Adding a Relying Party in ADFS 3.0

Prerequisites

* Note that followings are the key information should be provided by the application owner.

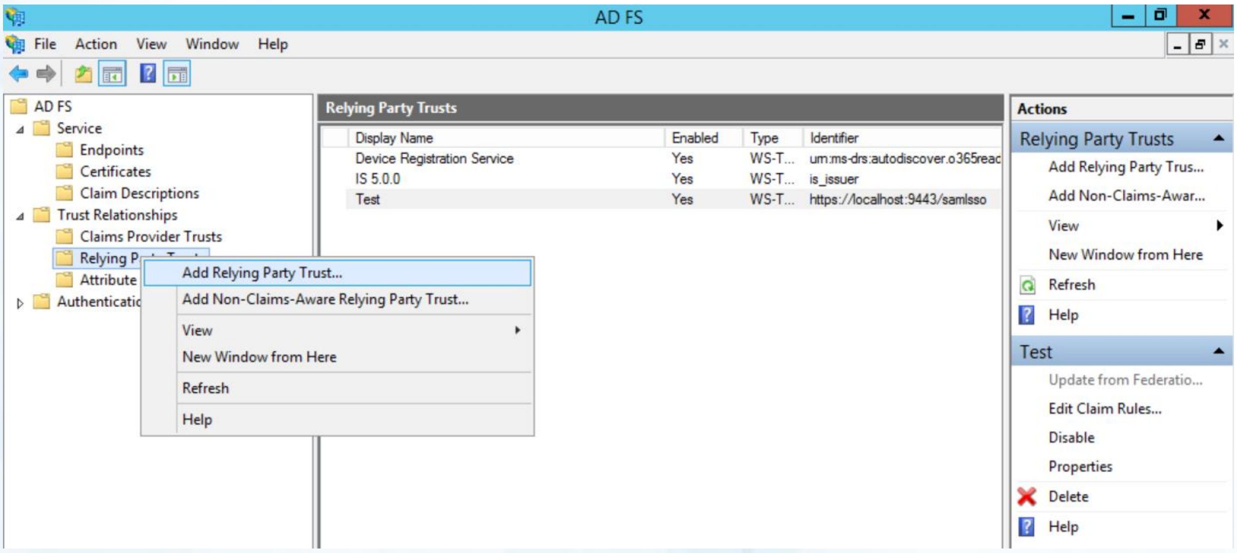
Client_id	**Ex : uo7gBYHg_qA7yAQdmh6otn5MUfwa**
Client_id redirect URL	Ex: https://apidev.oasys.lk:9443/carbon/
Commonauth endpoint	Ex: https://apidev.oasys.lk:9443/token
Relying party trust identifier	Ex: wso2km21AzureLive
Certificate	Wso2 APIM Certificate (.crt)

* Below information should be provided by ADFS owner

Trusted URL	**Ex : https://<AD_FS_server>/adfs/ls**
Metadata URL	Ex: http://<AD_FS_server>/adfs/services/trust

Steps

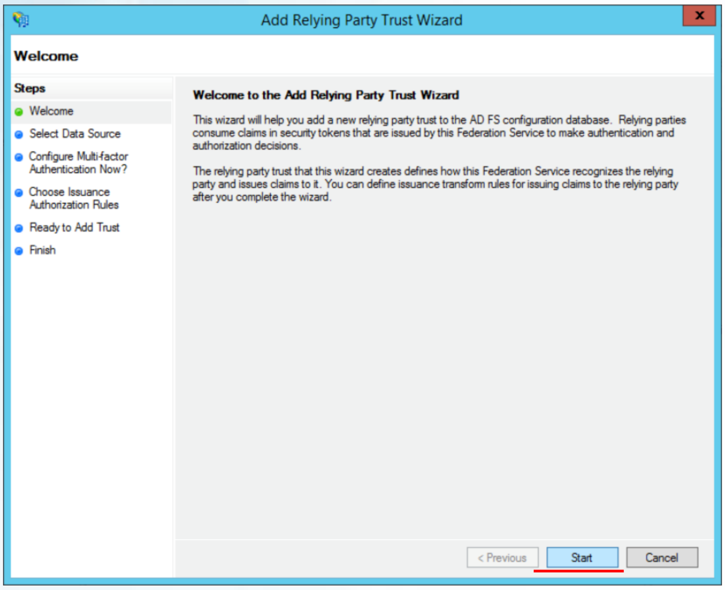
In ADFS Management UI expand Trust Relationship, right click on Relying Party Trust and select Add Relying Party Trust…



Relying Party Trusts

Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-T...	urn:ms-drs:autodiscover.o365reac
IS 5.0.0	Yes	WS-T...	is_issuer
Test	Yes	WS-T...	https://localhost:9443/samlsso

Follow the wizard as shown below



Add Relying Party Trust Wizard

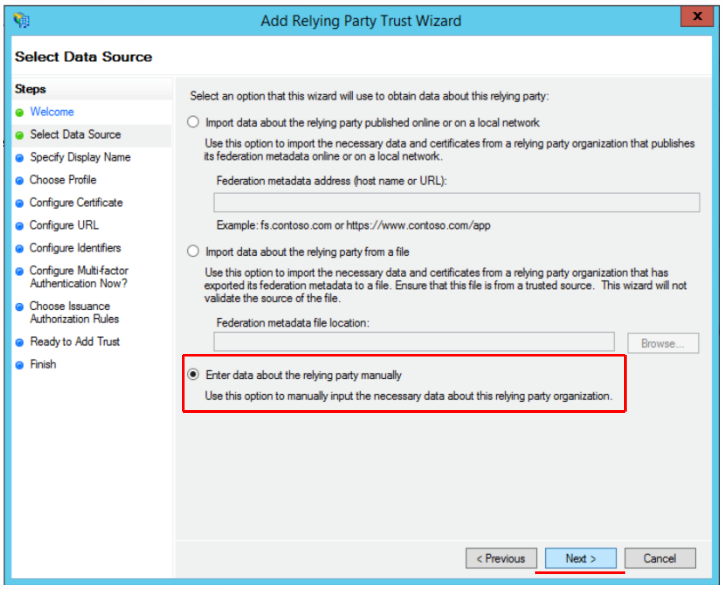
Welcome

Steps
- Welcome
- Select Data Source
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Welcome to the Add Relying Party Trust Wizard

This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.



Add Relying Party Trust Wizard

Select Data Source

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

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

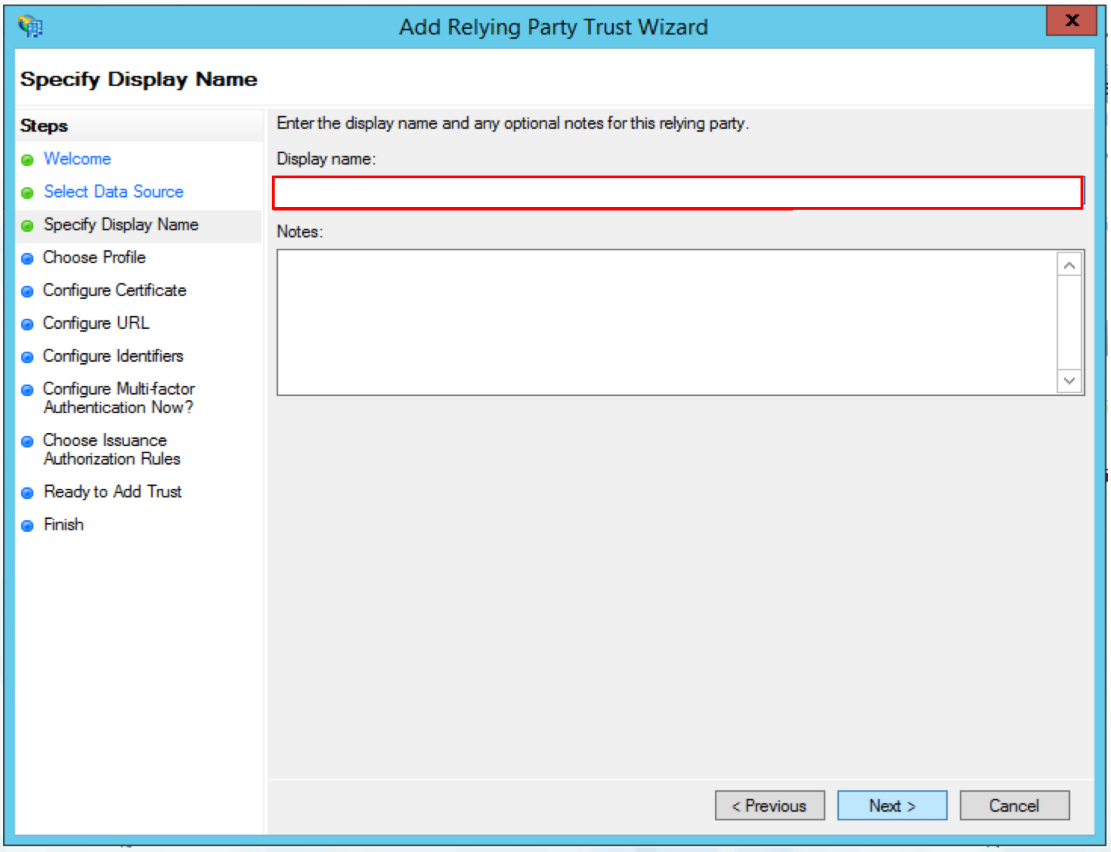
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

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.

Type a desired display name (wso2km21AzureLive) for the relying party and click **Next**



Add Relying Party Trust Wizard

Specify Display Name

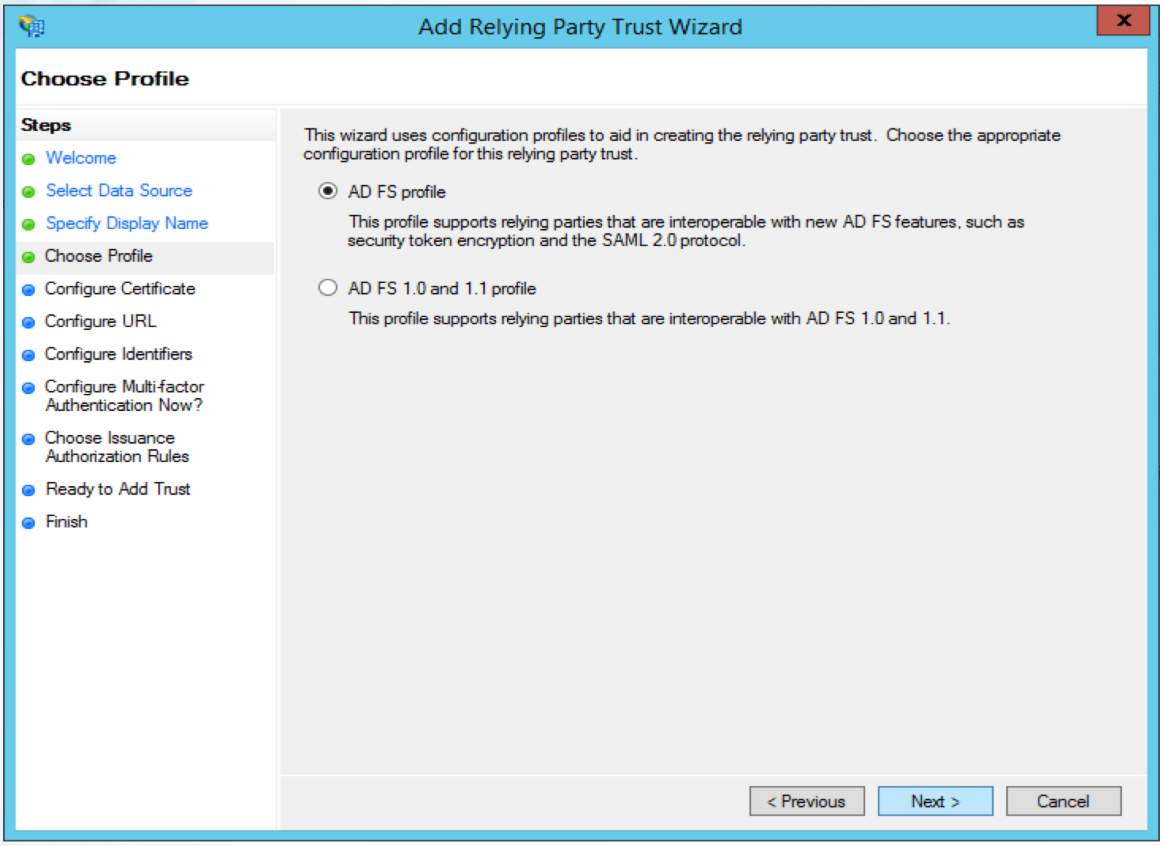
Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

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

Display name:

Notes:

Select AD FS Profile and Click Next.



Add Relying Party Trust Wizard

Choose Profile

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

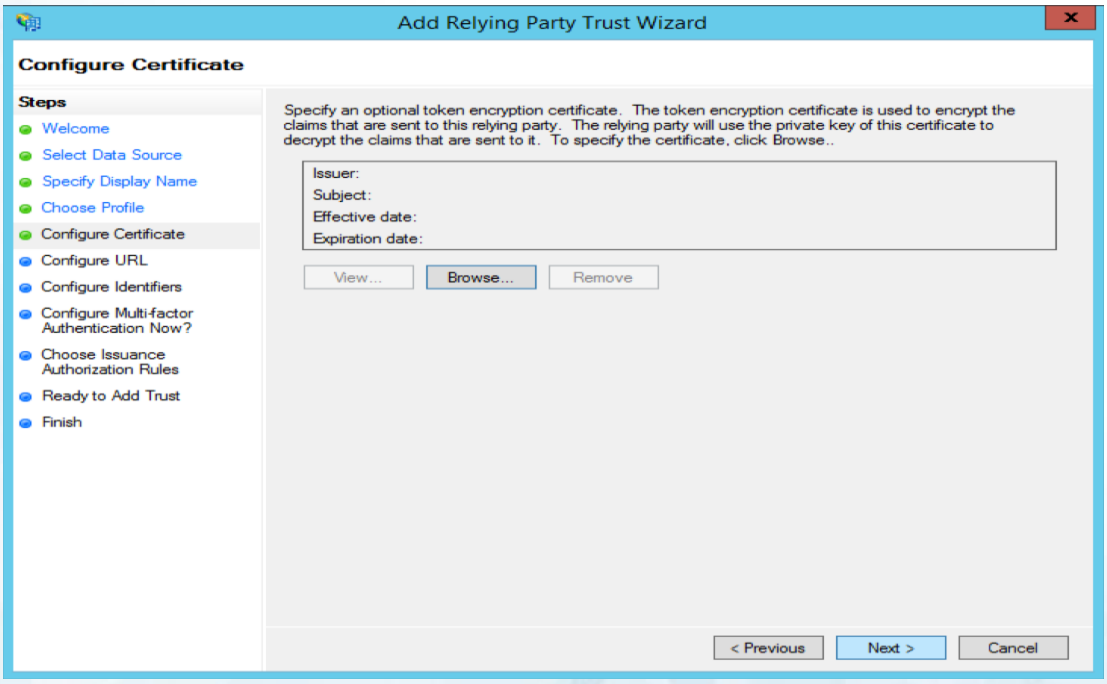
● AD FS profile

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.

We are not using an encryption certificate so click Next.



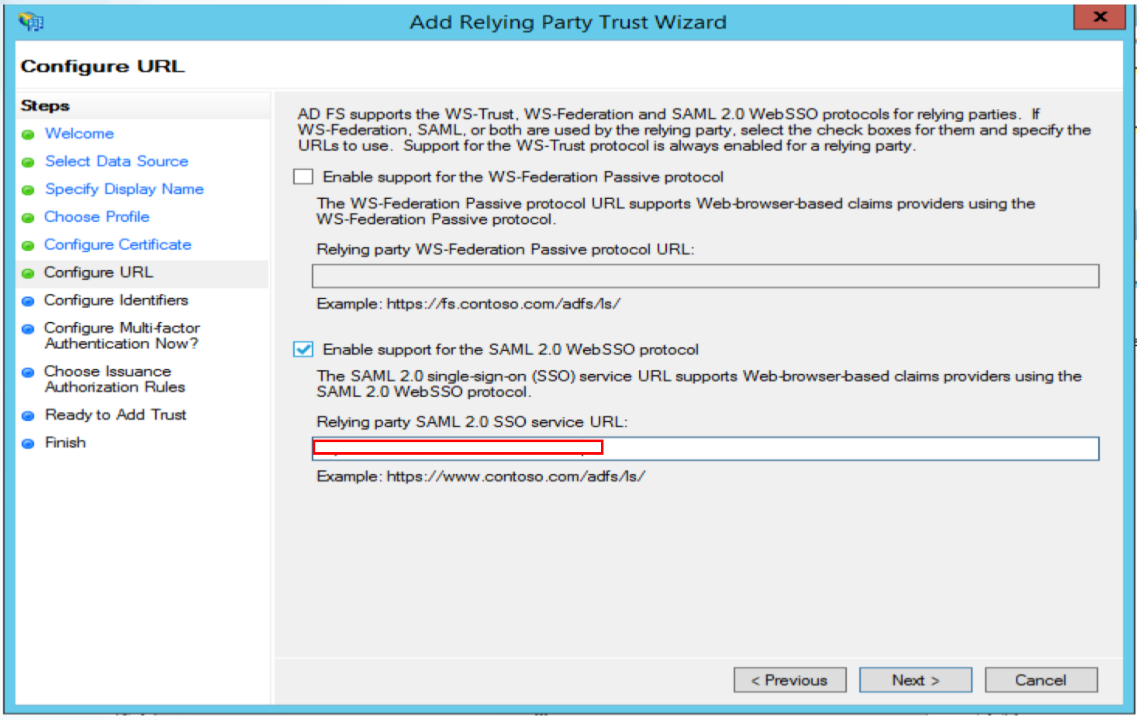
Add Relying Party Trust Wizard

Configure Certificate

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:

Set the relying party SAML 2.0 SSO service url to the commonauth endpoint.(Ex : https://apidev.oasys.lk:9443/token)



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/

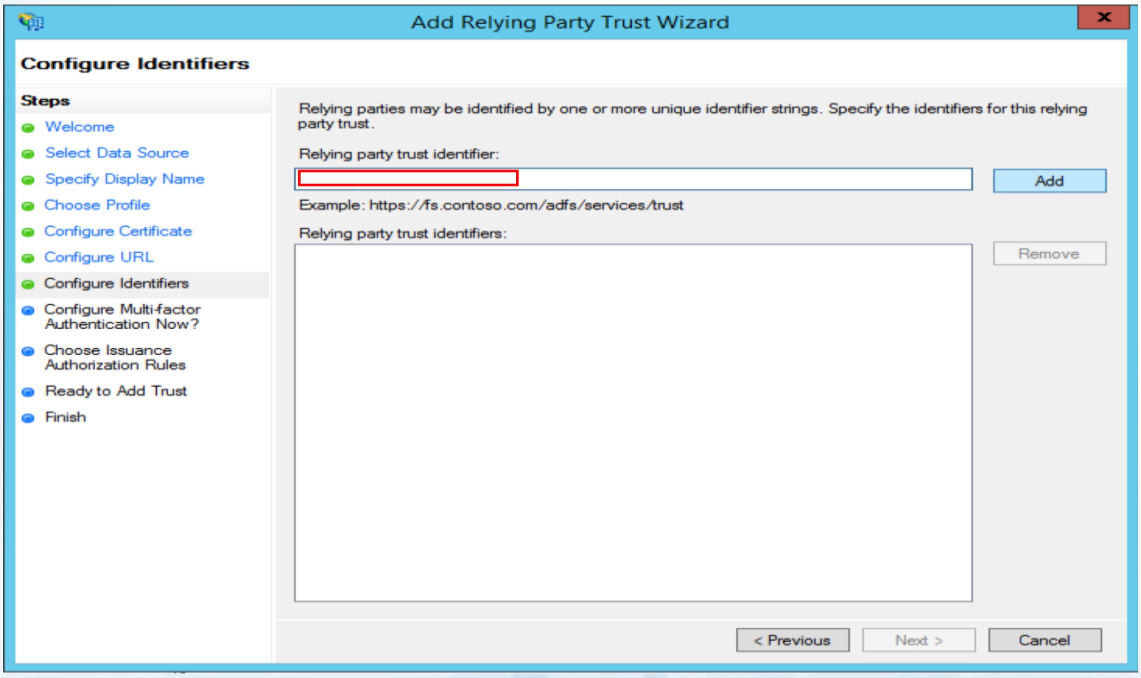
☑ Enable support for the SAML 2.0 WebSSO protocol

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/

Add the relying party trust identifier and click Next. The value you enter here should be entered in APIM Identity Provider (IdP) settings as well. (ex: wso2km21AzureDev) Setting up the IdP is explained in the next section.



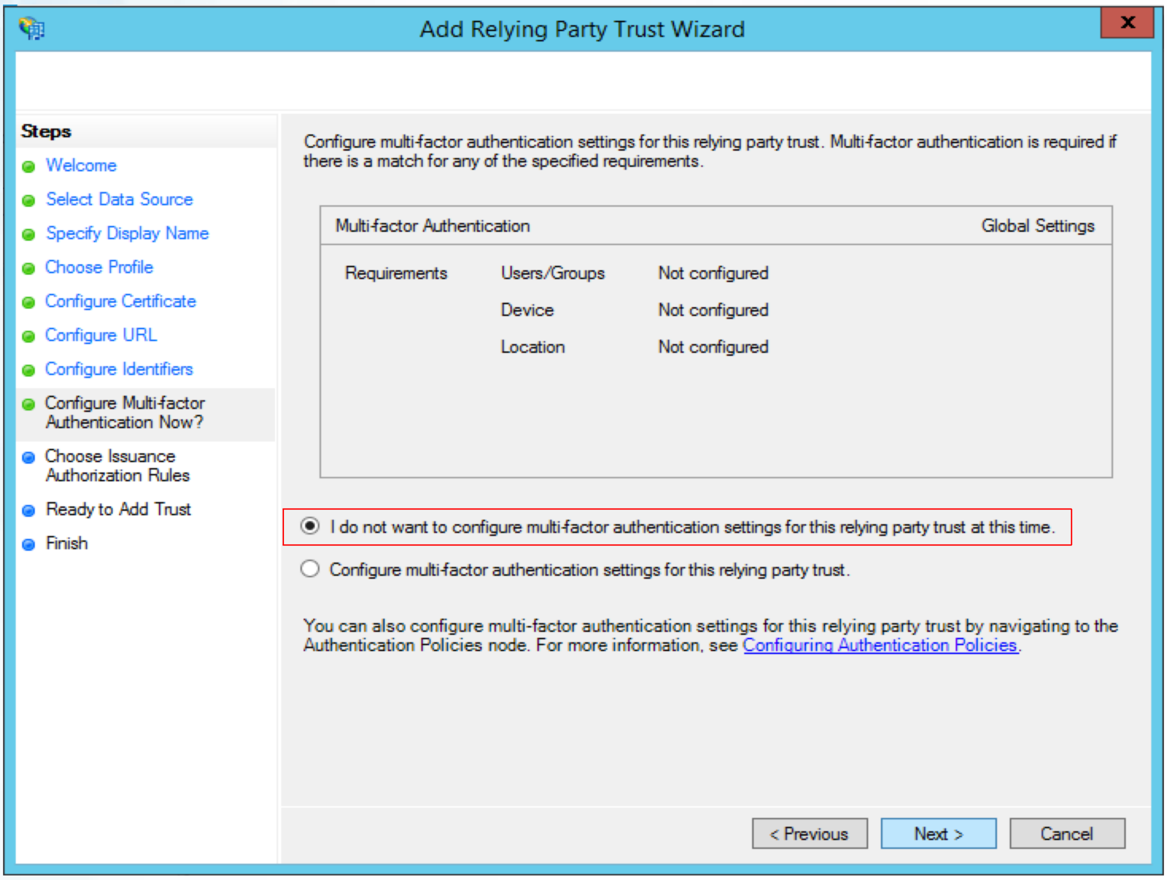
Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:

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

Relying party trust identifiers:

We won’t be configuring multi-factor authentication so click Next.



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.

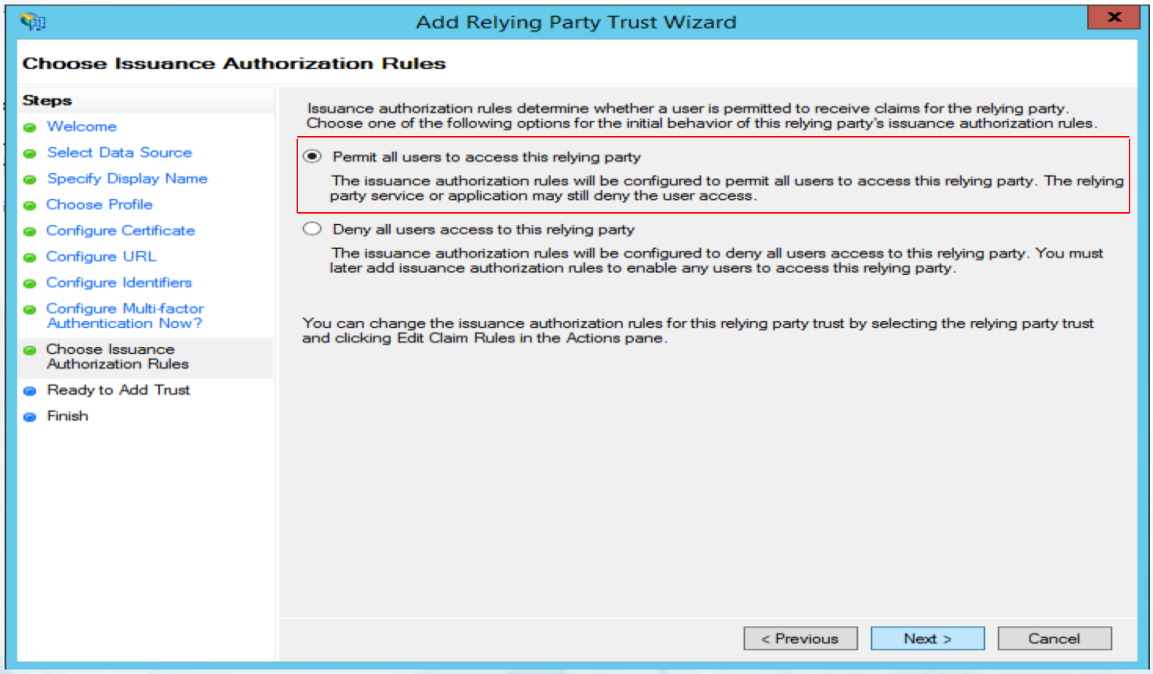
Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

● 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.

Select Permit all users to access this relying party and click 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

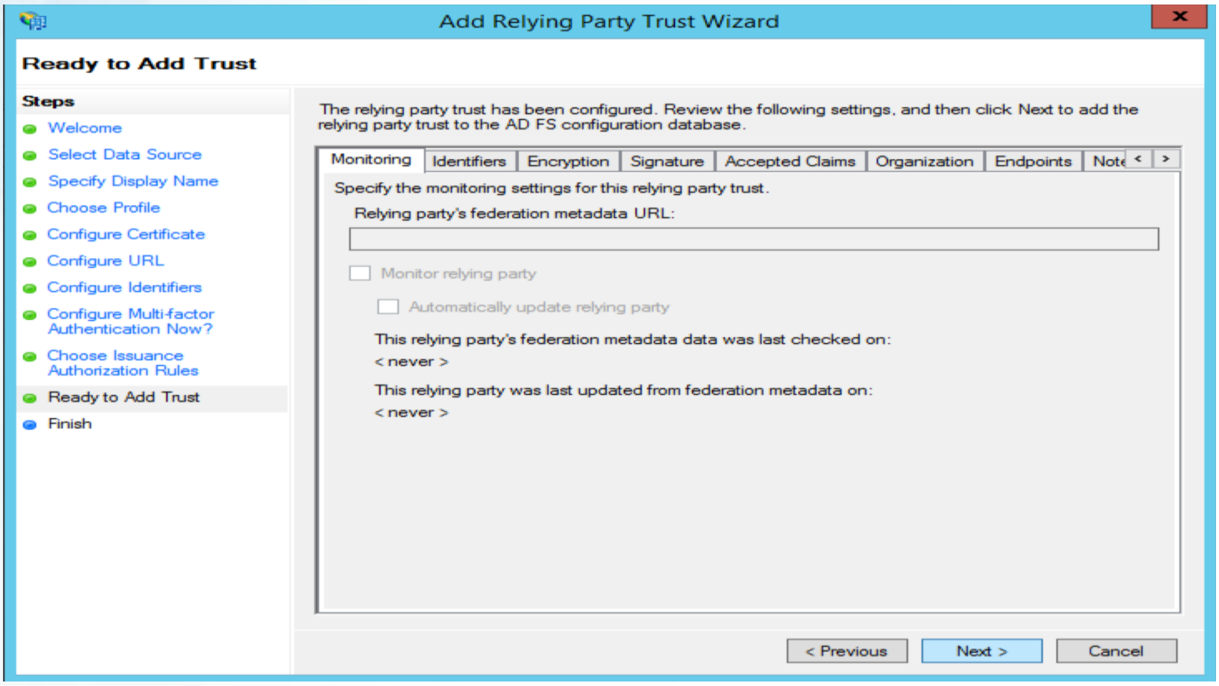
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ 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.

Review the Settings & click Next



Add Relying Party Trust Wizard

Ready to Add Trust

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

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.

Monitoring | Identifiers | Encryption | Signature | Accepted Claims | Organization | Endpoints | Note

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

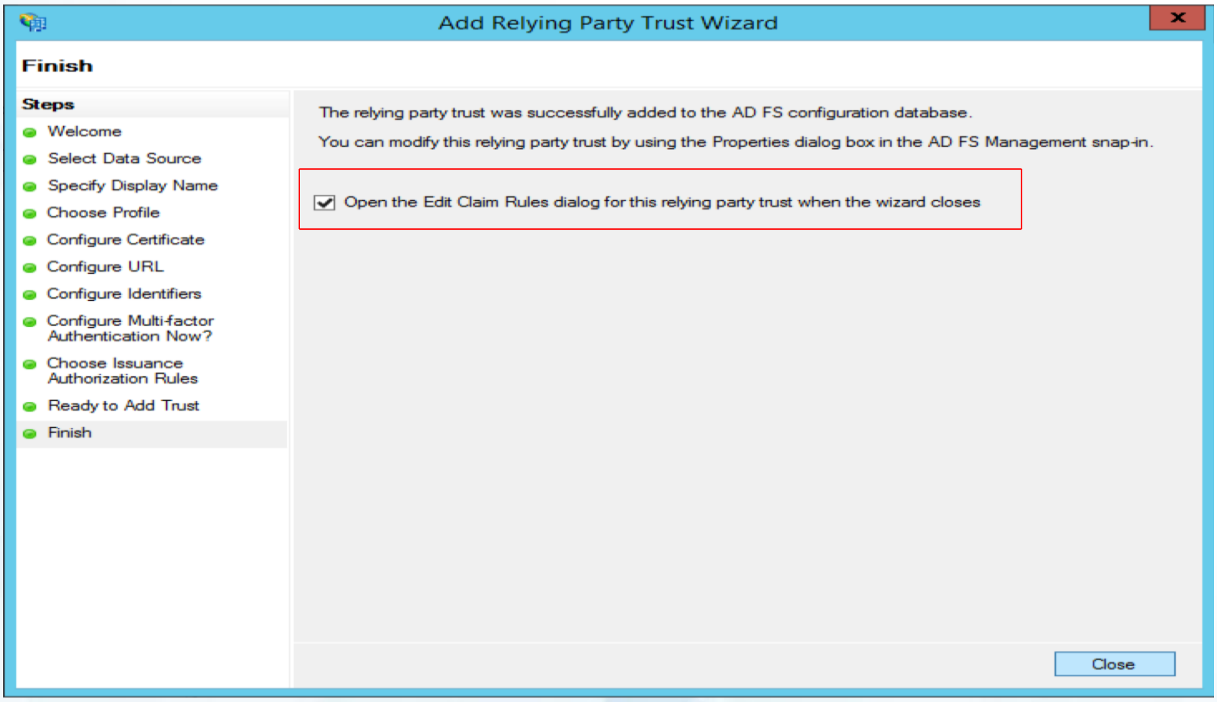
□ Monitor relying party

□ 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 >

Click Close to finish adding the relying party trust. Also let the wizard to open the Claim Rules dialog



Add Relying Party Trust Wizard

Finish

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

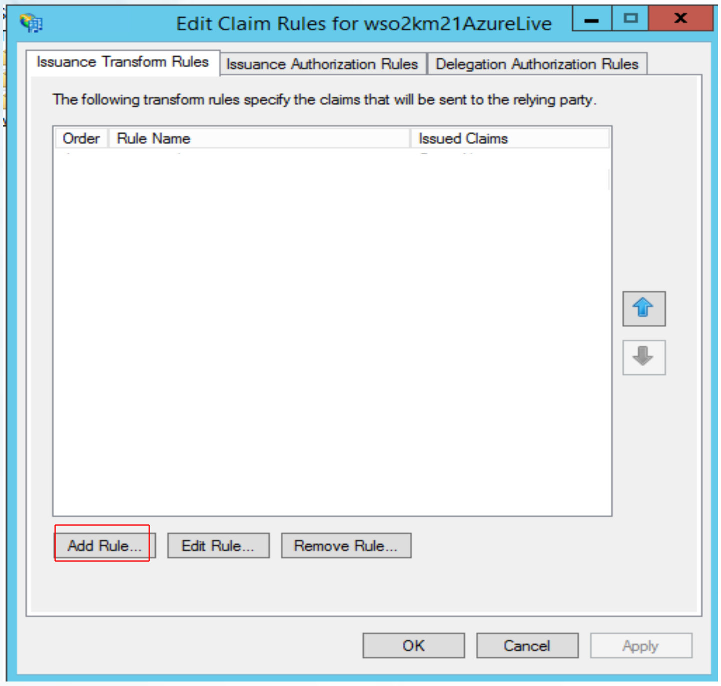
The relying party trust was successfully added to the AD FS configuration database.

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

In the Edit Claim Rule dialog we will specify which claims to be sent to the relying party.

First click Add Rule…

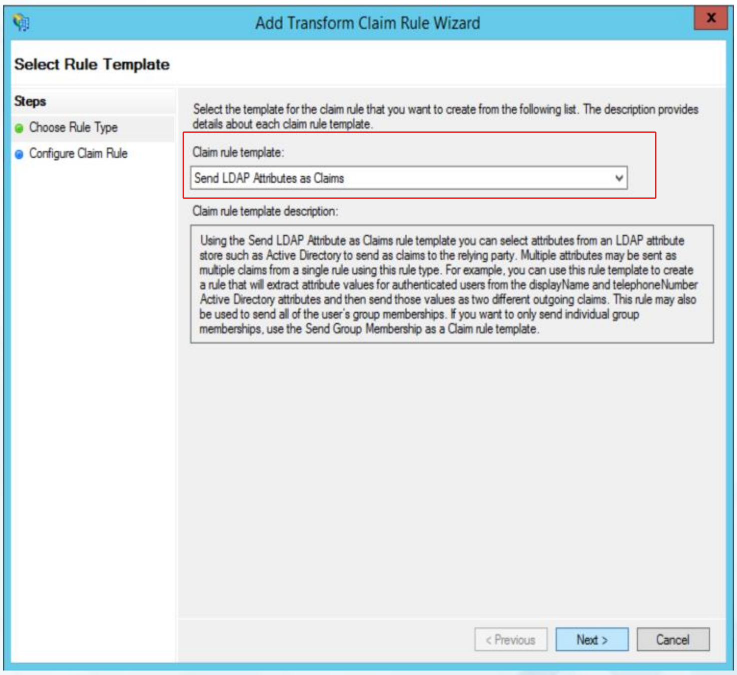


Edit Claim Rules for wso2km21AzureLive

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

Order	Rule Name	Issued Claims

Select Send LDAP Attributes as a claim and click Next.



Add Transform Claim Rule Wizard

Select Rule Template

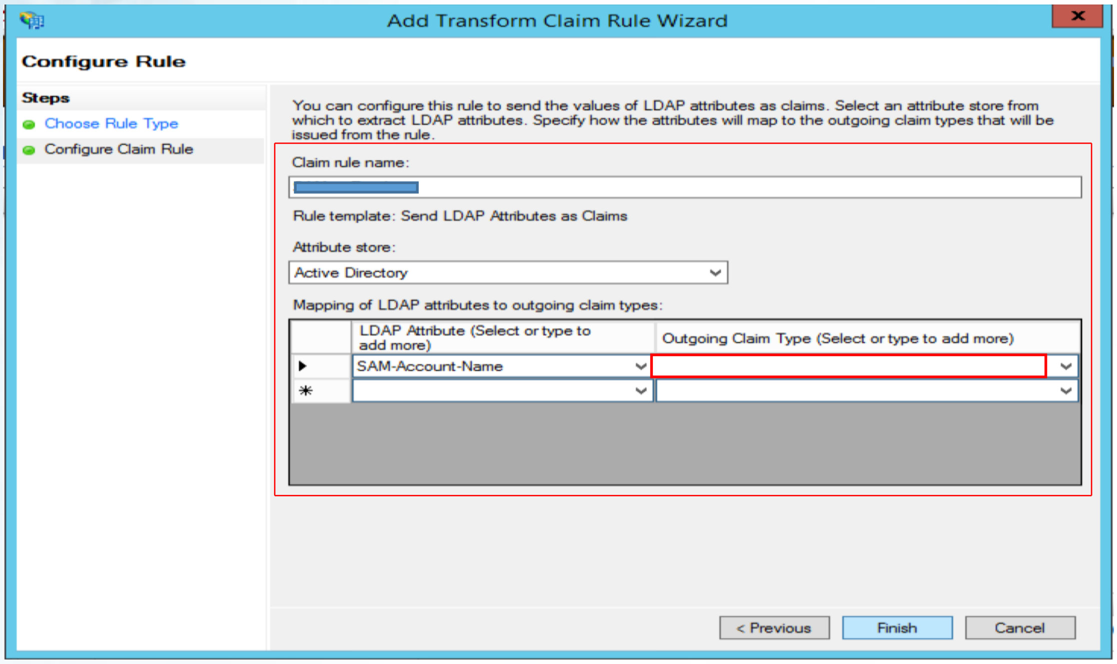
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

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.

Set a Claim rule name (ex:sam-email) and map **SAM-Account-Name** to **Given Name**. Then click Finish.



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

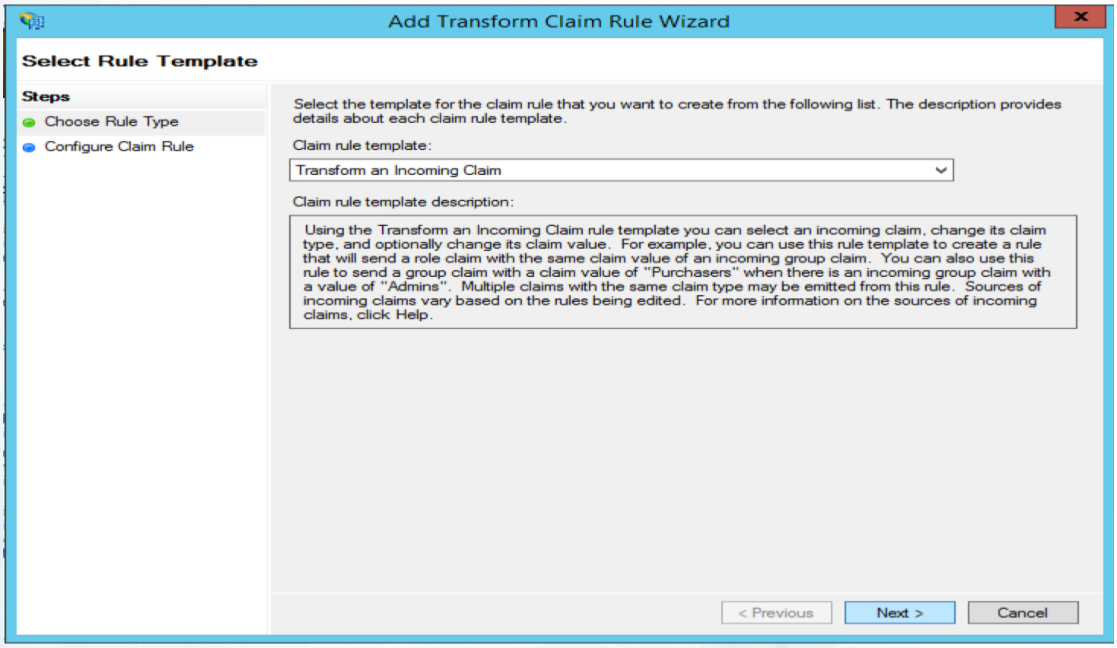
Attribute store:

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	
*		

Click Add Rule… again to transform the Given Name claim to NameID claim. Select Transform an Incoming Claim and click Next.



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.

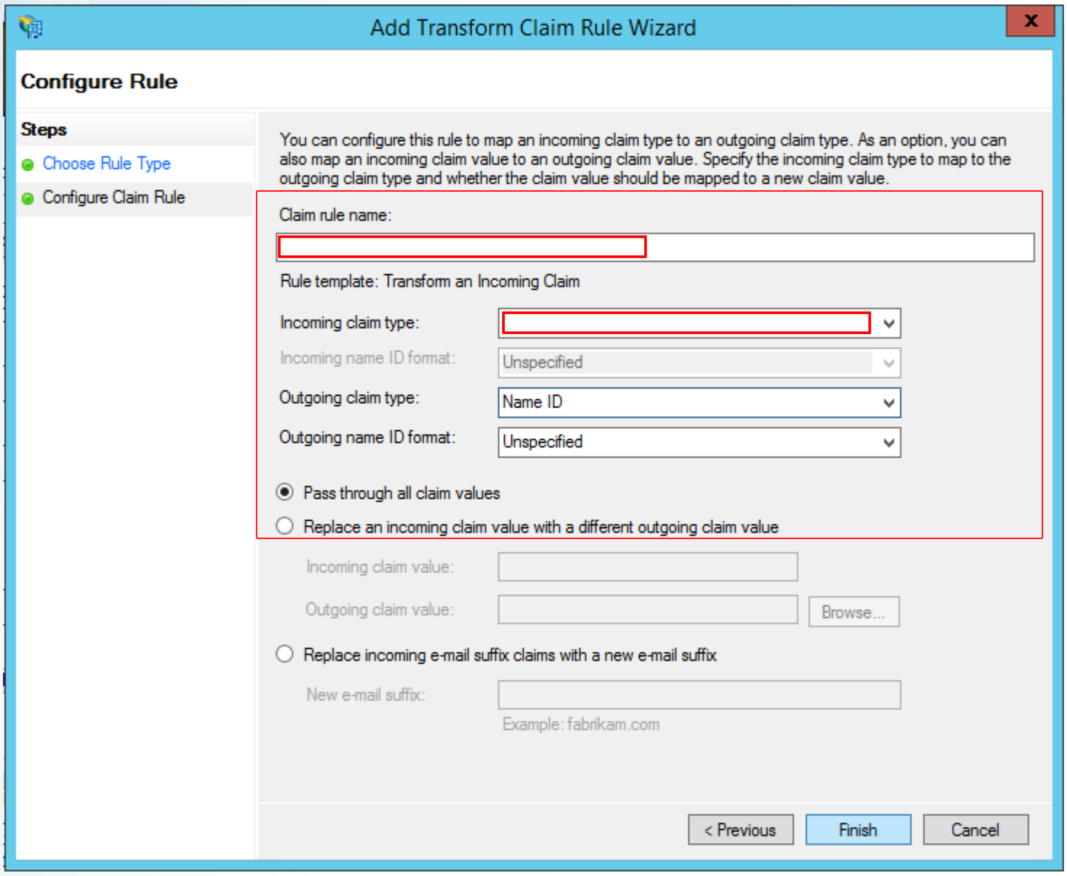
Claim rule template:

Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.

Set the Claim rule name as unique_name . Select the incoming claim type as Given Name and outgoing claim type and ID format as Name ID and Unspecified respectively. Then click Finish.



You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Unspecified

● Pass through all claim values

○ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

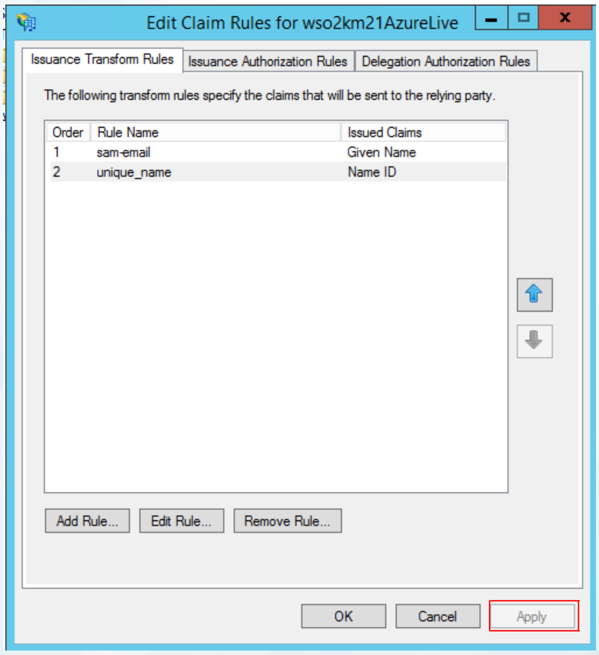
Outgoing claim value:

○ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

Then **Apply** and **Close** the Claim Rule Dialog



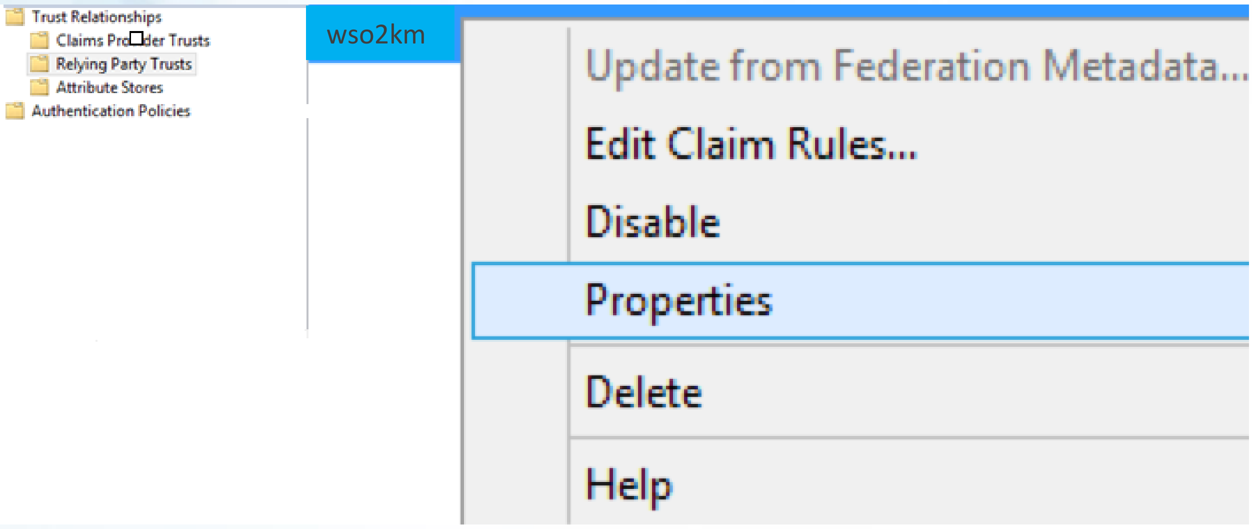
Edit Claim Rules for wso2km21AzureLive
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

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

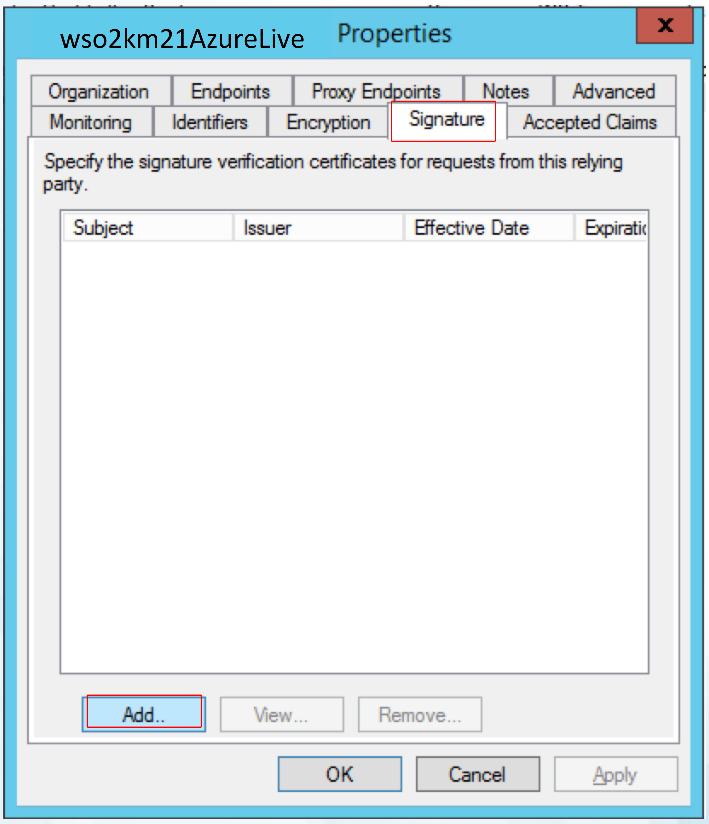
Order	Rule Name	Issued Claims
1	sam-email	Given Name
2	unique_name	Name ID

Before we wrap up things in AD FS side, there are few configuration changes needed to be done in Relying Party Trust properties. For that right click on the Relying Party Trust we just created and select Properties.

Go to Signature tab and click Add.

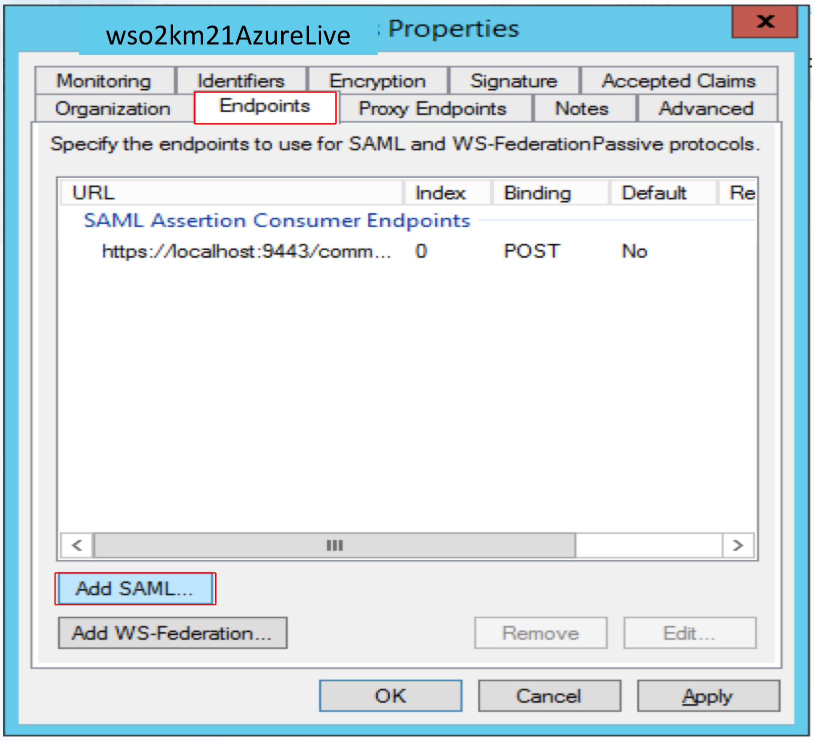


The certificate which should be added here. (APIM Certificate provided by the application owner)



Specify the signature verification certificates for requests from this relying party.

Next move to the Endpoint tab. Here we have to set the SAML logout endpoint. Click Add SAML…

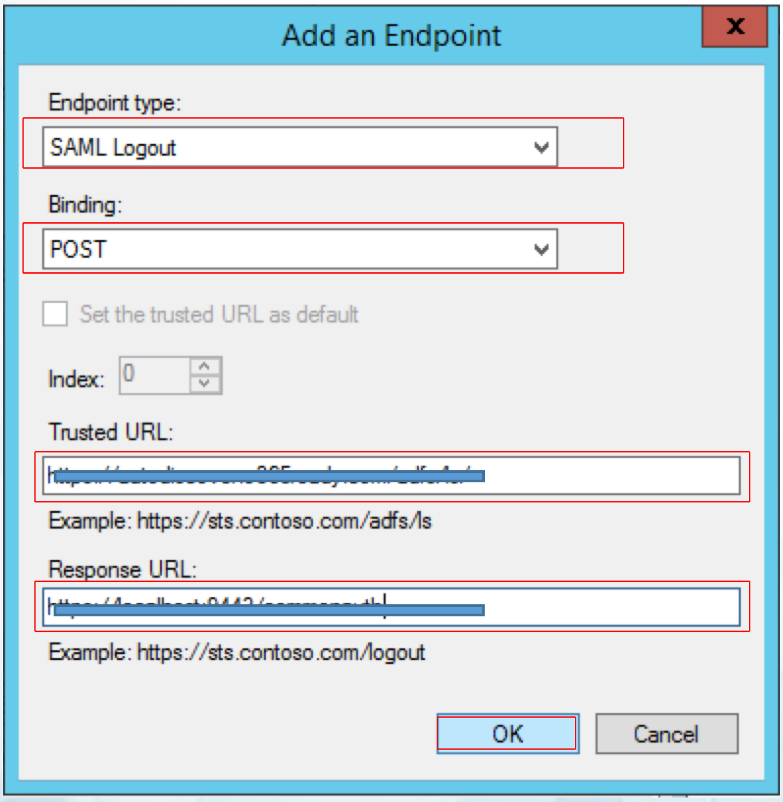


wso2km21AzureLive Properties

Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://localhost:9443/comm...	0	POST	No	

Select Endpoint Type as SAML Logout and the Binding as POST. Set the Trusted URL as https://<AD_FS_server>/adfs/ls and the Response URL as the /commonauth endpoint of Apim. Once it is done save the property settings of the Relying Party by Clicking OK.



Add an Endpoint

Endpoint type: SAML Logout

Binding: POST

□ Set the trusted URL as default

Index: 0

Trusted URL: [redacted]

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

Response URL: [redacted]

Example: https://sts.contoso.com/logout