

Configurar logon único com CUCM e AD FS 2.0

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Baixe e instale o AD FS 2.0 no Windows Server](#)

[Configurar o AD FS 2.0 no Windows Server](#)

[Importar os metadados de IDP para CUCM / Baixar os metadados de CUCM](#)

[Importar metadados do CUCM para o servidor do AD FS 2.0 e criar regras de reivindicação](#)

[Concluir a habilitação de SSO no CUCM e executar o teste de SSO](#)

[Troubleshooting](#)

[Definir Logs SSO para Depuração](#)

[Localizar O Nome Do Serviço De Federação](#)

[Nome Do Certificado E Do Serviço De Federação Sem Ponto](#)

[O tempo está fora de sincronia entre os servidores CUCM e IDP](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar o SSO (Single Sign-On, Logon único) no Cisco Unified Communications Manager e no Active Directory Federation Service.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Communications Manager (CUCM)
- Conhecimento Básico do Serviço de Federação do Active Directory (AD FS)

Para habilitar o SSO em seu ambiente de laboratório, você precisa desta configuração:

- Windows Server com AD FS instalado.
- CUCM com sincronização LDAP configurada.
- Um usuário final com a função Superusuários CCM padrão selecionada.

Componentes Utilizados

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

- Windows Server com AD FS 2.0
- CUCM 10.5.2

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

O procedimento para o AD FS 2.0 com Windows Server 2008 R2 é fornecido. Estas etapas também funcionam para o AD FS 3.0 no Windows Server 2016.

Baixe e instale o AD FS 2.0 no Windows Server

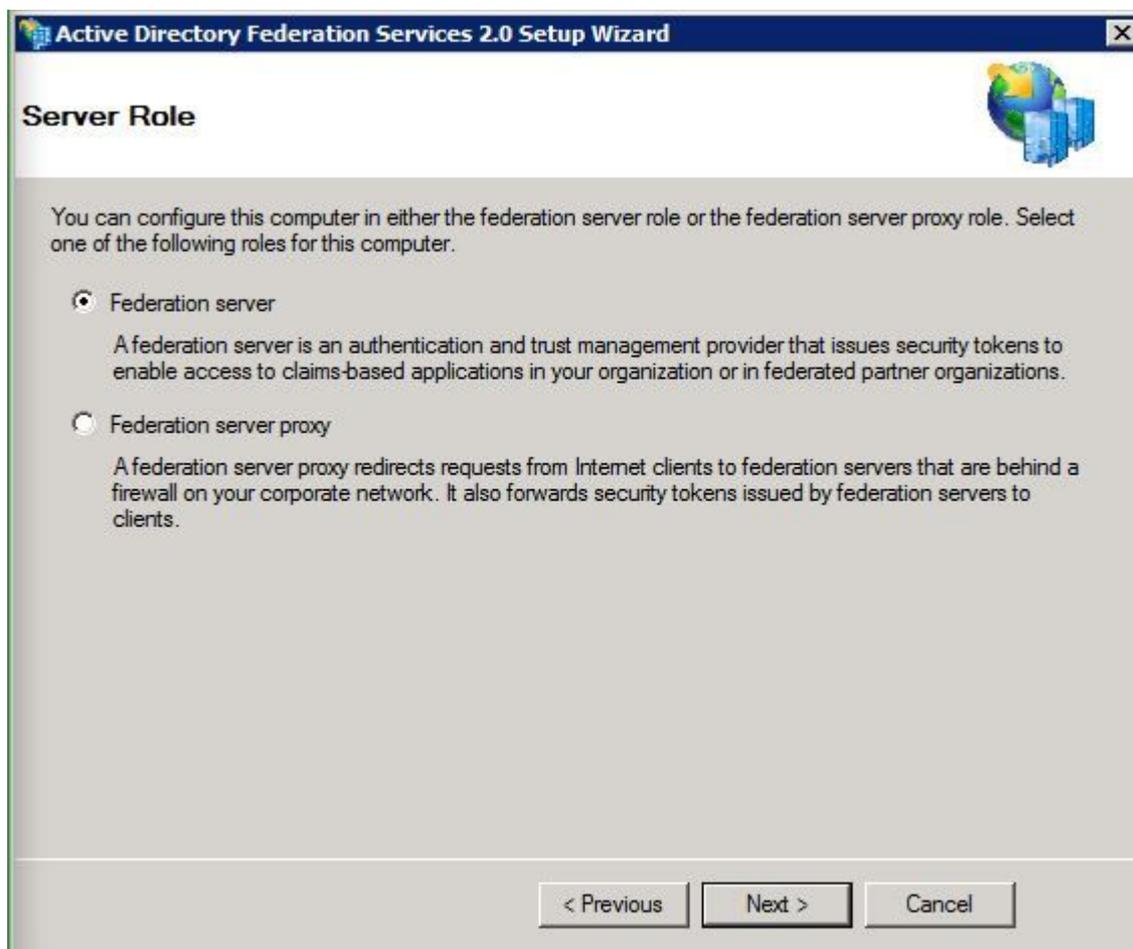
Etapa 1. Navegue para [Baixar AD FS 2.0](#).

Etapa 2. Certifique-se de selecionar o download apropriado com base no Windows Server.

Etapa 3. **Mova** o arquivo baixado para o Windows Server.

Etapa 4. Continue com a instalação:

Etapa 5. Quando solicitado, escolha **Servidor de Federação**:



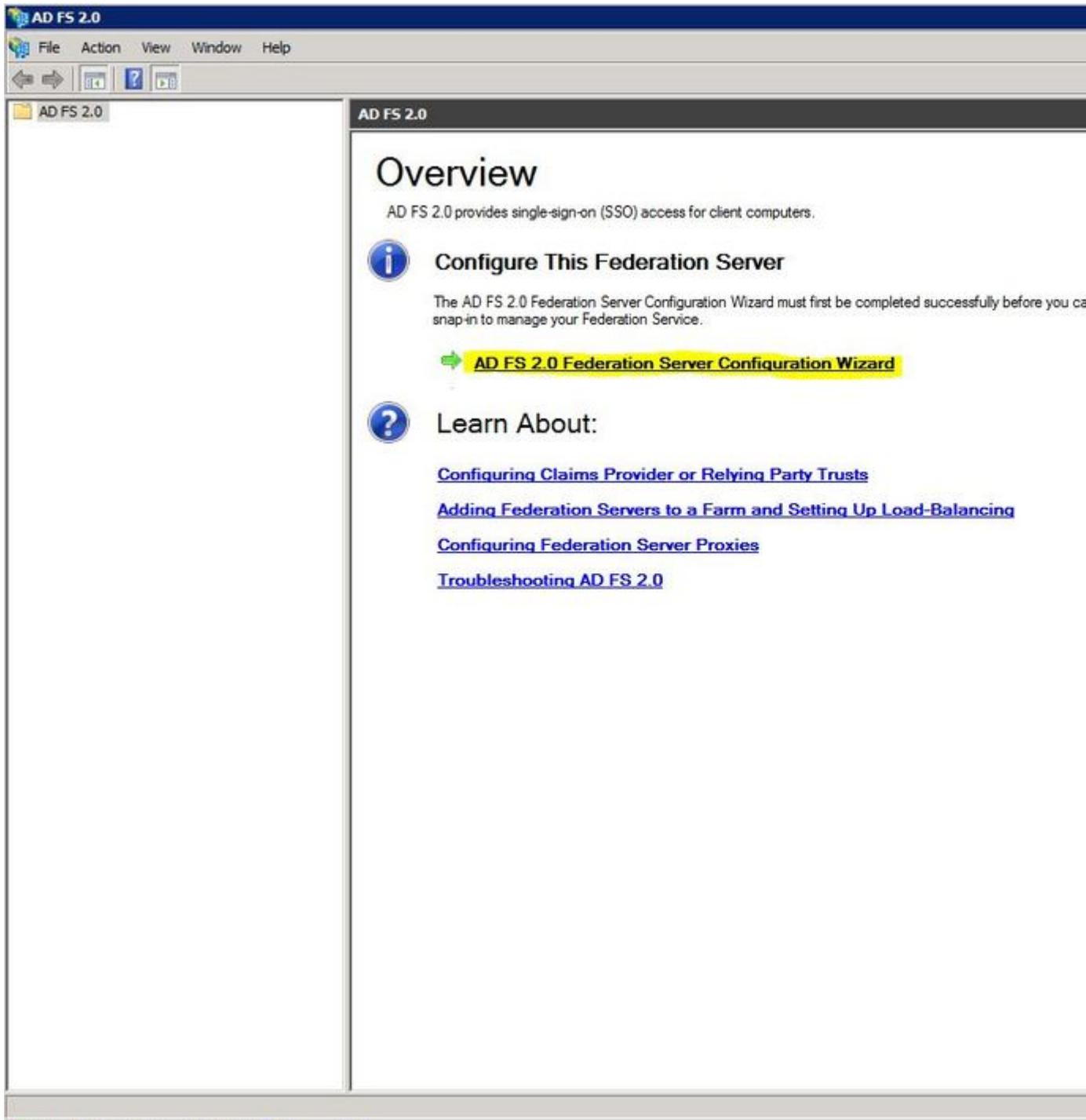
Etapa 6. Algumas dependências são instaladas automaticamente - depois disso, clique em **Concluir**.

Agora que o AD FS 2.0 está instalado no servidor, você precisa adicionar algumas configurações.

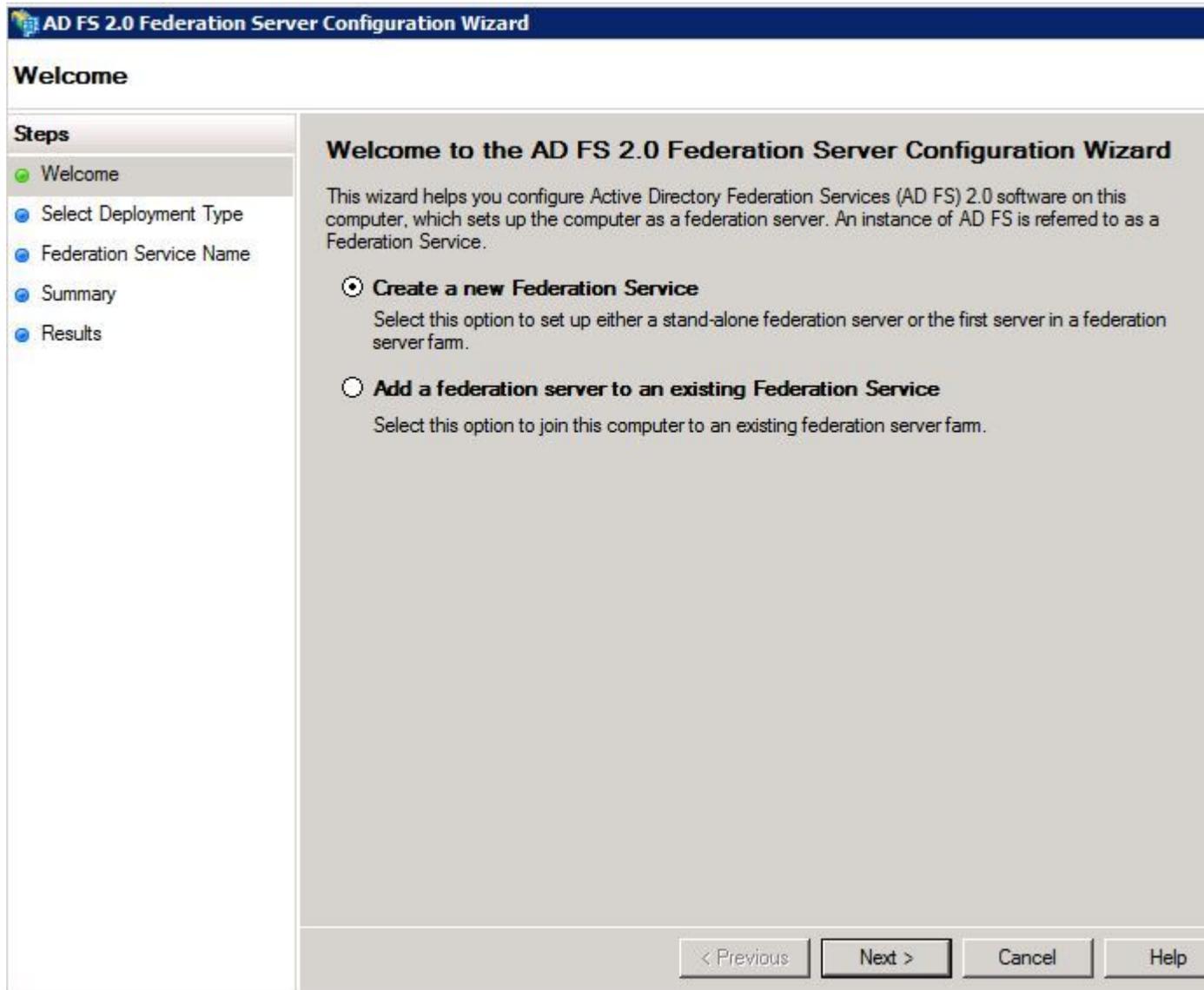
Configurar o AD FS 2.0 no Windows Server

Etapa 1. Se a janela do AD FS 2.0 não abrir automaticamente após a instalação, clique em **Iniciar** e procure Gerenciamento do AD FS 2.0 para abri-la manualmente.

Etapa 2. Escolha o **Assistente de Configuração do Servidor de Federação do AD FS 2.0**.



Etapa 3. Em seguida, clique em **Criar um novo Serviço de Federação**.



Etapa 4. Para a maioria dos ambientes, o **servidor de federação autônomo** é suficiente.

Select Stand-Alone or Farm Deployment

Steps

- Welcome
- Select Deployment Type
- Federation Service Name
- Existing Database
- Summary
- Results

You can create either a stand-alone federation server for evaluation purposes or a small production environment, or you can create a federation server in a new farm for load balancing and high availability.

Select one of the following options. Either of these options will use the Windows Internal Database to store configuration data.

 New federation server farm

This option will create a new Federation Service with settings for high availability and load balancing. This computer will be the primary federation server in the farm. Later, you can scale out this farm by adding more federation servers.

To create a federation server farm, you must run this wizard while you are logged on with an account that has sufficient permissions in Active Directory to create a container object (for sharing certificates) and to set an SPN (for the service account), such as an account that is a member of the Domain Admins group.

 Stand-alone federation server

This option will create a new Federation Service on this computer. This option is recommended for evaluation purposes or a small production environment. If you select this option, you will not be able to add more servers to create a farm.

i You can use SQL Server with AD FS 2.0 to take advantage of the full feature set and achieve maximum scalability. To set up AD FS to use SQL Server, use the command-line version of this wizard. For more information, click Help

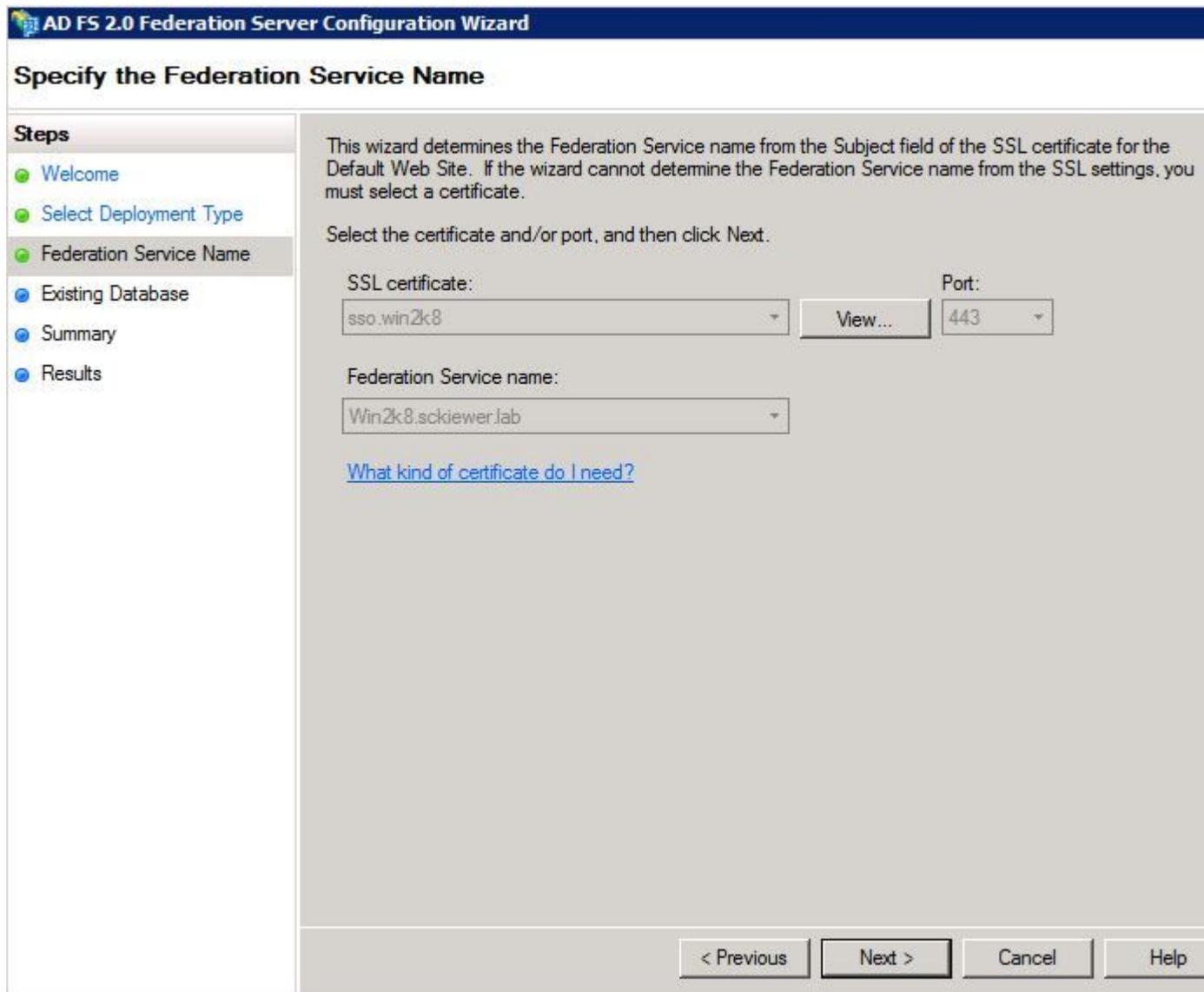
< Previous

Next >

Cancel

Help

Etapa 5. Em seguida, você será solicitado a escolher um certificado. Esse campo será preenchido automaticamente enquanto o servidor tiver um certificado.



Etapa 6. Se já houver um banco de dados do AD FS no servidor, você precisará removê-lo para continuar.

Passo 7. Por fim, você está em uma tela de resumo na qual pode clicar em **Avançar**.

Importar os metadados de IDP para CUCM / Baixar os metadados de CUCM

Etapa 1. Atualize a URL com o nome de host/FQDN do servidor Windows e baixe os metadados do servidor AD FS - <https://hostname/federationmetadata/2007-06/federationmetadata.xml>

Etapa 2. Navegue até **Cisco Unified CM Administration > System > SAML Single Sign-On**.

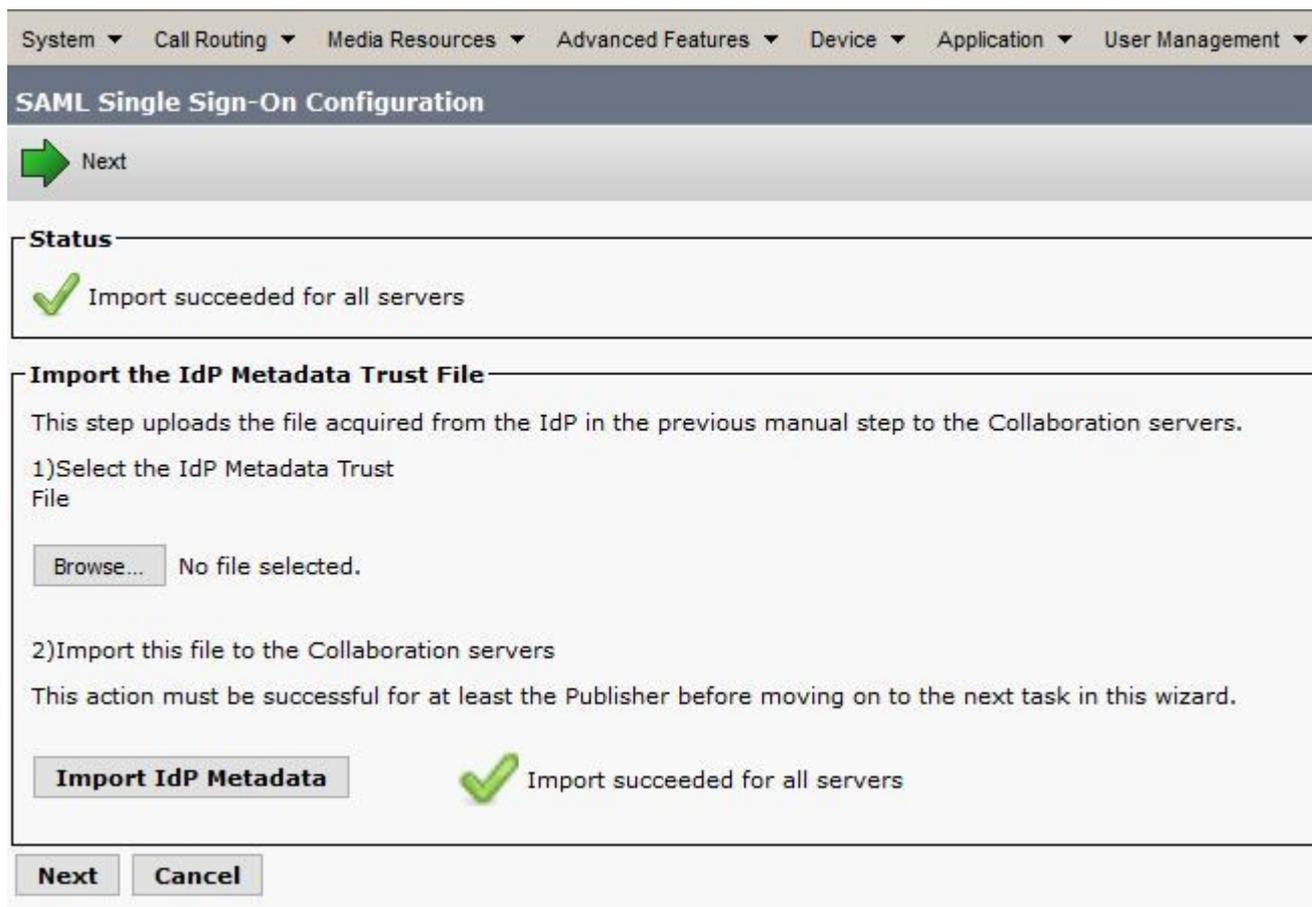
Etapa 3. Clique em **Ativar SAML SSO**.

Etapa 4. Se você receber um alerta sobre Conexões do Servidor Web, clique em **Continuar**.

Etapa 5. Em seguida, o CUCM instrui você a baixar o arquivo de metadados do seu IdP. Neste cenário, o servidor AD FS é o IdP e você baixou os metadados na Etapa 1, então clique em **Avançar**.

Etapa 6. Clique em **Browse > Selecione o .xml na Etapa 1 > Clique em Import IdP Metadata.**

Passo 7. Uma mensagem indica que a importação foi bem-sucedida:



The screenshot shows a web-based configuration interface for SAML Single Sign-On. At the top, there is a navigation menu with items: System, Call Routing, Media Resources, Advanced Features, Device, Application, and User Management. Below the menu is a header for 'SAML Single Sign-On Configuration'. A green arrow icon with the text 'Next' is visible. The main content area is titled 'Status' and displays a green checkmark icon followed by the text 'Import succeeded for all servers'. Below this, there is a section titled 'Import the IdP Metadata Trust File'. It contains instructions: 'This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.' followed by '1) Select the IdP Metadata Trust File'. There is a 'Browse...' button and the text 'No file selected.'. Below that, it says '2) Import this file to the Collaboration servers' and 'This action must be successful for at least the Publisher before moving on to the next task in this wizard.'. At the bottom of this section, there is an 'Import IdP Metadata' button and a green checkmark icon with the text 'Import succeeded for all servers'. At the very bottom of the wizard, there are 'Next' and 'Cancel' buttons.

Etapa 8. Clique em Next.

Etapa 9. Agora que você tem os metadados de IdP importados para o CUCM, é necessário importar os metadados do CUCM para seu IdP.

Etapa 10. Clique em **Download Trust Metadata File.**

Etapa 11. Clique em Next.

Etapa 12. Mova o arquivo .zip para o Windows Server e extraia o conteúdo para uma pasta.

Importar metadados do CUCM para o servidor do AD FS 2.0 e criar regras de reivindicação

Etapa 1. Clique em **Iniciar** e procure **Gerenciamento do AD FS 2.0.**

Etapa 2. Clique em **Necessário: Adicionar uma terceira parte confiável.**

Observação: se essa opção não for exibida, feche a janela e abra-a novamente.

Etapa 3. Depois de abrir o **Assistente de Adição de Confiança de Terceira Parte Confiável**, clique em **Iniciar.**

Etapa 4. Aqui, você precisa importar os arquivos XML extraídos na etapa 12. Selecione **Importar dados sobre a terceira parte confiável de um arquivo**, navegue até os arquivos de pasta e escolha o XML do editor.

Observação: Use as etapas anteriores para qualquer servidor do Unified Collaboration no qual você pretenda utilizar o SSO.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Select Data Source'. On the left, a 'Steps' pane lists: Welcome, Select Data Source (highlighted), Specify Display Name, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains three radio button options: 1. 'Import data about the relying party published online or on a local network' (unselected), with a text box for 'Federation metadata address (host name or URL)' and an example 'fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data about the relying party from a file' (selected), with a text box for 'Federation metadata file location' containing 'C:\Users\Administrator\Desktop\SPMetadata_1cucm1052.sckiewer.lab.xml' and a 'Browse...' button. 3. 'Enter data about the relying party manually' (unselected). At the bottom are buttons for '< Previous', 'Next >', 'Cancel', and 'Help'.

Etapa 5. Clique em Next.

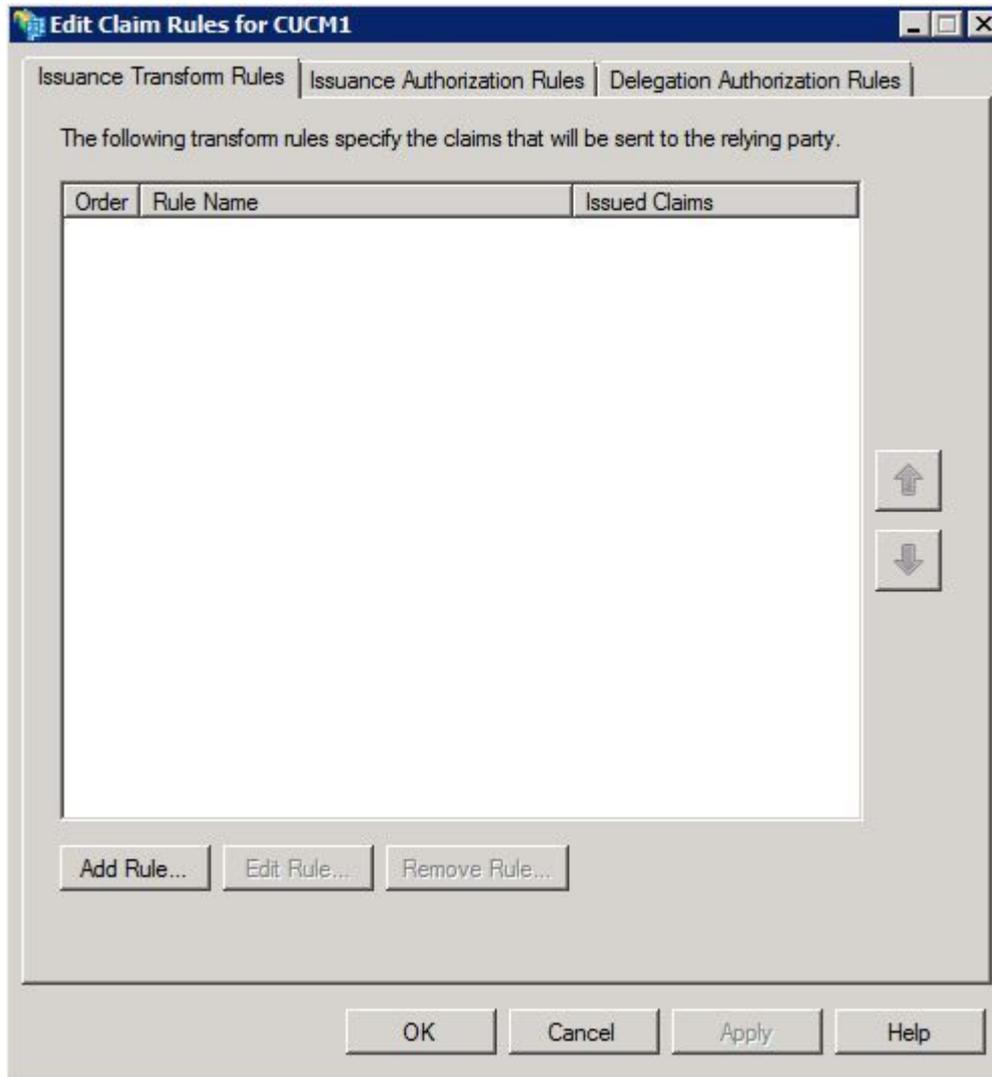
Etapa 6. Edite o **Nome para Exibição** e clique em **Avançar**.

Passo 7. Escolha **Permitir que todos os usuários acessem esta terceira parte confiável** e clique em **Avançar**.

Etapa 8. Clique em **Avançar** novamente.

Etapa 9. Nesta tela, certifique-se de que você tenha **Abrir a caixa de diálogo Editar regras de reivindicação para esta confiança da terceira parte confiável quando o assistente fechar** marcada e, em seguida, clique em **Fechar**.

Etapa 10. A janela Editar regras de reivindicação é aberta:



Etapa 11. Nessa janela, clique em **Adicionar regra**.

Etapa 12. Para **Modelo de regra de declaração**, escolha **Enviar atributos LDAP como declarações** e clique em **Avançar**.

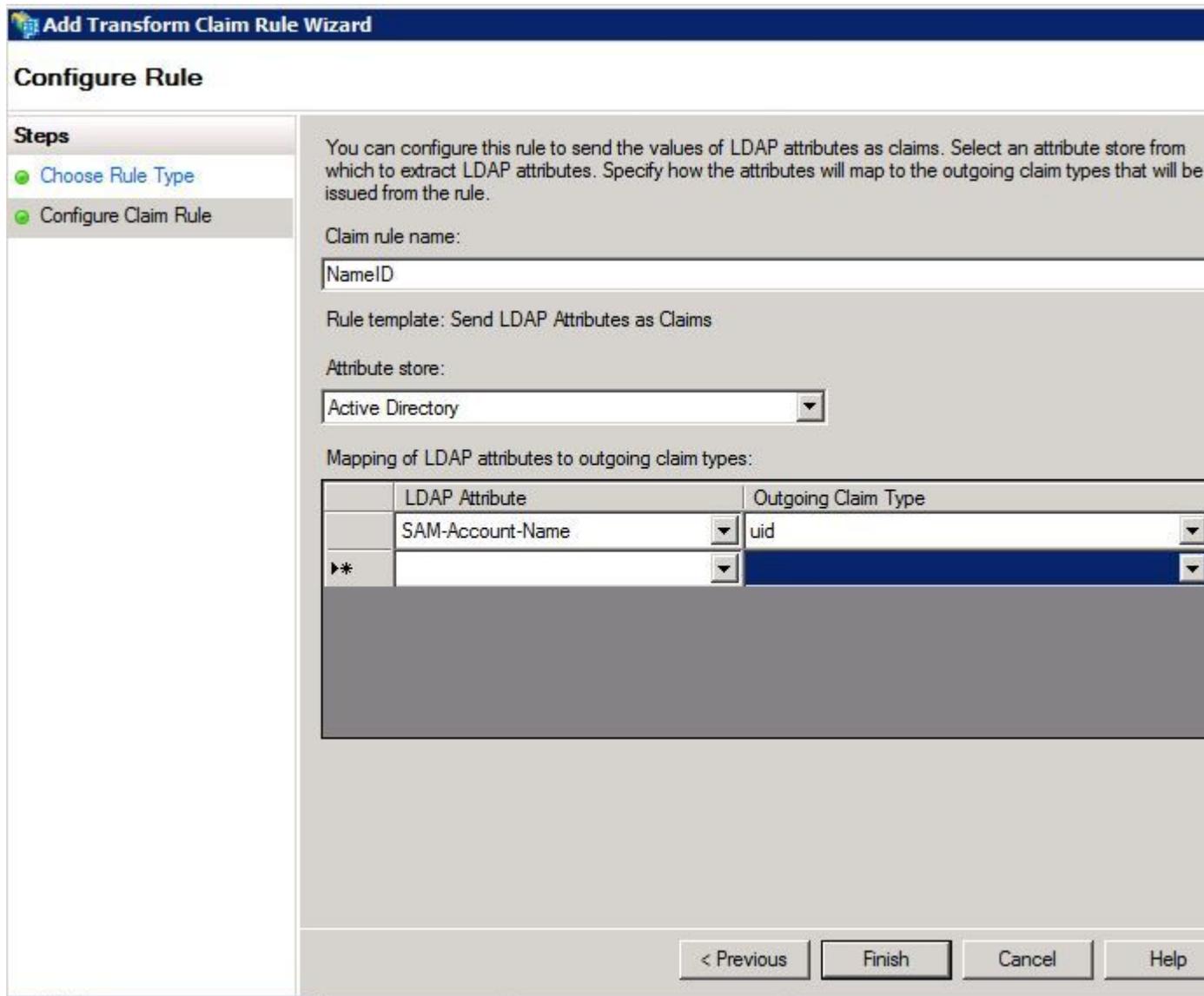
Etapa 13. Na próxima página, digite **NameID** para o **Nome da regra de reivindicação**.

Etapa 14. Escolha **Active Directory** para o **repositório de atributos**.

Etapa 15. Escolha **SAM-Account-Name** para o **Atributo LDAP**.

Etapa 16. Insira **uid** para **Tipo de Declaração de Saída**.

Observação: o uid não é uma opção na lista suspensa - ele deve ser inserido manualmente.



Etapa 17. Clique em Finish.

Etapa 18. A primeira regra está terminada. Clique em **Adicionar regra** novamente.

Etapa 19. Escolha **Enviar reivindicações usando uma regra personalizada**.

Etapa 20. Insira um **Nome da regra de Declaração**.

Etapa 21. No campo **Regra personalizada**, cole este texto:

```
c:[Digite == "http://schemas.microsoft.com/ws/2008/06/identity/reivindicações/windowsaccountname"]
=> issue(Tipo = "http://schemas.xmlsoap.org/ws/2005/05/identity/claim/nameidentifier", Emissor = c.Issuer,
OriginalIssuer = c.OriginalIssuer, Valor = 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\_FEDERATION\_SERVICE\_NAME/com/adfs/service/trust",
Propriedades["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"CUCM_ENTITY_ID");
```

Etapa 22. Certifique-se de alterar AD_FS_SERVICE_NAME e CUCM_ENTITY_ID para os valores apropriados.

Observação: se não tiver certeza sobre o Nome do Serviço do AD FS, siga as etapas para localizá-lo. A ID da entidade do CUCM pode ser extraída da primeira linha no arquivo de metadados do CUCM. Existe um entityID na primeira linha do arquivo que se parece com isto, entityID=1cucm1052.sckiewer.lab,. Insira o valor sublinhado na seção apropriada da regra de reivindicação.

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, specifically the 'Configure Rule' step. The 'Steps' pane on the left shows 'Choose Rule Type' and 'Configure Claim Rule' as completed steps. The main area contains the following text:

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language.

Claim rule name: CUCM SSO Custom Rule

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
=> 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://win2k8.sckiewer.lab/adfs/com/adfs/service/trust", Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "1cucm1052.sckiewer.lab");
```

[More about the claim rule language...](#)

At the bottom, there are buttons for '< Previous', 'Finish', 'Cancel', and 'Help'.

Etapa 23. Clique em Finish.

Etapa 24. Click OK.

Observação: as regras de reivindicação são necessárias para qualquer servidor do Unified Collaboration no qual você pretende utilizar o SSO.

Concluir a habilitação de SSO no CUCM e executar o teste de SSO

Etapa 1. Agora que o servidor AD FS está totalmente configurado, você pode voltar para o CUCM.

Etapa 2. Você parou na página de configuração final:

SAML Single Sign-On Configuration

 Back

Status

 The server metadata file must be installed on the IdP before this test is run.

Test SSO Setup

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test

1) Pick a valid username to use for this test

You must already know the password for the selected username.
This user must have administrator rights and also exist in the IdP.

 Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrative access.

Valid administrator Usernames

sckiewer

2) Launch SSO test page

Etapa 3. Selecione o usuário final que tem a função **Superusuários CCM padrão** selecionada e clique em Executar teste de SSO...

Etapa 4. Certifique-se de que o navegador permita pop-ups e insira suas credenciais no prompt.

SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test. Please close this window and click "Finish" on the SAML configuration wizard to complete the setup.

Close

Etapa 5. Clique em **Fechar** na janela pop-up e em **Concluir**.

Etapa 6. Após uma breve reinicialização das aplicações Web, o SSO é ativado.

Troubleshooting

Definir Logs SSO para Depuração

Para definir os logs de SSO para depuração, você deve executar esse comando na CLI do CUCM: **set samltrace level debug**

Os logs de SSO podem ser baixados do RTMT. O nome do conjunto de logs é **Cisco SSO**.

Localizar O Nome Do Serviço De Federação

Para localizar o nome do serviço de federação, clique em **Iniciar** e procure **Gerenciamento do AD FS 2.0**.

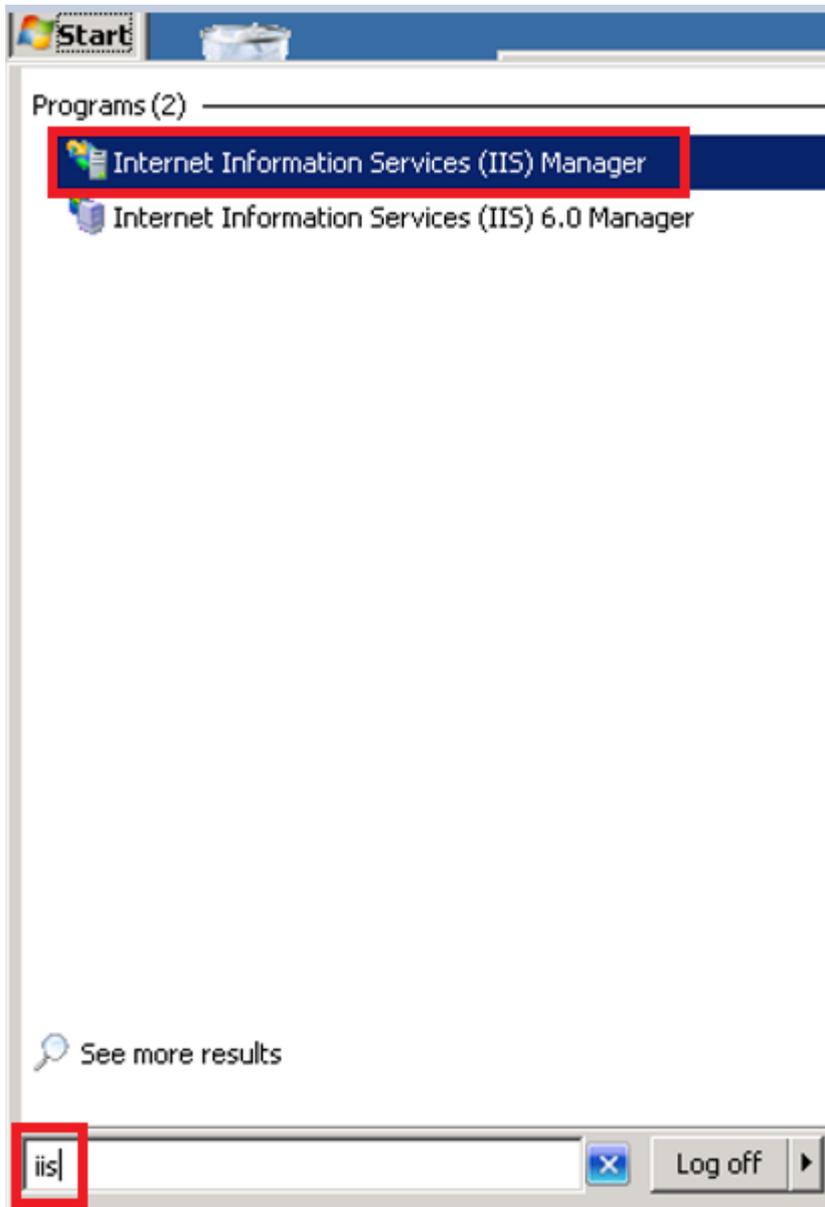
- Clique em Editar **Propriedades do Serviço de Federação...**
- Na tab Geral, procure o **nome do Serviço de Federação**

Nome Do Certificado E Do Serviço De Federação Sem Ponto

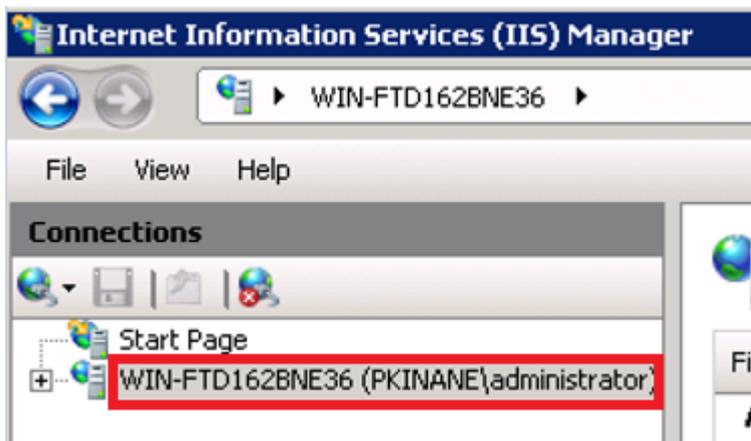
Se você receber esta mensagem de erro no assistente de configuração do AD FS, precisará criar um novo certificado.

O certificado selecionado não pode ser usado para determinar o nome do Serviço de Federação porque ele tem um nome de Entidade sem ponto (nome curto). Selecione outro certificado sem um nome de Entidade sem ponto (nome abreviado) e tente novamente.

Etapa 1. Clique em Iniciar, procure por iis e abra o Gerenciador dos Serviços de Informações da Internet (IIS)



Etapa 2. Clique no nome do servidor.



Etapa 3. Clique em Certificados do servidor.

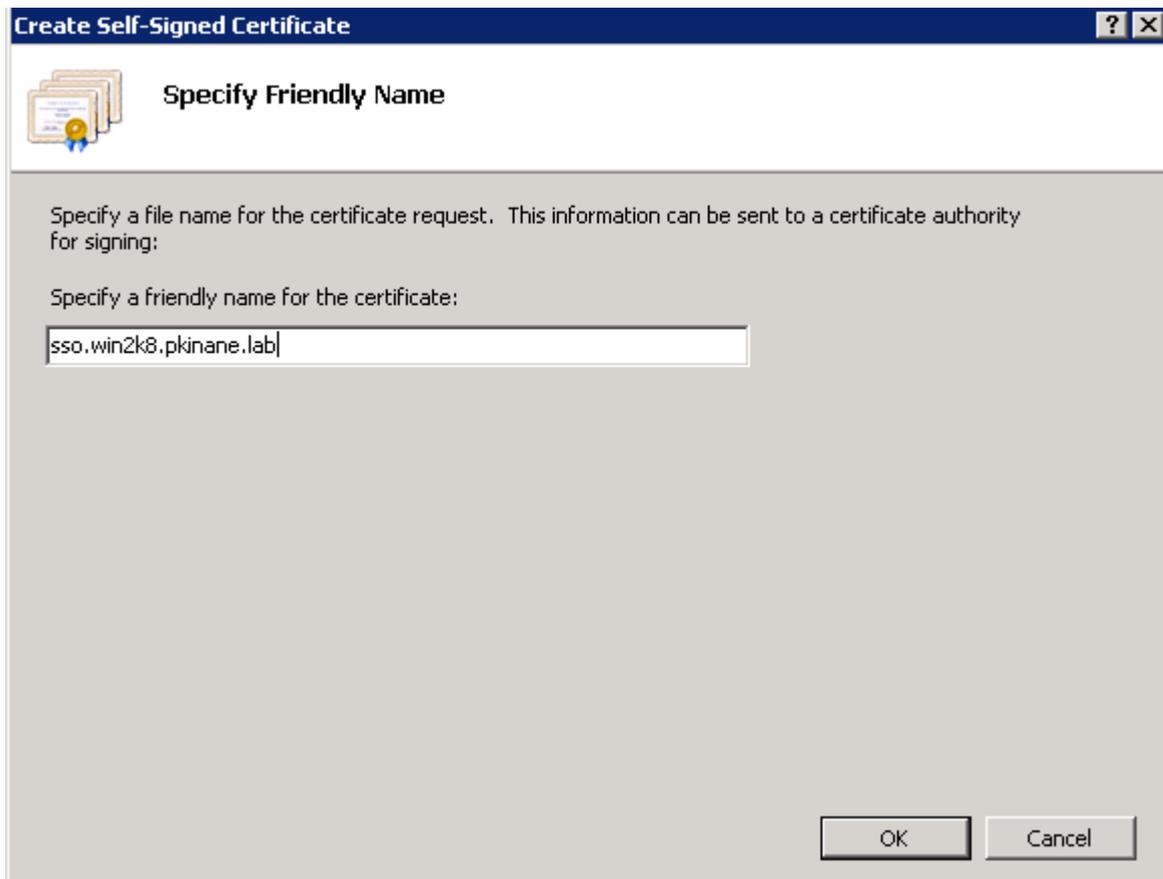
IIS



Etapa 4. Clique em Criar certificado autoassinado.



Etapa 5. Insira o nome desejado para o alias do certificado.



O tempo está fora de sincronia entre os servidores CUCM e IDP

Se você receber esse erro ao executar o teste de SSO do CUCM, será necessário configurar o Windows Server para usar os mesmos servidores NTP que o CUCM.

Resposta SAML inválida. Isso pode ser causado quando o tempo está fora de sincronia entre os servidores Cisco Unified Communications Manager e IDP. Verifique a configuração do NTP em ambos os servidores. Execute "utils ntp status" na CLI para verificar esse status no Cisco Unified Communications Manager.

Depois que o Windows Server tiver os servidores NTP corretos especificados, você precisará executar outro teste de SSO e ver se o problema persiste. Em alguns casos, é necessário distorcer o período de validade da asserção. Mais detalhes sobre esse processo [aqui](#).

Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)

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.