ORACLE
FINANCIAL SERVICES

SAML 2.0 SSO Implementation for Oracle Financial Services Lending and Leasing

Using Active Directory and Active Directory Federation Services as Identity Provider (IdP)

ORACLE WHITE PAPER | May 2022

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

Introduction

The indent of this document is to showcase a proof-of-concept on SAML 2.0 based Single Sign-On feature using Active Directory Federation Services (henceforth termed as AD FS) for Oracle Financial Services Lending and Leasing product (henceforth termed as OFSLL).

This document covers the basic steps followed to install and configure AD FS, followed by configuration of Weblogic Managed Server where the OFSLL application is deployed. The details mentioned are more of a lab setup, for production additional settings may be required which is out-of-scope of this document. This is a reference document for following audiences:

- System Administrators
- Weblogic Administrators
- Product Managers
- Technical Resources

Pre-requisite

Components

The list of components required for this POC are

- Windows 2012 R2 Server (henceforth referred as AD Server)
  - MS Active Directory installed and configured
  - MS Active Directory Federation Services

Note: Windows 2012 R2 server comes default with AD FS 3.0 however does support 2.0, the scope of this document is AD FS 2.0

  - IIS Manager

Note: IIS Installation is out-of-scope; IIS can be installed as stand-alone or while installing AD FS, would get auto-selected as part of dependent required components.

- Weblogic 10.3.6 Server (henceforth referred as OFSLL Server)

Assumptions

- Windows 2012 R2 Domain Server is installed and configured as a domain controller and Active Directory is installed and configured on AD Server. The detailed installation and configuration steps of Windows 2012 R2 server and MS Active Directory are out-of-scope.
- Weblogic is installed and configured with an OFSLL domain. The domain should have at least one Managed Server (henceforth referred as ofsll_managedserver2) apart from Admin Server. JRF templates are applied and OFSLL application is deployed on to the Managed Server.
- The steps covered in this document are for a single Weblogic node setup and does not cover that of cluster setup. Where ever there is a difference for cluster setup same is denoted.

» Add few users to Active Directory on AD Server
» Install IIS Manager on AD Server

Installation of Active Directory Federation Services

Install AD FS on AD Server

Logon to AD Server (Active Directory Domain Server) using an administrator Id.

» Open Server Manager
» Click Add Roles and Features
» Proceed the steps until Select server roles interface
» Click Active Directory Federation Services and proceed with next

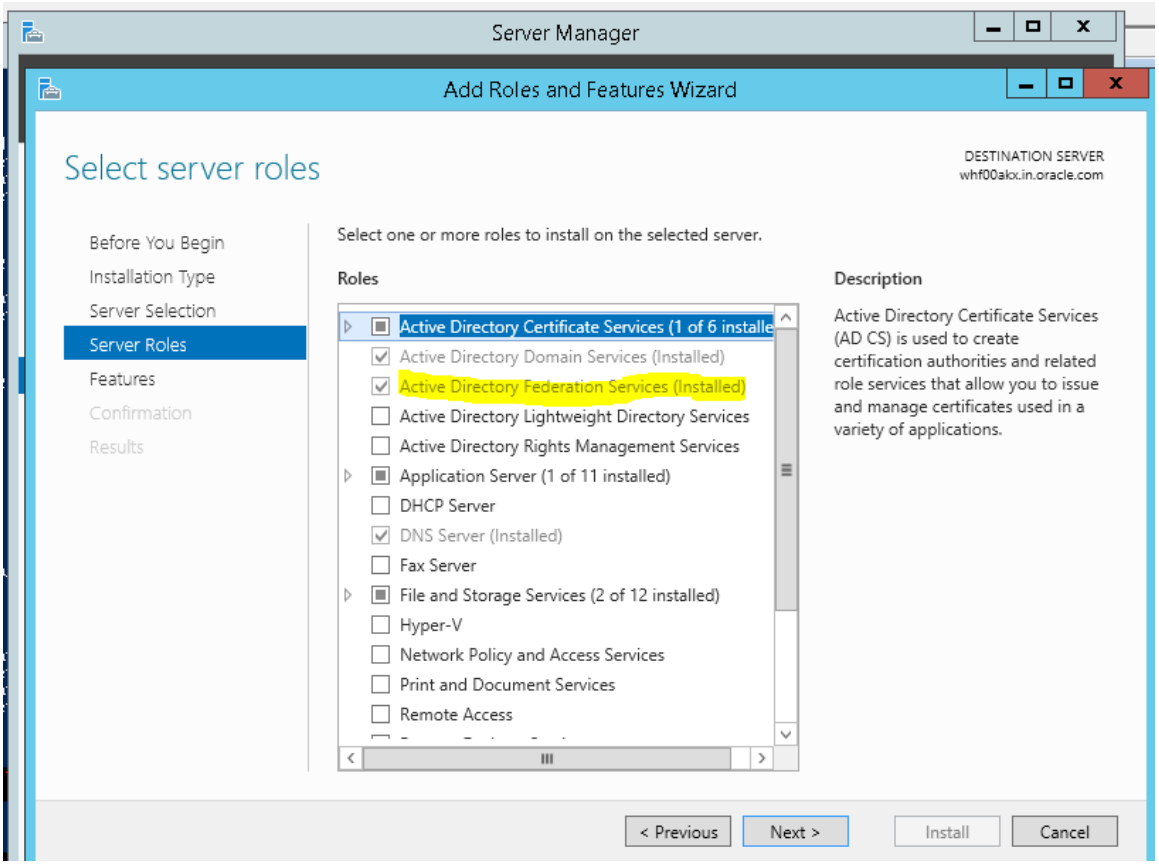

Figure 1. Install AD FS –Server Roles

» On the Select Features interface, click Next

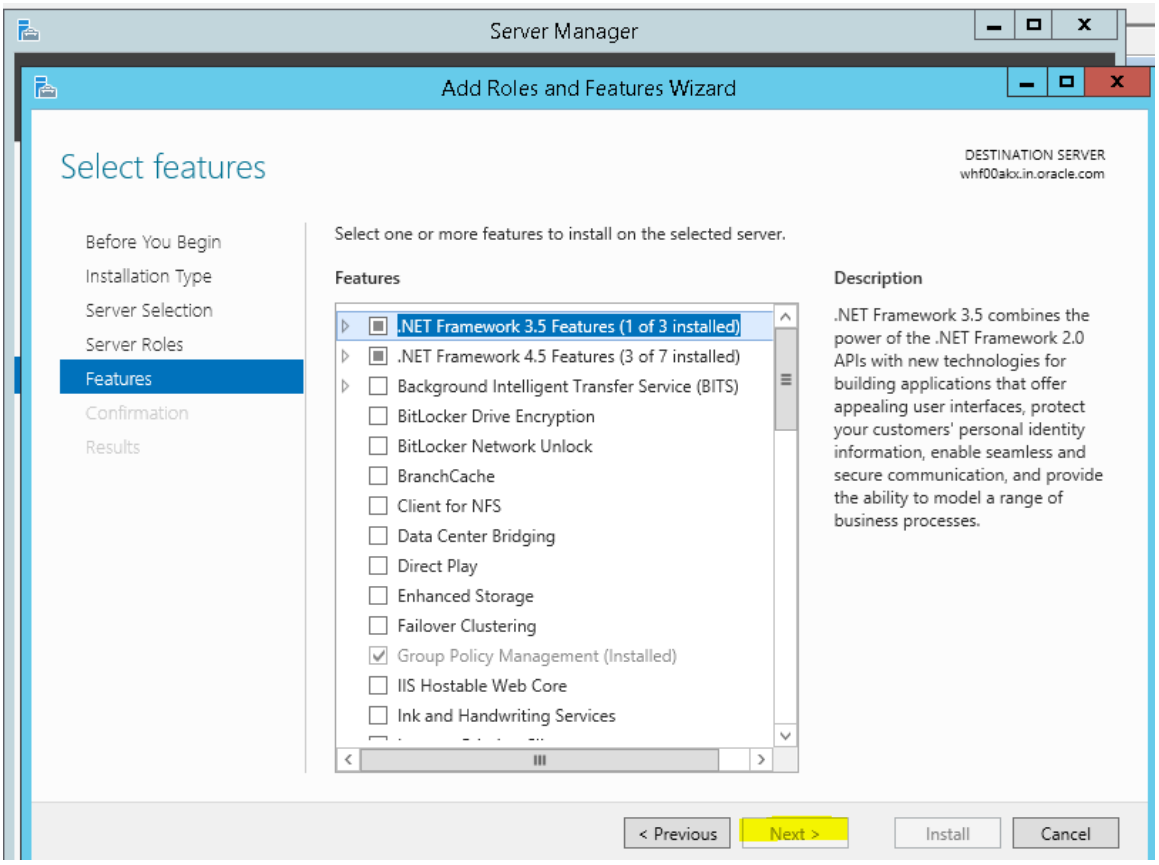

Figure 2. Install AD FS – Select Features

» On the Active Directory Federation Services (AD FS) interface, click Next

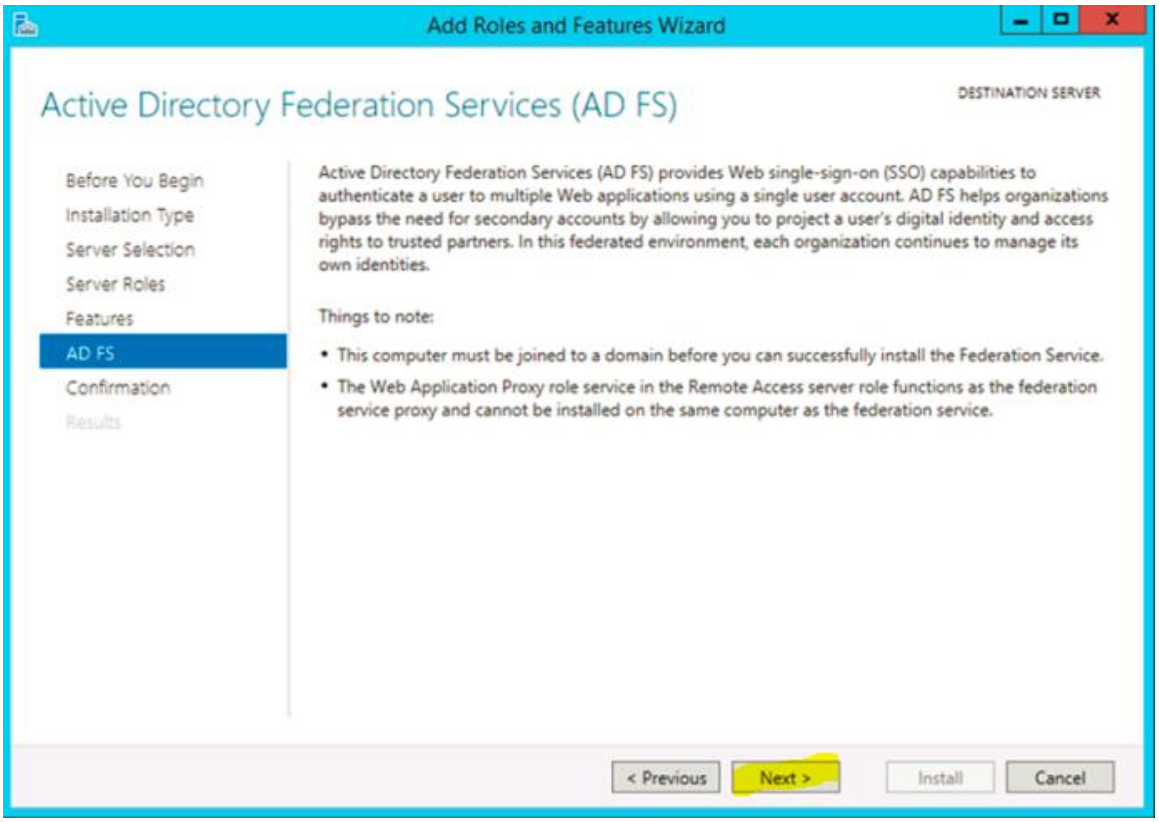

Figure 3. Install AD FS – AD FS Page

» Click Install

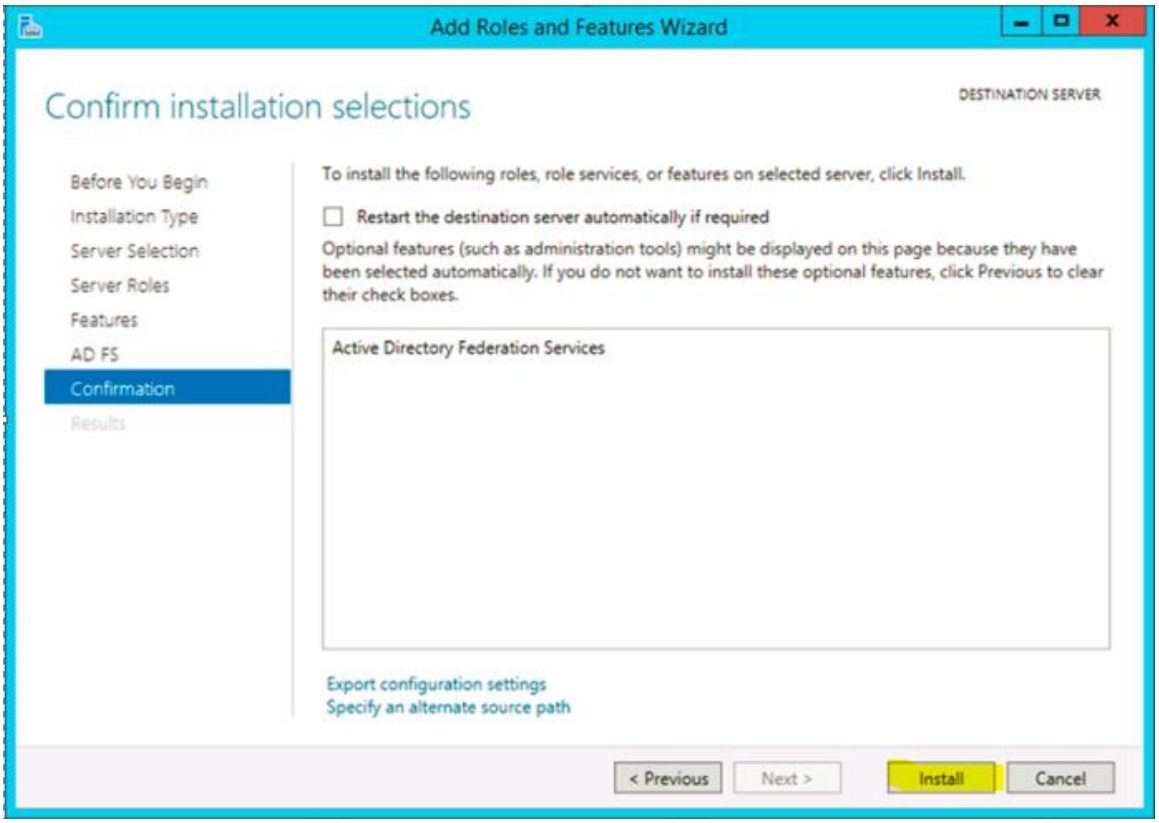

Figure 4. Install AD FS – Confirmation Page

» Once the installation completed, click “Configure the federation service on this server”

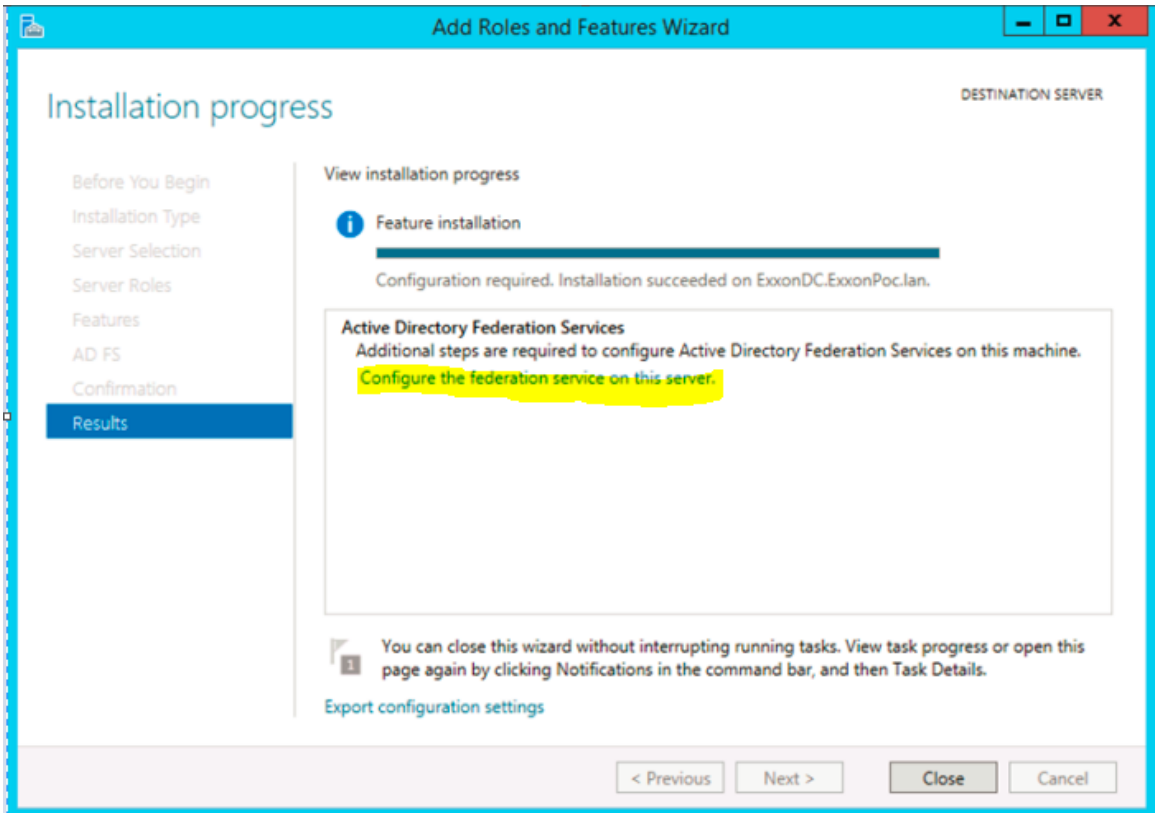

Figure 5. Install AD FS – Result Page

Configure AD FS

Before configuring AD FS ensure following are made available:

» An Active Directory domain administrator account
  » Default “Administrator” account can also be used
» A publicly trusted certificate for SSL server authentication

Note: Since this is a POC, a self-signed certificate was used. Self-signed certificate can be created various ways; here going to showcase the self-signed certificate using makecert.exe and pvk2pfx.exe available as part of Windows 2012 R2 server, available as part of Windows SDK disk.

How to Create Self-signed Certificate

This step is optional and required since this POC is using a self-signed certificate.

- Open Windows Power Shell command prompt on AD Server
- Run following commands:
  - makecert.exe -n "CN=*.ofsll.com" -pe -a sha1 -len 2048 -r -cy authority -sv CACer.pvk CACer.cer –e 10/10/2020

Note: a wild card self-signed certificate is created in above sample with an expiration year of 2020

  - pvk2pfx.exe -pvk CACer.pvk -spc CACer.cer -pfx CACer.pfx -pi <password>

How to Register the Certificate

The self-signed certificate (CACer.pfx) created above must be registered with AD Server.

- Import above certificate using following steps:
  - Open IIS Manager, click on Server Certificates

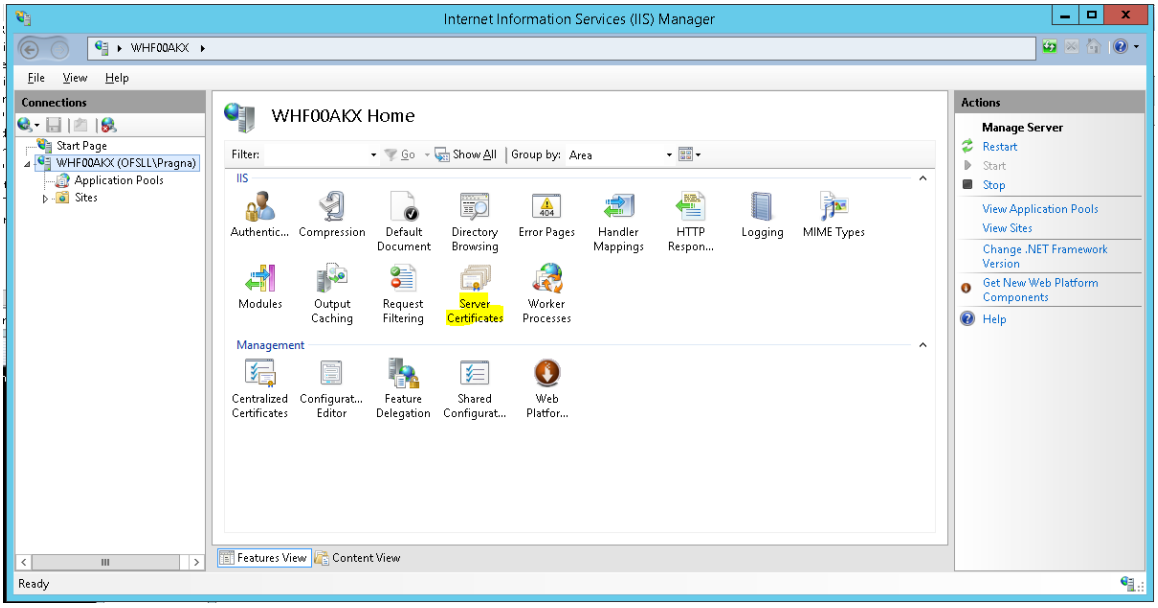

Figure 6. IIS Manager – Main Page

» Click on import link

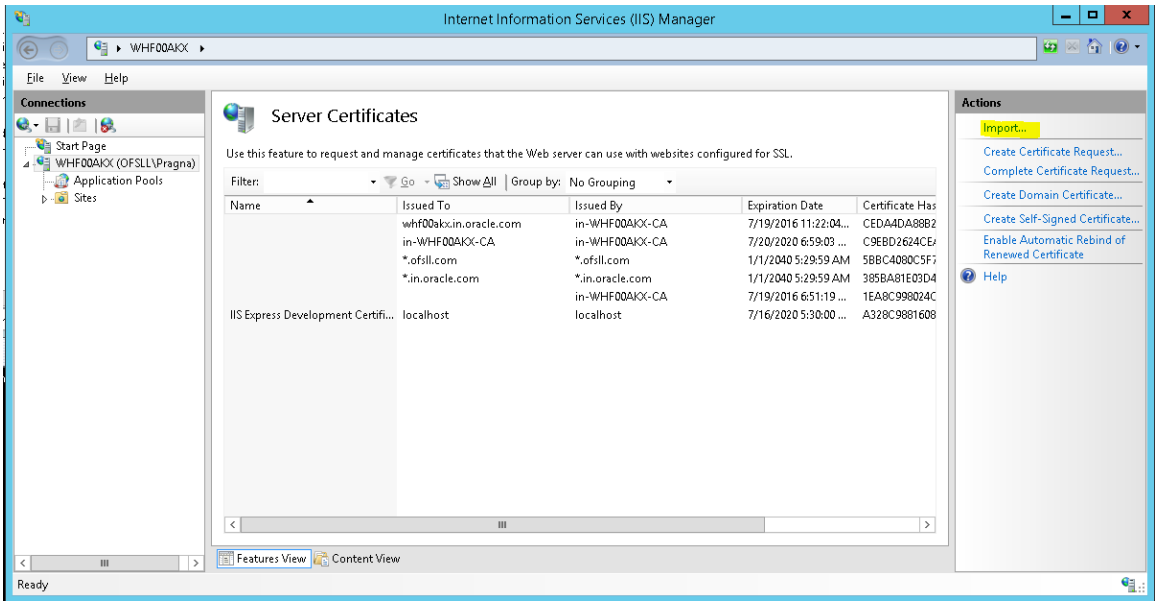

Figure 7. IIS Manager - Server Certificates

» Upload the certificate “CACer.pfx” file generated in previous section and password

» Click Ok to import the certificate

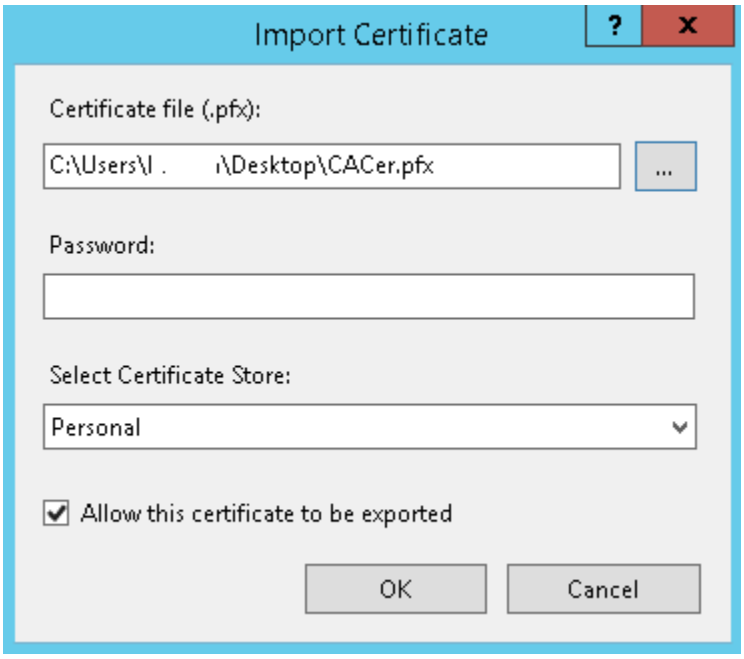

Figure 8. IIS Manager – Import Certificate

Now all pre-requisites are met and system is ready to configure AD FS.

AD FS Configuration

» On the Welcome interface, click Create the first federation server in a federation server farm, and click Next

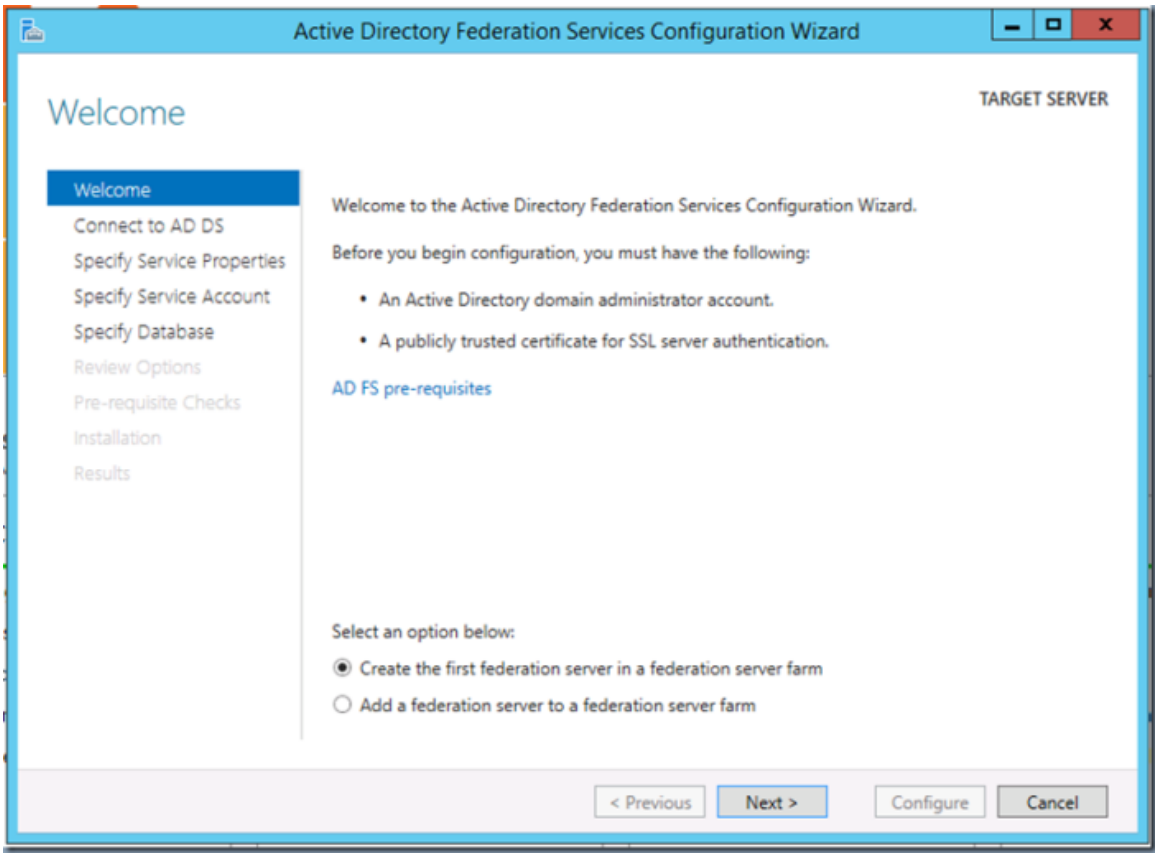

Figure 9. AD FS Configuration – Welcome Page

» On the Connect to Active Directory Domain Services interface, proceed with Next.

» In the first panel of the AD FS Configuration Wizard we will specify the AD account that has permissions to perform the federation service configuration.

Note: This account must be a Domain Administrator or can also be the default "administrator" user account.

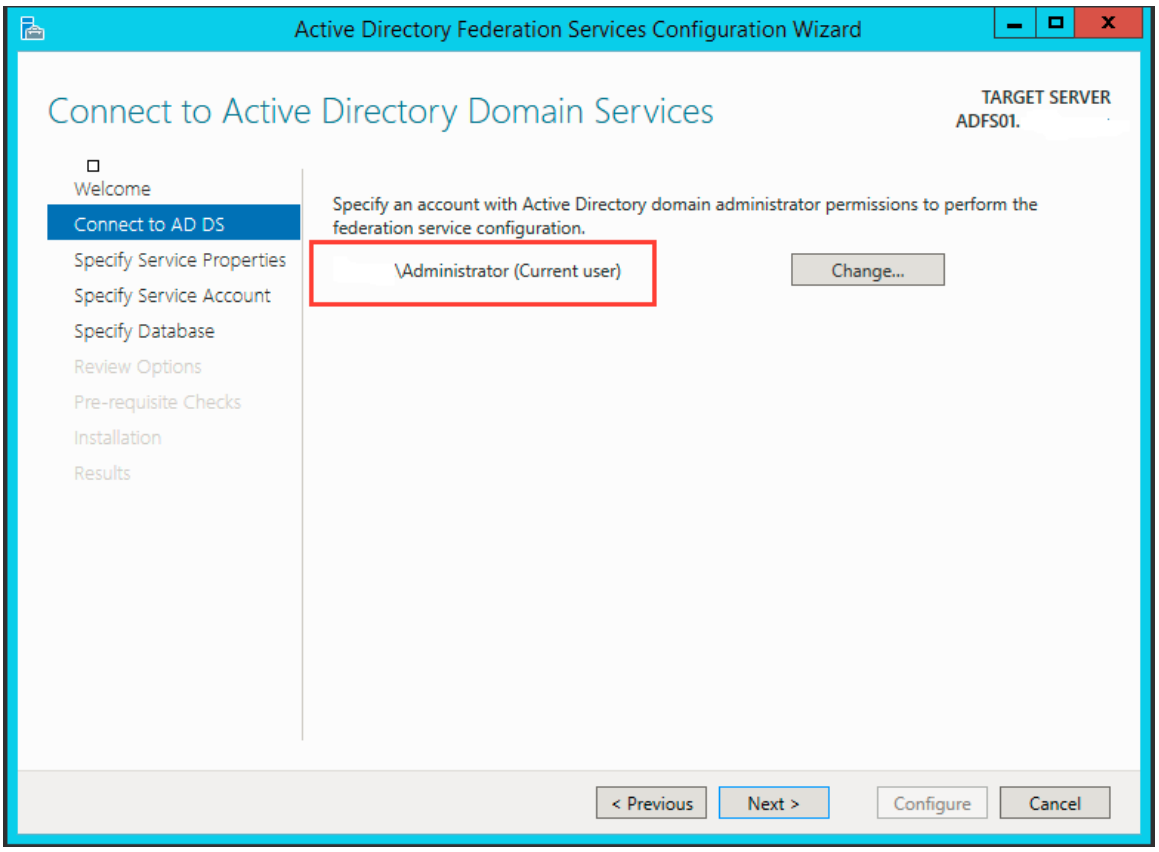

Figure 10. AD FS Configuration – AD Service Interface

» In the next panel, specify the service properties.

  » SSL Certificate → Select the certificate that was imported in previous section from the dropdown

  » Federation Service Name → Edit the default Federation Service Name of *.OFSLL.COM so that it reads as for example, STS.OFSLL.COM. This will be the federation service address and will serve as the root of sign-in URL.

Note: Ensure the service name is unique and no other services are using the same name.

  » Federation Service Display Name → Provide a Name for the Service

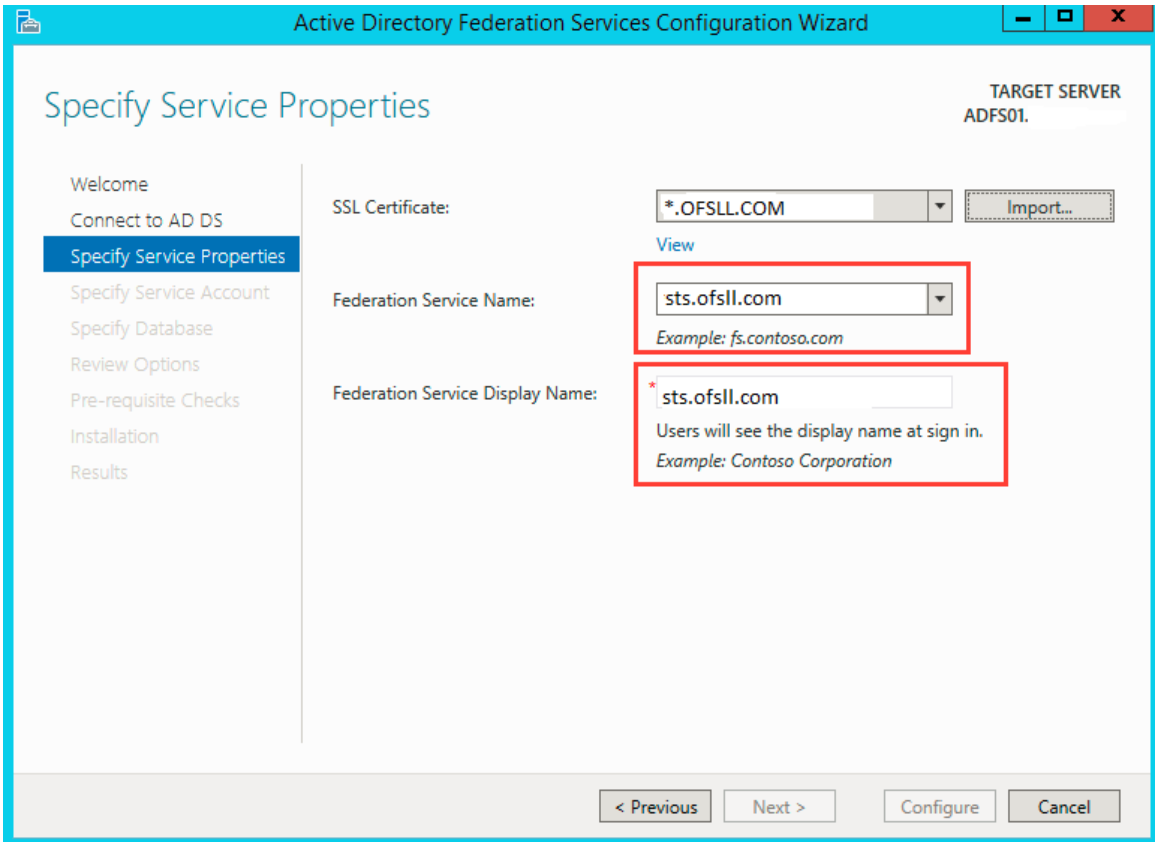

Figure 11. AD FS Configuration – Service Property Setup

» On the Specify Service Account interface, click create a domain user account or group Managed Service Account and then enter “ADFS_SVC”, and click next

  » This is going to be the managed service account used by AD FS Service to run.

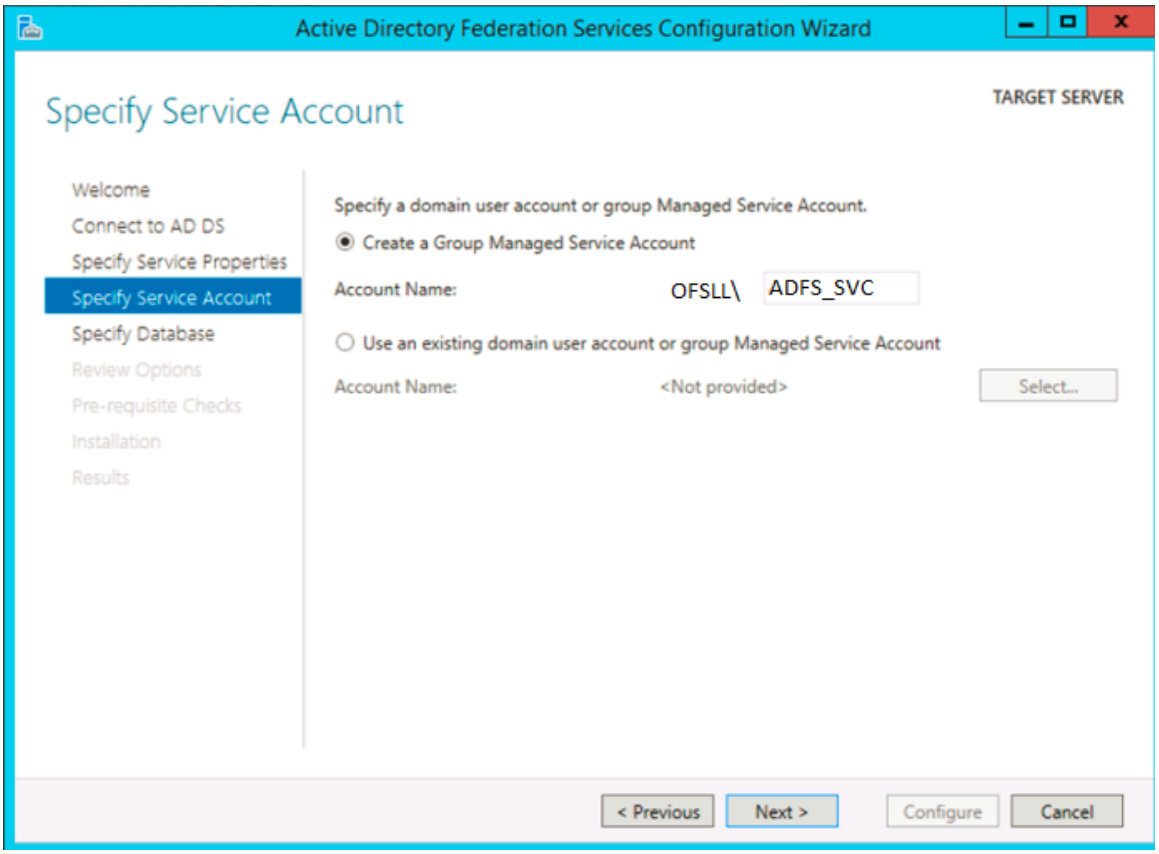

Figure 12. AD FS Configuration – Service Account Setup

» On the Specify Configuration Database interface, click Create a database on this server using Windows Internal Database, and click Next

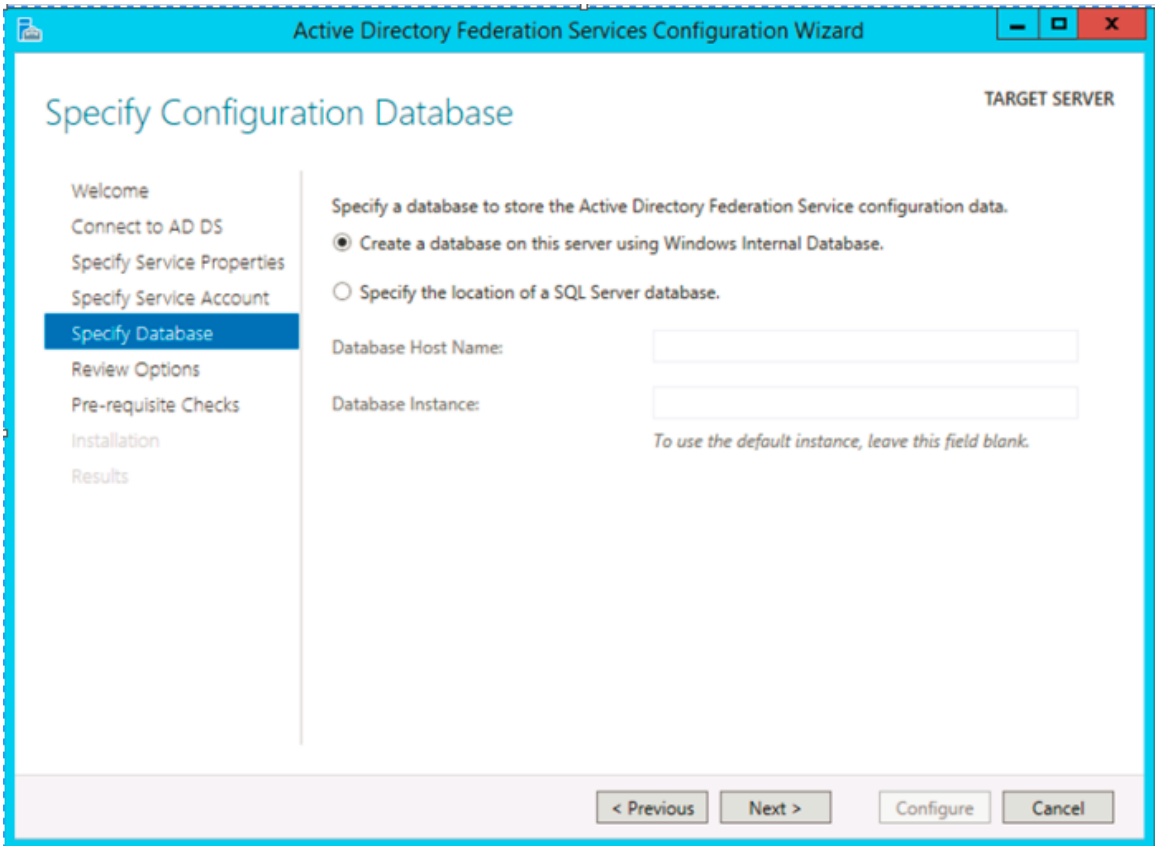

Figure 13. AD FS Configuration – Service Database Setup

» On the Review Options interface, click Next

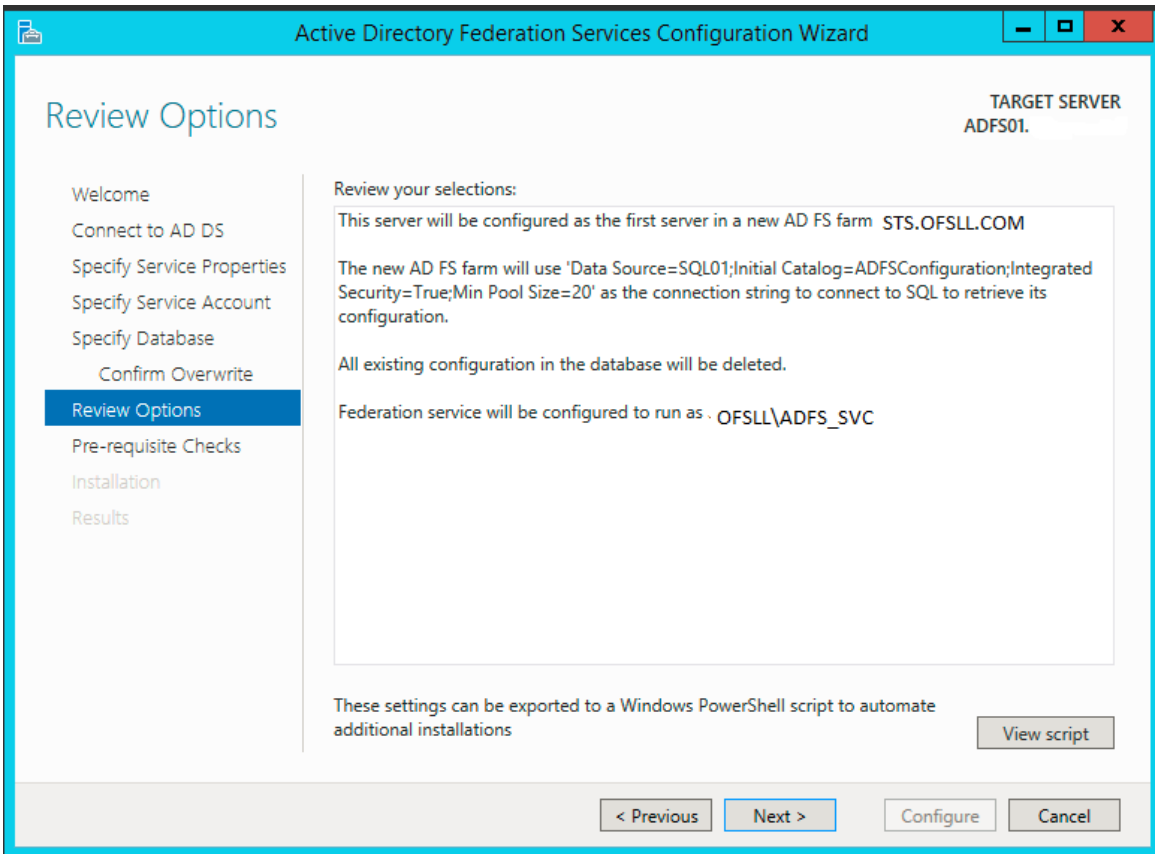

Figure 14. AD FS Configuration – Review Page

» On the Pre-requisite Checks interface, verify that all prerequisite passed and click Configure

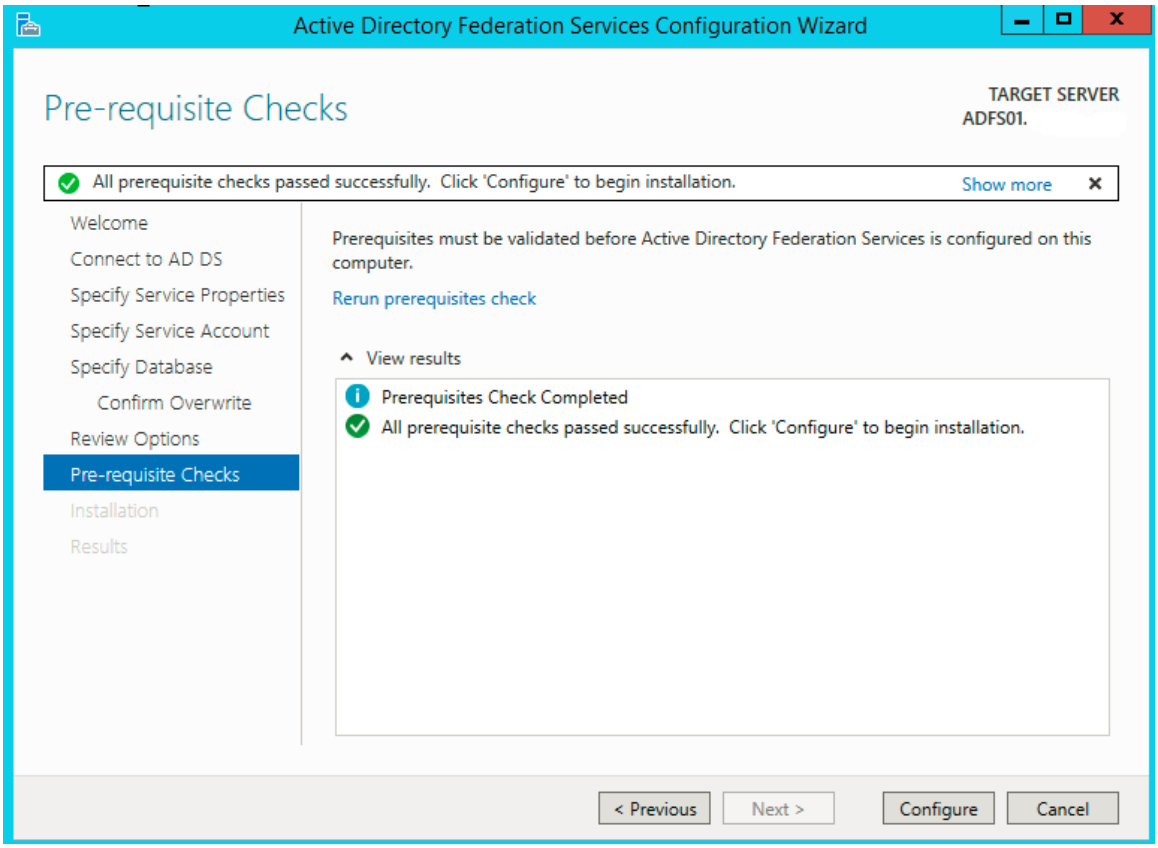

Figure 15. AD FS Configuration – Pre-requisite Check Page

» On the Results interface, click Close

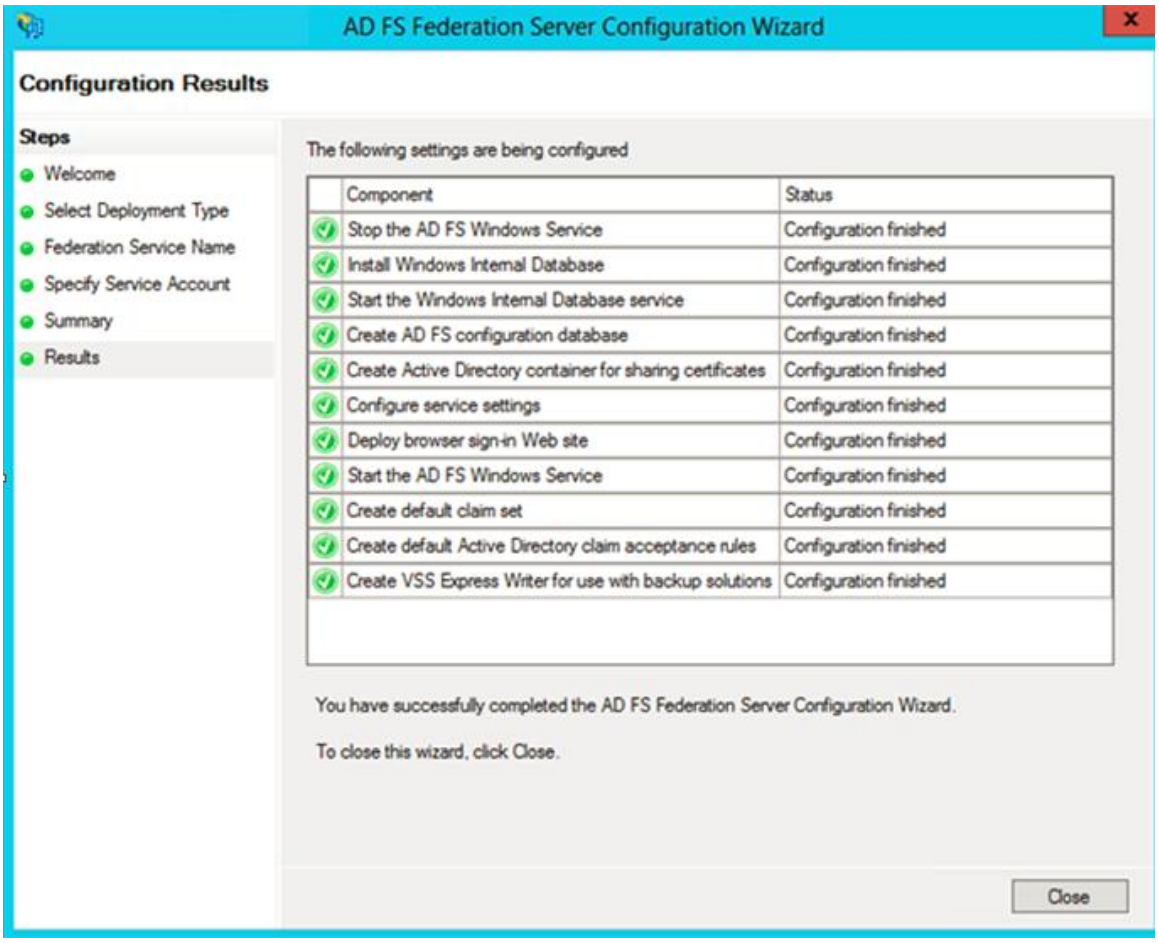

Figure 16. AD FS Configuration – Result Page

Verify AD FS Installation

Verify that the AD FS configuration is working properly.

» Logon to AD server, open Internet Explorer.

» Browse the URL of the federation metadata https://<your federation service name>/federationmetadata/2007-06/federationmetadata.xml

  » For example, https://sts.ofsll.com/federationmetadata/2007-06/federationmetadata.xml

» Verify that no certificate-related warnings appear. If necessary, check the certificate and DNS settings. If successful below federation metadata file would open up.

  » There may be a requirement to add the new service name (in this case sts.ofsll.com) be part of DNS entry or define an entry in HOSTS file.

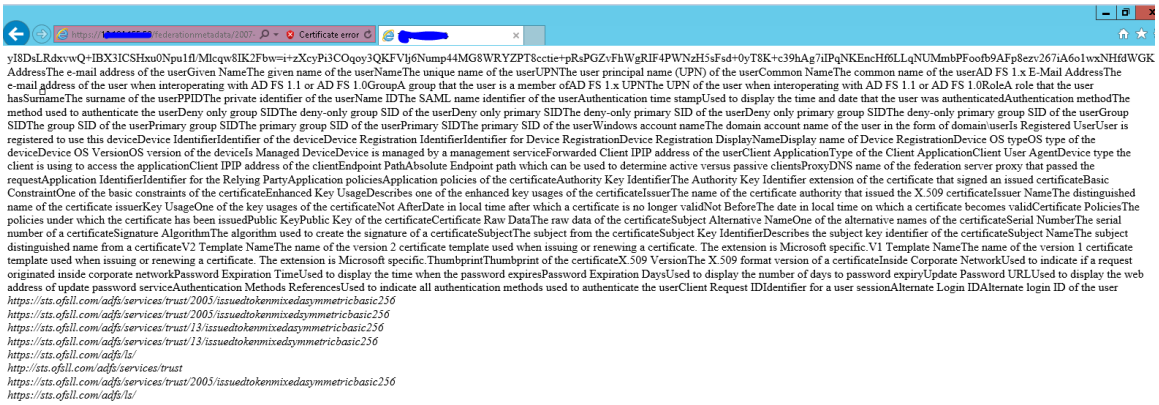

Figure 17. AD FS Configuration – Federation Metadata

All the pre-requisites are met for SAML 2.0 Web SSO Implementation on OFSLL Server. Ensure to download the above federationmedata.xml file in a safe place. This file is required as Identity Provider (IdP) file for Web SSO implementation on OFSLL Server (i.e. OFSLL Domain Weblogic Server).

Configuration on Weblogic Domain Server as Service Provider (SP)

FTP the federationmedata.xml downloaded in previous step onto OFSLL Server.

Pre-configuration of Managed Server

Before configuring the domain as Service Provider (SP), the SSL port has to be enabled on the Weblogic Managed Server (in this case on ofsll_managedserver2).

Note: While adding the endpoints in AD FS Management, http protocol errors out saying needs to be https URL; so SSL has to be enabled on managed server.

Enable SSL

- Go to WebLogic Console, enable SSL in weblogic
- Save and Activate Changes

Note: The default demo SSL certificate available as part of Weblogic domain has lesser bits length and encryption algorithm. The certificate while referred on AD server is going to error out. Hence the demo certificate has to be regenerated with a higher bits length of minimum 1024 as well as with a minimum SHA1 algorithm.

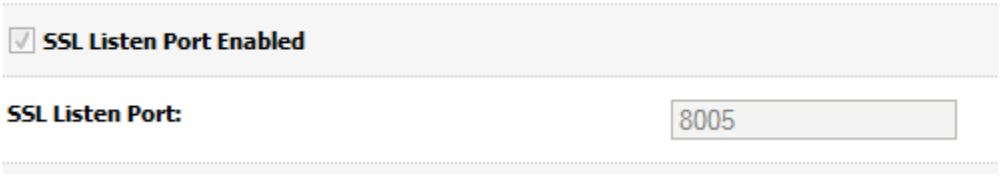

Figure 18. Weblogic Server – Enable SSL

Creation of Self-Signed Domain Certificate

Once again since this is POC, a self-signed certificate is created and used as part of Weblogic Domain. Steps followed to create a self-signed certificate for Weblogic domain are:

- Logon on to OFSLL physical server via putty
- Set the JDK classpath to the JDK1.6+ path
- Run the following command
  - $JAVA_HOME/bin/keytool -genkey -alias mykey -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keypass password1 -keystore identity.jks -storepass password123

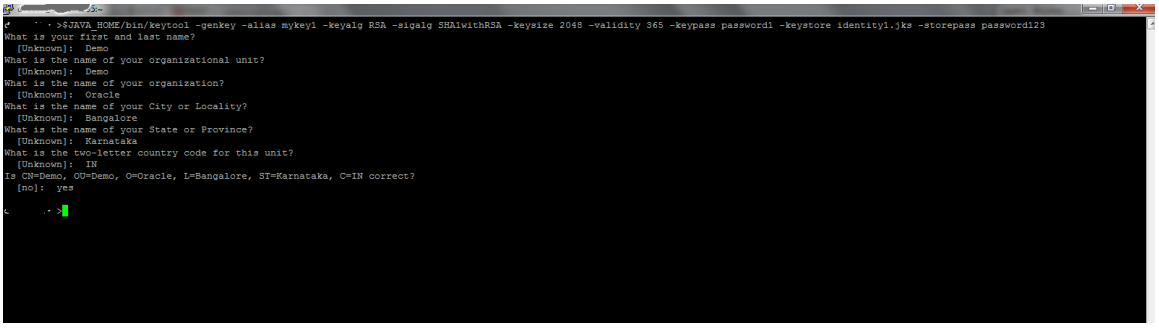

Figure 19. Weblogic Physical Server – Identity Generation

- $JAVA_HOME/bin/keytool -export -alias mykey -file root.cer -keystore identity.jks -storepass password123

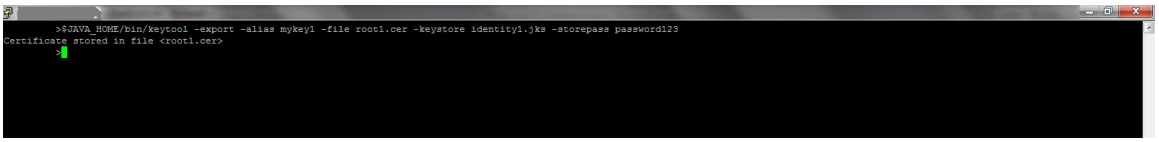

Figure 20. Weblogic Physical Server – Certificate Generation

» $JAVA_HOME/bin/keytool -import -alias mykey -file root.cer -keystore trust.jks -storepass password123

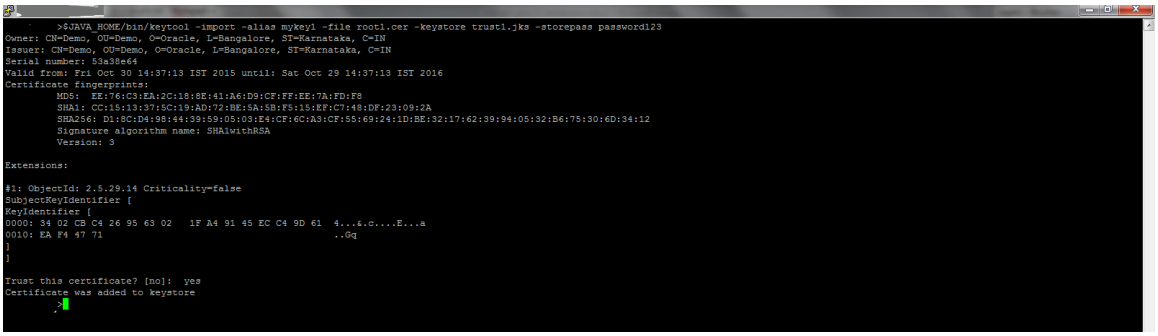

Figure 21. Weblogic Physical Server – Keystore Generation

» Copy the keystore files in the $DOMAIN_HOME location, where $DOMAIN_HOME is the Weblogic Domain path location.

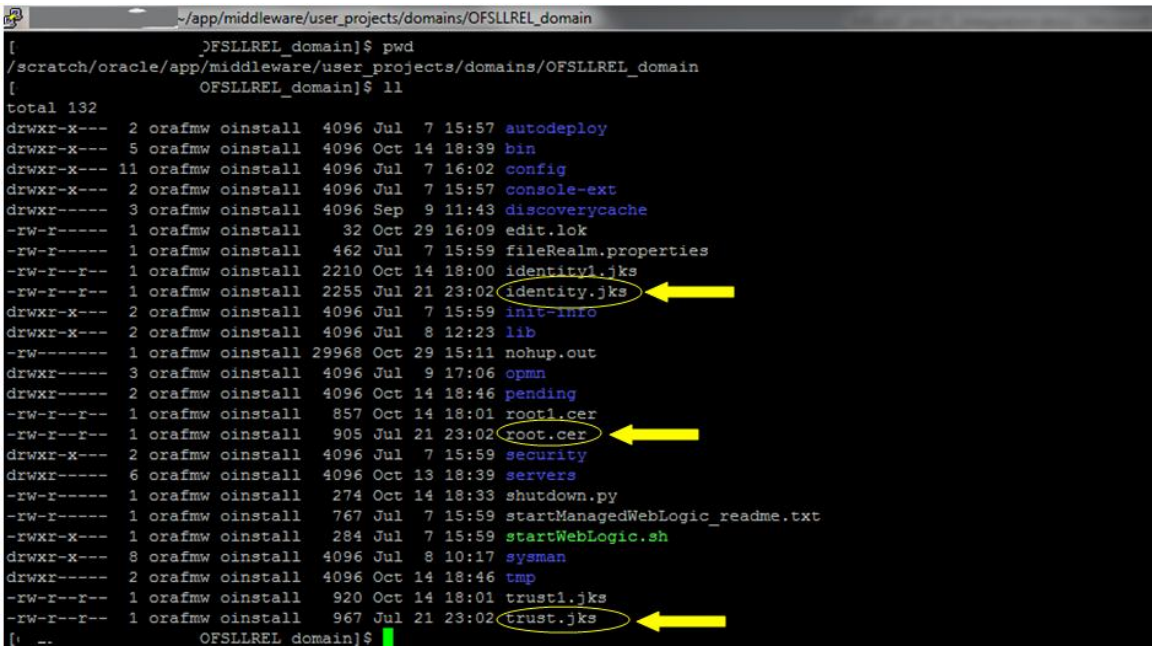

Figure 22. Weblogic Physical Server – Domain Location

Steps to configure Custom Identity and Custom Trust

- Login to Weblogic Admin console --> Environment --> Servers --> ofsll_managedserver2 --> Configuration -> Keystores
- Click on “Change” button next to Keystores

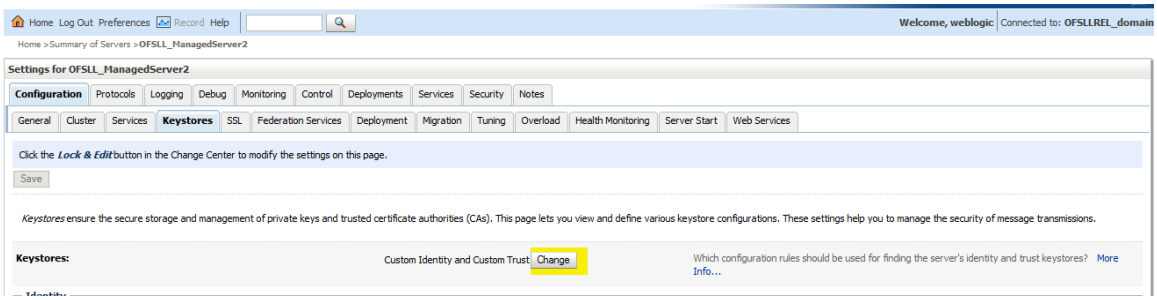

Figure 23. Weblogic Server – Keystore Location

- Click on the drop down menu next to Keystores and select " Custom Identity and Custom Trust "
- Fill in the following information :
  - Custom Identity Keystore → location of the Identity keystore; for example identity.jks

Note: By default Weblogic will look for this keystore file in $DOMAIN_HOME location.

  - Custom Identity Keystore Type → jks
  - Custom Identity Keystore Passphrase → this would be the storepass; for example in our case it is password123
  - Custom Trust Keystore → location of the Trust keystore; for example trust.jks

Note: By default Weblogic will look for this keystore file in $DOMAIN_HOME location.

  - Custom Trust Keystore Type →jks
  - Custom Trust Keystore Passphrase → this would be the storepass; for example in our case it is password123

» Save the changes

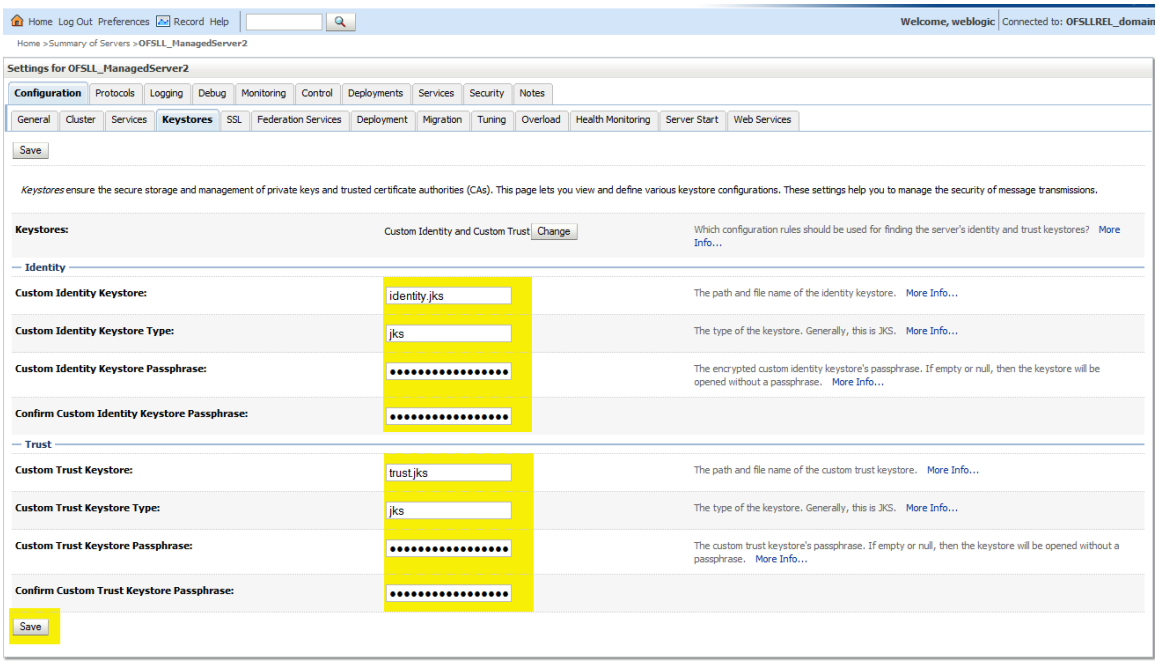

Figure 24. Weblogic Server – Keystore Settings

» Click on SSL tab
  » Private Key Alias → This would be certificate alias; for example in our case it's "myKey"
  » Private Key Passphrase → This would be keypass; for example in our case it's "password1"

» Save the changes

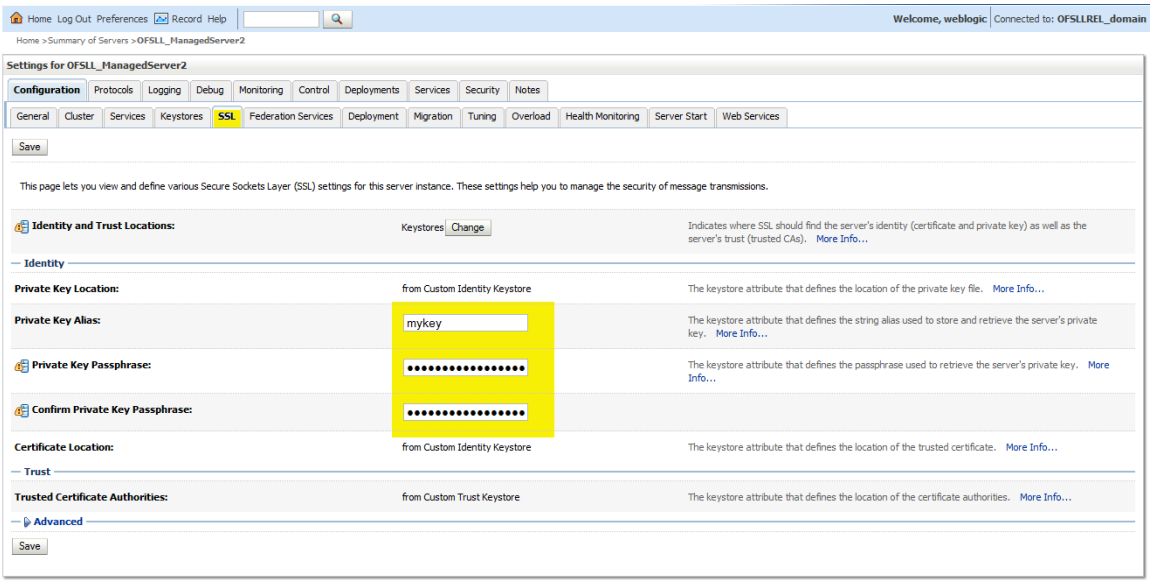

Figure 25. Weblogic Server – SSL Settings

» Click on the "Advanced " field under the SSL tab

  » Set the " Hostname Verification: " to None

Note: We need to select the hostname verification as none if the CN of the certificate is not the same as the hostname of the machine where Weblogic is installed.

  » Use JSSE SSL → Checked

» Save the changes

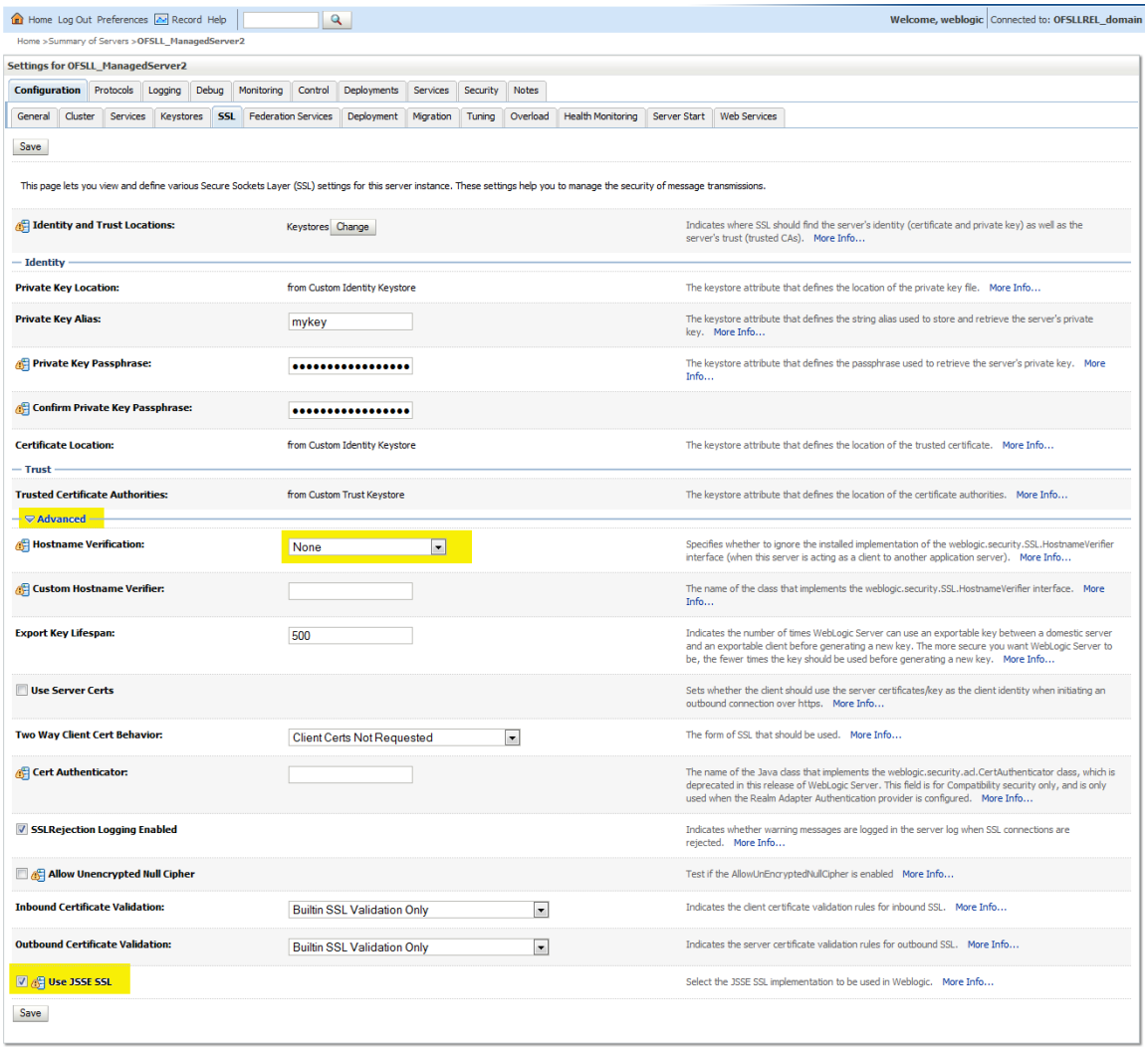

Figure 26. Weblogic Server – SSL Advanced Settings

Configuring the domain as SAML 2.0 Service Provider

OFSLL Server is now pre-configured with required SSL and custom identity/trust settings as required by AD FS. Now let's proceed with SAML 2.0 Identity Settings on the OFSLL Server.

Creating SAML Identity Asserter

- Log into Weblogic Admin console on the OFSLL Domain
- Go to Security Realms -> myrealm -> Providers -> Authentication
- Click the "Lock and Edit" button in the top-left hand corner
- In the Authentication Providers screen, click the "New button" and select SAML2IdentityAsserter.
- Name the new asserter SAMLIdentityAssert (or similar) and click "OK"
- Activate Changes and Restart the server

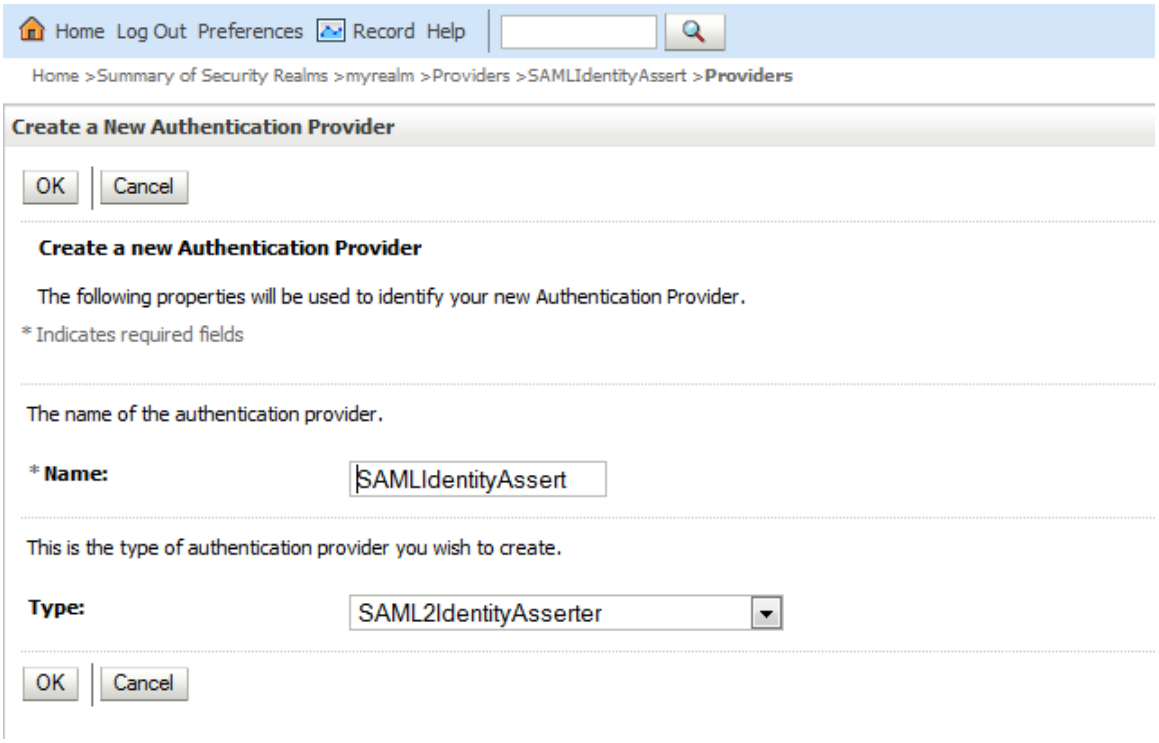

Figure 27. Weblogic Server – SAML2 Identity Asserter Setup

- It has to say exactly SAML 2.0 Identity Assertion Provider "Supports Security Assertion Markup Language v2.0" and not 1.1 and shown below.

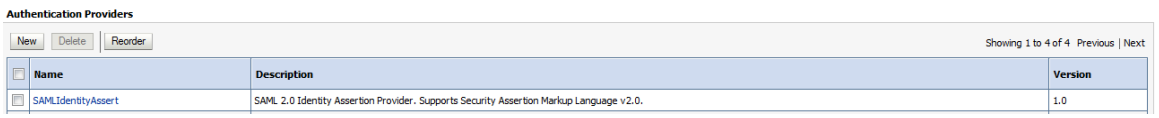

Figure 28. Weblogic Server – SAML 2.0 version

Configuring SAML 2.0 Service Provider (SP)

- Log into Weblogic Admin console on the OFSLL Domain
- Go to Environment →Servers ofsll_managedserver2→ Federation Services→SAML 2.0 Service Provider
- Most fields can be left as default except noted below
  - Enabled → Checked
  - Always Sign Authentication Requests → Checked
  - Force Authentication → Unchecked
  - Preferred Binding → POST
  - Default URL → https://<WeblogicServerName>:<ManagedServerPort>/ofsll142/faces/pages/OfsllHome.jspx ; for example https://ofsll.oracle.com:9704/ofsll142/faces/pages/OfsllHome.jspx
- Save and Activate Changes

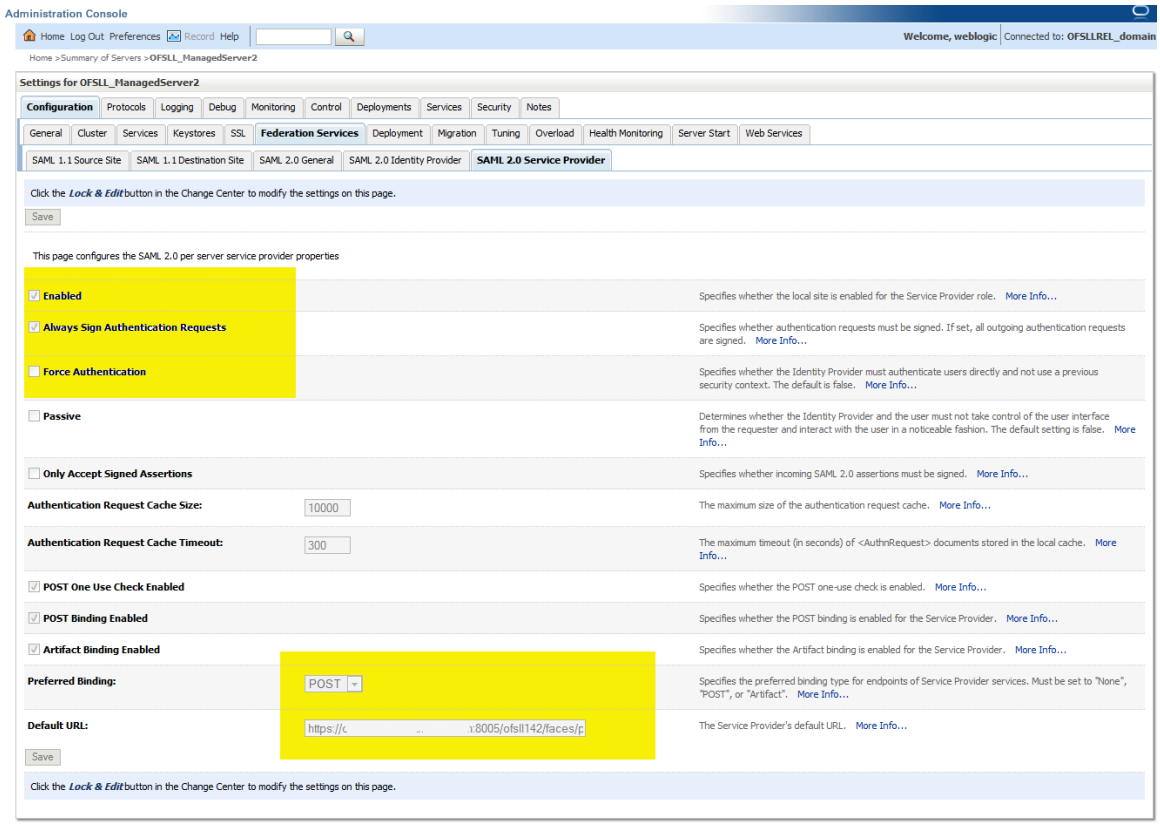

Figure 29. Weblogic Server – SAML2.0 Service Provider

Configuring SAML 2.0 Federation properties for the Domain

- Log into Weblogic Admin console on the OFSLL Domain
- Go to Environment → Servers → ofsll_managedserver2→ Federation Services → SAML 2.0 General
- Lock and Edit

- Most fields can be left as default except noted below
  - Replicated Cache Enabled → Un-checked

Note: this should not be checked for a single node managed server setup; only applicable for cluster setup.

  - Contact Person Given Name → Insert your first name
  - Contact Person Surname → Insert last name
  - Contact Person Type Select from list → pick one – doesn't matter which
  - Contact Person Company → Oracle
  - Contact Person Telephone Number → Insert a phone number
  - Contact Person Email Address → Your email address
  - Organization Name → Oracle
  - Organization URL → http://www.oracle.com/
  - Published Site URL must be in format → https://<WeblogicServerName>:<ManagedServerPort>/saml2; for example https://ofsll.oracle.com:9704/saml2

Note: If you have a cluster of Managed Servers, this should be the externally visible entry point to all Managed Servers in the cluster i.e. the URL exposed via a web server in front of the Managed Servers.

  - Entity ID → Domain name or similar, this must be unique; for example sso_domain
  - Single Sign-on Signing Key Alias → myKey (this is the customer keystore)
  - Single Sign-on Signing Key Pass Phrase → myKey passphrase
  - Confirm Single Sign-on Signing Key Pass Phrase → myKey passphrase
  - Recipient Check Enabled → Un-checked
- Save and Activate Changes

» Restart the server

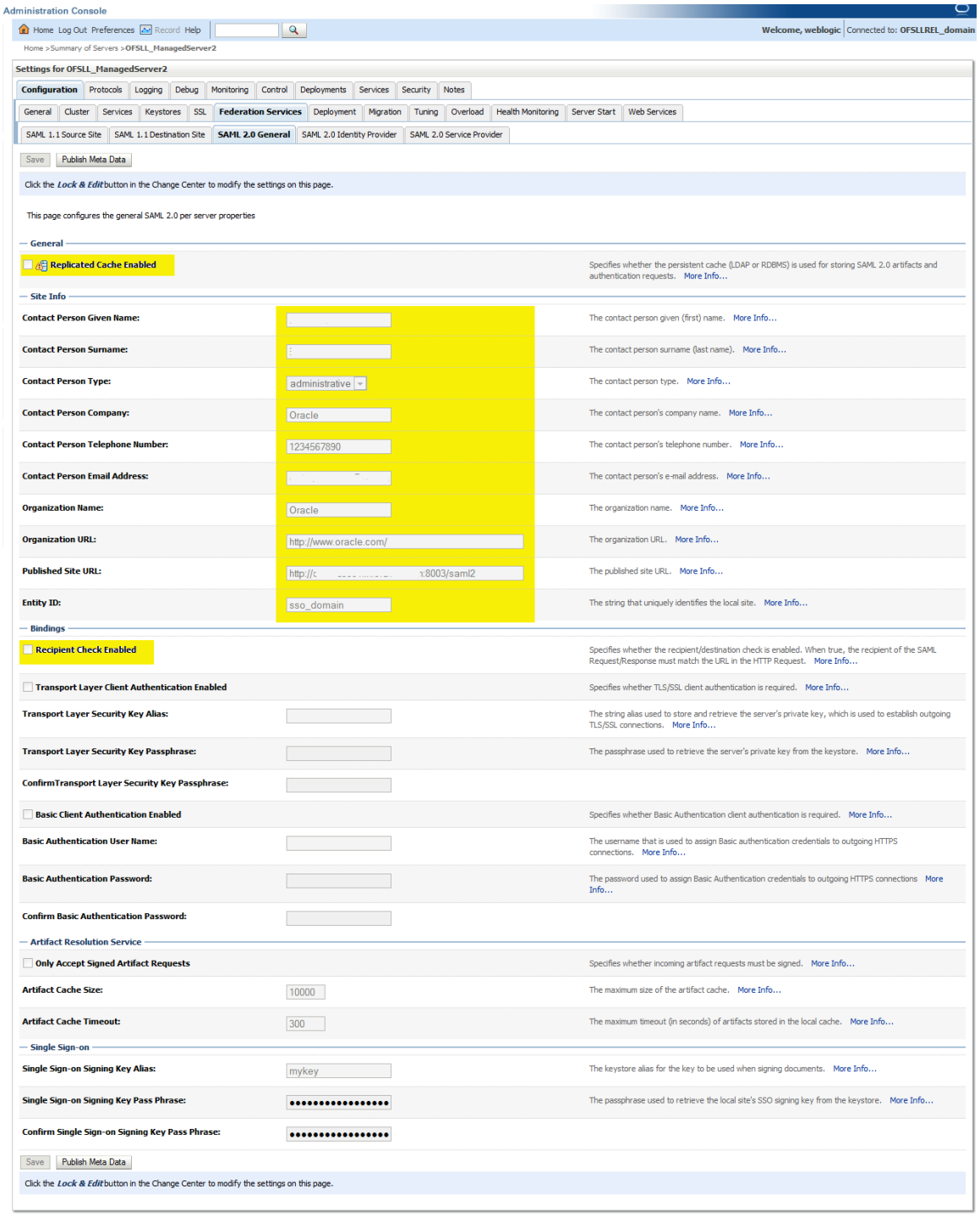

Figure 30. Weblogic Server – SAML2.0 General

» Go to Environment →Servers →ofsll_managedserver2→ Federation Services →SAML 2.0 General

» Publish the Service provider (SP) metadata to an XML file using the “Publish Meta Data” button. Keep the file in a safe place – it will be used by AD Server at later stage. For example ofsll_metadata.xml in this case.

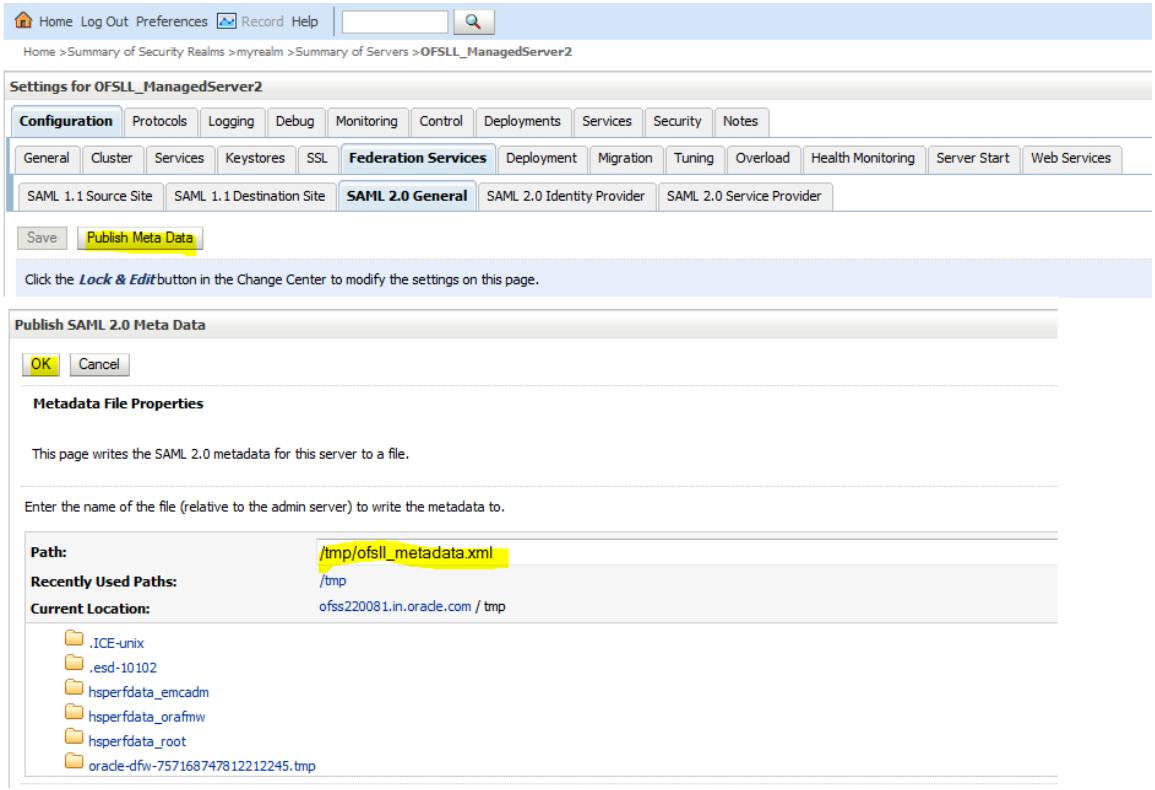

Figure 31. Weblogic Server – Publish Meta Data

» The Published ofsll_metadata.xml file would look as below

Figure 32. Weblogic Service Provider Metadata

Configuring Identity Provider (IdP) as Service Provider on the Domain

» Log into Weblogic Admin console on OFSLL Server

» Go to Security Realms → myrealm → Providers → Authentication

» Select the SAMLIdentityAssert created previously and click on the Management tab

» Create a New Web Single Sign-On Identity Provider Partner, named SAML_SSO_IDP01 (the name is immaterial but it must match when referenced later)

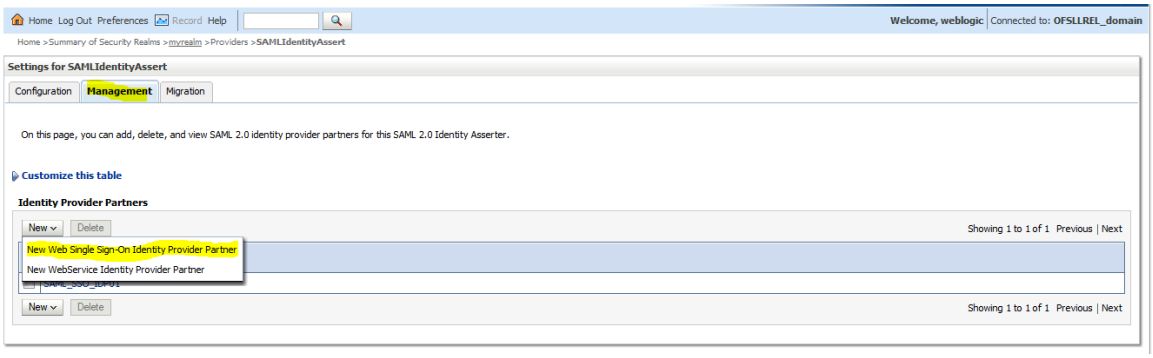

Figure 33. Weblogic Domain – Identity Provider

» In the file browse screen, select the Identity Provider (IdP) metadata file (i.e. federationmetadata.xml)

Note: Federation Metadata Import fails with a java error if imported directly. The xml metadata needs to be changed manually.

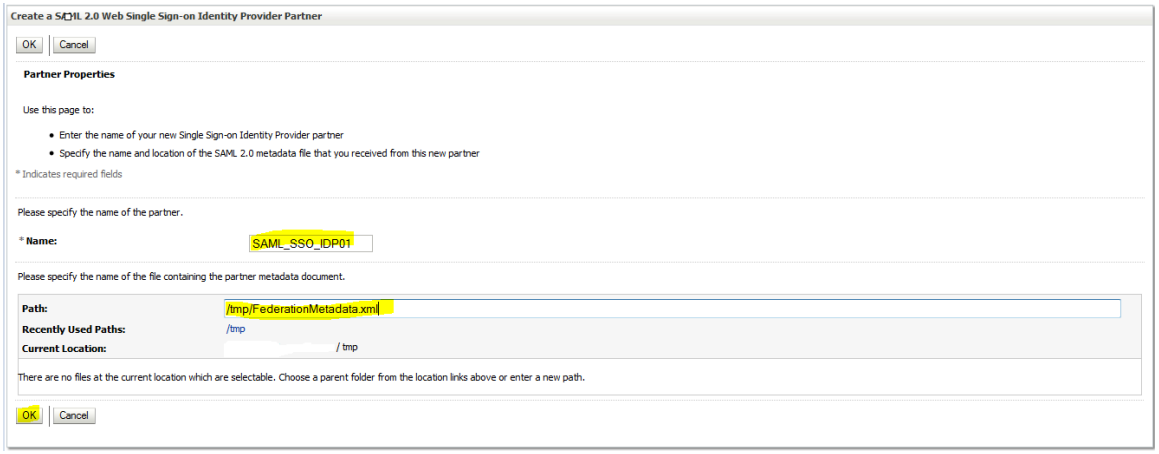

Figure 34. Weblogic Domain – Identity Provider

Modify Federation Metadata

Remove the WS-Trust metadata content and the metadata signature as follows:

» Open FederationMetadata.xml with a XML editor.

» Delete the sections of the file shown below

WS-TRUST METADATA TAGS

Description	Section starts with	Section ends with
Metadata document signature	<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">	</ds:Signature>
WS-Trust & WS-Federation application service metadata	<RoleDescriptor xsi:type="fed:ApplicationServiceType"	</RoleDescriptor>
WS-Trust & WS-Federation security token service metadata	<RoleDescriptor xsi:type="fed:SecurityTokenServiceType"	</RoleDescriptor>

» Save the edited file.

Remove the Service Provider metadata section from already edited Federation Metadata XML.

» Open the previously modified FederationMetadata.xml using a XML editor.

» Delete the following section of the file.

SP METADATA TAGS

Description	Section starts with	Section ends with
SAML 2.0 SP metadata	<SPSSODescriptor WantAssertionsSigned=”true”	</SPSSODescriptor>

» The starting two elements of the resulting modified file should look like:

  » <EntityDescriptor …>

  » <IDPSSODescriptor…>

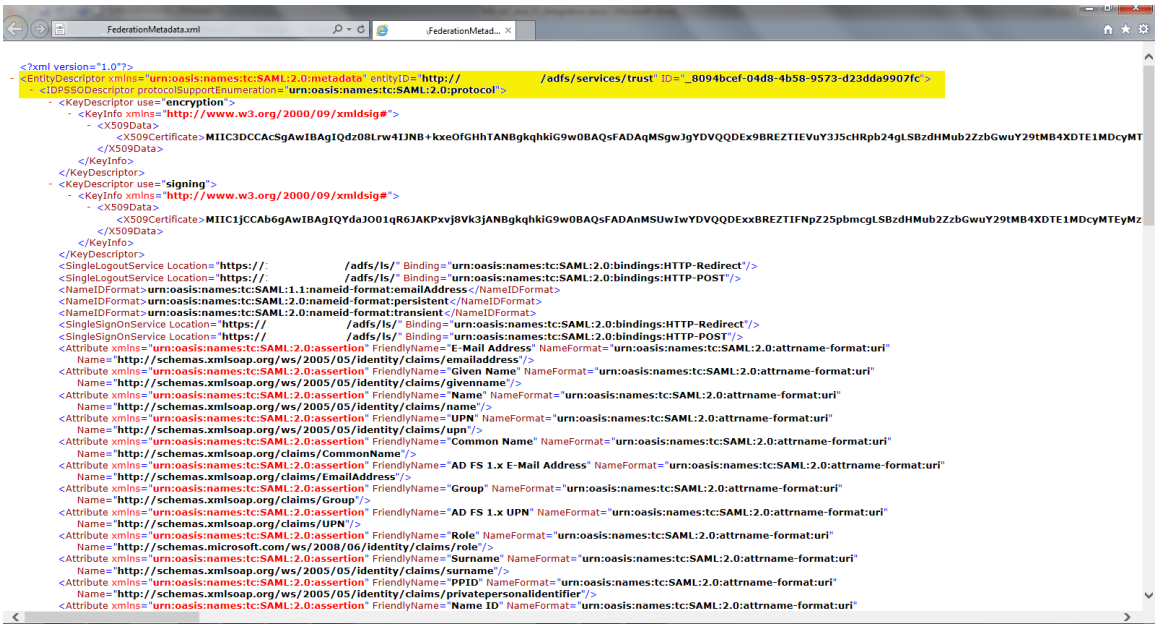

Figure 35. Modified Federation Metadata

» Save the file.

» Import the modified FederationMetadata.xml file on to OFSLL Domain

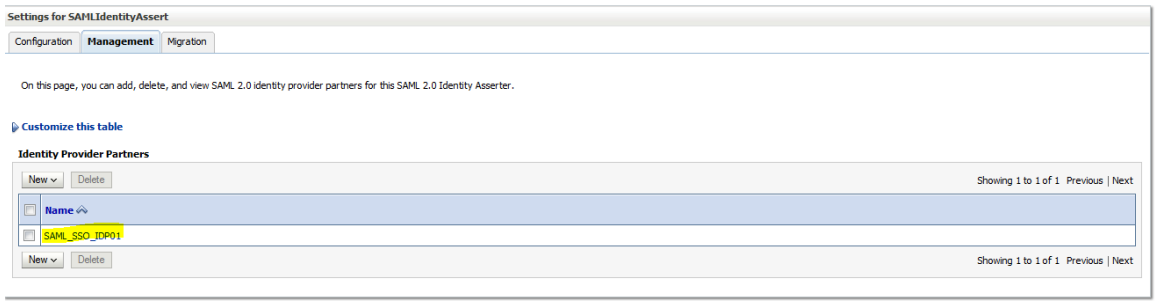

Figure 36. Weblogic Domain – Identity Provider

» Click on the Identity Provider Partner, SAML_SSO_IDP01 that got created in above step, and leave most fields as default except noted below

  » Name → SAML_SSO_IDP01

  » Enabled → Checked

  » Description → SAML_SSO_IDP01

  » Redirect URI → /ofsll42/faces/*

Note: this is the OFSLL application URL context and depends on your application context defined

  » Only Accept Signed Artifact Requests → Checked

» Save

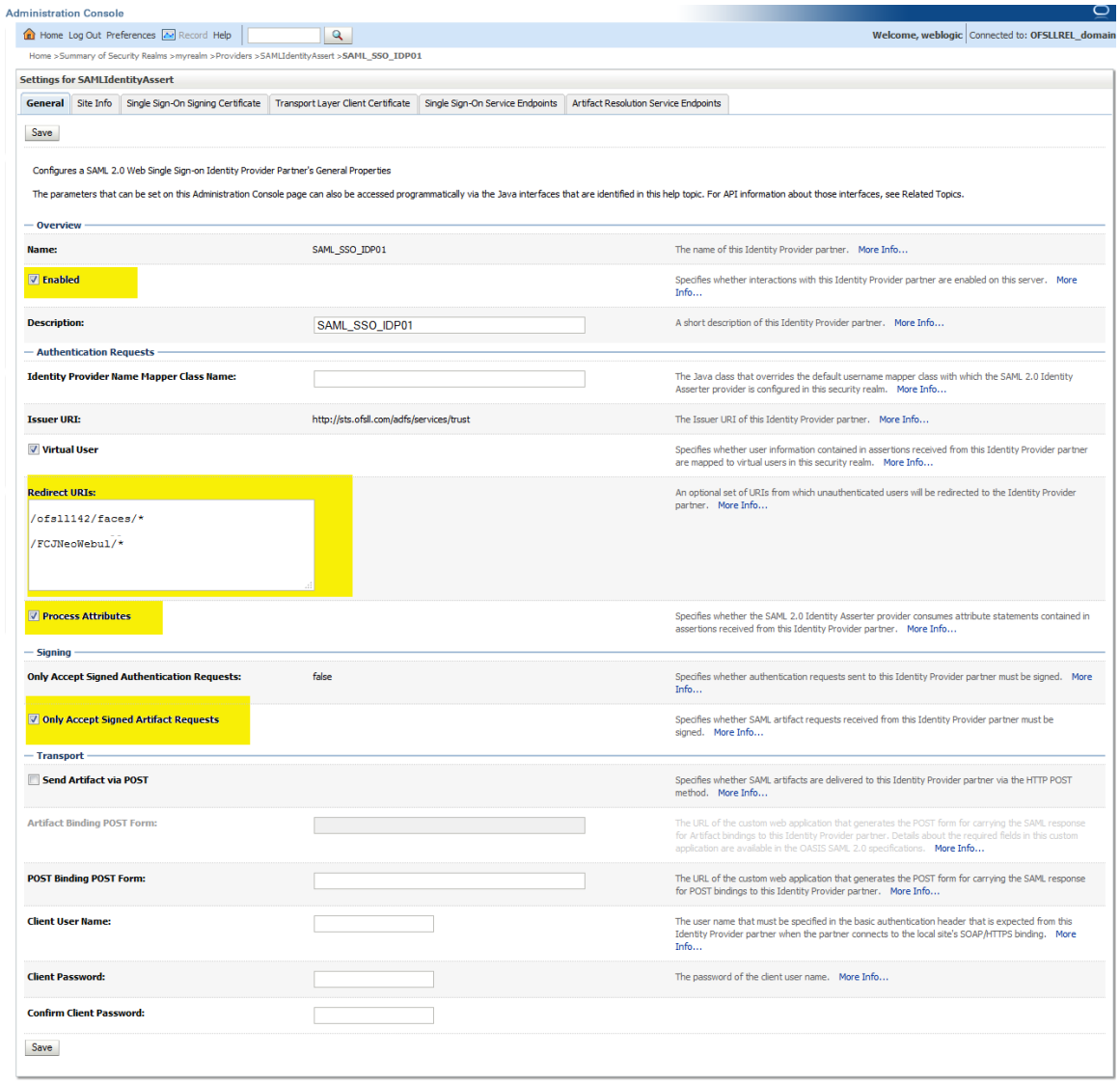

Figure 37. Weblogic Domain – Identity Provider

Configure Domain for SSO

- Add Active Directory as Authentication Provider
  - Log into Weblogic Admin console on OFSLL Domain
  - Go to Security Realms → myrealm → Providers → Authentication
  - Add New Authentication Provider of Type ActiveDirectoryAthentication

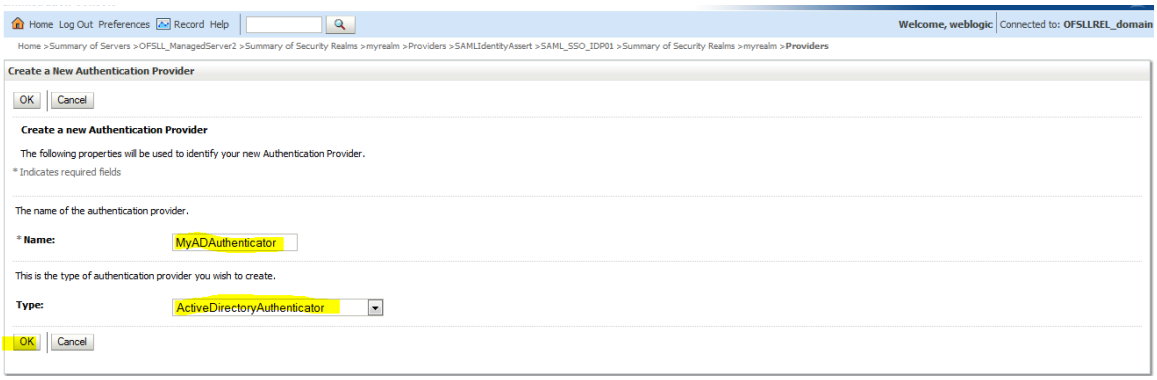

Figure 38. Weblogic Domain – New Authentication Provider

- Go to Provider Specific tab and filling the following details
  - Host → <active directory server name>
  - Port → 389 (default port of AD Server)
  - Principal → CN=administrator, CN=Users, DC=ofsll, DC=com

Note: User Id should be domain administrator of AD Server; DC details are that of Domain Name

  - Credential → password of administrator
  - User Base DN → OU=MyOrg, DC=ofsll, DC=com
  - All Users Filter →(&(sAMAccountName=*)(objectclass=user)) or the value can be (&(cn=*)(objectclass=user))
  - User From Name Filter → (&(sAMAccountName=%u)(objectclass=user)) or the value can be (&(cn=%u)(objectclass=user))
  - User Name Attribute → sAMAccountName or the value can be cn
  - User Object Class → user
  - Group Base DN → OU=MyOrg, DC=ofsll, DC=com
  - All Groups Filter → (&(cn=*)(objectclass=group))
  - Group From Name Filter → (&(cn=%g)(objectclass=group))
  - Static Group DNs from Member DN Filter → (&(member=%M)(objectclass=group))
  - GUID Attribute → objectguid

» Restart servers, first admin server, then Managed Server

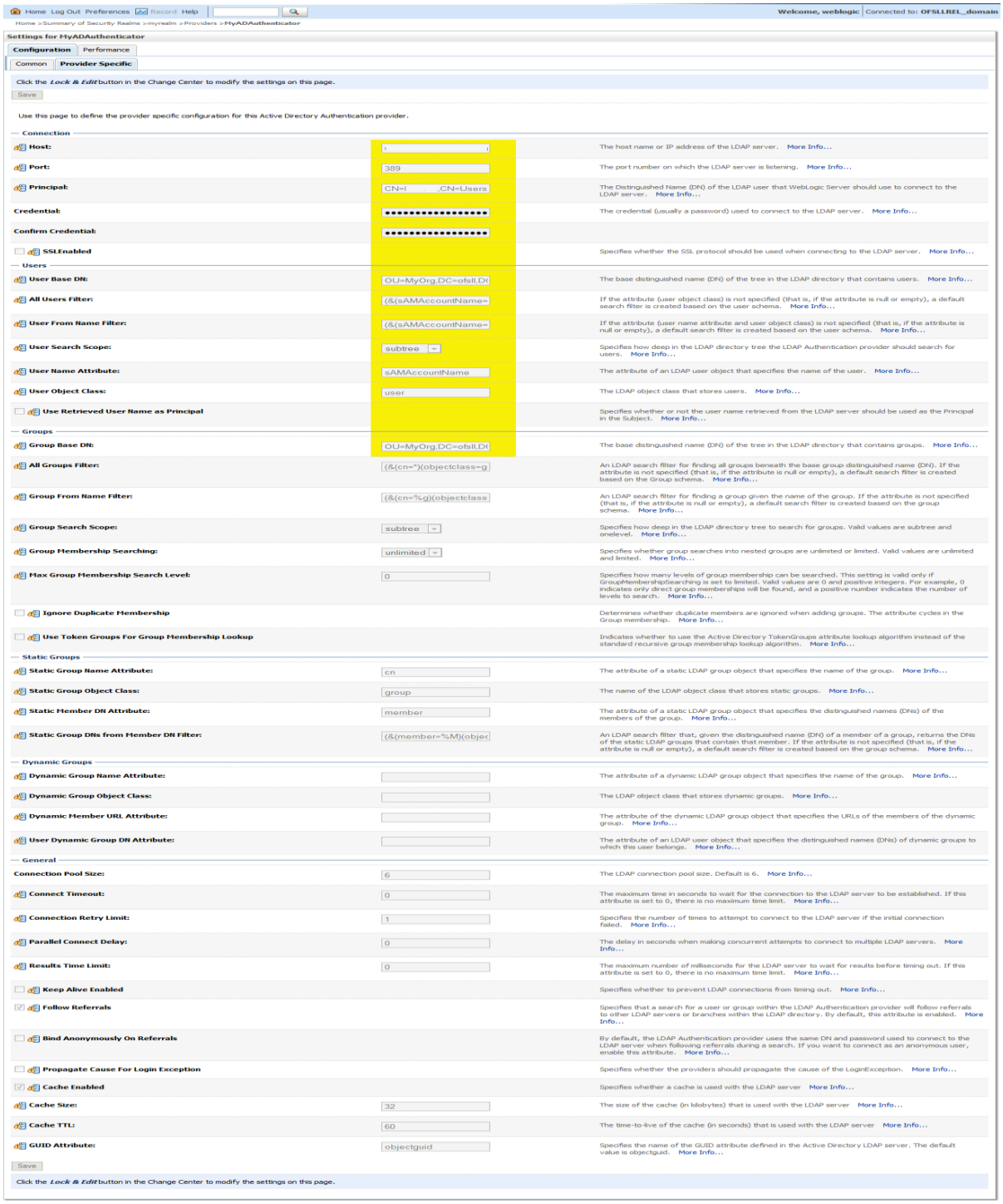

Figure 39. Weblogic Domain –Provider Specific Details

» Ensure the AD Provider Control Flag is set as either Optional or Sufficient

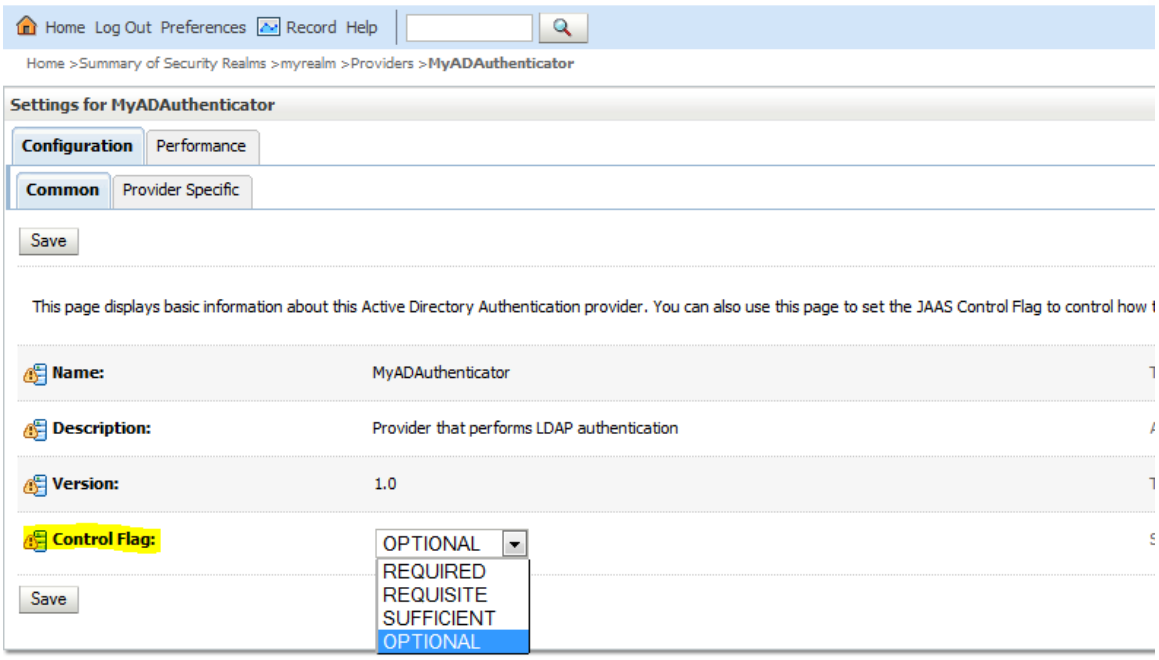

Figure 40. Weblogic Domain –Provider Specific Details

» Ensure the order of the Authentication providers are such that SAML Assert is first followed by AD Authenticator as show below

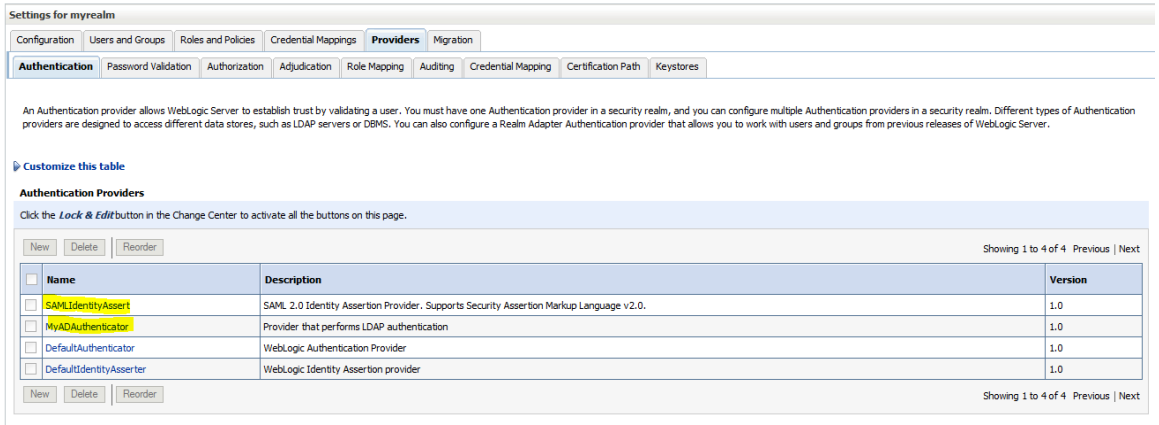

Figure 41. Weblogic Domain –Authentication Provider Order

Configuring Domain as a partner with the Identity Provider (IdP)

FTP the ofsll_metadata.xml file that was published by the OFSLL Domain server in the previous step on to AD Server. Next the OFSLL domain configured in previous section is going to be registered and configured as part of Relying Party on AD FS.

Configure Relying Party

» On AD Server, open AD FS Management Console from Server Management Console → Tools → ADFS Management

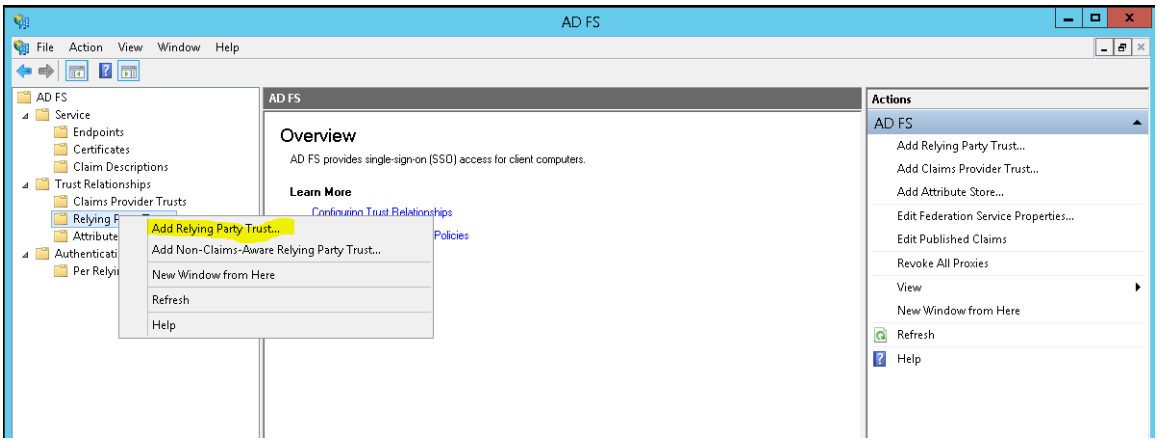

Figure 42. AD FS Server – Relying Party Trust

» Click start on the Welcome Page

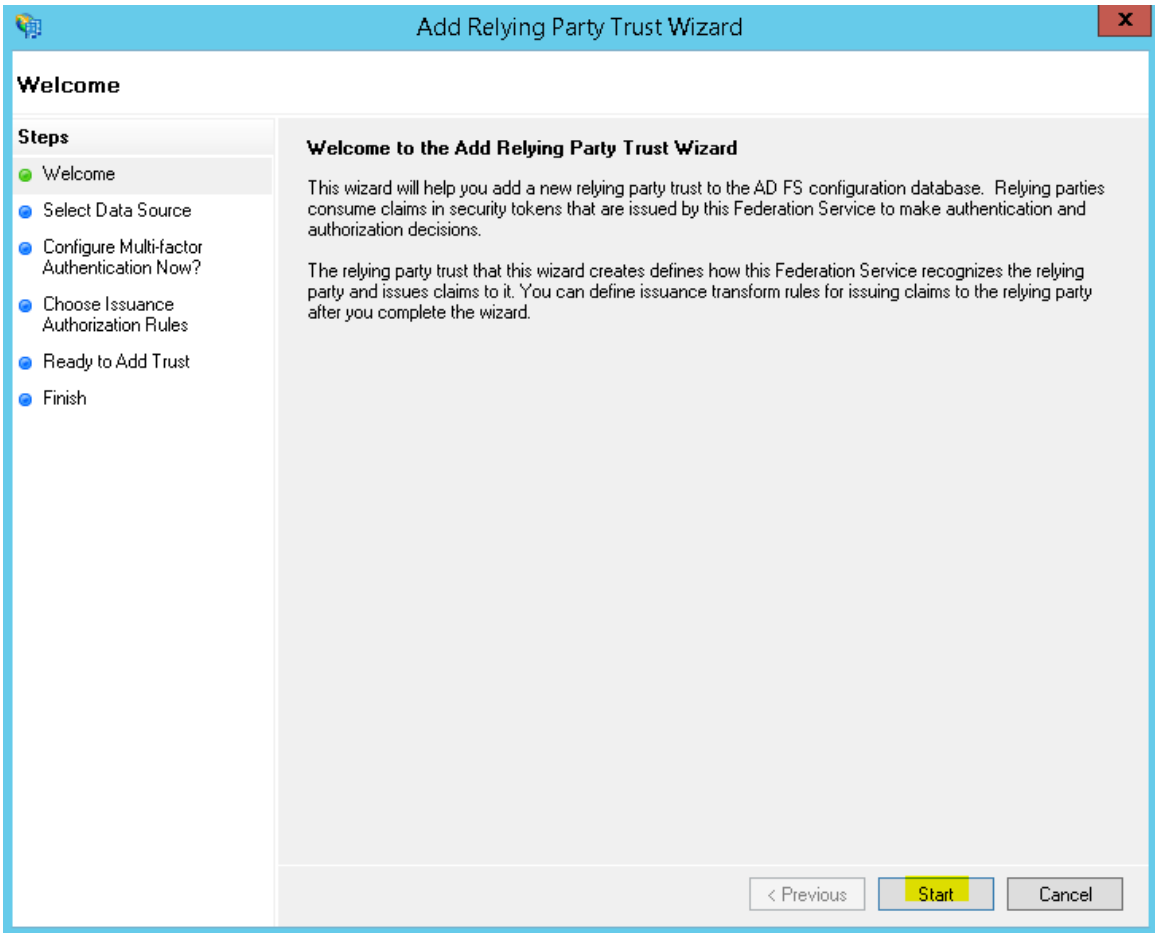

Figure 43. AD FS Server – Welcome Page

» Select “Import data about the relying party from a file option and provide the path where the OFSLL Domain metadata file is copied; for example, ofsll_medata.xml

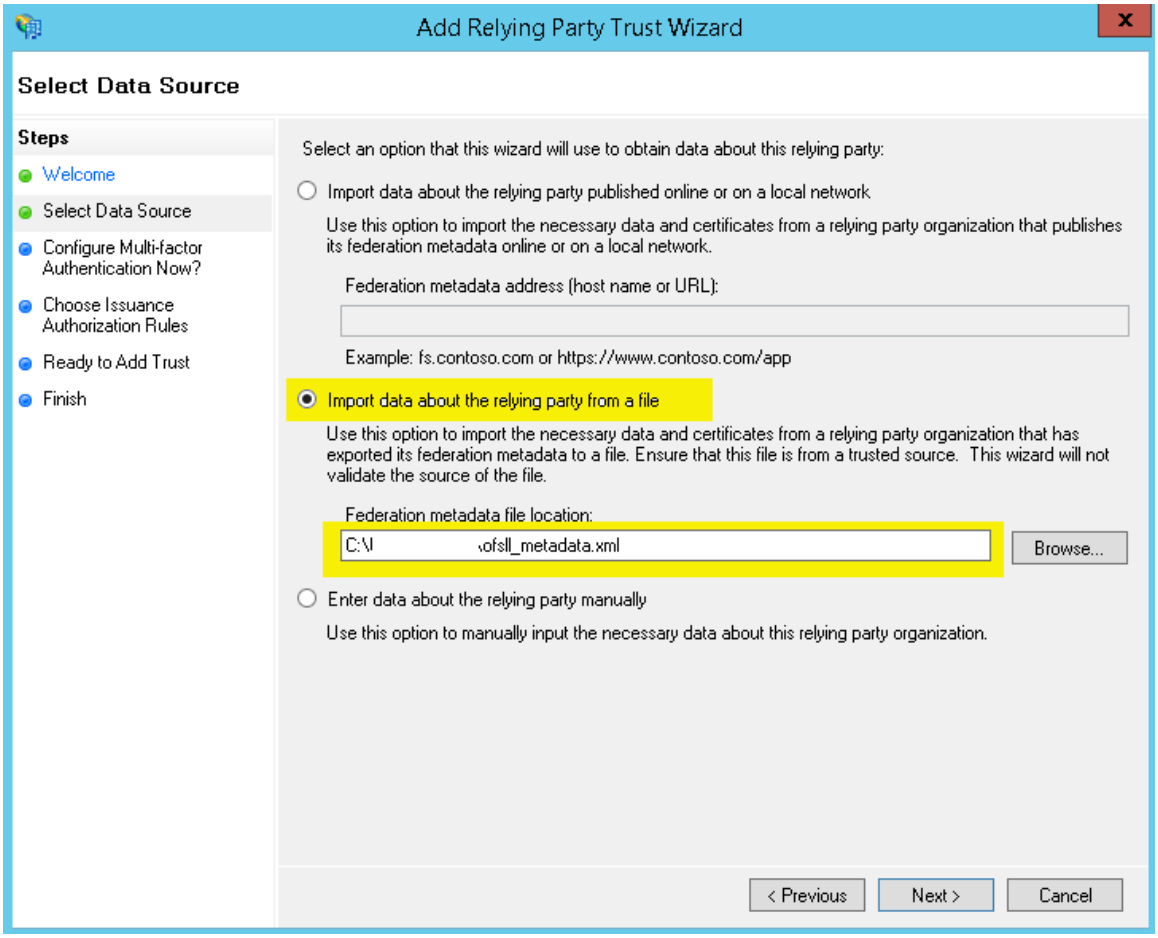

Figure 44. AD FS Server – Define the metadata source

» Click “Ok” on below message

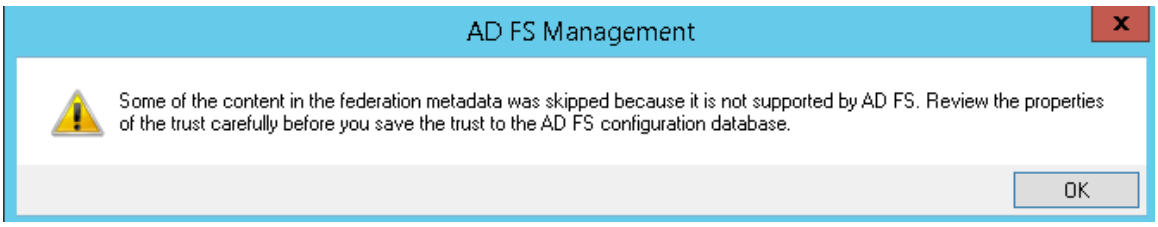

Figure 45. AD FS Server – Warning Message

» Provide an unique Display Name and click Next

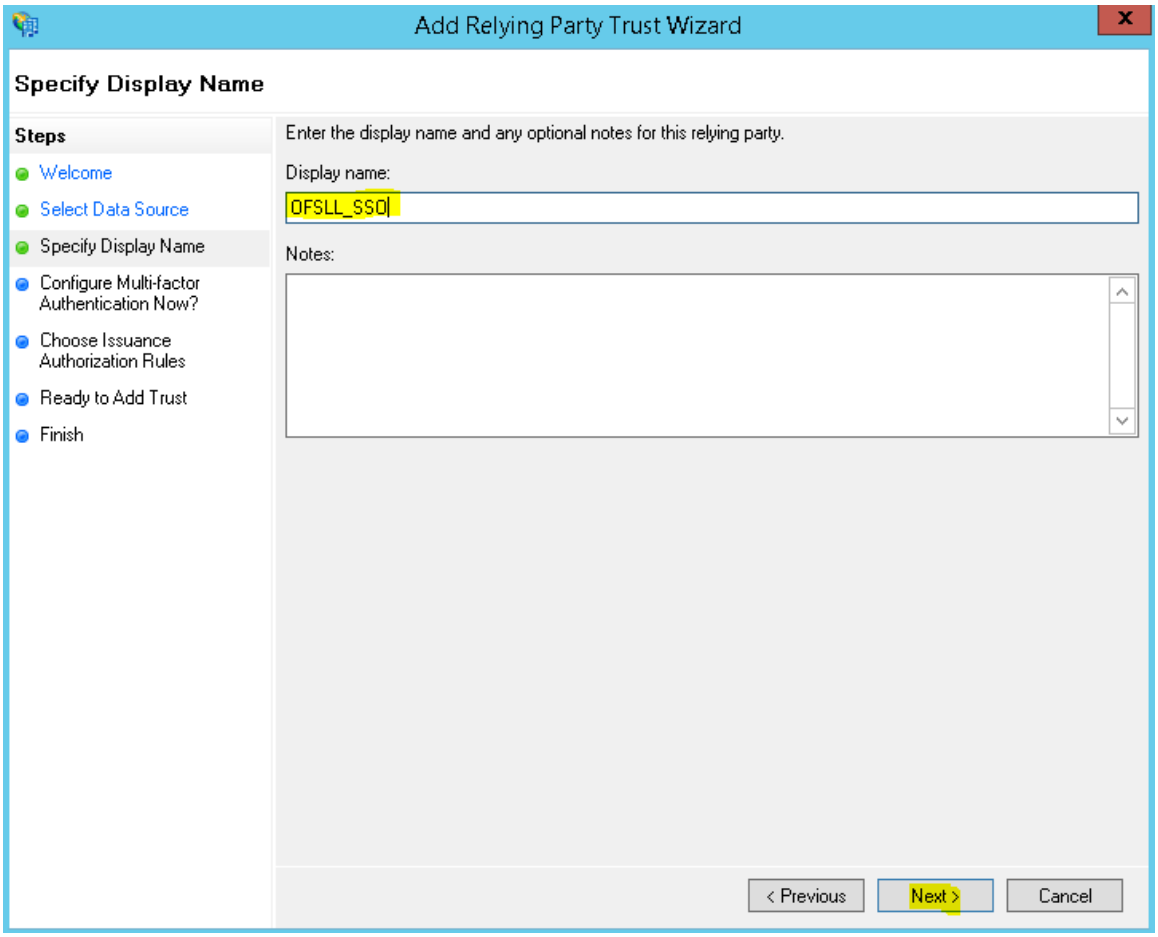

Figure 46. AD FS Server – Relying Party Display Name

» Retain the default as shown below and continue Next

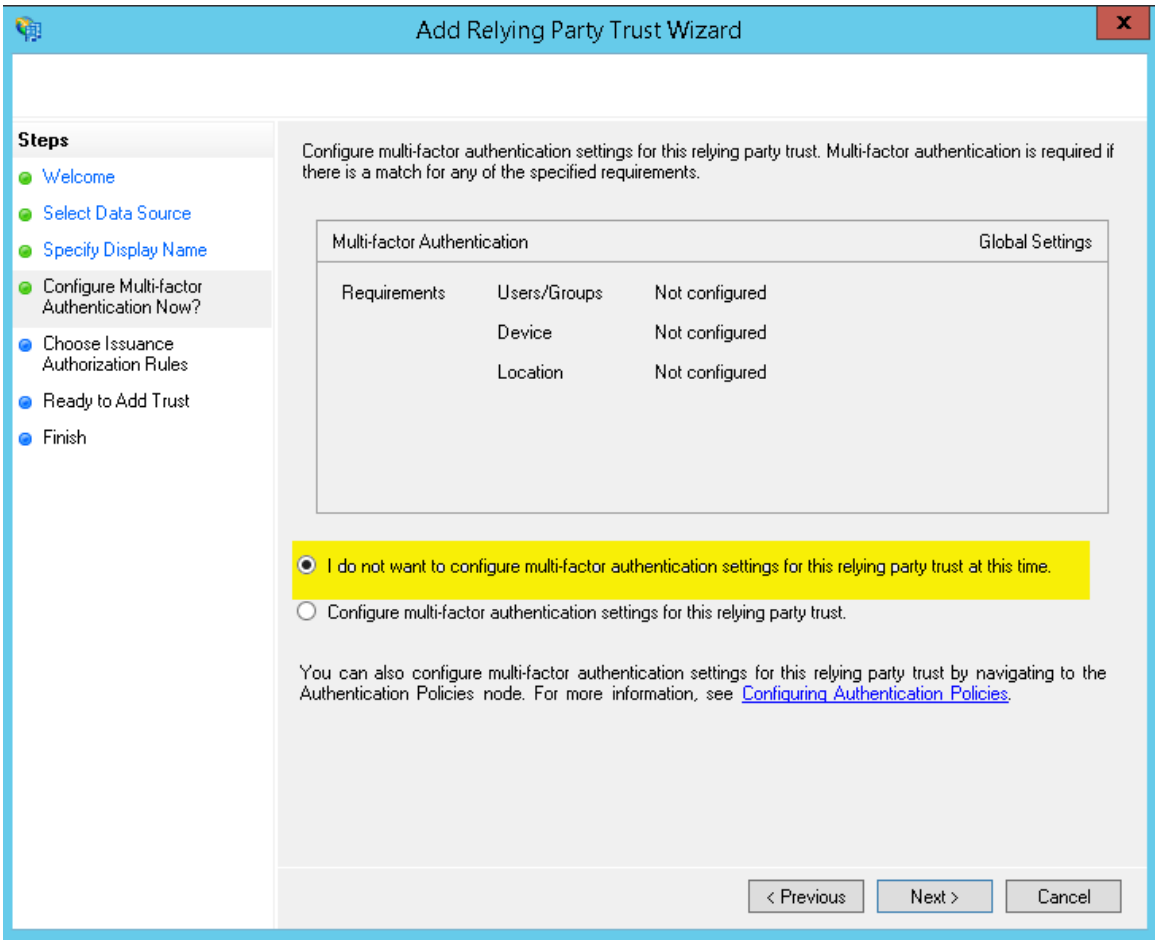

Figure 47. AD FS Server – Multi-factor Authentication

» Retain the default as shown below and continue Next

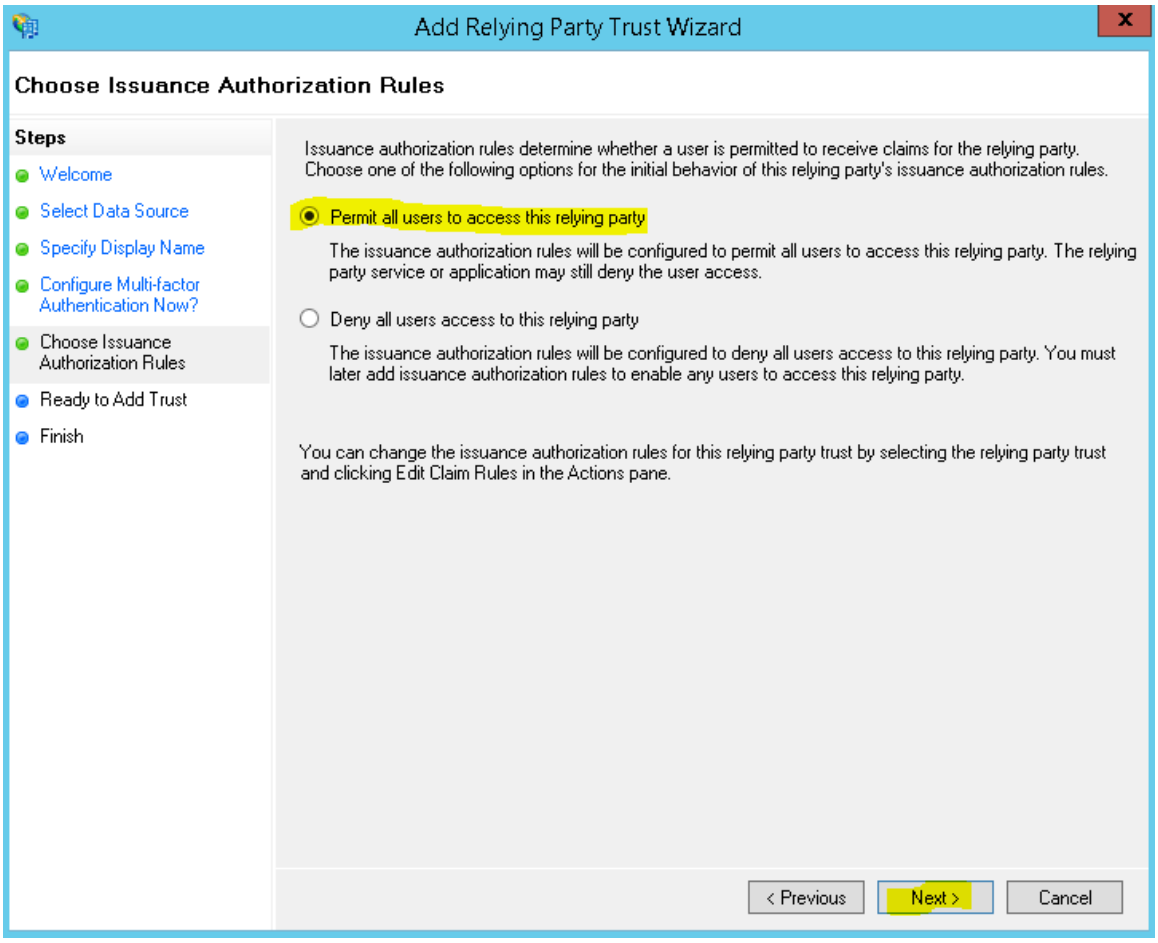

Figure 48. AD FS Server – Authorization Rules

» Next screen verify the following Tabs

  » Identifiers Tab – ensure the “relying party identifiers” are showing the values correctly

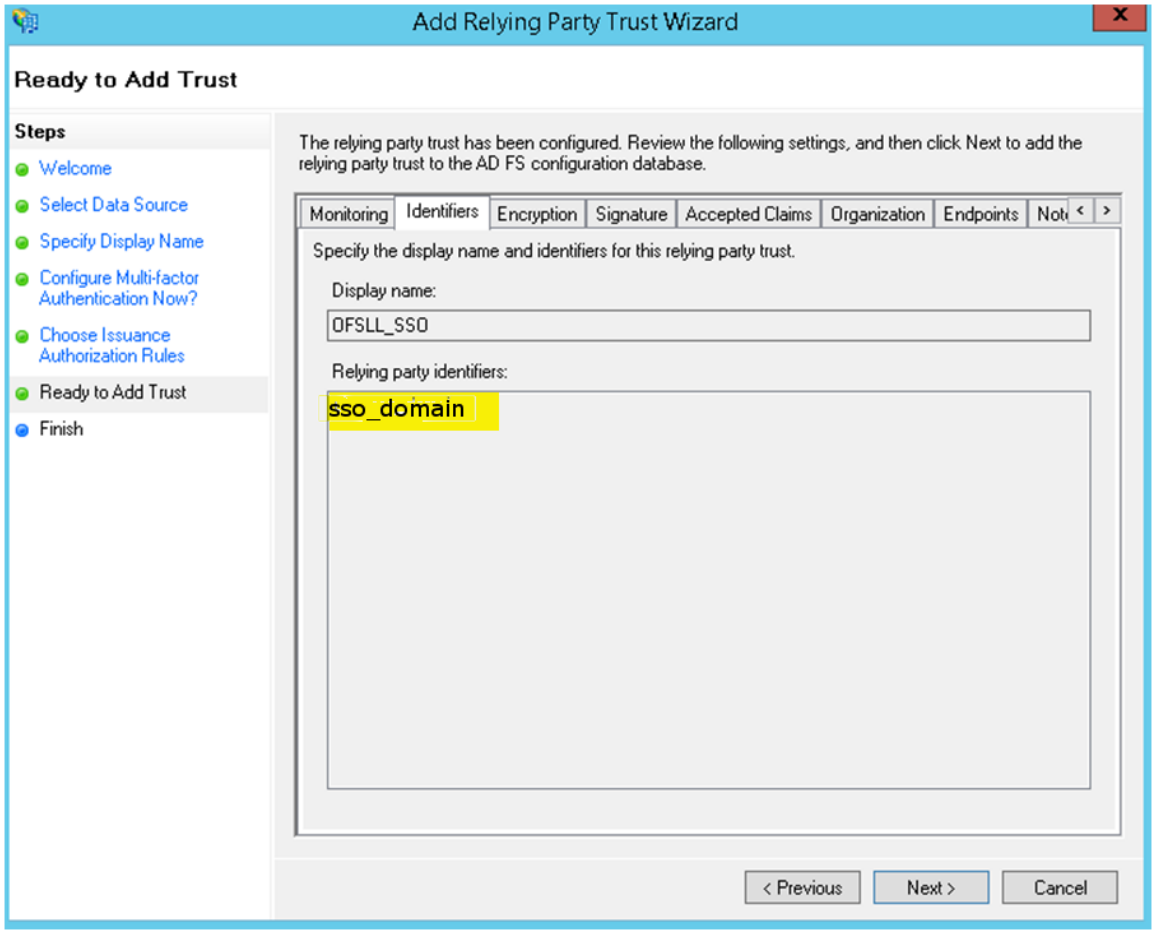

Figure 49. AD FS Server – Identifiers Tab

» Signature Tab – ensure the certificates are valid by selecting the certificate and click “View”

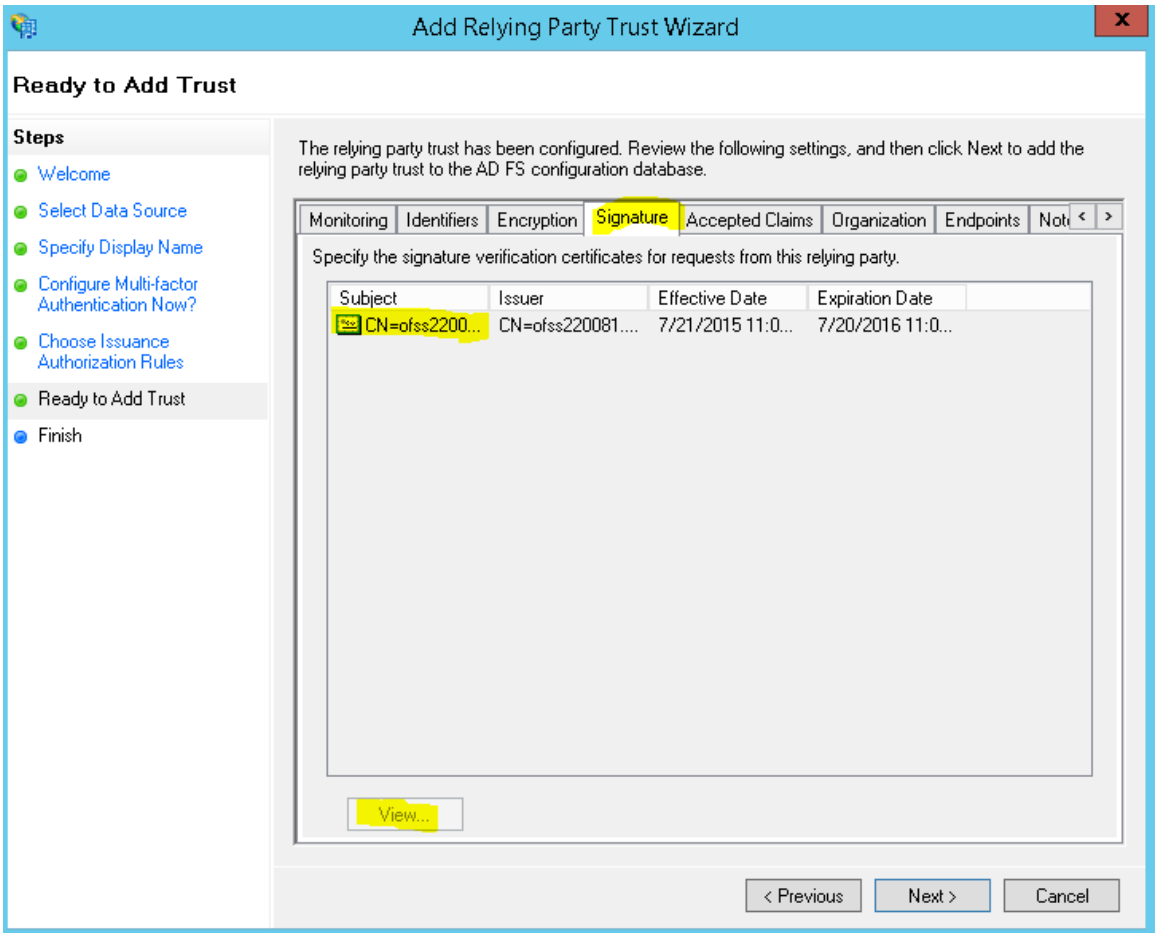

Figure 50. AD FS Server – Signature Tab

» Certificate details can be reviewed

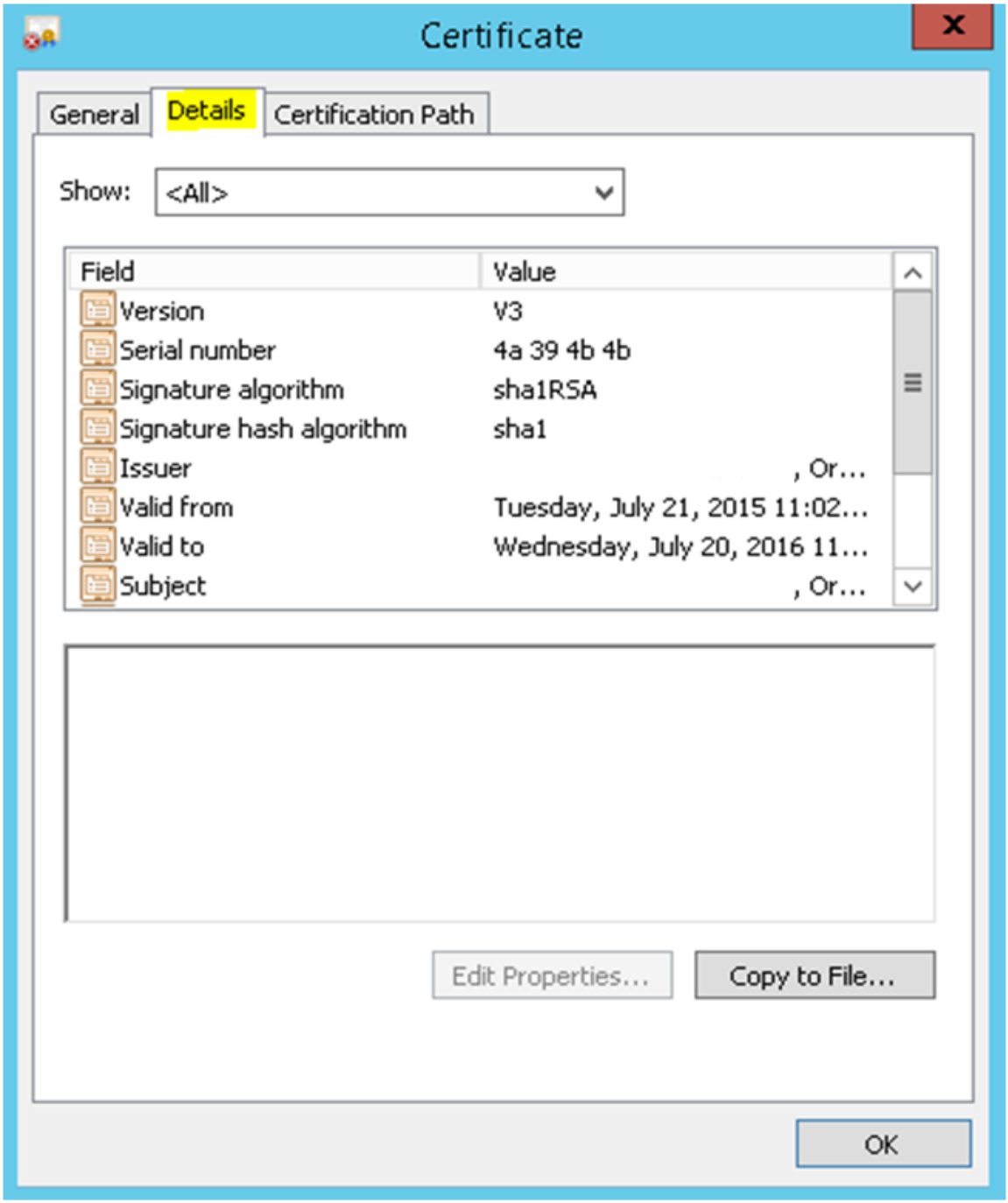

Figure 51. AD FS Server – Certificate Details

» Click Ok and then Next to compete the metadata load and creation of Relying Party Trust.

Editing the Relying Party Trusts

» Select the newly created Relying Party Trust and click “Properties”

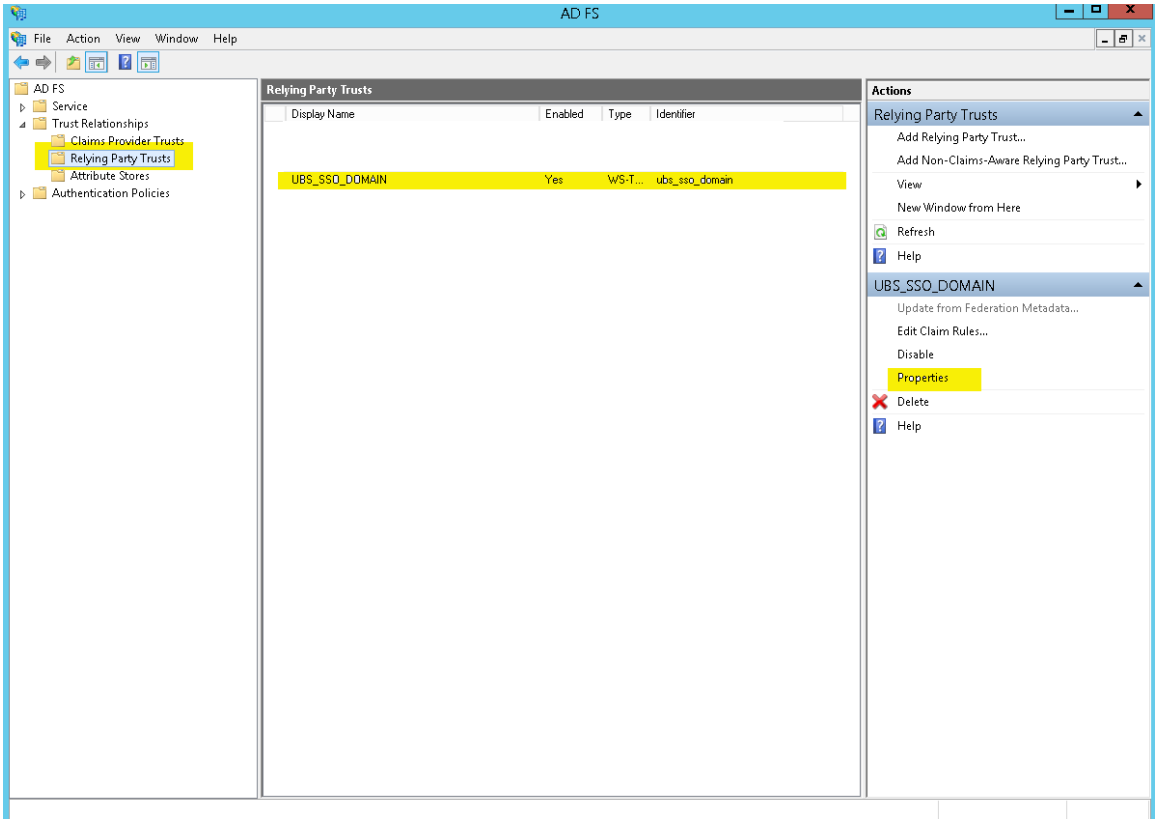

Figure 52. AD FS Server – Edit Relying Party Trust

» Change algorithm from SHA-256 to SHA-1 Since SHA-1 is the encryption algorithm used while creating SSL Certificate

Note: This step is optional and only required if the encryption key used is SHA-1 else ignore this step

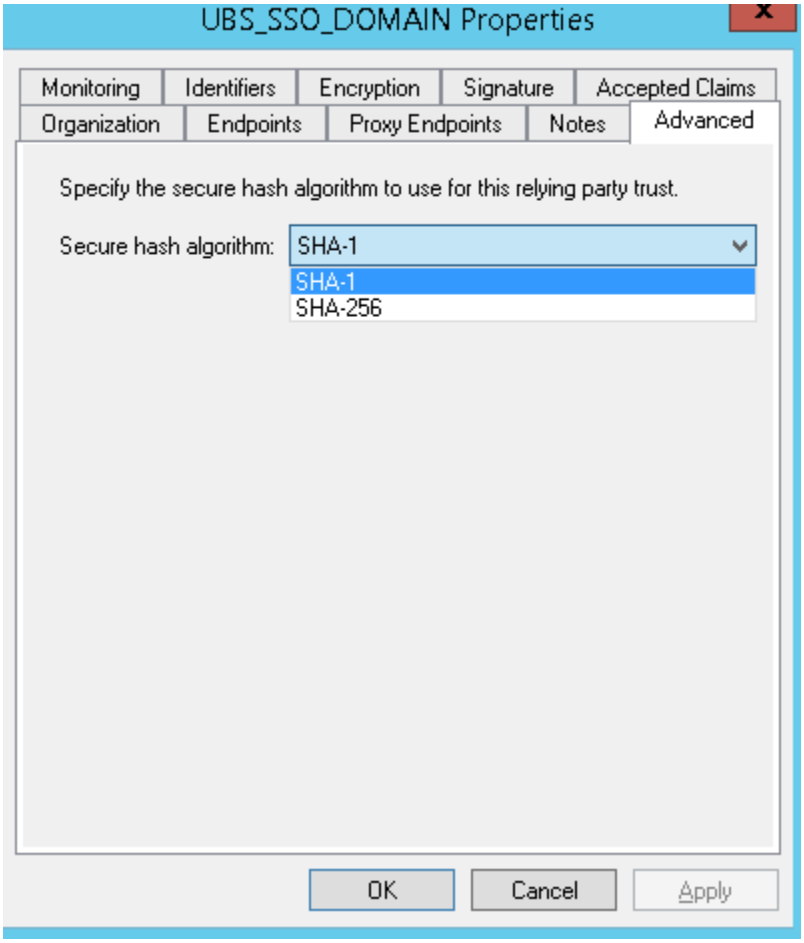

Figure 53. AD FS Relying Party – Advanced Tab

» Click on “Endpoints” and “Add SAML” to add end points.

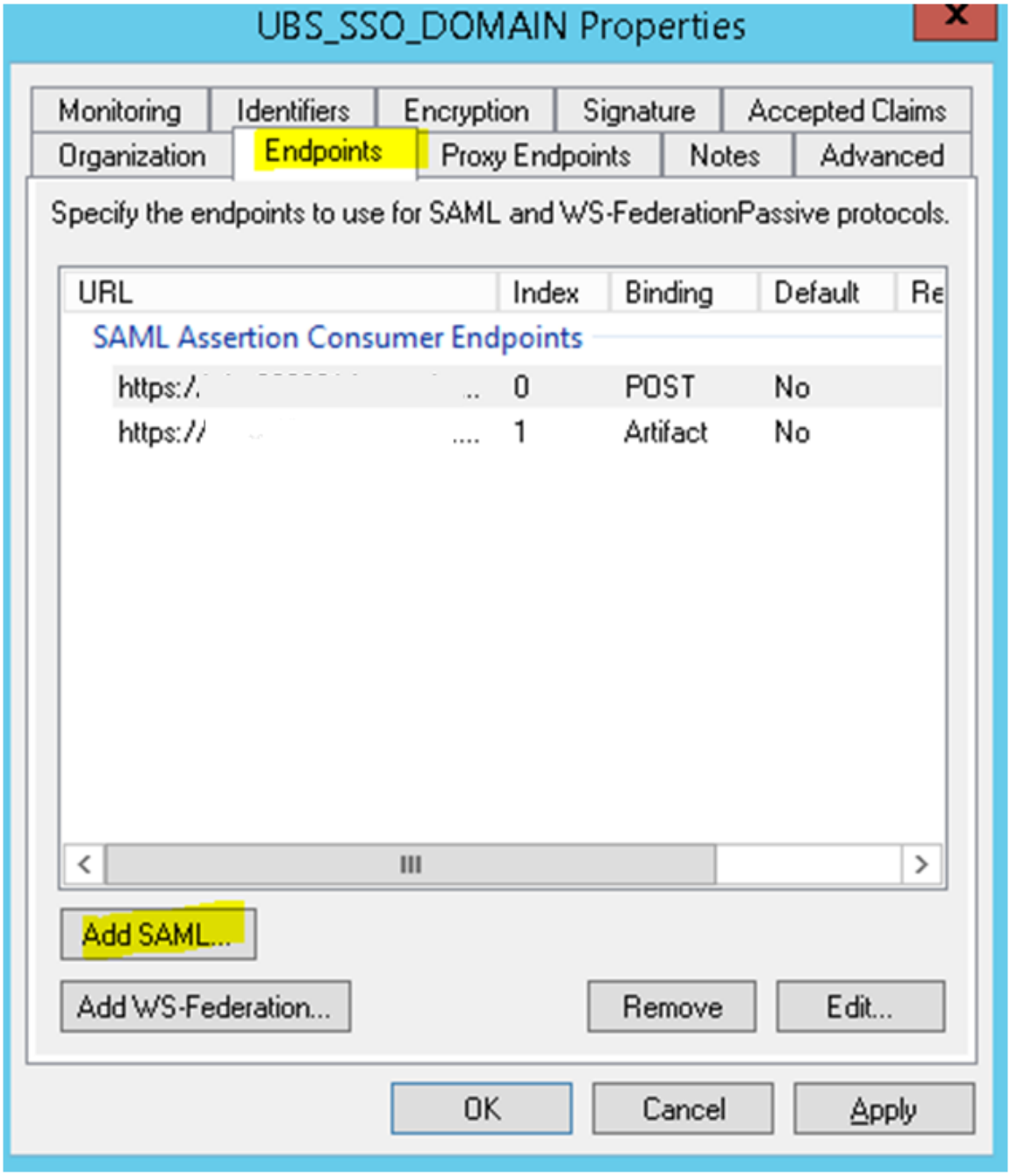

Figure 54. AD FS Relying Party – Endpoints Tab

- Enter following values
  - Binding → POST
  - Index → 0
  - Trusted URL → https://<WeblogicServerNamer>:<ManagedServerPort>/saml2/sp/acs/post ; for example https://ofsll.oracle.com:9704/saml2/sp/acs/post
- Click Ok

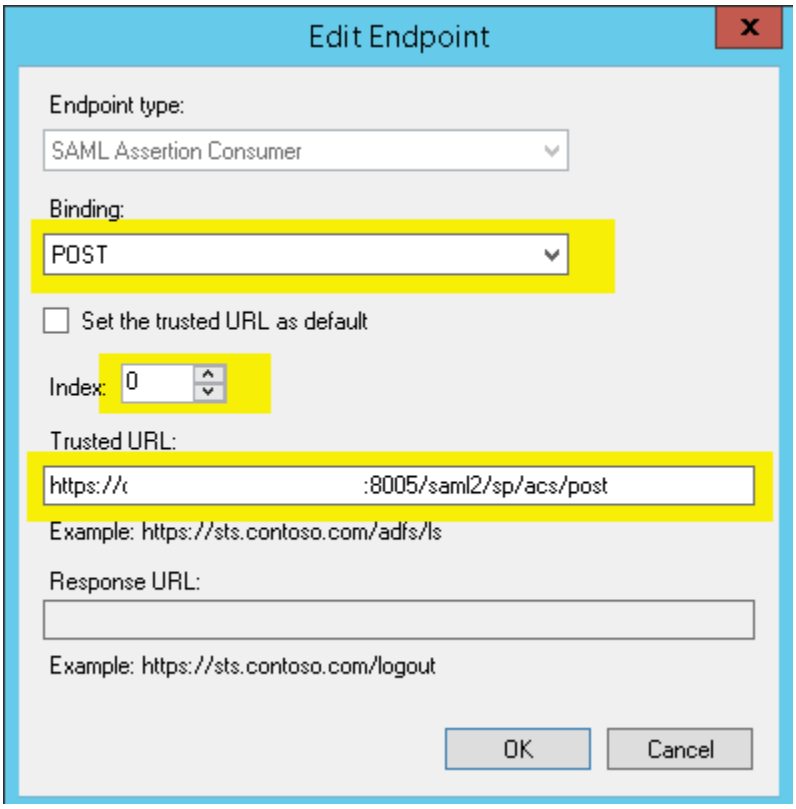

Figure 55. AD FS Relying Party – Add Endpoint

- Add another SAML end point details with following values
  - Binding → Artifact
  - Index → 1
  - Trusted URL → https://<WeblogicServerName>:<ManagedServerPort>/saml2/sp/acs/artifacts; for example https://ofsll.oracle.com:9704/saml2/sp/acs/artifacts
- Click Ok

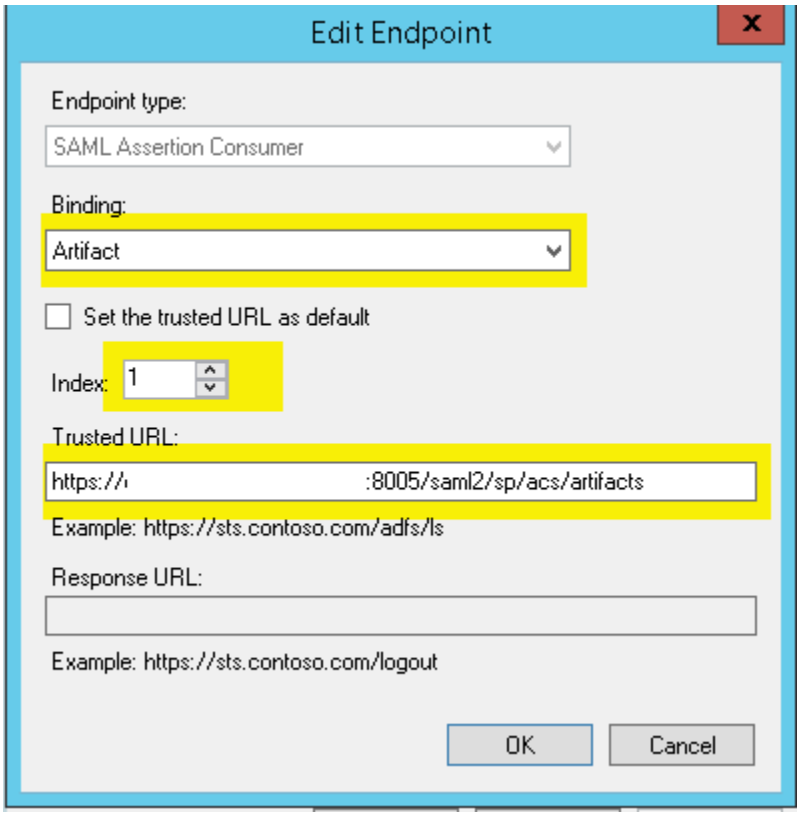

Figure 56. AD FS Relying Party – Add Endpoint

Adding Rules

» Select the newly created Relying Party Trust and click “Edit Claim Rules”

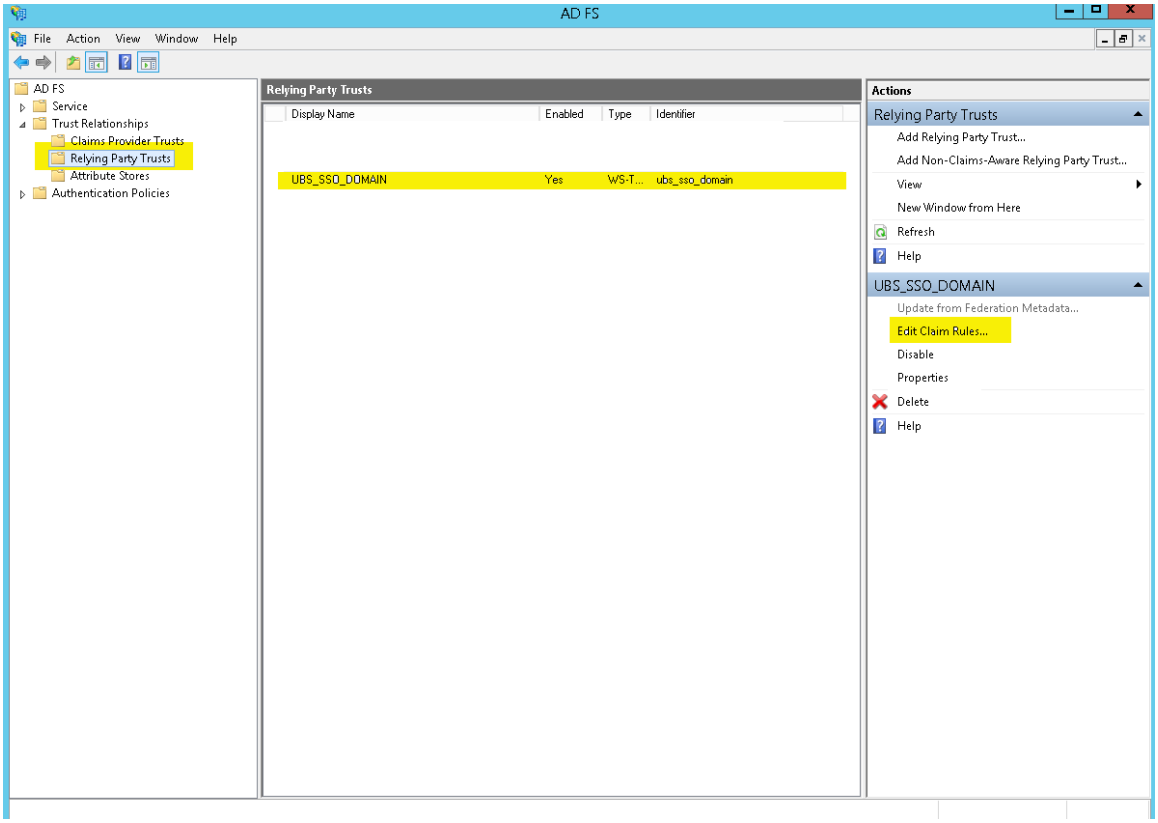

Figure 57. AD FS Relying Party – Edit Claims

» On “Issuance Transform Rules” tab, click on “Add Rule”

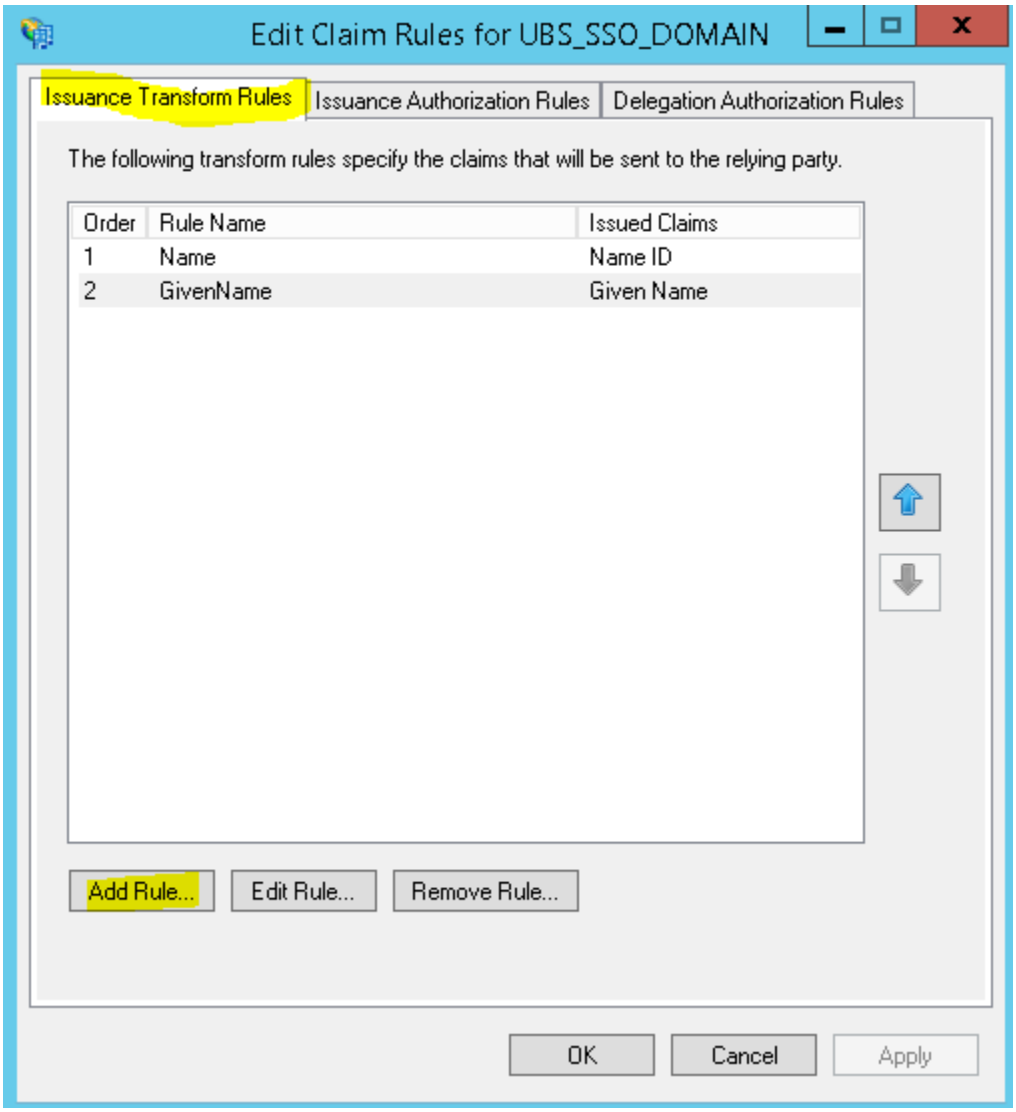

Figure 58. AD FS Relying Party – Add Rules

» Click on Next

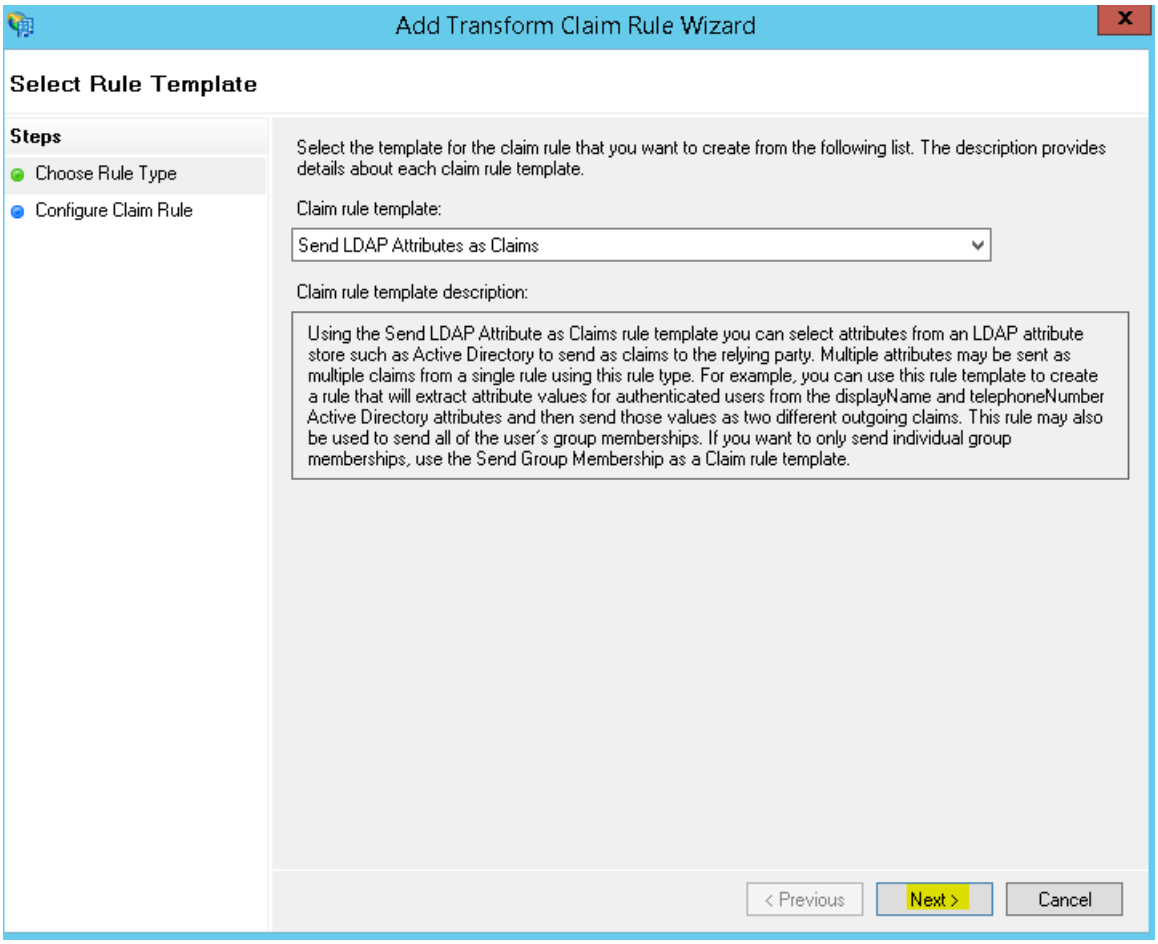

Figure 59. AD FS Relying Party – Rule Template

- Enter the following details
  - Claim rule name → Name
  - Attribute Store → Active Directory
  - LDAP Attribute → SAM-Account-Name
  - Outgoing Claim Type → Name ID
- Click OK

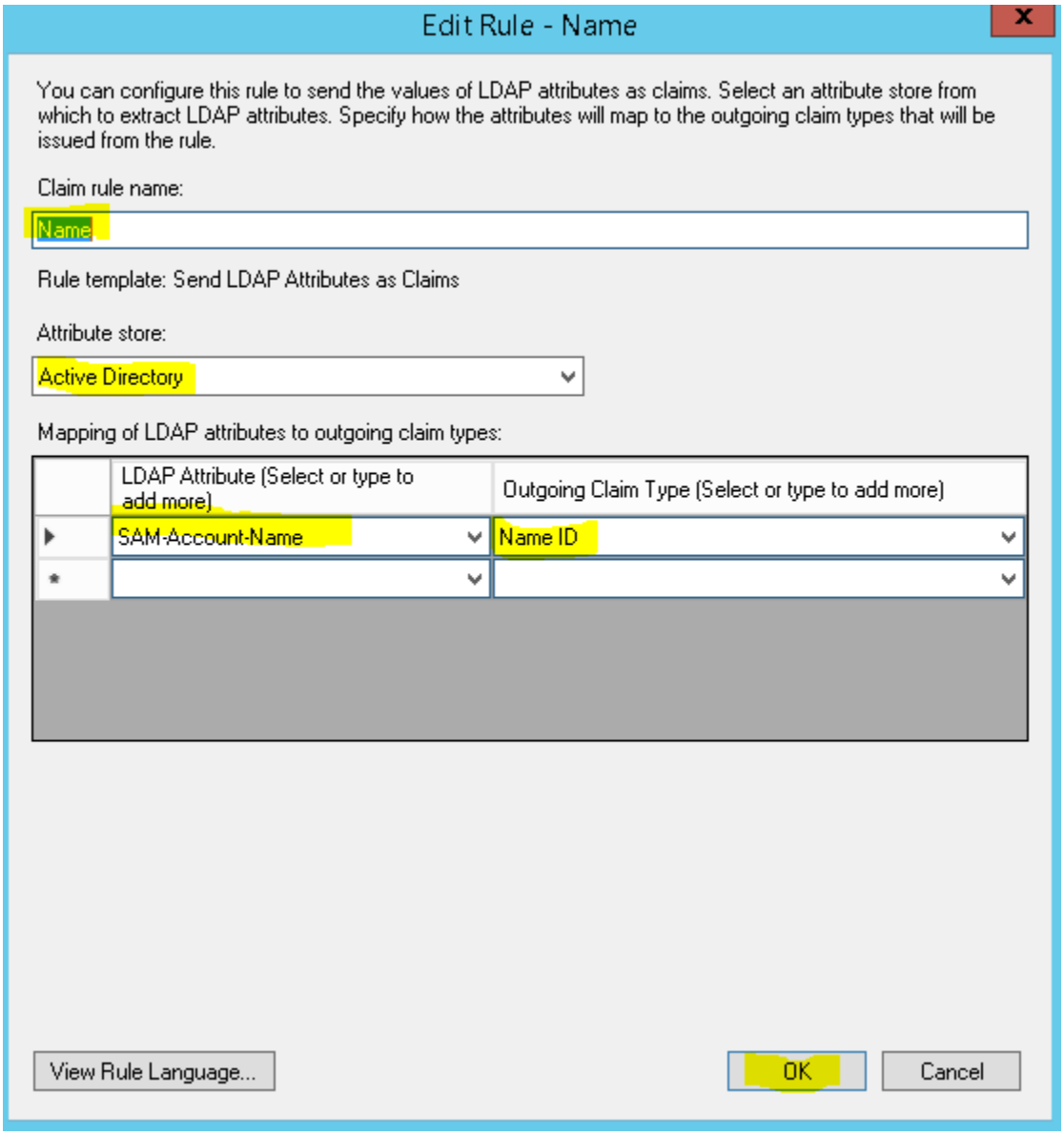

Figure 60. AD FS Relying Party – Add Name Rule

- Add another set of Claim rules with following values
  - Claim rule name → GivenName
  - Attribute Store → Active Directory
  - LDAP Attribute → Given-Name
  - Outgoing Claim Type → GivenName
- Click OK

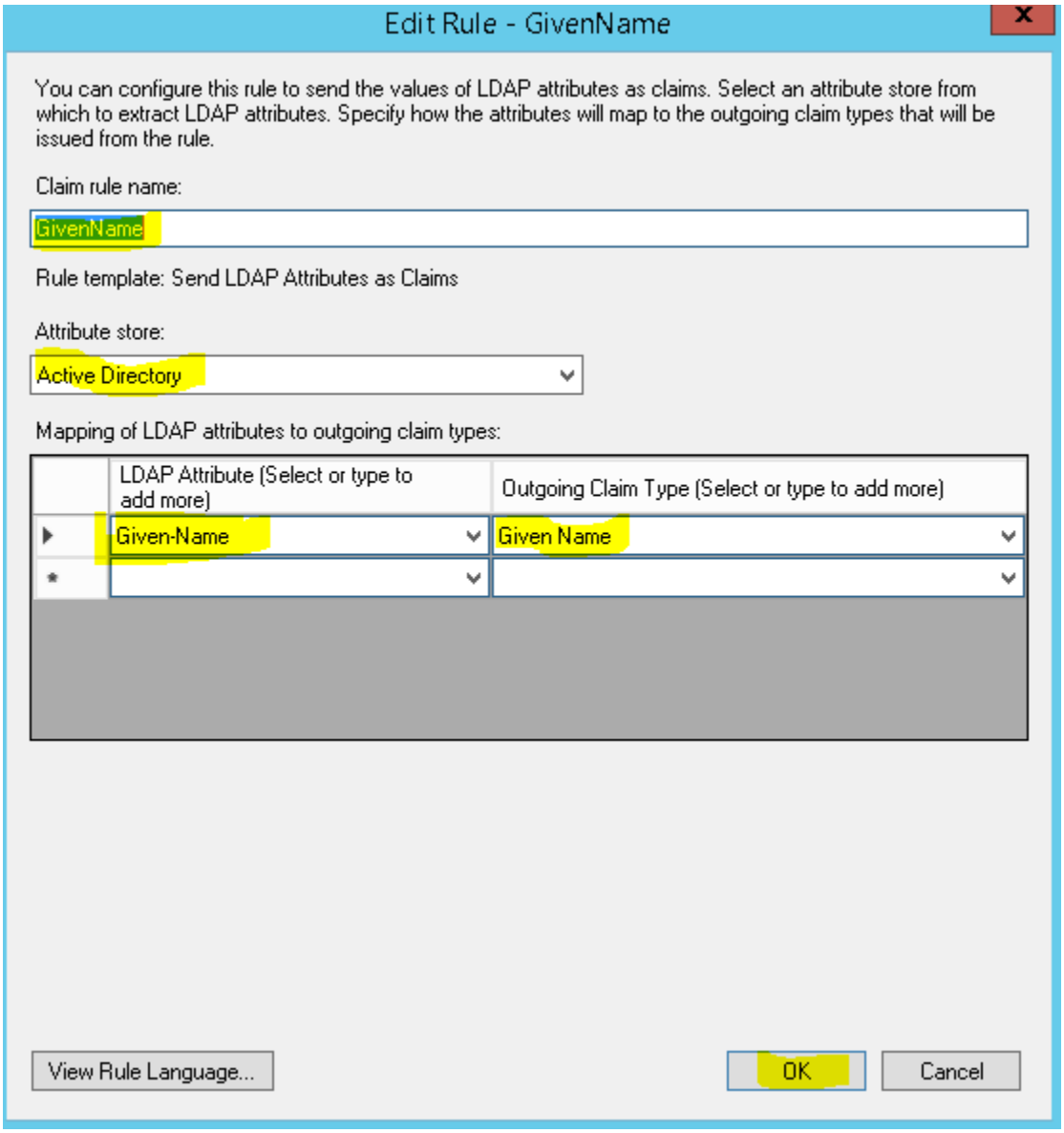

Figure 61. AD FS Relying Party – Add GivenName Rule

User Management in AD

With the SAML 2.0 SSO integration, the user managements are handled within AD Server. Following are the steps that can be followed for user management within AD Server.

Create an AD Organization

Various organizations can be created within Active Directory, and users can be mapped to a specific organization. To create an organization:

- Logon to AD Server with administrator privilege user Id
- Open Server Manager → Tools → Active Directory Users and Computers
- Click on the domain name at the left pane and right click, select New → Organizational Unit
- Enter a name for the Organization Unit and click OK

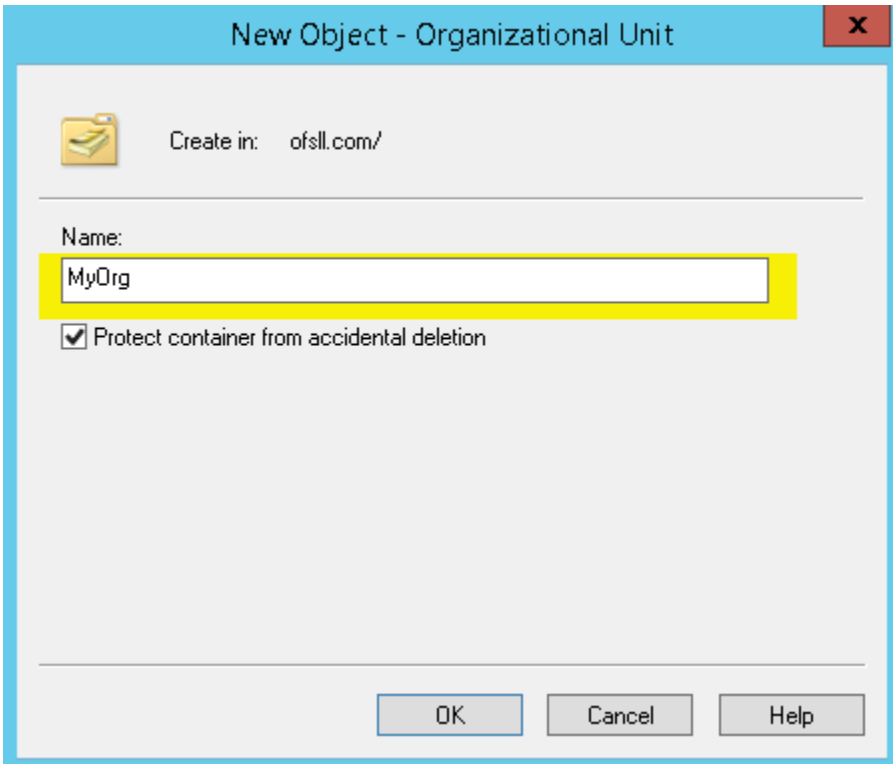

Figure 62. AD – Organizational Unit

Create an AD Group

Various groups can be created for a given organization, and users are mapped to a specific group within an organization. To create a group

- Right-click on the newly created organizational unit name and select New → Group
- Enter a name for the Group, other values can be default and click OK

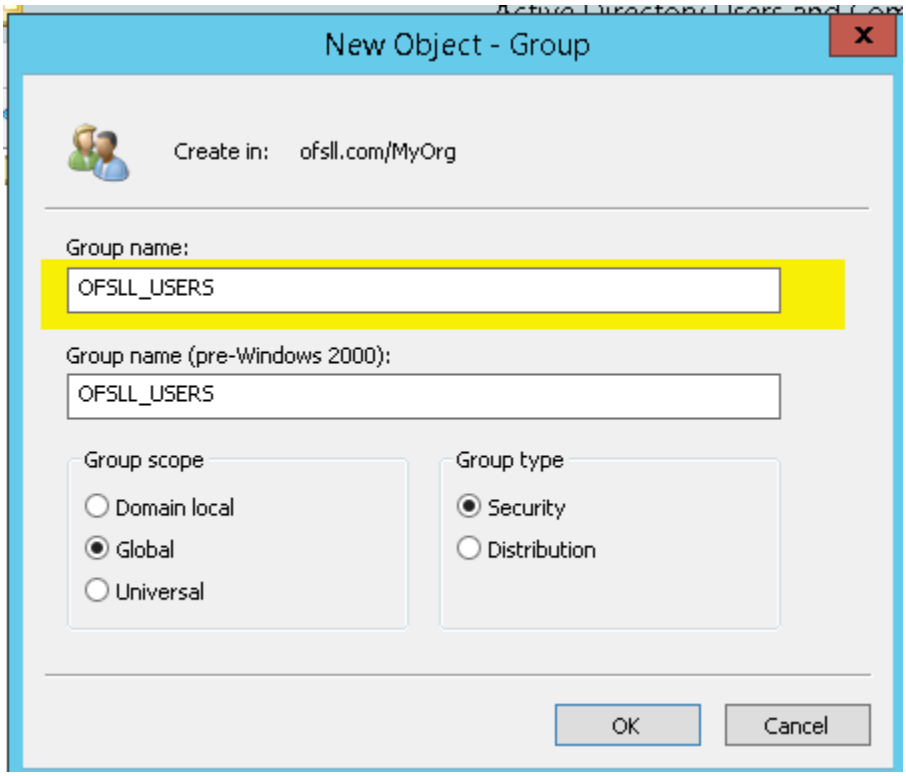

Figure 63. AD – Create Group

Create an AD User

Various users can be created for a given organizational unit and mapped to a given Group. To create an User

- Right-click on the newly created organizational unit name and select New → User
- Enter name of the User, provide a unique name for the User Logon field and click Next until User Id is created

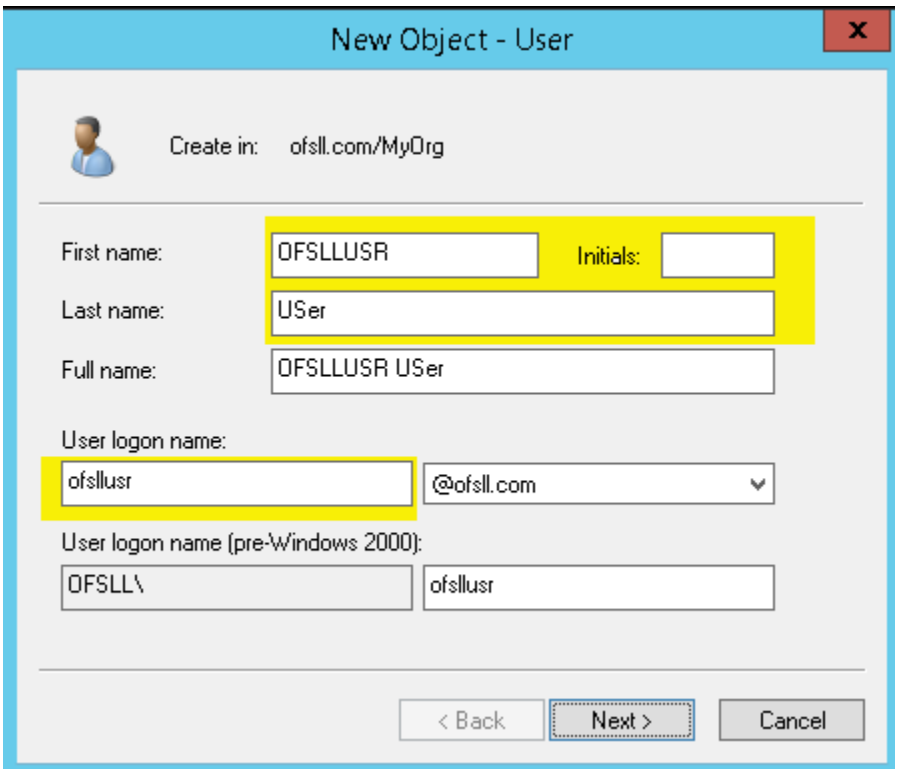

Figure 64. AD – Create User

AD Group Mapping to AD User

AD Users created in above steps should be mapped to AD groups defend. To map the users to the group

- Right-click on the newly created user and select “Add to a group”
- Enter a valid group name and click OK

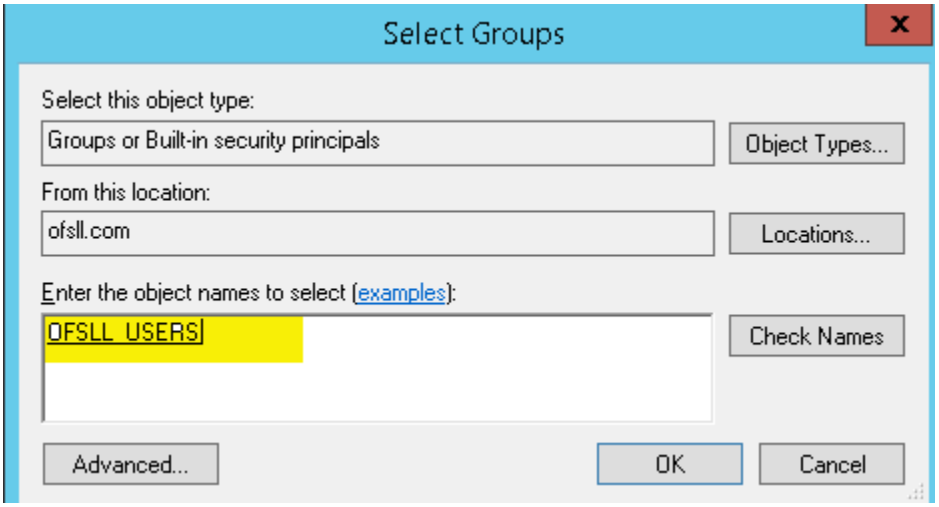

Figure 65. AD – Group Mapping

Users are now mapped and the AD Group. User provision steps are complete and as next steps these users are provisioned with OFSLL application access by adding these AD groups to Application via Enterprise Manager as mentioned in next section.

Addition of Active Directory Groups in EM

With user provisioning defined in AD Server, to provide access provision to these users to OFSLL application these AD groups must be mapped as Enterprise Role within OFSLL Server. This mapping is managed through Weblogic Enterprise Manager. Below are the steps to be followed:

- Login to OFSLL http://<WeblogicServerName>:<AdminPort>/em; for example http://ofsll.oracle.com:8001/em
- Select deployed OFSLL application as shown below

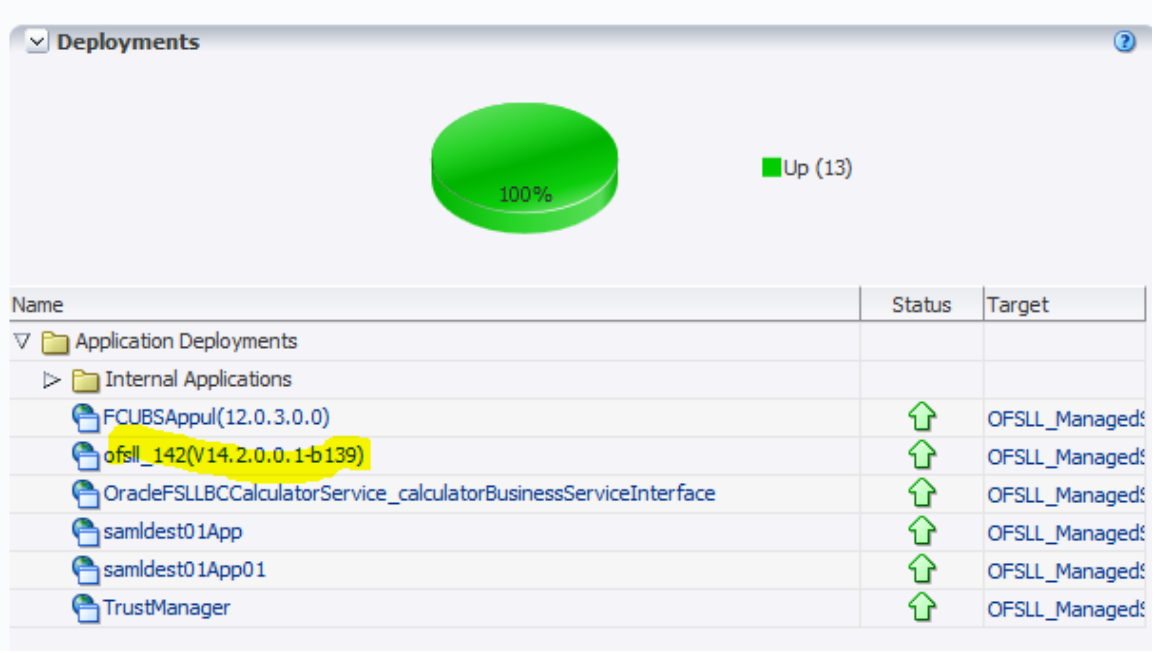

Figure 66. Weblogic EM –Deployments

» Select Application Deployment -> Security -> Application Roles

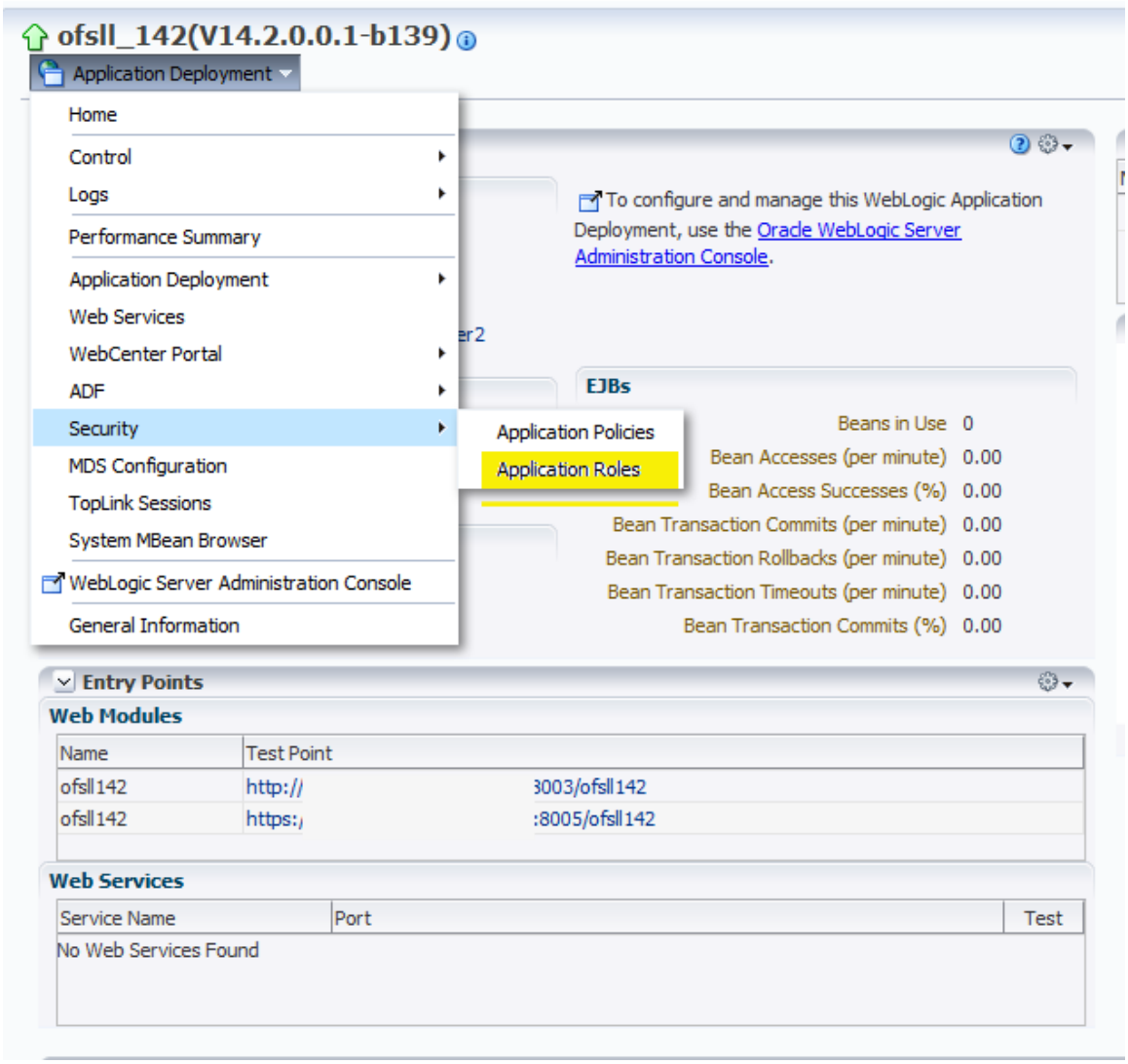

Figure 67. Weblogic EM – Application Roles

» Click on “Execute” button and below details shows up

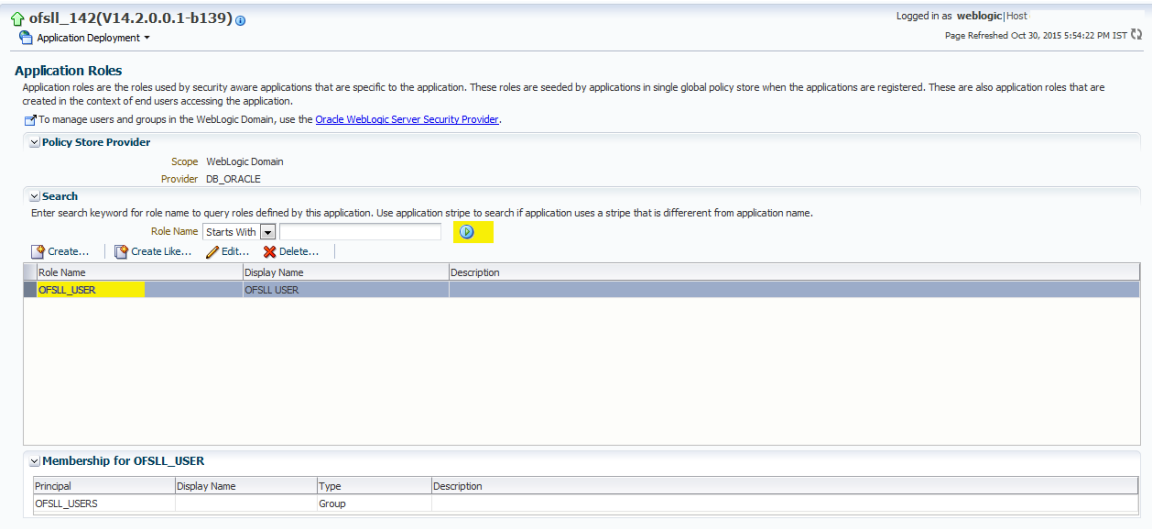

Figure 68. Weblogic EM – Application Roles

» Click on “Edit”

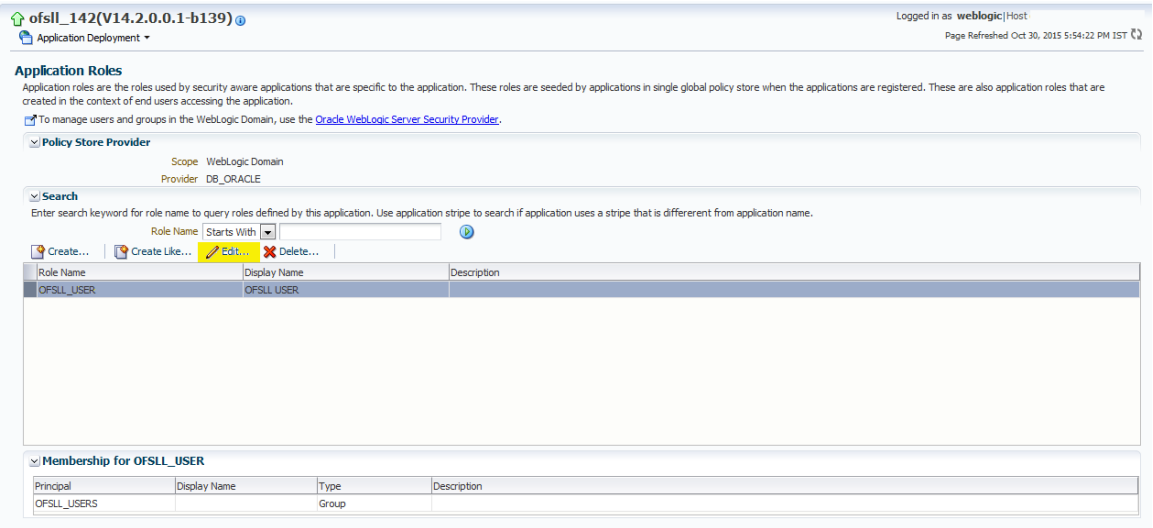

Figure 69. Weblogic EM – Edit Application Roles

» Click on Members → “Add”

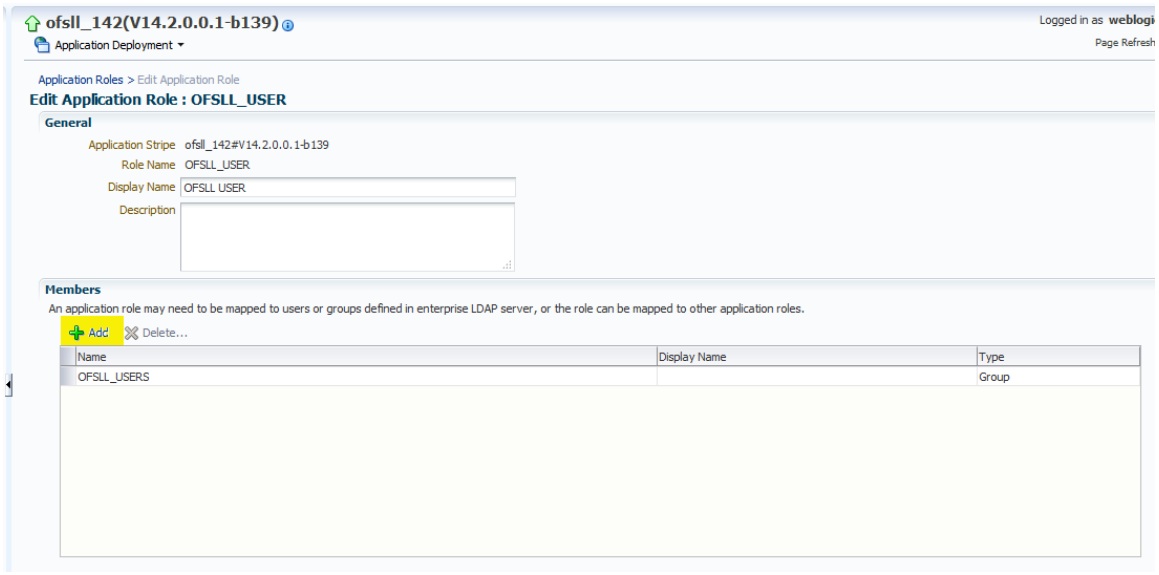

Figure 70. Weblogic EM – Enterprise Roles List

» On Add principal screen select Type as “Group” and click on Search.

Note: sometimes there is a chance that the AD related groups are not going to show up.

» Under Advanced Option, select the check-box and click ok

» Enter the AD group name manually and click OK, once again OK.

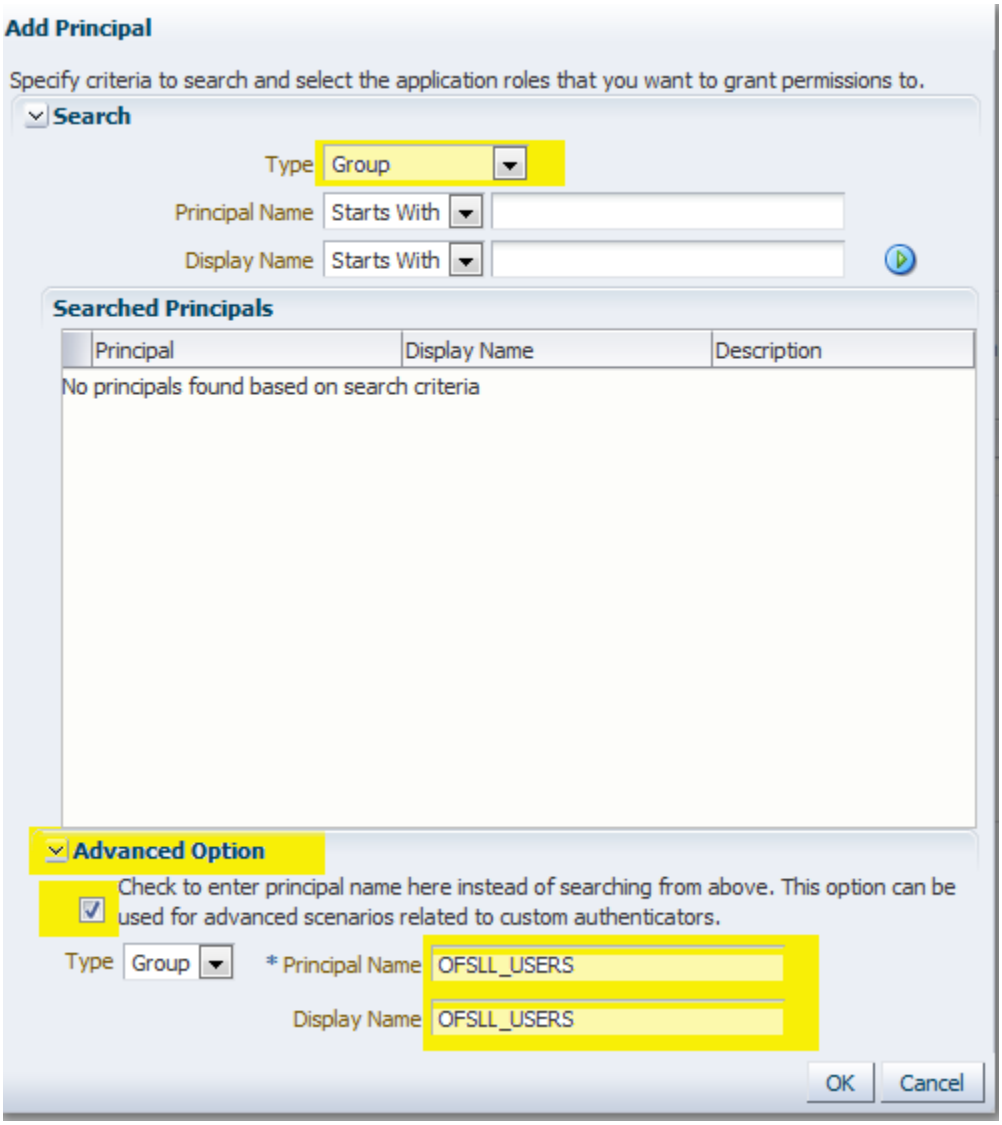

Figure 71. Weblogic EM – Addition of Enterprise Roles

The users defined to the AD Group now have access permission to OFSLL application.

Addition of Application Roles in EM

This is particular settings is only required for granting access permission to the Customer Service screen, wherein the customer service screen is accessed directly from outside the OFSLL application by 3rd party system.

- Logon to http://<Weblogic ServerName>:<AdminPort>/em ; for example http://ofsll.oracle.com:8001/em
- Select deployed OFSLL application as shown below

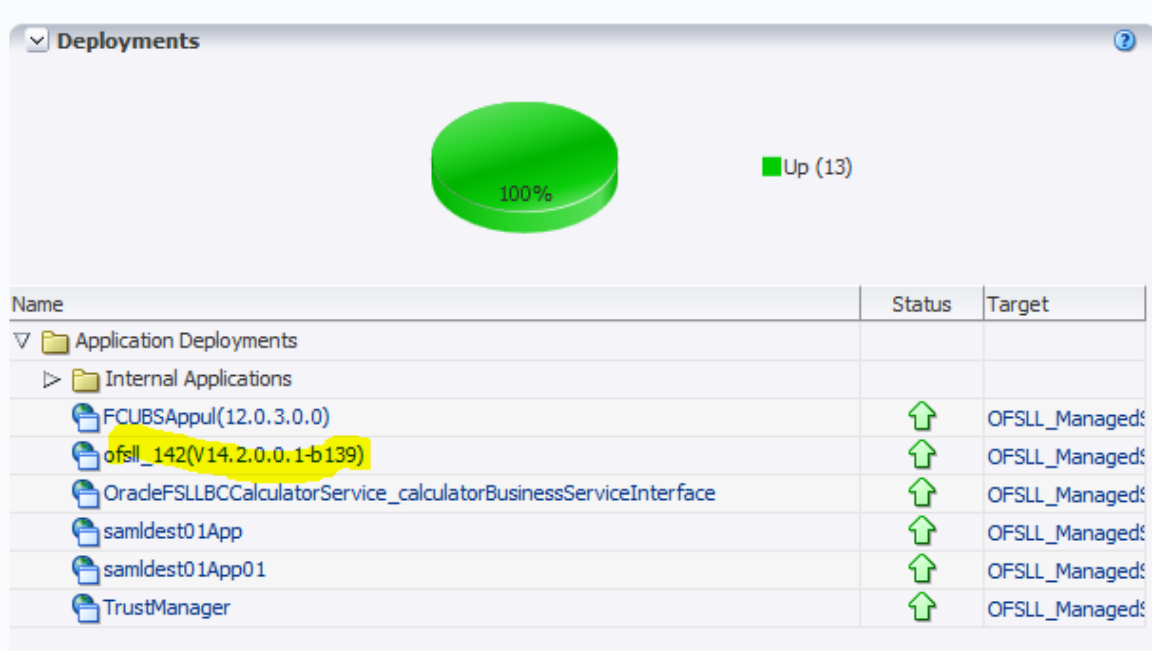

Figure 72. Weblogic EM –Deployments

» Select Application Deployment -> Security -> Application Policies

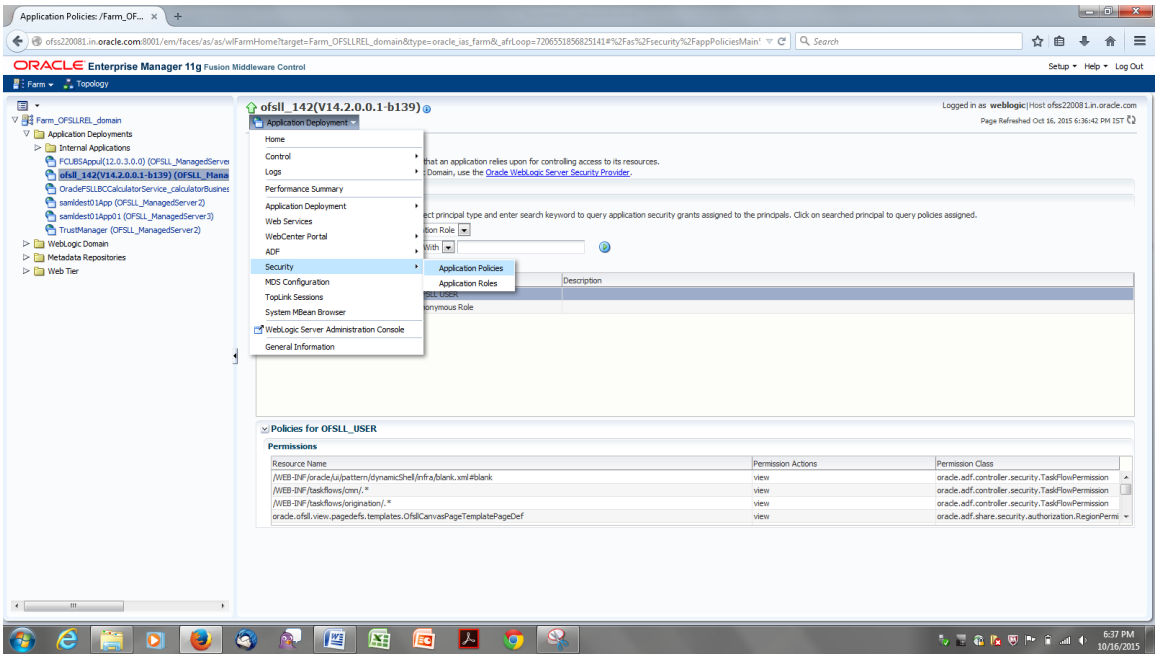

Figure 73. Weblogic EM –Security Policies

» Below detail shows up

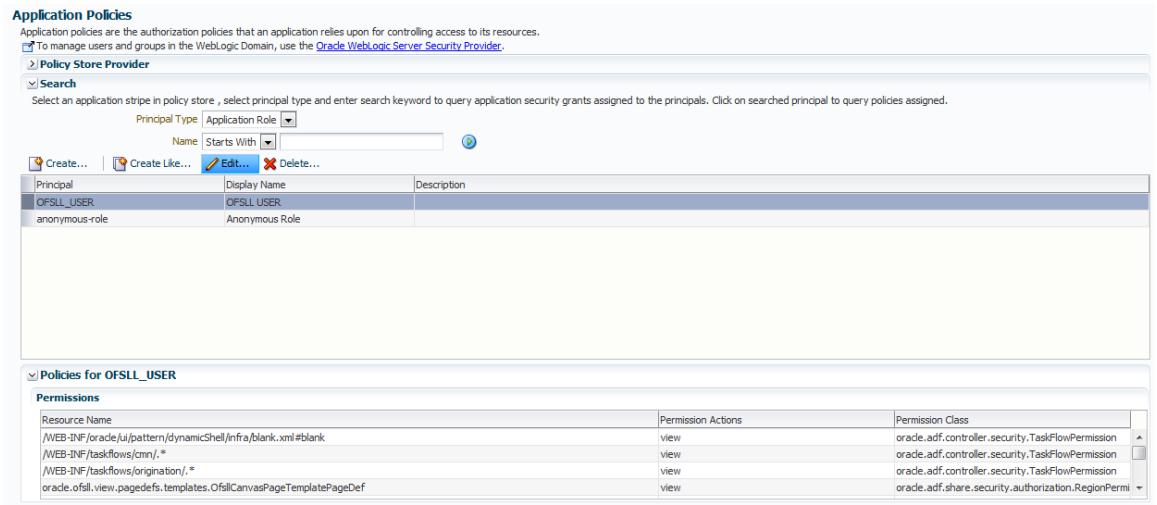

Figure 74. Weblogic EM – Application Policies

» For the Principal “OFSLL_USER” click on “Edit” below screen shows up

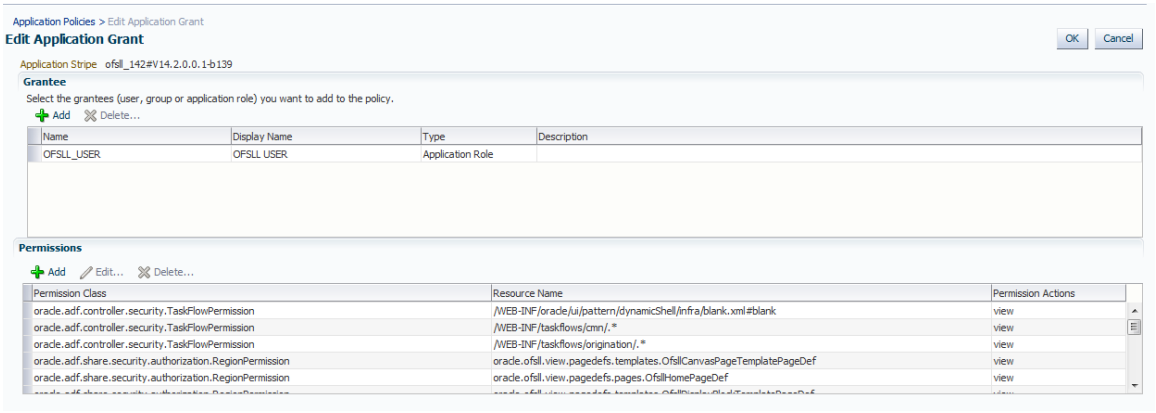

Figure 75. Weblogic EM – Application Grant

» There is a likely chance that there is no permission defined for “oracle.ofsll.view.pagedefs.pages.OfsllCustomerServicePageDef” Resource Name, which you need to add by clicking “Add” button under Permissions Tab

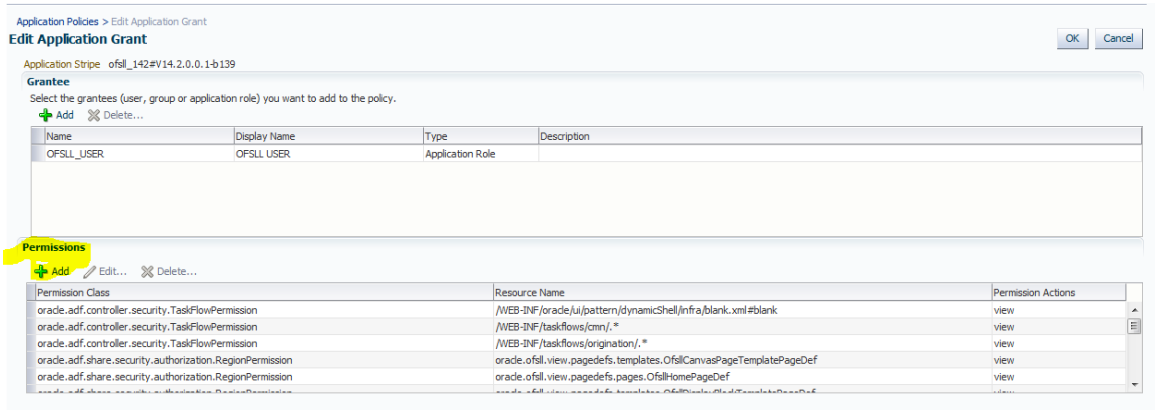

Figure 76. Weblogic EM – Edit Application Permissions

» Below screen pops-up do not do anything here just click continue

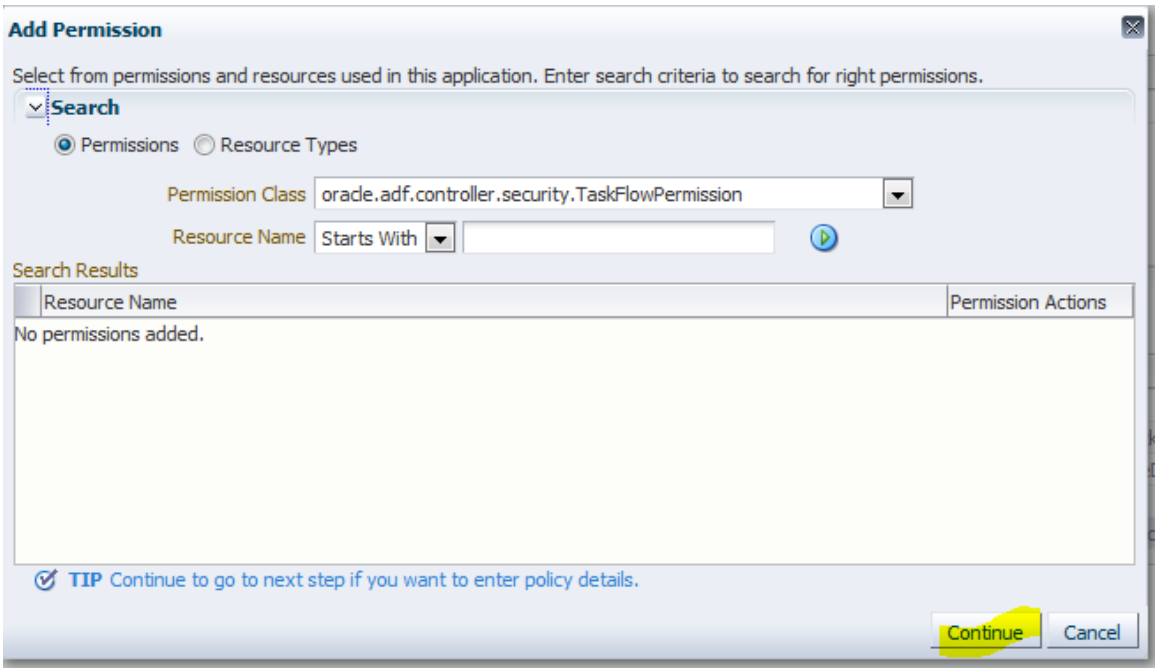

Figure 77. Weblogic EM – Add Permission

» Enter the following values as shown in the image below and "select"
  » Permission Class → oracle.adf.share.security.authorization.RegionPermission
  » Resource Name → oracle.ofsll.view.pagedefs.pages.OfsllCustomerServicePageDef
  » Permission Actions → view
» Click Select

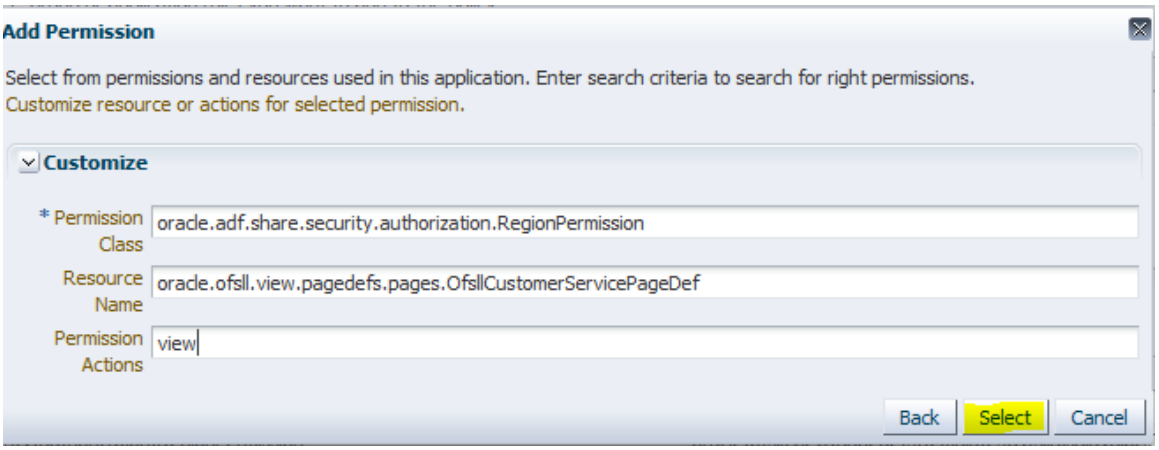

Figure 78. Weblogic EM – Add Permission

» Click "Ok" on subsequent screens and ensure the record is saved

» Login to the OFSLL application with following context; https://<WeblogicServerName>:<ManagedServerPort>/<OfsllContext>/faces/pages/OfsllHome.jspx ; for example https://ofsll.oracle.com:9704/ofsll142/faces/pages/OfsllHome.jspx

» The AD FS Sign-In page opens up, wherein provide your AD User Id/password credentials.

Note: on Firefox/Chrome browser the browser based AD FS Sign-In page opens whereas on IE a popup window open up.

» Below IE AD FS Sign-in dialog box window

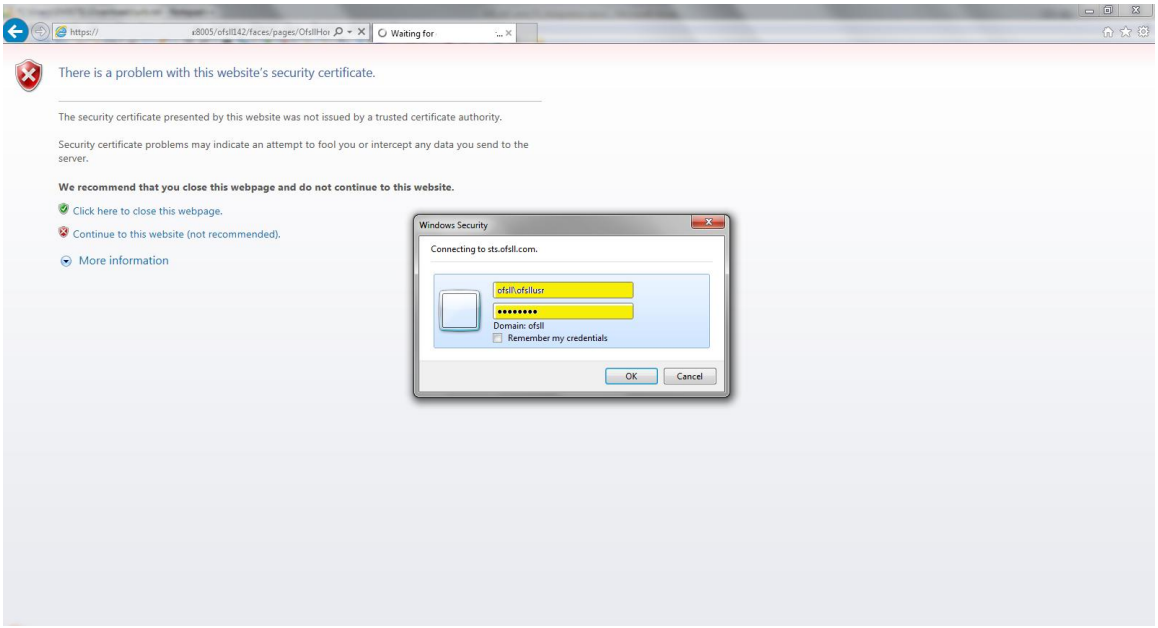

Figure 79.Internet Explorer: AD FS Sing-In pop-up windows

» On successful authentication, OFSLL Home page opens up

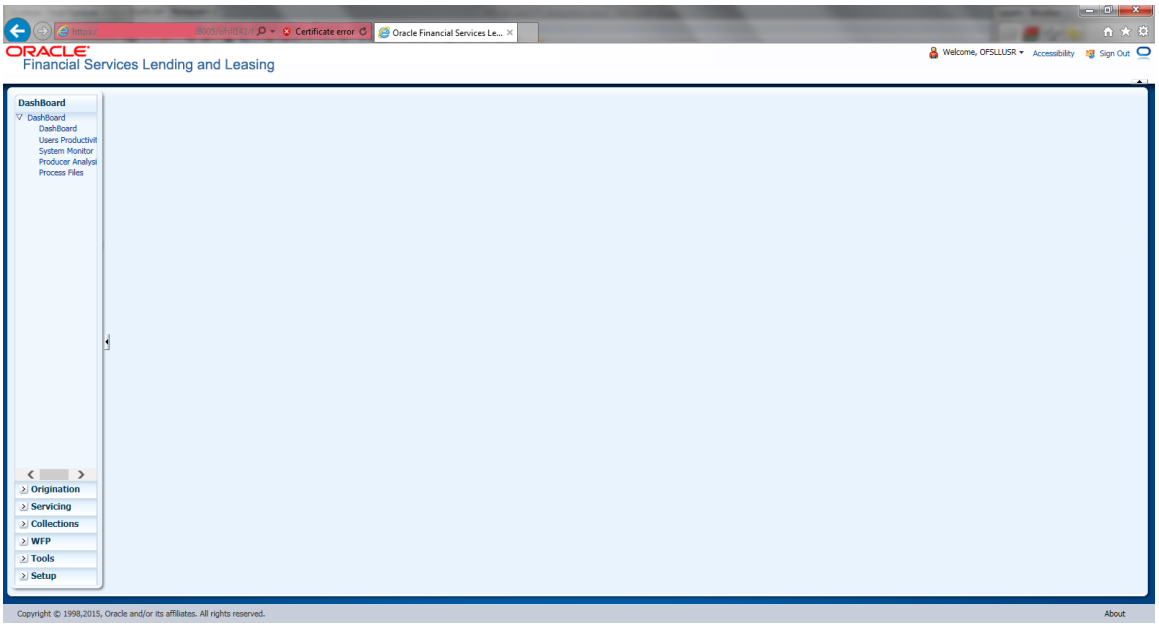

Figure 80. Internet Explorer: OFSLL Home Page

» AD FS Sign-In Page while using Firefox or Google Chrome browser

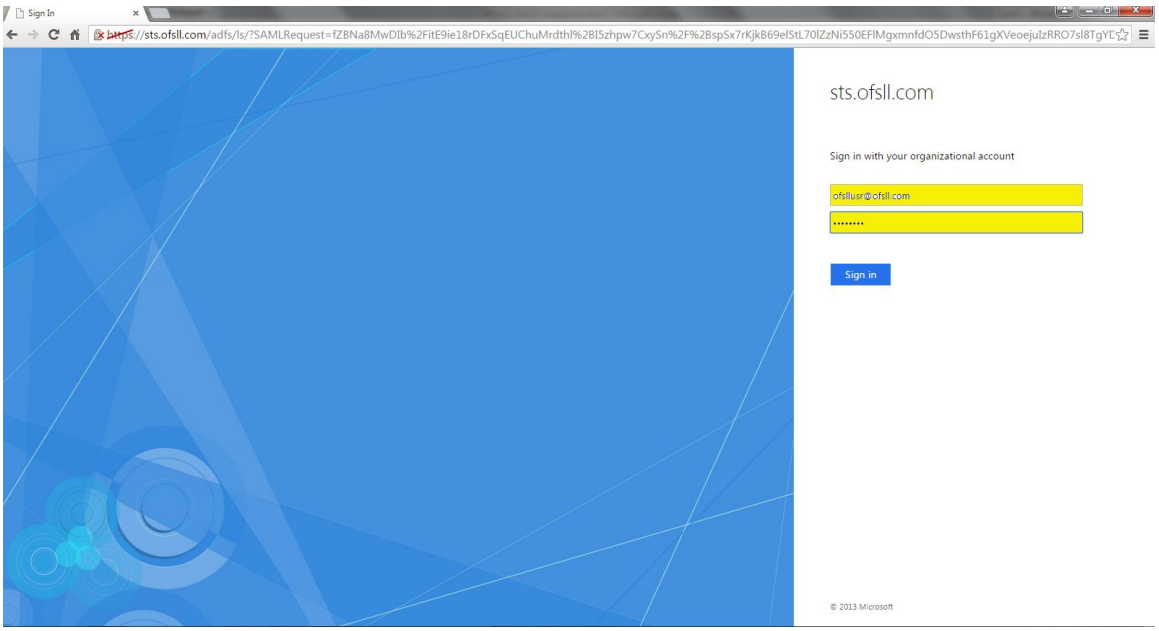

Figure 81. Google Chrome: AD FS Sign-In Page

Troubleshooting

- AD FS related alerts can be viewed and monitored within the AD Server as part of Server Management Console
- On Weblogic server, the SAML debug can be enabled by setting following properties as part of weblogic startup script

    - EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES} -Dweblogic.debug.DebugSecuritySAML2Atn=true -Dweblogic.debug.DebugSecuritySAML2CredMap=true -Dweblogic.debug.DebugSecuritySAML2Lib=true -Dweblogic.debug.DebugSecuritySAML2Service=true"

- Once the debug properties are enabled, the weblogic server log file will have SAML enabled debug logs captured

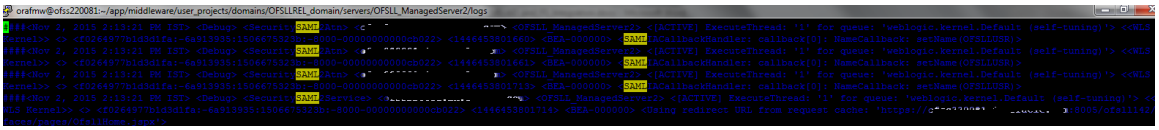

Figure 82. Weblogic Log: SAML Debug logs

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services

White Paper Title

Author: [OPTIONAL]
Contributing Authors: [OPTIONAL]