

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 | MARCH 2017



Disclaimer

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



Table of Contents

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

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



Introduction

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

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

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

Pre-requisite

Components

The list of components required for this POC are

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

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

» IIS Manager

Note: IIS Installation is out-of-scope; IIS can be installed as stand-alone or while installing AD FS, would get 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 Lightweight Directory Services 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 Image: Comparison of the services	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	
Active Directory Before You Begin Installation Type Server Selection Server Roles Features AD FS Confirmation Results	Add Roles and Features Wizard Federation Services (AD FS) Active Directory Federation Services (AD FS) provides Web single-sign-on (SSO) cap authenticate a user to multiple Web applications using a single user account. AD FS bypass the need for secondary accounts by allowing you to project a user's digital ic rights to trusted partners. In this federated environment, each organization continue own identities. Things to note: • This computer must be joined to a domain before you can successfully install the • The Web Application Proxy role service in the Remote Access server role functions service proxy and cannot be installed on the same computer as the federation service	DESTINATIO abilities to helps org- lentity and s to mana Federation s as the fe vice.	n Servi	X TER ons is	
	< Previous Next > Instal		Cance		

Figure 3. Install AD FS – AD FS Page

» Click Install

<u>لم</u>	Add Roles and Features Wizard	-			×
Confirm instal	lation selections	DESTINATIO	IN 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 Install Restart the destination server automatically if required Optional features (such as administration tools) might be displayed on this page be been selected automatically. If you do not want to install these optional features, cli their check boxes. Active Directory Federation Services	L cause they ck Previou	r have is to cl	lear	
	Export configuration settings Specify an alternate source path				ļ
	Export configuration settings Specify an alternate source path < Previous Next > Insta		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 🕨		🖬 🛛 🖄 🔞 🗸
Elle View Help Connections Start Page Start Page WHFI00AKX (OFSLL)Pragna) Application Pools b. Sites	WHF00AKX Home Filter: • • •	Actions Manage Server Restart Start Stop View Application Pools View Stes Change AET Framework Version Get New Web Platform Components Web Platform Components Help
< m >	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:	tes anage certificates that the Wet co - Construction or a cle.com in wHF004KC-CA -ofslicom *.in.oracle.com localhost	server can use with websites co by: No Grouping • Issued By in-WHF00AKC-CA in-WHF00AKC-CA •.ofsIL.com •.in-UrHF00AKC-CA Iocalhost	Infigured for SSL. Expiration Date 7/19/2016 11:22:04 7/20/2026 65:90 3 1/1/2040 5:29:59 AM 1/1/2040 5:29:59 AM 7/19/2016 6:51:19 7/16/2020 5:30:00	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.

Ъ А	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 permissi federation service configuration. \Administrator (Current user) Change	ons to perform the
	< 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

	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.

A A	Active Directory Federa	ation Services Configura	ition 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 Man Account Name: Use an existing dom Account Name:	ation Services Configura ccount or group Managed Se laged Service Account OFSLL\ ain user account or group Ma <not provid<="" td=""><td>ervice Account. ADFS_SVC anaged Service Account ded></td><td>TARGET SERVER</td></not>	ervice Account. ADFS_SVC anaged Service Account ded>	TARGET SERVER
Pre-requisite Checks Installation Results				
		< Previous	Next > Configu	re 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

۵ ا	Active Directory Federation Services	Configuration Wizard	- • ×
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 Ig Windows Internal Database.	TARGET SERVER
Specify Service Account	O Specify the location of a SQL Server	database.	
Review Options	Database Host Name:		
Pre-requisite Checks	Database Instance:		
Results			
	< 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 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 SE 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		
Review Options	All prerequisite checks passed successfully. Click 'Configure' to begin insta	allation.	
Pre-requisite Checks Installation			
Results			
	< Previous Next > Configu	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 Active Directory claim acceptance rules Create VSS Express Writer for use with backup solutions	Status Configuration finished 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.

🗲 🗇 🧟 https://10000000/federationmetadata/2007- 🔎 👻 🛿 Certificate error 🖒 🖉 🗫 💿 🗙	ê ★
yISDLRdv:wQ+IBX3ICSH:w01Npu1fMR:qvSIRZPbw:i=XxQpFi2COqpy3QKVIpSNupfAHMGSWR/YZPTScA ddres:nDte-mail address of the userfixers NumErn E given name of the userNumE DTL be unique name of the userFix e-mail gdress of the user vhem interoperating with AD FS 1.1 or AD FS 1.0GroupA group that the user is a memb hasSummerThe summare of the userFDDTD private identifier of the userNumE DTL FS AML name identifier of the method used to authenticate the userDerDY only group SIDThe deny-only group SID of the userDerDy only primary FS SIDThe group SID of the userPDTDs private identifier of the userNumE DTL FS AML name identifier of the grintered to use this deviceDevice IdentifierIdentifier of the deviceDevice Registration IdentifierIdentifier for Devi deviceDevice OS VersionOS version of the deviceIs Managed DeviceDevice Registrational IdentifierIdentifier for Devi deviceDevice OS VersionOS version of the deviceIs Managed DeviceDevice Registrational IdentifierIdentifier for Devi deviceDevice OS VersionOS version of the deviceIs Managed DeviceDevice Registrational IdentifierIdentifier for Devi deviceDevice OS VersionOS version of the Relyung PartyApplication policies of the certificate Constrainflore of the basic constration of the certificateEnhanced Rey UsageDeviceNex or of the enhanced Rey usag name of the certificate issuerKey UsageOde of the Key usageIs of the version 2 certificate Esplayee Mona bioleise under which the certificate las been issuedPublic Key biolic Key of the versificate Certificate Rew Dual The mumber of a certificateSinguture AlgorithmThe algorithm which to version 2 certificate Esplayee and the version 2 certificate Esplayee used when i template used when issuing or renewing a certificate. The cettension is Microsoft specific. ThumbprintThumbprint to implicits under which the certificate version 2 certificate Esplayee used version adverse of update password serviceAuthentication. Methods ReferencesUsed to indicate all authentication methods vi htp://sta.ofil.com/adf.tevvices.truit.2005/sisuedRokenmix	i=rpReVZrFhWgRIF4PWXrEI5iFat+07/TRK+c390Ag/iPgPXEncHffGL1qVUMmbPFcofbAfpSerz/07/A601wxFIHHWGK NThe user principal name (UPN) of the user common NamcThe common name of the userAD FS 1 x LUPNThe LUPN of the user when interoperating with AD FS 1 L or AD FS 1 LORAL volc that the user or adAD FS 1 x LUPNThe LUPN of the user when interoperating with AD FS 1 L or AD FS 1 LORAL volc that the user of the user/Monitoriation time stampulced to display the time and date that the user was multicurcial Automatication method. The user/Monitoriation time stampulced to display the time and date that the user was multicurcial Registered UserUsers a c RegistrationDevice Registration DisplayNameDisplay name of Device RegistrationClinent User AgenDevice type the can be used to determine active versus passive clientBroyODNS name of the Client ApplicationClient User AgenDevice type the can be used to determine active versus passive clientBroyODNS name of the foreation server proxy that passed the teAuthority Key Identifier The Authority Key Identifier extension of the certificate that signed an issued certificateBasic go of the certificateBaser the automity that issued the X509 certificateBase the Basic ges of the certificateBaser the automity that issued the X509 certificateBase basic suit or tension age certificate authority that issued the X509 certificateBase basic suit or certificateBaser the automit base throad the part fractions of the certificateBaser NameThe Basinguished ch a certificateBaser the automit base student the subject key identifier of the certificateBaser NameThe simplex suit or cerving a certificate. The extension is Microsoft specificat / 11 remplate Name The sawout Client Davis of the data stude is days to assword Explainted to a forget assword Explainted to a forget assword Explainted to a singlex the subject key identifier of the certificateBase based to authenticate the userClient Request IDIdentifier for a user sessionAlternate Login IDAlternate login ID of the user the certificateBaser and the sertificate
https://ste.otell.com/adte/lo/	

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.

£	ſ	~/app	/middleware,	/user_pro	jects/	dom	ains/OFSI	LLREL_domain
E.		21	FSLLREL de	omain]	s pw	d		
/scratch/or	cac	le/app/r	middleware	e/user	pro	ject	ts/doma	ains/OFSLLREL domain
E-		OI	FSLLREL de	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	2	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		orafmw	oinstall	4096	Jul		17:06	nmqo
drwxr		orafmw	oinstall	4096	Oct	14	18:46	
-rw-rr		orafmw	oinstall	857	Oct	14	18:01	rootl.cer
-rw-rr		orafmw	oinstall	905	Jul	21	23:020	(root.cer)
drwxr-x		orafmw	oinstall	4096	Jul		15:59	security
drwxr	6	orafmw	oinstall	4096	Oct	13	18:39	
-rw-r		orafmw	oinstall	274	Oct	14	18:33	shutdown.py
-rw-r		orafmw	oinstall	767	Jul		15:59	startManagedWebLogic_readme.txt
-rwxr-x		orafmw	oinstall	284	Jul		15:59	startWebLogic.sh
drwxr-x		orafmw	oinstall	4096	Jul		10:17	
drwxr		orafmw	oinstall	4096	Oct	14	18:46	
-rw-rr		orafmw	oinstall	920	Oct	14	18:01	trust1.jks
-rw-rr		orafmw	oinstall	967	Jul	21	23:020	trust.jks
ft		01	FSLLREL de	omainl	S			

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: OFSLLREL_doma
Home >Summary	of Servers >01	SLL_Mana	gedServe	er2								
Settings for OFS	LL_Managed	Server2										
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 &	Edit button in	n the Chang	ge Center	to modify the	settings on	this page.						
Save												
Keystores ensu	re the secure s	torage and	l manager	ment of private	e keys and t	rusted certificat	e authorities	(CAs). This	s page lets y	ou view and define va	rious keystore co	e configurations. These settings help you to manage the security of message transmissions.
Keystores:						Custor	n Identity ar	nd Custom 1	Trust Chang	je	Which o Info	ch configuration rules should be used for finding the server's identity and trust keystores? More
- Identify												

Figure 23. Weblogic Server - Keystore Location

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

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

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

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

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

» Save the changes

🔒 Home Log Out	Preferences	Necord H	elp		٩										w	/elcome, weblog	jic Co	onnected to: OFSI	LREL_domai
Home >Summary of Servers >OFSLL_NanagedServer2																			
Settings for OFSLL_ManagedServer2																			
Configuration	Protocols	Logging Debu	Jg Mo	onitoring	Control	Deployments	ments Services Security Notes												
General Cluste	r Services	Keystores	SSL	Federatio	n Services	Deployment	Migration	Tuning	Overload	Health Monitoring	Server Sta	art Web Se	ervices						
Save																			
	_			-								_					_		
Keystores ensur	e the secure s	torage and mani	agemen'	t of private	keys and t	rusted certificate	e authorities	(CAs). This	page lets y	ou view and define v	arious keystor	re configuratio	ions. Thes	e settings help	o you to ma	anage the security	ofme	ssage transmission	15.
Keystores:						Custon	Identity an	d Custom Ti	rust Chang	e	Whi Info	ich configurati	tion rules	should be used	d for findin	g the server's iden	itity ar	id trust keystores	More
— Identity —																			
Custom Identit	y Keystore:					iden	iity.jks				The	The path and file name of the identity keystore. More Info							
Custom Identit	y Keystore 1	Type:				jks	jks						The type of the keystore. Generally, this is JKS. More Info						
Custom Identit	y Keystore 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 Custon	1 Identity Ke	ystore Passp	hrase:			•••	•••••	•••••											
— Trust ——																			
Custom Trust K	eystore:					trust	jks				The	The path and file name of the custom trust keystore. More Info							
Custom Trust Keystore Type:											The	The type of the keystore. Generally, this is JKS. More Info							
Custom Trust Keystore Passphrase:							••••••	•••••			The pas	The custom trust keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. More Info							
Confirm Custon	n Trust 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

😭 Home Log	Out Pref	ferences 📐	Record Help		G								Welcome, weblog	ic Connected to: OFSLLREL_domain		
Home >Summa	iry of Ser	vers > OFSLL_	HanagedSer	ver2												
Settings for O	FSLL_Ma	anagedServ	er2													
Configuratio	n Prot	ocols Loggi	ng Debug	Monitorin	ig Control	Deployments	Services	Security	Notes							
General Clu	uster 5	Services Ke	ystores S	SL Federa	ation Services	Deployment	Migration	Tuning	Overload	Health Monitoring	Server Start	Web Services				
Save																
This page let:	s you vier	v and define v	arious Secur	e Sockets La	iyer (SSL) setti	ngs for this serv	er instance. 1	'hese settir	ngs help you	to manage the secur	ity of message	transmissions.				
년 Identity				,	Keystores C	nange			India serv	Indicates where SSL should find the server's identity (certificate and private key) as well as the server's trust (trusted CAs). More Info						
— Identity –																
Private Key	Location	1:				1	from Custom I	dentity Ke	ystore		The	The keystore attribute that defines the location of the private key file. More Info				
Private Key	Alias:						mykey				The key.	The keystore attribute that defines the string alias used to store and retrieve the server's private key. More Info				
👍 Private K	ey Pass	phrase:					•••••	•••••	•••		The keystore attribute that defines the passphrase used to retrieve the server's private key. More Info					
👍 Confirm I	Private	Key Passphr	ase:				•••••	•••••	•••							
Certificate L	ocation:					1	from Custom I	dentity Ke	ystore		The	eystore attribute	e that defines the location of the trusted certific	ate. More Info		
— Trust —																
Trusted Cert	Trusted Certificate Authorities: from Custom Trust Keystore The keystore attribute that defines the location of the certificate authorities. More Info									norities. More Info						
— 🖗 Advance	ed															
Save																

Figure 25. Weblogic Server – SSL Settings

- » Click on the "Advanced " field under the SSL tab
 - » Set the "Hostname Verification: "to None

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

- » Use JSSE SSL → Checked
- » Save the changes

Home Log Out Preferences Record Help	Q					Welcome, weblogic	Connected to: OFSLLREL_domain	
Settings for OFSLL_ManagedServer2								
Configuration Protocols Logging Debug Monitorin	ng Control Deployments	Services Securi	ty Notes					
General Cluster Services Keystores SSL Feder	ation Services Deployment	Migration Tunin	g Overload	Health Monitoring	Server Start We	eb Services		
Save								
This page lets you view and define various Secure Sockets La	ayer (SSL) settings for this serv	er instance. These s	ettings help you	u to manage the secur	rity of message transr	missions.		
街 Identity and Trust Locations:	Keystores Change				Indicates w server's tru	where SSL should find the server's identity (certificate and pri ust (trusted CAs). More Info	vate key) as well as the	
- Identity								
Private Key Location:	from Custom Identity Keyst	vre			The keysto	ore attribute that defines the location of the private key file.	More Info	
Private Key Alias:	mykey				The keysto key. More	ore attribute that defines the string alias used to store and re re Info	trieve the server's private	
n Private Key Passphrase:	•••••	•			The keysto Info	ore attribute that defines the passphrase used to retrieve the	server's private key. More	
👸 Confirm Private Key Passphrase:	•••••	•						
Certificate Location:	from Custom Identity Keyst	vre			The keysto	ore attribute that defines the location of the trusted certificat	e. More Info	
Trusted Certificate Authorities:	from Custom Trust Keystore				The keysto	ore attribute that defines the location of the certificate autho	ities. More Info	
- Advanced		_					1.00.01.0.01.0	
(1) Hostname vermcation:	None				interface (whether to ignore the installed implementation of the weblogic (when this server is acting as a client to another application se	rver). More Info	
n Custom Hostname Verifier:					The name o Info	of the class that implements the weblogic.security.SSL.Hostn	ameVerifier interface. More	
Export Key Lifespan:	500				Indicates t and an exp be, the fev	the number of times WebLogic Server can use an exportable I portable client before generating a new key. The more secure wer times the key should be used before generating a new ke	ey between a domestic server you want WebLogic Server to y. More Info	
Use Server Certs					Sets wheth outbound o	her the dient should use the server certificates/key as the die connection over https. More Info	nt identity when initiating an	
Two Way Client Cert Behavior:	Client Certs Not Requ	ested	•		The form o	of SSL that should be used. More Info		
Æु Cert Authenticator:					The name of deprecated used when	of the Java dass that implements the weblogic.security.ad.C d in this release of WebLogic Server. This field is for Compatib t the Realm Adapter Authentication provider is configured.	ertAuthenticator class, which is ility security only, and is only fore Info	
SSLRejection Logging Enabled					Indicates w rejected.	whether warning messages are logged in the server log when More Info	SSL connections are	
🔲 縃 Allow Unencrypted Null Cipher					Test if the	AllowUnEncryptedNullCipher is enabled More Info		
Inbound Certificate Validation:	Builtin SSL Validation	Only	•		Indicates t	the client certificate validation rules for inbound SSL. More I	ıfo	
Outbound Certificate Validation:	Builtin SSL Validation	Only	-		Indicates t	the server certificate validation rules for outbound SSL. Mor	≥ Info	
🗹 🎦 Use JSSE SSL					Select the	JSSE SSL implementation 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 Preference	es 🔁 Record Help						
Home >Summary of Security R	Home >Summary of Security Realms >myrealm >Providers >SAMLIdentityAssert > Providers						
Create a New Authentication	n Provider						
OK Cancel							
Create a new Authentica	ition 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 authentication	n provider.						
* Name:	SAMLIdentityAssert						
This is the type of authenticat	This is the type of authentication 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.

1	Authentication Providers							
	New Delete Reorder	Showing 1 to 4 of 4 Previous						
	Name	Description	Version					
	SAMLIdentityAssert	SAML 2.0 Identity Assertion Provider. Supports Security Assertion Markup Language v2.0.	1.0					

Figure 28. Weblogic Server - SAML 2.0 version

Configuring SAML 2.0 Service Provider (SP)

- » Log into Weblogic Admin console on the OFSLL Domain
- » Go to Environment → Servers ofsll_managedserver2 → Federation Services → SAML 2.0 Service Provider
- » Most fields can be left as default except noted below
 - » Enabled \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

Iministration Console						ž
🚹 Home Log Out Preferences 🔤 Record Help	Q				Welcome, weblogic	onnected to: OFSLLREL_domai
Home >Summary of Servers >OFSLL_ManagedServer2						
Settings for OFSLL_ManagedServer2						
Configuration Protocols Logging Debug Moni	itoring Control Deployments Services	Security Notes				
General Cluster Services Keystores SSL Fe	ederation Services Deployment Migra	tion 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 Provider	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					
C Enabled				Specifies	whether the local site is enabled for the Service Provider role.	lore Info
Always Sign Authentication Requests				Specifies are signed	whether authentication requests must be signed. If set, all outgo d. More Info	ing authentication requests
Force Authentication				Specifies security c	whether the Identity Provider must authenticate users directly an context. The default is false. More Info	id not use a previous
Passive				Determine from the r Info	es whether the Identity Provider and the user must not take contr requester and interact with the user in a noticeable fashion. The o	rol of the user interface default setting is false. More
Only Accept Signed Assertions				Specifies	whether incoming SAML 2.0 assertions must be signed. More Inf	fo
Authentication Request Cache Size:	10000			The maxin	mum size of the authentication request cache. More Info	
Authentication Request Cache Timeout:	300			The maxin Info	mum timeout (in seconds) of <authnrequest> documents stored i</authnrequest>	in the local cache. More
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. $\ensuremath{{\rm N}}$	lore Info
Artifact Binding Enabled				Specifies	whether the Artifact binding is enabled for the Service Provider.	More Info
Preferred Binding:	POST 🔽			Specifies "POST", o	the preferred binding type for endpoints of Service Provider servi or "Artifact". More Info	ices. Must be set to "None",
Default URL:	https://c	n:8005/ofsll142/faces	/p	The Servi	ice Provider's default URL. More Info	
Save						
Click the Lock & Edit button in the Change Center to mo	odify 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 → 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

ministration Console						
😭 Home Log Out Preferences 🔤 Record Help	<u> </u>	Welcome, weblogic Connected to: OFSLLREL_doma				
Home >Summary of Servers >OFSLL_ManagedServer2						
Settings for OFSLL_ManagedServer2	Control Decloyments Convices Convicts Notes					
Configuration Protocols Logging Debug Montoring Control Depugnents Services Security Notes						
SAMI 1.1 Source Site SAMI 1.1 Destination Site SAMI 2.0.0	eneral SAMI 2.0 Identity Provider SAMI 2.0 Service Provider	Server Surver Surver Stervers				
Come Databal Mate Data						
Save Publish Meta Data						
Click the Lock & Edit button in the Change Center to modify the s	ettings on this page.					
This page configures the general SAML 2.0 per server properties						
— General						
Cache Enabled		Specifies whether the persistent cache (LDAP or RDBMS) is used for storing SAML 2.0 artifacts and authentication requests. More Info				
— Site Info						
Contact Person Given Name:		The contact person given (first) name. More Info				
Contact Person Surname:		The contact person surname (last name). More Info				
Contact Person Type:	administrative 💌	The contact person type. More Info				
Contact Person Company:	Oracle	The contact person's company name. More Info				
Contact Person Telephone Number:	1234567890	The contact person's telephone number. More Info				
Contact Person Email Address:		The contact person's e-mail address. More Info				
Organization Name:	Oracle	The organization name. More Info				
Organization URL:	http://www.oracle.com/	The organization URL. More Info				
Published Site URL:	http://c 1:8003/saml2	The published site URL. More Info				
Entity ID:	sso_domain	The string that uniquely identifies the local site. More Info				
Bindings Recipient Check Enabled		Specifies whether the recipient/destination check is enabled. When true, the recipient of the SAML Request/Response must match the URL in the HTTP Request. More Info				
Transport Layer Client Authentication Enabled		Specifies whether TLS/SSL client authentication is required. More Info				
Transport Layer Security Key Alias:		The string alias used to store and retrieve the server's private key, which is used to establish outgoing TLS/SSL connections. More Info				
Transport Layer Security Key Passphrase:		The passphrase used to retrieve the server's private key from the keystore. More $\ensuremath{Info}\xspace$.				
ConfirmTransport Layer Security Key Passphrase:						
Basic Client Authentication Enabled		Specifies whether Basic Authentication dient 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 $\begin{tabular}{c} More Info \end{tabular}$				
Confirm Basic Authentication Password:						
- Artifact Resolution Service						
Only Accept Signed Artifact Requests		Specifies whether incoming artifact requests must be signed. More Info				
Artifact Cache Size:	10000	The maximum size of the artifact cache. More Info				
Artifact Cache Timeout:	300	The maximum timeout (in seconds) of artifacts stored in the local cache. More info				
Single Sign-on Single Sign-on Signing Key Alias:	mykey	The keystore alias for the key to be used when signing documents. More Info				
Single Sign-on Signing Key Pass Phrase:	••••••	The passphrase used to retrieve the local site's SSO signing key from the keystore. More Info				
Confirm Single Sign-on Signing Key Pass Phrase:	••••••					
Save Publish Meta Data						
Click the Lock & Editbutton in the Change Center to modify the settings on this page.						

Figure 30. Weblogic Server – SAML2.0 General

- » Go to Environment →Servers →ofsll_managedserver2→ Federation Services →SAML 2.0 General
- » Publish the Service provider (SP) metadata to an XML file using the "Publish Meta Data" button. Keep the file in a safe place it will be used by AD Server at later stage. For example ofsll_metadata.xml in this case.

tes Overload Health Monitoring Server Start Web Servic rvice Provider
Dverload Health Monitoring Server Start Web Servic
Overload Health Monitoring Server Start Web Servic
rvice Provider

Figure 31. Weblogic Server – Publish Meta Data

» The Published ofsll_metadata.xml file would look as below

FLL_Metadata.xml - Notepad	
File Edit Format View Help	
xml version="1.0" encoding="UTF-8" standalone="no"?	^
<pre><md:entitydescriptor entityid="sso_domain" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"></md:entitydescriptor></pre>	
<pre>kmd:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false" protocolSupportEnumeration="urn:</pre>	oasis:names:tc:SAML:2.0:protocol">
<md:keydescriptor use="signing"></md:keydescriptor>	
<ds:keyinfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"></ds:keyinfo>	
<pre><ds:x509data></ds:x509data></pre>	
<ds:x509certificate></ds:x509certificate>	
MIIC/2CCAdegAwIBAgIEIK/JBUZANBgkqhkiGawIBAQUFADAOMQAwUWIWIKAwHQYD	
VQUDEMAXINGAXOUQUINI INYC JE UNI AGEWOXINI EMINUKIMI I ASINJ BAHIVOXUDASINOUMI I ASINJ BAHIVOXUDI AL	
BRINGER I DE SQUIINTEZANDRINGANI DIENE JEANGANATURI UTILITI DI ANDREGNICI GWODAUE FAAD. ANDRAIT DE ANGREGNE ANDREGNICO (CONCOLO DE SECONDE SUCCESSION AND ANDREGNICA UNA DE SAUCESSION AND ANDREGNICA	
Ago Amili Begreage Amile Cazed version of 15 architest Dispersion and a second and and a second and and a sec	=
0x05x027025Cill50pk01v0C00rAsh0wr1+txb0gr7j00yr5rg1c01220x01+txtwaliarc1-qb0y00yc0	
stallishing a Reference in the state of the	
+ssf18/14h028rCawIE446Z0twIDZE5vd8KPBkua1Mb0rGt/9sXfwIDA0ABovEwHzAdBrNVH04E	
FeOU@vE725X3U6vtv5heCRU711Z1@gEwD0YJKoZIhvcNAOEFB0ADgeEBAERhePABGv05K17g04V9	
cjk/pQXxymXCkMCpW97TkwzEtP2ghhEQ116iUCza+tIyrGHx1m05ntsNeBeI5100LdB9smyEpAgf	
MBTrkfhpunM7GYqR355mx1A8m1E2574Q46cbN8nETiVBk00J1FFfrpihVwcWPSsbIrnXE7bHZDqZ	
OGAxd7ZjgQwZJ115rYxQXA1FX4phGDDYCZHUwP5mSmIKpzGLjnWFRD8yU3dYpzpNtA1KCRF+G2E3	
YQ9yHu5zTH+aQHaUzJjOIvg55xCG/Y19aK8zHiqBdjzIXQha7KI/lqAVzldUjqfIghWK92w2q6Zm	
49S3V5F7oxNX/kb8Ym0=	
<pre><md:artifactresolutionservice <="" binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" index="0" location="http://</pre></td><td>9452/saml2/sp/ars/soap" td=""></md:artifactresolutionservice></pre>	
<pre>(md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0;bindings:HIIP-POSI" Location="http://</pre>	:9452/sam12/sp/acs/post index=
<pre>(ma:Assertion.onsumerservice Binding= urn:oasis:names:tc:SAML:2.0:bindings:HITP-Artifact" Location="http:// actableSConservice.setablesconduction="http://</pre>	:9452/sami2/sp/acs/artifact
(md.)====================================	
	×
	2 .H

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...>

Image: Second					
<pre>cml varians"1.0?> Excloser.close</pre>	🕞 🖻 FederationMetadata.xml	Fi 🙆 ک ד کر	ederationMetad ×		
<pre>c?setUpDecipionts fullings/uninceditions_uniced/standards_cnt/u/D= http:// / /dfs/services/trust_D=_0094bcf-0408-4b58-9573-423dde0902fc =</pre>					,
• EBRUEDEXCIPACT mines um noads menessis XAML2.2.0) metades ent/UDE http:// // // // // // // // // // // // //	?xml version="1.0"?>				
<pre>> <kpre>> <kpre>></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></kpre></pre>	EntityDescriptor xmins="urn:oasis:names:tc:SAML:2.0:	metadata" entityID="ht	tp://	/adfs/services/trust"ID="_8094bcef-04d8-4b58-9573-d23dda9907fc">	
<pre>- <<keyubschptor uss="BrCryption">: - <<keyubschptor uss="BrCryption">: - <<keyubschptor uss="BrCryption">: - <<keyubschptor uss="BrCryption">: - <<keyubschptor uss="Signing">: - <<keyubschptor>: - <<keyubschptor>: - <<keyubschptor>: - <<keyubschptor>: - <<keyubschptor>: - <<keyubschptor>: - <<keyubschptor>: - <<ke>: - <<keyubschptor>: - <keyubschptor>: - <keyubschptor< td=""><td> <idpssgdescriptor protocolsupportenumeration="urn; </td><td>:oasis:names:tc:SAML:2</td><td>.0:protocol"></idpssgdescriptor></td><td></td><td></td></keyubschptor<></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></ke></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></keyubschptor></pre>	 <idpssgdescriptor protocolsupportenumeration="urn; </td><td>:oasis:names:tc:SAML:2</td><td>.0:protocol"></idpssgdescriptor>				
<pre> - ckeyIntesting: - ckeyIntesting:</pre>	- <keydescriptor use="encryption"></keydescriptor>				
<pre> Control Contents MIIC3DCCAc5gAwIBAg1Qdz08Lrw4IJNB+kxe0fGHhTANBgkqhkiG9w0BAQsFADAqMSgwJgYDVQQDEx9BREZTIEVuY3J5cHRpb24gL5BzdHMub2ZzbGwuY29tMB4XDTE1MDcyMT XY30D2da5 KeyJerios KeyJ</pre>	 <keyinto xmins="http://www.w3.org/2000 </td><td>i/u9/xmiasig#"></keyinto>				
<pre></pre>	XE00Cortificates MUC2DCCAcEgAwi XE00Cortificates MUC2DCCAcEgAwi Automatical Automatical	PAGIOd-091 mu411NP+1	CONTANDAL	abkicow0840cE404aM6aw1aXDV00DEx088E7TIEVuX215cH8pb24aL68zdHM	
<pre></pre>	(X509Certilicate Milesbeckesgawi	BAGIQUZUBLIWHIJNBH	CREOIGHILLANDGR	langan and an and an	IND2220GW0129CMD4XD1E1MDCyM1
<pre></pre> </td <td></td> <td></td> <td></td> <td></td> <td></td>					
<pre> - <keybacriptor use_="signing^"> - <keybacriptor use_="signing^"> - <keybacriptor use_="signing^"> - <ktopbat> - <ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></ktopbat></keybacriptor></keybacriptor></keybacriptor></pre>					
<pre> - **KeyInfo sumis= "http://www.wa.org/2000/09/xmldsige"> - **KeyInfo sumis= "http://www.wa.org/2000/09/xmldsige"> - **KeyInfo sumis= "http://www.wa.org/2000/09/xmldsige"> - **KeyInfo sumis= "http://www.wa.org/2000/09/xmldsige"> - *KeyInfo sumis= "http:// sumis="http://s</pre>	 <keydescriptor use="signing"></keydescriptor> 				
<pre>- cXS00Data> cXS00ccrtificate> MIICI_JCCAbsgAwIBAgIQYdaJO01q63AKPxyj8Vk3JANBgkqhkiG9w0BAQsFADAnMSUwIwYDVQQDExxBREZTIFNPZ25pbmcgLSBzdHMub2ZzbGwuY29IMB4XDTE1MDcyMTEyKz cXS09Data> cXs09Ccrtificate> MIICI_JCCAbsgAwIBAgIQYdaJO01q63AKPxyj8Vk3JANBgkqhkiG9w0BAQsFADAnMSUwIwYDVQQDExxBREZTIFNPZ25pbmcgLSBzdHMub2ZzbGwuY29IMB4XDTE1MDcyMTEyKz cXS09Data> cXs09Ccrtificate> MIICI_JCCAbsgAwIBAgIQYdaJO01q63AKPxyj8Vk3JANBgkqhkiG9w0BAQsFADAnMSUwIwYDVQQDExxBREZTIFNPZ25pbmcgLSBzdHMub2ZzbGwuY29IMB4XDTE1MDcyMTEyKz cXs09Data> cXs09Ccrtificate> MIICI_JCCAbsgAwIBAgIQYdaJO01q65/JKF cSingleSignotService Location= "http:// cSingleSignotService Location="http:// cSingleSignotService Location="http:// cSingleSignot</pre>	- <keyinfo xmlns="http://www.w3.org/2000</p></td><td>/09/xmldsig#"></keyinfo>				
<pre> cXS90Cattlicate=MIICLjCCAb6gAwIBAg1QYdaJ001q&GJAKPxvj8Vk3jANBgkqhkiG9w0BAQsFADAnMSUw1wYDVQQQExxBREZTIFNpZ25pbmcgLSBzdHMub2ZzbGwuY29tMB4XDTE1MDcyMTEyMz c/KeyInfos c/KeyI</pre>	- <x509data></x509data>				
<pre></pre> <pre> </pre> </td <td><x509certificate>MIIC1jCCAb6gAwIF</x509certificate></td> <td>BAgIQYdaJO01qR6JAKF</td> <td>xvj8Vk3jANBgkq</td> <td>hkiG9w0BAQsFADAnMSUwIwYDVQQDExxBREZTIFNpZ25pbmcgLSBzdHMub2Z</td> <td>zbGwuY29tMB4XDTE1MDcyMTEyMz</td>	<x509certificate>MIIC1jCCAb6gAwIF</x509certificate>	BAgIQYdaJO01qR6JAKF	xvj8Vk3jANBgkq	hkiG9w0BAQsFADAnMSUwIwYDVQQDExxBREZTIFNpZ25pbmcgLSBzdHMub2Z	zbGwuY29tMB4XDTE1MDcyMTEyMz
/info/key/info /info/key/info					
<pre> <td></td><td></td><td></td><td></td><td></td></pre>					
<pre><singlelogouservice <="" location="https://" td=""><td></td><td></td><td></td><td></td><td></td></singlelogouservice></pre>					
<pre><singlelogouservice <="" location="https://" td=""><td><singlelogoutservice bindin<="" location="https://:</td><td>/adfs/ls/" td=""><td>g="urn:oasis:nam</td><td>nes:tc:SAML:2.0:bindings:HTTP-Redirect"/></td><td></td></singlelogoutservice></td></singlelogouservice></pre>	<singlelogoutservice bindin<="" location="https://:</td><td>/adfs/ls/" td=""><td>g="urn:oasis:nam</td><td>nes:tc:SAML:2.0:bindings:HTTP-Redirect"/></td><td></td></singlelogoutservice>	g="urn:oasis:nam	nes:tc:SAML:2.0:bindings:HTTP-Redirect"/>		
<pre>chamilly of models: manest: ctsAML:1.indexied format: time index of models: chamiles of models: manest: ctsAML:1.indexied format: time index of models: manest: ctsAML:1.index of models: manest: ctsAML:1.index</pre>	<singlelogoutservice bindin<="" location="https://:</td><td>/adts/ls/" td=""><td>g="urn:oasis:nam</td><td>hes:tc:SAML:2.0:bindings:HTTP-POST"/></td><td></td></singlelogoutservice>	g="urn:oasis:nam	hes:tc:SAML:2.0:bindings:HTTP-POST"/>		
<pre>chantedDromats/uncoals/namesic:CSAML2.0:nameid=format:provisent</pre> //initial/provisent	<nameidformat>urn:oasis:names:tc:SAML:1.1:</nameidformat>	nameld-format:emailAd	idress <td>ormat></td> <td></td>	ormat>	
<pre><singlesignonservice <br="" https:="" location="https://
<SingleSignOnservice Location="></singlesignonservice></pre>	<nameidformat>urn:odsis:names:tc:SAML:2.0:</nameidformat>	nameid-format:persiste	t (NameIDFormal	ats	
<pre><singlesignonservice <="" einding="umroasis:namest:CSAML:20.binding_s:HTTP-POST/>
</pre> <pre></pre> <pre></pre> <pre></pre> <pre></pre> <pre>//science:</pre> <pre>//</td><td><SingleSignOnService Location=" https:="" location="https:// / /ddfs/fs/" td=""><td>/adfs/ls/" Bindin</td><td>a="urn:oasis:nan</td><td>nes:tc:SAMI :2 0:bindings:HTTP-Redirect*/></td><td></td></singlesignonservice></pre>	/adfs/ls/" Bindin	a="urn:oasis:nan	nes:tc:SAMI :2 0:bindings:HTTP-Redirect*/>		
<pre><attribute friendlyname="E Nail Address" name="http://schemas.xnisoap.org/ws/2005/05/identity/claims/givenname" nameformat="urn:oadis:names:tc:SAML:2.0:attrname-format:url" xnins="urn:oadis:names:tc:SAML:2.0:assertion"> </attribute></pre> <attribute name="http://schemas.xnisoap.org/ws/2005/05/identity/claims/givenname" xnins="urn:oadis:names:tc:SAML:2.0:attrname-format:url"> Attribute xnins="urn:oadis:names:tc:SAML:2.0:attrname-format:url" Name="http://schemas.xnisoap.org/ws/2005/05/identity/claims/givenname"> <!--</td--><td><pre>singleSignOnService Location="https://</pre></td><td>/adfs/ls/" Bindin</td><td>g="urn:oasis:nan</td><td>nestc:SAMI : 2 0:bindings:HTTP-POST"/></td><td></td></attribute></attribute></attribute></attribute></attribute>	<pre>singleSignOnService Location="https://</pre>	/adfs/ls/" Bindin	g="urn:oasis:nan	nestc:SAMI : 2 0:bindings:HTTP-POST"/>	
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"/> <ttr> <ttr> <ttr></ttr></ttr></ttr>	<attribute friendlynam<="" td="" xmins="urn:oasis:names:tc:SAML:2.0</td><td>assertion"><td>="E-Mail Addres</td><td>s" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute>	="E-Mail Addres	s" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"		
<pre><attribute friendlyname="Given Name" name="http://schemas.xmisoap.org/ws/2005/05/identity/claims/givenname" nameformat="um:oasis:namest:ctSAML:2.0:attrname-format:uri" xmins="um:oasis:namest:ctSAML:2.0:assertion"></attribute> </pre>	Name="http://schemas.xmlsoap.org/ws/2	005/05/identity/claim	s/emailaddress"/	>	
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"/> < <td><td< td=""><td><attribute friendlynam<="" td="" xmlns="urn:oasis:names:tc:SAML:2.0</td><td>:assertion"><td>="Given Name" </td><td>NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute></td></td<></td>	<td< td=""><td><attribute friendlynam<="" td="" xmlns="urn:oasis:names:tc:SAML:2.0</td><td>:assertion"><td>="Given Name" </td><td>NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute></td></td<>	<attribute friendlynam<="" td="" xmlns="urn:oasis:names:tc:SAML:2.0</td><td>:assertion"><td>="Given Name" </td><td>NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute>	="Given Name"	NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"	
<pre><attribute ;="" <="" friendlyname="Name" name="http://schemas.xmisoop.org/vs/2003/05/identity/claims/name" nameformat="um:coasis:namest:ct:SAML:2.0:attrname-format:uri" pre="" vameformat="um:coasis:namest:ct:SAML:2.0:attrname-format:uri" xmine="um:coasis:namest:ctSAML:2.0:assertion"> <attribute <="" friendlyname="Tomp" nameformat="um:coasis:namest:ct:SAML:2.0:attrname-format:uri" p="" xmine="um:coasis:namest:ct:SAML:2.0:astertion"> <attribute <="" friendlyname="Tomp" nameformat="um:coasis:namest:ct:SAML:2.0:attrname-format:uri" p="" xmine="um:coasis:namest:ct:SAML:2.0:astertion"> <attribute <="" p="" xmine="um:coasis:namest:ct:SAML:2.0:attrname-format:uri"> <attribute <="" p="" xmine="um:coasis:namest:ct:SAML:2.0:attrname-format:uri"> <attribute <="" p="" xmine="um:coasis:namest:ct:SAML:2.0:attrname-format:uri"> Name="Tomp://schemas.xmisoop.org/claims/commonName'/> <attribute <="" p="" xmine="um:coasis:namest:ct:SAML:2.0:attrname-format:uri"> Name="Tomp://schemas.xmisoop.org/claims/commonName"/> <attribute <="" p="" xmine="um:coasis:namest:ct:SAML:2.0:attrname-format:uri"> Name="Tomp://schemas.xmisoop.org/claims/commonName"/> <attribute <="" a="" xmine="um:coasis:namest:ct:SAML:2.0:attrname-format:uri"> Name="Tomp://schemas.xmisoop.org/claims/commonName"/> <attribute: claims="" commind(name="Couge" schemas.xmisoop.org=""></attribute:> Name="Tomp://schemas.xmisoop.org/claims/common"/> <attribute: claims="" commonname"="" schemas.xmisoop.org=""></attribute:> <attribute: claims="" commonname"="" schemas.xmisoop.org=""></attribute:> </attribute></attribute></attribute></attribute></attribute></attribute></attribute></attribute></attribute></attribute></attribute></attribute></pre>	Name="http://schemas.xmlsoap.org/ws/2	005/05/identity/claim	s/givenname"/>		
Name="http://schemas.xmisoop.org/ws/2005/identity/claims/name*/> <a 05="" 2005="" claims="" identity="" lschemas.xmisoop.org="" name*="" tribus="" ws=""> <a 05="" 2005="" claims="" identity="" lschemas.xmisoop.org="" tribus="" upm*="" ws=""> Name="http://schemas.xmisoop.org/ws/2005/05/identity/claims/upm*/> <a 05="" 2005="" claims="" identity="" lschemas.xmisoop.org="" tribus="" upm*="" ws=""> <a 05="" 2005="" claims="" identity="" lschemas.xmisoop.org="" tribus="" upm*="" ws=""> <a 05="" 2005="" claims="" identity="" lschemas.xmisoop.org="" tribus="" upm*="" ws=""> <a 05="" 2005="" claims="" identity="" lschemas.xmisoop.org="" tribus="" upm*="" ws=""> <a 05="" 2005="" claims="" identity="" lschemas.xmisoop.org="" tribus="" upm*="" ws=""> <a cl<="" claims="" lschemas.xmisoop.org="" td="" tribus=""><td><attribute friendlyname<="" td="" xmins="urn:oasis:names:tc:SAML:2.0</td><td>:assertion"><td>e="Name" NameFo</td><td>ormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute></td>	<attribute friendlyname<="" td="" xmins="urn:oasis:names:tc:SAML:2.0</td><td>:assertion"><td>e="Name" NameFo</td><td>ormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute>	e ="Name" NameFo	ormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"		
<pre><attribute "urn:oadiscnames:tc:saml:2.0:assertion"="" 2<="" friendlyname="UPN" http:="" name="http://schemas.xmisoap.org/claims/cloims/claims/c</td><td>Name=" nameformat="urn:oadiscnames:tc:SAML:2.0:attrname-format:uri" schemas.xmlsoap.org="" td="" urn:oadiscnames:tc:saml:2.0:attrname-format:uri"="" ws="" xmines=""><td>005/05/identity/claim</td><td>s/name"/></td><td></td><td></td></attribute></pre>	005/05/identity/claim	s/name"/>			
Hame= ntp://schemas.xmisoap.org/Ws/2/duss/Us/identity/cams/upn/> Attribute xmins="umroads:samest:csAML:2.0:acttrname-format:uri" Hame="ntp://schemas.xmisoap.org/claims/format/mame="AD FS 1.x E-Mail Address" NameFormat="umroadsis:namest:csAML:2.0:acttrname-format:uri" Hame="ntp://schemas.xmisoap.org/claims/formating/format="AD FS 1.x E-Mail Address" NameFormat="umroadsis:namest:csAML:2.0:acttrname-format:uri" Hame="ntp://schemas.xmisoap.org/claims/formating/format="AD FS 1.x E-Mail Address" NameFormat="umroadsis:namest:csAML:2.0:acttrname-format:uri" Hame="ntp://schemas.xmisoap.org/claims/formating/format="AD FS 1.x E-Mail Address" NameFormat="umroadsis:namest:csAML:2.0:acttrname-format:uri" Hame="ntp://schemas.xmisoap.org/claims/formating/format="address" NameFormat="umroadsis:namest:csAML:2.0:acttrname-format:uri" Hame="ntp://schemas.xmisoap.org/claims/formating/format="address" NameFormat="umroadsis:namest:csAML:2.0:acttrname-format:uri" Hame="ntp://schemas.xmisoap.org/claims/formating/format="address" NameFormat="umroadsis:namest:csAML:2.0:acttrname-format:uri" Autribute xmis="umroadsis:namest:csAML:2.0:acttrname-format:uri" Autribute xmis="umroadsis:namest:csAML:2.0:acttrname-format:uri"	<attribute namefori<="" td="" upn"="" xmins="urn:oasis:names:tc:SAML:2.0</td><td>:assertion FriendlyNam</td><td>e="><td>mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute>	mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"			
<pre>Knowled Amines unitodes.indires.it.co.wdc.2.co.dosection = neurophane = common name nameromat = unitodes.indires.it.co.autiname = tormat.un Name="http://schemas.xmisoa.prog/claims/CommonName">Kameromat="unitodes.indires.it.co.autiname=format.un" Kame="http://schemas.xmisoa.prog/claims/CommonName">Kameromat="unitodes.indires.it.co.autiname=format.un" Kame="http://schemas.xmisoa.prog/claims/CommonName">Kameromat="unitodes.indires.it.co.autiname=format.un" Kame="http://schemas.xmisoa.prog/claims/CommonName">Kameromat="unitodes.indires.it.co.autiname=format.un" Kame="http://schemas.xmisoa.prog/claims/CommonName">Kameromat="unitodes.indires.it.co.autiname=format.un" Kame="http://schemas.xmisoa.prog/claims/CommonName">Kameromat="unitodes.indires.it.co.autiname=format.un" Kame="http://schemas.xmisoa.prog/claims/CommonName">Kameromat="unitodes.indires.it.co.autiname=format.un" Kame="http://schemas.xmisoa.prog/claims/CommonName">Kameromat="unitodes.indires.it.co.autiname=format.un" Kame="http://schemas.xmisoa.prog/claims/CommonName">Kameromat="unitodes.indires.it.co.autiname=format.un" Kame="http://schemas.xmisoa.prog/claims/Common FriendlyName="Group" NameFormat="unitodes.it.co.autiname=format.un" Kame="http://schemas.xmisoa.prog/claims/Common FriendlyName="Group" NameFormat="unitodes.it.co.autiname=format.un" Kame="http://schemas.xmisoa.prog/claims/Common FriendlyName="Group" NameFormat="unitodes.it.co.autiname=format.un" Kame="http://schemas.xmisoa.prog/claims/Common FriendlyName="Group" NameFormat="unitodes.it.co.autiname=format.un"</pre>	Name="http://scnemas.xmisoap.org/ws/2	005/05/identity/claim	s/upn ⁻ />	e" NameFormat="urp.co.cicu.amos.to.6AML/2 Quattroamo_format.uvi"	
<pre>rtaile= ntup/_fscientes_tmissdp.ivff[Centus/Limits/Commonder /s Attribute xnins="unr.oasis.nemest.tc:SAML:2.0:attrname-format:url" flame="ntup/_fscientes_tmissdp.org/clains/EmailAddress" /s flame="ntup/_fscientes</pre>	CAttribute Annis- unitodsis.names.tc.SAME.2.0	Control PriendlyNam		e Nameronnat- unitoasis.names.tt.SAME.2.0.attinameronnat.un	
Knowe while "university of the second secon	http://scienas.kinsodp.org/claim	accortion" FriendlyNam	- AD ES 1 V E-M	all Address" NameFormat="urn:oasis:names:tc:SAMI :2 0:attrname-format:uri"	
<attribute <="" friendlyname="Group" nameformat="um:oasis:namestc::SAML:2.0:attrname-format:uri" p="" xmins="um:oasis:mamestc::SAML:2.0:assertion"></attribute>	Name="http://schemas.xmisoan.org/claim	s/FmailAddress"/>	- AD 13 1.X C M	an Address Haneronnat- ann.odsis.names.tc.SAME.2.0.attribuite format.an	
Names "http://cshamas.xm/caap.org/claims/Croup"/>	<attribute group"="" namef<="" td="" xmins="urn:oasis:names:tc:SAML:2.0</td><td>assertion FriendlyNam</td><td>e="><td>ormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute>	ormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"			
name- mup.//schemas.ximsoap.org/claims/aroup//	Name="http://schemas.xmlsoap.org/claim	s/Group"/>	•		
<attribute <="" friendlyname="AD FS 1.x UPN" nameformat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" td="" xmlns="urn:oasis:names:tc:SAML:2.0:assertion"><td><attribute friendlynam<="" td="" xmlns="urn:oasis:names:tc:SAML:2.0</td><td>:assertion"><td>="AD FS 1.x UPN</td><td>I" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute></td></attribute>	<attribute friendlynam<="" td="" xmlns="urn:oasis:names:tc:SAML:2.0</td><td>:assertion"><td>="AD FS 1.x UPN</td><td>I" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute>	="AD FS 1.x UPN	I" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"		
Name="http://schemas.xmlsoap.org/claims/UPN"/>	Name="http://schemas.xmlsoap.org/claim	s/UPN"/>			
<attribute <="" friendlyname="Role" nameformat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" td="" xmlns="urn:oasis:names:tc:SAML:2.0:assertion"><td><attribute friendlyname<="" td="" xmlns="urn:oasis:names:tc:SAML:2.0</td><td>:assertion"><td>e="Role" NameFor</td><td>mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute></td></attribute>	<attribute friendlyname<="" td="" xmlns="urn:oasis:names:tc:SAML:2.0</td><td>:assertion"><td>e="Role" NameFor</td><td>mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute>	e="Role" NameFor	mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"		
Name="http://schemas.microsoft.com/ws/2008/06/identity/claims/role"/>	Name="http://schemas.microsoft.com/ws/	/2008/06/identity/clai	ms/role"/>		
<attribute <="" friendlyname="Surname" nameformat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" td="" xmlns="urn:oasis:names:tc:SAML:2.0:assertion"><td><attribute friendlynam<="" td="" xmlns="urn:oasis:names:tc:SAML:2.0</td><td>:assertion"><td>e="Surname" Nam</td><td>heFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute></td></attribute>	<attribute friendlynam<="" td="" xmlns="urn:oasis:names:tc:SAML:2.0</td><td>:assertion"><td>e="Surname" Nam</td><td>heFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute>	e="Surname" Nam	heFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"		
Name= "http://schemas.xmlsoap.org/ws/2005/05//dentity/claums/sumame"/>	Name="http://schemas.xmlsoap.org/ws/2	005/05/identity/claim	s/surname"/>		
<a -="" <="" minis="um:oasis:names:tc:SAML:2.0:assertion" name+ormat="un:oasis:names:tc:SAML:2.0:attrname+format:uri" rendiyname+"ppid"="" td="" tribute=""><td><attribute namefo<="" ppid"="" td="" xmins="urn:oasis:names:tc:SAML:2.0</td><td>cassertion FriendlyNam</td><td>e="><td>rmat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute></td>	<attribute namefo<="" ppid"="" td="" xmins="urn:oasis:names:tc:SAML:2.0</td><td>cassertion FriendlyNam</td><td>e="><td>rmat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"</td><td></td></attribute>	rmat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"			
value= http://schemas.xmisoap.org/ws/z005/05/usi/uentus/changa/bioineertonalidentineer/>	<pre>nume= nup://schemas.xmisoap.org/ws/2</pre>	coustion" Friendlyblam	s/privatepersona	moenuner />	
CARCING A MINISS OF A CONSTRUCT A CONSTRUC	CACHOOLE ANNUS - GITLOGSISTIGHES.(C.SAME.2.0	Assertion Phenolynami	- Home ID Nam	ier ofmat= unitvasistnamestic.sAmet.2.0.attrilame*lormat.un	\ \

Figure 35. Modified Federation Metadata

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

Settings for SAMLIdentityAssert							
Configurat	m Man	agement	Migration				
On this p	On this page, you can add, delete, and view SAML 2.0 identity provider partners for this SAML 2.0 identity Asserter.						
🖟 Custom							
Identity	Identity Provider Partners						
New ~	Delete]		Showing 1 to 1 of 1 Previous Next			
🗖 Nai	ne 🗠						
SAK SSO (DPO)							
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

ninistration Console		
🔒 Home Log Out Preferences 🔤 Record Help	Q	Welcome, weblogic Connected to: OFSLLREL_dom
Home >Summary of Security Realms >myrealm >Providers >!	5AMLIdentityAssert >SAML_SSO_IDP01	
ettings for SAMLIdentityAssert		
General Site Info Single Sign-On Signing Certificate	Transport Layer Client Certificate Single Sign-On Service Endpoint	Artifact Resolution Service Endpoints
Save		
Configures a SAML 2.0 Web Single Sign-on Identity Provi The parameters that can be set on this Administration Co	der Partner's General Properties nsole page can also be accessed programmatically via the Java interfac	s that are identified in this help topic. For API information about those interfaces, see Related Topics.
– Overview Name:	SAML SSO IDP01	The name of this Identity Provider partner. More Info
Enabled		Specifies whether interactions with this Identity Provider partner are enabled on this server. More
Description		Info
Description.	SAML_SSO_IDP01	A site coesciption of this spenary provide parallel. Processing
Authentication Requests		
Identity Provider Name Mapper Class Name:		The Java class that overrides the default username mapper class with which the SAML 2.0 Identity Asserter provider is configured in this security realm. More Info
Issuer URI:	http://sts.ofsll.com/adfs/services/trust	The Issuer URI of this Identity Provider partner. More Info
🖉 Virtual User		Specifies whether user information contained in assertions received from this Identity Provider partner are mapped to virtual users in this security realm. More Info
Redirect URIs:		An optional set of URIs from which unauthenticated users will be redirected to the Identity Provider partner. More Info
/ofsll142/faces/*		
/FCJNeoWebul/*		
Process Attributes		Specifies whether the SAML 2.0 Identity Asserter provider consumes attribute statements contained in assertions received from this Identity Provider partner. More Info
- Signing		
Only Accept Signed Authentication Requests:	false	Specifies whether authentication requests sent to this Identity Provider partner must be signed. More $Info\ldots$
Only Accept Signed Artifact Requests		Specifies whether SAML artifact requests received from this Identity Provider partner must be signed. More Info
- Transport		
Send Artifact via POST		Specifies whether SAML artifacts are delivered to this Identity Provider partner via the HTTP POST method. More Info
Artifact Binding POST Form:		The LRL of the custom web application that generates the POCT form for carrying the SAML response for Attlinct brandyse to this identity Provider partner. Destails about the required fields in this custom explication are available in the OACS SAML 2.0 specifications. Were Info
POST Binding POST Form:		The URL of the custom web application that generates the POST form for carrying the SAML response for POST bindings to this Identity Provider partner. More Info
Client User Name:		The user name that must be specified in the basic authentication header that is expected from this Identity Provider partner when the partner connects to the local site's SOAP/HTTPS binding. More Info
Client Password:		The password of the client user name. More Info
Confirm Client Password:		
Save		

Figure 37. Weblogic Domain - Identity Provider
Configure Domain for SSO

- » Add Active Directory as Authentication Provider
 - » Log into Weblogic Admin console on OFSLL Domain
 - » Go to Security Realms \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: MyAD/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

😰 Home Log Out Preferences 🚁 Record Help		Welcome, weblogic Connected to: OFSLLREL_domain
Home >Summary of Security Realms >myrealm >Providers >MyADAuthenticator Settings for MyADAuthenticator		
Configuration Performance		
Common Provider Specific Click the Lock & Editbutton in the Change Center to modify the settings on this page.		
Save		
Use this page to define the provider specific configuration for this Active Directory Authentication	n provider.	
- Connection		The host name or IP address of the LDAP server. More Info
de Port:	389	The port number on which the LDAP server is listening. More Info
(문 Principal:	CN=ICN=Users	The Distinguished Name (DN) of the LDAP user that WebLogic Server should use to connect to the
Credentiak		LDAP server. More Info The credential (usually a password) used to connect to the LDAP server. More Info
Confirm Credential:		
C 🖉 SSLEnabled		Specifies whether the SSL protocol should be used when connecting to the LDAP server. More Info
- Users		The base distinguished name (DN) of the tree in the LDAP directory that contains users. More lofo
All Users Filter:	(% (a MM assount) lamon	If the attribute (user object class) is not specified (that is, if the attribute is null or empty), a default
	(G(SAWACCOUNTRAINE)	search filter is created based on the user schema. More Info
A User From name Filter:	(8(sAMAccountName=	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
de User Object Class:	user	The LDAP object class that stores users. More Info
Croups		specines whener or not the user name retrieved from the LDAP server should be used as the Principal in the Subject. More Info
Groups කිසි වර්ග කරගත් ක	OU=MyOrg.DC=ofsll.D(The base distinguished name (DN) of the tree in the LDAP directory that contains groups. More Info
at Groups Filter:	(&(cn-*)(objectclass-g	An LDAP search filter for finding all groups beneath the base group distinguished name (DN). If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the Group schema. More Inflo.,
🖑 Group From Name Filter:	(&(cn=%g)(objectclass	An LDAP search filter for finding a group given the name of the group. If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the group schema. More Info
後 Group Search Scope:	subtree v	Specifies how deep in the LDAP directory tree to search for groups. Valid values are subtree and onelevel. More Info
🏀 Group Membership Searching:	unlimited v	Specifies whether group searches into nested groups are unlimited or limited. Valid values are unlimited and limited. More Info
👸 Hax Group Membership Search Level:	0	Specifies how many levels of group membership can be searched. This setting is valid only if GroupMembershipSearching is set to limited. Valid values are 0 and positive integers. For example, 0 indicates only direct group memberships will be found, and a positive number indicates the number of
🗌 🐠 Ignore Duplicate Membership		Determines whether duplicate members are ignored when adding groups. The attribute cycles in the Group membership. More to fe
🗌 🚛 Use Token Groups For Group Membership Lookup		Indicates whether to use the Active Directory TokenGroups attribute lookup algorithm instead of the standard recursive groups membership lookup algorithm. More Info
— Static Groups		
C Static Group Name Attribute:	cn	The attribute of a static LDAP group object that specifies the name of the group. More Info
Static Group Object Class:	group	The name or the LDAP object class that stores static groups. More Into
	member	members of the group. More info
and Static Group Diffs from Prember Dif Filter:	(&(member=%M)(objec	An LDAP search nerr mar, given the astinguished name (try) of a memoir of a group, returns the une of the state LDAP groups that contain that member. If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the group schema. More Info
🏀 Dynamic Group Name Attribute:		The attribute of a dynamic LDAP group object that specifies the name of the group. More Info
委 Dynamic Group Object Class:		The LDAP object class that stores dynamic groups. More Info
他 Dynamic Member URL Attribute:		The attribute of the dynamic LDAP group object that specifies the URLs of the members of the dynamic group. More Info
🖑 User Dynamic Group DN Attribute:		The attribute of an LDAP user object that specifies the distinguished names (DNs) of dynamic groups to which this user belongs. More Info
Connection Pool Size:	6	The LDAP connection pool size. Default is 6. More Info
a Connect Timeout:	0	The maximum time in seconds to wait for the connection to the LDAP server to be established. If this attribute is set to 0, there is no maximum time limit. More Info
ණු Connection Retry Limit:	1	Specifies the number of times to attempt to connect to the LDAP server if the initial connection field. More take
생물 Parallel Connect Delay:	0	The delay in seconds when making concurrent attempts to connect to multiple LDAP servers. More
▲ Results Time Limit:	0	The maximum number of milliseconds for the LDAP server to wait for results before timing out. If this
A Keep Alive Enabled		attribute is set to 0, there is no maximum time limit. More Info Specifies whether to prevent LDAP connections from timing out. More Info
☑ 🖉 Follow Referrals		Specifies that a search for a user or group within the LDAP Authentication provider will follow referrals
🗌 🐠 Bind Anonymously On Referrals		Informs COmparations of the Information of the Comp Carectory of your and password used to connect to the DAP environment of the Comparation of the Comparation of the Comparation of the Comparation of the DAP environment when following referring adviring asserds. If you want to connect as an anomyous user,
/ / Propagate Cause For Login Exception		enable this attribute. More Info Specifies whether the providers should propagate the cause of the Louisefficienting. More take
☑ 🖉 Cache Enabled		Specifies whether a cache is used with the LDAP server More Info
4월 Cache Size:	32	The size of the cache (in kilobytes) that is used with the LDAP server More Info
신음 Cache TTL:	60	The time-to-live of the cache (in seconds) that is used with the LDAP server More Info
6일 GUID Attribute:	objectguid	Specifies the name of the GUID attribute defined in the Active Directory LDAP server. The default value is objectguid. More Info
Save		
Click the Lock & Edit button in the Change Center to modify the settings on this page.		

Figure 39. Weblogic Domain – Provider Specific Details

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

🔒 Home Log Out Preferences 🛛	Record Help	
Home >Summary of Security Realms	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 J/	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 J MyADAuthenticator	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 J/ MyADAuthenticator Provider that performs LDAP authentication	AAS Control Flag to control how f
This page displays basic informati	ion about this Active Directory Authentication provider. You can also use this page to set the J/ MyADAuthenticator Provider that performs LDAP authentication 1.0	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	nyrealm									
Configuration	Users and Groups	Roles and Policies	Credential Mappings	Providers	Migration	١				
Authentica	tion Password Valida	tion Authorization	Adjudication Re	ole Mapping	Auditing	Credential Mapping	Certification Path	Keystores		
An Authentic providers an	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 Click the Loc	tion Providers	Change Center to act	ivate all the buttons of	n this page.						
New	New Delete Reorder Showing 1 to 4 of 4 Previous Next									
🔲 Name			Description							Version
SAMLIC	lentityAssert	:	SAML 2.0 Identity Ass	ertion Provider	r. Supports S	Security Assertion Ma	arkup Language v2.0.			1.0
MyADA	uthenticator	1	Provider that perform	s LDAP authen	tication					1.0
Default	Authenticator		WebLogic Authenticat	ion Provider						1.0
Default	IdentityAsserter		WebLogic Identity As	sertion provide	r					1.0
New [lelete Reorder								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.	15
	< 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

\$	Add Relying Party Trust Wizard	X
Select Data Source		
Select Data Source Steps Velcome Select Data Source Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that published 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 validate the source of the file. Federation metadata file location: C:V vols1_metadata.xml Brow C:V vols1_metadata.xml	s s se
	< Previous Next > Can	el

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.	w the properties
	ОК

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		
	< 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 i there is a match for any of the specified requirements	íf
 Welcome Select Data Source 		1
Specify Display Name	Multi-factor Authentication Global Settings	
Configure Multi-factor Authentication Now?	Requirements Users/Groups Not configured	
 Choose Issuance Authorization Rules 	Device Not configured	
Ready to Add Trust	Ĩ	
 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>. 	
	< 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 Auth	orization 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 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	>
	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	1	V3
Serial n	umber	4a 39 4b 4b
Signatu	ire algorithm	sha1RSA =
Signatu	ire hash algorithm	sha1
Issuer		, Or
i Valid m	om	Tuesday, July 21, 2015 11:02
Valid Co		wednesday, July 20, 2016 11
	•	, 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						
Monitoring Id Organization	lentifiers Endpoints	Encryption Proxy End	Signature points N	Accepted	Claims anced	
URL SAML Accept	ion Consur	or SAML and	wS-Federations	Default	Re	
https:/	····	ner enapoin 0	POST	No		
https://		1	Artifact	No		
<					>	
Add SAML						
Add WS-Federa	ation		Remove	e Edi	t	
	[OK	Cance	a <u>A</u>	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 X
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 Consume	r v
Binding:	
Artifact	~
Set the trusted URL as	s default
Index: 1 😌	
Trusted URL:	
https:///	:8005/saml2/sp/acs/artifacts
Example: https://sts.conto	oso.com/adfs/ls
Response URL:	
Example: https://sts.conto	oso.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	Edit	: Claim R	Rules for	r UBS_:	sso_d(DMAIN	-		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 displayMame 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 🛛 🗙					
You car which to issued fi	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		
You car which to issued fi	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			(3 🕀 🖌
Logs			r I	To config	jure and manage this WebLogic A	Applica	tion
Performance Summary Application Deployment		Deployment, use the <u>Oracle WebLogic Server</u>		<u> </u>			
		F	- <u>Administration Console</u> .				
Web Services				_			
WebCenter P	ortal		► er.				
ADF			r II	EJBs			
Security			F I	Application Policies	Beans in Use	0	
MDS Configur	ation		٦.	Application Roles	Bean Accesses (per minute)	0.00	
TopLink Sessi	ons		12		Bean Access Successes (%)	0.00	
System MBea	Browser			Bean Tr	ansaction Commits (per minute)	0.00	
System Hoed	- i		-1	Bean Tra	nsaction Rollbacks (per minute)	0.00	0 0
' WebLogic Ser	ver Administratio	on Console	-1	Bean Tra	ansaction Timeouts (per minute)	0.00	
General Infor	mation		J		Bean Transaction Commits (%)	0.00	
Entry Poin	ts					-	٥.
Web Modules							
Name	Test Poin	t					
ofsll 142	http://			3003/ofsll142			
ofsll 142	https:/			:8005/ofsll142			
Web Services							
Service Name		Port					Test
	F 1	1	_				

Figure 67. Weblogic EM – Application Roles

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

of sl _ 142 (V14.2.0.0.1-b139)				
A spikation Deployment * Page Nafmehed Oxt 30, 2015 5:54:02 PM 15 Pplication Roles pplication roles are the roles used by security waver applications. These roles are seeded by applications in single global policy store when the applications are registered. These are also application roles that are specific to the application. To manage users and groups in the WebLogic Domain use the Oracle WebLogic Server Security Provider. Scope WebLogic Domain Note: The seeded by application uses a stripe that is different from application name. Scope WebLogic Domain Provider Book Scope WebLogic Domain Lister SWh I I I I I I I I I I I I I I I I I I I	ofsll_142(V14.2	2.0.0.1-b139) 🕦		Logged in as weblogic/Host
plication Roles plication roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in single global policy store when the applications are registered. These are also application roles that are exacted in the context of and users accessing the application. Policy Store Provider Scope WebLogic Domain Provider DB_ORACLE Sole Name DB_ORACLE Center Lister Center DB_ORACLE CENTER D	Application Deployment	•		Page Refreshed Oct 30, 2015 5:54:22 PM IST
To manage users and groups in the Weblogic Domain, use the Oracle Weblogic Server Security Provider. > Policy Store Provider Scope Weblogic Domain Provider DB_ORACLE > Search Enter search keyword for role name to query role defined by this application. Use application uses a stripe that is differerent from application name. Role Name Starts Wth I'' Create I''' Create Like I'' Create I''' Create Like OFSL_USSR OFSL USER	pplication Roles Application roles are the ro reated in the context of e	les used by security aware applications nd users accessing the application.	that are specific to the application. Th	ese roles are seeded by applications in single global policy store when the applications are registered. These are also application roles that are
✓ Policy Store Provider Scope WebLogic Domain Provider B	To manage users and g	roups in the WebLogic Domain, use the	Oracle WebLogic Server Security Prov	ider.
Scope Weblings Domain Provider DB_ORACLE Provider DB_ORACLE Search Enter search keyword for roles name to query roles defined by this application stripe to search if application uses a stripe that is different from application name. Role Name Starts With Role Orsel_USER Opslay Name Principal Display Name Principal Display Name Principal Display Name	Policy Store Provide	er		
Privider DB_ORACLE Search 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 Starts With		Scope WebLogic Domain		
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 Definition Create Control Create Control Create OFSL USER Membership for OFSLL_USER Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Description Create Principal Display Name Display Name Description Create Principal Display Name Description Create Principal Display Name Display Name Description Create Principal Display Name Display Nam Display Name Display Name Display Name Display N		Provider DB_ORACLE		
Enter search keyword for roles heffed by this application. Use application stripe to search if application uses a stripe that is different from application name. Role Name Starts With Role Create Create Create Create Create Create Create Create Create Create Create Create OrSaL.uses OrSaL USER	≤ Search			
Role Name Starts With Create Like Edit X Delete Role Name Display Name Description OFSL_USER OFSL_USER OFSL_USER	Enter search keyword for	r role name to query roles defined by t	is application. Use application stripe to	search if application uses a stripe that is differerent from application name.
Image: Contract Like ✓ Edit X Delete Rack Name Deplay Name Description OFSL_USER OFSL_USER		Role Name Starts With 💌		
Role Name Deploy Name Description OPSIL_USER OPSIL USER Membership for OFSLL_USER Principal Display Name Principal Display Name OPSIL Opsil Principal Opsil OPSIL Opsil Principal Opsil Opsil Opsil Opsil Opsil	Create 🛛 😭 Cr	eate Like 🥜 Edit 💥 Delete.	.	
OFEL_USER OFELLUSER ✓ Membership for OFSLL_USER Principal Display Name Type Description OFEL_USER	Role Name	Display Name	Descri	tion
Membership for OFSLL_USER Principal Display Name Type Description OFSL LISERS Group	OFSLL_USER	OFSLL USER		
≥ Membership for OFSLL_USER Principal Display Name Type Description OFSL USERS Group				
YMembership for OFSLL_USER Principal Display Name Type Description GPSL USERS Group				
Membership for OFSLL_USER Principal Display Name Type Description OFSL LISERS Group				
y Membership for OFSLL_USER Principal Display Name Type Description OFSL LISER Group OFSL LISER OFSU LISER				
Membership for OFSLL_USER Principal Display Name Type Description OFSL LISERS Group				
Membership for OFSLL_USER				
Membership for OFSLL_USER				
Membership for OFSLL_USER Principal Display Name Type Description OFSL LISTRS Group				
Membership for OFSLL_USER Principal Display Name Type Description OFSIL LISERS Group Open Description Open Description				
Principal Display Name Type Description	≤ Membership for 0	FSLL_USER		
OFSU LISERS Group	Principal	Display Name	Type Description	
	OESIL USERS		Group	

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 🕻
pplication Role Application roles are created in the conte	es the roles used by security aware applicatio ext of end users accessing the application.	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 Oracle WebLogic Server S	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			
	Digplay Namo	Time	Description	
Principal	Display Malle	Type	Description	

Figure 69. Weblogic EM – Edit Application Roles

» Click on Members \rightarrow "Add"

511_112(11112	.0.0.1-b139) 🔋		Logged in as web
pplication Deployment	•		Page Re
ication Roles > Edit Ap	plication Role		
Application Role	: OFSLL USER		
neral			
Application Stripe	ofsl_142#V14.2.0.0.1-b139		
Role Name	OFSLL_USER		
Display Name	OFSLL USER		
Description			
mbers			
mbers application role may n	eed to be mapped to users or groups defined in enterprise LDAP server, or the role can be m	apped to other application roles.	
application role may n	eed to be mapped to users or groups defined in enterprise LDAP server, or the role can be m	apped to other application roles.	
embers application role may n de Add X Delete Name	eed to be mapped to users or groups defined in enterprise LDAP server, or the role can be m	apped to other application roles.	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 y	ou want to grant permissi	ons to.
✓ Search			
Туре	Group 💌		
Principal Name	Starts With 💌		
Display Name	Starts With 💌		\bigcirc
Searched Principals			
Principal	Display Name	Description	
× Advanced Option			
Check to enter princip	pal name here instead of search cenarios related to custom auth	hing from above. This opt ienticators.	ion can be
Type Group 💌 * Prin	cipal Name OFSLL_USERS		
Dis	splay Name OFSLL_USERS		
		ОК	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	Up (13)		3
Name		Status	Target
V 🛅 Application Deployments			
Internal Applications			
FCUBSAppul(12.0.3.0.0)		Û	OFSLL_Manageds
C ofsl142(V14.2.0.0.1-b139)		Û	OFSLL_Managed
OracleFSLLBCCalculatorService_calculatorBusinessServiceInterface		Û	OFSLL_Managed
Cambridge Samldest0 1App		Û	OFSLL_Managed
amldest01App01		Û	OFSLL_Managed
Carl TrustManager		Û	OFSLL_Managed

Figure 72. Weblogic EM –Deployments

» Select Application Deployment -> Security -> Application Policies

ofss220081.in.oracle.com:8001/em/faces/as/wlFa	rmHome?target=Farm_OFSLLREL_domain&type=oracle_jas_farm&_afrLoop=7206551856825141#%2Fas%2Fsecurity%2FappPoliciesMain! 🤝 ⊄ 🛛 🔍 Search	☆ 自 ♣ 兪
	Idleware Control	Setup • Help •
Farm 👻 🚑 Topology		a na serie de la compe
Complete the set of the set		Logged in as weblogie(Host of as22008). In orac Dege Refreshed Oct 16, 2015 61642 PM1 urry polices assigned.
3	MOS Configuration Application Roles Description TopLink Seasons Biz USBR System Mean Branser onymous Role Ceff Weblags Server Administration Console General Information	
ł	MOS Configuration Application Reles Description TopLink Seasons System Riesen Bouwser © Webbage Server Administration Console © Webbage Server Administration Console ✓ Policies for OFSLL_USER	
ł	MOS Configuration Application Roles Description TopLink Seasons System Ream Bousser Of Websage Server Administration Console Central Information Policies for OFSLL_USER Permissions Internation Inte	
3	MOS Configuration Application Roles Description TopLick Series System Mean Braview omymous Role Of Wetkogs Server Administration Console General Information	Permission Class
ł	MOS Configuration Application Reles	Permission Class wake add controller security Tadd FlowPermission wake add controller security Tadd FlowPermission
3	MOS Configuration Application Roles Description TopLink Selos System Rean Browser	Permission Class arade. adf. controller. security. TaskflowPermission arade. adf. controller. security. TaskflowPermission arade. adf. controller. security. TaskflowPermission

Figure 73. Weblogic EM –Security Policies

» Below detail shows up

Policy Store Provider				
Search				
elect an application stripe in p	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.
Principa	al Type Application Role 💌			
	Name Starts With			
Create	Ke Ke Kelete			
incipal	Display Name	Description		
FSLL_USER	OFSLL USER			
ionymous-role	Anonymous Role			
Policies for OFSLL_USE	R			
volicies for OFSLL_USE	R			
folicies for OFSLL_USE	R		Rominstein & Hone	Berminian Plane
volicies for OFSLL_USE ermissions Resource Name	R		Permission Actions	Permission Class
Policies for OFSLL_USE ermissions Resource Name WEB INF Jorade (si/pattern/	R dynamicShell/nfra/blank.xmi#blank		Permission Actions view	Permission Class oracle.adf.controler.security.TaskFlowPermissio
Policies for OFSLL_USE termissions Resource Name //EB-INF/oradr/injattern/	R dynamicShell/nfra/blank.xml#blank		Permission Actions view view	Permission Class or acle.adf.controller.security.TaskFlowPermissio or acle.adf.controller.security.TaskFlowPermissio
Policies for OFSLL_USE >ermissions Resource Name /WEB-INF/forade/ui/pattern/ /WEB-INF/faskfows/originati	R dynamicShell/infra/blank.xmi#blank ion/.*		Permission Actions View View View	Permission Class oracle.adf.controller.security.TaskFlowPermissio oracle.adf.controller.security.TaskFlowPermissio 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 solf shares as a state of	descise films Descise Descriptions	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

olication Stripe ofsl 142#V1	4.2.0.0.1-b139			
rantee				
elect the grantees (user, grou	p or application role) you want to add to the	e policy.		
👍 Add 🛛 💥 Delete				
Name	Display Name	Туре	Description	
OFSLL USER	OFSLL USER	Application Role		
missions	lete			
rmissions Add // Edit % De Permission Class	lete	Resour	ce Name	Permission Actions
Permissions Add // Edit & De Permission Class orade.adf.controller.security	lete TaskFlowPermission	Resour	ce Name NF∫orade,ju/pattern/dynamicShell/nfra/blank.xml≠blank	Permission Actions view
Thissions Add Clit & De Permission Class oracle.adf.controller.security oracle.adf.controller.security	lete TaskflowPermission TaskflowPermission	Resou /WEB-1 /WEB-1	ce Name NF∫orade/ul/pattern/dynamicShel/infra,blank.xml≠blank NF[taskflows/orm].*	Permission Actions view view
TRISSIONS Add Clit & De Permission Class oracle.adf.controller.security oracle.adf.controller.security oracle.adf.controller.security	lete TaskFlowPermission TaskFlowPermission TaskFlowPermission	Resour /WEB- /WEB- /WEB-	ce Name NF/orach/ul/pattern/dynamicShell/infra/blank.xml≢blank NF/taakflows/orgination/.*	Permission Actions View view View
missions Add 2 Edit & De Permission Class orade.adf.controller.security orade.adf.controller.security orade.adf.controller.security	lete TaskFlowPernission TaskFlowPernission TaskFlowPernission Torization.RegionPernission	Resou /WEB- /WEB- /WEB- orade	ce Name NF∫orade,lu/pattern/dynamicShell/nfra/blank.xml≢blank NF∫taskflows/cmn∫.* NF∫taskflows/pagedefs.templates.OfSlCanvasPageTemplatePageDef	Permission Actions view view view view view
Edit & De Permission Class oracle.adf.controller.security oracle.adf.controller.security oracle.adf.share.security.aut oracle.adf.share.security.aut	lete TaskFlowPermission TaskFlowPermission TaskFlowPermission TaskFlowPermission Torization.RegionPermission	Resour /WEB- /WEB- /WEB- arade. arade.	ce Name NF/oradc/ui/pattern/dynamicShell/nfra/blank.xml=blank NF/taakflows/cmn/.* NF/taakflows/origination/.* ofal.view.pagedefs.sampalsers.pages.ofall=comePageDef ofal.view.pagedefs.pages.ofall=comePageDef	Permission Actions view view view 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	×
Select from permi Customize resour	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 a second	NAMES OF TAXABLE PARTY OF TAXABLE PARTY.	_ 0 X	
Control and the second	× X O Waiting for X	6 🕁 🕮	
There is a problem with this website's security cert	ficate.		
The security certificate presented by this website was not issu	d by a trusted certificate authority.		
Security certificate problems may indicate an attempt to fool server.	ou or intercept any data you send to the		
We recommend that you close this webpage and do not o	ontinue to this website.		
Click here to close this webpage.			
Continue to this website (not recommended).	Continue to this website (not recommended).		
More information	Connecting to situ of all con.		

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	×		No. of Concession, name	And Personnel Name		
← ⇒ C fi	SAM	1LRequest=fZBNa8MwDIb%2FitE9ie	18rDFxSqEUChuMrdthl%2BI5zh	pw7CxySn%2F%2BspSx7rKjkB69el	StL70lZzNi550EFIMgxmnfdO5DwsthF61gXVeoejuIzRRO7sl8Tg	YC☆ ≡
					sts.ofsll.com	
					Sign in with your organizational account	
					ofsilusr@ofsil.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