

# 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 2020





## 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.




ORACLE®



## Table of Contents

Disclaimer	1
Introduction	1
Pre-requisite	1
Components	1
Assumptions	1
Installation of Active Directory Federation Services	2
Install AD FS on AD Server	2
Configure AD FS	6
How to Create Self-signed Certificate	7
How to Register the Certificate	7
AD FS Configuration	9
Verify AD FS Installation	16
Configuration on Weblogic Domain Server as Service Provider (SP)	17
Pre-configuration of Managed Server	17
Enable SSL	18
Creation of Self-Signed Domain Certificate	18
Steps to configure Custom Identity and Custom Trust	20
Configuring the domain as SAML 2.0 Service Provider	23
Creating SAML Identity Asserter	23
Configuring SAML 2.0 Service Provider (SP)	24
Configuring SAML 2.0 Federation properties for the Domain	24



Configuring Identity Provider (IdP) as Service Provider on the Domain	28
Modify Federation Metadata	29
Configure Domain for SSO	33
Configuring Domain as a partner with the Identity Provider (IdP)	36
Configure Relying Party	36
Editing the Relying Party Trusts	45
Adding Rules	50
User Management in AD	55
Create an AD Organization	55
Create an AD Group	56
Create an AD User	57
AD Group Mapping to AD User	58
Addition of Active Directory Groups in EM	59
Addition of Application Roles in EM	64
Troubleshooting	70

## Introduction

The intent 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 ofsl\_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

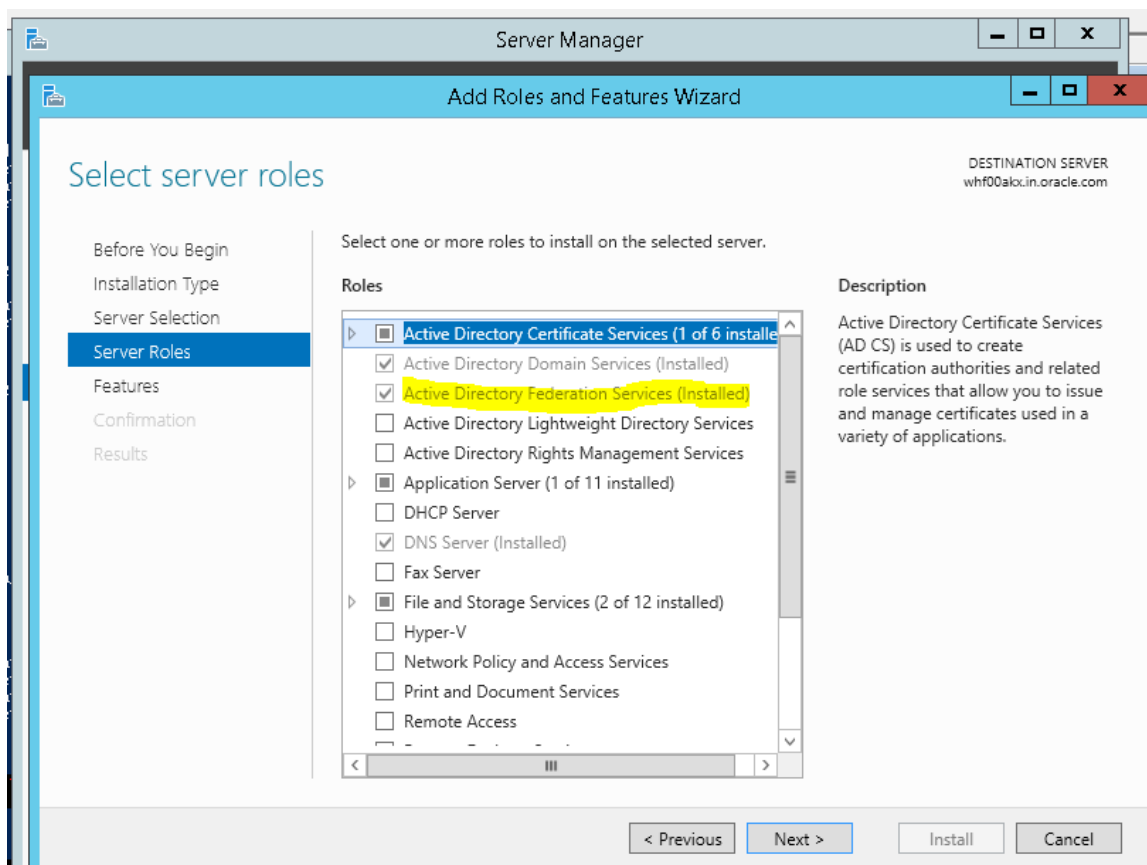


Figure 1. Install AD FS –Server Roles

» On the Select Features interface, click Next

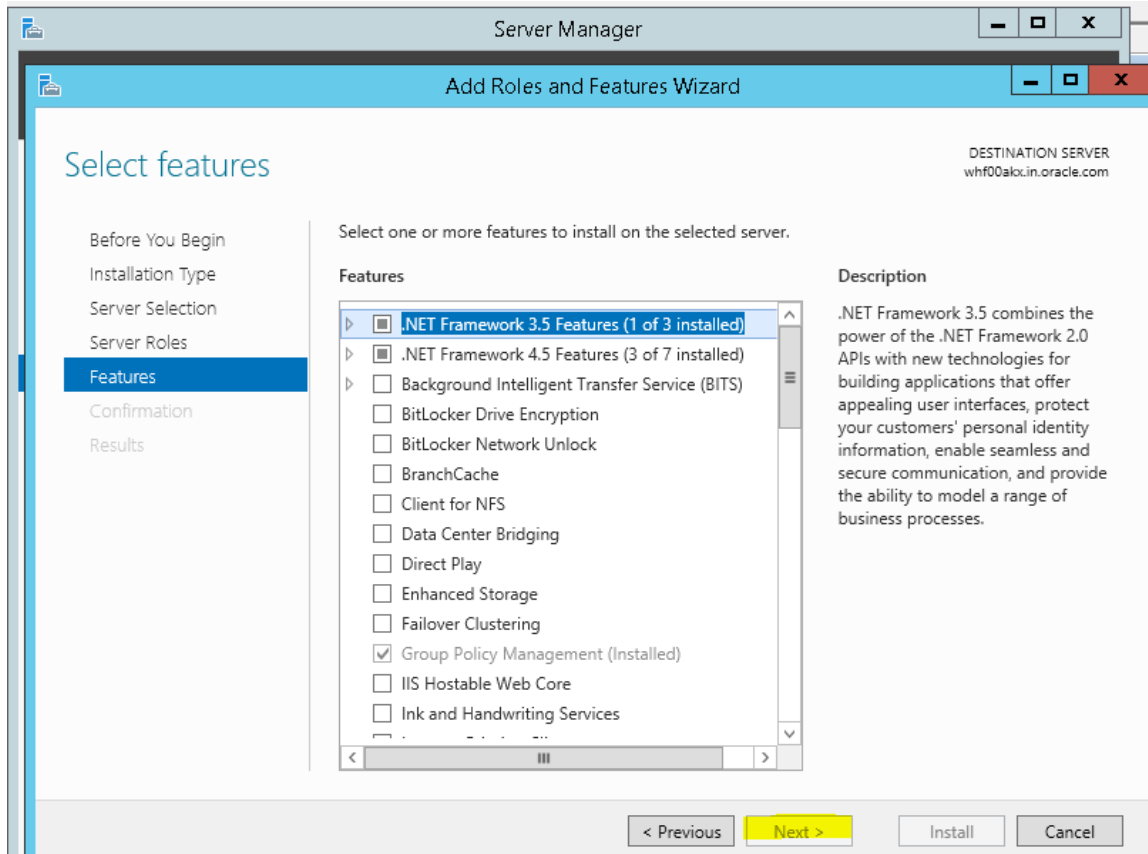


Figure 2. Install AD FS – Select Features

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

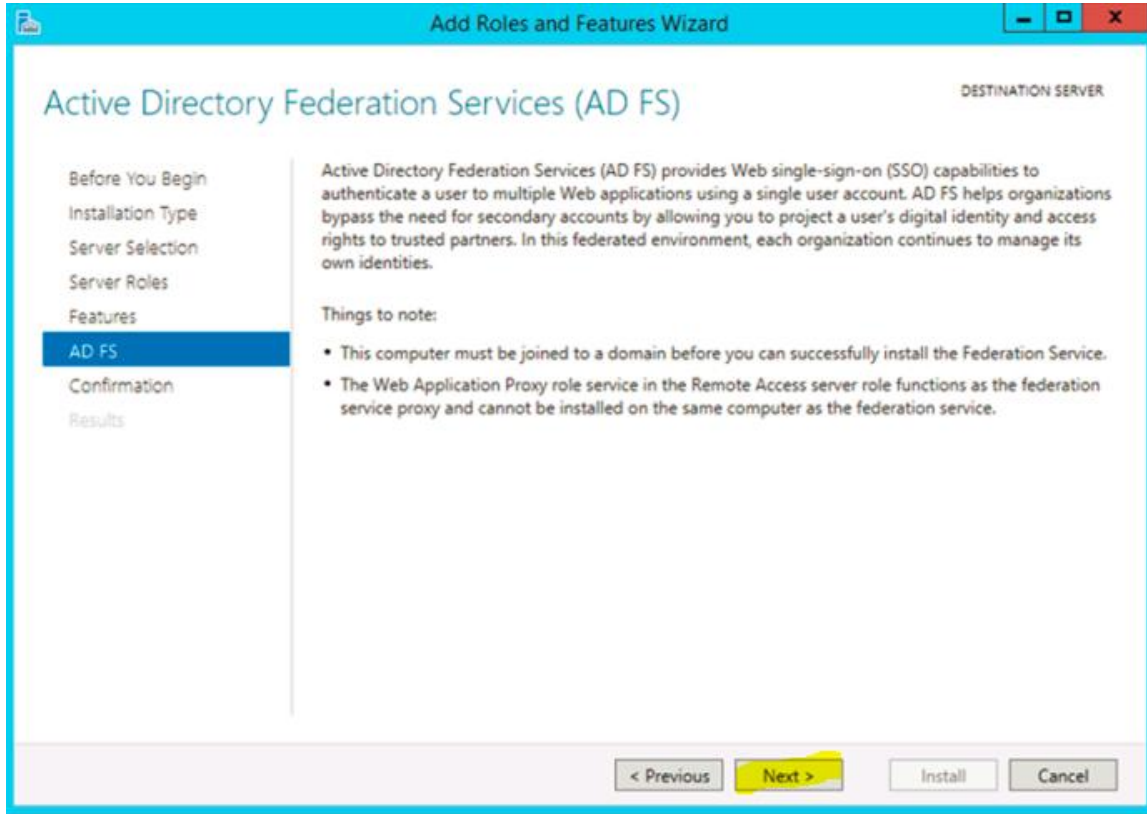


Figure 3. Install AD FS – AD FS Page



» Click Install

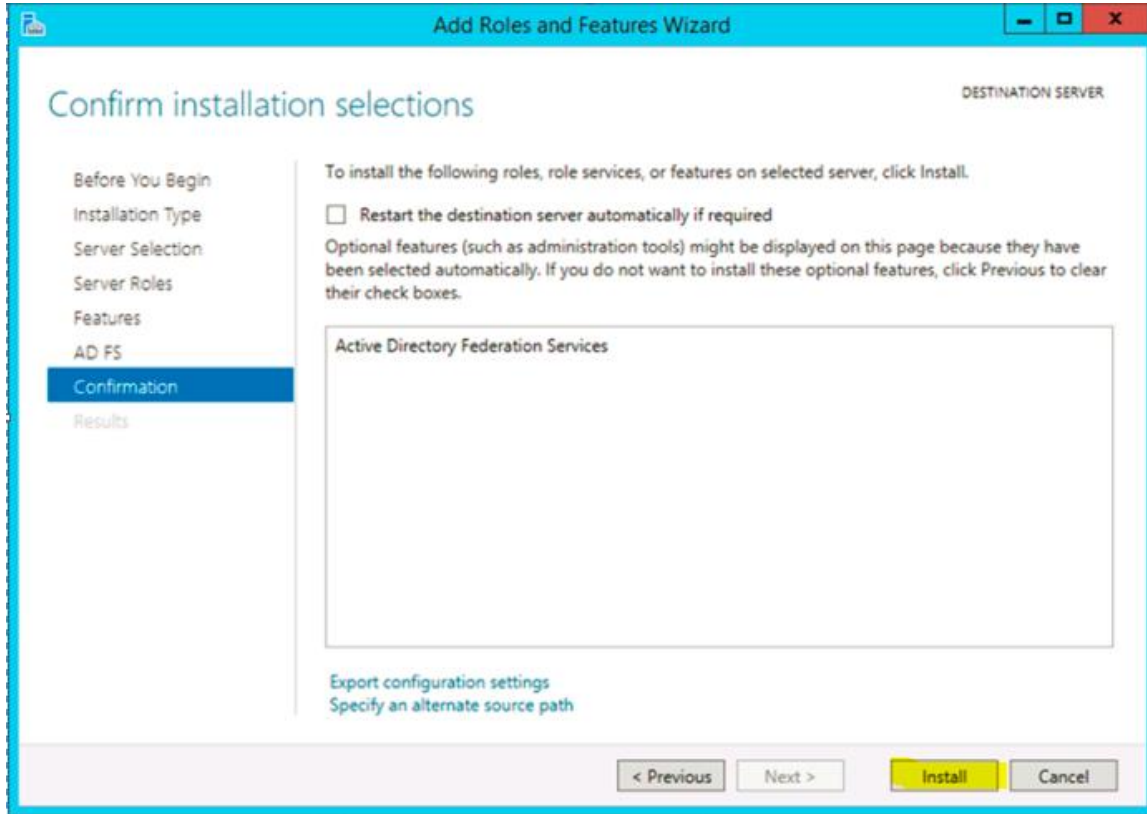


Figure 4. Install AD FS – Confirmation Page

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

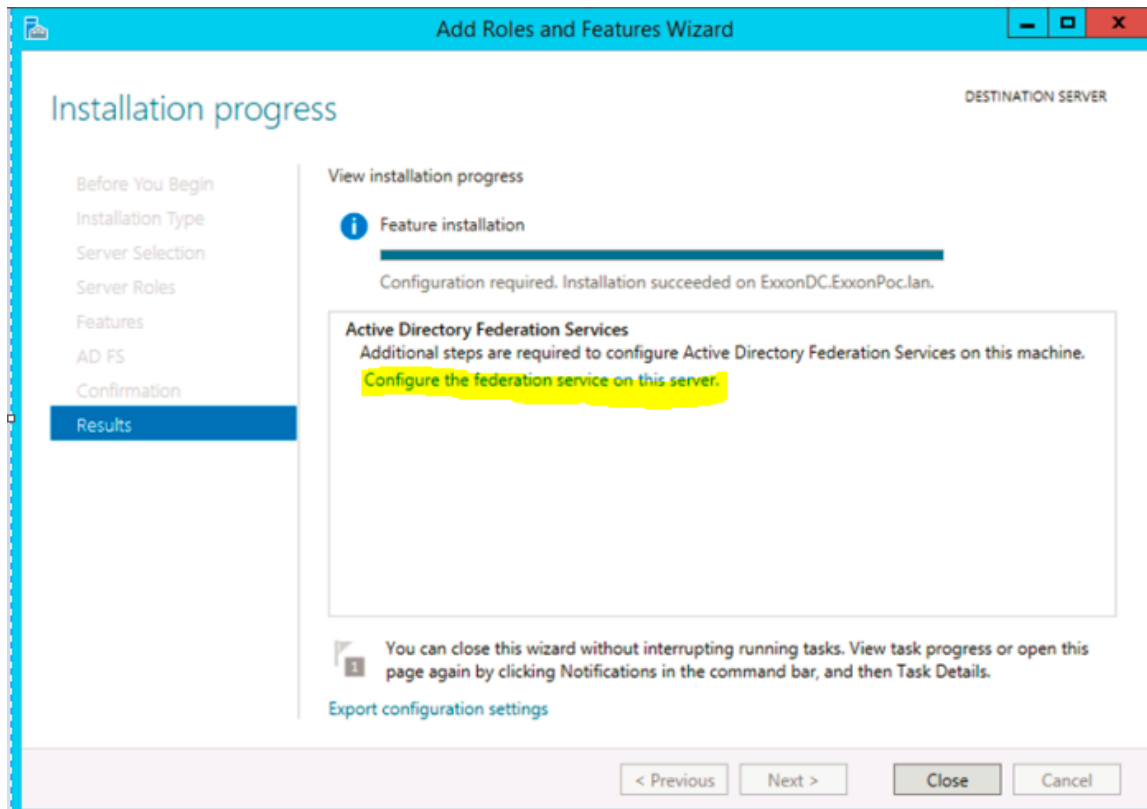


Figure 5. Install AD FS – Result Page

## 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

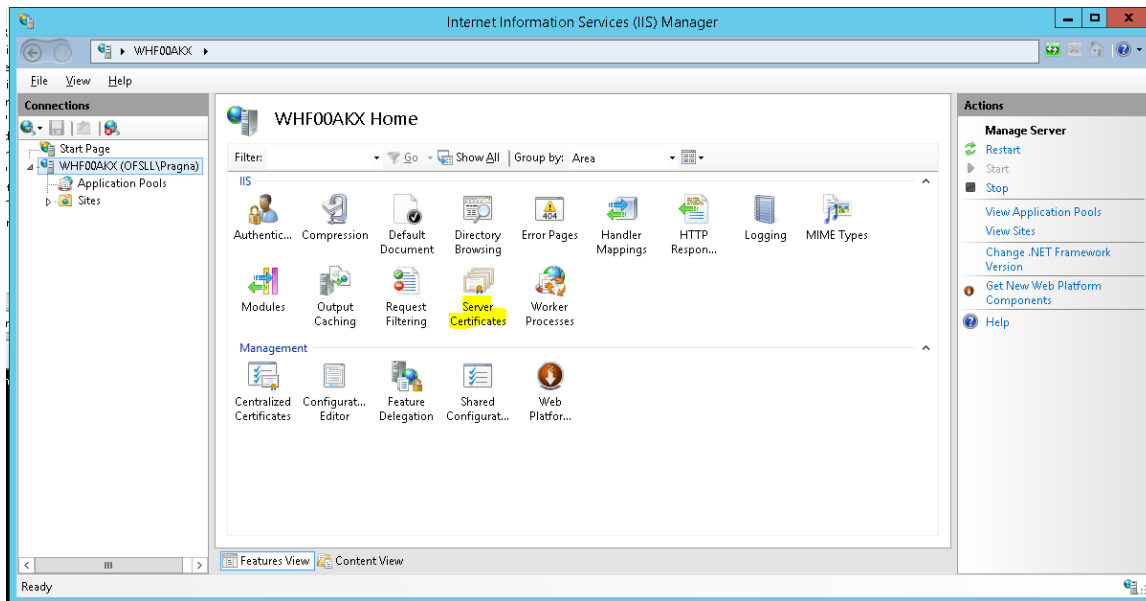


Figure 6. IIS Manager – Main Page

» Click on import link

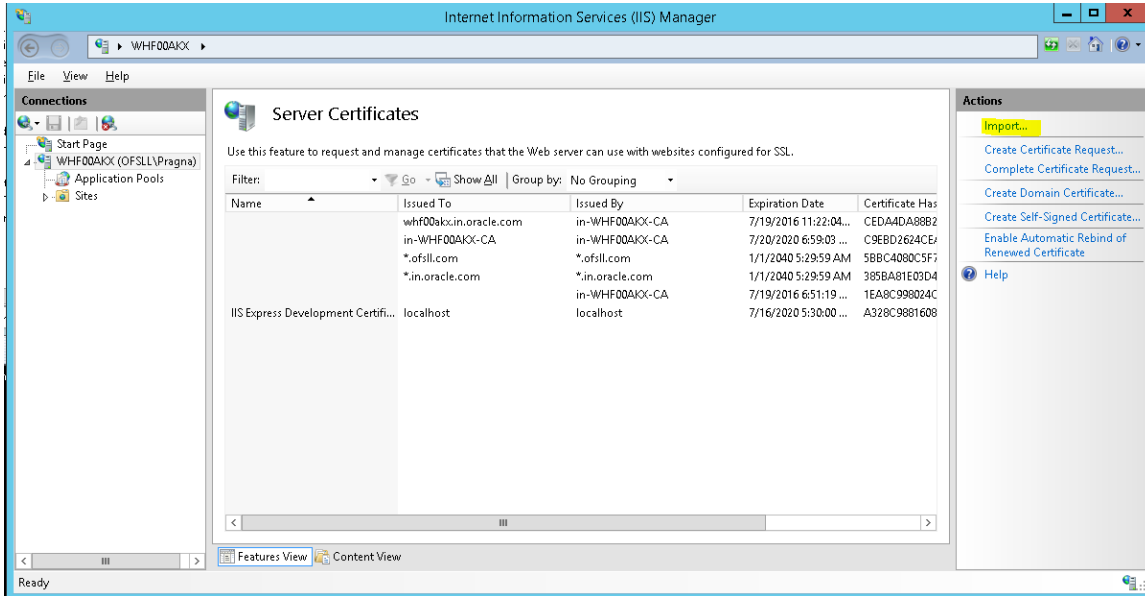


Figure 7. IIS Manager - Server Certificates

- » Upload the certificate “CACer.pfx” file generated in previous section and password
- » Click Ok to import the certificate

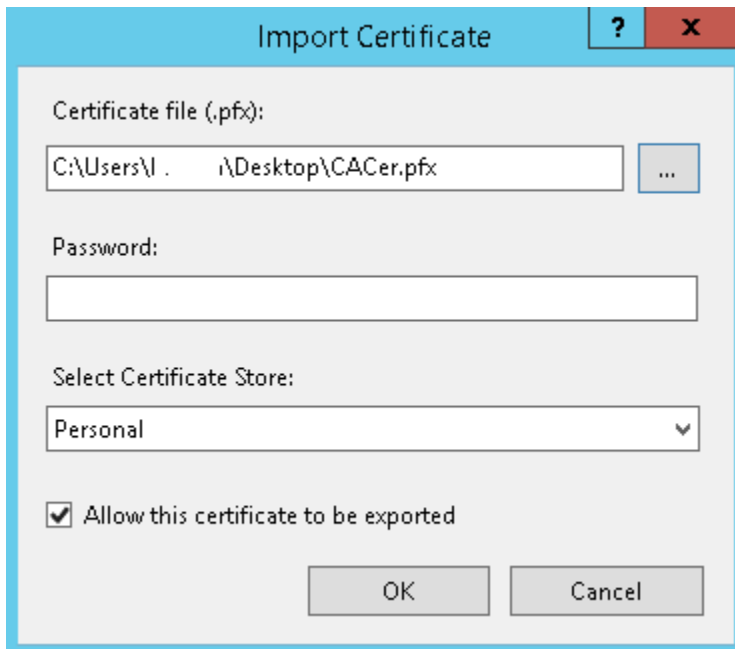


Figure 8. IIS Manager – Import Certificate

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

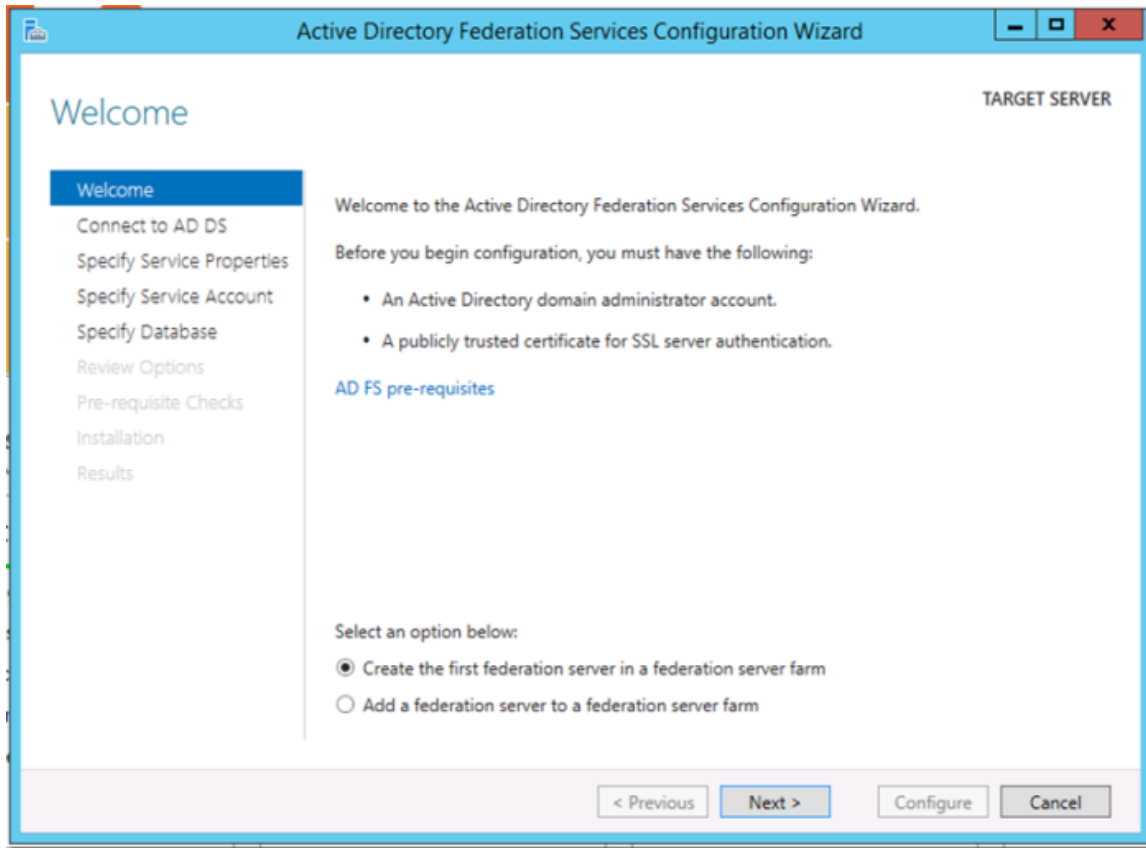


Figure 9. AD FS Configuration – Welcome Page

- » 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.*

---

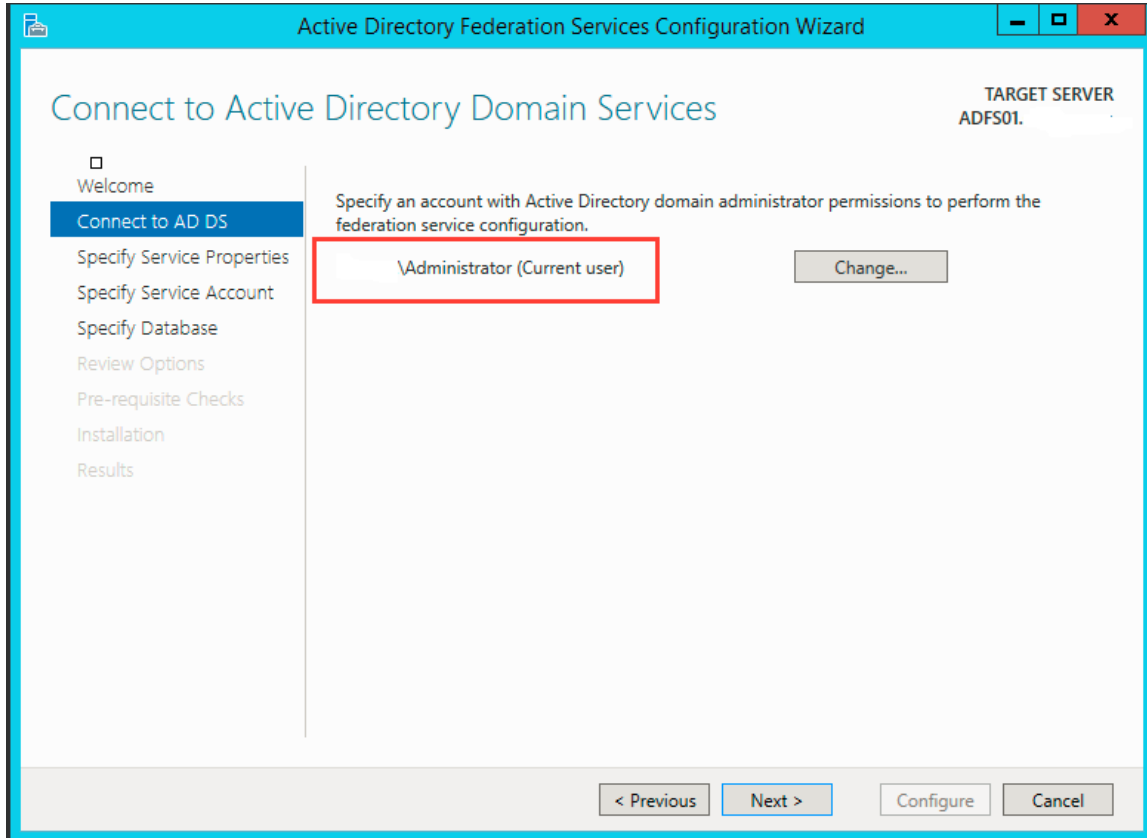


Figure 10. AD FS Configuration – AD Service Interface

- » 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

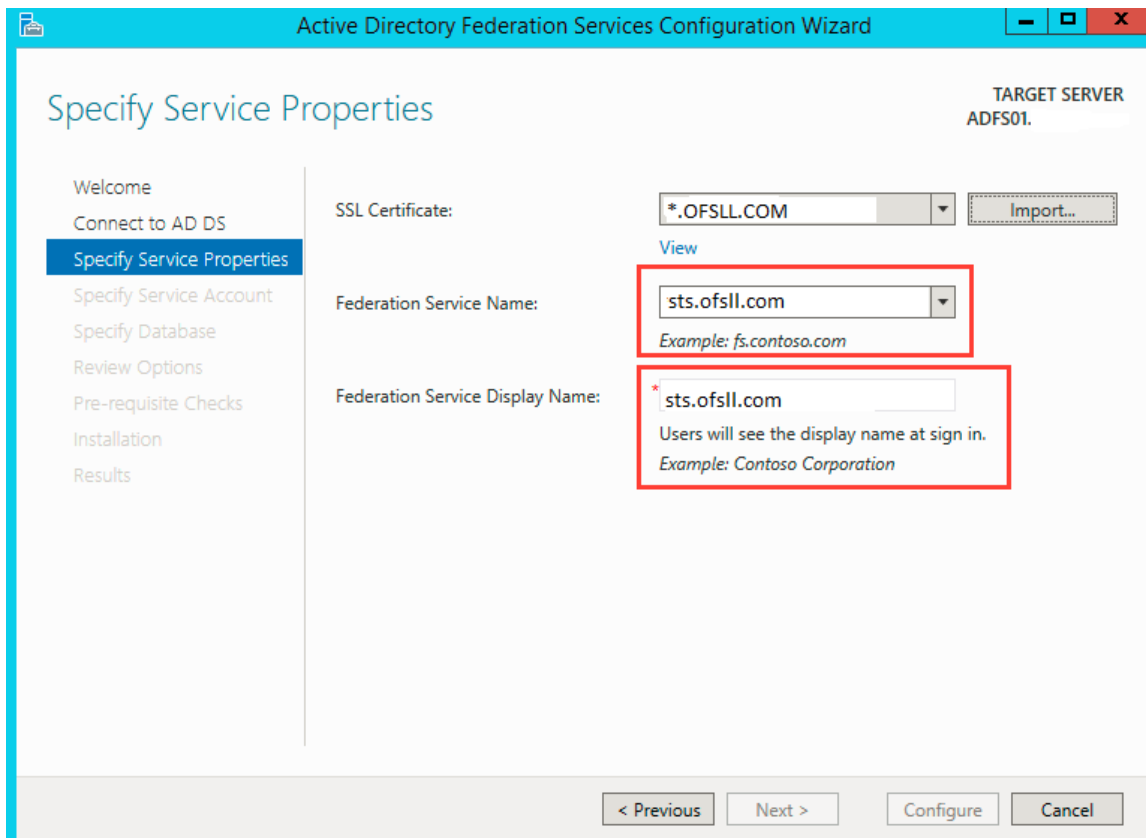


Figure 11. AD FS Configuration – Service Property Setup

- » 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.

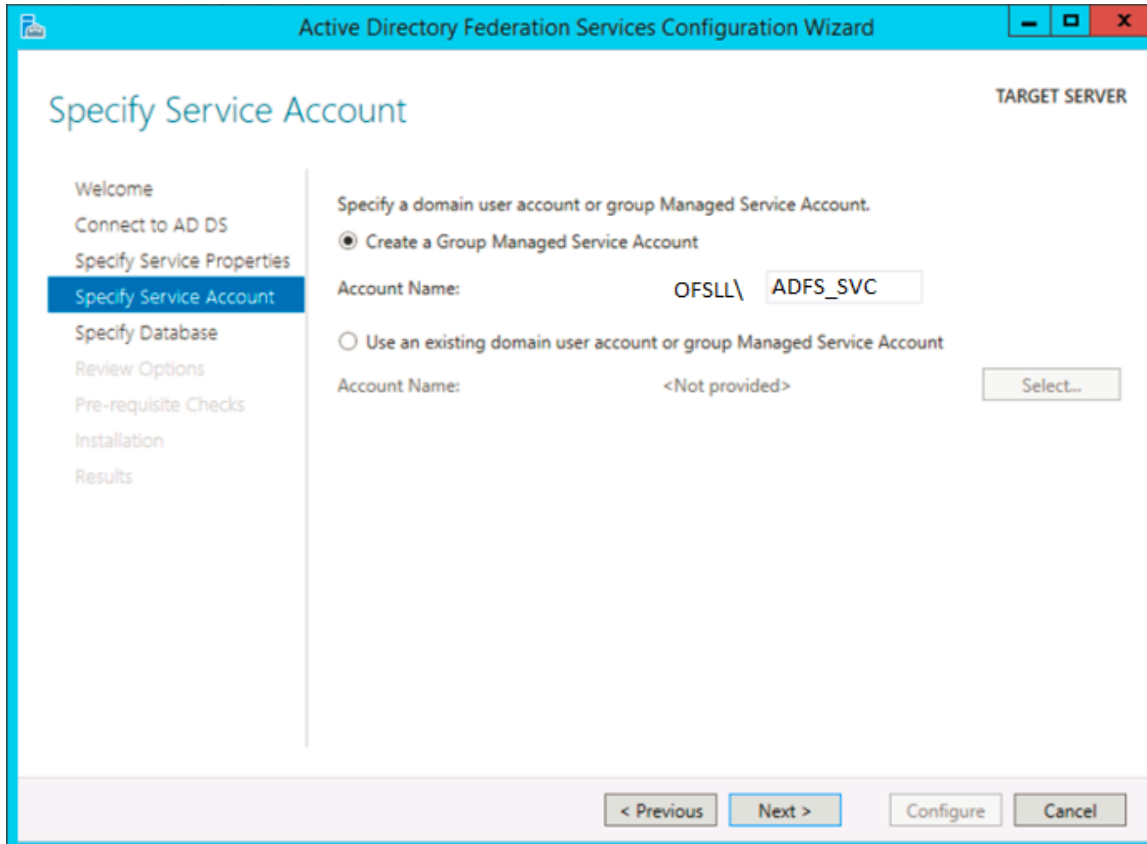


Figure 12. AD FS Configuration – Service Account Setup



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

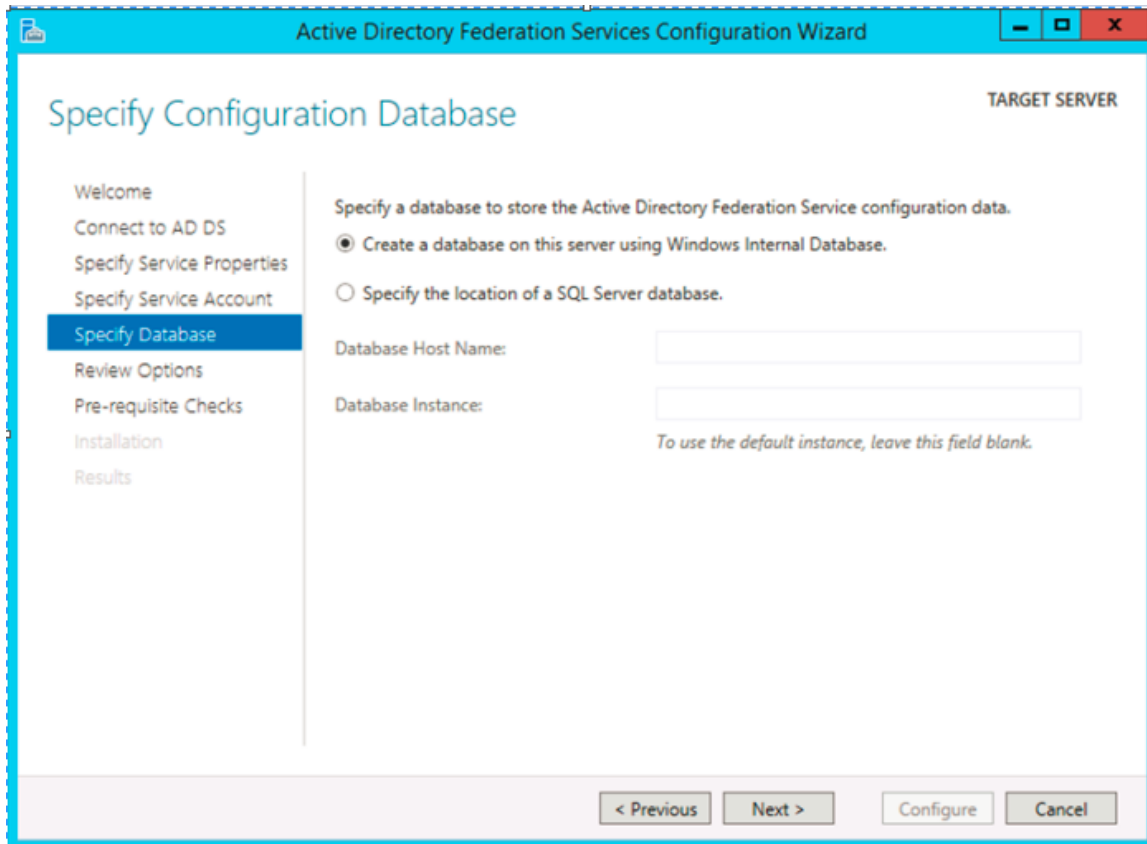


Figure 13. AD FS Configuration – Service Database Setup

» On the Review Options interface, click Next

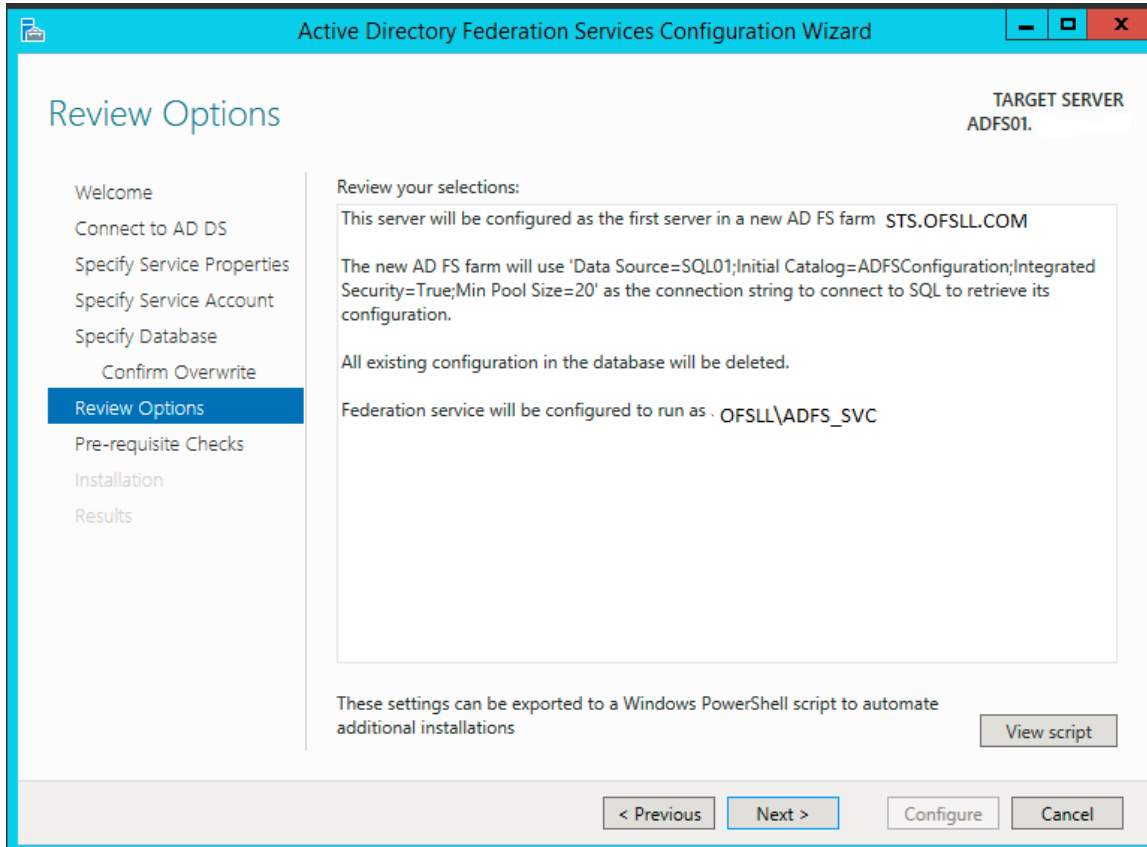


Figure 14. AD FS Configuration – Review Page

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

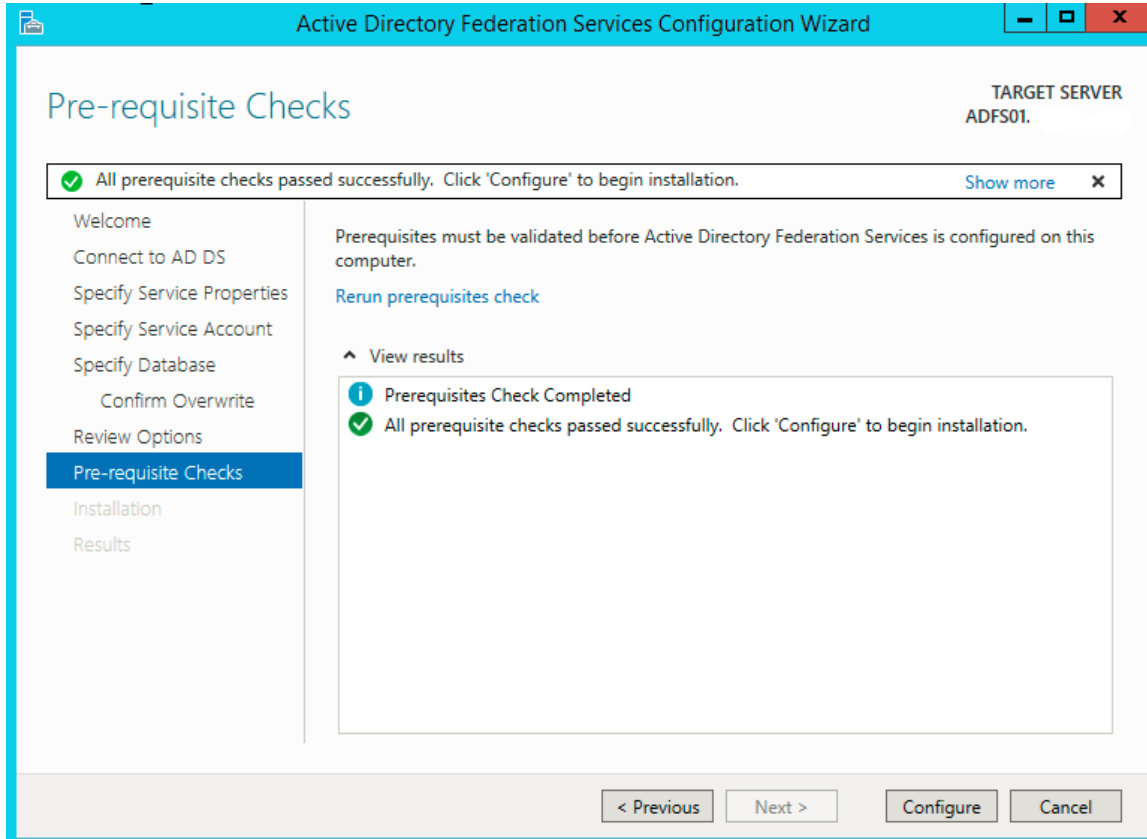


Figure 15. AD FS Configuration – Pre-requisite Check Page

» On the Results interface, click Close

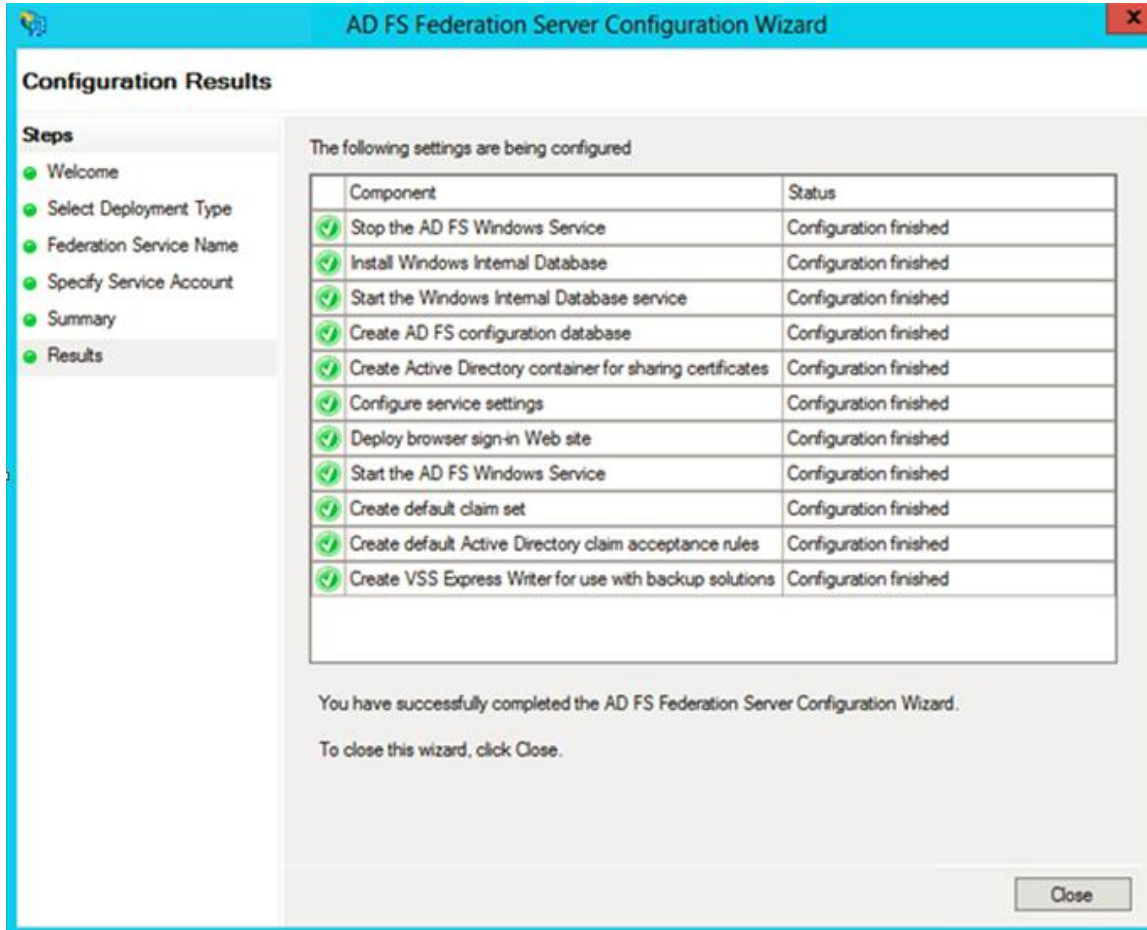


Figure 16. AD FS Configuration – Result Page

## 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.

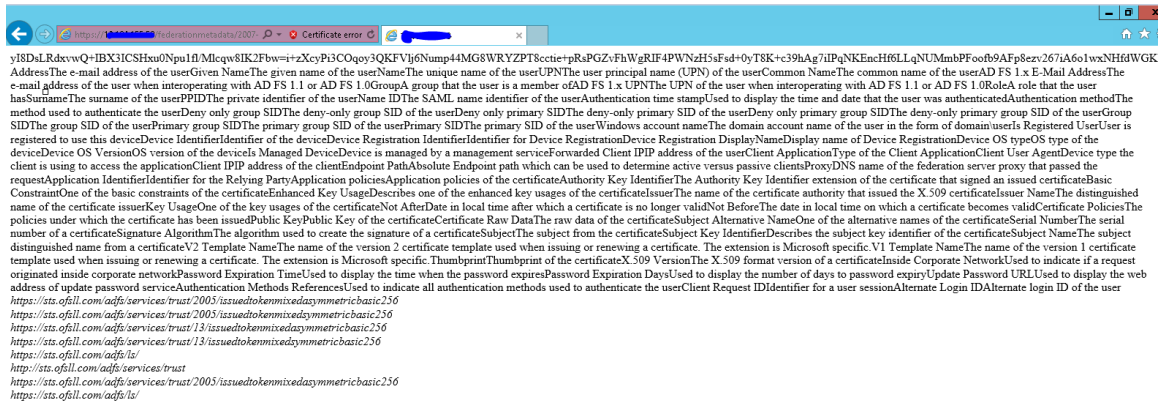


Figure 17. AD FS Configuration – Federation Metadata

All the pre-requisites are met for SAML 2.0 Web SSO Implementation on OFSLL Server. Ensure to download the above federationmetadata.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 federationmetadata.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.*

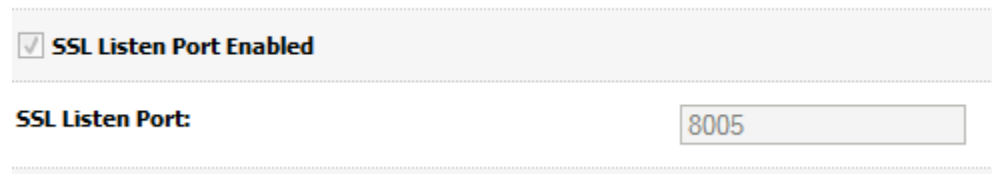


Figure 18. Weblogic Server – Enable SSL

## 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`

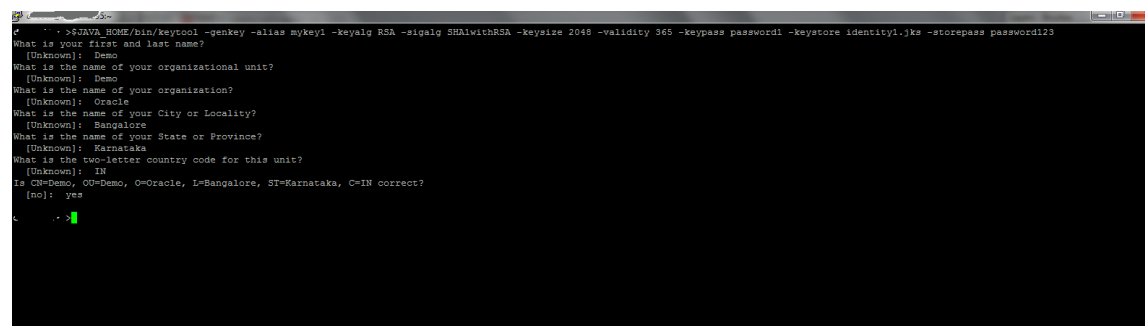


Figure 19. Weblogic Physical Server – Identity Generation

- » `$JAVA_HOME/bin/keytool -export -alias mykey -file root1.cer -keystore identity.jks -storepass password123`

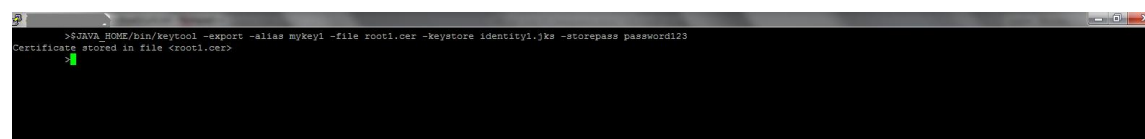
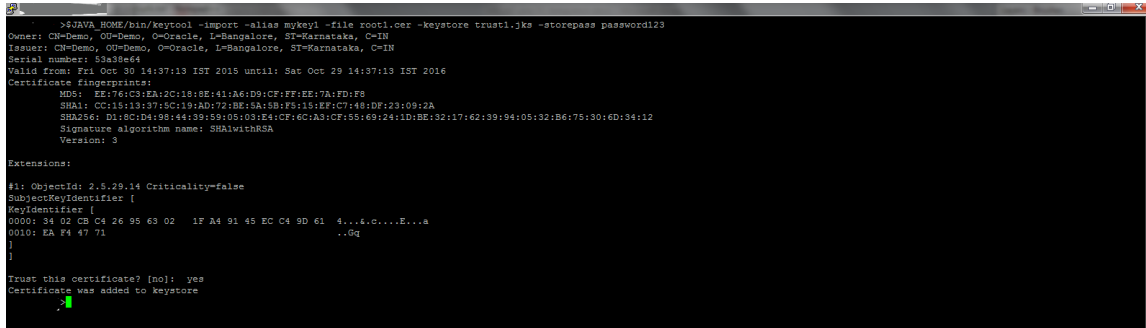


Figure 20. Weblogic Physical Server – Certificate Generation

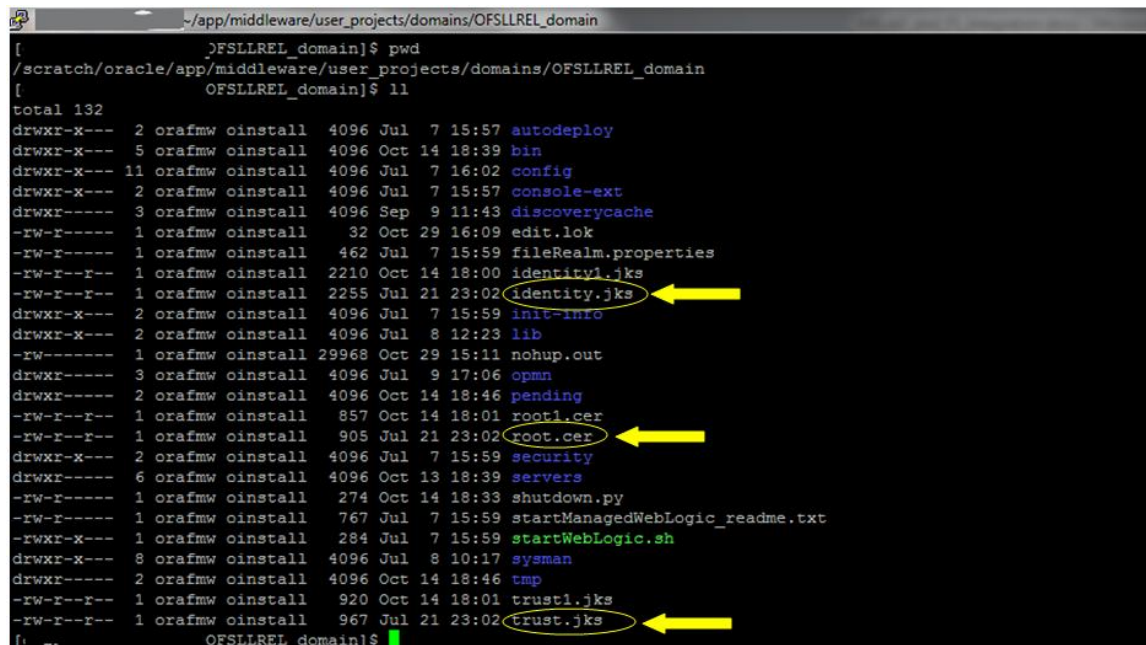
» \$JAVA\_HOME/bin/keytool -import -alias mykey -file root.cer -keystore trust.jks -storepass password123



```
>$JAVA_HOME/bin/keytool -import -alias mykey1 -file root1.cer -keystore trust1.jks -storepass password123
Owner: CN=Demo, OU=Demo, O=Oracle, L=Bangalore, ST=Karnataka, C=IN
Issuer: CN=Demo, OU=Demo, O=Oracle, L=Bangalore, ST=Karnataka, C=IN
Serial number: 34464
Valid from: Fri Oct 30 14:37:13 IST 2015 until: Sat Oct 29 14:37:13 IST 2016
Certificate fingerprints:
MD5: EF:76:03:2A:2C:19:8E:41:A4:D9:CF:FF:EE:7A:FD:FB
SHA1: CC:15:13:37:5C:19:AD:72:BE:5A:5B:15:8F:C7:48:DF:23:09:2A
SHA256: D1:8C:D4:98:44:39:59:05:03:E4:CF:6C:A3:CF:55:69:24:1D:BE:32:17:62:39:94:05:32:B6:75:30:6D:34:12
Signature algorithm name: SHA1withRSA
Version: 3
Extensions:
#1: ObjectID: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 34 02 03 04 26 95 63 02 1F A4 91 45 EC C4 9D 61 4...t.c....E...a
0010: EA F4 47 71 ..Gq
]
]
Trust this certificate? [no]: yes
Certificate was added to keystore
```

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.



```
~/app/middleware/user_projects/domains/OFSLLREL_domain
[ OFSLLREL_domain]$ pwd
/scratch/oracle/app/middleware/user_projects/domains/OFSLLREL_domain
[ OFSLLREL_domain]$ ll
total 132
drwxr-x--- 2 orafmw oinstall 4096 Jul  7 15:57 autodeploy
drwxr-x--- 5 orafmw oinstall 4096 Oct 14 18:39 bin
drwxr-x--- 11 orafmw oinstall 4096 Jul  7 16:02 config
drwxr-x--- 2 orafmw oinstall 4096 Jul  7 15:57 console-ext
drwxr----- 3 orafmw oinstall 4096 Sep  9 11:43 discoverycache
-rw-r----- 1 orafmw oinstall  32 Oct 29 16:09 edit.lock
-rw-r----- 1 orafmw oinstall  462 Jul  7 15:59 fileRealm.properties
-rw-r--r-- 1 orafmw oinstall 2210 Oct 14 18:00 identity1.jks
-rw-r--r-- 1 orafmw oinstall 2255 Jul 21 23:02 identity.jks
drwxr-x--- 2 orafmw oinstall 4096 Jul  7 15:59 init-info
drwxr-x--- 2 orafmw oinstall 4096 Jul  8 12:23 lib
-rw----- 1 orafmw oinstall 29968 Oct 29 15:11 nohup.out
drwxr----- 3 orafmw oinstall 4096 Jul  9 17:06 opmn
drwxr----- 2 orafmw oinstall 4096 Oct 14 18:46 pending
-rw-r--r-- 1 orafmw oinstall  857 Oct 14 18:01 root1.cer
-rw-r--r-- 1 orafmw oinstall  905 Jul 21 23:02 root.cer
drwxr-x--- 2 orafmw oinstall 4096 Jul  7 15:59 security
drwxr----- 6 orafmw oinstall 4096 Oct 13 18:39 servers
-rw-r----- 1 orafmw oinstall  274 Oct 14 18:33 shutdown.py
-rw-r----- 1 orafmw oinstall  767 Jul  7 15:59 startManagedWebLogic_readme.txt
-rwxr-x--- 1 orafmw oinstall  284 Jul  7 15:59 startWebLogic.sh
drwxr-x--- 8 orafmw oinstall 4096 Jul  8 10:17 sysman
drwxr----- 2 orafmw oinstall 4096 Oct 14 18:46 tmp
-rw-r--r-- 1 orafmw oinstall  920 Oct 14 18:01 trust1.jks
-rw-r--r-- 1 orafmw oinstall  967 Jul 21 23:02 trust.jks
[ OFSLLREL_domain]$
```

Figure 22. Weblogic Physical Server – Domain Location

## Steps to configure Custom Identity and Custom Trust

- » Login to Weblogic Admin console --> Environment --> Servers --> ofssl\_managedserver2 --> Configuration -> Keystores
- » Click on "Change" button next to Keystores

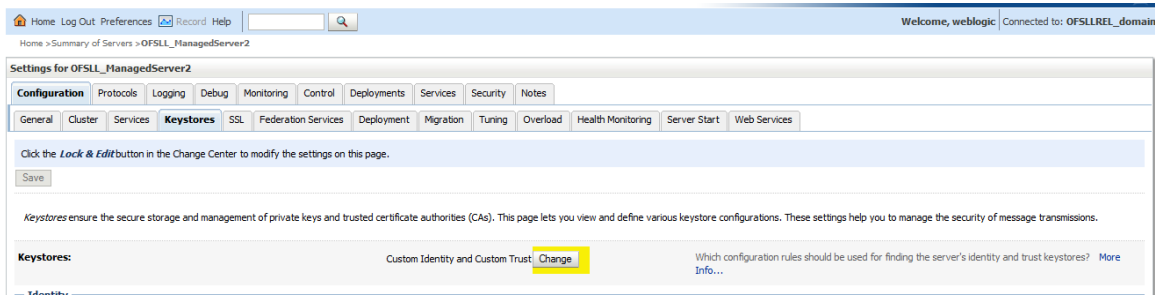


Figure 23. Weblogic Server – Keystore Location

- » 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

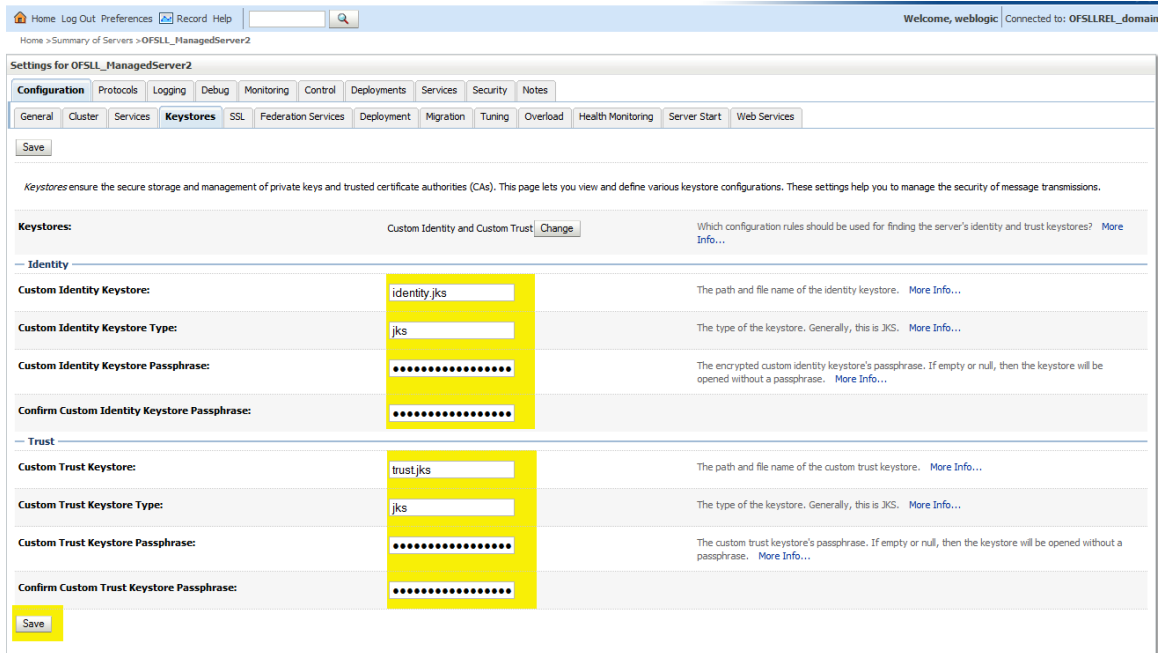


Figure 24. Weblogic Server – Keystore Settings

» 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

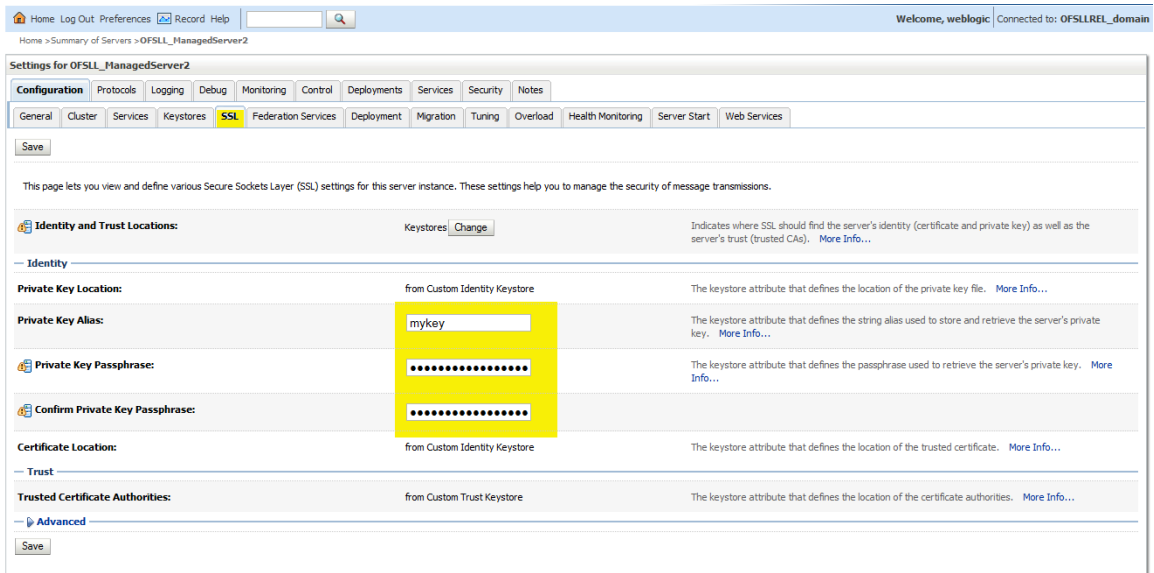


Figure 25. Weblogic Server – SSL Settings

- » 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

The screenshot shows the 'Settings for OFSSL\_ManagedServer2' page in the Weblogic Administration Console. The 'SSL' tab is selected, and the 'Advanced' section is expanded. The 'Hostname Verification' dropdown menu is highlighted in yellow and set to 'None'. The 'Use JSSE SSL' checkbox is also checked and highlighted in yellow. Other settings include 'Private Key Location' (from Custom Identity Keystore), 'Private Key Alias' (mykey), 'Private Key Passphrase', 'Certificate Location' (from Custom Identity Keystore), 'Trusted Certificate Authorities' (from Custom Trust Keystore), 'Custom Hostname Verifier', 'Export Key Lifespan' (500), 'Use Server Certs', 'Two Way Client Cert Behavior' (Client Certs Not Requested), 'Cert Authenticator', 'SSLRejection Logging Enabled', 'Allow Unencrypted Null Cipher', 'Inbound Certificate Validation' (Builtin SSL Validation Only), and 'Outbound Certificate Validation' (Builtin SSL Validation Only). A 'Save' button is located at the bottom left of the settings area.

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

Home Log Out Preferences Record Help

Home > Summary of Security Realms > myrealm > Providers > SAMLIdentityAssert > Providers

### Create a New Authentication Provider

OK Cancel

#### Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.

\* Indicates required fields

The name of the authentication provider.

\* **Name:**

This is the type of authentication provider you wish to create.

**Type:**

OK Cancel

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.

Authentication Providers

New Delete Reorder

Showing 1 to 4 of 4 Previous | Next

Name	Description	Version
SAMLIdentityAssert	SAML 2.0 Identity Assertion Provider. Supports Security Assertion Markup Language v2.0.	1.0

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 ofssl\_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>/ofssl142/faces/pages/OfsslHome.jspx> ; for example <https://ofssl.oracle.com:9704/ofssl142/faces/pages/OfsslHome.jspx>
- » Save and Activate Changes

Administration Console

Home Log Out Preferences Record Help Welcome, weblogic Connected to: OFSLLREL\_domain

Home > Summary of Servers > OFSLL\_ManagedServer2

Settings for OFSLL\_ManagedServer2

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload Health Monitoring Server Start Web Services

SAML 1.1 Source Site SAML 1.1 Destination Site SAML 2.0 General SAML 2.0 Identity Provider SAML 2.0 Service Provider

Click the **Lock & Edit** button in the Change Center to modify the settings on this page.

Save

This page configures the SAML 2.0 per server service provider properties

<input checked="" type="checkbox"/> Enabled	Specifies whether the local site is enabled for the Service Provider role. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> Always Sign Authentication Requests	Specifies whether authentication requests must be signed. If set, all outgoing authentication requests are signed. <a href="#">More Info...</a>
<input type="checkbox"/> Force Authentication	Specifies whether the Identity Provider must authenticate users directly and not use a previous security context. The default is false. <a href="#">More Info...</a>
<input type="checkbox"/> Passive	Determines whether the Identity Provider and the user must not take control of the user interface from the requester and interact with the user in a noticeable fashion. The default setting is false. <a href="#">More Info...</a>
<input type="checkbox"/> Only Accept Signed Assertions	Specifies whether incoming SAML 2.0 assertions must be signed. <a href="#">More Info...</a>
Authentication Request Cache Size:	10000 The maximum size of the authentication request cache. <a href="#">More Info...</a>
Authentication Request Cache Timeout:	300 The maximum timeout (in seconds) of <AuthRequest> documents stored in the local cache. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> POST One Use Check Enabled	Specifies whether the POST one-use check is enabled. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> POST Binding Enabled	Specifies whether the POST binding is enabled for the Service Provider. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> Artifact Binding Enabled	Specifies whether the Artifact binding is enabled for the Service Provider. <a href="#">More Info...</a>
Preferred Binding:	POST Specifies the preferred binding type for endpoints of Service Provider services. Must be set to "None", "POST", or "Artifact". <a href="#">More Info...</a>
Default URL:	https://c...:8005/ofssl142/faces/ The Service Provider's default URL. <a href="#">More Info...</a>


Save

Click the **Lock & Edit** button in the Change Center to modify the settings on this page.

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 → ofssl\_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://ofssl.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

Administration Console

Home Log Out Preferences Record Help Welcome, weblogic Connected to: OFSSLREL\_domain

Home > Summary of Servers > OFSSL\_ManagedServer2

Settings for OFSSL\_ManagedServer2

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL **Federation Services** Deployment Migration Tuning Overload Health Monitoring Server Start Web Services

SAML 1.1 Source Site SAML 1.1 Destination Site **SAML 2.0 General** SAML 2.0 Identity Provider SAML 2.0 Service Provider

Save Publish Meta Data

Click the **Lock & Edit** button in the Change Center to modify the settings on this page.

This page configures the general SAML 2.0 per server properties

— General

**Replicated Cache Enabled** Specifies whether the persistent cache (LDAP or RDBMS) is used for storing SAML 2.0 artifacts and authentication requests. [More Info...](#)

— Site Info

**Contact Person Given Name:**  The contact person given (first) name. [More Info...](#)

**Contact Person Surname:**  The contact person surname (last name). [More Info...](#)

**Contact Person Type:** administrative The contact person type. [More Info...](#)

**Contact Person Company:** Oracle The contact person's company name. [More Info...](#)

**Contact Person Telephone Number:** 1234567890 The contact person's telephone number. [More Info...](#)

**Contact Person Email Address:**  The contact person's e-mail address. [More Info...](#)

**Organization Name:** Oracle The organization name. [More Info...](#)

**Organization URL:** http://www.oracle.com/ The organization URL. [More Info...](#)

**Published Site URL:** http://c .....:8003/saml2 The published site URL. [More Info...](#)

**Entity ID:** sso\_domain The string that uniquely identifies the local site. [More Info...](#)

— Bindings

**Recipient Check Enabled** Specifies whether the recipient/destination check is enabled. When true, the recipient of the SAML Request/Response must match the URL in the HTTP Request. [More Info...](#)

**Transport Layer Client Authentication Enabled** Specifies whether TLS/SSL client authentication is required. [More Info...](#)

**Transport Layer Security Key Alias:**  The string alias used to store and retrieve the server's private key, which is used to establish outgoing TLS/SSL connections. [More Info...](#)

**Transport Layer Security Key Passphrase:**  The passphrase used to retrieve the server's private key from the keystore. [More Info...](#)

**Confirm Transport Layer Security Key Passphrase:**

**Basic Client Authentication Enabled** Specifies whether Basic Authentication client authentication is required. [More Info...](#)

**Basic Authentication User Name:**  The username that is used to assign Basic authentication credentials to outgoing HTTPS connections. [More Info...](#)

**Basic Authentication Password:**  The password used to assign Basic Authentication credentials to outgoing HTTPS connections. [More Info...](#)

**Confirm Basic Authentication Password:**

— Artifact Resolution Service

**Only Accept Signed Artifact Requests** Specifies whether incoming artifact requests must be signed. [More Info...](#)

**Artifact Cache Size:** 10000 The maximum size of the artifact cache. [More Info...](#)

**Artifact Cache Timeout:** 300 The maximum timeout (in seconds) of artifacts stored in the local cache. [More Info...](#)

— Single Sign-on

**Single Sign-on Signing Key Alias:** mykey The keystore alias for the key to be used when signing documents. [More Info...](#)

**Single Sign-on Signing Key Pass Phrase:** ..... The passphrase used to retrieve the local site's SSO signing key from the keystore. [More Info...](#)

**Confirm Single Sign-on Signing Key Pass Phrase:** .....

Save Publish Meta Data

Click the **Lock & Edit** button in the Change Center to modify the settings on this page.

Figure 30. Weblogic Server – SAML2.0 General

- » Go to Environment → Servers → ofsl\_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 ofsl\_metadata.xml in this case.

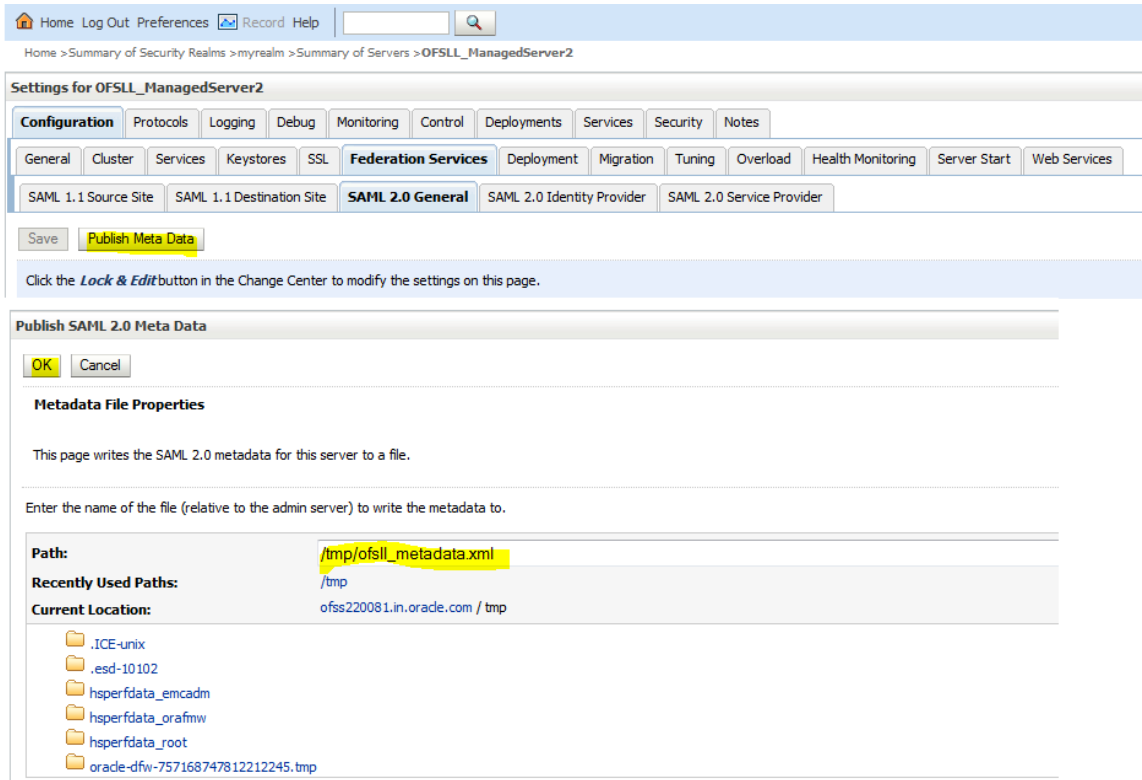


Figure 31. Weblogic Server – Publish Meta Data





» 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.*

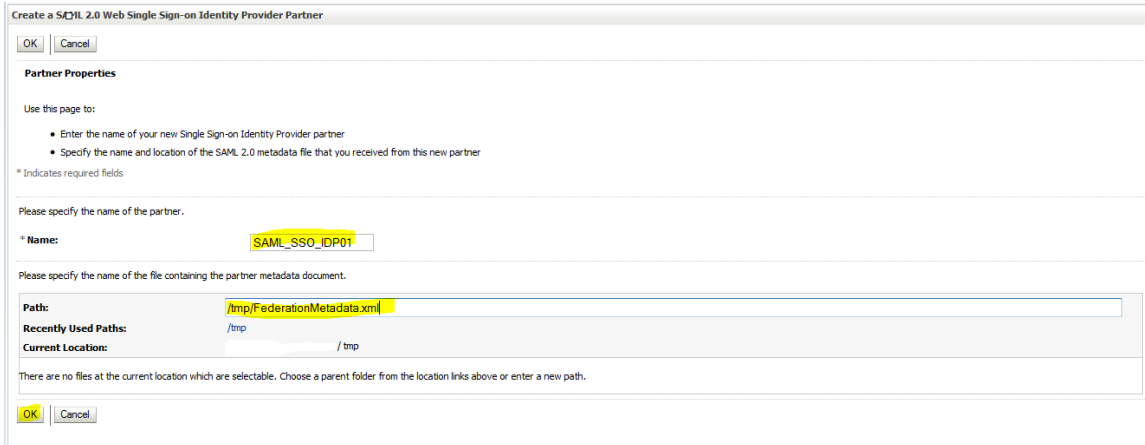


Figure 34. Weblogic Domain – Identity Provider

### 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...>

```

<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://.../adfs/services/trust/ID=..._8094bcef-04d8-4b58-9573-d23dda9907fc">
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <X509Data>
        <X509Certificate>MIIC3DCCAcSgAwIBAgIQdZ08LrW41DNB+kxeOFGHhTANBgkqhkiG9w0BAQsFADAQMSgwJgYDVQQDEEx9BREZTIEVudY353cHRpb24gLSBzdBHMub2Z2bGwuY291MB4XDTE1MDcyMTY...
      </X509Data>
    </KeyInfo>
    <KeyDescriptor>
      <KeyDescriptor use="siging">
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <X509Data>
            <X509Certificate>MIIC1JCCAbGwAwIBAgIQYdaJ001qR6JAKPxyj8VkjANBgkqhkiG9w0BAQsFADANMSUwIwYDVQQDEEx9BREZTIEVudY353cHRpb24gLSBzdBHMub2Z2bGwuY291MB4XDTE1MDcyMTY...
          </X509Data>
        </KeyInfo>
      </KeyDescriptor>
    <SingleLogoutService Location="https://.../adfs/ls/" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
    <NameIDFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress" NameIDFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" NameIDFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameIDFormat="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
    <SingleSignOnService Location="https://.../adfs/ls/" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
    <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="E-Mail Address" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"/>
    <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="Given Name" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"/>
    <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="Name" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"/>
    <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="UPN" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"/>
    <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="Common Name" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="http://schemas.xmlsoap.org/claims/CommonName"/>
    <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="AD FS 1.x E-Mail Address" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="http://schemas.xmlsoap.org/claims/EmailAddress"/>
    <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="Group" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="http://schemas.xmlsoap.org/claims/Group"/>
    <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="AD FS 1.x UPN" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="http://schemas.xmlsoap.org/claims/UPN"/>
    <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="Role" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="http://schemas.microsoft.com/ws/2008/06/identity/claims/role"/>
    <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="Surname" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname"/>
    <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="PPID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonidentifier"/>
    <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="Name ID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameid"/>
  </IDPSSODescriptor>
</EntityDescriptor>

```

Figure 35. Modified Federation Metadata

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

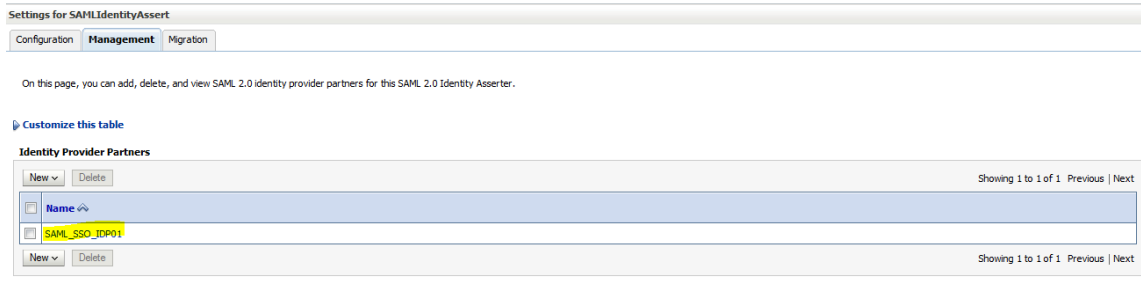


Figure 36. Weblogic Domain – Identity Provider

- » 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 → /ofs1142/faces/\*

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

- » Only Accept Signed Artifact Requests → Checked
- » Save

Administration Console

Home Log Out Preferences Record Help Welcome, weblogic Connected to: OFSLLREI\_domain

Home > Summary of Security Realms > myrealm > Providers > SAMLIdentityAssert > SAML\_SSO\_IDP01

### Settings for SAMLIdentityAssert

General Site Info Single Sign-On Signing Certificate Transport Layer Client Certificate Single Sign-On Service Endpoints Artifact Resolution Service Endpoints

Save

Configures a SAML 2.0 Web Single Sign-on Identity Provider Partner's General Properties

The parameters that can be set on this Administration Console page can also be accessed programmatically via the Java interfaces that are identified in this help topic. For API information about those interfaces, see Related Topics.

Overview

**Name:** SAML\_SSO\_IDP01 The name of this Identity Provider partner. [More Info...](#)

**Enabled** Specifies whether interactions with this Identity Provider partner are enabled on this server. [More Info...](#)

**Description:** SAML\_SSO\_IDP01 A short description of this Identity Provider partner. [More Info...](#)

Authentication Requests

**Identity Provider Name Mapper Class Name:** The Java class that overrides the default username mapper class with which the SAML 2.0 Identity Asserter provider is configured in this security realm. [More Info...](#)

**Issuer URI:** http://sts.ofsll.com/adfs/services/trust The Issuer URI of this Identity Provider partner. [More Info...](#)

**Virtual User** Specifies whether user information contained in assertions received from this Identity Provider partner are mapped to virtual users in this security realm. [More Info...](#)

**Redirect URIs:** An optional set of URIs from which unauthenticated users will be redirected to the Identity Provider partner. [More Info...](#)

/ofs1142/faces/\*  
/FCJNeoWebUI/\*

**Process Attributes** Specifies whether the SAML 2.0 Identity Asserter provider consumes attribute statements contained in assertions received from this Identity Provider partner. [More Info...](#)

Signing

**Only Accept Signed Authentication Requests:** false Specifies whether authentication requests sent to this Identity Provider partner must be signed. [More Info...](#)

**Only Accept Signed Artifact Requests** Specifies whether SAML artifact requests received from this Identity Provider partner must be signed. [More Info...](#)

Transport

**Send Artifact via POST** Specifies whether SAML artifacts are delivered to this Identity Provider partner via the HTTP POST method. [More Info...](#)

**Artifact Binding POST Form:** The URL of the custom web application that generates the POST form for carrying the SAML response for Artifact bindings to this Identity Provider partner. Details about the required fields in this custom application are available in the OASIS SAML 2.0 specifications. [More Info...](#)

**POST Binding POST Form:** The URL of the custom web application that generates the POST form for carrying the SAML response for POST bindings to this Identity Provider partner. [More Info...](#)

**Client User Name:** The user name that must be specified in the basic authentication header that is expected from this Identity Provider partner when the partner connects to the local site's SOAP/HTTPS binding. [More Info...](#)

**Client Password:** The password of the client user name. [More Info...](#)

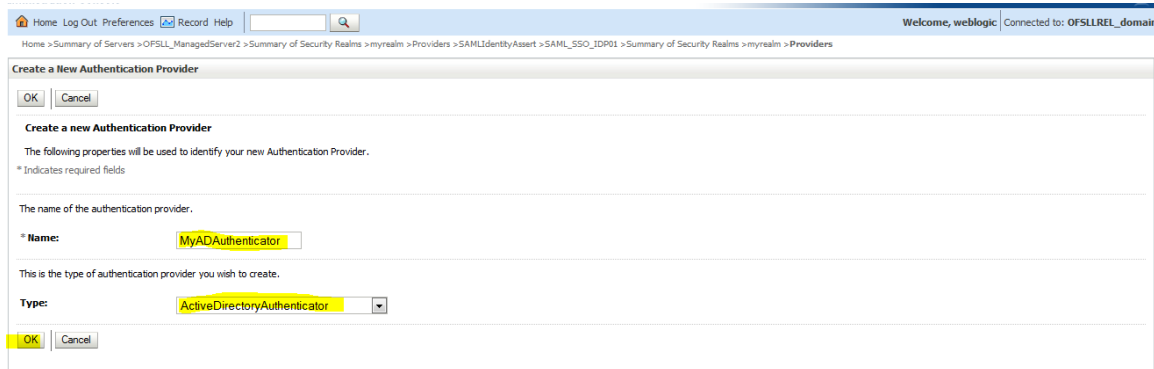
**Confirm Client Password:**

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 ActiveDirectoryAuthentication



The screenshot shows the 'Create a New Authentication Provider' dialog box in the Weblogic Admin console. The dialog has a title bar with 'OK' and 'Cancel' buttons. Below the title bar, there is a section titled 'Create a new Authentication Provider' with a sub-header 'The following properties will be used to identify your new Authentication Provider.' and a note '\* Indicates required fields'. The 'Name' field is labeled 'The name of the authentication provider.' and contains the text 'MyADAuthenticator'. The 'Type' field is labeled 'This is the type of authentication provider you wish to create.' and is a dropdown menu with 'ActiveDirectoryAuthenticator' selected. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

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=adminimator, 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 DN's from Member DN Filter → (&(member=%M)(objectclass=group))
- » GUID Attribute → objectguid

» Restart servers, first admin server, then Managed Server

The screenshot displays the 'Settings for MyADAuthenticator' configuration page. The 'Provider Specific' tab is active. The configuration is organized into several sections:

- Connection:**
  - Host:** [Empty]
  - Port:** 389
  - Principal:** CN=I CN=Users
  - Credential:** [Masked]
  - Confirm Credential:** [Masked]
  - SSL Enabled**
- Users:**
  - User Base DN:** OU=MyOrg,DC=ofsl,DC
  - All Users Filter:** (&(sAMAccountName=
  - User From Name Filter:** (&(sAMAccountName=
  - User Search Scope:** subtree
  - User Name Attribute:** sAMAccountName
  - User Object Class:** user
  - Use Retrieved User Name as Principal**
- Groups:**
  - Group Base DN:** OU=MyOrg,DC=ofsl,DC
  - All Groups Filter:** (&(cn=\*)(objectclass=g
  - Group From Name Filter:** (&(cn=%g)(objectclass=
  - Group Search Scope:** subtree
  - Group Membership Searching:** unlimited
  - Max Group Membership Search Level:** 0
  - Ignore Duplicate Membership**
  - Use Token Groups For Group Membership Lookup**
- Static Groups:**
  - Static Group Name Attribute:** cn
  - Static Group Object Class:** group
  - Static Member DN Attribute:** member
  - Static Group DN's from Member DN Filter:** (&(member=%M)(objec
- Dynamic Groups:**
  - Dynamic Group Name Attribute:** [Empty]
  - Dynamic Group Object Class:** [Empty]
  - Dynamic Member URL Attribute:** [Empty]
  - User Dynamic Group DN Attribute:** [Empty]
- General:**
  - Connection Pool Size:** 6
  - Connect Timeout:** 0
  - Connection Retry Limit:** 1
  - Parallel Connect Delay:** 0
  - Results Time Limit:** 0
  - Keep Alive Enabled**
  - Follow Referrals**
  - Bind Anonymously On Referrals**
  - Propagate Cause For Login Exception**
  - Cache Enabled**
  - Cache Size:** 32
  - Cache TTL:** 60
  - GUID Attribute:** objectguid

At the bottom, there is a 'Save' button and a note: 'Click the Lock & Edit button in the Change Center to modify the settings on this page.'

Figure 39. Weblogic Domain –Provider Specific Details

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

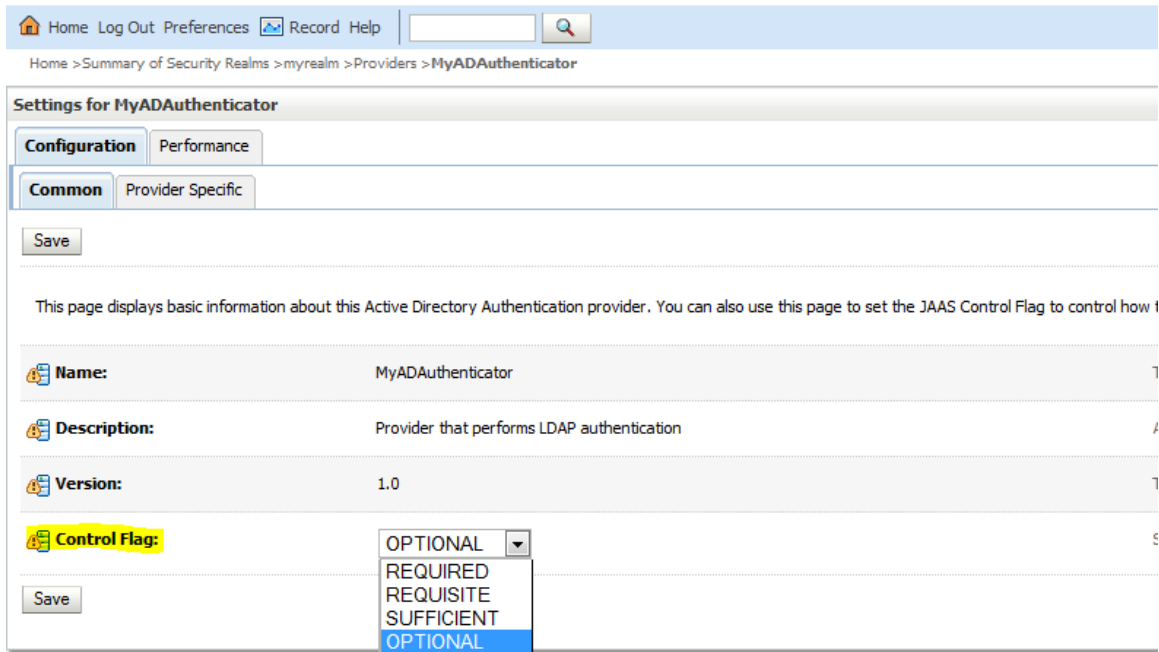


Figure 40. Weblogic Domain –Provider Specific Details

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

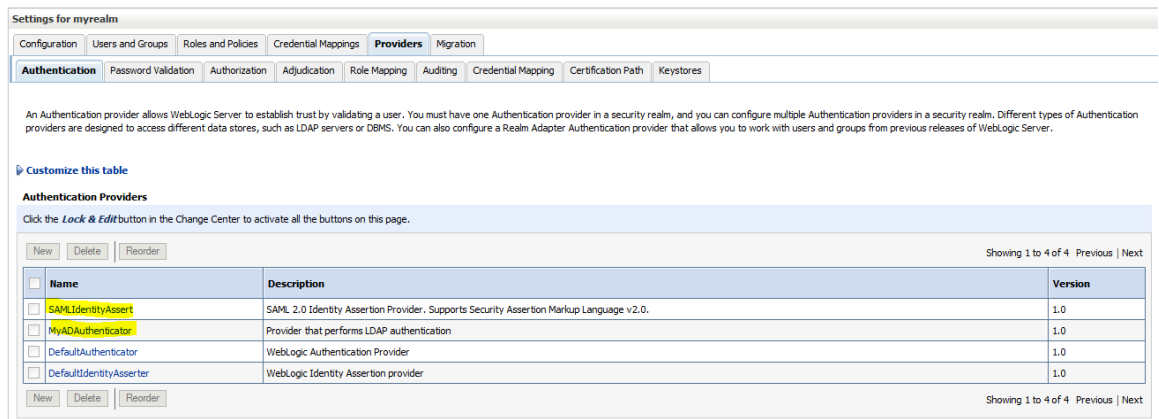


Figure 41. Weblogic Domain –Authentication Provider Order

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

FTP the ofssl\_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

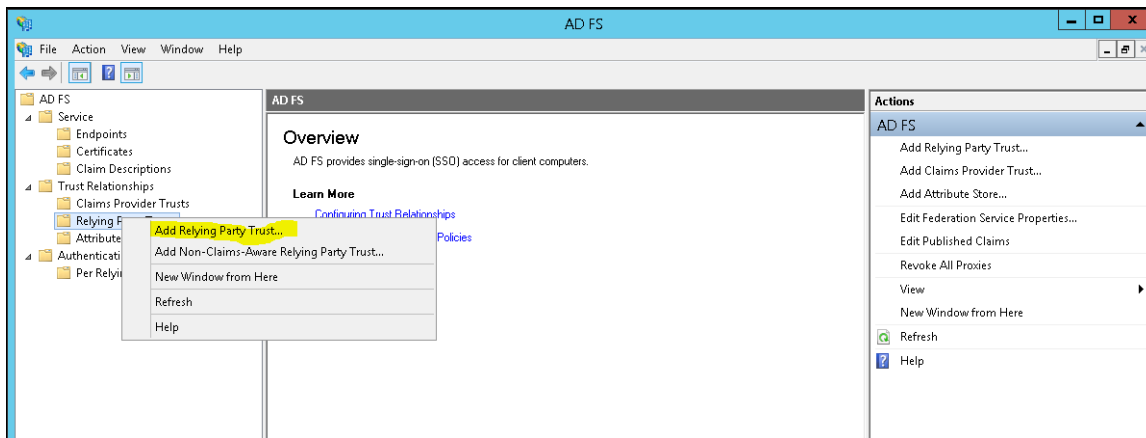


Figure 42. AD FS Server – Relying Party Trust



» Click start on the Welcome Page

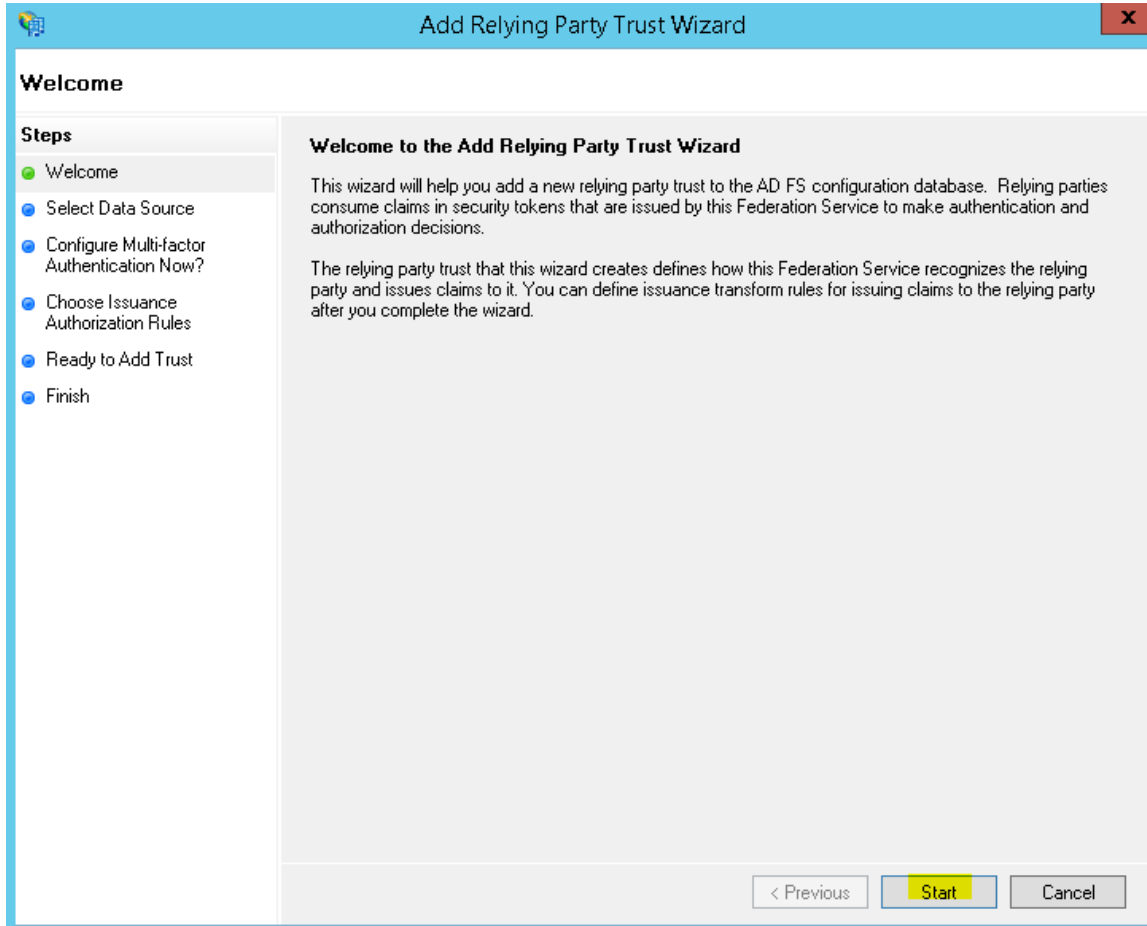


Figure 43. AD FS Server – Welcome Page

- » 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, ofssl\_metadata.xml

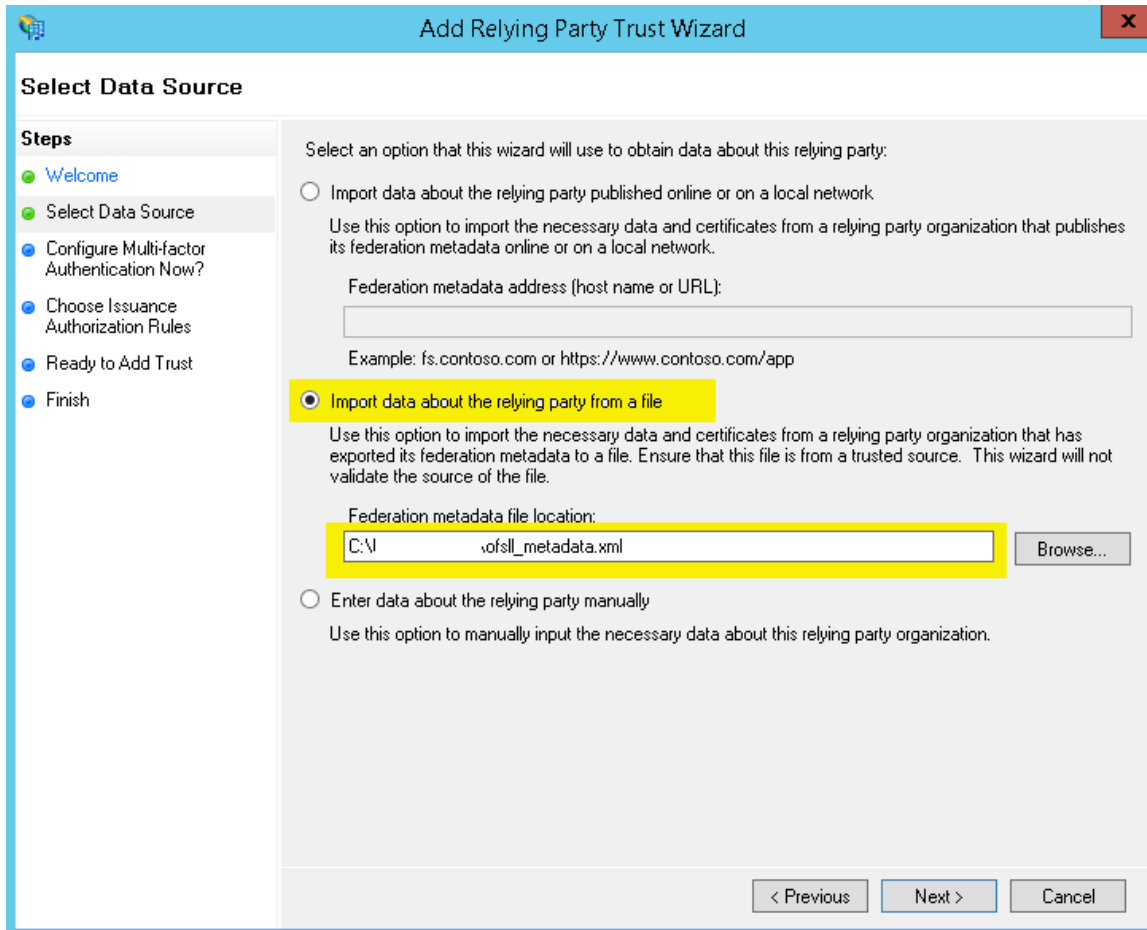


Figure 44. AD FS Server – Define the metadata source

- » Click "Ok" on below message

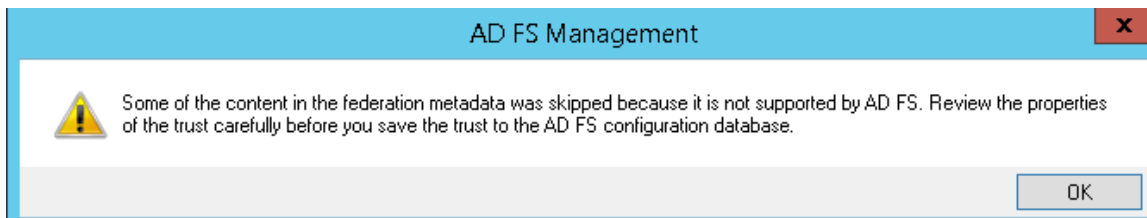


Figure 45. AD FS Server – Warning Message

» Provide an unique Display Name and click Next

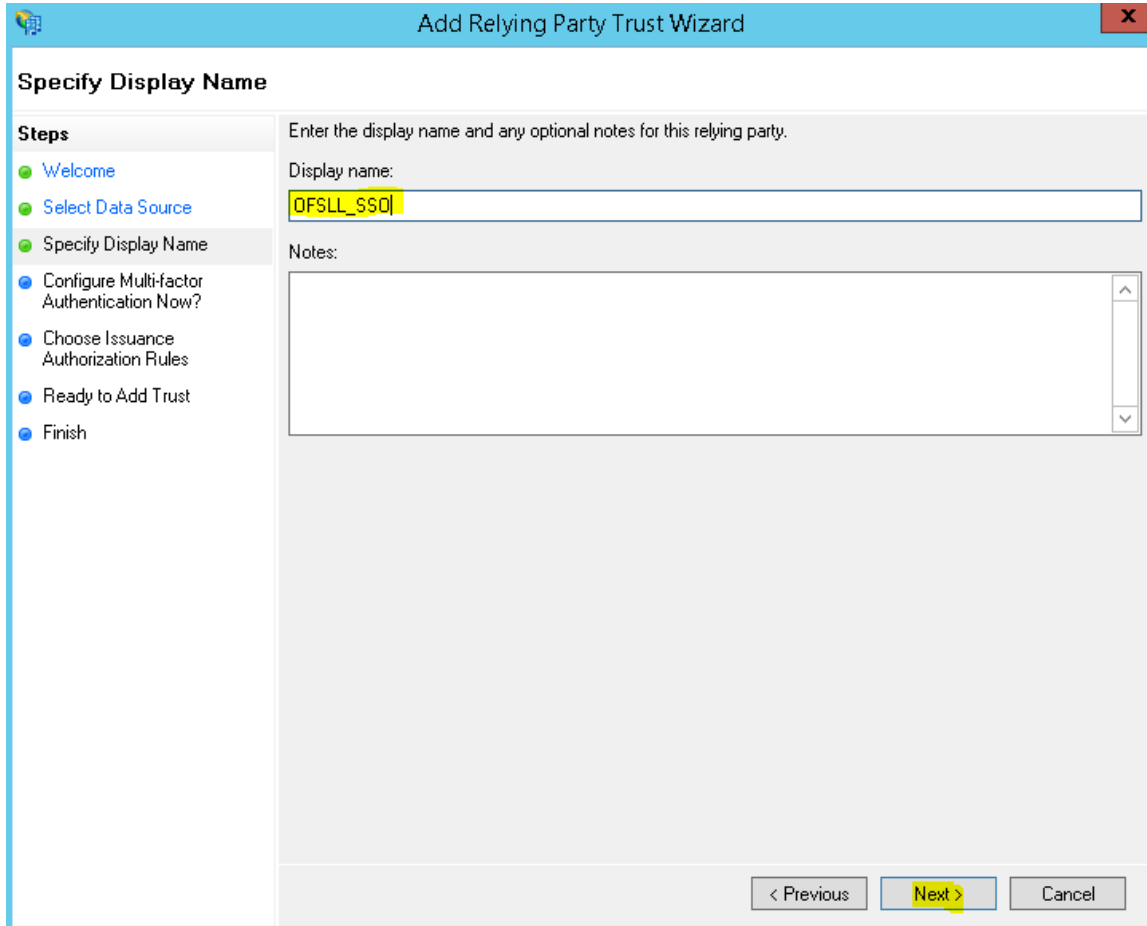


Figure 46. AD FS Server – Relying Party Display Name

» Retain the default as shown below and continue Next

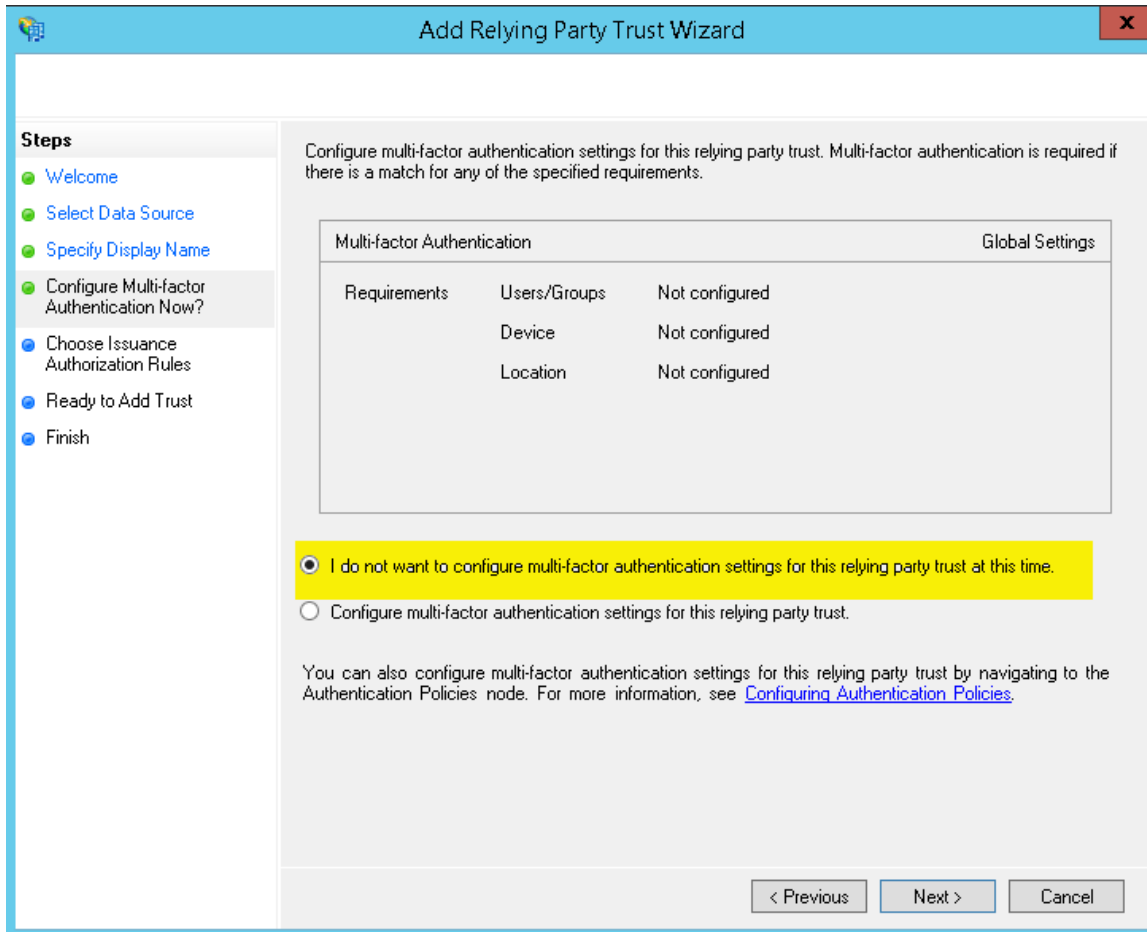


Figure 47. AD FS Server – Multi-factor Authentication

» Retain the default as shown below and continue Next

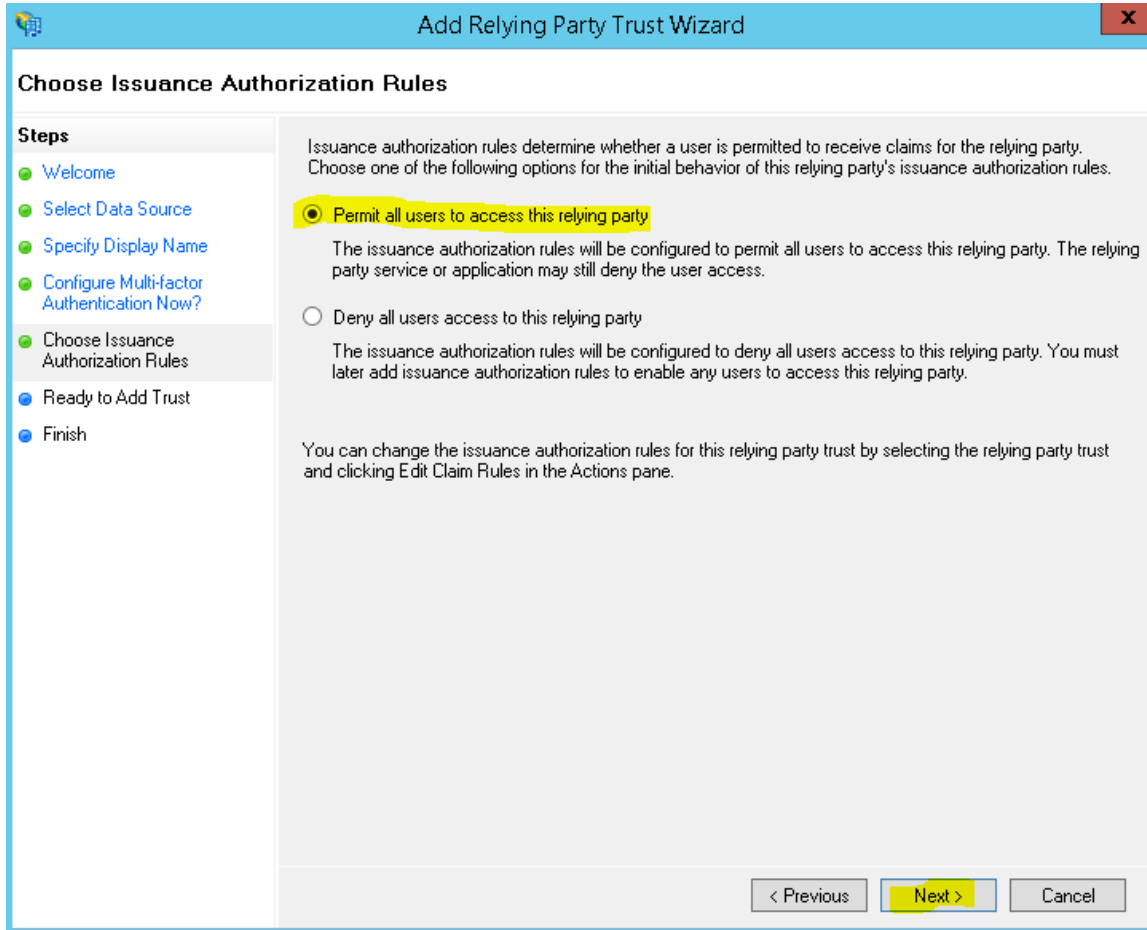


Figure 48. AD FS Server – Authorization Rules

- » Next screen verify the following Tabs
  - » Identifiers Tab – ensure the “relying party identifiers” are showing the values correctly

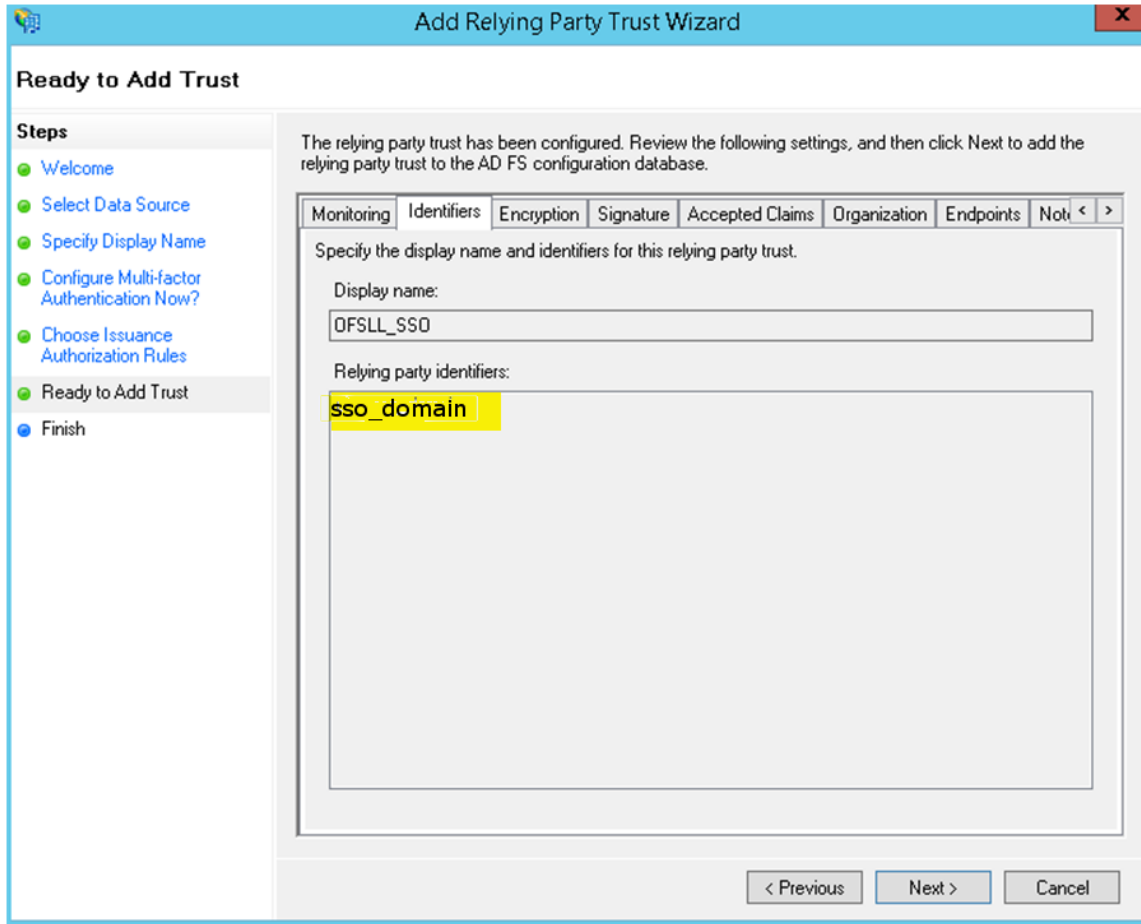


Figure 49. AD FS Server – Identifiers Tab

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

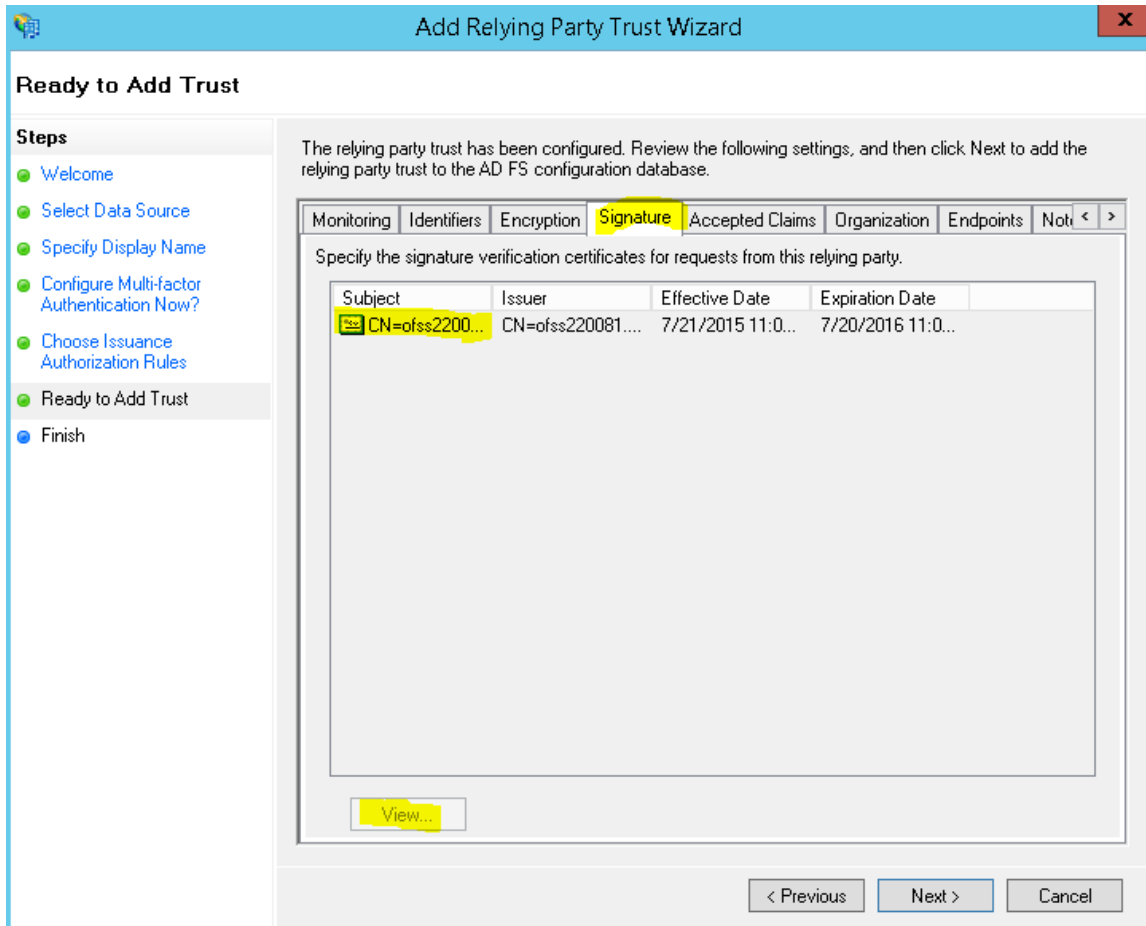


Figure 50. AD FS Server – Signature Tab

» Certificate details can be reviewed

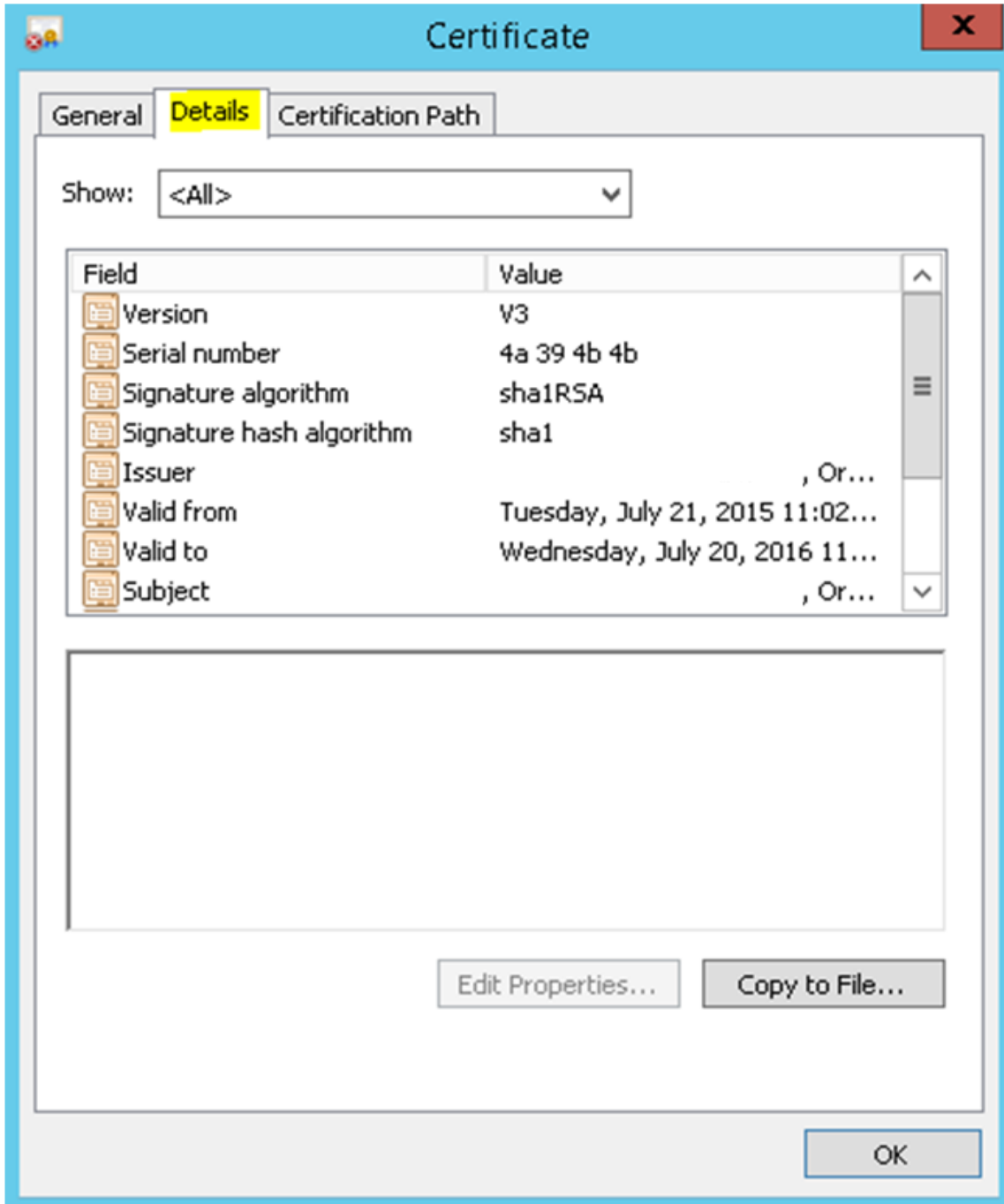


Figure 51. AD FS Server – Certificate Details

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



## Editing the Relying Party Trusts

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

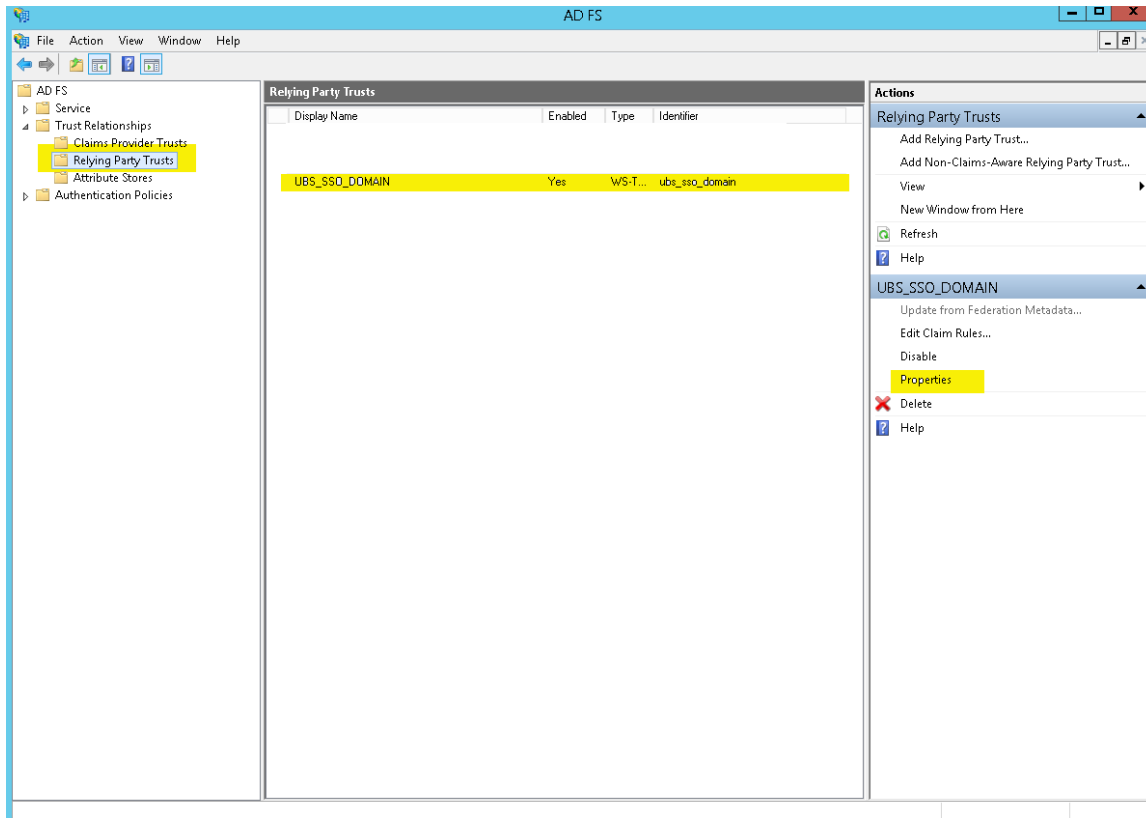


Figure 52. AD FS Server – Edit Relying Party Trust

- » 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*

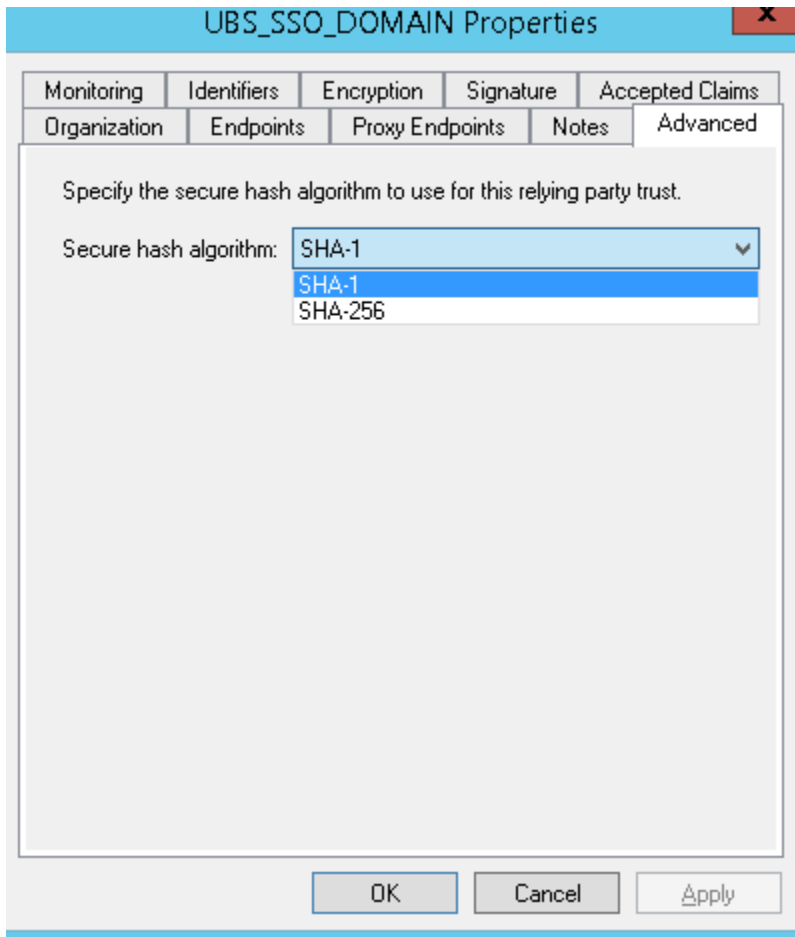


Figure 53. AD FS Relying Party – Advanced Tab

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

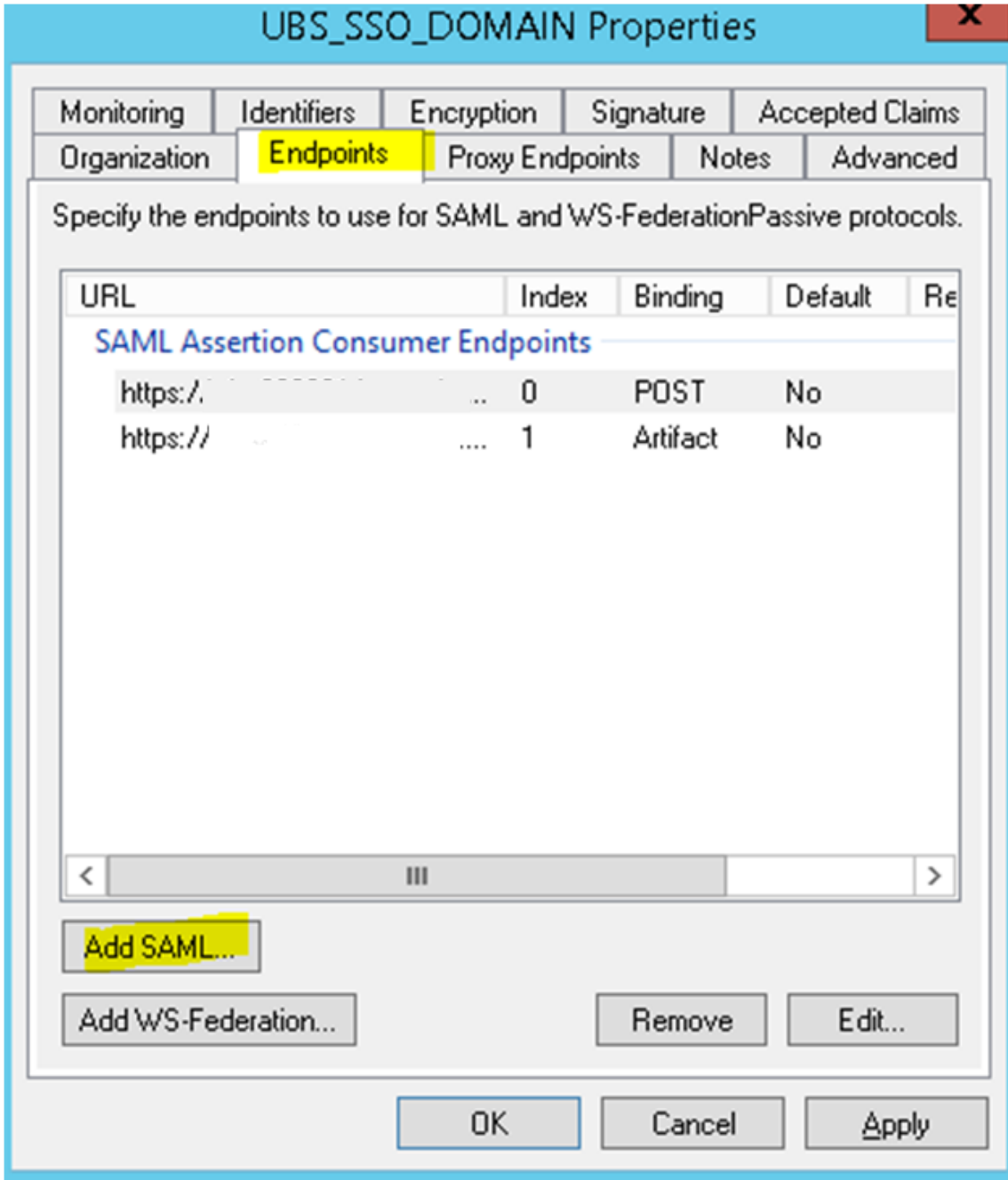


Figure 54. AD FS Relying Party – Endpoints Tab

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

The screenshot shows the 'Edit Endpoint' dialog box with the following configuration:

- Endpoint type: SAML Assertion Consumer
- Binding: POST
- Set the trusted URL as default:
- Index: 0
- Trusted URL: https://t:8005/saml2/sp/acs/post
- Example: https://sts.contoso.com/adfs/ls
- Response URL: (empty)
- Example: https://sts.contoso.com/logout

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://ofssl.oracle.com:9704/saml2/sp/acs/artifacts>
- » Click Ok

The screenshot shows the 'Edit Endpoint' dialog box with the following configuration:

- Endpoint type: SAML Assertion Consumer
- Binding: Artifact
- Set the trusted URL as default:
- Index: 1
- Trusted URL: https:// :8005/saml2/sp/acs/artifacts
- Example: https://sts.contoso.com/adfs/ls
- Response URL: (empty)
- Example: https://sts.contoso.com/logout

Figure 56. AD FS Relying Party – Add Endpoint

## Adding Rules

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

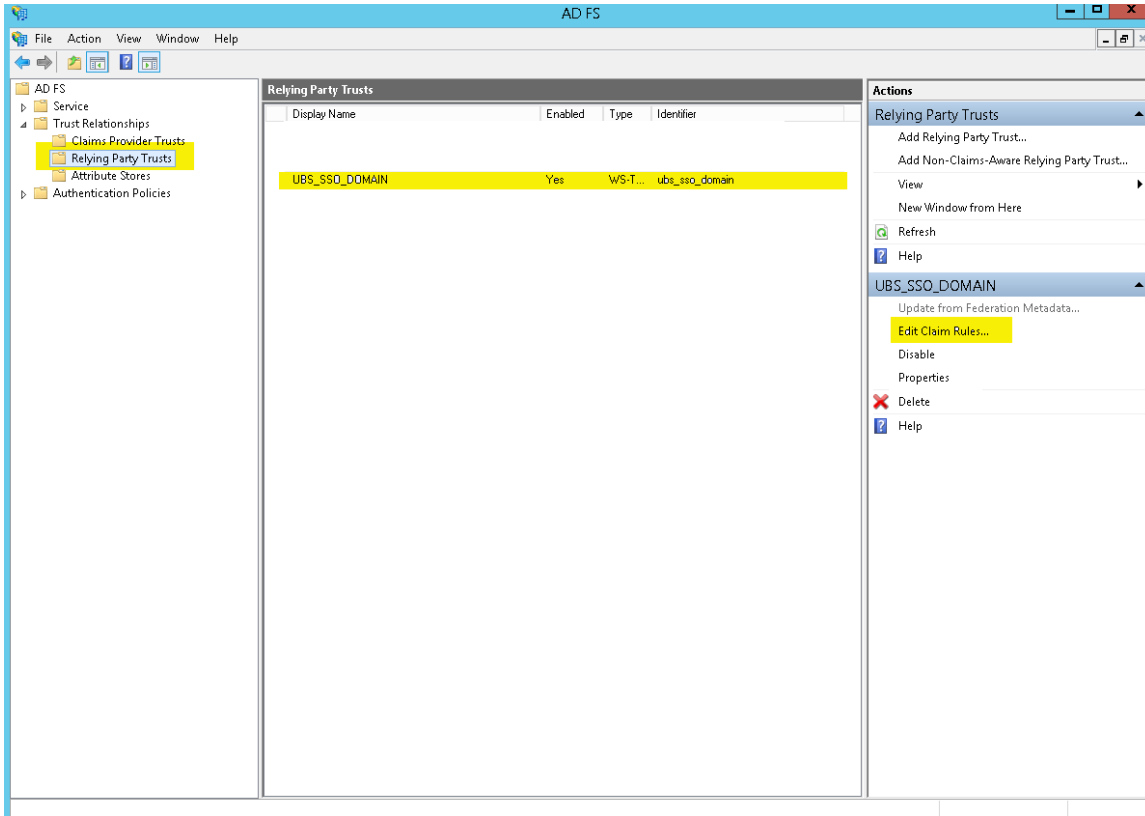


Figure 57. AD FS Relying Party – Edit Claims

» On "Issuance Transform Rules" tab, click on "Add Rule"

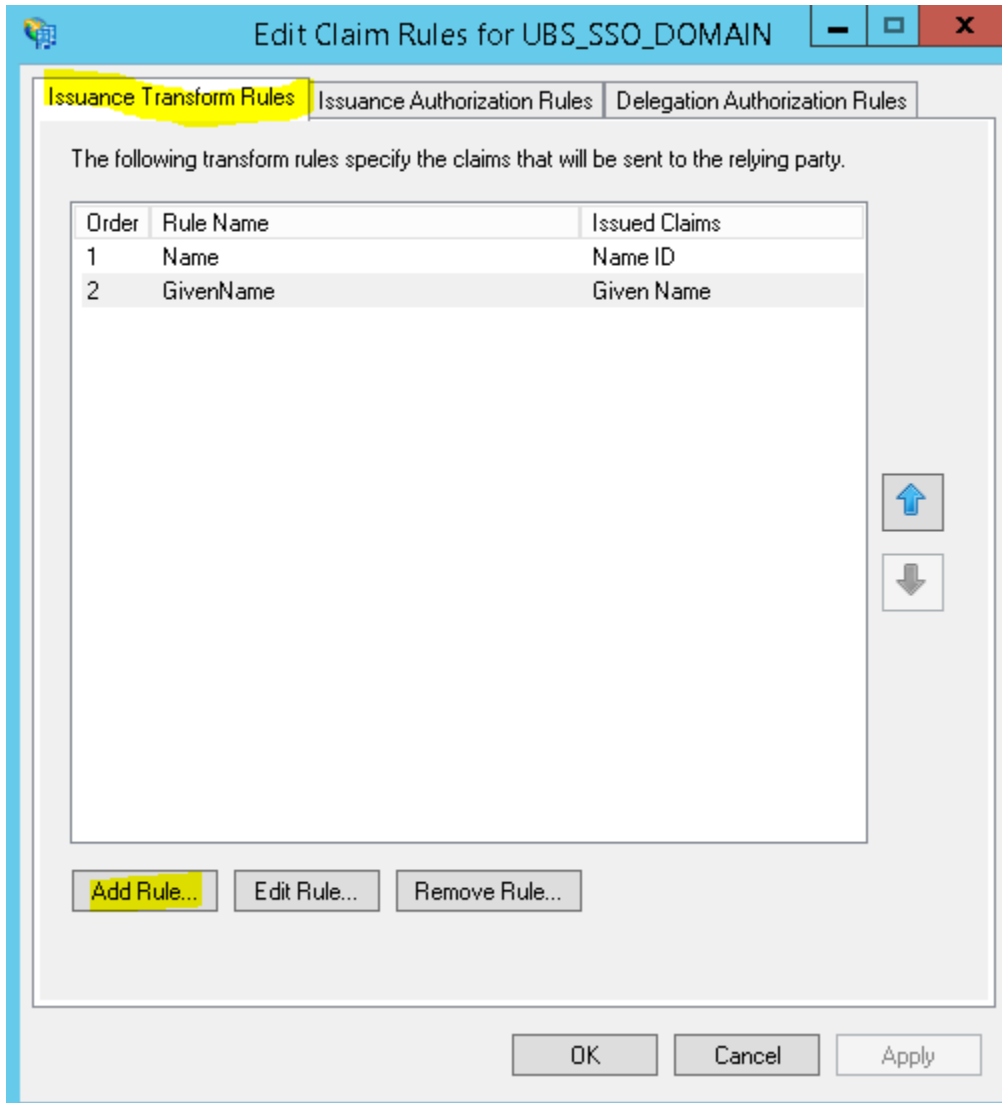


Figure 58. AD FS Relying Party – Add Rules

» Click on Next

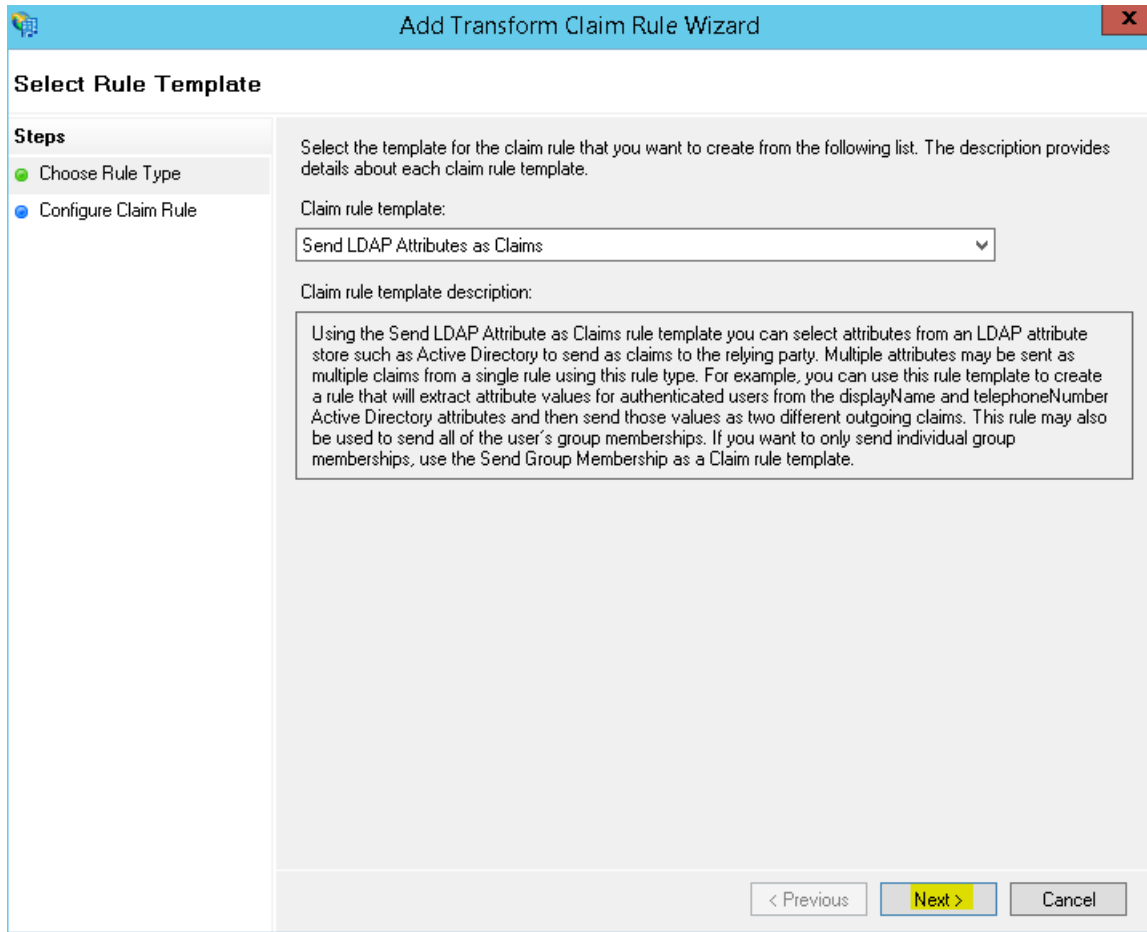


Figure 59. AD FS Relying Party – Rule Template



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

**Edit Rule - Name** ✕

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:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name	Name ID
*		

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

**Edit Rule - GivenName** ✕

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:

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)
▶	<input type="text" value="Given-Name"/>	<input type="text" value="Given Name"/>
*	<input type="text"/>	<input type="text"/>

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

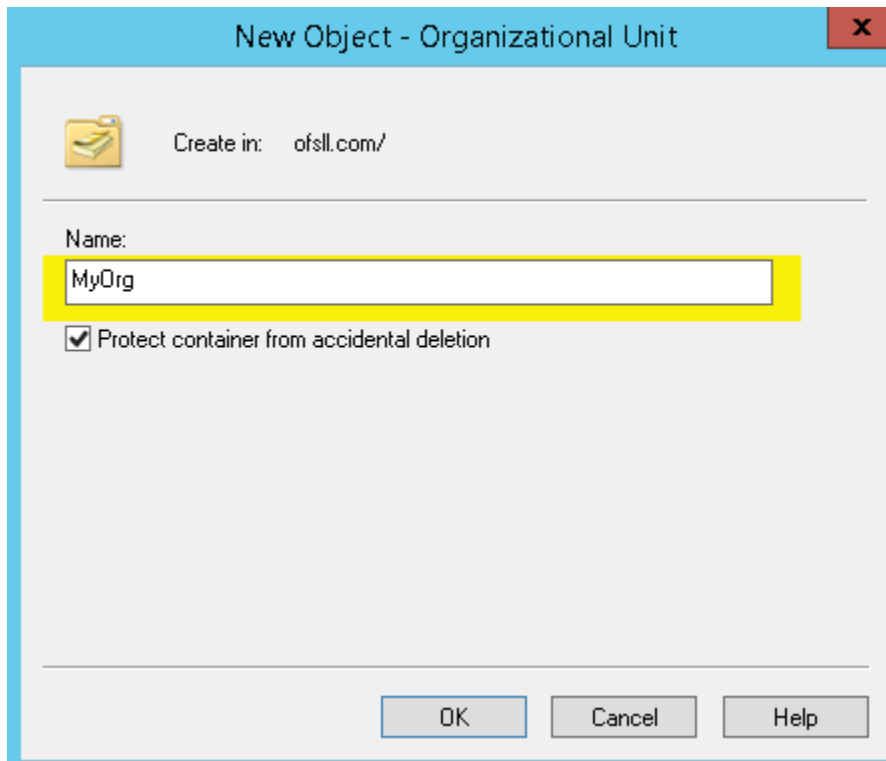


Figure 62. AD – Organizational Unit

## 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

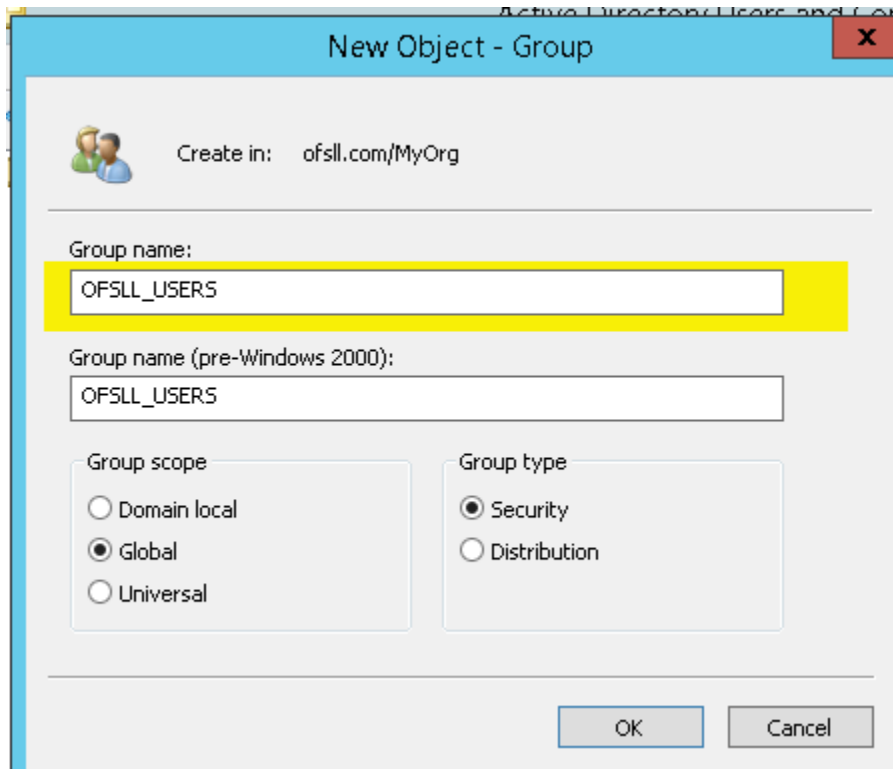


Figure 63. AD – Create Group

## 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

The screenshot shows the 'New Object - User' dialog box. The title bar reads 'New Object - User' with a close button (X) on the right. Below the title bar, there is a user icon and the text 'Create in: ofssl.com/MyOrg'. The main area contains several input fields: 'First name:' with 'OFSSLUSR' and 'Initials:' with an empty field; 'Last name:' with 'USer'; 'Full name:' with 'OFSSLUSR USer'; 'User logon name:' with 'ofsslusr' and a dropdown menu showing '@ofssl.com'; and 'User logon name (pre-Windows 2000):' with 'OFSSL\' and 'ofsslusr'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a dashed border.

Figure 64. AD – Create User

## AD Group Mapping to AD User

AD Users created in above steps should be mapped to AD groups depend. 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

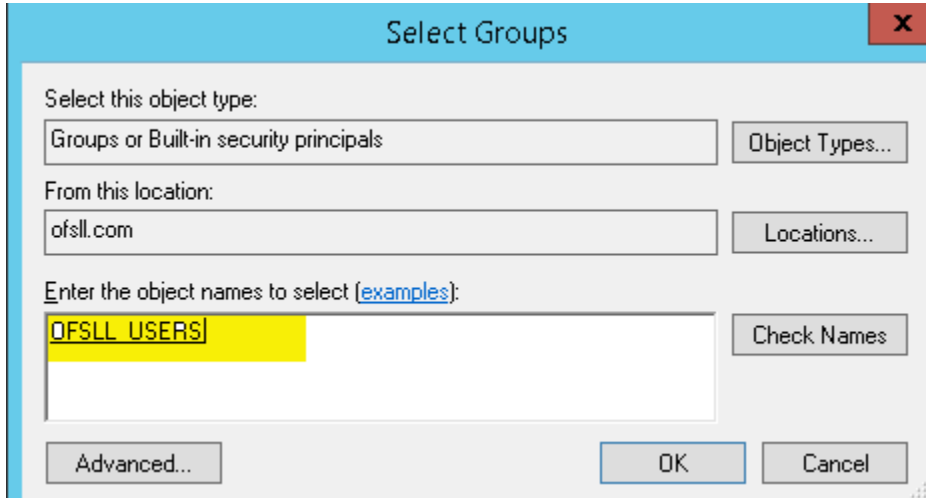


Figure 65. AD – Group Mapping

Users are now mapped and the AD Group. User provision steps are complete and as next steps these users are provisioned with OFSSL 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

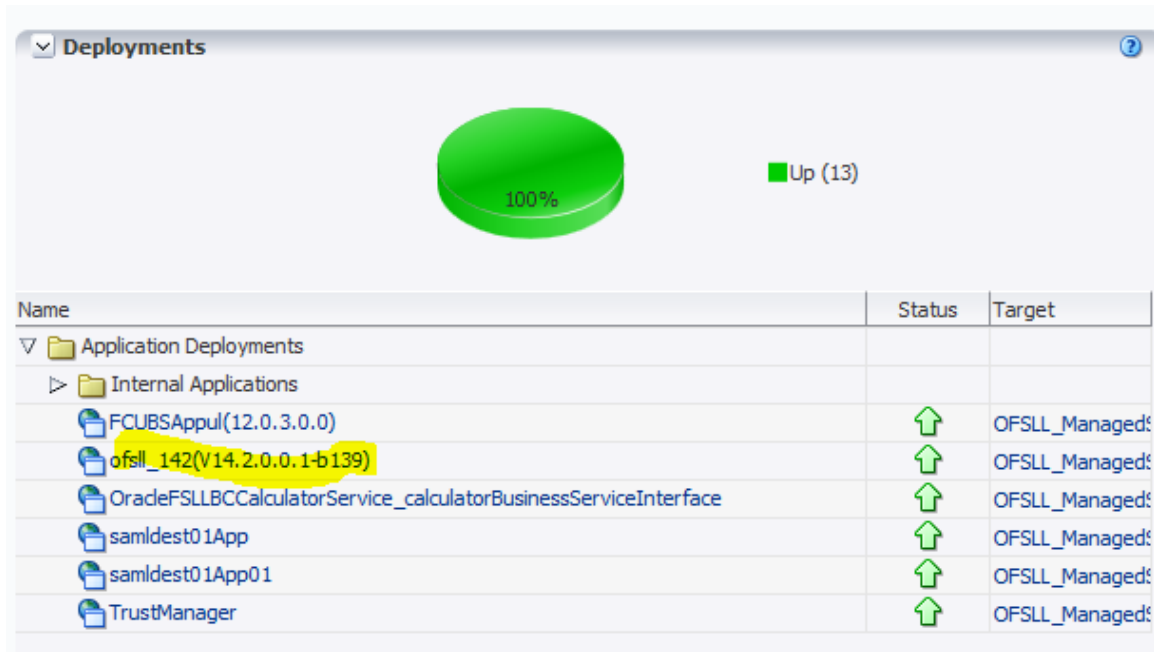


Figure 66. Weblogic EM –Deployments

» Select Application Deployment -> Security -> Application Roles

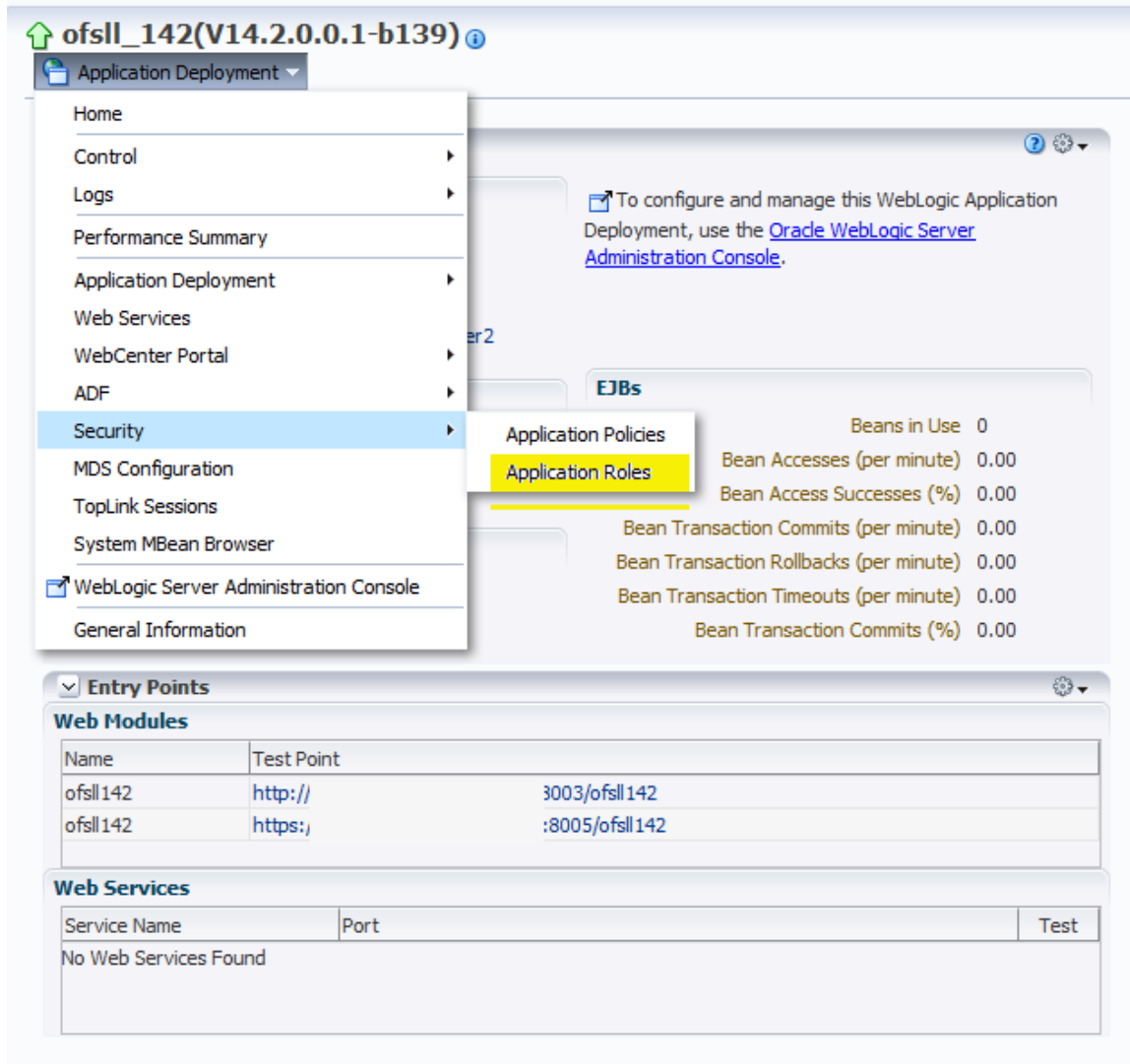


Figure 67. Weblogic EM – Application Roles



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

The screenshot shows the 'Application Roles' page in Weblogic EM. At the top, it displays 'ofssl\_142(V14.2.0.0.1-b139)' and 'Application Deployment'. The user is logged in as 'weblogic|Host'. The page title is 'Application Roles'. Below the title, there is a description of application roles and a link to the Oracle WebLogic Server Security Provider. The 'Policy Store Provider' section shows 'Scope: WebLogic Domain' and 'Provider: DB\_ORACLE'. The 'Search' section has a search bar and a 'Starts With' dropdown. Below the search bar, there are buttons for 'Create...', 'Create Like...', 'Edit...', and 'Delete...'. A table lists the role 'OFSSL\_USER' with its display name 'OFSSL\_USER' and an empty description. Below the table, there is a 'Membership for OFSSL\_USER' section with a table showing the principal 'OFSSL\_USERS' as a 'Group'.

Role Name	Display Name	Description
OFSSL_USER	OFSSL_USER	

Principal	Display Name	Type	Description
OFSSL_USERS		Group	

Figure 68. Weblogic EM – Application Roles

» Click on “Edit”

This screenshot is identical to Figure 68, but the 'Edit...' button in the search bar area is highlighted in yellow, indicating the next step in the process.

Figure 69. Weblogic EM – Edit Application Roles

» Click on Members → “Add”

The screenshot shows the 'Edit Application Role' page in Weblogic EM. The page title is 'ofsl\_142(V14.2.0.0.1-b139)' and the user is logged in as 'weblogi'. The page is titled 'Edit Application Role : OFSLL\_USER'. Under the 'General' section, the 'Application Stripe' is 'ofsl\_142#V14.2.0.0.1-b139', the 'Role Name' is 'OFSLL\_USER', the 'Display Name' is 'OFSLL USER', and the 'Description' field is empty. Under the 'Members' section, there is a table with one row: 'OFSLL\_USERS' with a 'Type' of 'Group'. The 'Add' button is highlighted in yellow.

Application Roles > Edit Application Role  
Logged in as **weblogi**  
Page Refresh

### Edit Application Role : OFSLL\_USER

**General**

Application Stripe ofsl\_142#V14.2.0.0.1-b139  
Role Name OFSLL\_USER  
Display Name OFSLL USER  
Description

**Members**  
An application role may need to be mapped to users or groups defined in enterprise LDAP server, or the role can be mapped to other application roles.

+ Add: ✕ Delete...

Name	Display Name	Type
OFSLL_USERS		Group

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.

**Add Principal**

Specify criteria to search and select the application roles that you want to grant permissions to.

**Search**

Type: Group

Principal Name: Starts With

Display Name: Starts With

**Searched Principals**

Principal	Display Name	Description
No principals found based on search criteria		

**Advanced Option**

Check to enter principal name here instead of searching from above. This option can be used for advanced scenarios related to custom authenticators.

Type: Group

\* Principal Name: OFSLL\_USERS

Display Name: OFSLL\_USERS

OK Cancel

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 OFSSL application by 3<sup>rd</sup> party system.

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

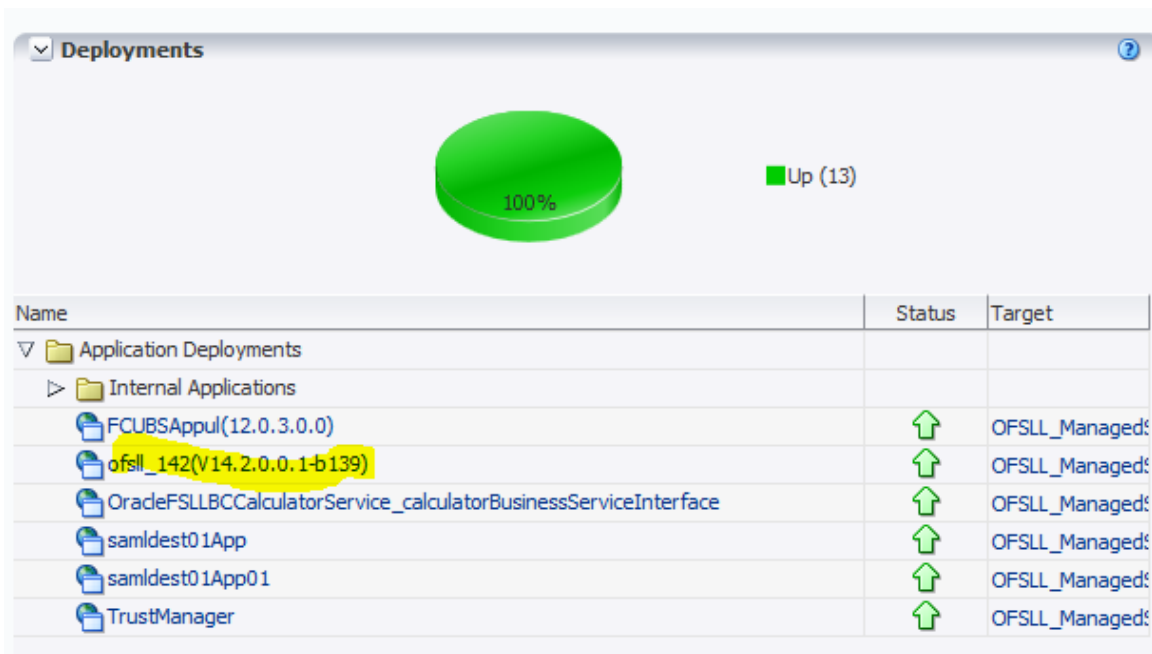


Figure 72. Weblogic EM –Deployments

» Select Application Deployment -> Security -> Application Policies

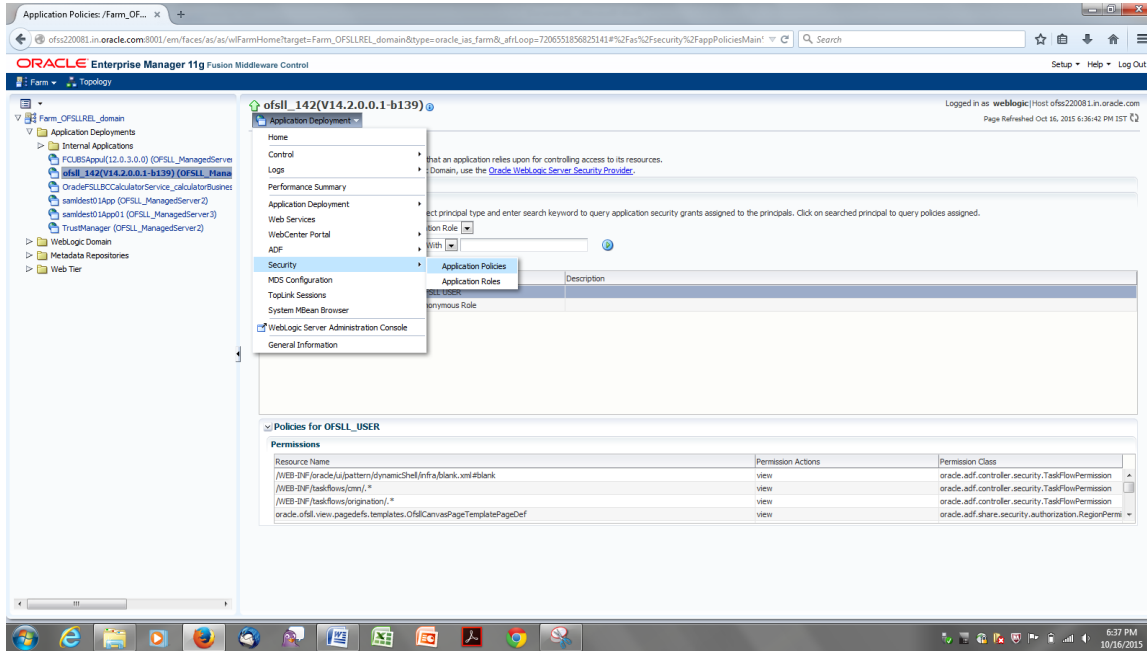


Figure 73. Weblogic EM –Security Policies

» Below detail shows up

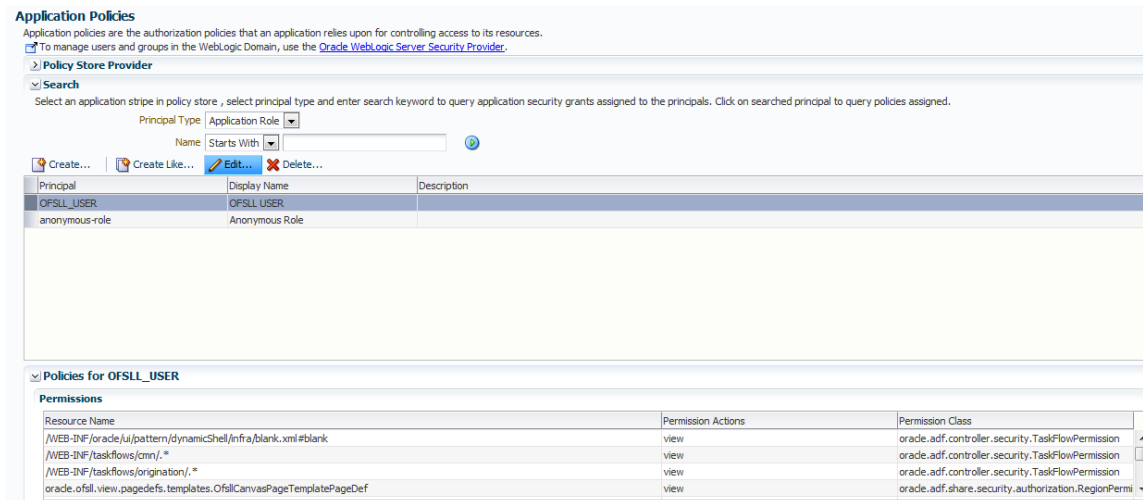


Figure 74. Weblogic EM – Application Policies

» For the Principal “OFSLL\_USER” click on “Edit” below screen shows up

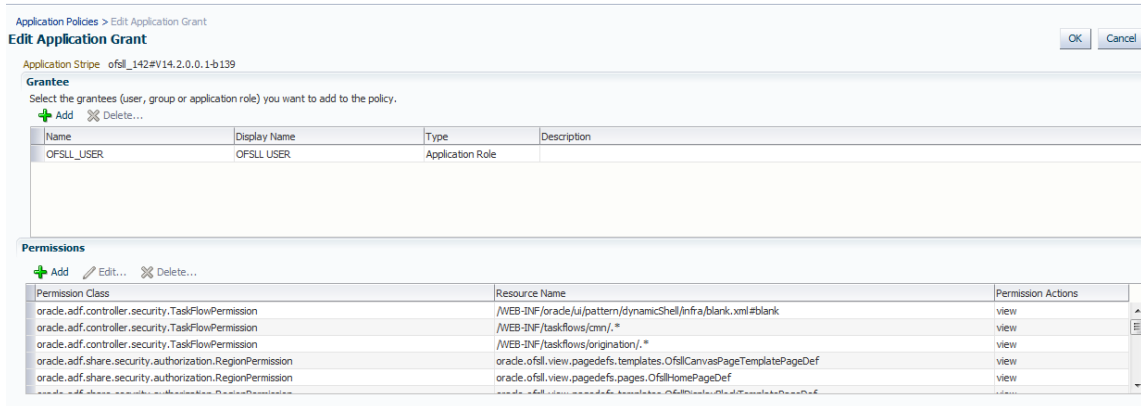


Figure 75. Weblogic EM – Application Grant

» 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

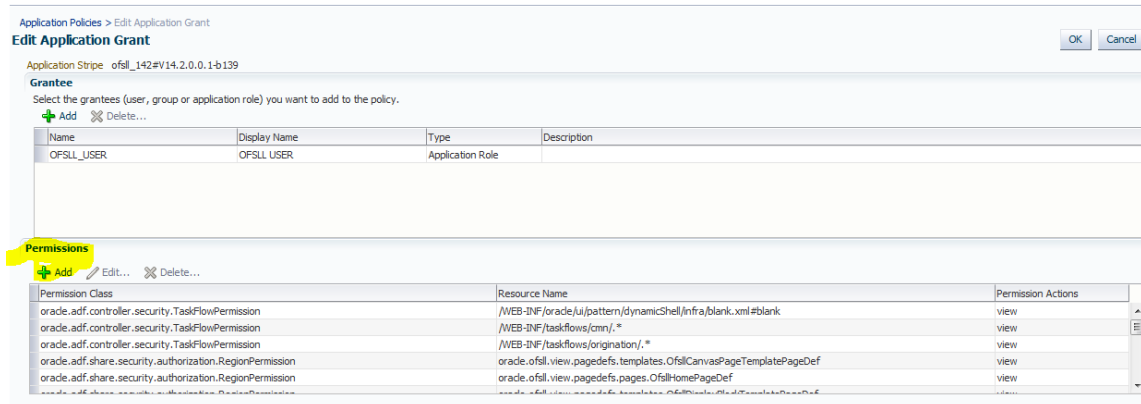


Figure 76. Weblogic EM – Edit Application Permissions

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

**Add Permission**

Select from permissions and resources used in this application. Enter search criteria to search for right permissions.

**Search**

Permissions  Resource Types

Permission Class: oracle.adf.controller.security.TaskFlowPermission

Resource Name: Starts With [ ] [Search]

**Search Results**

Resource Name	Permission Actions
No permissions added.	

**TIP** Continue to go to next step if you want to enter policy details.

**Continue** **Cancel**

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

**Add Permission**

Select from permissions and resources used in this application. Enter search criteria to search for right permissions.  
Customize resource or actions for selected permission.

**Customize**

\* Permission Class: oracle.adf.share.security.authorization.RegionPermission

Resource Name: oracle.ofsll.view.pagedefs.pages.OfsllCustomerServicePageDef

Permission Actions: view

**Back** **Select** **Cancel**

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

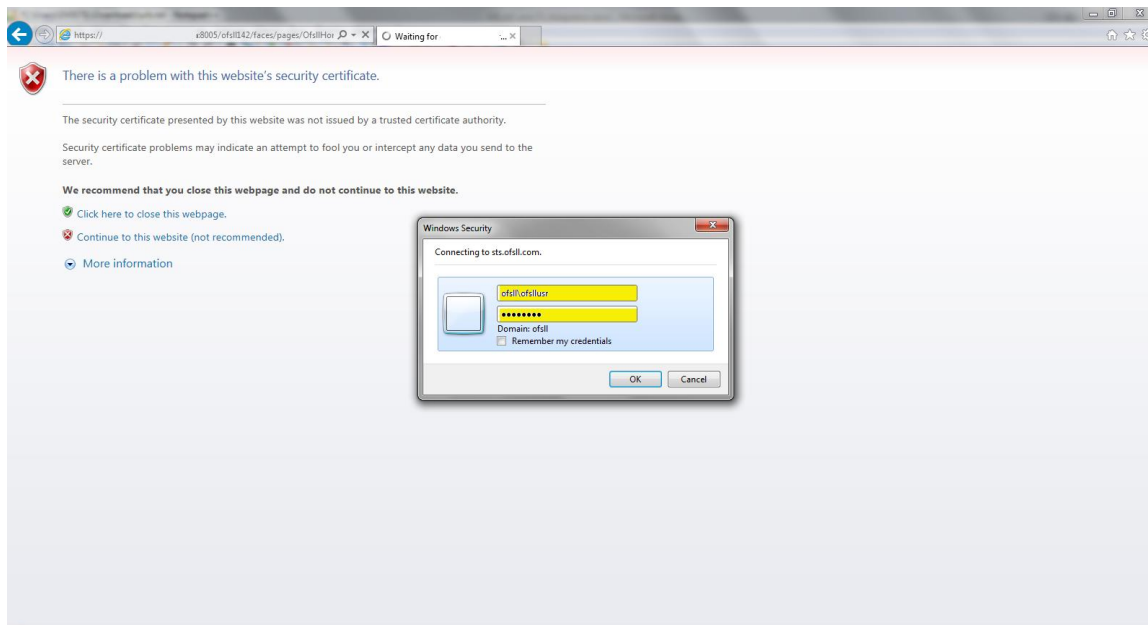


Figure 79. Internet Explorer: AD FS Sing-In pop-up windows

- » On successful authentication, OFSLL Home page opens up



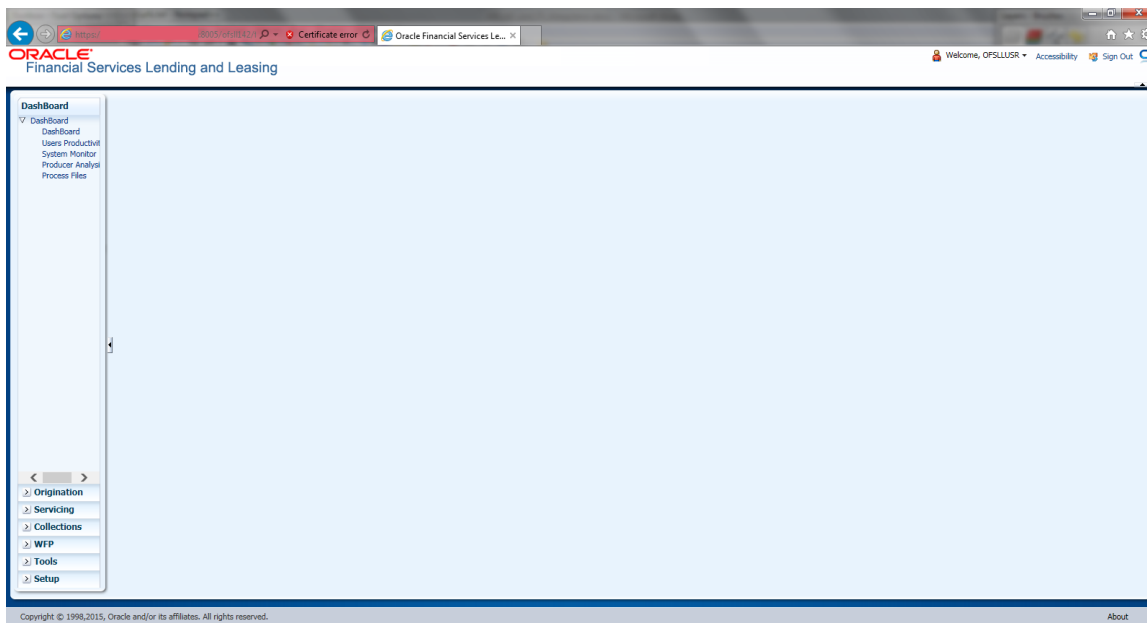


Figure 80. Internet Explorer: OFSLL Home Page

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

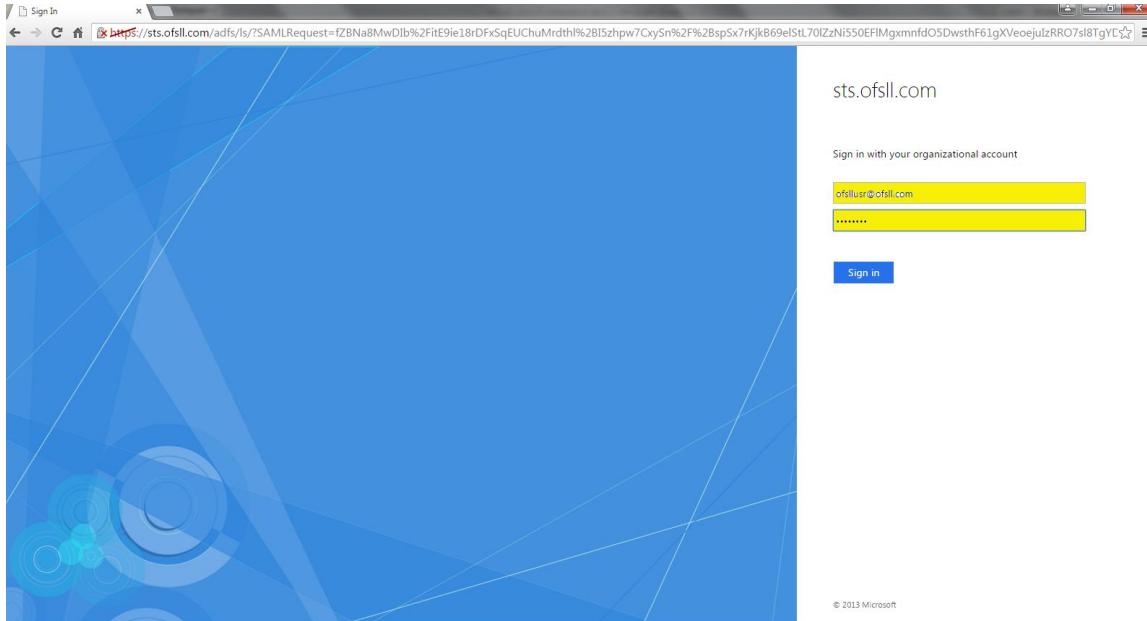


Figure 81. Google Chrome: AD FS Sign-In Page

## 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

```
orafmw@ofss220081:~/app/middleware/user_projects/domains/OFSSLREL_domain/servers/OFSSL_ManagedServer2/logs:
## Nov 2, 2015 2:13:21 PM IST: <Debug> <Security> [SAML] <Access> ..... <OFSSL_ManagedServer2> [ACTIVE] ExecuteThread: '1' for queue: 'weblogic.kernel.Default (self-tuning)' <<WS
Server>> <-> <02649776143d1fa-6a81393515066732d-000-000000000002> <14463301680> <BEL-030000> [SAML] <CallbackHandler: callback[0]: NameCallback: asfName (OFSSLFSR)>
## Nov 2, 2015 2:13:21 PM IST: <Debug> <Security> [SAML] <Access> ..... <OFSSL_ManagedServer2> [ACTIVE] ExecuteThread: '1' for queue: 'weblogic.kernel.Default (self-tuning)' <<WS
Server>> <-> <02649776143d1fa-6a81393515066732d-000-000000000002> <14463301680> <BEL-030000> [SAML] <CallbackHandler: callback[0]: NameCallback: asfName (OFSSLFSR)>
## Nov 2, 2015 2:13:21 PM IST: <Debug> <Security> [SAML] <Access> ..... <OFSSL_ManagedServer2> [ACTIVE] ExecuteThread: '1' for queue: 'weblogic.kernel.Default (self-tuning)' <<WS
Server>> <-> <02649776143d1fa-6a81393515066732d-000-000000000002> <14463301710> <BEL-030000> [SAML] <CallbackHandler: callback[0]: NameCallback: asfName (OFSSLFSR)>
## Nov 2, 2015 2:13:21 PM IST: <Debug> <Security> [SAML] <Access> ..... <OFSSL_ManagedServer2> [ACTIVE] ExecuteThread: '1' for queue: 'weblogic.kernel.Default (self-tuning)' <<
WS Server>> <-> <02649776143d1fa-6a81393515066732d-000-000000000002> <14463301710> <BEL-030000> <Only redirect URL from request cache: https://o*****.*****.xR090/OFSSL142
/owa/powa/OFSSLUser.aspx>
```

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

CONNECT WITH US

-  [blogs.oracle.com/oracle](https://blogs.oracle.com/oracle)
-  [facebook.com/oracle](https://facebook.com/oracle)
-  [twitter.com/oracle](https://twitter.com/oracle)
-  [oracle.com](https://oracle.com)

**Integrated Cloud Applications & Platform Services**

Copyright © 2020, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615

White Paper Title

Author: [OPTIONAL]  
Contributing Authors: [OPTIONAL]