

Configurar SAML SSO no Cisco Unified Communications Manager com ADFS 3.0

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Pré-verificação da configuração](#)

[A Records](#)

[Registros de Ponteiro \(PTR\)](#)

[É necessário que os registros SRV estejam em vigor para o Jabber Discovery Services](#)

[Configuração inicial do ADFS3](#)

[Configurar SSO no CUCM com ADFS](#)

[Configuração LDAP](#)

[Metadados do CUCM](#)

[Configurar entidade confiadora do ADFS](#)

[Metadados IDP](#)

[Configurar SSO no CUC](#)

[Metadados CUC](#)

[Configurar SSO no Expressway](#)

[Importar metadados para o Expressway C](#)

[Exportar Metadados Do Expressway C](#)

[Adicione uma confiança de terceira parte confiável para o Cisco Expressway-E](#)

[OAuth com login de atualização](#)

[Caminho de autenticação](#)

[Arquitetura SSO](#)

[Fluxo de login no local](#)

[Fluxo de login de MRA](#)

[OAuth](#)

[Token de acesso/atualização](#)

[O fluxo de concessão do código de autorização OAuth é melhor](#)

[Configurar Kerberos](#)

[Selecionar autenticação do Windows](#)

[O ADFS suporta o Kerberos NTLM](#)

[Configurar o Microsoft Internet Explorer](#)

[Adicione o URL do ADFS em Segurança > Zonas de Intranet > Sites](#)

[Adicione nomes de host CUCM, IMP e Unity a Security > Trusted Sites](#)

[Autenticação de usuário](#)

[Login no Jabber em SSO](#)

[Troubleshoot](#)

[Internet Explorer \(IE\)](#)

[Sites Adicionando ao IE](#)

[Problema Fora de Sincronização](#)

[Revogar um Token](#)

[Arquivo de bootstrap](#)

[SSO com falha devido ao MSIS7066](#)

Introduction

Este documento descreve as etapas para configurar o Single Sign-On com o Active Directory 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 Active Directory
 - Serviços de Federação do Active Directory

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.

The screenshot shows the DNS console with the following structure:

- DNS
 - AD
 - Forward Lookup Zones
 - _msdcs.fhlab.com
 - fhlab.com (selected)
 - _msdcs
 - _sites
 - _tcp
 - _udp
 - DomainDnsZones
 - ForestDnsZones
 - Reverse Lookup Zones
 - 228.89.10.in-addr.arp
 - Trust Points
 - Conditional Forwarders
 - Global Logs

Name	Type
_msdcs	
_sites	
_tcp	
_udp	
DomainDnsZones	
ForestDnsZones	
(same as parent folder)	Start of Authority (SOA)
(same as parent folder)	Name Server (NS)
(same as parent folder)	Host (A)
ad	Host (A)
cmpubhcsc	Host (A)
cmsubhcsc	Host (A)
cucpubhcsc	Host (A)
cucsubhcsc	Host (A)
expwyc	Host (A)
expwye	Host (A)
imppubhcsc	Host (A)
imsubhcsc	Host (A)

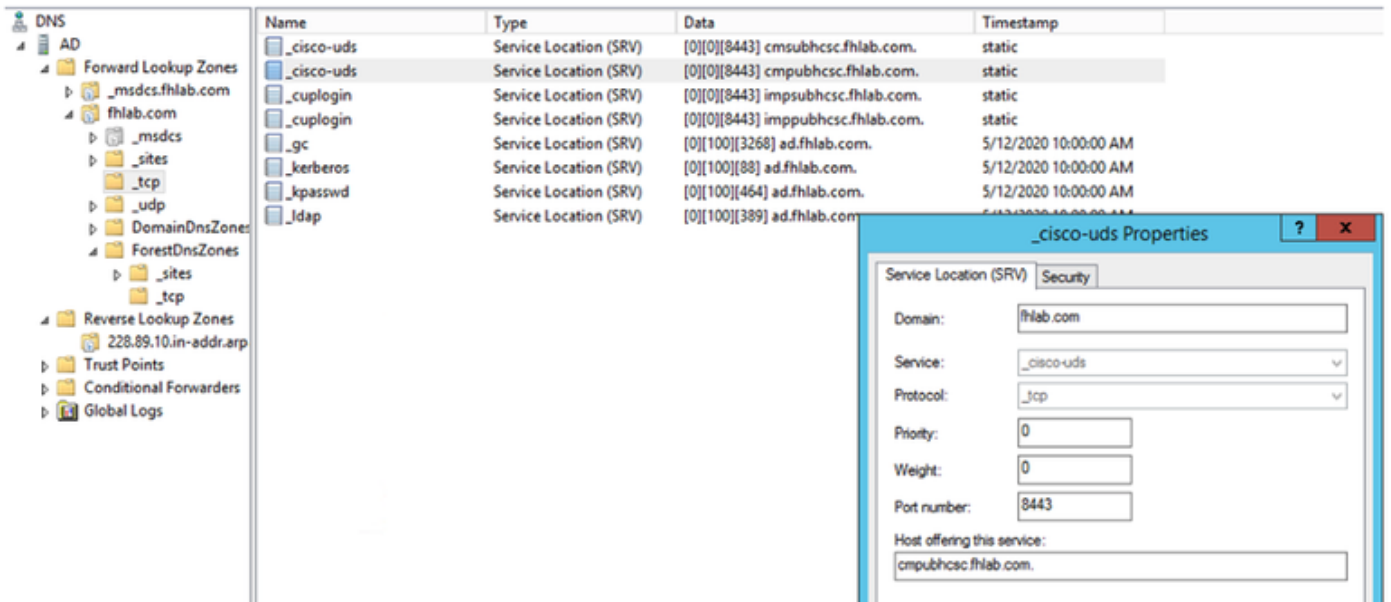
Registros de Ponteiro (PTR)

The screenshot shows the DNS console with the following structure:

- DNS
 - AD
 - Forward Lookup Zones
 - _msdcs.fhlab.com
 - fhlab.com (selected)
 - _msdcs
 - _sites
 - _tcp
 - _udp
 - DomainDnsZones
 - ForestDnsZones
 - _sites
 - _tcp
 - Reverse Lookup Zones
 - 228.89.10.in-addr.arp

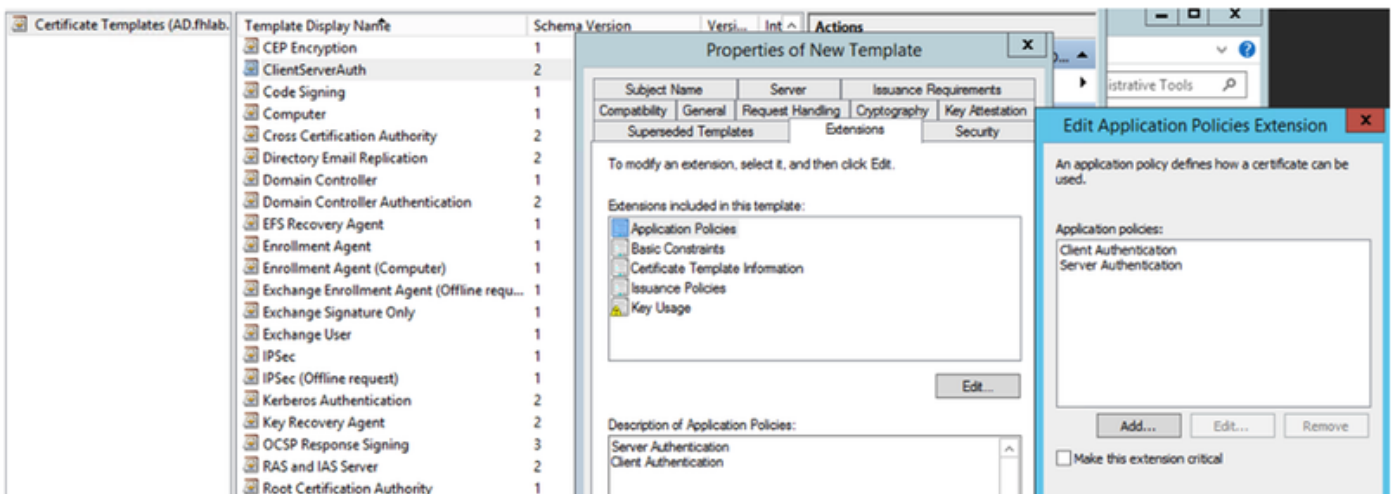
Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[14], ad.fhlab.com., hostmaster.fhlab.co...	static
(same as parent folder)	Name Server (NS)	ad.fhlab.com.	static
10.89.228.144	Pointer (PTR)	expwyc.fhlab.com.	static
10.89.228.145	Pointer (PTR)	expwye.fhlab.com.	static
10.89.228.146	Pointer (PTR)	cmpubhcsc.fhlab.com.	static
10.89.228.147	Pointer (PTR)	cmsubhcsc.fhlab.com.	static
10.89.228.148	Pointer (PTR)	imppubhcsc.fhlab.com.	static
10.89.228.150	Pointer (PTR)	imsubhcsc.fhlab.com.	static
10.89.228.151	Pointer (PTR)	cucpubhcsc.fhlab.com.	static
10.89.228.153	Pointer (PTR)	cucsubhcsc.fhlab.com.	static
10.89.228.154	Pointer (PTR)	win10.fhlab.com.	5/12/2020 10:00:00 AM
10.89.228.226	Pointer (PTR)	ad.fhlab.com.	5/12/2020 11:00:00 AM
10.89.228.227	Pointer (PTR)	win10ext.fhlab.com.	5/7/2020 4:00:00 PM

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

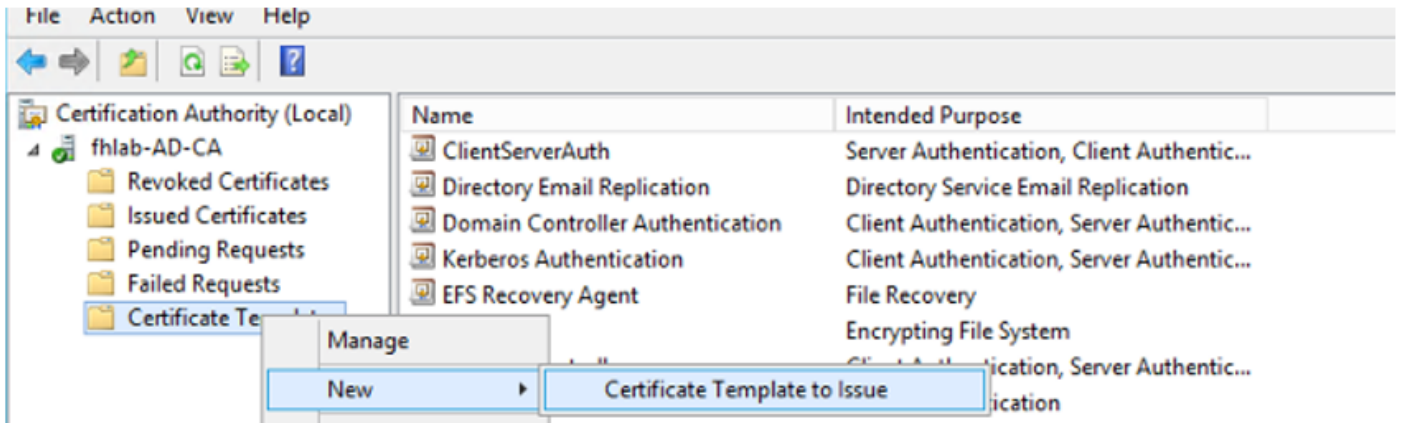


- CA raiz (supondo que os certificados sejam assinados pela AC empresarial)

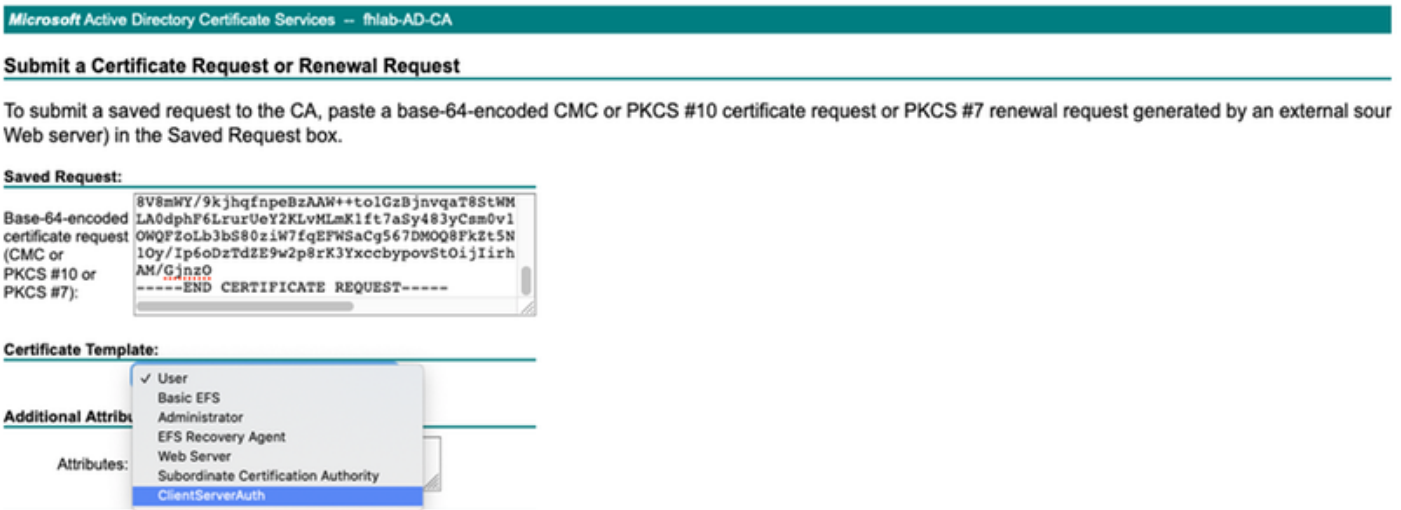
Um Modelo de Certificado precisa ser criado com base no Modelo de Certificado do Servidor Web, o primeiro é duplicado, renomeado e, na guia Extensões, as Políticas de Aplicativo são modificadas adicionando uma Política de Aplicativo de Autenticação de Cliente. Este modelo é necessário para assinar todos 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.

Generate Certificate Signing Request

Generate Close

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose** tomcat

Distribution* Multi-server(SAN)

Common Name* cmpubhcsc-ms.fhlab.com

Subject Alternate Names (SANs)

Auto-populated Domains

cmpubhcsc.fhlab.com
cmsubhcsc.fhlab.com
imppubhcsc.fhlab.com
impsubhcsc.fhlab.com

Parent Domain fhlab.com

Other Domains

Browse... No file selected.
Please import .TXT file only.
For more information please refer to the notes in the Help Section

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

Generate Close

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

Cisco Unified Operating System Administration

Navigation Cisco Unified OS Administration Go
osadmin Search Documentation About Logout

Show Settings Security Software Upgrades Services Help

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

7 records found

Certificate List (1 - 7 of 7) Rows per Page 50

Find Certificate List where Certificate begins with tomcat Find Clear Filter

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat	cmpubhcsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/18/2022	Certificate Signed by fhlab-AD-CA
tomcat-ECDSA	cmpubhcsc-EC.fhlab.com	Self-signed	EC	cmpubhcsc.fhlab.com	cmpubhcsc-EC.fhlab.com	04/02/2025	Self-signed certificate generated by system
tomcat-trust	imppubhcsc-EC.fhlab.com	Self-signed	EC	imppubhcsc.fhlab.com	imppubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
tomcat-trust	cmsubhcsc-EC.fhlab.com	Self-signed	EC	cmsubhcsc.fhlab.com	cmsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
tomcat-trust	impsubhcsc-EC.fhlab.com	Self-signed	EC	impsubhcsc.fhlab.com	impsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
tomcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

Certificate List (1 - 6 of 6) Rows per Page 50

Find Certificate List where Certificate begins with tomcat Find Clear Filter

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat	cmpubhcsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/28/2022	Certificate Signed by fhlab-AD-CA
tomcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate
tomcat-trust	imppubhcsc-EC.fhlab.com	Self-signed	EC	imppubhcsc.fhlab.com	imppubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
tomcat-trust	cmsubhcsc-EC.fhlab.com	Self-signed	EC	cmsubhcsc.fhlab.com	cmsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
tomcat-trust	impsubhcsc-EC.fhlab.com	Self-signed	EC	impsubhcsc.fhlab.com	impsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

- IIS

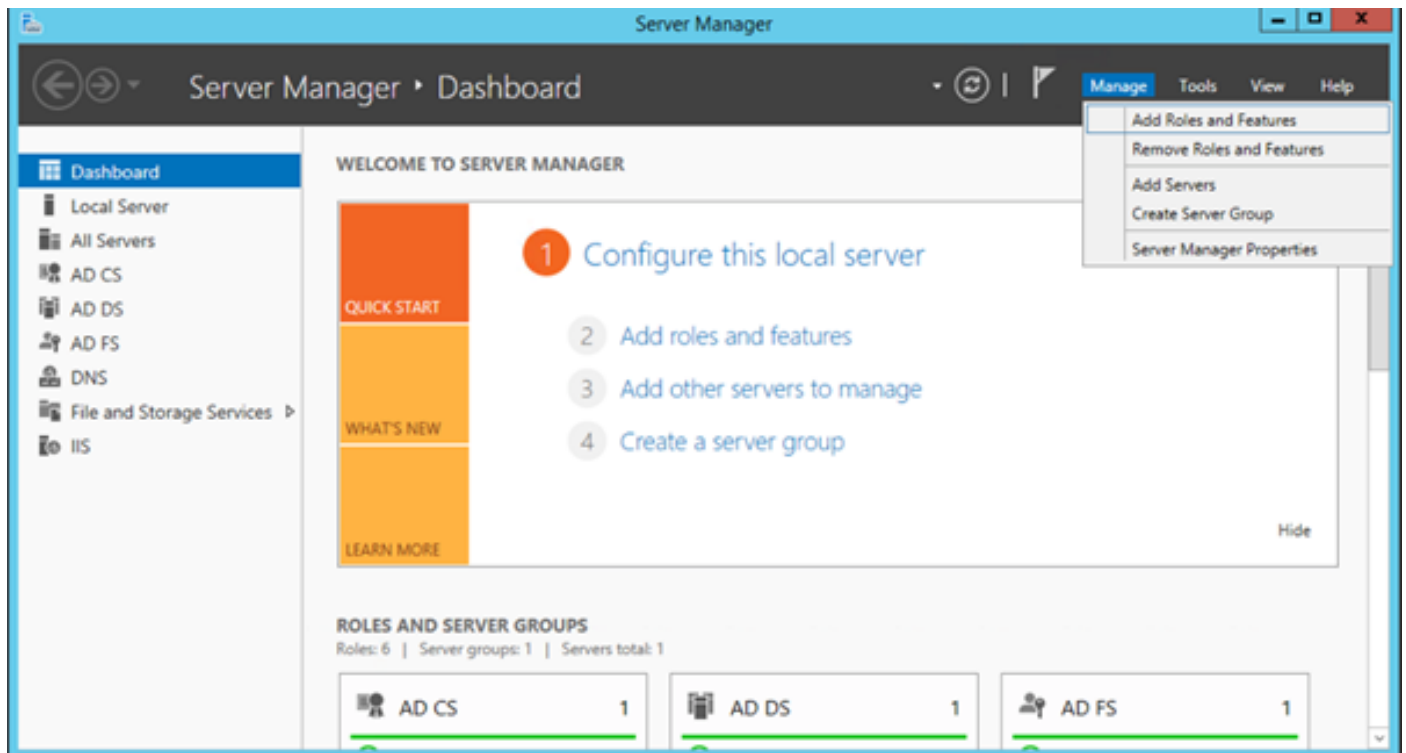
Caso contrário, esta seção passará pela instalação dessas funções. Caso contrário, ignore esta

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

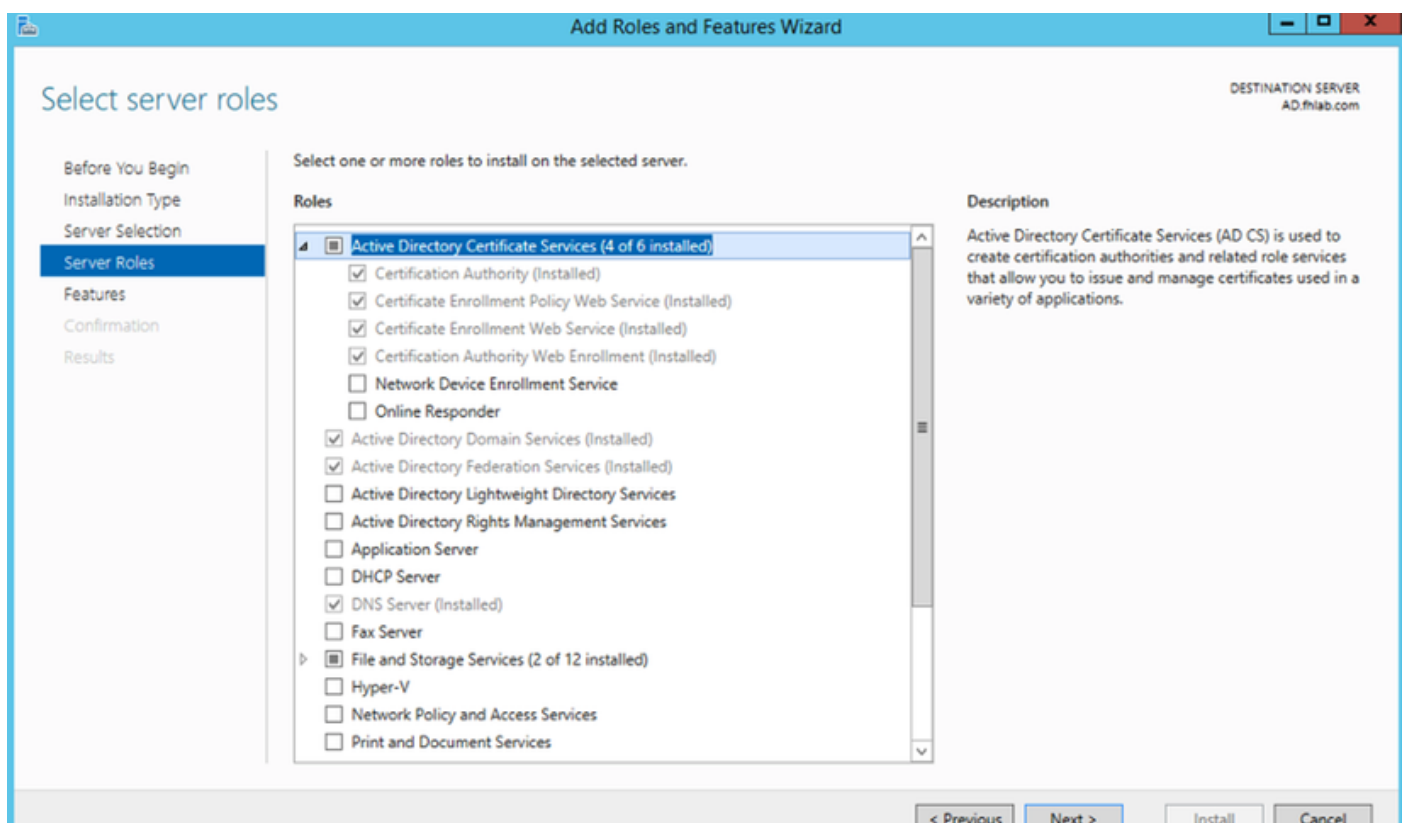
Depois de instalar o Windows 2012 R2 com DNS, promova o servidor para um controlador de domínio.

A próxima tarefa será instalar o Microsoft Certificate Services.

Navegue até Gerenciador de servidores e adicione uma nova função:



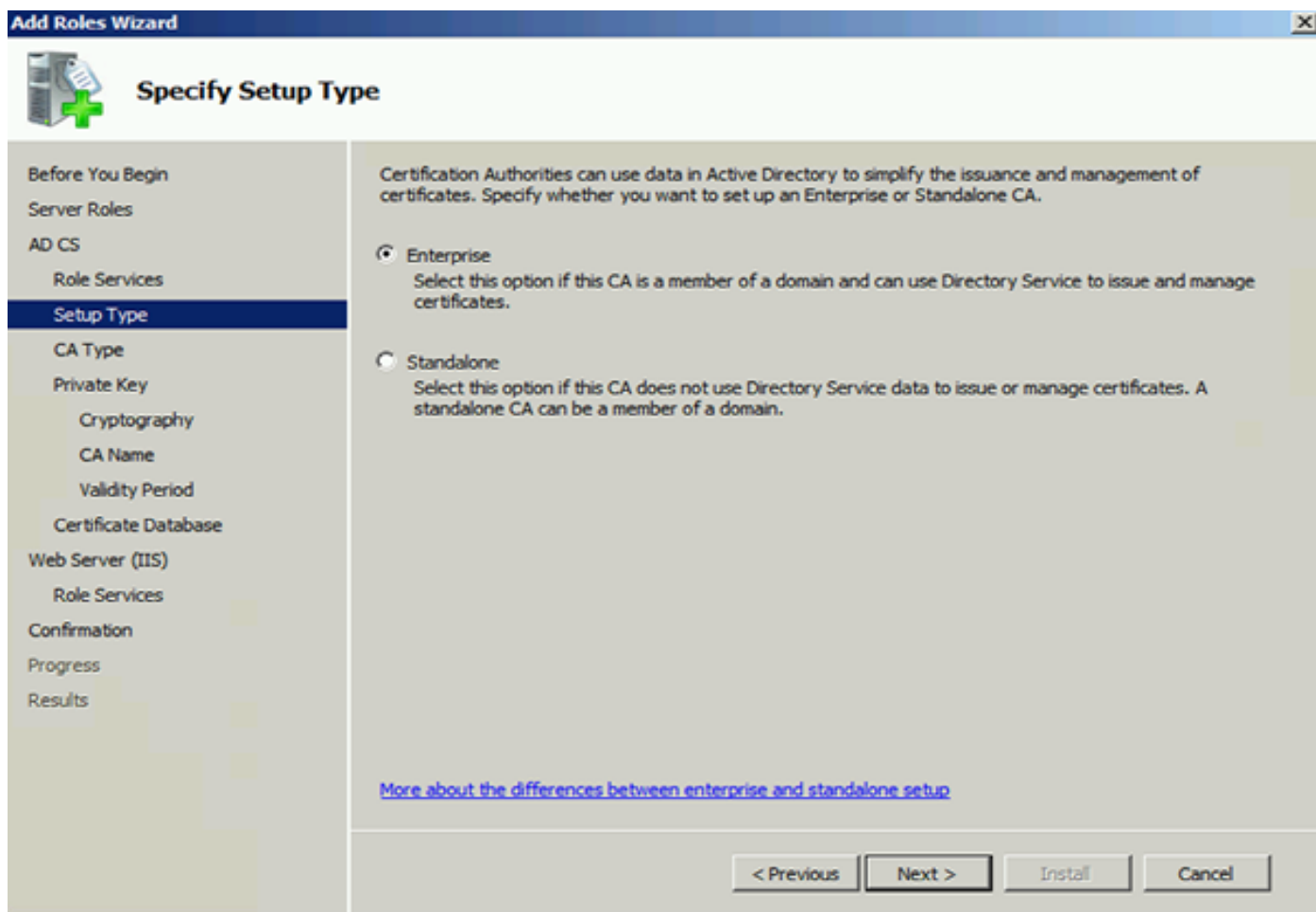
Selecione a função **Serviços de Certificados do Active Directory**.



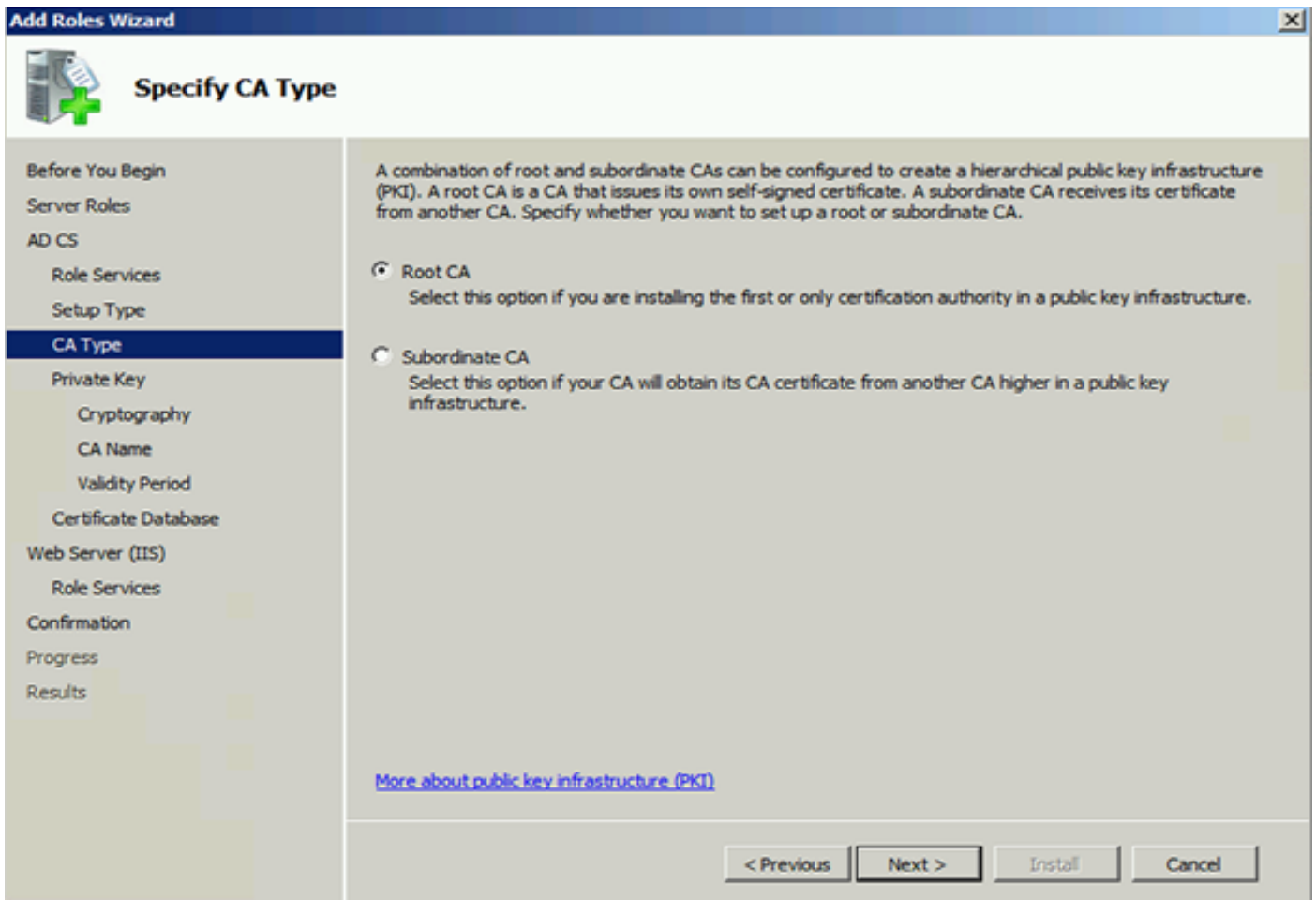
E implante esses serviços - Serviço Web de Política de Registro de Certificado da Autoridade de Certificação primeiro. Depois que essas duas funções forem instaladas, configure-as e instale o **Serviço Web de Inscrição de Certificados e Inscrição na Web de Autoridade de Certificação**. Configure-os.

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

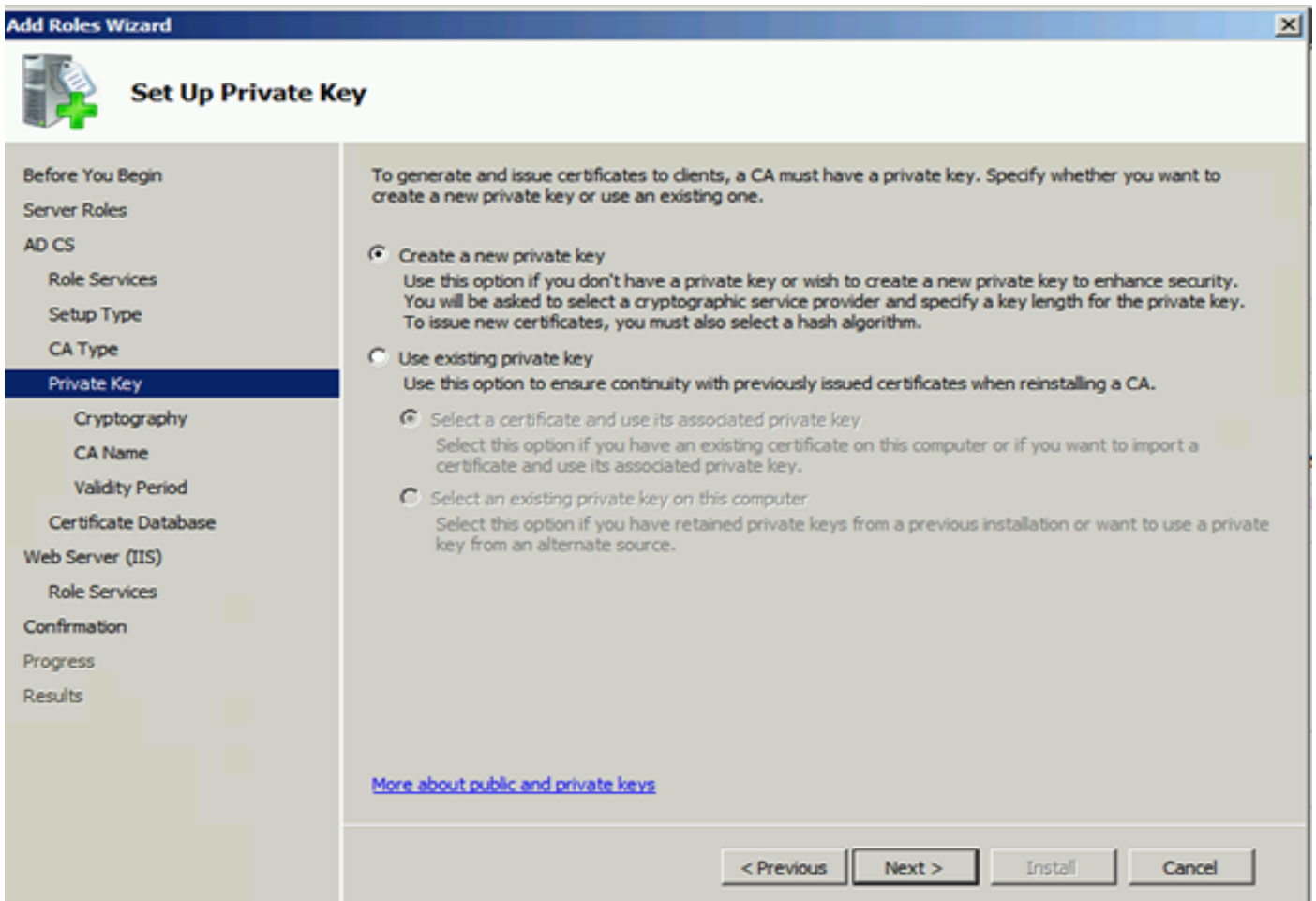
Dependendo da sua implantação, você pode selecionar Empresa ou Independente.



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**.

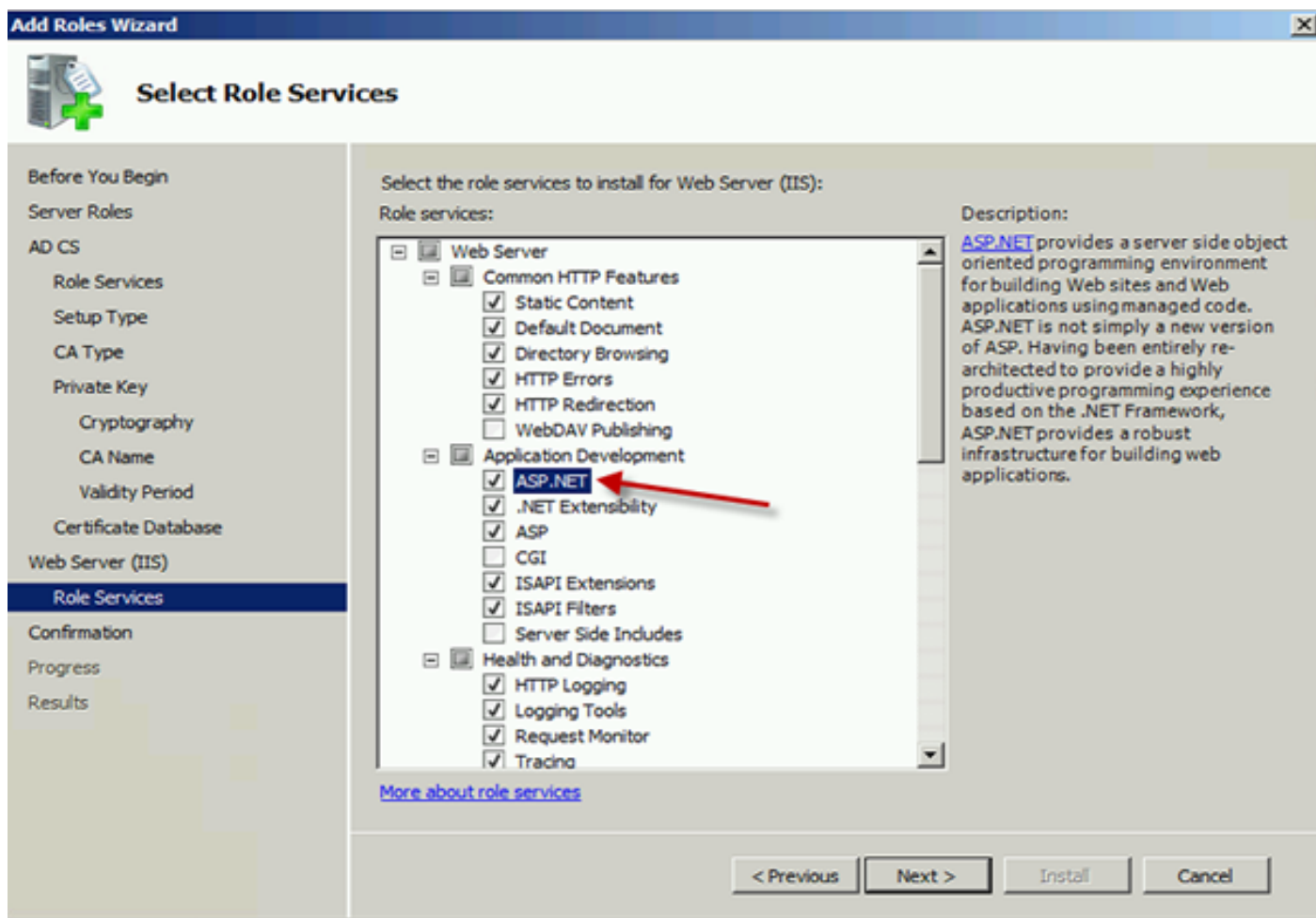


A próxima etapa é criar uma chave privada para sua CA.

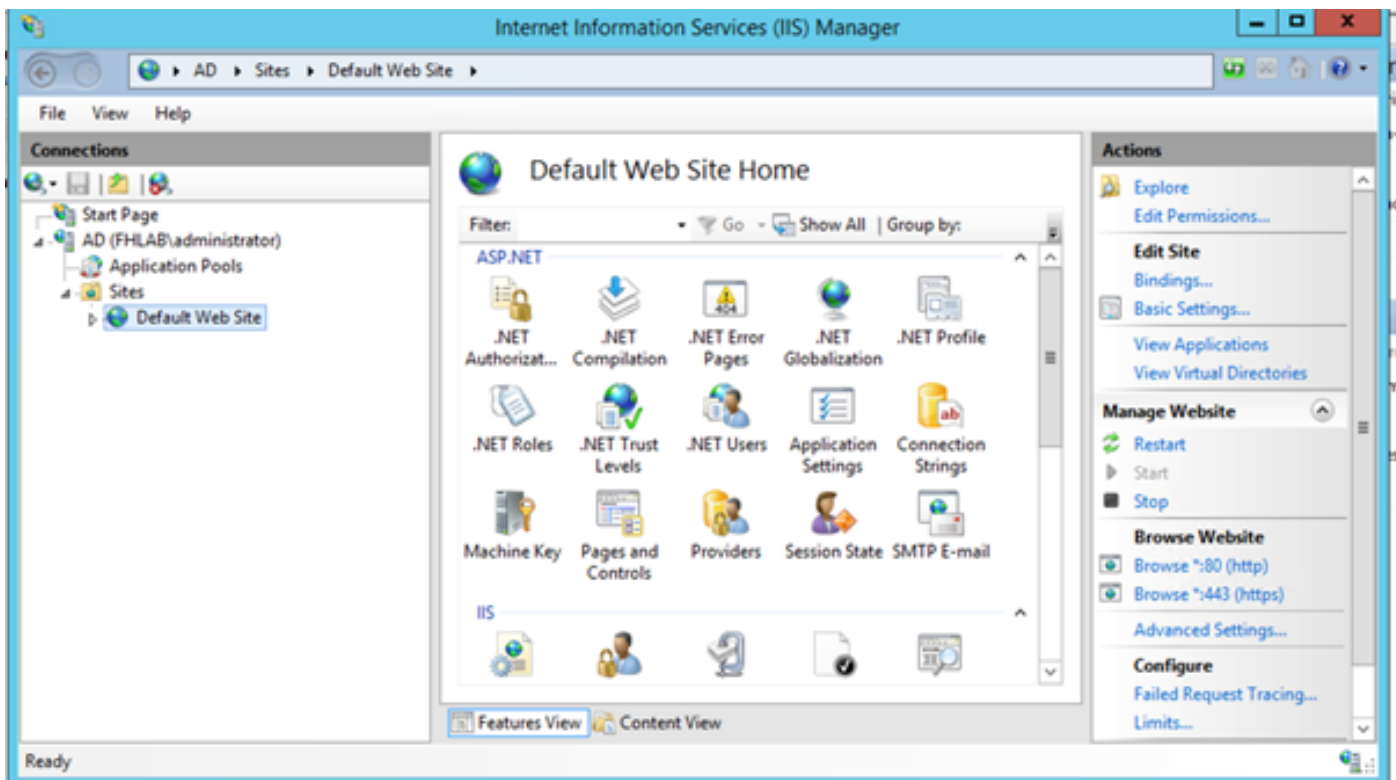


Esta etapa só é necessária se você instalar o ADFS3 em um Windows Server 2012 separado.

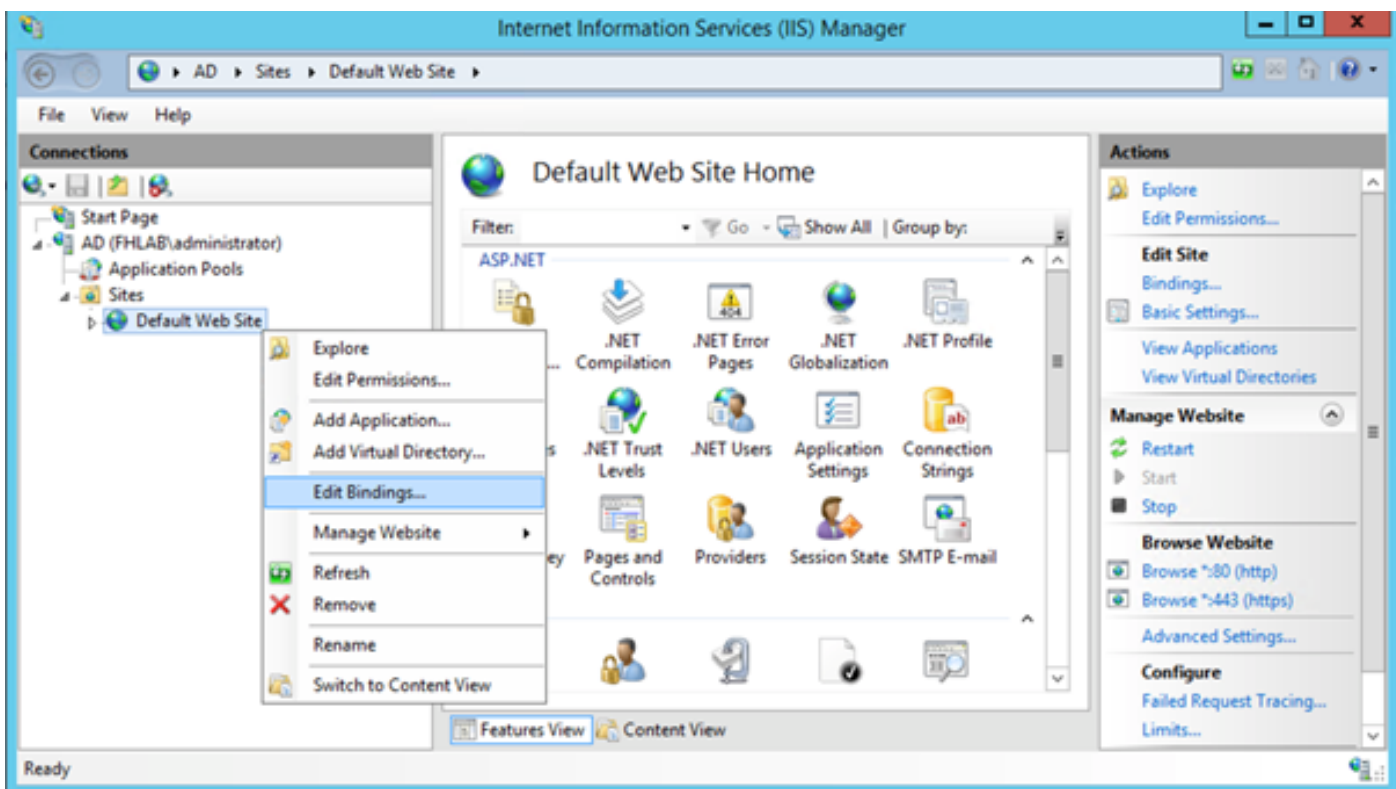
Depois de configurar a AC, os serviços de função do IIS precisam ser configurados. Isso é necessário para a inscrição na Web na CA. Para a maioria das implantações de ADFS, é necessária uma função extra no IIS, clique em **ASP.NET** em Desenvolvimento de Aplicativos.



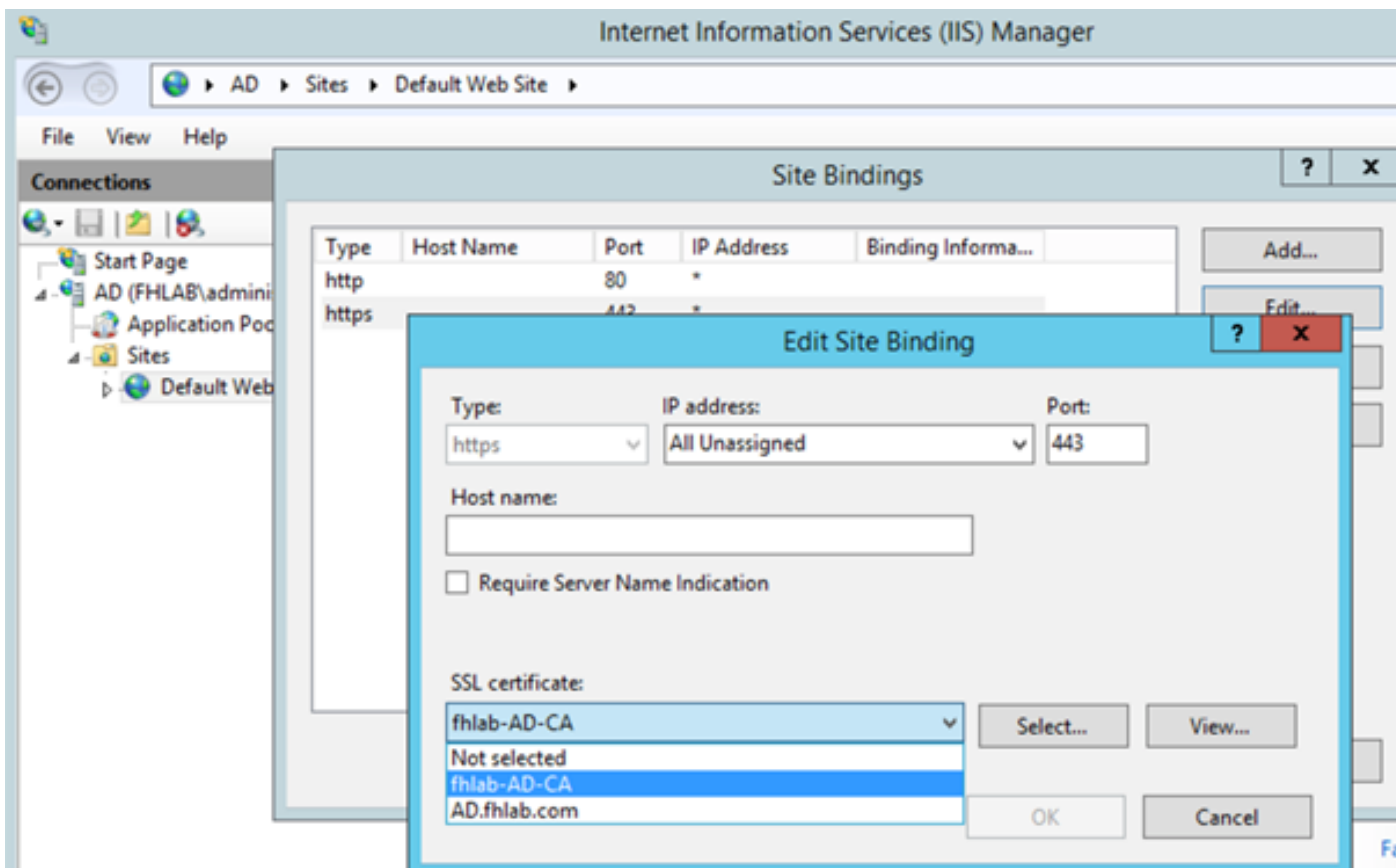
No Server Manager, clique em **Web Server > IIS** e, em seguida, clique com o botão direito do mouse em **Default Web Site**. A associação precisa ser alterada para permitir também HTTPS além do HTTP. Isso é feito para suportar HTTPS.



Selecione **Editar vínculos**.

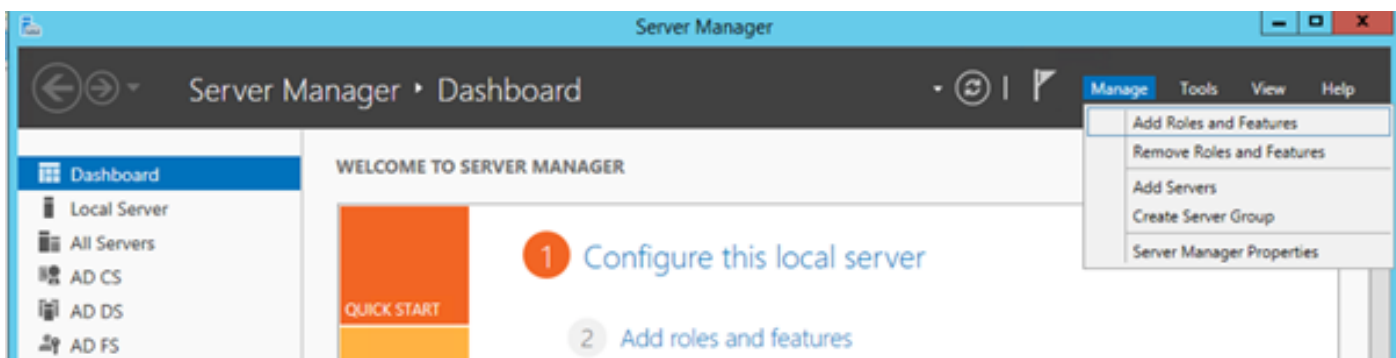


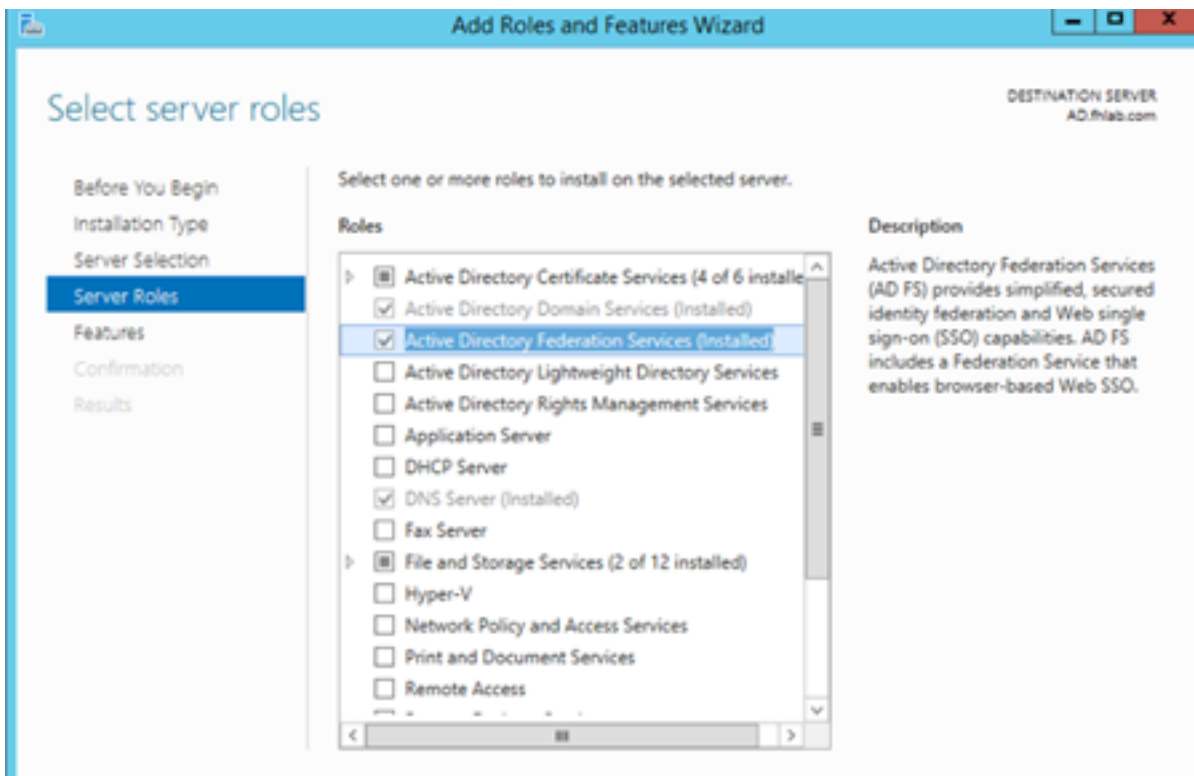
Adicione uma nova associação de site e selecione **HTTPS** como o tipo. Para o certificado SSL, escolha o certificado do servidor que deve ter o mesmo FQDN do seu servidor AD.



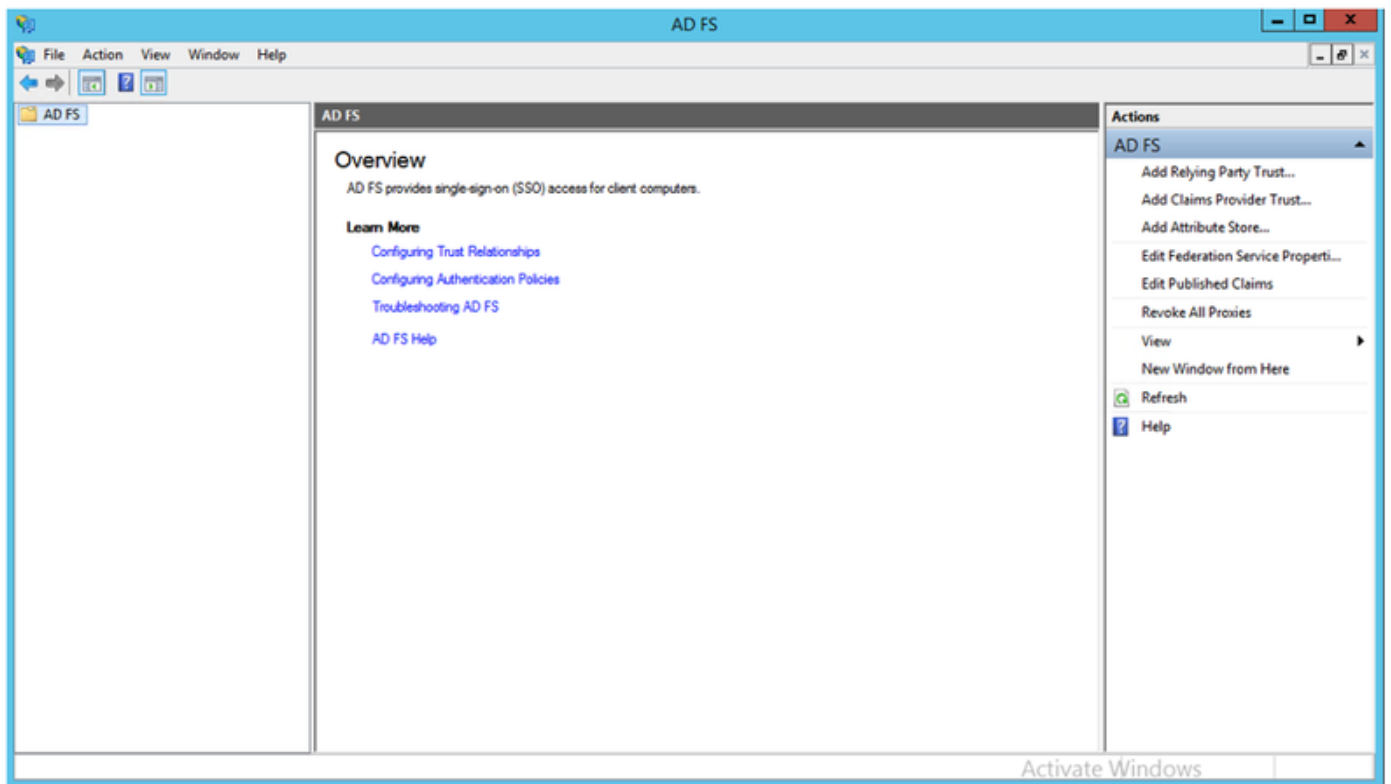
Todas as funções de pré-requisito estão instaladas no ambiente, por isso agora pode continuar com a instalação dos Serviços de Federação do Ative Directory do ADFS3 (no Windows Server 2012).

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





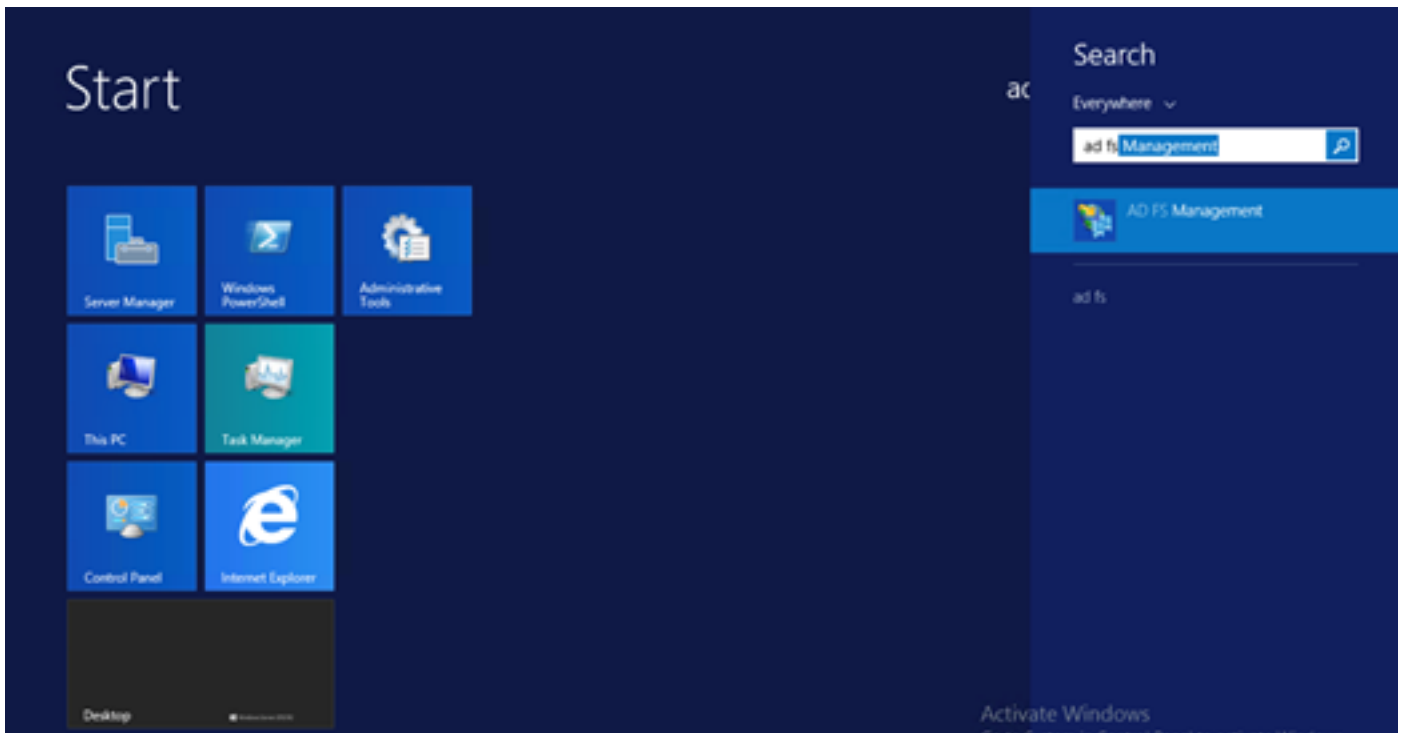
Quando a instalação for concluída, você poderá abri-la na barra de tarefas ou no menu Iniciar.



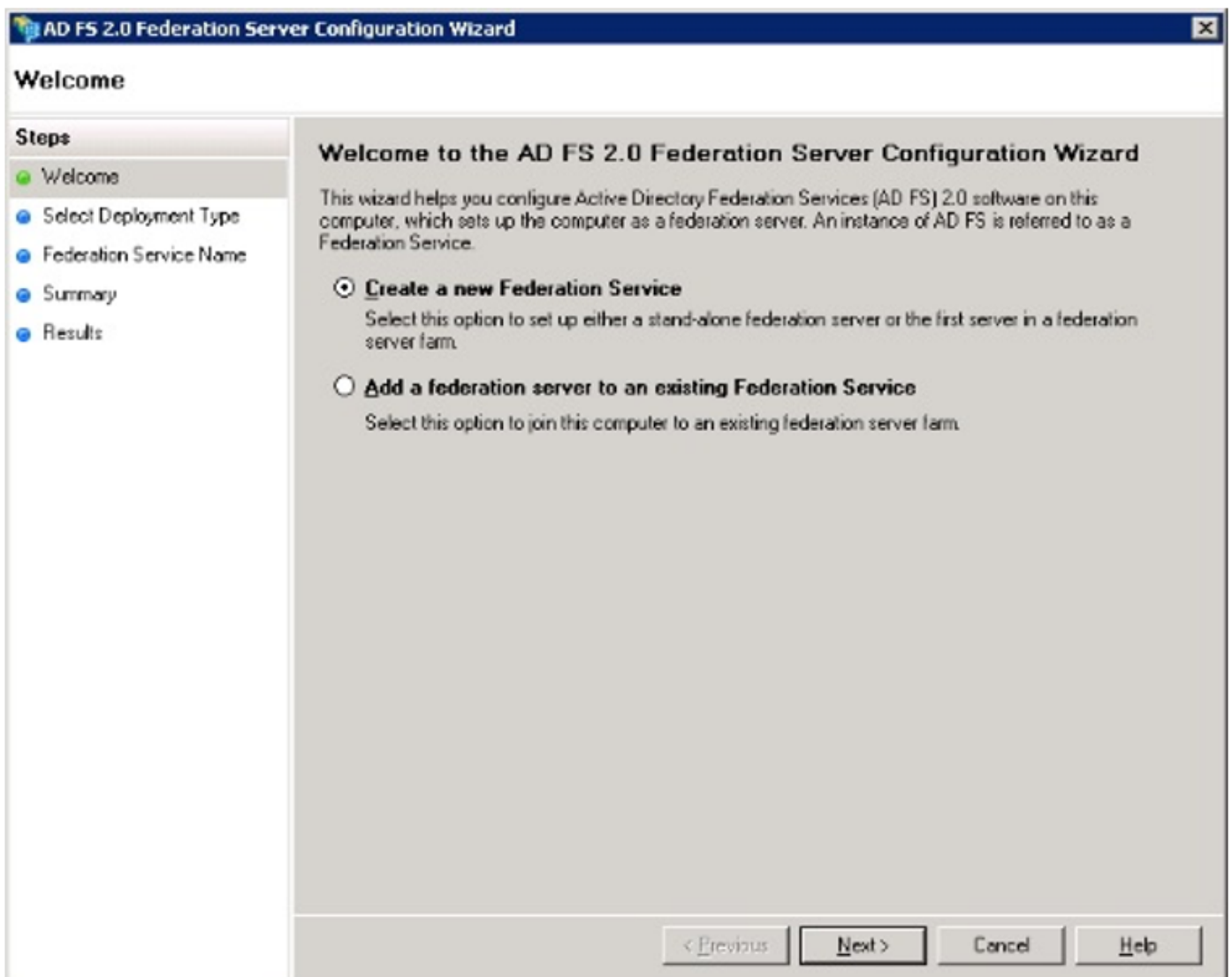
Configuração inicial do ADFS3

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

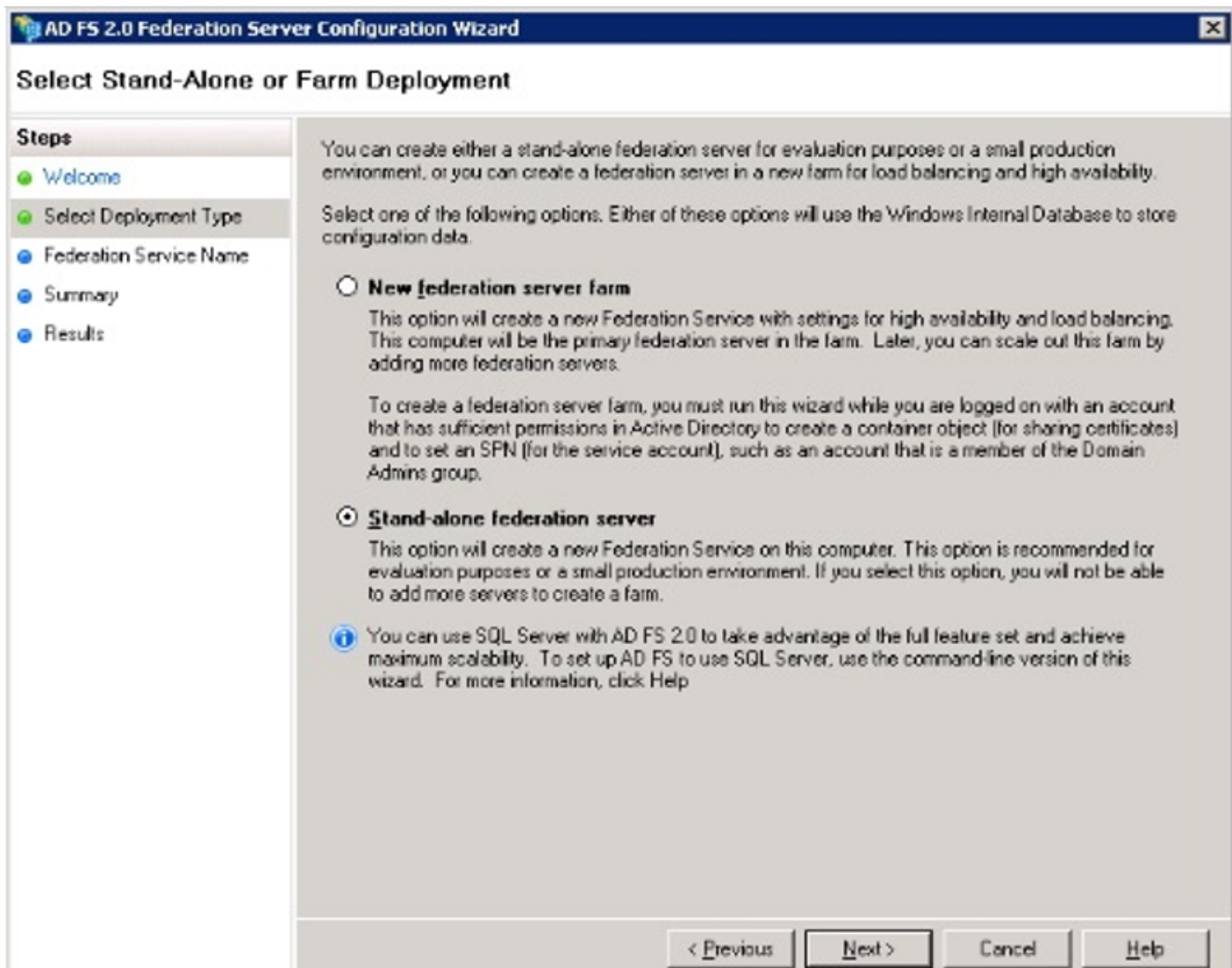
Selecione **Windows** e digite **Gerenciamento do AD FS** para iniciar o console de Gerenciamento do ADFS como mostrado na imagem.



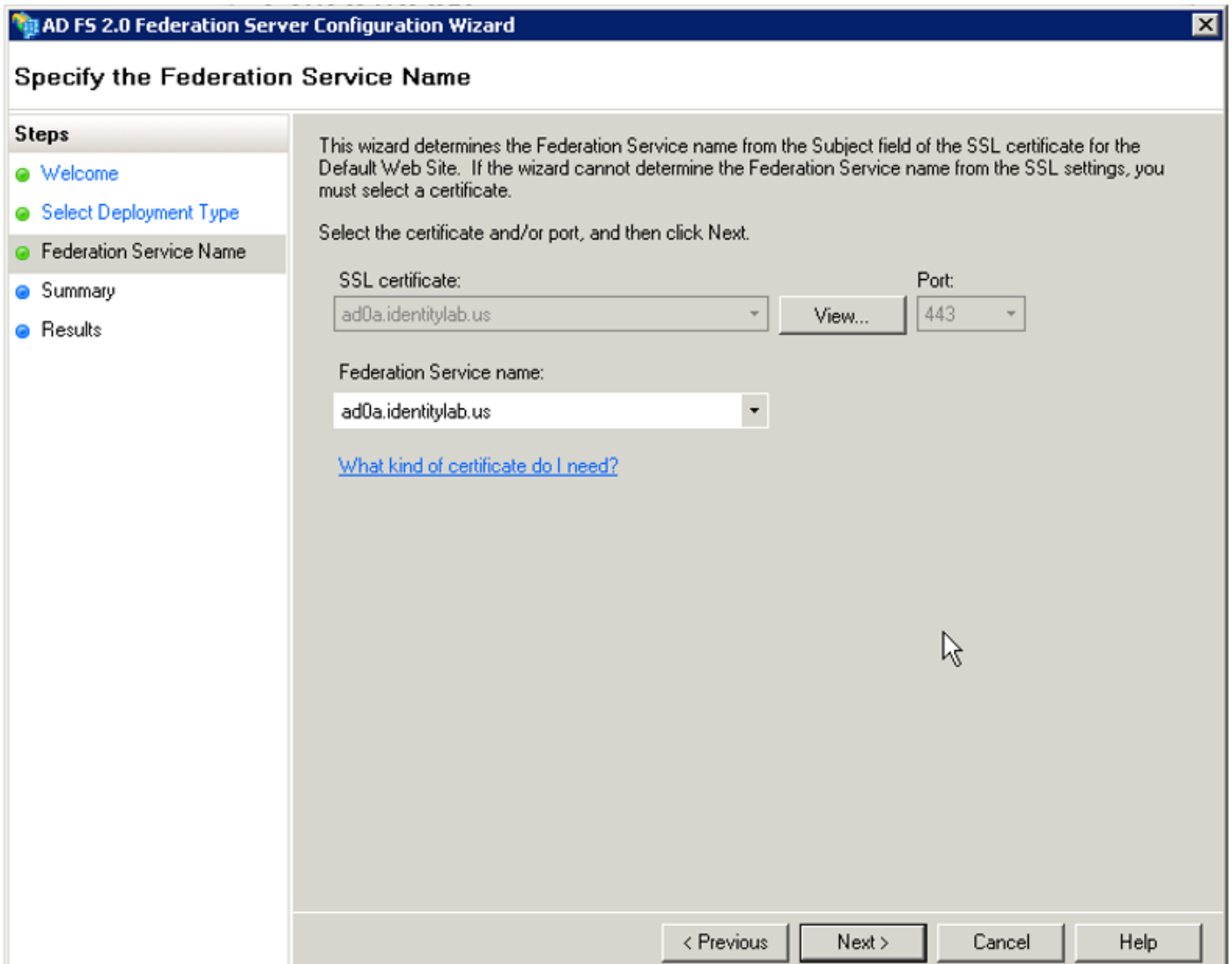
Selecione a opção **Assistente de Configuração do Servidor de Federação do AD FS 3.0** para iniciar a configuração do servidor ADFS. Essas capturas de tela representam as mesmas etapas no AD FS 3.



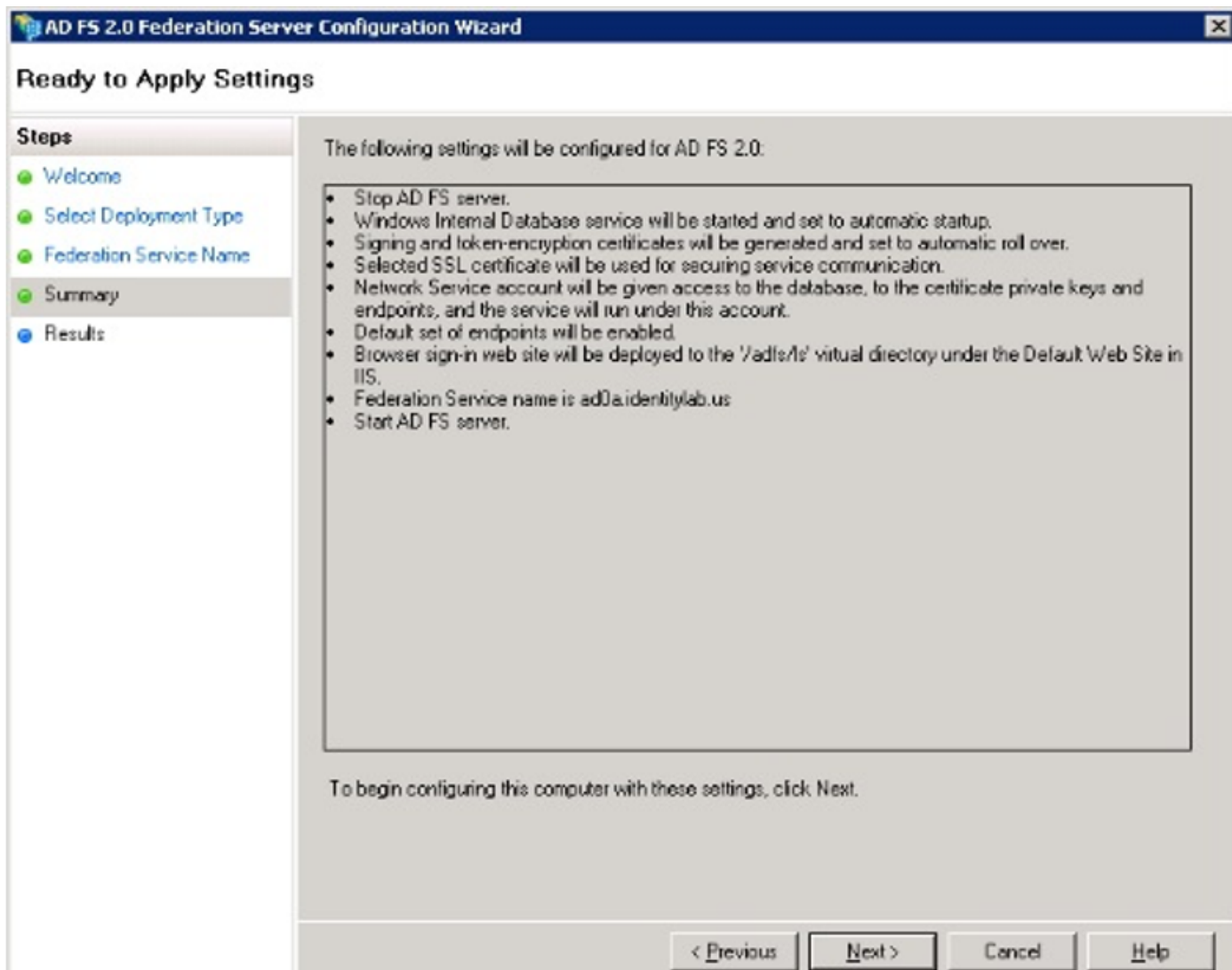
Selecione Criar um novo **Serviço de Federação** e clique em **Avançar**.



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.

AD FS 2.0 Federation Server Configuration Wizard

Configuration Results

Steps

- Welcome
- Select Deployment Type
- Federation Service Name
- Summary
- Results**

The following settings are being configured

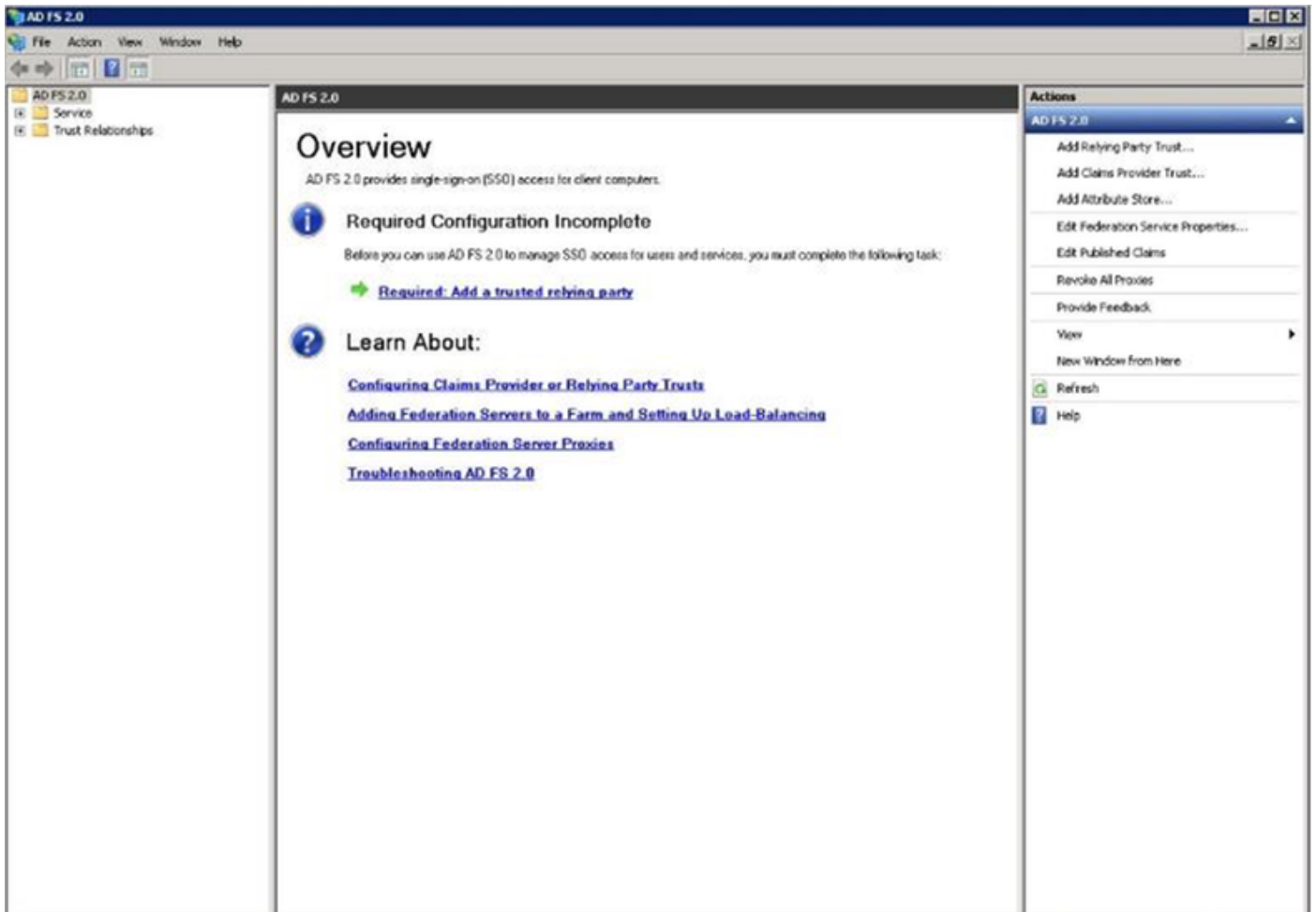
Component	Status
Stop the AD FS 2.0 Windows Service	Configuration finished
Install Windows Internal Database	Configuration finished
Start the Windows Internal Database service	Configuration finished
Create AD FS configuration database	Configuration finished
Configure service settings	Configuration finished
Deploy browser sign-in Web site	Configuration finished
Start the AD FS 2.0 Windows Service	Configuration finished
Create default claim set	Configuration finished
Create default Active Directory claim acceptance rules	Configuration finished

You have successfully completed the AD FS 2.0 Federation Server Configuration Wizard.

To close this wizard, click Close.

Close

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 Active Directory e a autenticação LDAP precisa ser configurada antes de prosseguir. Navegue até a **guia Sistema > Sistema LDAP** conforme mostrado na imagem.

LDAP System Configuration

Status



Please Delete All LDAP Directories Before Making Changes on This Page



Please Disable LDAP Authentication Before Making Changes on This Page

LDAP System Information

Enable Synchronizing from LDAP Server

LDAP Server Type

Microsoft Active Directory



LDAP Attribute for User ID

sAMAccountName



Em seguida, navegue até a [guia Sistema > Diretório LDAP](#).

LDAP Directory



Save



Delete



Copy



Perform Full Sync Now



Add New

Status



Status: Ready

LDAP Directory Information

LDAP Configuration Name*

LDAP1

LDAP Manager Distinguished Name*

fhlab\administrator

LDAP Password*

.....

Confirm Password*

.....

LDAP User Search Base*

cn=users,dc=fhlab,dc=com

LDAP Custom Filter for Users

< None >

Synchronize*

Users Only Users and Groups

LDAP Custom Filter for Groups

< None >

LDAP Directory Synchronization Schedule

Perform Sync Just Once

Perform a Re-sync Every*

7

DAY

Next Re-sync Time (YYYY-MM-DD hh:mm)*

2020-05-24 00:00

Standard User Fields To Be Synchronized			
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

[Add Another Redundant LDAP Server](#)

[Save](#)
[Delete](#)
[Copy](#)
[Perform Full Sync Now](#)
[Add New](#)

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

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | farfar | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

LDAP Authentication

[Save](#)

Status
Status: Ready

LDAP Authentication for End Users

Use LDAP Authentication for End Users

LDAP Manager Distinguished Name*

LDAP Password*

Confirm Password*

LDAP User Search Base*

LDAP Server Information

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

[Add Another Redundant LDAP Server](#)

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.

End User Configuration Related Links: [Back to Find List Users](#)

Confirm MLPP Password
 MLPP Precedence Authorization Level

CAPF Information

Associated CAPF Profiles [View Details](#)

Permissions Information

Groups:

- Standard CCM End Users
- Standard CCM Super Users**
- Standard CTI Allow Control of All Devices
- Standard CTI Enabled

[View Details](#)

Roles:

- Standard AXL API Access
- Standard Admin Rep Tool Admin
- Standard CCM Admin Users
- Standard CCM End Users
- Standard CCMADMIN Administration

[View Details](#)

Conference Now Information

Enable End User to Host Conference Now
 Meeting Number
 Attendees Access Code

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.

System > Call Routing > Media Resources > ... > Device > User Manager > ... > Administration

SAML Single Sign-On

SSO Mode

Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)
 Per node (One metadata file per node)

Status

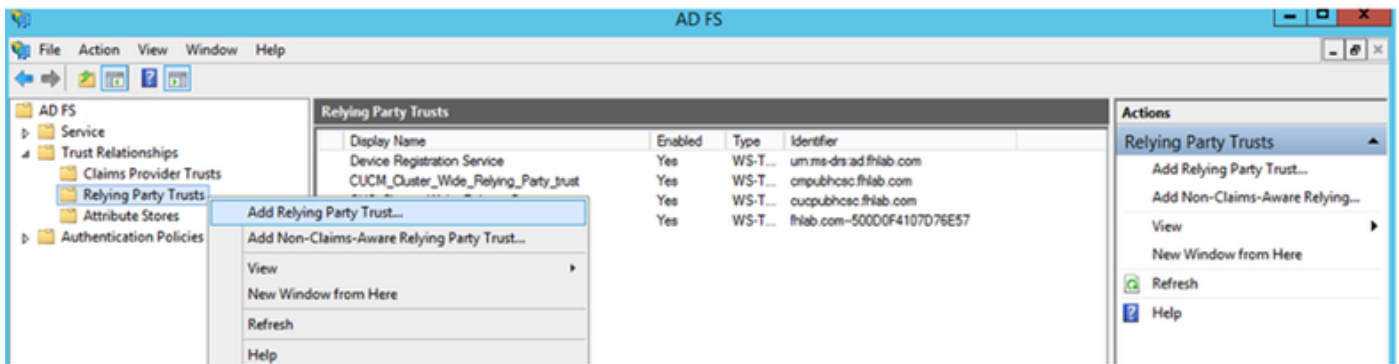
- RTMT is enabled for SSO. You can change SSO for RTMT [here](#).
- SAML SSO enabled

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cmpubhcsc.fhlab.com	SAML	N/A	April 20, 2020 2:00:57 PM PDT	File	April 18, 2020 8:05:38 PM PDT	Passed - April 20, 2020 2:02:15 PM PDT <input type="button" value="Run SSO Test..."/>
cmsubhcsc.fhlab.com	SAML	IdP	April 20, 2020 2:00:57 PM PDT	File	April 18, 2020 8:05:37 PM PDT	Passed - April 20, 2020 1:49:45 PM PDT <input type="button" value="Run SSO Test..."/>
imppubhcsc.fhlab.com	SAML	IdP	April 20, 2020 2:00:57 PM PDT	File	April 18, 2020 8:05:37 PM PDT	Passed - May 24, 2020 12:02:56 PM PDT <input type="button" value="Run SSO Test..."/>
impsubhcsc.fhlab.com	SAML	IdP	April 20, 2020 2:00:57 PM PDT	File	April 18, 2020 8:05:37 PM PDT	Passed - May 24, 2020 12:03:26 PM PDT <input type="button" value="Run SSO Test..."/>

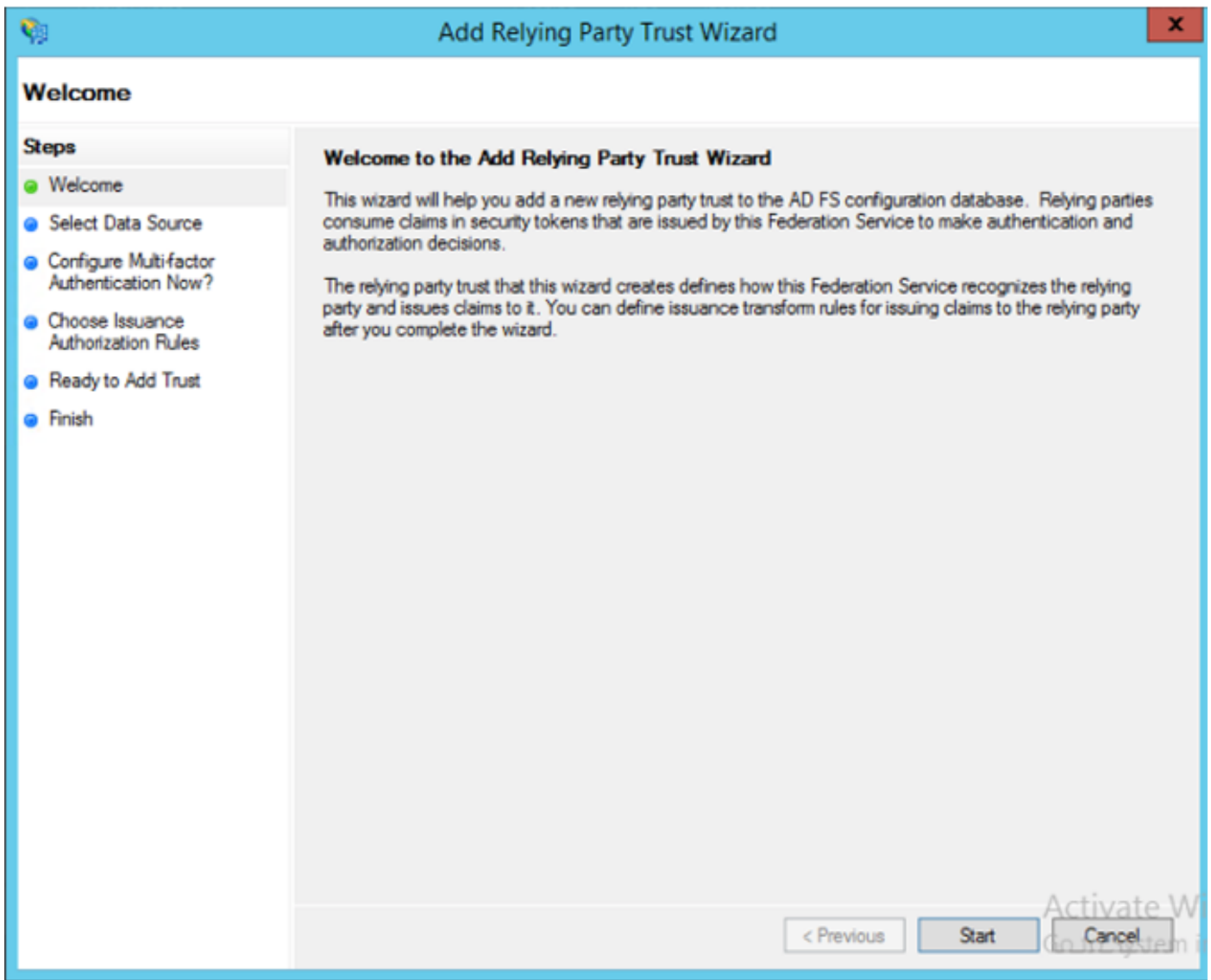
Salve os dados localmente com um nome significativo como sp_cucm0a.xml, você precisará deles depois.

Configurar entidade confiadora do ADFS

Volte para o console de gerenciamento do AD FS 3.0.

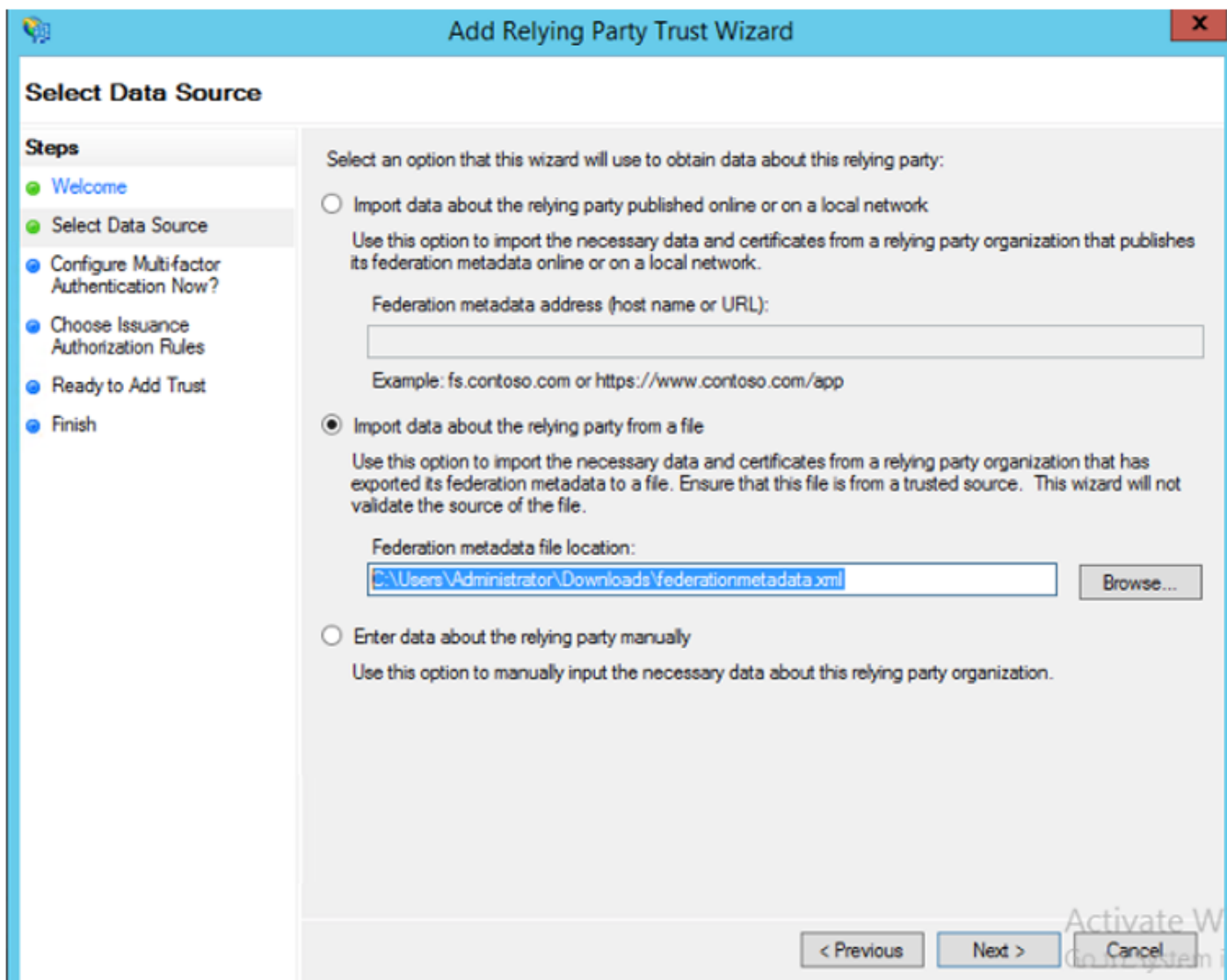


Clique no **Assistente para Adicionar Confiança de Terceiros Confiantes**.



Clique em **Iniciar** para continuar.

Selecione o arquivo XML de metadados **federationmetadata.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.

Add Relying Party Trust Wizard

Specify Display Name

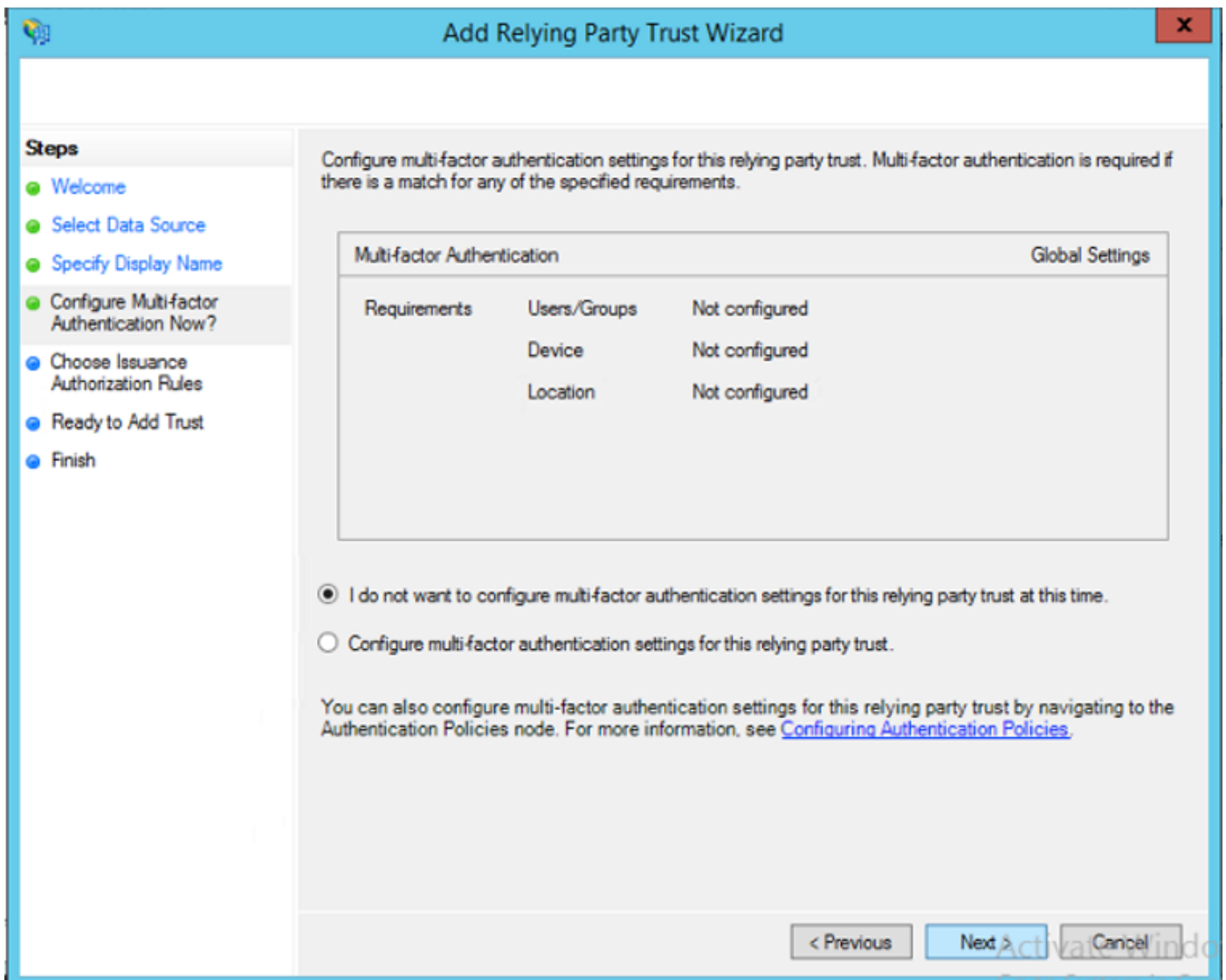
Enter the display name and any optional notes for this relying party.

Display name:

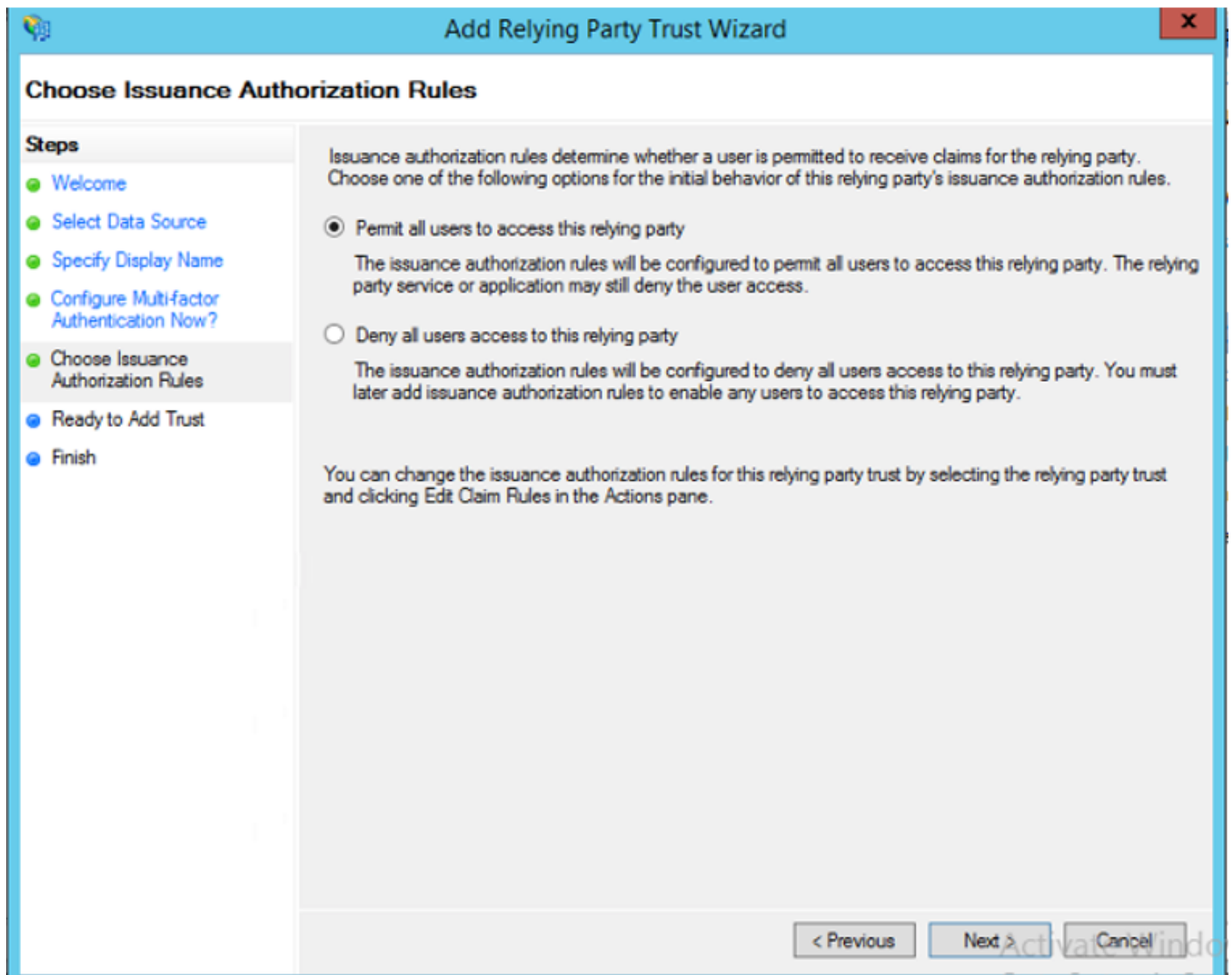
Notes:

< Previous Next > Cancel

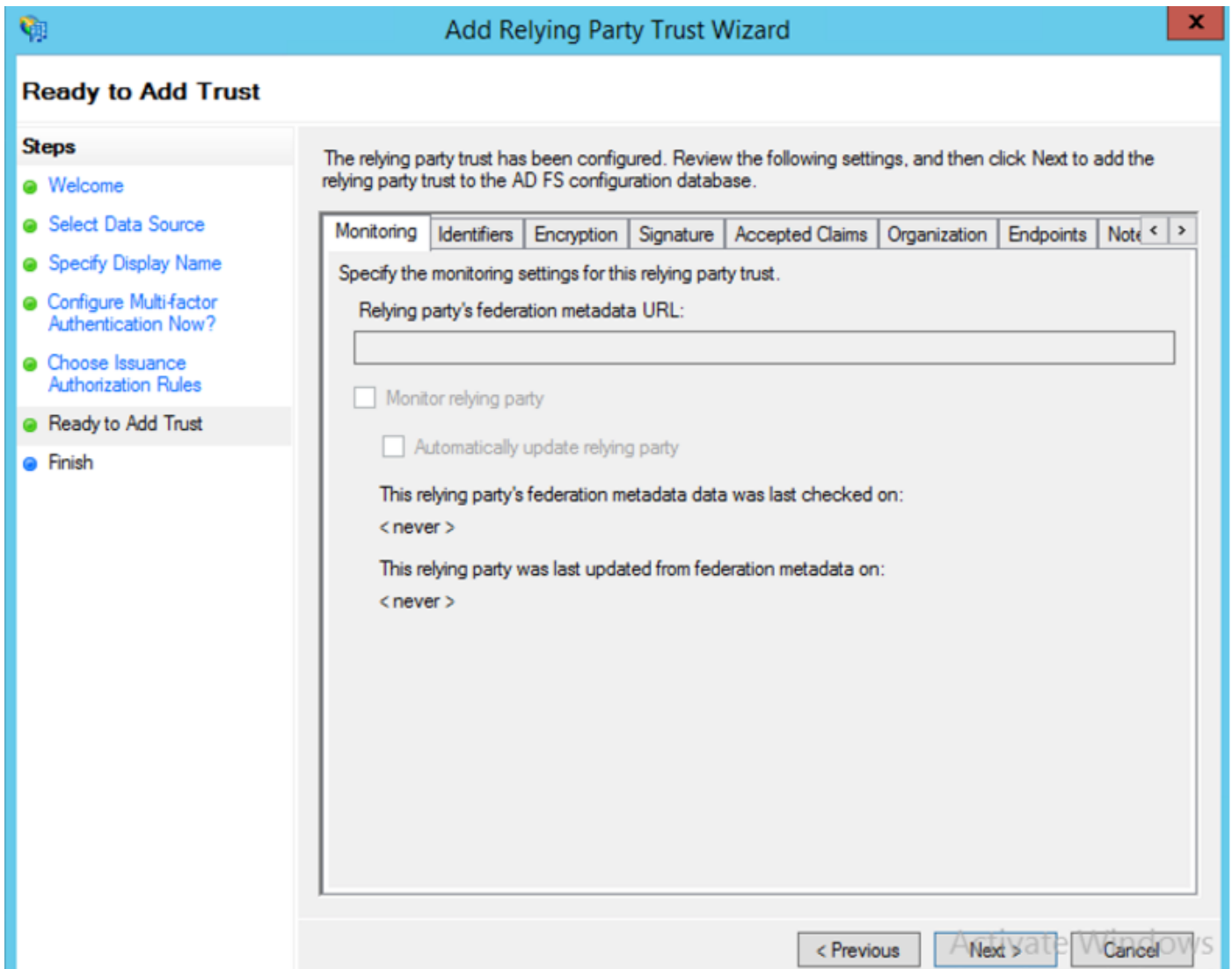
Selecione a primeira opção e clique em **Avançar**.



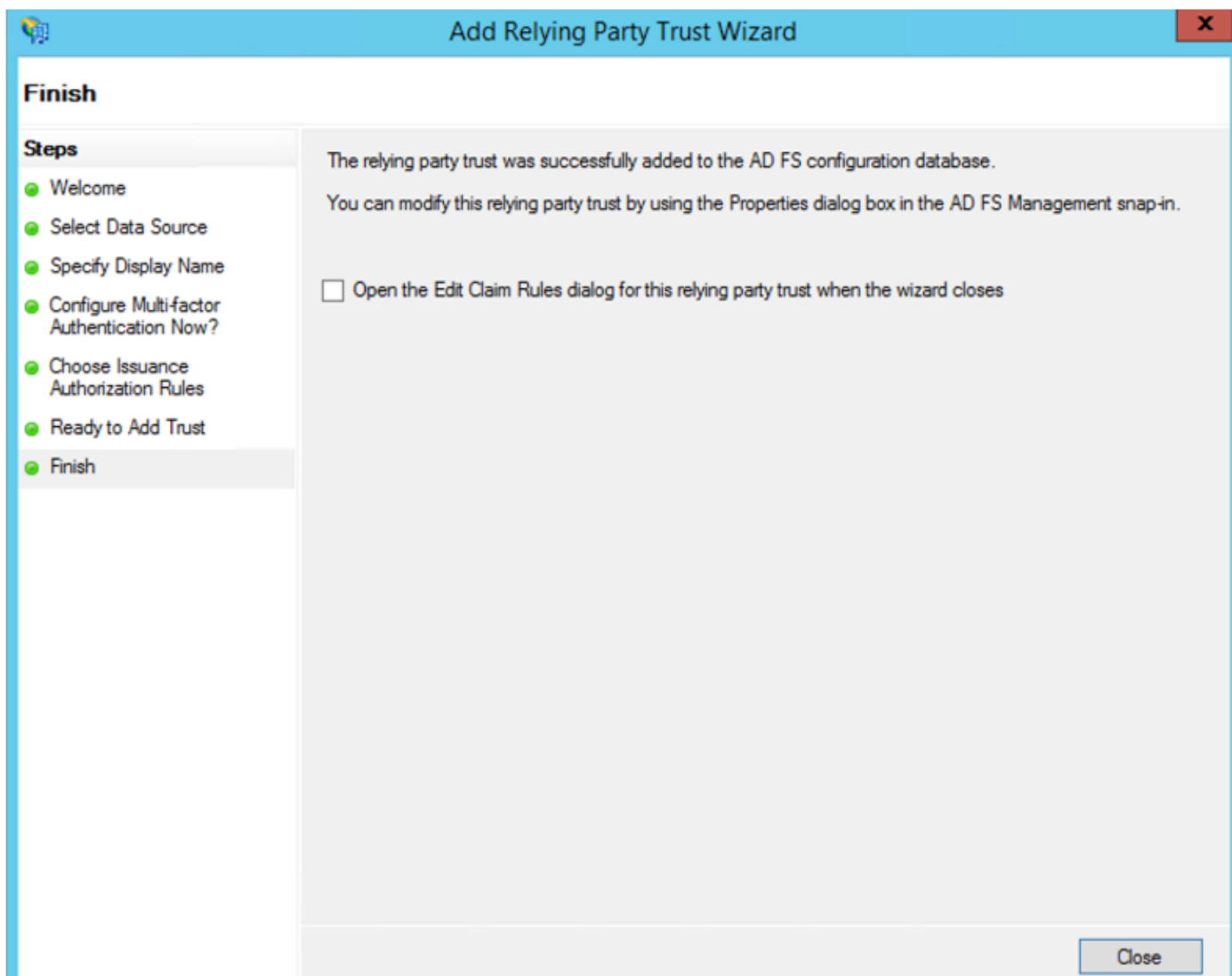
Selecione **Permitir que todos os usuários acessem esta terceira parte confiável** e clique em **Avançar** conforme mostrado na imagem.



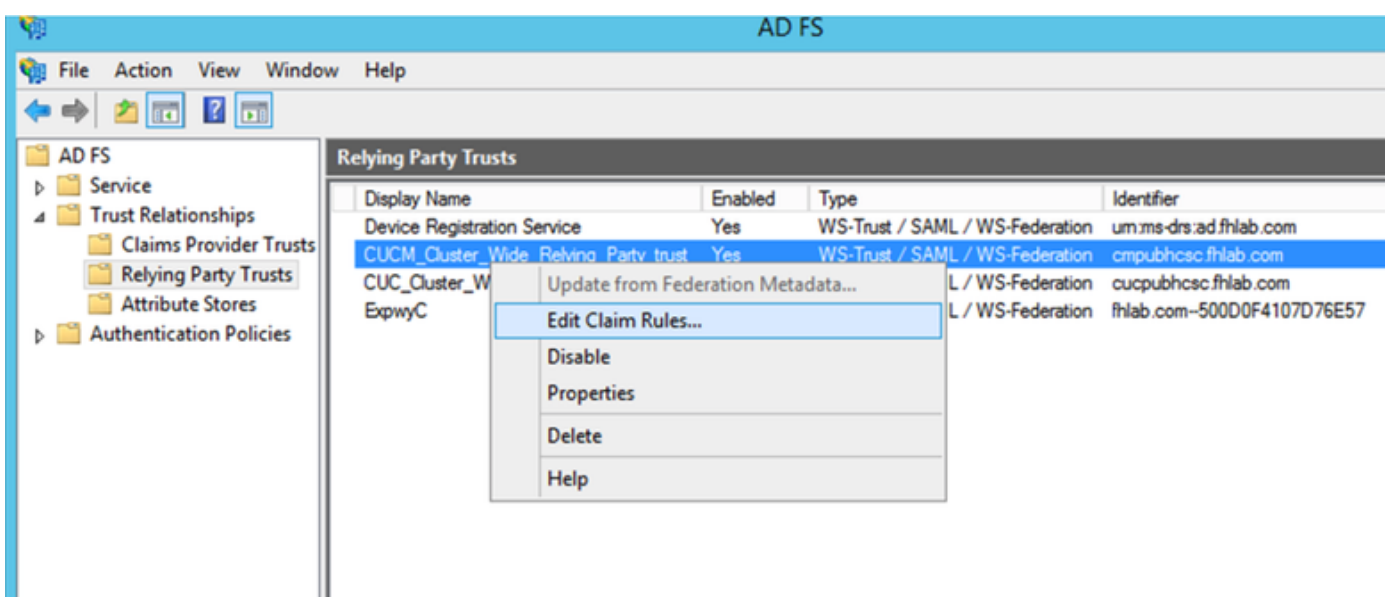
Revise a configuração e clique em **Avançar** conforme mostrado na imagem.



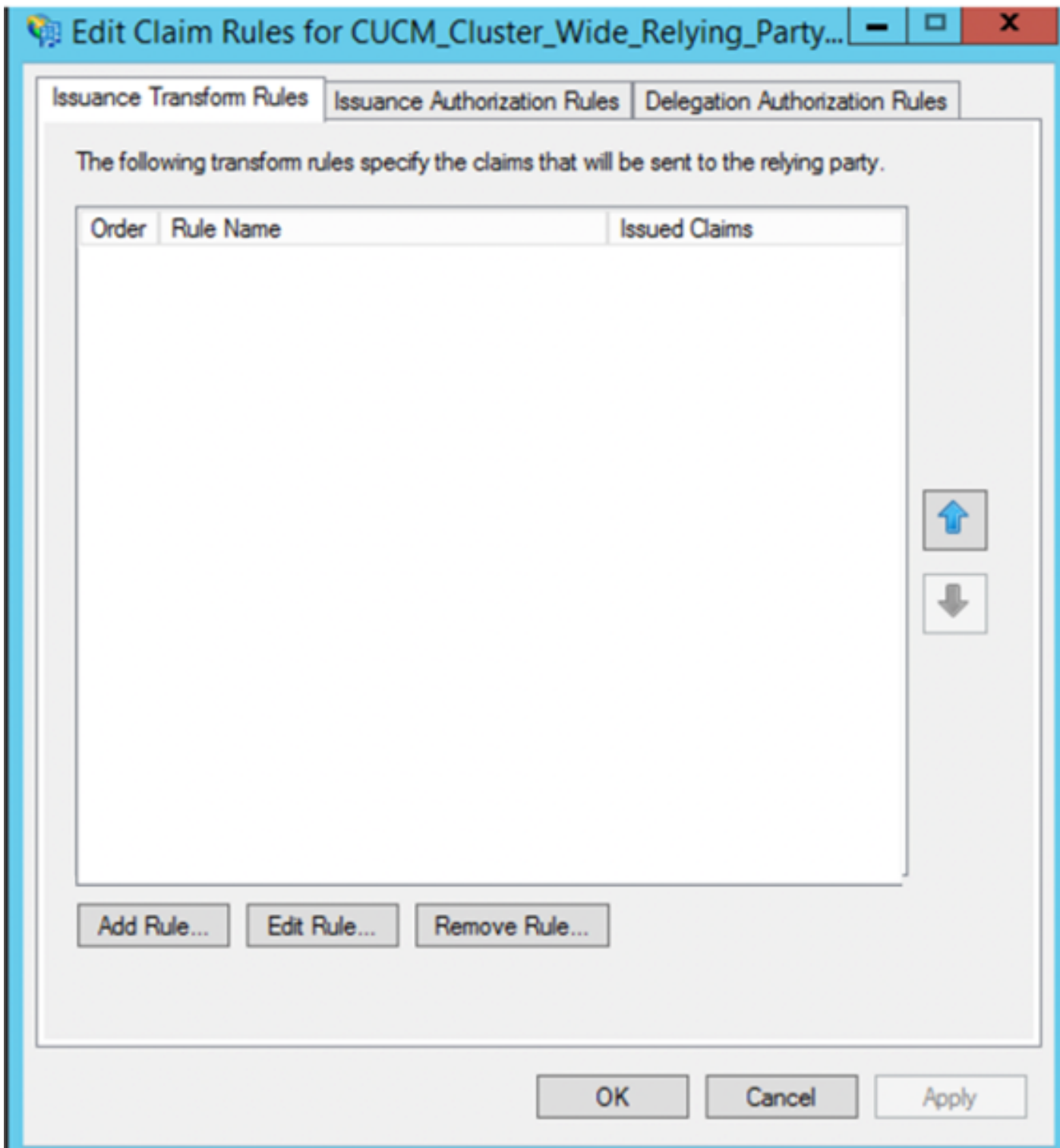
Desmarque a caixa e clique em **Fechar**.



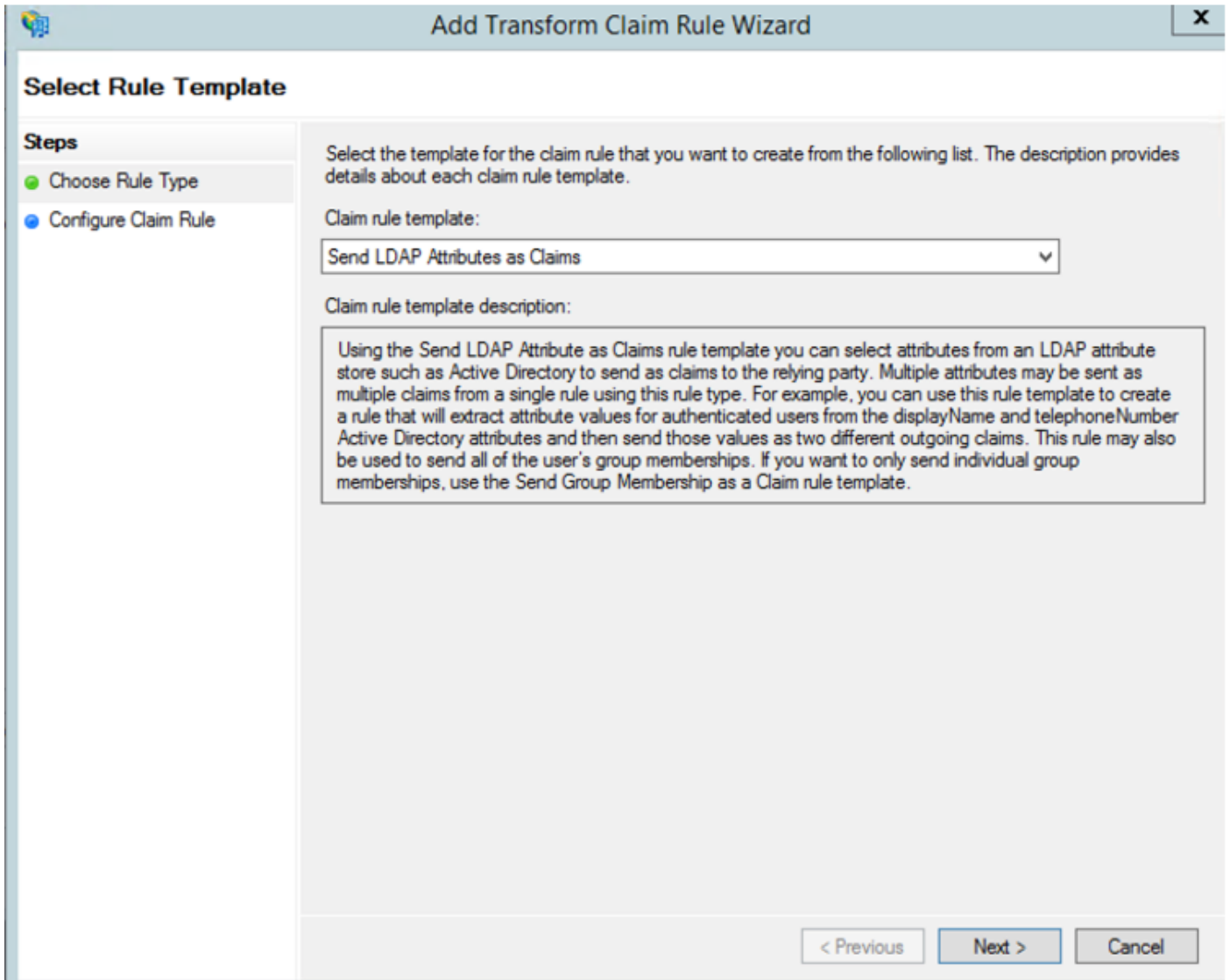
Com o botão do mouse secundário, selecione a **Confiança da terceira parte confiável** que você acabou de criar e **edite a configuração das regras de reivindicação**, como mostrado na imagem.



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.

Edit Rule - NameID

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

Claim rule name:

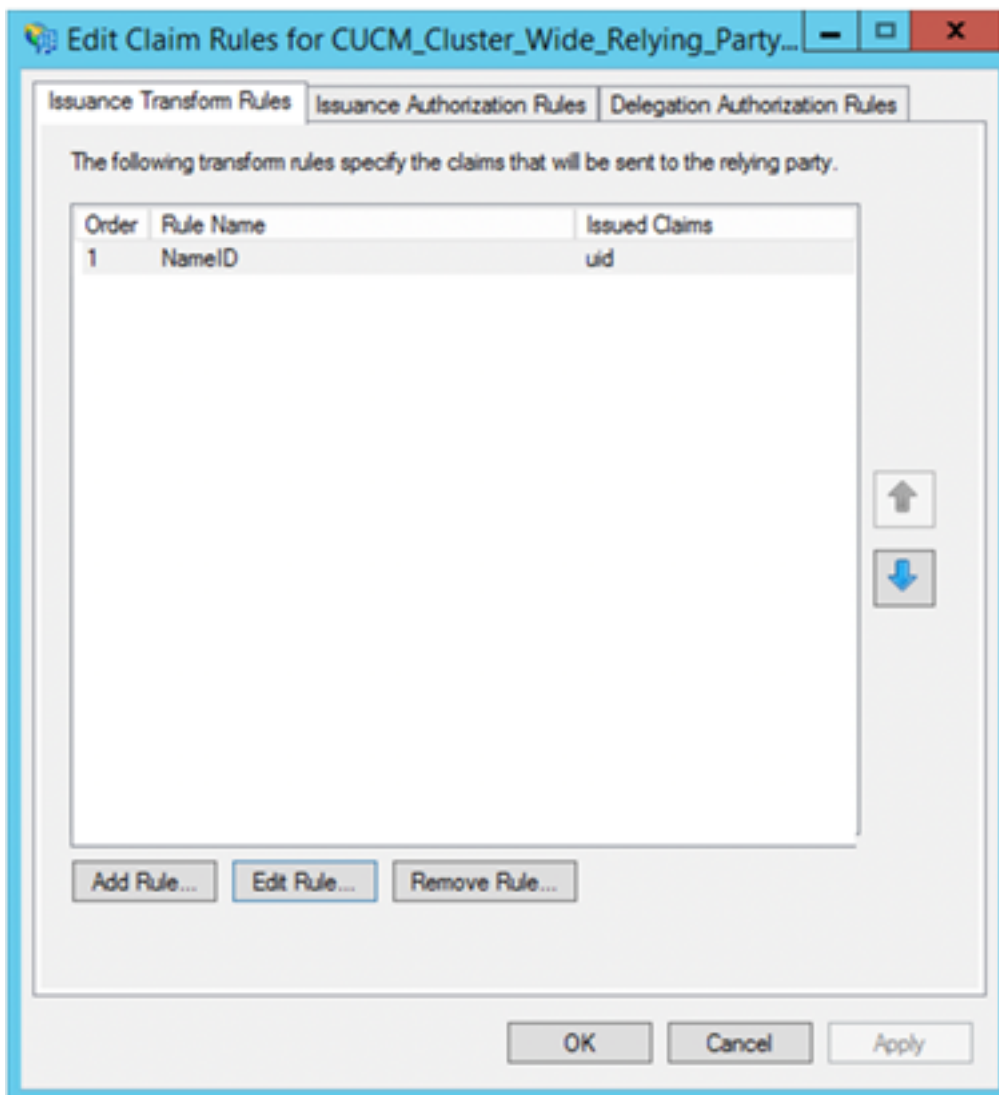
Rule template: Send LDAP Attributes as Claims

Attribute store:

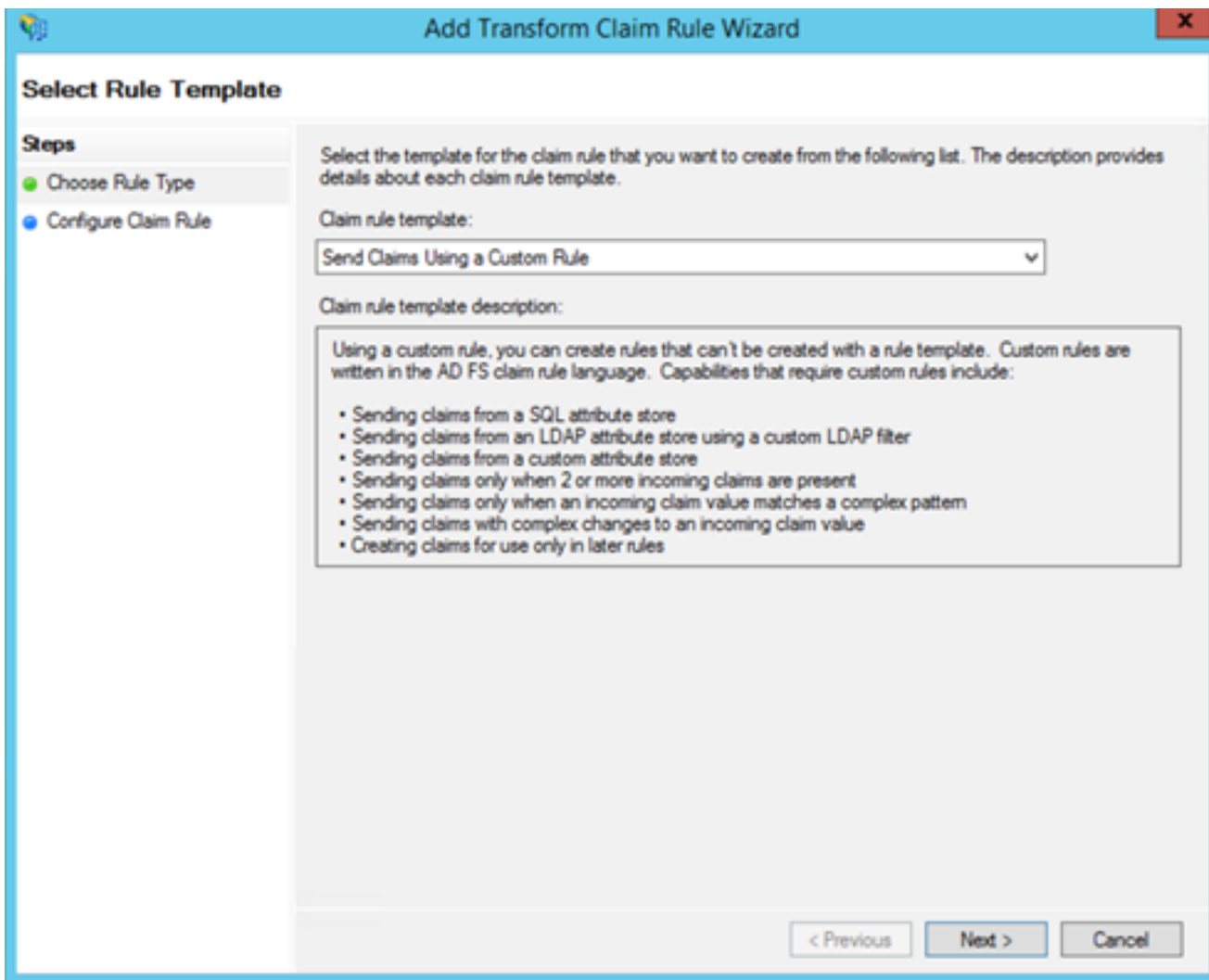
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name	uid
*		

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.

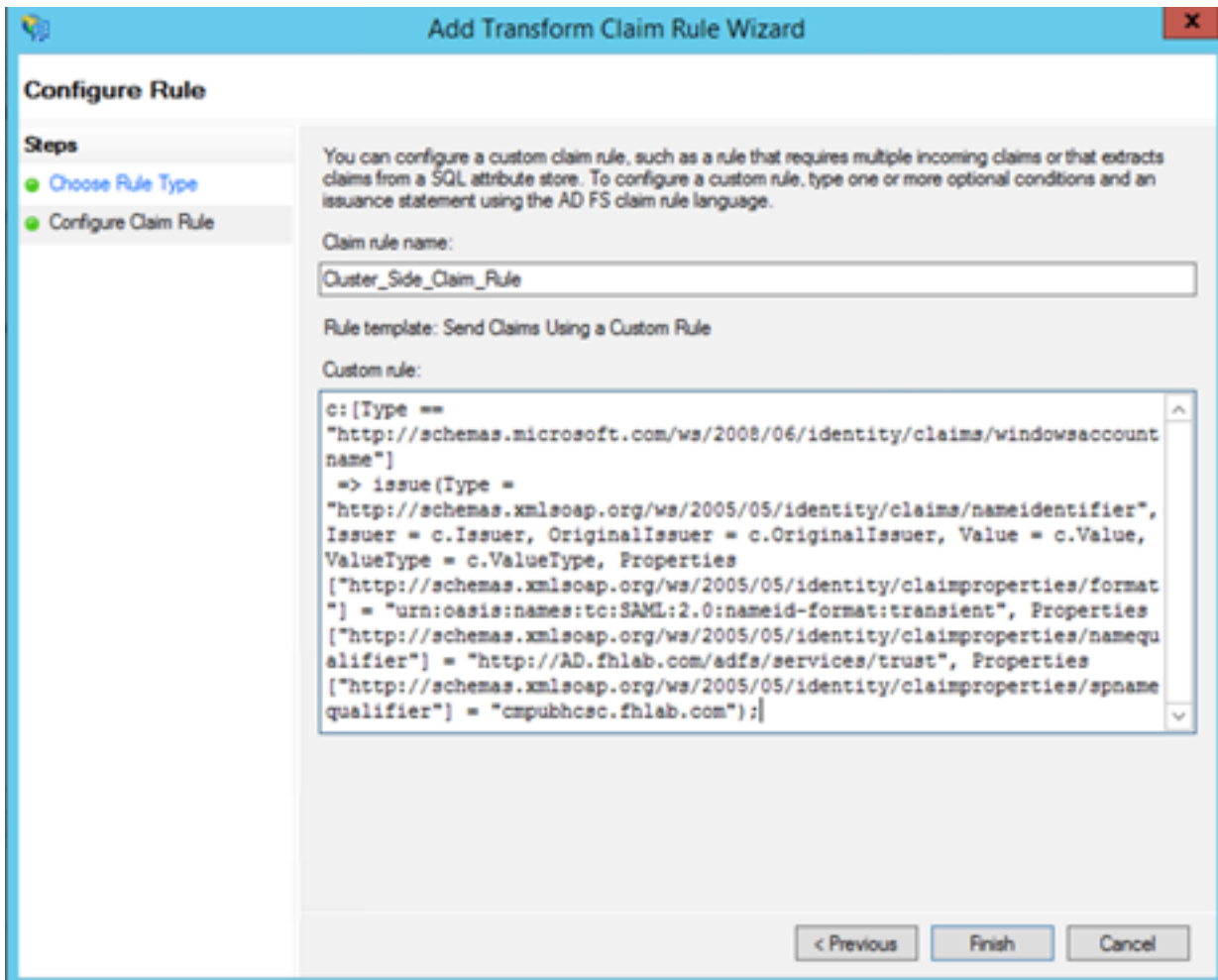
Copie e cole este texto na janela de regras diretamente daqui. Às vezes, os orçamentos são alterados se forem editados em um editor de texto e isso fará com que a regra falhe quando você testar o SSO:

```
c:[Type ==
```

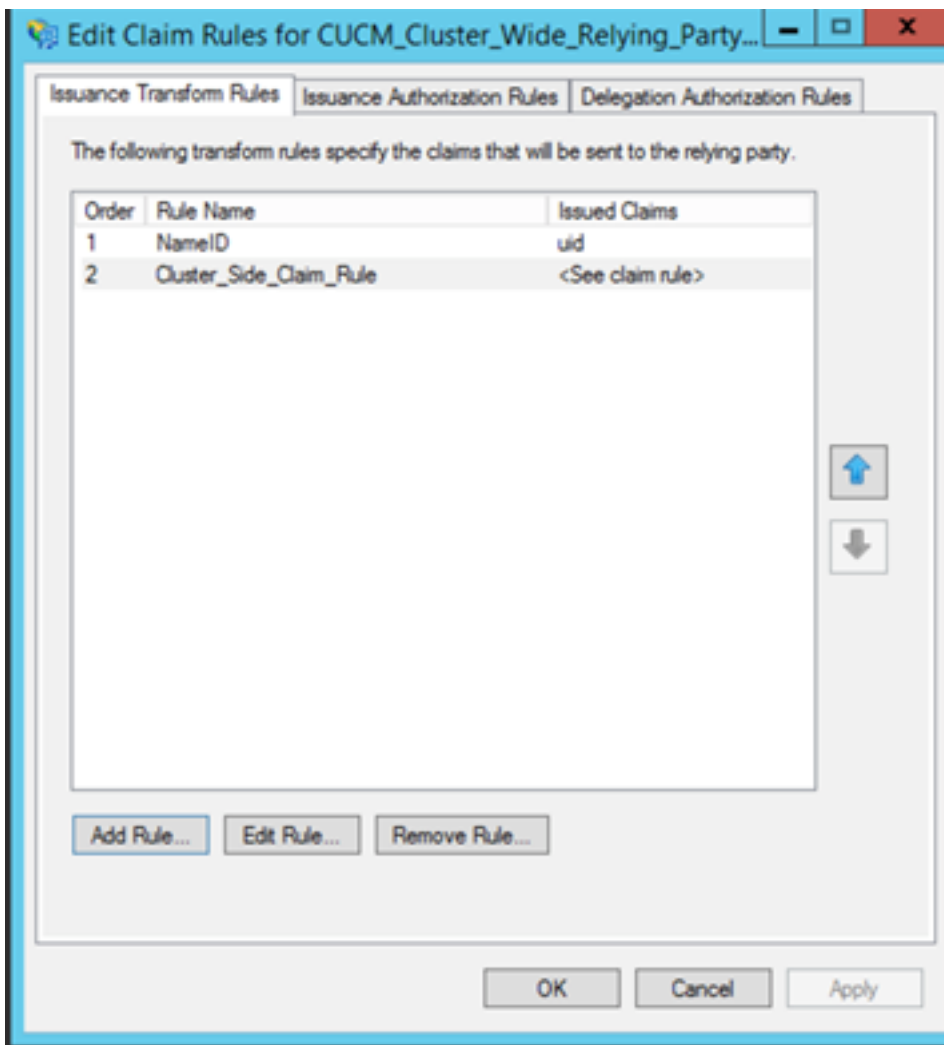
```
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"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");
```

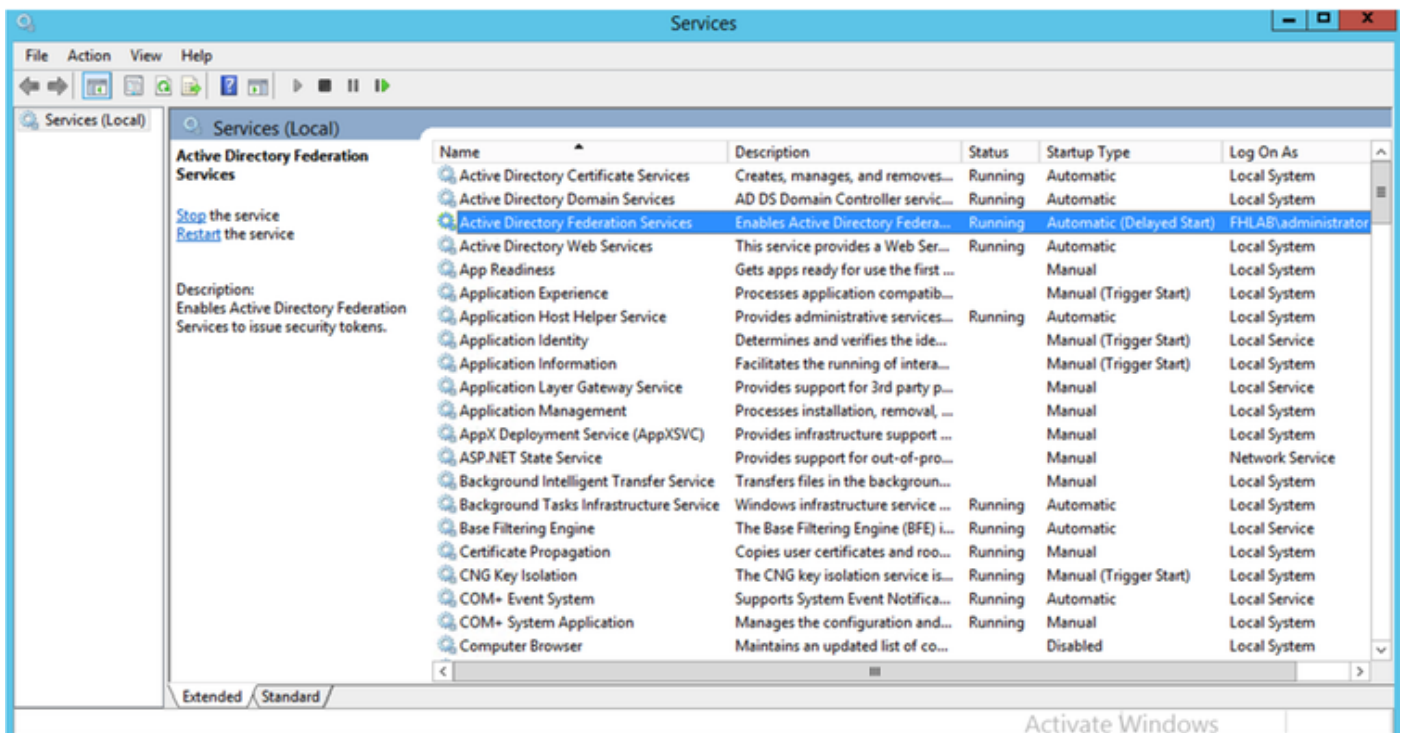
Clique em **Concluir** para continuar.



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



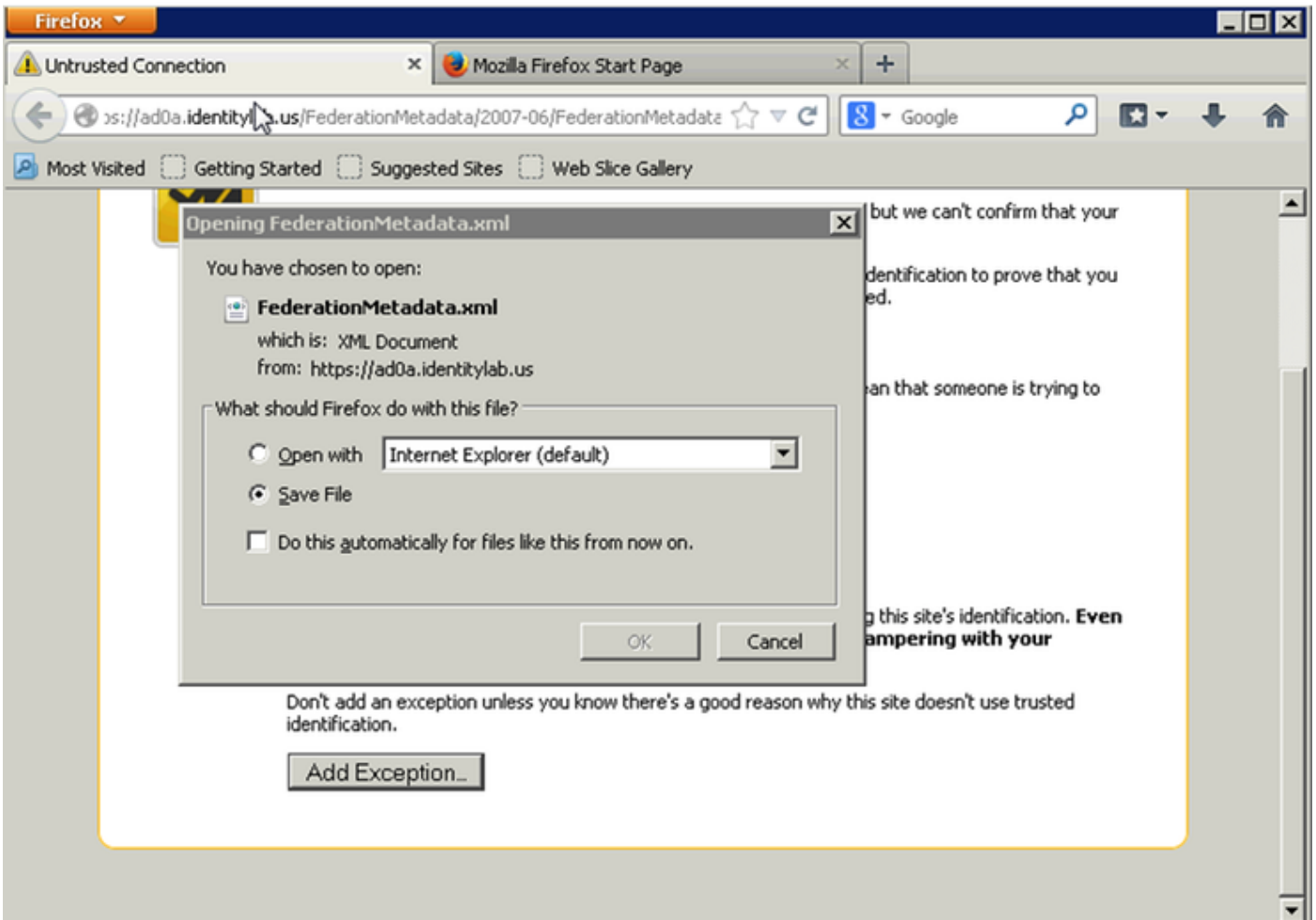
O CUCM foi adicionado com êxito como uma parte confiável ao ADFS.



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**.

Find and List Cisco Unified CM X

Navigation Cisco Unified CM Administration Go

Server

Cisco Unified CM

Cisco Unified CM Group

Presence Redundancy Groups

Phone NTP Reference

Date/Time Group

BLF Presence Group

Region Information

Device Pool

Device Mobility

DHCP

LDAP

SAML Single Sign-On

Cross-Origin Resource Sharing (CORS)

Location Info

MLPP

Physical Location

SRST

Enterprise Parameters

Enterprise Phone Configuration

Service Parameters

Security

Application Server

Licensing

Geolocation Configuration

Geolocation Filter

E911 Messages

Manager Group

where Name begins with Find Clear Filter

active query. Please enter your search criteria using the options above.

<https://cnpubhsc.fhlab.com:8443/ccmadmin/samlSingleSignOn.do>

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

Firefox

Find and List Users | SAML Single Sign-On | Find and List LDAP Directories

https://cucm0a/ccmadmin/samlSingleSignOn.do

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go
admin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

SAML Single Sign-On

Enable SAML SSO | Update IdP Metadata File | Export All Metadata | Fix All Disabled Servers

Status

SAML SSO disabled

SAML Single Sign-On (1 - 1 of 1) Rows per Page: 50

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cucm0a	Disabled	N/A	Never	File	Never	Never

Run Test...

Selecione Ativar SSO SAML.

Clique em Continuar para confirmar o aviso.

Reset Warning - Mozilla Firefox

https://cucm0a/ccmadmin/genericDialogWindow.do?windowTitleKey=genericDialogWindow.windowTitle.ssoenable

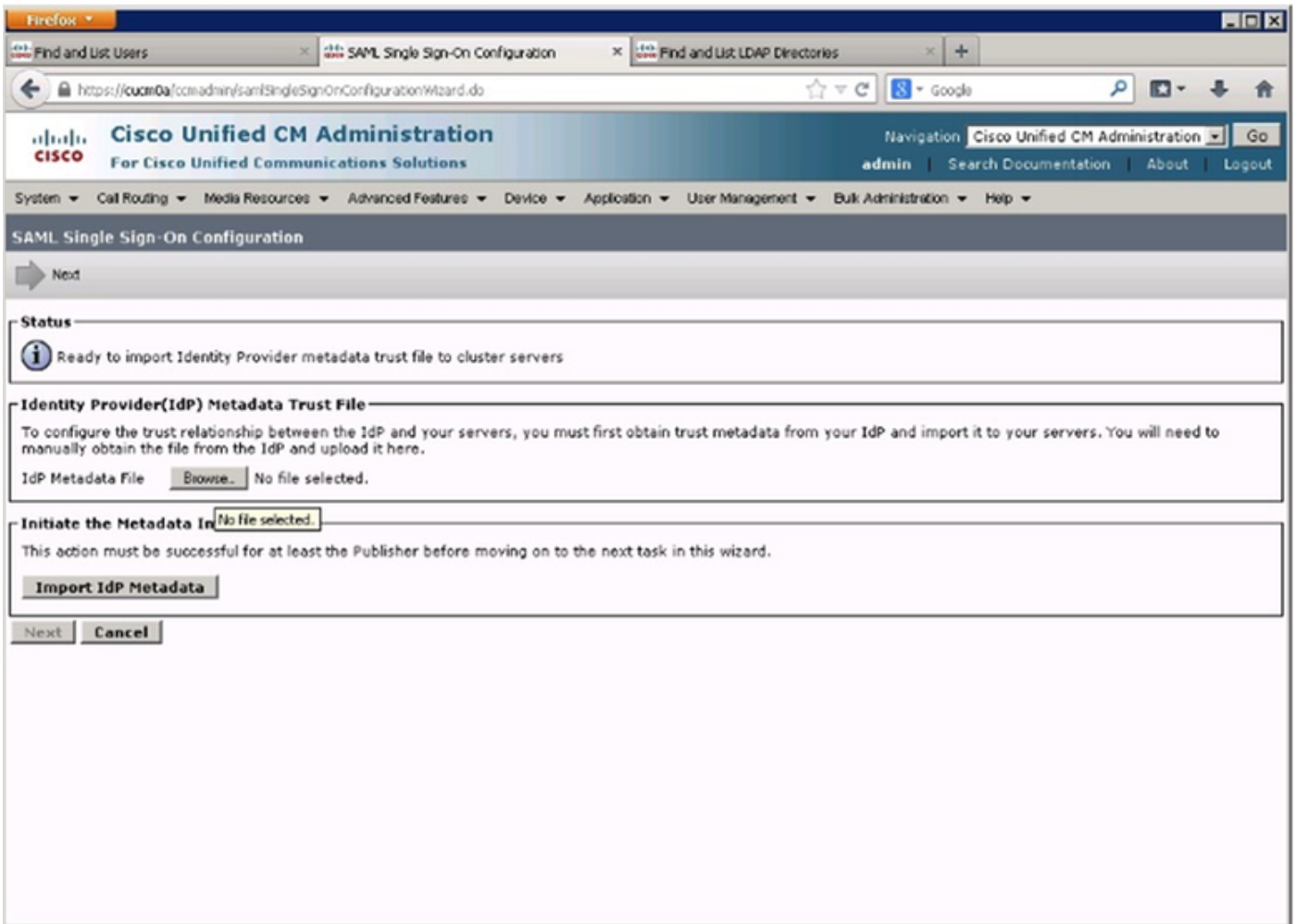
Web server connections will be restarted

Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.

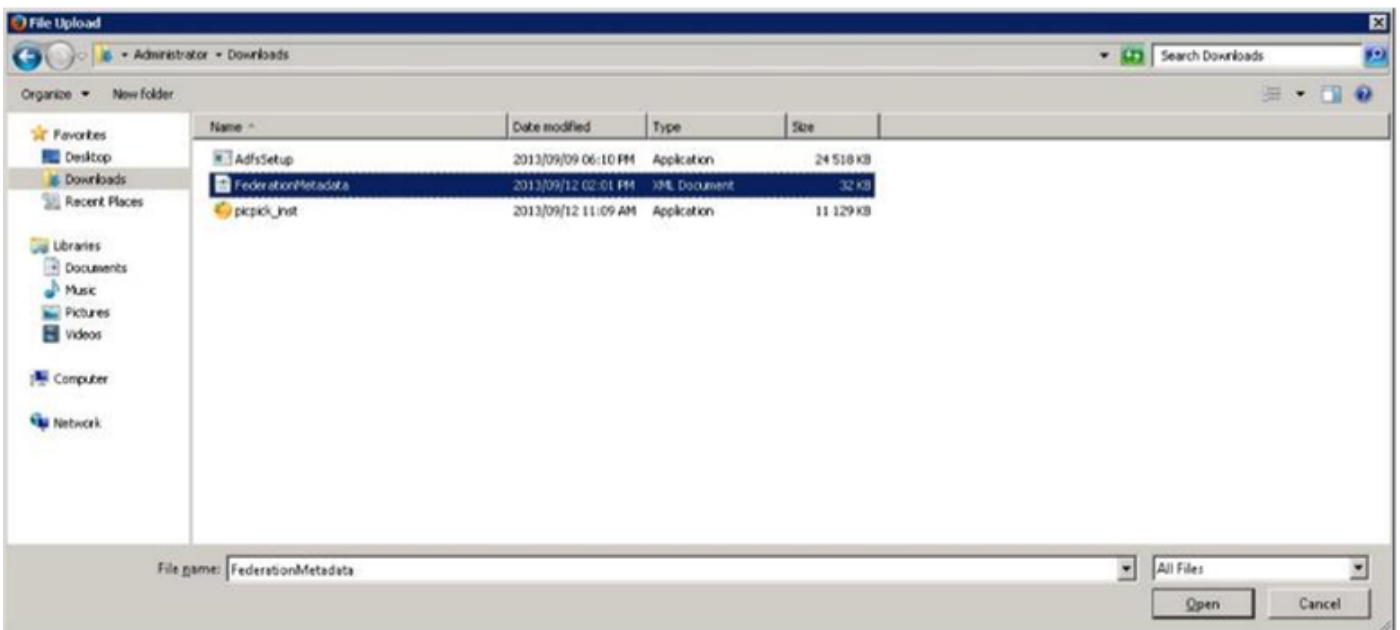
Continue Cancel

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.

SAML Single Sign-On Configuration - Windows Internet Explorer

Navigation Cisco Unified CM Administration admin | Search Documentation | About | Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

SAML Single Sign-On Configuration

Next

Status
✔ Import succeeded for all servers

Identity Provider(IdP) Metadata Trust File
To configure the trust relationship between the IdP and your servers, you must first obtain trust metadata from your IdP and import it to your servers. You will need to manually obtain the file from the IdP and upload it here.
IdP Metadata File

Initiate the Metadata Import
This action must be successful for at least the Publisher before moving on to the next task in this wizard.
 ✔ Import succeeded for all servers

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

SAML Single Sign-On Configuration - Mozilla Firefox

https://cmpubhcsc.fhlab.com:8443/ccadmin/samlSingleSignOnConfigurationWizard3.do?servei

SAML Single Sign-On Configuration

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 can be run on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is successful.

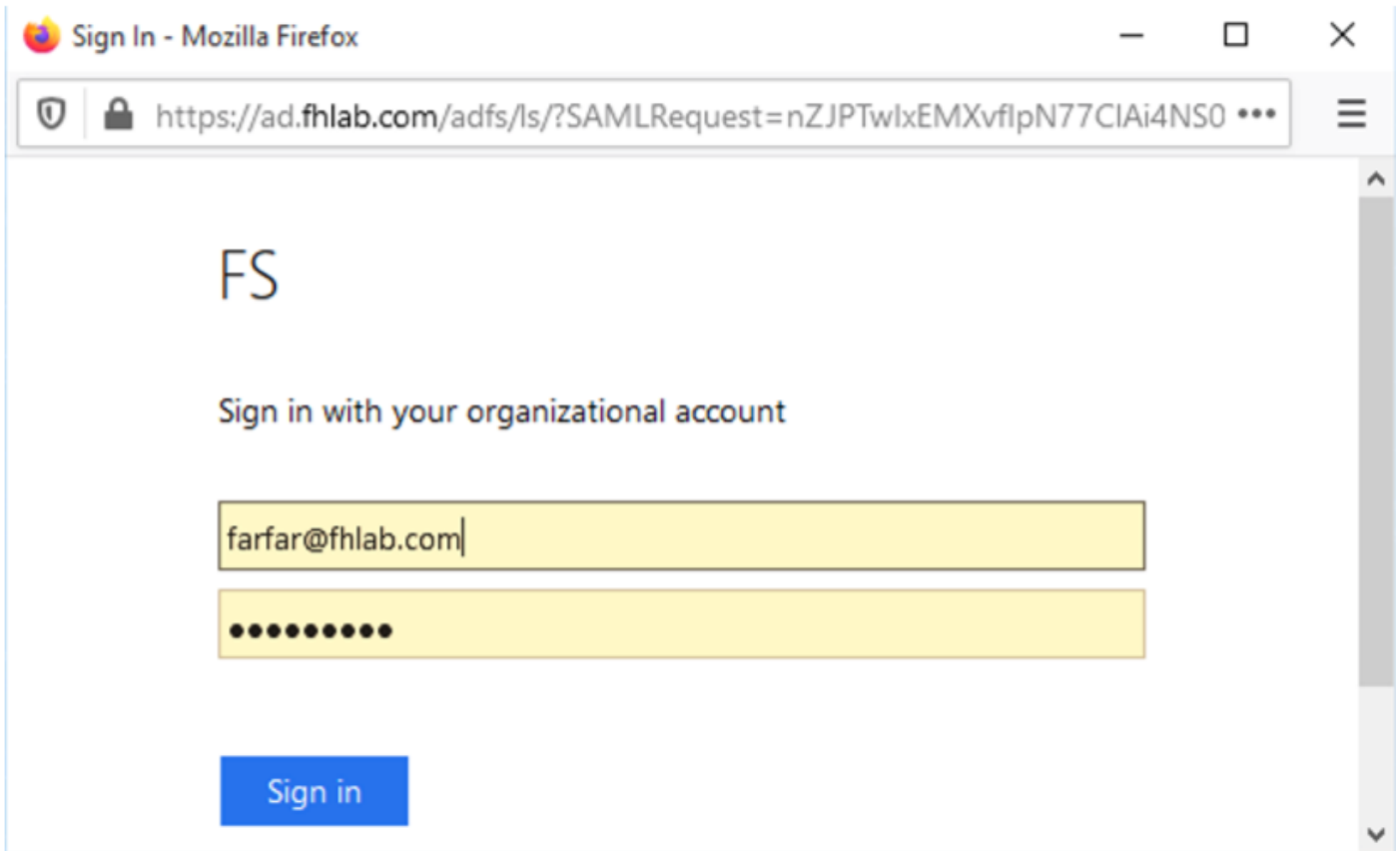
1) Pick a valid username to use for this test
You must already know the password for the selected username. This user must have administrator rights and also exist in the IdP.

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

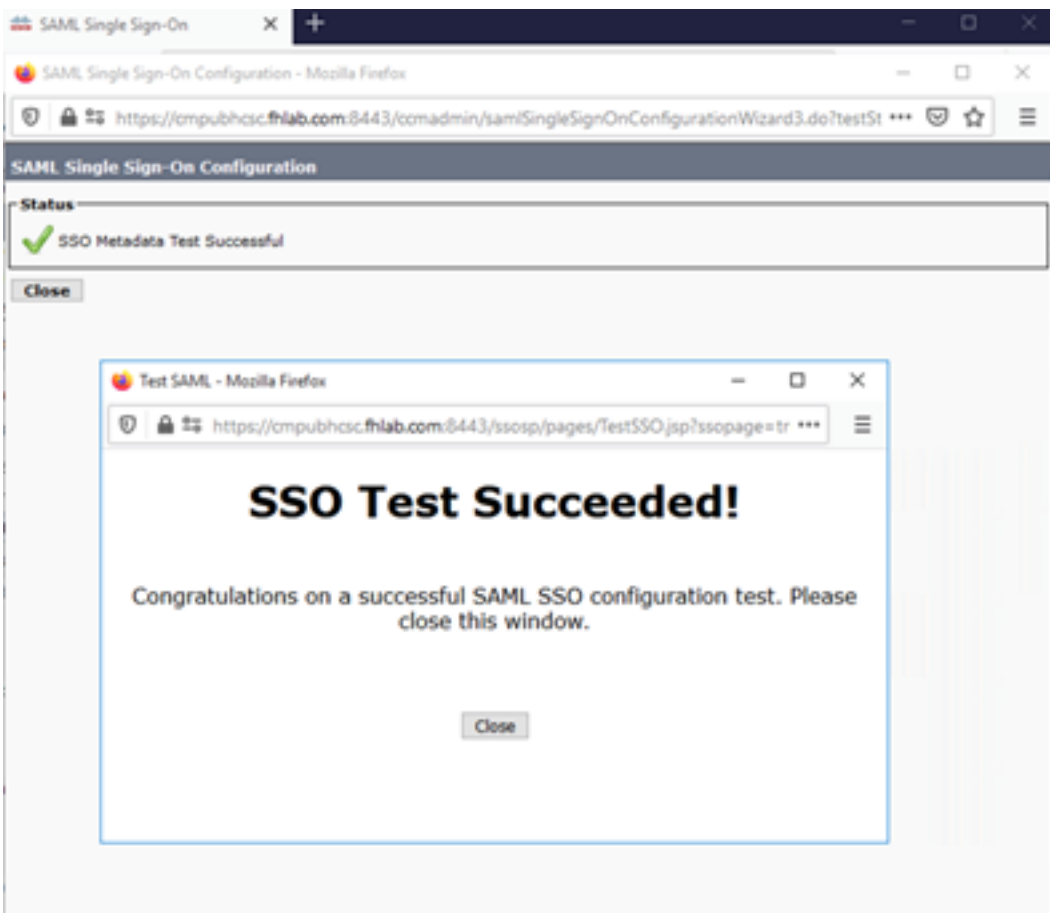
Valid administrator Usernames

2) Launch SSO test page

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.

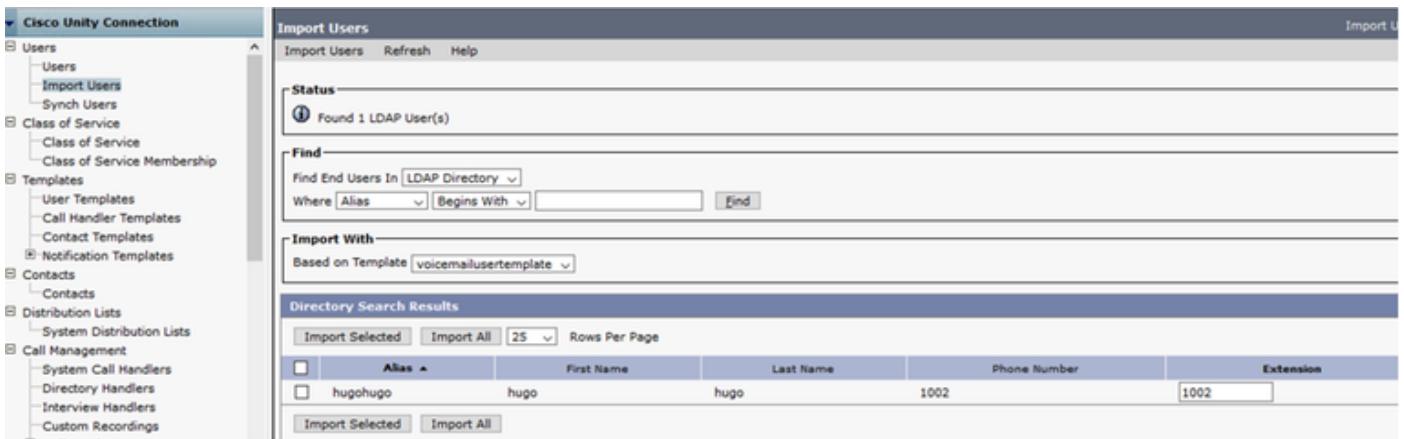
The screenshot shows the Cisco Unity Connection Administration web interface. The left sidebar is expanded to 'System Settings' > 'LDAP' > 'SAML Single Sign-On'. The main content area is titled 'SAML Single Sign-On' and includes a 'SSO Mode' section with two radio buttons: 'Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)' (selected) and 'Per node (One metadata file per node)'. Below this are buttons for 'Disable SAML SSO', 'Update IDP Metadata File', 'Export All Metadata', and 'Fix All Disabled Servers'. A table below shows the configuration for two servers:

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cucpubhsc.fhlab.com	SAML	N/A	April 29, 2020 10:52:36 AM PDT	File	April 28, 2020 5:54:01 PM PDT	Passed - April 29, 2020 11:05:10 AM PDT
cucsubhsc.fhlab.com	SAML	IDP	April 29, 2020 10:52:36 AM PDT	File	April 28, 2020 5:54:00 PM PDT	Passed - April 29, 2020 11:05:37 AM PDT

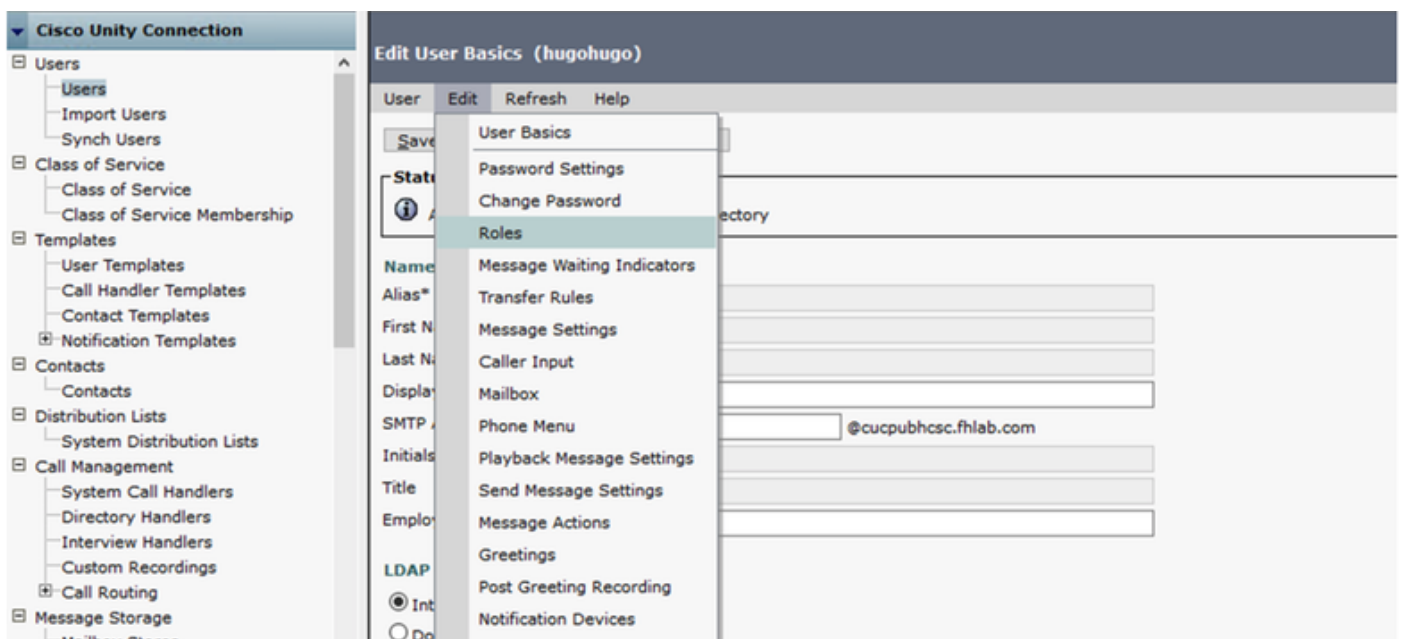
Configure a autenticação LDAP.

The screenshot shows the Cisco Unity Connection Administration web interface. The left sidebar is expanded to 'System Settings' > 'LDAP' > 'LDAP Authentication'. The main content area is titled 'LDAP Authentication' and includes a 'Status' section showing 'Status: Ready'. Below this is the 'LDAP Authentication for End Users' section with a checked box 'Use LDAP Authentication for End Users' and fields for 'LDAP Manager Distinguished Name*' (fhlab\Administrator), 'LDAP Password*', 'Confirm Password*', and 'LDAP User Search Base*' (cn=users,dc=fhlab,dc=com). The 'LDAP Server Information' section has fields for 'Host Name or IP Address for Server*' (10.89.228.226), 'LDAP Port*' (389), and 'Use TLS' (unchecked). A 'Save' button is at the bottom.

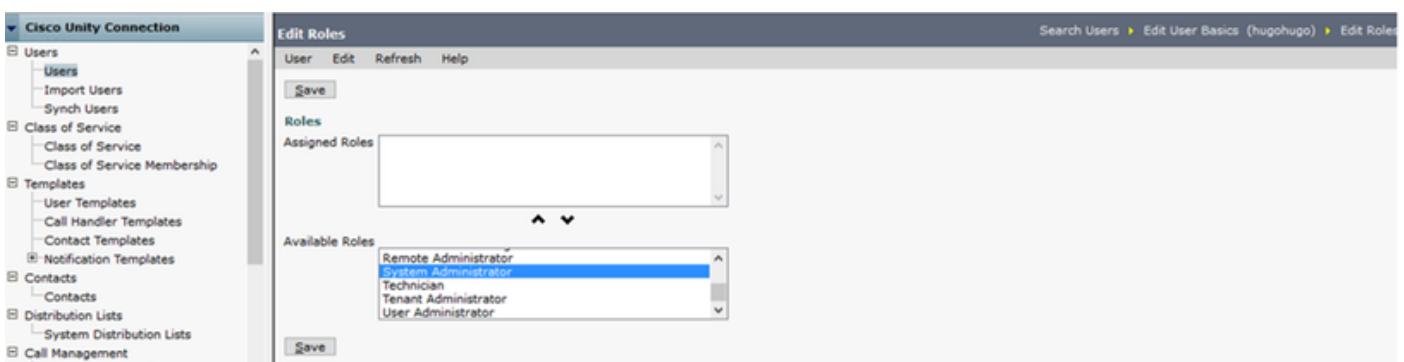
Importe os usuários do LDAP que terão correio de voz atribuído e também o usuário que servirá para testar o SSO.



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

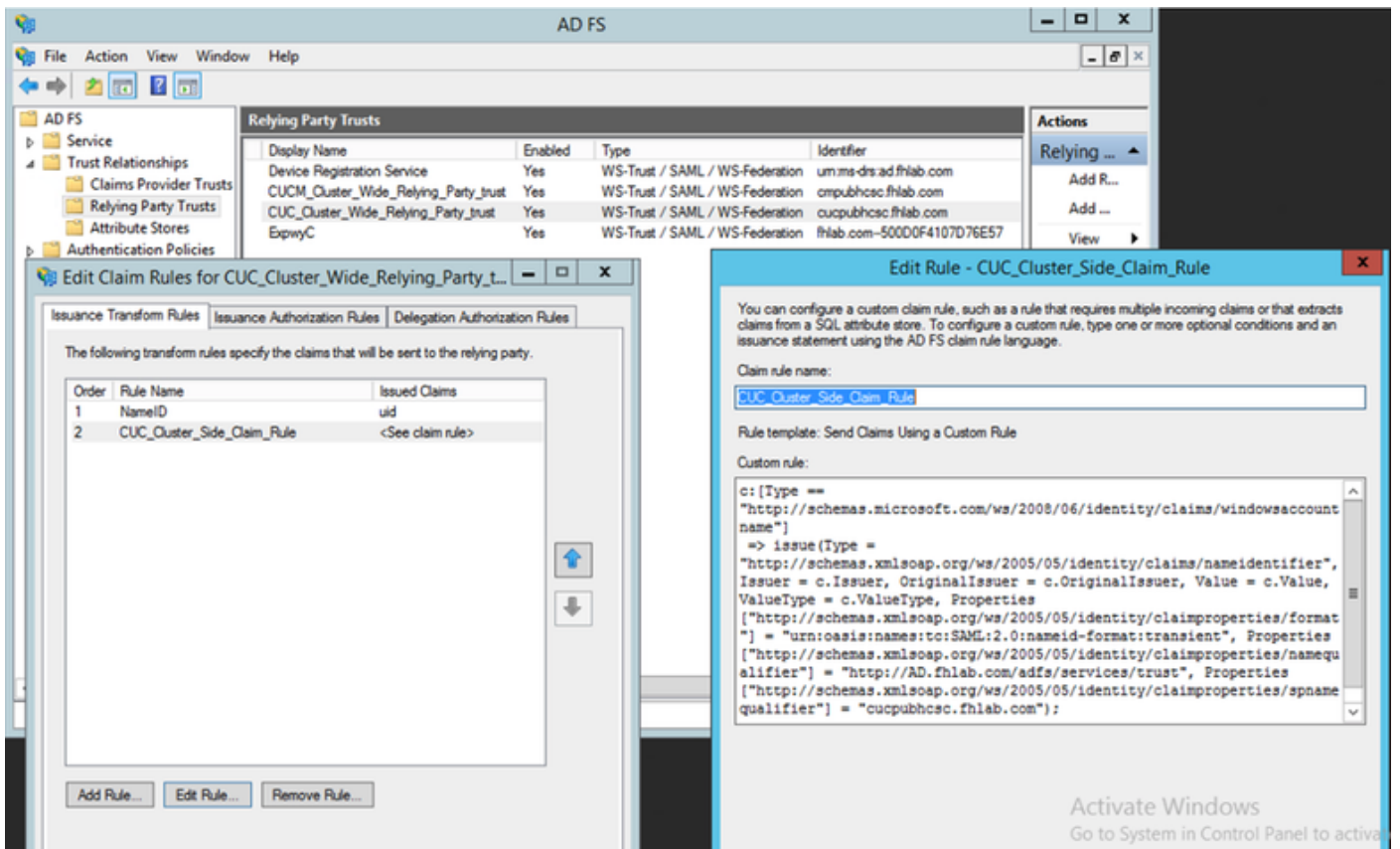


Atribua ao usuário de teste a função de Administrador do sistema.

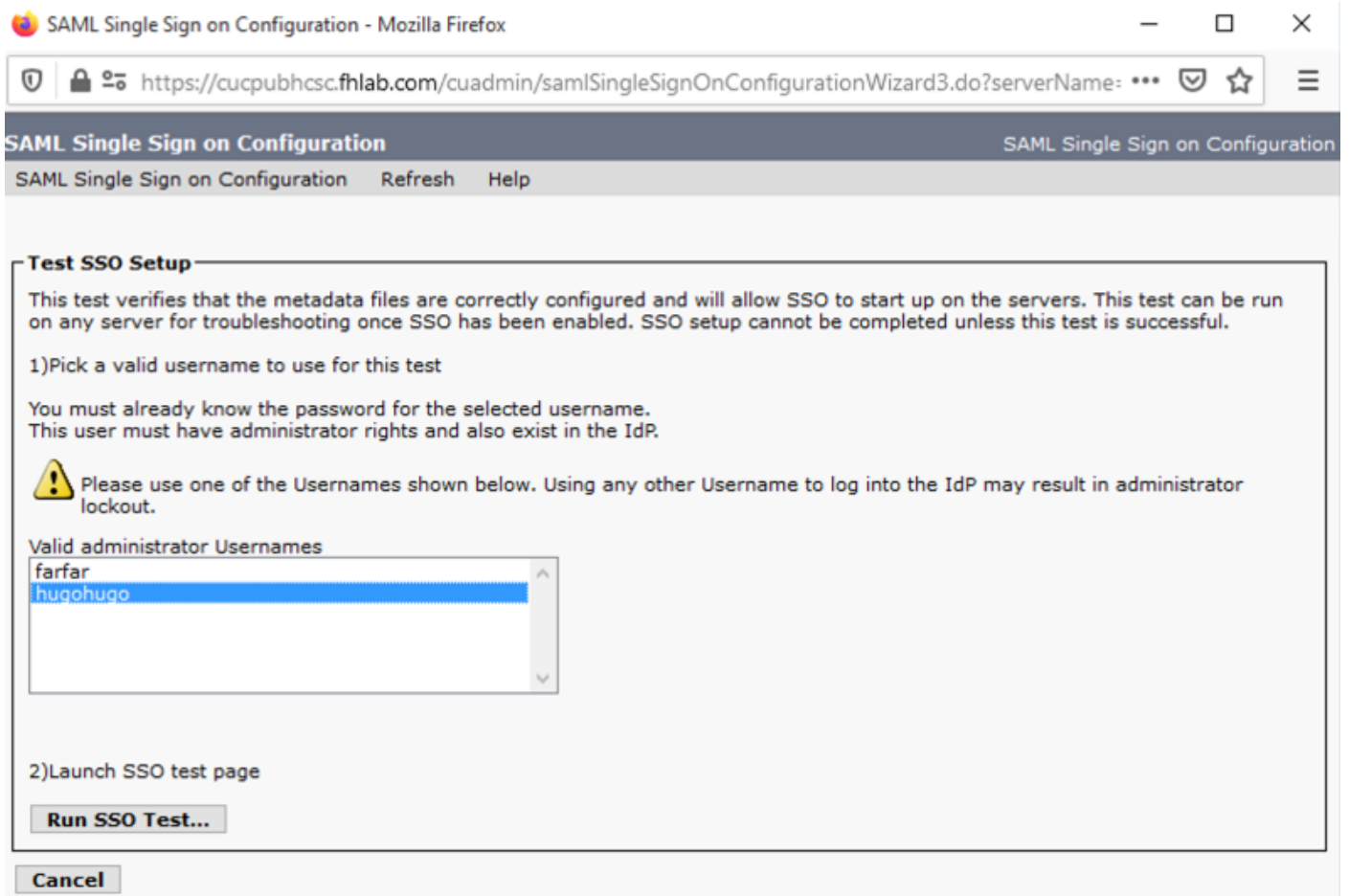


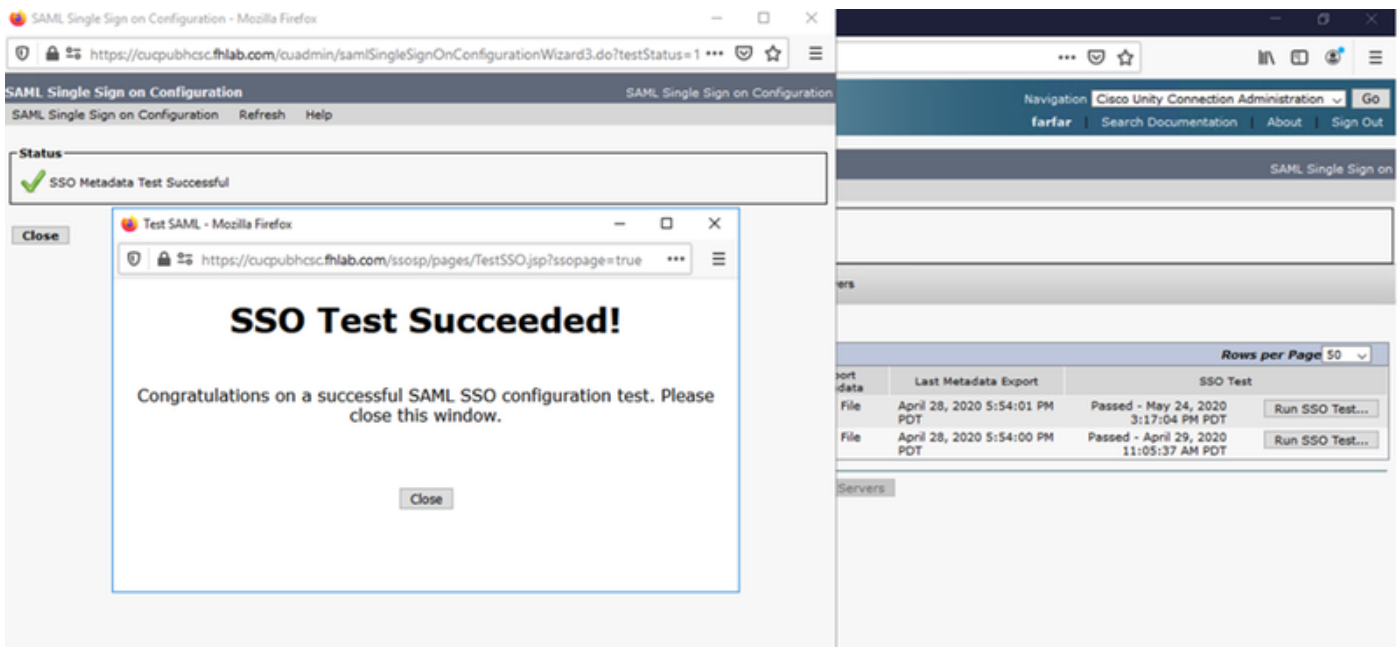
Metadados CUC

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

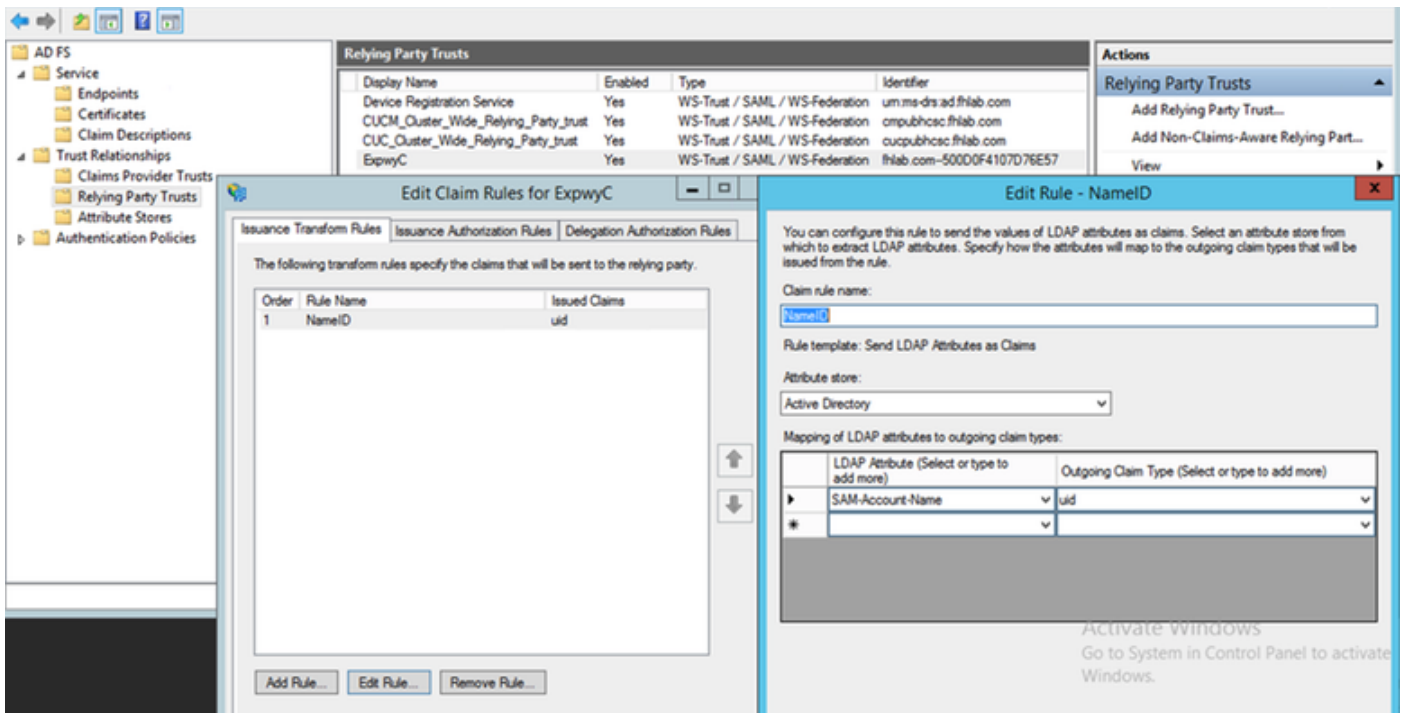
Vá para a configuração -> Unified Communications -> IDP -> Export SAML Data

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.

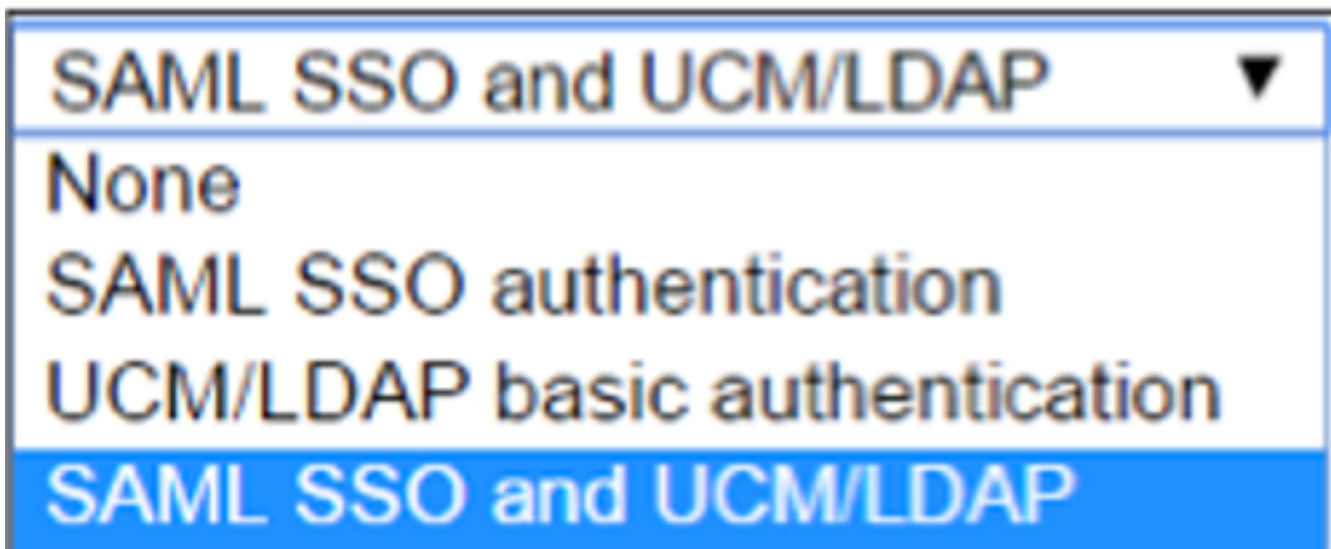


OAuth com login de atualização

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**.

SSO and OAuth Configuration		
OAuth Token Expiry Timer (minutes) *	60	60
OAuth Refresh Token Expiry Timer (days) *	60	60
Redirect URIs for Third Party SSO Client		
SSO Login Behavior for iOS *	Use embedded browser (WebView)	Use embedded browser (WebView)
OAuth with Refresh Login Flow *	Enabled	Disabled
Use SSO for RTMT *	True	True

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

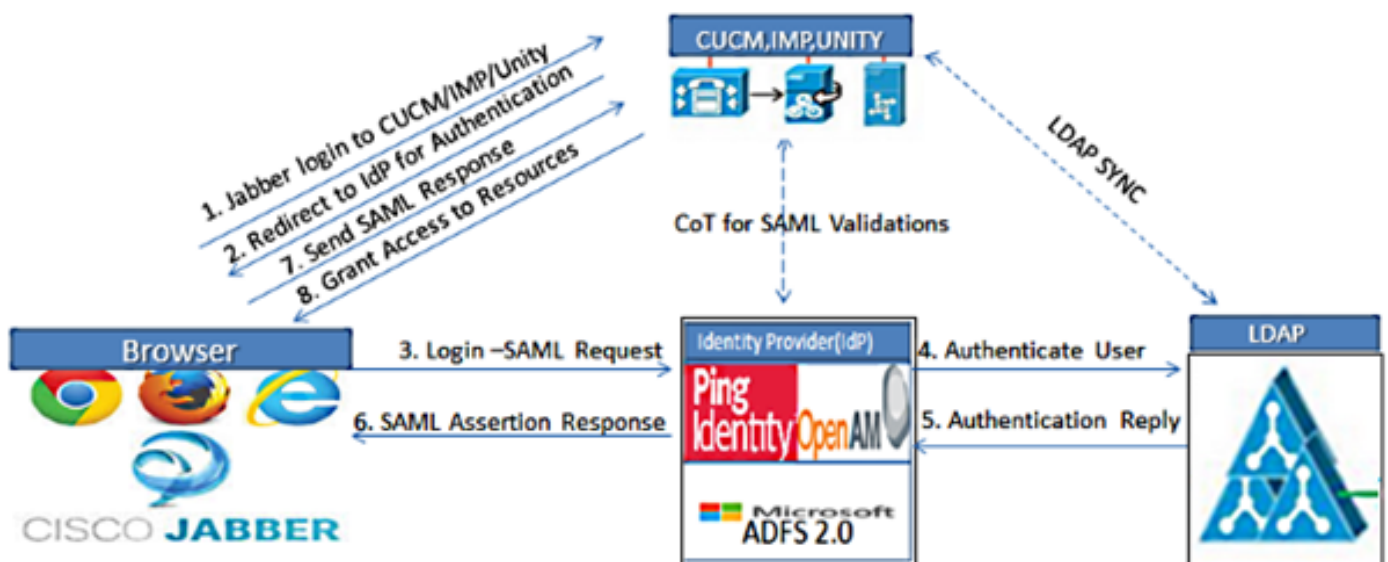
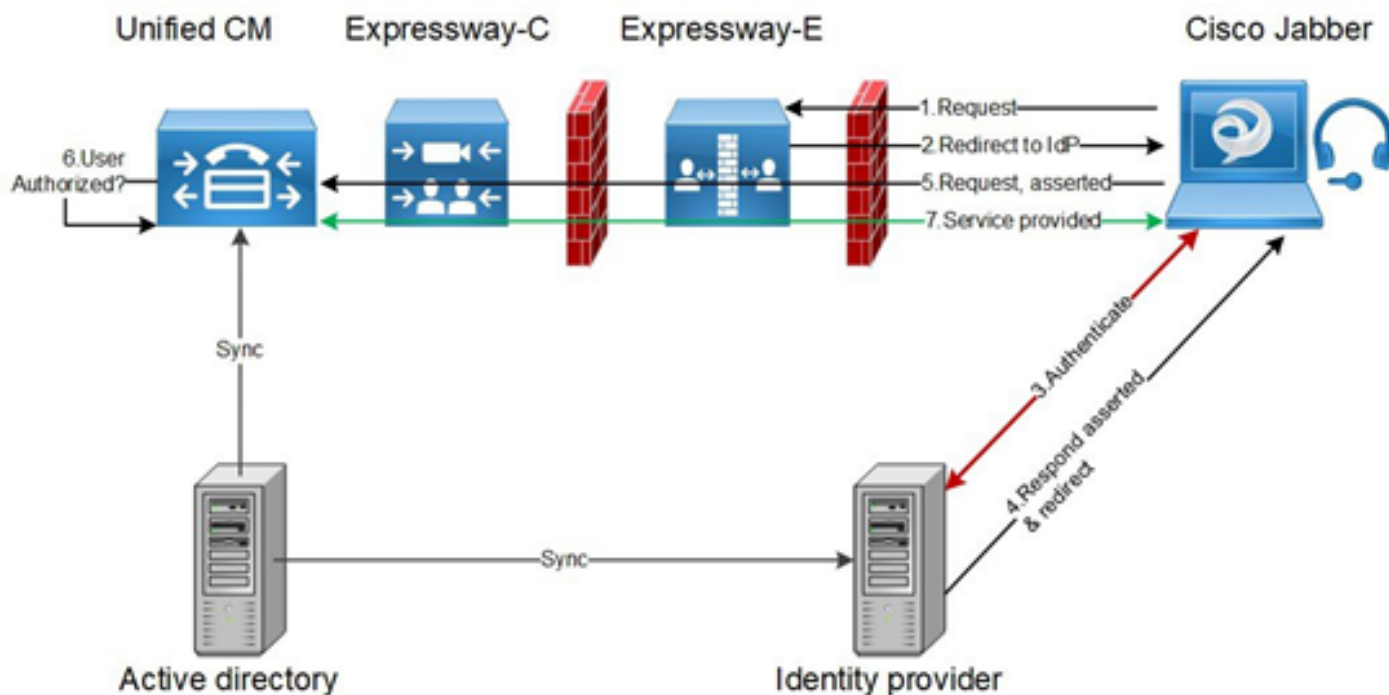


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

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 autenticação 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.

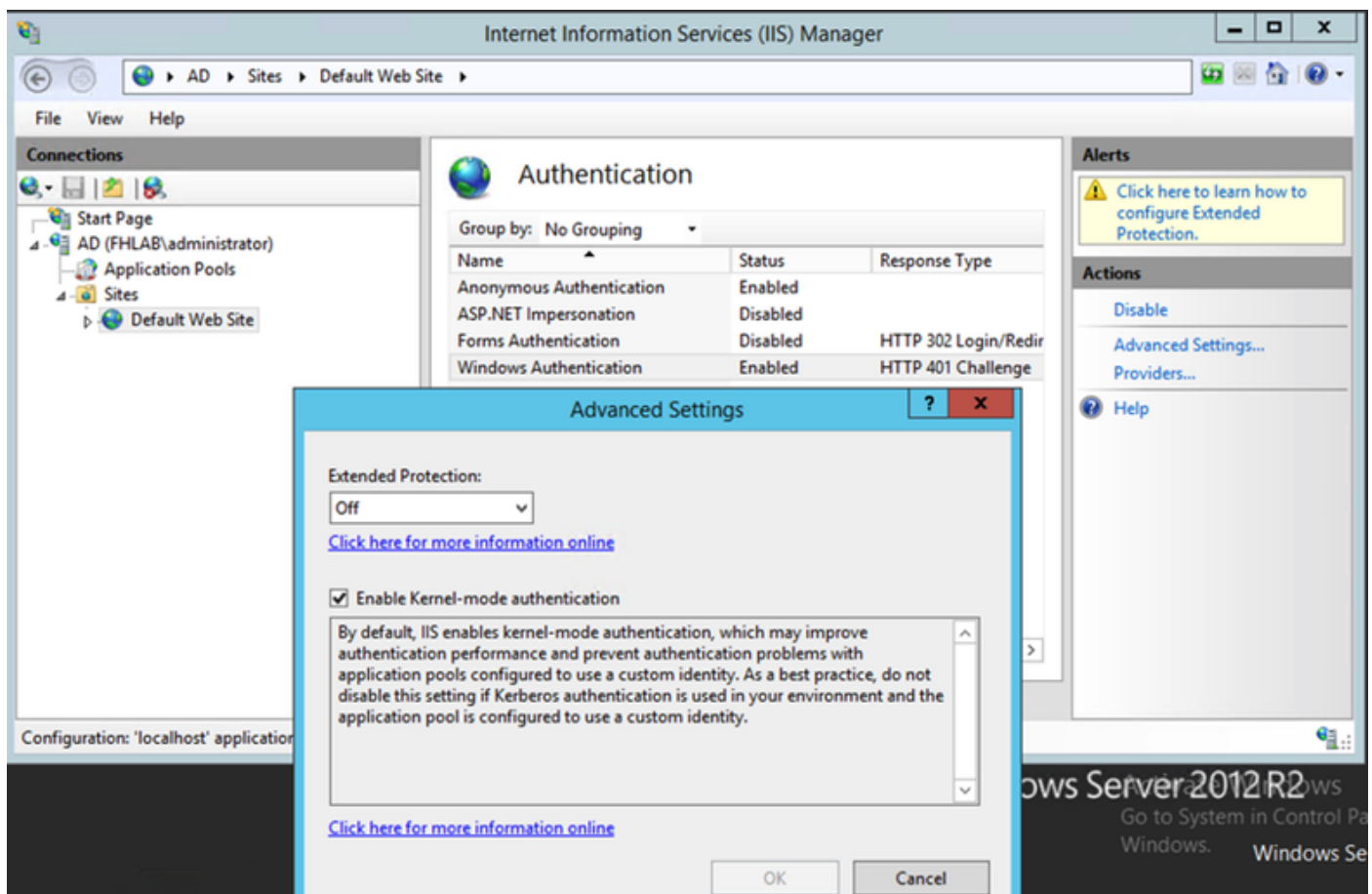
O fluxo de concessão de código de autorização OAuth suporta o uso de tokens de atualização. Isso proporciona uma melhor experiência ao usuário final, pois ele não precisa se autenticar novamente com a mesma frequência (por padrão, 60 dias)

Configurar Kerberos

Selecionar autenticação do Windows

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

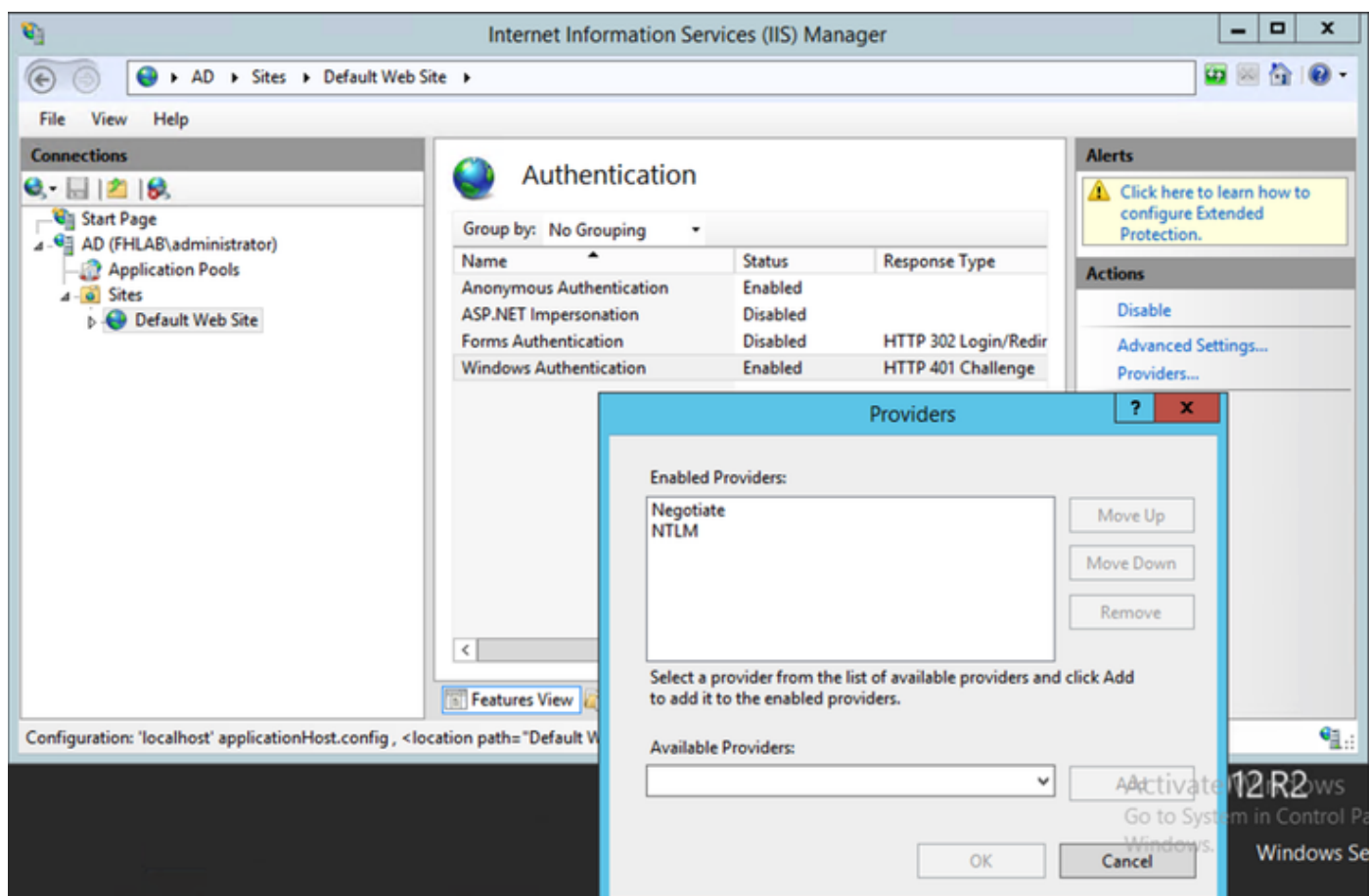
1. Desmarque Ativar autenticação no modo Kernel.
2. Verifique se a proteção estendida está desativada.



O ADFS suporta o Kerberos NTLM

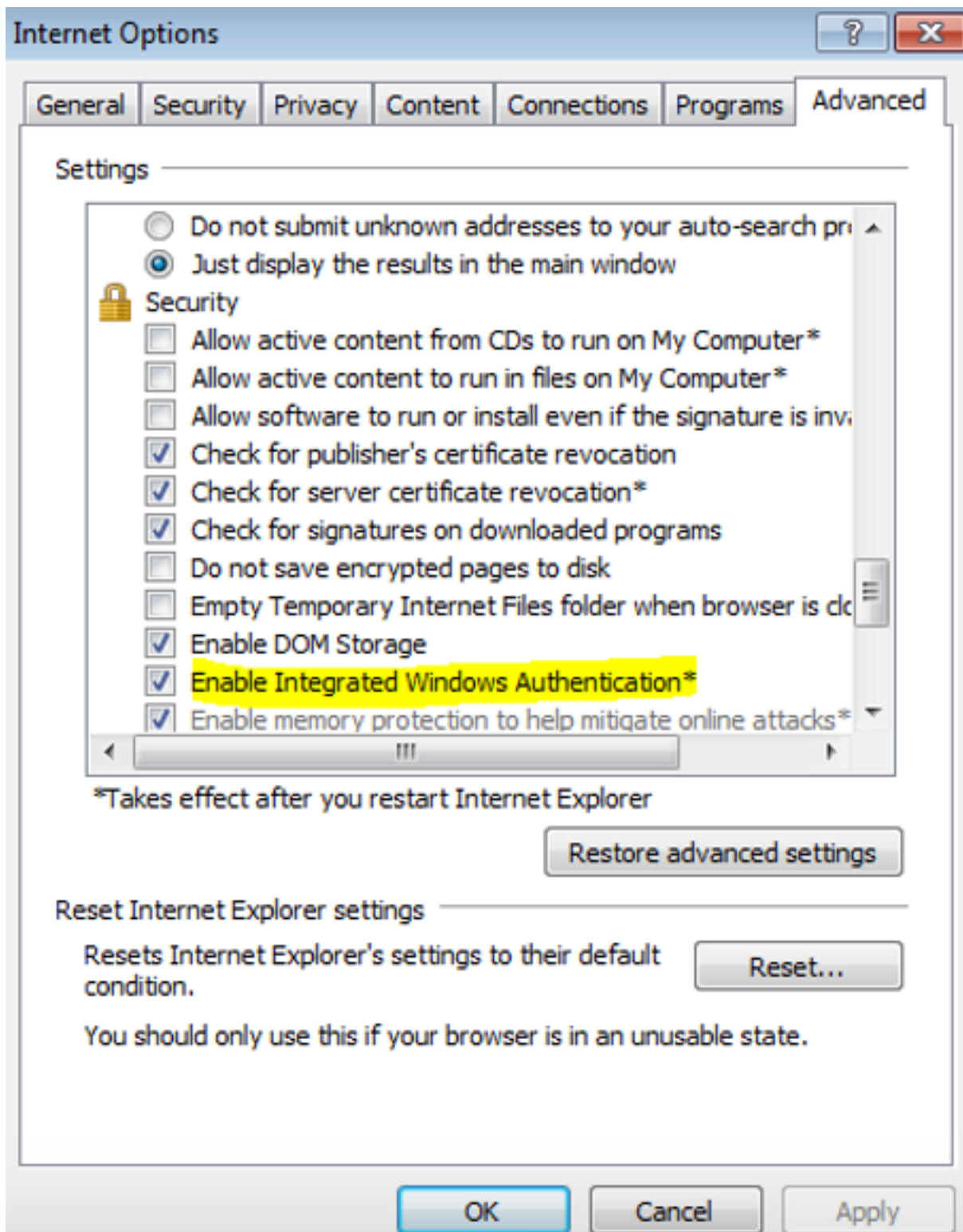
Certifique-se de que o AD FS Versão 3.0 suporta o protocolo Kerberos e o protocolo NT LAN Manager (NTLM) porque todos os clientes não Windows não podem usar Kerberos e dependem do NTLM.

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

