Configurar único Sinal-em usar CUCM e AD FS 2.0 (Windows Server 2008 o R2)

Índice

Introdução

Este documento descreve como configurar único Sinal-em usar uma comunicação unificada Cisco controla (CUCM) e o serviço da federação do diretório ativo (AD FS) 2.0 (Windows Server 2008 R2).

Contribuído por Scott Kiewert, engenheiro de TAC da Cisco.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco unificou o gerente de uma comunicação
- Conhecimento de Basick de ADFS 2.0

A fim permitir o SSO em seu ambiente de laboratório, você precisa esta configuração

- Windows Server com o AD FS 2.0 instalado
- CUCM com a sincronização LDAP configurada.
- **Um utilizador final** com o papel de **superusuários do padrão CCM** selecionado.

Componentes Utilizados

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

- Windows Server com AD FS 2.0
- CUCM

Informação interna de Cisco

Transfira e instale AD FS 2.0 em seu Windows Server

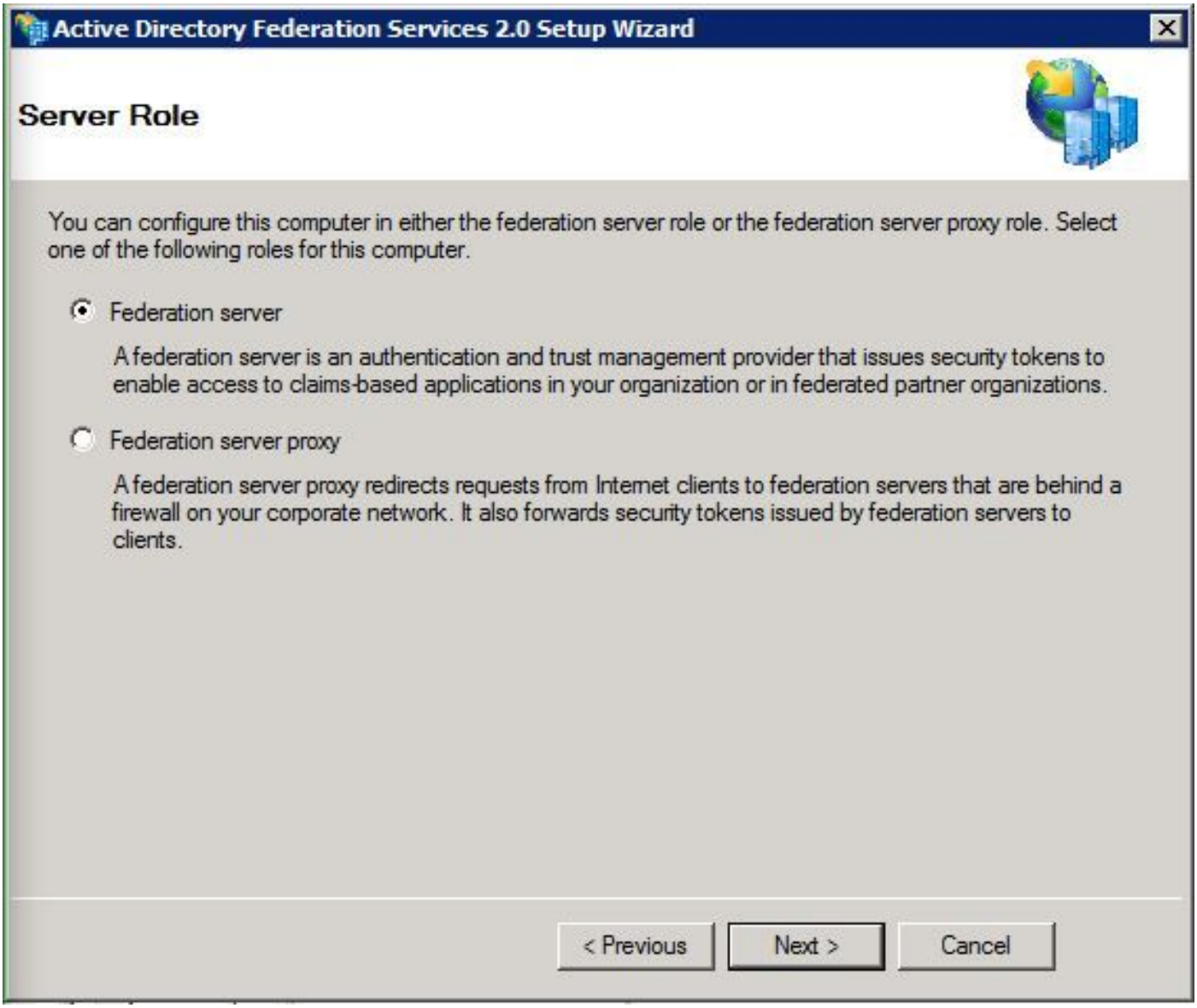
Etapa 1. Navegue a https://www.microsoft.com/en-us/download/details.aspx?id=10909 e o clique continua.

Etapa 2. Na janela pop-up, certifique-se de você selecionar a transferência apropriada baseada em seu Windows Server.

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

Etapa 4. Continue com a instalação:

Etapa 5. Quando alertado, selecione o **server da federação**:



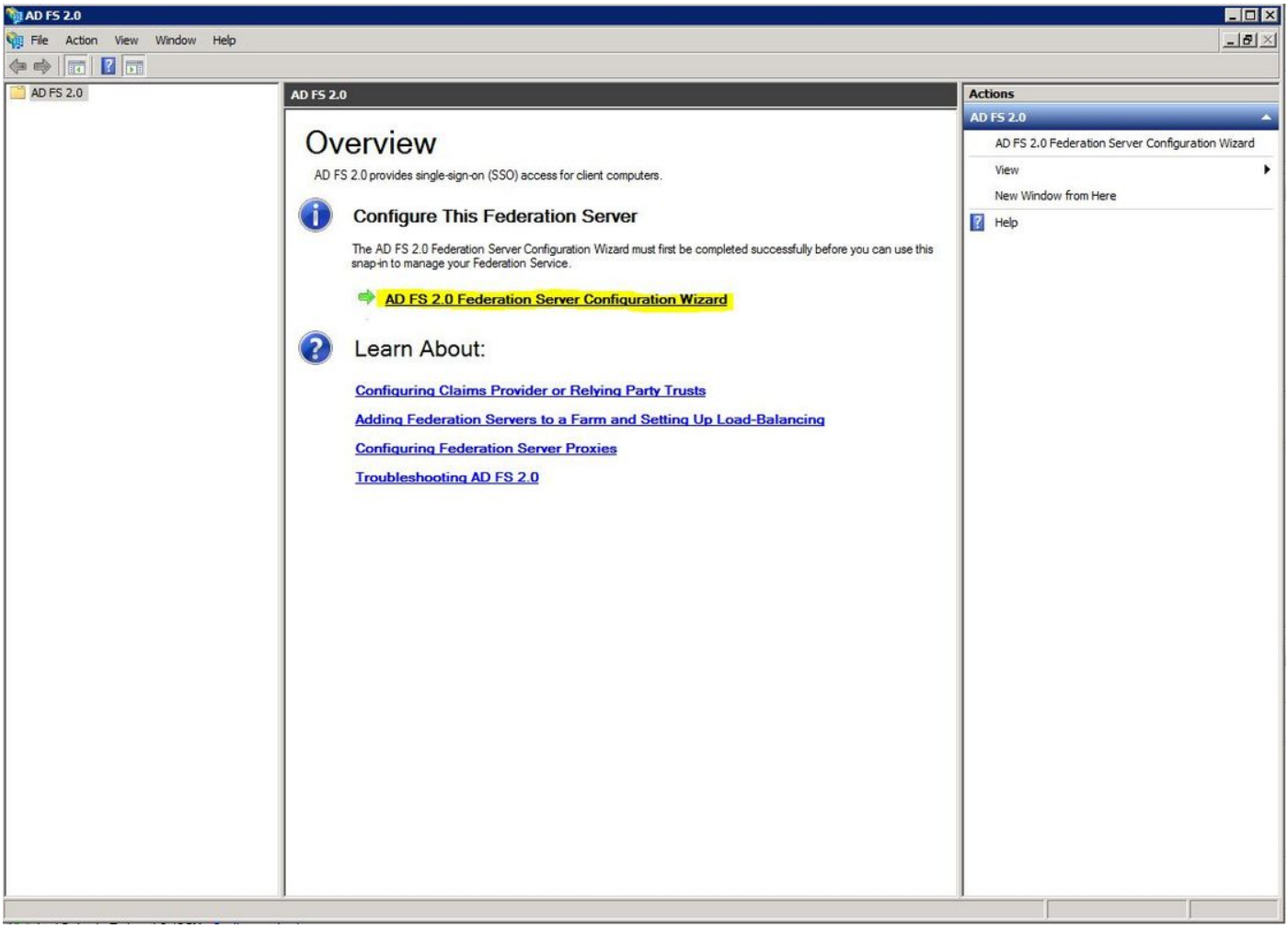
Etapa 6. Algumas dependências podem ser instaladas automaticamente e você é alertado clicar o **revestimento**.

Agora que você tem AD FS 2.0 instalado em seu server, você precisa de adicionar alguma configuração.

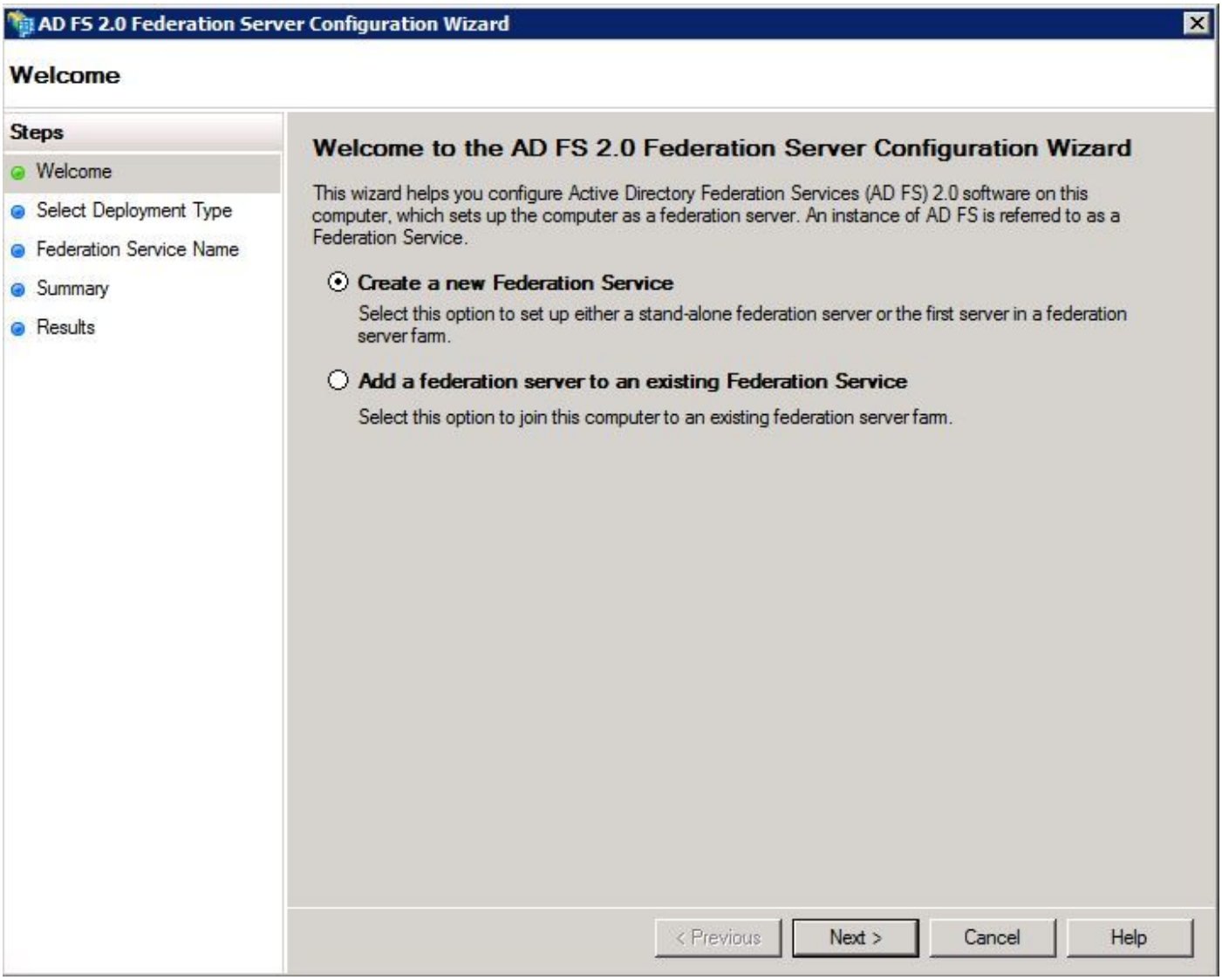
Configurar AD FS 2.0 em seu Windows Server

Etapa 1. O indicador AD FS 2.0 deve ter aberto depois que a instalação, contudo, você pode encontrá-la clicando o **começo** e procurando pelo Gerenciamento AD FS 2.0.

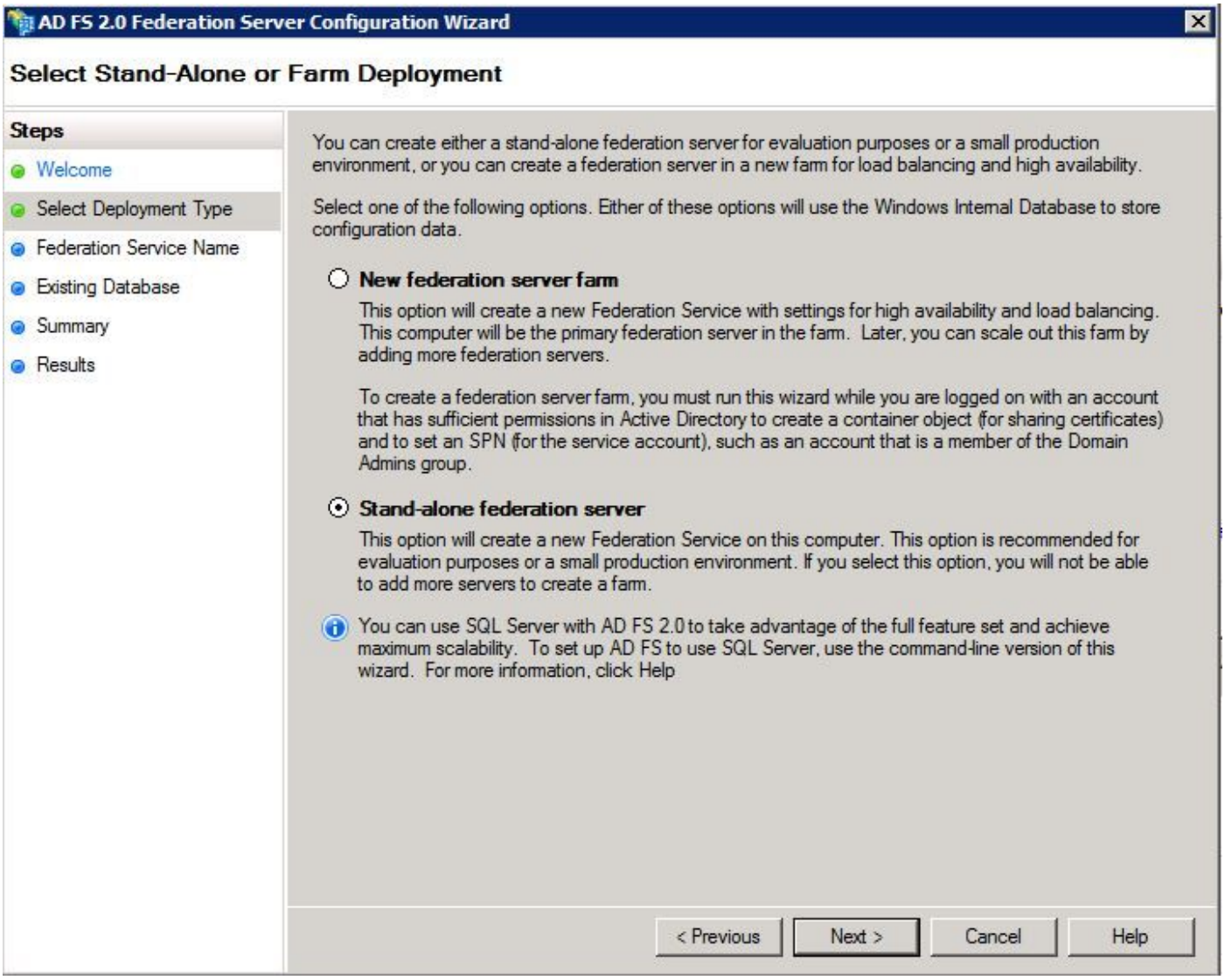
Etapa 2. Uma vez que você tem o indicador AD FS aberto, selecione o **assistente da configuração do servidor da federação AD FS 2.0.**



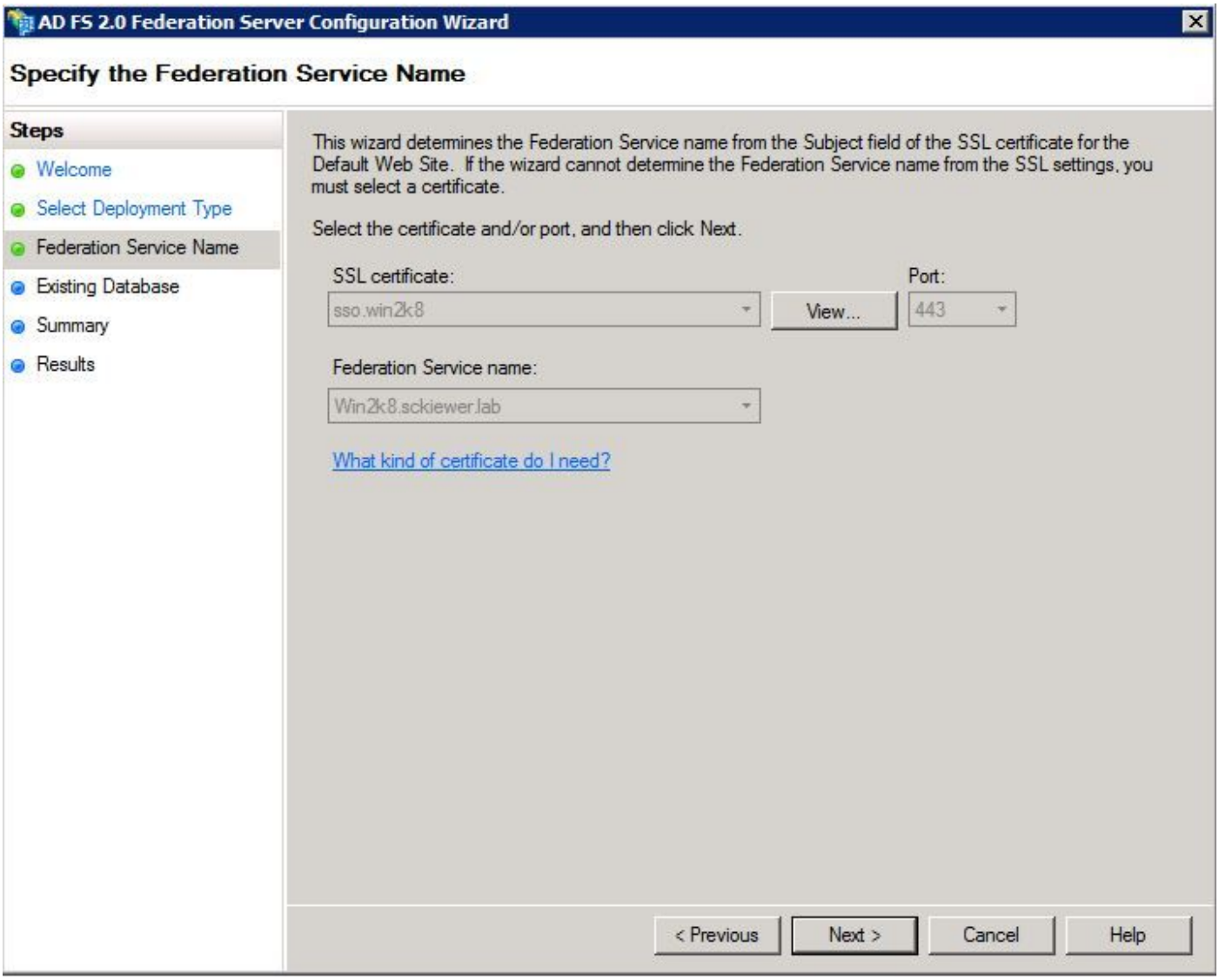
Etapa 3. Em seguida, o clique **cria um serviço novo da federação.**



Etapa 4. Para um ambiente de laboratório, o server autônomo da federação é suficiente.



Etapa 5. Em seguida, você é pedido para selecionar um certificado que os usos do server. Isto se o automóvel povoar enquanto o server tem um certificado já.



Etapa 6. Se você tem um base de dados existente AD FS no server, você precisa de removê-lo para continuar.

Etapa 7. Finalmente, você é em uma tela sumária onde você possa apenas clicar **em seguida**.

Importe os Metadata de Idp a CUCM/transferência os Metadata CUCM

Etapa 1. Transfira os metadata de seu server AD FS navegando à seguinte URL: https://hostname/federationmetadata/2007-06/federationmetadata.xml

Etapa 2. Navegue a **Cisco unificou a administração** > o **sistema** > o **SAML CM único Sinal-em**

Etapa 3. O clique **permite SAML SSO**

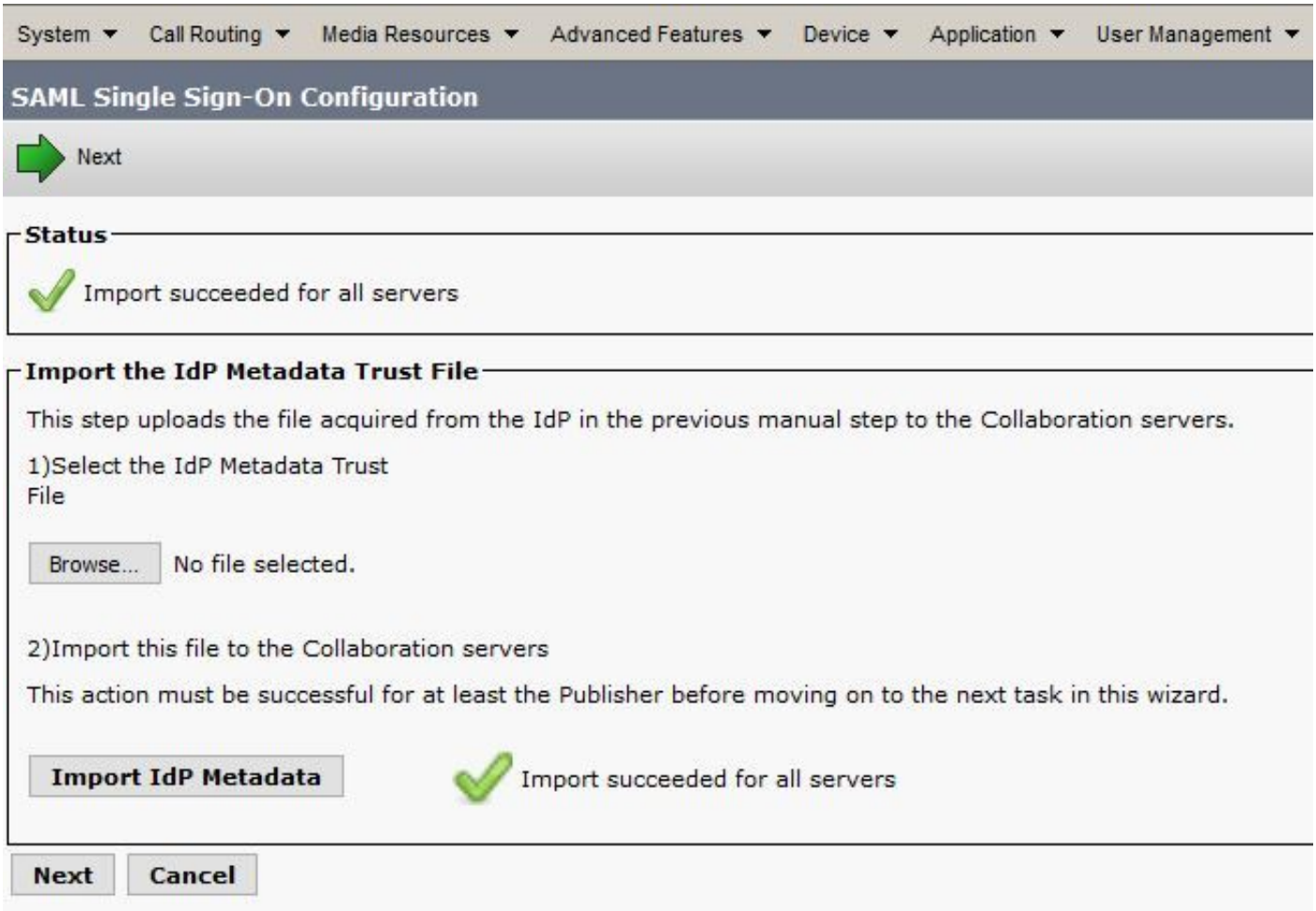
Etapa 4. Você pode receber um aviso sobre as conexões do servidor de Web que precisam de ser restaurado, simplesmente batida **continua**

Etapa 5. Em seguida, CUCM instrui-o transferir o arquivo dos metadata de seu IdP. Nesta encenação, seu server AD FS é o IdP, e nós transferimos os metadata em **etapa 1** acima, assim que o clique **em seguida**.

Etapa 6. Você é pedido para importar o arquivo.

Etapa 7. O clique **consulta** > seleciona o .xml de **etapa 1** > **Metadata de IdP da importação do** clique.

Etapa 8. Você deve receber uma mensagem que a importação era bem sucedida:



Etapa 9. Clique **em seguida**

Etapa 10. Agora que você tem os metadata de IdP importado em CUCM, você precisa de importar os metadata de CUCM em seu IdP.

Etapa 11. **Arquivo dos Metadata da confiança da transferência do** clique

Etapa 12. Clique **em seguida**

Etapa 13. Mova o arquivo do .zip que foi transferido em **etapa 12 a** seu Windows Server e extraia os índices a um dobrador.

Importe CUCM Metatdata ao server AD FS 2.0 e crie regras da reivindicação

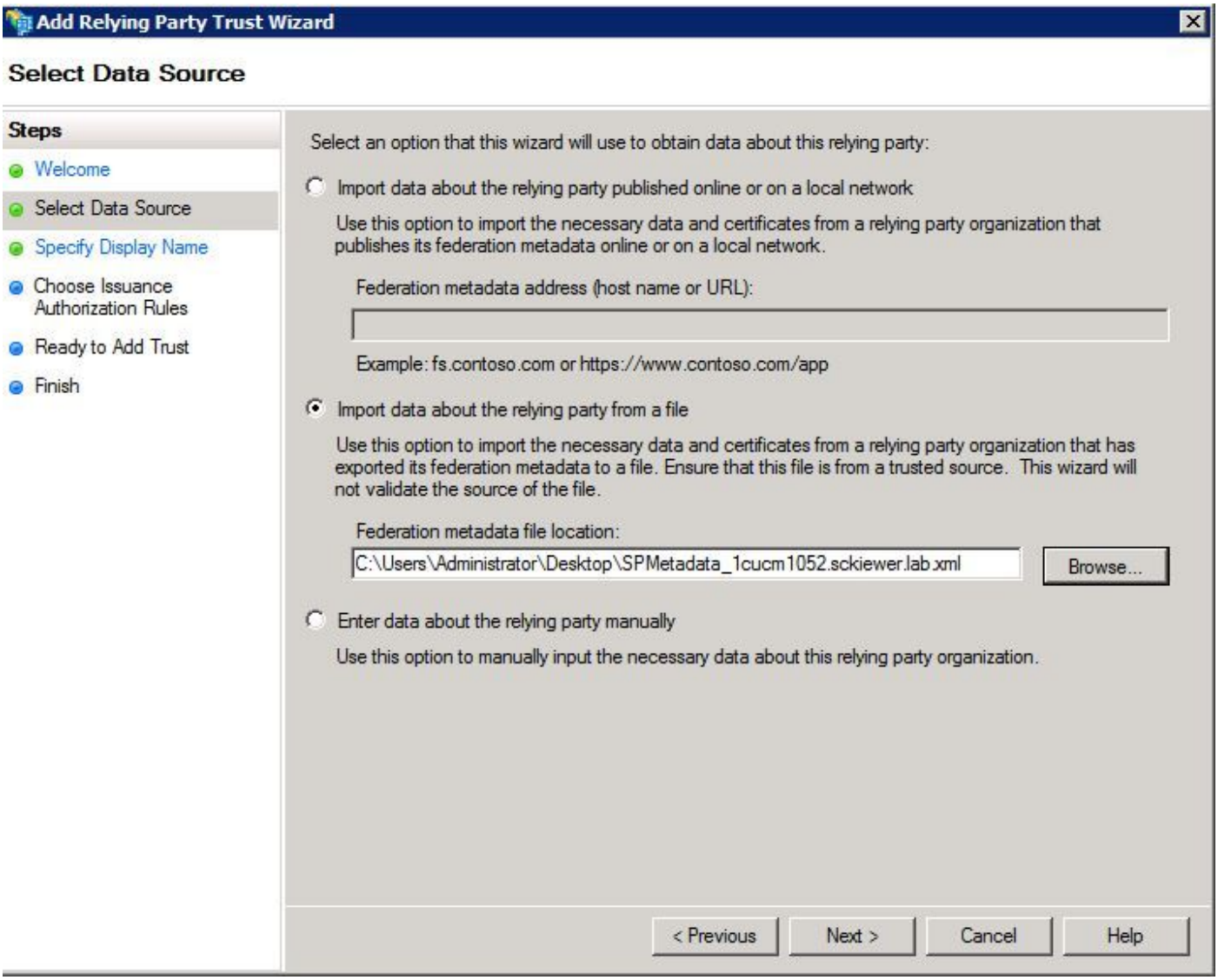
Etapa 1. Neste momento, vá para trás a seu server AD FS e abra a janela de gerenciamento AD FS 2.0 clicando o **começo** e procurando pelo **Gerenciamento AD FS 2.0.**

Etapa 2. Clique **exigido: Adicionar um partido de confiança confiado** (nota: se você não vê este, você pode precisar de fechar o indicador e de abri-lo alternativo. Esta opção não aparecerá se o indicador foi deixado aberto desde que o **assistente do server da federação** terminado).

Etapa 3. Uma vez que você tem o **assistente de confiança da confiança do partido adicionar** aberto, clique o **começo**.

Etapa 4. Aqui, você precisa de importar os arquivos do .xml que você extraiu em **etapa 13**, assim que seleciona **dados da importação sobre o partido de confiança de um arquivo** e consulta ao dobrador que contém os arquivos, seleciona o .xml para seu editor.

Nota: Siga as mesmas etapas acima para todo o Collaboration Server que unificado você quiser usar sobre o SSO.



Etapa 5. Clique **em seguida**

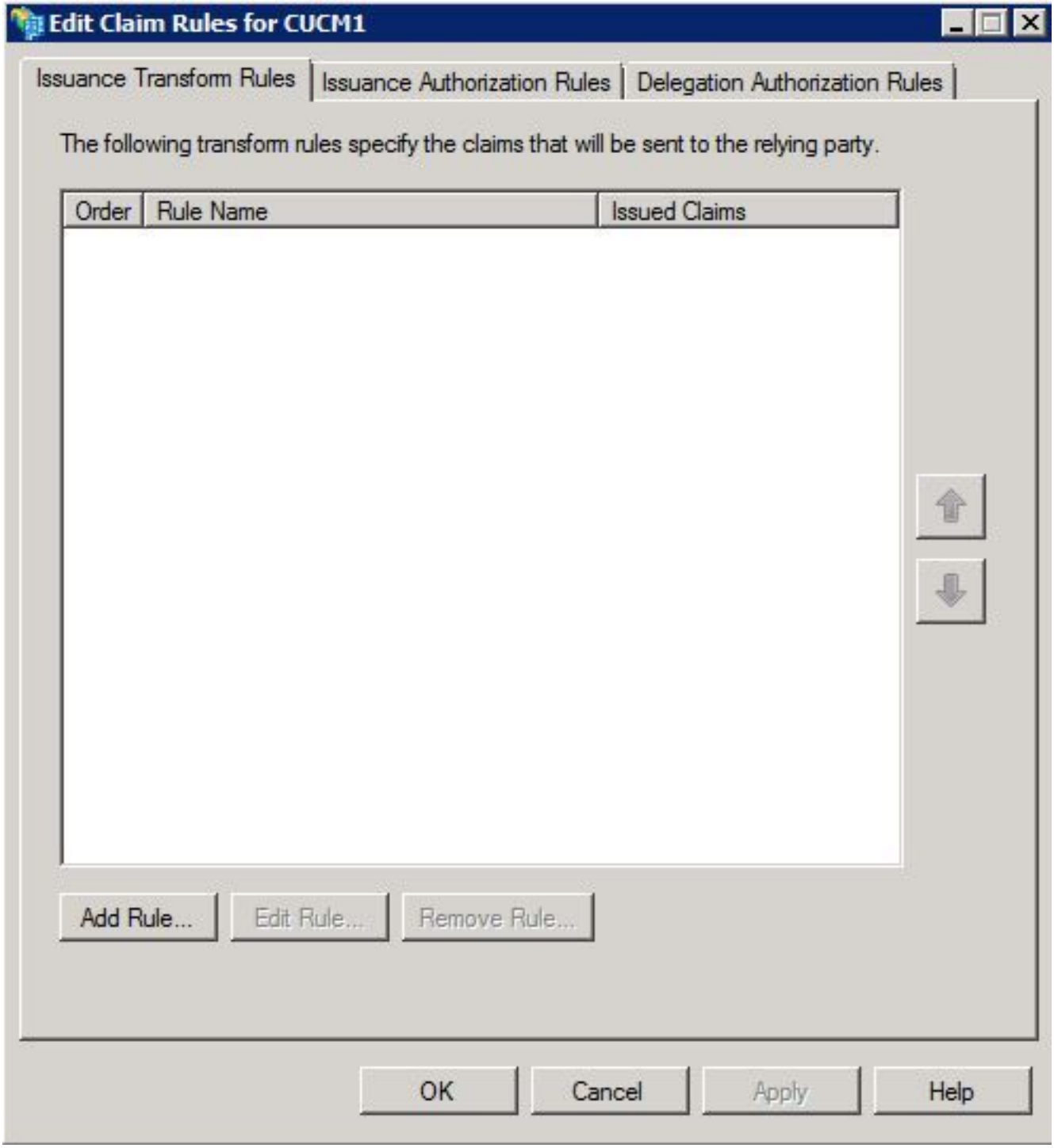
Etapa 6. Edite o **nome do indicador** ao que quer que você gostaria então de clicar **em seguida.**

Etapa 7. Selecione a **licença todos os usuários para alcançar este partido de confiança** e para clicá-lo **em seguida**

Etapa 8. Clique **em seguida** uma vez mais

Etapa 9. Nesta tela, certifique-se de você ter **aberto o diálogo das regras da reivindicação da edição para esta confiança de confiança do partido quando o assistente se fecha** verificado, a seguir clicam **perto**

Etapa 10. Você deve agora ser trazido a um indicador que olhe como este:



Etapa 11. Neste indicador, o clique **adiciona a regra**.

Etapa 12. Para o **molde da regra da reivindicação**, seleto **envie atributos LDAP como reivindicações** e clique-os **em seguida.**

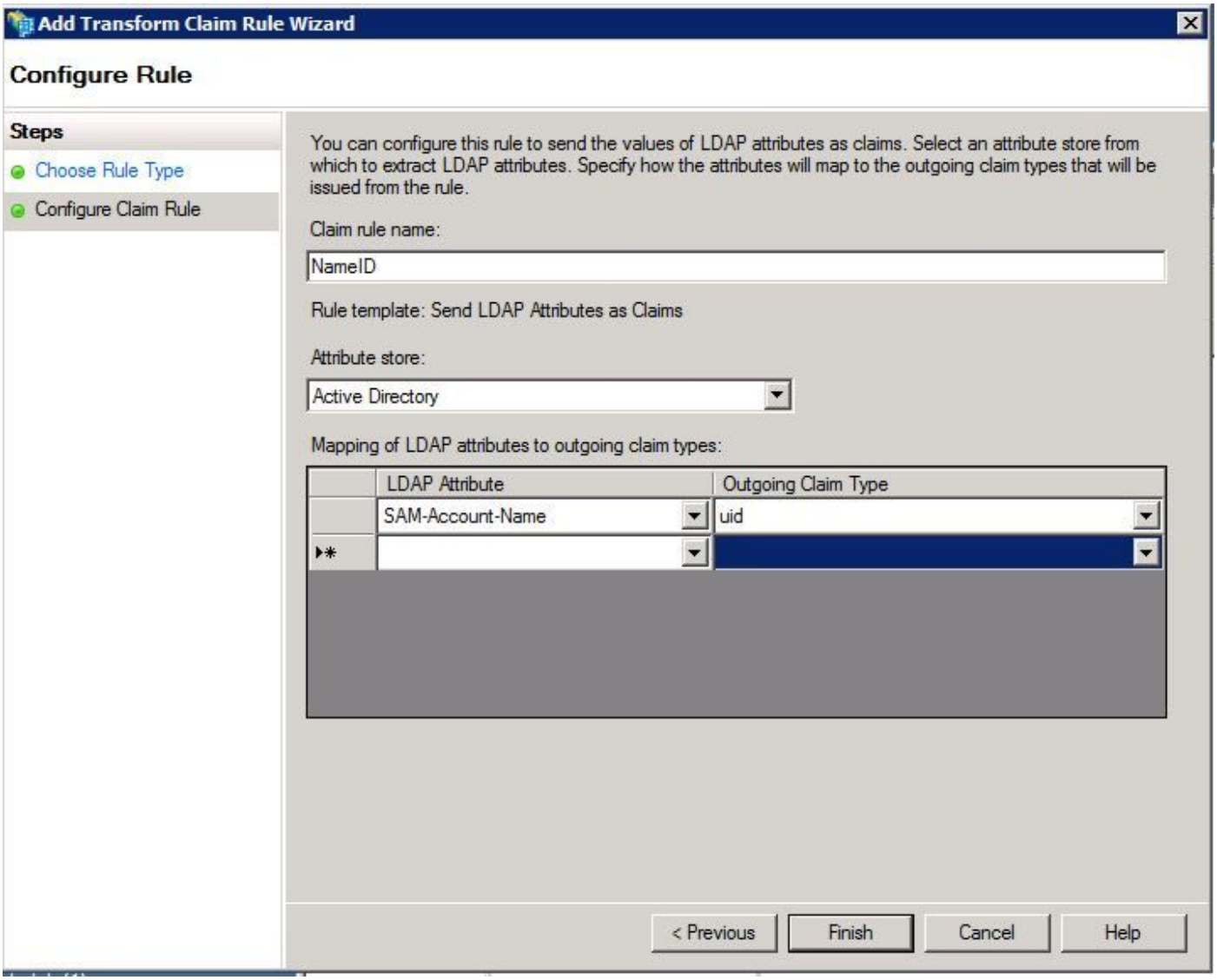
Etapa 13. Na página seguinte, entre em **NameID** para o **nome da regra da reivindicação**

Etapa 14. **Diretório ativo** seleto para a **loja do atributo**

Etapa 15. **SAM-Conta-nome** seleto para o **atributo LDAP**

Etapa 16. Incorpore o **uid** para **tipo que parte da reivindicação**

Nota: **o uid** não é uma opção que autofill ou para aparecer para baixo na lista de gota



Etapa 17. **Revestimento do** clique

Etapa 18. Você deve agora ver sua regra, contudo, nós precisaremos de adicionar uma outra regra assim que o clique **adiciona a regra** outra vez.

Etapa 19. Seleto **envie reivindicações usando uma regulamentação aduaneira**

Etapa 20. Dê entrada com um **nome da regra da reivindicação** (este pode ser qualquer coisa)

Etapa 21. No campo da **regulamentação aduaneira**, cole o seguinte texto:

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

edição do => (tipo = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", expedidor = c.Issuer, OriginalIssuer = c.OriginalIssuer, valor = c.Value, ValueType = c.ValueType, propriedades

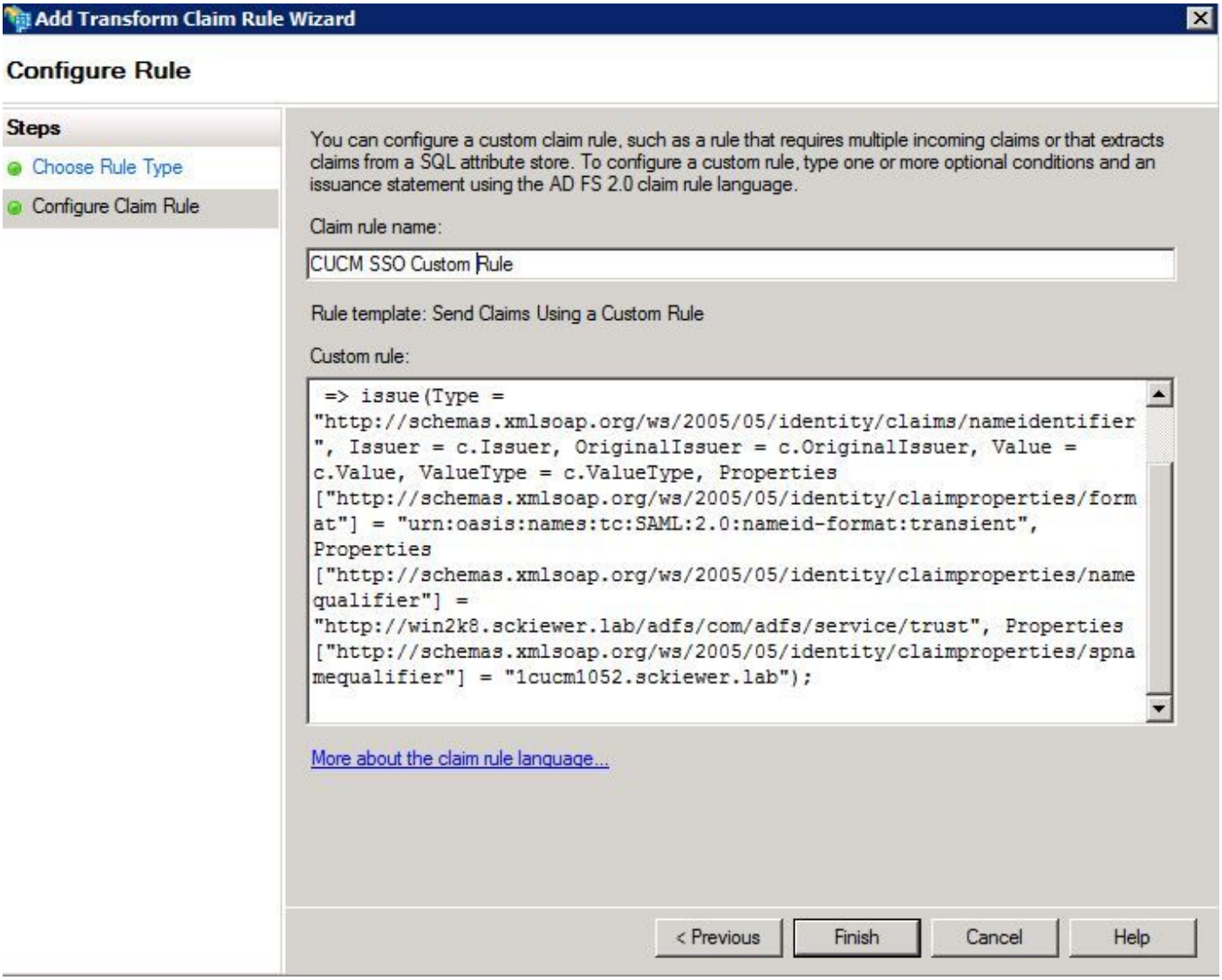
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",

propriedades ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] = "http:// <AD_FS_SERVICE_NAME>

/adfs/com/adfs/service/trust", propriedades ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "<CUCM_FQDN>");

Etapa 22. Certifique-se de você alterar os dois blocos de texto azul com os valores apropriados.

Nota: Se você não é certo sobre o **nome do serviço AD FS**, vá aos comentários deste documento aprender como idendtify o **nome do serviço AD FS.**



Etapa 23. **Revestimento do** clique

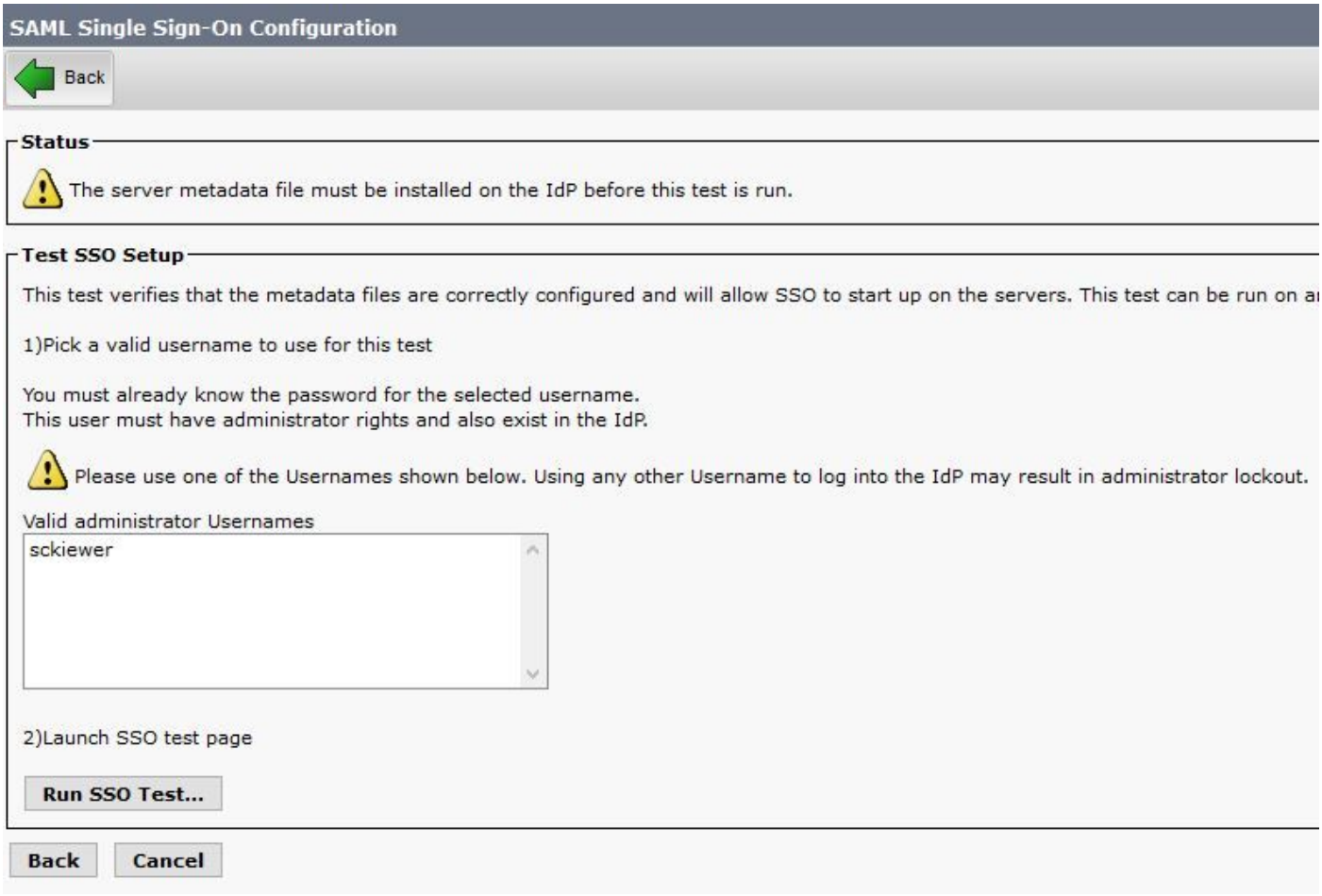
Etapa 24. Clique em OK.

Nota: As regras da reivindicação são precisadas para todo o Collaboration Server que unificado você quiser usar sobre o SSO.

Termine permitir o SSO em CUCM e execute o teste SSO

Etapa 1. Agora que o server AD FS é configurado inteiramente, você pode ir para trás a CUCM.

Etapa 2. Você deve sentar-se em uma página que olhe como esta:



Etapa 3. Vá adiante e selecione seu utilizador final que tem o papel de **superusuários do padrão CCM** selecionado e clique-o **para executar o teste SSO…**

Etapa 4. Uma janela pop-up deve aparecer que possa tomar aproximadamente 30 segundos para carregar, mas eventualmente você deve é presentado com um desafio para entrar.

Etapa 5. Incorpore a senha que você configurou no servidor ldap para o usuário selecionado e você deve então ver:

Etapa 6. **O fim do** clique na janela pop-up e **termina** então.

O SSO é configurado agora em seu laboratório.

Troubleshooting

Ajuste logs SSO para debugar

Para ajustar o SSO os logs para debugar-lo têm que executar este comando no CLI do CUCM:
ajuste o nível do samltrace debugam

Os logs SSO podem ser transferidos de RTMT. O nome do grupo do log é **Cisco SSO**.

Encontrando o nome do serviço da federação

Você pode confirmar o nome do serviço da federação clicando o **começo** e procurando por e abrindo o **Gerenciamento AD FS 2.0**.

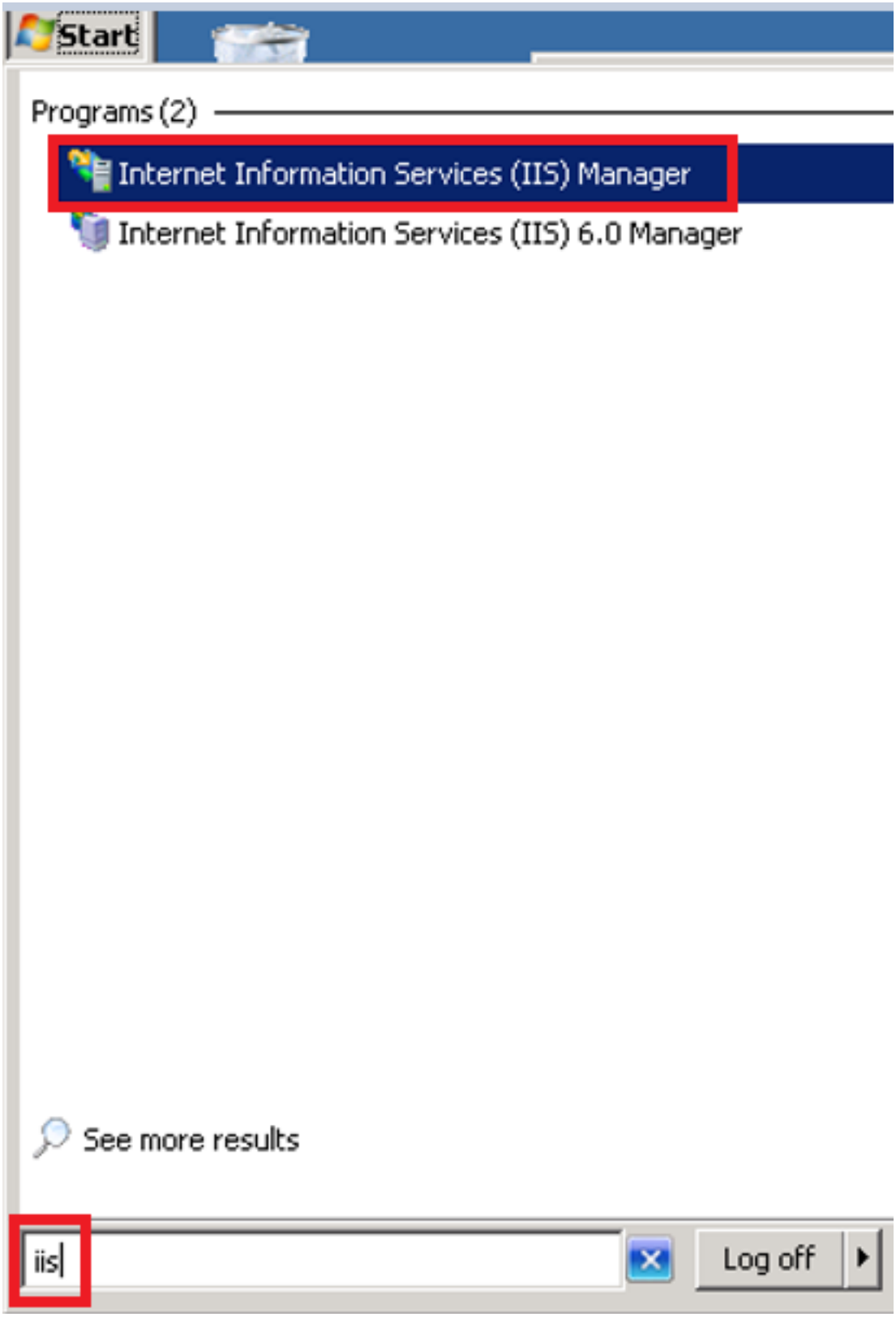
• Clique editam sobre **propriedades do serviço da federação…**
• Quando no tab geral procure o **nome do serviço da federação**

Certificado Dotless quando Specifing o nome do serviço da federação

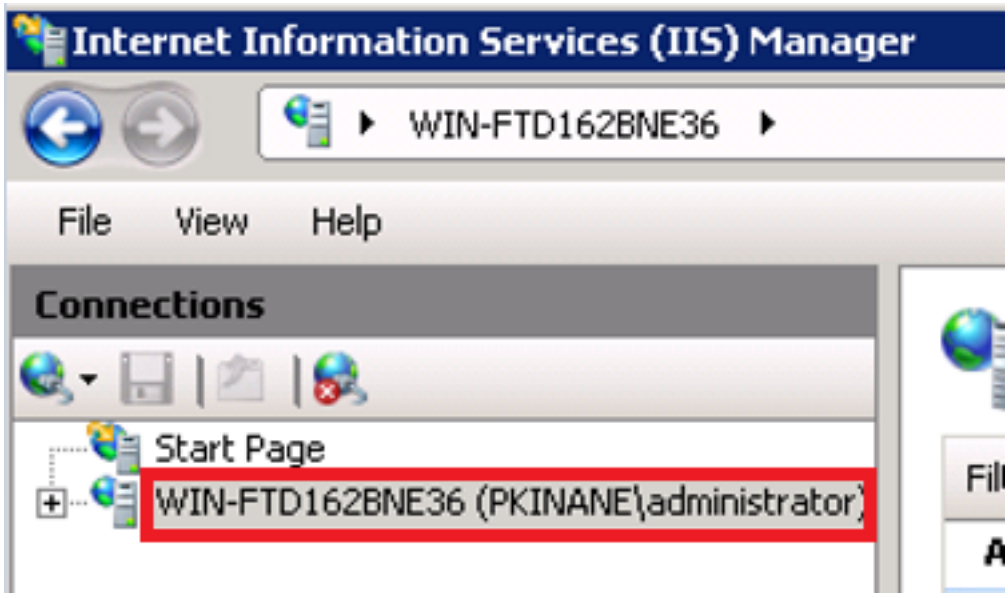
Se você recebe o seguinte Mensagem de Erro ao dirigir o wizard de configuração AD FS, você precisará de criar um certificado novo.

“O certificado selecionado não pode ser usado para determinar o nome do serviço da federação porque o certificado selecionado tem um nome do sujeito (curto-Nomeado) dotless (por exemplo, fabrikam). Selecione um outro certificado sem um nome do sujeito (curto-Nomeado) dotless (por exemplo, fs.fabrikam.com), e tente-o então outra vez.”

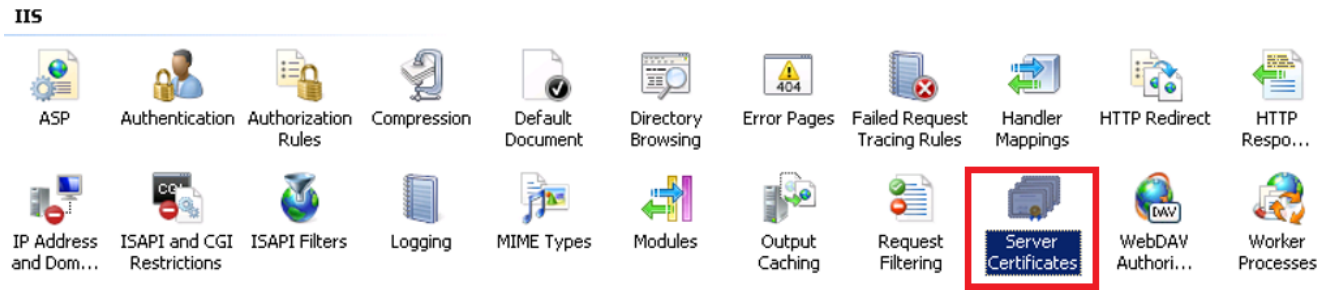
Clique o começo e a busca para iis a seguir abre o gerente do Internet Information Services (IIS)



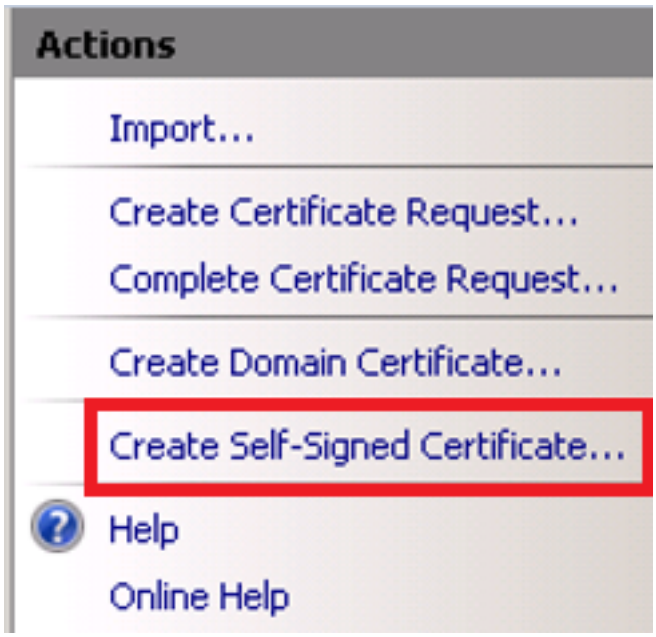
Clique sobre seu nome de server



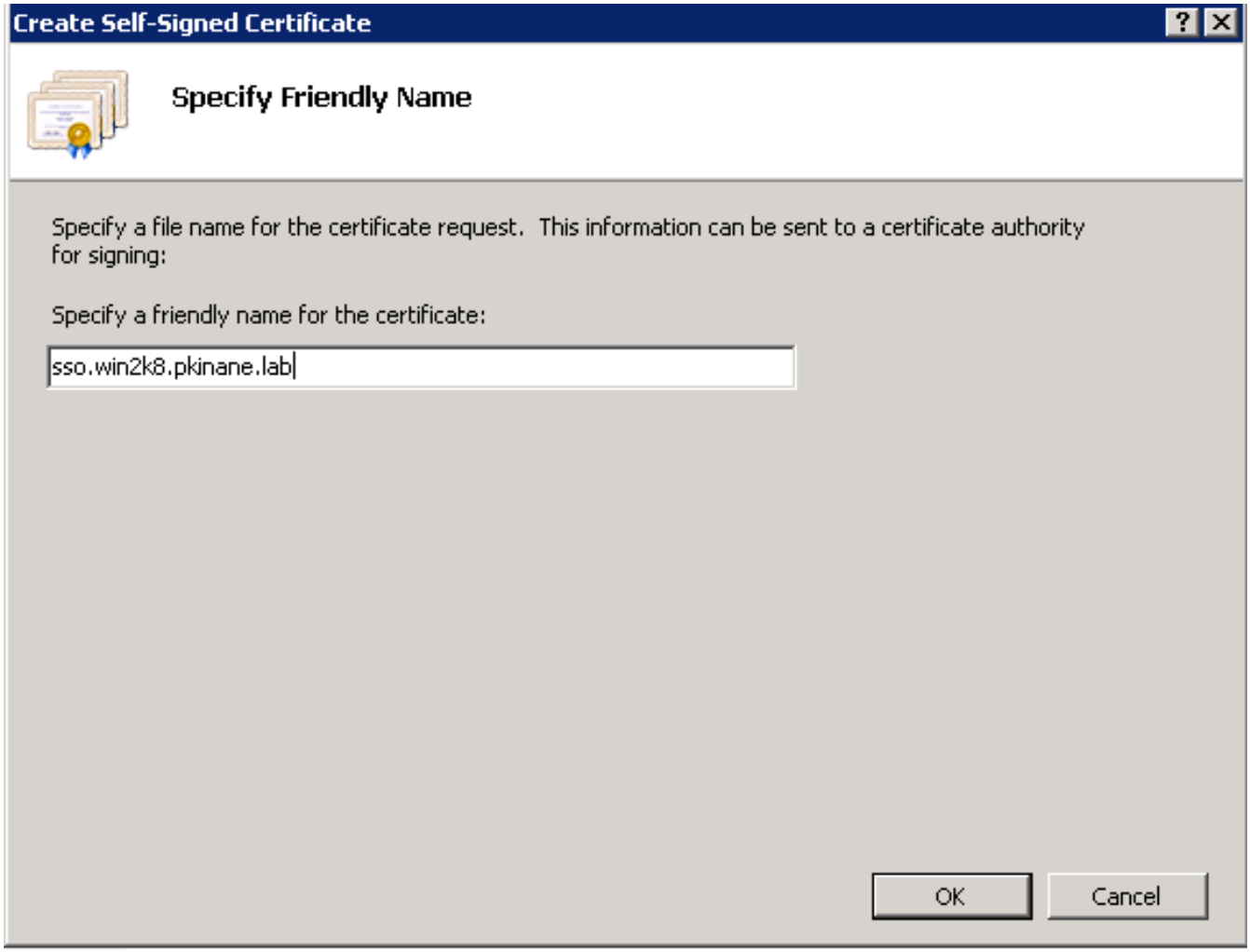
Clique sobre certificados de servidor



Clique criam sobre o certificado auto-assinado



Dê entrada com o nome que você quer para o pseudônimo de seu certificado



O tempo é fora da sincronização entre os server CUCM e IDP

Se você está recebendo o erro alistado abaixo ao tentar executar o teste SSO de CUCM, você pode precisar de configurar Windows Server para usar os mesmos servidores de NTP que o CUCM. O processo para fazer isto é coberto nos comentários de.

"Resposta inválida de SAML. Isto pode ser causado quando o tempo é fora da sincronização entre o gerente das comunicações unificadas de Cisco e server IDP. Verifique por favor a configuração de NTP em ambos os server. Execute dos "o estado NTP utils" do CLI para verificar este estado no gerente das comunicações unificadas de Cisco."

Uma vez que Windows Server tem os servidores de NTP especificaram-no devem obter os metadata do Idp outra vez e transferi-los arquivos pela rede ao CUCM. Então vá diretamente ao teste SSO e veja se você ainda obtém o mesmo erro.