

SAML 2.0 SSO Implementation for Oracle Financial Services Lending and Leasing

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

ORACLE WHITE PAPER | MAY 2019



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		



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 autoselected 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

a	Server Manager	_ D X
h	Add Roles and Features Wizard	_ D X
Select server role	S	DESTINATION SERVER whf00akxin.oracle.com
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection Server Roles Features Confirmation Results	Active Directory Certificate Services (1 of 6 installe Active Directory Domain Services (Installed) Active Directory Federation Services (Installed) Active Directory Federation Services (Installed) Active Directory Federation Services (Installed) Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services 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 Immode Access	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.
	< Previous Next	> Install Cancel

Figure 1. Install AD FS –Server Roles

» On the Select Features interface, click Next

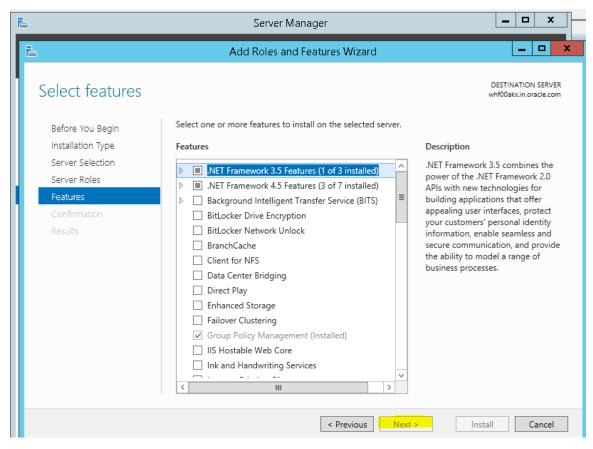


Figure 2. Install AD FS - Select Features

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

a	Add Roles and Features Wizard	-		X	
	Add Roles and Features Wizard Federation Services (AD FS) Active Directory Federation Services (AD FS) provides Web single-sign-on (SSO) authenticate a user to multiple Web applications using a single user account. Al bypass the need for secondary accounts by allowing you to project a user's digi rights to trusted partners. In this federated environment, each organization con own identities. Things to note: • This computer must be joined to a domain before you can successfully install • The Web Application Proxy role service in the Remote Access server role func service proxy and cannot be installed on the same computer as the federation	D FS helps on ital identity ar itinues to man l the Federation ctions as the f	to ganizat nd acce nage its on Serv	ions ss ice.	
	< Previous Next >	Install	Cance	H	

Figure 3. Install AD FS – AD FS Page

» Click Install

ā.	Add Roles and Features Wizard	_			×
Confirm install	ation selections	DESTINATIO	N SER	VER	
Before You Begin Installation Type Server Selection Server Roles Features AD FS Confirmation Results	To install the following roles, role services, or features on selected server, click Inst Restart the destination server automatically if required Optional features (such as administration tools) might be displayed on this page b been selected automatically. If you do not want to install these optional features, of their check boxes. Active Directory Federation Services	ecause they			
	Export configuration settings Specify an alternate source path				I,
	< Previous Next > Inst		Cance	el]

Figure 4. Install AD FS – Confirmation Page

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

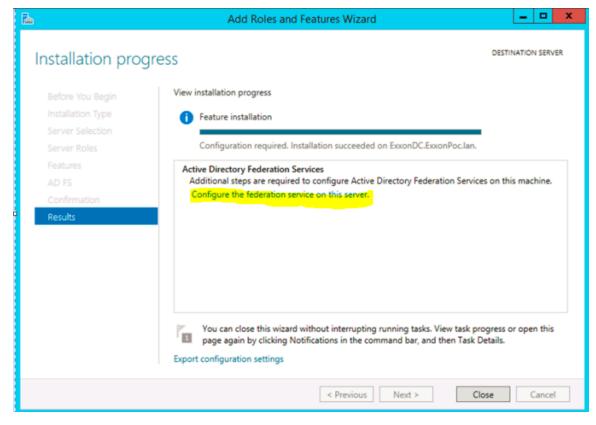


Figure 5. Install AD FS - Result Page

Configure AD FS

Before configuring AD FS ensure following are made available:

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

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

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

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

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

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

How to Register the Certificate

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

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

N	Internet Information Services (IIS) Manager	_ D X
i 💽 🖣 🖣 WHFODAKX 🕨		🖬 🛛 🔂 🕡 🗸
	WHF00AKX Home Filter: • • •	Actions Manage Server Restart Start Start Start Start Start Start Change AET Framework View Sites Change AET Framework Version Get New Web Platform Components Web Platform Components Help
< III >	Testure: View Inc. Content View	
Ready		• 1 .:

Figure 6. IIS Manager - Main Page

» Click on import link

V j		Internet Informa	tion Services (IIS) Manage	er		_ D X
💽 🖣 🕨 WHFOOAKX 🔸						🖸 🛛 🟠 🔞 🗸
<u>F</u> ile <u>V</u> iew <u>H</u> elp						
Ele View Help Connections Start Page Start Page WHF00AXX (OFSLLVPragna) Application Pools b- Stes	Vise this feature to request and m Filter:	anage certificates that the Wet ©o		Expiration Date 7/19/2016 11:22:04 7/20/2020 6:59:03 1/1/2040 5:29:59 AM 1/1/2040 5:29:59 AM 7/19/2016 6:51:19	Certificate Has CEDA4DA3882 CSED240A025F7 385BA81E03D4 1EA8C998024C A328C9881608	Actions Import Create Certificate Request Complete Certificate Request Create Self-Signed Certificate Create Self-Signed Certificate Enable Automatic Rebind of Renewed Certificate Philp
	<	Ш			>	
< III >	Features View 💦 Content Vie	w				
Ready						¶ <u>⊒</u> .:

Figure 7. IIS Manager - Server Certificates

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

Import Certificate ? ×
Certificate file (.pfx):
C:\Users\I . i\Desktop\CACer.pfx
Password:
Select Certificate Store:
Personal 🗸
Allow this certificate to be exported
OK Cancel

Figure 8. IIS Manager - Import Certificate

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

AD FS Configuration

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

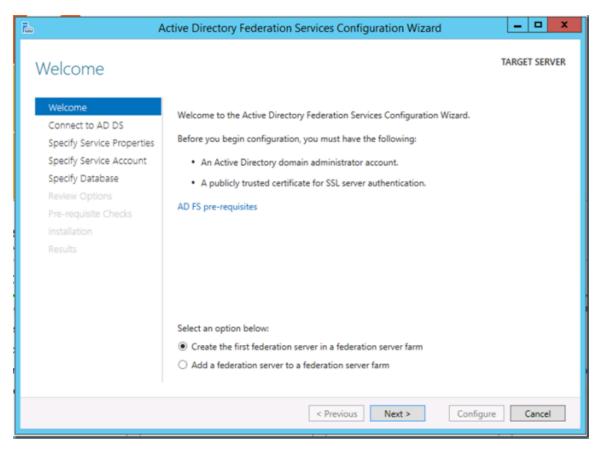


Figure 9. AD FS Configuration – Welcome Page

- » On the Connect to Active Directory Domain Services interface, proceed with Next.
 - » In the first panel of the AD FS Configuration Wizard we will specify the AD account that has permissions to perform the federation service configuration.

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

🚡 A	ctive Directory Federation Services Configuration Wizard	_ 🗆 X
Connect to Active	e Directory Domain Services	TARGET SERVER ADFS01.
Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Review Options Pre-requisite Checks Installation Results	Specify an account with Active Directory domain administrator permiss federation service configuration. \Administrator (Current user)	
	< Previous Next >	Configure Cancel

Figure 10. AD FS Configuration – AD Service Interface

- » In the next panel, specify the service properties.
 - » SSL Certificate \rightarrow 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 signin URL.

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

» Federation Service Display Name \rightarrow Provide a Name for the Service

la /	Active Directory Federation Servi	ces Configuration Wizard 📃 🗖 🗙
Specify Service P	roperties	TARGET SERVER ADFS01.
Welcome Connect to AD DS	SSL Certificate:	*.OFSLL.COM View
Specify Service Properties Specify Service Account Specify Database	Federation Service Name:	sts.ofsII.com
Review Options Pre-requisite Checks Installation Results	Federation Service Display Name:	* sts.ofsII.com Users will see the display name at sign in. <i>Example: Contoso Corporation</i>
	4	Previous Next > Configure Cancel



- » 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.

Active Directory Federation Services Configuration Wizard				- 🗆 X
A Specify Service A Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Review Options Pre-requisite Checks	CCOUNT Specify a domain user a Create a Group Mar Account Name:	ccount or group Managed Se	ervice Account. ADFS_SVC anaged Service Account	TARGET SERVER
Pre-requisite Checks Installation Results				
		< Previous	Next > Configu	Cancel

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

A 🗟	Active Directory Federation Services	Configuration Wizard	_ 🗆 X
Specify Configura Welcome Connect to AD DS Specify Service Properties	Specify a database to store the Active D Create a database on this server usin	irectory Federation Service configuration on g Windows Internal Database.	TARGET SERVER
Specify Service Account Specify Database Review Options Pre-requisite Checks Installation Results	 Specify the location of a SQL Server Database Host Name: Database Instance: 	To use the default instance, leave this field	i blank.
	< Pr	evious Next > Configure	Cancel

Figure 13. AD FS Configuration – Service Database Setup

» On the Review Options interface, click Next

🚡 A	ctive Directory Federation Services Configuration Wizard
Review Options	TARGET SERVER ADFS01.
Welcome	Review your selections:
Connect to AD DS	This server will be configured as the first server in a new AD FS farm STS.OFSLL.COM
Specify Service Properties	The new AD FS farm will use 'Data Source=SQL01;Initial Catalog=ADFSConfiguration;Integrated
Specify Service Account	Security=True;Min Pool Size=20' as the connection string to connect to SQL to retrieve its configuration.
Specify Database	coniguration.
Confirm Overwrite	All existing configuration in the database will be deleted.
Review Options	Federation service will be configured to run as . OFSLL\ADFS SVC
Pre-requisite Checks	· -
Installation	
Results	
	These settings can be exported to a Windows PowerShell script to automate additional installations
	additional installations View script
	< Previous Next > Configure Cancel

Figure 14. AD FS Configuration – Review Page

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

<u>م</u>	ctive Directory Federation Services Configuration Wizard		x
Pre-requisite Che	cks ,	TARGET SI ADFS01.	ERVER
All prerequisite checks pas	sed successfully. Click 'Configure' to begin installation.	Show more	×
Welcome Connect to AD DS	Prerequisites must be validated before Active Directory Federation Services is co computer.	nfigured on t	his
Specify Service Properties Specify Service Account	Rerun prerequisites check		
Specify Database	View results Prerequisites Check Completed		_
Confirm Overwrite Review Options	 All prerequisites checks passed successfully. Click 'Configure' to begin insta 	allation.	
Pre-requisite Checks			
Results			
	< Previous Next > Configur	re Cano	cel

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

» On the Results interface, click Close

\$ 0	AD FS Federation Server Configuration W	izard X
Configuration Results		
Configuration Results Steps • Welcome • Select Deployment Type • Federation Service Name • Specify Service Account • Summary • Results	The following settings are being configured Component Stop the AD FS Windows Service Install Windows Internal Database Start the Windows Internal Database service Create AD FS configuration database Create AD FS configuration database Create Active Directory container for sharing certificates Configure service settings Configure service settings Deploy browser sign-in Web site Start the AD FS Windows Service Create default claim set Create default Active Directory claim acceptance rules Create VSS Express Witter for use with backup solutions	Status Configuration finished
	You have successfully completed the AD FS Federation Serv To close this wizard, click Close.	rer Configuration Wizard.

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 <u>https://<your federation service name>/federationmetadata/2007-</u> 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.

Not access the provide sector of the sector
https://sts.ofsil.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



Figure 19. Weblogic Physical Server - Identity Generation

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

	_ 0 _X
>\$JAVA HOME/bin/keytool -export -alias mykeyl -file rootl.cer -keystore identityl.jks -storepass password123	-
Certificate stored in file (rootl.ger>	

Figure 20. Weblogic Physical Server - Certificate Generation

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

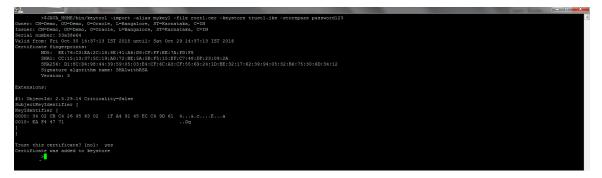


Figure 21. Weblogic Physical Server – Keystore Generation

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

8	-	~/ap	p/middleware	/user_pro	jects/	dom	ains/OFSI	LLREL_domain
F:)	FSLLREL d	omain	s pw	d		
/scratch/or	ac						ts/doma	ains/OFSLLREL domain
E-		0	FSLLREL d	omain]	\$ 11			
total 132								
drwxr-x		orafmw	oinstall	4096	Jul		15:57	autodeploy
drwxr-x		orafmw	oinstall	4096	Oct	14	18:39	
drwxr-x	11	orafmw	oinstall	4096	Jul		16:02	config
drwxr-x		orafmw	oinstall	4096	Jul		15:57	
drwxr		orafmw	oinstall	4096	Sep		11:43	discoverycache
-rw-r		orafmw	oinstall	32	Oct	29	16:09	edit.lok
-rw-r		orafmw	oinstall	462	Jul		15:59	fileRealm.properties
-rw-rr		orafmw	oinstall	2210	Oct	14	18:00	identity1.jks
-rw-rr		orafmw	oinstall	2255	Jul	21	23:020	identity.jks
drwxr-x		orafmw	oinstall	4096	Jul		15:59	init-info
drwxr-x		orafmw	oinstall	4096	Jul		12:23	
-rw		orafmw	oinstall	29968	Oct	29	15:11	nohup.out
drwxr							17:06	
drwxr		orafmw	oinstall	4096	Oct	14	18:46	
-rw-rr		orafmw	oinstall					
-rw-rr		orafmw	oinstall	905	Jul	21	23:020	root.cer
drwxr-x		orafmw	oinstall	4096	Jul		15:59	
drwxr								
-rw-r								shutdown.py
-rw-r								startManagedWebLogic_readme.txt
-rwxr-x								startWebLogic.sh
drwxr-x								
			oinstall				18:46	
-rw-rr								trust1.jks
-rw-rr						21	23:02	trust.jks
[0	FSLLREL d	omain]	Ş			

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

🔒 Home Log Ou	t Preferences	Recor	rd Help		Q							Welcome, weblogic Connected to: OF5LLREL_doma
Home >Summary	Home >Summary of Servers >OFSLL_ManagedServer2											
Settings for OFSLL_ManagedServer2												
Configuration	Protocols	Logging	Debug	Monitoring	Control	Deployments	Services	Security	Notes			
General Clust	er Services	Keysto	res SS	SL Federati	on Services	Deployment	Migration	Tuning	Overload	Health Monitoring	Server Start	rt Web Services
Click the Lock 8	Edit button in	n the Chang	ge Center	to modify the	settings on	this page.						
Save												
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:						Custor	n Identity an	d Custom 1	Trust Chang	e	Which o Info	ch configuration rules should be used for finding the server's identity and trust keystores? More
- Idontity												

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 P	eferences	Necord H	elp		٩										Wel	come, weblogic	Conne	ected to: OFS	LLREL_domai
Home >St	ummary of S	ervers >OF	SLL_ManagedS	erver2																
Settings f	or OFSLL_	4anaged	5erver2																	
Configur	ation Pr	otocols	Logging Debi	Jg M	onitoring	Control	Deployments	Services	Security	Notes										
General	Cluster	Services	Keystores	SSL	Federatio	on Services	Deployment	Migration	Tuning	Overload	Health Monitoring	Server Star	rt Web Service	s						
Save																				
Keyston	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.																			
Keystor	25:						Custon	Identity an	d Custom Ti	rust Chang	e	Whic Info	ch configuration ru	iles shoi	ld be used f	for finding t	he server's identil	ty and tr	ust keystores	? More
— Identi	- Identity																			
Custom	Identity K	eystore:					iden	ity.jks				The	The path and file name of the identity keystore. More Info							
Custom	Identity K	eystore 1	уре:				jks					The	The type of the keystore. Generally, this is JKS. More Info							
Custom	Identity K	eystore F	assphrase:				••••	•••••	•••••				The encrypted custom identity keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. More Info							
Confirm	Custom Id	lentity Ke	ystore Passp	hrase:			•••	•••••	•••••											
— Trust																				
Custom	Trust Key	store:					trust	iks				The	The path and file name of the custom trust keystore. More Info							
Custom	Trust Key	store Typ	e:				jks					The	type of the keyste	ore. Ger	ierally, this is	s JKS. Mo	re Info			
Custom	Trust Key	store Pas	sphrase:				••••	••••••	•••••				The custom trust keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. More Info						ithout a	
Confirm	Custom T	ust Keys	tore Passphra	ise:			•••	•••••	•••••											
Save																				

Figure 24. Weblogic Server – Keystore Settings

- » Click on SSL tab
 - » Private Key Alias \rightarrow 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

tings fo	r OFSLL	Managed	Server2															
onfigura	tion P	rotocols	Logging De	bug N	Monitoring	Control	Deployments	Services	Security	Notes								
eneral	Cluster	Services	Keystores	SSL	Federation	Services	Deployment	Migration	Tuning	Overload	Health Monitoring	Server Start	Web Services					
ave																		
his page	lets you	view and de	efine various S	ecure So	ickets Layer ((SSL) setti	ngs for this serv	er instance.	These setti	ings help you	to manage the secu	ity of message	transmissions.					
Identi	itv and 1	rust Loca	tions:					Keystores C	hange			Indica	ates where SSL sh	rould find the server's identity (certificate and private key) as well as the				
									lango					CAs). More Info				
Identity	v ——																	
rivate K	ey Locat	tion:					f	from Custom	Identity Ke	ystore		The k	eystore attribute	that defines the location of the private key file. More Info				
rivate K	ey Alias:							mykey					The keystore attribute that defines the string alias used to store and retrieve the server's private					
												key.	key. More Info					
Privat	e Key P	assphrase	s					•••••	•••••	•••			The keystore attribute that defines the passphrase used to retrieve the server's private key. More ${\rm Info}_{\cdots}$					
Confir	m Priva	te Key Pa	ssphrase:					•••••	•••••	••••								
ertificat	e Locati	on:					f	from Custom	Identity Ke	eystore		that defines the location of the trusted certificate. More Info						
Trust –																		
	ertificat	e Authori	ties:				f	from Custom	Trust Keys	tore		The k	The keystore attribute that defines the location of the certificate authorities. More Info					
usted C																		

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

Home >Sumn	nary of	Servers >OF	SLL_Mana	gedServe	r2									
ttings for (OFSLL	_Managed	Server2											
onfigurati	on F	rotocols	Logging	Debug	Monitoring	Control	Deployments	Services	Security	Notes				
General C	luster	Services	Keyston	es SSL	Federatio	on Services	Deployment	Migration	Tuning	Overload	Health Monitoring	Server Start	Web Services	
Save														
This page le	ts you	view and de	efine variou	s Secure !	Sockets Laye	r (SSL) setti	ngs for this serve	er instance.	These setti	ngs help you	to manage the secur	ity of message	transmissions.	
🔁 Identity	y and 1	frust Loca	tions:		I	Keystores	Change							ould find the server's identity (certificate and private key) as well as the CAs). More Info
Identity														
rivate Key	Loca	tion:				from Custon	n Identity Keysto	re				The l	eystore attribute	that defines the location of the private key file. More Info
rivate Key	/ Alias	•				mykey							More Info	that defines the string alias used to store and retrieve the server's private
🖶 Private	Key P	assphrase	s			•••••	•••••	•				The l Info.		that defines the passphrase used to retrieve the server's private key. $\ensuremath{\operatorname{More}}$
🗄 Confirm	ı Priva	te Key Pas	ssphrase:			•••••	•••••	•						
ertificate	Locati	on:				from Custon	n Identity Keysto	re				The	eystore attribute	that defines the location of the trusted certificate. More Info
rusted Ce	rtifica	te Authori	ties:			from Custor	n Trust Keystore					The	eystore attribute	that defines the location of the certificate authorities. More Info
⊽Advan	ced —													
🚰 Hostnai	me Ve	rification:				None		•						nore the installed implementation of the weblogic.security.SSL.HostnameVerifie rver is acting as a client to another application server). Nore Info
🗄 Custom	Hostr	name Veril	fier:									The I Info		that implements the weblogic.security.SSL.HostnameVerifier interface. More
xport Key	Lifesp	an:				500						and	an exportable dien	f times WebLogic Server can use an exportable key between a domestic serve th before generating a new key. The more secure you want WebLogic Server tr e key should be used before generating a new key. More Info
Use Ser	ver Ce	rts												t should use the server certificates/key as the client identity when initiating an ver https. More Info
wo Way C	lient C	ert Behav	ior:			Client Ce	rts Not Requ	ested		•		The	form of SSL that sh	nould be used. More Info
🗄 Cert Au	thenti	cator:										depr	ecated in this relea	dass that implements the weblogic.security.ad.CertAuthenticator dass, which ase of WebLogic Server. This field is for Compatibility security only, and is only adapter Authentication provider is configured. More Info
SSLReje	ection	Logging Er	abled									Indic rejec	ates whether warr ted. More Info	ning messages are logged in the server log when SSL connections are
🛛 街 Allov	w Unei	ncrypted N	Iull Cipher									Test	if the AllowUnEncr	ryptedNullCipher is enabled More Info
nbound Ce	rtifica	te Validat	ion:			Builtin S	SL Validation	Only		•		Indic	ates the client cer	tificate validation rules for inbound SSL. More Info
)utbound (ertific	ate Valida	ation:			Builtin St	SL Validation	Only		•		Indic	ates the server ce	ertificate validation rules for outbound SSL. More Info
🛛 🚑 Use	JSSE S	isl										Selec	t the JSSE SSL imp	elementation to be used in Weblogic. More Info
Save														

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 Preferen	ces 🔤 Record Help									
Home >Summary of Security Realms >myrealm >Providers >SAMLIdentityAssert > Providers										
reate a New Authentication Provider										
OK Cancel										
Create a new Authentic	ation Provider									
The following properties will * Indicates required fields	The following properties will be used to identify your new Authentication Provider. * Indicates required fields									
The name of the authenticat	ion provider.									
* Name:	SAMLIdentityAssert									
This is the type of authentica	ation provider you wish to create.									
Туре:	SAML2IdentityAsserter									
OK Cancel										

Figure 27. Weblogic Server - SAML2 Identity Asserter Setup

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

	Authentication Providers New Delete Reorder Showing 1 to 4 of 4 Previous								
	Name	Description	Version						
E] 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 ofsII_managedserver2 → Federation Services → SAML 2.0 Service Provider
- » Most fields can be left as default except noted below
 - » Enabled \rightarrow Checked
 - » Always Sign Authentication Requests → Checked
 - » Force Authentication → Unchecked
 - » Preferred Binding → POST
 - » Default URL → <u>https://<WeblogicServerName>:<ManagedServerPort>/ofsll142/faces/pages/OfsllHome.jspx</u>; for example <u>https://ofsll.oracle.com:9704/ofsll142/faces/pages/OfsllHome.jspx</u>
- » Save and Activate Changes

dministration Console						Ž
🟦 Home Log Out Preferences 🔤 Record Help	Q				Welcome, weblogic	Connected to: OFSLLREL_domai
Home >Summary of Servers >OFSLL_ManagedServer2						
Settings for OFSLL_ManagedServer2						
Configuration Protocols Logging Debug Moni	itoring Control Deployments Service	s Security Notes				
General Cluster Services Keystores SSL Fe	ederation Services Deployment Migra	ation Tuning Overload	Health Monitoring	Server Start	Web Services	
SAML 1.1 Source Site SAML 1.1 Destination Site SA	AML 2.0 General SAML 2.0 Identity Provide	SAML 2.0 Service Pr	ovider			
Click the Lock & Edit button in the Change Center to mo	odify the settings on this page.					
Save						
This page configures the SAML 2.0 per server service pro	ovider properties					
✓ Enabled				Specifies	whether the local site is enabled for the Service Provider role.	More Info
Always Sign Authentication Requests					whether authentication requests must be signed. If set, all outg ed. More Info	oing authentication requests
Force Authentication					whether the Identity Provider must authenticate users directly a context. The default is false. More Info	nd not use a previous
Passive					es whether the Identity Provider and the user must not take con requester and interact with the user in a noticeable fashion. The	
Only Accept Signed Assertions				Specifies	whether incoming SAML 2.0 assertions must be signed. More Ir	ıfo
Authentication Request Cache Size:	10000			The maxir	imum size of the authentication request cache. More Info	
Authentication Request Cache Timeout:	300			The maxir Info	imum timeout (in seconds) of <authnrequest> documents stored</authnrequest>	in the local cache. More
V POST One Use Check Enabled				Specifies	whether the POST one-use check is enabled. More Info	
V 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 🚽				the preferred binding type for endpoints of Service Provider service "Artifact". More Info	vices. Must be set to "None",
Default URL:	https://c	n:8005/ofsll142/faces	6/p	The Servi	ice Provider's default URL. More Info	
Save						
Click the Lock & Edit button in the Change Center to mo	dify 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 \rightarrow 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 \rightarrow Insert last name
- » Contact Person Type Select from list \rightarrow pick one doesn't matter which
- » Contact Person Company → Oracle
- » Contact Person Telephone Number → Insert a phone number
- » Contact Person Email Address \rightarrow Your email address
- » Organization Name → Oracle
- » Organization URL → http://www.oracle.com/
- » Published Site URL must be in format → <u>https://<WeblogicServerName>:<ManagedServerPort>/saml2;</u> for example <u>https://ofsll.oracle.com:9704/saml2</u>

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 \rightarrow Domain name or similar, this must be unique; for example sso_domain
- » Single Sign-on Signing Key Alias \rightarrow 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 \rightarrow Un-checked
- » Save and Activate Changes

» Restart the server

Home Log Out Preferences 🔤 Record Help	Q	Welcome, weblogic Connected to: OFSLLREL_d
ome >Summary of Servers >OFSLL_ManagedServer2		
tings for OFSLL_ManagedServer2		
nfiguration Protocols Logging Debug Monitoring	Control Deployments Services Security Notes	
eneral Cluster Services Keystores SSL Federati	ion Services Deployment Migration Tuning Overload Health Mo	nitoring 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	
ave Publish Meta Data		
Click the Lock & Edit button in the Change Center to modify the	e settings on this page.	
	a decenings on and pages	
This page configures the general SAML 2.0 per server properties	5	
General		
ළ <mark>ු</mark> 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		dunancason regocasa. Proceenonia
ontact Person Given Name:		The contact person given (first) name. More Info
ontact Person Surname:		The contact person surname (last name). More Info
ontact Person Type:	administrative v	The contact person type. More Info
		The analysis of the second
ontact Person Company:	Oracle	The contact person's company name. More Info
ontact Person Telephone Number:	1234567890	The contact person's telephone number. More Info
ontact 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
ublished Site URL:		
ublished Site URL:	http://cn:8003/saml2	The published site URL. More Info
ntity 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 dient authentication is required. More Info
ransport 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
ransport 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
onfirm Basic Authentication Password:		
Artifact Resolution Service		
Only Accept Signed Artifact Requests		Specifies whether incoming artifact requests must be signed. More Info
vrtifact Cache Size:	10000	The maximum size of the artifact cache. More Info
rtifact Cache Timeout:	300	The maximum timeout (in seconds) of artifacts stored in the local cache. More Info
Single Sign-on		
ingle Sign-on Signing Key Alias:	mykey	The keystore alias for the key to be used when signing documents. More Info
Single Sign-on Signing Key Pass Phrase:	•••••	The passphrase used to retrieve the local site's SSO signing key from the keystore. More Info
Confirm Single Sign-on Signing Key Pass Phrase:	•••••	
Save Publish Meta Data		

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.

ttings for OFSLL_M	anaged	Server2										
			Debug	Manthadaa	Control	Deployments	Comisso (-	Notes			
onfiguration Prot	ocois	Logging	Debug	Monitoring	Control	Deployments	Services	Security	Notes			
General Cluster	Services	Keystor	res SSL	Federati	on Service	s Deployment	Migration	Tuning	Overload	Health Monitoring	Server Start	Web Services
SAML 1.1 Source Site	SAML	1.1 Destin	nation Site	SAML 2.0) General	SAML 2.0 Ident	ity Provider	SAML 2.0	Service Prov	vider		
Save Publish Meta	Data											
Click the <i>Lock & Edit</i>	button in	the Chan	ge Center	to modify the	settings on	this page.						
blish SAML 2.0 Me	ta Data											
OK Cancel												
Metadata File Pro	perties											
Metadata File Pro	perties											
Metadata File Pro		metadata	a for this s	erver to a file								
		metadata	a for this s	erver to a file	•							
	SAML 2.0					a to.						
This page writes the	SAML 2.0		admin ser	ver) to write	the metadata							
This page writes the s Enter the name of the Path:	SAML 2.0 file (relat		admin ser		the metadata							
This page writes the source of the Enter the name of the Path:	SAML 2.0 file (relat		admin ser //	ver) to write mp/ofsll_m	the metadata	ni						
This page writes the	SAML 2.0 file (relat		admin ser //	ver) to write mp/ofsll_m	the metadata	ni						
This page writes the sentence of the Path: Recently Used Pat	SAML 2.0 file (relat		admin ser //	ver) to write mp/ofsll_m	the metadata	ni						
This page writes the Enter the name of the Path: Recently Used Pat Current Location:	SAML 2.0 file (relat hs:		admin ser //	ver) to write mp/ofsll_m	the metadata	ni						
This page writes the i Enter the name of the Path: Recently Used Pat Current Location: .ICE-unix .esd-10102	SAML 2.0 file (relat hs:	ive to the	admin ser //	ver) to write mp/ofsll_m	the metadata	ni						
This page writes the i Enter the name of the Path: Recently Used Pat Current Location: .ICE-unix .esd-10102 hsperfdata,	SAML 2.0 file (relat hs: _emcadm	ive to the	admin ser //	ver) to write mp/ofsll_m	the metadata	ni						
This page writes the i Enter the name of the Path: Recently Used Pat Current Location: .ICE-unix .esd-10102	SAML 2.0 file (relat hs: _emcadm _orafmw	ive to the	admin ser //	ver) to write mp/ofsll_m	the metadata	ni						

Figure 31. Weblogic Server – Publish Meta Data

» The Published ofsll_metadata.xml file would look as below

3	FLL_Metadata.xml - Notepad	
File Edit Format View Help		
<pre>c?xml version="1.0" encoding="UTF-8" standalone= rmd:EntityDescriptor xmlns:md="unr:oasis:namest: rdmd:SpOSoDescriptor AuthnRequestsSigned="false" rmd:KeyDescriptor use="signing"> cds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/ cds:X509Data> cds:X509Data> rds:X509Data rd</pre>	<pre>cc:SAML:2.0:metadata" entityID="sso_domain"> WantAssertionsSigned="false" protocolSupportEnumeration="urn /xmldsig#"> MQ@wGwYDVQQLEwRPRINTWRGwFQYD aFWcXDDA3MDUwNTASMjBaMCgxDTAL LMIIBIjANBgkqhkiG9w0BAQEFAADC BByyK7aY/IM4kxHpl+bK78IrD2Doi Htbl29QXVr4A+WAnu+trquyuuyLo AfbagWC2pQ1baKz91kcHzYwL37VbA g981+1TX2uUSM/11Dr1Ljn6nawrbg tc/0sXfwIDAQABoyEwHzAdBgWHQ4E H5QADggEBAEKhePABGy65K1ZgQ4Y9 klmeSntsNeBEI51AQLdB9smyEpAgf JIFFfrp1hWscWPSbIrnXE7DHZDqZ _jmWFRD8yU3dYpzpHtalkCRF+62E3</pre>	:oasis:names:tc:SAML:2.0:protocol">
<pre><md:assertionconsumerservice <br="" binding="urn:oasis:</pre></td><td>::names:tc:SAML:2.0:bindings:SOAP" index="0" location="http://</td><td>9452/saml2/sp/ars/soap">:9452/saml2/sp/acs/post" index= :9452/saml2/sp/acs/artifact</md:assertionconsumerservice></pre>		
2	Ш	

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 \rightarrow myrealm \rightarrow Providers \rightarrow 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
Home >Summary of Security Realms > <u>myrealm</u> >Providers > SAMLIdentityAssert	
Settings for SAMLIdentityAssert	
Configuration Management Migration	
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	
New v Delete	Showing 1 to 1 of 1 Previous Next
New Web Single Sign-On Identity Provider Partner	
New WebService Identity Provider Partner	
New Delete	Showing 1 to 1 of 1 Previous Next

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 5411 2.0 Web Single Sign	-on Identity Provider Partner
OK Cancel	
Partner Properties	
Use this page to:	
Enter the name of your new	Single Sign-on Identity Provider partner
 Specify the name and location 	n 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 cont	taining the partner metadata document.
Path:	(tmp)FederationMetadata.xm
Recently Used Paths:	/tmp
Current Location:	/ tmp
There are no files at the current locatio	n which are selectable. Choose a parent folder from the location links above or enter a new path.
OK Cancel	

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.

- $\ensuremath{\,{\rm w}}$ 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...>

(+)⊕ 🖻	FederationMetadata.xml	D-0 🥖	$\mathbf{FederationMetad}$ ×		
xml versio</td <td></td> <td></td> <td></td> <td></td> <td></td>					
	riptor xmlns="urn:oasis:names:tc:SAML:2.			/adfs/services/trust" ID="_8094bcef-04d8-4b58-9573-d23dda9907fc">	
	ODescriptor protocolSupportEnumeration="un	n:oasis:names:tc:S	AML:2.0:protocol">		
	yDescriptor use="encryption">				
	<keyinfo xmlns="http://www.w3.org/200</td><td>0/09/xmldsig#"></keyinfo>				
	- <x509data></x509data>	TD 4 - TO 4-001 4T	NR . In of cult TANR -	kghkiG9w0BAQsFADAgMSgwJgYDVQQDEx9BREZTIEVuY3J5cHRpb24gLSBzdHN	
	MIIC3DCCAC5gAw	ribagiQuzu8Lrw41	JNB+KXeOIGHIIIANBG	ĸqnĸiG9w0BAQSFADAqmSgwJgTDVQQDEX9BKEZTTEVuT3J3CHKpD24gLSB20HM	UB222DGWUT29CMB4XDTE1MDCyMT
	evDescriptor>				
	vDescriptor use="signing">				
	<kevinfo xmins="http://www.w3.org/200</td><td>0/09/xmldsia#"></kevinfo>				
	- <x509data></x509data>	1 I I I I I I I I I I I I I I I I I I I			
	<x509certificate>MIIC1jCCAb6qAw</x509certificate>	IBAqIQYdaJO01qR	6JAKPxvj8Vk3jANBgk	qhkiG9w0BAQsFADAnMSUwIwYDVQQDExxBREZTIFNpZ25pbmcqLSBzdHMub22	zbGwuY29tMB4XDTE1MDcyMTEyMz
	eyDescriptor>				
	igleLogoutService Location="https://:			nes:tc:SAML:2.0:bindings:HTTP-Redirect"/>	
	igleLogoutService Location="https://:			nes:tc:SAML:2.0:bindings:HTTP-POST"/>	
	meIDFormat>urn:oasis:names:tc:SAML:1.				
	meIDFormat>urn:oasis:names:tc:SAML:2.0				
	meIDFormat>urn:oasis:names:tc:SAML:2.0 ngleSignOnService Location="https://			nt> mes:tc:SAML:2.0:bindings:HTTP-Redirect*/>	
	igleSignOnService Location= https://			mes:tc:SAML:2.0:bindings:HTTP-Redirect /> mes:tc:SAML:2.0:bindings:HTTP-POST"/>	
				55" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"	
	Name="http://schemas.xmlsoap.org/ws/				
				NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"	
	Name="http://schemas.xmlsoap.org/ws/				
				ormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"	
P. C.	Name="http://schemas.xmlsoap.org/ws/	2005/05/identity/	claims/name"/>		
				rmat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"	
	Name="http://schemas.xmlsoap.org/ws/				
				ne" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"	
	Name="http://schemas.xmlsoap.org/clai				
				fail Address" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"	
	Name="http://schemas.xmlsoap.org/clain			Format="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"	
	Name="http://schemas.xmlsoap.org/clai		yname= Group namer	-ormat= urn:oasis:names:tc:SAML:2.0:attrname-format:uri	
				N" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"	
	Name="http://schemas.xmlsoap.org/clai		Viane AD 13 1.X OF	W Name of Mat- unit.ousis.numes.tc.SAME.2.0.utti nume formut.uni	
			vName="Role" NameFo	rmat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"	
	Name="http://schemas.microsoft.com/w				
				meFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"	
	Name="http://schemas.xmlsoap.org/ws/				
<att< td=""><td>ribute xmlns="urn:oasis:names:tc:SAML:2</td><td>0:assertion" Friend</td><td>yName="PPID" NameFo</td><td>ormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></att<>	ribute xmlns="urn:oasis:names:tc:SAML:2	0:assertion" Friend	yName="PPID" NameFo	ormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"	
	Name="http://schemas.xmlsoap.org/ws/				
	ribute xmlns="urn:oasis:names:tc:SAML:2	0:assertion" Friend	yName= "Name ID" Nar	meFormat="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	ettings for SAMLIdentityAssert								
Configuratio	Manageme	nt Migration							
On this pa	On this page, you can add, delete, and view SAML 2.0 identity provider partners for this SAML 2.0 Identity Asserter.								
🖟 Customiz	e this table								
Identity F	rovider Partne	5							
New ~	Delete		Showing 1 to 1 of 1 Previous Next						
🗖 Nam	e 🗠								
	SSO_IDP01								
New ~	Delete		Showing 1 to 1 of 1 Previous Next						

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 → /ofsII42/faces/*

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

- » Only Accept Signed Artifact Requests \rightarrow Checked
- » Save

1

dministrati	on Consol	0					Q
🟠 Home	Log Out Pre	ferences 🔤 Record Help	Q			Welcome, weblogic	Connected to: OFSLLREL_domain
Home >Su	ummary of Se	curity Realms >myrealm >Providers >S	AMLIdentityAssert >SAML_SSO_IDP0	1			
Settings fo	or SAMLIde	ntityAssert					
General	Site Info	Single Sign-On Signing Certificate	Transport Layer Client Certificate	Single Sign-On Service Endpoints	Artifact Resolution Service En	ndpoints	
Save							
Configur	es a SAML 2.	0 Web Single Sign-on Identity Provid	er Partner's General Properties				
The para	meters that	can be set on this Administration Cor	nsole page can also be accessed progr	ammatically via the Java interfaces	that are identified in this help to	ppic. For API information about those interfaces, see Related Topics.	
— Overvi	iew						
Name:			SAML_SSO_IDP01		The	e name of this Identity Provider partner. More Info	
🔽 Enabl	led				Spei	ecifies whether interactions with this Identity Provider partner are enal	bled on this server. More
Descript	ion:		SAML_SSO_IDP01		A sh	hort description of this Identity Provider partner. More Info	
— Auther	ntication Re	equests					
Identity	Provider N	ame Mapper Class Name:				e Java class that overrides the default username mapper class with where reprovider is configured in this security realm. More Info	ich the SAML 2.0 Identity
Issuer U	RI:		http://sts.ofsll.com/adfs/s	ervices/trust	The	Issuer URI of this Identity Provider partner. More Info	
Virtua	al User				Spe are	edifies whether user information contained in assertions received from mapped to virtual users in this security realm. More Info	this Identity Provider partner
Redirect	URIs:					optional set of URIs from which unauthenticated users will be redirecte	ed to the Identity Provider
/ofsll	L142/fac	es/*			part	ther. More Info	
/FCJNe	eoWebul/	- *	al and				
V Proce	ess Attribut	es			Spease	ecifies whether the SAML 2.0 Identity Asserter provider consumes attri ertions received from this Identity Provider partner. More Info	ibute statements contained in
— Signing	g						
Only Acc	ept Signed	Authentication Requests:	false		Spe Info	ecifies whether authentication requests sent to this Identity Provider p o	arther must be signed. More
✓ Only .		ed Artifact Requests				edies whether SAML artifact requests received from this Identity Prov ned. More Info	ider partner must be
	Artifact via	POCT			Con	cifies whether SAML artifacts are delivered to this Identity Provider pa	artner via the HTTP POST
E Schu	Artifuce vic					thod. More Info	
Artifact	Binding POS	ST Form:			for J	URL of the custom web application that generates the POST form for Artifact bindings to this Identity Provider partner, Details about the re dication are available in the OASIS SAML 2.0 specifications. More Infi	equired fields in this custom
POST Bin	iding POST	Form:				URL of the custom web application that generates the POST form for POST bindings to this Identity Provider partner. More Info	carrying the SAML response
Client Us	ser Name:					e user name that must be specified in the basic authentication header t ntity Provider partner when the partner connects to the local site's SO 0	
Client Pa	issword:				The	e password of the client user name. More Info	
Confirm	Client Pass	word:					
Save							

Figure 37. Weblogic Domain - Identity Provider

Configure Domain for SSO

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

A Home Log Out Preferences 🐼 Record Help	Welcome, weblogic Connected to: OF5LLREL_domain
Home >Summary of Servers >OFSLL_ManagedServer2 >Summary of Security Realms >myrealm >Providers >SAMLIdentityAssert >SAML_SSO_IDP01 >Summary of Security Realms >myrealm >Providers	
Create a New Authentication Provider	
OK Cancel	
Create a new Authentication Provider	
The following properties will be used to identify your new Authentication Provider. * Indicates required fields	
The name of the authentication provider.	
Name: NtyAD/Authenticator	
This is the type of authentication provider you wish to create.	
Type: ActiveDirectoryAuthenticator	
OK Cancel	

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=ofsII, DC=com

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

- » Credential \rightarrow password of administrator
- » User Base DN → OU=MyOrg, DC=ofsII, 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 \rightarrow (&(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

tings for MyADAuthenticator		
onfiguration Performance		
Common Provider Specific		
lick the Lock & Editbutton in the Change Center to modify the settings on this page.		
Jse this page to define the provider specific configuration for this Active Directory Authentical	tion provider	
See this page to denne the provider specific configuration for this Active Directory Authentical	uon provider,	
Host:	N 1	The host name or IP address of the LDAP server. More Info
음 Port:	389	The port number on which the LDAP server is listening. More Info
물 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
redential:		The credential (usually a password) used to connect to the LDAP server. More Info
onfirm Credential:	•••••	
∃ d∰ SSLEnabled		Specifies whether the SSL protocol should be used when connecting to the LDAP server. More Info.
Users	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 emoty), a default
		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
a and a sector of the sector o		
		Specifies whether or not the user name retrieved from the LDAP server should be used as the Principa in the Subject. More Info
Groups	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 droup scheme. Mere Info
g Group From Name Filter:	(&(cn=%g)(objectclass	An LDAP search life 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 scheme. More Lpfo:
n Group Search Scope:	subtree 👻	Specifies how deep in the LDAP directory tree to search for groups. Valid values are subtree and onelevel. More Info
Course Manufacture Courses		
읍 Group Membership Searching:	unlimited 👻	Specifies whether group searches into nested groups are unlimited or limited. Valid values are unlimite and limited. More Info
है Max Group Membership Search Level:	0	Specifies how many levels of group membership can be searched. This setting is valid only if Group/membership/secriting is set to limited. Value 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
ाgnore Duplicate Membership		Determines whether duplicate members are ignored when adding groups. The attribute cycles in the Group membership. More Info
생 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		standard recursive group membership lookup algorithm. More Info
E Static Group Name Attribute:	cn	The attribute of a static LDAP group object that specifies the name of the group. More Info
号 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. Nore Info
🖥 Static Group DNs from Hember DN Filter: Dynamic Groups	(&(member=%M)(objec	An LDAP search filter that, given the distinguished name (DN) of a member of a group, returns the DN 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.
Bynamic 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 dynam group. More Info
십 User Dynamic Group DN Attribute:		The attribute of an LDAP user object that specifies the distinguished names (DNs) of dynamic groups i which this user belongs. More Info
General	6	The LDAP connection pool size. Default is 6. More Info
2 Connect Timeout:	0	The maximum time in seconds to wait for the connection to the LDAP server to be established. If this
	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
	-	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
A Reep Alive Enabled		Specifies whether to prevent LDAP connections from timing out. More Info
dि 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. M Info
a 🖞 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 stribute. How Enfo.,
🕂 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
음 Cache Size:	32	The size of the cache (in klobytes) that is used with the LDAP server More Info
	60	The time-to-live of the cache (in seconds) that is used with the LDAP server More Info
Cache TTL:		
] Cache TTL:	objectguid	Specifies the name of the GUID attribute defined in the Active Directory LDAP server. The default value is objectpuid. More Info

Figure 39. Weblogic Domain – Provider Specific Details

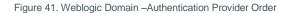
» Ensure the AD Provider Control Flag is set as either Optional or Sufficient

🔒 Home Log Out Preferences 🛛	Record Help	
Home >Summary of Security Realms	s >myrealm >Providers >MyADAuthenticator	
Settings for MyADAuthenticato	or and the second se	
Configuration Performance		
Common Provider Specific		
Save		
This page displays basic informati	ion about this Active Directory Authentication provider. You can also use this page to set the J4	AAS Control Flag to control how t
This page displays basic informati	ion about this Active Directory Authentication provider. You can also use this page to set the JA MyADAuthenticator	AAS Control Flag to control how t
		AAS Control Flag to control how f
a Name:	MyADAuthenticator	AAS Control Flag to control how f

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 n	Settings for myrealm									
Configuration	Users and Groups	Roles and Policies	Credential Mappings	Providers	Migration	1				
Authentical	ion Password Valida	tion Authorization	Adjudication R	ole Mapping	Auditing	Credential Mapping	Certification Path	Keystores		
	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.									
Authentica	tion Providers	Change Center to act	ivate all the buttons of	on this page.						
New D										
🗌 Name			Description							Version
SAMLIC	entityAssert	:	SAML 2.0 Identity As	ertion Provider	. Supports 9	ecurity Assertion Ma	arkup Language v2.0.			1.0
MyADA	uthenticator	1	Provider that perform	s LDAP authen	tication					1.0
Default	Authenticator		WebLogic Authentica	ion Provider						1.0
Default	IdentityAsserter		WebLogic Identity As	sertion provide	r					1.0
New D	New Delete Rearder Showing 1 to 4 of 4 Previous Next									



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

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

Configure Relying Party

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

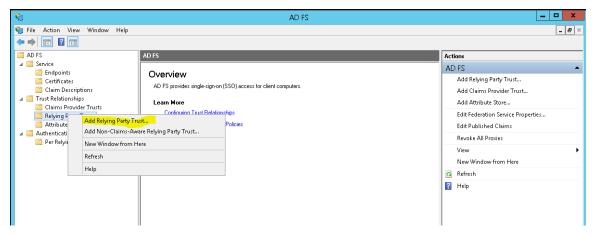


Figure 42. AD FS Server - Relying Party Trust

» Click start on the Welcome Page

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

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

Select Data Source Steps Select an option that this wizard will use to obtain data about this relying party: • Welcome Import data about the relying party published online or on a local network. • Select Data Source Configure Multi-factor Authentication Now? • Choose Issuance Authorization Rules Federation metadata address (host name or URL): • Finish Import data about the relying party from a file • Finish Import data about the relying party from a file • Select Is federation metadata is file Location: [C:M] Selectation metadata is in file Location: [C:M] • Finish Import data about the relying party manually Use this option to import the necessary data about this relying party organization.	\$	Add Relying Party Trust Wizard
 Welcome Select an option that this wizard will use to obtain data about this reging 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): 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:\U vofsll_metadata.xml Enter data about the relying party manually 	Select Data Source	
< Previous Next > Cancel	 Welcome Select Data Source Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust 	 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:V vofsl_metadata.xml Browse 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	x
Some of the content in the federation metadata was skipped because it is not supported by AD FS. Review of the trust carefully before you save the trust to the AD FS configuration database.	the properties
	OK

Figure 45. AD FS Server – Warning Message

» Provide an unique Display Name and click Next

\$	Add Relying Party Trust Wizard	x
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	OFSLL_SSO	
🥥 Specify Display Name	Notes:	
 Configure Multi-factor Authentication Now? 		-
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
💿 Finish		<u> </u>
	< Previous Next > Cancel]

Figure 46. AD FS Server - Relying Party Display Name

» Retain the default as shown below and continue Next

\$	Add Relying Party Trust Wizard	x
Steps	Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required	l if
 Welcome 	there is a match for any of the specified requirements.	
Select Data Source		7
Specify Display Name	Multi-factor Authentication Global Settings	_
Configure Multi-factor Authentication Now?	Requirements Users/Groups Not configured	
Choose Issuance	Device Not configured	
Authorization Rules	Location Not configured	
 Ready to Add Trust Finish 		
	 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 <u>Configuring Authentication Policies</u>. 	e
	< Previous Next > Cancel	

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.					
	< Previous Cancel					

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

\$	Add Relying Party Trust Wizard
Ready to Add Trust	
Steps • Welcome • Select Data Source • Specify Display Name • Configure Multi-factor Authentication Now? • Choose Issuance Authorization Rules • Ready to Add Trust • Finish	Image: Control of the series of the serie

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	x
Ready to Add Trust		
Ready to Add Trust 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 Not < Specify the signature verification certificates for requests from this relying party. Subject Issuer Effective Date Expiration Date Image: CN=ofss2200 CN=ofss220081 7/21/2015 11:0 7/20/2016 11:0	>
	<pre> View </pre> Cancel	

Figure 50. AD FS Server – Signature Tab

» Certificate details can be reviewed

6 8	(Certificate 🛛 🗙
General De	tails Certification F	Path
Show: <a< td=""><td> ></td><td>~</td></a<>	>	~
Field		Value 🔨
C Version		V3
Serial n		4a 39 4b 4b
	ire algorithm	sha1RSA =
	ire hash algorithm	sha1
Issuer		, Or
Valid fr Valid to		Tuesday, July 21, 2015 11:02
Subject		Wednesday, July 20, 2016 11 , Or 🗸
	•	, or 🗸
,		
		Edit Properties Copy to File
		OK

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"

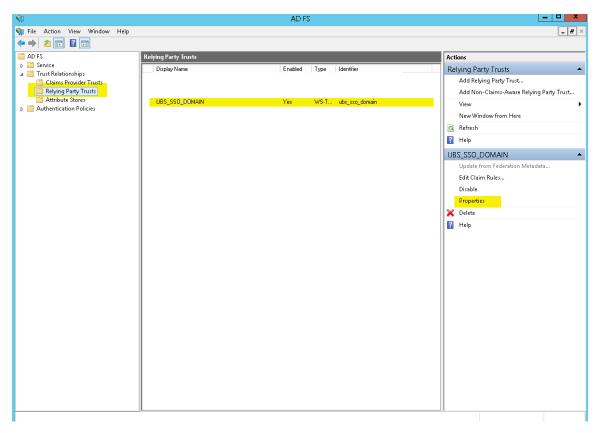


Figure 52. AD FS Server - Edit Relying Party Trust

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

UBS_SSO_DOMAIN Properties								
Monitoring Identifiers	Encryption	Signature	Accepted Claims					
Organization Endpoints	Proxy End	lpoints No	tes Advanced					
Specify the secure hash a	Specify the secure hash algorithm to use for this relying party trust.							
Secure hash algorithm:	SHA-1		~					
	SHA-1							
	SHA-256							
L	014							
	OK	Cancel	Apply					

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

Figure 53. AD FS Relying Party – Advanced Tab

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

UBS_SSO_DOMAIN Properties						
Organization	dentifiers Endpoints	Encryption Proxy Enc			anced	
URL SAML Assert		Ind	ex Binding		Re	
https://		0	POST	No		
https://		1	Artifact			
<		111			>	
Add SAML						
Add WS-Feder	ation		Remov	e Edi	t	
	[OK	Cance	el A	pply	

Figure 54. AD FS Relying Party - Endpoints Tab

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

	Edit Endpoint 🛛 🗙
Endpoint type:	
SAML Assertion Consum	er v
Binding:	
POST	~
Set the trusted URL a	as default
Index: 0 🗘	
Trusted URL:	
https://c	:8005/saml2/sp/acs/post
Example: https://sts.con	toso.com/adfs/ls
Response URL:	
Example: https://sts.com	toso.com/logout
	OK Cancel

Figure 55. AD FS Relying Party - Add Endpoint

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

	Edit Endpoint X
Endpoint type:	
SAML Assertion Consumer	r 🗸
Binding:	
Artifact	~
Set the trusted URL as	default
Index: 1 😳	
Trusted URL:	
https:///	:8005/saml2/sp/acs/artifacts
Example: https://sts.conto	so.com/adfs/ls
Response URL:	
Example: https://sts.conto	so.com/logout OK Cancel

Figure 56. AD FS Relying Party - Add Endpoint

Adding Rules

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

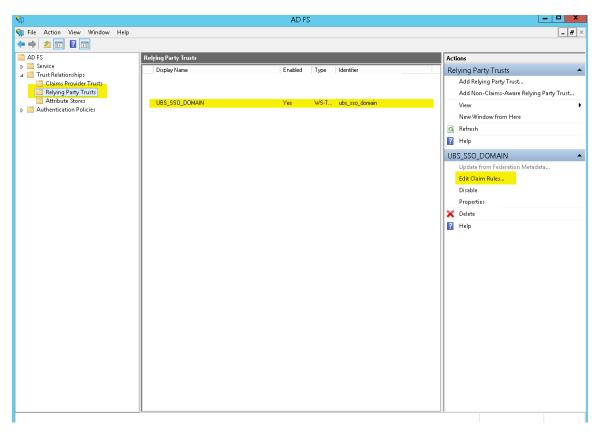


Figure 57. AD FS Relying Party - Edit Claims

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

\$ 1		: Claim R					-		x
Issuance	Transform Rules	Issuance	Authorizati	on Rules	: Delega	tion Authori	zation F	lules	
The foll	owing transform r	ules specify	the claims	that will	be sent to) the relying	party.		
Order	Rule Name				Issued Cla	aims			
1	Name				Name ID				
2	GivenName				Given Na	me			
								•	
Add F	Rule Edit F	Rule	Remove F	lule					
				01	κ [Cancel		Apply	

Figure 58. AD FS Relying Party – Add Rules

» Click on Next

\$	Add Transform Claim Rule Wizard
Select Rule Template	
Steps Choose Rule Type Configure Claim Rule	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 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.
	< Previous Next > Cancel

Figure 59. AD FS Relying Party - Rule Template

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

	Editl	Rule - Name 🛛 🗙					
which to	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 ru	le name:						
Name							
Rule ter	nplate: Send LDAP Attributes as Claims						
Attribute	e store:						
Active [Directory	v					
Mapping	g of LDAP attributes to outgoing claim type	35.					
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)					
•	SAM-Account-Name	Name ID 🗸 🗸 🗸					
*	¥						
View F	Rule Language	OK Cancel					

Figure 60. AD FS Relying Party - Add Name Rule

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

		Edit Rule	e - GivenNa	me	X		
which to	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 ru	le name:						
GivenN	ame						
Rule ter	mplate: Send LDA	P Attributes as Claims					
Attribute	e store:						
Active [Directory		~				
Mapping	g of LDAP attribute	es to outgoing claim type:	s:				
	LDAP Attribute (: add more)	Select or type to	Outgoing Claim	n Type (Select or type to add	more)		
•	Given-Name	~	Given Name		~		
*		~			×		
View F	Rule Language]		OK	Cancel		

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 \rightarrow Tools \rightarrow Active Directory Users and Computers
- » Click on the domain name at the left pane and right click, select New \rightarrow Organizational Unit
- » Enter a name for the Organization Unit and click OK

New Object - Organizational Unit	x
Create in: ofsll.com/	
Name:	
МуОгд	
Protect container from accidental deletion	
OK Cancel Help	

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 \rightarrow Group
- $\boldsymbol{\ast}$ Enter a name for the Group, other values can be default and click OK

New	New Object - Group					
Create in: ofsll.com/l	MyOrg					
Group name:						
OFSLL_USERS						
Group name (pre-Windows 2000): OFSLL_USERS						
Group scope	Group type					
🔿 Domain local	 Security 					
Global						
○ Universal						
	OK Cancel					

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 \rightarrow User
- » Enter name of the User, provide a unique name for the User Logon field and click Next until User Id is created

	New Ot	oject - U	ser		x
🧏 Create in:	ofsll.com/MyO	rg			
First name:	OFSLLUSR		Initials:		
Last name:	USer				
Full name:	OFSLLUSR US	er			
User logon name:					
ofsllusr	[@ofsll.com		~	
User logon name (pre	Windows 2000):				
OFSLLV		ofsllusr			
		< Back	Next >	Cancel	

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 Grou	ups 🛛 🗙
Select this object type: Groups or Built-in security principals	Object Types
From this location: ofsll.com	Locations
Enter the object names to select (<u>examples</u>): OFSLL_USERS	Check Names
Advanced	OK Cancel

Figure 65. AD – Group Mapping

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

Addition of Active Directory Groups in EM

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

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

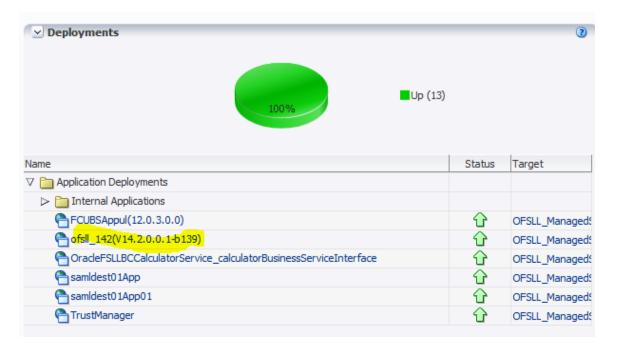


Figure 66. Weblogic EM – Deployments

» Select Application Deployment -> Security -> Application Roles

Home			1				
Control			F			(2 🕀 🔹
Logs			To configure and manage this WebLogic		Applicat	tion	
Performance Summary			Deployment, use the <u>Oracle WebLogic Server</u> Administration Console.		2		
Application De	ployment		F	Administratio	on Console.		
Web Services				-			
WebCenter P	ortal		⊧ ^{er}	2			
ADF			۰	EJBs			
Security			F I	Application Policies	Beans in Use	0	
MDS Configur	ation			Application Roles	Bean Accesses (per minute)	0.00	
TopLink Sessi	ons		12		Bean Access Successes (%)	0.00	
System MBea				Bean Tr	ansaction Commits (per minute)	0.00	
· ·			-1	Bean Tra	nsaction Rollbacks (per minute)	0.00	
T WebLogic Ser	ver Administratio	on Console	-1	Bean Transaction Timeouts (per minute)		0.00).00
General Infor	mation		J		Bean Transaction Commits (%)	0.00	
Entry Poin	ts					-	۰.
Web Modules							
Name	Test Poin	nt					
ofsll 142	http://			3003/ofsll142			
ofsll 142	https:/			:8005/ofsll142			
Web Services							
Service Name		Port					Test
No Web Service	F 1						

Figure 67. Weblogic EM – Application Roles

» Click on "Execute" button and below details shows up

Implement <	ofsll_142(V14.2	2.0.0.1-b139) 🕦		Logged in as weblogic Host
parkator roles are the roles used by security wave 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 reated in the context of end users accessing the application. We the <u>Cracket WebLogic Server Security Provider</u> Policy Store Provider Scope WebLogic Domain Provider DB_ORACLE Provider DB_ORACLE Provider Deplay Name Description Possel USER Provider Deplay Name Description Provider Description Provider Description Provider Description Provider Description Provider Deplay Name Description Provider Description Provider Deplay Name Description Provider Description Provider Deplay Name Description Provider Description Provider Description Provider Description Provider Deplay Name Description Provider D	Application Deployment	•		Page Refreshed Oct 30, 2015 5:54:22 PM IST
> Policy Store Provider Scope Weblog: Domain Provider DB_ORACLE > Search Enter search keyword for roles name to query roles defined by this application. Use application uses a stripe that is differerent from application name. Role Name Starts With ② Create ③ Oresit Like ③ Oresit Like ● Departy Name ○ OPSIL_USER ○ OPSIL USER	reated in the context of e	nd users accessing the application.		s in single global policy store when the applications are registered. These are also application roles that are
Scope WebLogic Domain Provider D6 Scape WebLogic Domain Enter search keyword for role name to query roles defined by this application, stripe to search if application uses a stripe that is differerent from application name. Role Name Stripts @ Create Like @ Edite Like @ Create Like @ Edite Like @ Create Like @ Description OFSUL_USER OFSUL_USER	To manage users and g	groups in the WebLogic Domain, use the	de WebLogic Server Security Provider.	
Provider DB_ORACLE Search Enter search Keyword for role name to query roles defined by this application. Use application uses a stripe that is different from application name. Role Name Starts With Create Create Create.	≥ Policy Store Provide	er		
✓ 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 different from application name. Role Name Starts With ↓ Or Create ♥ Create Like ♥ Edt ♥ Delete Role Name Display Name OFSL_USER OFSL_USER		Scope WebLogic Domain		
Enter search keyword for role name to query roles defined by this application. Use application uses a stripe that is different from application name. Role Name Starts With Image: Control of the strip of t		Provider DB_ORACLE		
Role Name Starts With Image: Control of Starts Image: Control of Control of Starts Image: Control of Starts Image: Control of Starts Image: Control of	≤ Search			
Image: Create	Enter search keyword for	r role name to query roles defined by t		hat is differerent from application name.
Inde Name Display Name Description OFSUL_USER OFSUL_USER		Role Name Starts With 💌		
OFBL_USER OFBL USER >> Membership for OFSLL_USER Principal Display Name Type Description	Create 🛛 😭 Cr	reate Like 🥜 Edit 💥 Delete.		
Yembership for OFSLL_USER Principal Display Name Type Description	Role Name	Display Name	Description	
Principal Display Name Type Description	OFSLL_USER	OFSLL USER		
Principal Display Name Type Description				
Principal Display Name Type Description				
Principal Display Name Type Description				
Principal Display Name Type Description				
Principal Display Name Type Description				
Principal Display Name Type Description				
Principal Display Name Type Description				
Principal Display Name Type Description				
Principal Display Name Type Description				
Principal Display Name Type Description				
	≤ Membership for 0	FSLL_USER		
	Principal	Display Name	Description	

Figure 68. Weblogic EM – Application Roles

» Click on "Edit"

ofsll_142(V	(14.2.0.0.1-b139) 🕦			Logged in as weblogic Host
Application Deplo	oyment -			Page Refreshed Oct 30, 2015 5:54:22 PM IST 🕻
		ns that are specific to the ap	oplication. These roles are seeded by applications in single global policy store when th	e applications are registered. These are also application roles that are
To manage user	s and groups in the WebLogic Domain, use t	he <u>Oracle WebLogic Server S</u>	Security Provider.	
≥ Policy Store F	Provider			
	Scope WebLogic Domain			
	Provider DB_ORACLE			
⊻ Search				
Enter search keyv	vord for role name to query roles defined by	this application. Use applica	tion stripe to search if application uses a stripe that is differerent from application na	ime.
	Role Name Starts With 💌			
Create	😭 Create Like 🧪 Edit 🗶 Delet	e		
Role Name	Display Name		Description	
OFSLL_USER	OFSLL USER			
⊻ Membership	for OFSLL_USER			
	Display Name	Type	Description	
Principal	Display Malle	Type	Description	

Figure 69. Weblogic EM – Edit Application Roles

» Click on Members \rightarrow "Add"

	.0.0.1-b139) 🔋		Logged in as web
Application Deployment	•		Page Re
lication Roles > Edit App	Dication Role		
Application Role			
eneral	_		
Application Stripe	ofsll_142#V14.2.0.0.1-b139		
Role Name	OFSLL_USER		
Display Name	OFSLL USER		
Description			
embers			
	eed to be mapped to users or groups defined in enterprise LDAP server, or t	e role can be mapped to other application roles.	
🕂 Add 🕺 Delete			
Add X Delete		Display Name	Туре

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 se	lect the application	roles that you want to	grant perm	issions to.
✓ Search				
Туре	Group	•		
Principal Name	Starts With 💌			
Display Name	Starts With 💌			
Searched Principals				
Principal	Display Na	ime	Description	
Advanced Option				
Check to enter princi		ad of searching from a custom authenticators		option can be
Type Group 💌 * Prin	cipal Name OFSLL	USERS		
Dis	play Name OFSLL	USERS		
				OK Cancel

Figure 71. Weblogic EM – Addition of Enterprise Roles

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

Addition of Application Roles in EM

This is particular settings is only required for granting access permission to the Customer Service screen, wherein the customer service screen is accessed directly from outside the 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	U p (13)		3
Name		Status	Target
Internal Applications			
FCUBSAppul(12.0.3.0.0)		Û	OFSLL_Managed
C ofsl_142(V14.2.0.0.1-b139)		Û	OFSLL_Managed
OracleFSLLBCCalculatorService_calculatorBusinessServiceInterf	ace	Û	OFSLL_Managed
amldest0 1App		Û	OFSLL_Managed
Samldest01App01		Û	OFSLL_Managed
TrustManager		Û	OFSLL_Managed

Figure 72. Weblogic EM –Deployments

» Select Application Deployment -> Security -> Application Policies

ofss220081.in.oracle.com:8001/em/faces/as/wIFi	rmHome?target=Farm_OFSLLREL_domain&type=oracle_jas_farm&_afrLoop=7206551856825141#%2Fas%2Fsecurity%	%2FappPoliciesMain!	☆ 自 ♣ 合
DRACLE Enterprise Manager 11g Fusion Mi	ddieware Control		Setup + Help + L
Farm - 👗 Topology			a south a south a south a
Constant Section	ofsll_142(V14.2.0.0.1-b139) o formation formation	rants assigned to the principals. Click on searched princip	Logged in as weblegic (host offs22008 Lin.orad Page Referend Oct 16, 2015 6 Jileo J PH 15 al to query policies assigned.
	Permissions		
		Permission Actions	Permission Class
	Permissions	Permission Actions view	Permission Class orade.adf.controller.security.TaskFlowPermission
	Permissions Resource Name / WEB 24 Fordel Jupattern Johannik Shell (Infra Johank, uml 4blank / WEB 24 Fordel Androng Com /, *		oracle.adf.controller.security.TaskFlowPermission oracle.adf.controller.security.TaskFlowPermission
	Permissions Resource Name //VEB-INF (oracle, iu/pattern/dynamicShel/nfra_blank.uml#blank	view	oracle.adf.controller.security.TaskFlowPermission

Figure 73. Weblogic EM –Security Policies

» Below detail shows up

Policy Store Provider				
Search				
elect an application stripe in pr	olicy store , select principal type and ent	ter search keyword to query application security	grants assigned to the principals. Click on searched princi	pal to query policies assigned.
Principal	al Type Application Role 💌			
	Name Starts With 💌	•		
1. 1.				
incipal	Display Name	Description		
FSLL_USER	OFSLL USER			
nonymous-role	Anonymous Role			
unitation for OFELL USER				
volicies for OFSLL_USEF	٤			
-	R			
ermissions	R			
ermissions Resource Name			Permission Actions	Permission Class
ermissions lesource Name WEB-INF/oracle/ui/pattern/d	R dynamicShell/nfra/blank.xml#blank		view	oracle.adf.controller.security.TaskFlowPermissio
rermissions Resource Name /WEB-INF/oracle/ui/pattern/c /WEB-INF/taskflows/cmn/.*	dynamicShell/infra/blank.xml#blank			oracle.adf.controller.security.TaskFlowPermissic oracle.adf.controller.security.TaskFlowPermissic
Policies for OFSLL_USEF Permissions Resource Name (NEB-INF/orade/u/patten/i/ WEB-INF/askflows/ormin-it	dynamicShell/infra/blank.xml#blank		view	oracle.adf.controller.security.TaskFlowPermissio

Figure 74. Weblogic EM – Application Policies

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

Application Policies > Edit Applicati Edit Application Grant	ion Grant			ОК	Cancel
Application Stripe ofsl_142#V1	4.2.0.0.1-b139				
Grantee					
Select the grantees (user, grou	up or application role) you want to add to th	ne policy.			
🕂 Add 🛛 💥 Delete					
Name	Display Name	Type	Description		
OFSLL_USER	OFSLL USER	Application Role			
Permissions					
👍 Add 🥒 Edit 💥 De	elete				
Permission Class		Resou	urce 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	E
oracle.adf.controller.security	.TaskFlowPermission	/WEB	-INF/taskflows/origination/.*	view	
oracle.adf.share.security.aut	thorization.RegionPermission	oracle	ofsll.view.pagedefs.templates.OfsllCanvasPageTemplatePageDef	view	
oracle.adf.share.security.aut	thorization.RegionPermission	oracle	ofsll.view.pagedefs.pages.OfsllHomePageDef	view	-
and the solid shares as a solid solid	de antre Reis Dis eter De antre la stra	and all all all all all all all all all al			

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

plication Stripe ofsll_142#V1	4 2 0 0 1 4 139			
rantee	.2.0.0.10109			
	p or application role) you want to add to the	noicy		
Add 💥 Delete	p or application roley you want to add to the	poncy.		
Name	Display Name	Туре	Description	
OFSLL USER	OFSLL USER	Application Role		
rmissions				
🗜 Add 🖉 Edit 💥 De	lete	Resou	rre Name	Permission Actions
🗜 Add 🖉 Edit 💥 De Permission Class			rce Name Ni [©] forade /u/loattern/dvnamicShell/infra/blank.xml≠blank	Permission Actions
Add / Edit X De Permission Class orade.adf.controller.security	TaskFlowPermission	/WEB-1	rce Name INF/orade,Julpattern/dynamicShell/nfra/blank.xml≢blank INF/blashRows/cmn/.*	
Edit X De Permission Class orade.adf.controller.security orade.adf.controller.security	TaskFlowPermission TaskFlowPermission	/WEB-1 /WEB-1	INF/oracle/ui/pattern/dynamicShell/infra/blank.xml#blank	view
Edit & De Permission Class oracle.adf.controller.security oracle.adf.controller.security oracle.adf.controller.security.adf	TaskFlowPermission TaskFlowPermission TaskFlowPermission	/WEB-1 /WEB-1 /WEB-1 /WEB-1	INF/orade/ui/pattern/dynamicShell/infra/blank.xml#blank INF/taskflows/cmn/.*	view view
Add // Edit & De Permission Class orade.adf.controller.security orade.adf.controller.security orade.adf.controller.security	TaskFlowPermission TaskFlowPermission TaskFlowPermission horization.RegionPermission	/WEB-1 /WEB-1 /WEB-1 /WEB-1 oracle-	NF/oracle,lui/pattern/dynamicShell/infra/blank.xml≠blank INF/taskflows/cmn/.* INF/taskflows/origination/.*	view view 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 permis	ssions.
≤ 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.	Continue Cancel

Figure 77. Weblogic EM – Add Permission

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

Add Permission	1	×
	issions and resources used in this application. Enter search criteria to search for right permissions. ce or actions for selected permission.	
Customize		
* Permission Class	oracle.adf.share.security.authorization.RegionPermission	
Resource Name	oracle.ofsll.view.pagedefs.pages.OfsllCustomerServicePageDef	
Permission Actions	view	
	Back Select Cancel	

Figure 78. Weblogic EM – Add Permission

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

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

Constitution and Angel -	the second s								
د الله معند (Altor Altor Alto	X O Waiting for	A ☆ ⊕							
There is a problem with this website's security certifi	cate.								
The security certificate presented by this website was not issued	The security certificate presented by this website was not issued by a trusted certificate authority.								
Security certificate problems may indicate an attempt to fool yo server.	u or intercept any data you send to the								
We recommend that you close this webpage and do not con	tinue to this website.								
Click here to close this webpage.									
Continue to this website (not recommended).	Windows Security								
More information	Connecting to sts.ofull.com.								

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

» On successful authentication, OFSLL Home page opens up

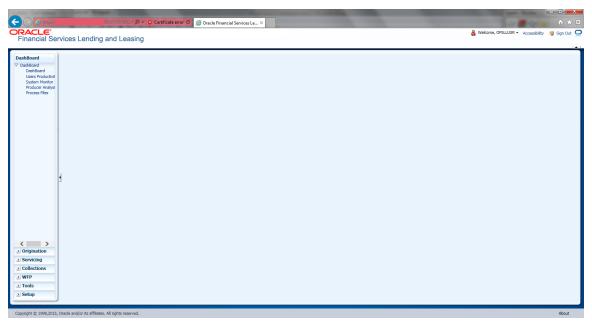


Figure 80. Internet Explorer: OFSLL Home Page

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

🗋 Sign In	×	the second se	Statement and American State	Concession of the local division of the loca	and the second se	
← ⇒ C fi	SAM	ILRequest=fZBNa8MwDIb%2FitE9i	ie18rDFxSqEUChuMrdthl%2BI5z	hpw7CxySn%2F%2BspSx7rKjkB69e	elStL70lZzNi550EFlMgxmnfdC	D5DwsthF61gXVeoejuIzRRO7sl8TgYE☆ 〓
					sts.ofsll.com	1
					Sign in with your orga	nizational account
					ofsllusr@ofsll.com	
					Sign in	
					/	
					-	
					© 2013 Microsoft	

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

Troubleshooting

- » AD FS related alerts can be viewed and monitored within the AD Server as part of Server Management Console
- » On Weblogic server, the SAML debug can be enabled by setting following properties as part of weblogic startup script
 - » EXTRA_JAVA_PROPERTIES="\${EXTRA_JAVA_PROPERTIES} -Dweblogic.debug.DebugSecuritySAML2Atn=true -Dweblogic.debug.DebugSecuritySAML2CredMap=true -Dweblogic.debug.DebugSecuritySAML2Lib=true -Dweblogic.debug.DebugSecuritySAML2Service=true"
- » Once the debug properties are enabled, the weblogic server log file will have SAML enabled debug logs captured



Figure 82. Weblogic Log: SAML Debug logs



CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

f

Oracle Corporation, World Headquarters 500 Oracle Parkway Redwood Shores, CA 94065, USA Worldwide Inquiries Phone: +1.650.506.7000 Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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

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

White Paper Title

Author: [OPTIONAL] Contributing Authors: [OPTIONAL]

Oracle is committed to developing practices and products that help protect the environment