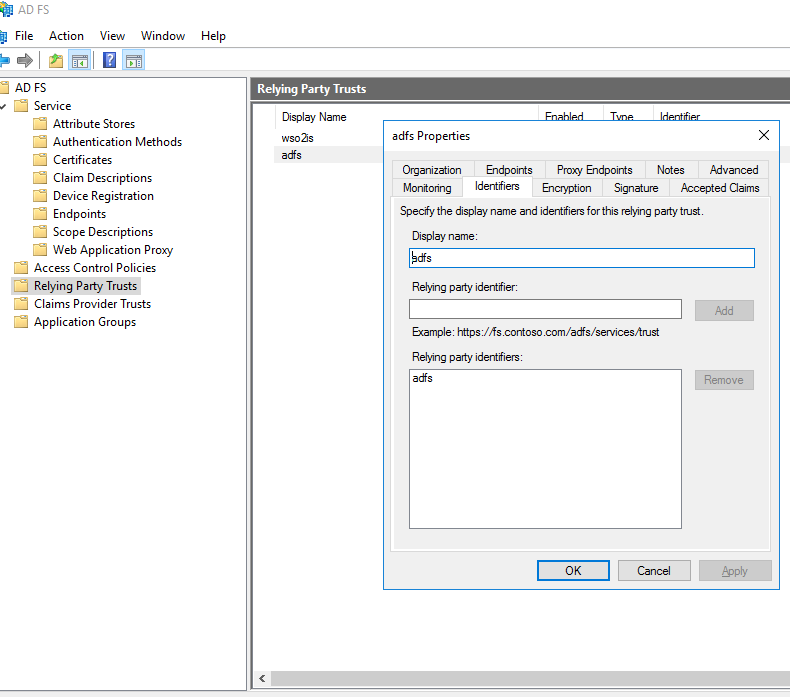
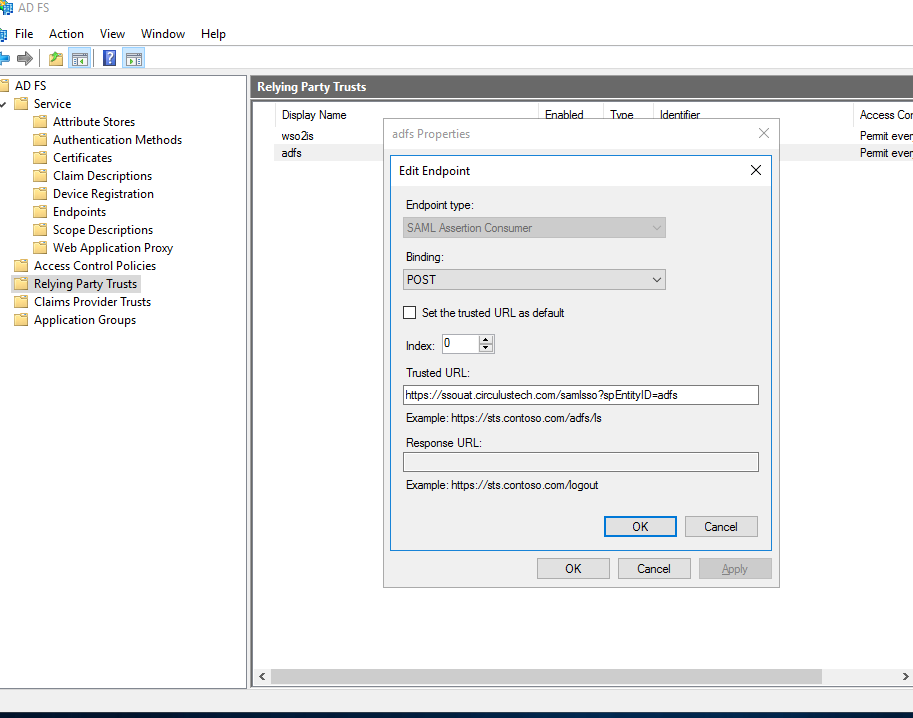
**ADFS: -**

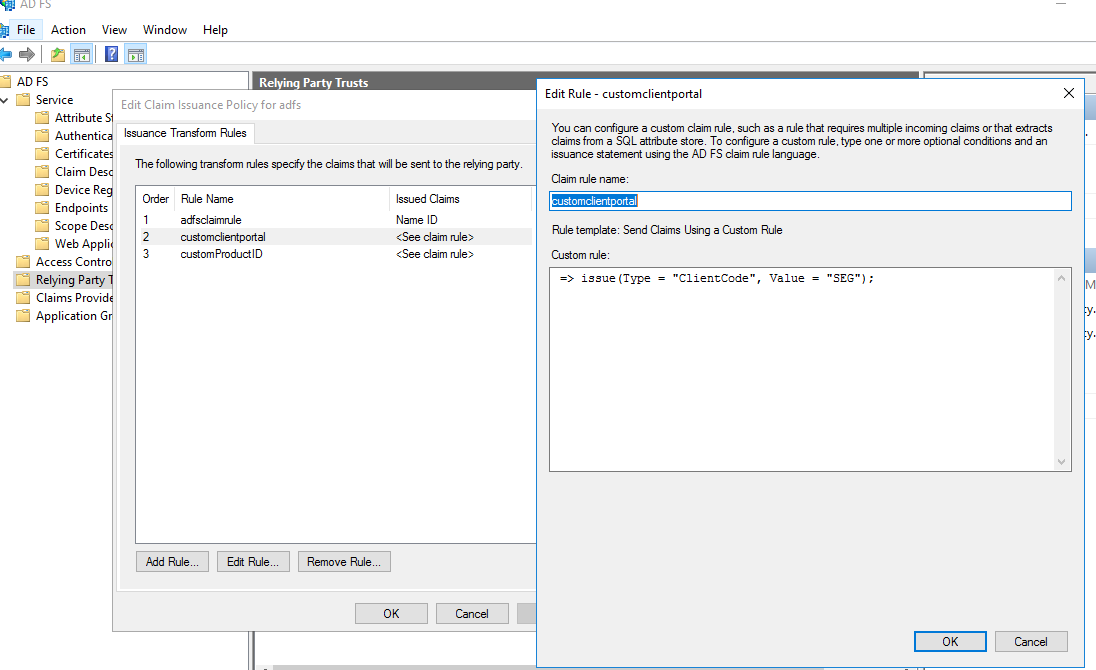
**Relying Party Trust Name: - adfs**



**Endpoint URL: -**



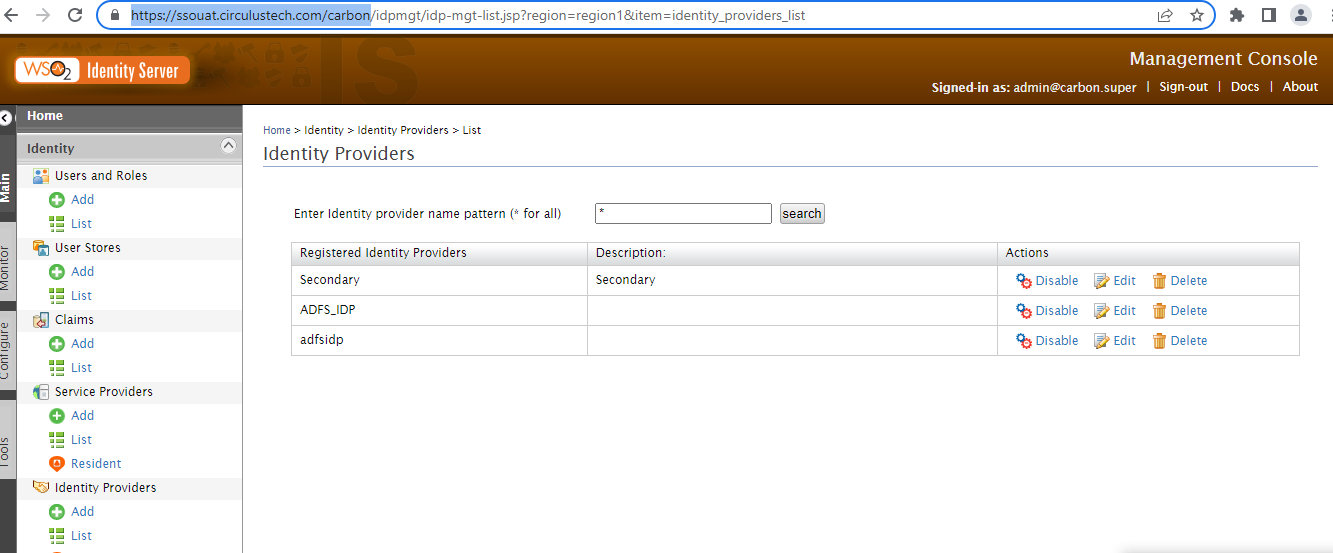
CLIAMS: -

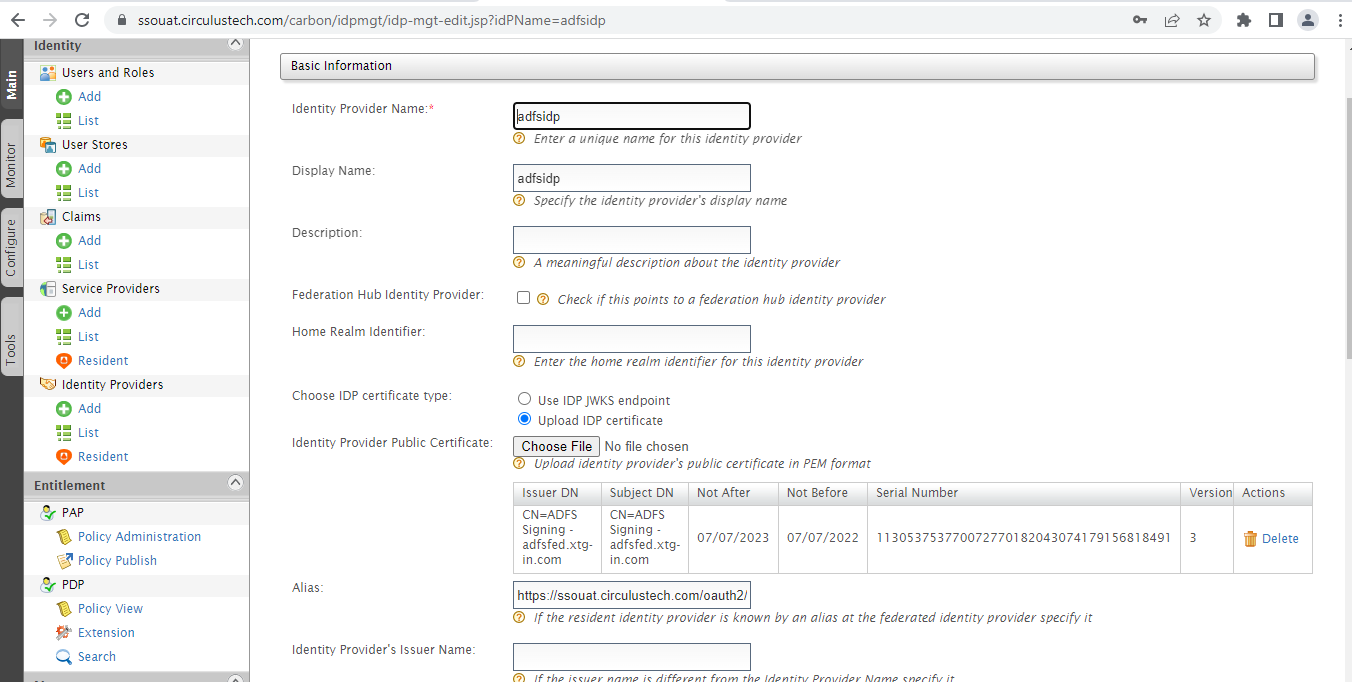


FederatedXML File:-

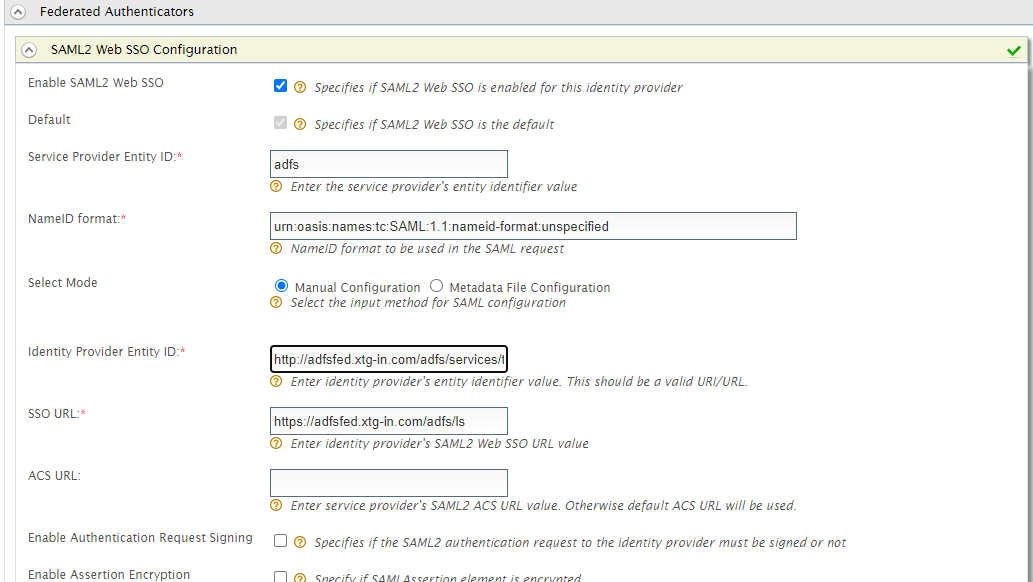


**IDENTITY PROVIDER**

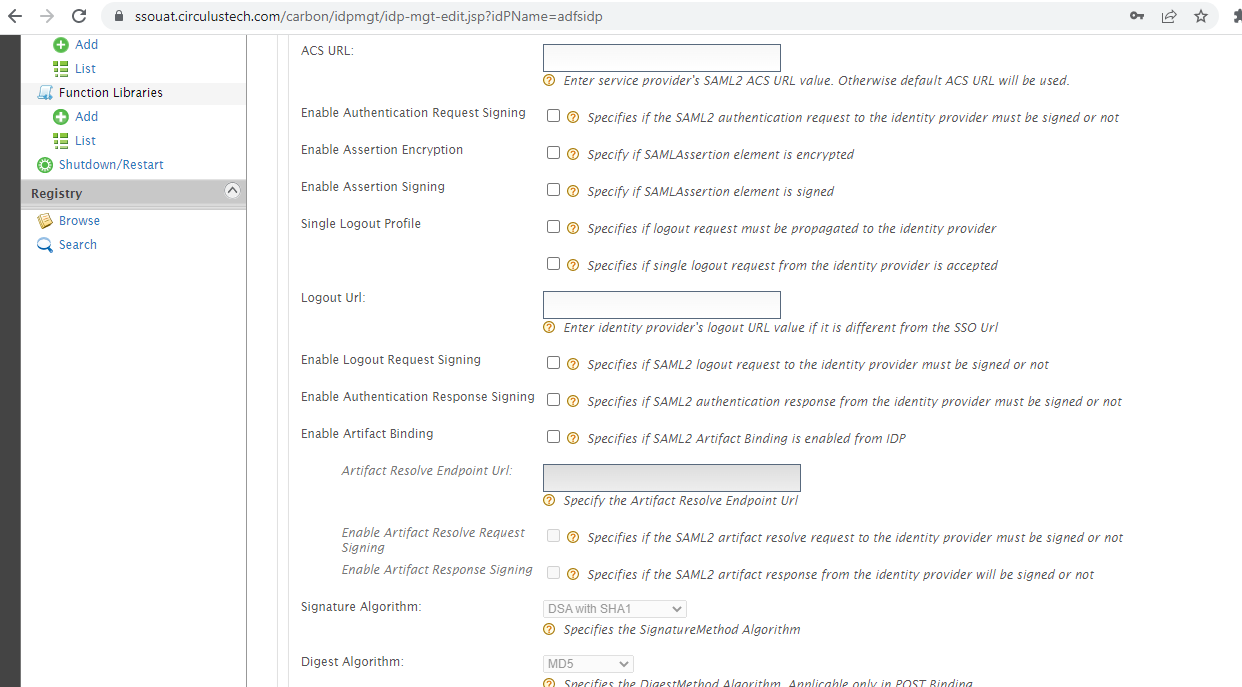


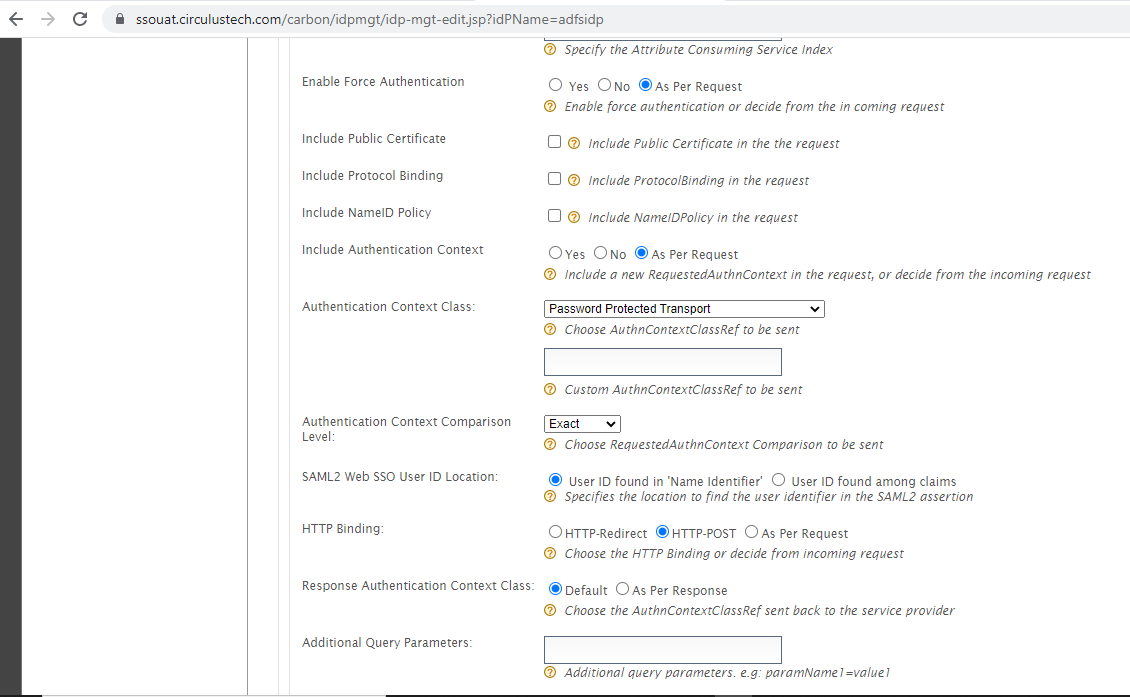


Alias : - https://ssouat.circulustech.com/oauth2/token

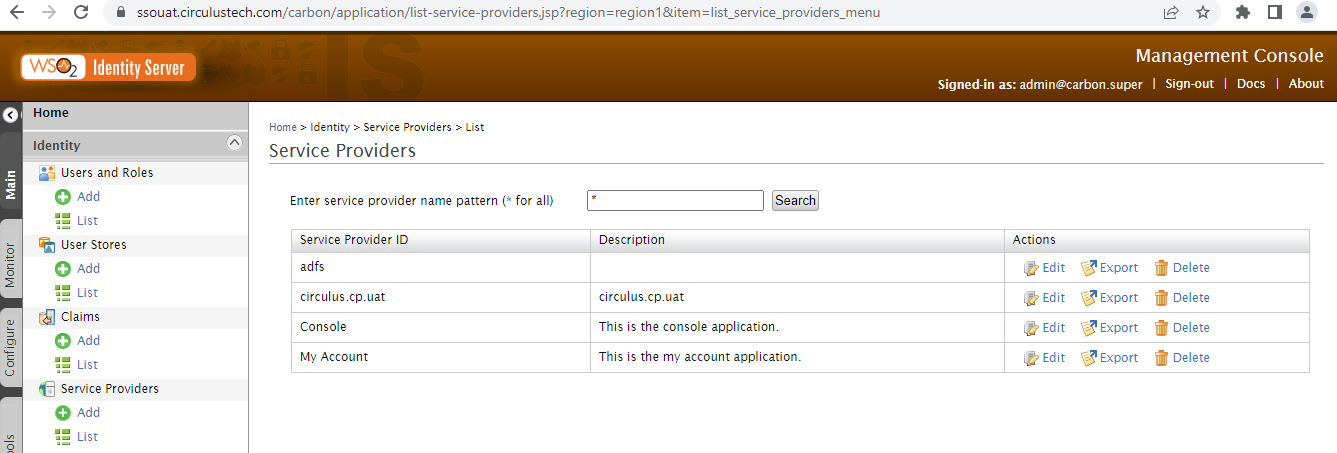


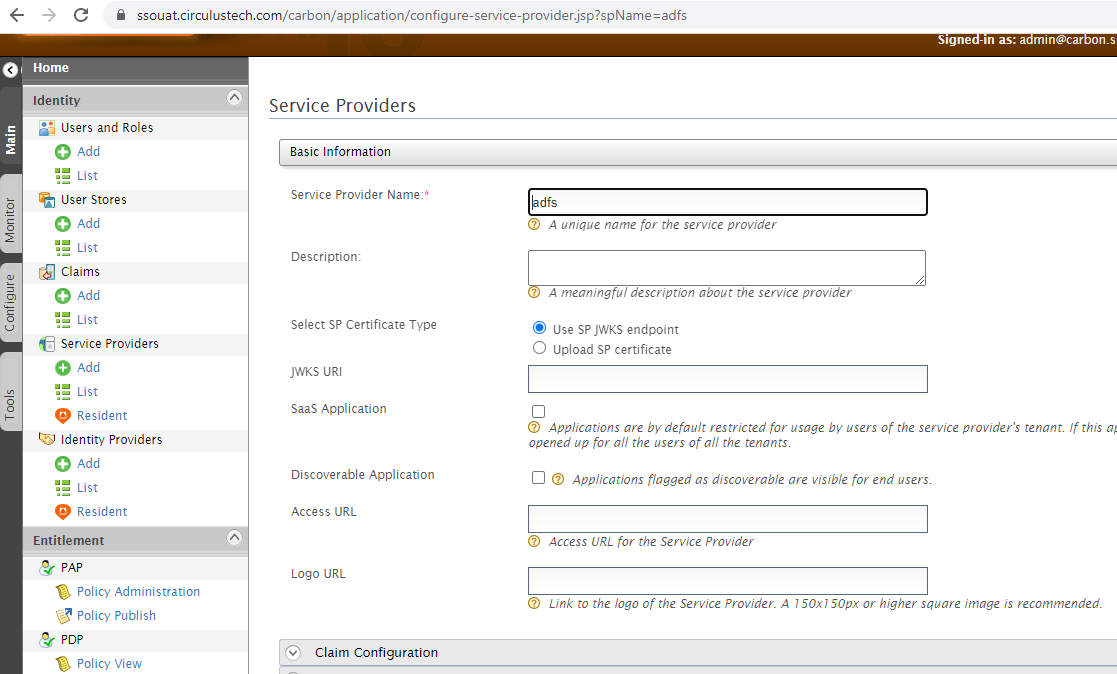
Identity Provider ID : http://adfsfed.xtg-in.com/adfs/services/trust

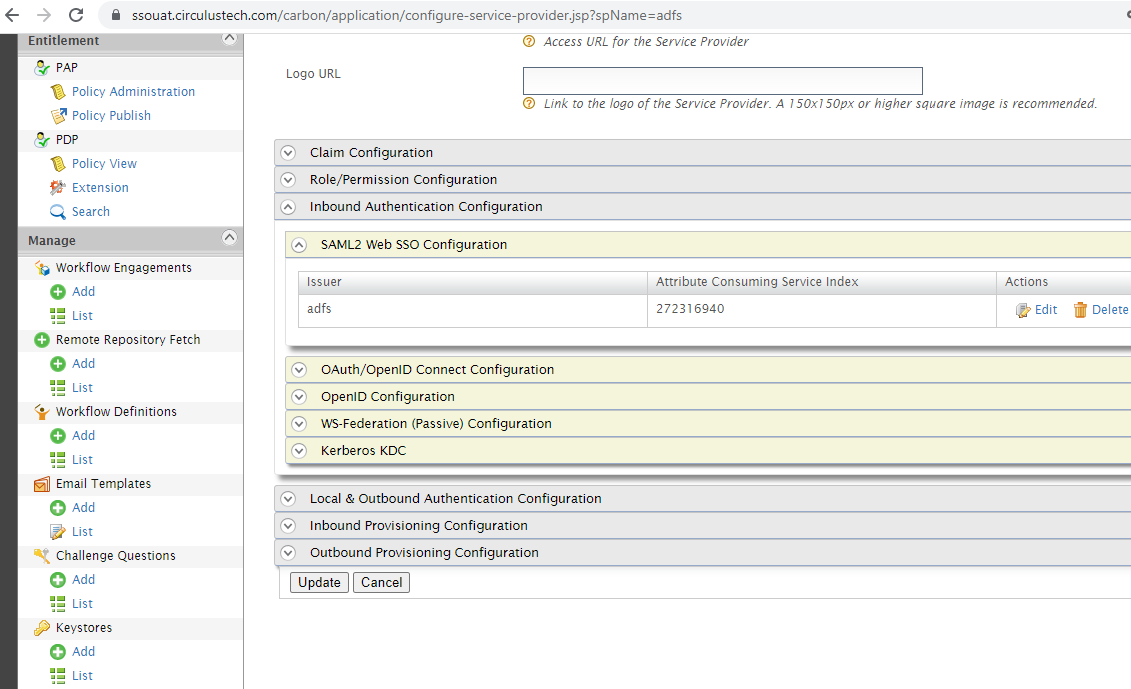


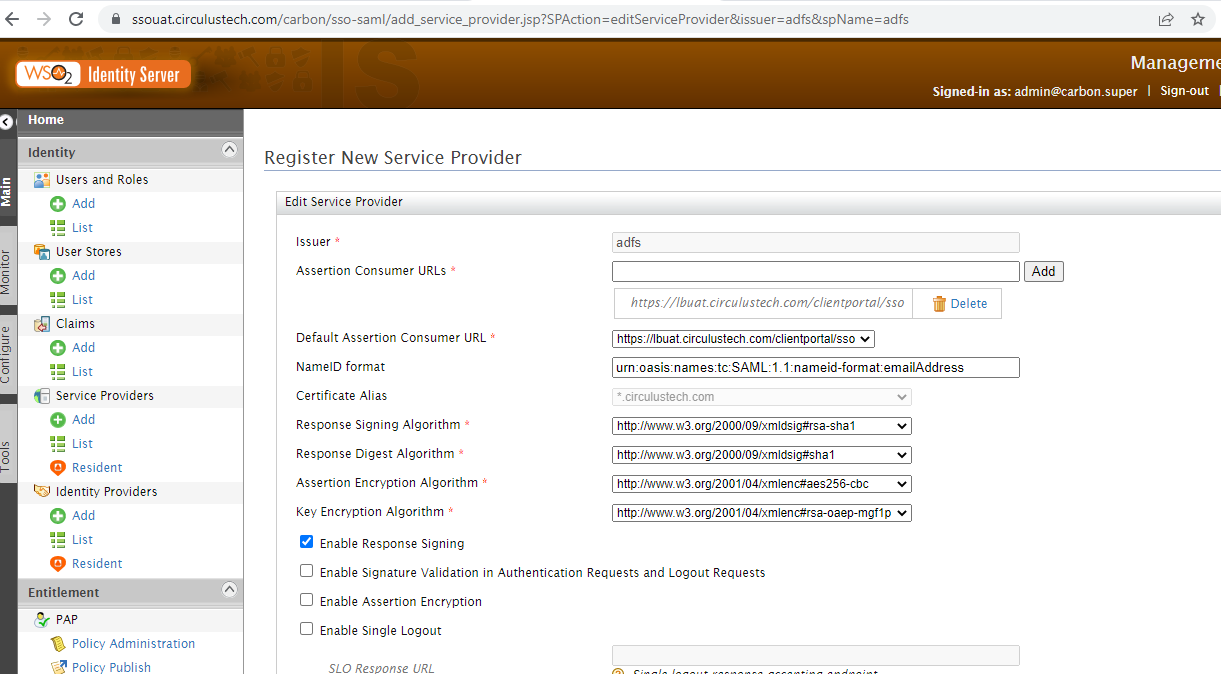


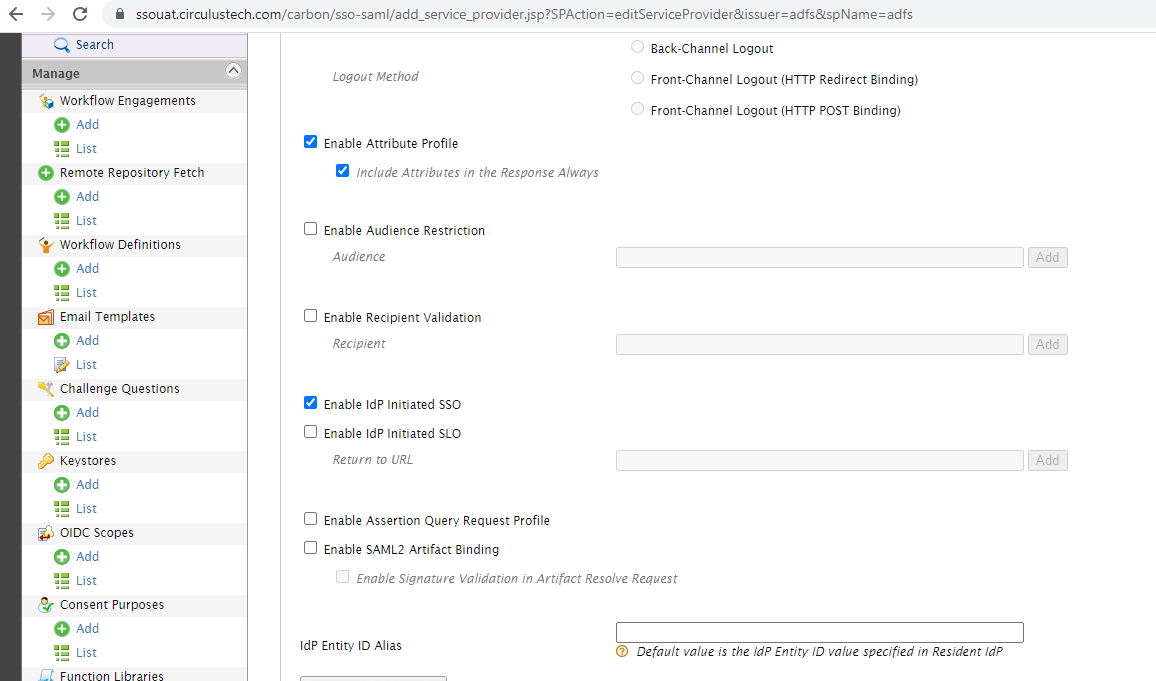
**SERVICE -PROVIDER**

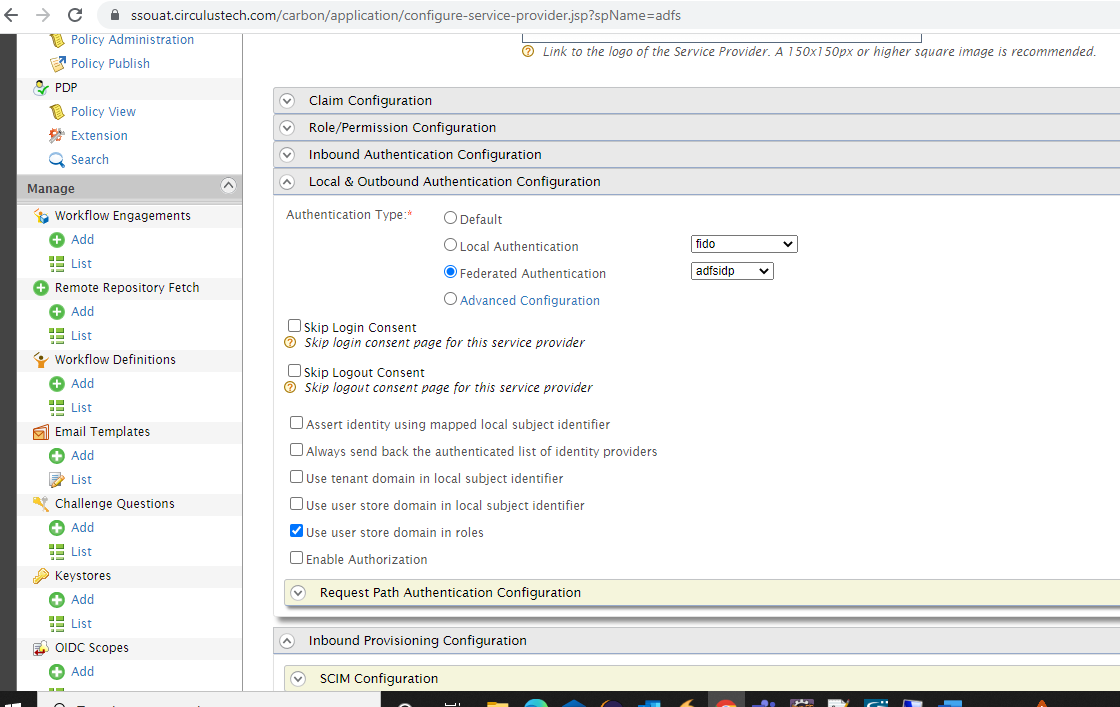






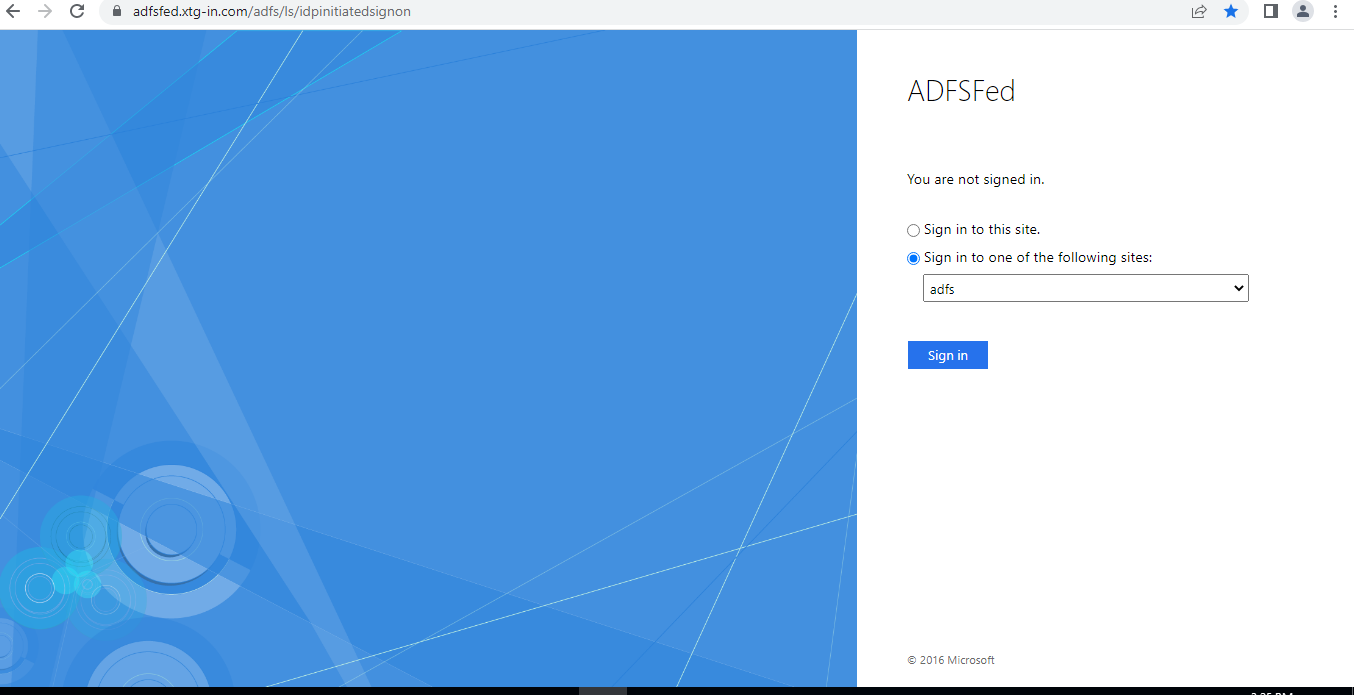






Login Page: -

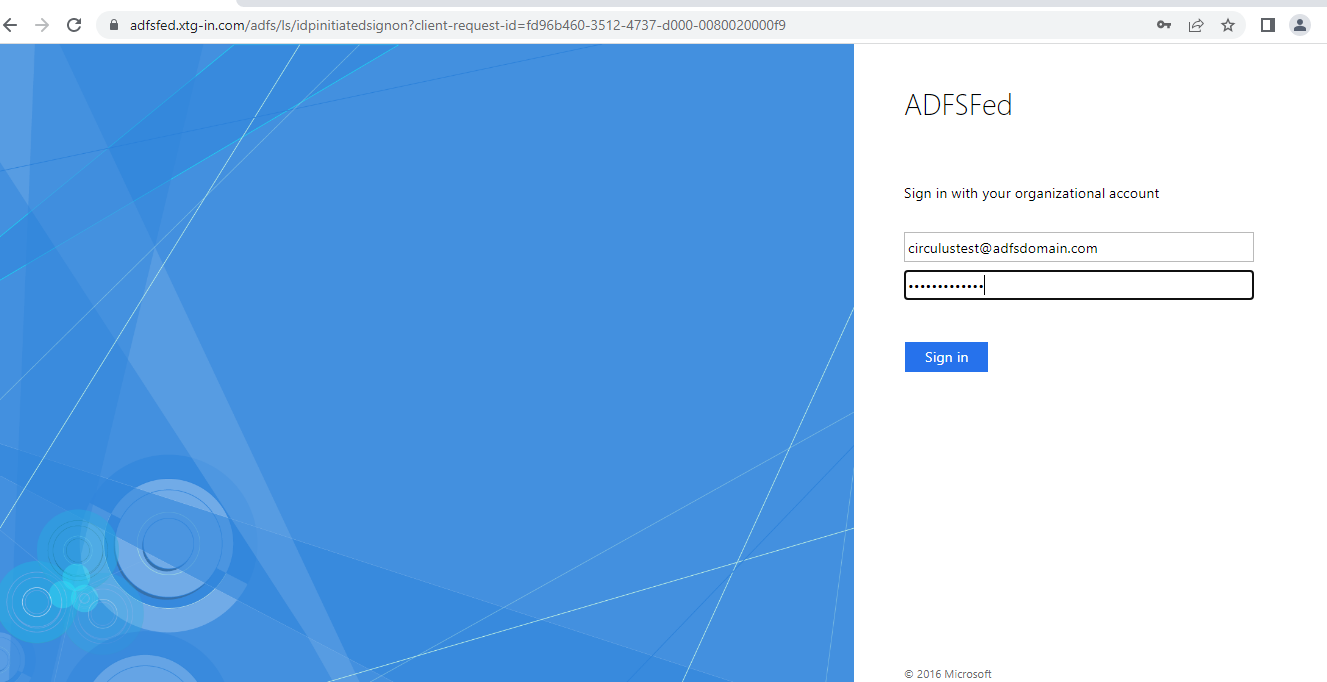
<https://adfsfed.xtg-in.com/adfs/ls/idpinitiatedsignon>



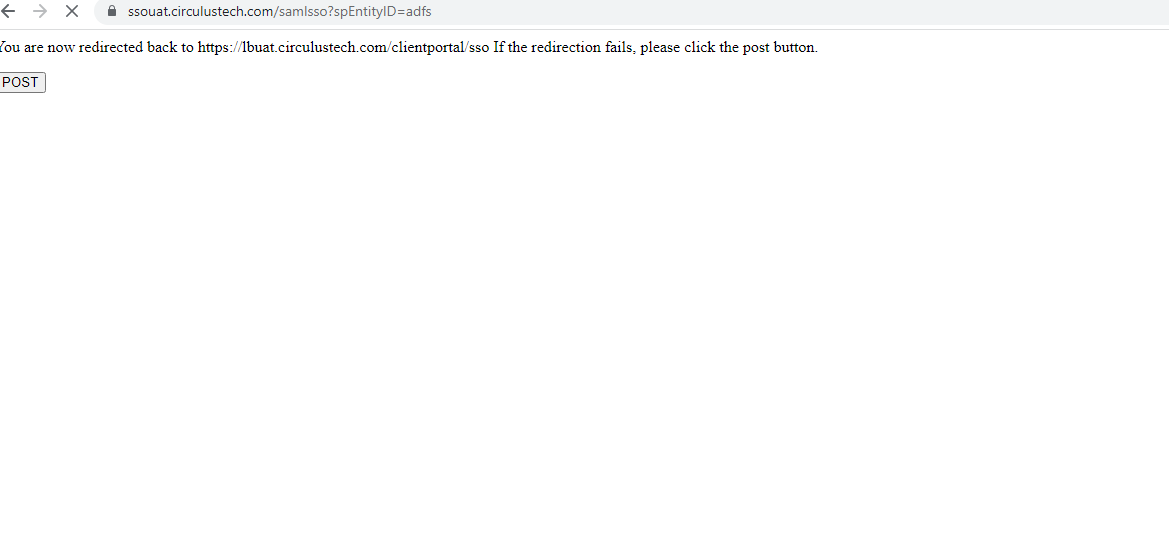
**Login Credentials for the test user: -**

circulustest@adfsdomain.com

!X3n0@$1234;!



Navigating to Client Portal



**Logs generating in the client portal :-**

DEBUG LoginManagerImpl:175 [UID: |CID: |CIID: |XID: |SID: ] - sso input values :: {ClientCode=SEG, Subject=circulustest@adfsdomain.com}  
DEBUG LoginManagerImpl:201 [UID: |CID: |CIID: |XID: |SID: ] - Invoking Rest Template :  userDetails::   {productID=null, encryptPassword=, moduleName=CLIENT\_PORTAL, mobileLoc=, ipAddress=122.183.21.66, employeeId=circulustest@adfsdomain.com, emailId=, language=ENGLISH, sessionId=nTvr9Jvp3yWMRlzKMXE3x7NykM-WsLEWoKlVhGLHyULtOyaLbe7z!-1740608342!1657521085417, source=WEB, operatingSystem=Windows, mobileNum=, clientCode=SEG, browser=Chrome 10, browserVersion=103.0.0.0}

Reference Links: -

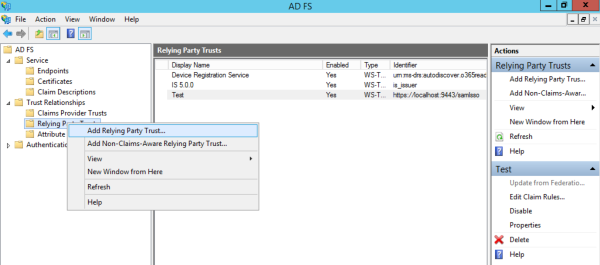
[Setting AD FS 3.0 as a SAML Federated Authenticator in WSO2 Identity Server | by Omindu | Medium](https://omindu.medium.com/setting-ad-fs-3-0-as-a-saml-federated-authenticator-in-wso2-identity-server-947ad007e3e7)

# Prerequisites

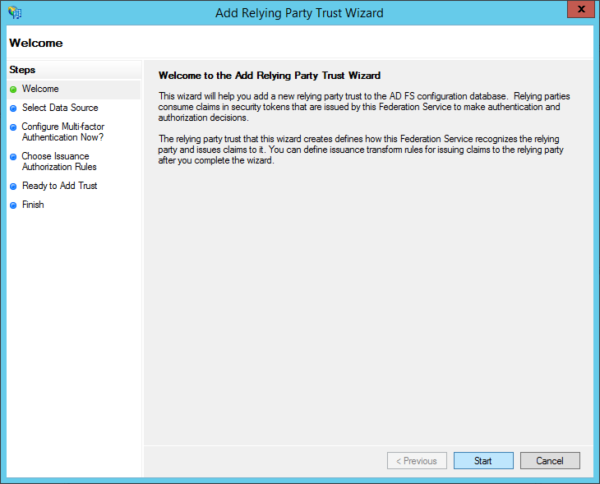
* WSO2 Identity Server 5.1.0 M3 or above Identity Server Service Pack 2 (yet to be released)
* ADFS 3.0

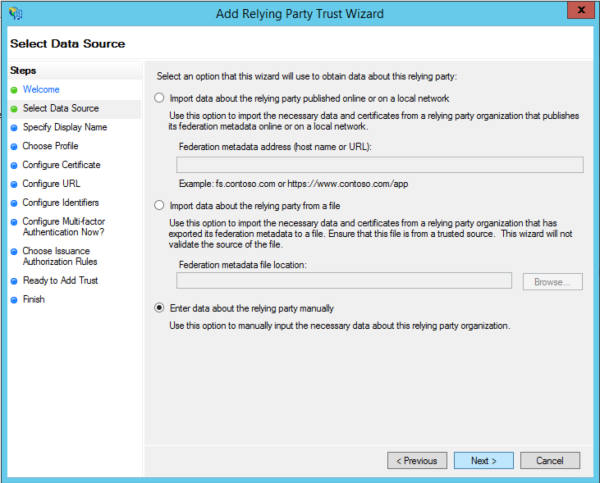
# Adding IS as a Relying Party in ADFS

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

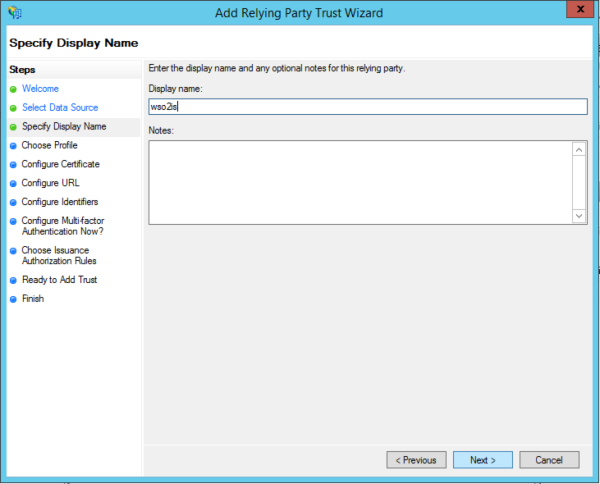


Follow the wizard as shown below

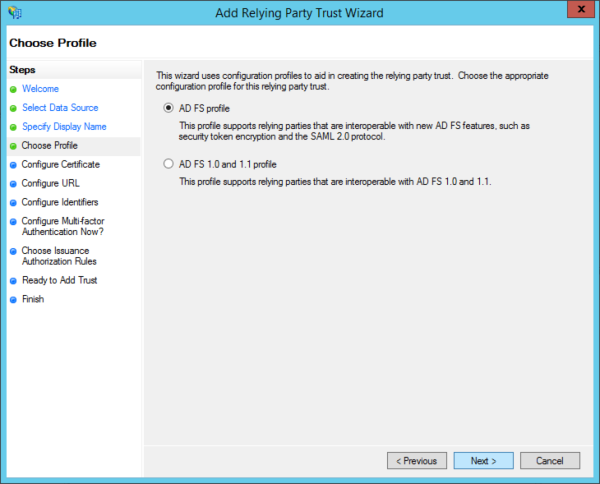




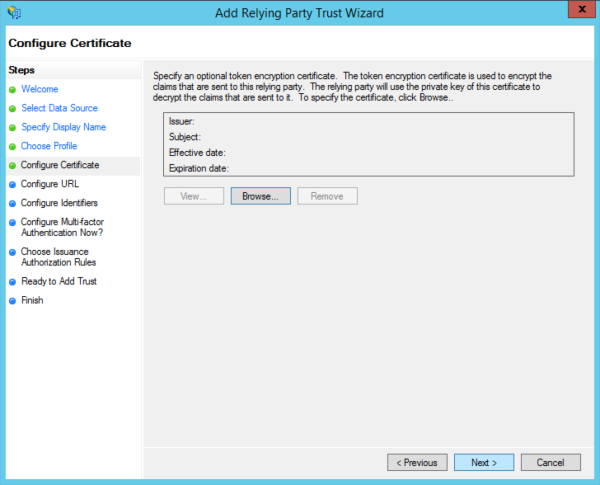
Type a desired display name for the relying party and click **Next.**



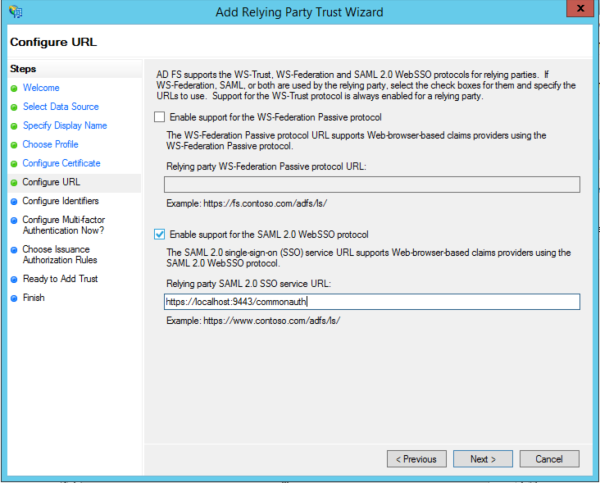
Select AD FS Profile and Click **Next.**



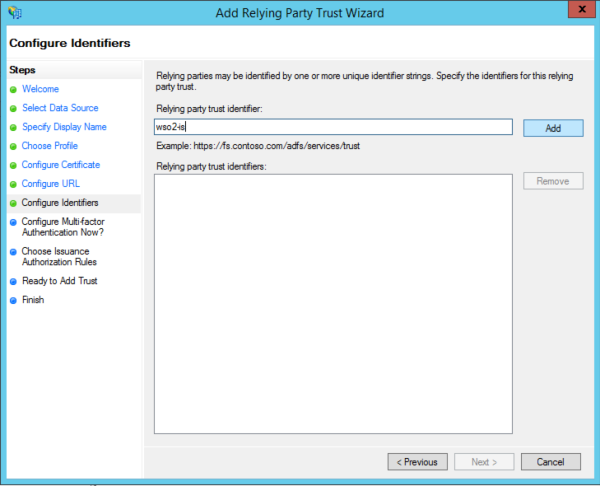
We are not using an encryption certificate so click **Next.**



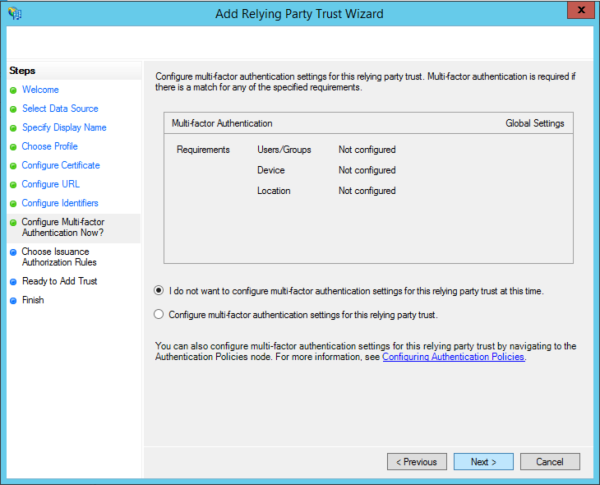
Set the relying party SAML 2.0 SSO service url to the **commonauth** endpoint of IS. e.g:[**https://localhost:9443/commonauth**](https://localhost:9443/commonauth)



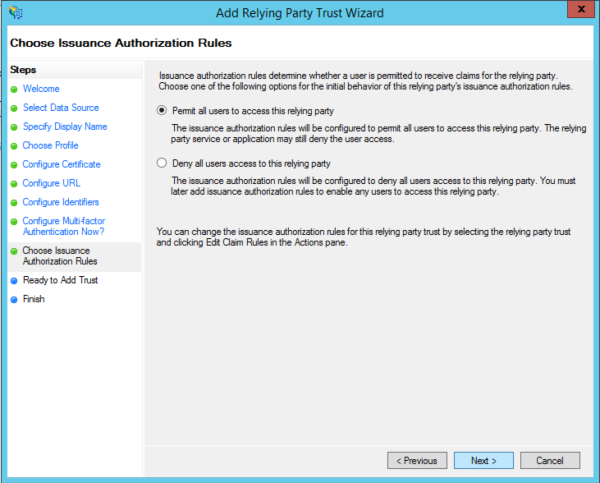
Add the relying party trust identifier and click **Next**. The value you enter here should be entered in IS IdP settings as well. Setting up the IdP is explained in the next section.



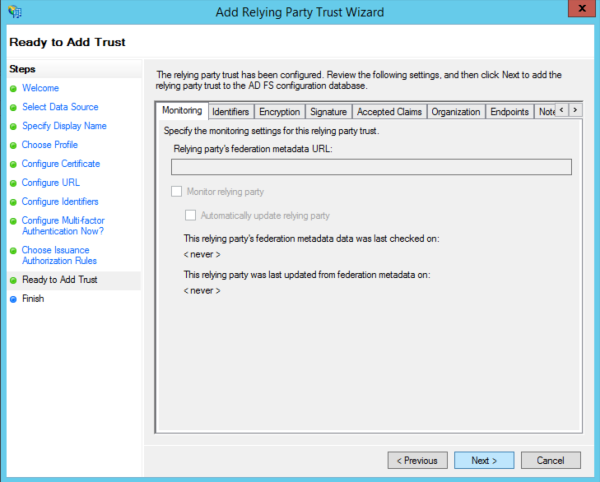
We won’t be configuring multi-factor authentication so click **Next.**



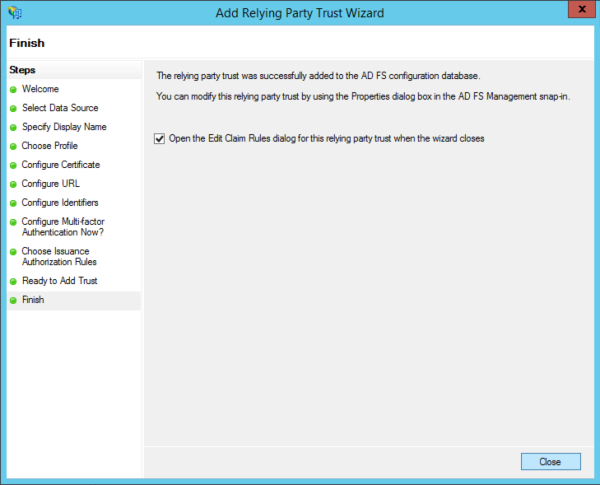
Select **Permit all users to access this relying party**and click **Next.**



Review the settings and click **Next.**

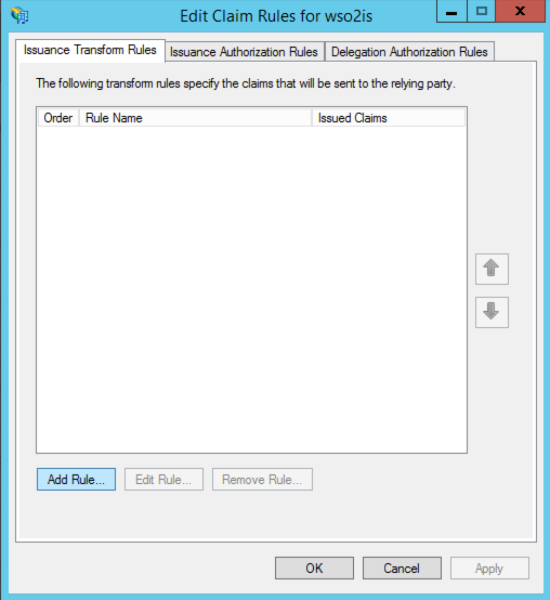


Click **Close** to finish adding the relying party trust. Also let the wizard to open the Claim Rules dialog

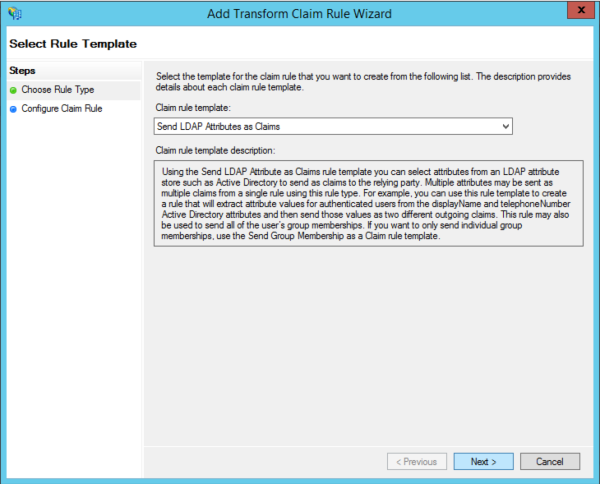


In the **Edit Claim Rule**dialog we will specify which claims to be sent to the relying party. In this example I’m sending the SAM-Account-Name LDAP attribute as a NameID claim.

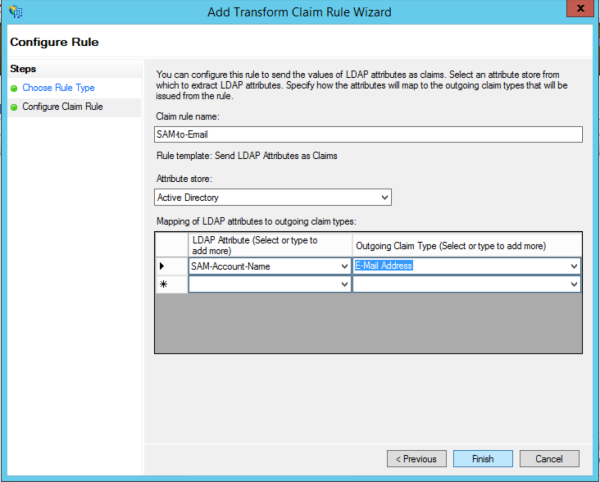
First click **Add Rule…**



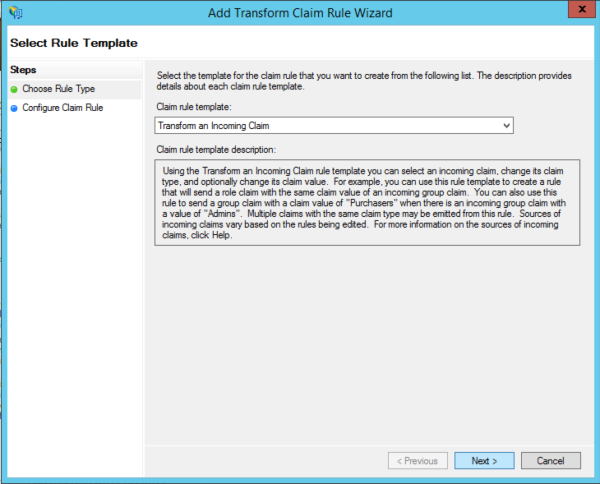
Select **Send LDAP Attributes as a claim**and click **Next.**



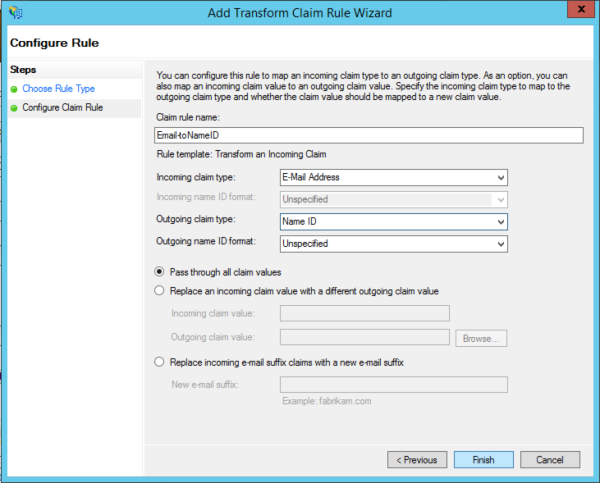
Set a **Claim rule name**and map SAM-Account-Name to E-Mail Address. Then click **Finish.**



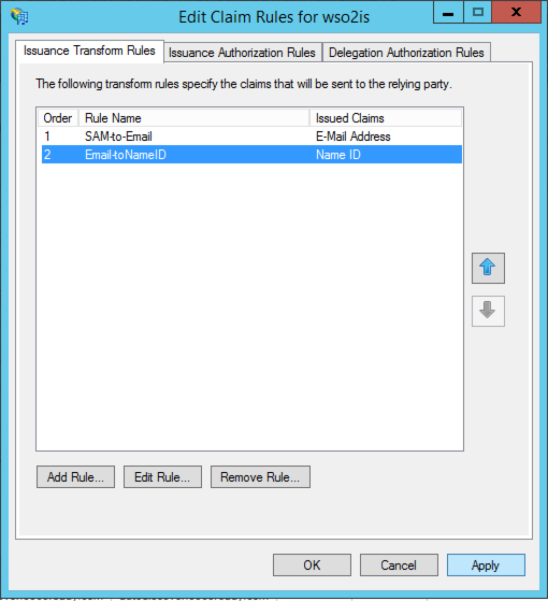
Click **Add Rule…**again to transform the email address claim to NameID claim. Select **Transform an Incoming Claim**and click **Next.**



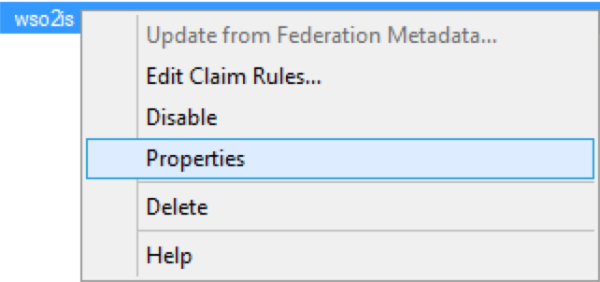
Set the Claim rule name. Select the incoming claim type as **E-Mail Address**and outgoing claim type and ID format as **Name ID**and **Unspecified**respectively. Then click **Finish.**



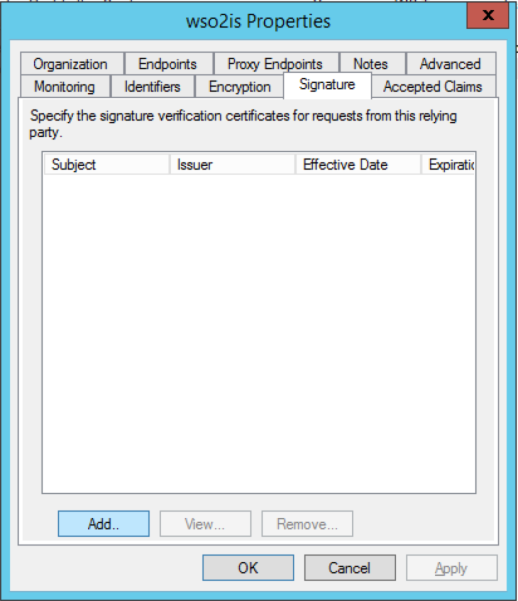
Then apply and close the claim rules dialog.



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.**



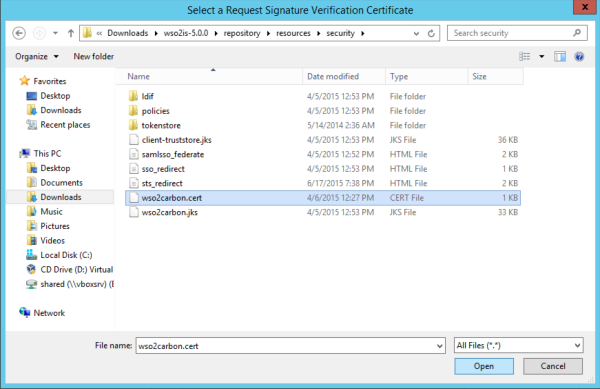
Goto **Signature**tab and click **Add.**



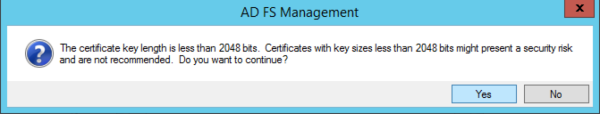
The certificate which should be added here depends on a couple of things. If the Service Provider in IS is under the super tenant domain. The public certificate of IS should be used. Else, the public certificate of the tenant domain should be selected. The public certificate of the tenant can be exported from the Key Management feature of the IS management console. In this post, the service provider is added in the super tenant domain and the default keystore has not been change. Therefore the default wso2carbon certificate is used. You can export the certificate from **wso2carbon.jks**which is located at **/repository/resources/security/** directory.

The default public certificate can be exported as follows.

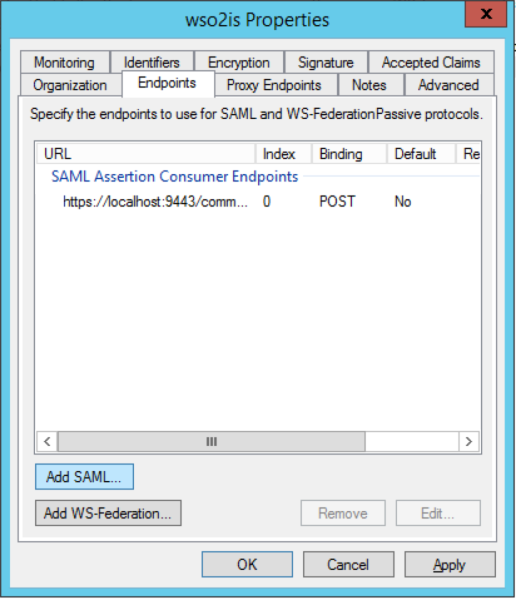
*keytool -export -keystore wso2carbon.jks -alias wso2carbon -storepass wso2carbon -file wso2carbon.cert*



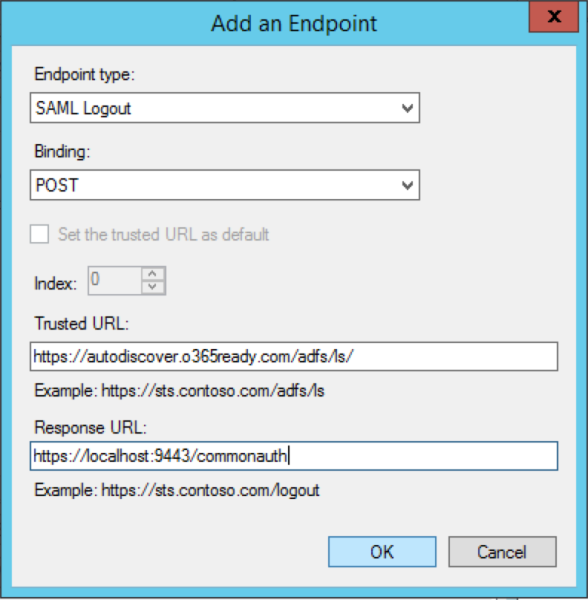
When importing the default certificate you will get the following dialog. Click **Yes**to proceed.



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

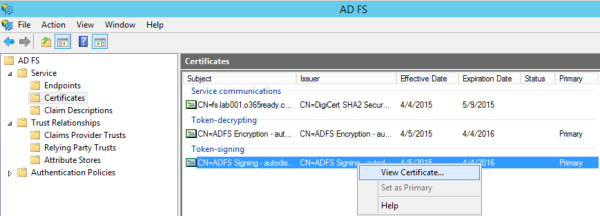


Select Endpoint Type as SAML Logout and the Binding as POST. Set the Trusted URL as**https://<AD\_FS\_server>/adfs/ls** and the Response URL as the **/commonauth** endpoint of IS. Once it is done save the property settings of the RP.



Next we will move on to configuring AD FS as an Identity Provider in IS. For the configurations we will have to add the Token signing certificate of AD FS. To export the token signing certificate of IS do as follows.

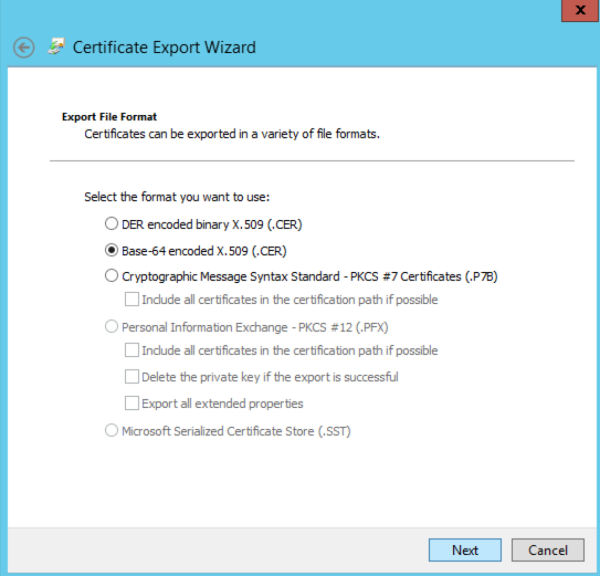
In AD FS management UI, click on Certificates under Service, right click on Token-signing certificate and select **View Certificate.**



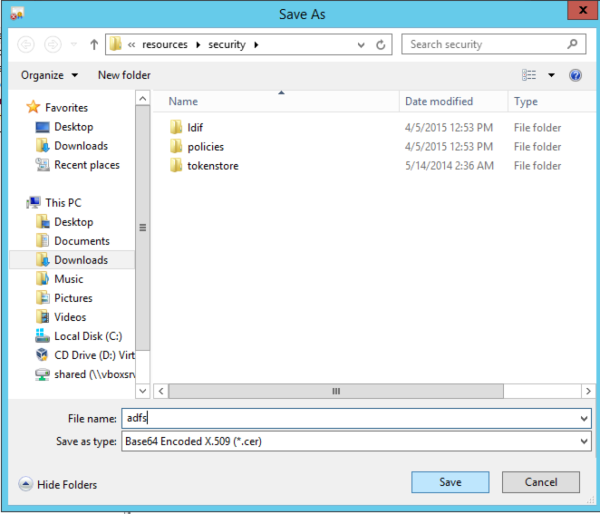
Goto **Details** tab and click **Copy to File…**Then follow the Certificate Export Wizard.

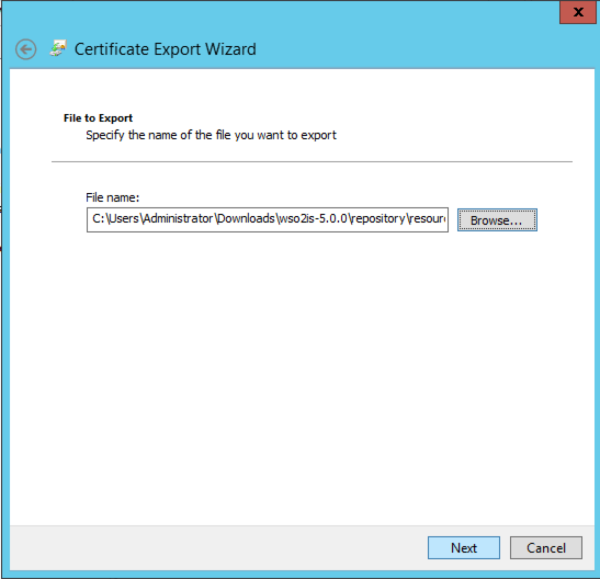


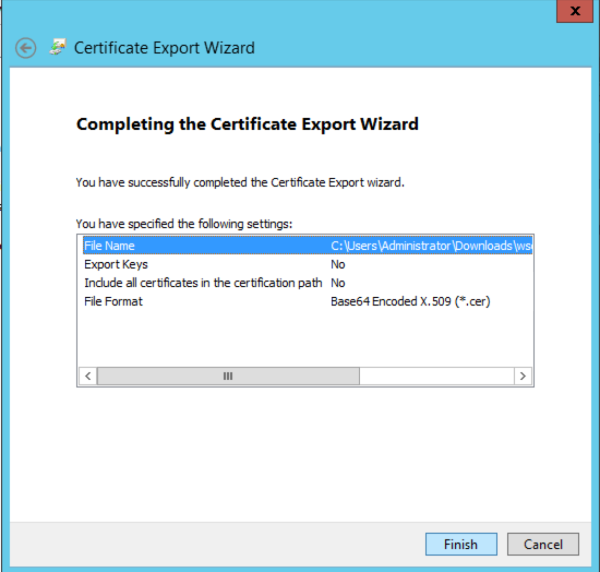
Select Base-64 encoded X.509 (.cer) and click **Next.**



Save the certificate to a desired location and Finish the wizard.



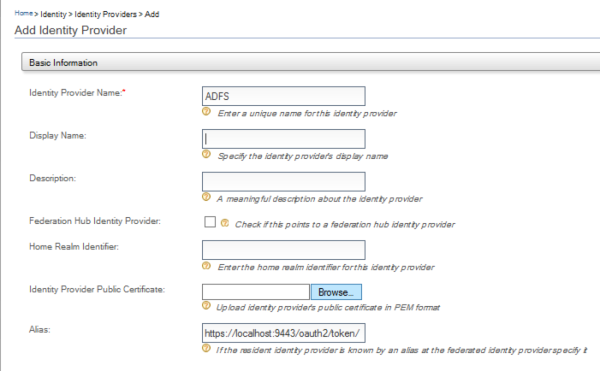




We will move on to configuring IS next.

# Adding AD FS as a Federated Authenticator in IS

Login to IS Management console and click **Add**under Identity Providers. Type a unique name for the IdP and add the Token-signing certificate of ADFS by clicking the **Browse**button.



Next set the SAML Web SSO Configuration under Federated Authenticators.

* Check **Enable SAML2 Web SSO**
* Identity Provider Entity Id: This can be found in FederationMetadata.xml under **entityID**attribute. The FederationMetadata.xml can be accessed through **https://<AD\_FS\_server>/FederationMetadata/2007-06/FederationMetadata.xml**. The Entity ID is usually in the form **http://<AD\_FS\_server>/adfs/services/trust**
* Service Provider Entity Id should be same as what’s given in AD FS RP trust identifier. **eg:wso2-is**
* SSO URL should be in the form of **http://<AD\_FS\_server>/adfs/ls**
* Check **Enable Logout**
* Logout URL should be the same as SSO URL
* Check **Enable Logout Request Signing**
* Select **HTTP Binding**as **POST**

Once the details are entered click **Register** to save the IdP.

