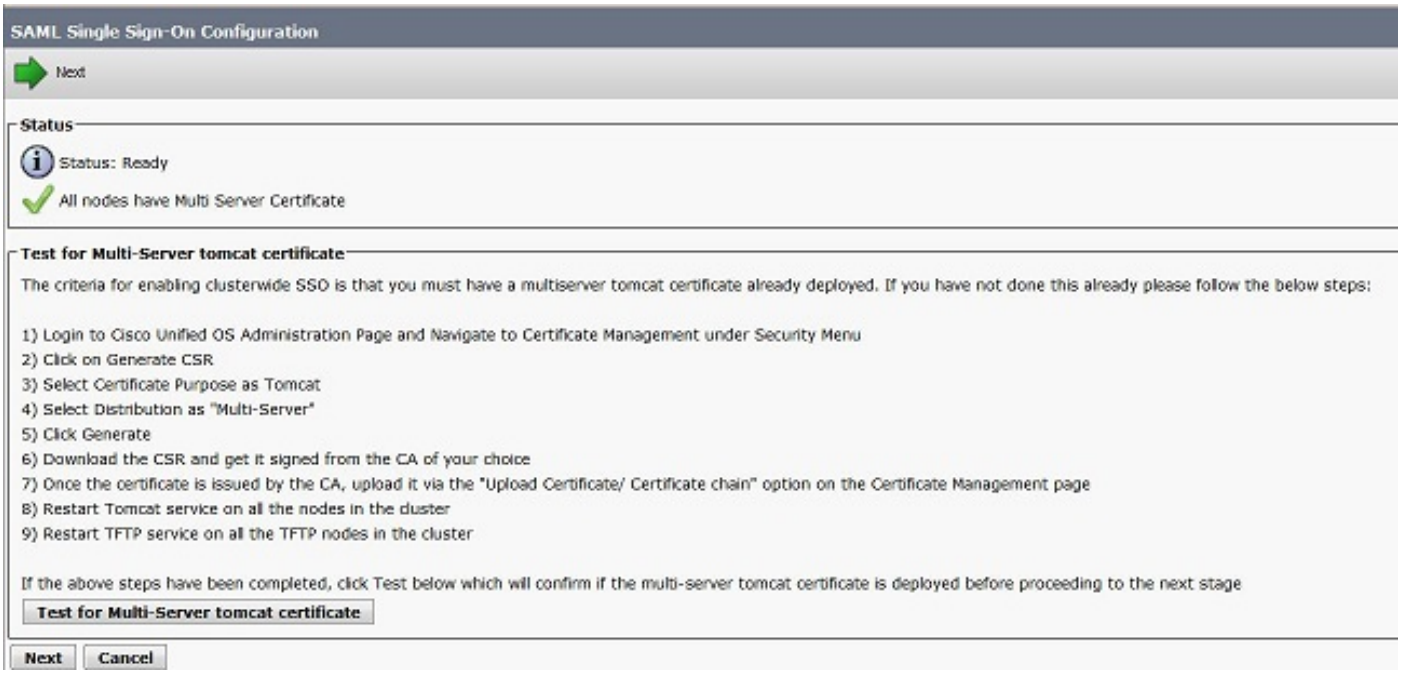
Como mostrado na imagem, o pop-up notifica o aviso de reinicialização do servidor Web e as informações para escolher o SAML SSO ou o SSO SAML por nó de todo o cluster de acordo com o idp. Clique em **Continuar**.



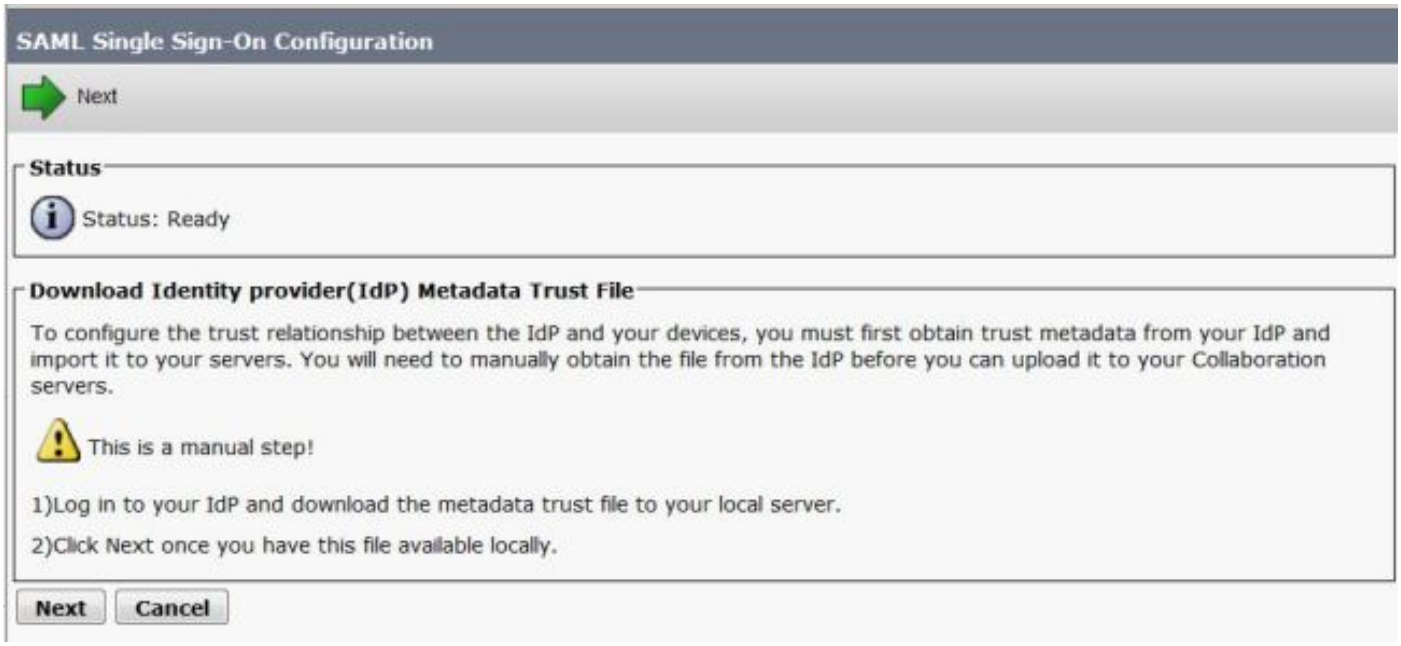
O critério para ativar o SSO em todo o cluster é que você deve ter um certificado tomcat multiservidor já implantado. Clique em **Test for Multi-Server tomcat Certificate**, conforme mostrado na imagem:



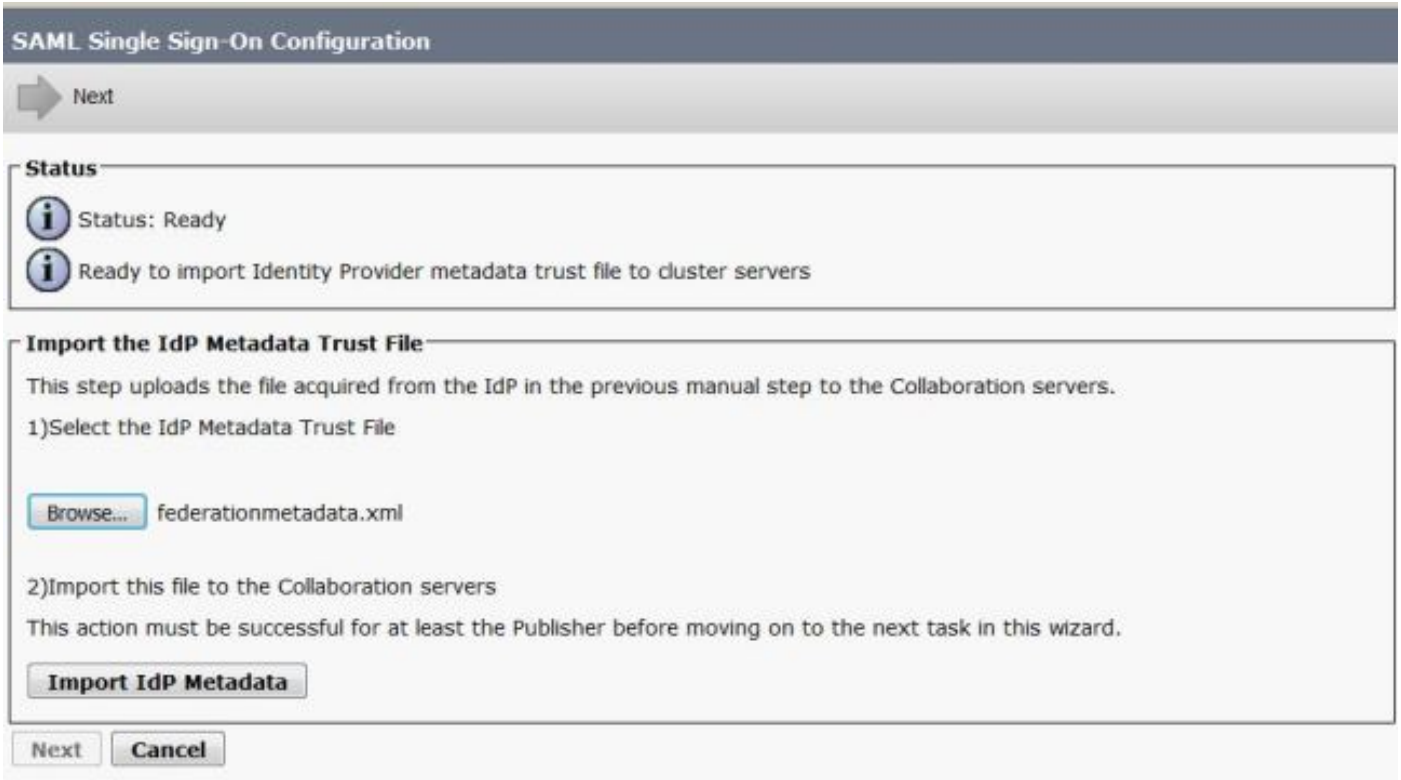
Depois de confirmado, todos os nós têm o Certificado de servidor múltiplo exibido e **Todos os nós têm o Certificado de servidor múltiplo** e, em seguida, clique em **Avançar**, conforme mostrado na imagem:



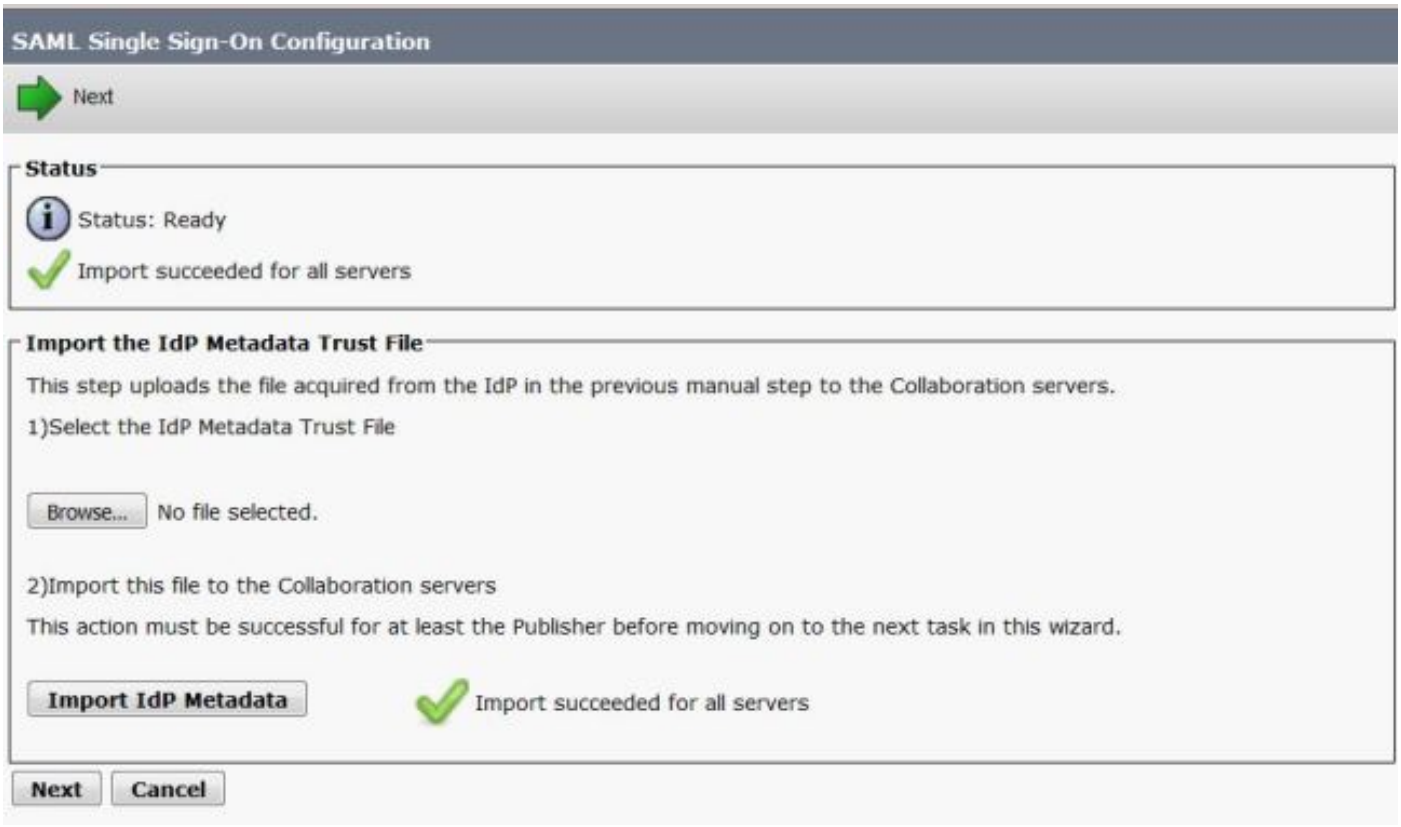
Como mostrado na imagem, clique em **Avançar**.



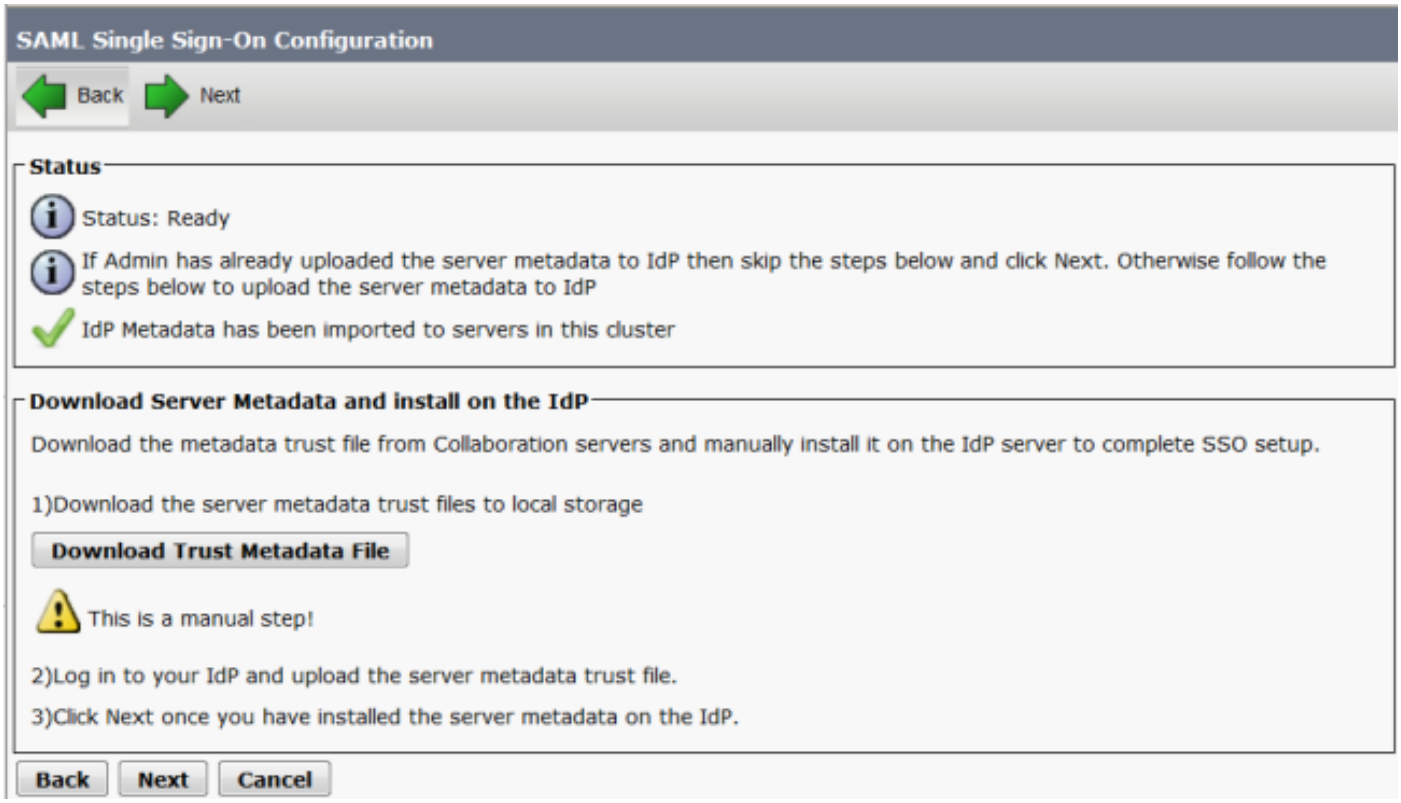
Navegue e selecione os metadados IdP baixados. Clique em **Importar Metadados do IdP**, como mostrado na imagem:



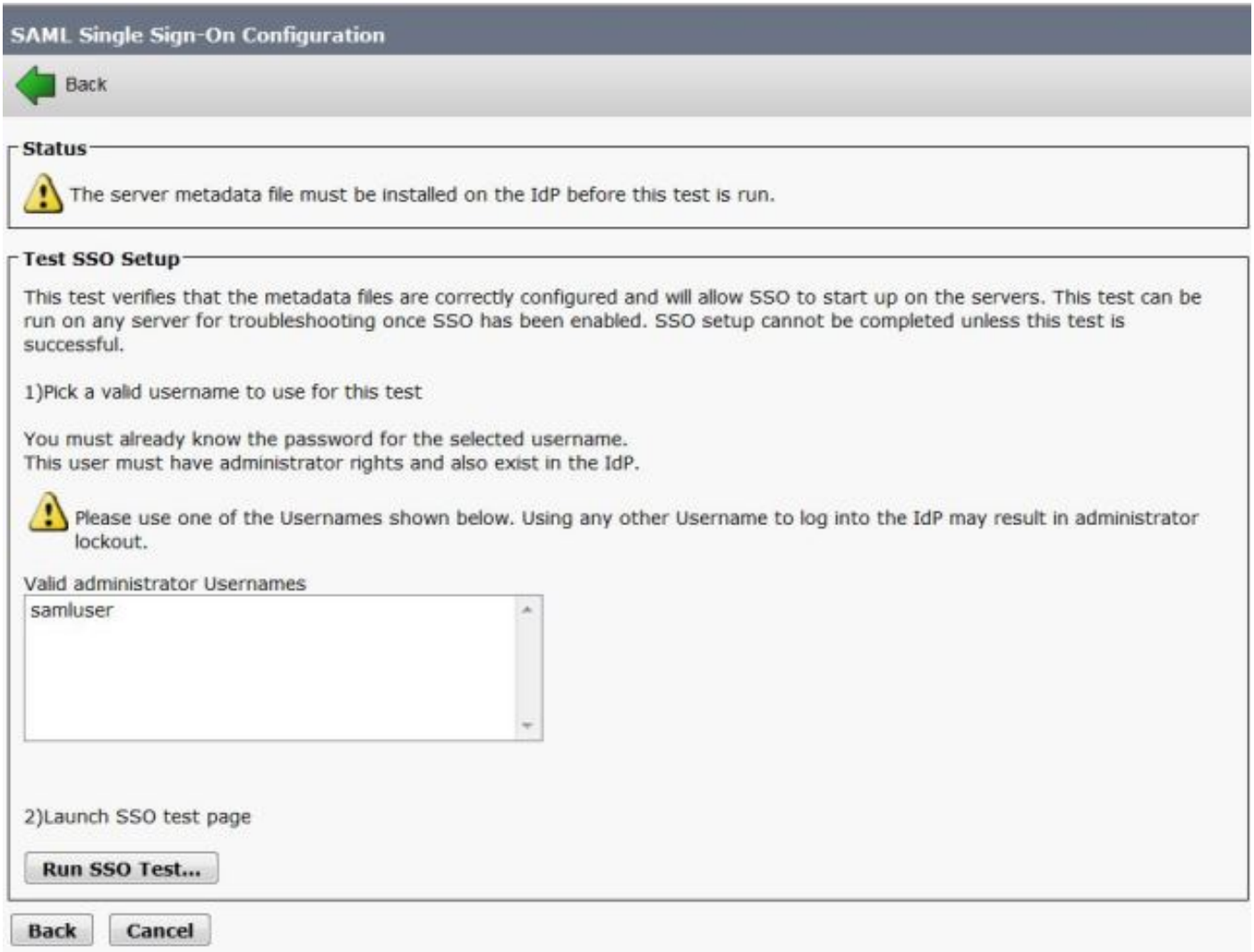
A página confirma a Importação bem-sucedida para todos os servidores e clique em **Avançar**, como mostrado na imagem:



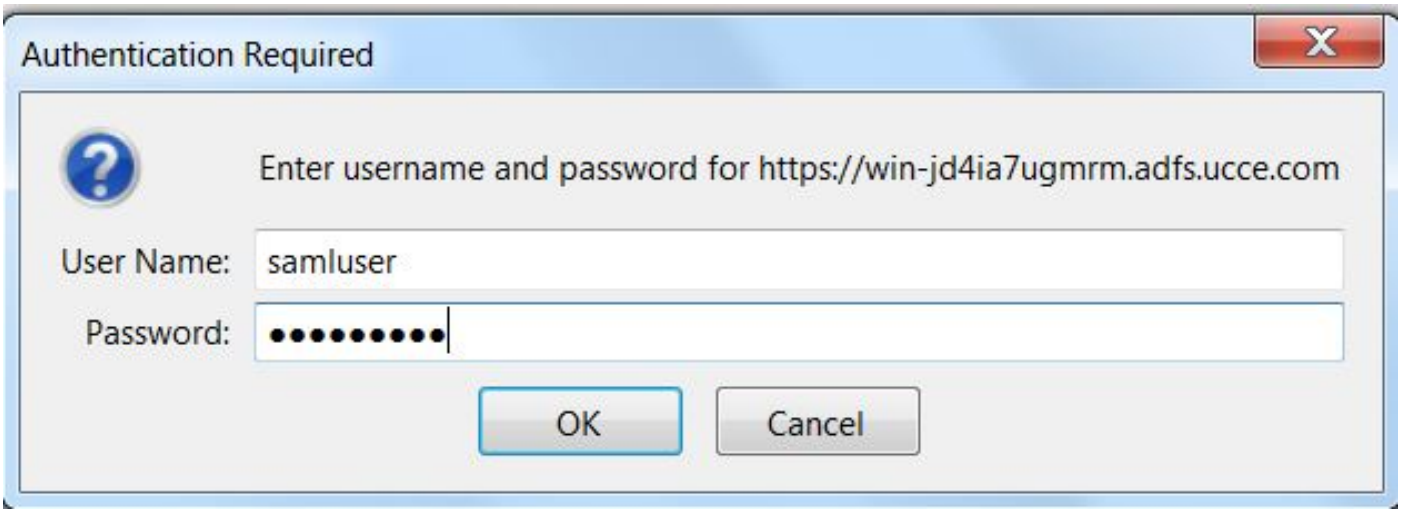
Como mostrado na imagem, clique em **Avançar**, pois já exportou os metadados SP da página de configuração inicial do SSO SAML.



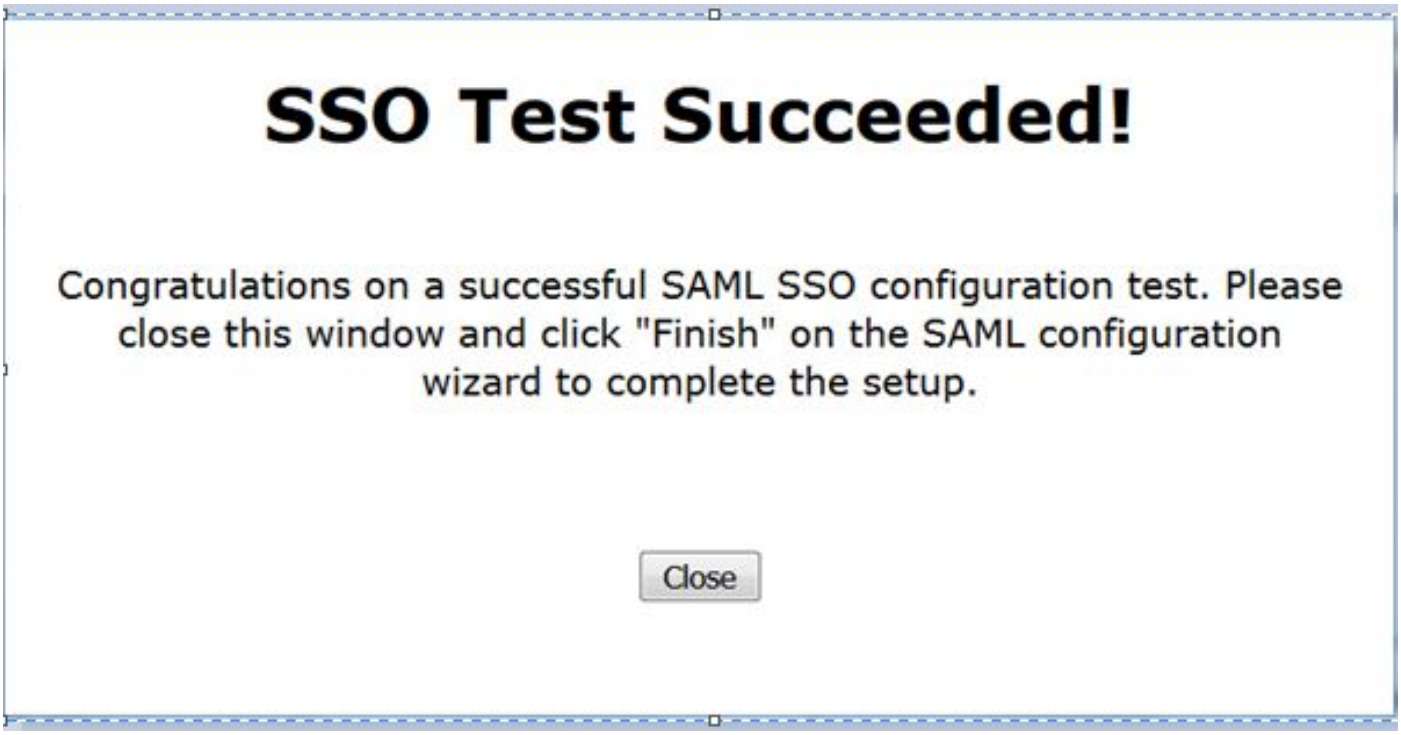
O CUCM deve estar em sincronia com o diretório LDAP. O assistente mostra os usuários administradores válidos configurados no diretório LDAP. Selecione o usuário e clique em **Executar teste SSO**, conforme mostrado na imagem:



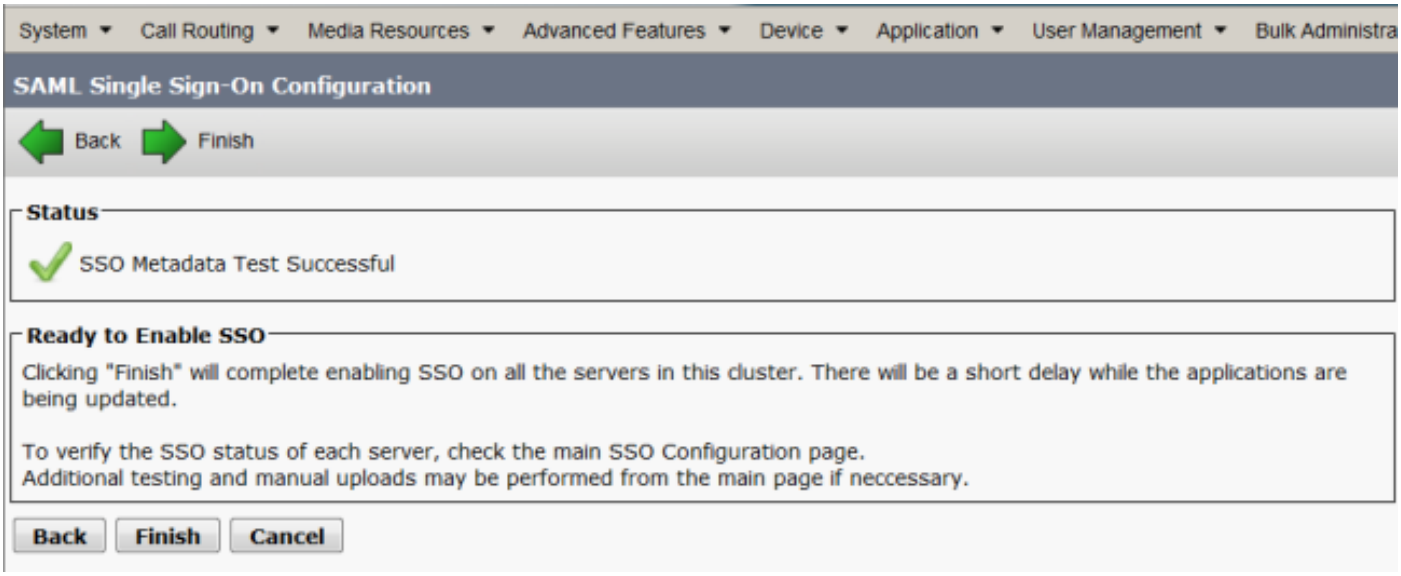
Como mostrado na imagem, digite a ID de usuário e a respectiva senha assim que ela solicitar.



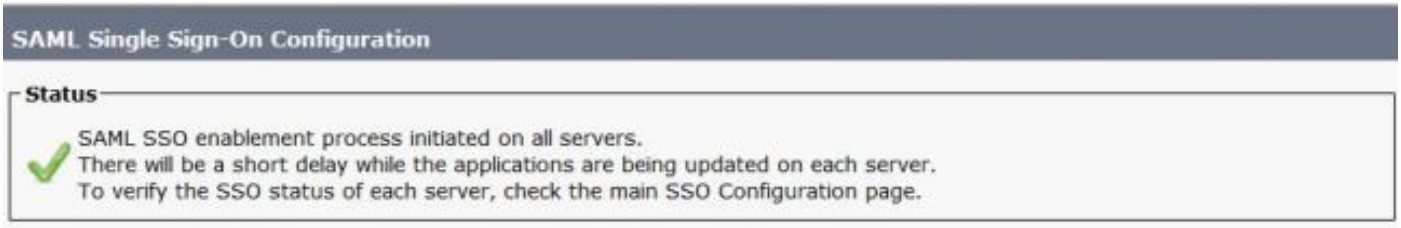
O pop-up, como mostrado na imagem, confirma que o teste foi bem-sucedido.



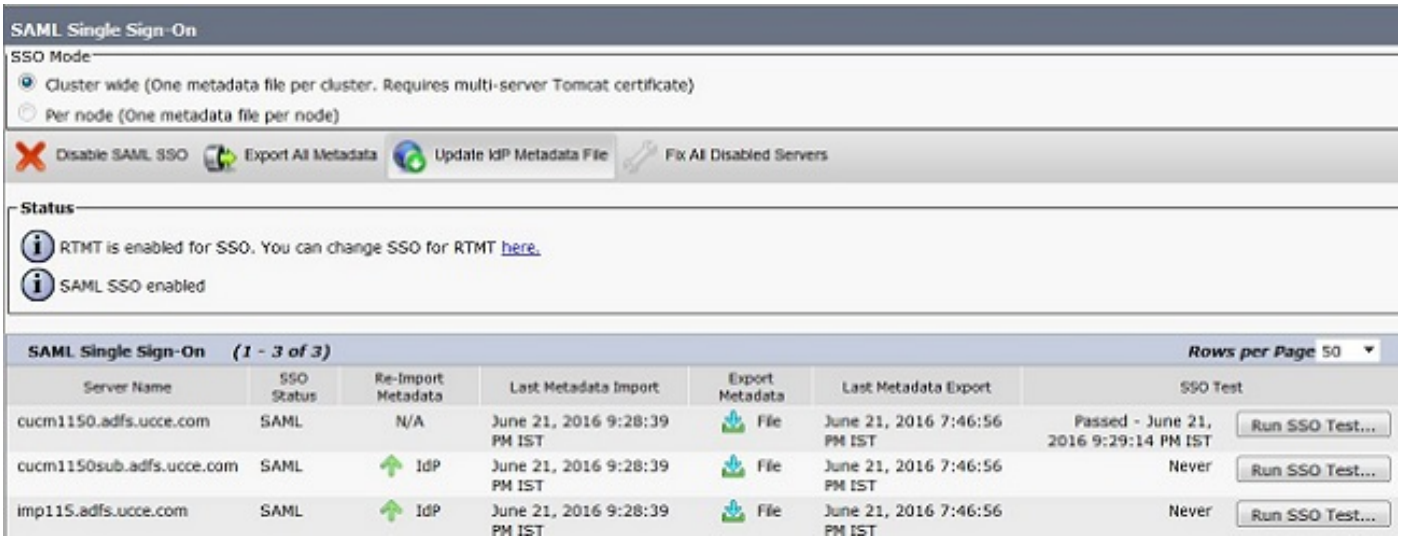
Como mostrado na imagem, clique em **Concluir** para concluir a configuração para ativar SSO.



A página mostrada na imagem confirma que o processo de ativação de SSO SAML é iniciado em todos os servidores.



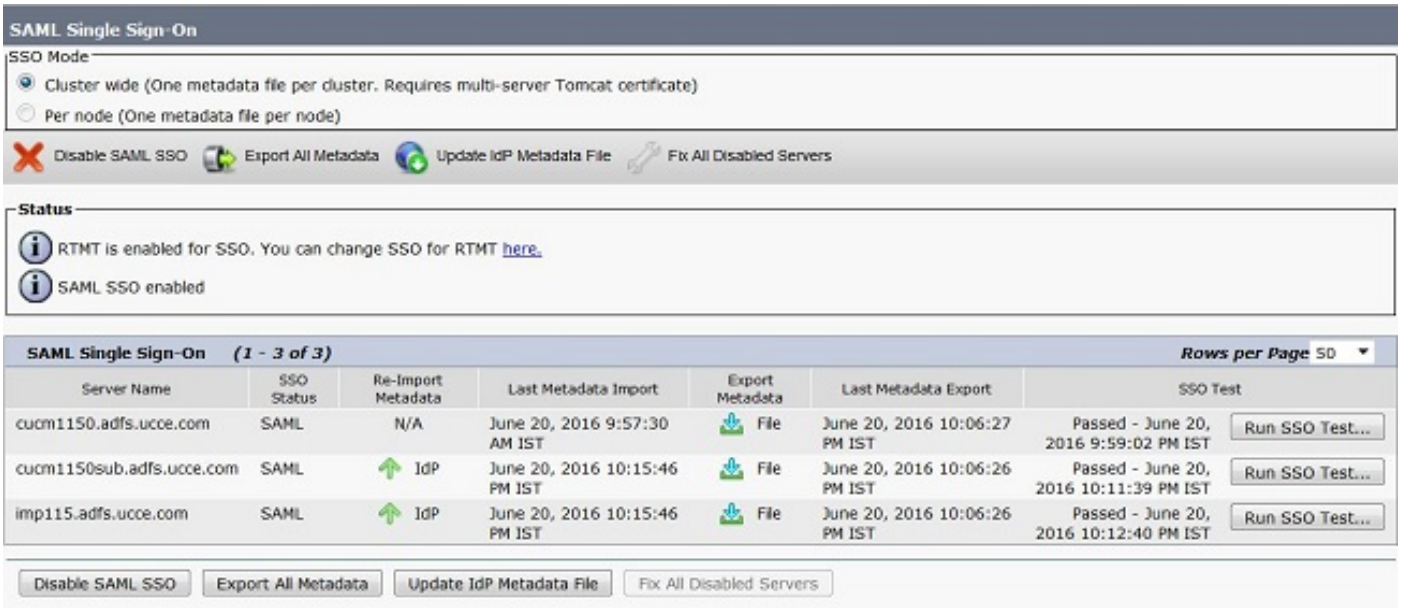
Faça logoff e logon novamente no CUCM usando as credenciais de SSO SAML. Navegue até **Sistema >Logon único SAML**. Clique em **Executar Teste SSO** para outros nós no cluster, conforme mostrado na imagem:



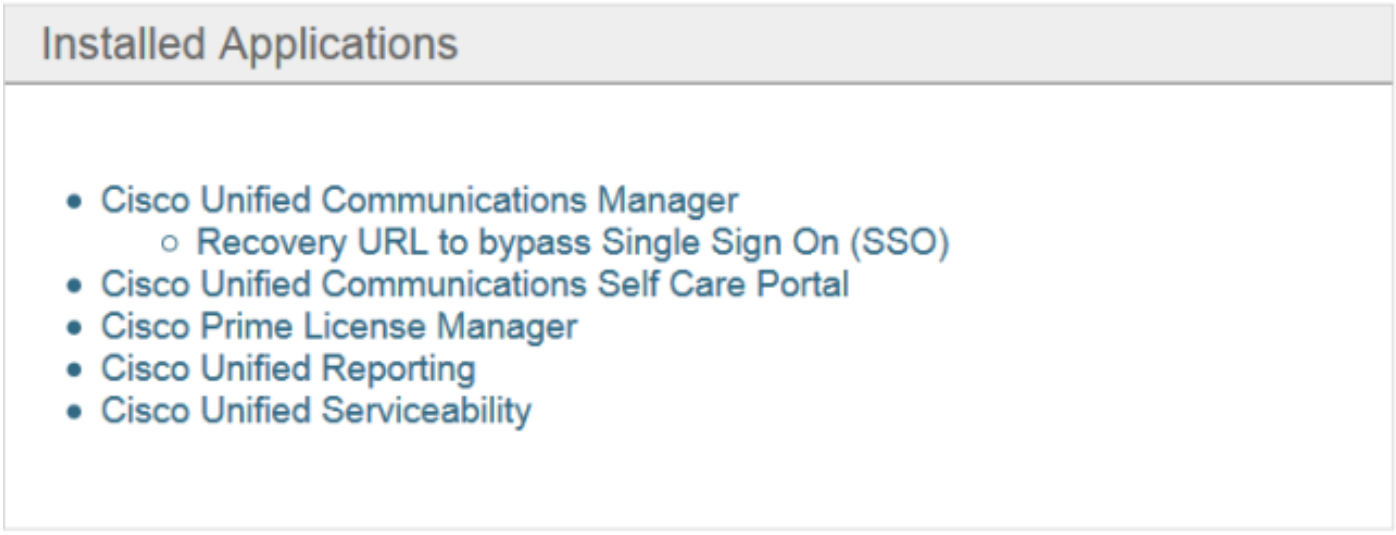
Verificar

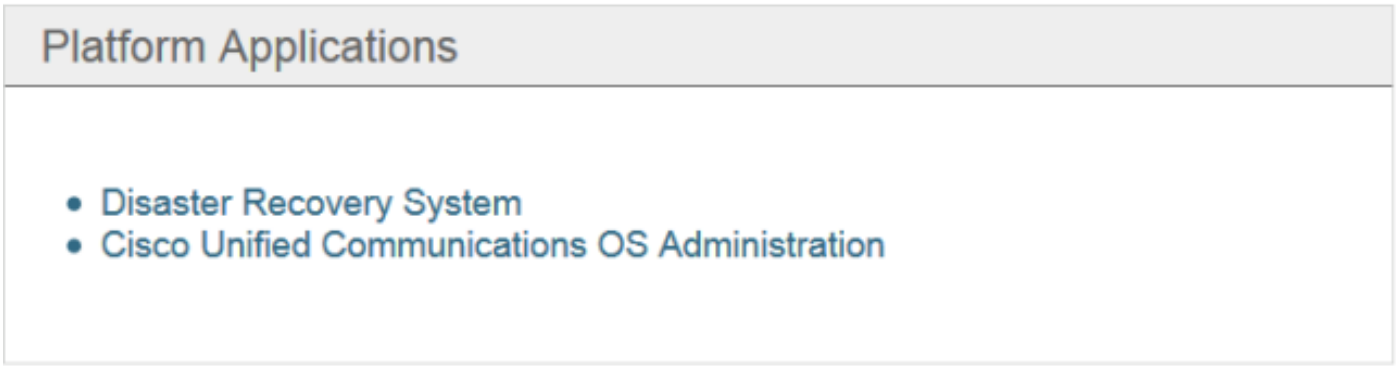
Use esta seção para confirmar se a sua configuração funciona corretamente.

Confirme se o Teste SSO foi bem-sucedido para os nós que estão ativados para SSO SAML. Navegue até **Sistema >Logon único SAML**. Testes SSO bem-sucedidos mostram o status Passado.



Quando o SSO SAML é ativado, os aplicativos instalados e os aplicativos de plataforma são listados para a página de login do CUCM, como mostrado nesta imagem.





Quando o SSO SAML é ativado, os aplicativos instalados e os aplicativos de plataforma são listados para a página de login IM e Presence, como mostrado nesta imagem:

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Para definir os logs SSO como debug, use o comando **set samltrace level DEBUG**

Colete os registros SSO usando RTMT ou do **ativelog /tomcat/logs/ssosp/log4j/*.log** local usando CLI.

Exemplo de logs SSO mostra os metadados gerados e enviados a outros nós

```
2016-05-28 14:59:34,026 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call GET
API to generate Clusterwide SP Metadata in the Local node.
2016-05-28 14:59:47,184 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call to
post the generated SP Metadata to other nodes
2016-05-28 14:59:47,185 INFO  [http-bio-443-exec-297] cluster.SAMLSSOClusterManager -
Begin:postClusterWideSPMetaData
2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Nodes
[cucm1150, cucm1150sub.adfs.ucce.com]
2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post
ClusterWideSPMetadata to the cucm1150
2016-05-28 14:59:47,187 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post
ClusterWideSPMetadata to the cucm1150sub.adfs.ucce.com
```