ADFS Server Setup Documentation

Help Desk Technology International Corporation

http://www.servicepro.solutions

Table of Contents

1. Introduction

This document outlines configuring ADFS Server Settings for use in ServicePRO.

Active Directory Federation Service (ADFS) is a software component provided by Microsoft that allows for login using active directory credentials.

From Microsoft's *Developer Network* page on AD FS:

> AD FS is a standards-based service that allows the secure sharing of identity information between trusted business partners (known as a federation) across an extranet. When a user needs to access a Web application from one of its federation partners, the user's own organization is responsible for authenticating the user and providing identity information in the form of "claims" to the partner that hosts the Web application. The hosting partner uses its trust policy to map the incoming claims to claims that are understood by its Web application, which uses the claims to make authorization decisions.

2. ADFS Server Settings – Server, End Points and Claims

The following items need to be configured as a prerequisite for single-sign on (SSO) using ADFS:

1. A Windows Server 2012 or Windows Server 2012 R2
2. Active Directory present, where each user has an email address attribute
3. A Service Socket Layer (SSL) certificate, used for communications between federation servers and clients
4. Certificate fingerprint
5. DNS entry configured for the federation server
6. IIS server installed

Configuring ADFS

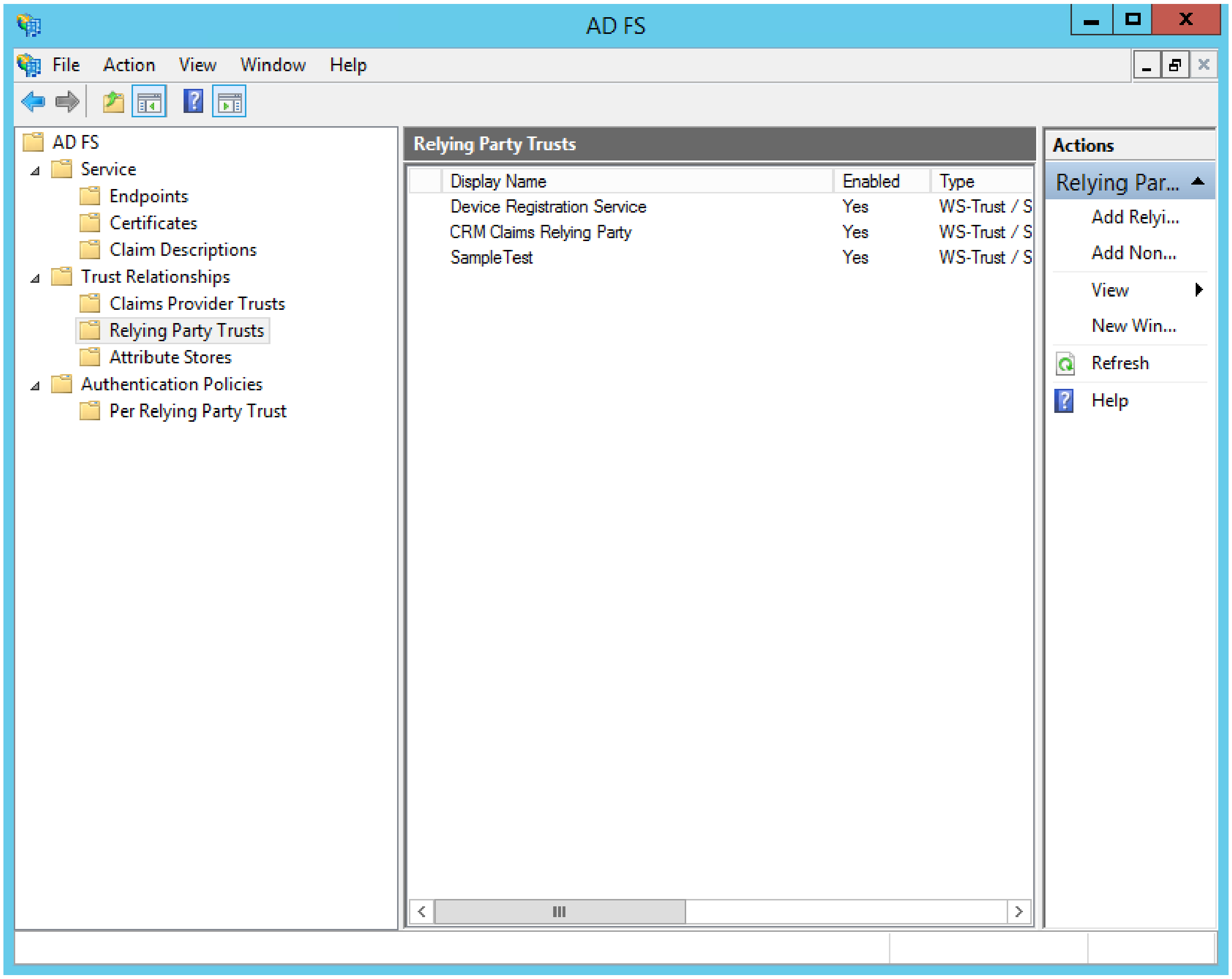
For instructions on configuring the ADFS, please refer to Microsoft's Developer Network page on Deploying and Configuring AD FS.

When the ADFS is fully configured, open the "AD FS Management" console from the installed programs.

A. Instructions for Adding Relying Party Trust

Step 1: Trust Relationships Node - Relying Party Trust Node

In the “**Trust Relationships**” node, select “**Relying Party Trust**”.



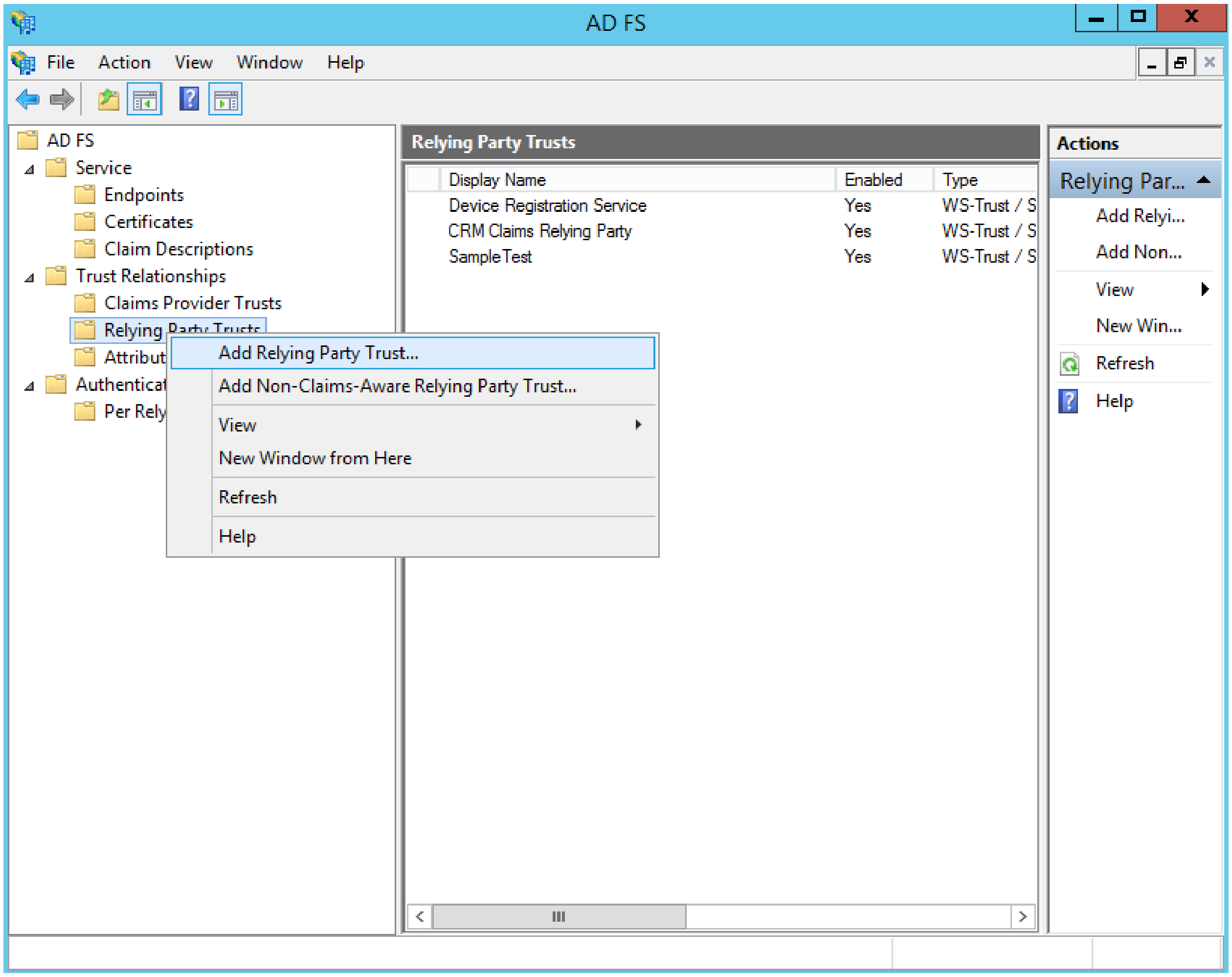
Relying Party Trusts

Display Name	Enabled	Type
Device Registration Service	Yes	WS-Trust / S
CRM Claims Relying Party	Yes	WS-Trust / S
SampleTest	Yes	WS-Trust / S

Step 2: Add Relying Party Trust

Right-click on an item under “**Trust Relationships**” and select “**Add Relying Party Trust...**”

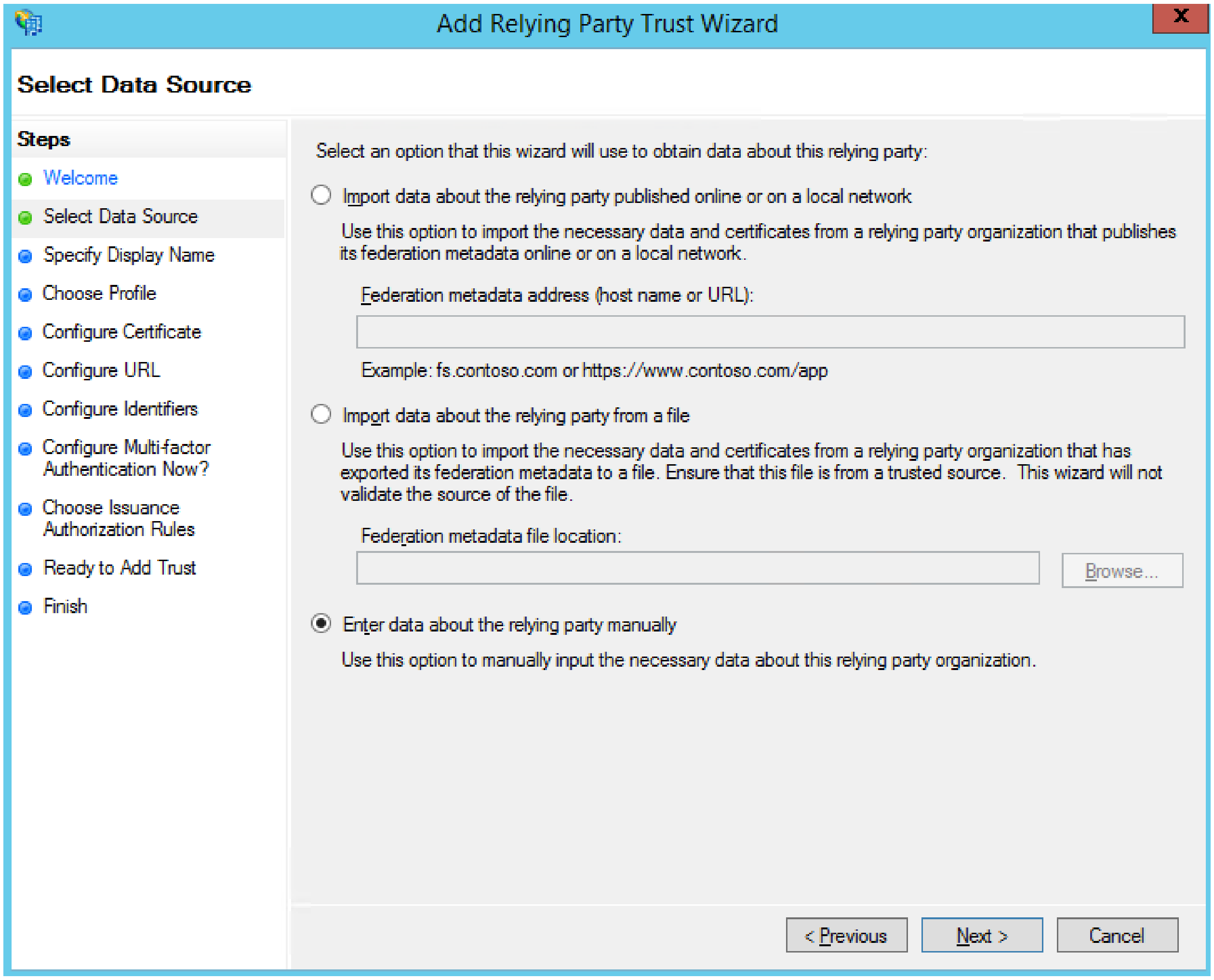
Alternatively, in the actions pane on the right, select “**Add Relying Party trust**”.



Display Name	Enabled	Type
Device Registration Service	Yes	WS-Trust / S
CRM Claims Relying Party	Yes	WS-Trust / S
SampleTest	Yes	WS-Trust / S

Step 3: Select Data Source

Select the option "**Enter Data about the relying party manually**".



Add Relying Party Trust Wizard

Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

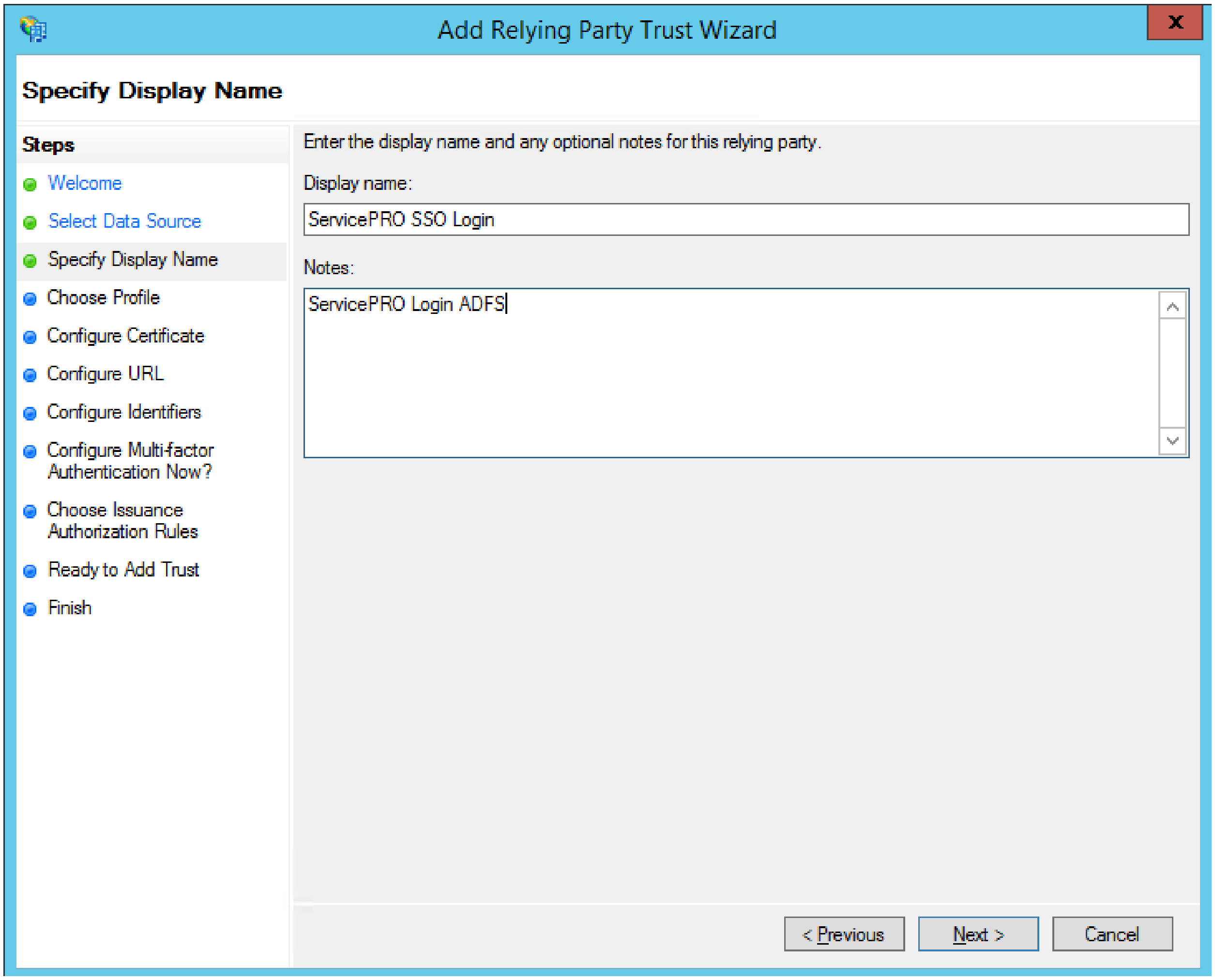
Federation metadata file location:

● Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

Step 4: Specify Display Name

Enter a *Display name* and write notes for the relying party.



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

Display name:

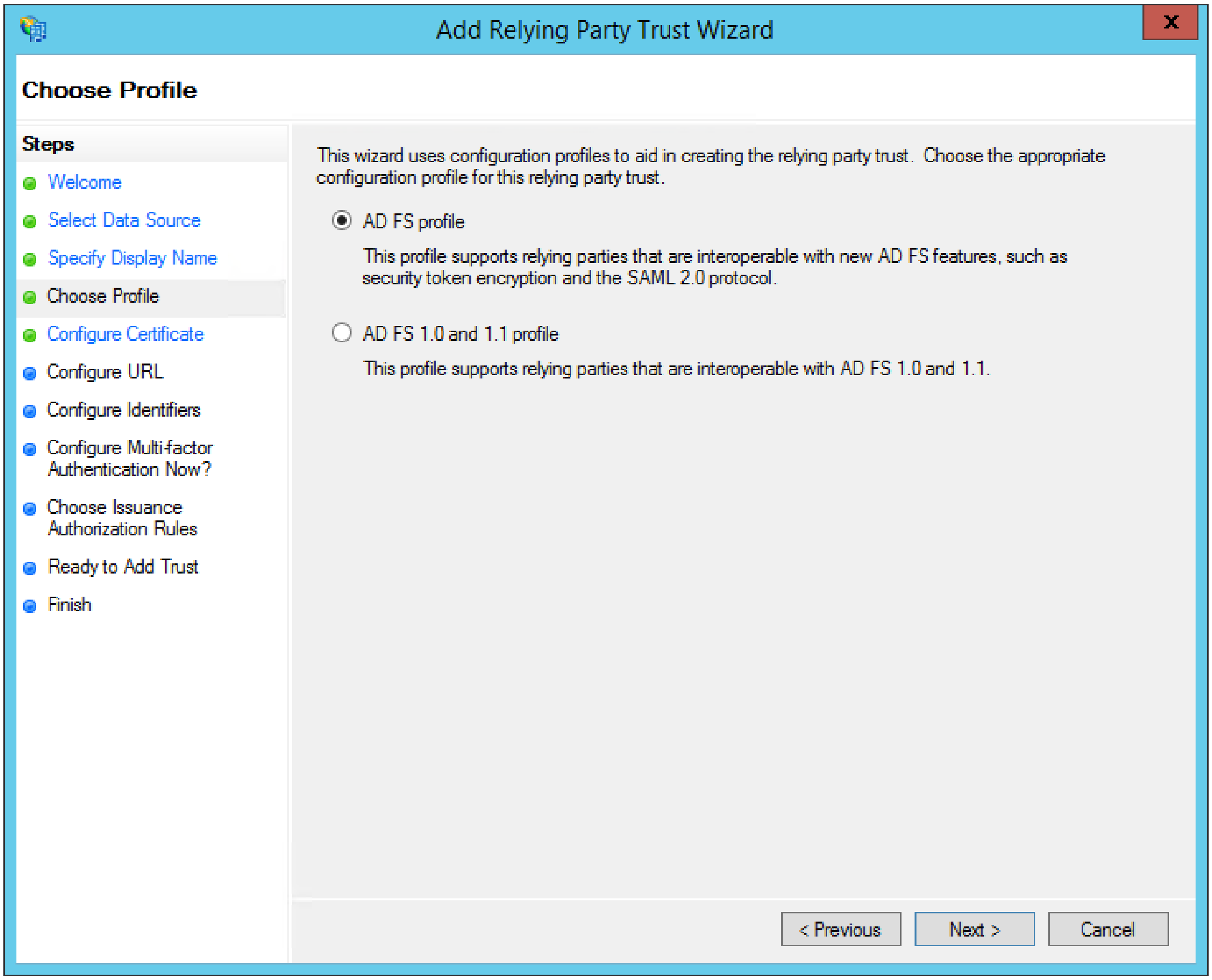
ServicePRO SSO Login

Notes:

ServicePRO Login ADFS

Step 5: Choose Profile

Select the "AD **FS Profile**" radio button.



This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.

● AD FS profile

This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.

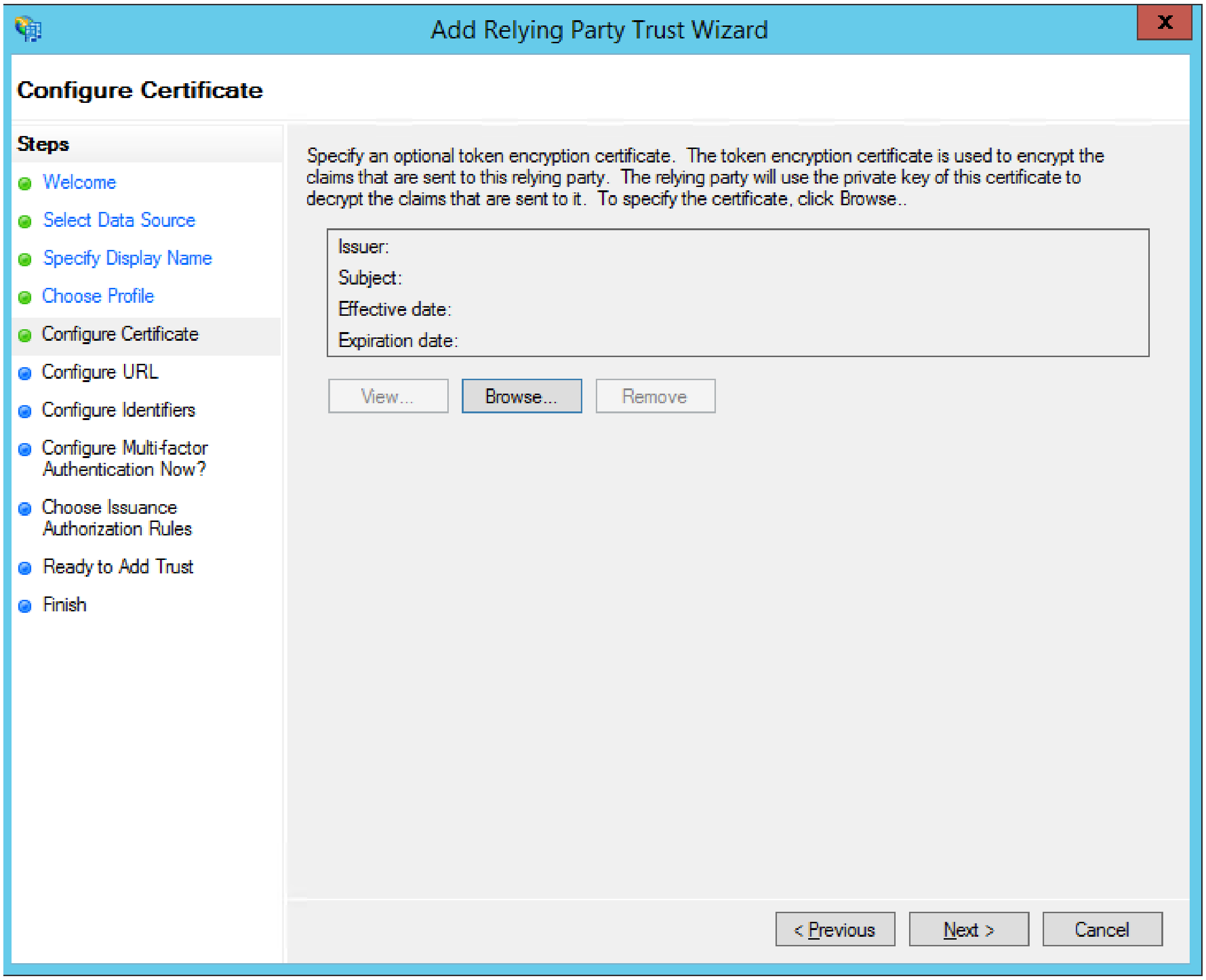
○ AD FS 1.0 and 1.1 profile

This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

Step 6: Configure Certificate

Select “**Next**”.

NOTE: Do not select a token encryption certificate. Defining a certificate here will prevent proper communication with ServicePRO.

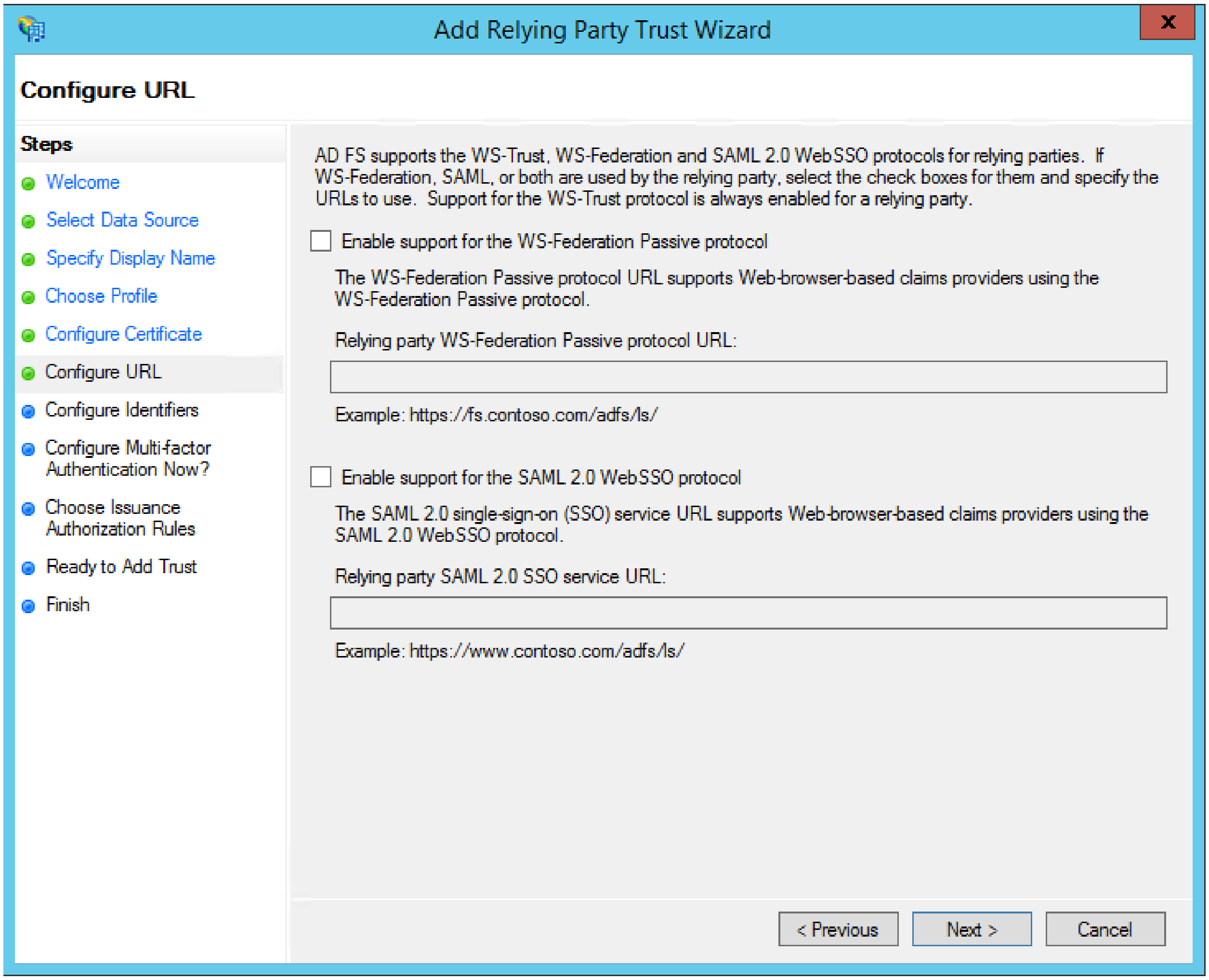


Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse..

Issuer:
Subject:
Effective date:
Expiration date:

Step 7: Configure URL

Select “**Next**”.



Add Relying Party Trust Wizard

Configure URL

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

□ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

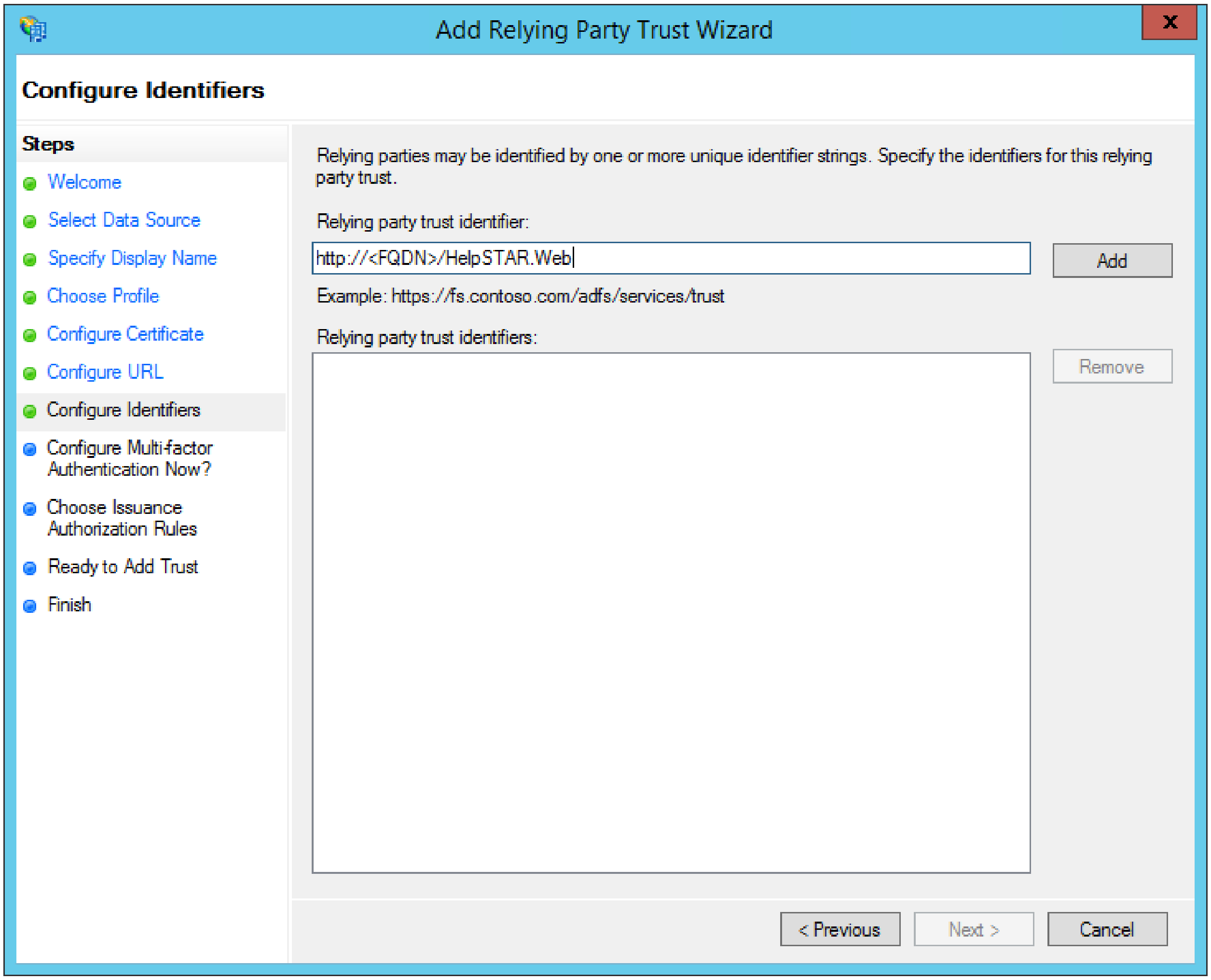
Relying party SAML 2.0 SSO service URL:

Example: https://www.contoso.com/adfs/ls/

Step 8: Configure Identifiers

Enter the *Relying party trust identifier* (replace <FQDN> with domain information), and select the "**Add**" button.

NOTE: Relying party trust Identifier URLs must be identical to the URLs displayed on the ServicePRO endpoint configuration form when added to ADFS (including case sensitivity). To ensure it is identical, users may copy and paste the URL from the form.



Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

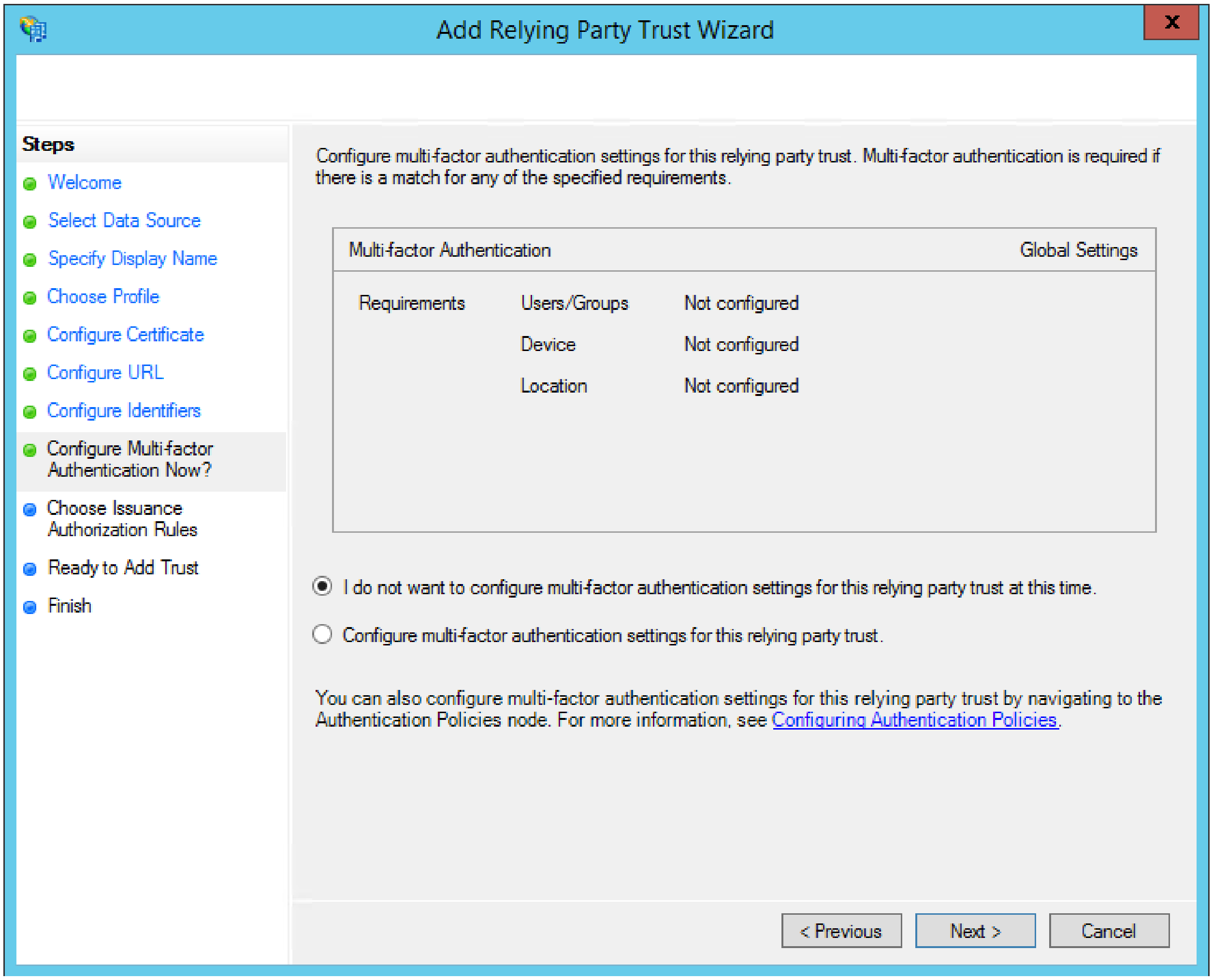
Relying party trust identifier: http://<FQDN>/HelpSTAR.Web

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

Step 9: Configure Multi-Factor Authentication Now?

Select “**Next**”.



Add Relying Party Trust Wizard

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

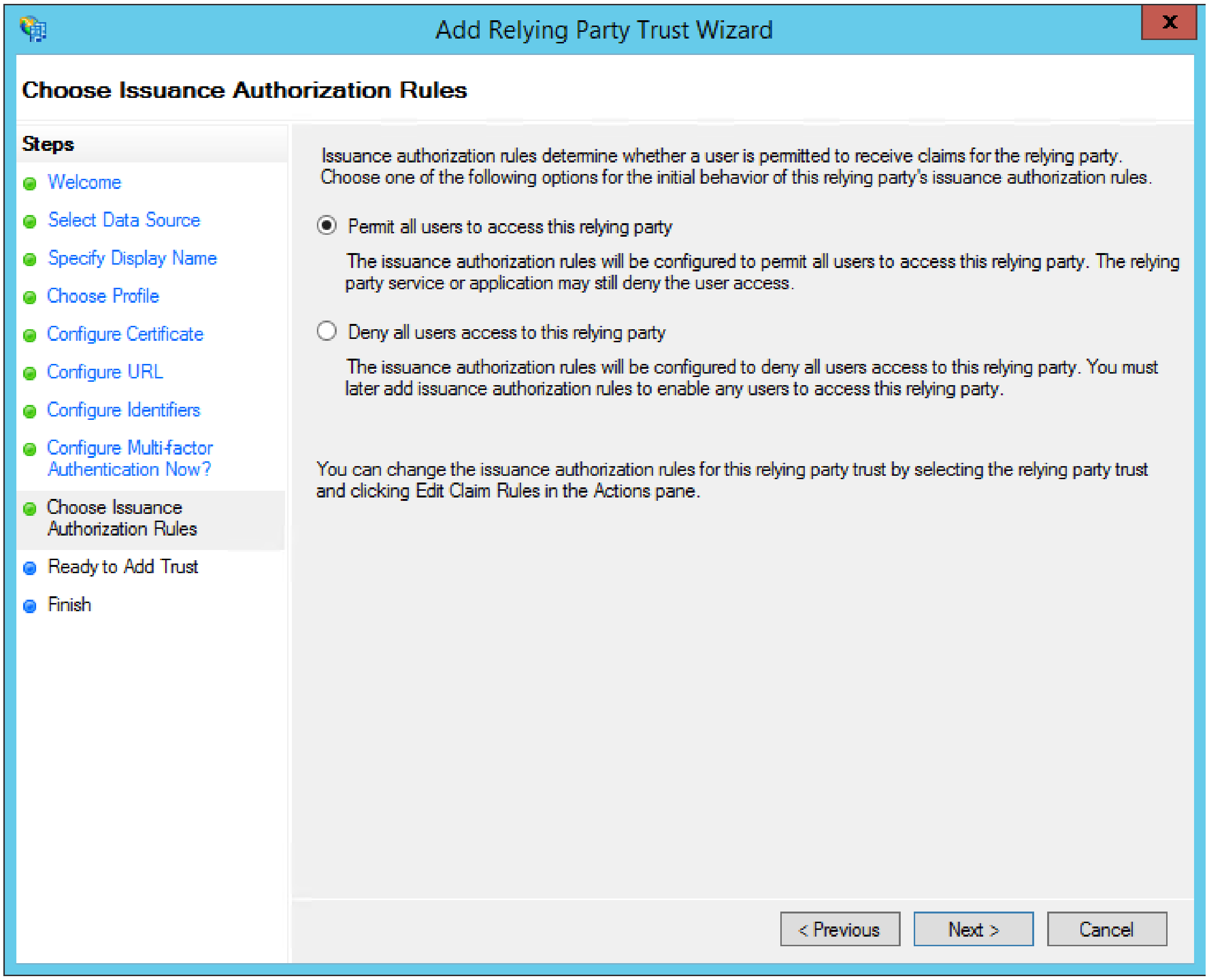
● I do not want to configure multi-factor authentication settings for this relying party trust at this time.

○ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see Configuring Authentication Policies.

Step 10: Choose Issuance Authorization Rules

Leave the default selected radio button to “**Permit all users to access the relying party**” and select “**Next**”.



Choose Issuance Authorization Rules

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

● Permit all users to access this relying party

The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

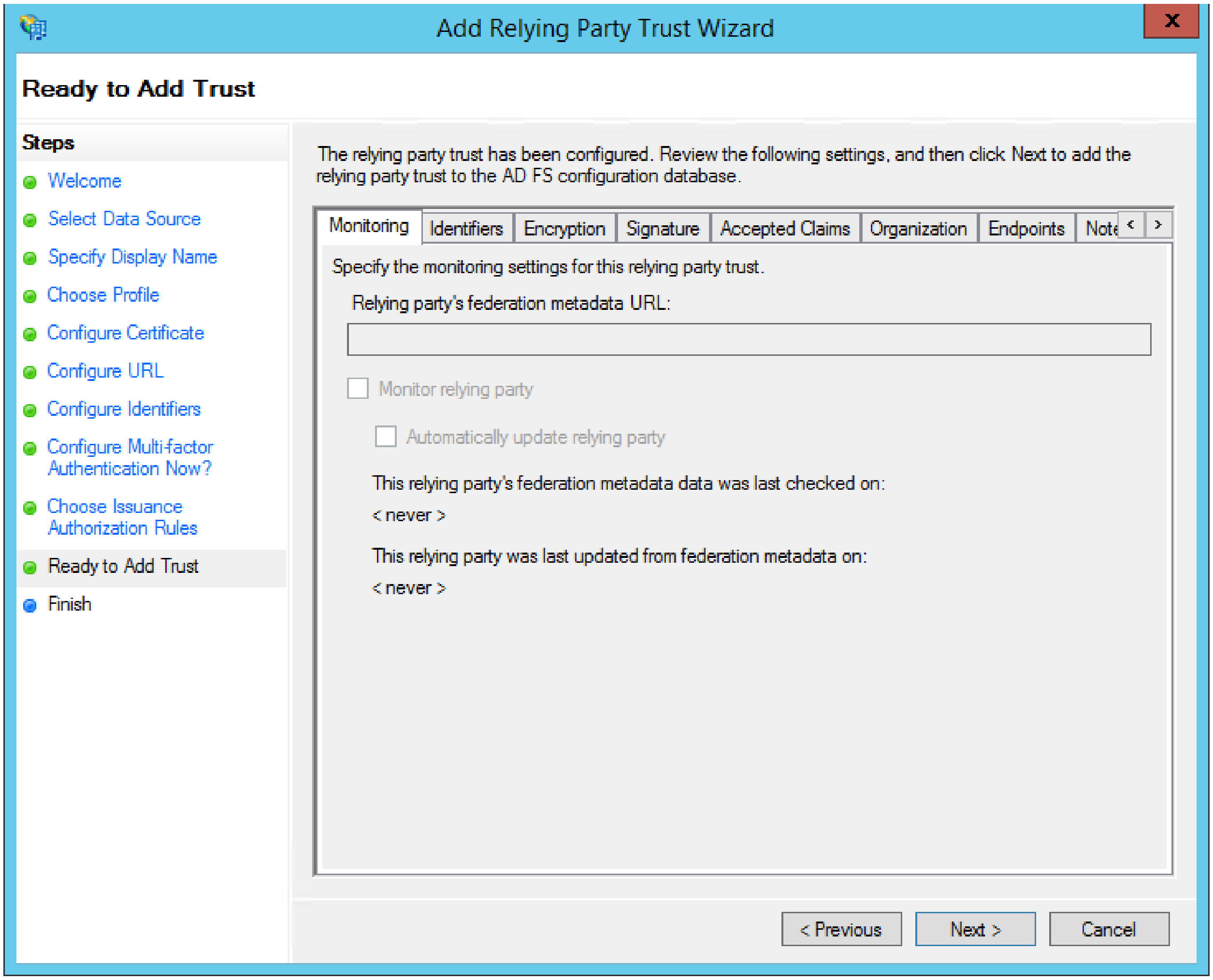
○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

Step 11: Ready to Add Trust

Review the steps and select “**Next**”.



Add Relying Party Trust Wizard

Ready to Add Trust

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

□ Monitor relying party

□ Automatically update relying party

This relying party's federation metadata data was last checked on:

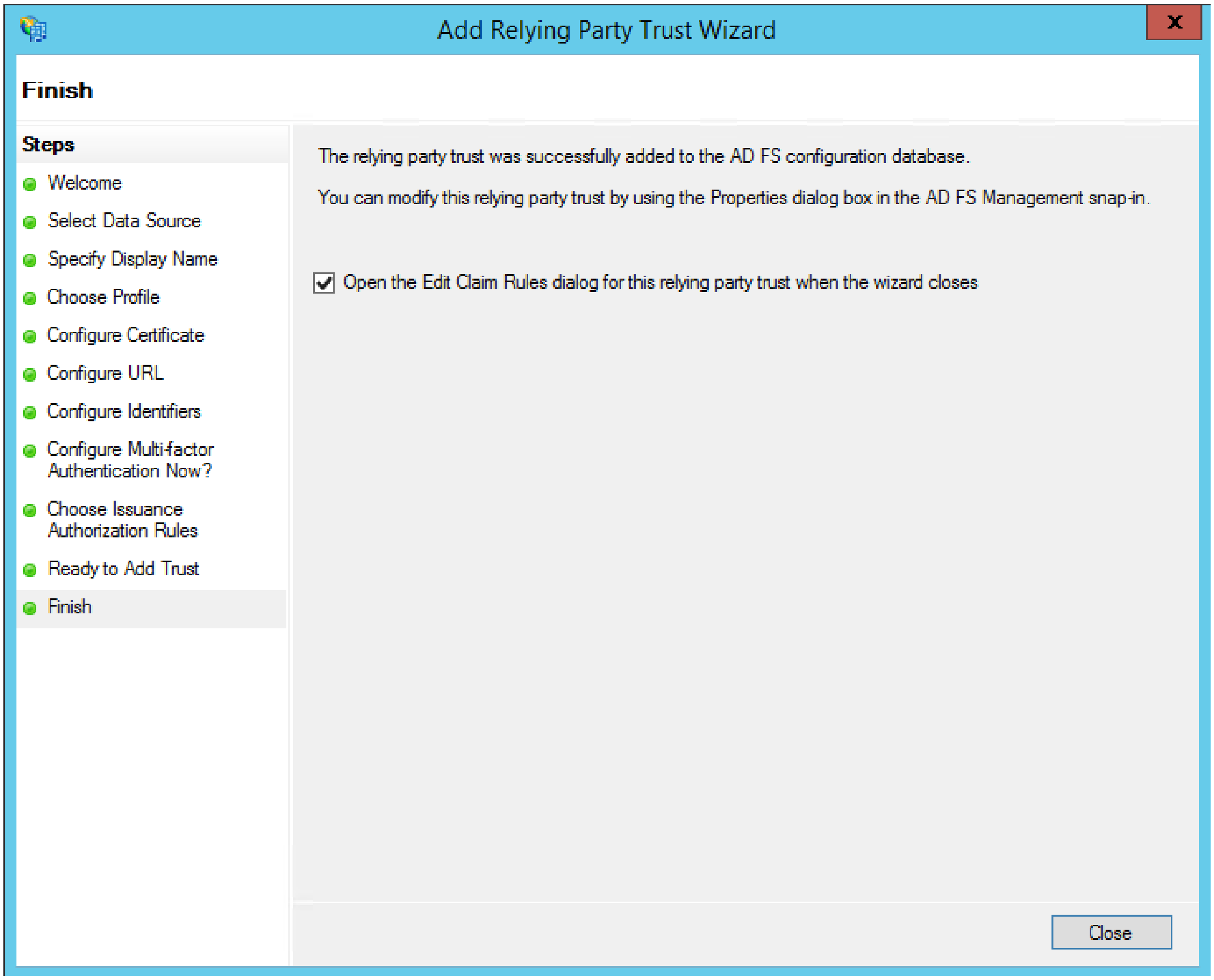
< never >

This relying party was last updated from federation metadata on:

< never >

Step 12: Finish

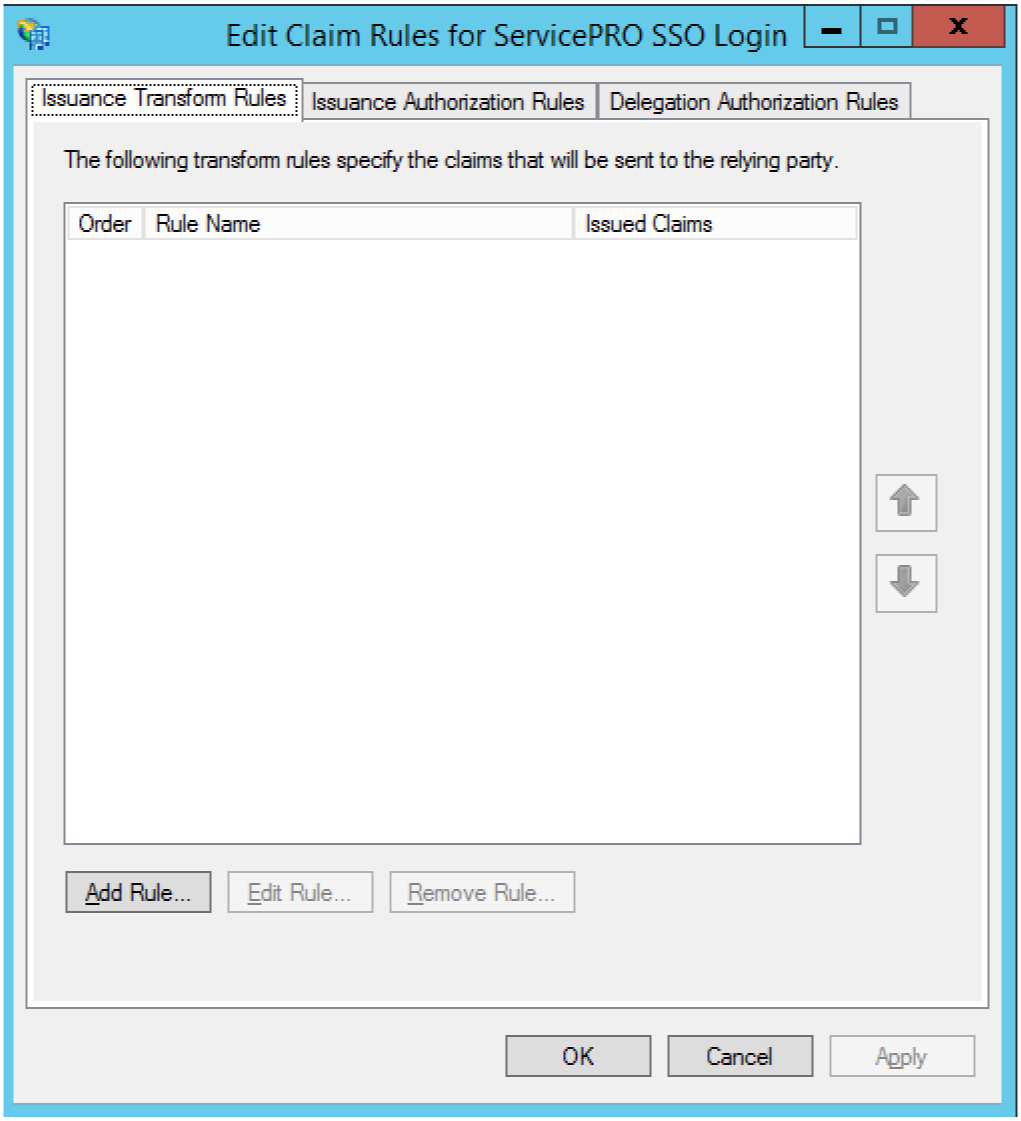
Select the checkbox to open the *Edit Claim Rules* dialog after closing this wizard.



The relying party trust was successfully added to the AD FS configuration database.

You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.

☑ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

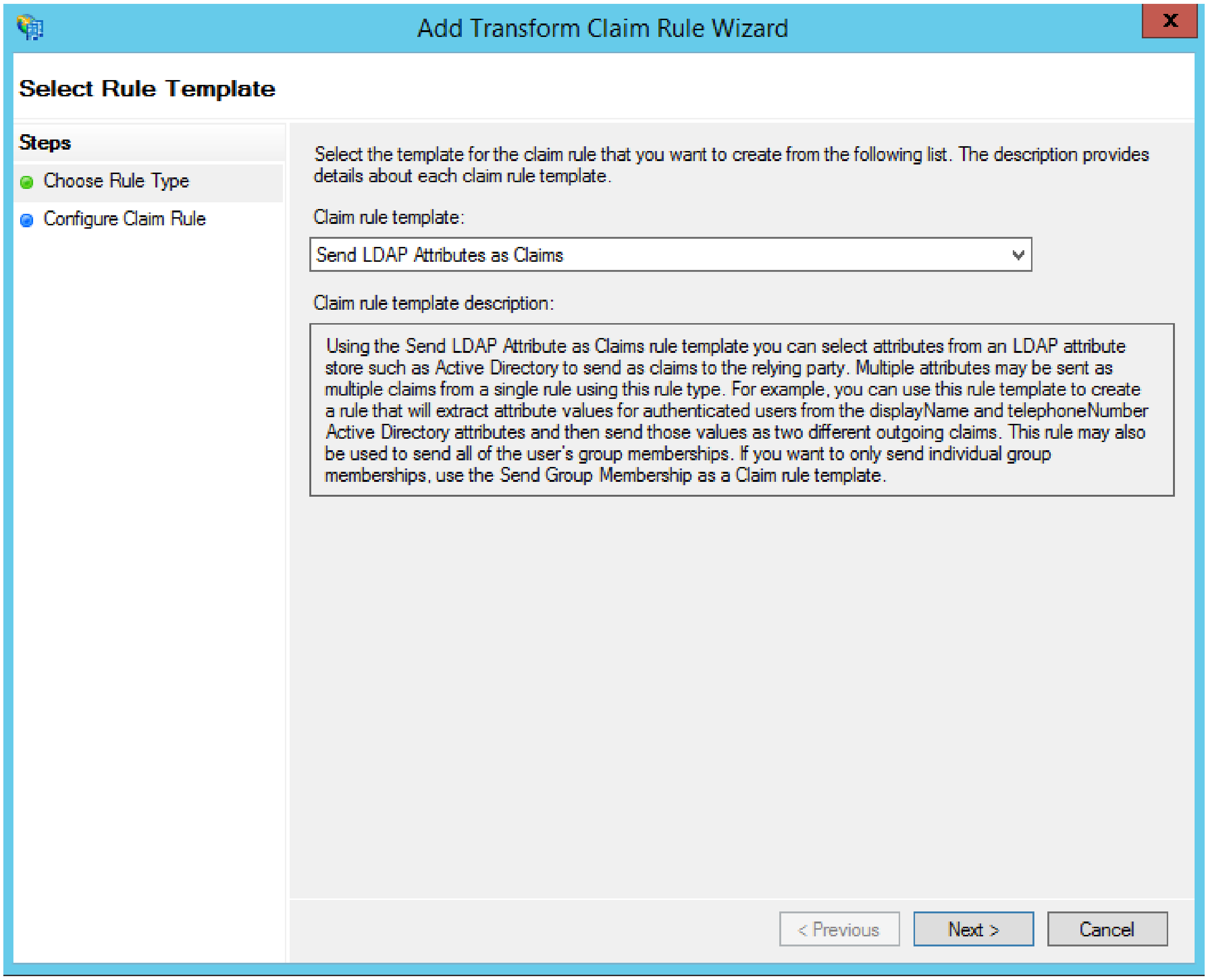


Edit Claim Rules for ServicePRO SSO Login
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims

Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply



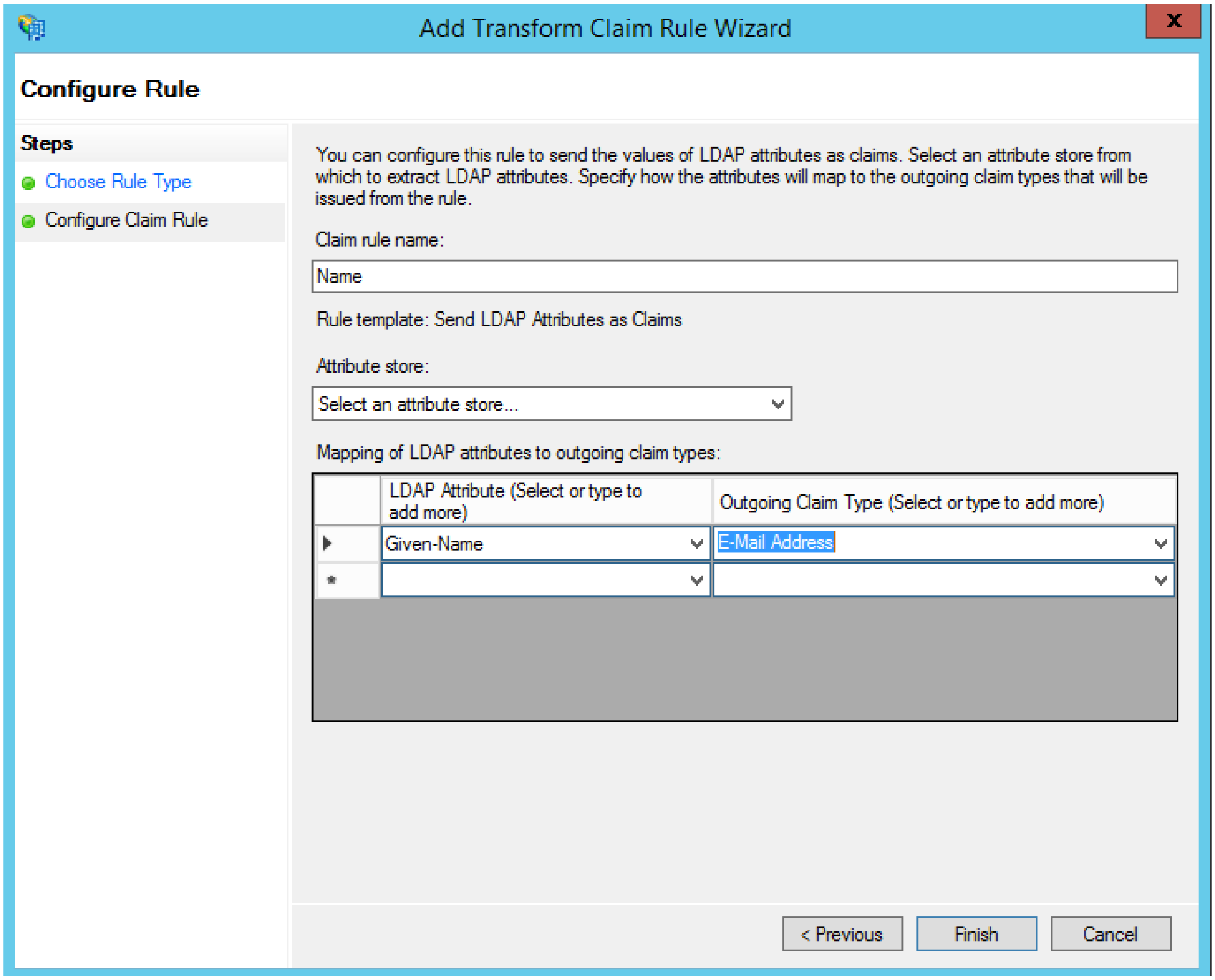
Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.



Configure Rule

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:

Name

Rule template: Send LDAP Attributes as Claims

Attribute store:

Select an attribute store...

Mapping of LDAP attributes to outgoing claim types:

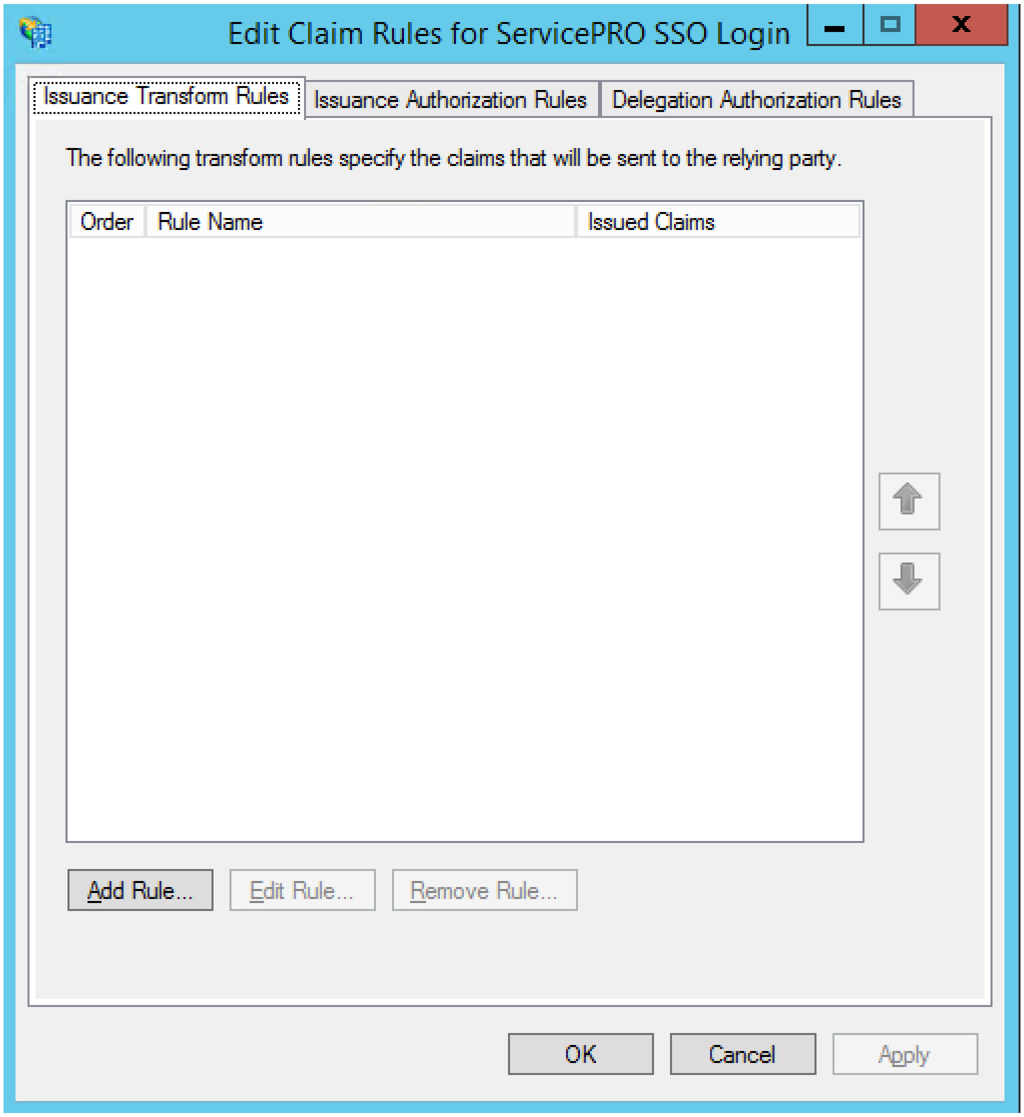
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	Given-Name	E-Mail Address
*		

B. Creating Claims

After the Relying Party Trust has been successfully added, create claims that each partner understands and appropriately mapped in the AD FS trust policy for exchange between federation partners.

Step 1: Edit Claim Rules for ServicePRO SSO Login

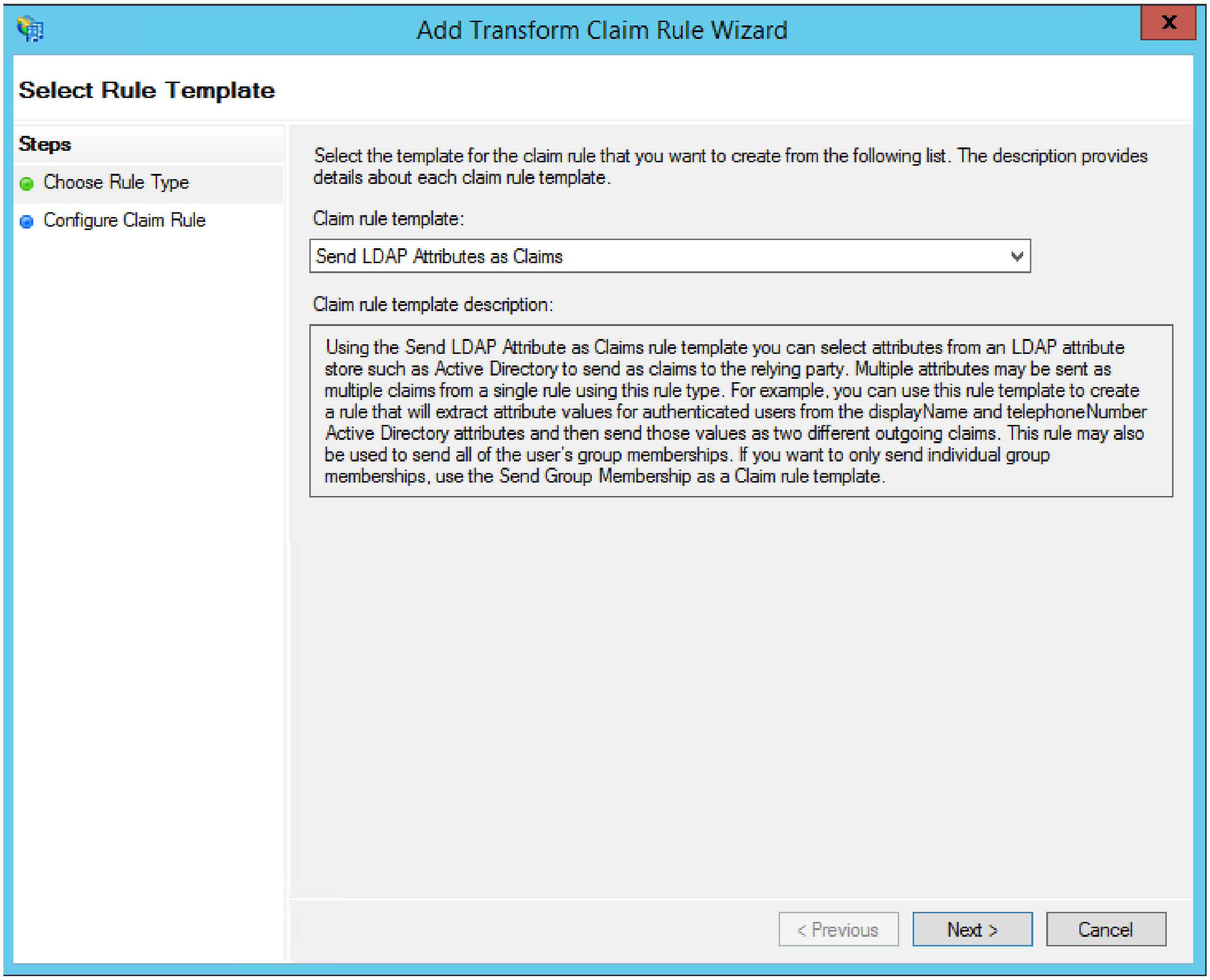
Under the Issuance Transform Rules tab, select "**Add Rule…**"



The following transform rules specify the claims that will be sent to the relying party.

Step 2: Add Transform Claim Rule Wizard

1) Under the “**Claim rule template**” dropdown, select “**Send LDAP Attributes as Claims**”.
2) Select “Next”.



Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

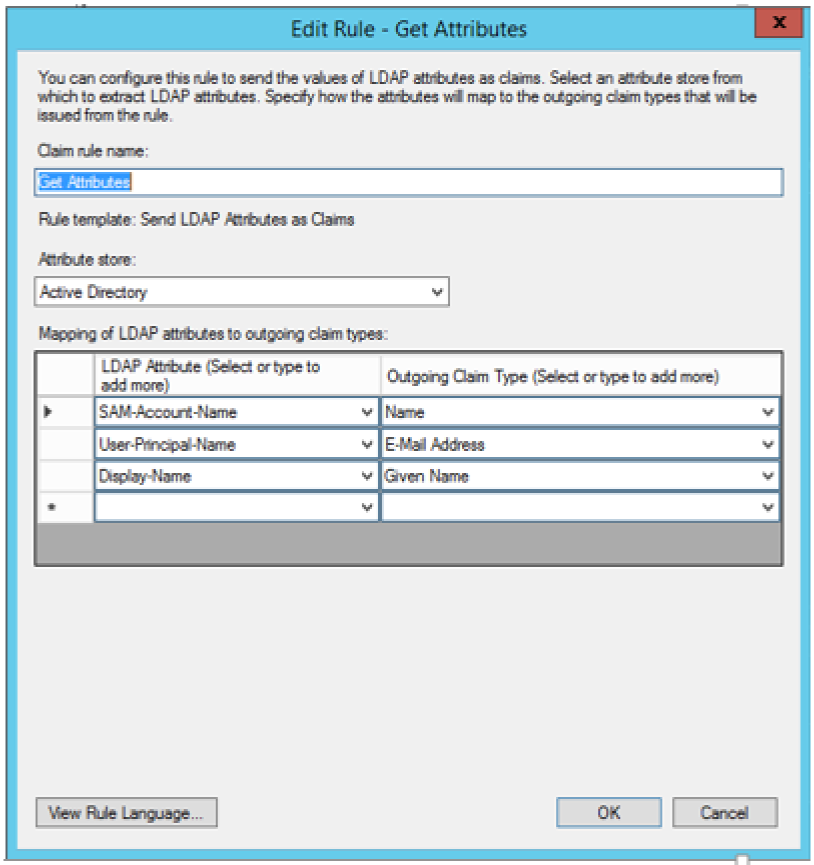
Step 3: Edit Rule – Get Attributes

Enter a name for “Claim rule name”.

In the Attribute store dropdown menu, select “Active Directory”.

In the Grid for “Mapping of LDAP attributes to outgoing claim types”:

1. Select “SAM-Account-Name” from the dropdown list, and in the outgoing claim type, select “Name”.
2. Select “User-Principal – Name” from the dropdown list, and in the outgoing claim type, select “E-mail Address”.
3. Select “Display Name” from the dropdown list, and in the outgoing claim type, select “Given Name”.



Edit Rule - Get Attributes

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: Get Attributes

Rule template: Send LDAP Attributes as Claims

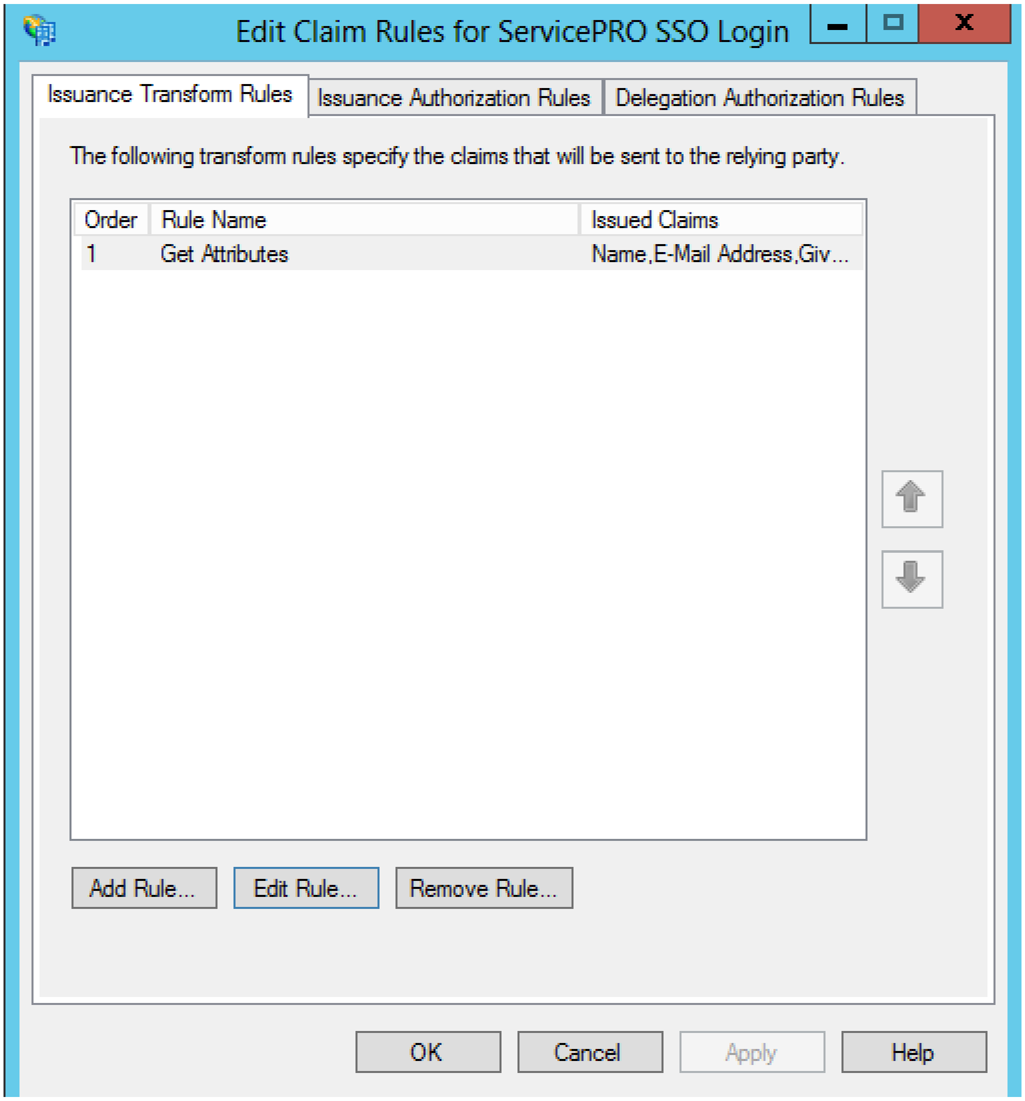
Attribute store: Active Directory

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	Name
	User-Principal-Name	E-Mail Address
	Display-Name	Given Name
*		

Step 4: Edit Claim Rules for ServicePRO SSO Login

Select “Apply” and “OK” to save changes.


Edit Claim Rules for ServicePRO SSO Login
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply
Help

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Get Attributes	Name,E-Mail Address,Giv...

3. Minimum Claims to be configured for successful ADFS SSO authentication

The following are the minimum claims needed to be configured for successful ADFS SSO authentication:

1. LDAP Attribute -> Outgoing Claim
2. SAM-Account-Name -> Name,
3. User-Principal-Name -> Email Address,
4. Display-Name -> Given Name.

4. Active Directory Fields mapping to Claims

Active Directory Field	ADFS Claim
Mail	emailaddress
Name	name
givenName	givenname
telephoneNumber	homephone
Pager	otherphone
Mobile	mobilephone
Department	AD Sync selected

5. Resources

1. **For more details on the types of claim rules:**
   - https://technet.microsoft.com/en-us/library/ee913563(v=ws.11).aspx
2. **For more details on the role of claims:**
   - https://technet.microsoft.com/en-us/library/ee913589(v=ws.11).aspx
3. **[Internal] To Configure ADFS:**
   - https://seroter.wordpress.com/2013/04/22/using-active-directory-federation-services-to-authenticate-authorize-node-js-apps-in-windows-azure/
4. **Steps to configuring ADFS (end to end):**
   - https://blogs.technet.microsoft.com/canitpro/2015/09/11/step-by-step-setting-up-ad-fs-and-enabling-single-sign-on-to-office-365/
5. **Troubleshooting steps to be followed:**
   - https://technet.microsoft.com/en-us/library/adfs2-troubleshooting-things-to-check(v=ws.10).aspx