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 | DECEMBER 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.

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 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.

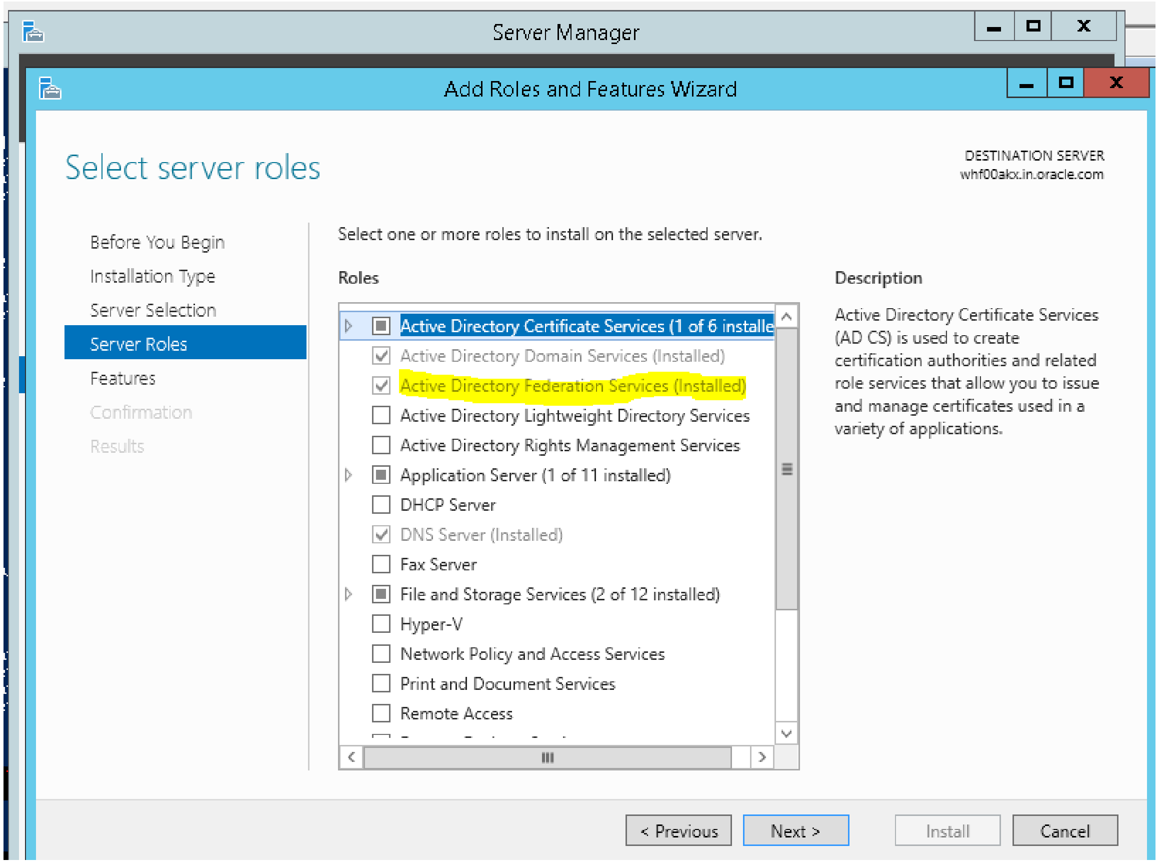
- Add few users to Active Directory on AD Server
- Install IIS Manager on AD Server

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



Select server roles

DESTINATION SERVER
whf00akx.in.oracle.com

Select one or more roles to install on the selected server.

Roles

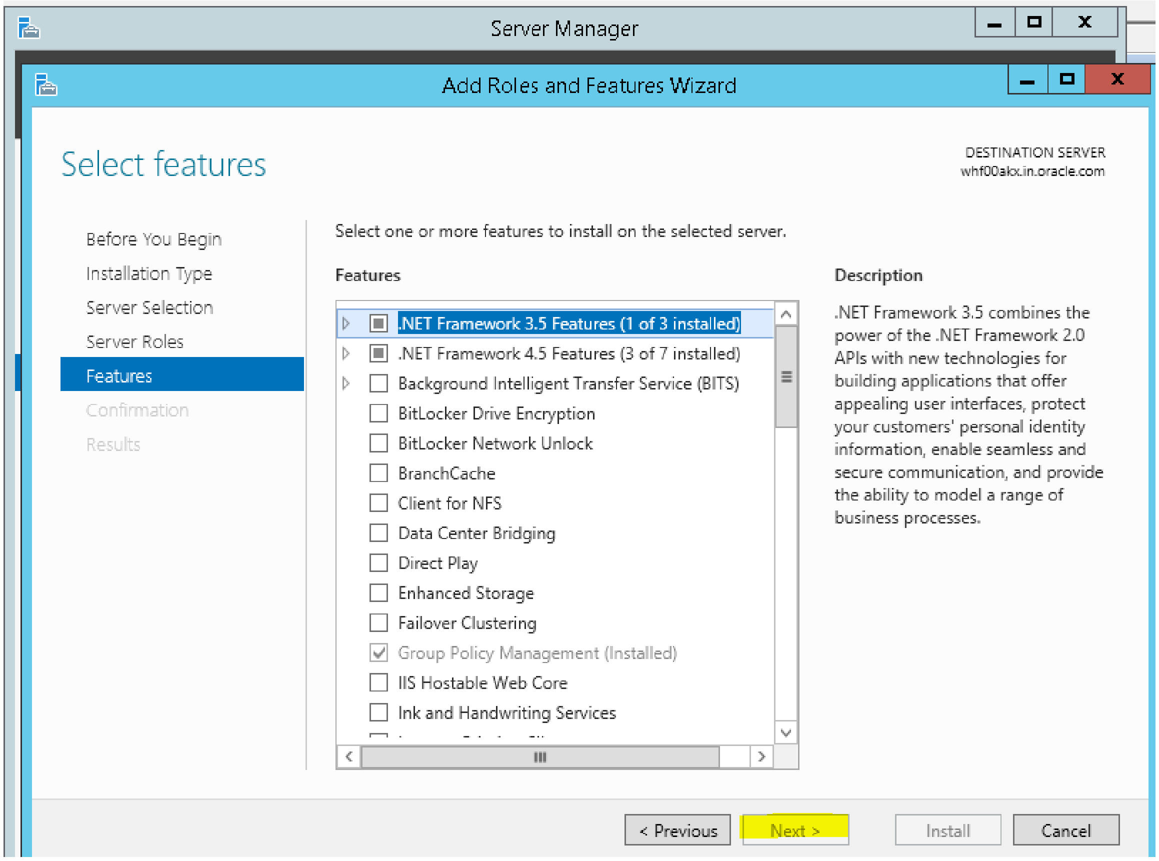
- ■ Active Directory Certificate Services (1 of 6 installe
- ☑ Active Directory Domain Services (Installed)
- ☑ Active Directory Federation Services (Installed)
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- ■ Application Server (1 of 11 installed)
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Figure 1. Install AD FS –Server Roles

» On the Select Features interface, click Next



Select features

DESTINATION SERVER
whf00akx.in.oracle.com

Select one or more features to install on the selected server.

Features

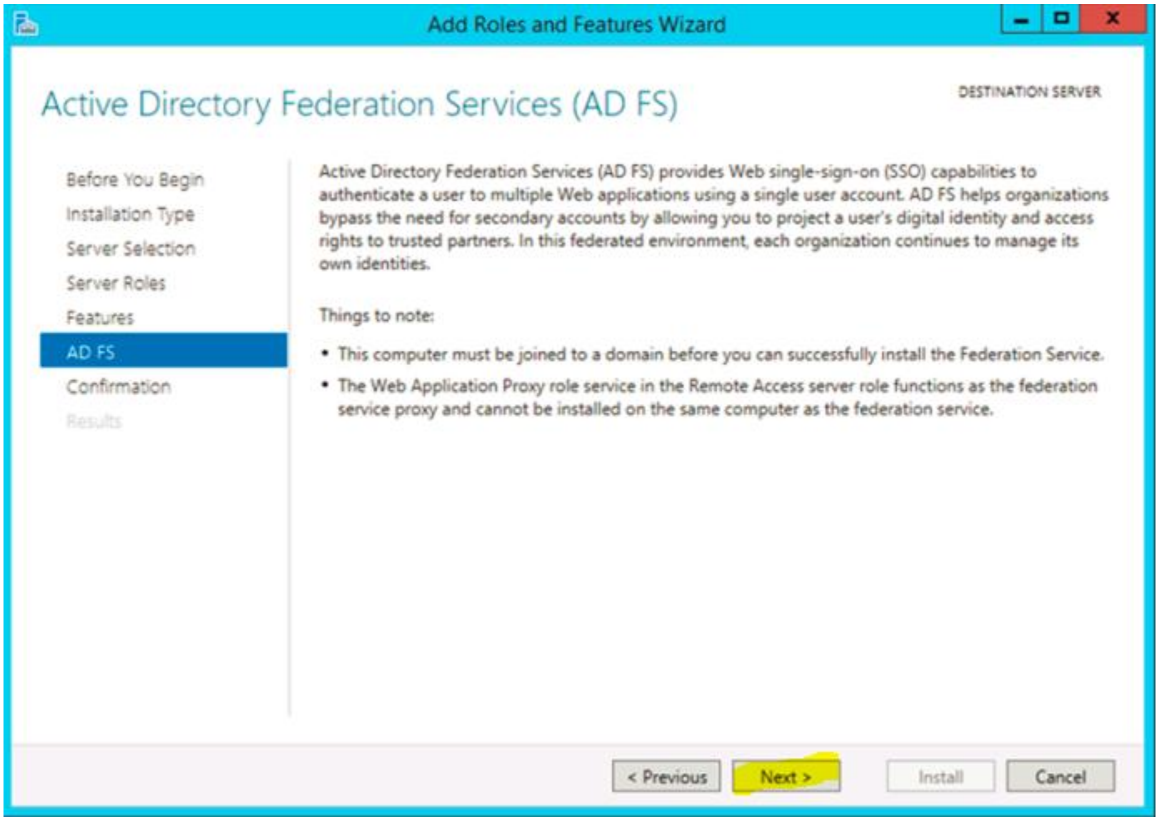
- ▣ .NET Framework 3.5 Features (1 of 3 installed)
- ▣ .NET Framework 4.5 Features (3 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- ☑ Group Policy Management (Installed)
- □ IIS Hostable Web Core
- □ Ink and Handwriting Services

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

Figure 2. Install AD FS – Select Features

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



Active Directory Federation Services (AD FS)

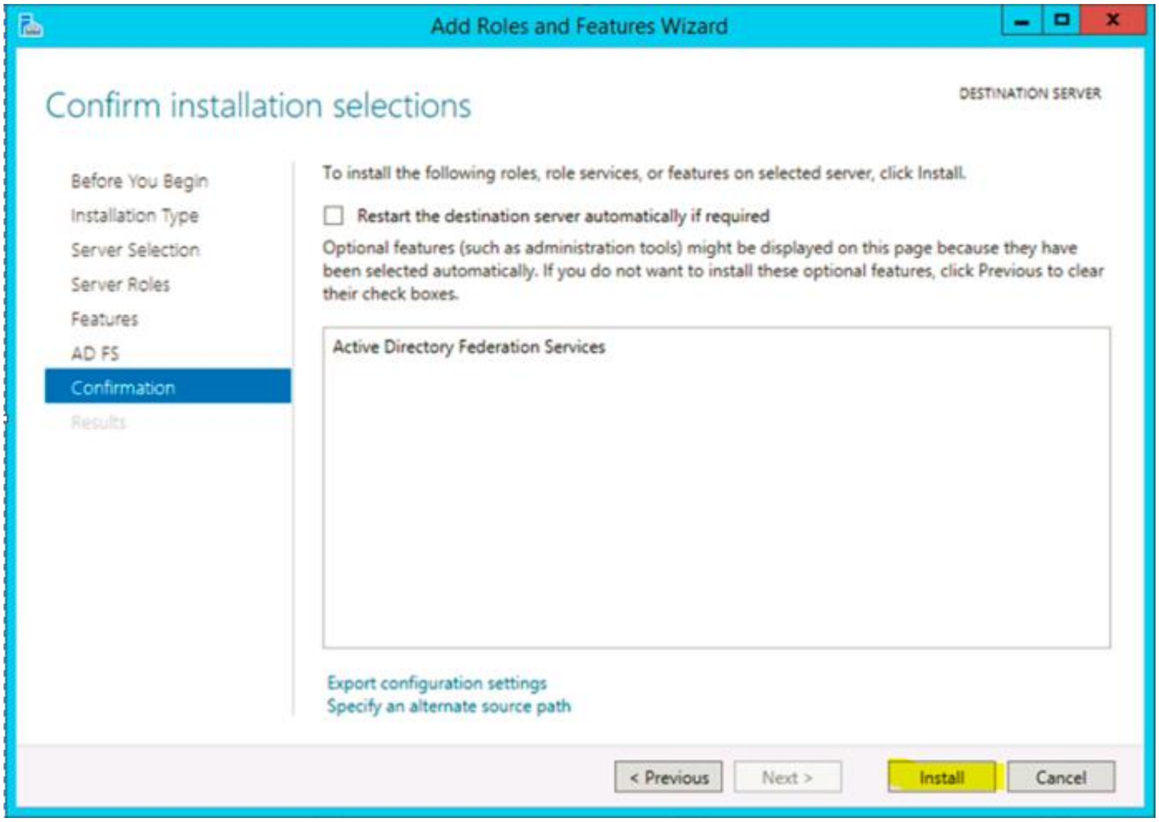
Active Directory Federation Services (AD FS) provides Web single-sign-on (SSO) capabilities to authenticate a user to multiple Web applications using a single user account. AD FS helps organizations bypass the need for secondary accounts by allowing you to project a user's digital identity and access rights to trusted partners. In this federated environment, each organization continues to manage its own identities.

Things to note:

- This computer must be joined to a domain before you can successfully install the Federation Service.
- The Web Application Proxy role service in the Remote Access server role functions as the federation service proxy and cannot be installed on the same computer as the federation service.

Figure 3. Install AD FS – AD FS Page

» Click Install



Confirm installation selections

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

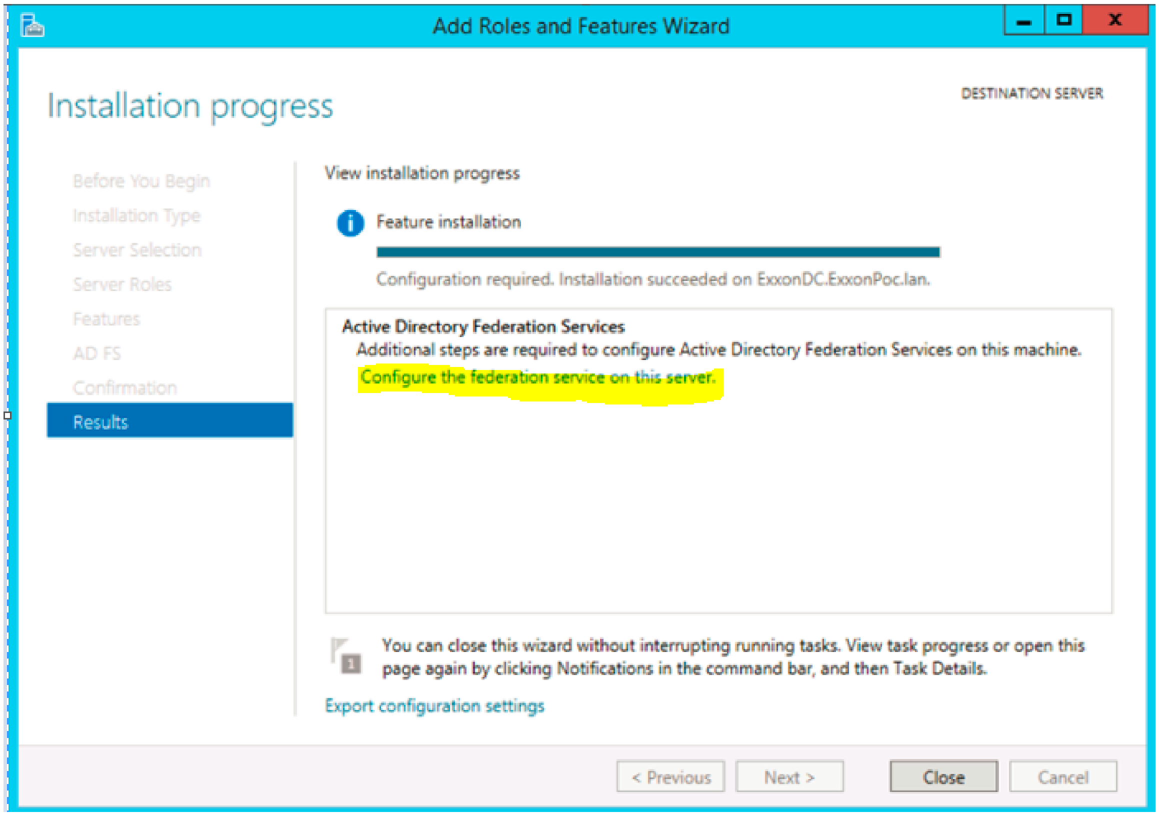
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Federation Services

Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

Figure 4. Install AD FS – Confirmation Page

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



View installation progress

Feature installation

Configuration required. Installation succeeded on ExxonDC.ExxonPoc.lan.

Active Directory Federation Services

Additional steps are required to configure Active Directory Federation Services on this machine.

Configure the federation service on this server.

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

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

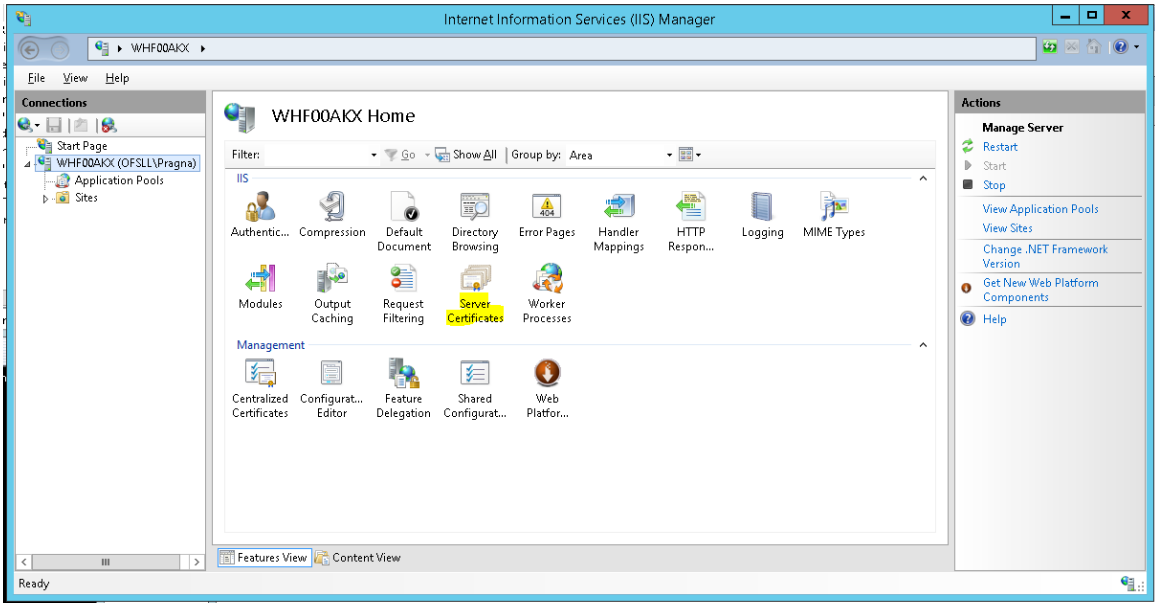
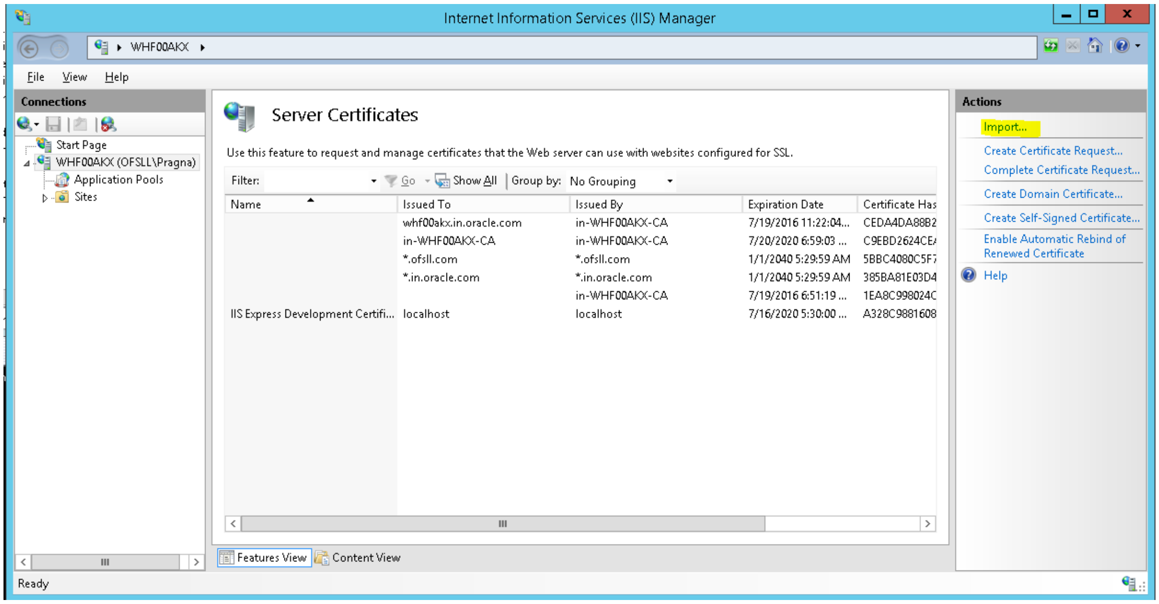


Figure 6. IIS Manager – Main Page

- Click on import link


Internet Information Services (IIS) Manager
WHF00AKX
File
View
Help
Connections
Start Page
WHF00AKX (OFSLL\Pragna)
Application Pools
Sites
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready

Server Certificates

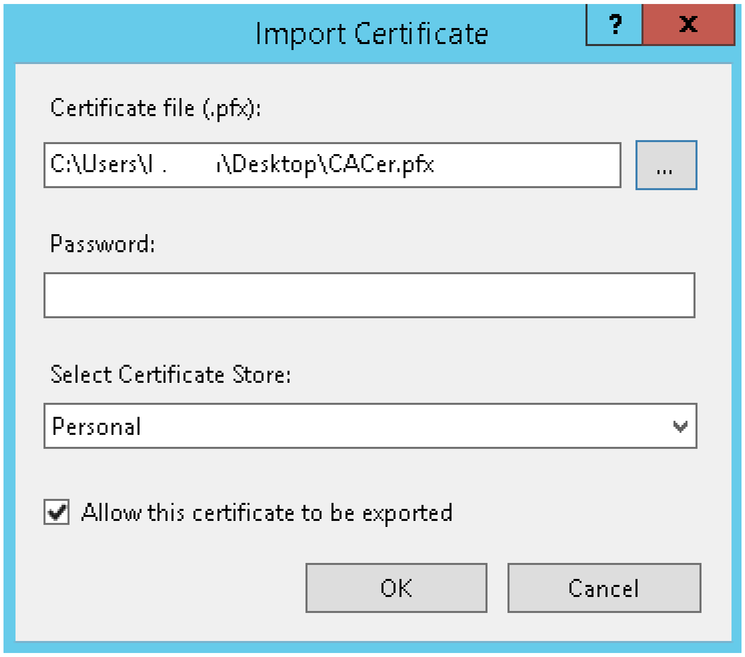
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go Show All | Group by: No Grouping

Name	Issued To	Issued By	Expiration Date	Certificate Has
	whf00akx.in.oracle.com	in-WHF00AKX-CA	7/19/2016 11:22:04...	CEDA4DA88B2
	in-WHF00AKX-CA	in-WHF00AKX-CA	7/20/2020 6:59:03 ...	C9EBD2624CEA
	*.ofsll.com	*.ofsll.com	1/1/2040 5:29:59 AM	5BBC4080C5F7
	*.in.oracle.com	*.in.oracle.com	1/1/2040 5:29:59 AM	385BA81E03D4
		in-WHF00AKX-CA	7/19/2016 6:51:19 ...	1EA8C998024C
IIS Express Development Certifi...	localhost	localhost	7/16/2020 5:30:00 ...	A328C9881608

Figure 7. IIS Manager - Server Certificates

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



Certificate file (.pfx):

C:\Users\l .   i\Desktop\CACer.pfx

Password:

Select Certificate Store:

Personal

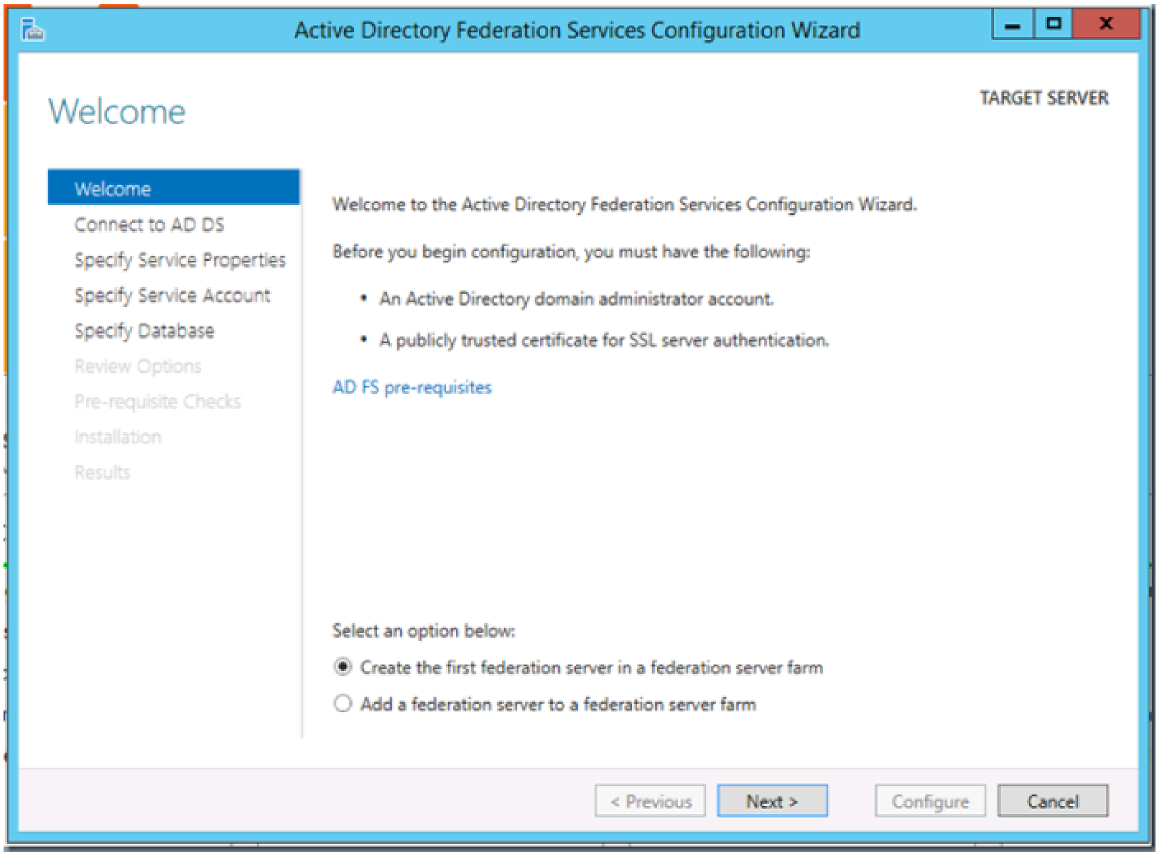
☑ Allow this certificate to be exported

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



Welcome to the Active Directory Federation Services Configuration Wizard.

Before you begin configuration, you must have the following:

- An Active Directory domain administrator account.
- A publicly trusted certificate for SSL server authentication.

Select an option below:

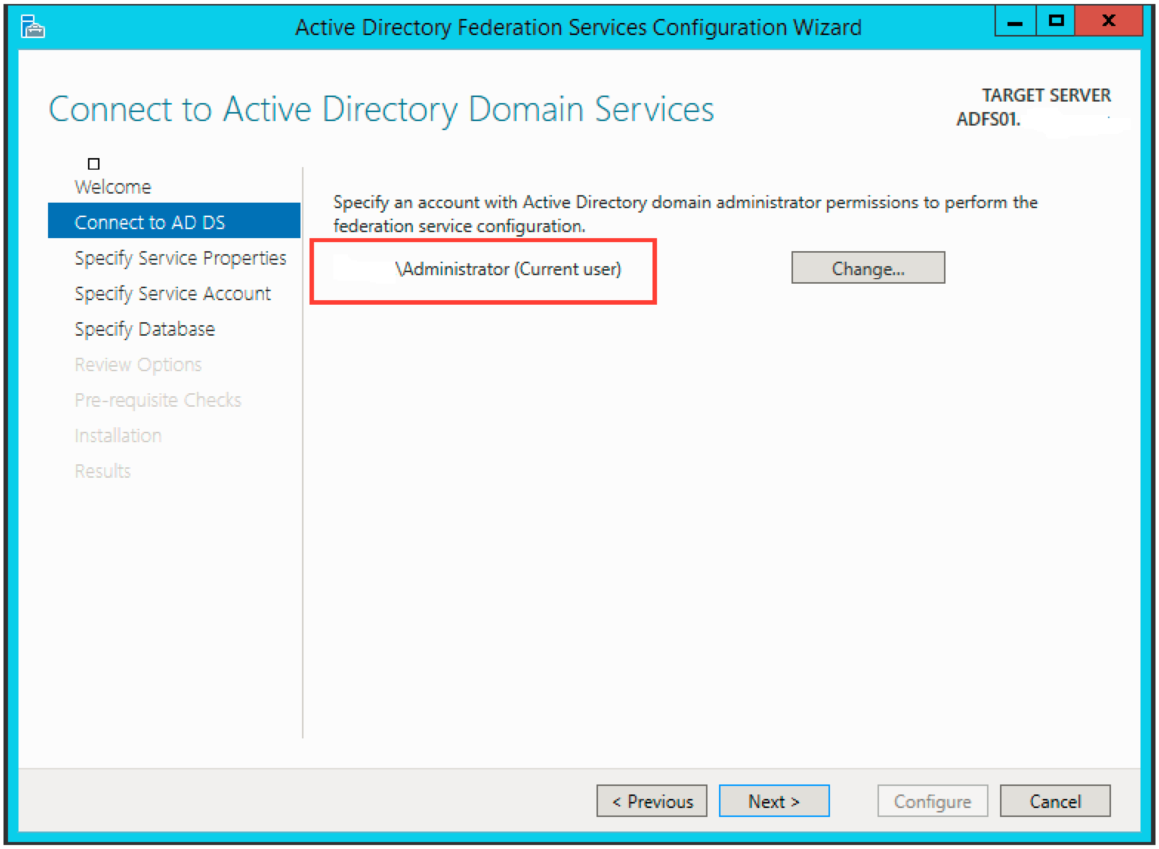
● Create the first federation server in a federation server farm

○ Add a federation server to a federation server farm

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.



Connect to Active Directory Domain Services

TARGET SERVER
ADFS01.

Specify an account with Active Directory domain administrator permissions to perform the federation service configuration.

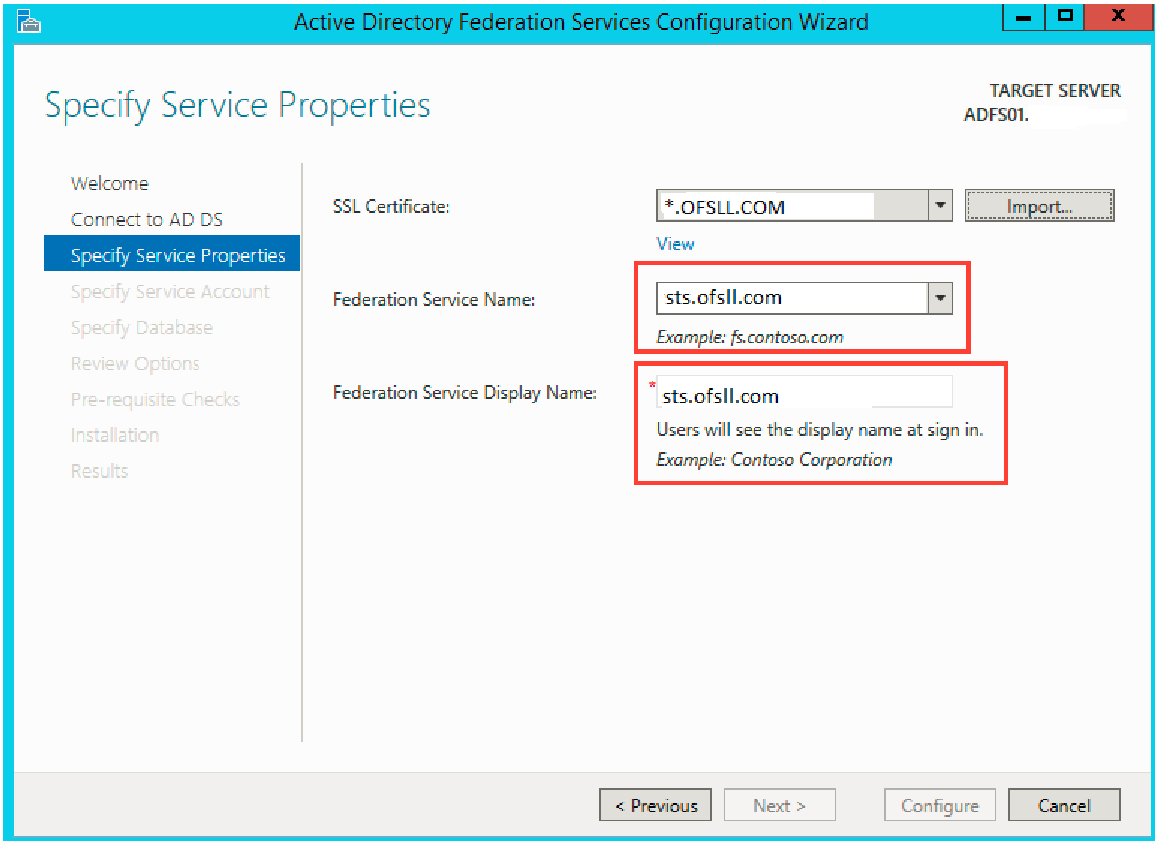
\Administrator (Current user)

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



Active Directory Federation Services Configuration Wizard

Specify Service Properties

TARGET SERVER
ADFS01.

SSL Certificate: *.OFSLL.COM

Federation Service Name: sts.ofsll.com

Example: fs.contoso.com

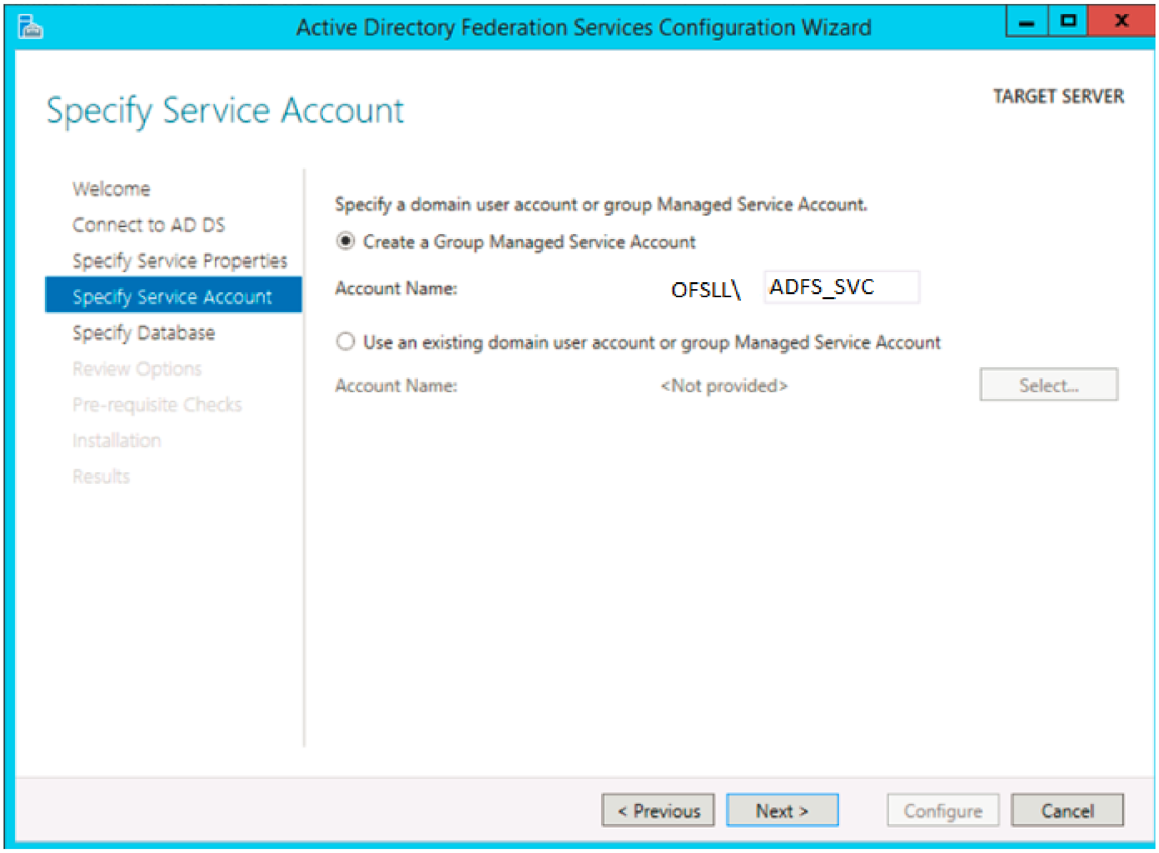
Federation Service Display Name: * sts.ofsll.com

Users will see the display name at sign in.

Example: Contoso Corporation

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.



Specify Service Account

Specify a domain user account or group Managed Service Account.

● Create a Group Managed Service Account

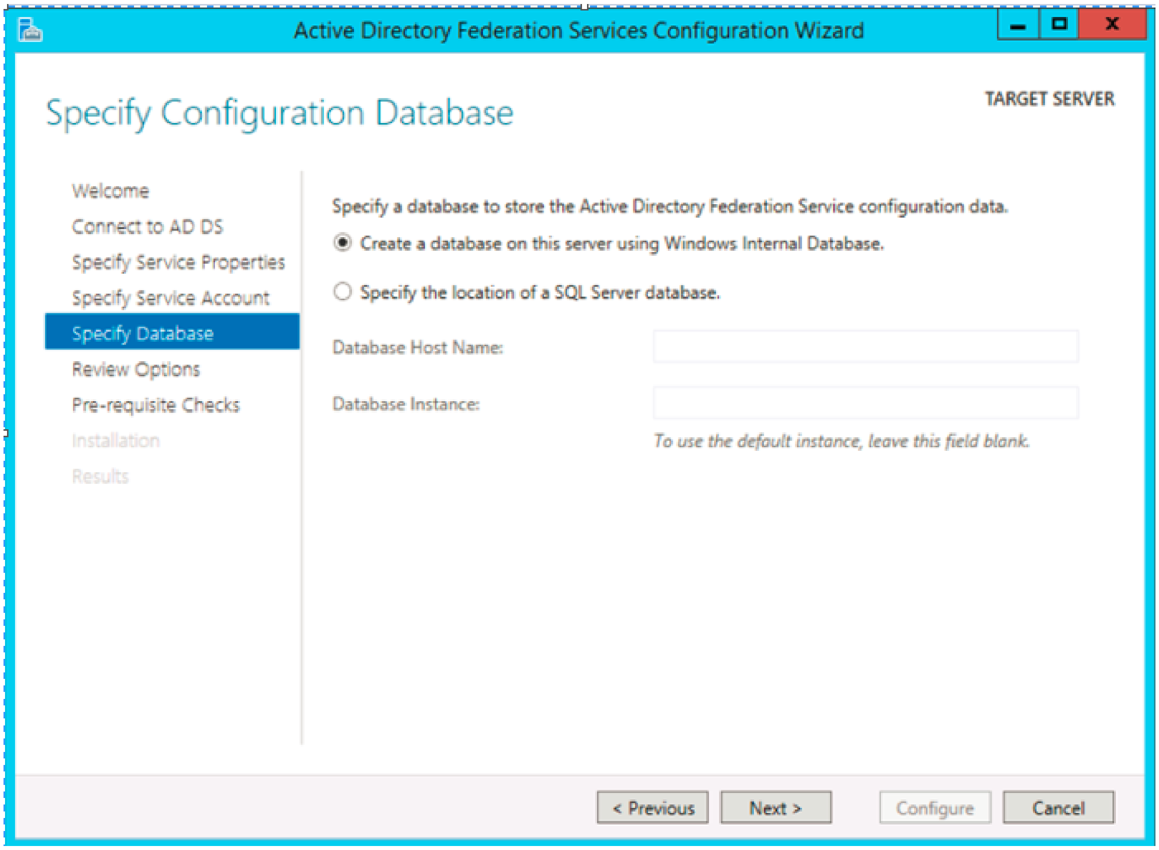
Account Name: OFSLL\ ADFS_SVC

○ Use an existing domain user account or group Managed Service Account

Account Name: <Not provided>

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



Active Directory Federation Services Configuration Wizard

Specify Configuration Database

TARGET SERVER

Specify a database to store the Active Directory Federation Service configuration data.

● Create a database on this server using Windows Internal Database.

○ Specify the location of a SQL Server database.

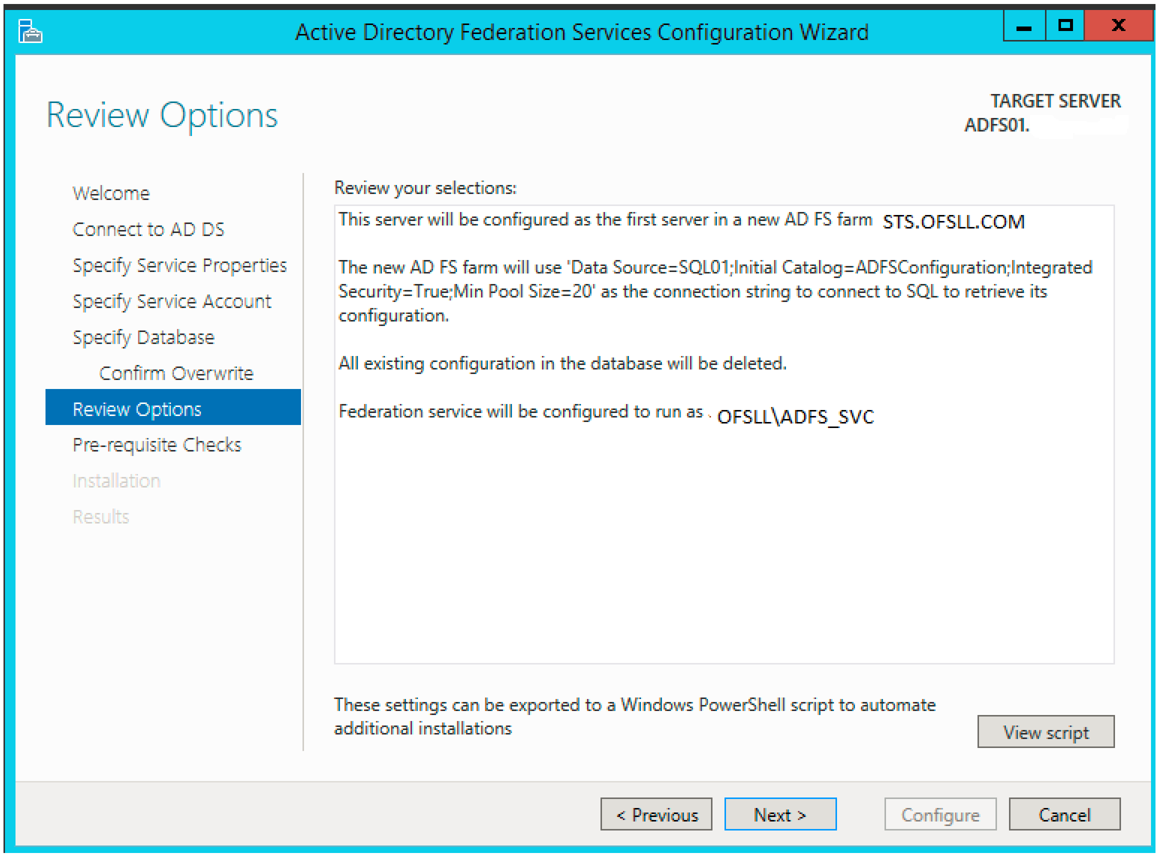
Database Host Name:

Database Instance:

To use the default instance, leave this field blank.

Figure 13. AD FS Configuration – Service Database Setup

» On the Review Options interface, click Next



Review Options

TARGET SERVER
ADFS01.

Review your selections:

This server will be configured as the first server in a new AD FS farm STS.OFSLL.COM

The new AD FS farm will use 'Data Source=SQL01;Initial Catalog=ADFSConfiguration;Integrated Security=True;Min Pool Size=20' as the connection string to connect to SQL to retrieve its configuration.

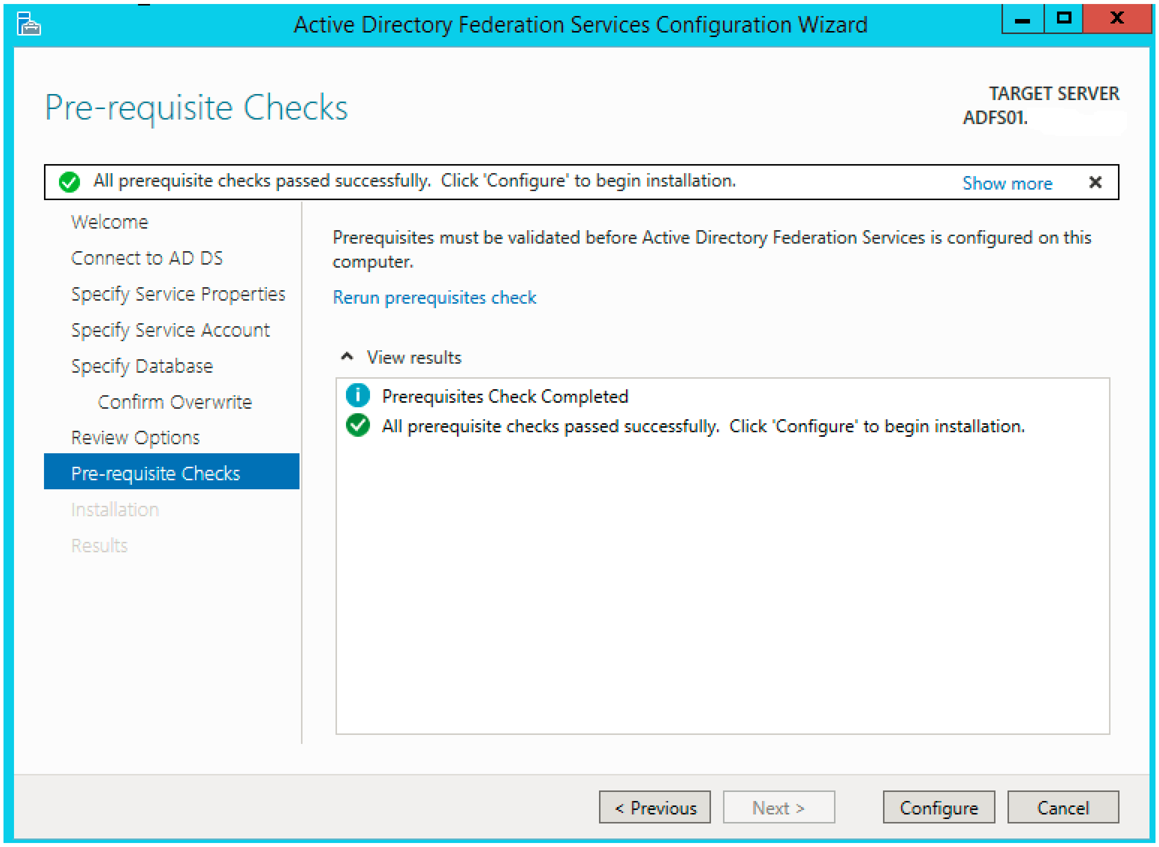
All existing configuration in the database will be deleted.

Federation service will be configured to run as . OFSLL\ADFS_SVC

These settings can be exported to a Windows PowerShell script to automate additional installations

Figure 14. AD FS Configuration – Review Page

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



✓ All prerequisite checks passed successfully. Click 'Configure' to begin installation.

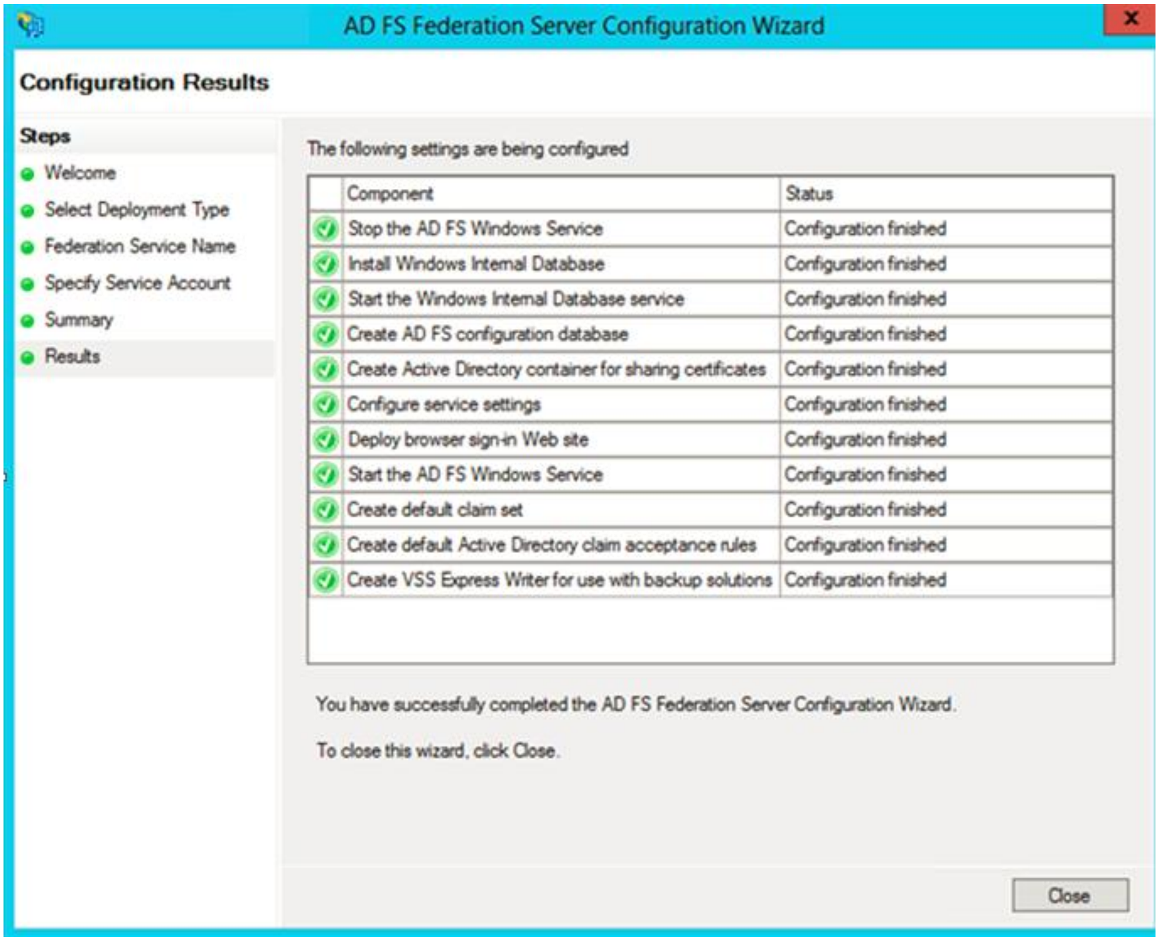
Prerequisites must be validated before Active Directory Federation Services is configured on this computer.

ⓘ Prerequisites Check Completed

✓ All prerequisite checks passed successfully. Click 'Configure' to begin installation.

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

- » On the Results interface, click Close



AD FS Federation Server Configuration Wizard

Configuration Results

The following settings are being configured

	Component	Status
✓	Stop the AD FS Windows Service	Configuration finished
✓	Install Windows Internal Database	Configuration finished
✓	Start the Windows Internal Database service	Configuration finished
✓	Create AD FS configuration database	Configuration finished
✓	Create Active Directory container for sharing certificates	Configuration finished
✓	Configure service settings	Configuration finished
✓	Deploy browser sign-in Web site	Configuration finished
✓	Start the AD FS Windows Service	Configuration finished
✓	Create default claim set	Configuration finished
✓	Create default Active Directory claim acceptance rules	Configuration finished
✓	Create VSS Express Writer for use with backup solutions	Configuration finished

You have successfully completed the AD FS Federation Server Configuration Wizard.

To close this wizard, click Close.

Figure 16. AD FS Configuration – Result Page

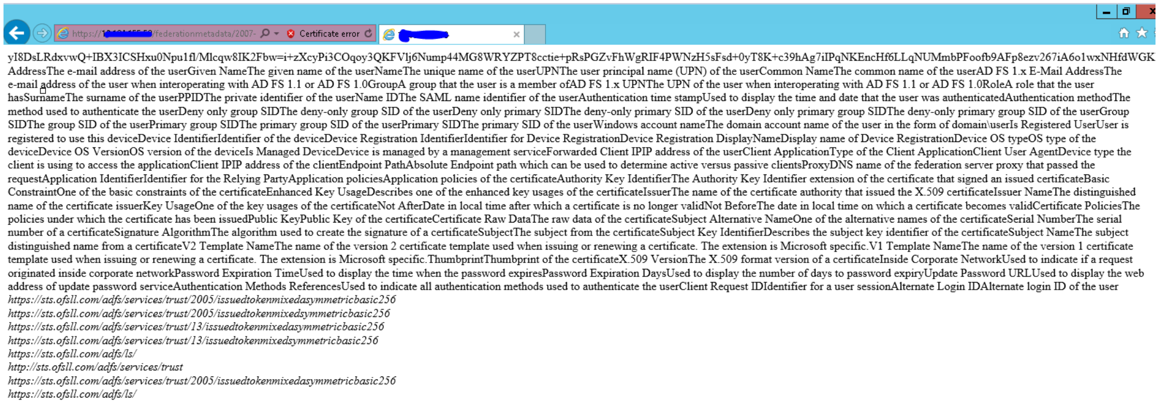
Verify AD FS Installation

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.



```
yI8DsLRdxvwQ+IBX3ICSHxu0Npu1fl/Mlcqw8IK2Fbw=i+zXcyPi3COqoy3QKFVlj6Nump44MG8WRYZPT8cctie+pRsPGZvFhWgRIF4PWNzH5sFsd+0yT8K+c39hAg7iIPqNKEncHf6LLqNUMmbPFoofb9AFp8ezv267iA6o1wxNHfdWGK
AddressThe e-mail address of the userGiven NameThe given name of the userNameThe unique name of the userUPNThe user principal name (UPN) of the userCommon NameThe common name of the userAD FS 1.x E-Mail AddressThe
e-mail address of the user when interoperating with AD FS 1.1 or AD FS 1.0GroupA group that the user is a member ofAD FS 1.x UPNThe UPN of the user when interoperating with AD FS 1.1 or AD FS 1.0RoleA role that the user
hasSurnameThe surname of the userPPIDThe private identifier of the userName IDThe SAML name identifier of the userAuthentication time stampUsed to display the time and date that the user was authenticatedAuthentication methodThe
method used to authenticate the userDeny only group SIDThe deny-only group SID of the userDeny only primary SIDThe deny-only primary SID of the userDeny only primary group SIDThe deny-only primary group SID of the userGroup
SIDThe group SID of the userPrimary group SIDThe primary group SID of the userPrimary SIDThe primary SID of the userWindows account nameThe domain account name of the user in the form of domain\userIs Registered UserUser is
registered to use this deviceDevice IdentifierIdentifier of the deviceDevice Registration IdentifierIdentifier for Device RegistrationDevice Registration DisplayNameDisplay name of Device RegistrationDevice OS typeOS type of the
deviceDevice OS VersionOS version of the deviceIs Managed DeviceDevice is managed by a management serviceForwarded Client IPIP address of the userClient ApplicationType of the Client ApplicationClient User AgentDevice type the
client is using to access the applicationClient IPIP address of the clientEndpoint PathAbsolute Endpoint path which can be used to determine active versus passive clientsProxyDNS name of the federation server proxy that passed the
requestApplication IdentifierIdentifier for the Relying PartyApplication policiesApplication policies of the certificateAuthority Key IdentifierThe Authority Key Identifier extension of the certificate that signed an issued certificateBasic
ConstraintOne of the basic constraints of the certificateEnhanced Key UsageDescribes one of the enhanced key usages of the certificateIssuerThe name of the certificate authority that issued the X.509 certificateIssuer NameThe distinguished
name of the certificate issuerKey UsageOne of the key usages of the certificateNot AfterDate in local time after which a certificate is no longer validNot BeforeThe date in local time on which a certificate becomes validCertificate PoliciesThe
policies under which the certificate has been issuedPublic KeyPublic Key of the certificateCertificate Raw DataThe raw data of the certificateSubject Alternative NameOne of the alternative names of the certificateSerial NumberThe serial
number of a certificateSignature AlgorithmThe algorithm used to create the signature of a certificateSubjectThe subject from the certificateSubject Key IdentifierDescribes the subject key identifier of the certificateSubject NameThe subject
distinguished name from a certificateV2 Template NameThe name of the version 2 certificate template used when issuing or renewing a certificate. The extension is Microsoft specific.V1 Template NameThe name of the version 1 certificate
template used when issuing or renewing a certificate. The extension is Microsoft specific.ThumbprintThumbprint of the certificateX.509 VersionThe X.509 format version of a certificateInside Corporate NetworkUsed to indicate if a request
originated inside corporate networkPassword Expiration TimeUsed to display the time when the password expiresPassword Expiration DaysUsed to display the number of days to password expiryUpdate Password URLUsed to display the web
address of update password serviceAuthentication Methods ReferencesUsed to indicate all authentication methods used to authenticate the userClient Request IDIdentifier for a user sessionAlternate Login IDAlternate login ID of the user
https://sts.ofsll.com/adfs/services/trust/2005/issuedtokenmixedasymmetricbasic256
https://sts.ofsll.com/adfs/services/trust/2005/issuedtokenmixedsymmetricbasic256
https://sts.ofsll.com/adfs/services/trust/13/issuedtokenmixedasymmetricbasic256
https://sts.ofsll.com/adfs/services/trust/13/issuedtokenmixedsymmetricbasic256
https://sts.ofsll.com/adfs/ls/
http://sts.ofsll.com/adfs/services/trust
https://sts.ofsll.com/adfs/services/trust/2005/issuedtokenmixedasymmetricbasic256
https://sts.ofsll.com/adfs/ls/
```

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

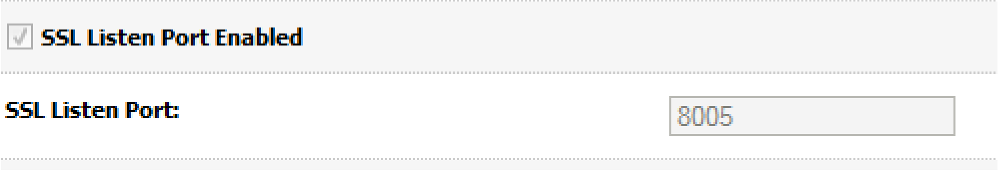
Before configuring the domain as Service Provider (SP), the SSL port has to be enabled on the Weblogic Managed Server (in this case on ofsll_managedserver2).

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.



☑ SSL Listen Port Enabled

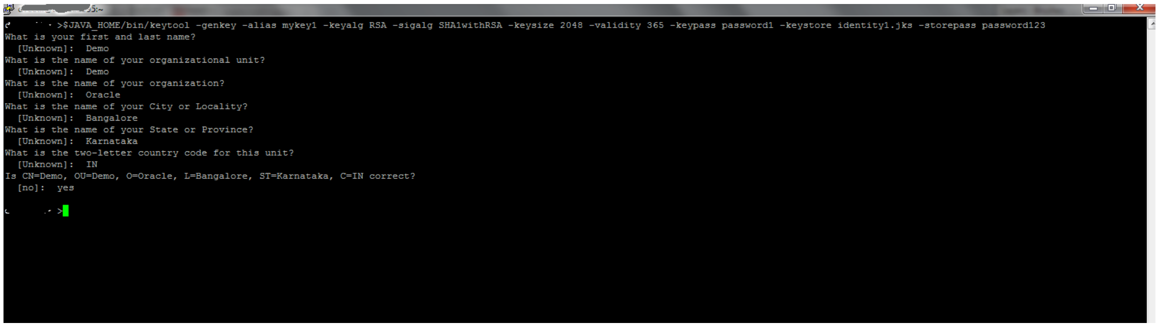
SSL Listen Port: 8005

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:

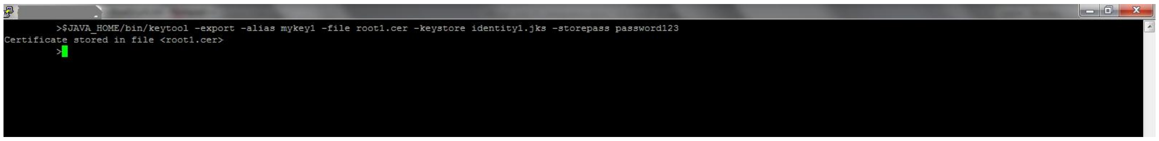
- Logon on to OFSLL physical server via putty
- Set the JDK classpath to the JDK1.6+ path
- Run the following command
  - $JAVA_HOME/bin/keytool -genkey -alias mykey -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keypass password1 -keystore identity.jks -storepass password123



```
>$JAVA_HOME/bin/keytool -genkey -alias mykey1 -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keypass password1 -keystore identity1.jks -storepass password123
What is your first and last name?
  [Unknown]:  Demo
What is the name of your organizational unit?
  [Unknown]:  Demo
What is the name of your organization?
  [Unknown]:  Oracle
What is the name of your City or Locality?
  [Unknown]:  Bangalore
What is the name of your State or Province?
  [Unknown]:  Karnataka
What is the two-letter country code for this unit?
  [Unknown]:  IN
Is CN=Demo, OU=Demo, O=Oracle, L=Bangalore, ST=Karnataka, C=IN correct?
  [no]:  yes

>
```

Figure 19. Weblogic Physical Server – Identity Generation

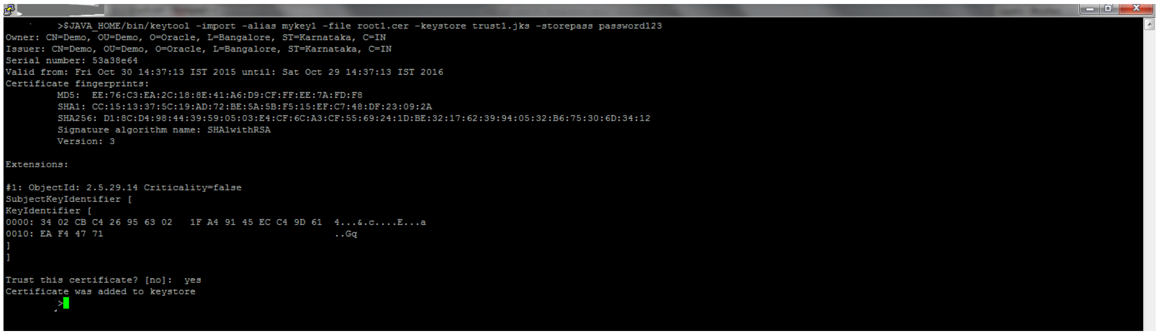
  - $JAVA_HOME/bin/keytool -export -alias mykey -file root.cer -keystore identity.jks -storepass password123



```
        >$JAVA_HOME/bin/keytool -export -alias mykey1 -file root1.cer -keystore identity1.jks -storepass password123
Certificate stored in file <root1.cer>
        >
```

Figure 20. Weblogic Physical Server – Certificate Generation

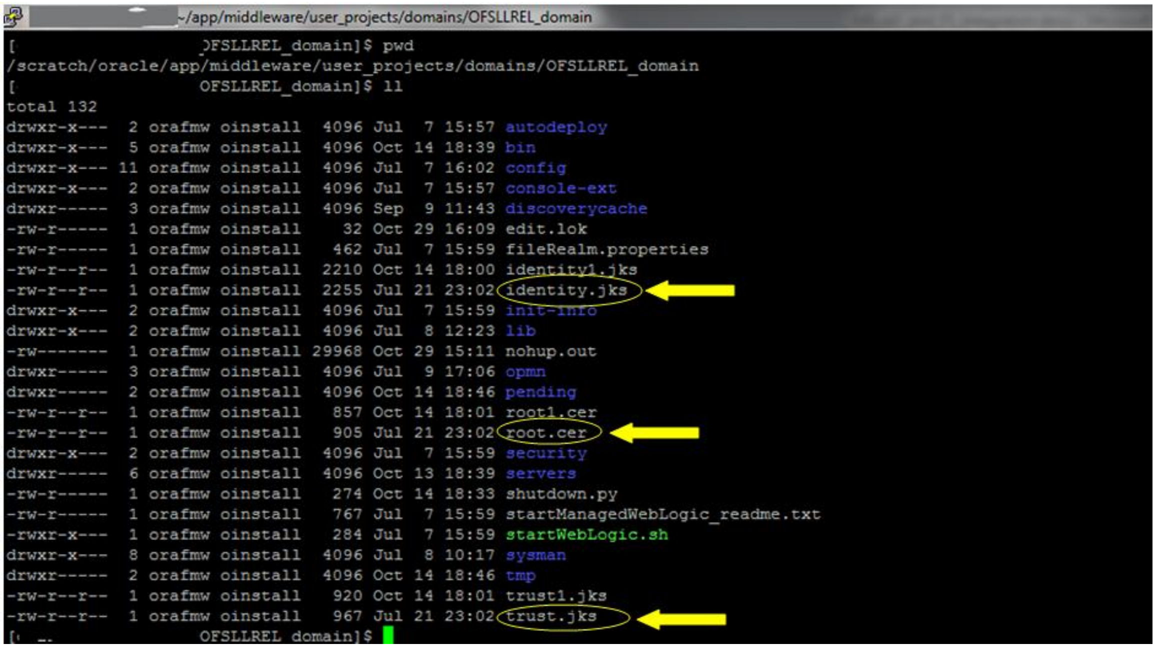
- $JAVA_HOME/bin/keytool -import -alias mykey -file root.cer -keystore trust.jks -storepass password123



```
[redacted]>$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: 53a38e64
Valid from: Fri Oct 30 14:37:13 IST 2015 until: Sat Oct 29 14:37:13 IST 2016
Certificate fingerprints:
         MD5:  EE:76:C3:EA:2C:18:8E:41:A6:D9:CF:FF:EE:7A:FD:F8
         SHA1: CC:15:13:37:5C:19:AD:72:BE:5A:5B:F5:15:EF: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 CB C4 26 95 63 02   1F A4 91 45 EC C4 9D 61  4...&.c....E...a
0010: EA F4 47 71                                        ..Gq
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
[redacted]>
```

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.



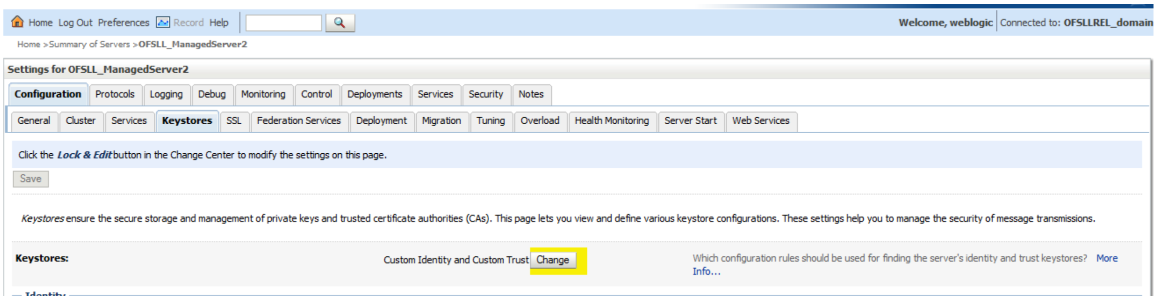
[redacted]~/app/middleware/user_projects/domains/OFSLLREL_domain

```
[[redacted]OFSLLREL_domain]$ pwd
/scratch/oracle/app/middleware/user_projects/domains/OFSLLREL_domain
[[redacted]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.lok
-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
[[redacted]OFSLLREL_domain]$
```

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



Settings for OFSLL_ManagedServer2

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

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you to manage the security of message transmissions.

Keystores: Custom Identity and Custom Trust

Which configuration rules should be used for finding the server's identity and trust keystores? More Info...

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

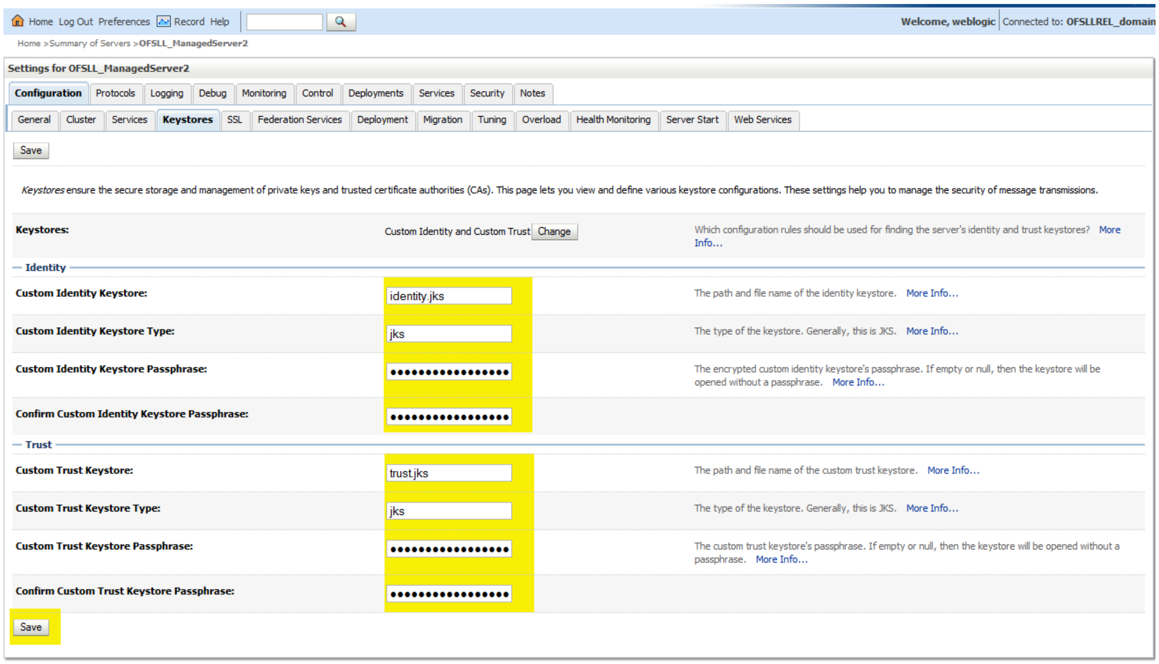
Note: By default Weblogic will look for this keystore file in $DOMAIN_HOME location.

  - 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



Home Log Out Preferences Record Help
Welcome, weblogic | Connected to: OFSLLREL_domain
Home >Summary of Servers >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
Save

Settings for OFSLL_ManagedServer2

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you to manage the security of message transmissions.

Keystores: Custom Identity and Custom Trust [Change] — Which configuration rules should be used for finding the server's identity and trust keystores? More Info...

— Identity

Custom Identity Keystore: identity.jks — The path and file name of the identity keystore. More Info...

Custom Identity Keystore Type: jks — The type of the keystore. Generally, this is JKS. More Info...

Custom Identity Keystore Passphrase: ••••••••••••••••• — The encrypted custom identity keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. More Info...

Confirm Custom Identity Keystore Passphrase: •••••••••••••••••

— Trust

Custom Trust Keystore: trust.jks — The path and file name of the custom trust keystore. More Info...

Custom Trust Keystore Type: jks — The type of the keystore. Generally, this is JKS. More Info...

Custom Trust Keystore Passphrase: ••••••••••••••••• — The custom trust keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. More Info...

Confirm Custom Trust Keystore Passphrase: •••••••••••••••••

Save

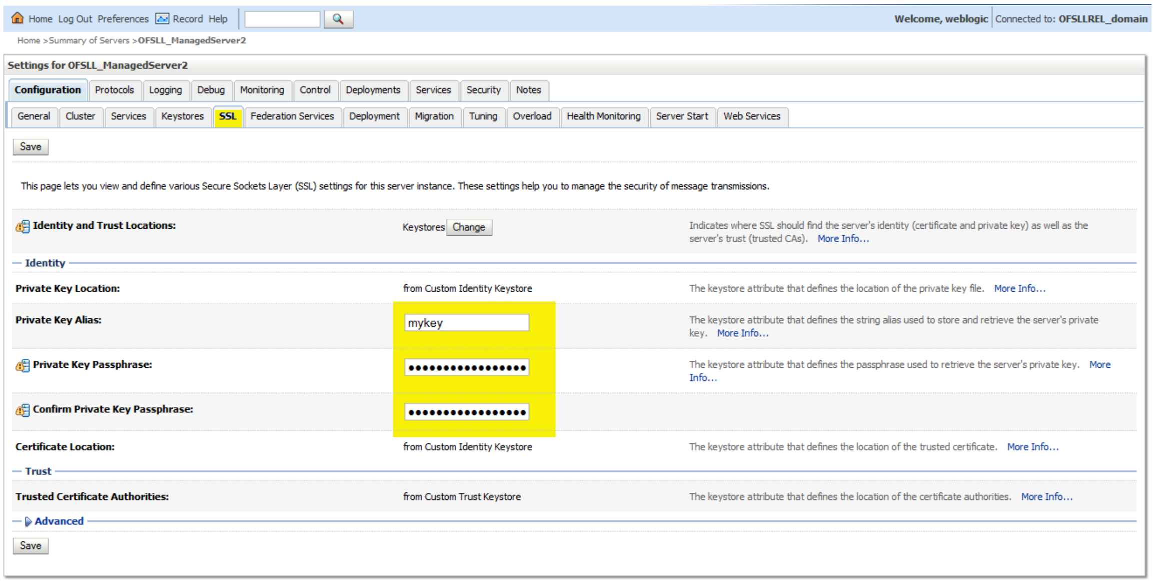
Figure 24. Weblogic Server – Keystore Settings

» 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



Home Log Out Preferences Record Help
Welcome, weblogic | Connected to: OFSLLREL_domain
Home >Summary of Servers >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
Save

Settings for OFSLL_ManagedServer2

This page lets you view and define various Secure Sockets Layer (SSL) settings for this server instance. These settings help you to manage the security of message transmissions.

Identity and Trust Locations: Keystores [Change] — Indicates where SSL should find the server's identity (certificate and private key) as well as the server's trust (trusted CAs). More Info...

— Identity

Private Key Location: from Custom Identity Keystore — The keystore attribute that defines the location of the private key file. More Info...

Private Key Alias: mykey — The keystore attribute that defines the string alias used to store and retrieve the server's private key. More Info...

Private Key Passphrase: ••••••••••••••••• — The keystore attribute that defines the passphrase used to retrieve the server's private key. More Info...

Confirm Private Key Passphrase: •••••••••••••••••

Certificate Location: from Custom Identity Keystore — The keystore attribute that defines the location of the trusted certificate. More Info...

— Trust

Trusted Certificate Authorities: from Custom Trust Keystore — The keystore attribute that defines the location of the certificate authorities. More Info...

— Advanced

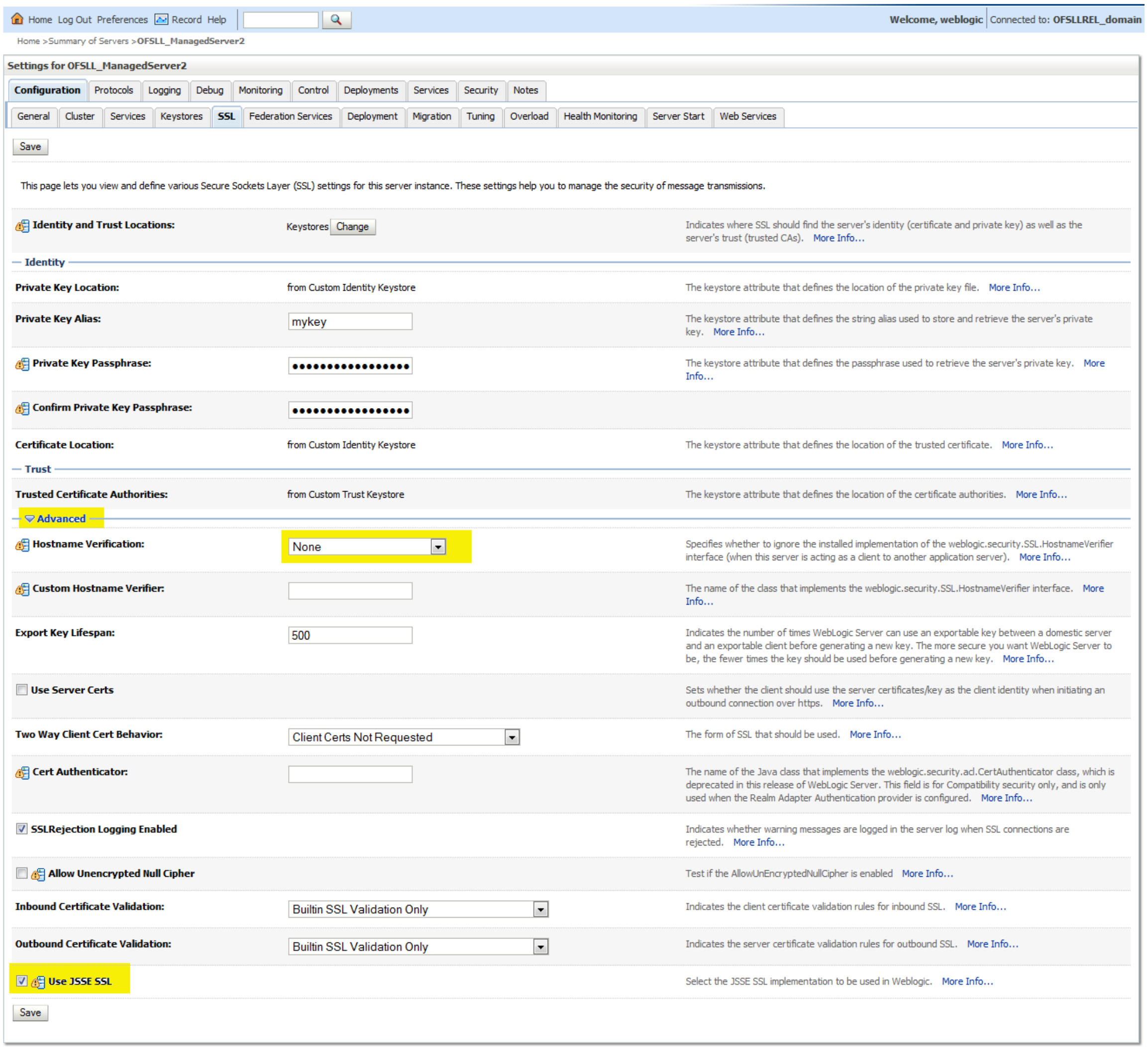
Save

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



Settings for OFSLL_ManagedServer2

This page lets you view and define various Secure Sockets Layer (SSL) settings for this server instance. These settings help you to manage the security of message transmissions.

Identity and Trust Locations:	Keystores Change	Indicates where SSL should find the server's identity (certificate and private key) as well as the server's trust (trusted CAs). More Info...
Identity		
Private Key Location:	from Custom Identity Keystore	The keystore attribute that defines the location of the private key file. More Info...
Private Key Alias:	mykey	The keystore attribute that defines the string alias used to store and retrieve the server's private key. More Info...
Private Key Passphrase:	•••••••••••••••••	The keystore attribute that defines the passphrase used to retrieve the server's private key. More Info...
Confirm Private Key Passphrase:	•••••••••••••••••	
Certificate Location:	from Custom Identity Keystore	The keystore attribute that defines the location of the trusted certificate. More Info...
Trust		
Trusted Certificate Authorities:	from Custom Trust Keystore	The keystore attribute that defines the location of the certificate authorities. More Info...
Advanced		
Hostname Verification:	None	Specifies whether to ignore the installed implementation of the weblogic.security.SSL.HostnameVerifier interface (when this server is acting as a client to another application server). More Info...
Custom Hostname Verifier:		The name of the class that implements the weblogic.security.SSL.HostnameVerifier interface. More Info...
Export Key Lifespan:	500	Indicates the number of times WebLogic Server can use an exportable key between a domestic server and an exportable client before generating a new key. The more secure you want WebLogic Server to be, the fewer times the key should be used before generating a new key. More Info...
□ Use Server Certs		Sets whether the client should use the server certificates/key as the client identity when initiating an outbound connection over https. More Info...
Two Way Client Cert Behavior:	Client Certs Not Requested	The form of SSL that should be used. More Info...
Cert Authenticator:		The name of the Java class that implements the weblogic.security.acl.CertAuthenticator class, which is deprecated in this release of WebLogic Server. This field is for Compatibility security only, and is only used when the Realm Adapter Authentication provider is configured. More Info...
☑ SSLRejection Logging Enabled		Indicates whether warning messages are logged in the server log when SSL connections are rejected. More Info...
□ Allow Unencrypted Null Cipher		Test if the AllowUnEncryptedNullCipher is enabled More Info...
Inbound Certificate Validation:	Builtin SSL Validation Only	Indicates the client certificate validation rules for inbound SSL. More Info...
Outbound Certificate Validation:	Builtin SSL Validation Only	Indicates the server certificate validation rules for outbound SSL. More Info...
☑ Use JSSE SSL		Select the JSSE SSL implementation to be used in Weblogic. More Info...

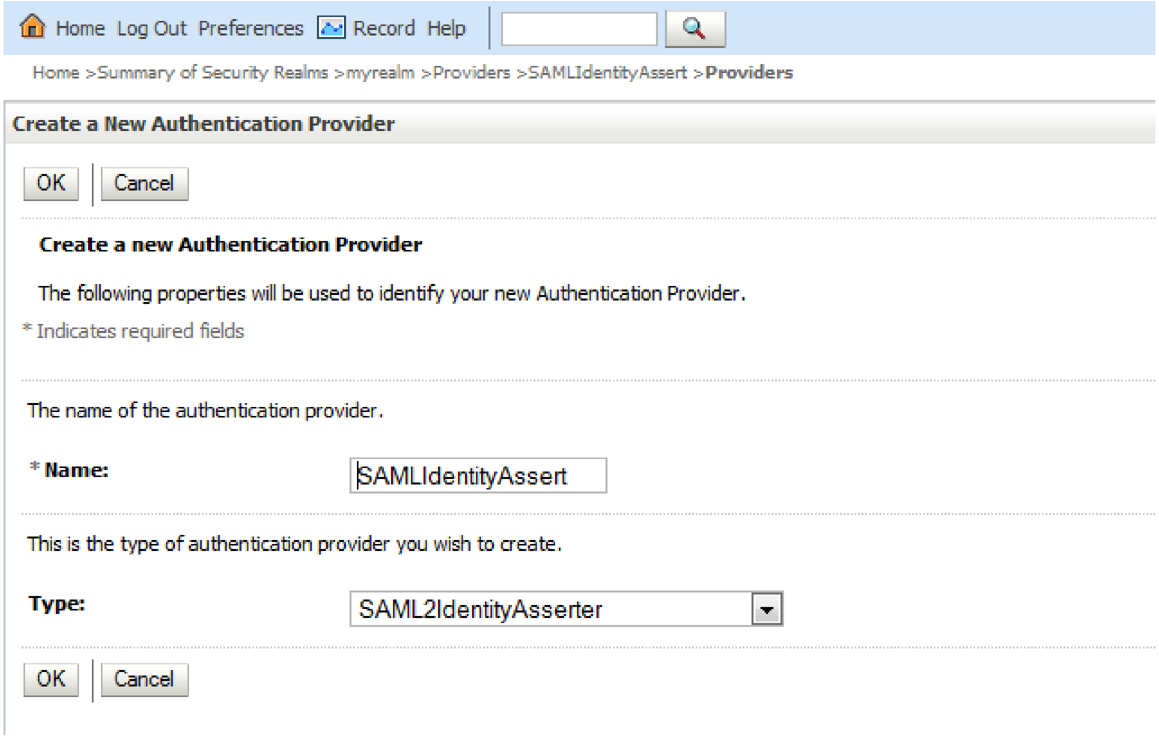
Figure 26. Weblogic Server – SSL Advanced Settings

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
OK
Cancel

Create a New Authentication Provider

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.

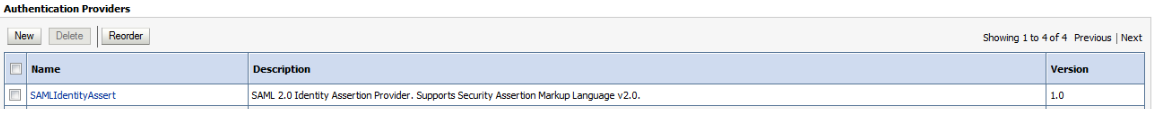
* Name: SAMLIdentityAssert

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

Type: SAML2IdentityAsserter

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.



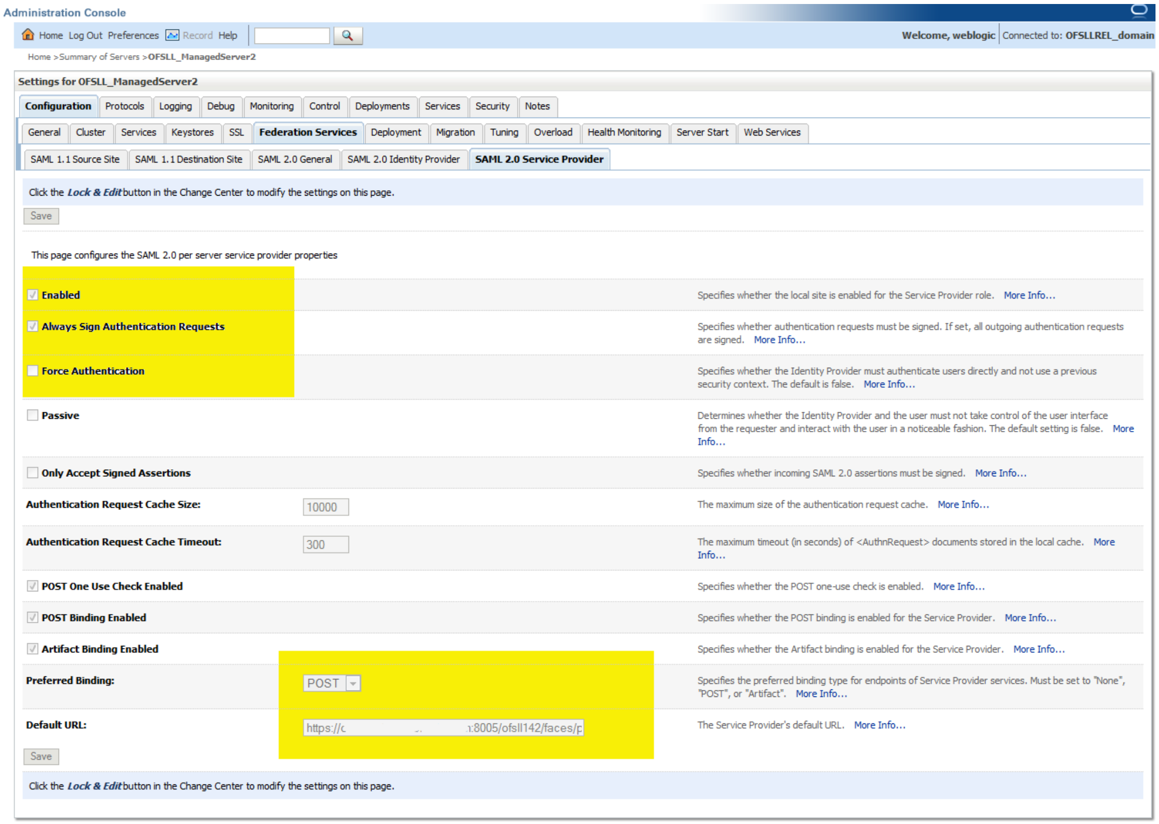
Authentication Providers

	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 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



Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic | Connected to: OFSLLREL_domain
Home >Summary of Servers >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
Save

Settings for OFSLL_ManagedServer2

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

This page configures the SAML 2.0 per server service provider properties

☑ Enabled		Specifies whether the local site is enabled for the Service Provider role. More Info...
☑ Always Sign Authentication Requests		Specifies whether authentication requests must be signed. If set, all outgoing authentication requests are signed. More Info...
□ Force Authentication		Specifies whether the Identity Provider must authenticate users directly and not use a previous security context. The default is false. More Info...
□ 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. More Info...
□ Only Accept Signed Assertions		Specifies whether incoming SAML 2.0 assertions must be signed. More Info...
Authentication Request Cache Size:	10000	The maximum size of the authentication request cache. More Info...
Authentication Request Cache Timeout:	300	The maximum timeout (in seconds) of <AuthnRequest> documents stored in the local cache. More Info...
☑ POST One Use Check Enabled		Specifies whether the POST one-use check is enabled. More Info...
☑ POST Binding Enabled		Specifies whether the POST binding is enabled for the Service Provider. More Info...
☑ Artifact Binding Enabled		Specifies whether the Artifact binding is enabled for the Service Provider. More Info...
Preferred Binding:	POST	Specifies the preferred binding type for endpoints of Service Provider services. Must be set to "None", "POST", or "Artifact". More Info...
Default URL:	https://c :8005/ofsll142/faces/p	The Service Provider's default URL. More Info...

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 → 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

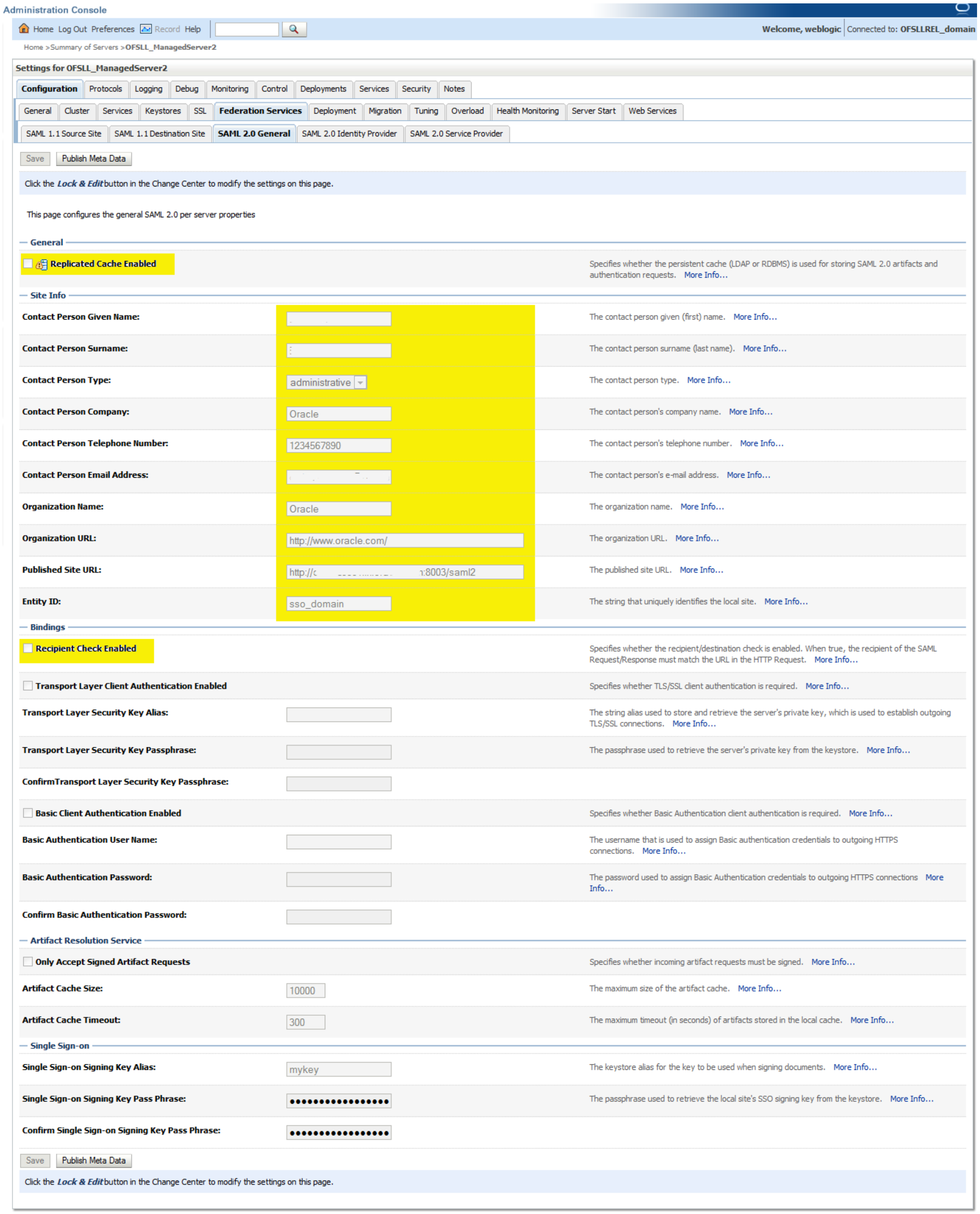
Note: this should not be checked for a single node managed server setup; only applicable for cluster setup.

  - 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



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
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 n: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...
ConfirmTransport 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...

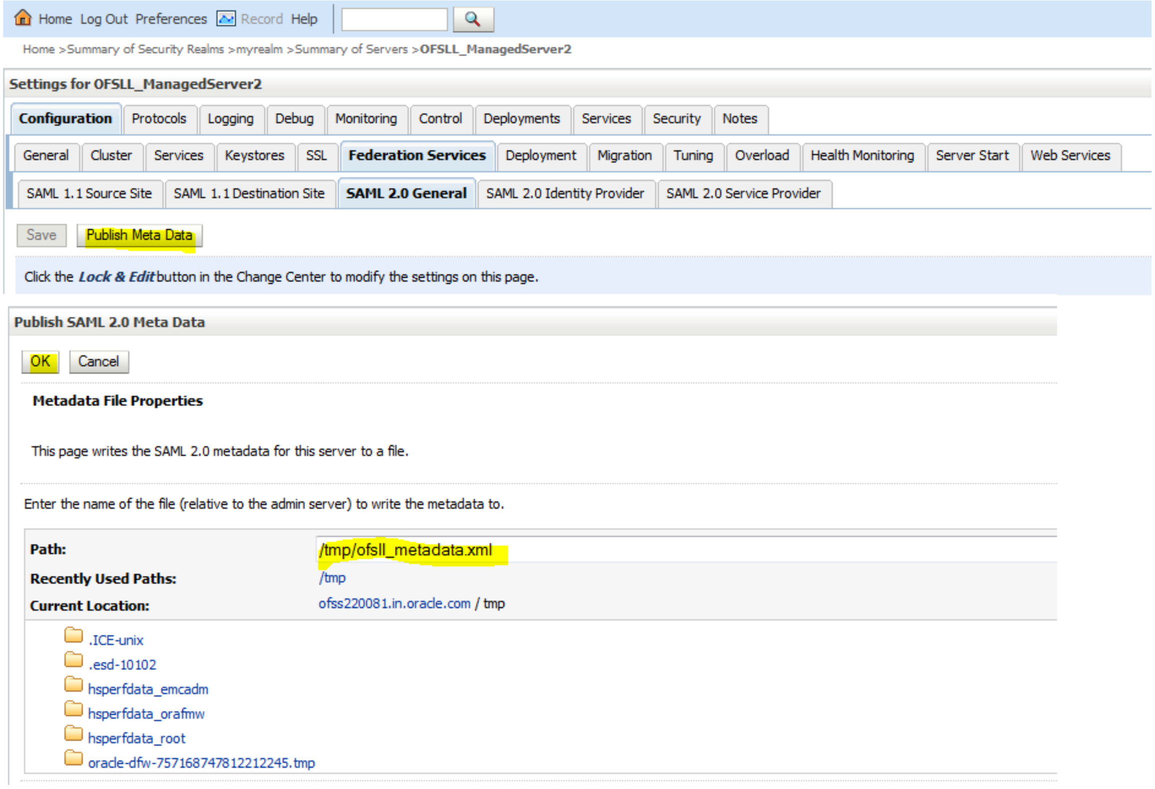
Single Sign-on

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:	•••••••••••••••••	

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 →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.



Home Log Out Preferences Record Help
Home >Summary of Security Realms >myrealm >Summary of Servers >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
Save Publish Meta Data
OK Cancel

Settings for OFSLL_ManagedServer2

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

Publish SAML 2.0 Meta Data

Metadata File Properties

This page writes the SAML 2.0 metadata for this server to a file.

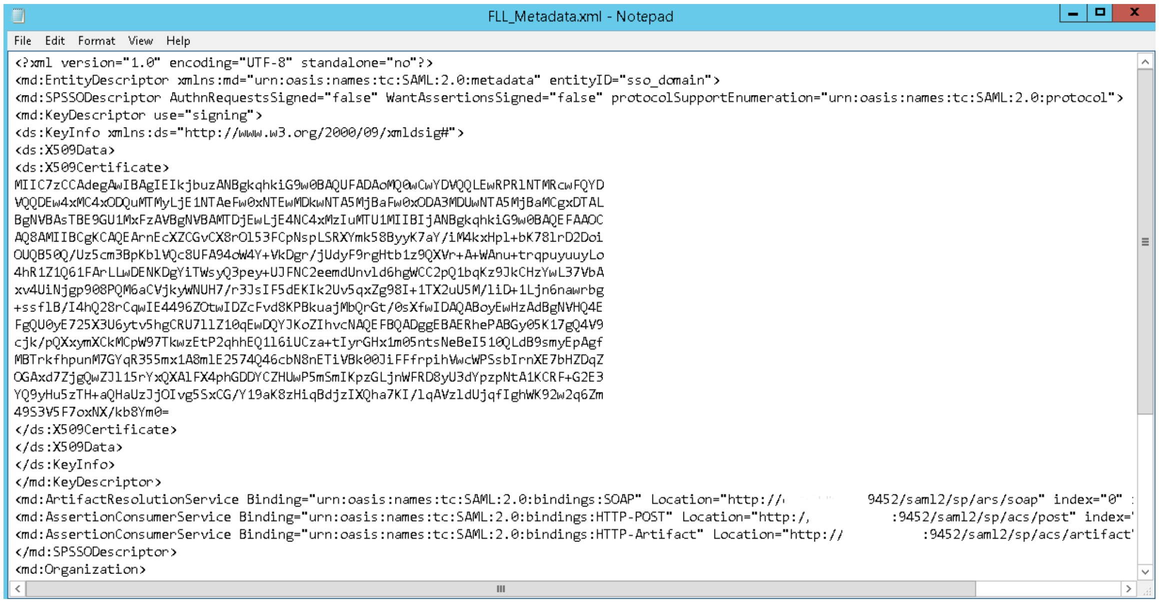
Enter the name of the file (relative to the admin server) to write the metadata to.

Path:	/tmp/ofsll_metadata.xml
Recently Used Paths:	/tmp
Current Location:	ofss220081.in.oracle.com / tmp

- .ICE-unix
- .esd-10102
- hsperfdata_emcadm
- hsperfdata_orafmw
- hsperfdata_root
- oracle-dfw-757168747812212245.tmp

Figure 31. Weblogic Server – Publish Meta Data

- The Published ofsll_metadata.xml file would look as below

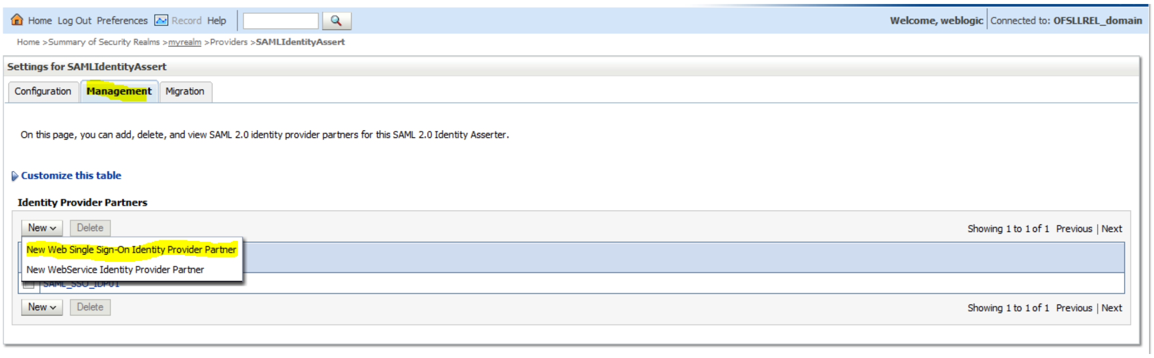


```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="sso_domain">
<md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIC7zCCAdegAwIBAgIEIkjbuzANBgkqhkiG9w0BAQUFADAoMQ0wCwYDVQQLEwRPRlNTMRcwFQYD
VQQDEw4xMC4xODQuMTMyLjE1NTAeFw0xNTEwMDkwNTA5MjBaFw0xODA3MDUwNTA5MjBaMCgxDTAL
BgNVBAsTBE9GU1MxFzAVBgNVBAMTDjEwLjE4NC4xMzIuMTU1MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEArnEcXZCGvCX8rOl53FCpNspLSRXYmk58ByyK7aY/iM4kxHpl+bK78lrD2Doi
OUQB50Q/Uz5cm3BpKblVQc8UFA94oW4Y+VkDgr/jUdyF9rgHtb1z9QXVr+A+WAnu+trqpuyuuyLo
4hR1Z1Q61FArLLwDENKDgYiTWsyQ3pey+UJFNC2eemdUnvld6hgWCC2pQ1bqKz9JkCHzYwL37VbA
xv4UiNjgp908PQM6aCVjkyWNUH7/r3JsIF5dEKIk2Uv5qxZg98I+1TX2uU5M/liD+1Ljn6nawrbg
+ssflB/I4hQ28rCqwIE4496ZOtwIDZcFvd8KPBkuajMbQrGt/0sXfwIDAQABoyEwHzAdBgNVHQ4E
FgQU0yE725X3U6ytv5hgCRU7llZ10qEwDQYJKoZIhvcNAQEFBQADggEBAERhePABGy05K17gQ4V9
cjk/pQXxymXCkMCpW97TkwzEtP2qhhEQ1l6iUCza+tIyrGHx1m05ntsNeBeI510QLdB9smyEpAgf
MBTrkfhpunM7GYqR355mx1A8mlE2574Q46cbN8nETiVBk00JiFFfrpihVwcWPSsbIrnXE7bHZDqZ
OGAxd7ZjgQwZJl15rYxQXAlFX4phGDDYCZHUwP5mSmIKpzGLjnWFRD8yU3dYpzpNtA1KCRF+G2E3
YQ9yHu5zTH+aQHaUzJjOIvg5SxCG/Y19aK8zHiqBdjzIXQha7KI/lqAVzldUjqfIghWK92w2q6Zm
49S3V5F7oxNX/kb8Ym0=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="http://      9452/saml2/sp/ars/soap" index="0" :
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http:/,        :9452/saml2/sp/acs/post" index='
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="http://        :9452/saml2/sp/acs/artifact'
</md:SPSSODescriptor>
<md:Organization>
```

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)


Home
Log Out
Preferences
Record
Help
Welcome, weblogic
Connected to: OFSLLREL_domain
Configuration
Management
Migration
Customize this table
New
Delete
New Web Single Sign-On Identity Provider Partner
New WebService Identity Provider Partner
Showing 1 to 1 of 1 Previous | Next

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

Settings for SAMLIdentityAssert

On this page, you can add, delete, and view SAML 2.0 identity provider partners for this SAML 2.0 Identity Asserter.

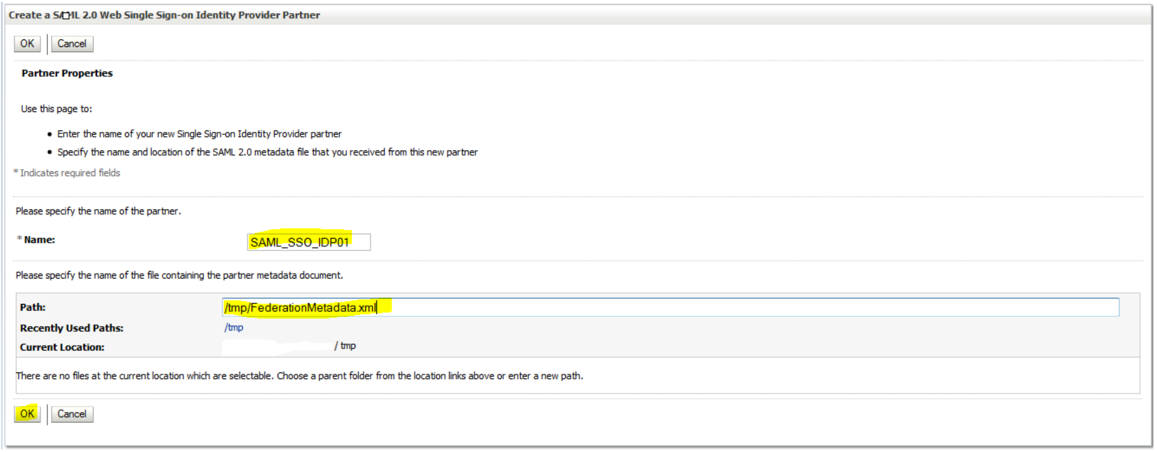
Identity Provider Partners

SAML_SSO_IDP01

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.



Create a SAML 2.0 Web Single Sign-on Identity Provider Partner

Partner Properties

Use this page to:

- Enter the name of your new Single Sign-on Identity Provider partner
- Specify the name and location of the SAML 2.0 metadata file that you received from this new partner

* Indicates required fields

Please specify the name of the partner.

* **Name:** SAML_SSO_IDP01

Please specify the name of the file containing the partner metadata document.

Path: /tmp/FederationMetadata.xml

Recently Used Paths: /tmp

Current Location: [redacted] / tmp

There are no files at the current location which are selectable. Choose a parent folder from the location links above or enter a new path.

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.

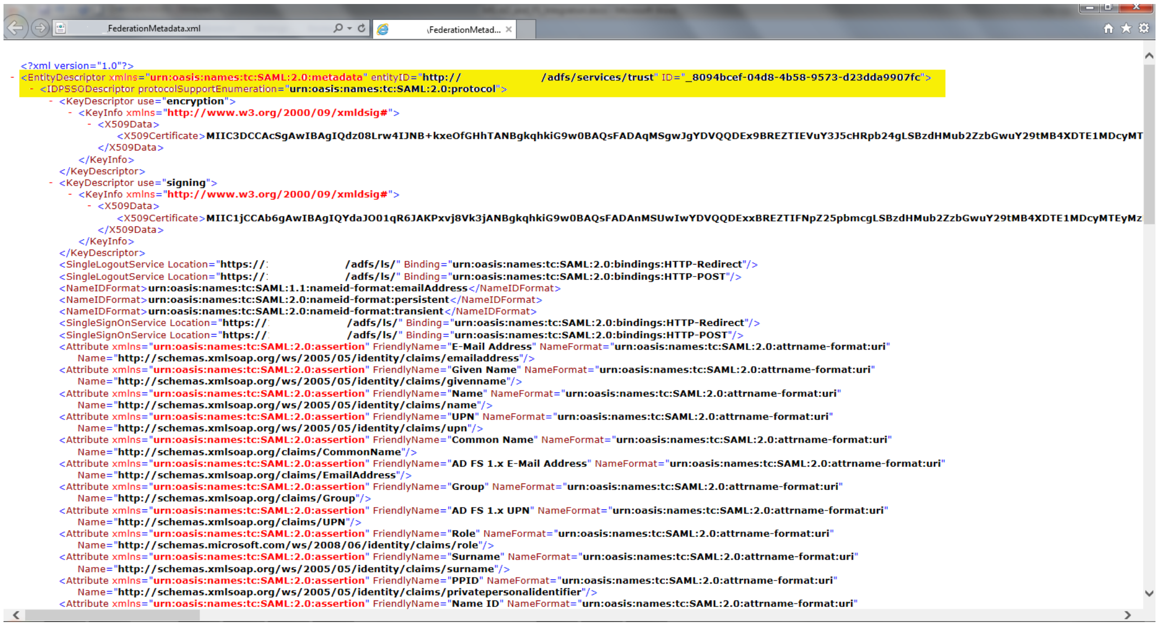
Remove the Service Provider metadata section from already edited Federation Metadata XML.

- 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…>

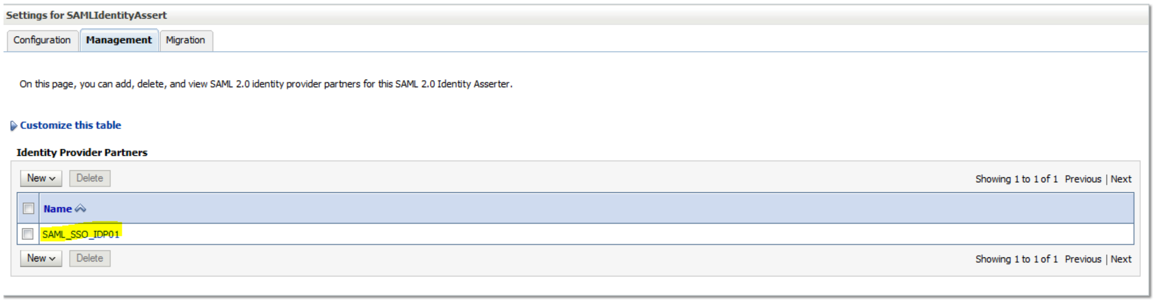


```
  <?xml version="1.0"?>
- <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://              /adfs/services/trust" ID="_8094bcef-04d8-4b58-9573-d23dda9907fc">
  - <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    - <KeyDescriptor use="encryption">
      - <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        - <X509Data>
            <X509Certificate>MIIC3DCCAcSgAwIBAgIQdz08Lrw4IJNB+kxeOfGHhTANBgkqhkiG9w0BAQsFADAqMSgwJgYDVQQDEx9BREZTIEVuY3J5cHRpb24gLSBzdHMub2ZzbGwuY29tMB4XDTE1MDcyMT
          </X509Data>
        </KeyInfo>
      </KeyDescriptor>
    - <KeyDescriptor use="signing">
      - <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        - <X509Data>
            <X509Certificate>MIIC1jCCAb6gAwIBAgIQYdaJO01qR6JAKPxvj8Vk3jANBgkqhkiG9w0BAQsFADAnMSUwIwYDVQQDExxBREZTIFNpZ25pbmcgLSBzdHMub2ZzbGwuY29tMB4XDTE1MDcyMTEyMz
          </X509Data>
        </KeyInfo>
      </KeyDescriptor>
      <SingleLogoutService Location="https://:              /adfs/ls/" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
      <SingleLogoutService Location="https://:              /adfs/ls/" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
      <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
      <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
      <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
      <SingleSignOnService Location="https://              /adfs/ls/" Binding="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-POST"/>
      <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/privatepersonalidentifier"/>
      <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="Name ID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
```

Figure 35. Modified Federation Metadata

» Save the file.

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



Settings for SAMLIdentityAssert

On this page, you can add, delete, and view SAML 2.0 identity provider partners for this SAML 2.0 Identity Asserter.

Identity Provider Partners

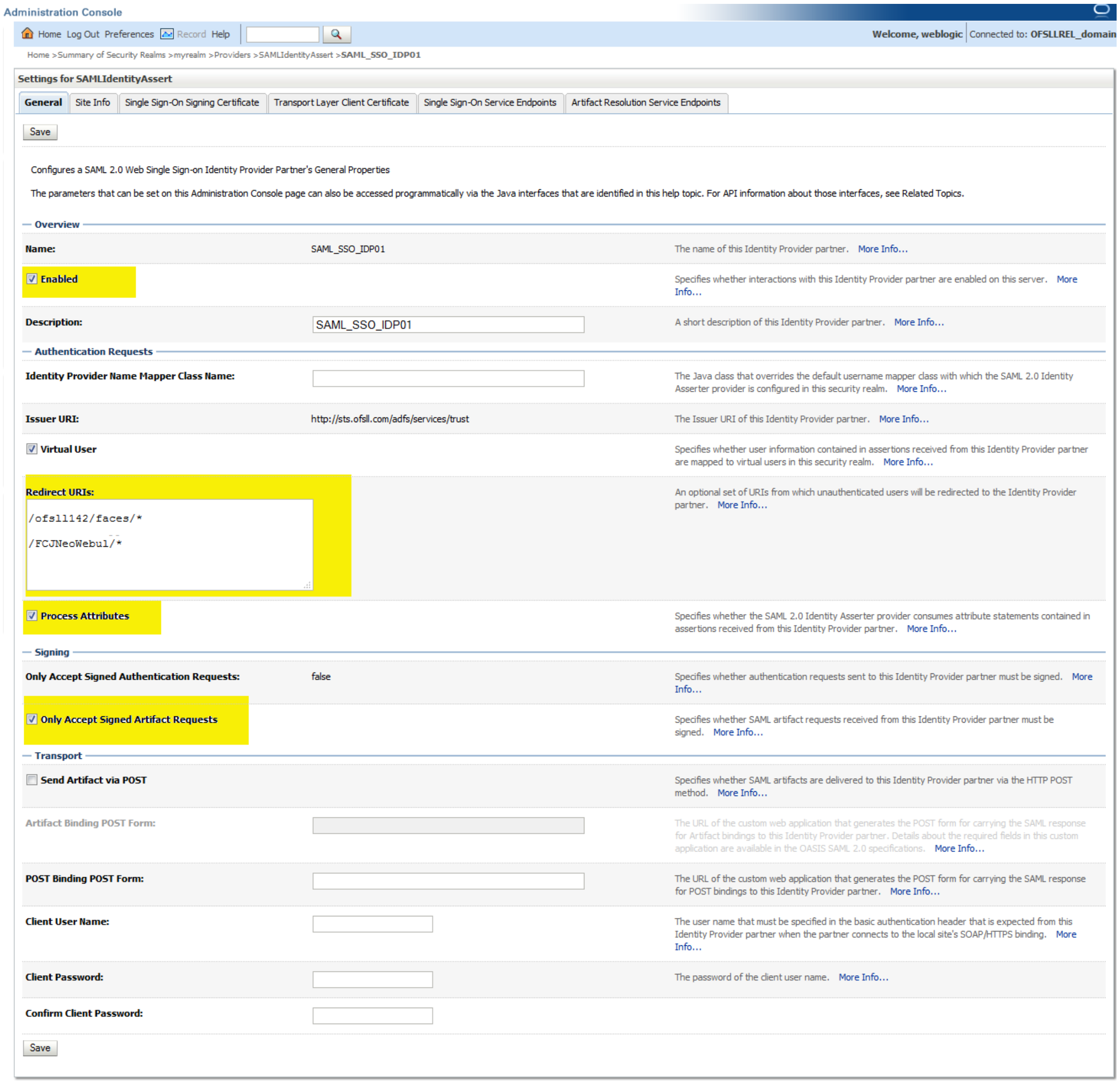
□	Name
□	SAML_SSO_IDP01

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



Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic | Connected to: OFSLLREL_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

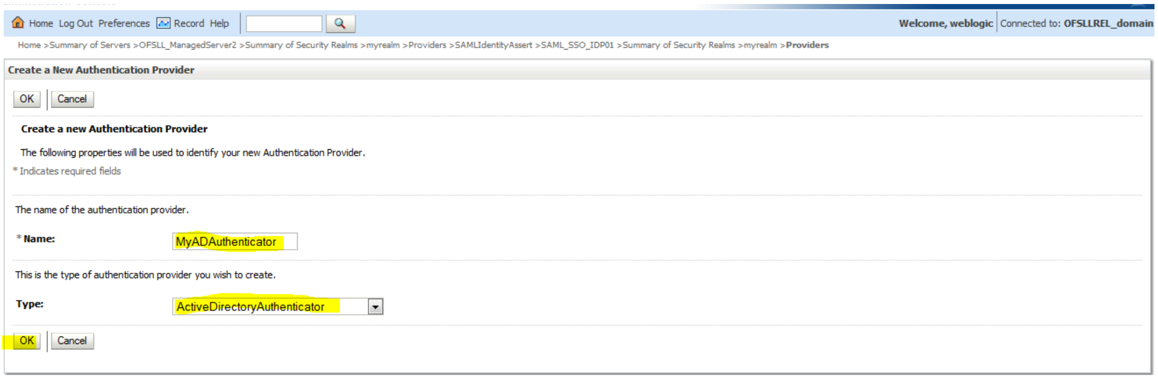
The parameters that can be set on this Administration Console page can also be accessed programmatically via the Java interfaces that are identified in this help topic. For API information about those interfaces, see Related Topics.

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: /ofsll142/faces/* /FCJNeoWebul/*		An optional set of URIs from which unauthenticated users will be redirected to the Identity Provider partner. More Info...
☑ **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:		

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



Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: OFSLLREL_domain
Home >Summary of Servers >OFSLL_ManagedServer2 >Summary of Security Realms >myrealm >Providers >SAMLIdentityAssert >SAML_SSO_IDP01 >Summary of Security Realms >myrealm >Providers
OK
Cancel

Create a New Authentication Provider

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:** MyADAuthenticator

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

Type: ActiveDirectoryAuthenticator

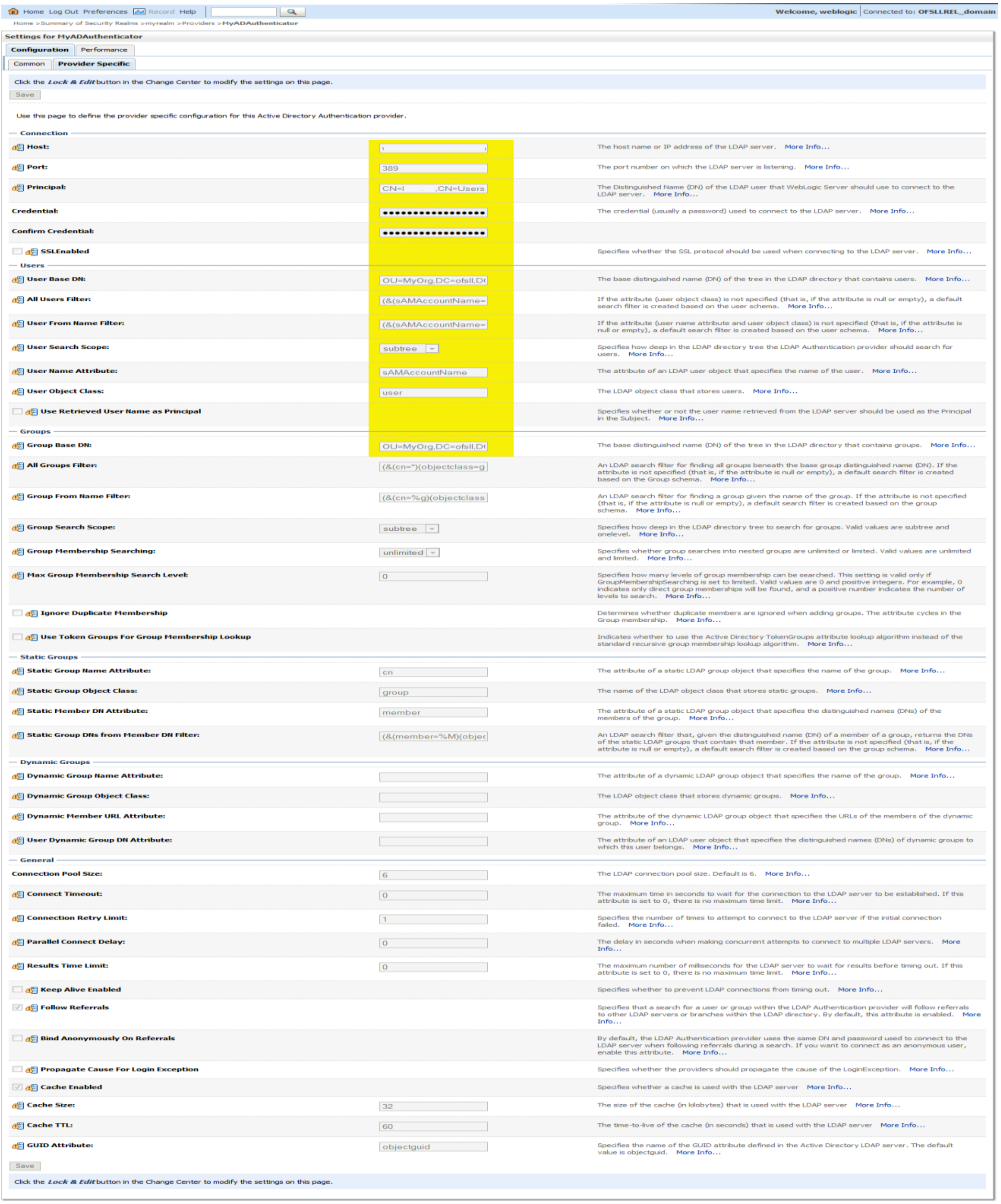
Figure 38. Weblogic Domain – New Authentication Provider

- 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


Home Log Out Preferences Record Help
Welcome, weblogic | Connected to: OFSLLREL_domain
Home >Summary of Security Realms >myrealm >Providers >MyADAuthenticator
Configuration
Performance
Common
Provider Specific
Save

Settings for MyADAuthenticator

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

Use this page to define the provider specific configuration for this Active Directory Authentication provider.

Connection

Host:		The host name or IP address of the LDAP server. More Info...
Port:	389	The port number on which the LDAP server is listening. More Info...
Principal:	CN=I ,CN=Users	The Distinguished Name (DN) of the LDAP user that WebLogic Server should use to connect to the LDAP server. More Info...
Credential:	••••••••••••••••••	The credential (usually a password) used to connect to the LDAP server. More Info...
Confirm Credential:	••••••••••••••••••	
□ SSLEnabled		Specifies whether the SSL protocol should be used when connecting to the LDAP server. More Info...

Users

User Base DN:	OU=MyOrg,DC=ofsll,D(	The base distinguished name (DN) of the tree in the LDAP directory that contains users. More Info...
All Users Filter:	(&(sAMAccountName=	If the attribute (user object class) is not specified (that is, if the attribute is null or empty), a default search filter is created based on the user schema. More Info...
User From Name Filter:	(&(sAMAccountName=	If the attribute (user name attribute and user object class) is not specified (that is, if the attribute is null or empty), a default search filter is created based on the user schema. More Info...
User Search Scope:	subtree	Specifies how deep in the LDAP directory tree the LDAP Authentication provider should search for users. More Info...
User Name Attribute:	sAMAccountName	The attribute of an LDAP user object that specifies the name of the user. More Info...
User Object Class:	user	The LDAP object class that stores users. More Info...
□ Use Retrieved User Name as Principal		Specifies whether or not the user name retrieved from the LDAP server should be used as the Principal in the Subject. More Info...

Groups

Group Base DN:	OU=MyOrg,DC=ofsll,D(	The base distinguished name (DN) of the tree in the LDAP directory that contains groups. More Info...
All Groups Filter:	(&(cn=*)(objectclass=g	An LDAP search filter for finding all groups beneath the base group distinguished name (DN). If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the Group schema. More Info...
Group From Name Filter:	(&(cn=%g)(objectclass	An LDAP search filter for finding a group given the name of the group. If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the group schema. More Info...
Group Search Scope:	subtree	Specifies how deep in the LDAP directory tree to search for groups. Valid values are subtree and onelevel. More Info...
Group Membership Searching:	unlimited	Specifies whether group searches into nested groups are unlimited or limited. Valid values are unlimited and limited. More Info...
Max Group Membership Search Level:	0	Specifies how many levels of group membership can be searched. This setting is valid only if GroupMembershipSearching is set to limited. Valid values are 0 and positive integers. For example, 0 indicates only direct group memberships will be found, and a positive number indicates the number of levels to search. More Info...
□ Ignore Duplicate Membership		Determines whether duplicate members are ignored when adding groups. The attribute cycles in the Group membership. More Info...
□ Use Token Groups For Group Membership Lookup		Indicates whether to use the Active Directory TokenGroups attribute lookup algorithm instead of the standard recursive group membership lookup algorithm. More Info...

Static Groups

Static Group Name Attribute:	cn	The attribute of a static LDAP group object that specifies the name of the group. More Info...
Static Group Object Class:	group	The name of the LDAP object class that stores static groups. More Info...
Static Member DN Attribute:	member	The attribute of a static LDAP group object that specifies the distinguished names (DNs) of the members of the group. More Info...
Static Group DNs from Member DN Filter:	(&(member=%M)(objec	An LDAP search filter that, given the distinguished name (DN) of a member of a group, returns the DNs of the static LDAP groups that contain that member. If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the group schema. More Info...

Dynamic Groups

Dynamic Group Name Attribute:		The attribute of a dynamic LDAP group object that specifies the name of the group. More Info...
Dynamic Group Object Class:		The LDAP object class that stores dynamic groups. More Info...
Dynamic Member URL Attribute:		The attribute of the dynamic LDAP group object that specifies the URLs of the members of the dynamic group. More Info...
User Dynamic Group DN Attribute:		The attribute of an LDAP user object that specifies the distinguished names (DNs) of dynamic groups to which this user belongs. More Info...

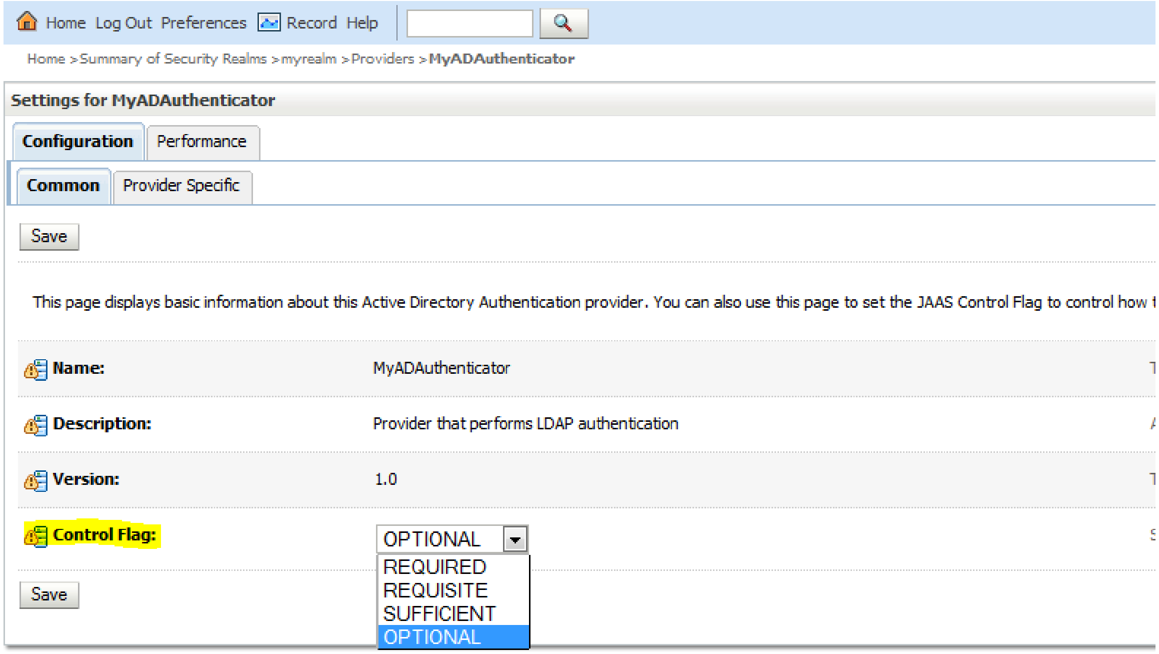
General

Connection Pool Size:	6	The LDAP connection pool size. Default is 6. More Info...
Connect Timeout:	0	The maximum time in seconds to wait for the connection to the LDAP server to be established. If this attribute is set to 0, there is no maximum time limit. More Info...
Connection Retry Limit:	1	Specifies the number of times to attempt to connect to the LDAP server if the initial connection failed. More Info...
Parallel Connect Delay:	0	The delay in seconds when making concurrent attempts to connect to multiple LDAP servers. More Info...
Results Time Limit:	0	The maximum number of milliseconds for the LDAP server to wait for results before timing out. If this attribute is set to 0, there is no maximum time limit. More Info...
□ Keep Alive Enabled		Specifies whether to prevent LDAP connections from timing out. More Info...
☑ Follow Referrals		Specifies that a search for a user or group within the LDAP Authentication provider will follow referrals to other LDAP servers or branches within the LDAP directory. By default, this attribute is enabled. More Info...
□ Bind Anonymously On Referrals		By default, the LDAP Authentication provider uses the same DN and password used to connect to the LDAP server when following referrals during a search. If you want to connect as an anonymous user, enable this attribute. More Info...
□ Propagate Cause For Login Exception		Specifies whether the providers should propagate the cause of the LoginException. More Info...
☑ Cache Enabled		Specifies whether a cache is used with the LDAP server More Info...
Cache Size:	32	The size of the cache (in kilobytes) that is used with the LDAP server More Info...
Cache TTL:	60	The time-to-live of the cache (in seconds) that is used with the LDAP server More Info...
GUID Attribute:	objectguid	Specifies the name of the GUID attribute defined in the Active Directory LDAP server. The default value is objectguid. More Info...

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


Home Log Out Preferences Record Help
Home >Summary of Security Realms >myrealm >Providers >MyADAuthenticator
Configuration
Performance
Common
Provider Specific
Save
REQUIRED
REQUISITE
SUFFICIENT
OPTIONAL
Save

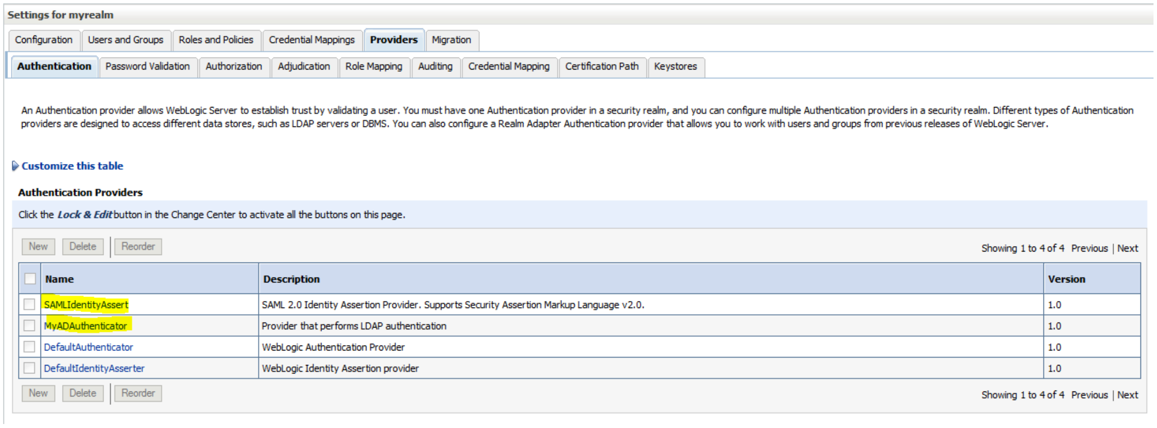
Settings for MyADAuthenticator

This page displays basic information about this Active Directory Authentication provider. You can also use this page to set the JAAS Control Flag to control how t

Name:	MyADAuthenticator
Description:	Provider that performs LDAP authentication
Version:	1.0
Control Flag:	OPTIONAL

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



Settings for myrealm

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS. You can also configure a Realm Adapter Authentication provider that allows you to work with users and groups from previous releases of WebLogic Server.

Authentication Providers

Click the ***Lock & Edit*** button in the Change Center to activate all the buttons on this page.

□	Name	Description	Version
□	SAMLIdentityAssert	SAML 2.0 Identity Assertion Provider. Supports Security Assertion Markup Language v2.0.	1.0
□	MyADAuthenticator	Provider that performs LDAP authentication	1.0
□	DefaultAuthenticator	WebLogic Authentication Provider	1.0
□	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

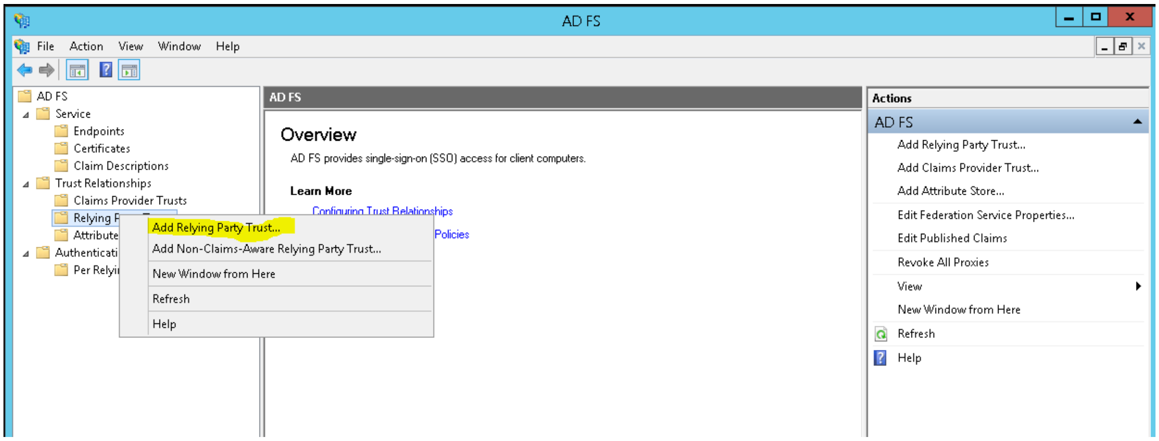
Figure 41. Weblogic Domain –Authentication Provider Order

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

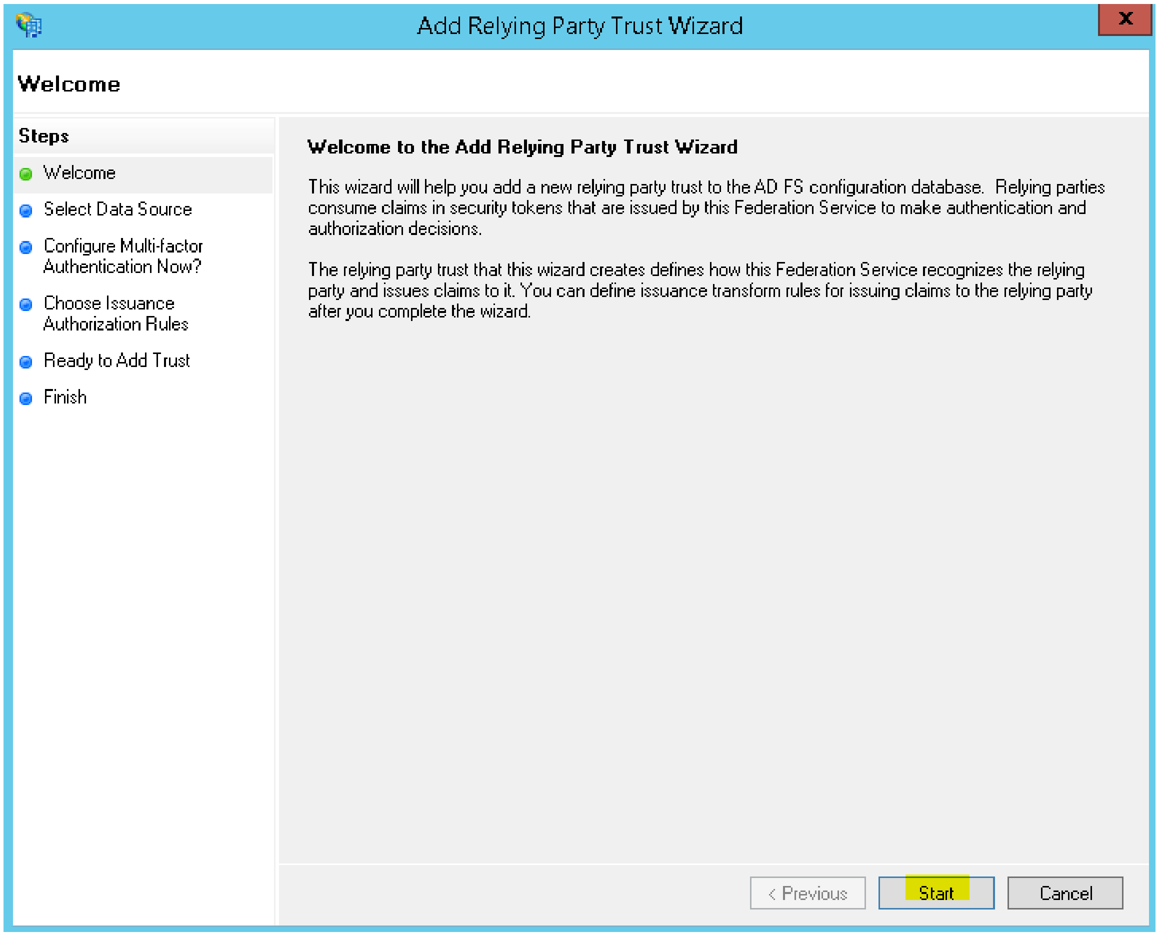
» On AD Server, open AD FS Management Console from Server Management Console → Tools → ADFS Management



AD FS provides single-sign-on (SSO) access for client computers.

Figure 42. AD FS Server – Relying Party Trust

- Click start on the Welcome Page



Add Relying Party Trust Wizard
Welcome
Steps
Welcome
Select Data Source
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
< Previous
Start
Cancel

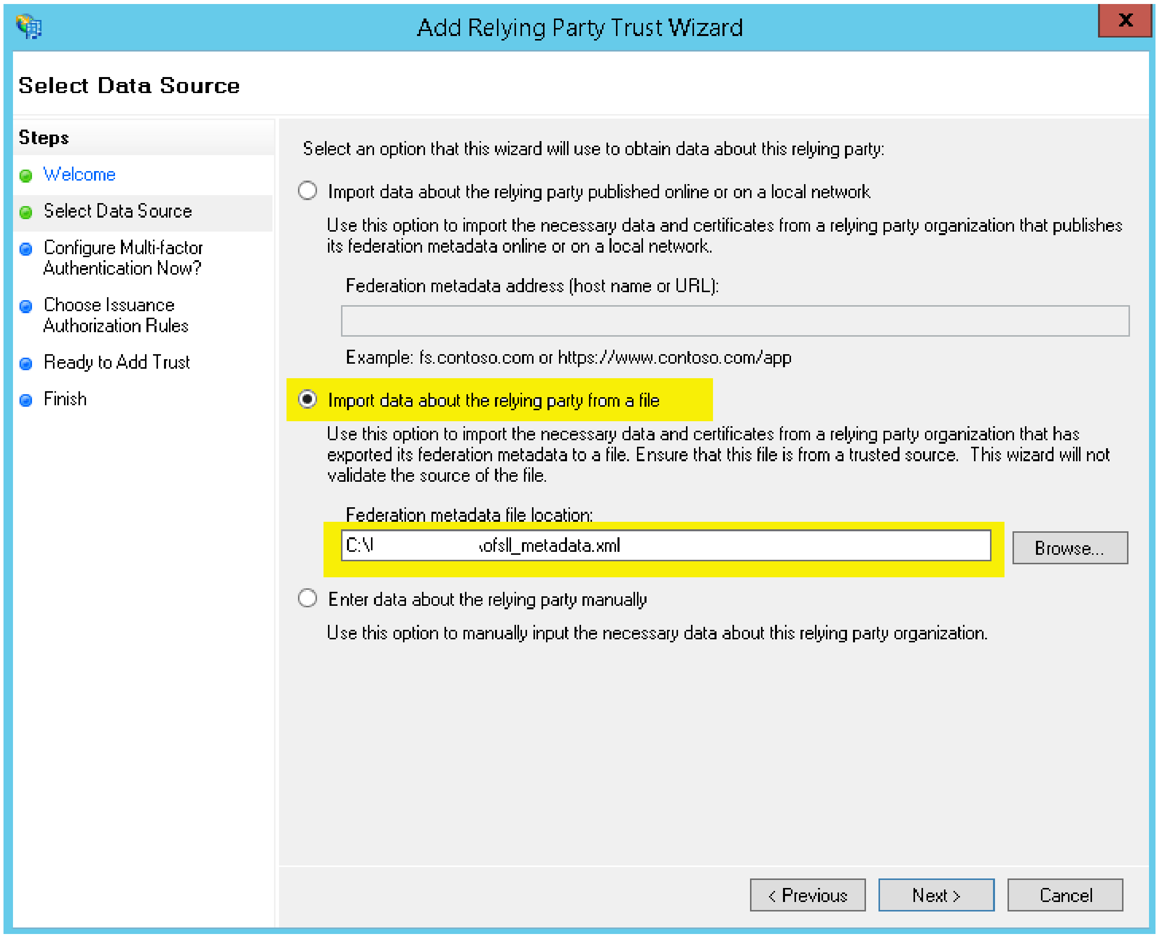
Welcome to the Add Relying Party Trust Wizard

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

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

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



Add Relying Party Trust Wizard

Select Data Source

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

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

● Import data about the relying party from a file

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

Federation metadata file location:

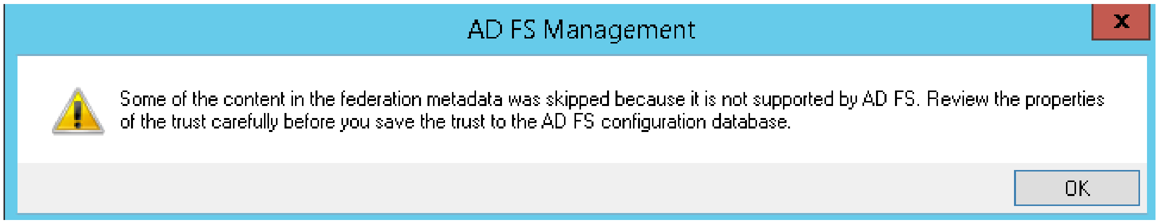
C:\ \ofsll_metadata.xml

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

Figure 44. AD FS Server – Define the metadata source

- Click “Ok” on below message

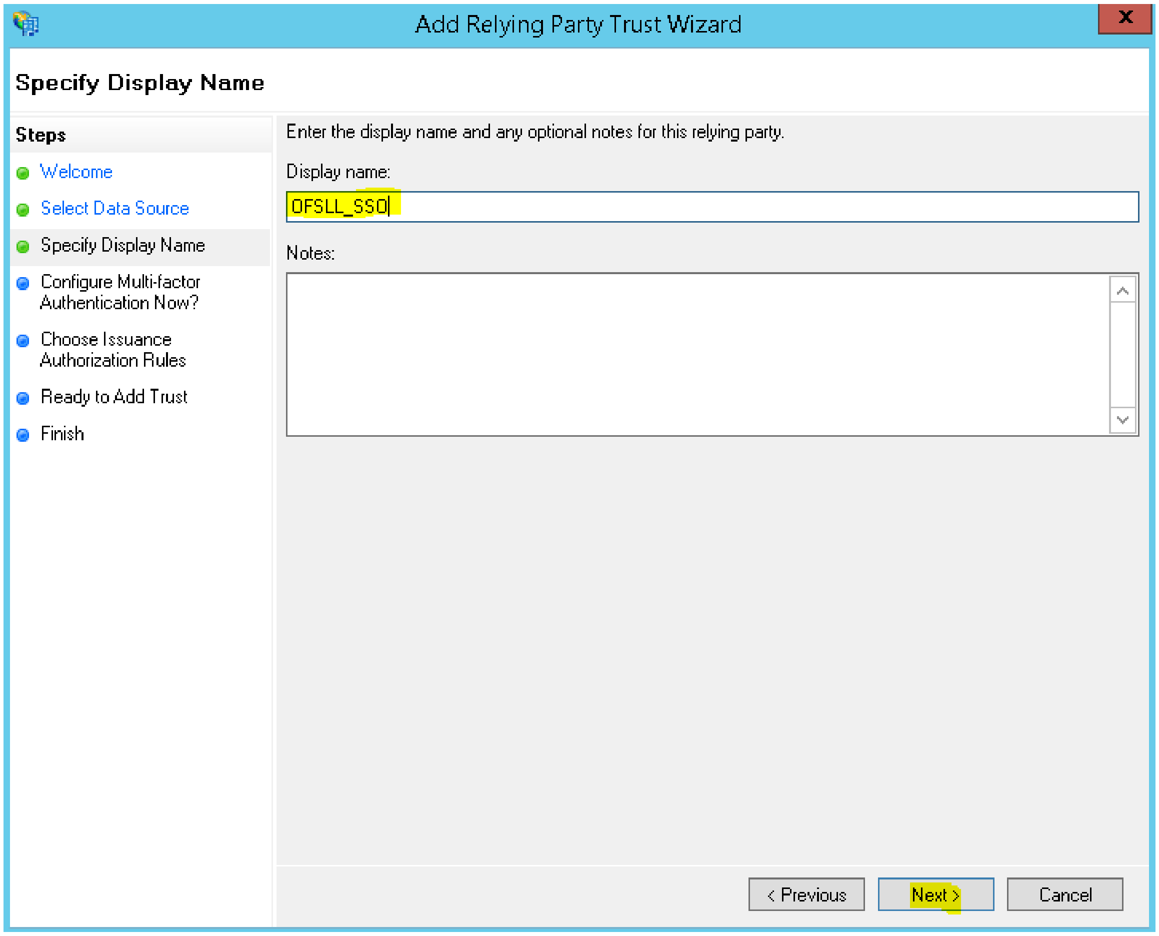


AD FS Management

Some of the content in the federation metadata was skipped because it is not supported by AD FS. Review the properties of the trust carefully before you save the trust to the AD FS configuration database.

Figure 45. AD FS Server – Warning Message

» Provide an unique Display Name and click Next



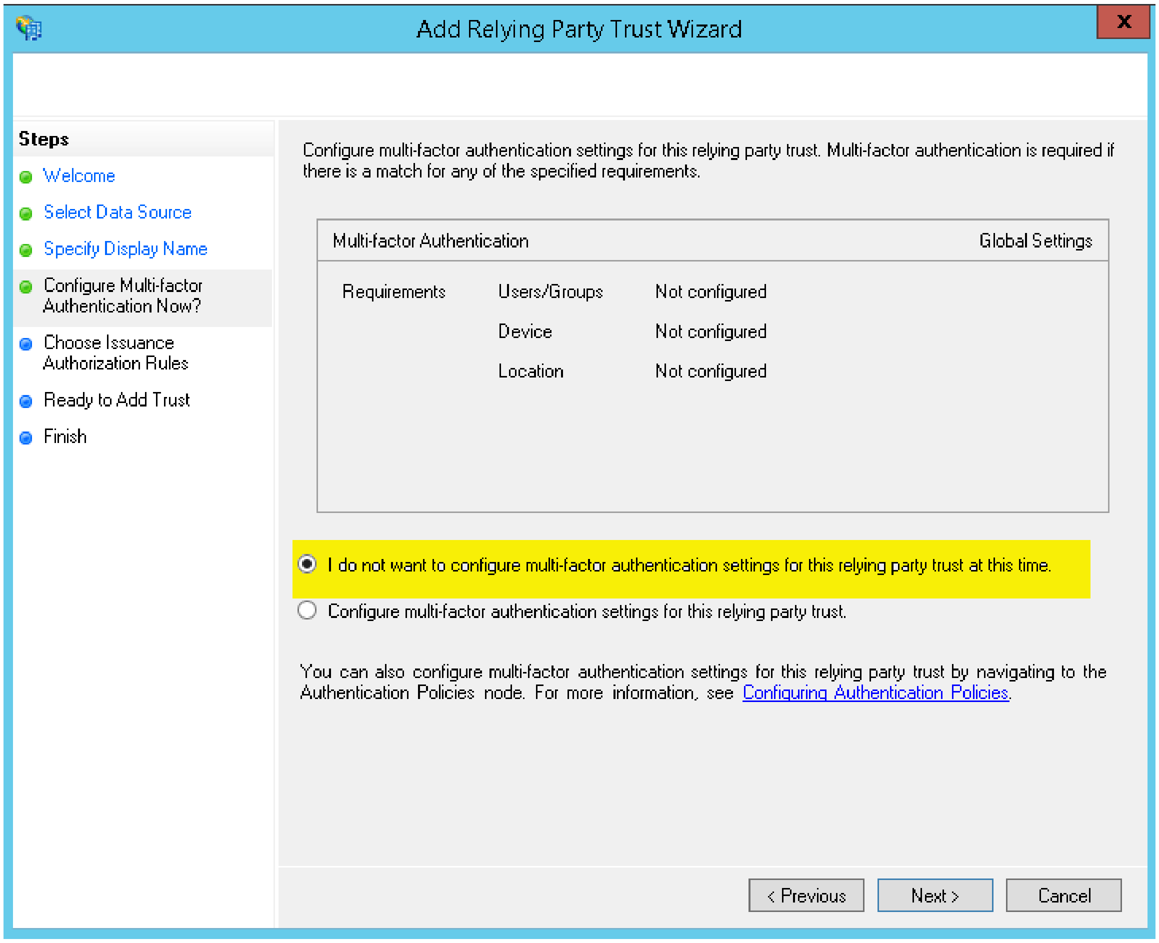
Enter the display name and any optional notes for this relying party.

Display name: OFSLL_SSO

Notes:

Figure 46. AD FS Server – Relying Party Display Name

- Retain the default as shown below and continue Next



Add Relying Party Trust Wizard
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

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

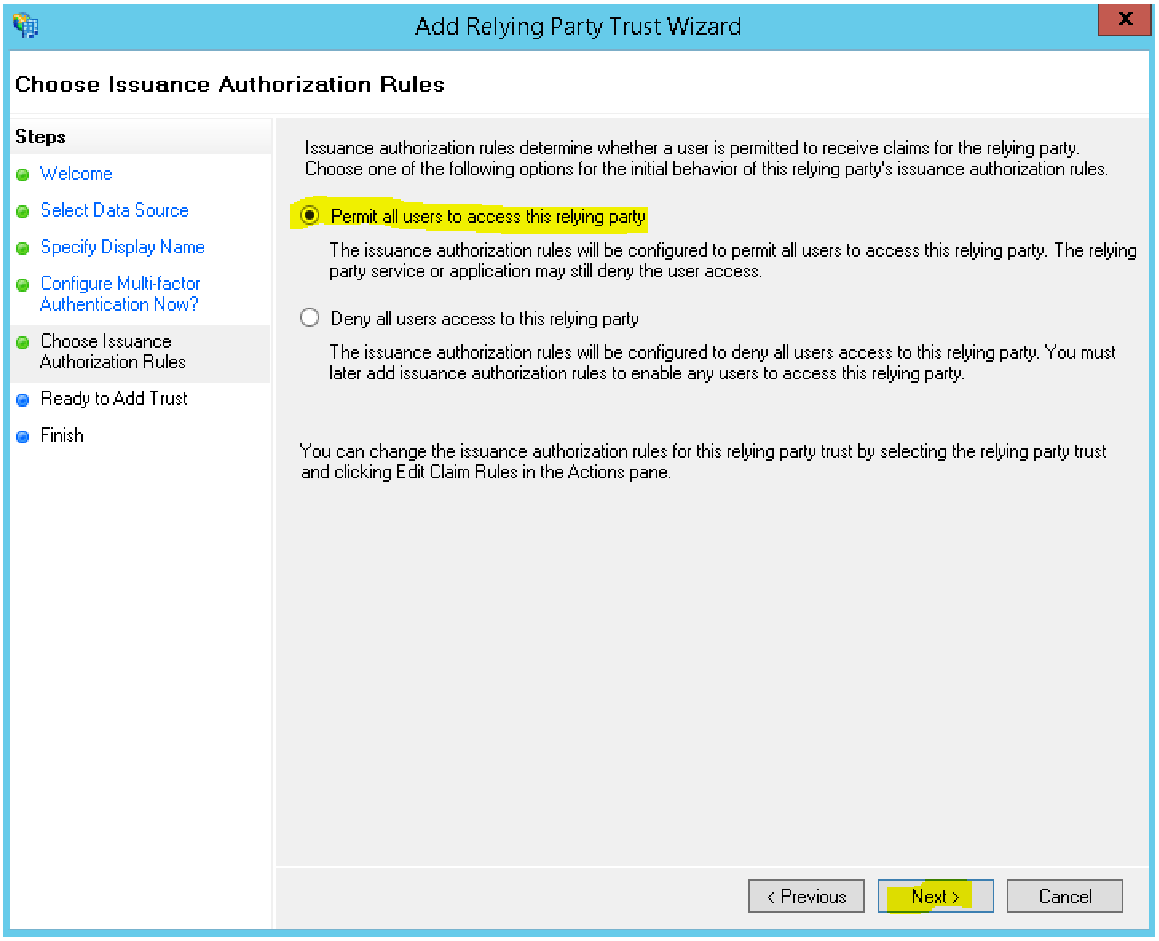
● I do not want to configure multi-factor authentication settings for this relying party trust at this time.

○ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see Configuring Authentication Policies.

Figure 47. AD FS Server – Multi-factor Authentication

» Retain the default as shown below and continue Next



Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

Steps

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

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

● Permit all users to access this relying party

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

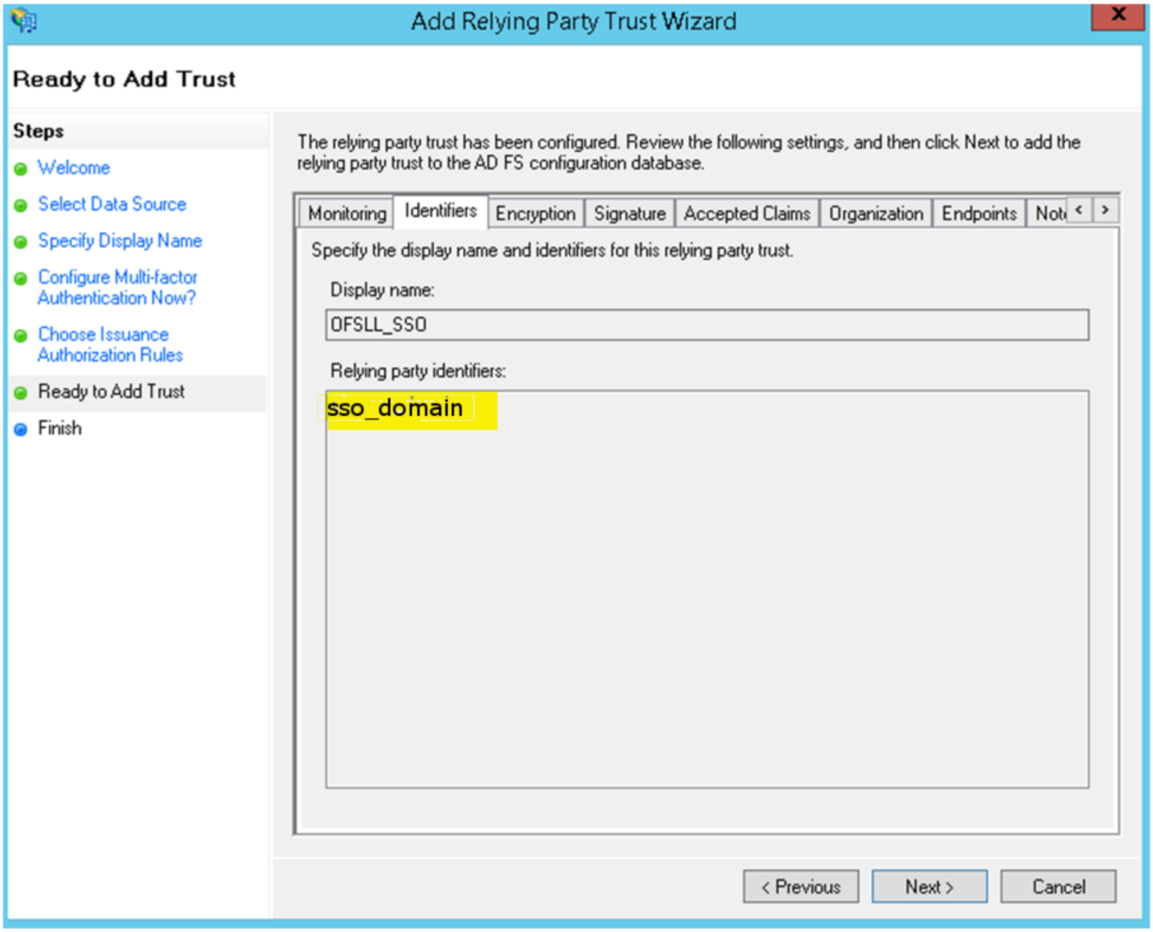
○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

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



The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

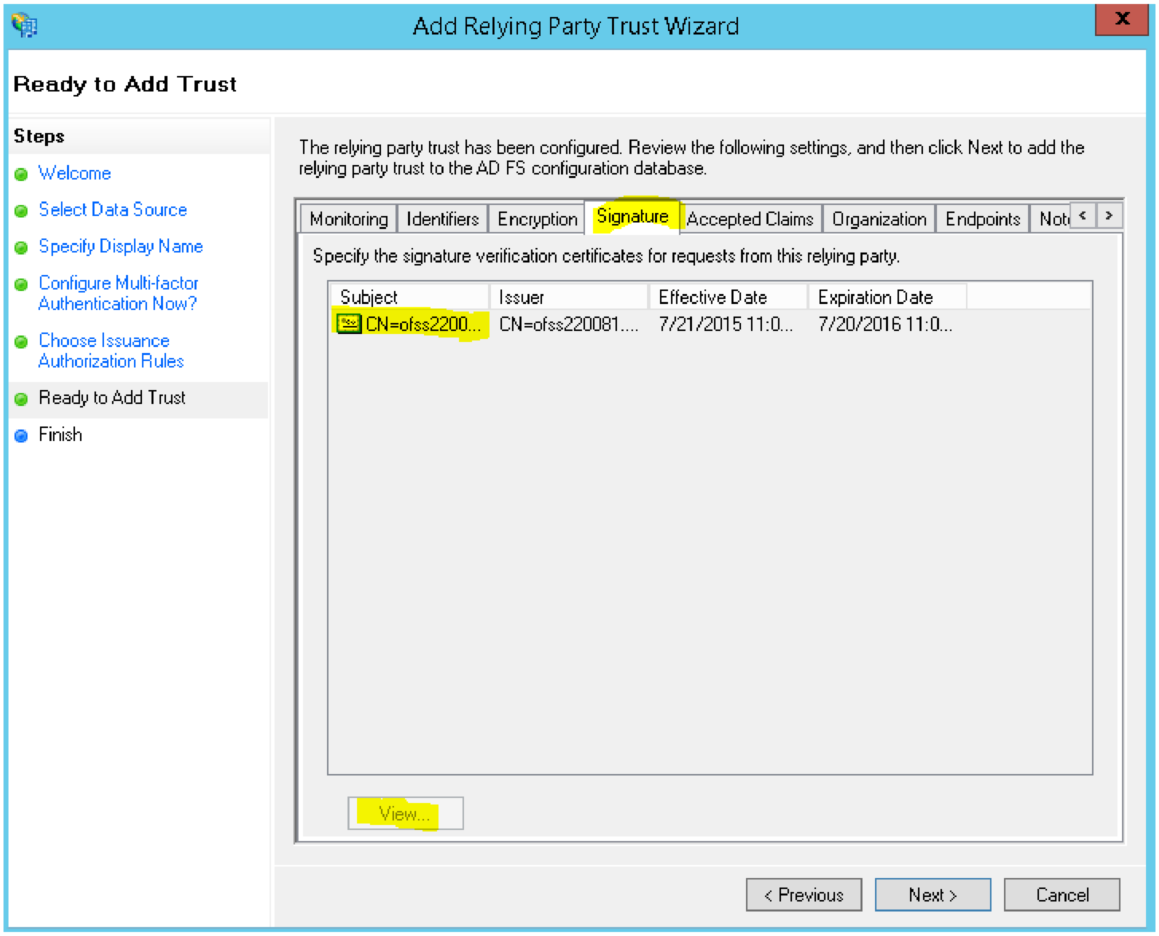
Specify the display name and identifiers for this relying party trust.

Display name: OFSLL_SSO

Relying party identifiers: sso_domain

Figure 49. AD FS Server – Identifiers Tab

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



Add Relying Party Trust Wizard

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

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

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

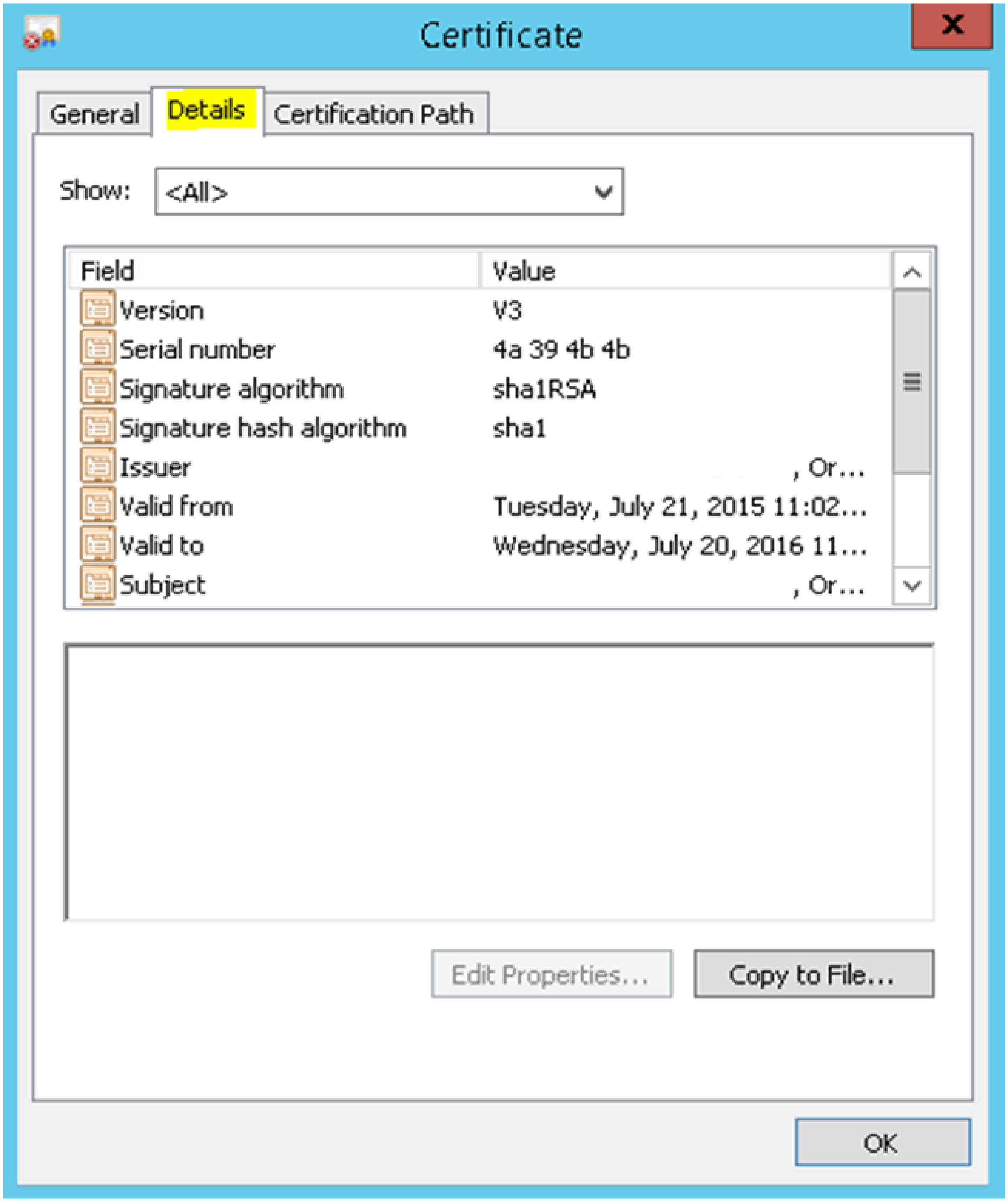
Specify the signature verification certificates for requests from this relying party.

Subject	Issuer	Effective Date	Expiration Date
CN=ofss2200...	CN=ofss220081....	7/21/2015 11:0...	7/20/2016 11:0...

View...
< Previous
Next >
Cancel

Figure 50. AD FS Server – Signature Tab

- Certificate details can be reviewed



Show: <All>

Field	Value
Version	V3
Serial number	4a 39 4b 4b
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	, Or…
Valid from	Tuesday, July 21, 2015 11:02…
Valid to	Wednesday, July 20, 2016 11…
Subject	, Or…

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”

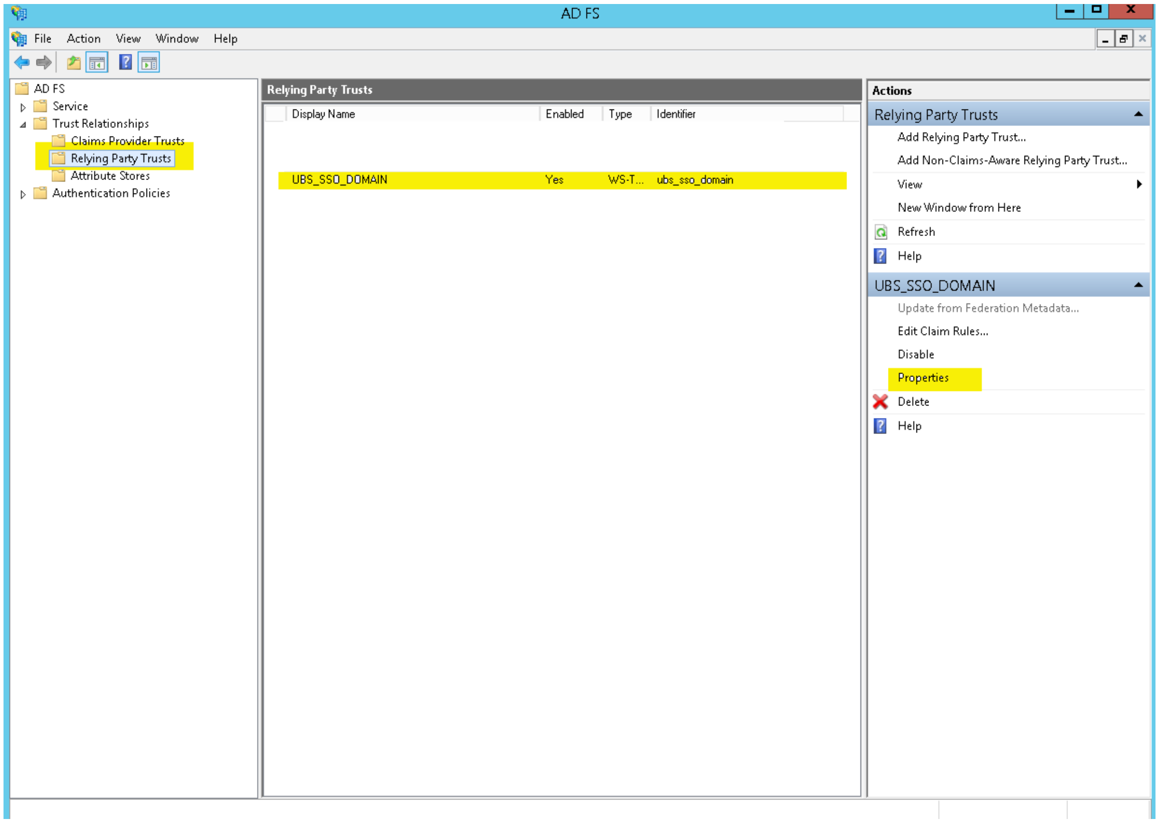
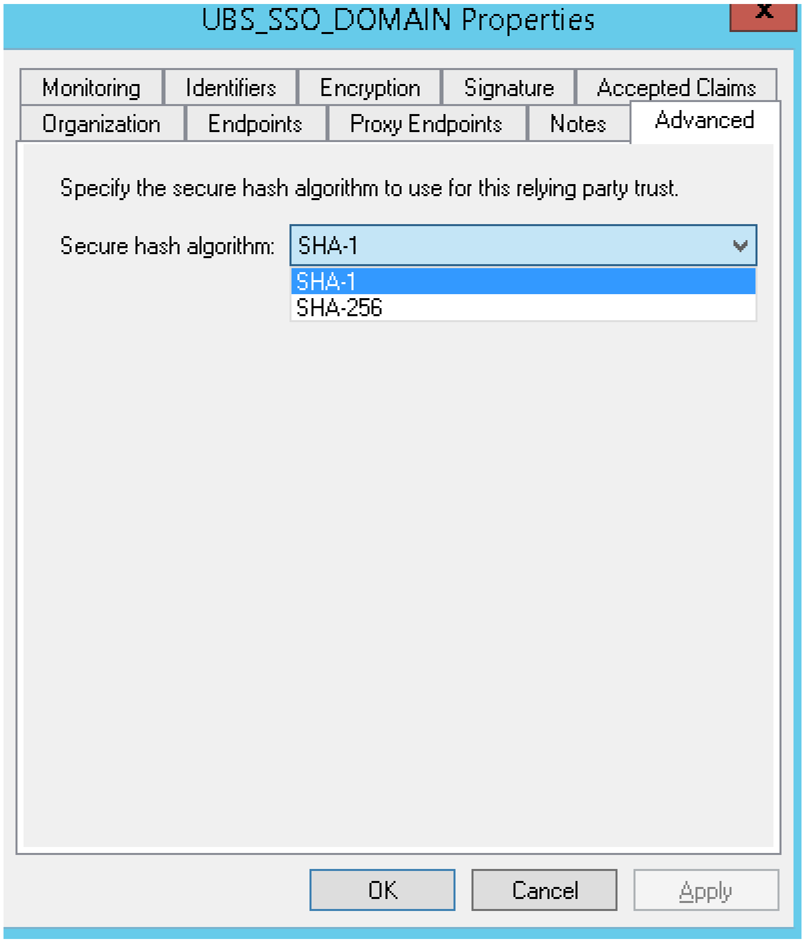


Figure 52. AD FS Server – Edit Relying Party Trust

» 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



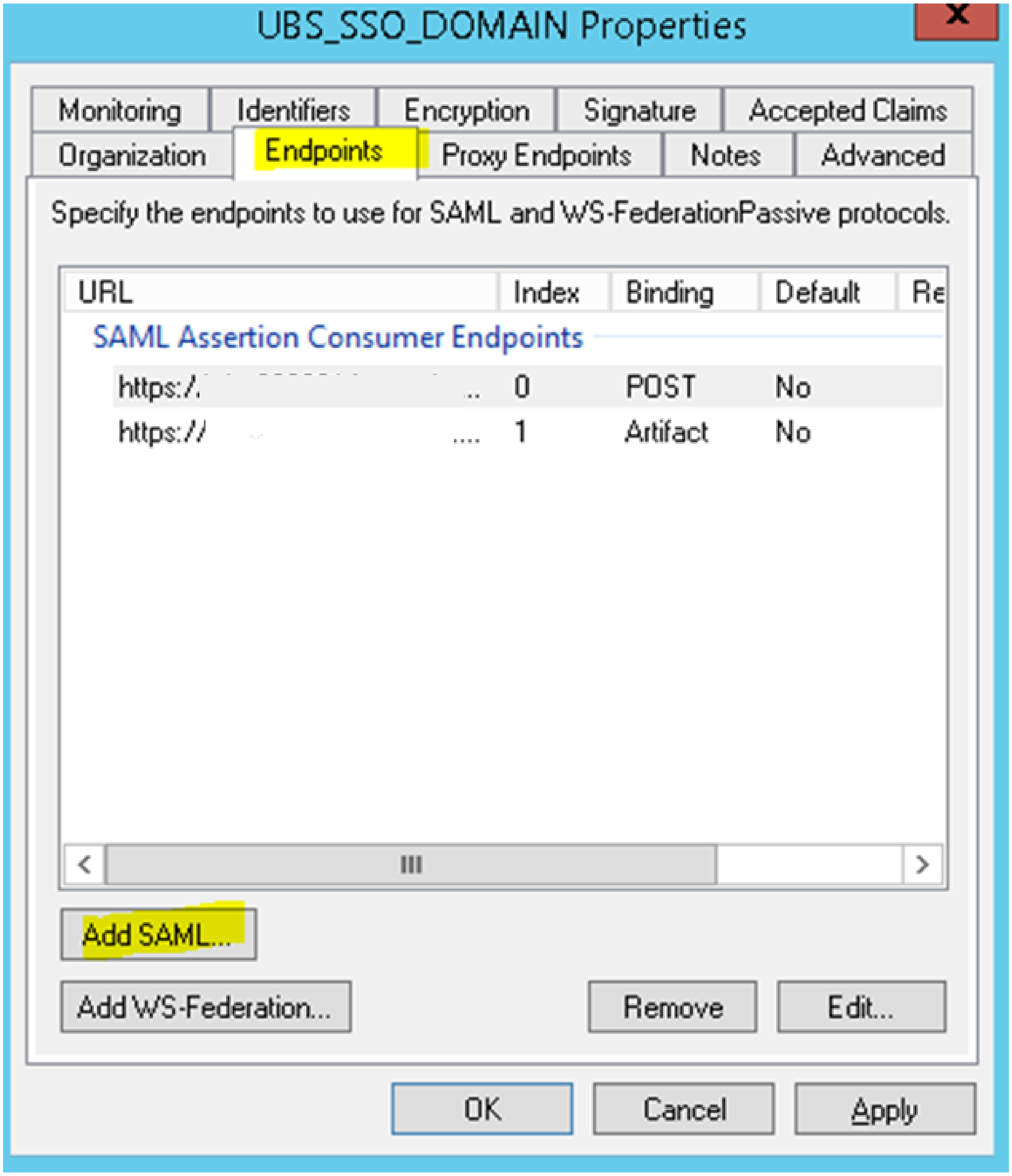
Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-1

SHA-1
SHA-256

Figure 53. AD FS Relying Party – Advanced Tab

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

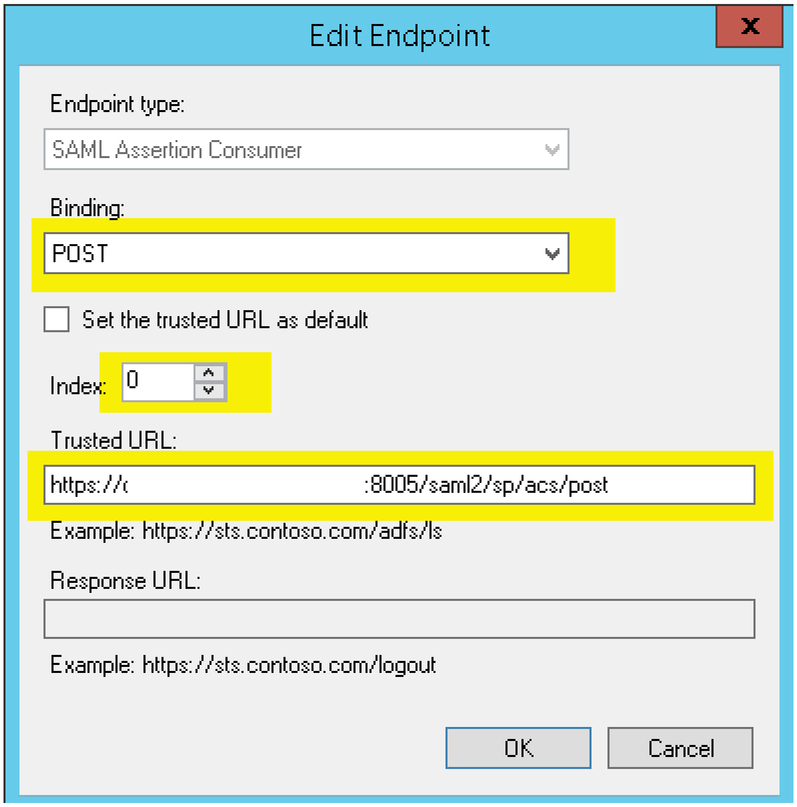


Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https:/. ...	0	POST	No	
https://	1	Artifact	No	

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



Endpoint type: SAML Assertion Consumer

Binding: POST

☐ Set the trusted URL as default

Index: 0

Trusted URL: https://c :8005/saml2/sp/acs/post

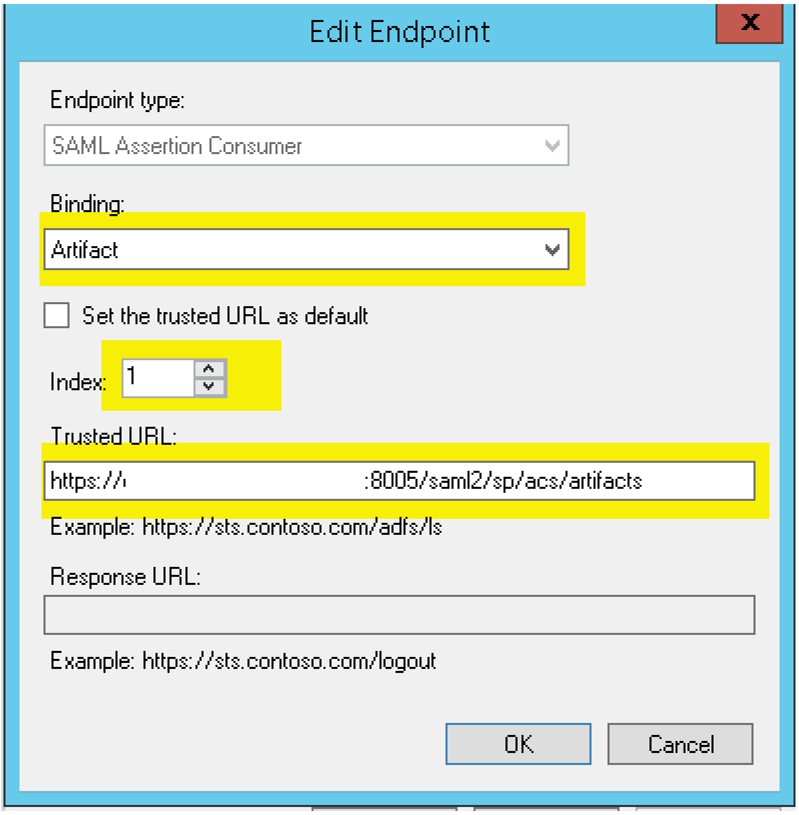
Example: https://sts.contoso.com/adfs/ls

Response URL:

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://ofsll.oracle.com:9704/saml2/sp/acs/artifacts
- Click Ok



Edit Endpoint

Endpoint type:

SAML Assertion Consumer

Binding:

Artifact

☐ Set the trusted URL as default

Index: 1

Trusted URL:

https://ı   :8005/saml2/sp/acs/artifacts

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

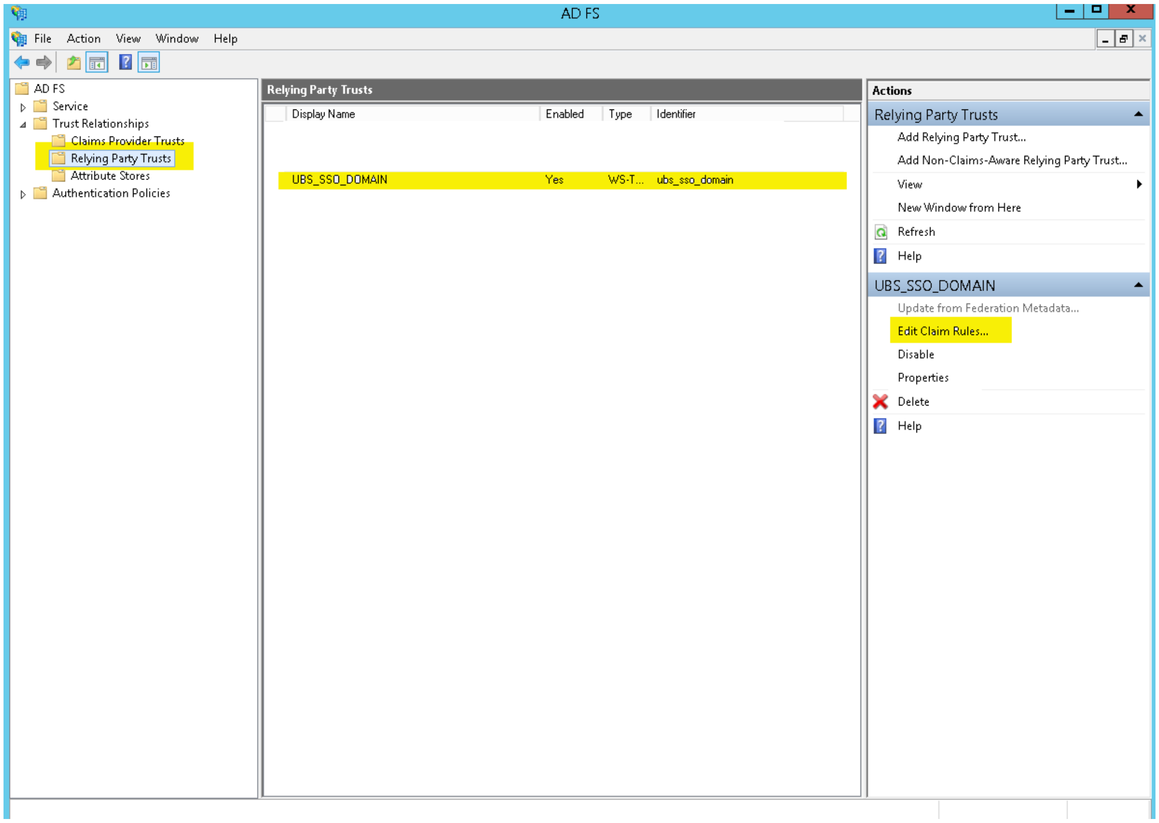
Response URL:

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

Figure 56. AD FS Relying Party – Add Endpoint

Adding Rules

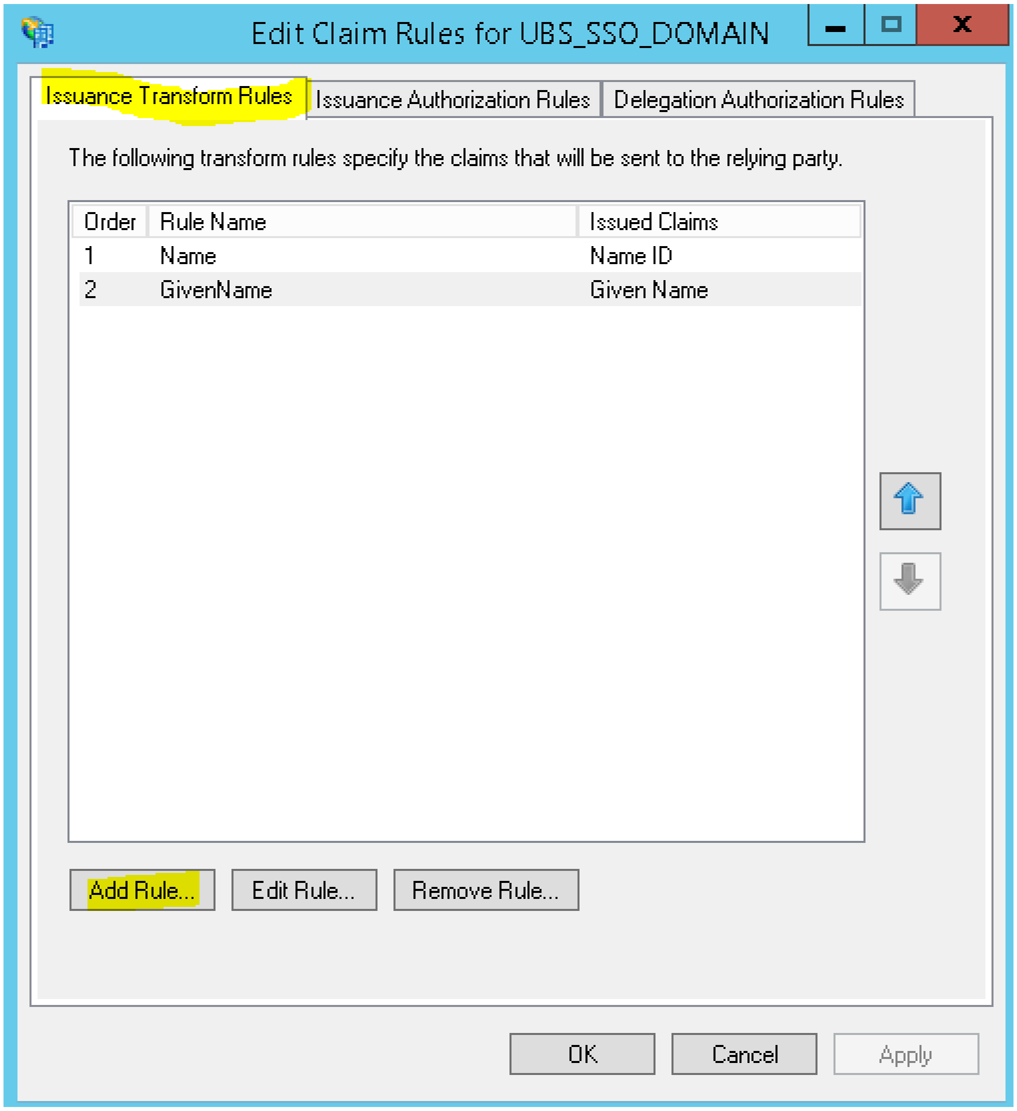
» Select the newly created Relying Party Trust and click “Edit Claim Rules”



Display Name	Enabled	Type	Identifier
UBS_SSO_DOMAIN	Yes	WS-T...	ubs_sso_domain

Figure 57. AD FS Relying Party – Edit Claims

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



Edit Claim Rules for UBS_SSO_DOMAIN
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

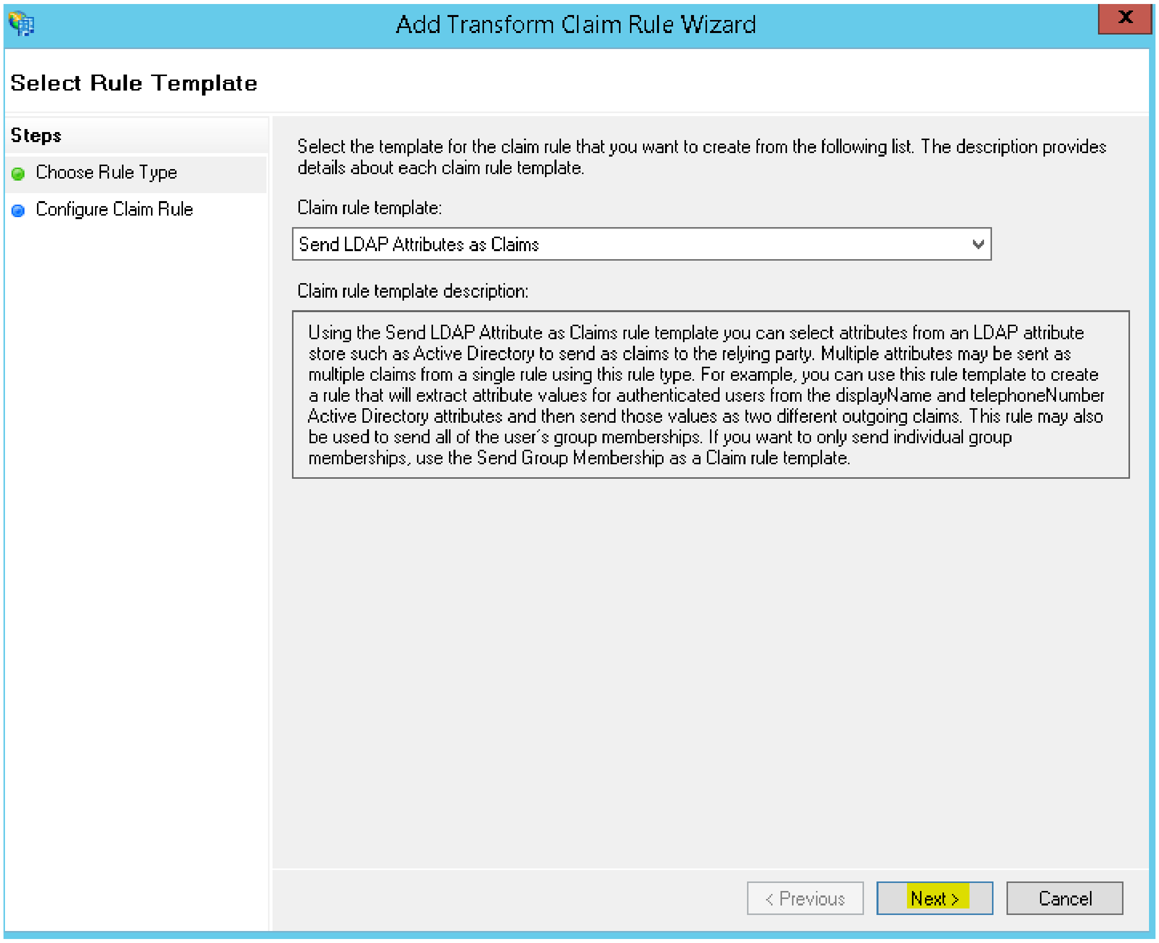
The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Name	Name ID
2	GivenName	Given Name

Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

Figure 58. AD FS Relying Party – Add Rules

» Click on Next



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

Claim rule template:

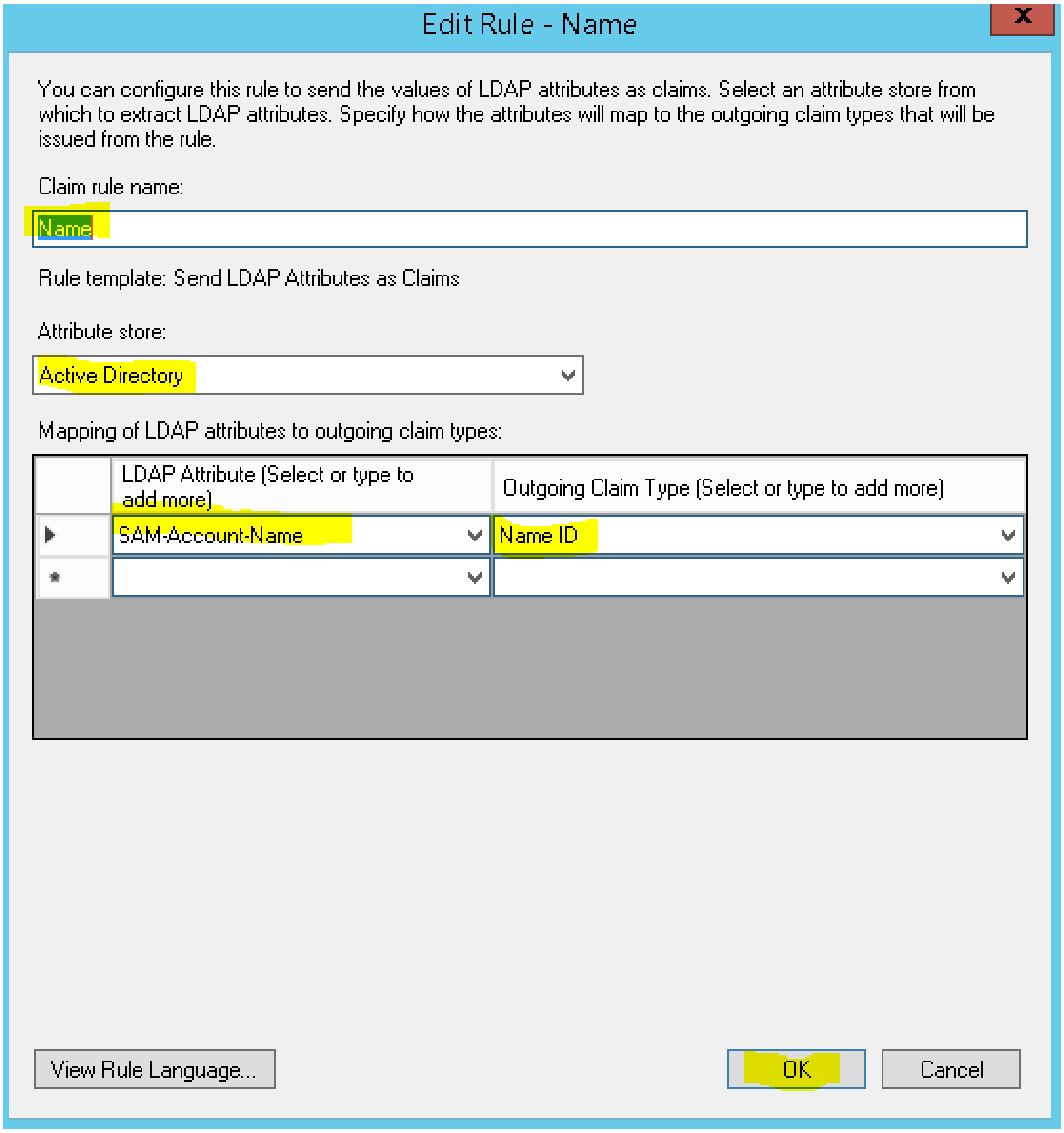
Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

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:

Name

Rule template: Send LDAP Attributes as Claims

Attribute store:

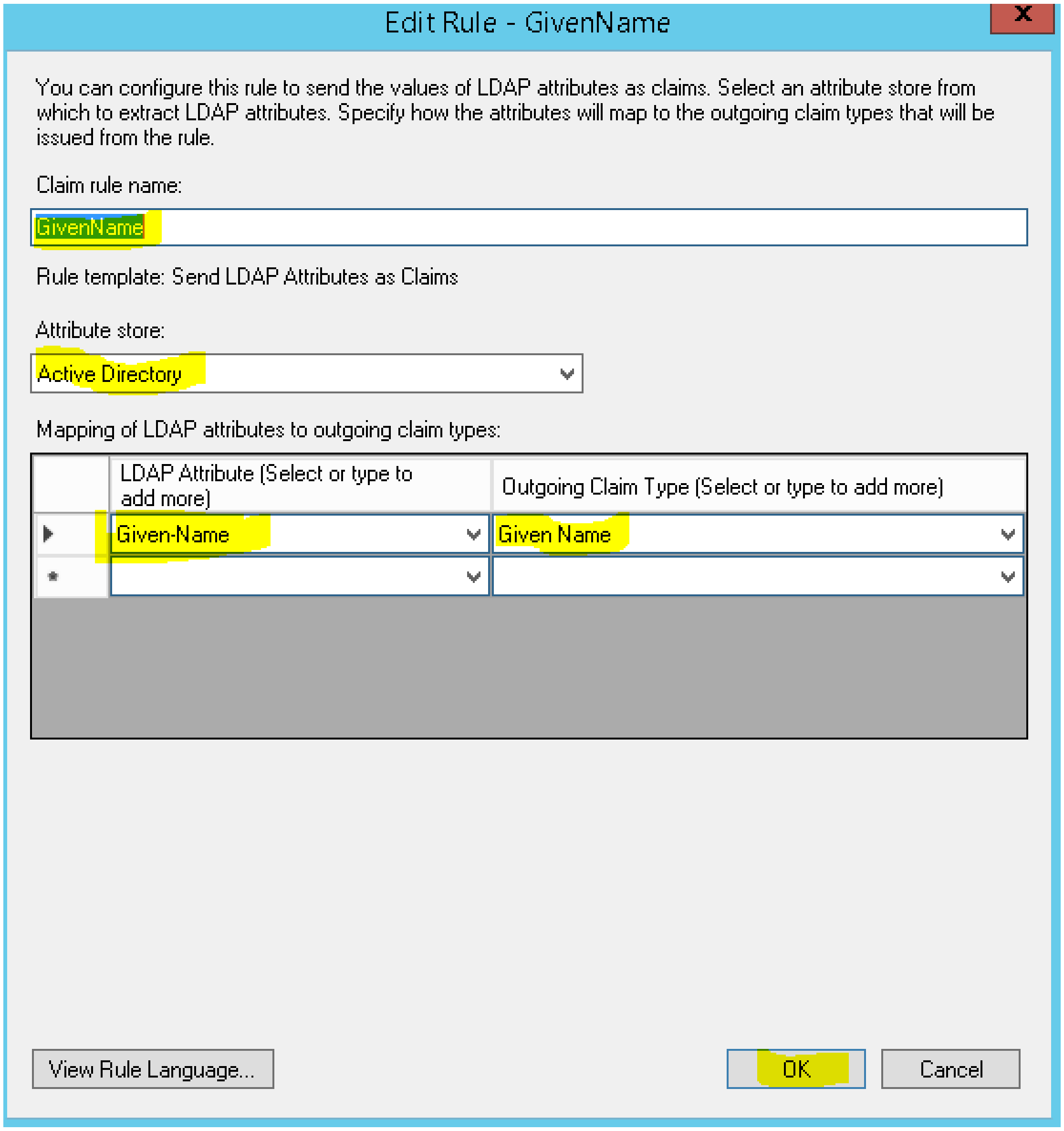
Active Directory

Mapping of LDAP attributes to outgoing claim types:

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

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

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

Figure 61. AD FS Relying Party – Add GivenName Rule

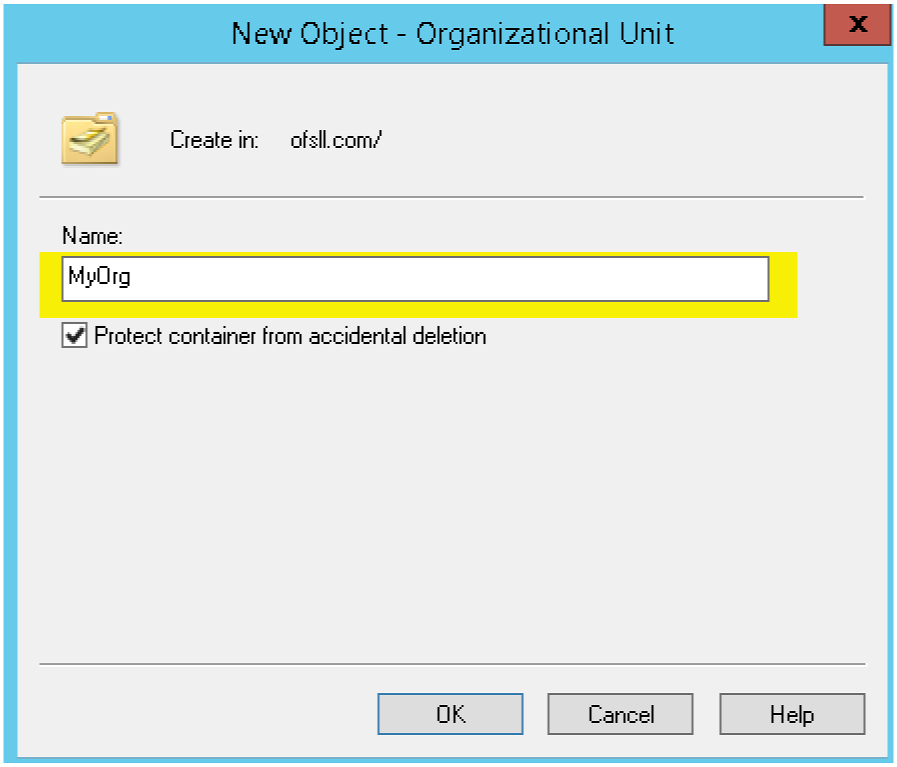
User Management in AD

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



New Object - Organizational Unit

Create in: ofsll.com/

Name: MyOrg

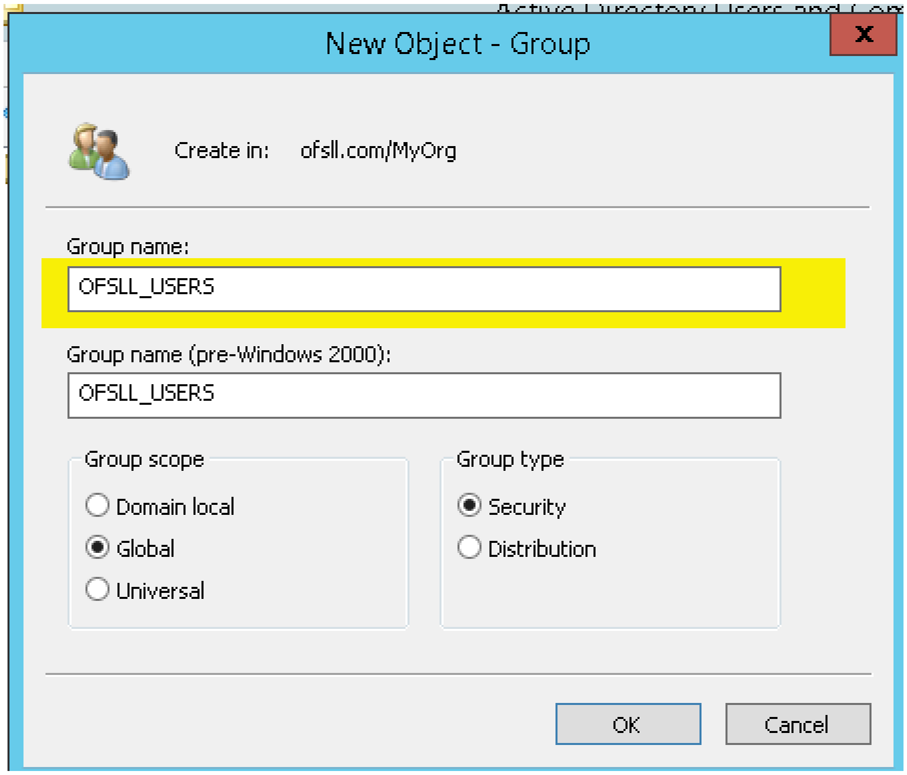
☑ Protect container from accidental deletion

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



New Object - Group

Create in: ofsll.com/MyOrg

Group name: OFSLL_USERS

Group name (pre-Windows 2000): OFSLL_USERS

Group scope

○ Domain local
● Global
○ Universal

Group type

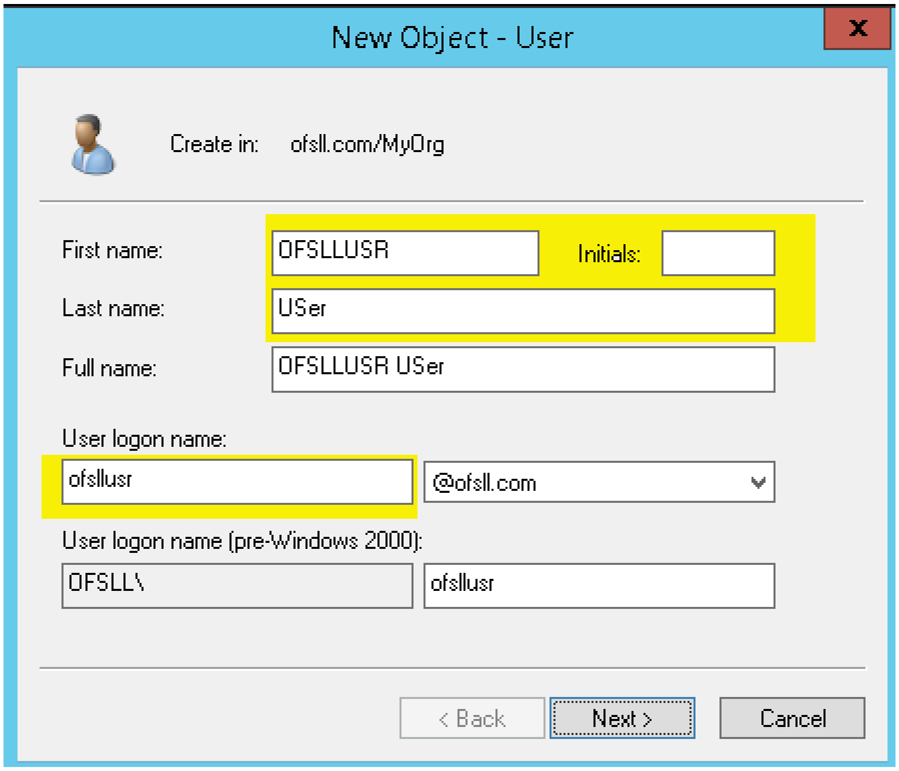
● Security
○ Distribution

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



New Object - User

Create in: ofsll.com/MyOrg

First name: OFSLLUSR

Initials:

Last name: USer

Full name: OFSLLUSR USer

User logon name: ofsllusr @ofsll.com

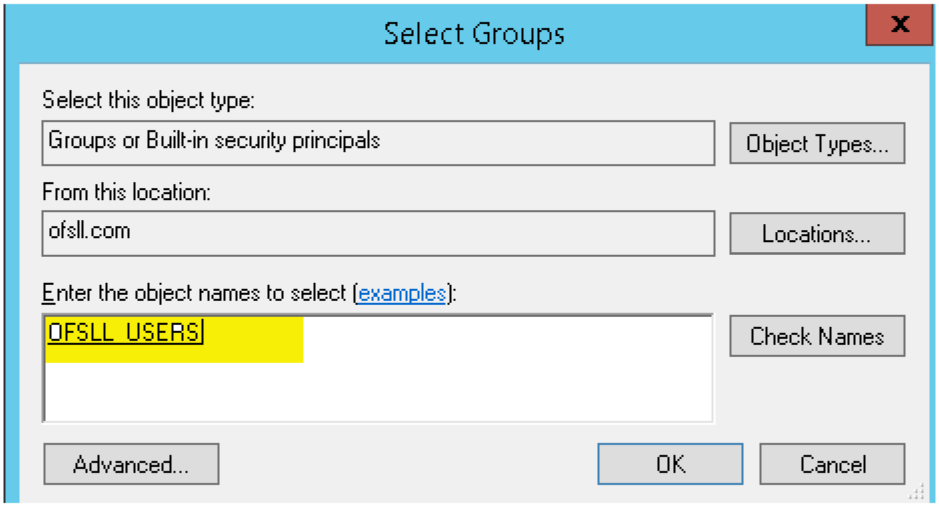
User logon name (pre-Windows 2000): OFSLL\ ofsllusr

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



Select this object type:
Groups or Built-in security principals

From this location:
ofsll.com

Enter the object names to select (examples):
OFSLL USERS

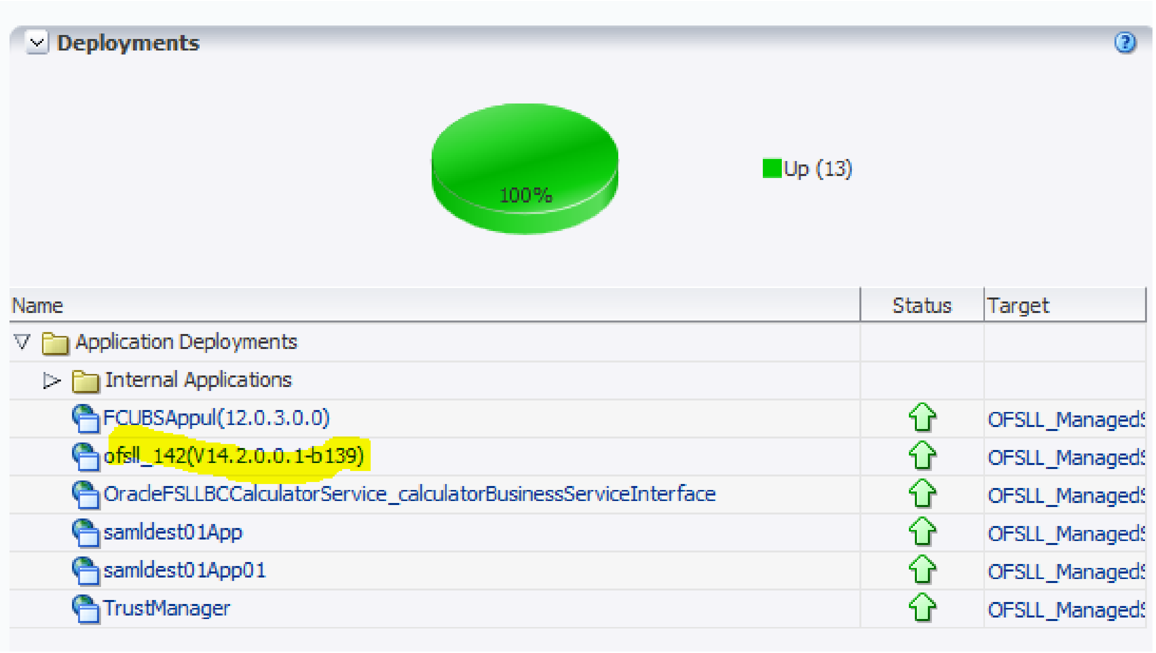
Figure 65. AD – Group Mapping

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:

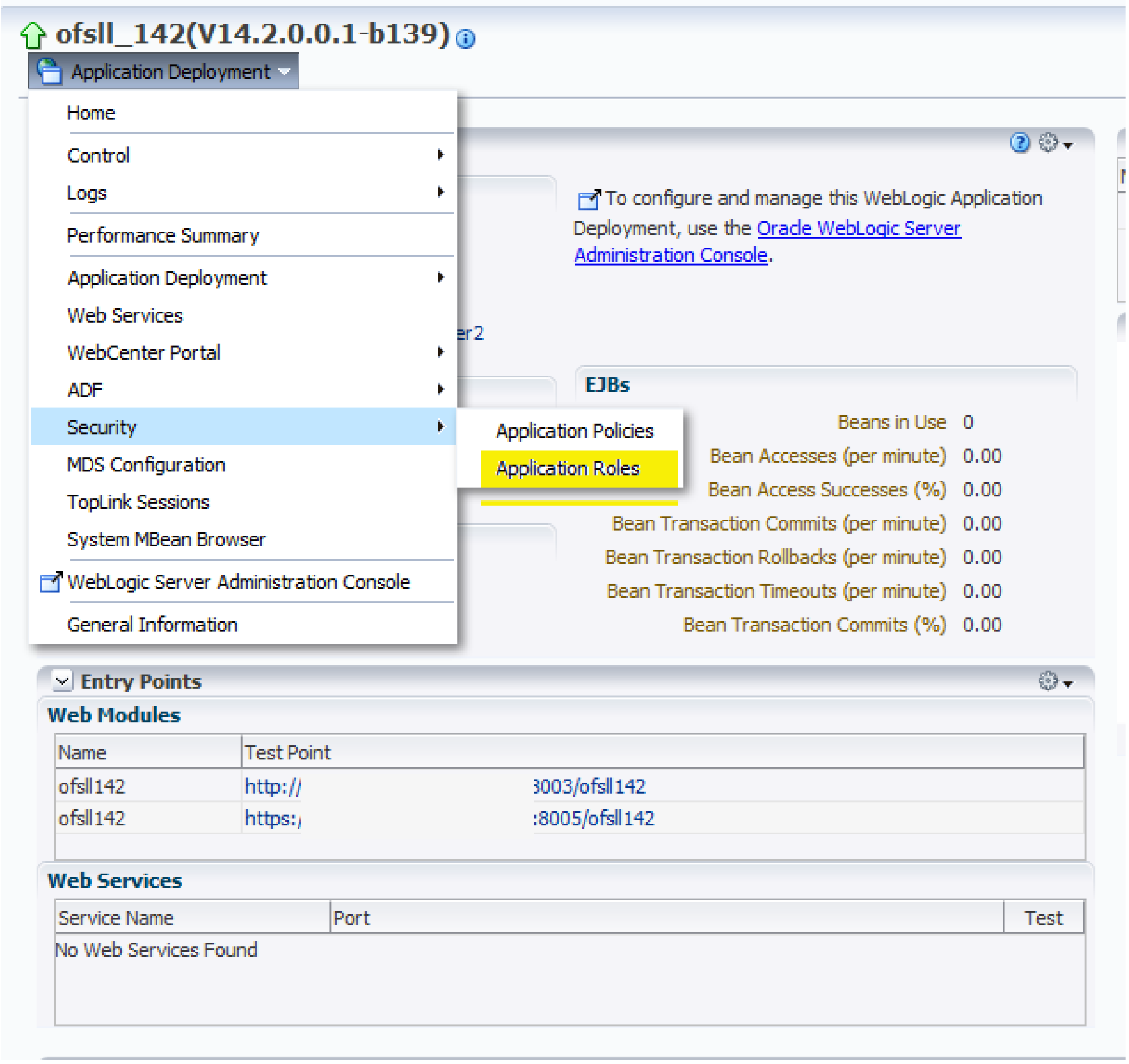
- Login to OFSLL http://<WeblogicServerName>:<AdminPort>/em; for example http://ofsll.oracle.com:8001/em
- Select deployed OFSLL application as shown below



Name	Status	Target
▽ Application Deployments		
▷ Internal Applications		
FCUBSAppul(12.0.3.0.0)	⇧	OFSLL_Managed
ofsll_142(V14.2.0.0.1-b139)	⇧	OFSLL_Managed
OracleFSLLBCCalculatorService_calculatorBusinessServiceInterface	⇧	OFSLL_Managed
samldest01App	⇧	OFSLL_Managed
samldest01App01	⇧	OFSLL_Managed
TrustManager	⇧	OFSLL_Managed

Figure 66. Weblogic EM –Deployments

- Select Application Deployment -> Security -> Application Roles



To configure and manage this WebLogic Application Deployment, use the Oracle WebLogic Server Administration Console.

Beans in Use	0
Bean Accesses (per minute)	0.00
Bean Access Successes (%)	0.00
Bean Transaction Commits (per minute)	0.00
Bean Transaction Rollbacks (per minute)	0.00
Bean Transaction Timeouts (per minute)	0.00
Bean Transaction Commits (%)	0.00

Web Modules

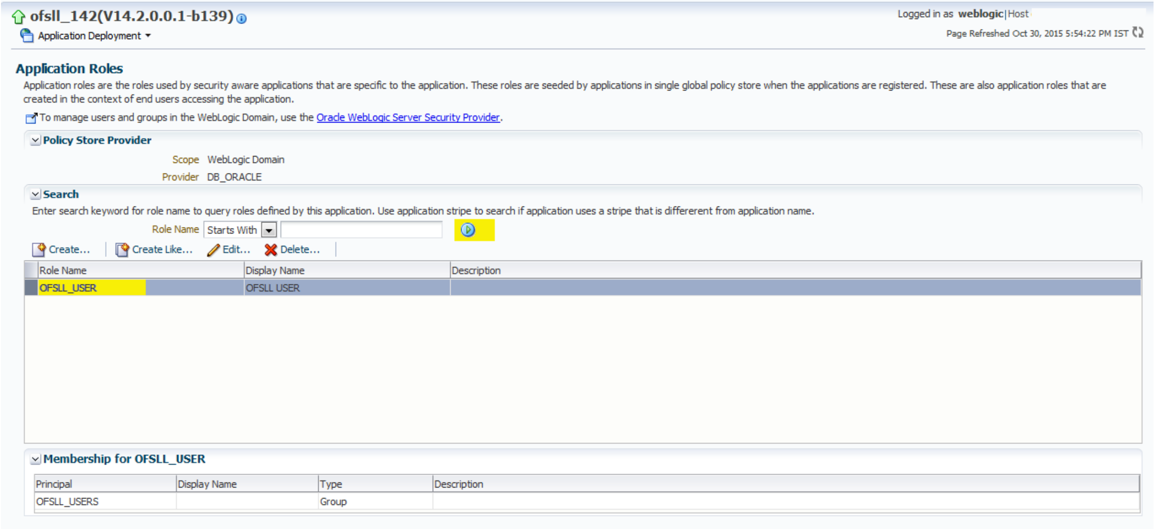
Name	Test Point
ofsll142	http:// 3003/ofsll142
ofsll142	https:, :8005/ofsll142

Web Services

Service Name	Port	Test
No Web Services Found		

Figure 67. Weblogic EM – Application Roles

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



ofsll_142(V14.2.0.0.1-b139)
Application Deployment ▾

Logged in as **weblogic**|Host
Page Refreshed Oct 30, 2015 5:54:22 PM IST

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in single global policy store when the applications are registered. These are also application roles that are created in the context of end users accessing the application.

To manage users and groups in the WebLogic Domain, use the Oracle WebLogic Server Security Provider.

Policy Store Provider

Scope WebLogic Domain
Provider DB_ORACLE

Search

Enter search keyword for role name to query roles defined by this application. Use application stripe to search if application uses a stripe that is differerent from application name.

Role Name Starts With

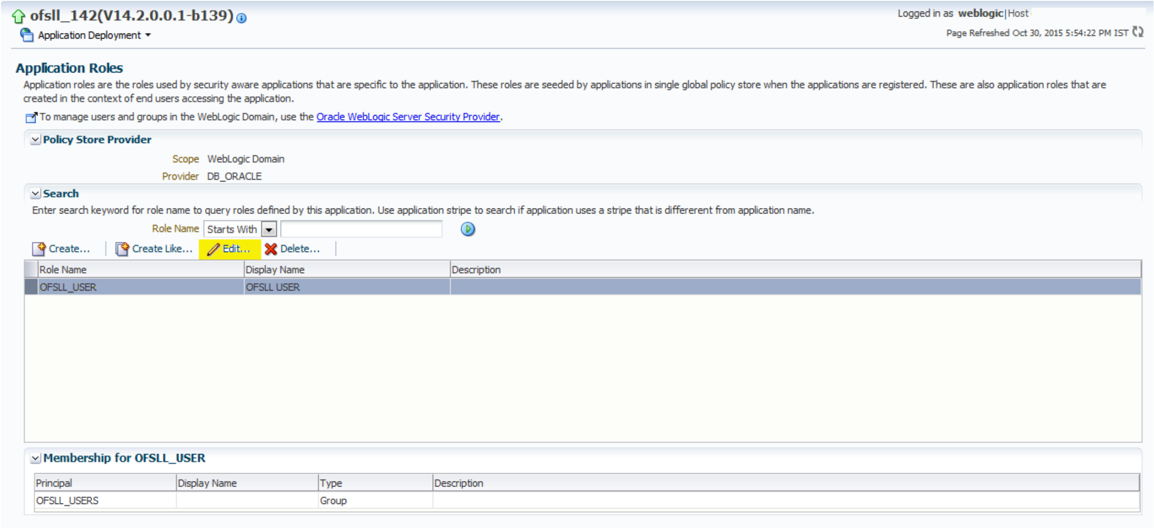
Role Name	Display Name	Description
OFSLL_USER	OFSLL USER	

Membership for OFSLL_USER

Principal	Display Name	Type	Description
OFSLL_USERS		Group	

Figure 68. Weblogic EM – Application Roles

» Click on “Edit”



ofsll_142(V14.2.0.0.1-b139)
Application Deployment ▾

Logged in as **weblogic**|Host
Page Refreshed Oct 30, 2015 5:54:22 PM IST

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in single global policy store when the applications are registered. These are also application roles that are created in the context of end users accessing the application.

To manage users and groups in the WebLogic Domain, use the Oracle WebLogic Server Security Provider.

Policy Store Provider

Scope WebLogic Domain
Provider DB_ORACLE

Search

Enter search keyword for role name to query roles defined by this application. Use application stripe to search if application uses a stripe that is differerent from application name.

Role Name Starts With

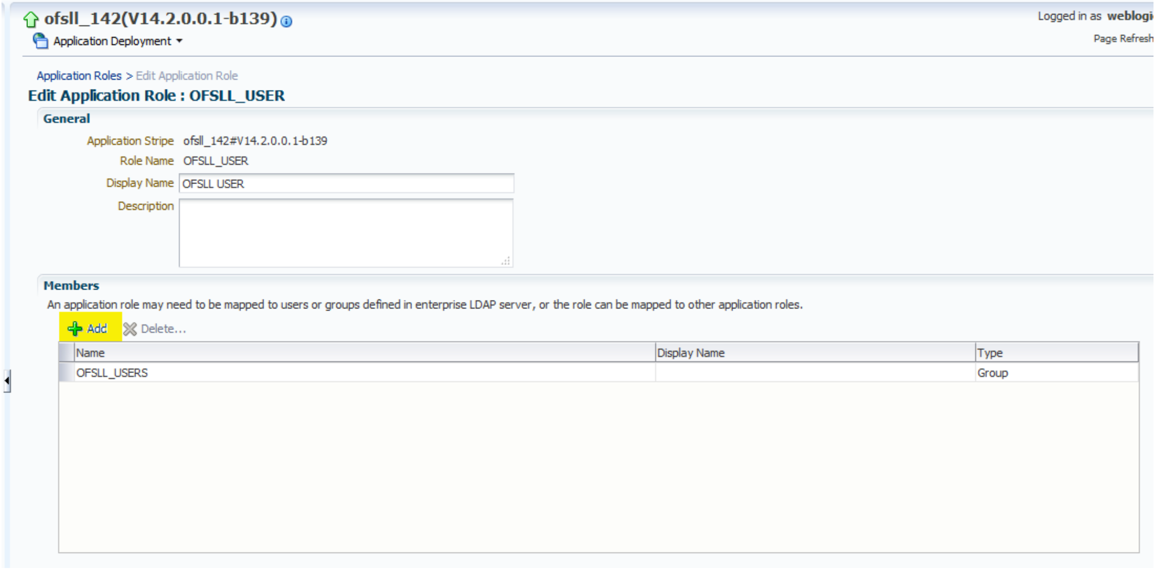
Role Name	Display Name	Description
OFSLL_USER	OFSLL USER	

Membership for OFSLL_USER

Principal	Display Name	Type	Description
OFSLL_USERS		Group	

Figure 69. Weblogic EM – Edit Application Roles

» Click on Members → "Add"



ofsll_142(V14.2.0.0.1-b139)

Logged in as weblogi

Page Refresh

Application Roles > Edit Application Role

Edit Application Role : OFSLL_USER

General

Application Stripe ofsll_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.

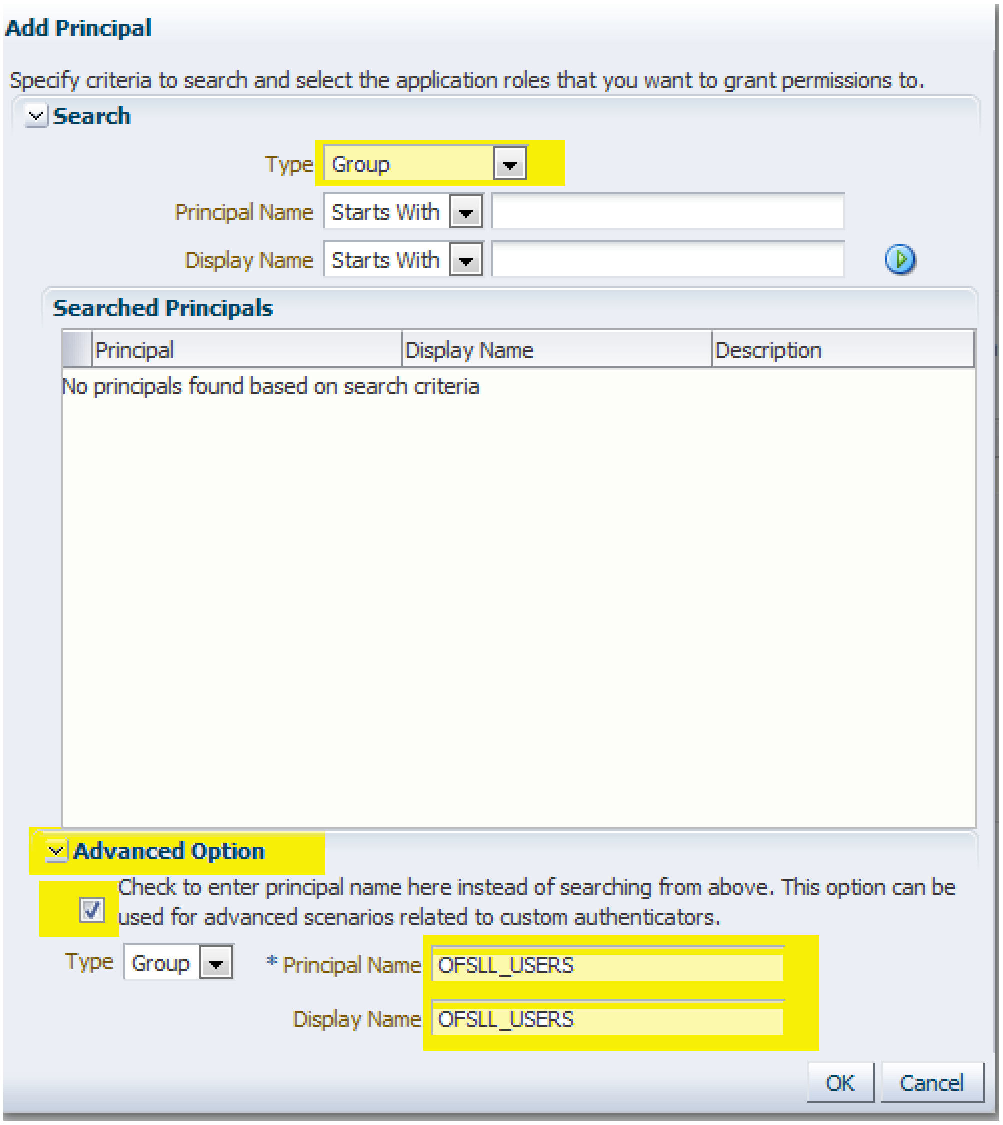
Name	Display Name	Type
OFSLL_USERS		Group

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

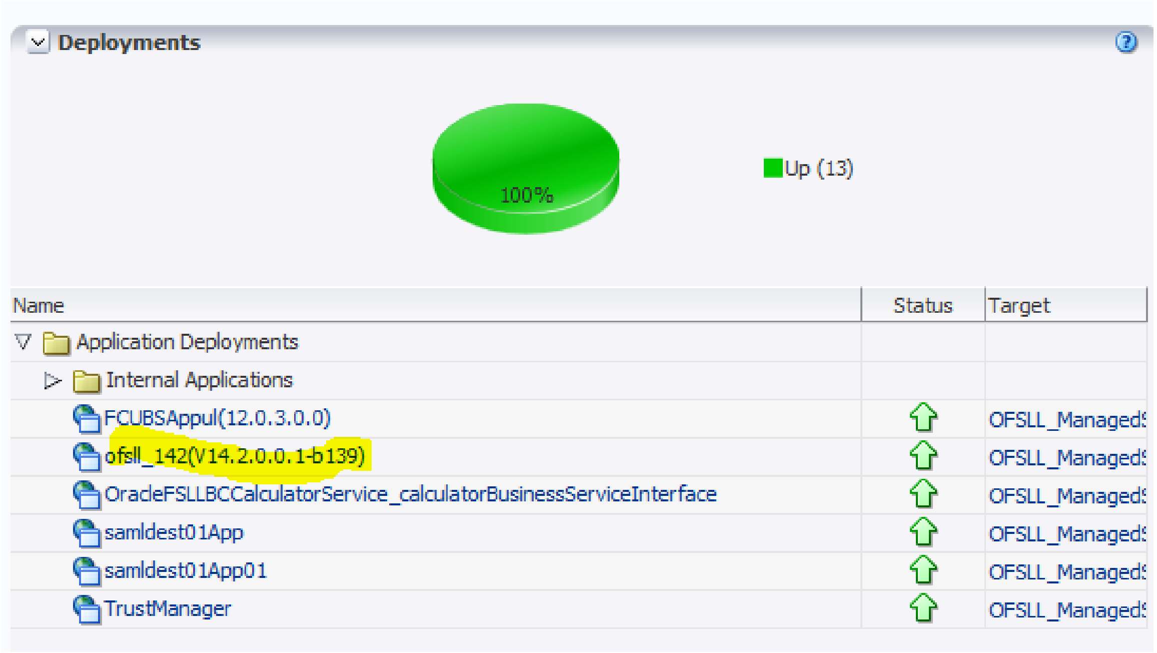
Figure 71. Weblogic EM – Addition of Enterprise Roles

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



Deployments

Name	Status	Target
▽ Application Deployments		
▷ Internal Applications		
FCUBSAppul(12.0.3.0.0)	⇧	OFSLL_ManagedS
ofsll_142(V14.2.0.0.1-b139)	⇧	OFSLL_ManagedS
OracleFSLLBCCalculatorService_calculatorBusinessServiceInterface	⇧	OFSLL_ManagedS
samldest01App	⇧	OFSLL_ManagedS
samldest01App01	⇧	OFSLL_ManagedS
TrustManager	⇧	OFSLL_ManagedS

Figure 72. Weblogic EM –Deployments

» Select Application Deployment -> Security -> Application Policies

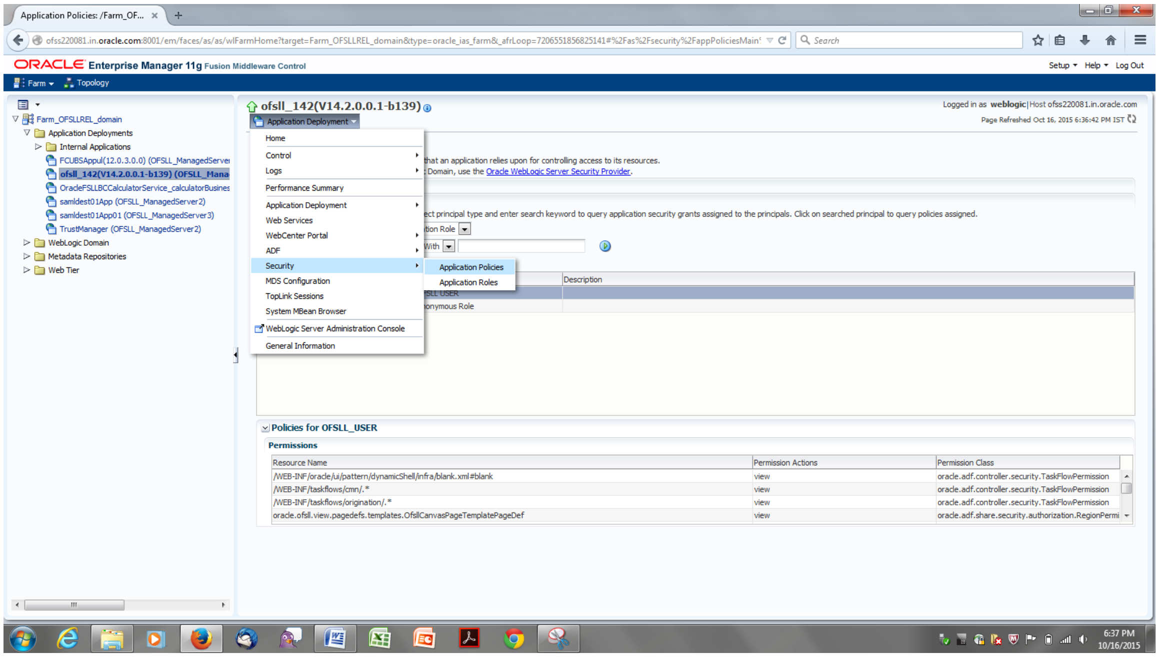
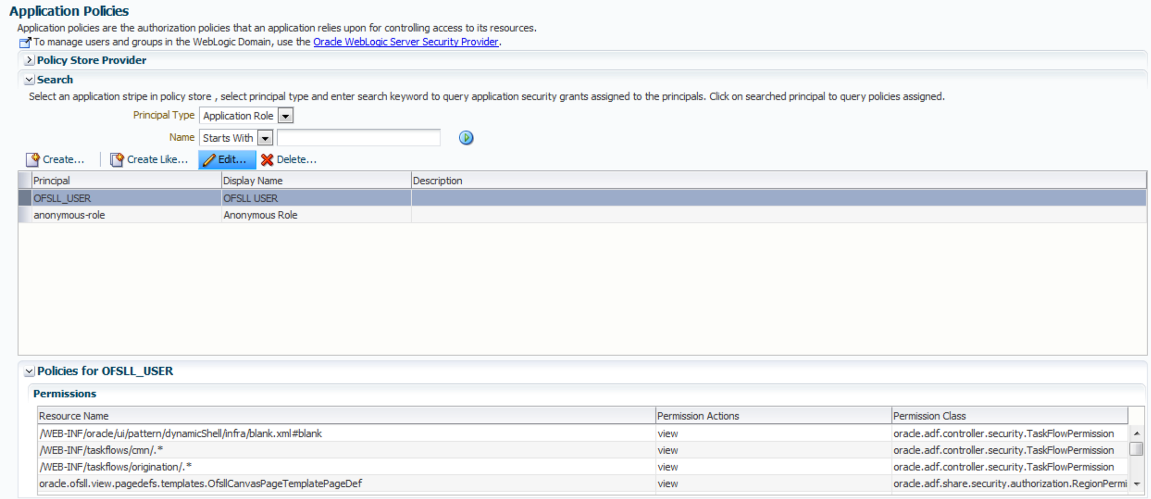

Application Policies: /Farm_OF...
ofss220081.in.oracle.com:8001/em/faces/as/as/wlFarmHome?target=Farm_OFSLLREL_domain&type=oracle_ias_farm&_afrLoop=7206551856825141#%2Fas%2Fsecurity%2FappPoliciesMain
Search
ORACLE Enterprise Manager 11g Fusion Middleware Control
Setup
Help
Log Out
Farm
Topology
Farm_OFSLLREL_domain
Application Deployments
Internal Applications
FCUBSAppul(12.0.3.0.0) (OFSLL_ManagedServer
ofsll_142(V14.2.0.0.1-b139) (OFSLL_Mana
OracleFSLLBCCalculatorService_calculatorBusines
samldest01App (OFSLL_ManagedServer2)
samldest01App01 (OFSLL_ManagedServer3)
TrustManager (OFSLL_ManagedServer2)
WebLogic Domain
Metadata Repositories
Web Tier
ofsll_142(V14.2.0.0.1-b139)
Application Deployment
Home
Control
Logs
Performance Summary
Application Deployment
Web Services
WebCenter Portal
ADF
Security
Application Policies
Application Roles
MDS Configuration
TopLink Sessions
System MBean Browser
WebLogic Server Administration Console
General Information
Logged in as weblogic|Host ofss220081.in.oracle.com
Page Refreshed Oct 16, 2015 6:36:42 PM IST
6:37 PM
10/16/2015

Figure 73. Weblogic EM –Security Policies

» Below detail shows up



Application Policies

Application policies are the authorization policies that an application relies upon for controlling access to its resources.

To manage users and groups in the WebLogic Domain, use the Oracle WebLogic Server Security Provider.

Policy Store Provider

Search

Select an application stripe in policy store , select principal type and enter search keyword to query application security grants assigned to the principals. Click on searched principal to query policies assigned.

Principal Type: Application Role

Name: Starts With

Principal	Display Name	Description
OFSLL_USER	OFSLL USER	
anonymous-role	Anonymous Role	

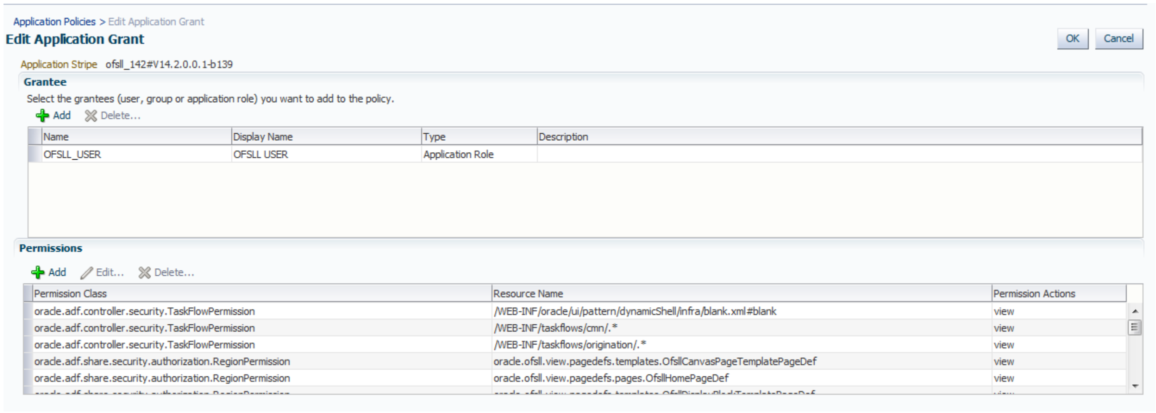
Policies for OFSLL_USER

Permissions

Resource Name	Permission Actions	Permission Class
/WEB-INF/oracle/ui/pattern/dynamicShell/infra/blank.xml#blank	view	oracle.adf.controller.security.TaskFlowPermission
/WEB-INF/taskflows/cmn/.*	view	oracle.adf.controller.security.TaskFlowPermission
/WEB-INF/taskflows/origination/.*	view	oracle.adf.controller.security.TaskFlowPermission
oracle.ofsll.view.pagedefs.templates.OfsllCanvasPageTemplatePageDef	view	oracle.adf.share.security.authorization.RegionPermi

Figure 74. Weblogic EM – Application Policies

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



Application Policies > Edit Application Grant

Edit Application Grant

Application Stripe ofsll_142#V14.2.0.0.1-b139

Grantee

Select the grantees (user, group or application role) you want to add to the policy.

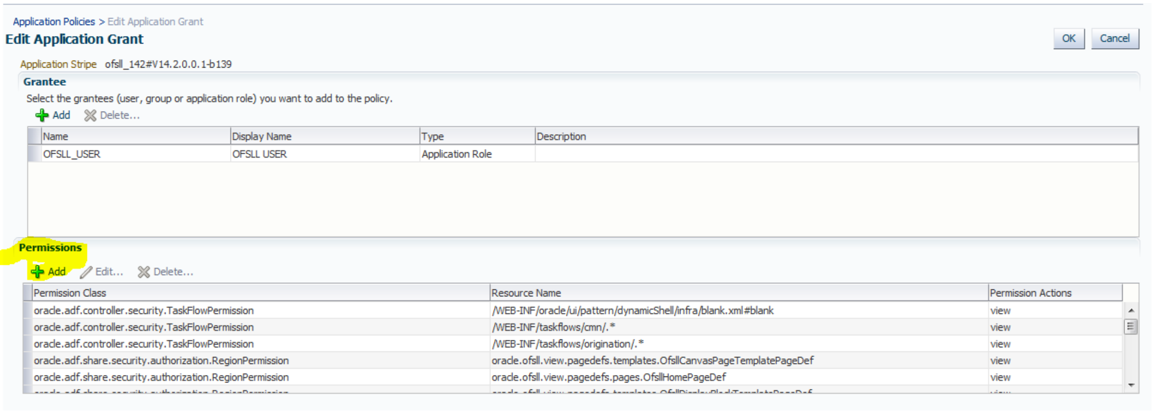
Name	Display Name	Type	Description
OFSLL_USER	OFSLL USER	Application Role	

Permissions

Permission Class	Resource Name	Permission Actions
oracle.adf.controller.security.TaskFlowPermission	/WEB-INF/oracle/ui/pattern/dynamicShell/infra/blank.xml#blank	view
oracle.adf.controller.security.TaskFlowPermission	/WEB-INF/taskflows/cmn/.*	view
oracle.adf.controller.security.TaskFlowPermission	/WEB-INF/taskflows/origination/.*	view
oracle.adf.share.security.authorization.RegionPermission	oracle.ofsll.view.pagedefs.templates.OfsllCanvasPageTemplatePageDef	view
oracle.adf.share.security.authorization.RegionPermission	oracle.ofsll.view.pagedefs.pages.OfsllHomePageDef	view

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



Application Policies > Edit Application Grant

Edit Application Grant

Application Stripe ofsll_142#V14.2.0.0.1-b139

Grantee

Select the grantees (user, group or application role) you want to add to the policy.

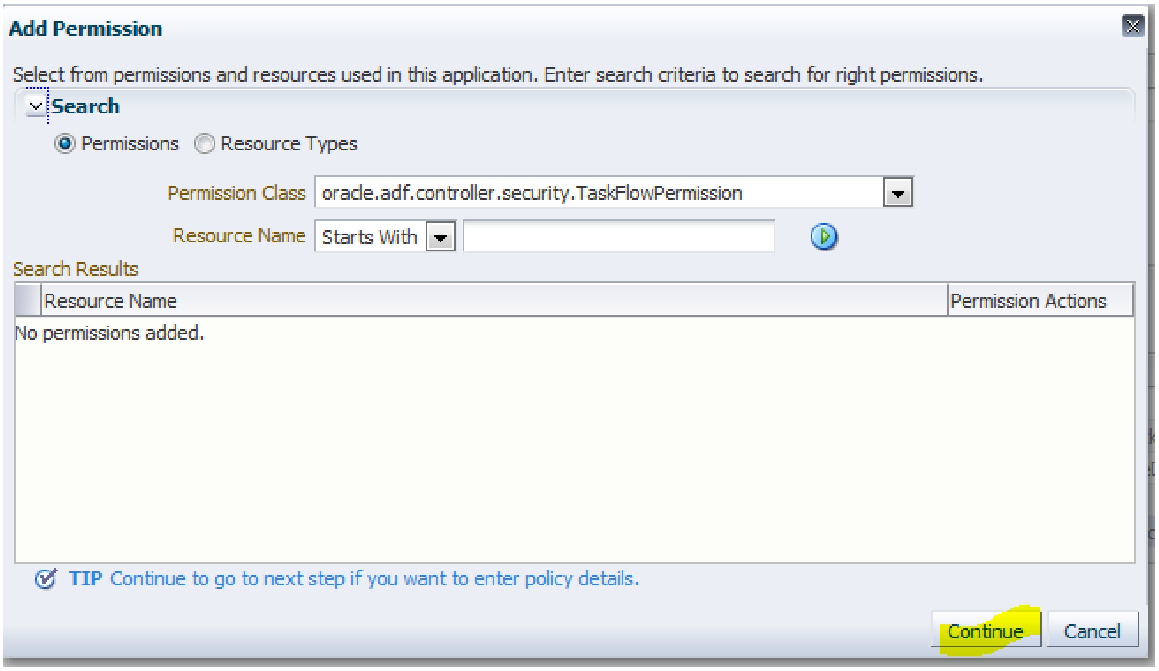
Name	Display Name	Type	Description
OFSLL_USER	OFSLL USER	Application Role	

Permissions

Permission Class	Resource Name	Permission Actions
oracle.adf.controller.security.TaskFlowPermission	/WEB-INF/oracle/ui/pattern/dynamicShell/infra/blank.xml#blank	view
oracle.adf.controller.security.TaskFlowPermission	/WEB-INF/taskflows/cmn/.*	view
oracle.adf.controller.security.TaskFlowPermission	/WEB-INF/taskflows/origination/.*	view
oracle.adf.share.security.authorization.RegionPermission	oracle.ofsll.view.pagedefs.templates.OfsllCanvasPageTemplatePageDef	view
oracle.adf.share.security.authorization.RegionPermission	oracle.ofsll.view.pagedefs.pages.OfsllHomePageDef	view

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 Results

Resource Name	Permission Actions
No permissions added.	

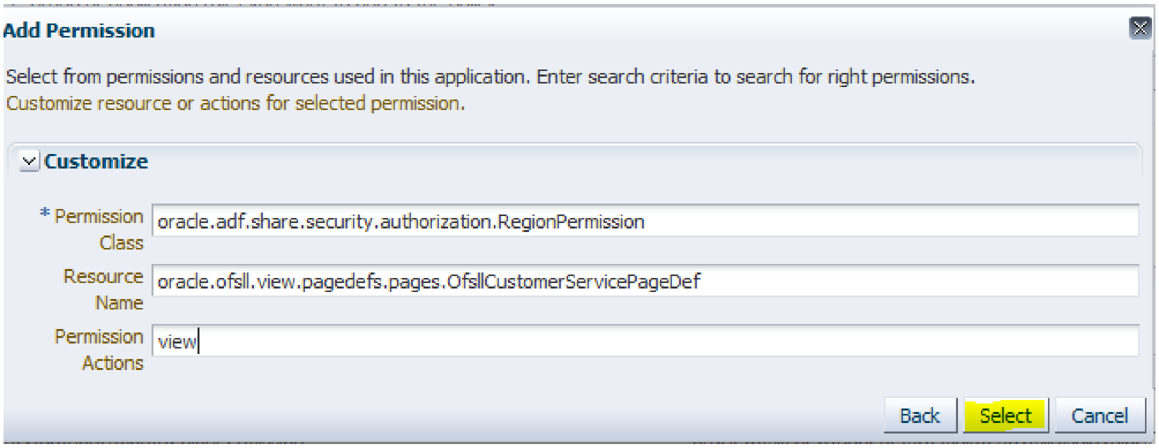
TIP Continue to go to next step if you want to enter policy details.

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

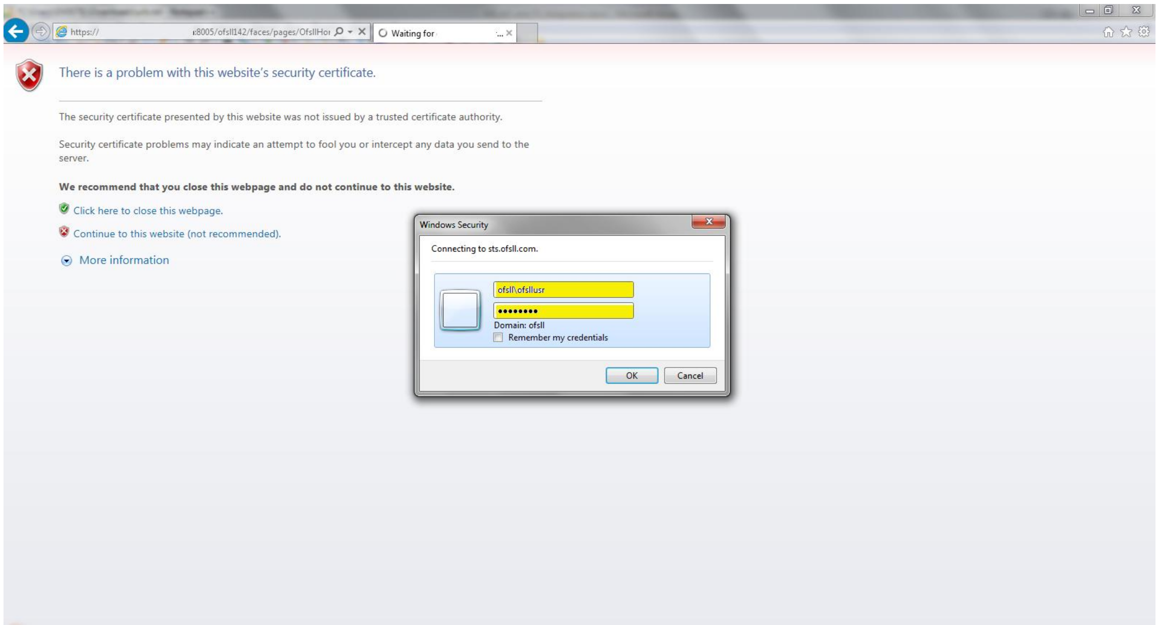
Figure 78. Weblogic EM – Add Permission

» 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



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Windows Security

Connecting to sts.ofsll.com.

ofsll\ofsllusr

••••••••

Domain: ofsll

□ Remember my credentials

OK | Cancel

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

- On successful authentication, OFSLL Home page opens up

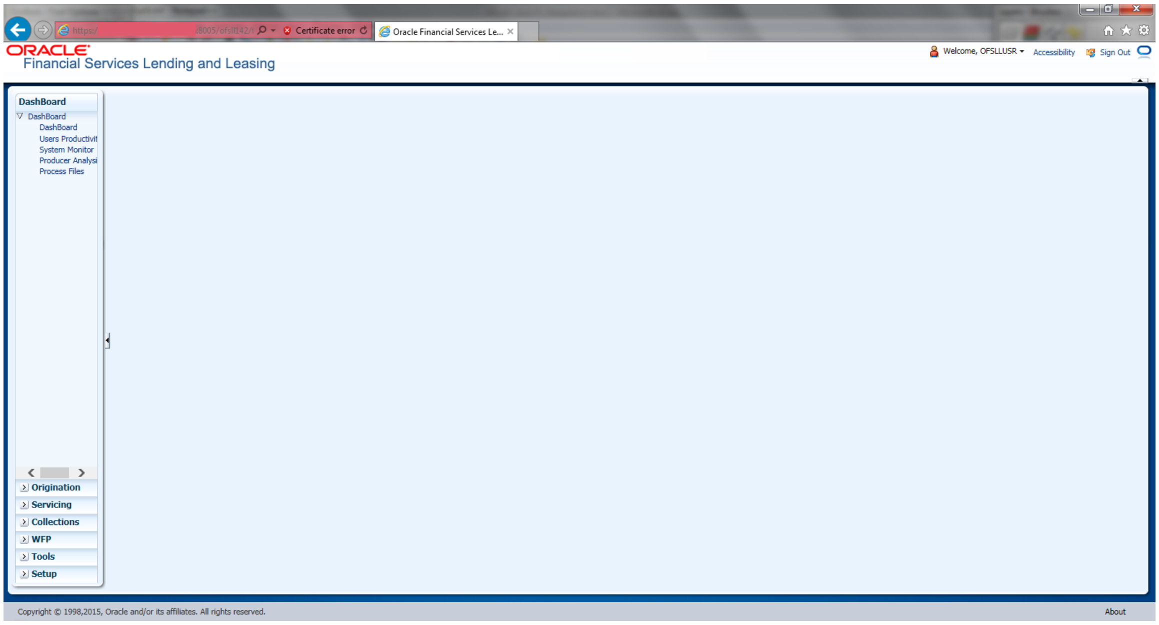
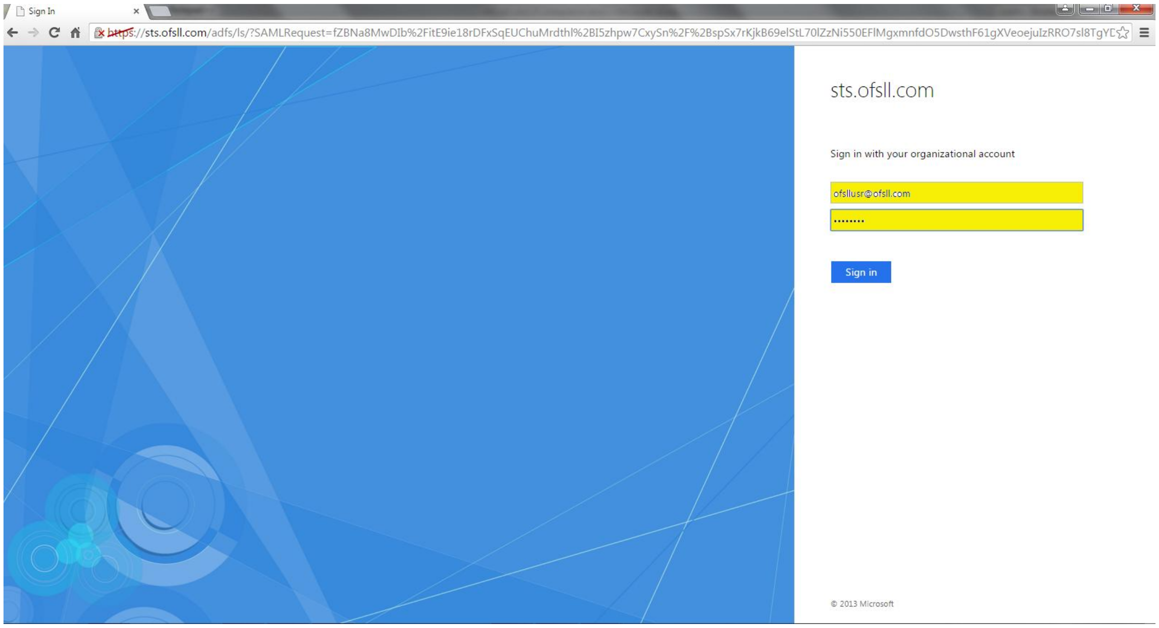


Figure 80. Internet Explorer: OFSLL Home Page

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



https://sts.ofsll.com/adfs/ls/?SAMLRequest=fZBNa8MwDIb%2FitE9ie18rDFxSqEUChuMrdthl%2BI5zhpw7CxySn%2F%2BspSx7rKjkB69elStL70lZzNi550EFlMgxmnfdO5DwsthF61gXVeoejuIzRRO7sl8TgYD

sts.ofsll.com

Sign in with your organizational account

ofsllusr@ofsll.com

••••••••

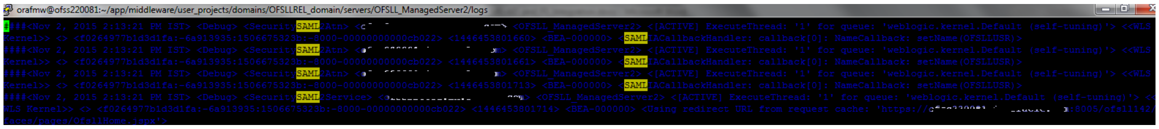
Figure 81. Google Chrome: AD FS Sign-In Page

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/OFSLLREL_domain/servers/OFSLL_ManagedServer2/logs
####<Nov 2, 2015 2:13:21 PM IST> <Debug> <SecuritySAML2Atn> <[redacted]> <OFSLL_ManagedServer2> <[ACTIVE] ExecuteThread: '1' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS
Kernel>> <> <f0264977b1d3d1fa:-6a913935:1506675323b:-8000-00000000000cb022> <1446453801660> <BEA-000000> <SAMLIACallbackHandler: callback[0]: NameCallback: setName(OFSLLUSR)>
####<Nov 2, 2015 2:13:21 PM IST> <Debug> <SecuritySAML2Atn> <[redacted]> <OFSLL_ManagedServer2> <[ACTIVE] ExecuteThread: '1' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS
Kernel>> <> <f0264977b1d3d1fa:-6a913935:1506675323b:-8000-00000000000cb022> <1446453801661> <BEA-000000> <SAMLIACallbackHandler: callback[0]: NameCallback: setName(OFSLLUSR)>
####<Nov 2, 2015 2:13:21 PM IST> <Debug> <SecuritySAML2Atn> <[redacted]> <OFSLL_ManagedServer2> <[ACTIVE] ExecuteThread: '1' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS
Kernel>> <> <f0264977b1d3d1fa:-6a913935:1506675323b:-8000-00000000000cb022> <1446453801713> <BEA-000000> <SAMLIACallbackHandler: callback[0]: NameCallback: setName(OFSLLUSR)>
####<Nov 2, 2015 2:13:21 PM IST> <Debug> <SecuritySAML2Service> <[redacted]> <OFSLL_ManagedServer2> <[ACTIVE] ExecuteThread: '1' for queue: 'weblogic.kernel.Default (self-tuning)'> <<
WLS Kernel>> <> <f0264977b1d3d1fa:-6a913935:1506675323b:-8000-00000000000cb022> <1446453801714> <BEA-000000> <Using redirect URL from request cache: 'https://[redacted]:8005/ofsll142/
faces/pages/OfsllHome.jspx'>
```

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
- facebook.com/oracle
- twitter.com/oracle
- oracle.com

Integrated Cloud Applications & Platform Services

White Paper Title

Author: [OPTIONAL]
Contributing Authors: [OPTIONAL]