Configurar SAML SSO no Cisco Unified Communications Manager com ADFS 3.0

Contents

Introduction

Este documento descreve as etapas para configurar o Single Sign-On com o Ative Diretory Federation Service (ADFS 3.0) com o uso do Windows 2012 R2 nos produtos Cisco Unified Communication Manage (CUCM), Cisco Unity Connection (CUC) e Expressway. As etapas para configurar o Kerberos também estão incluídas neste documento.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento dos produtos Single Sign-On (SSO) e Windows.

Componentes Utilizados

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

- CUCM 11.5
- CUC 11.5
- Expressway 12
- Windows 2012 R2 Server com as seguintes funções:
  - Serviços de Certificados do Ative Diretory
  - Serviços de Federação do Ative Diretory

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Pré-verificação da configuração

Antes de instalar o ADFS3, estas funções de servidor já precisam existir no ambiente:

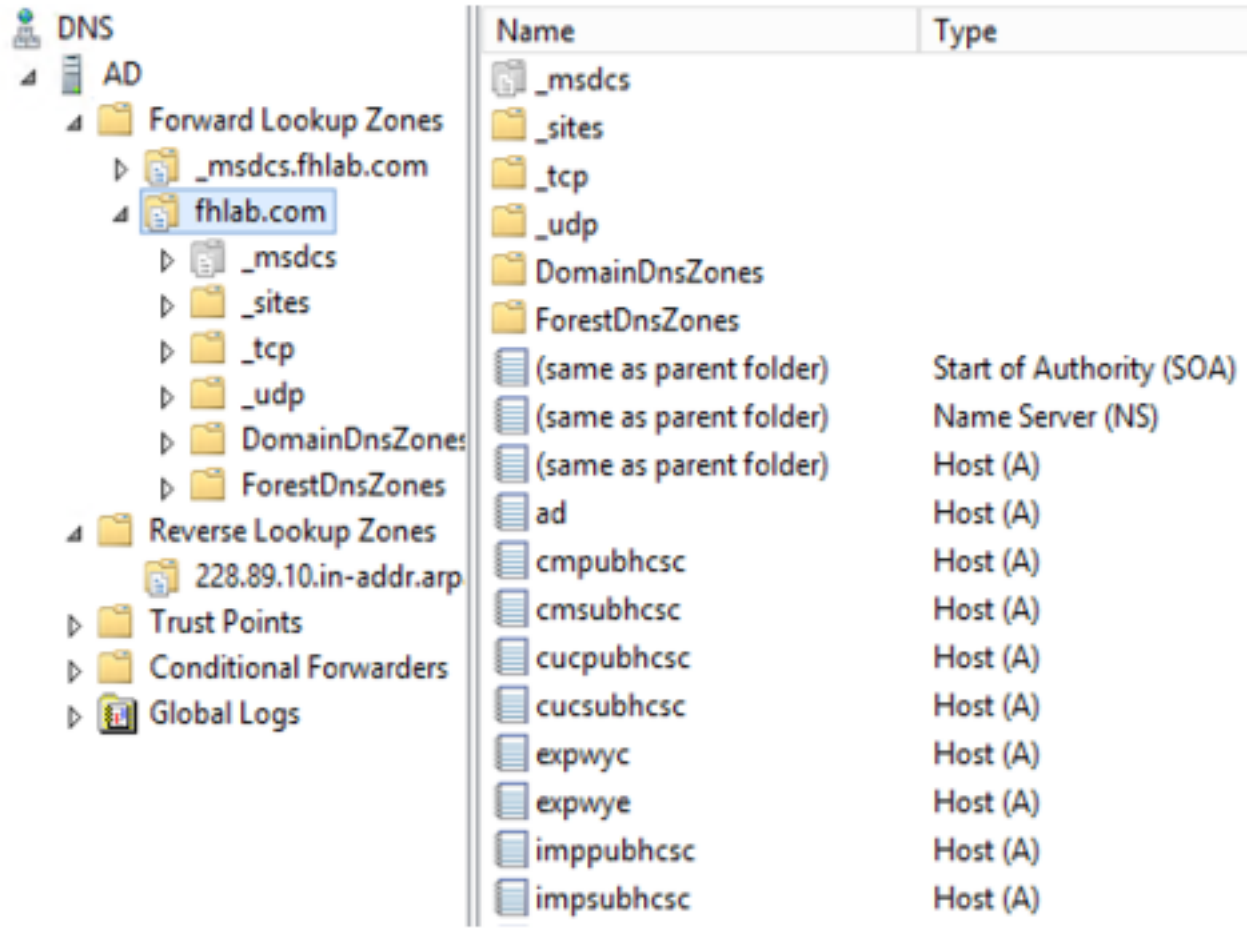
Domain Controller e DNS

Todos os servidores devem ser adicionados como Registros A junto com seu Registro de Ponteiro (um tipo de registro DNS que resolve um endereço IP para um domínio ou nome de host)

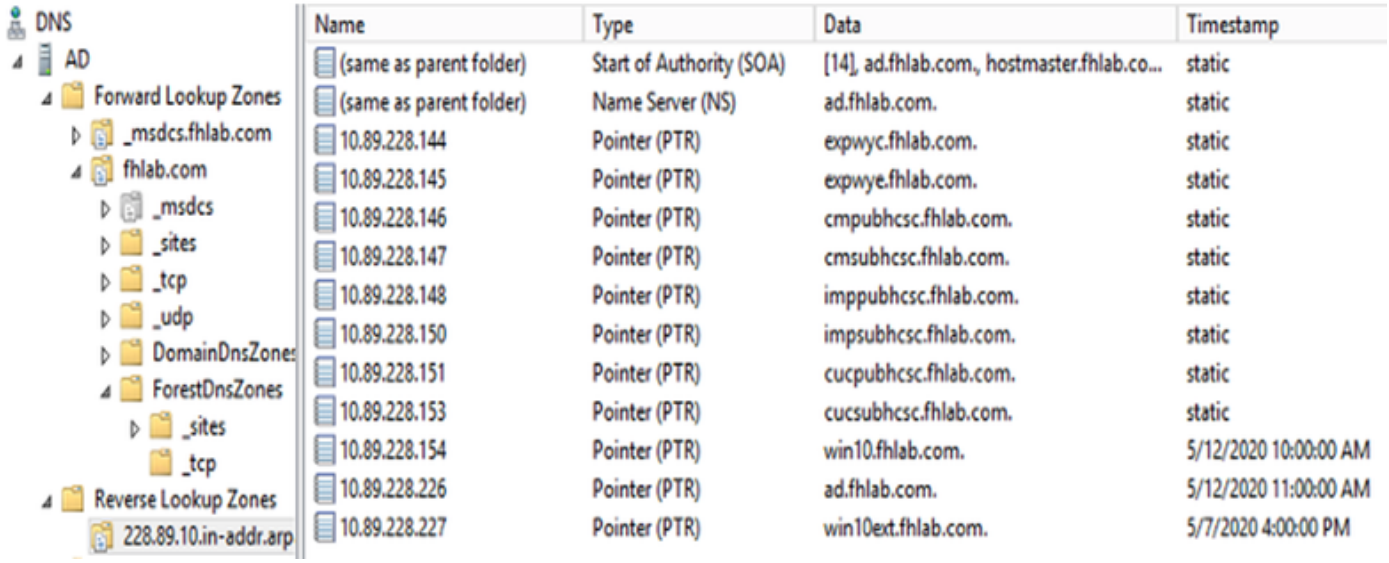
A Records

Em fhlab.com. os hosts cmpubhcsc, cmsubhcsc, cucpubhcsc, cucsubhcsc, expwyc, exwye,

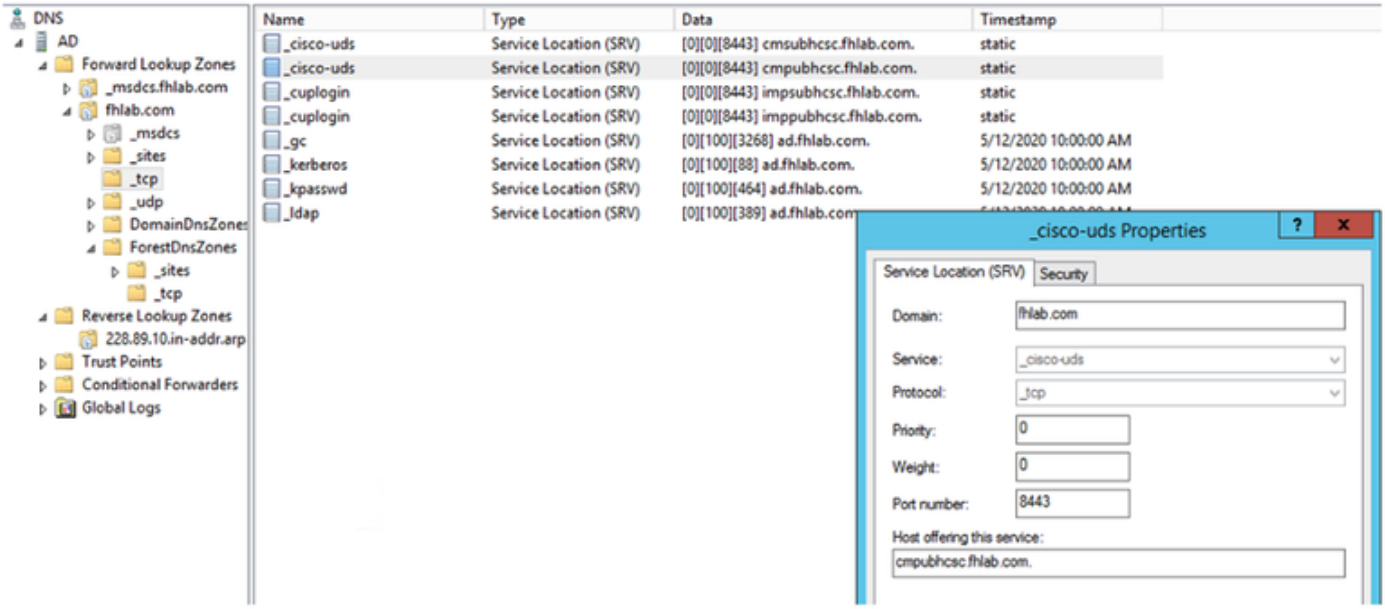
impubhcsc e imsubhcsc foram adicionados.



Registros de Ponteiro (PTR)

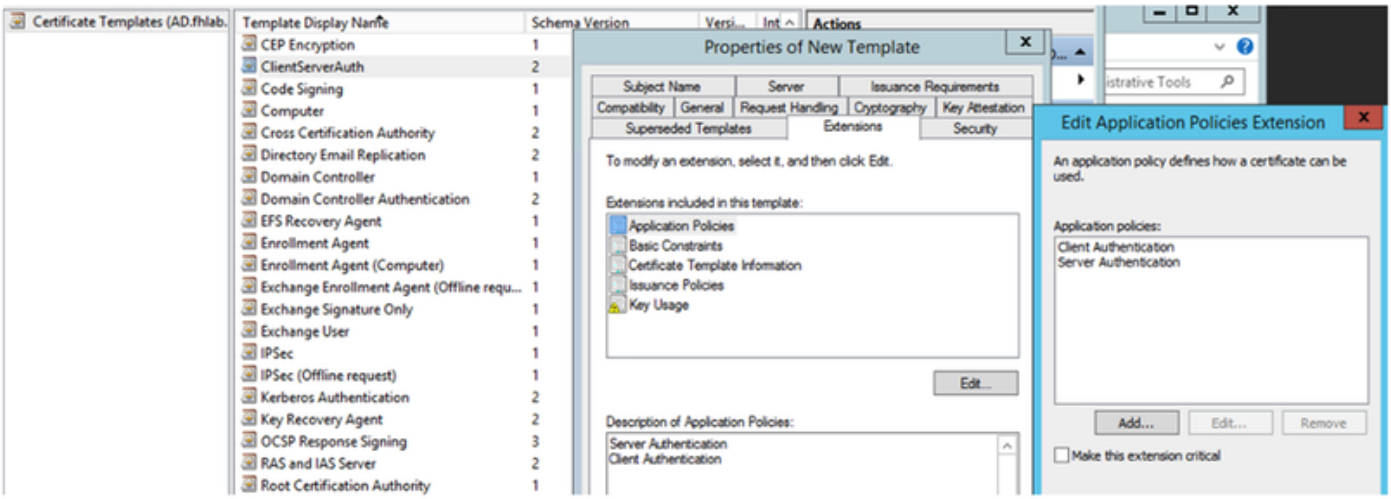


Énecessário que os registros SRV estejam em vigor para o Jabber Discovery Services

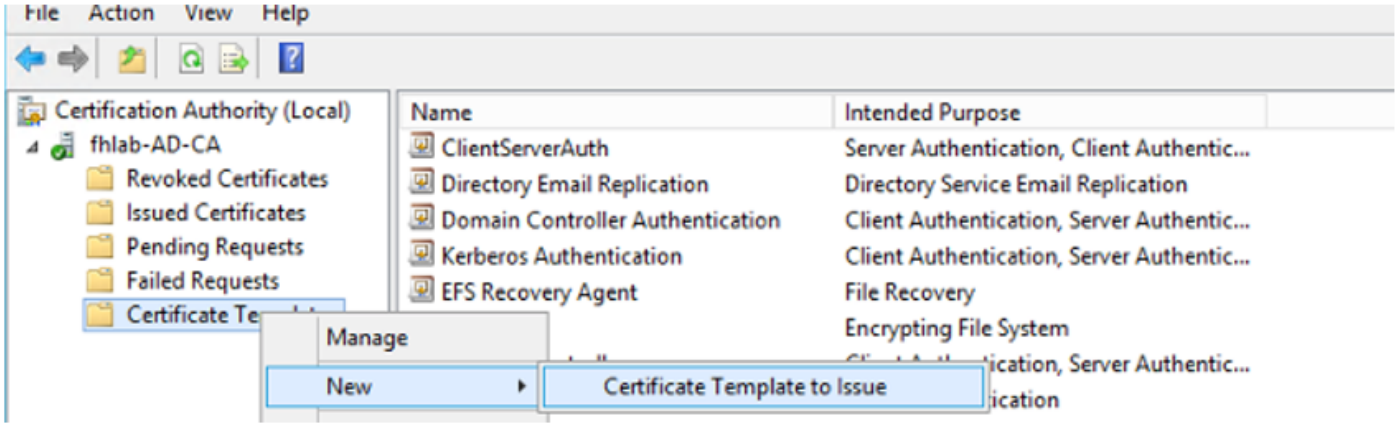


- CA raiz (supondo que os certificados sejam assinados pela AC empresarial)

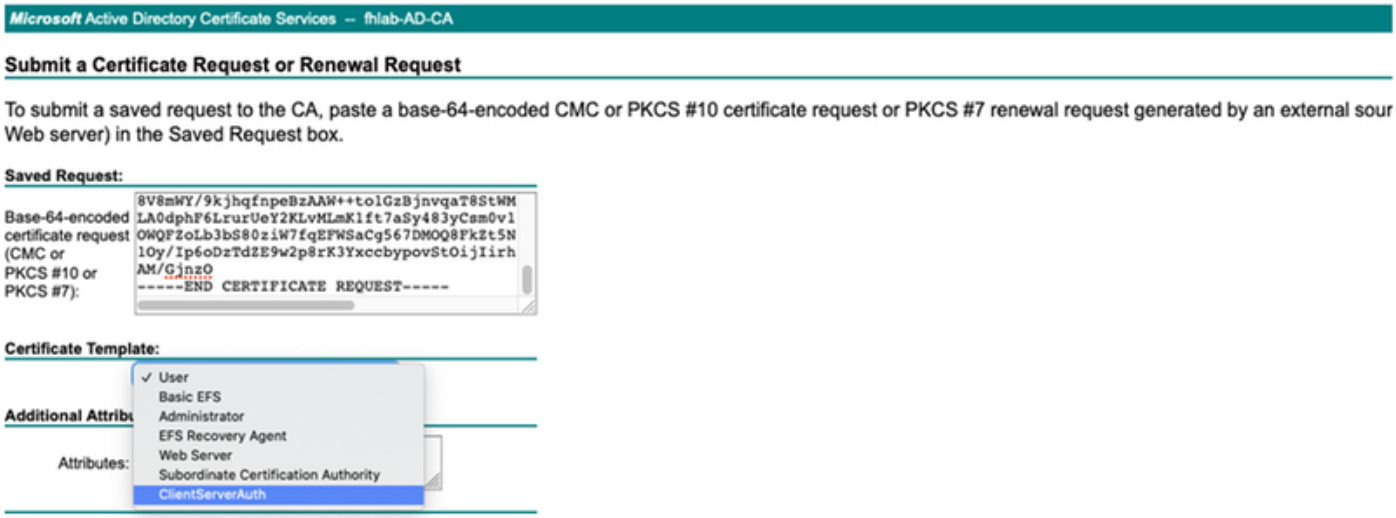
Um Modelo de Certificado precisa ser criado com base no Modelo de Certificado do Servidor Web, o primeiro é duplicado, renomeado e, na guia Extensões, as Políticas de Aplicativo são modificadas adicionando uma Política de Aplicativo de Autenticação de Cliente. Este modelo é necessário para assinar todos os certificados internos (CUCM, CUC, IMP e Expressway Core) em um ambiente de LAB, a CA interna também pode assinar as Solicitações de Assinatura de Certificado (CSR) do Expressway E.



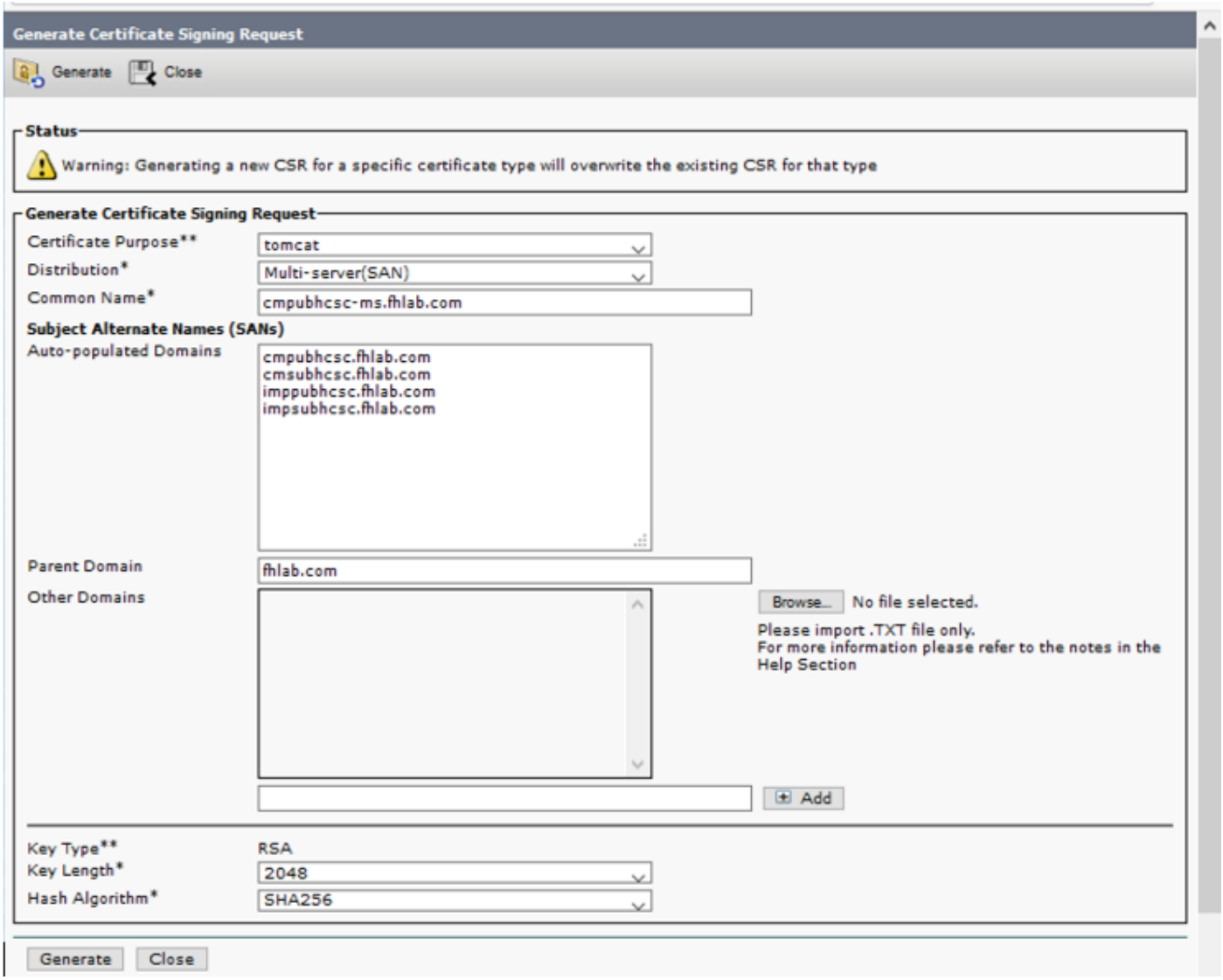
O modelo criado precisa ser emitido para poder assinar o CSR.



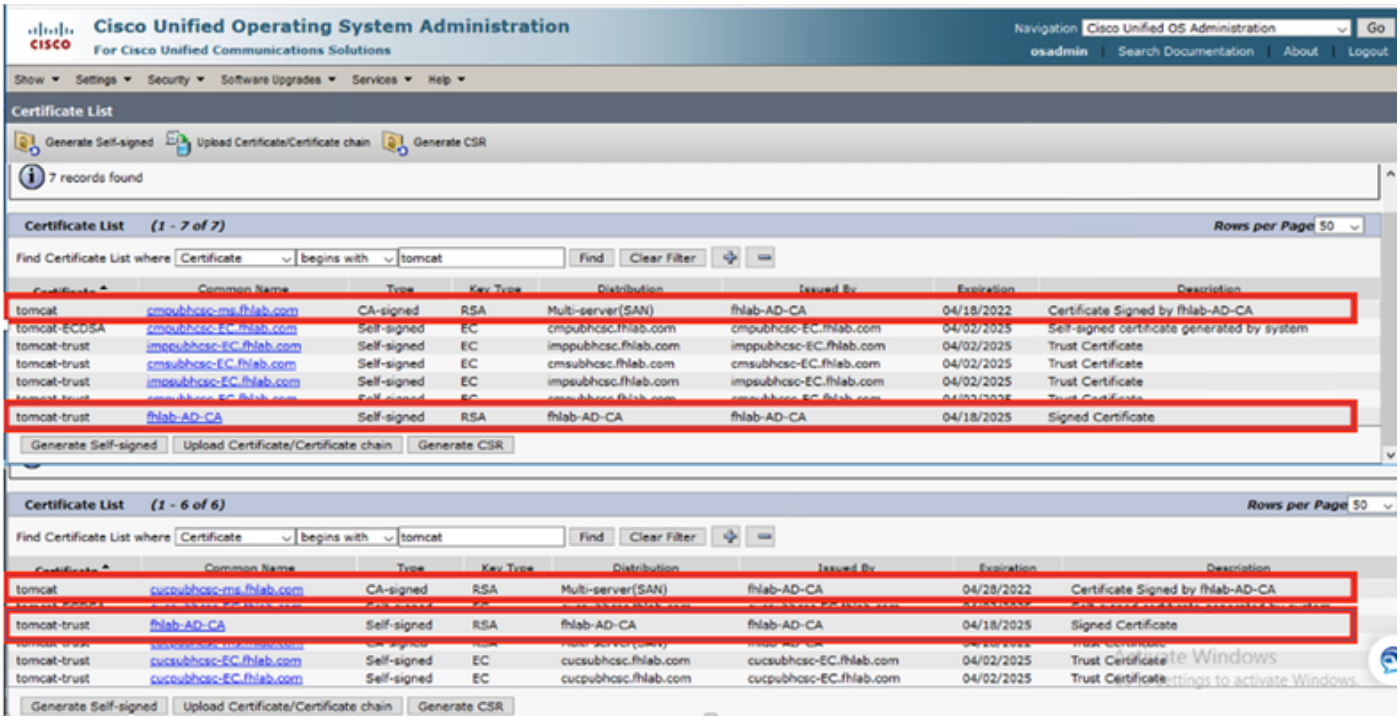
Na Web do certificado CA, selecione o modelo que foi criado anteriormente.



CUCM, IMP e CUC Multi-Server CSR devem ser gerados e assinados pela CA. A finalidade do certificado deve ser tomcat.



O certificado raiz da CA deve ser carregado para o Tomcat Trust e o certificado assinado para tomcat.



- IIS

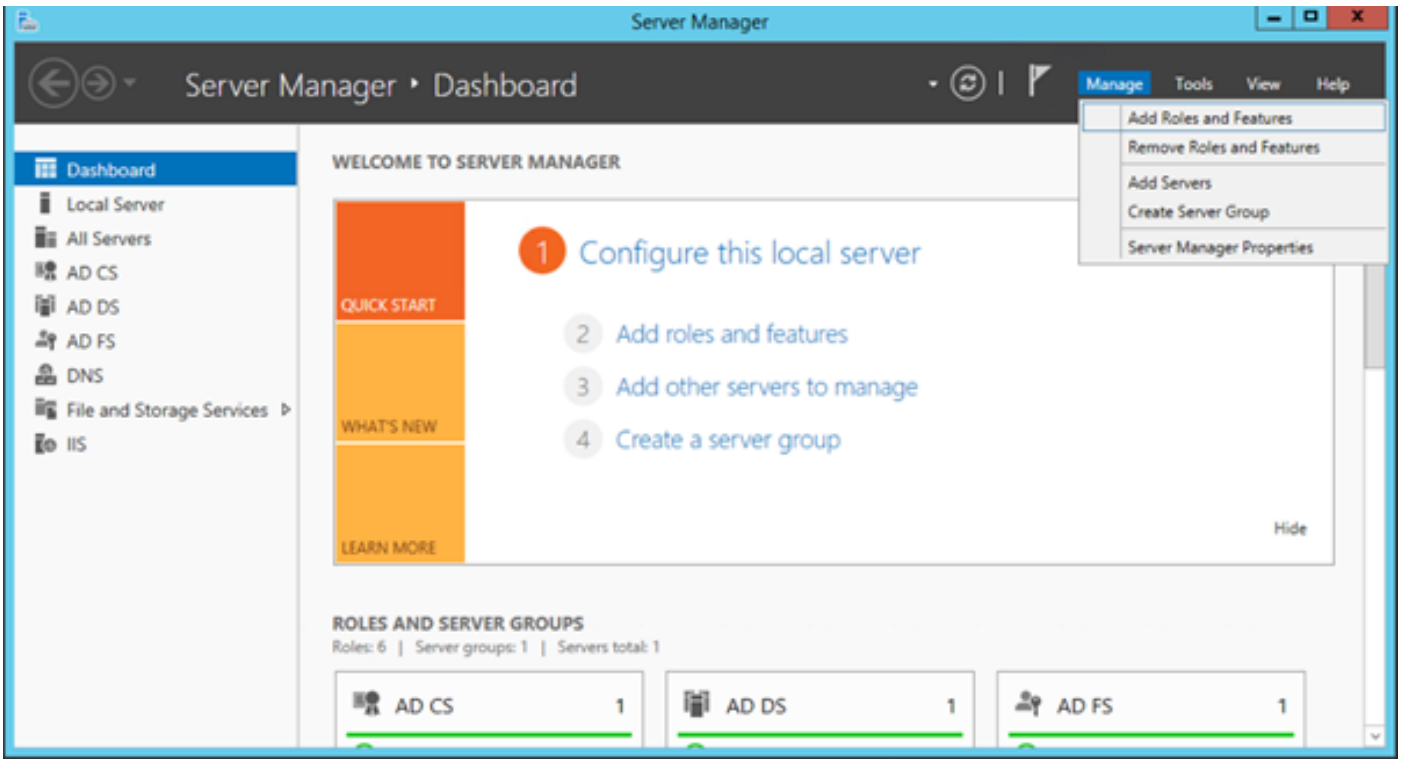
Caso contrário, esta seção passará pela instalação dessas funções. Caso contrário, ignore esta

seção e continue diretamente com o download do ADFS3 da Microsoft.

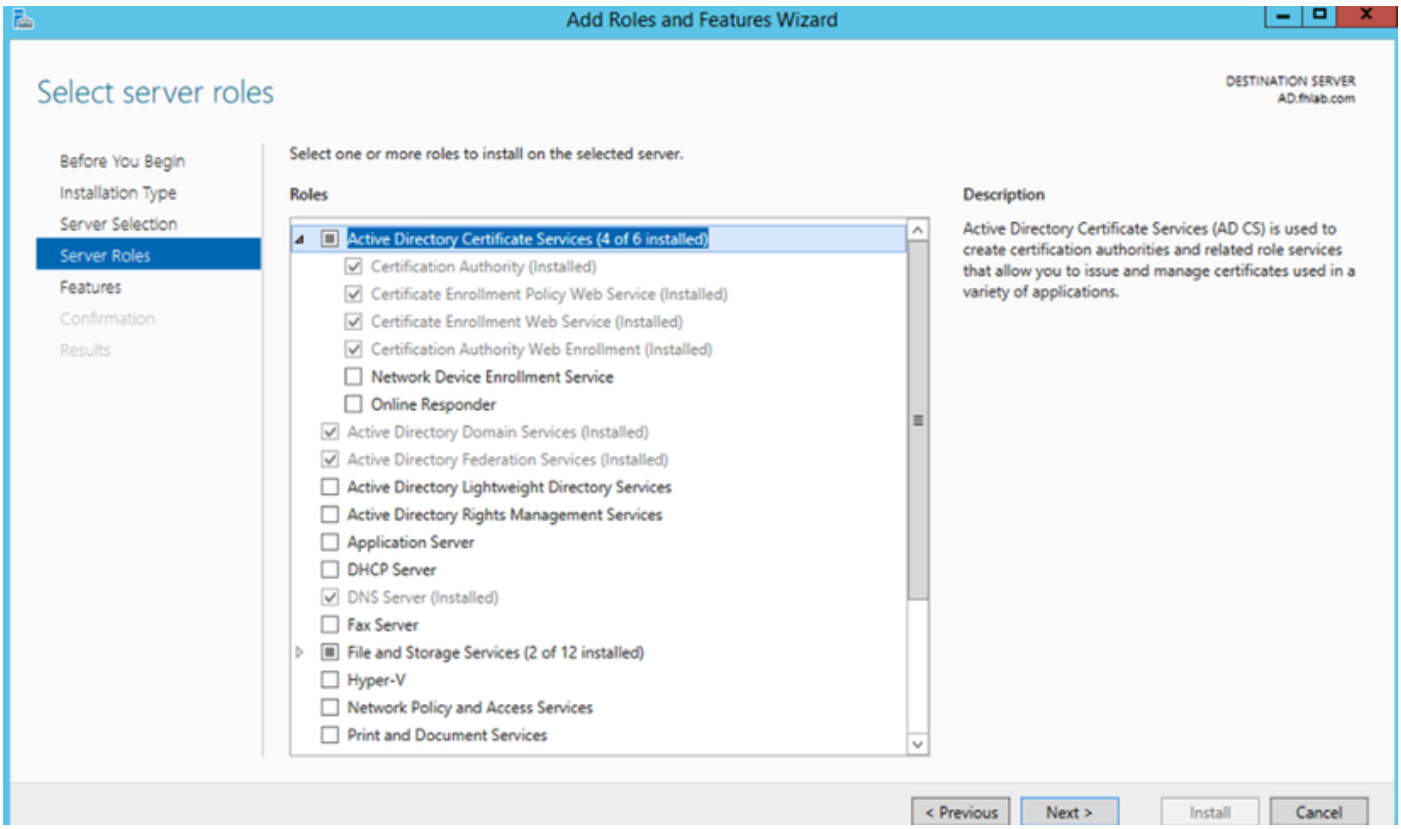
Depois de instalar o Windows 2012 R2 com DNS, promova o servidor para um controlador de domínio.

A próxima tarefa será instalar o Microsoft Certificate Services.

Navegue até Gerenciador de servidores e adicione uma nova função:



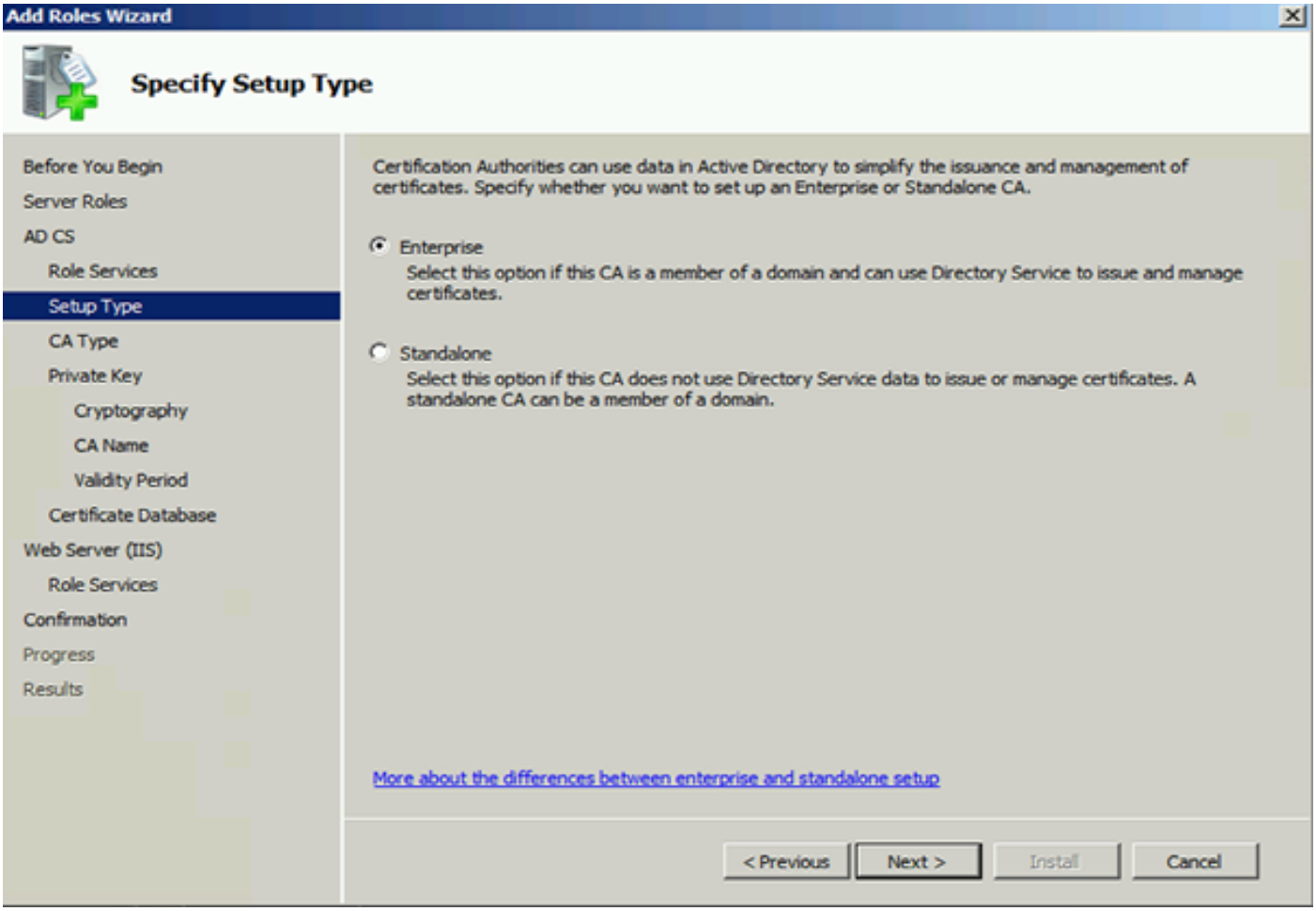
Selecione a função **Serviços de Certificados do Ative Diretory**.



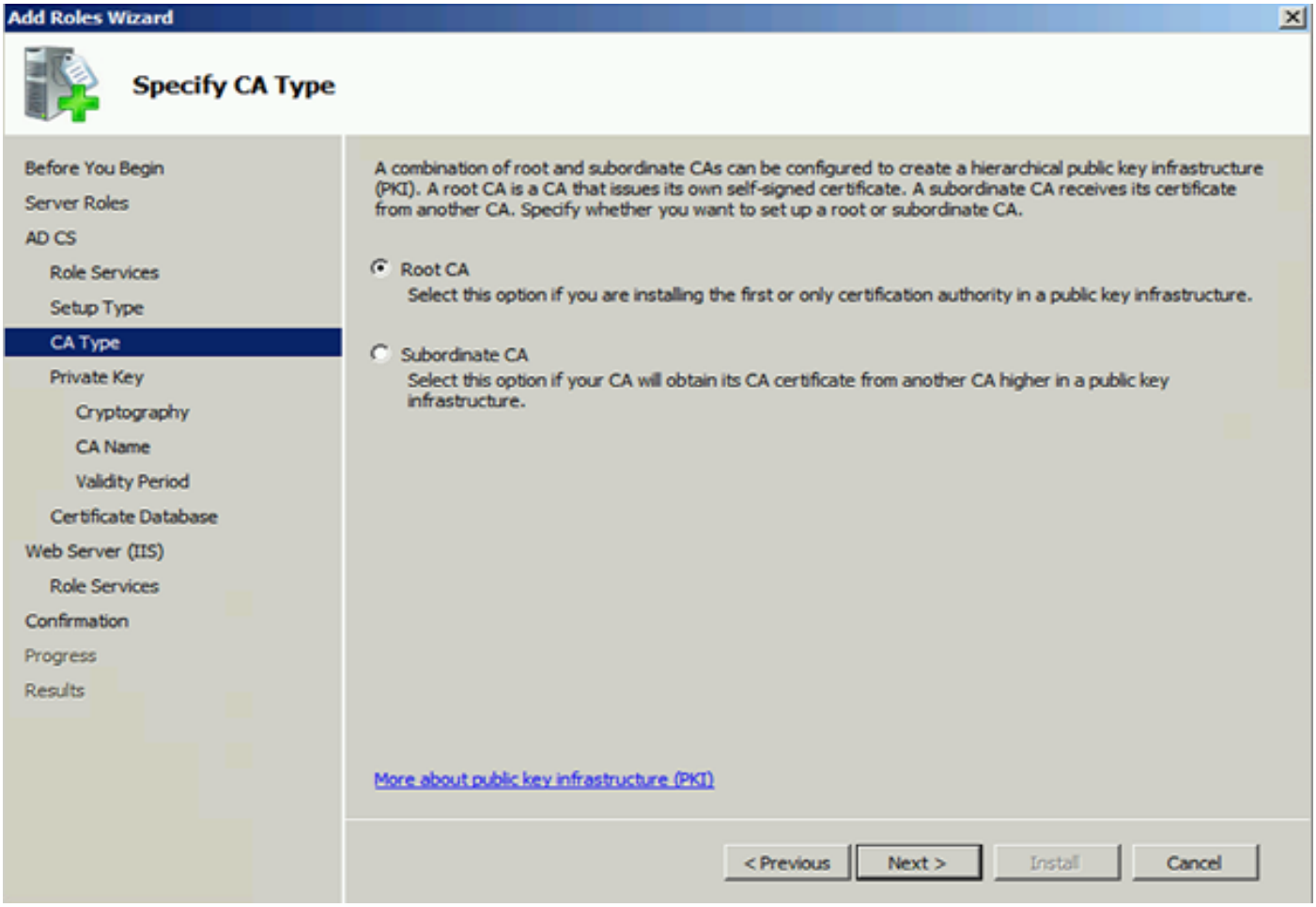
E implante esses serviços - Serviço Web de Política de Registro de Certificado da Autoridade de Certificação primeiro. Depois que essas duas funções forem instaladas, configure-as e instale o **Serviço Web de Inscrição de Certificados** e **Inscrição na Web de Autoridade de Certificação**. Configure-os.

Os serviços e recursos de função adicionais necessários, como o IIS, também serão adicionados quando a Autoridade de Certificação estiver instalada.

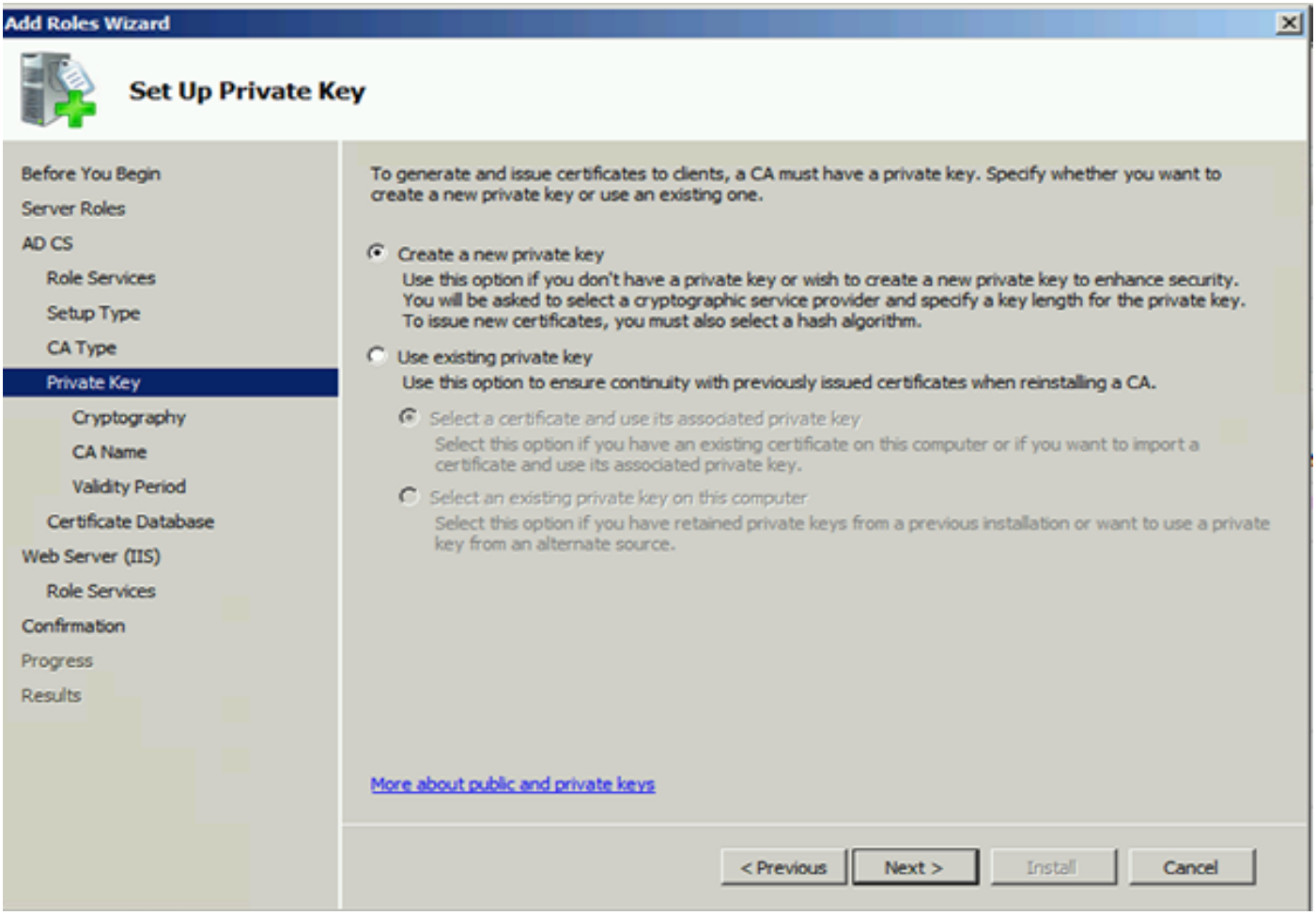
Dependendo da sua implantação, você pode selecionar Empresa ou Independente.



Para o tipo de CA, você pode selecionar CA raiz ou CA subordinada. Se não houver outra CA já em execução na organização, selecione **CA raiz**.

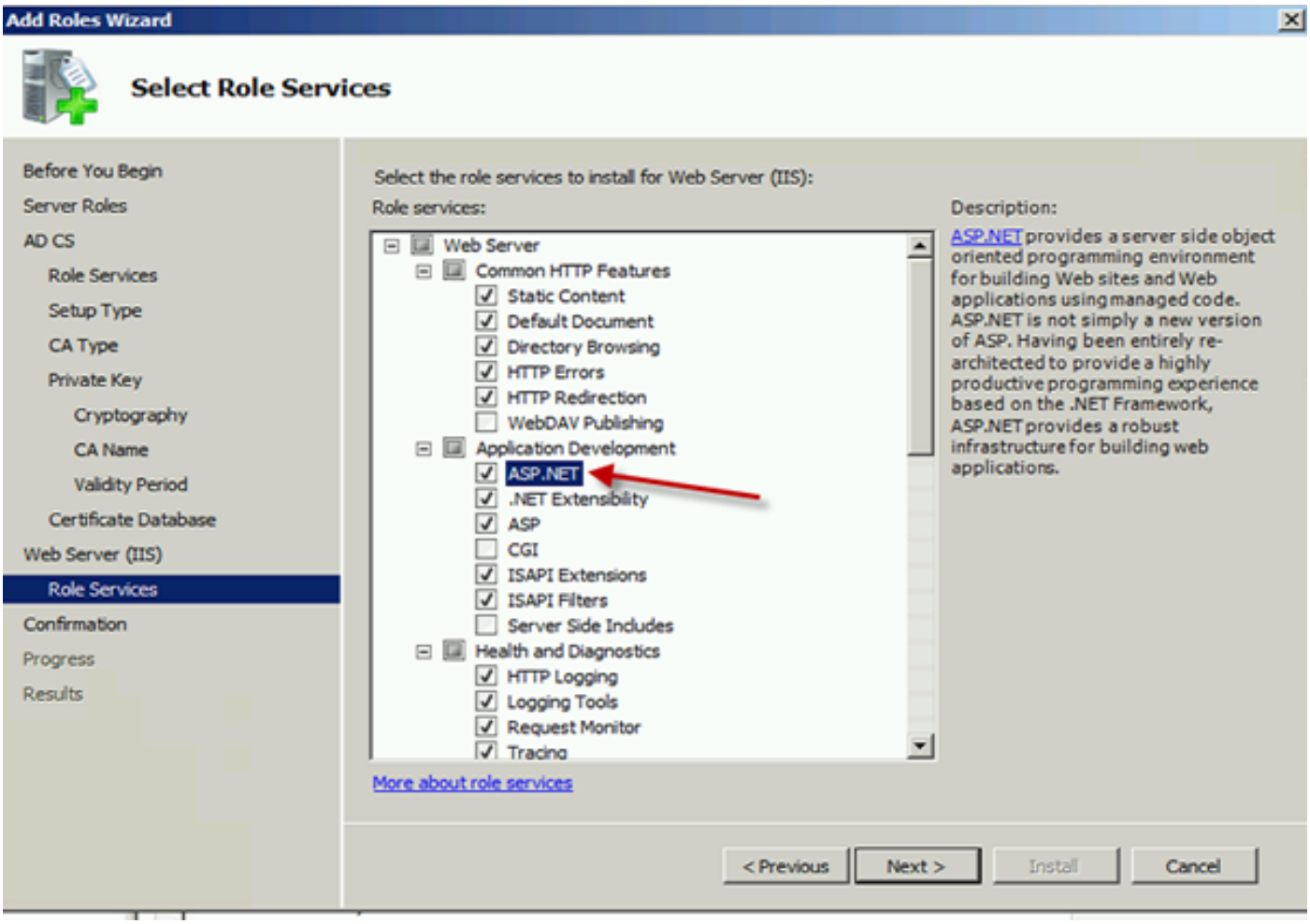


A próxima etapa é criar uma chave privada para sua CA.

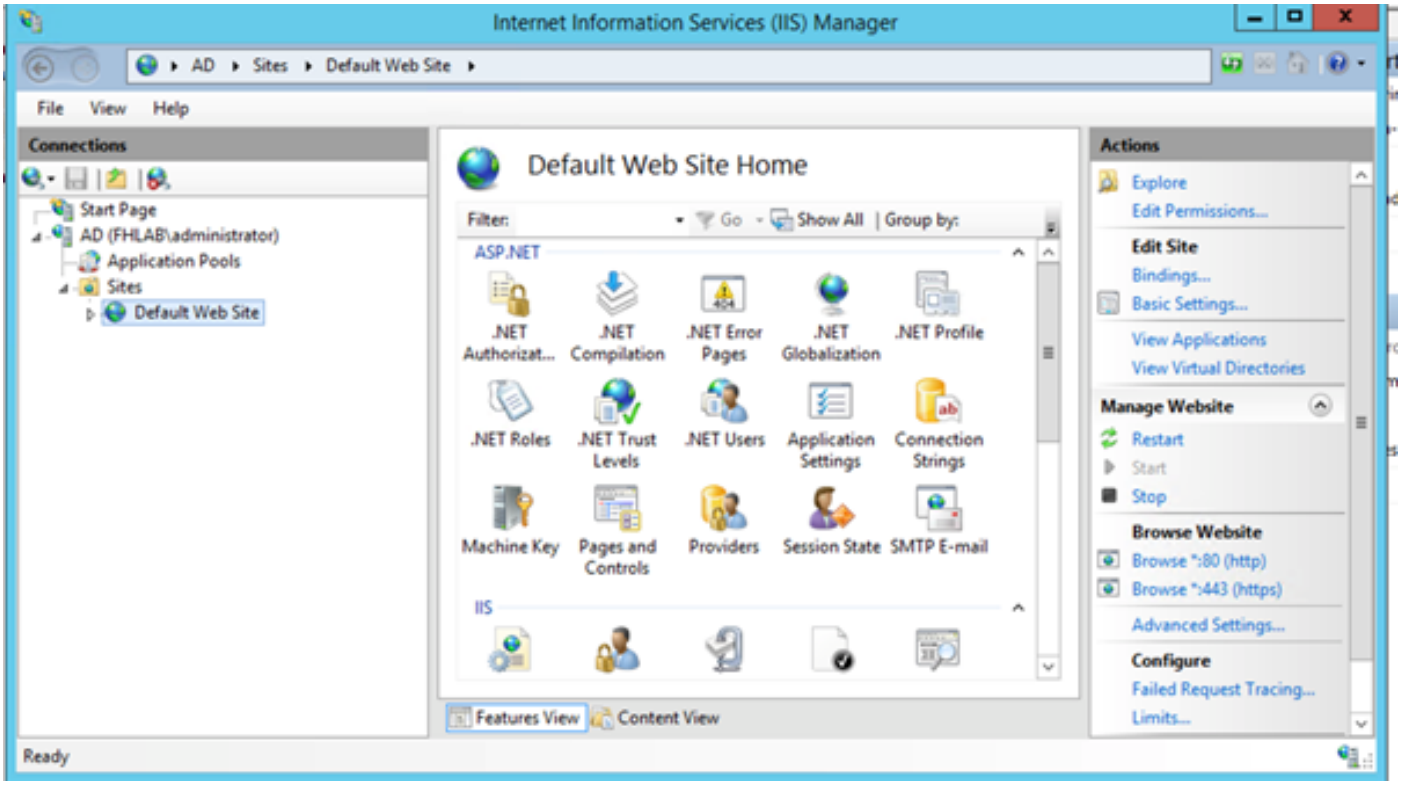


Esta etapa só é necessária se você instalar o ADFS3 em um Windows Server 2012 separado.

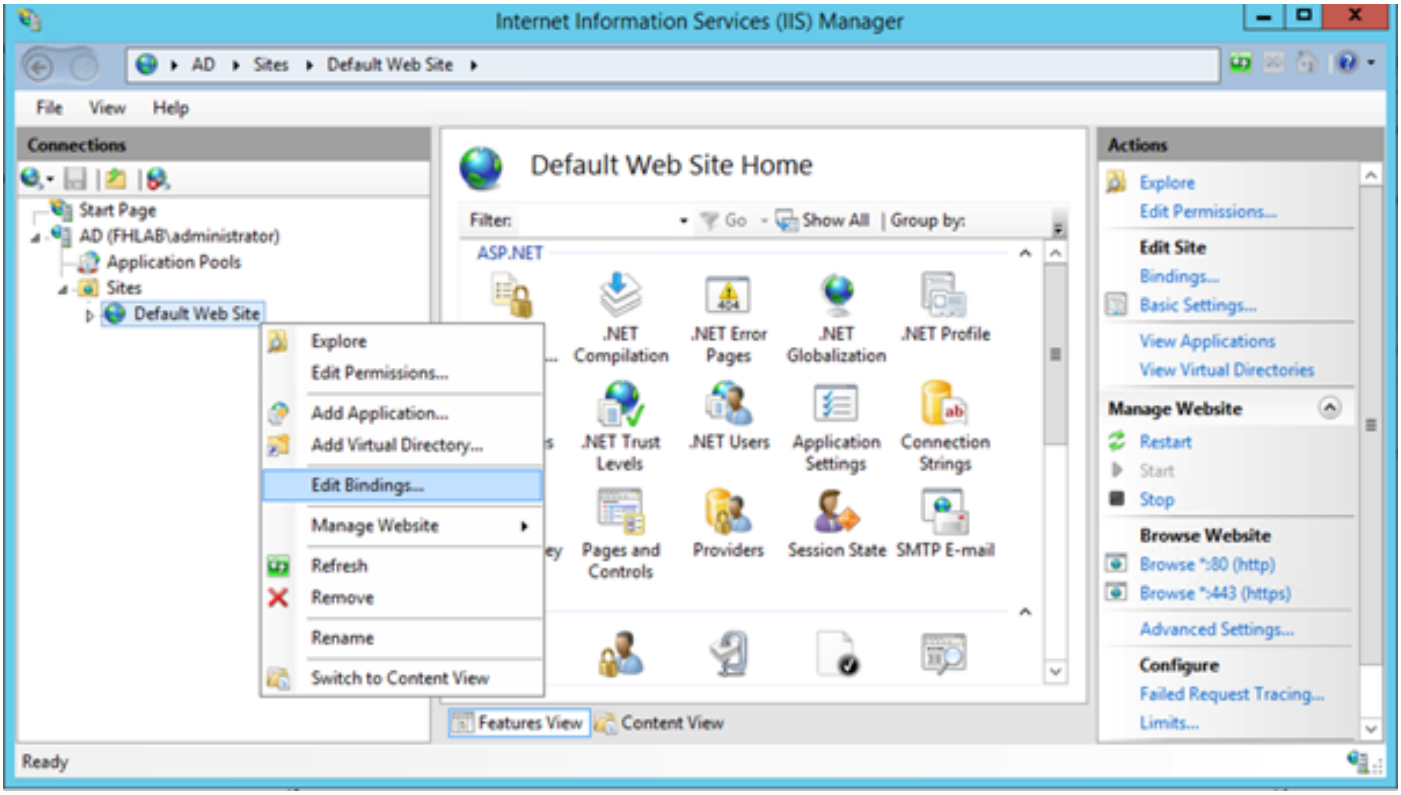
Depois de configurar a AC, os serviços de função do IIS precisam ser configurados. Isso é necessário para a inscrição na Web na CA. Para a maioria das implantações de ADFS, é necessária uma função extra no IIS, clique em **ASP.NET** em Desenvolvimento de Aplicativos.



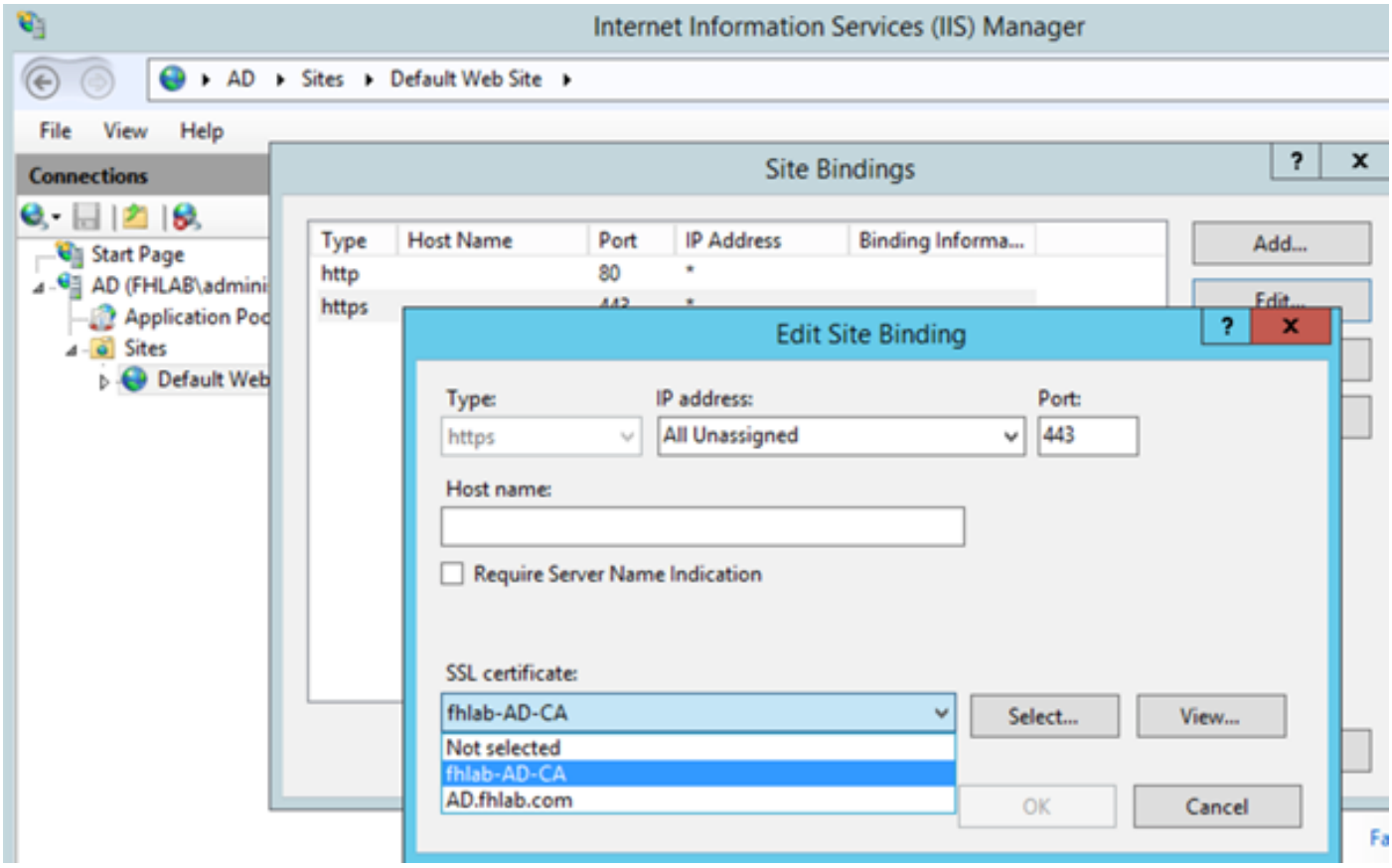
No Server Manager, clique em **Web Server > IIS** e, em seguida, clique com o botão direito do mouse em **Default Web Site**. A associação precisa ser alterada para permitir também HTTPS além do HTTP. Isso é feito para suportar HTTPS.



Selecione **Editar vínculos**.

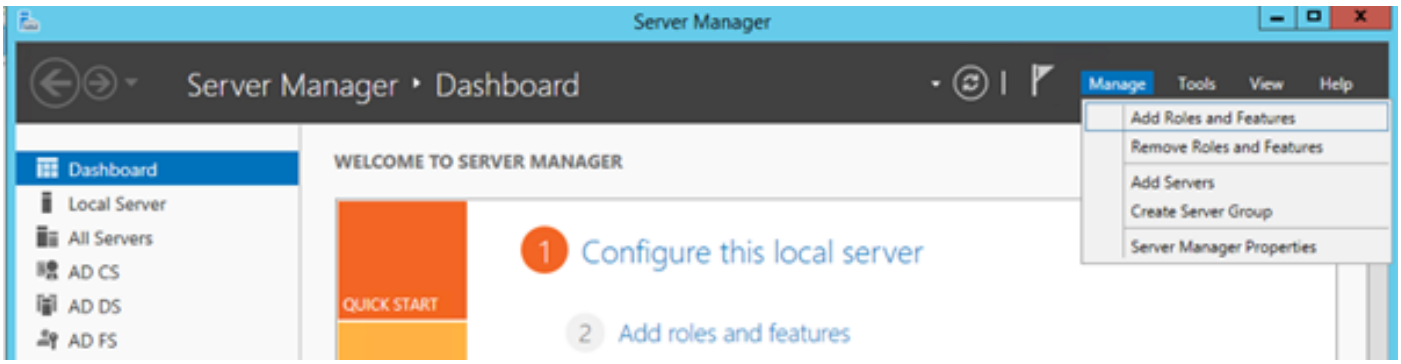


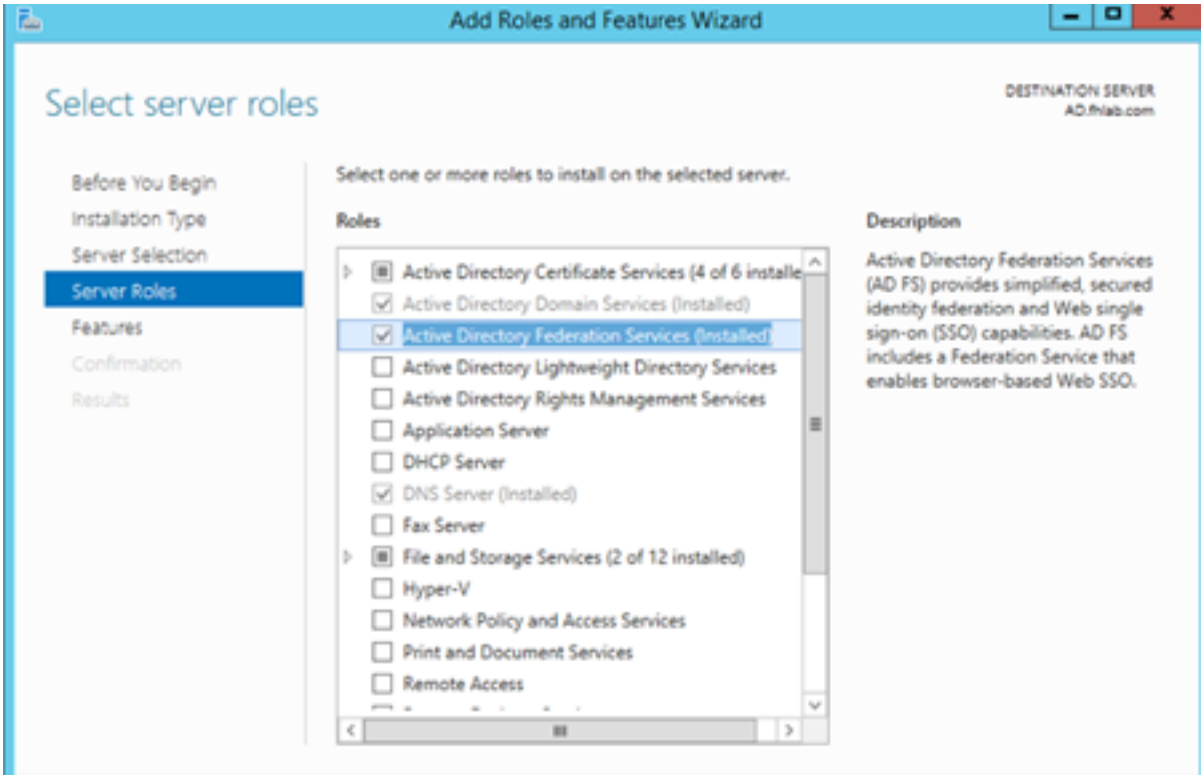
Adicione uma nova associação de site e selecione **HTTPS** como o tipo. Para o certificado SSL, escolha o certificado do servidor que deve ter o mesmo FQDN do seu servidor AD.



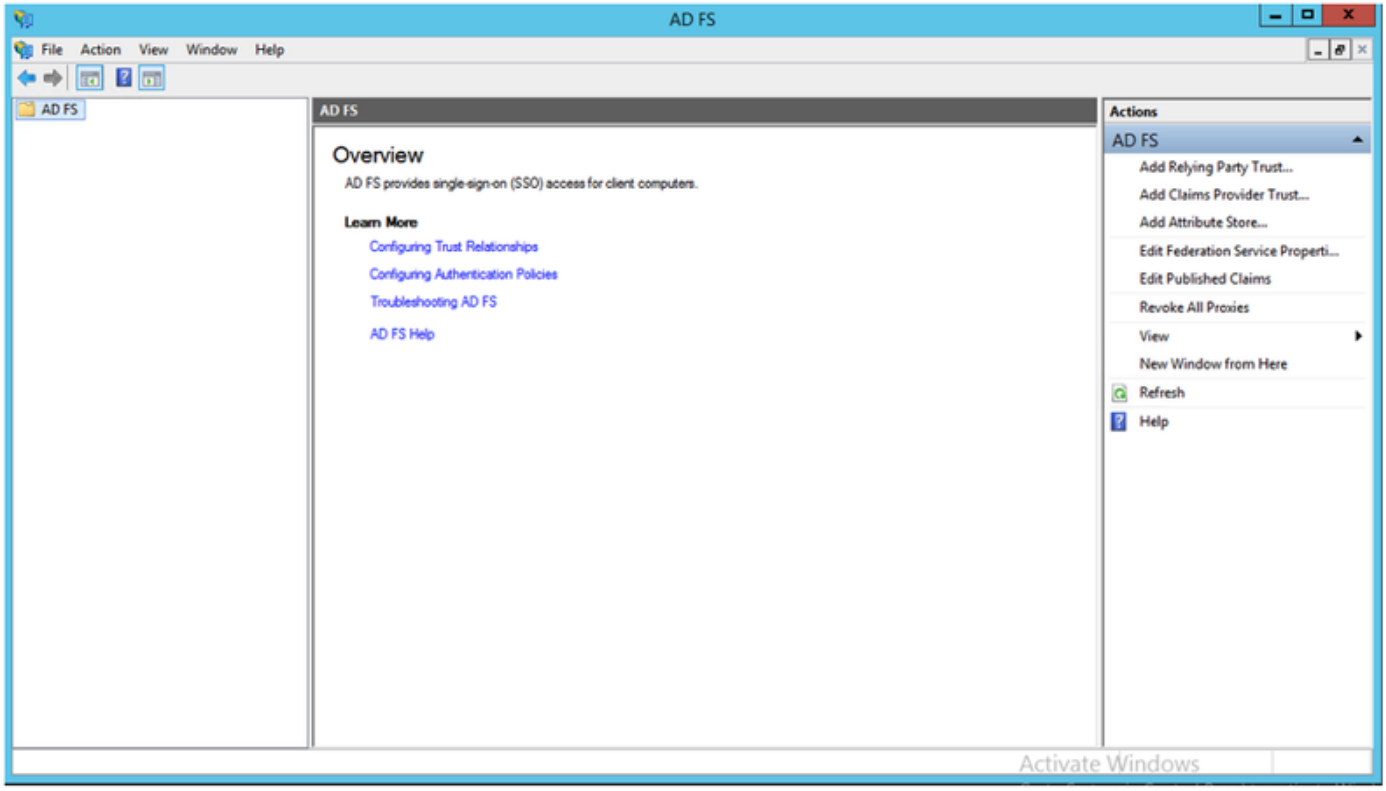
Todas as funções de pré-requisito estão instaladas no ambiente, por isso agora pode continuar com a instalação dos Serviços de Federação do Ative Diretory do ADFS3 (no Windows Server 2012).

Para a Função de Servidor, navegue para **Server Manager > Manage > Add Server Roles and Features** e selecione **Ative Diretory Federation Services** se você instalar o IDP dentro da rede do cliente, na LAN privada.





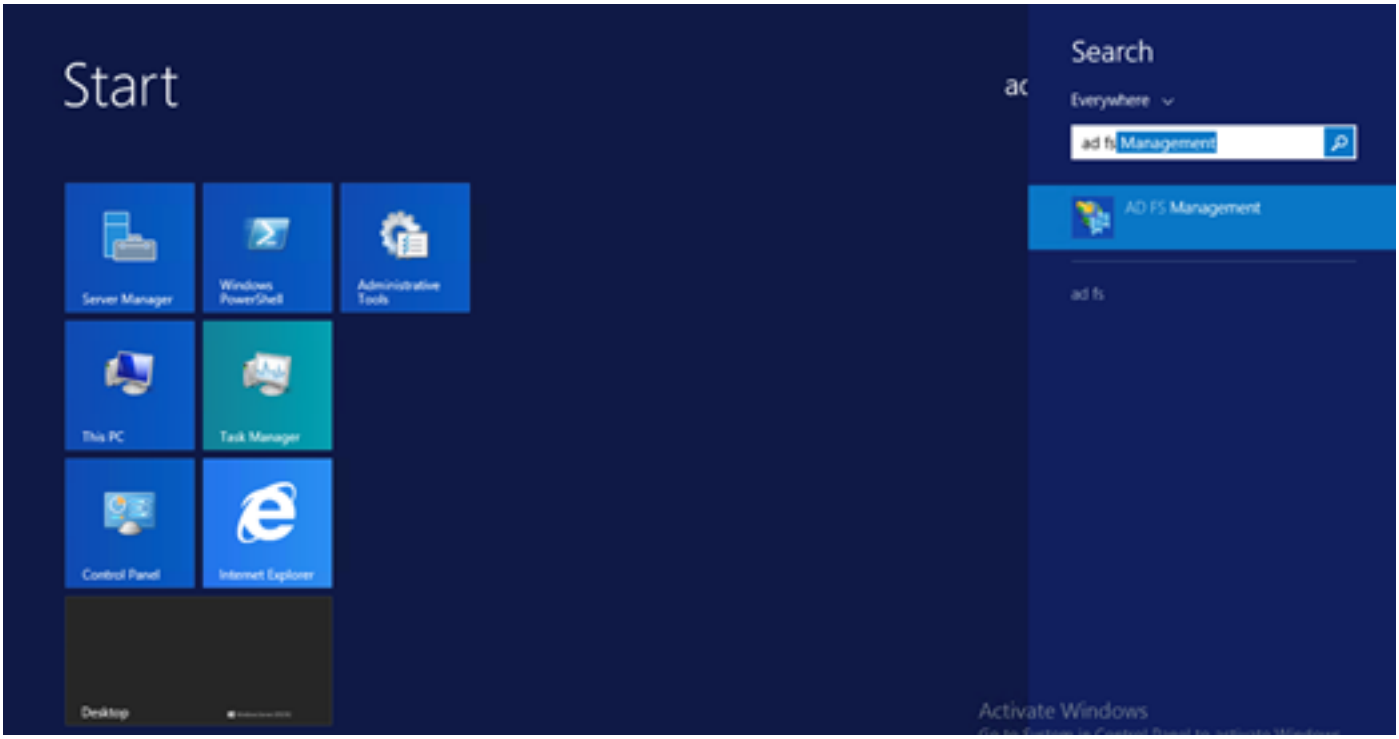
Quando a instalação for concluída, você poderá abri-la na barra de tarefas ou no menu Iniciar.



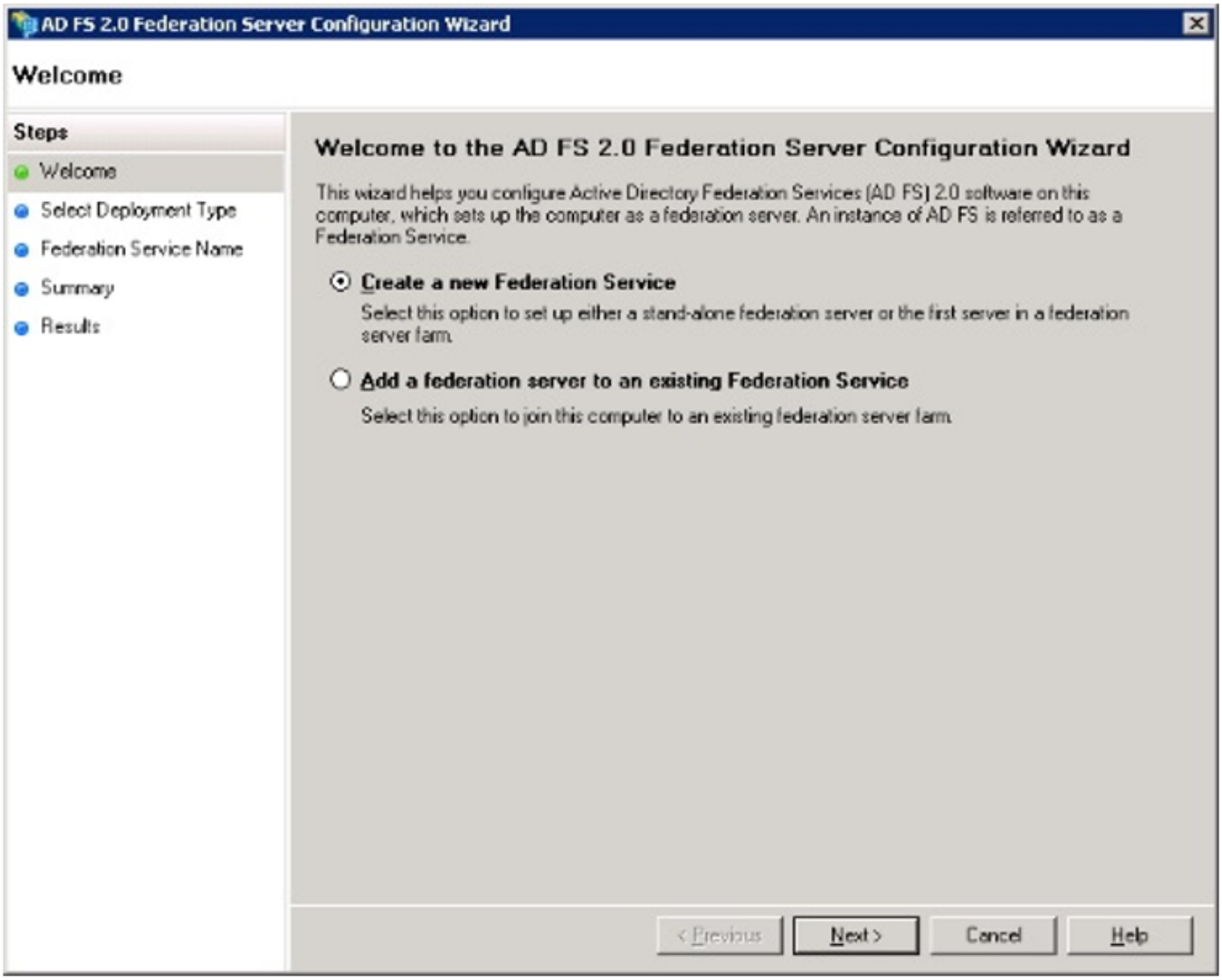
Configuração inicial do ADFS3

Esta seção passará pela instalação de um novo servidor de Federação independente, mas também poderá ser usada para instalá-lo em um Controlador de Domínio

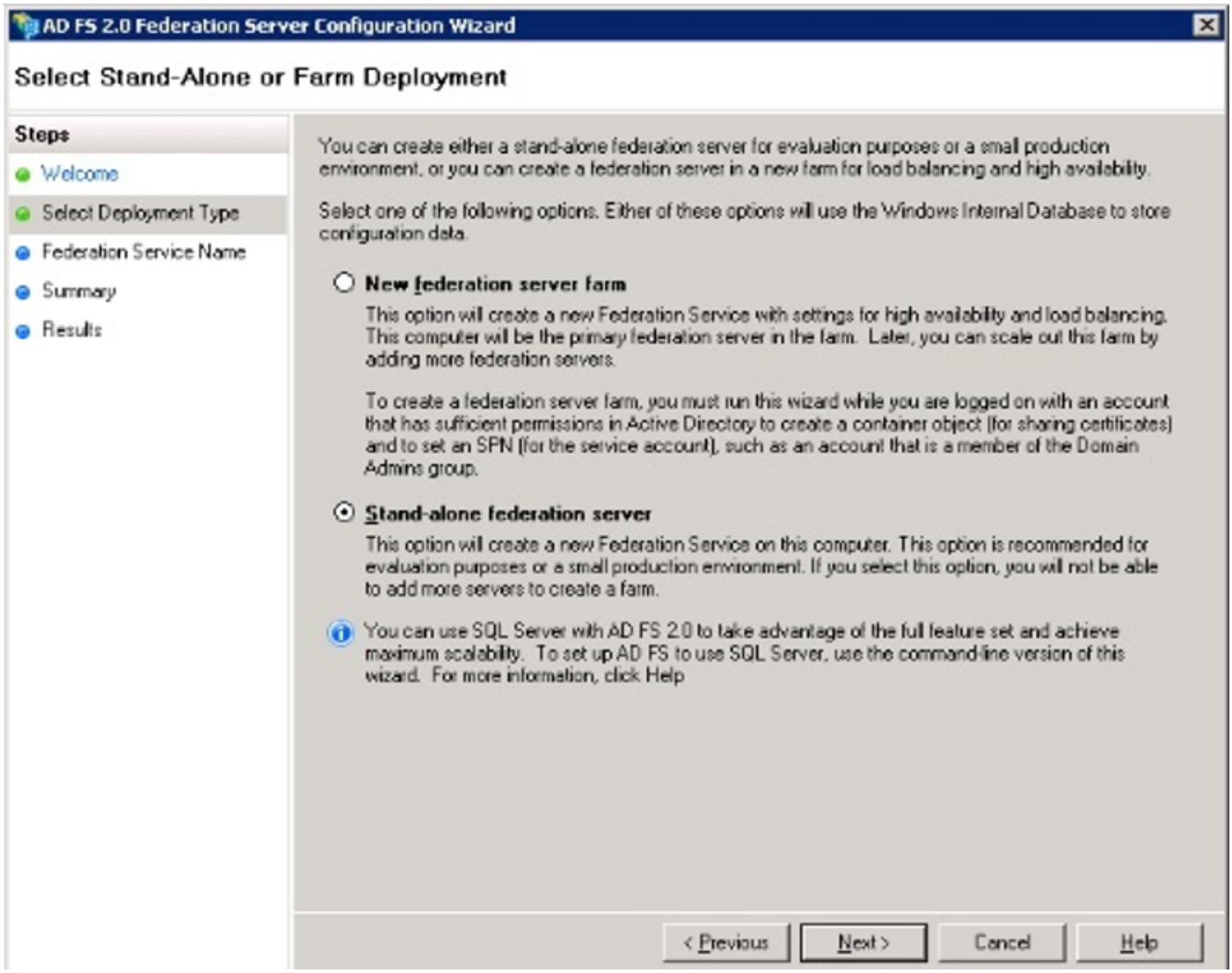
Selecione **Windows** e digite **Gerenciamento do AD FS** para iniciar o console de Gerenciamento do ADFS como mostrado na imagem.



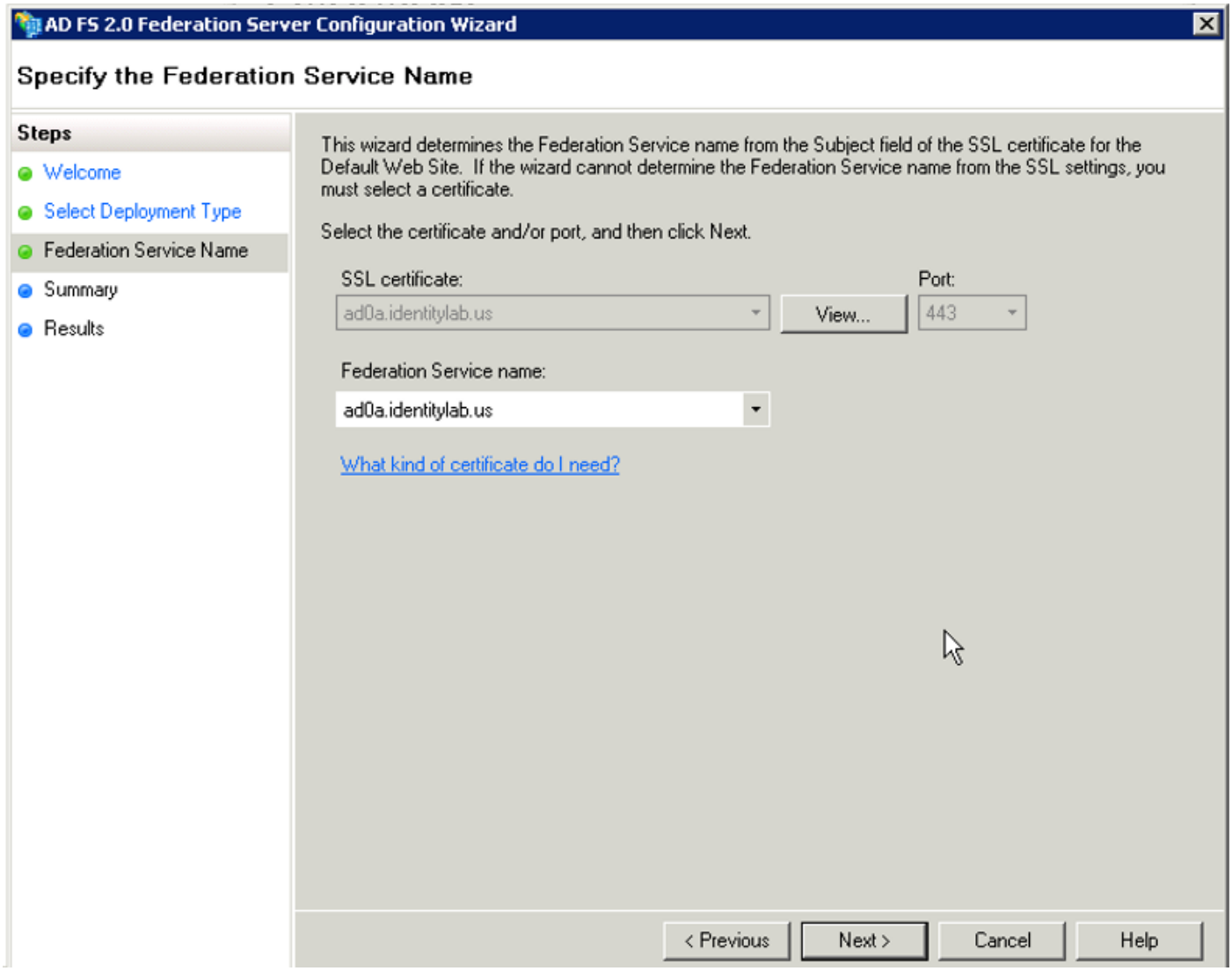
Selecione a opção **Assistente de Configuração do Servidor de Federação do AD FS 3.0** para iniciar a configuração do servidor ADFS. Essas capturas de tela representam as mesmas etapas no AD FS 3.



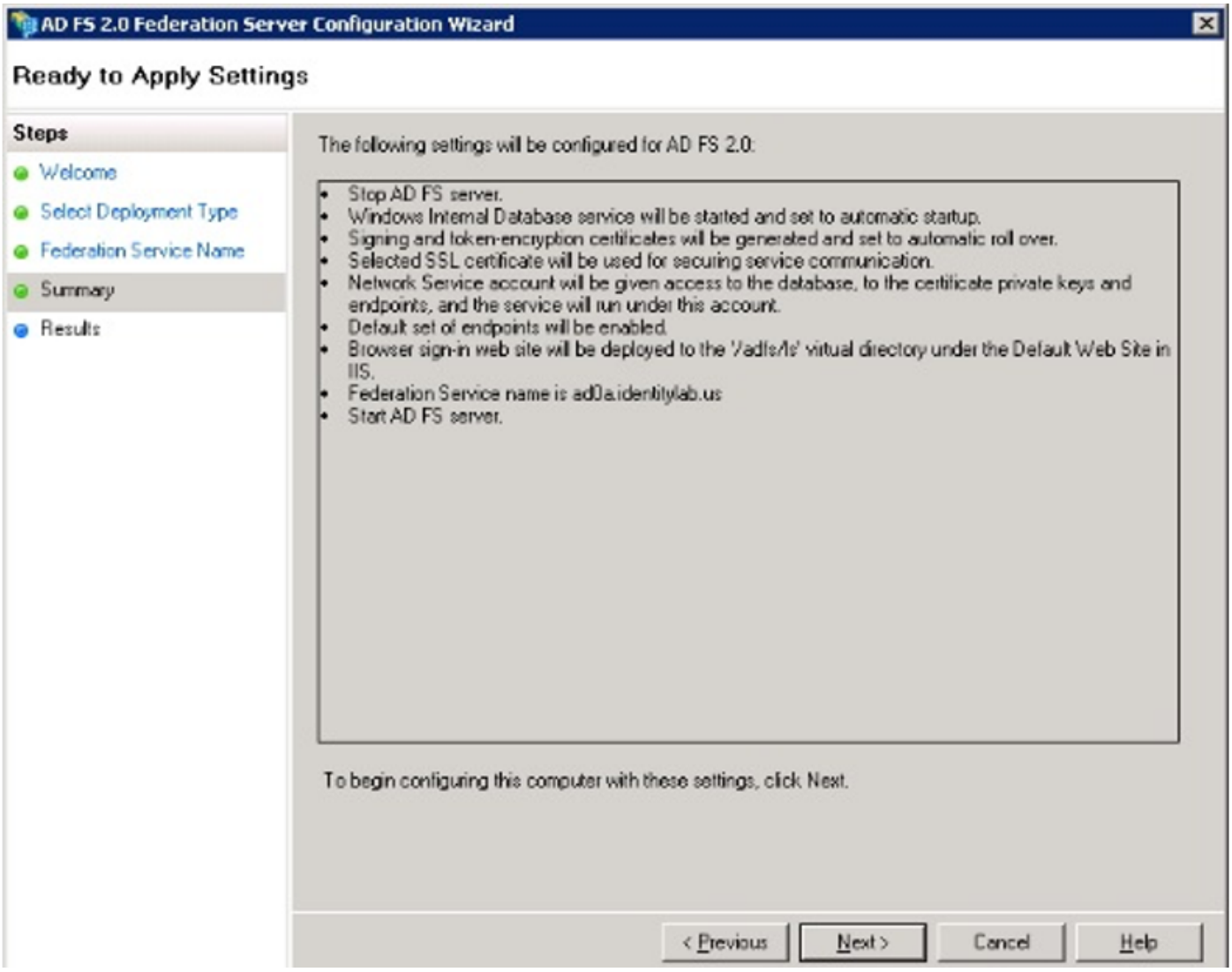
Selecione Criar um novo **Serviço de Federação** e clique em **Avançar**.



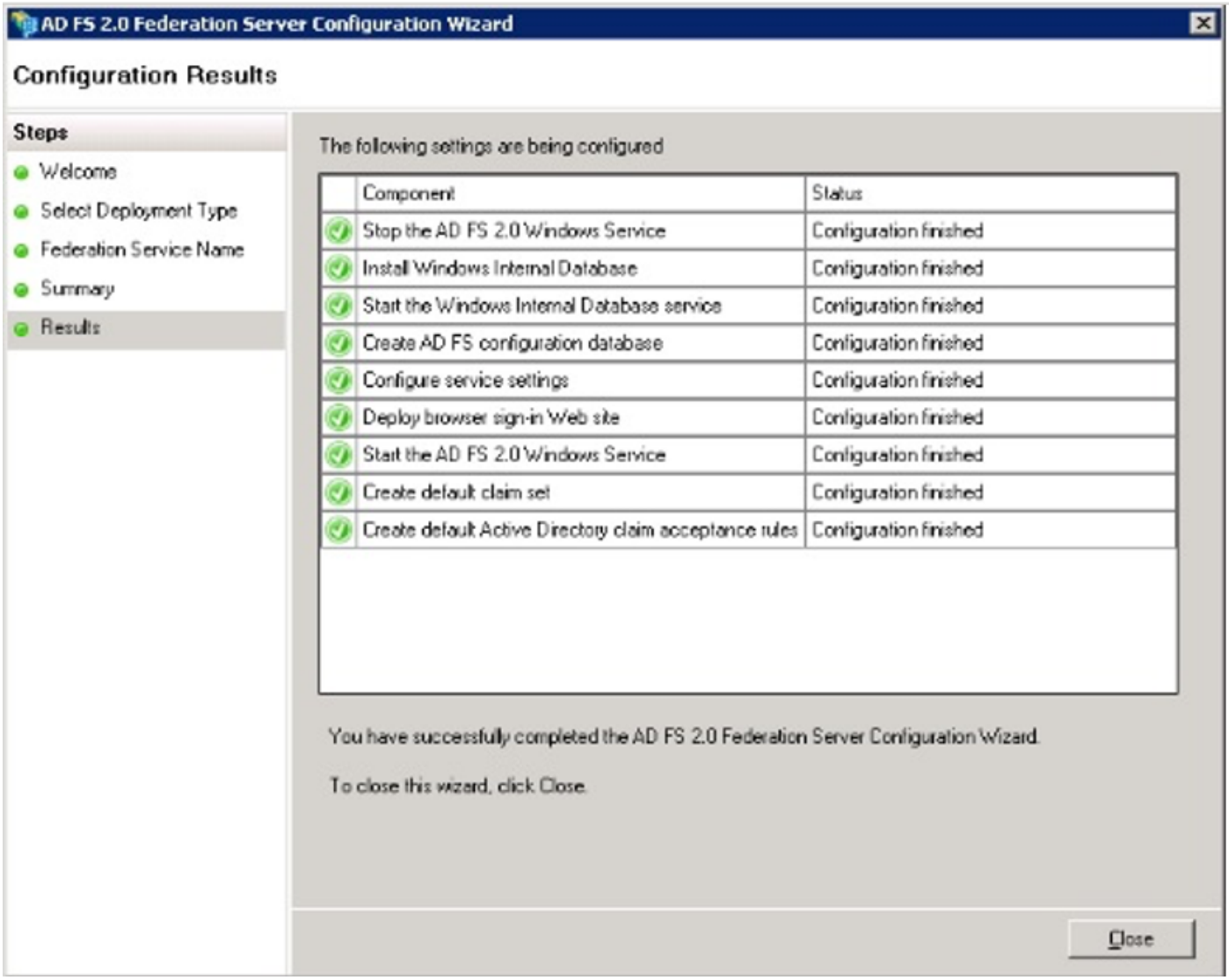
Selecione o Servidor de Federação Independente e clique em **Avançar** conforme mostrado na imagem.



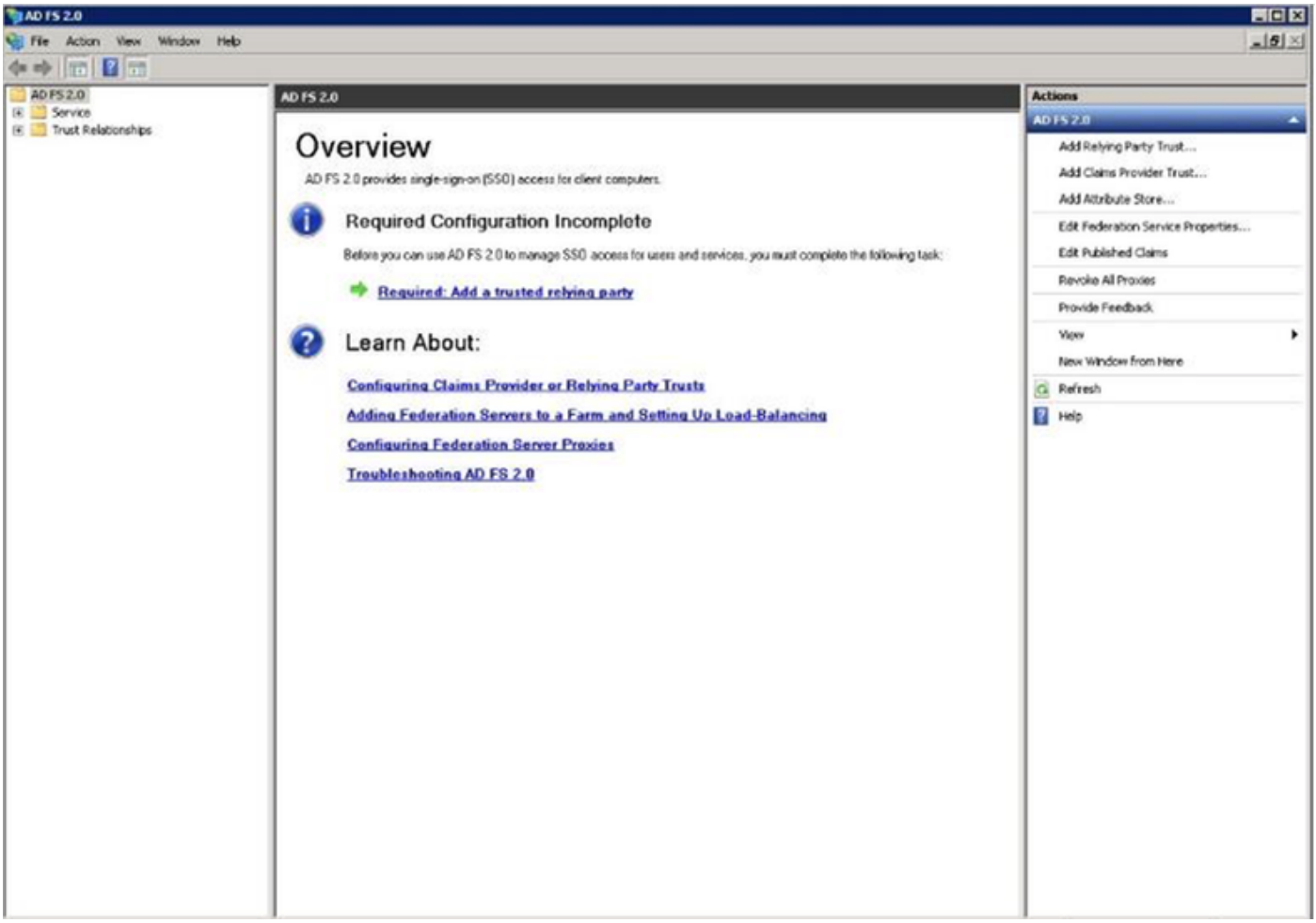
Em certificado SSL, selecione o certificado autoassinado na lista. O nome do Serviço de Federação será preenchido automaticamente. Clique em Next.



Revise as configurações e clique em **Avançar** para aplicar as configurações.



Confirme se todos os componentes foram concluídos com êxito e clique em **Fechar** para encerrar o assistente e retornar ao console de gerenciamento principal. Isso pode levar alguns minutos.

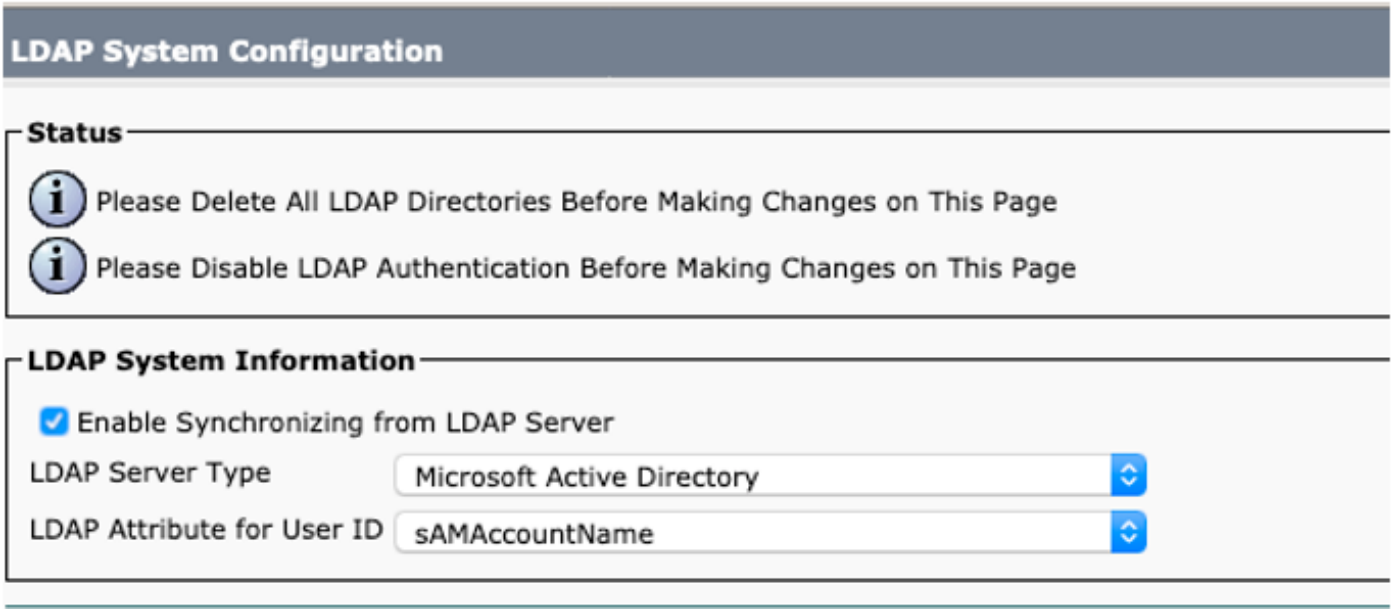


O ADFS agora está efetivamente ativado e configurado como um provedor de identidade (IdP). Em seguida, você precisa adicionar o CUCM como um parceiro confiável. Antes de fazer isso, é necessário primeiro fazer alguma configuração na Administração do CUCM.

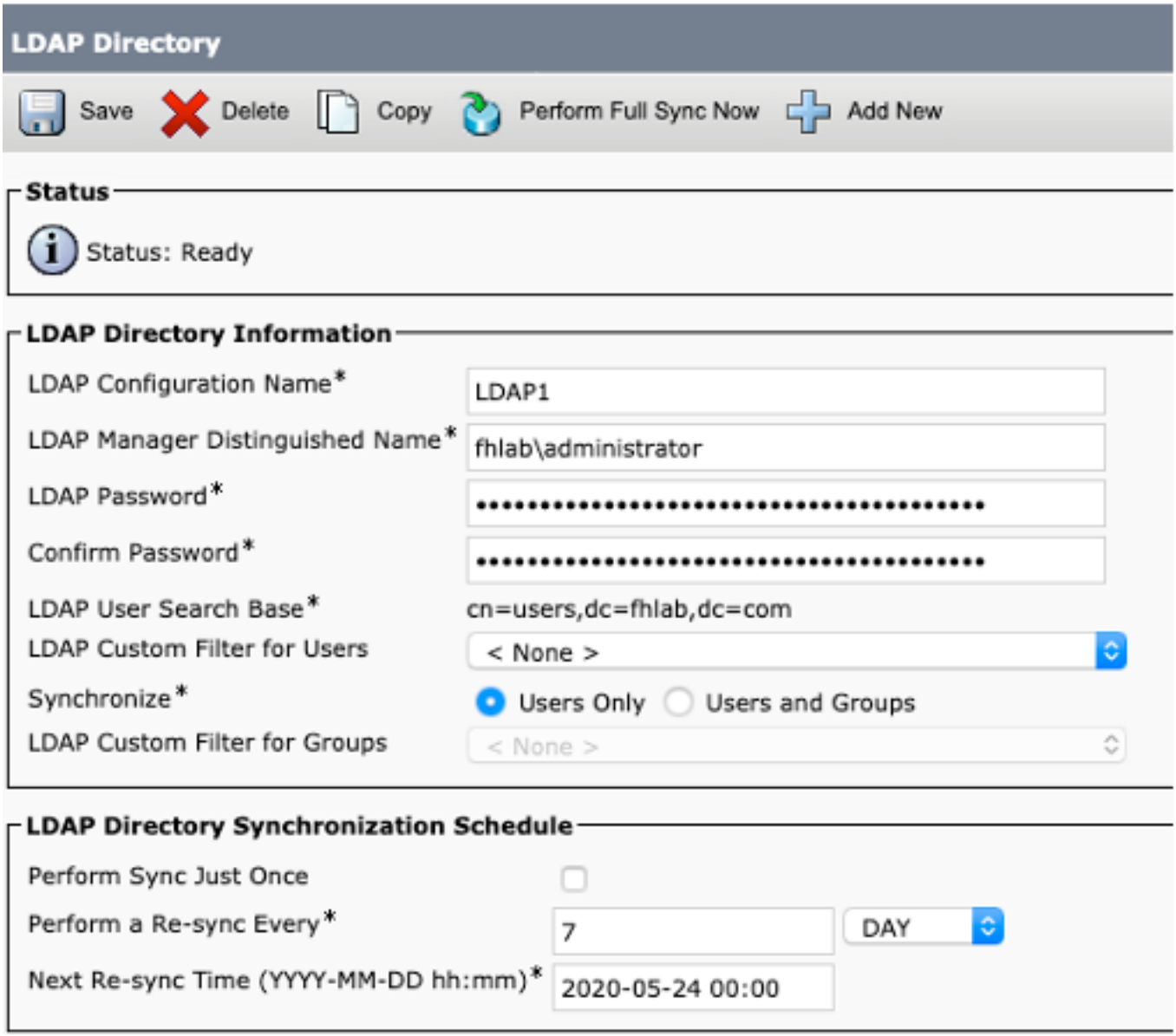
Configurar SSO no CUCM com ADFS

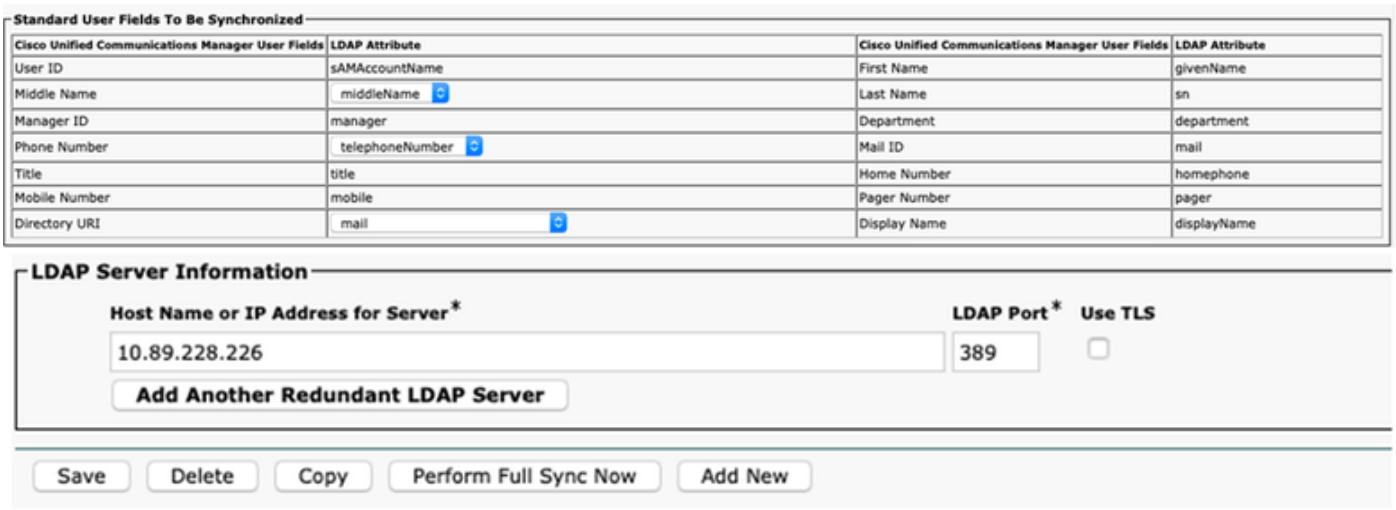
Configuração LDAP

O cluster precisa ser integrado ao LDAP com o Ative Diretory e a autenticação LDAP precisa ser configurada antes de prosseguir. Navegue até a **guia Sistema > Sistema LDAP** conforme mostrado na imagem.



Em seguida, navegue até a **guia Sistema > Diretório LDAP**.





Standard User Fields To Be Synchronized

Cisco Unified Communications Manager User Fields	LDAP Attribute	Cisco Unified Communications Manager User Fields	LDAP Attribute
User ID	sAMAccountName	First Name	givenName
Middle Name	middleName	Last Name	sn
Manager ID	manager	Department	department
Phone Number	telephoneNumber	Mail ID	mail
Title	title	Home Number	homephone
Mobile Number	mobile	Pager Number	pager
Directory URI	mail	Display Name	displayName

LDAP Server Information

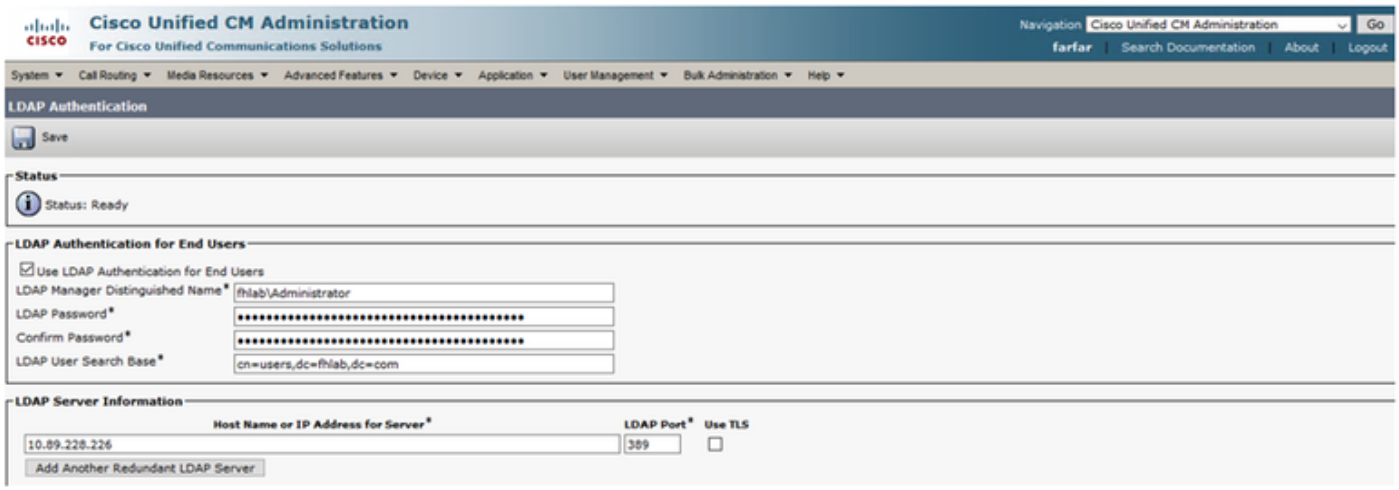
Host Name or IP Address for Server* | LDAP Port* | Use TLS

10.89.228.226 | 389

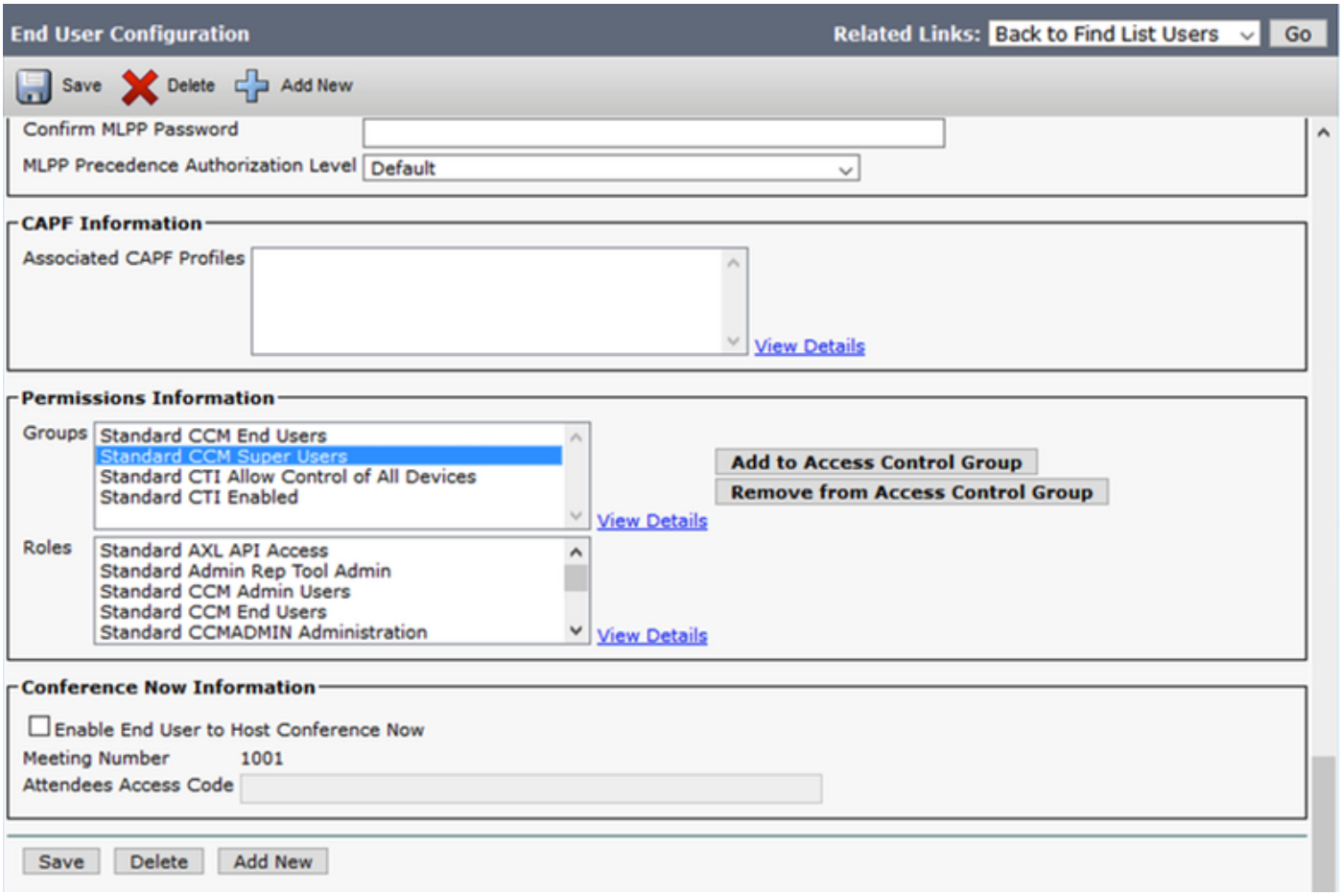
Add Another Redundant LDAP Server

Save | Delete | Copy | Perform Full Sync Now | Add New

Após os usuários do Ative Diretory terem sido sincronizados com o CUCM, a autenticação LDAP precisa ser configurada.



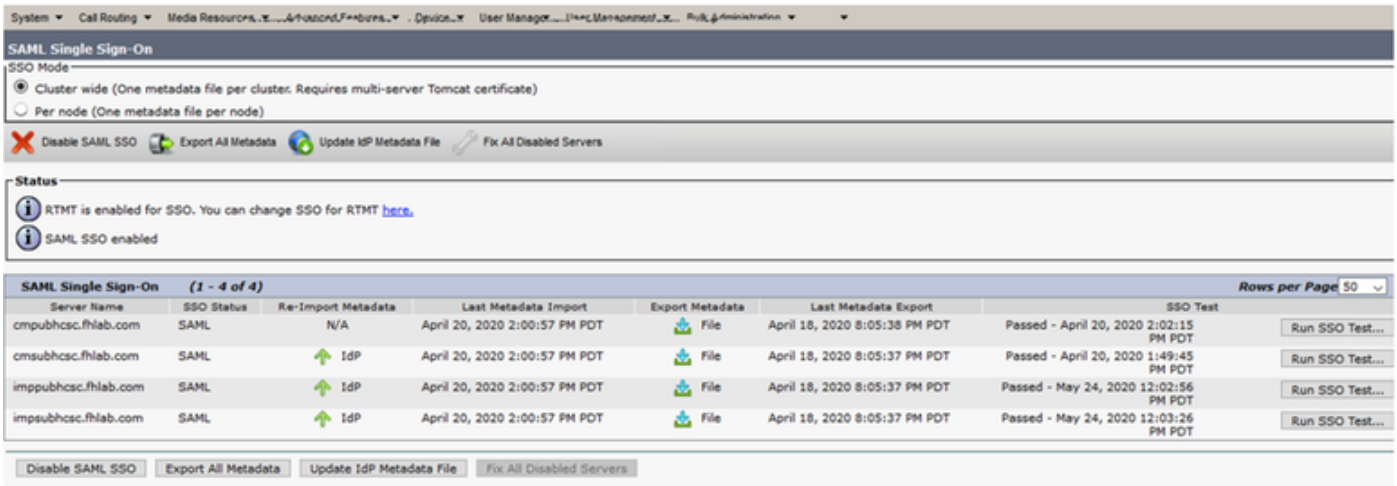
Um usuário final no CUCM precisa ter determinados grupos de controle de acesso atribuídos ao seu perfil de usuário final. O ACG é o padrão para superusuários do CCM. O usuário será usado para testar o SSO quando o ambiente estiver pronto.



Metadados do CUCM

Esta seção mostrará o processo para o Editor do CUCM.

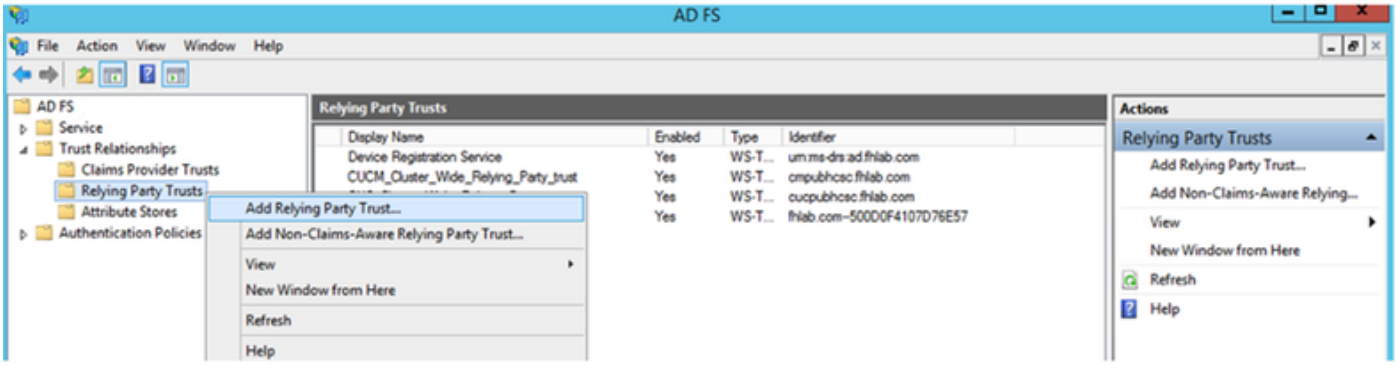
A primeira tarefa é obter os metadados do CUCM, para o que você precisa navegar até a URL; **https://<CUCM Pub FQDN>:8443/ssosp/ws/config/metadados/sp** ou pode ser baixado da **guia System > SAML Single Sign-on**. Isso pode ser feito por nó ou por cluster. Preferível fazer este cluster inteiro.



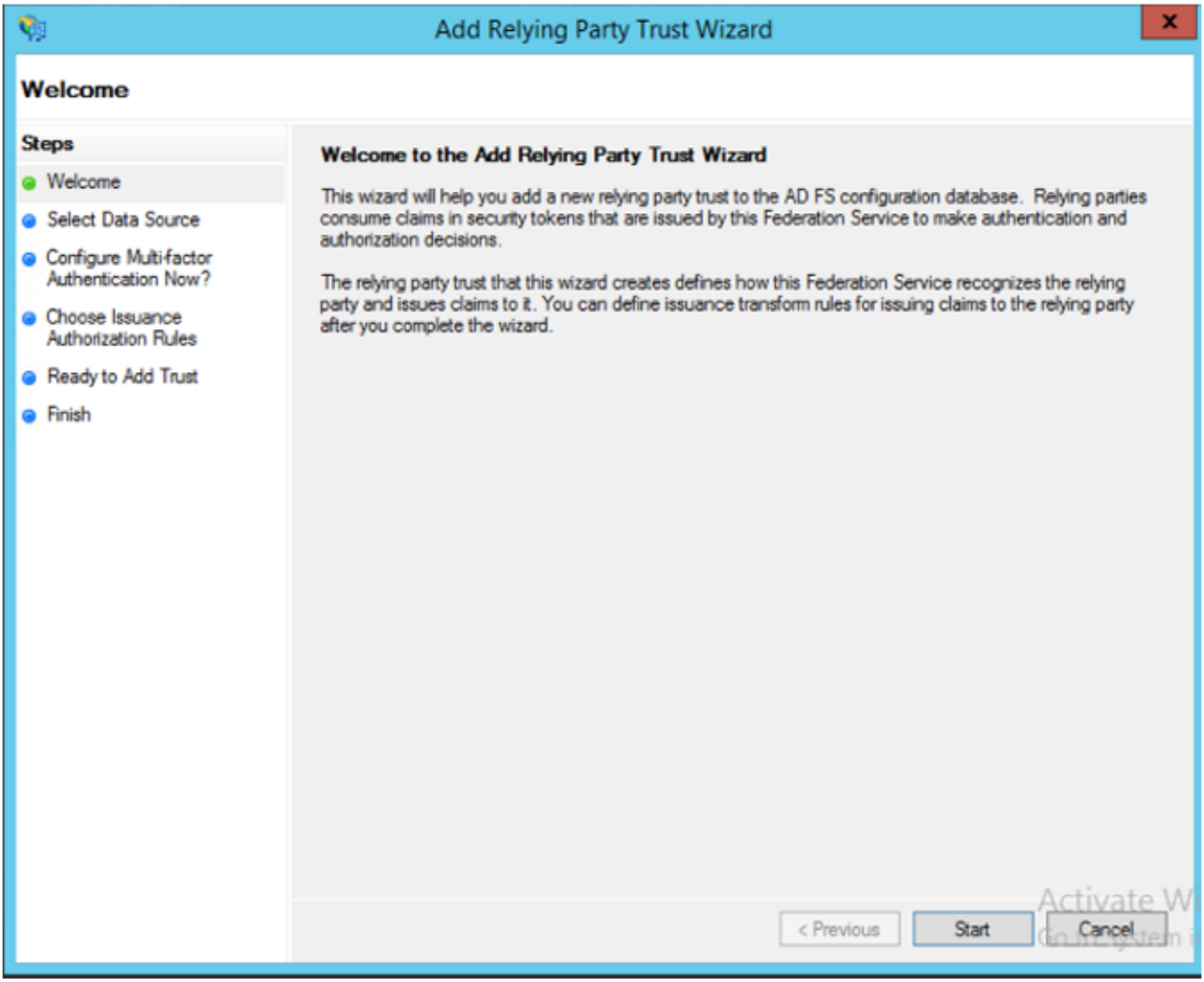
Salve os dados localmente com um nome significativo como sp_cucm0a.xml, você precisará deles depois.

Configurar entidade confiadora do ADFS

Volte para o console de gerenciamento do AD FS 3.0.

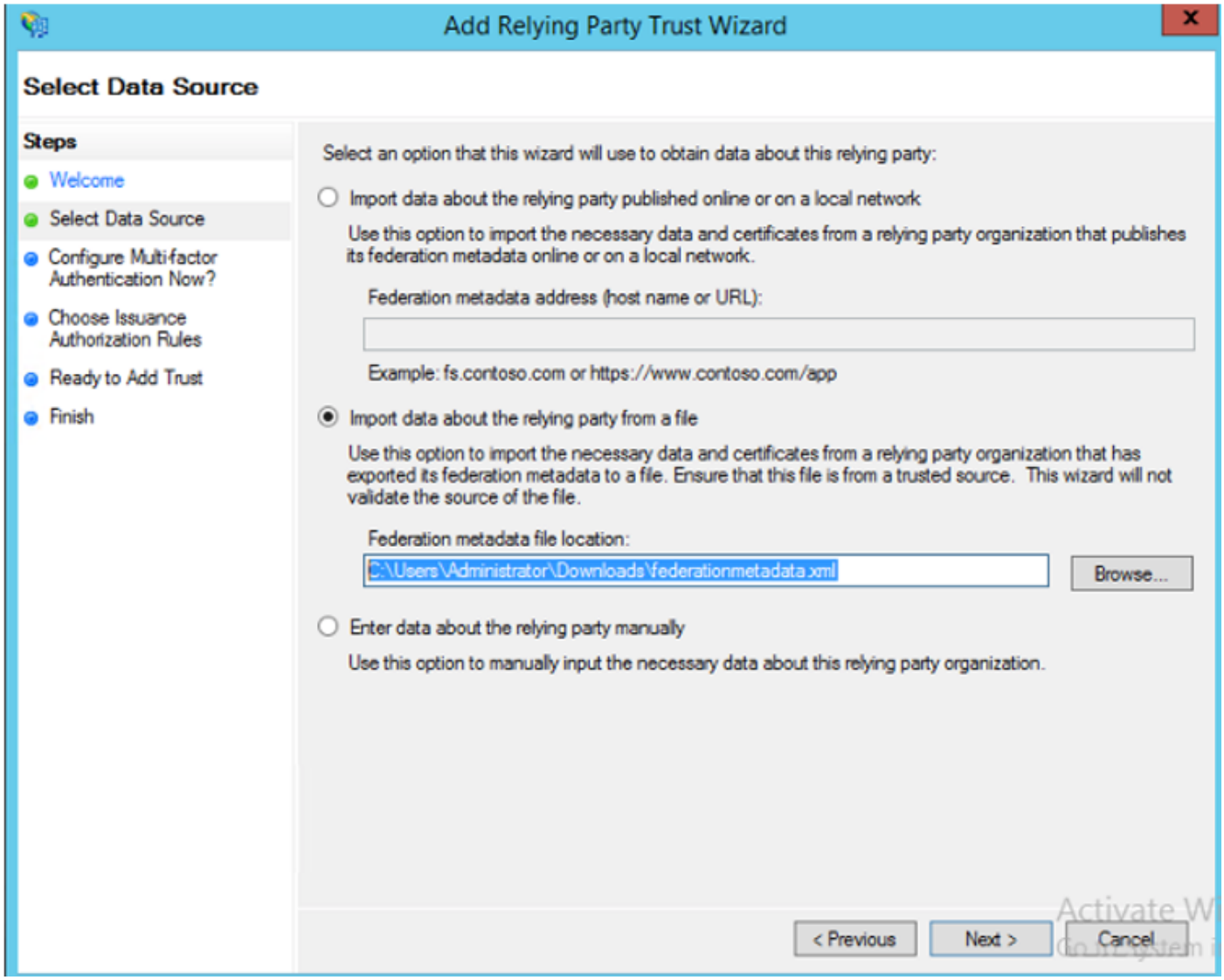


Clique no **Assistente para Adicionar Confiança de Terceiros Confiantes**.

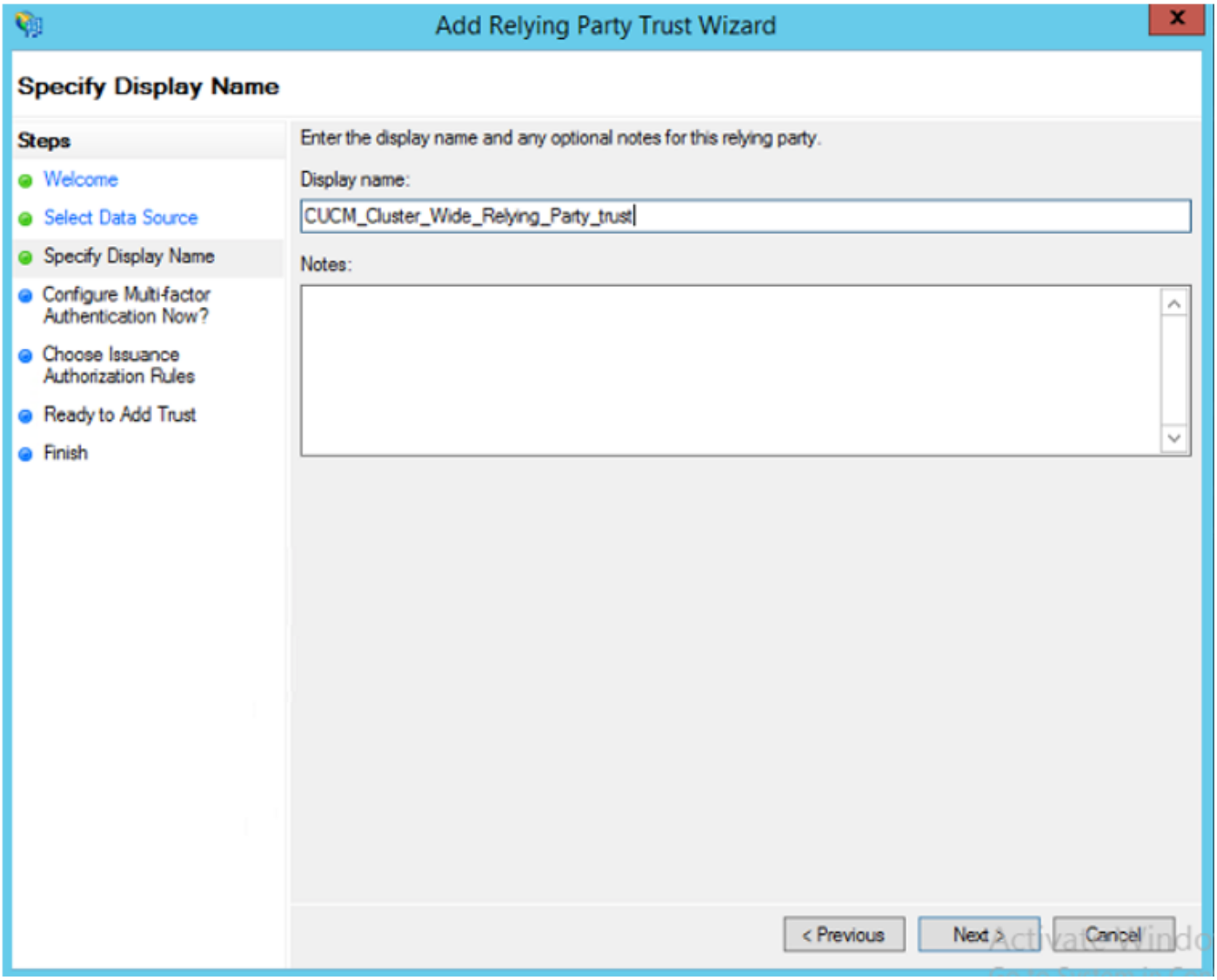


Clique em **Iniciar** para continuar.

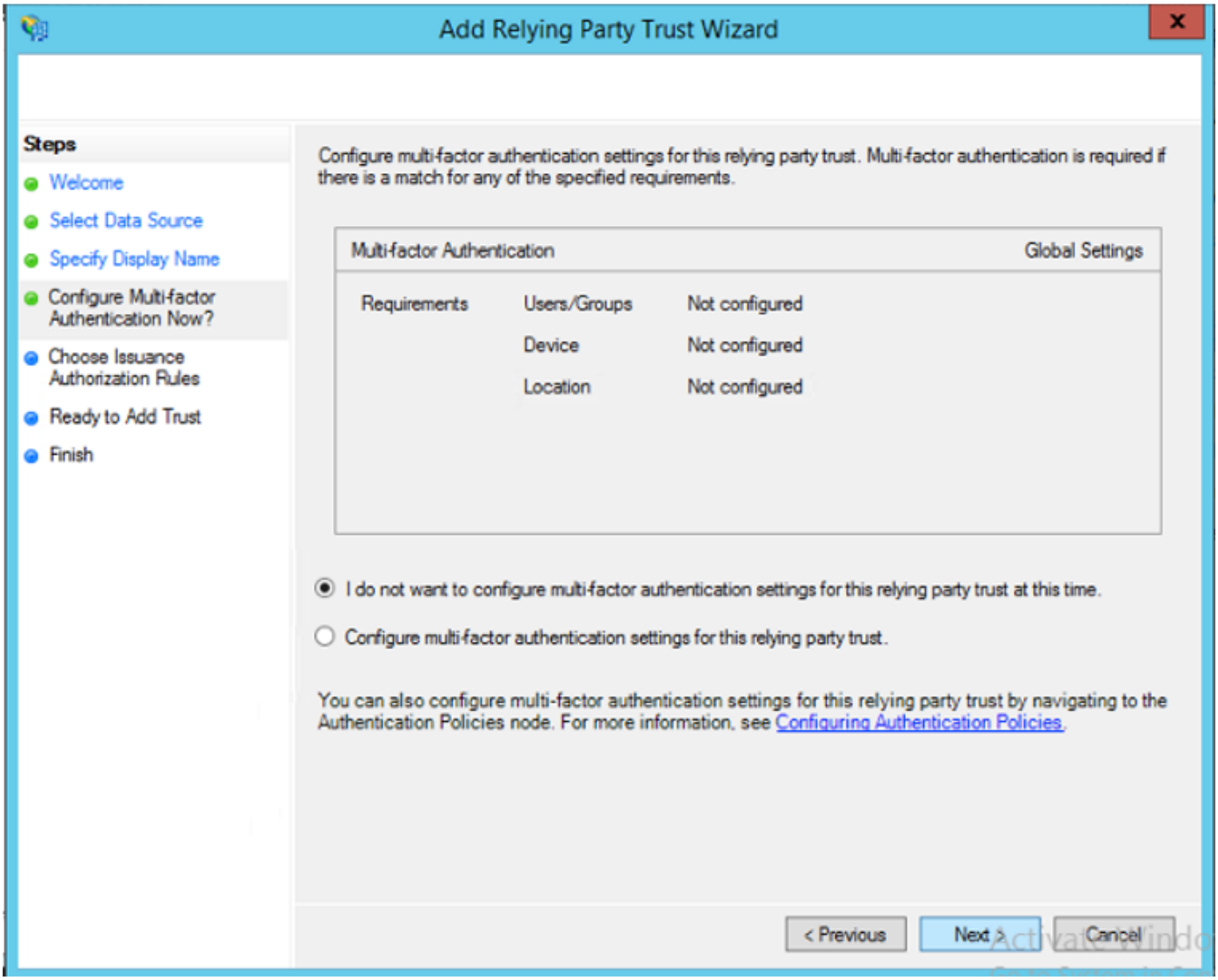
Selecione o arquivo XML de metadados **federationmedatada.xml** que você salvou anteriormente e clique em **Avançar**.



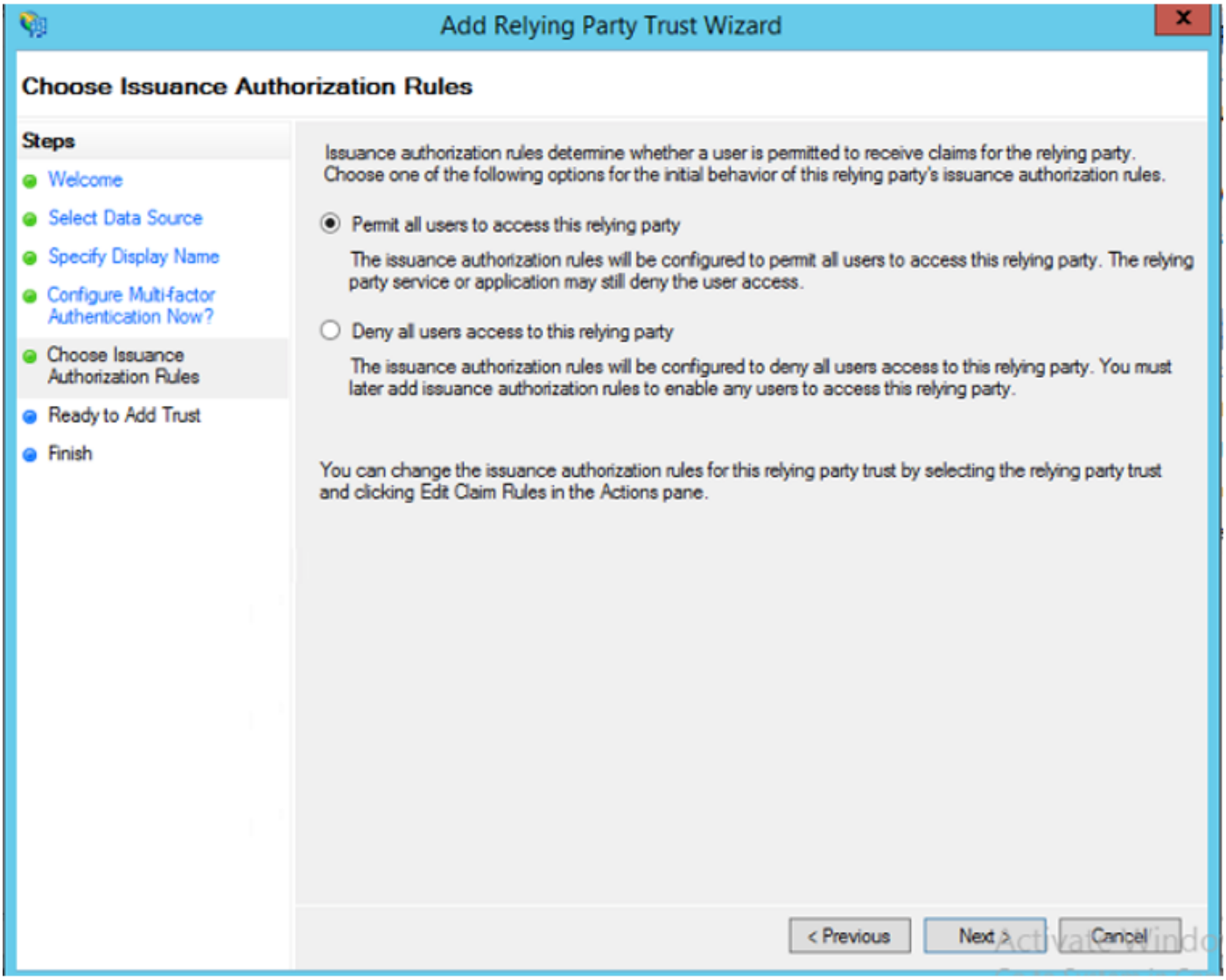
Use **CUCM_Cluster_Wide_Relying_Party_trust** como o nome de exibição e clique em **Avançar**.



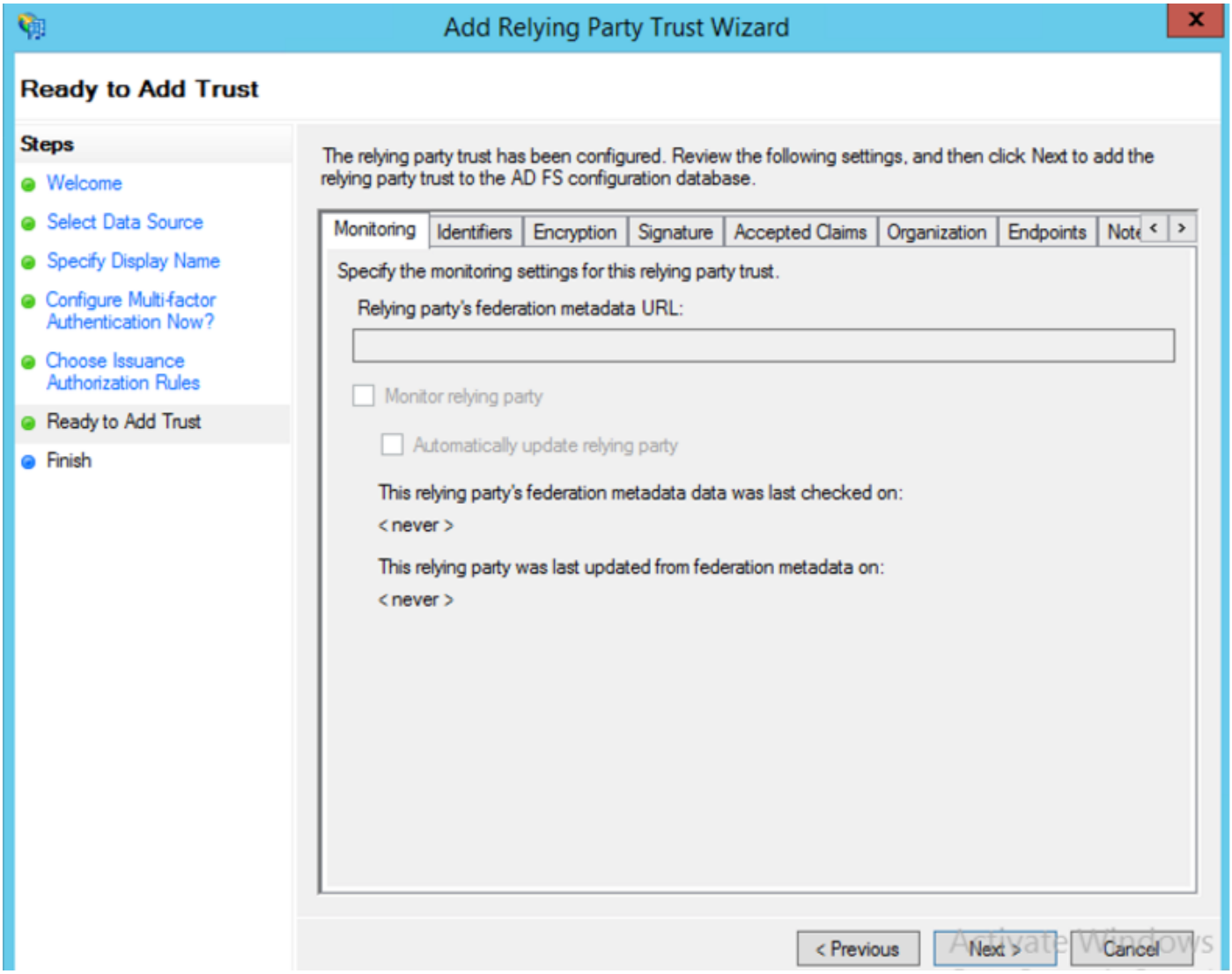
Selecione a primeira opção e clique em **Avançar**.



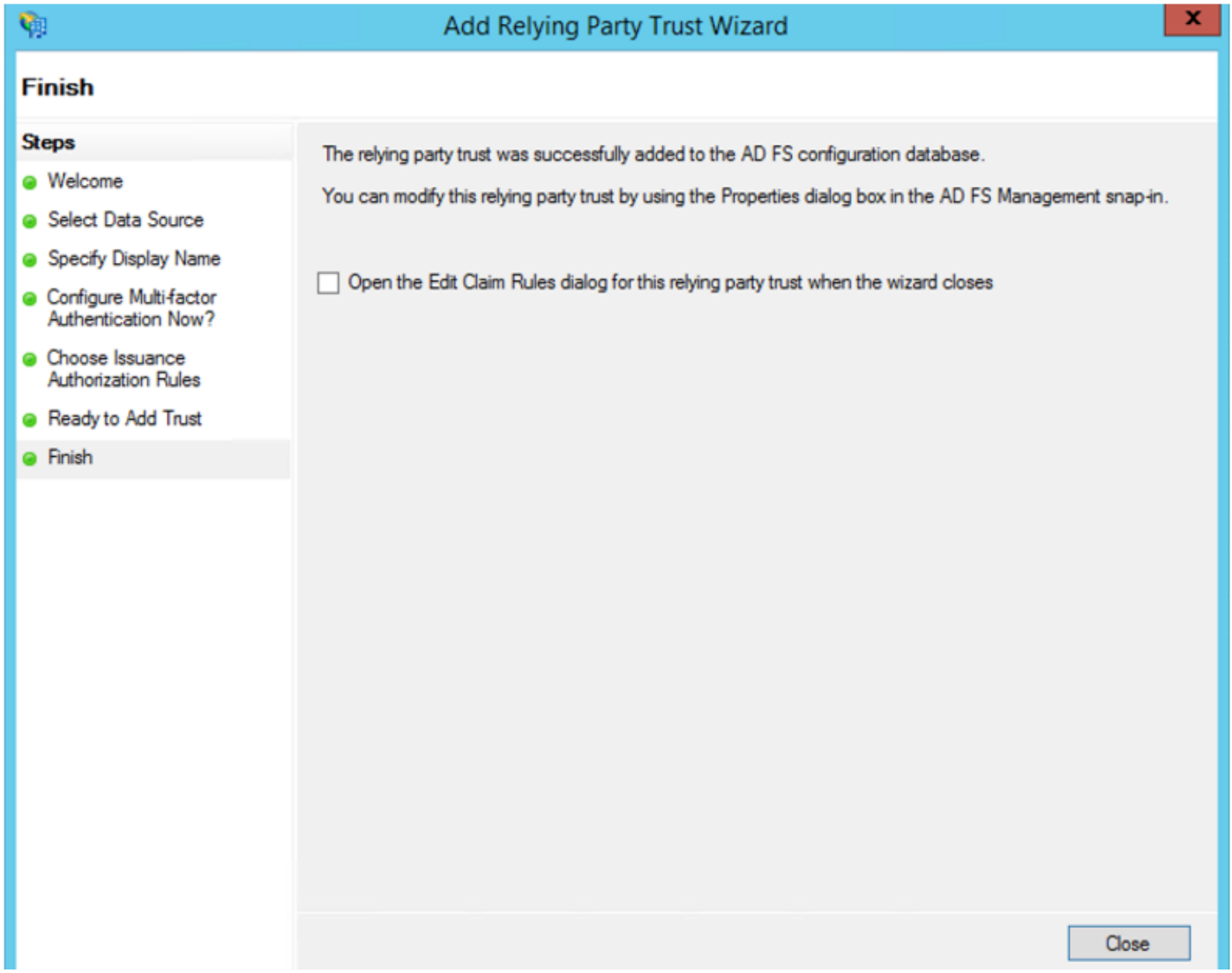
Selecione **Permitir que todos os usuários acessem esta terceira parte confiável** e clique em **Avançar** conforme mostrado na imagem.



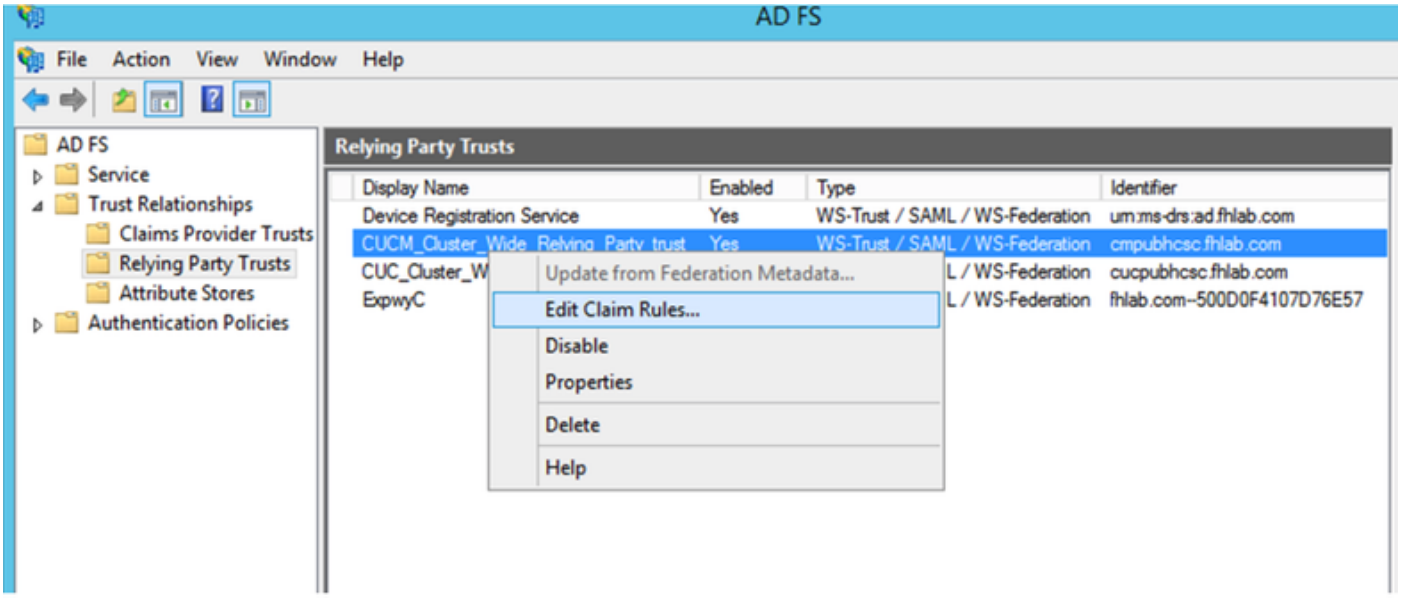
Revise a configuração e clique em **Avançar** conforme mostrado na imagem.



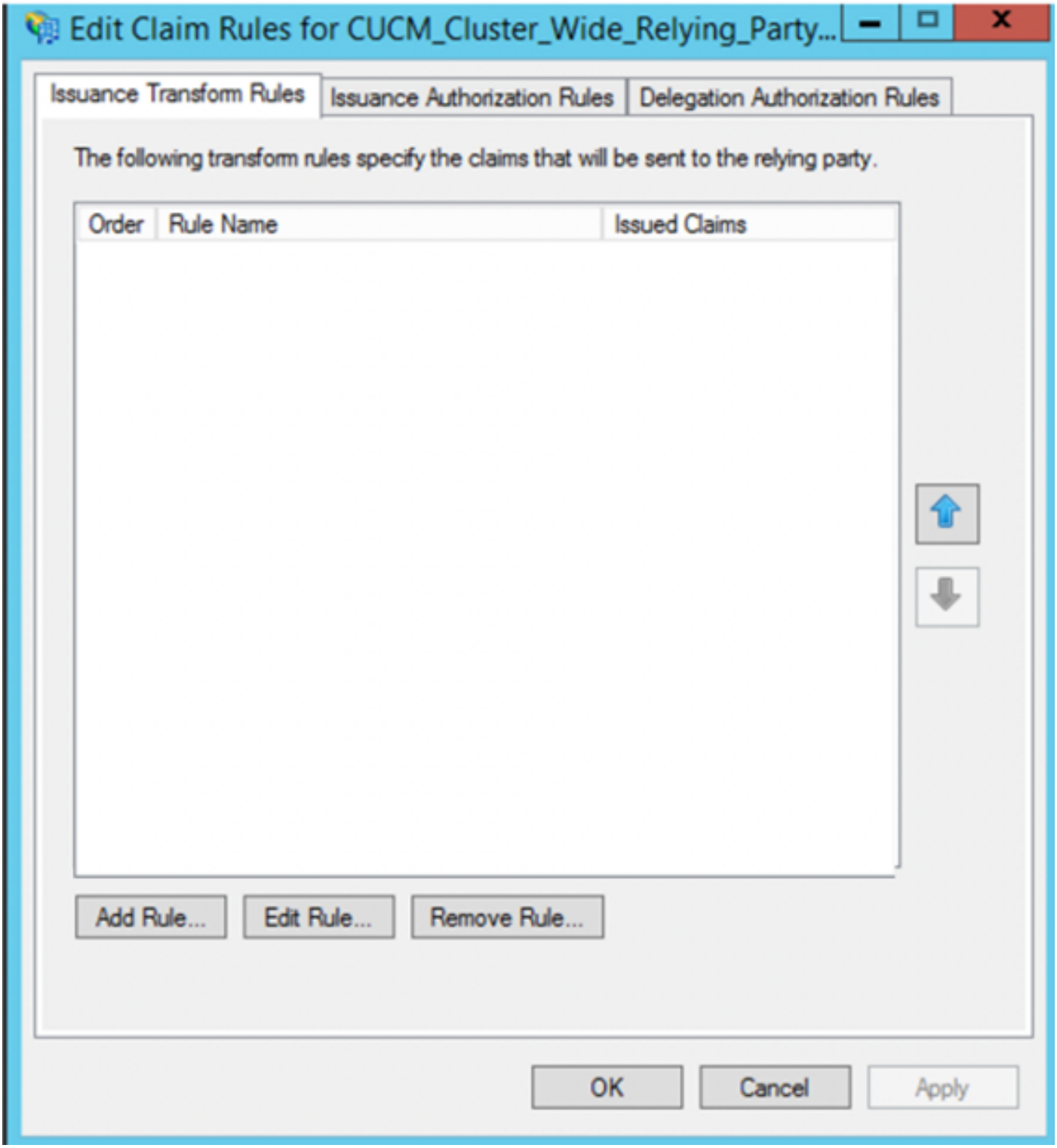
Desmarque a caixa e clique em **Fechar**.



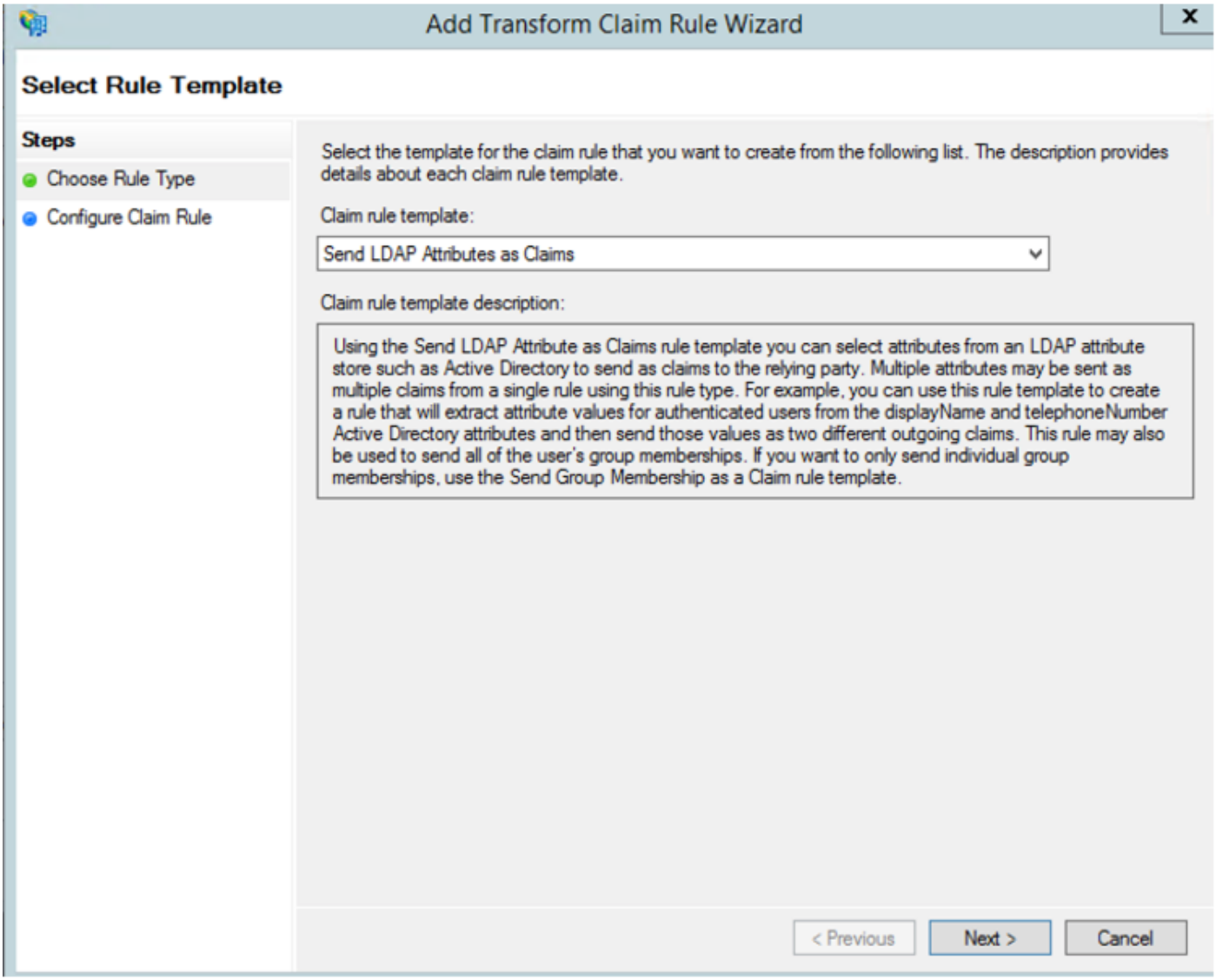
Com o botão do mouse secundário, selecione a **Confiança da terceira parte confiável** que você acabou de criar e **edite a** configuração **das regras de reivindicação**, como mostrado na imagem.



Clique em **Adicionar regra** conforme mostrado na imagem.



Selecione **Enviar atributos LDAP como reivindicações** e clique em **Avançar**.



Configure estes parâmetros:

Nome da regra de reivindicação: NameID

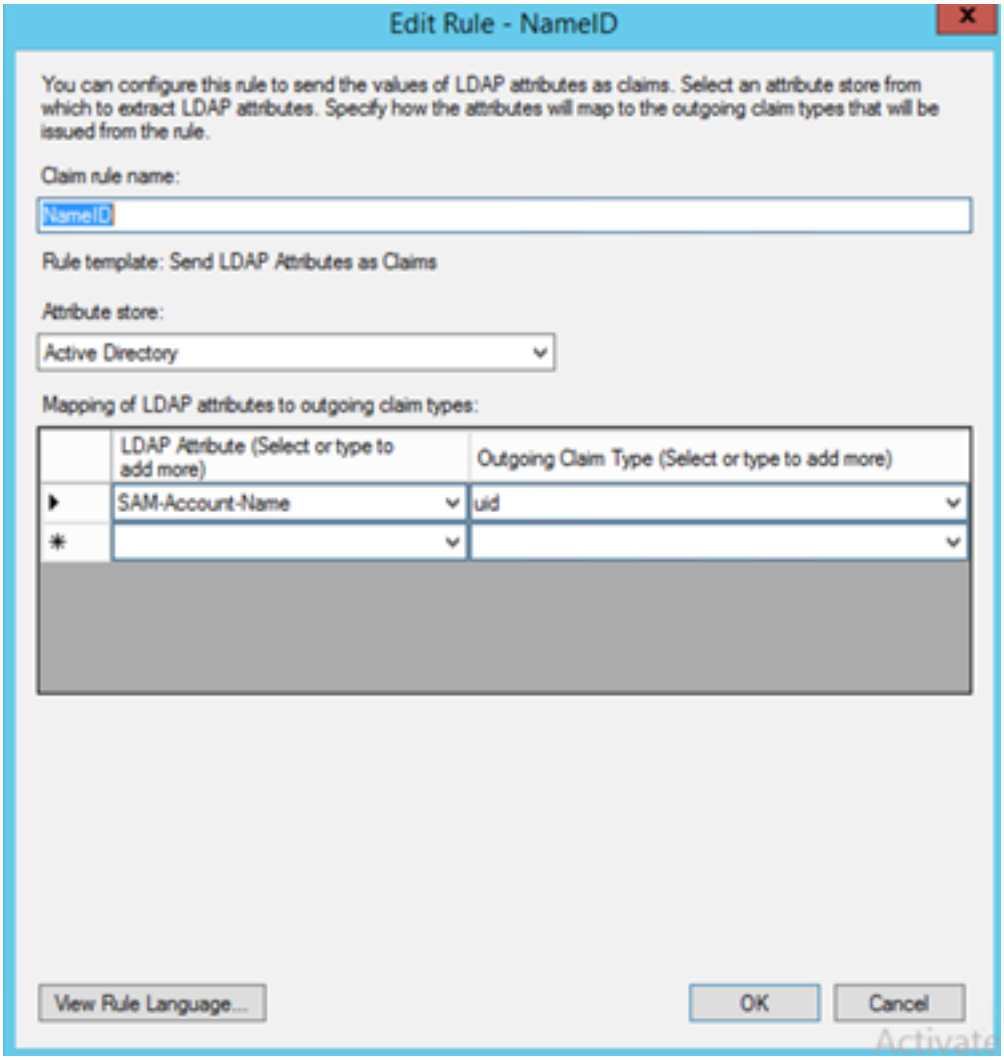
Repositório de atributos: Ative Diretory (clique duas vezes na seta do menu suspenso)

Atributo LDAP: SAM-Account-Name

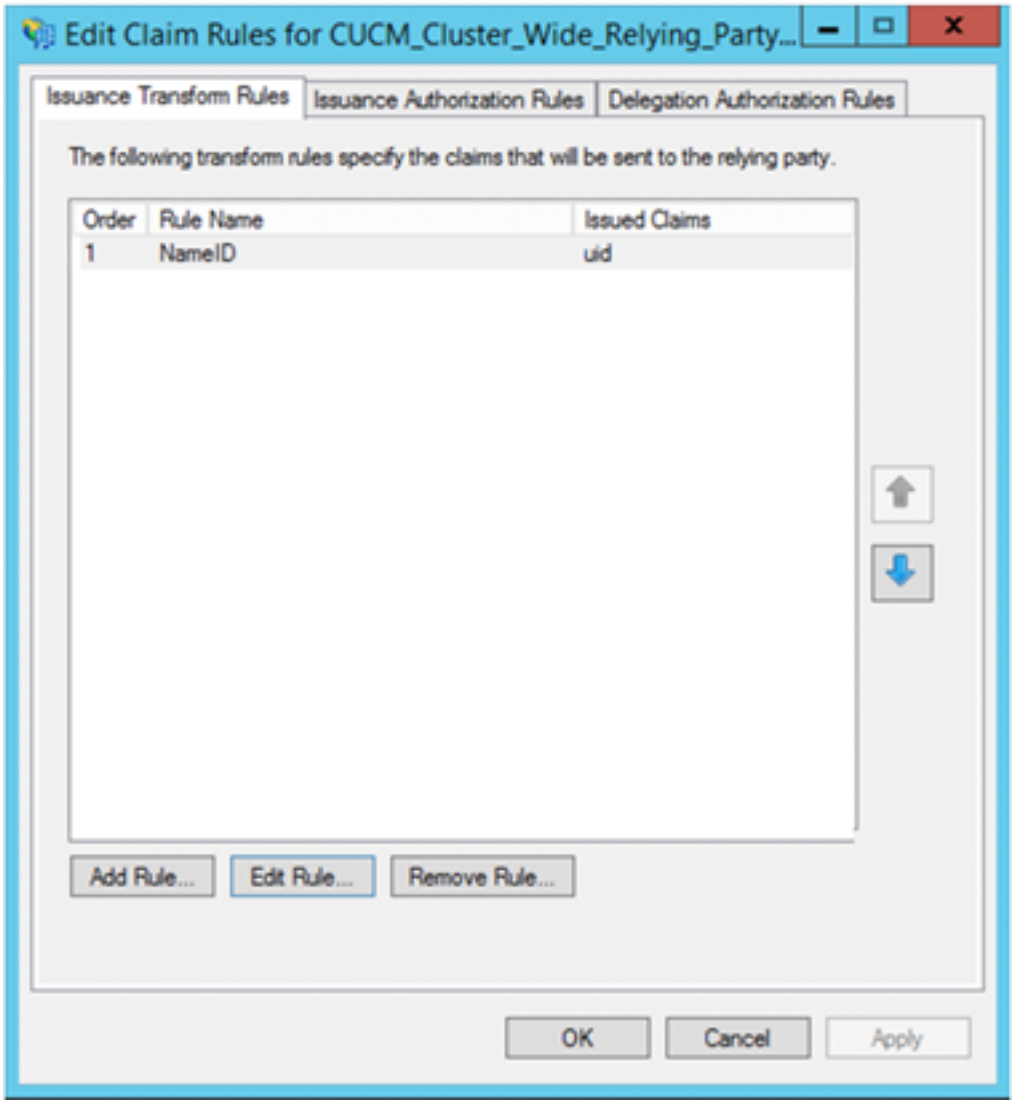
Tipo de solicitação de saída: uid

Clique em **FINISH/OK** para continuar.

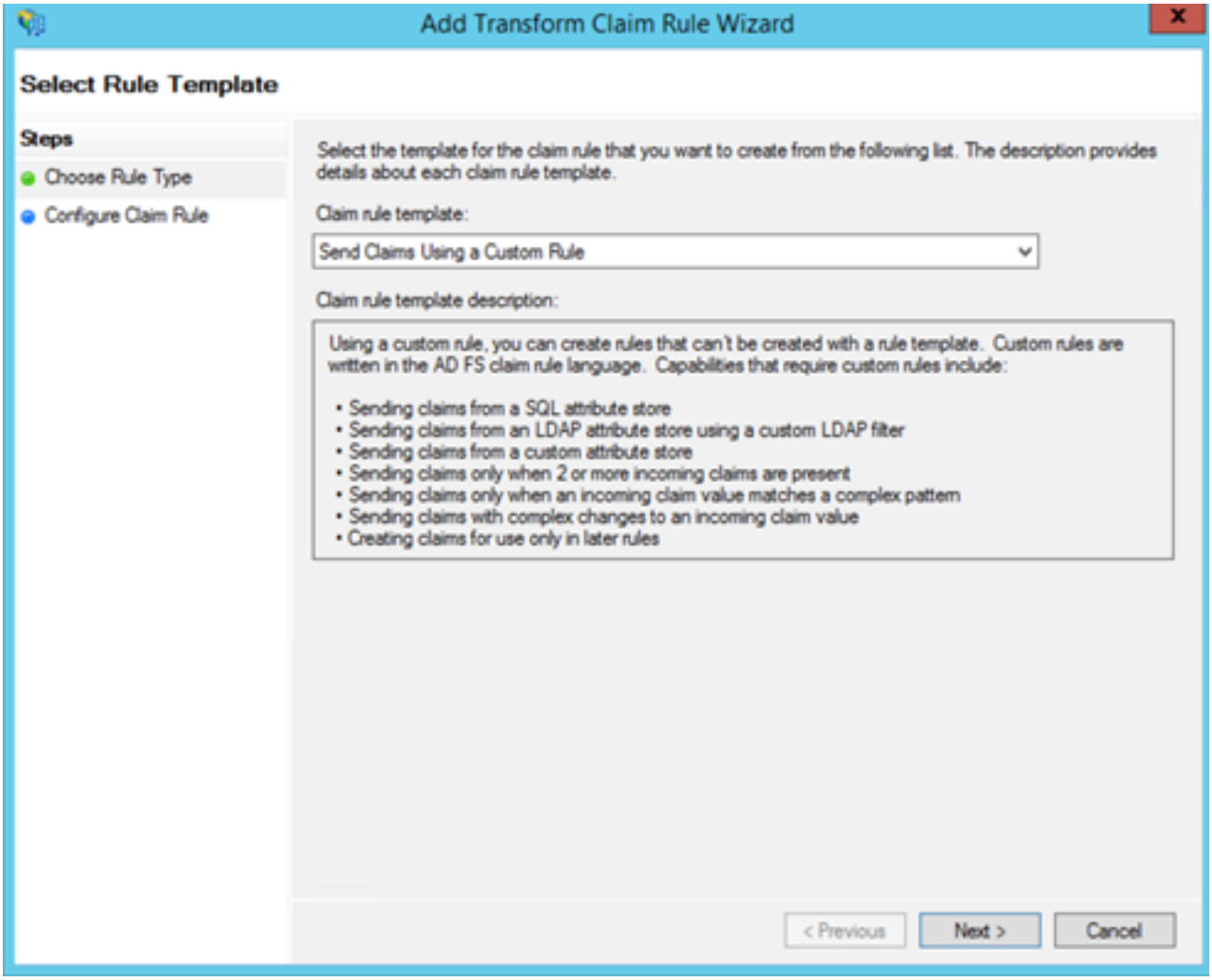
Observe que o uid não está em minúsculas e ainda não existe no menu suspenso. Digite.



Clique em **Adicionar regra** novamente para adicionar outra regra.



Selecione **Enviar reivindicações usando uma regra personalizada** e clique em **Avançar**.

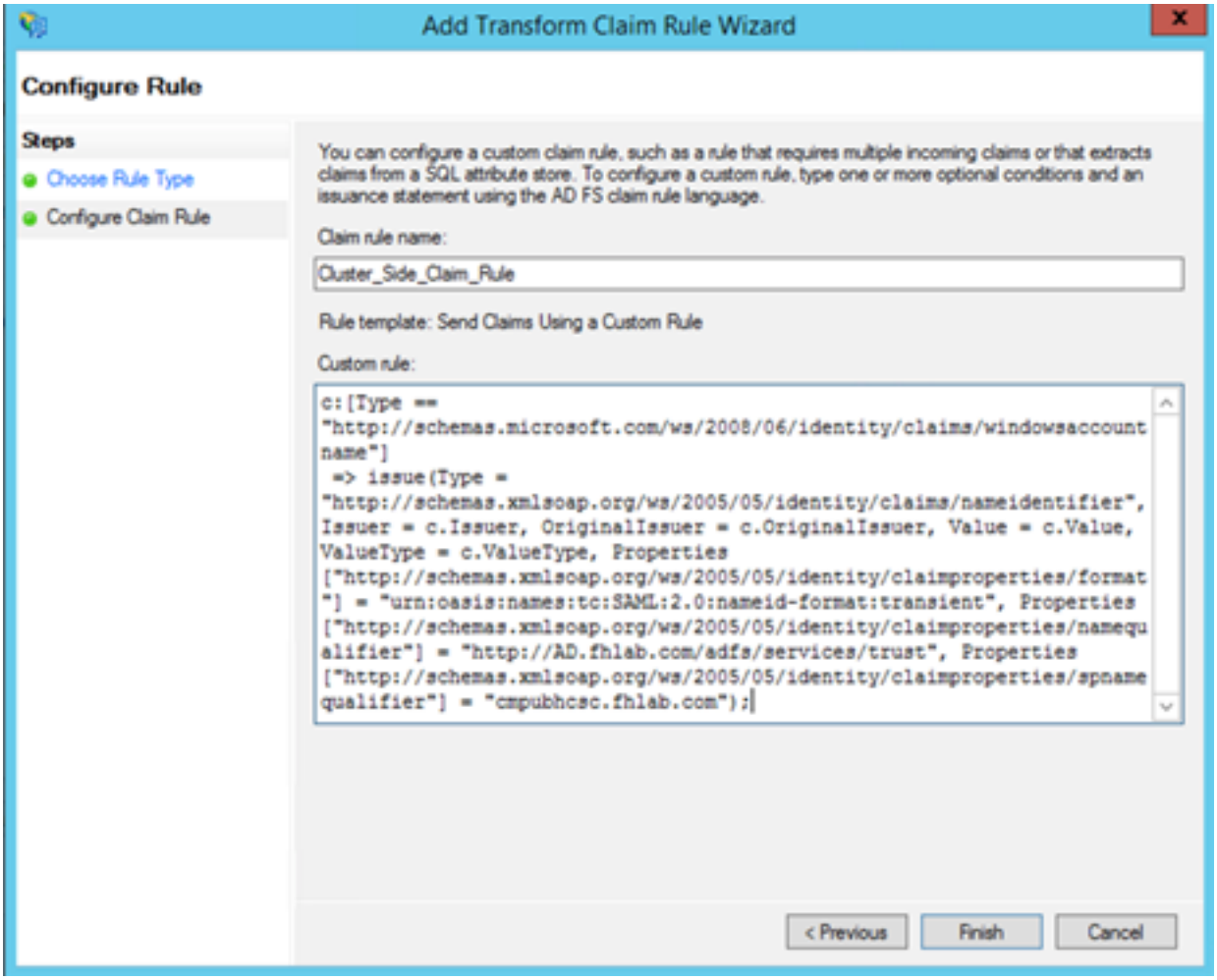


Crie uma regra personalizada chamada Cluster_Side_Claim_Rule.

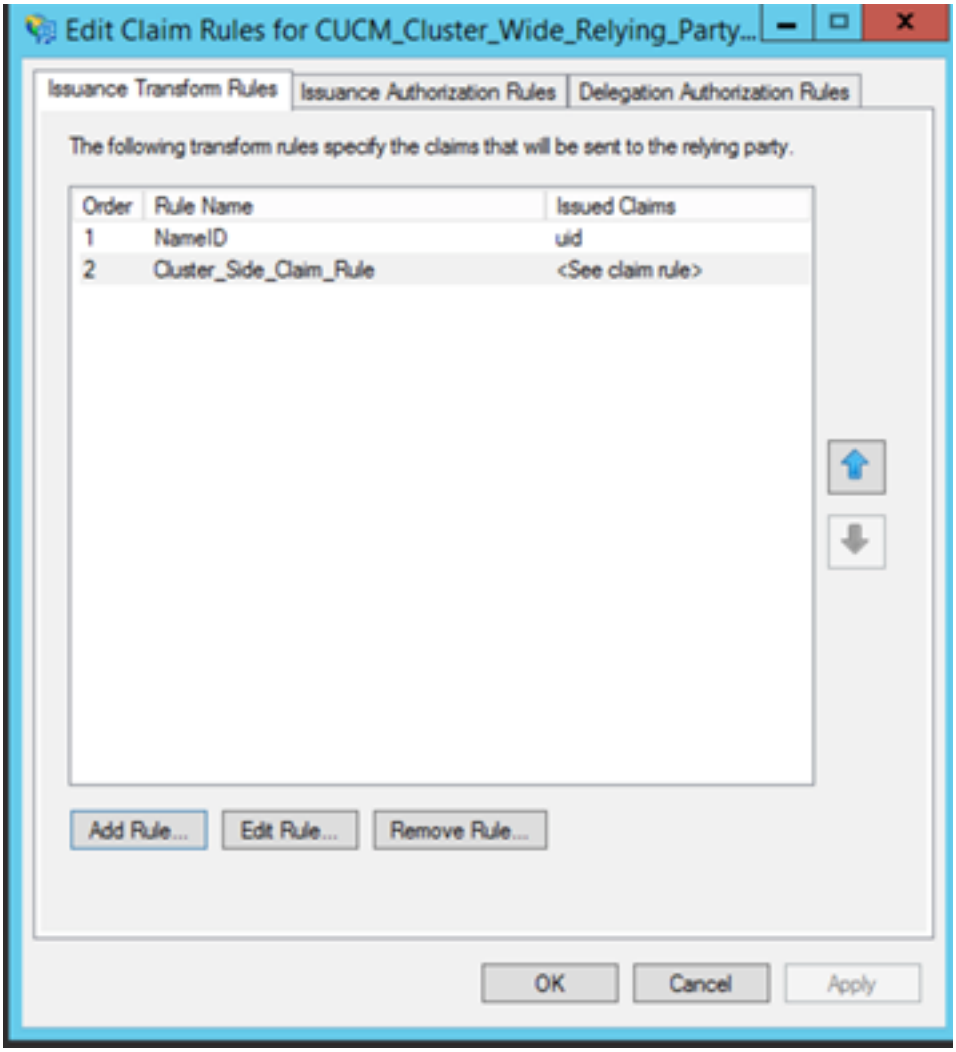
Copie e cole este texto na janela de regras diretamente daqui. Às vezes, os orçamentos são alterados se forem editados em um editor de texto e isso fará com que a regra falhe quando você testar o SSO:

```
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://<ADFS FQDN>/adfs/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"<CUCM Pub FQDN>");

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://AD.fhlab.com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"cmpubhcsc.fhlab.com");
```

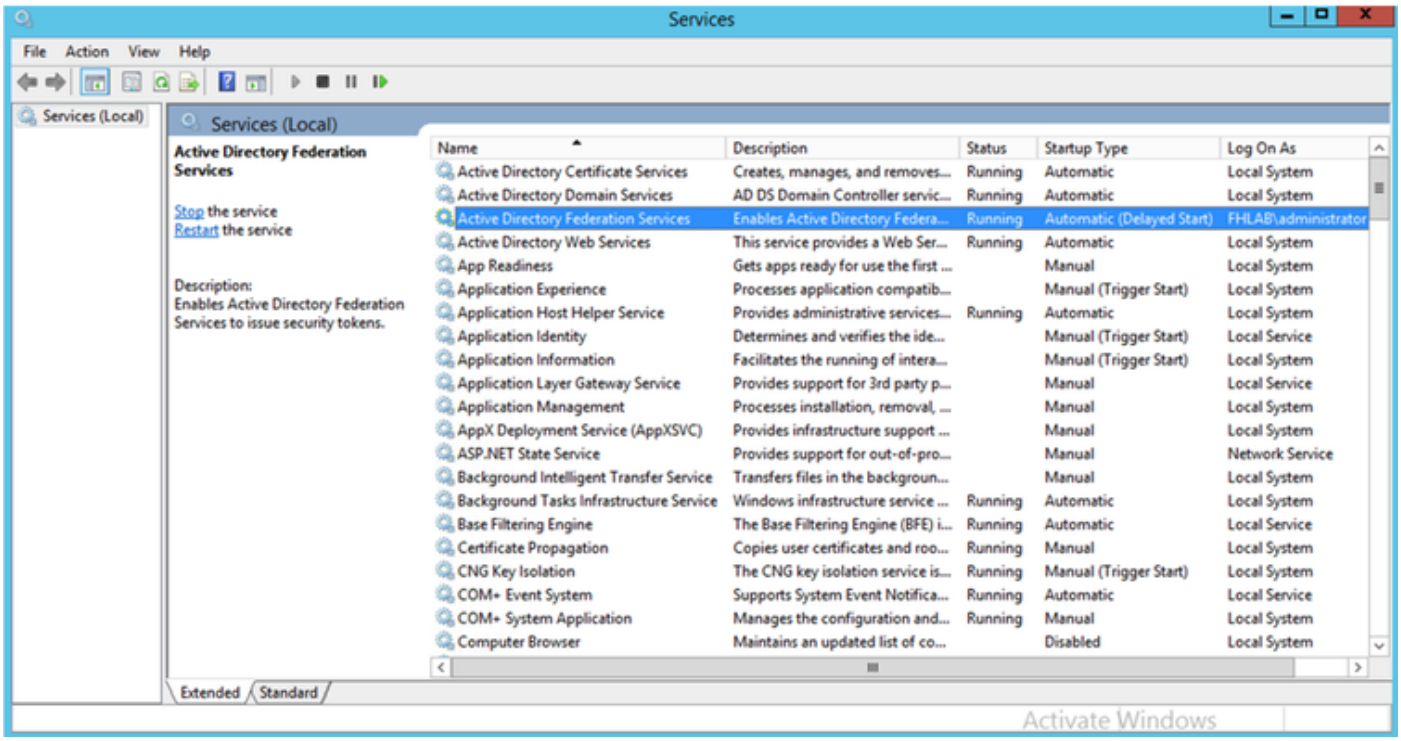
Clique em **Concluir** para continuar.



Agora você deve ter duas regras definidas no ADFS. Clique em **Aplicar** e em **OK** para fechar a janela de regras.



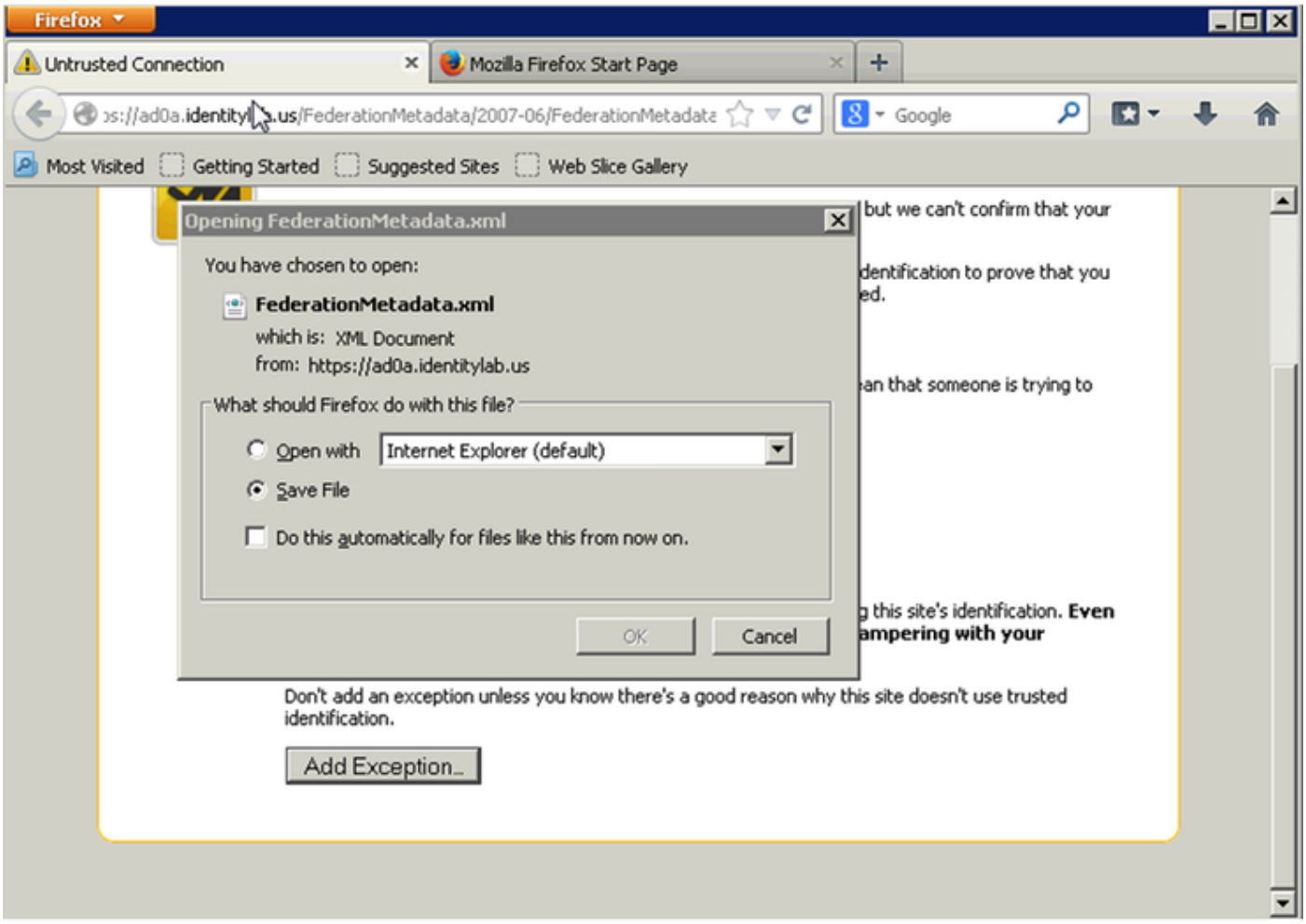
O CUCM foi adicionado com êxito como uma parte confiável ao ADFS.



Antes de continuar, reinicie o serviço ADFS. Navegue até **Menu Iniciar > Ferramentas Administrativas > Serviços**.

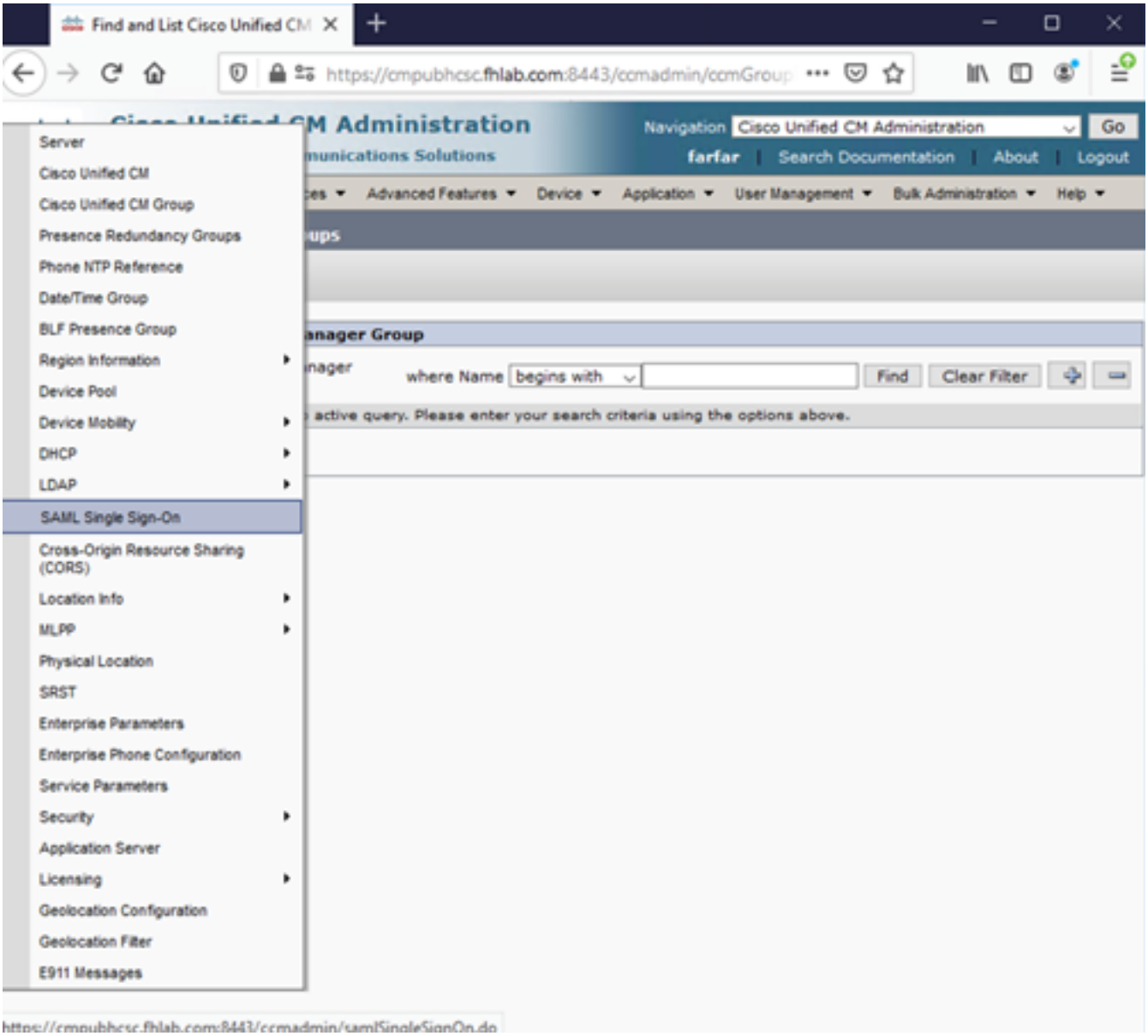
Metadados IDP

Você precisa fornecer ao CUCM informações sobre nosso IdP. Essas informações são trocadas usando metadados XML. Certifique-se de executar esta etapa no servidor onde o ADFS está instalado.

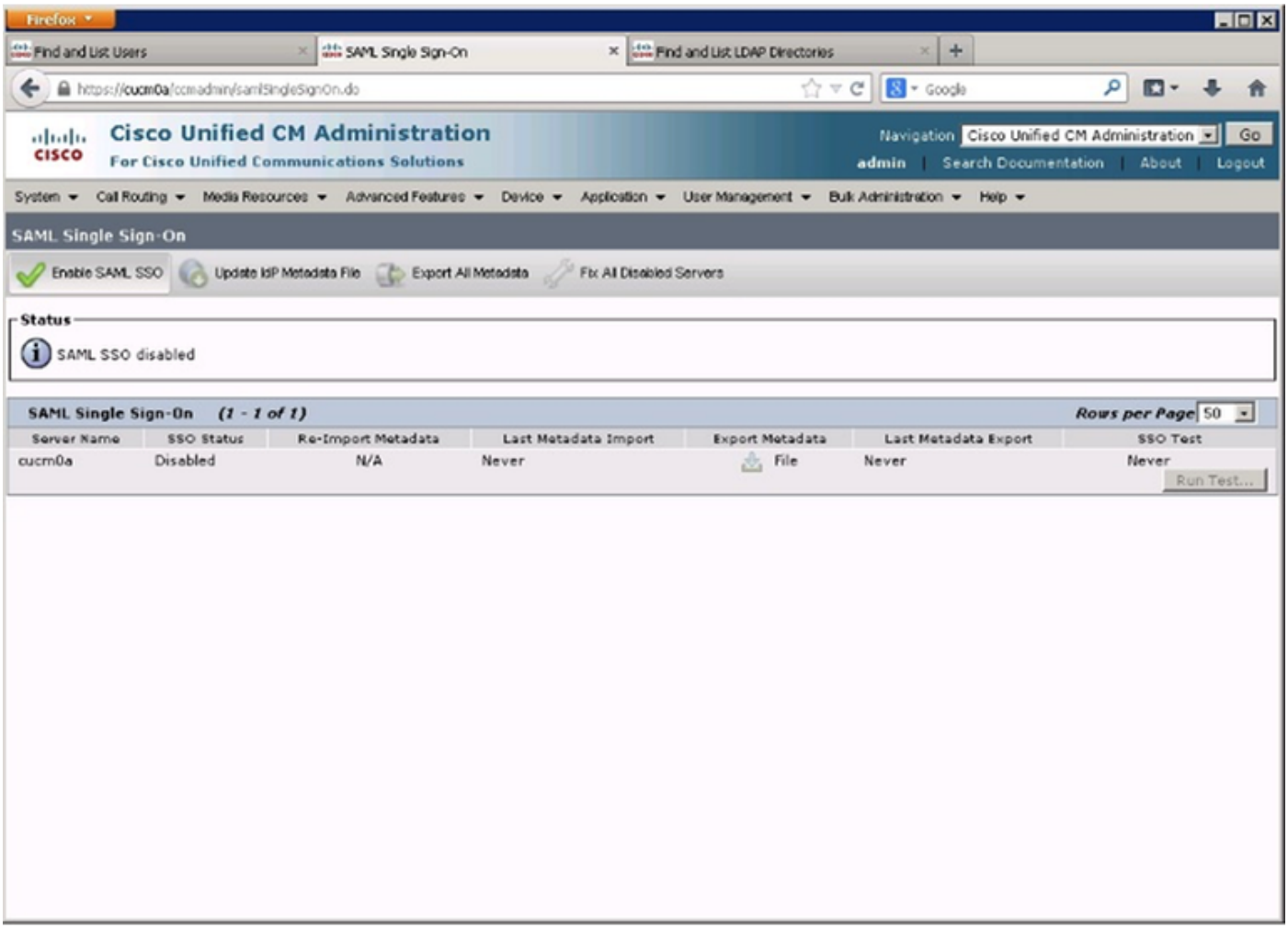


Primeiro, você precisa se conectar ao ADFS (IdP) usando um navegador Firefox para baixar os metadados XML. Abra um navegador em https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml e SALVE os metadados em uma pasta local.

Agora, navegue até a configuração do CUCM até o **menu** do sistema **> menu de logon único SAML**.



Volte para a Administração do CUCM e selecione **SYSTEM > SAML Single Sign-On**.

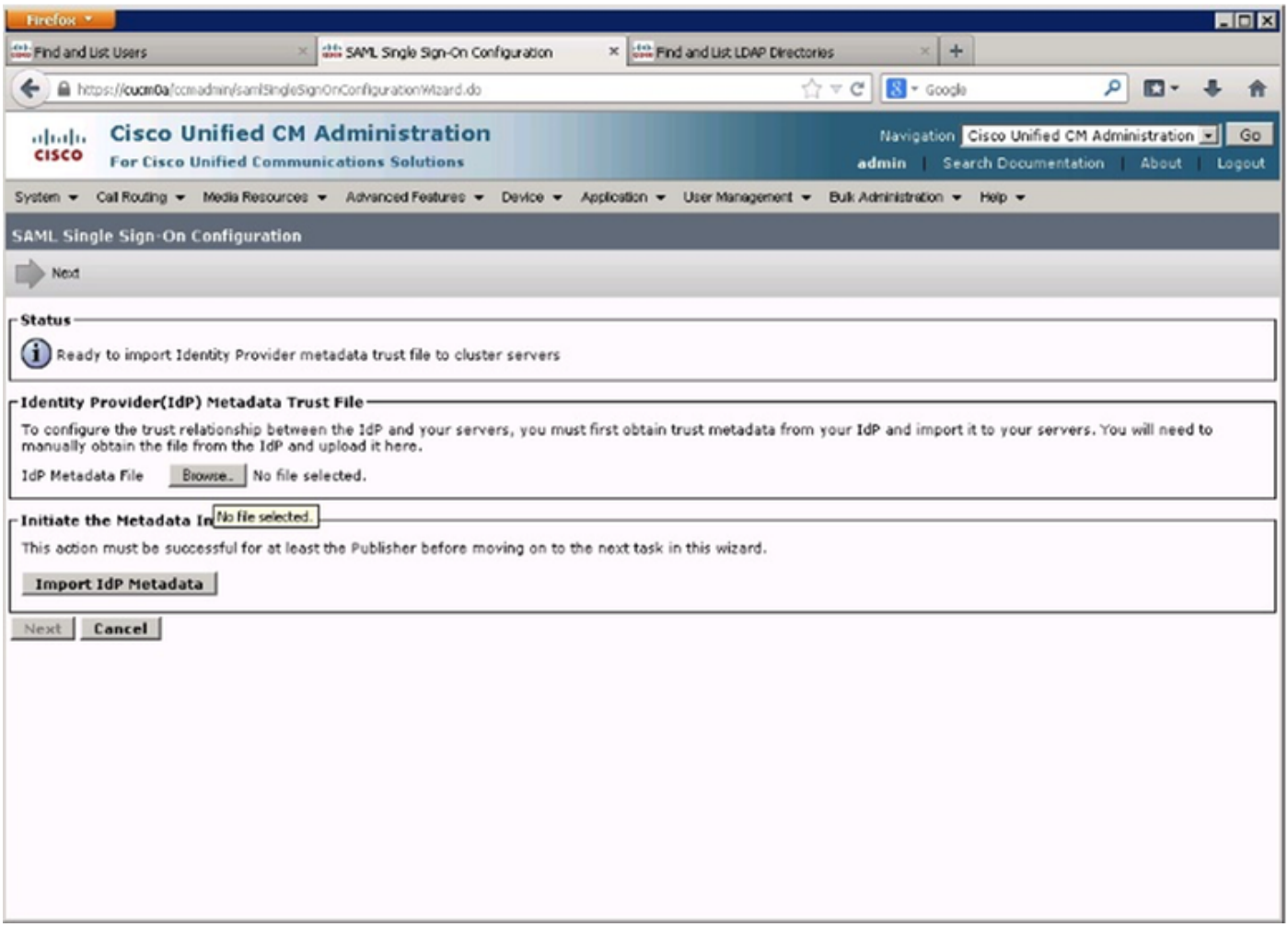


Selecione **Ativar SSO SAML**.

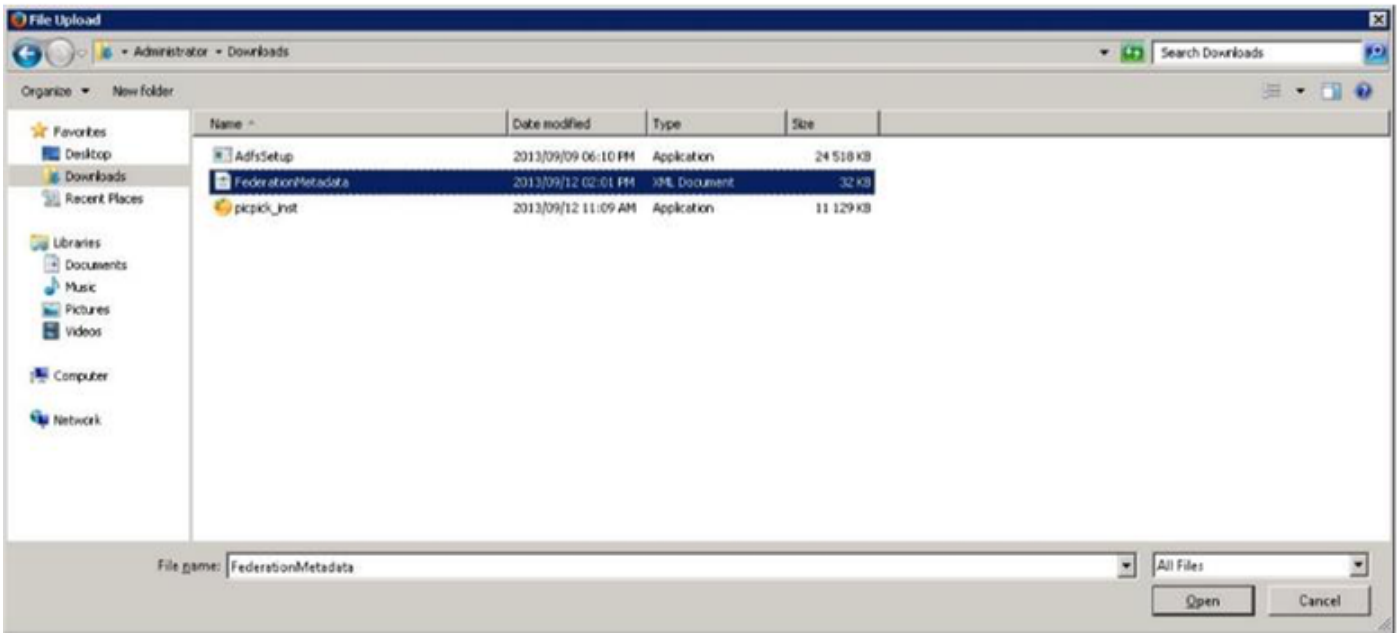
Clique em **Continuar** para confirmar o aviso.

Na tela SSO e clique em **Procurar.** para importar o arquivo XML de metadados

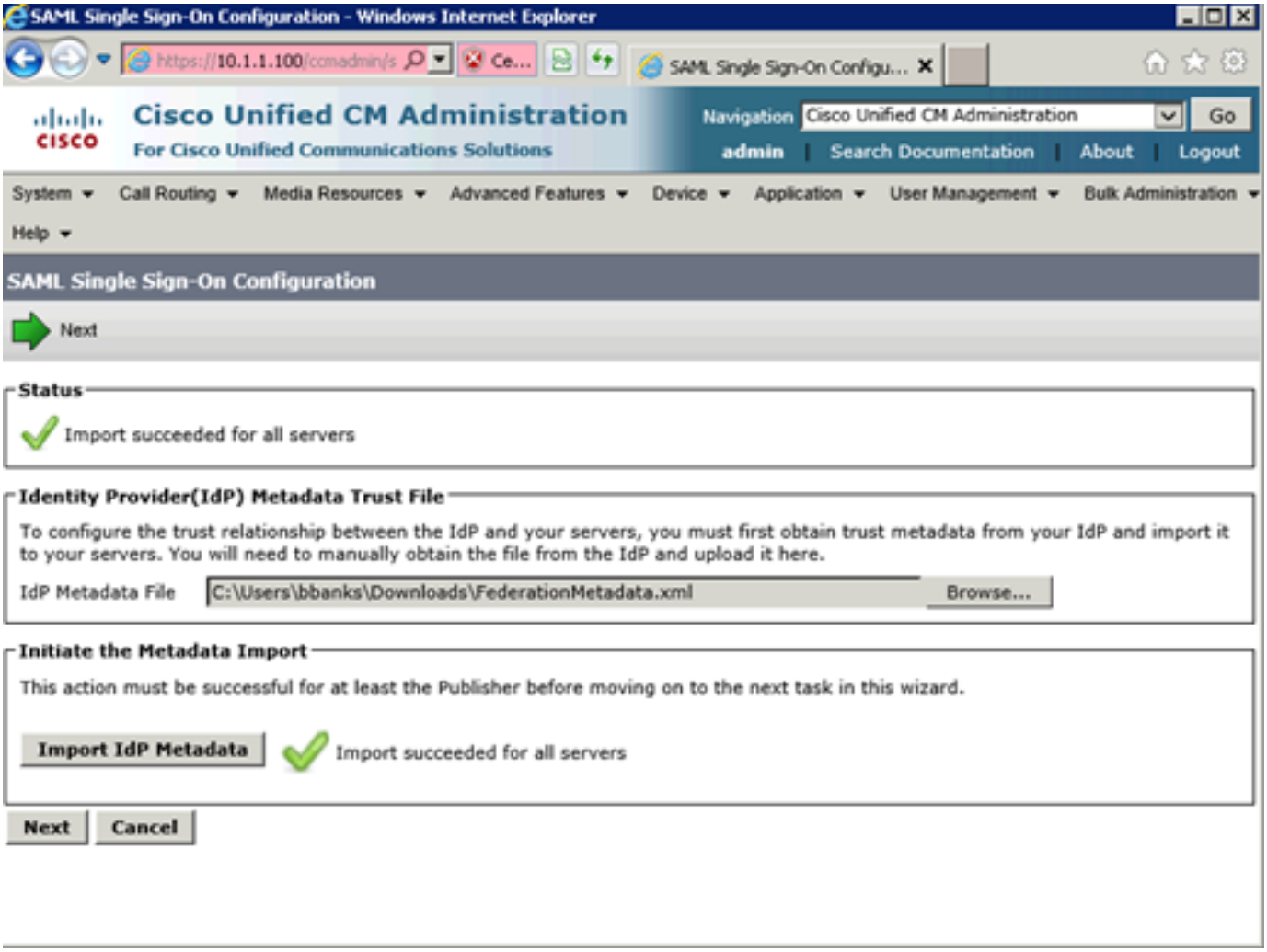
FederationMetadata.xml que você salvou anteriormente, como mostrado na imagem.



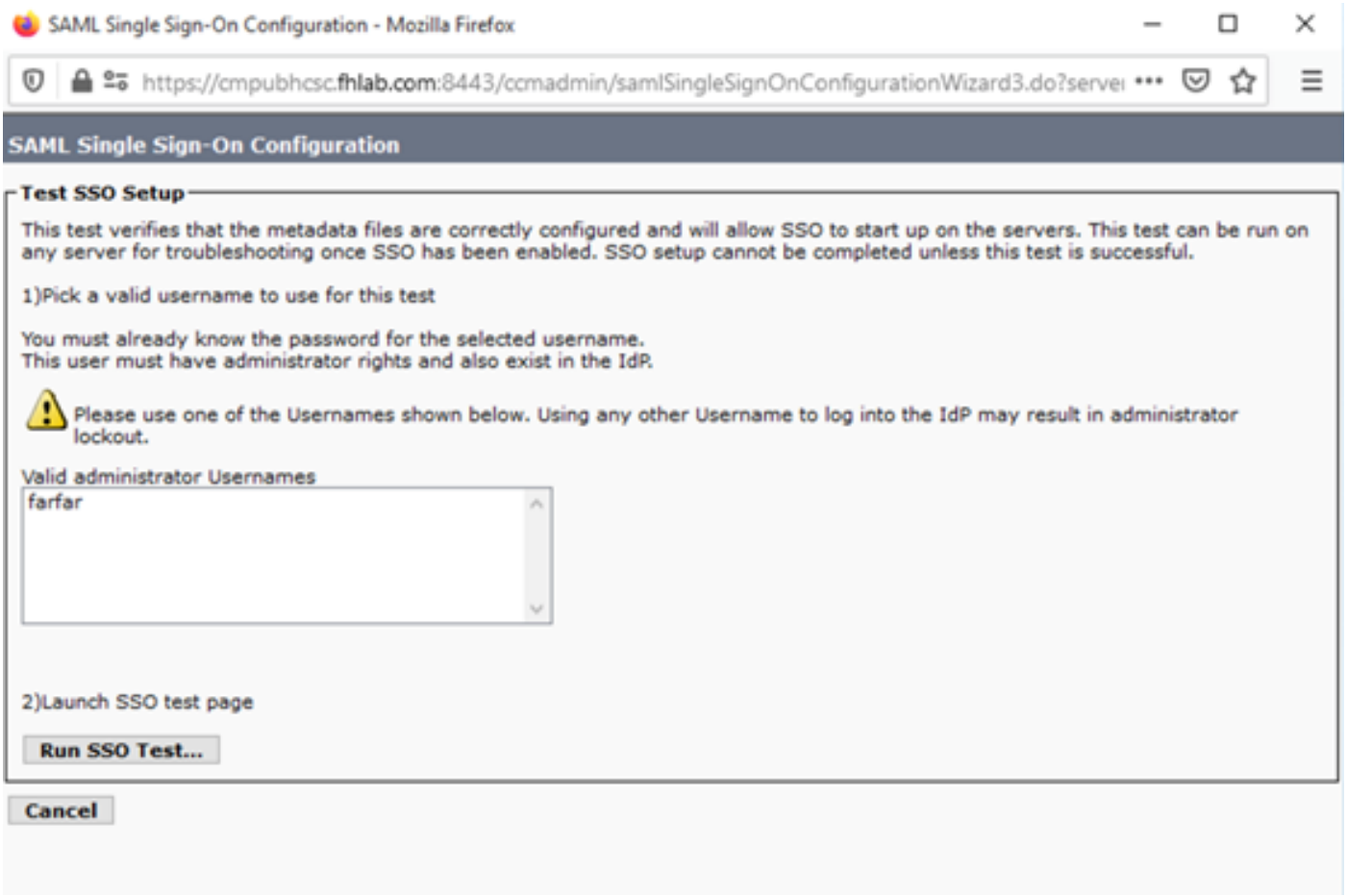
Selecione o arquivo XML e clique em **Abrir** para carregá-lo no CUCM em Downloads em Favoritos.



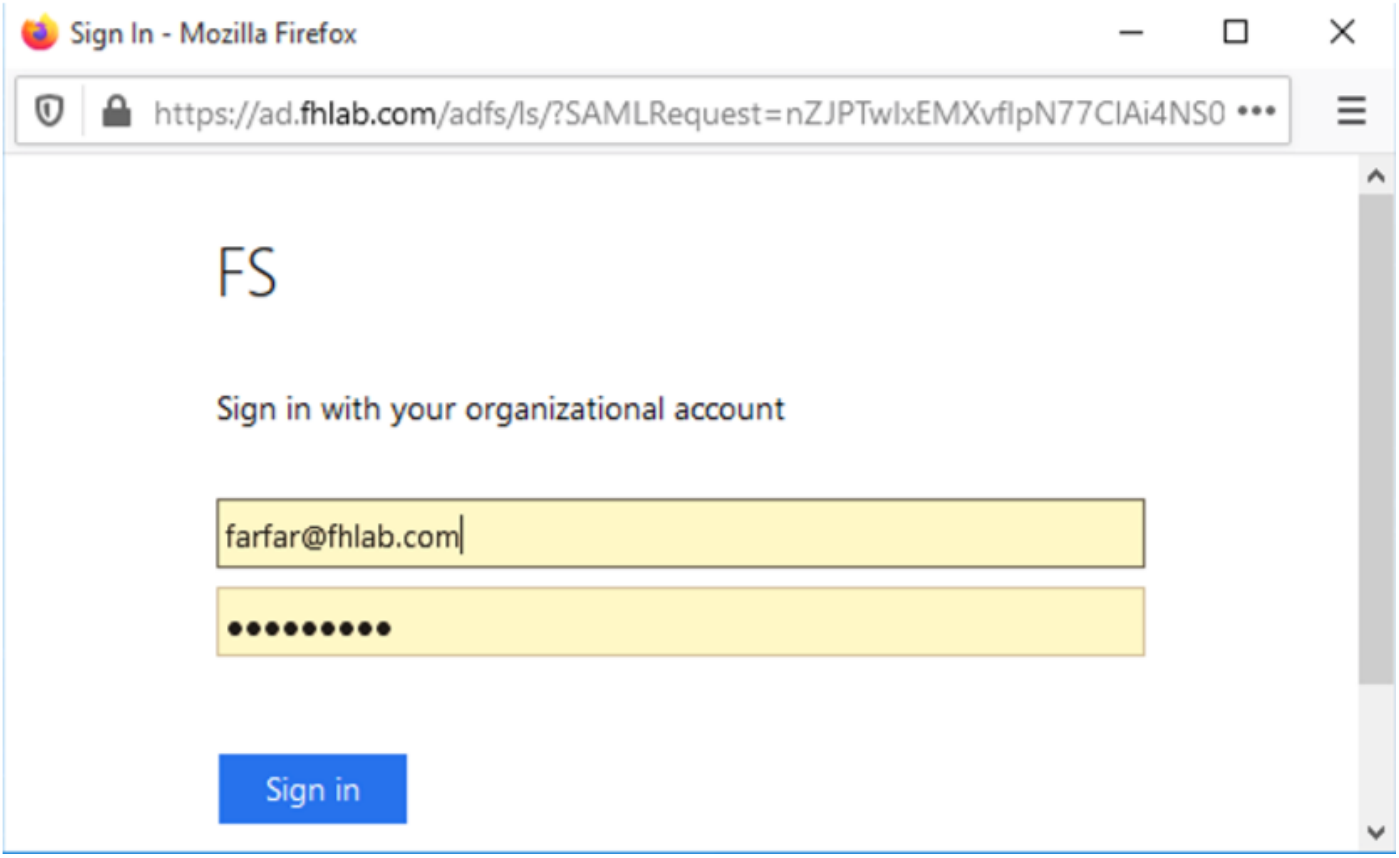
Depois de fazer o upload, clique em Importar metadados IdP para importar as informações do IdP para o CUCM. Confirme se a importação foi bem-sucedida e clique em Avançar para continuar.



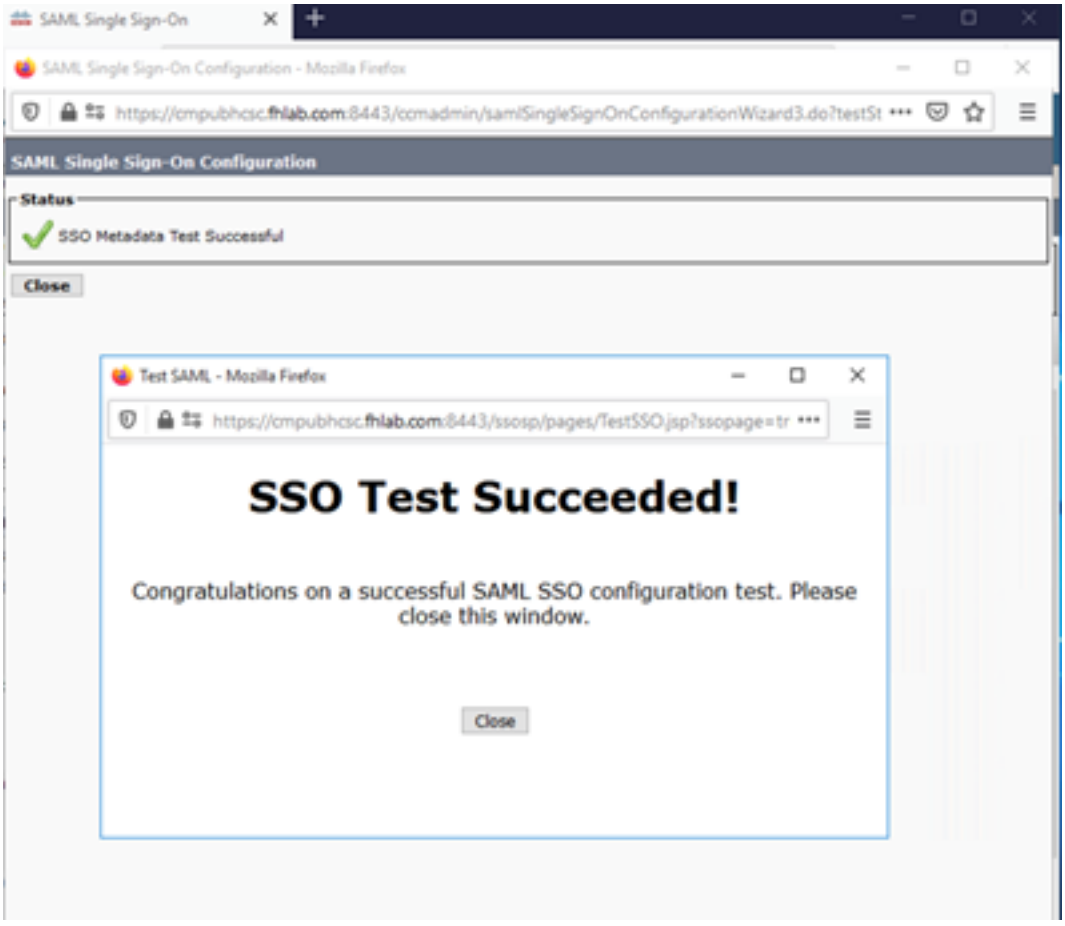
Selecione o usuário que pertence ao CCM Super Users padrão e clique em RUN SSO TEST.



Quando apresentado com uma caixa de diálogo de autenticação de usuário, faça login com o nome de usuário e a senha apropriados.



Se tudo estiver configurado corretamente, você deverá ver uma mensagem informando Teste SSO bem-sucedido!



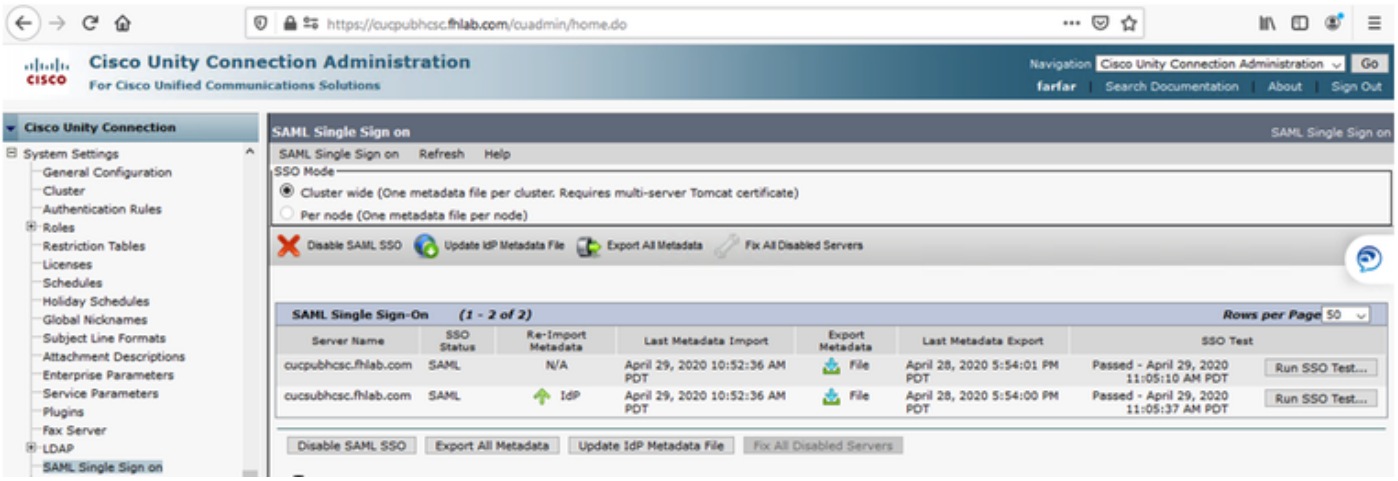
Clique em FECHAR e CONCLUIR para continuar.

Agora concluímos com êxito as tarefas básicas de configuração para ativar SSO no CUCM usando ADFS.

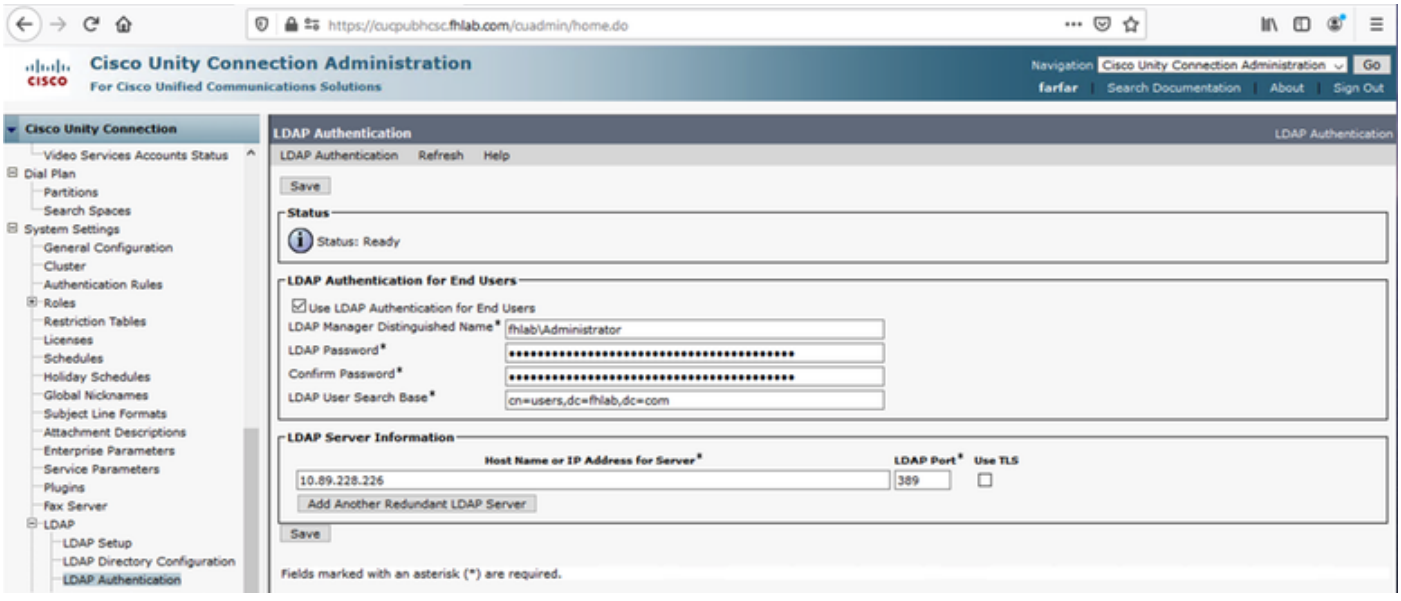
Configurar SSO no CUC

O mesmo processo pode ser seguido para ativar SSO no Unity Connection.

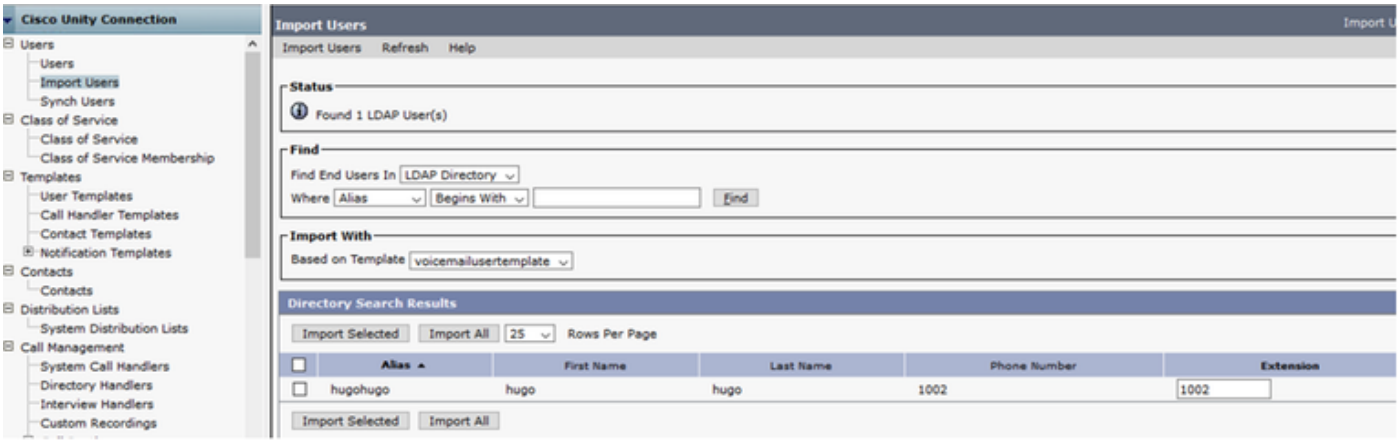
Integração LDAP com CUC.



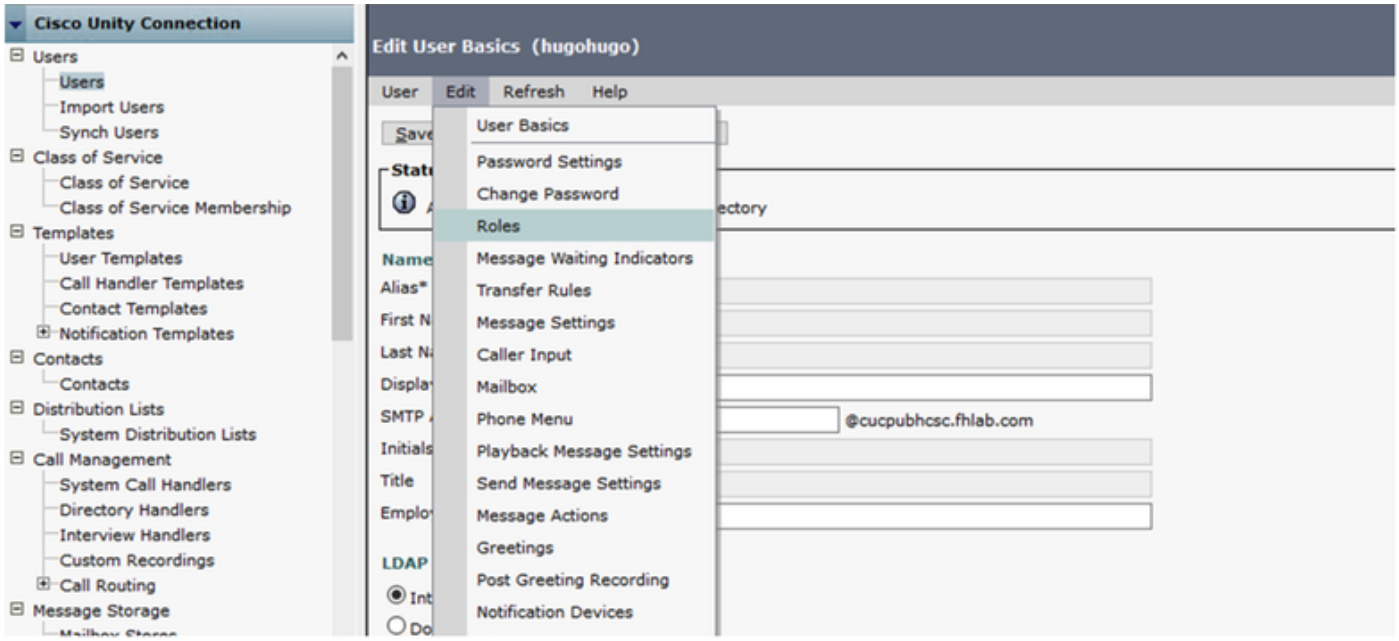
Configure a autenticação LDAP.



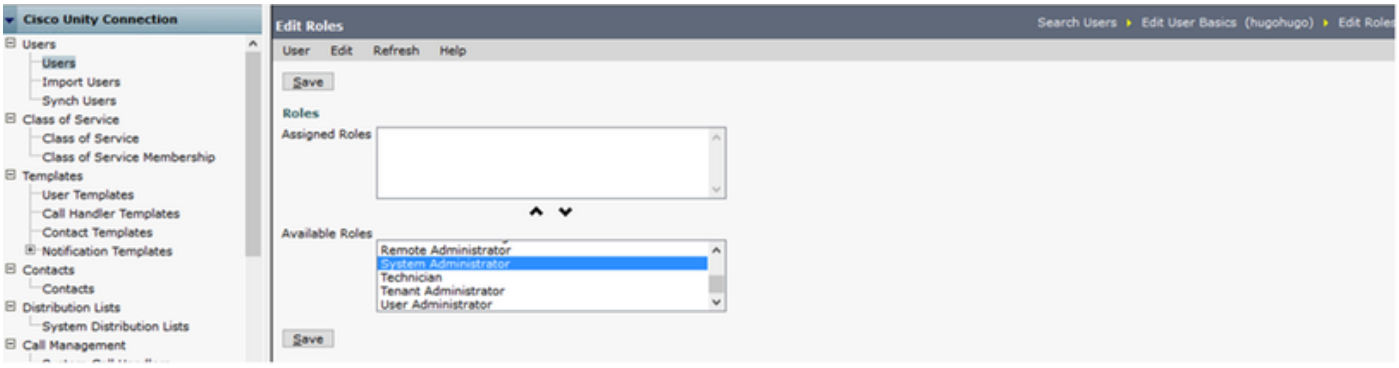
Importe os usuários do LDAP que terão correio de voz atribuído e também o usuário que servirá para testar o SSO.



Navegue até **Usuários > Editar > Funções** como mostrado na imagem.

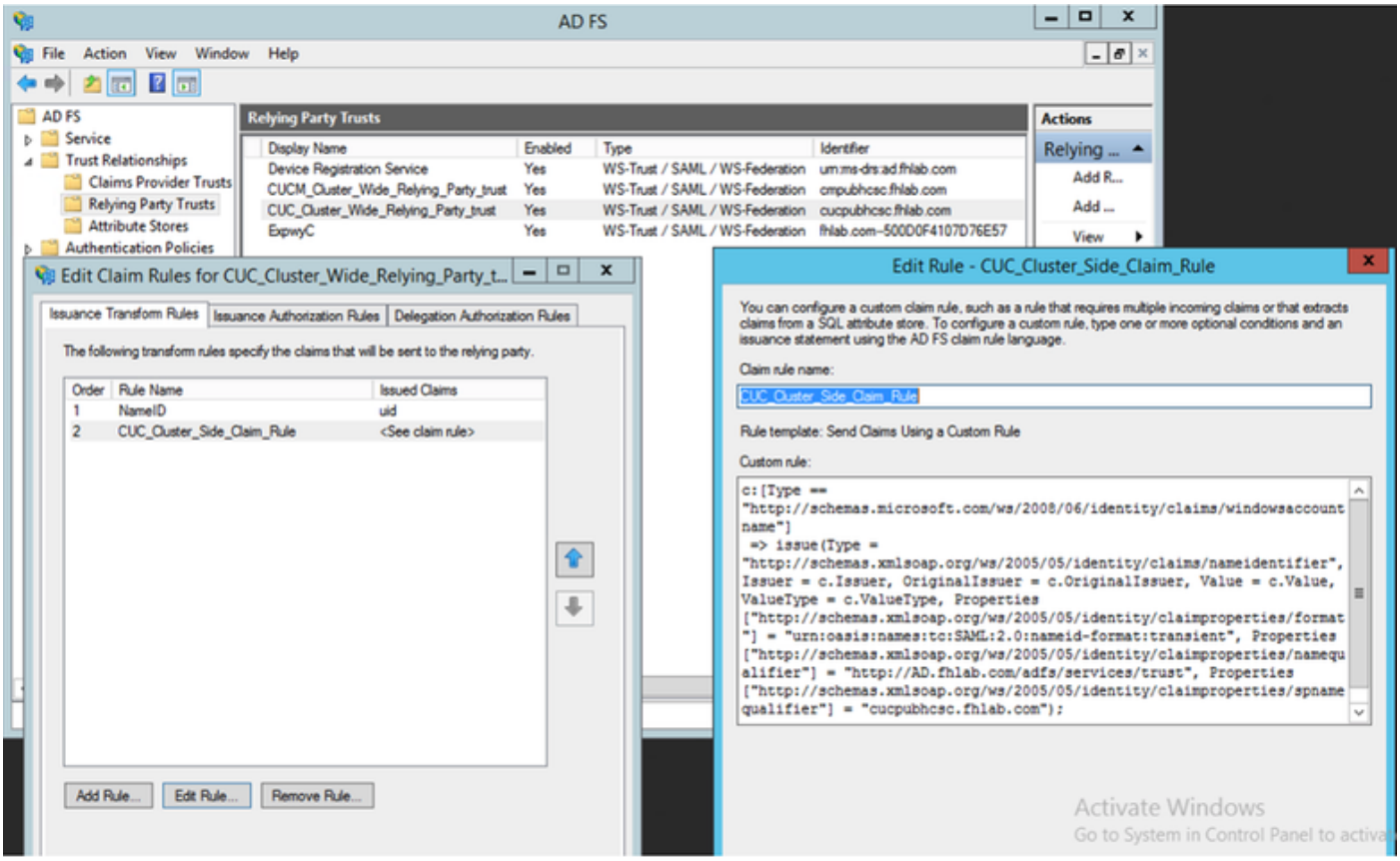


Atribua ao usuário de teste a função de Administrador do sistema.

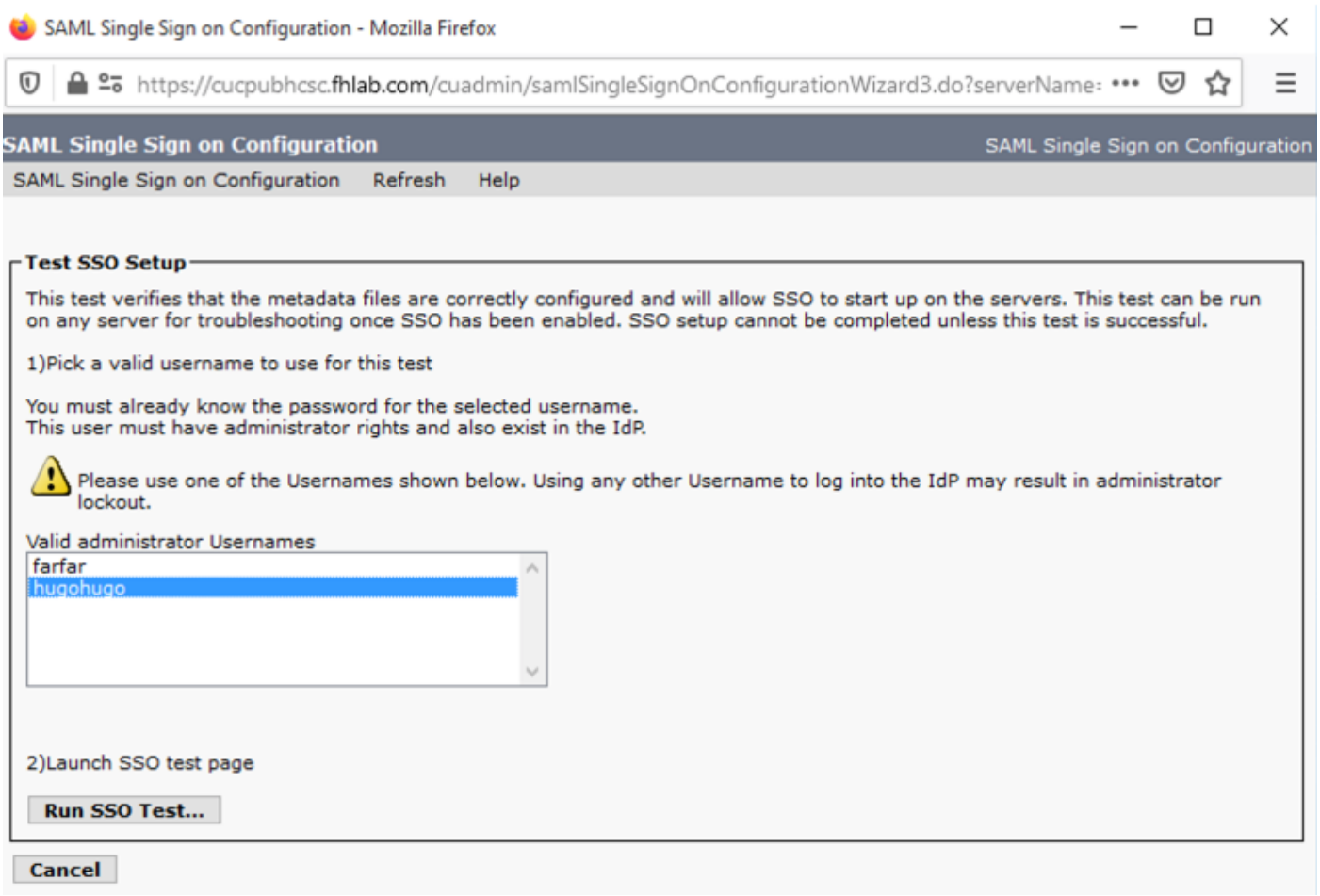


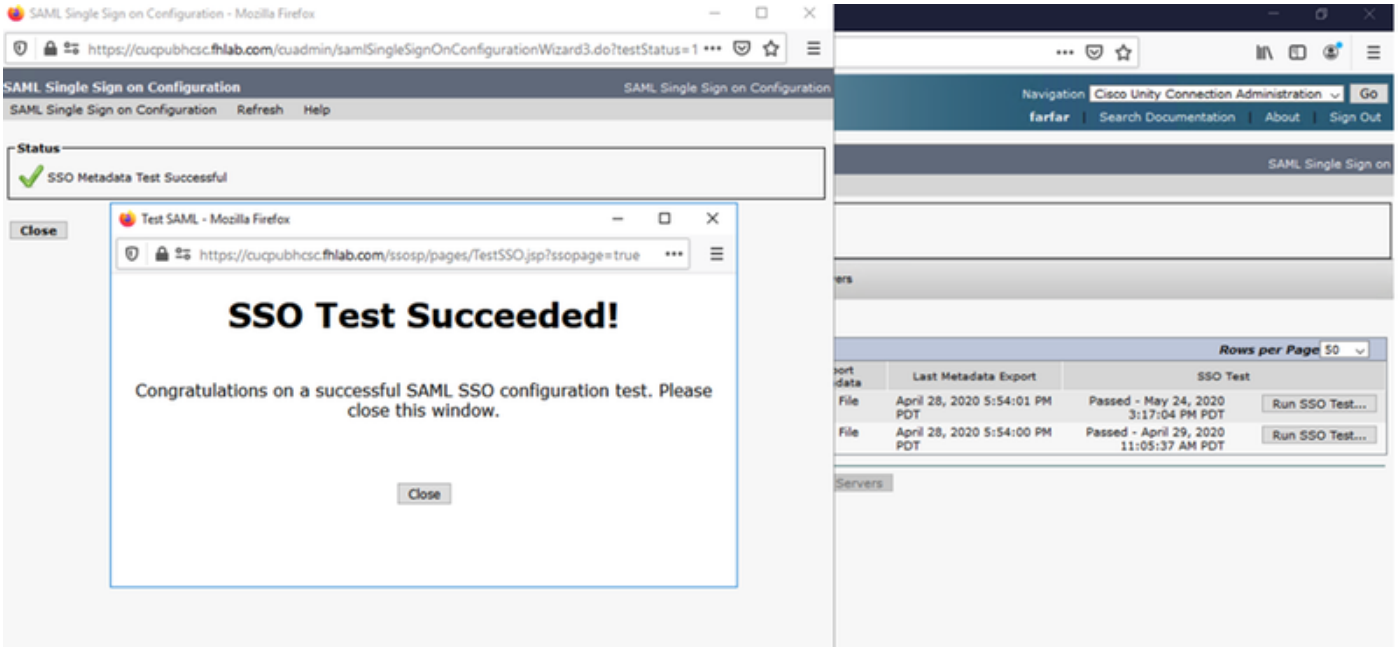
Metadados CUC

Você já deve ter baixado os metadados do CUC, criado o ConyingPartyTrust para CUC e carregado os metadados do CUC e criado as regras do AD FS no ADFS 3.0



Vá para SAML Single Sign-On (Logon único SAML) e ative SAML SSO.





Configurar SSO no Expressway

Importar metadados para o Expressway C

Abra um navegador em https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml e SALVE os metadados em uma pasta local

Carregar para **Configuração > Comunicações Unificadas > IDP**.

Exportar Metadados Do Expressway C

Vá para a configuração -> Unified Communications -> IDP -> Export SAML Data

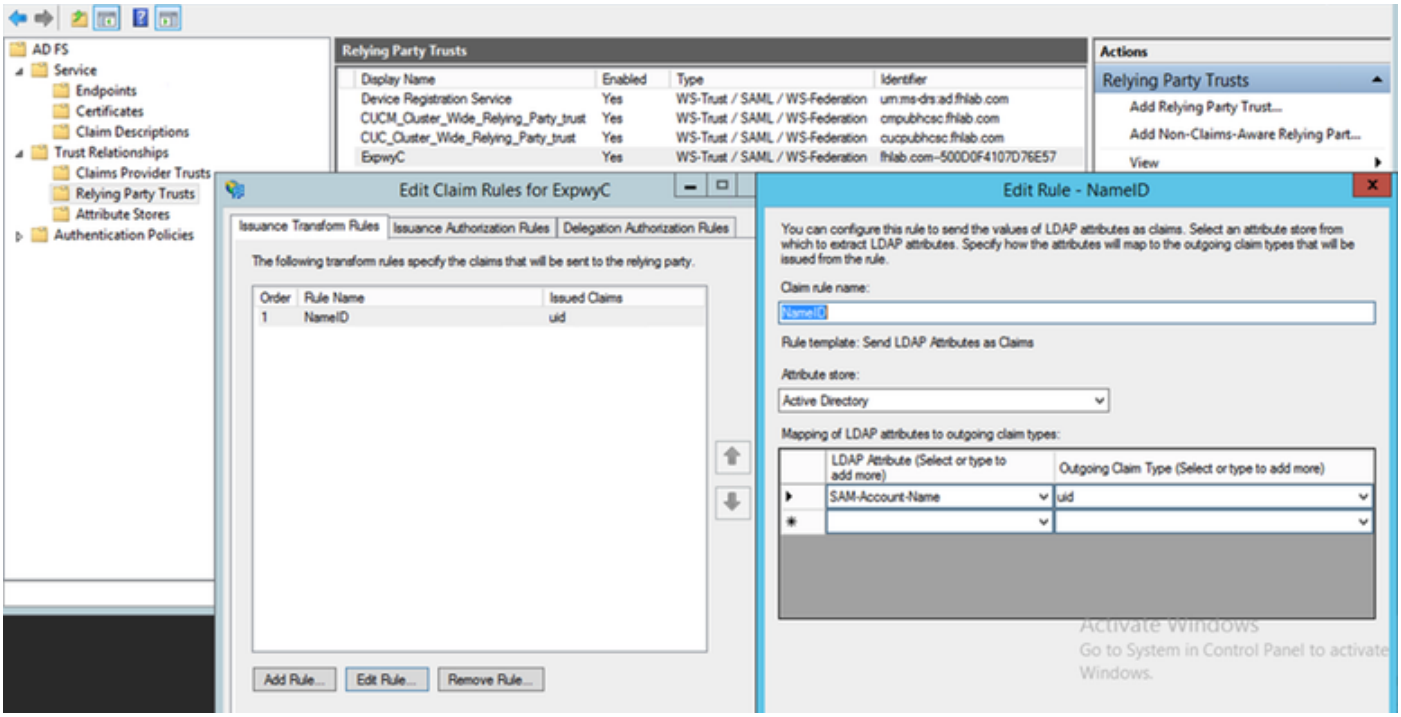
O modo cluster usa um certificado autoassinado (com longa duração) que está incluído no SAML

metadados e usados para assinar solicitações SAML

- No modo de cluster-wide, para fazer o download do único arquivo de metadados para cluster, clique em Download
- No modo por peer, para baixar o arquivo de metadados de um peer individual, clique em Download ao lado do peer. Para exportar tudo em um arquivo .zip, clique em Baixar tudo.

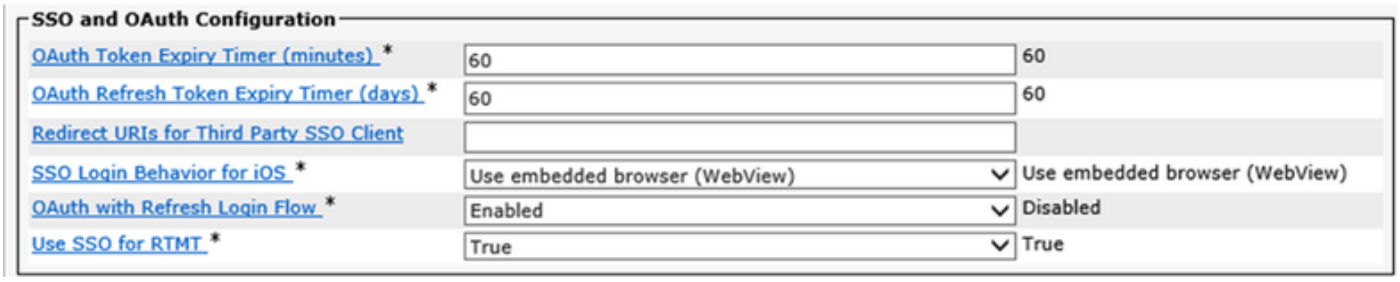
Adicione uma confiança de terceira parte confiável para o Cisco Expressway-E

Primeiro, crie Confianças de terceira parte para o Expressway-Es e, em seguida, adicione uma regra de declaração para enviar identidade como atributo UID.

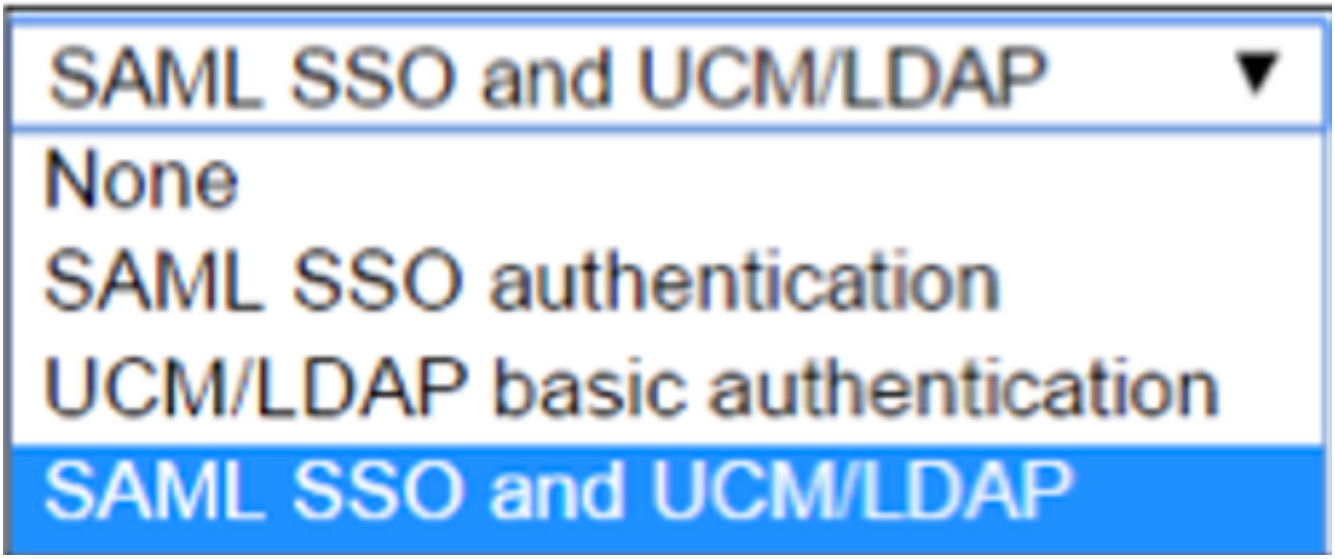


OAuth com login de atualização

Em Parâmetros do Cisco CUCM Enterprise, Verifique se OAuth com parâmetro de fluxo de login de atualização está ativado. Vá para **Cisco Unified CM Administration > Enterprise Parameters > SSO and OAuth Configuration**.



Caminho de autenticação



- Se o caminho de autenticação estiver definido como "autenticação SSO SAML", somente os

clientes Jabber que usam um cluster Unified CM habilitado para SSO poderão usar MRA neste Expressway. Esta é uma configuração somente SSO.
- O suporte de MRA do Expressway para todos os telefones IP, todos os endpoints do TelePresence e todos os clientes Jabber associados a um cluster do Unified CM não configurado para SSO exigirão que o caminho de autenticação inclua a autenticação UCM/LDAP.
- Se um ou mais clusters do Unified CM oferecerem suporte a Jabber SSO, selecione "SAML SSO e UCM/LDAP" para permitir SSO e autenticação básica.

Arquitetura SSO

O SAML é um formato de dados padrão aberto baseado em XML que permite que os administradores acessem um conjunto definido de aplicativos de colaboração da Cisco de forma transparente após se conectarem a um desses aplicativos. O SAML SSO usa o protocolo SAML 2.0 para oferecer login único entre domínios e produtos para soluções de colaboração da Cisco.

Fluxo de login no local

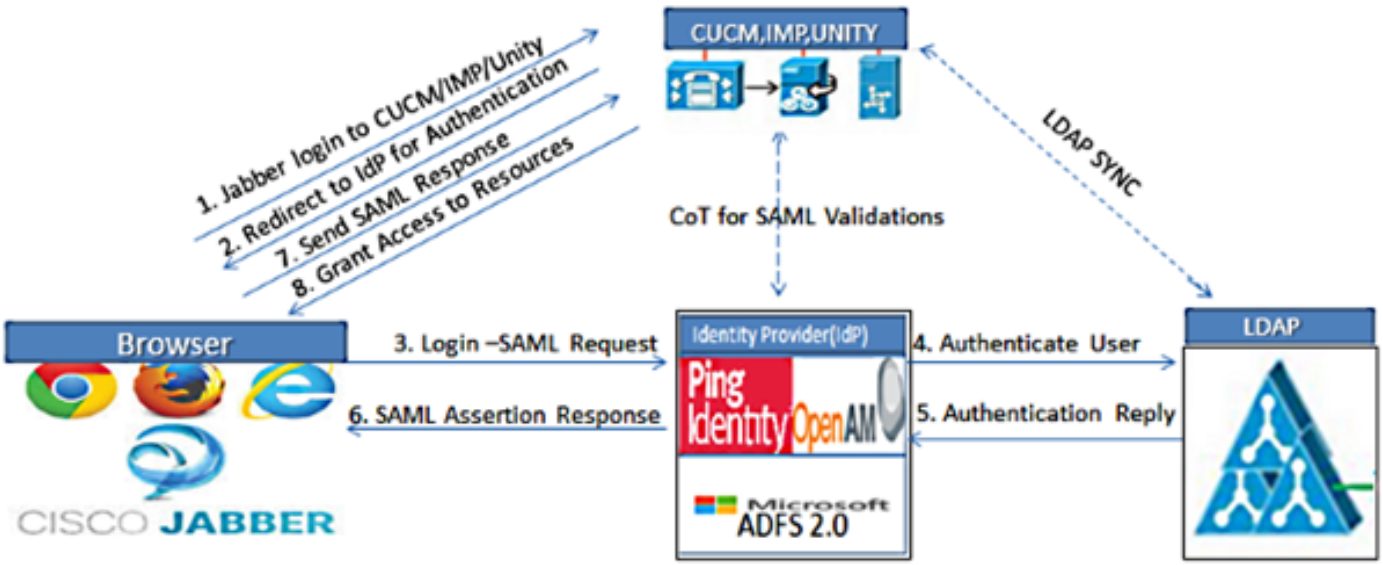
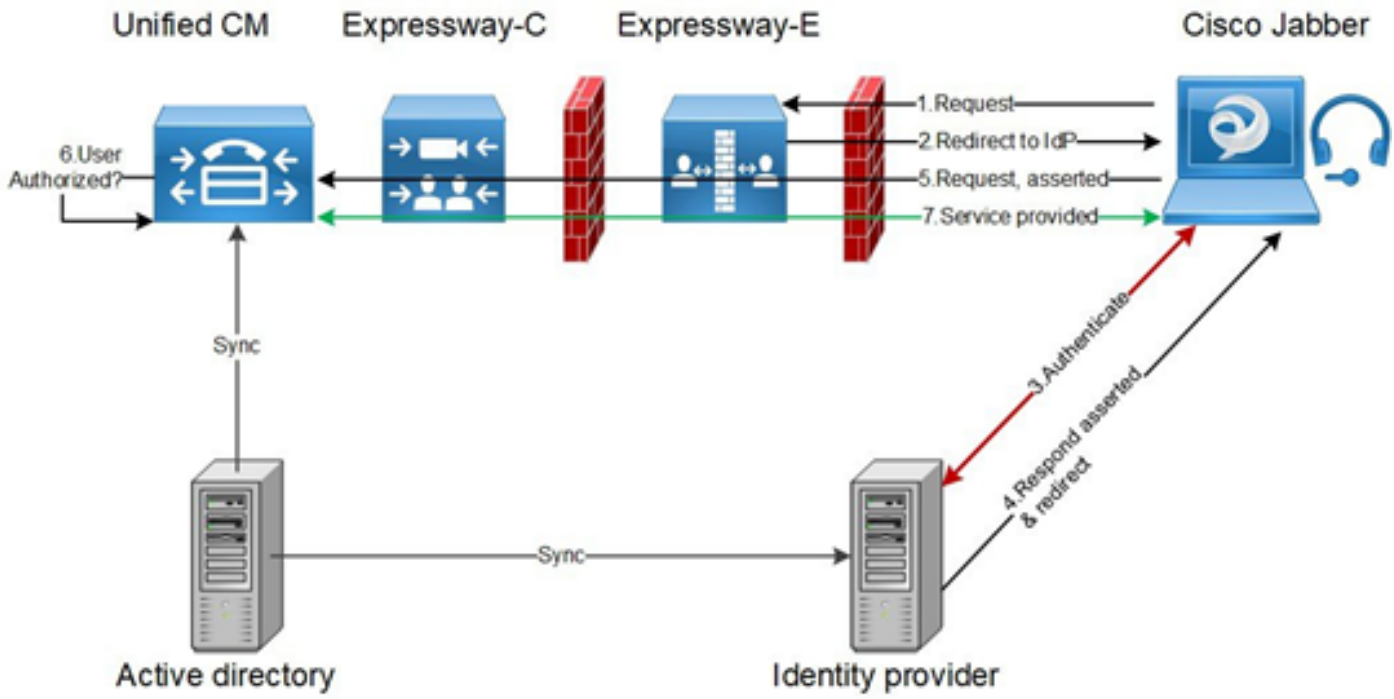


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Fluxo de login de MRA



OAuth

OAuth é um padrão que suporta autorização. Um usuário deve ser autenticado antes de ser autorizado. O fluxo de concessão de código de autorização fornece um método para que um cliente obtenha acesso e atualize tokens para acessar um recurso (serviços Unified CM, IM&P, Unity e Expressway). Esse fluxo também é baseado no redirecionamento e, portanto, exige que o cliente possa interagir com um agente de usuário HTTP (navegador da Web) controlado pelo usuário. O cliente fará uma solicitação inicial ao servidor de autorização usando HTTPS. O servidor OAuth redireciona o usuário para um serviço de autenticação. Isso pode ser executado no Unified CM ou em um IdP externo se o SSO SAML estiver habilitado. Dependendo do método de autenticação usado, uma exibição de página da Web pode ser apresentada ao usuário final para se autenticar. (A autenticação Kerberos é um exemplo que não exibiria uma página da Web.) Ao contrário do fluxo de concessão implícito, um fluxo de concessão de código de autenticação bem-sucedido fará com que os servidores OAuth emitam um "Código de autorização" para o navegador da Web. Este é um código exclusivo de uso único e de vida curta que é então passado de volta do navegador para o cliente. O cliente fornece este "Código de autorização" ao servidor de autorização juntamente com um segredo pré-compartilhado e recebe em troca um "Token de acesso" e um "Token de atualização". O segredo do cliente usado nesta etapa permite que o serviço de autorização limite o uso somente para clientes registrados e autenticados. Os tokens são usados para as seguintes finalidades:

Token de acesso/atualização

Token de acesso: Este token é emitido pelo servidor de autorização. O cliente apresenta o token a um servidor de recursos quando precisa acessar recursos protegidos nesse servidor. O servidor de recursos pode validar o token e confiar em conexões usando o token. (Os tokens de acesso da Cisco têm como padrão uma vida útil de 60 minutos)

Atualizar token: Este token é emitido novamente pelo servidor de autorização. O cliente apresenta esse token ao servidor de autorização juntamente com o segredo do cliente quando o token de acesso expirou ou está prestes a expirar. Se o token de atualização ainda for válido, o servidor de autorização emitirá um novo token de acesso sem exigir outra autenticação. (Os tokens de atualização da Cisco têm como padrão uma vida útil de 60 dias). Se o token de atualização expirou, um novo fluxo de concessão de código de autorização OAuth completo deve ser iniciado

para obter novos tokens.

O fluxo de concessão do código de autorização OAuth é melhor

No fluxo de concessão implícito, o token de acesso é passado ao cliente Jabber através de um agente de usuário HTTP (navegador). No fluxo de concessão do código de autorização, o token de acesso é trocado diretamente entre o servidor de autorização e o cliente Jabber. O token é solicitado ao servidor de autorização usando um código de autorização único limitado por tempo. Essa troca direta do token de acesso é mais segura e reduz a exposição ao risco.

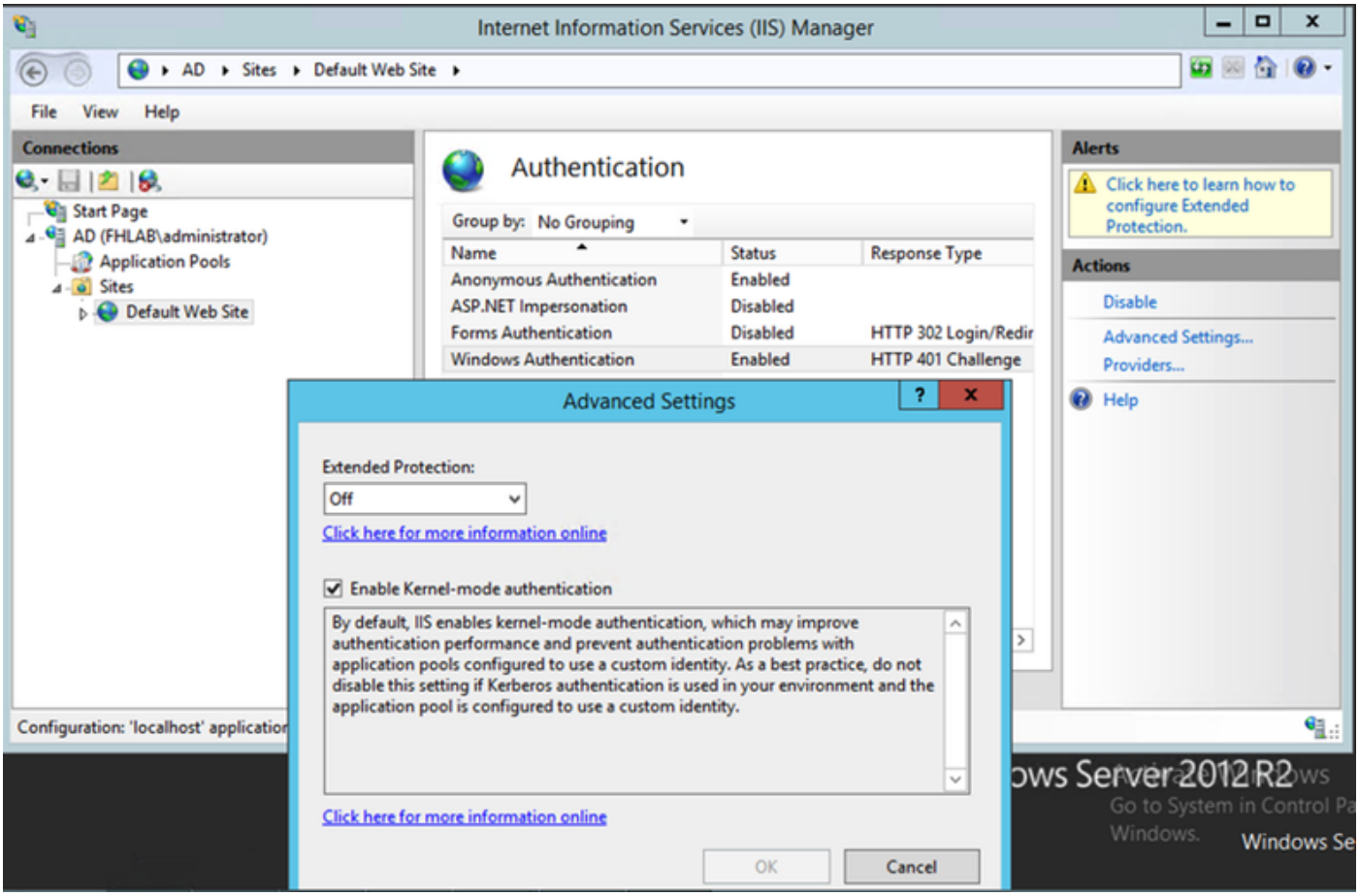
O fluxo de concessão de código de autorização OAuth suporta o uso de tokens de atualização. Isso proporciona uma melhor experiência ao usuário final, pois ele não precisa se autenticar novamente com a mesma frequência (por padrão, 60 dias)

Configurar Kerberos

Selecionar autenticação do Windows

Gerenciador dos Serviços de Informações da Internet (IIS) > Sites > Site Padrão > Autenticação > Autenticação do Windows > Configurações Avançadas.

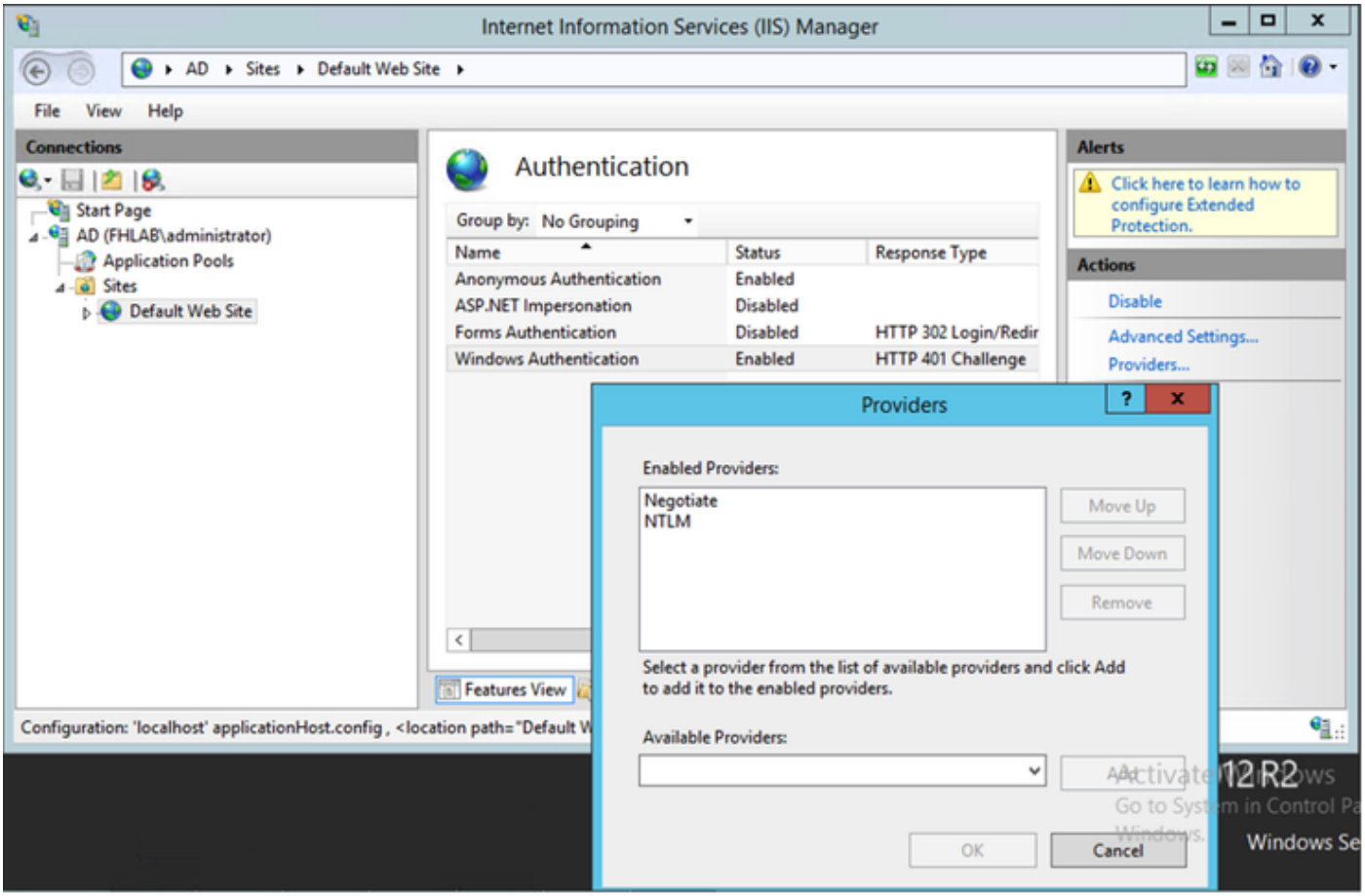
1. Desmarque Ativar autenticação no modo Kernel.
2. Verifique se a proteção estendida está desativada.



O ADFS suporta o Kerberos NTLM

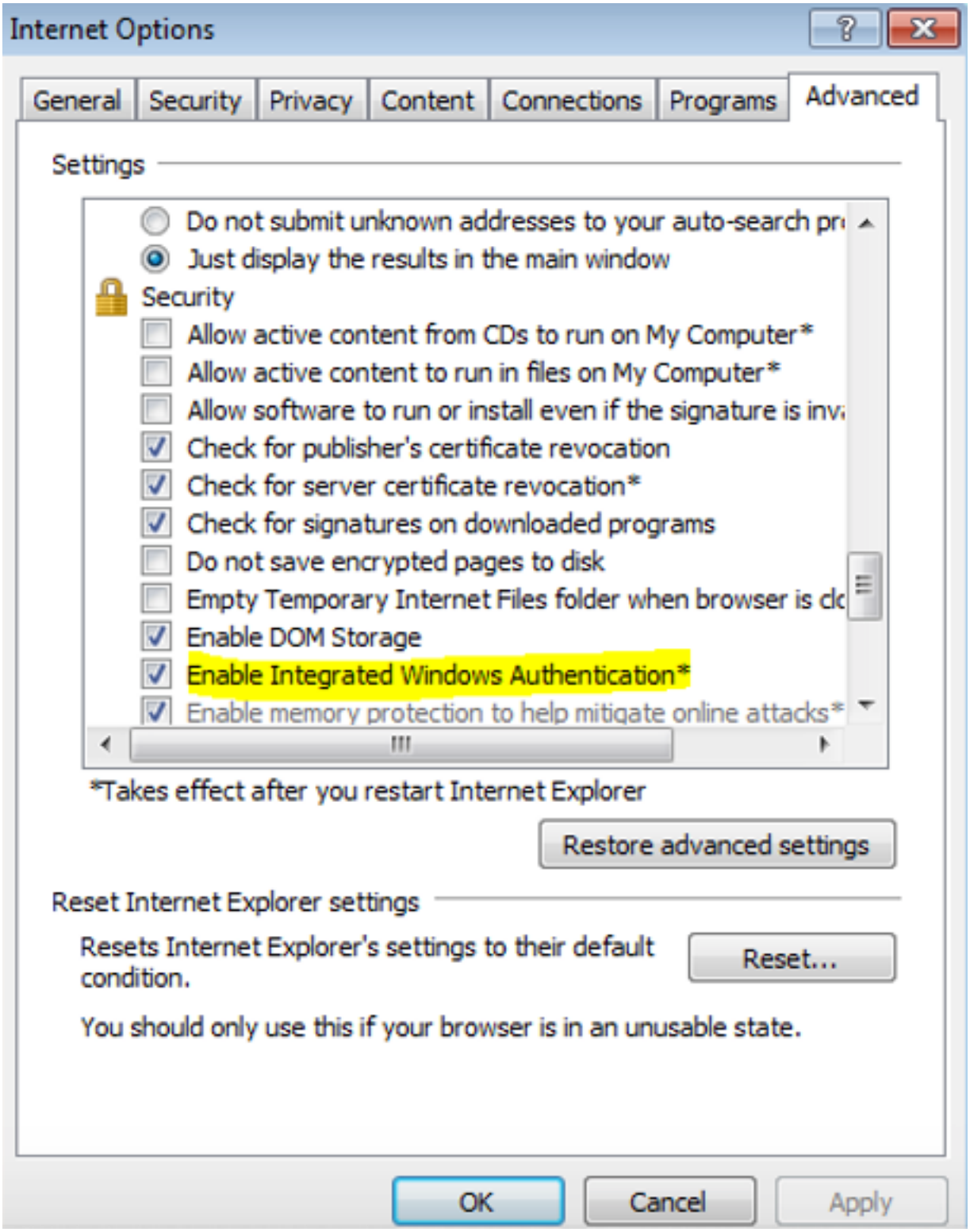
Certifique-se de que o AD FS Versão 3.0 suporta o protocolo Kerberos e o protocolo NT LAN Manager (NTLM) porque todos os clientes não Windows não podem usar Kerberos e dependem do NTLM.

No painel direito, selecione Provedores e verifique se Negociar e NTLM estão presentes em Provedores Habilitados:



Configurar o Microsoft Internet Explorer

Verifique se **Internet Explorer > Advanced > Enable Integrated Windows Authentication** está marcado.



Adicione o URL do ADFS em Segurança > Zonas de Intranet > Sites