Single Sign-on Configuration Guide -SAML Oracle Banking APIs Patchset Release 22.2.3.0.0

Part No. F72988-01

February 2024

# ORACLE

Single Sign-on Configuration Guide -SAML February 2024

Oracle Financial Services Software Limited Oracle Park Off Western Express Highway Goregaon (East) Mumbai, Maharashtra 400 063 India Worldwide Inquiries: Phone: +91 22 6718 3000 Fax:+91 22 6718 3001

www.oracle.com/financialservices/

Copyright © 2006, 2024, Oracle and/or its affiliates. All rights reserved.

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

# **Table of Contents**

1.	Pref	face1–1
1	1.1	Intended Audience
1	1.2	Documentation Accessibility
1	1.3	Access to Oracle Support
1	1.4	Structure
1	1.5	Related Information Sources1-1
2.	Intro	oduction2–1
3.	Con	ofiguration
3	3.1	Identity Provider Configuration at IDCS
3	3.2	SAML Authentication Provider configuration
3	3.3	SQL Authentication Provider configuration
3	3.4	OHS Configuration
3	3.5	Database Configuration
3	3.6	IDCS OAuth Integration
3	3.7	WebLogic configuration for OAuth
3	8.8	OBAPI configuration for OAuth
3	3.9	Default Admin Configuration
3	3.10	Logout Configurations

# 1. Preface

# 1.1 Intended Audience

This document is intended for the following audience:

- Customers
- Partners

# 1.2 **Documentation Accessibility**

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <a href="http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.">http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.</a>

# 1.3 Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit

http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit

http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs\_if you are hearing impaired.

# 1.4 Structure

This manual is organized into the following categories:

Preface gives information on the intended audience. It also describes the overall structure of the User Manual.

The subsequent chapters describes following details:

- Introduction
- Preferences & Database
- Configuration / Installation.

# 1.5 **Related Information Sources**

For more information on Oracle Banking APIs Patchset Release 22.2.3.0.0, refer to the following documents:

Oracle Banking APIs Installation Manuals



# 2. Introduction

This document covers step-by-step details on configuration required at IDCS side (Application and User) and WebLogic console configurations for SAML and SQL Authentication Providers. Document also includes the configuration required on OHS to enable different URL's for internal and external user login.

Home



# 3. Configuration

To enable SAML authentication it involves configuration at WebLogic server (console) and IDCS console.

# 3.1 Identity Provider Configuration at IDCS

Steps to configure Identity Provide at IDCS

1. Login to Oracle Identity Cloud Service (IDCS) console with admin login. In dashboard click on **Add Application** in Application and Services widget or navigate through the breadcrumb menu as highlighted in screenshot.

### Dashboard

Users	🛶 🎍	Applications an	d Services 🛛 😨	Groups	🍲 🎂
-		-	$\bigcirc$	-	
Total	_	Total		Total	_
		- Created	– Removed		
Passwords		Logins		All Reports	
-	Ŷ	-	8		
Resets		Total			
- Failed Attempts		- Failed Attempts			

2. In popup window select SAML Application.

### Add Application

🗆 Select All 🛛 🕂 A	dd 🗙 Remove 🔘 Activate 🖉 Deactivate				
$\sim$	Add Application		×		
	App Catalog	Add an application from the Application Catalog.	•	2	T
•	SAML Application	Create an application that supports SAML for Single Sign On.	C	>	Ξ
•	Mobile Application	Create a mobile/single-page application that uses OAuth 2.0. These applications cannot maintain the confidentiality of their client secret.	•	2	1
•	Confidential Application	Create a web-server/server-side application that uses OAuth 2.0. These apps typically run on a server and can maintain the confidentiality of their client secret.	¢	9	T
•	Enterprise Application	Create a web application that is protected by the App Gateway.		>	Ŧ



- 3. In Add SAML Application page provide below mentioned fields and click on Next.
  - i. Name
  - ii. Description

#### Add SAML Application

Add SAML Application			
Cancel		2 SSO Configuration	Next >
Details		550 configuration	
	OBDX_SAML_CONFIG		
Description	SAML Configuration for OBDX user authentication.		
Application Icon			
	Upload		
Application URL / Relay State	Add Remove		

- 4. Fill below mentioned fields as per section.
  - i. General
    - a. Entity Id: A unique identifier / name for the service provider.
    - Assertion Consumer URL: End point to which assertion will be sent by IDCS. Recommended URL format <u><OHS\_URL>/saml2/sp/acs/post</u>

e.g. <PROTOCOL>://<OHS\_HOST>:<OHS\_PORT>/saml2/sp/acs/post http://whf000xxx.bank.com:9999/saml2/sp/acs/post

- c. NameID Format: Select value as "Unspecified".
- d. NameID Value:- Select value as "User Name".

### Add SAML Application

Add SAML Application				
< Back		2		Finish
Details		SSO Config	guration	
			Download Signing Certificate	Download Identity Provider Metadata
✓ General Use this section to define the required SSO attributes for the app * Entity ID	lication and to upload the application's sig OBDX_SAML	ning certificat	ie.	
	http://example.com/saml2/sp/acs/post			
* NameID Format				
* NamelD Value	User Name 🔻			
Signing Certificate	Upload			



- ii. Advance Settings
  - a. Signed SSO :- Select value as "Assertion"
  - b. Enable Single Logout: This field should be checked.
  - c. Logout Binding: Select value as "Redirect".
  - d. Single Logout URL: End point which IDCS will make call to do single logout functionality.

Recommended URL format <OHS\_URL>/digx-infra/sso-logout

e.g. <PROTOCOL>://<OHS\_HOST>:<OHS\_PORT>/digx-infra/sso-logout http://whf000xxx.bank.com:9999/digx-infra/sso-logout

e. Logout Response URL: -Recommended URL format <OHS\_URL>/digx-infra/sso-logout

e.g. <PROTOCOL>://<OHS\_HOST>:<OHS\_PORT>/digx-infra/sso-logout http://whf000xxx.bank.com:9999/digx-infra/sso-logout

#### Add SAML Application

Advanced Settings

This section contains additional configuration options.

In

Signed SSO	Assertion <b>•</b>
clude Signing Certificate in Signature	
Signature Hashing Algorithm	SHA-256 💌
Enable Single Logout	✓
* Logout Binding	Redirect 💌
* Single Logout URL	http://example.com:9999/digx-infra/ssc
* Logout Response URL	http://example.com:9999

Encrypt Assertion 🔲

- 5. Click on Finish / Save.
- 6. Click on Activate button to activate your application.

#### **Edit Application**

Applications > OBDX_SAML_CONFIG		
OBDX_SAML_C		S Activate X Remove
Details SSO Configuration Users G	roups	Save
Application Type	SAML Application	
* Name	OBDX_SAML_CONFIG	
Description	SAML Configuration for OBDX user authentication.	
Application Icon	$\frown$	



- 7. Navigate to Dashboard and search the application you have created.
- 8. Navigate to **SSO Configuration** tab and click on "**Download Identity Provider Metadata**". Keep the downloaded xml file, it will be required to upload in WebLogic console. Same is explain in WebLogic console configuration steps.

### **Edit Application**

OBDX_SAML_CONFIG				⊘ Activate → X Remove
Details SSO Configuration Users Groups				
			Download Signing Certificate	Download Identity Provider Metadata
<i>▲</i> General				
Use this section to define the required SSO attributes for the appli	cation and to upload the application	's signing certificate		
* Entity ID				
* Assertion Consumer URL				
* NameID Format	Email address	*		
* NamelD Value	Primary Email	*		
Signing Certificate	Upload			

- 9. Copy / FTP the downloaded IDC metadata xml file to WebLogic server using winscp / putty.
- 10. Navigate to **Users** tab in application to add the users related to application.
- 11. Click on **Assign Users** or **Assign (+)** button to search and add the users into application. If user is not available follow steps mentioned in Section 1.3 to create new user.

#### **Edit Application**

			L_CONFIG XX user authentication.	Ø Deactivate	🗙 Remove
Details	SSO Configuration	Users	Groups Select All + Assign X Revoke		
			No users are assigned to this application.		

#### **Assign Users**



#### Configuration

As	Assign Users ×								×				
0	Pleas	se select up to 4	0 users to assig	n.									^
C	) Select	All								superadmin	ı	0	l
									S	elected: 1	Clear Selection	on	1
		First Name	Last Name	Email									1
		Super	Admin										1
		superadmin	superadmin										1
													1
													Ŧ
Pa	ge 1 of	1 (1-2 of 2 item	ns) K <	1 > >								OK	

12. Logout from IDCS console.



# 3.2 SAML Authentication Provider configuration.

Steps to configure SAML Authentication Providers changes into WebLogic console.

1. Login to WebLogic console with admin login and navigate to "Security Realms".

#### Security Realms

ORACLE WebLogic Server Adr	ministration Console 14.1.1	Q
Change Center	😰 Home Log Out Preferences 🔛 Record Help	Welcome, weblogic Connected to: trunk_dom_repl_domain
View changes and restarts	Home >Summary of Servers >Summary of Security Realms	
Click the Lock & Edit button to modify, add or delete items in this domain.	Summary of Security Realms	
Lock & Edit Release Configuration	multiple active security realms in a WebLogic Server domain, but only one car	ecurity roles, security policies, and security providers—that are used to protect WebLogic resources. You can have be set as the default security realm, which is reserved for domain administrative purposes. In this WebLogic Server domain. Click the name of the realm to explore and configure that realm.
Domain Structure		
trunk_dom_repl_domain  -Environment  -Servers  Clusters	Customize this table Realms (Filtered - More Columns Exist)	
Coherence Clusters	Click the Lock & Edit button in the Change Center to activate all the buttons	on this page.
Machines Virtual Hosts	New Delete	Showing 1 to 1 of 1 Previous   Next
Work Managers Concurrent Templates	🗆 Name 🏟	Default Realm
Startup and Shutdown Classes	myrealm	true
Security Realms	New Delete	Showing 1 to 1 of 1 Previous   Next
How do I 🗉		
Configure new security realms     Coable automatic realm costart		

2.  $\rightarrow$  Click on **myrealm** or your realm name present in screen. Navigate to "**Providers**" tab.

### Providers

Q
Connected to: obdx_domain
figure multiple
o 2 of 2 Previous Next
rsion
o 2 of 2 Previous   Next
6i

3. Select "DefaultAuthenticator" and change the Control Flag value to "SUFFICIENT".

#### **Default Authenticator**

ORACLE WebLogic Server Ad	ministration Console 14.1.1		Q						
Change Center	A Home Log Out Preferences		Welcome, weblogic Connected to: trunk_dom_repl_domain						
View changes and restarts	Home >Summary of Servers >Sun	Home >Summary of Servers >Summary of Security Realms >movealm >Providers >DefaultAuthenticator							
Click the Lock & Edit button to modify, add or delete items in this domain.	Settings for DefaultAuthentic	itor							
Lock & Edit	Configuration Performance	Migration							
Release Configuration	Common Provider Specific								
Domain Structure	Click the Lock & Edit button is	the Change Center to modify the settings on this page.							
trunk_dom_repl_domain	Save								
	This page displays basic inform sequence.	ation about this WebLogic Authentication provider. You can also use this	page to set the JAAS Control Flag to control how this provider is used in the login						
	🚝 Name:	DefaultAuthenticator	The name of this WebLogic Authentication provider. More Info						
Concurrent Templates Startup and Shutdown Classes	街 Description:	WebLogic Authentication Provider	A short description of the Authentication provider. More Info						
Deployments     Services     Security Realms	街 Version:	1.0	The version number of the Authentication provider. More Info						
-Interoperability *	🕂 Control Flag:	SUFFICIENT V	Returns how the login sequence uses the Authentication provider. More Info						
How do I	Sow								
Configure authentication and identity assertion providers     Configure the Password Validation provider		the Change Center to modify the settings on this page.							



- Again, navigate to "Security Realms" → myrealms → Providers and click on New button to create new Authentication Provider. Fill the below mentioned fields with appropriate values and click on OK.
  - i. Name: Name of authentication provider.
  - ii. Type :- Select value as "SAML2IdentityAsserter".

#### **Create Authentication Provider**

	ninistration Console 14.1.1			Q
Change Center	🙆 Home Log Out Prefe	rences 🚵 Record Help	٩	Welcome, weblogic Connected to: trunk_dom_repl_domain
View changes and restarts	Home >Summary of Server	s >Summary of Security Realms >myrealm	>Providers >DefaultAuthenticator >Sun	mmary of Security Realms >myrealm >Providers
No pending changes exist. Click the Release	Create a New Authentic	ation Provider		
Configuration button to allow others to edit the domain.	OK Cancel			
Lock & Edit Release Configuration	Create a new Authen	tication Provider	antiontics Devides	
Domain Structure	* Indicates required fields		entication Provider.	
trunk_dom_repLdomain  Chrowinoment  Servers  Clusters  Coherence Clusters	The name of the authent	ication provider. SAML_OBDX_CONFIG		
Machines Virtual Hosts Work Managers Concurrent Templates Startup and Shutdown Classes	This is the type of auther Type:	tication provider you wish to create. SAML2IdentityAsserter	~	
Solitup and Studiowi Classes  Deployments  Services  Security Realms  -Interonerability	OK Cancel			
How do I 😑				
Manage security providers				

- 5. Restart Admin Server.
- Login to WebLogic console and navigate to "Security Realms" → myrealms → Providers newly created authentication provider (e.g. SAML\_OBAPI\_CONFIG) and navigate to "Management" tab.
- 7. Click on New button to add the Identity Provider Partner and select "New Web Single Sign-On Identity Provider Partner"

#### Management

ORACLE WebLogic Server Ad	ministration Console 14.1.1	Q
Change Center	🔒 Home Log Out Preferences 🔤 Record Help	Welcome, weblogic Connected to: OBDX21ADMIN
View changes and restarts	Home >Summary of Security Realms >myrealm >Providers >SAML	
No pending changes exist. Click the Release Configuration button to allow others to edit the	Settings for SAML	
domain.	Configuration Management Migration	
Lock & Edit Release Configuration	On this page, you can add, delete, and view SAML 2.0 identity provider partners for this SAML 2.0 Identity Asserter.	
Domain Structure	Customize this table	
OBDX21ADMIN  -Environment  Deployments	Identity Provider Partners	
B-Services	New ~ Delete	Showing 0 to 0 of 0 Previous   Next
-Security Realms -Interoperability -Diagnostics	Name 🗞	
er Diagnostics	There are no items to display	
	New - Dolete	Showing 0 to 0 of 0 Previous   Next
	New Web Single Sign-On Identity Provider Partner	
	New WebService Identity Provider Partner	
How do I 🖂		
Create a SAML 2.0 Web Single Sign-on		

8. Provide the name for the identity partner and select the IDC metadata xml copied to WebLogic server. Click **OK** button to save.



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

	Use this page to:						
Domain Structure	one one page (0.						
trunk_dom_repl_domain	Enter the name of your new Single Sign-on Identity Provider partner						
₽-Environment	Specify the name and location of the SAML 2.0 metadata file that you received from this new partner						
***Servers	* Indicates required fields						
Clusters	- indicates required neids						
Coherence Clusters							
Machines	Please specify the name of the pa	tner.					
Virtual Hosts							
Work Managers     Concurrent Templates	* Name:	WebSSO-IdP-Partner-0					
Startup and Shutdown Classes							
Deployments	Please specify the name of the file	containing the partner metadata document.					
Services							
Security Realms	Path:	/scratch/app/domain/trunk dom repl domain/IDCSMetadata.xml					
Interonerability	Recently Used Paths:	/scratch/app/domain/trunk. dom.repl_domain					
How do I							
	Current Location:	100.76.153.182 / scratch / app / domain / trunk_dom_repl_domain					
Create a SAML 2.0 Web Single Sign-on	🗀 bin						
Identity Provider partner	Common						
<ul> <li>Configure authorization providers</li> </ul>	Config						
	init-info						
System Status	ims						
Health of Running Servers as of 9:09 AM	logs						
Failed (0)	orchestration						
Critical (0)	i original						
Overloaded (0)	servers						
Warning (0)	IDCSMetadata.xml						
OK (2)							
	OK Cancel						

- 9. Open the newly added Identity Provider Partner and select below mentioned checkboxes and field and click on **Save**.
  - i. Enable: Checked
  - ii. Virtual User: Checked
  - iii. Redirect URIs: /digx-infra/admin-dashboard

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

Domain Structure							
trunk_dom_repl_domain	The parameters that can be set on this Administration Console page can also be accessed programmatically via the Jave interfaces that are identified in this help topic. For API information about those interfaces, see Related Topics.						
Clusters	- Overview -						
Coherence Clusters Machines	Name:	IDCS_IT	The name of this Identity Provider partner. More Info				
Virtual Hosts Work Managers Concurrent Templates	🗹 Enabled		Specifies whether interactions with this Identity Provider partner are enabled on this server. More Info				
Startup and Shutdown ClassesDeployments	Description:		A short description of this Identity Provider partner. More Info				
Security Realms	- Authentication Requests -						
How do I	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.				
How do 1	rapper class frame.		realm. More Info				
Create a SAML 2.0 Web Single Sign-on Identity Provider partner     Configure authentication and identity	Issuer URI:	https://idcs- 93e9366b4e3e4ce68a7c4dafb329cbdf.ldentity.c9dev2.oc9qadev.com:443/fed	The Issuer URI of this Identity Provider partner. More Info				
assertion providers  Manage security providers	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				
System Status							
Health of Running Servers as of 11:40 AM	Redirect URIs: /digx-infra/admin-das	hboard	An optional set of URIs from which unauthenticated users will be redirected to the Identity Provider partner. More Info				
Failed (0)           Critical (0)           Overloaded (0)           Warning (0)           OK (2)							
	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				

10. Navigate to "Environment" → "Servers" and select the server on which SSO authentication application will be deployed.



#### Servers

ORACLE WebLogic Server Ad	ministration Console 14.1.1						Q
Change Center	🔒 Home Log Out Preferences 🔤	Record Help	Q		Welcome	, weblogic Conne	ected to: trunk_dom_repl_doma
View changes and restarts	Home >Providers >SAML_OBDX_IT >IDC	S_IT > Summary of Security R	ealms >myrealm >Providers	>SAML_OBDX_IT >Summary of	Servers >obdx_server1 >	Summary of Serve	rs
No pending changes exist. Click the Release	Summary of Servers						
Configuration button to allow others to edit the domain.	Configuration Control						
Lock & Edit Release Configuration Domain Structure trunk.dom.repl.domain Environment B-Clusters -Coherence ClustersMachines	A server is an instance of WebLogic ! This page summarizes each server th C2 Customize this table Servers (Filtered - More Column	nat has been configured in ti		-	n.		
Virtual Hosts	New Clone Delete					Show	ing 1 to 2 of 2 Previous   Next
Concurrent Templates	🗆 Name 🗇	Туре	Cluster	Machine	State	Health	Listen Port
Deployments	AdminServer(admin)	Configured			RUNNING	🖋 ОК	9011
Services Security Realms	obdx_server1	Configured	obdx_cluster	obdx_machine	RUNNING	🖋 ОК	19003
Interonerability	New Clone Delete					Show	ing 1 to 2 of 2 Previous   Next
How do I 🖂							

- 11. Navigate to "Federation Services" → "SAML 2.0 General" and provide values to below mentioned fields. Click on **Save**.
  - i. Published Site URL: Recommended URL format <u><OHS URL>/saml2</u> e.g. <<u>PROTOCOL>://<OHS\_HOST>:<OHS\_PORT>/saml2</u> <u>http://whf000xxx.bank.com:9999/saml2</u>
  - ii. Entity Id: Value should match with <u>Entity Id</u> provided in SAML configuration in IDCS console.
  - iii. Recipient Check Enabled: unchecked.

### SAML 2.0 General

o.g		
Published Site URL:	http://100.76.153.182:19003/saml2	The published site URL. More Info
Entity ID:	SAML_OBDX_IT	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

- 12. Navigate to "Federation Services" → "SAML 2.0 Service Provider" and provide values to blow mentioned fields and click on **Save**.
  - i. Enabled: Check box should be checked.
  - ii. Preferred Binding: Post
  - iii. Default URL: <OHS\_URL>/digx-infra/admin-dashboard

# 3.3 SQL Authentication Provider configuration.

Steps to configure SQL Authentication Providers changes into WebLogic console.

1. Login to WebLogic console with admin login and navigate to "Security Realms".



### Security Realms

			0
ORACLE WebLogic Server A			ž
Change Center	🏦 Home Log Out Preferences 🔤 Record Help	Q	Welcome, weblogic Connected to: trunk_dom_repl_domain
View changes and restarts	Home >Summary of Servers >Summary of Security Realms		
Click the Lock & Edit button to modify, add or delete items in this domain.	Summary of Security Realms		
Lock & Edit Release Configuration	multiple active security realms in a WebLogic Server dom	ain, but only one can be set as the default	policies, and security providersthat are used to protect WebLogic resources. You can have security realm, which is reserved for domain administrative purposes. r domain. Click the name of the realm to explore and configure that realm.
Domain Structure	This security realities page lists each security realities and	tas been configured in this webbogic serve	a domain, cack the name of the realm to explore and conlighte that realm.
trunk_dom_repl_domain	Customize this table Realms (Filtered - More Columns Exist)		
-ClustersCoherence ClustersMachines	Click the Lock & Edit button in the Change Center to act	ivate all the buttons on this page.	
	New Delete		Showing 1 to 1 of 1 Previous   Next
Concurrent Templates	Name 🗞	Default Realm	
Deployments	myrealm	true	
Security Realms	Now Delete		Showing 1 to 1 of 1 Previous   Next
How do I E			
Configure new security realms			
<ul> <li>Enable automatic realm restart</li> </ul>	1		

2.  $\rightarrow$  Click on **myrealm** or your realm name present in screen. Navigate to "**Providers**" tab.

### Providers

	Adminis	stration Console 1	14.1.1									Q
Change Center	1	🔒 Home Log Out	t Preferences 🔤	Record Help		Q			,	Welcome, weblogic	Connected to: obdx_	_domain
View changes and restarts		Home >Summary of	f Security Realms >m	nyrealm >Providers								
Click the Lock & Edit button to modify, add or delete items in this domain.	s	ettings for myrea	alm									
delete items in this domain.		Configuration U	lsers and Groups	Roles and Policies	Credential Map	pings Provide	ns Migrati	ion				
Domain Structure obdx_domain	11	Authentication	Password Validat	tion Authorization	Adjudication	Role Mapping	Auditing	Credential Mapping	Certification Path			
		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. Customize this table Authentication Providers Click the Lock & Edit button in the Change Center to activate all the buttons on this page. Showing 1 to 2 of 2 Previous   N					Next					
		Name			Descrip	tion				·	/ersion	
How do I		DefaultAuthentica	ator		WebLog	ic Authentication	Provider			1	.0	
Configure authentication and identity		DefaultIdentityAs	sserter		WebLog	ic Identity Asserti	on provider				.0	
assertion providers										Showing 1	to 2 of 2 Previous   I	Next
Configure the Password Validation provider												
<ul> <li>Manage security providers</li> </ul>	1 -											
<ul> <li>Set the IAAS control flag</li> </ul>												

- 3. Click on **New** button to create new Authentication Provider. Fill the below mentioned fields with appropriate values and click on **OK**.
  - i. Name: Name of authentication provider.
  - ii. Type :- Select value as "ReadOnlySQLAuthenticator".



### **Create New Authentication Provider**

ORACLE WebLogic Server Add	ministration Console 14.1.1			Q
Change Center	A Home Log Out Preference	es 🔤 Record Help	Q	Welcome, weblogic Connected to: test221_domain
View changes and restarts	Home >Summary of Servers >o	bdx_server1 >Summary of Servers >S	Summary of Security Realms >myreal	n >Providers >SQLAuth >Summary of Security Realms >myrealm >Providers
No pending changes exist. Click the Release Configuration button to allow others to edit the domain.	Create a New Authentication	n Provider		
Lock & Edit Release Configuration	Create a new Authentica The following properties will	tion Provider be used to identify your new Auth	entication Provider.	
Domain Structure	* Indicates required fields			
test21_domain  Extrinonment  Coherence  Cohe	The name of the authenticati * Name:	on provider. SQLAuth		
Virtual HostsWork ManagersConcurrent TemplatesStartup and Shutdown ClassesDeployments	Type:	tion provider you wish to create. ReadOnlySQLAuthenticator	*	
Services     Deta Sources	OK Cancel			
How do I   • Manage security providers  • Configure authentication and identity assertion providers				

4. Open newly created authentication provider (e.g. SQLAuth). Select the value of **Control** Flag as "SUFFICIENT"

### Settings for Read Only SQL Authentication Provider

delete items in this domain. Lock & Edit	Configuration Performance	2	
Release Configuration	Common Provider Specific		
Domain Structure	Click the Lock & Edit button	in the Change Center to modify the settings on this page.	
test221_domain	Save		
Environment     Servers     Custers     Coherence Clusters     Machines	This page displays basic infor sequence.	mation about this Read-only SQL Authentication provider. You can also use th	ils page to set the JAAS Control Flag to control how this provider is used in the login
Virtual Hosts	🛃 Name:	SQLAuth	The name of this Read-Only SQL Authentication provider. More Info
Concurrent Templates Startup and Shutdown Classes	🛃 Description:	Provider that performs DBMS authentication	A short description of this Read-Only SQL Authentication provider. More Info
-Services -Security Realms -Interoperability	전 Version:	1.0	The version number of this Read-Only SQL Authentication provider. More Info
How do I	🚝 Control Flag:	SUFFICIENT ~	Specifies how this Read-Only SQL Authentication provider fits into the login sequence. More Info
<ul> <li>Configure authentication and identity assertion providers</li> </ul>	Save		
Set the JAAS control flag	Click the Lock & Edit button	in the Change Center to modify the settings on this page.	
Manage security providers			
System Status			
Health of Running Servers as of 9:32 AM			

- 5. Navigate to "Provider Specific" tab to configuration related to SQL Authentication.
- 6. Provide the values to fields mentioned below with given value in case it is not auto populated.
  - i. Data Source Name: NONXA
  - ii. SQL Get Users Password: SELECT U\_PASSWORD FROM USERS WHERE U\_NAME = ?
  - iii. SQL User Exists: SELECT U\_NAME FROM USERS WHERE U\_NAME = ?
  - iv. SQL List Users: SELECT U\_NAME FROM USERS WHERE U\_NAME LIKE ?
  - v. SQL List Groups: SELECT G\_NAME FROM GROUPS WHERE G\_NAME LIKE ?
  - vi. VI. SQL Group Exists: SELECT G\_NAME FROM GROUPS WHERE G\_NAME = ?
  - vii. SQL Is Member: SELECT G\_MEMBER FROM GROUPMEMBERS WHERE G\_NAME = ? AND G\_MEMBER = ?



- viii. SQL List Member Groups: SELECT G\_NAME FROM GROUPMEMBERS WHERE G\_MEMBER = ?
- ix. SQL Get User Description: SELECT U\_DESCRIPTION FROM USERS WHERE U\_NAME = ?
- x. SQL Get Group Description: SELECT G\_DESCRIPTION FROM GROUPS WHERE G\_NAME = ?

Settings for Read Only SQL Authentication Provider

Deployments Services Security Realms	Data Source Name:	NONXA	The data source used by this Read-Only SQL Authentication provider. More Info
Interonerability Y	Group Membership Searching:	unlimited ~	Specifies whether recursive group membership searching is unlimited or limited. Valid values are unlimited andlimited. More Info
Configure authentication and identity assertion providers Manage security providers	Max Group Membership Search Level:	0	This specifies how many levels of group membership can be searched. This setting is valid only II Group Membership Searching is set to limited. Valid values are 0 and positive integers. For example, 0 indicates only direct group memberships will be found, a positive number indicates the number of levels to go down. More Info.
alth of Running Servers as of 9:38 AM	SQL Get Users Password:	SELECT U_PASSWORD F	The SQL statement used to look up a user's password. The SQL statement requires a single parameter for the username and must return a resultSet containing at most a single record containing the password. More Info
Failed (0) Critical (0) Overloaded (0) Warning (0)	SQL User Exists:	SELECT U_NAME FROM U	The SQL statement used to look up a user. The SQL statement requires a single parameter for the username and must return a resultSet containing al most a single record containing the user. More Info
OK (1)	SQL List Users:	SELECT U_NAME FROM L	The SQL statement used to retrieve users that match a particular wildcard search. The SQL statement requires a single parameter for the wildcarded usernames and returns a resultSet containing matching usernames. More Inflo
	SQL List Groups:	SELECT G_NAME FROM (	The SQL statement used to retrieve group names that match a wildcard Th SQL statement requires a single parameter for the wildcarded group name and return a resultSet containing matching group names <u>More Info</u>
	SQL Group Exists:	SELECT G_NAME FROM (	The SQL statement used to look up a group. The SQL statement requires a single parameter for the group name and must return a resultSet containin at most a single record containing the group More Info
	SQL Is Member:	SELECT G_MEMBER FRO	The SQL statement used to look up members of a group. The SQL statemer requires two parameters: a group name and a member or group name. It must return a resultSet containing the group names that matched More Info
	SQL List Member Groups:	SELECT G_NAME FROM (	The SQL statement used to look up the groups a user or group is a member of. The SQL statement requires a single parameter for the username or gro name and returns a resultSet containing the names of the groups that matched. More Info
	Descriptions Supported		Indicates whether user and group descriptions are supported by the databa used by the authentication provider. More Info
	SQL Get User Description:	SELECT U_DESCRIPTION	The SQL statement used to retrieve the description of a specific user. Only valid if Descriptions Supported is enabled. The SQL statement requires a single parameter for the username and must return a resultSet containing a most a single record containing the user description. More Info
	SQL Get Group Description:	SELECT G_DESCRIPTION	The SQL statement used to retrieve the description of a group. Only valid if Descriptions Supported is enabled. The SQL statement requires a single parameter for the group name and must return a resultificat containing at m a single record containing the group description. More Info
	Save		
	Click the Lock & Edit button in the Change Center to	o modify the settings on this page.	

- 7. Click on Save.
- 8. Navigate to "Security Realms"  $\rightarrow$  myrealms  $\rightarrow$  Providers and click on **Reorder** button.

### Authentication

<ul> <li>Set the IAAS control flag</li> </ul>		
<ul> <li>Manage security providers</li> </ul>		
Configure the Password Validation provider		
Configure authentication and identity     assertion providers	New Doleia Reorder Showing 1 b	o 4 of 4 Previous   Next
low do I 🖂	Default/dentity/Asserter     WebLogic Identity Assertion provider	1.0
-Interonerability	Default/uthenticator     WebLogic Authentication Provider	1.0
- Services - Security Realms	SQLAuth Provider that performs DBMS authentication	1.0
Startup and Shutdown Classes	SAML_TEST SAML 2.0 Identity Assertion Provider. Supports Security Assertion Markup Language v2.0.	1.0
	Name     Description	Version
Machines Virtual Hosts	New Dolor Reorder Showing to	o 4 of 4 Previous   Next
Coherence Clusters	Authentication Providers	
- Environment - Servers	Customize this table	
st221_domain *		
Domain Structure	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 cont Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBNS.	figure multiple
Release Configuration		
Lock & Edit	Authentication Password Validation Authorization Adjudication Role Mapping Auditing Credential Mapping Certification Path	
Lontiguration button to allow others to edit the domain.	Configuration Users and Groups Roles and Policies Oredential Mappings Providers Migration	



- 9. Reorder the authentication providers as given below.
  - i. SAML Authentication Provider
  - ii. SQL Authentication Provider
  - iii. Default Authenticator

### **Reorder Authentication Providers**

View changes and restarts	
No pending changes exist. Click the Release	Reorder Authentication Providers
Configuration button to allow others to edit the domain.	OK Cancel
Release Configuration	Reorder Authentication Providers You can reorder your Authentication Providers using the list below. By reordering Authentication Providers, you can alter the authentication sequence.
Domain Structure	Select authenticator(s) in the list and use arrows to move them up and down in the list.
test221_domain   Environmet  Serves  Coherence Clusters  -Motalines  -Withal Hods -Withal Hods -Withal Hods -Withal Hods -Withal Hods -Soutine Renjates -Soutine and Shutdown Classes -Security Realms	Image: Constraint of the second se
How do I	OK Cancel
Re-order authentication providers     Set the 1846 control floor	

10. Restart all the servers in domain including Admin Server.

\*\*Note: Accessing /saml2 uri from OHS (<OHS\_URL>/saml2), /saml2 uri has to be proxy bypassed from OHS

# 3.4 OHS Configuration

Provides details on configuration required on OHS to enable different URL's for internal and external users. i.e authentication with OBAPI or external service provider.

- 1. Open obapi.conf file from OHS server. You can find the location of obapi.conf file from httpd.conf file.
- 2. Verify if proxypass URLs are configured in obapi.conf file. If not then add entries as mentioned in below format.

ProxyPassMatch "/digx(.\*)" "<PROTOCOL>://<WL\_HOST\_NAME>:<WL\_PORT>/digx\$1"

ProxyPassReverse "/digx(.\*)" "<PROTOCOL>://<WL\_HOST\_NAME>:<WL\_PORT>/digx\$1"

ProxyPassMatch "/saml2(.\*)" "<PROTOCOL>://<WL\_HOST\_NAME>:<WL\_PORT>/saml2\$1"

ProxyPassReverse "/saml2(.\*)" <PROTOCOL>://<WL\_HOST\_NAME>:<WL\_PORT>/saml2\$1

ProxyPassMatch "/digx(.\*)" "http://whf000xxx.bank.com:19003/digx\$1"

ProxyPassReverse "/digx(.\*)" "http://whf000xxx.bank.com:19003/digx\$1"

ProxyPassMatch "/saml2(.\*)" "http:// whf000xxx.bank.com:19001/saml2\$1"

ProxyPassReverse "/saml2(.\*)" "http://whf000xxx.bank.com:19001/saml2\$1"



3. Add below virtual configuration into obapi.conf file.

##Virtual Hosts Listen <PORT\_1> <VirtualHost \*:<PORT\_1>> ServerName <HOST\_NAME> RewriteEngine On **RewriteOptions inherit** <Directory "\${DocumentRoot}"> Options FollowSymLinks AllowOverride all </Directory> </VirtualHost> Listen <PORT\_2> <VirtualHost \*:<PORT\_2>> ServerName <HOST\_NAME> RewriteEngine On RewriteRule "^(.\*)/config\.js\$" "<SERVER\_PROTOCOL>://<HOST\_NAME>:<PORT\_2>/framework/js/configurations/ config-admin.js" [R] <Directory "\${DocumentRoot}"> Options FollowSymLinks AllowOverride all </Directory> </VirtualHost>



\*\***Note:** Replace the <PORT\_1> & <PORT\_2> with the ports which are expose to outside world. Replace <SERVER\_PROTOCOL> and <HOST\_NAME> with appropriate values. E.g. http and whfxxx.sample.com (if hostname is not available then <HOST\_NAME> value can be IP address.)

```
# All other request passed through this rules.
m Ai other request passed through this rules.
ProxyPassMatch "/digx(.*)" "http://whf00qiw.in.oracle.com:19001/digx$1"
ProxyPassReverse "/digx(.*)" "http://whf00qiw.in.oracle.com:19001/digx$1"
ProxyPassMatch '/saml2(.*)" "http://whf00qiw.in.oracle.com:19001/saml2$1"
ProxyPassReverse "/saml2(.*)" "http://whf00qiw.in.oracle.com:19001/saml2$1"
##Virtual Hosts
Listen 8888
<VirtualHost *:8888>
     ServerName whf00qiw.in.oracle.com
     RewriteEngine On
     RewriteOptions inherit
     <Directory "${DocumentRoot}">
          Options FollowSymLinks
          AllowOverride all
          #Require all granted
     </Directory>
</VirtualHost>
Listen 9999
<VirtualHost *:9999>
          ServerName whf00qiw.in.oracle.com
          RewriteEngine On
RewriteRule "^(.*)/config\.js$" "http://whf00qiw.in.oracle.com:9999/framework/js/configurations/config-admin.js" [R]
     <Directory "${DocumentRoot}">
          Options FollowSymLinks
          AllowOverride all
          #Require all granted
     </Directory>
</VirtualHost>
```

4. Save obapi.conf file and restart ohs server.

# 3.5 Database Configuration

To enable SSO for external users below configuration need to be done in database.

 To enable SSO authentication for user type / enterprise role execute below query on intended database environment. Replace <USER\_TYPE> with the user type / enterprise role for which SSO authentication to be enabled.

UPDATE DIGX\_FW\_CONFIG\_ALL\_B SET PROP\_VALUE = 'External' WHERE PROP\_ID = '<USER\_TYPE>' AND CATEGORY\_ID = ' AuthenticationConfiguration ';

For example: - UPDATE DIGX\_FW\_CONFIG\_ALL\_B SET PROP\_VALUE = 'External' WHERE PROP\_ID = 'administrator' AND CATEGORY\_ID = 'AuthenticationConfiguration';



 Execute below query for redirection after authentication from SSO service provider back to OBAPI. Replace the value of <OHS\_URL\_FOR\_ADMIN\_USER\_LOGIN> with the OHS\_URL with port enable for external / admin user login, the virtual host enabled in section 3.4, step 3.

INSERT INTO DIGX\_FW\_CONFIG\_ALL\_B (PROP\_ID, CATEGORY\_ID, PROP\_VALUE, FACTORY\_SHIPPED\_FLAG, PROP\_COMMENTS, SUMMARY\_TEXT, CREATED\_BY, CREATION\_DATE, LAST\_UPDATED\_BY, LAST\_UPDATED\_DATE, OBJECT\_STATUS, OBJECT\_VERSION\_NUMBER, EDITABLE, CATEGORY\_DESCRIPTION) values ('SSO\_PUBLIC\_URL', 'dayoneconfig', '<OHS\_URL\_FOR\_ADMIN\_USER\_LOGIN>', 'N', null, 'Public SSO URL', 'ofssuser', to\_timestamp('29-09-22 10:05:56.00000000 AM', 'DD-MM-RR fmHH12:fmMI:SSXFF AM'), 'ofssuser', to\_timestamp('29-09-22 10:05:56.000000000 AM', 'DD-MM-RR

For Example: - INSERT INTO DIGX\_FW\_CONFIG\_ALL\_B (PROP\_ID, CATEGORY\_ID, PROP\_VALUE, FACTORY\_SHIPPED\_FLAG, PROP\_COMMENTS, SUMMARY\_TEXT, CREATED\_BY, CREATION\_DATE, LAST\_UPDATED\_BY, LAST\_UPDATED\_DATE, OBJECT\_STATUS, OBJECT\_VERSION\_NUMBER, EDITABLE, CATEGORY\_DESCRIPTION) values ('SSO\_PUBLIC\_URL', 'dayoneconfig', 'http:// whf000xxx.bank.com:9999', 'N', null, 'Public SSO URL', 'ofssuser', to\_timestamp('29-09-22 10:05:56.00000000 AM', 'DD-MM-RR fmHH12:fmMI:SSXFF AM'), 'ofssuser', to\_timestamp('29-09-22 10:05:56.000000000 AM', 'DD-MM-RR fmHH12:fmMI:SSXFF AM'), 'A', 1, 'N', null);

# 3.6 IDCS OAuth Integration

To fetch the user information from external SSO provider, application need to be registered as a client in IDCS. Below steps providers details on registering the application in IDCS.

1. Login to Oracle Identity Cloud Service (IDCS) console with admin login. In dashboard click on Add Application in Application and Services widget or navigate through the breadcrumb menu as highlighted in screenshot.

Users 🎄 🏂	Applications and Services	🖌 Groups 🛛 🏘 🏄
-	- 🗇	-
Total	Total	Total
	Created Removed	
Passwords	Logins	All Reports
- ?	- 8	
Resets	Total	
- Failed Attempts	- Failed Attempts	

### Dashboard



2. In popup window select **Confidential Application**.

## Add Application

		Cloud Service	License Type :	: Found	ation	?	SD
Applicatic	Add Applic	cation		× crij	iption, o	r t	٩
🗆 Select All 🛛 🕂 Ad		App Catalog	Add an application from the Application Catalog.				
		SAML Application	Create an application that supports SAML for Single Sign On.		0	1	
		Mobile Application	Create a mobile/single-page application that uses OAuth 2.0. These applications cannot maintain the confidentiality of their client secret.		0	1	=
	¢	Confidential Application	Greate a web-server/server-side application that uses OAuth 2.0. These apps Oppically run on a server and can maintain the confidentiality of their client secret.		0	7	=
	<b>~</b>	Enterprise Application	Create a web application that is protected by the App Gateway.		0	1	

- 3. In Add Confidential Application page provide below mentioned fields and click on Next.
  - i. Name
  - ii. Description

# Add Confidential Application

Add Confident	ial Applica	itior	)				
Cancel	1 Details		2 lient	Resources	Web Tier Policy	Authorization	Next >
App Details							
		* Name	OBDX_OAUTH	CONFIG			
	Des	cription	OAuth Configu details from ID		*		
	Applicat	ion Icon					
			Upload				

4. Select Configure this application as a client now option in screen as shown in below screenshot.



#### Configuration

### Add Confidential Application

Add Confid	lential Applica	tion				
< Back	<ul> <li>—</li> </ul>	2	3	(4)	5	Next >
	Details	Client	Resources	Web Tier Policy	Authorization	
• Configure this applic Authorization	Allowed Grant Types 🗌 Res	ource Owner 🗌 Clien	t Credentials 🗌 JW	□ Assertion □ SAML2 Ass	ertion 🗌 Refresh Token 🗌	Authorization Code 🗌 Implicit
		rice Code Client Authentication				
	Allow non-HTTPS URLs	cient Addiction				
	Redirect URL					
	Logout URL					
Po	ost Logout Redirect URL					
	Security 🗆 Trust	ed Client Certificate	Import			

- 5. Fill below mentioned fields as per section.
  - i. Authorization
    - a. Allowed Grant Types:- Select checkbox as "Client Credentials" and "JWT Assertion"

### Add Confidential Application

< Back	2	3	(4)	5	Next >
Details	Client	Resources	Web Tier Policy	Authorization	
• Configure this application as a client now O Authorization	Skip for later				
Allowed Grant Types	<ul> <li>□ Resource Owner  Clier</li> <li>□ Device Code</li> </ul>	nt Credentials 🗹 🛛 JWT	Assertion SAML2 Asse	ertion 🗌 Refresh Token 🗌	Authorization Code 🗌 Implicit
	Device Code     TLS Client Authentication				
Allow non-HTTPS URLs	0				
Redirect URL					
Logout URL					
Post Logout Redirect URL					
Security	□Trusted Client Certificate	Import			
Allowed Operations	Introspect     On behalf	Of			
ID Token Encryption Algorithm	None	•			

### ii. Token Issuance Policy

- a. Authorized Resources :- Select value as "Specific"
- b. Grant the client access to Identity Cloud Service Admin APIs: Click on Add button



## **Add Confidential Application**

Authorized O All Resources O Tagged Specific			
Resources			
+ Add Scope			
Resource	Protected	Scope	
No data to display.			
Grant the client access to Ident	ity Cloud Service Admin APIs		
+ Add			

c. In popup window search for "Identity Domain Administrator" and click on Add.

# Add App Role

Token Iss	suance Polic	y 🚯	Add App Role			×	
	Authorized Resources	<ul><li>All</li><li>Tagged</li><li>Specific</li></ul>	Select All	identity ×	٩	Î	
	Resources			Selected: 1 C	lear Selection	н	
	🕂 Add Scope		Nentity D	omain Administrator		I	
	Resource					Ш	
	No data to dis	play.				18	
	Grant the client	t access to Identity	,		- 1	Ш	
	🕂 Add					н	
	App Roles		Page 1 of 1 (1 o	f 1 items) K < 1 > X			
	No data to dis	play.			Ad		

d. Verify a row added in table for App Roles as shown like below screenshot



### **Add Confidential Application**

Token Issu	ance Policy	y 🚯				
	Authorized Resources	<ul><li>All</li><li>Tagged</li><li>Specific</li></ul>				
1	Resources					
	+ Add Scope					
	Resource		Protected	Scope		
	No data to disp	play.				
	Grant the client	access to Identity Cloud Service	e Admin APIs			
	+ Add					
7	App Roles			Protected		
	Identity Doma	in Administrator		No	×	

- e. Click on Next button on top.
- iii. Expose APIs to Other Applications: Select "Skip for later" and click on Next.

### Add Confidential Application

Add Confic	lential Applica	ation				
< Back	Details	Client	3 Resources	Web Tier Policy	5 Authorization	Next >
Specify the APIs that n						
	No	Resources are p	rotected by OAu	ıth		

iv. Web Tier Policy: - Select "Skip for later" and click on Next button.

Add Confide	ential Applica	ation				
< Back	Details	Client	Resources	4 Web Tier Policy	Authorization	Next >
	e, edit, and validate a web tie		you can import and ex	port existing policies.		

## Add Confidential Application

v. Click on "Finish"



### Add Confidential Application

Add Confider	itial Applica	ation				
< Back	Details	Client	Resources	Web Tier Policy	5 Authorization	Finish
Authorization	Enforce Grants as Auth					

6. After finish click a popup window will open with "Client ID" and "Client Secret" as shown in below screenshot. Copy the Client Id and Client Secret to text file to keep it handy as it will be required in further steps. Once copied click on "Close".

### Add Confidential Application

	License Type :: Foundation ? SD
Applications > OBDX_OAUTH_CONFIG	
OBDX_OAUTH_CONFIG OAuth Configuration for fetching user Application Added ×	Activate X Remove
Details         Configuration         Web Tier Policy         Us         Below is the new Client ID and Client Secret for your application.           App Details         This information also appears on the Configuration tab in the Details section for the application.	Generate Access Token Sawe
Application Type Conf Client Secret * Name OBC Description OAdur Configuration for returning user details from IDCS	
Application Icon	

7. Click on "Activate" button to activate the application.

### **Edit Application**

pplications > OBDX_OAUTH_CONFIG				
OBDX_OAUTH_ OAuth Configuration for fetching u		Activate X Remove		
Details Configuration Web Tier Policy App Details	Users Groups		Generate Access Token Save	
* Name Description	Onfidential Application OBDX_OAUTH_CONFIG OAuth Configuration for fetching user details from IDCS			
Application Icon				



8. Popup window asking confirmation to activate the application will open, click on "Ok" to activate the application.

#### Edit Application

Applications > OBDX_OAUTH_CONFIG		
OBDX_OAUTH		⊘ Activate → X Remove
Details Configuration Web Tier Policy App Details Application Type	Confirmation Are you sure that you want to activate the application OBDX_OAUTH_CONFIG?	Cenerate Access Token Save
	OBDX_OAUTH_CONFIG OAuth Configuration for fetching user details from IDCS	
Application Icon	$\sim$	

9. Logout from IDCS console.

# 3.7 WebLogic configuration for OAuth

To enable OAuth support on WebLogic server follow below mentioned steps.

- Login to WebLogic console with admin login and navigate to "Domain Structure" → "Deployments".
- 2. Click on "com.ofss.digx.connector"

### Deployments

elete items in this domain.	Confi	guration	Control	Monitoring					
Lock & Edit									
Release Configuration	This	page displ	avs the list	of Java EE applications and standalone app	lication modules installed to this domain.				
omain Structure				) or delete installed applications and modul		hox next to	the application nam	e and then using the r	ontrols on this name
t221_domain Environment Deployments	To ir	istall a new	application	n or module for deployment to targets in th				a and other damp of a	and one of these pages
Security Realms	Cus	tomize thi	is table						
-Interoperability Diagnostics	Depl	oyments							
	Install Update Delete Showing 1 to 24 of 24 Pro						to 24 of 24 Previous   Ne		
	0	Name 🔗			State	Health	Туре	Targets	Deployment Order
	0	@com.of	ss.digx.con	nnector	Active	🖋 ОК	Resource Adapter	obdx_server1	0
		🗄 👩 dig	e-admin		Active	🗸 ОК	Web Application	obdx_cluster	100
ow do I 🗄		🗄 👩 digi	k-auth		Active	🖋 ОК	Web Application	obdx_cluster	100
Install an enterprise application Configure an enterprise application		🗄 🦲 dig	e-cms		Active	🗸 ок	Web Application	obdx_server1	100
Update (redeploy) an enterprise application		🗄 👩 dig	c-coherence	e	Active	🗸 ок	Web Application	obdx_cluster	0
Monitor the modules of an enterprise application		🗄 👩 dig	e-common		Active	🖋 ОК	Web Application	obdx_server1	100
Deploy EJB modules		🗄 👩 dig	e-corporate	loan	Active	🗸 ок	Web Application	obdx_server1	100
Install a Web application		🗄 👩 dig	e-creditfacil	lity	Active	🗸 ок	Web Application	obdx_server1	100
/stem Status	0	E adig	e-edx		Active	🖋 ок	Web Application	obdx_server1	100
ealth of Running Servers as of 6:22 AM									

3. Navigate to "Configuration"  $\rightarrow$  "Outbound Connection Pools" tab and click on New.



## **Outbound Connection Pools Configuration**

Change Center	😰 Home Log Out Preferences 🔤 Record Help	٩	Welc	ome, weblogic Connected to: trunk_dom_repl_domain
View changes and restarts	Home >Summary of Deployments >com.ofss.digx.com	nector		
No pending changes exist. Click the Release	Settings for com.ofss.digx.connector			
Configuration button to allow others to edit the domain.	Overview Deployment Plan Configuration S	Security Targets Control Testing	Monitoring Notes	
Lock & Edit	General Properties Outbound Connection Po	ools Admin Objects Workload Instr	umentation	
Release Configuration				
Domain Structure trunk_dom_repl_domain B-Environment Deployments	This page displays a table of outbound connection p listed by connection factory interface and the instan connection pool group. Click the name of a group or Outbound Connection Pool Configuration Table	nces are listed by their JNDI names. Expand or instance to configure it. Automatically gen	a group to obtain configuration information	
Services     Security Realms	New Delete			Showing 1 to 1 of 1 Previous   Next
Interoperability     Diagnostics	Groups and Instances 🐟		Connection Factory Interface	
	javax.resource.cci.ConnectionFactory		javax.resource.cci.ConnectionFact	ory
	New Delete			Showing 1 to 1 of 1 Previous   Next
How do I				
Configure outbound connection pool properties				
System Status				
Health of Running Servers as of 6:26 AM				
Ealled (0)				

4. Select "javax.resource.cci.ConnectionFactory" and click on Next.

# **Outbound Connection Groups Configuration**

Change Center	🏦 Home Log Out Preferences 🛃 Record Help	٩	Welcome, weblogic	Connected to: trunk_dom_repl_domain
View changes and restarts	Home >Summary of Deployments >com.ofss.digx.com	sector		
No perding charges edd. Click the Release Configuration button to allow others to edit the domain. Lock & Edd Release Configuration Domain Structure trunk dom_repl_domain	Create a New Outbound Connection           Book         New         Finish         Cancel           Outbound Connection Group         In which outbound connection group do you want to Outbound Connection Groups	o create an instance?		Showing 1 to 1 of 1 Previous   Next
I <sup>™</sup> Deployments B <sup>™</sup> Services I <sup>™</sup> Security Realms B <sup>™</sup> Intercoperability B <sup>™</sup> Dignostics	Back Next Finish Cancel			Showing 1 to 1 of 1 Previous   Next
How do I				
Configure outbound connection pool properties				
System Status				
Health of Running Servers as of 6:26 AM				

5. Enter JNDI name as ra/DIGXConnectorSSOKEY and click on Finish.



### JNDI Configuration for Outbound Connection

Change Center	🏫 Home Log Out Preferences 🔤 Record Help	Q	Welcome, weblogic Connected to: trunk_dom_repl_domain
View changes and restarts	Home >Summary of Deployments >com.ofss.digx.conne	ector >Summary of Deployments >com.ofss.digx.connecto	R.
No pending changes exist. Click the Release Configuration button to allow others to edit the domain. Lock & Edit Release Configuration	Create a New Outbound Connection           Back         Finish         Cancel           JNDI name for Outbound Connection Instan- Enter the JNDI name that you want to use to obta		
Domain Structure	* Indicates required fields		
turik_don_reeLdonain 	The Orthound Connection Instance represents a con de * JNDI Name: Back Heat Frank Cancel	nnecton pool. The JNDI name can be used to obtain the ra/DIGXConnectorSSOKEY	i pool at runtime.

- 6. Again navigate to "Domain Structure"  $\rightarrow$  "Deployments".
- 7. Click on "com.ofss.digx.connector".

### Deployments

telete items in this domain.	Conf	figuration	Control	Monitoring						
Release Configuration  st221_domain Fervironment Deployments Scruckare Scruckare Ferviron Poloproptic	You To I	u can update	(redeploy) application		e application modules installed to this dor nodules from the domain by selecting the s in this domain, click <b>Install</b> .		x next to	the application nam	e and then using the c	ontrols on this page.
2 Diagnosocs	Ins	stall Upd	ate Dele	ete					Showing 1	to 24 of 24 Previous   Ne:
		Name 🔗			st	tate	Health	Туре	Targets	Deployment Order
		@com.of	ss.digx.con	nnector	Ac	ctive	🖋 ОК	Resource Adapter	obdx_server1	0
		🗄 👩 dig:	e-admin		Ac	tive	🗸 ОК	Web Application	obdx_cluster	100
ow do I		🗄 👩 dig:	k-auth		Ac	tive	🖌 ОК	Web Application	obdx_cluster	100
Install an enterprise application		E adig	c-cms		Ac	tive	🖌 ОК	Web Application	obdx_server1	100
Configure an enterprise application Update (redeploy) an enterprise application		E 👩 dig:	coherence	e	Ac	tive	🖌 ок	Web Application	obdx_cluster	0
Monitor the modules of an enterprise application	0	E adg	k-common		Ac	ctive	🖋 ОК	Web Application	obdx_server1	100
Deploy EJB modules	0	E adig	c-corporate	eloan	Ac	tive	🗸 ок	Web Application	obdx_server1	100
Install a Web application	0	E adig	c-creditfacil	lity	Ac	tive	🖌 ОК	Web Application	obdx_server1	100
ystem Status	0	E adig	k-edx		Ac	tive	🖋 ОК	Web Application	obdx_server1	100
Failed (0)	0	107	eurekaser	rver	Ac	tive	🖌 ОК	Web Application	obdx_server1	100

8. Navigate to "Security"  $\rightarrow$  "Outbound Credentials Mapping" tab and click on New.



### **Outbound Credentials Mappings**

Change Center	🔒 Home Log Out Preferences 🔛 Record Help	Q	Welcome, w	veblogic Connected to: trunk_dom_repl_domain
View changes and restarts	Home >Summary of Deployments >com.ofss.digx.conne	ctor >Summary of Deployments >com.ofss.di	gx.connector >Summary of Deployments >com.ofss.digx.co	onnector >Roles
No pending changes exist. Click the Release Configuration button to allow others to edit the domain. Lock & Edit Release Configuration	Settings for com.ofss.digx.connector           Overview         Deployment Plan         Configuration         S           Roles         Policies         Outbound Credential Mappi	ngs Inbound Principal Mappings Principal	Monitoring Notes	
Domain Structure           trunk_dom_repLdomain         #           #= Environment         #           #= Environments         #           #= Services         #           #= Services         #           #= Orienpoendity         #           #= Diagnostics         #	use default outbound credential mappings for all o contains the table of outbound credential mapping Customize this table Outbound Credential Mappings	utbound connection pools in the resource	E Enterprise Information System (EIS) to which you w adapter, or specify particular outbound credential may	
E Diagnostics	New Delete			Showing 0 to 0 of 0 Previous   Next
	🔲 WLS User 🐟	EIS User	Outbound Connection Pool	
		There are	no items to display	
	New Delete			Showing 0 to 0 of 0 Previous   Next
How do I				
<ul><li>Create outbound credential mappings</li><li>Delete outbound credential mappings</li></ul>				

9. Select "ra/DIGXConnectorSSOKEY" by navigating using next button. Once selected as shown in below screenshot, click on Next.

Change Center	🍙 Home Log Out: Preferences 🖂 Record: Help 🛛 🔍 Welcome, weblogic Connected to: trunk_dom_repl_domain
View changes and restarts No pending changes exist. Click the Release Configuration button to allow others to edit the domain.	Home >Summary of Deployments >coun.dis.dgs.connector >Summary of Deployments >coun.dis.dgs.connector >Summary of Deployments >coun.dis.dgs.connector >Roles Selecting a pool is required.
Lock & Edit Release Configuration	Create a New Security Credential Mapping Book, Next, Frieht, Cencel
Domain Structure	Outbound Connection Pool
trunk_dom_repl_domain	Which Outbound Connection Pool wood you like the credential map to be associated with? Selecting Resource Adapter Default will configure the credential mapping for all Outbound Connection Pool can then configure themselves to override these credentials.
Diagnostics	Showing 21 to 26 of 26 Previous   Next
	Outbound Connection Pool 🗠
	ra/DIGXConnectorOBSCF
	ra/DIGXConnectorOBTFPM_14.3
	ra/DIGXConnectorOBVAM
How do I	ra/DIGXConnector REWARDS
Create outbound credential mappings	r/DIGKConnectorSSOKEY
	Resource Adapter Default
System Status	Showing 21 to 26 of 26 Previous   Next
Health of Running Servers as of 6:37 AM	Back Next Frish Canes
Estlad (0)	

**Create New Security Credentials Mappings** 

10. Select "Default User" and click on Next.

## **Create New Security Credentials Mappings**

Change Center	🔝 Home Log Out Preferences 🚵 Record Help	9	Welcome, weblogic Connected to: trunk_dom_repl_domain
View changes and restarts	Home >Summary of Deployments >com.ofss.digx.connector >Sum	mary of Deployments >com.ofss.digx.connector >Su	ammary of Deployments >com.ofss.digs.connector >Roles
No pending changes exist. Click the Release Configuration button to allow others to edit the domain.	Create a New Security Credential Mapping Back Next Finish Cancel		
Lock & Edit Release Configuration Domain Structure	connections when the resource adapter is first started. Select	ting 'Default User' will configure the user that w	al connections' will configure the user that will be used for creating the initial will be used as the default for any authenticated WebLogic Server user that does not user that will be used for an unauthenticated WebLogic Server use. If you select
trunk_dom_repl_domain @=Environment ==Deployments B=Security Realms B=Interoperability B=Diagnostics	Overfigured user you must by each the WebGode Server user     Outgrand user you must by each the WebGode Server user     Outgrand user of the WebGode Server user     Outgrand to the WebGode Server user     Outgrand to the WebGode Server user     Outgrand to the WebGode Server user		
	Configured User Name WebLogic Server User Name:		
How do I	Back Next Finish Cancel		
Create outbound credential mappings			



- 11. Provide the below mentioned field values as given below.
  - i. EIS User Name: Client ID save in txt file generated from IDCS in section 3.5, step 6.
  - ii. EIS Password: Client Secret save in txt file generated from IDCS in section 3.5, step 6.
  - iii. EIS User Name: Client Secret save in txt file generated from IDCS section 3.5, step 6.

### Configure EIS UIS Username / Password

ORACLE WebLogic Server Adr	ministration Console 14.1.1			Q
Change Center	🏠 Home Log Out Preferences 🔝 Record Help	9	Welcome, weblogic	Connected to: trunk_dom_repl_domain
View changes and restarts	Home >Summary of Deployments >com.ofss.digx.connector >	Summary of Deployments >com.ofss.digc.connector >Summ	vary of Deployments >com.ofss.digx.connector >	Roles
No pending changes exist. Click the Release Configuration button to allow others to edit the domain.	Create a New Security Credential Mapping			
	Back Next Finish Cancel			
Lock & Edit Release Configuration	EIS User Name and Password Configure the EIS User Name and Password that you would like to map the WebLopic Server User to:			
Domain Structure	* Indicates required fields			
trunk_dom_repi_domain	Enter the EIS User Name:	6		
	* EIS User Name:	XXXXXXXXXXXXXXXXXXXXXX		
	Enter the EIS Password:	1		
	* EIS Password:			
	* Confirm Password::			
	Back Next Finish Cancel			
How do I				
Create outbound credential mappings				
System Status				
Health of Running Servers as of 6:39 AM				
Failed (0) Critical (0)				

12. Click on Finish to save the configuration.

# 3.8 **OBAPI configuration for OAuth**

To enable IDCS out of the box support for OAuth, execute the below query.

update DIGX\_FW\_CONFIG\_ALL\_B set prop\_value = <SSO\_PROVIDER\_URL> where prop\_id = 'SSO\_PROVIDER\_URL';

Replace <SSO\_PROVIDER\_URL> with respective SSO provider URL.

Restart all the managed servers.

For configuring any other service provider, a custom class needs to be written which implements com.ofss.digx.app.sms.service.user.external.IExternalUser interface.

The entry for the new custom class has to be made in database using the below script -

update DIGX\_FW\_CONFIG\_ALL\_B set prop\_value = <SSO\_PROVIDER\_CLASS> where prop\_id = 'SSO\_PROVIDER\_CLASS';

Replace <SSO\_PROVIDER\_CLASS> with the fully qualified name of the new custom class.

Also below queries need to be executed as well if there are any changes in the configuration-



update DIGX\_FW\_CONFIG\_ALL\_B set prop\_value = <SSO\_PROVIDER\_TOKEN\_SCOPE> where prop\_id = 'SSO\_PROVIDER\_TOKEN\_SCOPE';

update DIGX\_FW\_CONFIG\_ALL\_B set prop\_value = <SSO\_PROVIDER\_TOKEN\_URI> where prop\_id = 'SSO\_PROVIDER\_TOKEN\_URI';

update DIGX\_FW\_CONFIG\_ALL\_B set prop\_value = <SSO\_PROVIDER\_URL> where prop\_id = 'SSO\_PROVIDER\_URL';

update DIGX\_FW\_CONFIG\_ALL\_B set prop\_value = <SSO\_PROVIDER\_USER\_READ\_URI> where prop\_id = 'SSO\_PROVIDER\_USER\_READ\_URI';

Restart all the servers in domain.

# 3.9 **Default Admin Configuration**

OBAPI installer comes pre-shipped admin user with name "superadmin", so in order to login into the OBAPI application for completing Day 1 maintenances the same user need to be created in SSO Provider with same name post SSO integration.



# 3.10 Logout Configurations

Below query needs to be executed as part of the logout configurations.

Insert into DIGX\_FW\_CONFIG\_ALL\_B

(PROP\_ID,CATEGORY\_ID,PROP\_VALUE,FACTORY\_SHIPPED\_FLAG,PROP\_COMMENTS,S UMMARY\_TEXT,CREATED\_BY,CREATION\_DATE,LAST\_UPDATED\_BY,LAST\_UPDATED\_D ATE,OBJECT\_STATUS,OBJECT\_VERSION\_NUMBER,EDITABLE,CATEGORY\_DESCRIPTIO N)

values ('SSO\_LOGOUT\_URL','dayoneconfig','<LOGOUT\_URL>','Y',null,'SSO logout Url','ofssuser',sysdate,'ofssuser',sysdate,'A',1,'N',null);

Replace <LOGOUT\_URL> with respective url.

<u>Home</u>

