**Adding a Relying Party in ADFS 3.0**

**Prerequisites**

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

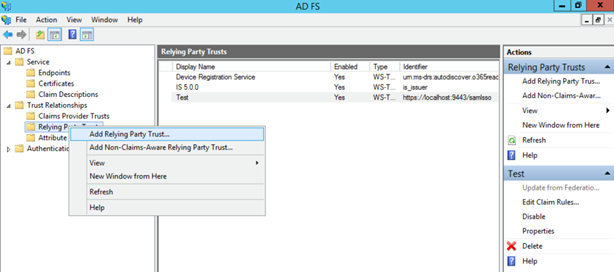
|  |  |
| --- | --- |
| Client\_id | LCjusy5ajAoqF87j3cqc765bPkAa |
| Client\_id redirect URL | <https://api.oasys.lk:9843/carbon> |
| Commonauth endpoint | <https://api.oasys.lk:9843/commonauth> |
| Relying party trust identifier | **WSO2IDSNDBOASYSLIVE** |
| Certificate | Attached Wso2 IDS certificate (.crt) |

\* Below information should be provided by ADFS owner

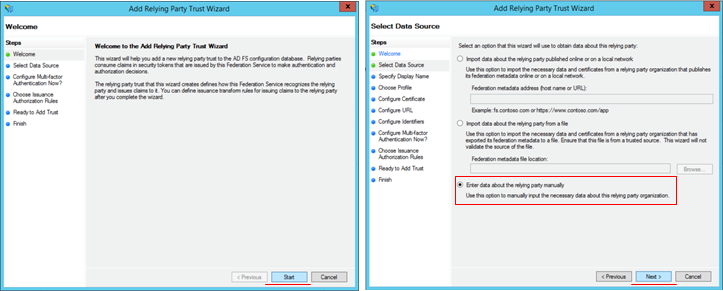
|  |  |
| --- | --- |
| Trusted URL | Ex : https://<AD\_FS\_server>/adfs/ls |
| Metadata URL | Ex: http://<AD\_FS\_server>/adfs/services/trust |

**Steps**

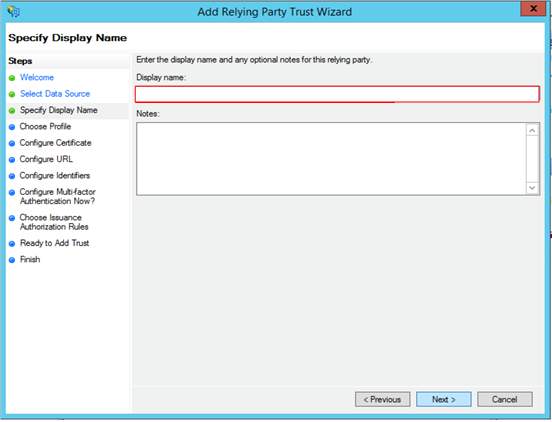
In ADFS Management UI expand Trust Relationship, right click on Relying Party Trust and select Add Relying Party Trust…



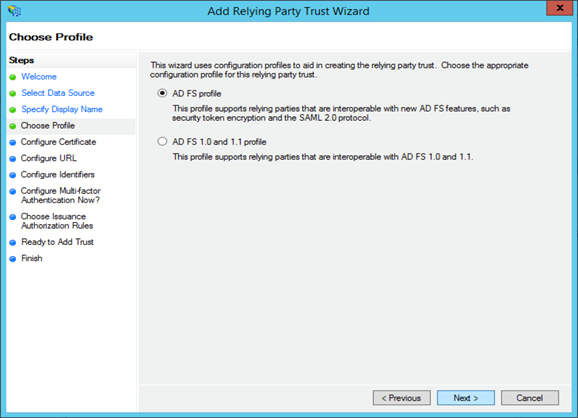
Follow the wizard as shown below



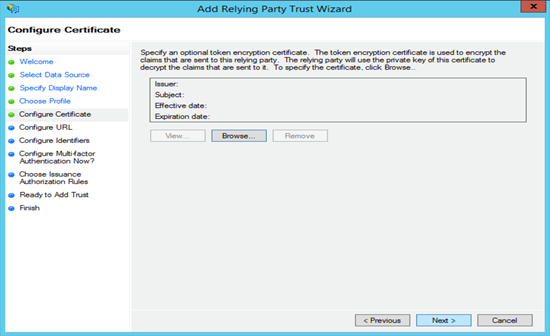
Type a desired display name (wso2km21AzureLive) for the relying party and click **Next**



Select AD FS Profile and Click Next.

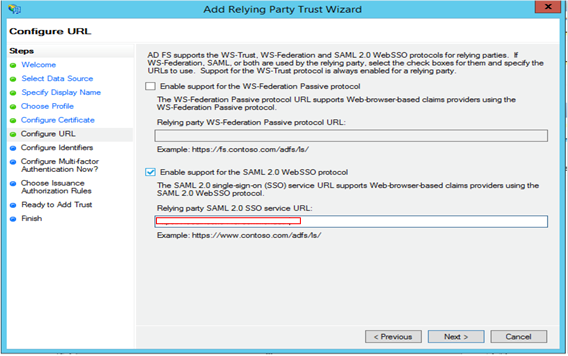


We are not using an encryption certificate so click Next.

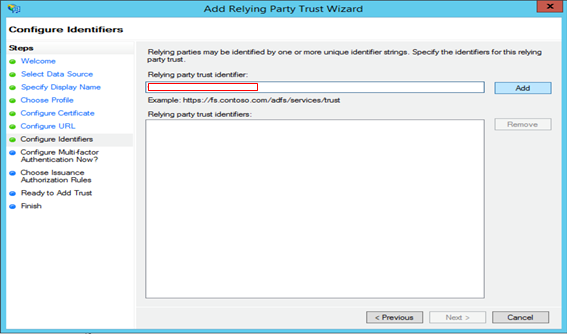


Set the relying party SAML 2.0 SSO service url to the commonauth endpoint.

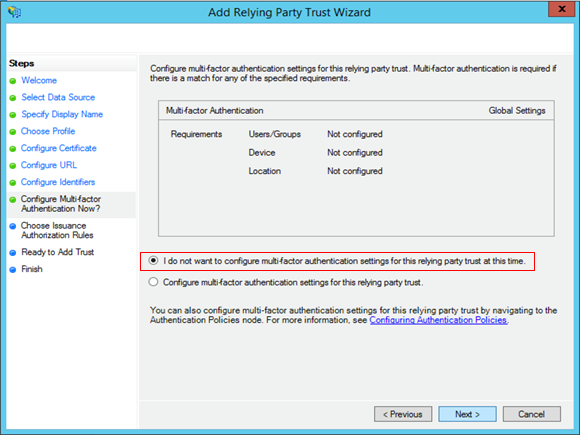
( Ex : <https://api.oasys.lk:9843/commonauth>)



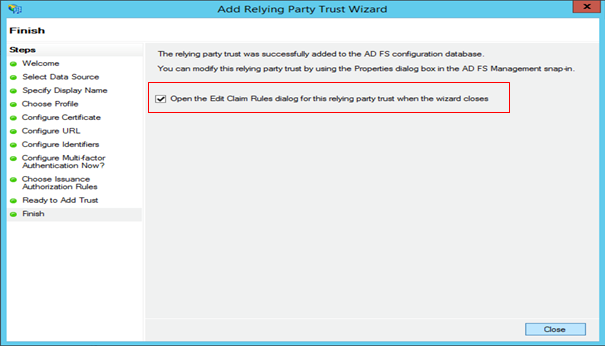
Add the relying party trust identifier and click Next. The value you enter here should be entered in APIM Identity Provider (IdP) settings as well. (ex: wso2km21AzureDev) Setting up the IdP is explained in the next section.



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

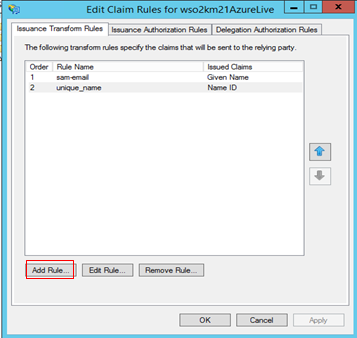


Click Close to finish adding the relying party trust. Also let the wizard to open the Claim Rules dialog

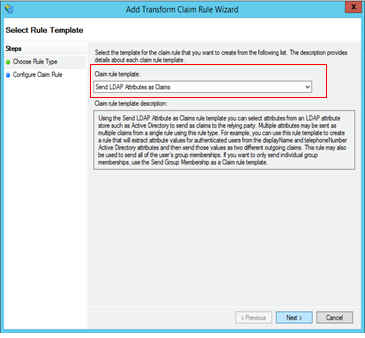


In the Edit Claim Rule dialog, we will specify which claims to be sent to the relying party.

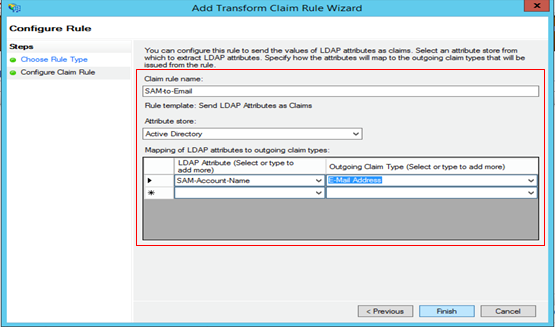
First click Add Rule…



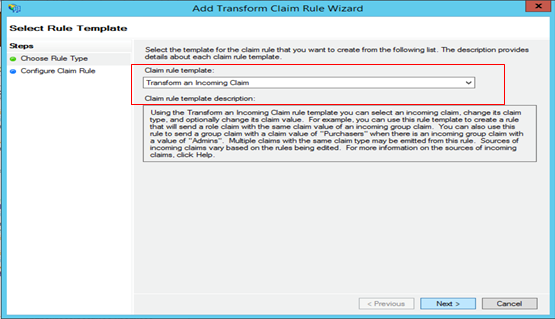
Select Send LDAP Attributes as a claim and click Next.



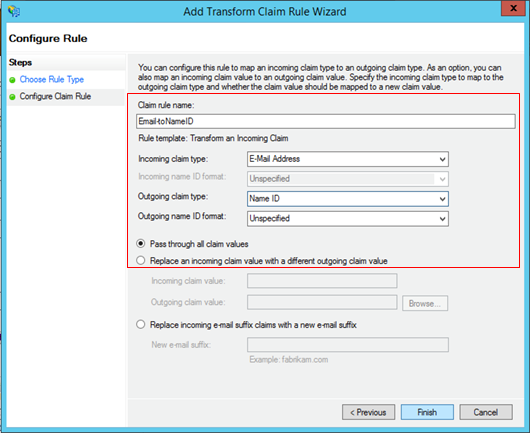
Set a Claim rule name (ex:sam-email) and map **SAM-Account-Name** to **Given Name**. Then click Finish.



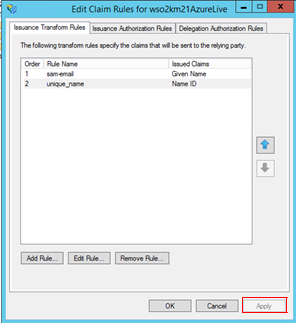
Click Add Rule… again to transform the Given Name claim to NameID claim. Select Transform an Incoming Claim and click Next.



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.

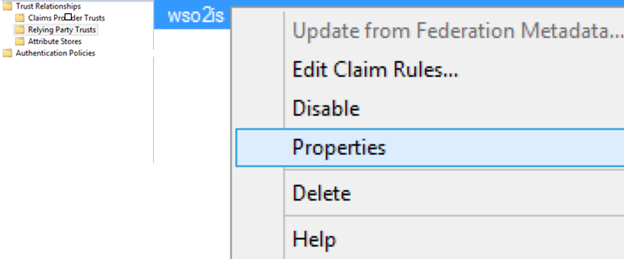


Then **Apply** and **Close** the Claim Rule Dialog

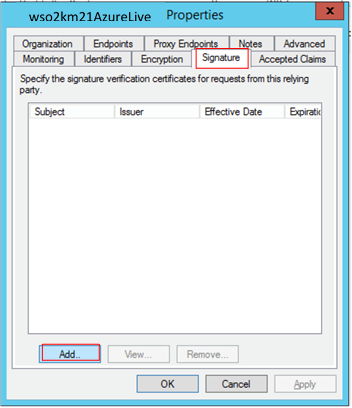


Before we wrap up things in AD FS side, there are few configuration changes needed to be done in Relying Party Trust properties. For that right click on the Relying Party Trust we just created and select Properties.

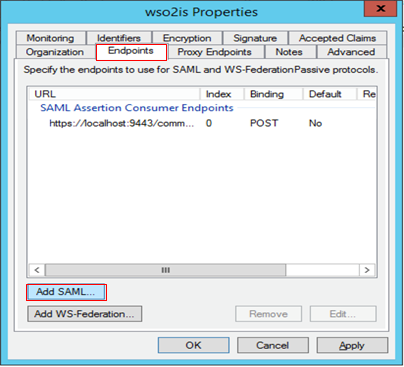
Go to Signature tab and click Add.



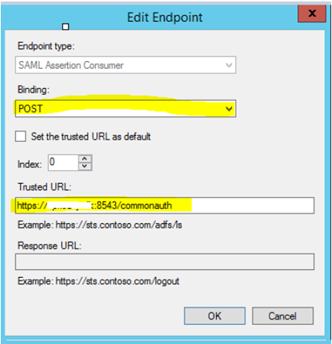
The certificate which should be added here. (APIM Certificate provided by the application owner)

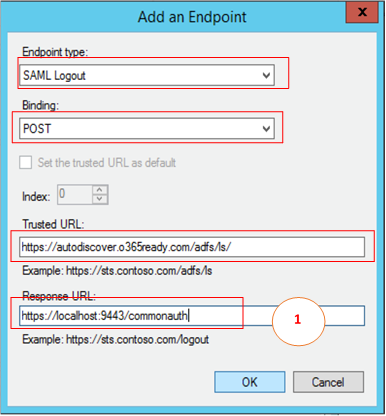


Next move to the Endpoint tab. Here we have to set the SAML logout endpoint. Click Add SAML…



Add SAML Assertion Consumer and SAML Logout Endpoint as Binding as POST. Once it is done save the property settings of the Relying Party by Clicking OK.





**Install Client ID using PowerShell**

Please run the following command with information given by Application owner .

Add-AdfsClient -Name "xxxxxxxxx" -ClientId "xxxxxxxxxxxxxxxxxxxxxxxxxxxx" -RedirectUri " https://api.oasys.lk:8543/carbon " -Description "OAuth 2.0 client for relaying party"

Finally,

1. Under Relying Party Trusts with global authentication settings only, select the same Relying Party Trust record.
2. Click Properties under the Actions panel at the right side to display the Edit Authentication Policy window.
3. Check the Users are required to provide credentials each time at sign in option.

