# Oracle® Banking APIs Single Sign-on Configuration-SAML



Patchset Release 22.2.4.0.0 F99666-01 June 2024

ORACLE

Oracle Banking APIs Single Sign-on Configuration-SAML, Patchset Release 22.2.4.0.0

F99666-01

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

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.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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 fail-safe, 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.

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

Intel and Intel Inside 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, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

# Contents

### Preface

Purpose	vi
Audience	vi
Documentation Accessibility	vi
Diversity and Inclusion	vi
Conventions	vii
Related Resources	vii
Screenshot Disclaimer	vii
Acronyms and Abbreviations	vii

### 1 Introduction

### 2 Configuration

2.1	Identity Provider Configuration at IDCS	2-1
2.2	SAML Authentication Provider configuration	2-5
2.3	SQL Authentication Provider configuration	2-9
2.4	OHS Configuration	2-13
2.5	Database Configuration	2-14
2.6	IDCS OAuth Integration	2-15
2.7	WebLogic configuration for OAuth	2-21
2.8	OBAPI configuration for OAuth	2-25
2.9	Default Admin Configuration	2-26
2.10	Logout Configurations	2-26

### 3 List of Topics

Index



### List of Figures

2-1	Dashboard	2-1
2-2	Add Application	2-2
2-3	Add SAML Application	2-2
2-4	Add SAML Application	2-3
2-5	Add SAML Application	2-3
2-6	Edit Application	2-4
2-7	Edit Application	2-4
2-8	Edit Application	2-5
2-9	Assign Users	2-5
2-10	Security Realms	2-6
2-11	Providers	2-6
2-12	Default Authenticator	2-6
2-13	Create Authentication Provider	2-7
2-14	Management	2-7
2-15	Create a SAML 2.0 Web Single Sign-on Identity Provider Partner	2-8
2-16	Settings for Create a SAML 2.0 Web Single Sign-on Identity Provider Partner	2-8
2-17	Servers	2-9
2-18	SAML 2.0 General	2-9
2-19	Security Realms	2-10
2-20	Providers	2-10
2-21	Create New Authentication Provider	2-11
2-22	Settings for Read Only SQL Authentication Provider	2-11
2-23	Settings for Read Only SQL Authentication Provider	2-12
2-24	Authentication	2-12
2-25	Reorder Authentication Providers	2-13
2-26	Dashboard	2-15
2-27	Add Application	2-16
2-28	Add Confidential Application	2-16
2-29	Add Confidential Application	2-17
2-30	Add Confidential Application	2-17
2-31	Add Confidential Application	2-18
2-32	Add App Role	2-18
2-33	Add Confidential Application	2-18
2-34	Add Confidential Application	2-19
2-35	Add Confidential Application	2-19
2-36	Add Confidential Application	2-19

2-37	Add Confidential Application	2-20
2-38	Edit Application	2-20
2-39	Edit Application	2-21
2-40	Deployments	2-21
2-41	Outbound Connection Pools Configuration	2-22
2-42	Outbound Connection Group Configuration	2-22
2-43	JNDI Configuration for Outbound Connection	2-22
2-44	Deployments	2-23
2-45	Outbound Credentials Mappings	2-23
2-46	Create New Security Credentials Mappings	2-24
2-47	Create New Security Credentials Mappings	2-24
2-48	Configure EIS UIS Username / Password	2-25

## Preface

- Purpose
- Audience
- Documentation Accessibility
- Diversity and Inclusion
- Conventions
- Related Resources
- Screenshot Disclaimer
- Acronyms and Abbreviations

### Purpose

This guide is designed to help acquaint you with the Oracle Banking APIs application. This guide provides answers to specific features and procedures that the user need to be aware of the module to function successfully.

### Audience

This document is intended for the following audience:

- Customers
- Partners

### **Documentation Accessibility**

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

#### Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

### **Diversity and Inclusion**

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and



the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

### Conventions

The following text conventions are used in this document:

Convention	Meaning		
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.		
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.		
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.		

## **Related Resources**

For more information on any related features, refer to the following documents:

Oracle Banking APIs Installation Manuals

### Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes.

# Acronyms and Abbreviations

The list of the acronyms and abbreviations used in this guide are as follows:

#### Table 1 Acronyms and Abbreviations

Abbreviation	Description	
OBAPI	Oracle Banking APIs	



# 1 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.



# 2 Configuration

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

- Identity Provider Configuration at IDCS
- SAML Authentication Provider configuration
- SQL Authentication Provider configuration
- OHS Configuration
- Database Configuration
- IDCS OAuth Integration
- WebLogic configuration for OAuth
- OBAPI configuration for OAuth
- Default Admin Configuration
- Logout Configurations

## 2.1 Identity Provider Configuration at IDCS

Steps to configure Identity Provide at IDCS

 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.

	lentity Cloud Service			
Users	🛶 🍰	Applications and Services	Groups	۵ 🗳
_		- 🖓	-	
Total	_	Total	Total	_
		Created Removed		
Passwords		Logins	All Reports	
_	9	- 8		
Resets		Total		
- Failed Attempts		- Failed Attempts		

#### Figure 2-1 Dashboard

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



🗆 Select All 🛛 🕂 Add	🗙 Remove	e 🛇 Activate 🖉 Deactivate				
$\sim$	Add Applio	cation		×		
	ß	App Catalog	Add an application from the Application Catalog.		0	Ξ
				-	0	Ξ
	>	SAML Application	Create an application that supports SAML for Single Sign On.			
		Mobile Application	Create a mobile/single-page application that uses OAuth 2.0. These applications cannot maintain the confidentiality of their client secret.		0	Ξ
	ø	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.		0	Ξ
	6	Enterprise Application	Create a web application that is protected by the App Gateway.		0	ъ

#### Figure 2-2 Add Application

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

#### Figure 2-3 Add SAML Application

#### Add SAML Application

Cancel		(2)	Next >
Details		SSO Configuration	
App Details			
* Name	OBDX_SAML_CONFIG		
Description	SAML Configuration for OBDX user authentication.		
Application Icon			
Application URL / Relay State	Upload Add Remove		

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

e.g. <protocol>://<OHS\_HOST>:<OHS\_PORT>/saml2/sp/acs/post

http://whf000xxx.bank.com:9999/saml2/sp/acs/post

- iii. NameID Format- Select value as "Unspecified".
- iv. NameID Value- Select value as "User Name".



Figure 2-4	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 appl	lication and to upload the application's sig	ning certificat	е.	
* Entity ID	OBDX_SAML			
* Assertion Consumer URL	http://example.com/saml2/sp/acs/post			
* NamelD Format	Unspecified 💌			
* NamelD Value	User Name 🔻			
Signing Certificate	Upload			

- b. Advance Settings
  - i. Signed SSO :- Select value as "Assertion"
  - ii. Enable Single Logout: This field should be checked.
  - iii. Logout Binding: Select value as "Redirect".
  - iv. 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

v. 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

Figure 2-5 Add SAML Application

Assertion 💌
SHA-256 💌
Redirect 💌
http://example.com:9999/digx-infra/ssc
http://example.com:9999

- Encrypt Assertion  $\square$
- 5. Click on Finish / Save.
- 6. Click on Activate button to activate your application.



Applications > OBDX_SAML_CONFIG		
OBDX_SAML_CO		Activate X Remove
Users Gr	oups	Save
Application Type	SAML Application	
* Name	OBDX_SAML_CONFIG	
Description	SAML Configuration for OBDX user authentication.	
Application Icon	$\sim$	

- 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.

Figure 2-7 Edit Application

Figure 2-6 Edit Application

OBDX_SAML_CONFIG SAML Configuration for OBDX user authentication				🛇 Activate	🗙 Remove
Details SSO Configuration Users Groups					
			Download Signing Certificate	Download Identity Provider	Metadata
▲ General Use this section to define the required SSO attributes for the appl	ication and to upload the application's sic	aning certificate			
* Entity ID					
* Assertion Consumer URL					
* NameID Format	Email address 🔹				
* NamelD Value	Primary Email				
Signing Certificate	Upload				

- 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.
- 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.



	OBDX_S									Ø Deactivate	🗙 Remove
Details	SSO Configuration	Users	Groups								
		0	C Select All	🕂 Assign	🗙 Revoke						
						Ŷ					
			Νοι	users a	re assig	gned t	o this	applic	ation.		
						Assign Users					

#### Figure 2-8 Edit Application

Figure 2-9 Assign Users

Select	t All					superadmi	n
						Selected: 1	Clear Selection
	First Name	Last Name	Email				
	Super	Admin					
<b>~</b>	superadmin	superadmin					

**12.** Logout from IDSC console.

# 2.2 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".

Figure 2-10	Security	Realms
-------------	----------	--------

ORACLE WebLogic Server			
Change Center	🔒 Home Log Out Preferences 🔤 Reco		Welcome, weblogic Connected to: trunk_dom_repl_doma
View changes and restarts	Home >Summary of Servers >Servers >Serve	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 WebL	ogic Server domain, but only one can be set as the default se	olicies, and security providers-that are used to protect WebLogic resources. You can have exurity realm, which is reserved for domain administrative purposes. domain, Click the name of the realm to explore and configure that realm.
Domain Structure	This occurry recurrs page into cach acc	and real national point configured in this research server i	domain click the name of the ream to explore and compare the ream.
runk_dom_repl_domain -Environment -Servers -Clusters	Customize this table Realms (Filtered - More Columns Exi		
Coherence Clusters Machines	Click the Lock & Edit button in the Char	nge Center to activate all the buttons on this page.	
	New Delete		Showing 1 to 1 of 1 Previous   Next
Concurrent Templates	🗆 Name 🗞	Default Realm	
Deployments	myrealm	true	
Services Security Realms	v Delete		Showing 1 to 1 of 1 Previous   Next
łow do I	•		
Configure new security realms			
Enable automatic realm restart			

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

Figure 2-11 Providers

Change Center	🔒 Home Log Ou	ut Preferences 🔤 Reco	rd Help		Q				Welcome, weblogic	Connected to: obdx_do
View changes and restarts	Home >Summary of	of Security Realms >myrealr	m >Providers							
Click the Lock & Edit button to modify, add or	Settings for myre	alm								
delete items in this domain.	Configuration L	Users and Groups Role	s and Policies	Credential Mappin	ngs Providers	Migratio	1			
Domain Structure	Authentication	Password Validation	Authorization	Adjudication	Role Mapping A	uditing	Credential Mappin	Certification Pat	1	
iÐ Servides ⇒Security Romas Ð Interoperability Ð ⊃Diegnostics	Authentication p Customize this Authentication	providers in a security real	Îm. Different type	es of Authenticatio	n providers are de					1 to 2 of 2 Previous   Nex
Security Realms Interoperability	Authentication p Customize this Authentication	roviders in a security real s table Providers	Îm. Different type	es of Authenticatio	n providers are de s on this page.				AP servers or DBMS.	
Security Realms Interoperability	Authentication p Customize this Authentication Click the Lock &	roviders in a security real s table Providers & <i>Edit</i> button in the Chang	Îm. Different type	es of Authentication	n providers are de s on this page.	esigned to a			AP servers or DBMS.	1 to 2 of 2 Previous   Nex
-Security Realms Pinteroperability - Diagnostics	Authentication p Customize this Authentication Click the Lock &	roviders in a security real s table Providers & Edit button in the Chang cator	Îm. Different type	es of Authentication	n providers are de s on this page.	esigned to a			AP servers or DBMS.	1 to 2 of 2 Previous   Nex Version
™Security Realms <sup>2</sup> Theroperability <sup>2</sup> Diagnostics	Authentication p Customize this Authentication Click the Lock & Name DefaultAuthentic	roviders in a security real s table Providers & Edit button in the Chang cator	Îm. Different type	es of Authentication	in providers are de is on this page.	esigned to a			AP servers or DBMS.	1 to 2 of 2 Previous   Nex Version 1.0

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

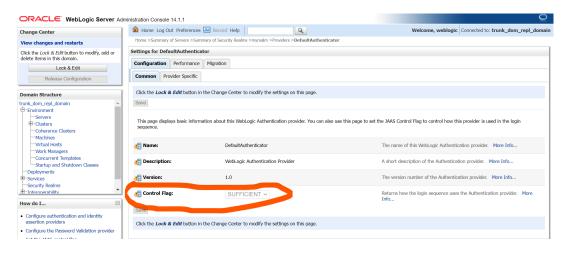


Figure 2-12 Default Authenticator



4. 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**.

- a. Name: Name of authentication provider.
- b. Type : Select value as "SAML2IdentityAsserter".

#### Figure 2-13 Create Authentication Provider

ORACLE WebLogic Server Adr	ministration Console 14.	1.1		Q
Change Center	Home Log Out P	references 📐 Record Help	Q	Welcome, weblogic Connected to: trunk_dom_repl_domain
View changes and restarts	Home >Summary of Se	rvers >Summary of Security Realm	ns >myrealm >Providers >DefaultAuthenticator >Su	mmary of Security Realms >myrealm >Providers
No pending changes exist. Click the Release Configuration button to allow others to edit the	Create a New Auther	tication Provider		
domain.	OK Cancel			
Lock & Edit	Create a new Aut	hentication Provider		
Release Configuration		rties will be used to identify your	r new Authentication Dravider	
Domain Structure	* Indicates required fi		Thew Addrendcadorr Provider.	
trunk_dom_repl_domain				
Environment     Servers	The name of the auth	entication provider.		
⊞-Clusters	* Name:	SAML OBDX CON	FIG	
Coherence Clusters				
Virtual Hosts	This is the type of au	thentication provider you wish to	o create.	
Concurrent Templates	Туре:	SAML2IdentityAsser	rter 🗸	
Services	OK Cancel			
Security Realms				
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\_OBDX\_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".

#### Figure 2-14 Management

ORACLE WebLogic Server Ad	ninistration 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 OBDX21ADMIN	Customize this table Identity Provider Partners	
Deployments     Services     Security Realms     Interoperability	New v Delete	Showing 0 to 0 of 0 Previous   Next
Diagnostics	There are no items to display	
	New Web Single Sign On Identity Provider Partner New Web Service Identity Provider Partner	Showing 0 to 0 of 0 Previous   Next
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.

Domain Structure	Use this page to:	
trunk_dom_repl_domain		new Single Sign on Identity Provider partner xation of the SAML 2.0 metadata file that you received from this new partner
Machines Virtual Hosts Work Managers Concurrent Templates	Please specify the name of the pa * Name:	rtner. WebSSO-IdP-Partner-0
Deployments     Services		e containing the partner metadata document.
Security Realms	Path:	/scratch/app/domain/trunk_dom_repl_domain/IDCSMetadata.xml
How do I	Recently Used Paths: Current Location:	/scratch/app/domain/trunk_dom_repl_domain 100.76.153.182 / scratch / app / domain / trunk_dom_repl_domain
Create a SAML 2.0 Web Single Sign-on Identity Provider partner     Configure authorization providers	bin common config init-info	
System Status	jms	
Health of Running Servers as of 9:09 AM	logs	
Failed (0)           Critical (0)           Overloaded (0)           Warning (0)           OK (2)	orchestration     original     servers     IDCSMetadata.xml	
UK (2)	OK Cancel	

#### Figure 2-15 Create a SAML 2.0 Web Single Sign-on Identity Provider Partner

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

# Figure 2-16 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 those interfaces, see Related	et on this Administration Console page can also be accessed programmatically via the Topics.	Java Interfaces that are identified in this help topic. For API Information about
Coherence Clusters	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
	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 realm. More Info
Create a SAML 2.0 Web Single Sign-on Identity Provider partner	Issuer URI:	https://idcs- 93e9366b4e3e4ce68a7c4dafb329cbdf.identity.c9dev2.oc9qadev.com:443/fed	The Issuer URI of this Identity Provider partner. More Info
<ul> <li>Configure authentication and identity assertion providers</li> </ul>		5365300046364060887040810325000.1061003.005480692.005480692011.4457160	
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-da	shboard	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)		æ	
	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.

#### Figure 2-17 Servers

In Home Log O	out Preferences 🔤 Record F	Help	Q		Welcome,	weblogic Conne	cted to: trunk_dom_repl_doma
Home >Providers	>SAML_OBDX_IT >IDCS_IT >Su	mmary of Security Realm	s >myrealm >Providers >S/	ML_OBDX_IT >Summary of Se	ervers >obdx_server1 >	Summary of Serve	rs
Summary of Serv	vers						
Configuration	Control						
This page summ	his table			-		Showi	ng 1 to 2 of 2 Previous   Next
□ Name 🖗	6	Туре	Cluster	Machine	State	Health	Listen Port
AdminSer	rver(admin)	Configured			RUNNING	🖋 ОК	9011
	rver1	Configured	obdx cluster	obdx machine	RUNNING	🖋 ок	19003
	Summary of Server Configuration A server is an in This page summ C2 Customize th Servers (Filte New Con Name @	Summary of Servers Configuration Control A server is an Instance of WebLogic Server th This page summarizes each server that has b C C Customize this table Servers (Filtered - More Columns Exist)	Summary of Servers Configuration Control A server is an instance of WebLopic Server that runs in its own Java This page summarizes each server that has been configured in the o Co Control Co Customize this table Servers (Filtered - More Columns Exist) New Come Delete Type	Hone >Photodes >SAML_OBDX_IT > DICS_IT >Summary of Security Realma >myrealm >Photodes >SA         Summary of Servers         Configuration         Configuration         Control         A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and This page summarizes each server that has been configured in the current WebLogic Server di Control         Customize this table         Servers (Filtered - More Columns Exist)         New       Cone         Delete         Name        Type	Home >Phonders >SAML_OBDX_IT >DDC3_IT >Summary of Security Realms >myrealm >Phonders >SAML_OBDX_IT >SUMMARY of Security Realms >myrealms >SUML_OBDX >SUMMARY of Security Realms >myrealms >SUML_OBDX >SUMMARY of Security Realms >myrealms >SUML_OBDX >SUMMARY of Security Realms >SUML_OBDX >SUMMARY of Security Realms >SUML_OBDX >SUMMARY of Security Security >SUMMARY of Se	None >Provides >SMIL_OBDX_IT >DCS_IT >Summary of Security Realms >myrealm >Provides >SMIL_OBDX_IT >Summary of Servers >obdserver1 >Provides >SMIL_OBDX_IT >SUMMARY of Servers >SMIL_OBDX_IT >SUMMARY of Server >SMIL_OBDX_IT >SMILE	None >Provides >SMPL_OBDX_IT > Docs_IT > Summary of Security Realms >myrealm >Provides >SMPL_OBDX_IT >Summary of Servers >odod_server1 >Summary of Servers         Summary of Servers         Configuration         Configuration         Configuration         Control         A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.         This page summarizes each server that has been configured in the current WebLogic Server domain.         Control         Customize this table         Servers (Filtered - More Columns Exist)         New       Configured         Show

- Navigate to "Federation Services" → "SAML 2.0 General" and provide values to below mentioned fields. Click on Save.
  - a. Published Site URL: Recommended URL format <OHS URL>/saml2 e.g. <PROTOCOL>://<OHS HOST>:<OHS PORT>/saml2

http://whf000xxx.bank.com:9999/saml2

- **b.** Entity Id: Value should match with Entity Id provided in SAML configuration in IDCS console.
- c. Recipient Check Enabled: unchecked.

#### Figure 2-18 SAML 2.0 General

organization orter		
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. Wore Info

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

# 2.3 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".

#### Figure 2-19 Security Realms

hange Center	🚹 Home Log Out Preferences 🔤 Record He	elp 🔍	Welcome, weblogic Connected to: trunk_dom_repl_dom
/iew changes and restarts	Home >Summary of Servers >Summary of Securit	ty Realms	
Click the Lock & Edit button to modify, add or lelete items in this domain.	Summary of Security Realms		
Lock & Edit Release Configuration	multiple active security realms in a WebLogic Se	erver domain, but only one can be set as the default secur	es, and security providers—that are used to protect WebLogic resources. You can have ity realm, which is reserved for domain administrative purposes. vain. Click the name of the realm to explore and configure that realm.
omain Structure	, , ,	,	, ,
unk_dom_repl_domain  -Environment -Servers -Clusters	Customize this table Realms (Filtered - More Columns Exist)		
Coherence Clusters	Click the Lock & Edit button in the Change Cer	nter 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 Startup and Shutdown Classes	🗆 Name 🗞	Default Realm	
Deployments	myrealm	true	
Security Realms	New Delete		Showing 1 to 1 of 1 Previous   Next

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

Figure 2-20 Providers

	dministration Console 1	4.1.1									Q
Change Center	Home Log Out	Preferences 🔤 Recor	d Help		Q				Welcome, weblogic	Connected to: obdx,	_doma
View changes and restarts	Home >Summary of	Home >Summary of Security Realms >myrealm >Providers									
Click the Lock & Edit button to modify, add or delete items in this domain.	Settings for myrea	ilm									
delete items in this domain.	Configuration U	sers and Groups Roles	and Policies	Credential Map	pings Provide	rs Migrat	tion				
Domain Structure obdx_domain	Authentication	Password Validation	Authorization	Adjudication	Role Mapping	Auditing	Credential Mapping	Certification Path			
Deployments     Posrvices     Posrvices     Posrvices     Posrvices     Posrvices     Posrvices     Posrvices	Authentication pr		m. Different typ	es of Authentica	tion providers are				iP servers or DBMS.	onfigure multiple 1 to 2 of 2 Previous	Next
	Name			Descrip	ition					Version	
How do I	DefaultAuthentica	ator		WebLog	ic Authentication	Provider				1.0	
Configure authentication and identity	DefaultIdentityAs	serter		WebLog	ic Identity Asserti	on provider				1.0	
assertion providers									Showing	1 to 2 of 2 Previous	Next
Configure the Password Validation provider											
Manage security providers											
<ul> <li>Cot the 1MAC control floor</li> </ul>											

3. Click on New button to create new Authentication Provider.

Fill the below mentioned fields with appropriate values and click on **OK**.

- a. Name: Name of authentication provider.
- b. Type :Select value as "ReadOnlySQLAuthenticator".

		Preferences 🔤 Record Help	Welcome, weblogic Connected to: test221 domain
Change Center	-		
View changes and restarts	Home >Summary of !	ervers >obdx_server1 >Summary of Servers >Summary of Security Realms >myrealm >Prov	iders >SQLAuth >Summary of Security Realms >myrealm >Providers
No pending changes exist. Click the Release	Create a New Auth	entication Provider	
Configuration button to allow others to edit th domain.	OK Cancel		
Lock & Edit	Carloer		
Release Configuration	Create a new Au	thentication Provider	
Release Comiguration	The following prop	erties will be used to identify your new Authentication Provider.	
Domain Structure	* Indicates required	ields	
test221_domain			
Environment     Servers	The name of the au	hentication provider.	
Servers     Clusters	* Name:	2014	
Coherence Clusters	Hume.	SQLAuth	
Machines Virtual Hosts	This is the type of a	thentication provider you wish to create.	
Work Managers	This is the type of the	anendadon provide you wan to create.	
Concurrent Templates	Type:	ReadOnlySQLAuthenticator ~	
Startup and Shutdown Classes			
Services	OK Cancel		
■-Messaging			
Data Sources			
How do I	=		
Manage security providers			
<ul> <li>Configure authentication and identity assertion providers</li> </ul>			

#### Figure 2-21 Create New Authentication Provider

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

#### Figure 2-22 Settings for Read Only SQL Authentication Provider

delete items in this domain.	Configuration Performan	Rc .	
Domain Structure		n in the Change Center to modify the settings on this page.	
test221_domain B-Environment	<ul> <li>Save</li> </ul>		
	This page displays basic inf sequence.	ormation about this Read-only SQL Authentication provider. You c	an also use this page to set the JMAS Control Flag to control how this provider is used in the login
Virtual Hosts	街 Name:	SQLAuth	The name of this Read-Only SQL Authentication provider. More Info
Concurrent Templates Startup and Shutdown Classes Deployments	description:	Provider that performs DBMS authentication	A short description of this Read-Only SQL Authentication provider. More Info
-Services -Security Realms -Interoperability	Version:	1.0	The version number of this Read-Only SQL Authentication provider. More Info
How do I	E 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		
<ul> <li>Set the JAAS control flag</li> </ul>	Click the Lock & Edit butto	n 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.
  - a. Data Source Name: NONXA
  - b. SQL Get Users Password: SELECT U\_PASSWORD FROM USERS WHERE U\_NAME = ?
  - c. SQL User Exists: SELECT U\_NAME FROM USERS WHERE U\_NAME = ?
  - d. SQL List Users: SELECT U\_NAME FROM USERS WHERE U\_NAME LIKE ?
  - e. SQL List Groups: SELECT G\_NAME FROM GROUPS WHERE G\_NAME LIKE ?
  - f. VI. SQL Group Exists: SELECT G\_NAME FROM GROUPS WHERE G\_NAME = ?
  - g. SQL Is Member: SELECT G\_MEMBER FROM GROUPMEMBERS WHERE G\_NAME = ? AND G\_MEMBER = ?
  - h. SQL List Member Groups: SELECT G\_NAME FROM GROUPMEMBERS WHERE G\_MEMBER = ?

- i. SQL Get User Description: SELECT U\_DESCRIPTION FROM USERS WHERE U\_NAME = ?
- j. SQL Get Group Description: SELECT G\_DESCRIPTION FROM GROUPS WHERE G\_NAME = ?

eployments iervices iecurity Realms	Data Source Name:	NONXA	The data source used by this Read-Only SQL Authentication provider. More Info
nterenershillty ·	Group Membership Searching:	unlimited ~	Specifies whether recursive group membership searching is unlimited or limited. Valid values are unlimited andlimited. More Info
	Max Group Membership Search Level:	0	This specifies how many levels of group membership can be searched. This setting is valid only If 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. Mere Info.
th 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
Falled (0) Critical (0) Overloaded (0) Warning (0)	SQL User Exists:	SELECT U_NAME FROM L	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 at 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 Info
	SQL List Groups:	SELECT G_NAME FROM (	The SQL statement used to retrieve group names that match a wildcard The SQL statement requires a single parameter for the wildcarded group name and return a resultSet containing matching group names More Info
5	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 containing at most a single record containing the group More Info
5	SQL Is Member:	SELECT G_MEMBER FRO	The SQL statement used to look up members of a group. The SQL statemen 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
2	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 grou 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 database used by the authentication provider. More Info
5	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 at most a single record containing the user description. More Info
5	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 resultSet containing at mo a single record containing the group description. More Info
	Save		
	Click the Lock & Edit button in the Change Center to	modify the settings on this page.	

Figure 2-23 Settings for Read Only SQL Authentication Provider

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

Figure 2-24 Authentication

domain.	Configuration	Users and Groups	Roles and Policies	Credential Map	ings Provide	rs Migrat	lon			
Lock & Edit	Authenticat	ion Password Validati	on Authorization	Adjudication	Role Mapping	Auditing	Credential Mapping	Certification Path		
Release Configuration										
omain Structure		ation provider allows W							ealm, and you can configure n servers or DBMS	ultiple
st221_domain	*	in providence in a coccarry			ion promotio are	accigned e		0001000 000011 00 2011		
Servers	Customize	this table								
⊕-Clusters		_								
Coherence Clusters	Authenticat	tion Providers								
Machines	New De	lete Reorder								
Virtual Hosts	INGW DO	Redider							Showing 1 to 4 of 4	Previous   Ne
Work Managers Concurrent Templates	Name		Description							Version
Startup and Shutdown Classes	SAML_	TEST	SAML 2.0 Iden	itity Assertion Pro	vider. Supports S	ecurity Asse	rtion Markup Language	≥ v2.0.		1.0
Services	SQLAut	h	Provider that p	performs DBMS a	thentication					1.0
Security Realms	Default	Authenticator	WebLogic Auth	entication Provid	er					1.0
ow do I	Default	IdentityAsserter	WebLogic Ider	ntity Assertion pro	vider					1.0
Configure authentication and identity assertion providers		Reorder							Showing 1 to 4 of 4	Previous   Ne
Configure the Password Validation provider										
	1									
Manage security providers										

9. Reorder the authentication providers as given below.



- a. SAML Authentication Provider
- b. SQL Authentication Provider
- c. Default Authenticator

#### Figure 2-25 Reorder Authentication Providers

view changes and restarts		
No pending changes exist. Click the Release Configuration button to allow others to edit the	Reorder Authentication Providers	
domain.	OK Cancel	
Lock & Edit	Reorder Authentication Providers	
Release Configuration		oviders using the list below. By reordering Authentication Providers, you can alter the authentication sequence.
Domain Structure		e arrows to move them up and down in the list.
test221_domain		
Entroment     Seners     Seners     Custers    Coherence Clusters    Machines    Machines    Wark Managers    Oronument Templates    Startup and Mutdown Classes    Deployments     Services	Image: Contract of the second seco	Σ Ξ
Security Realms     How do I	OK Cancel	
Re-order authentication providers		

**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

### 2.4 OHS Configuration

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

- 1. Open obdx.conf file from OHS server. You can find the location of obdx.conf file from httpd.conf file.
- Verify if proxypass URLs are configured in obdx.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(.*)" "http://wL_HOST_NAME>:<WL_PORT>/saml2$1"
ProxyPassReverse "/digx(.*)" "http://wL_HOST_NAME.com:19003/digx$1"
ProxyPassReverse "/saml2(.*)" "http://wL_HOST_NAME.com:19001/saml2$1"
```

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

```
"${DocumentRoot}">
        Options FollowSymLinks
        AllowOverride all
        </Directory></VirtualHost> Listen <PORT 2><VirtualHost
          *:<PORT 2>>
        ServerName <HOST NAME>
        RewriteEngine On
          RewriteRule
                         "^(.*)/config\.js$"
          "<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.
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>
              rnost ', 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 obdx.conf file and restart ohs server.

### 2.5 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 OBDX. 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 10:05:56.00000000 AM', 'DD-MM-RR fmHH12:fmMI:SSXFF AM'), 'A', 1, 'N', null);

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 10:05:56.00000000 AM', 'DD-MM-RR fmHH12:fmMI:SSXFF AM'), 'A', 1, 'N', null);

### 2.6 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.

 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.

	oud Service				
Users	🛶 🏄	Applications and	Services 📑	Groups	🍲 🎂
— Total	Ň	 Total		Total	<b></b> ,
		- Created	- Removed		
Passwords		Logins		All Reports	
-	Ŷ	-	Я		
 Resets	Ŷ	— Total	8		

Figure 2-26 Dashboard

2. In popup window select Confidential Application.



	C Identity Cloud Sonico	License Type :: F	oundation ?	SD
Applicatic	Add Application		× cription, or 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.	•	Ξ
	Mobile Application	Create a mobile/single-page application that uses OAuth 2.0. These applications cannot maintain the confidentiality of their client secret.	•	Ш
	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.	•	Ш
	Enterprise Application	Create a web application that is protected by the App Gateway.	0	Т

Figure 2-27 Add Application

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

#### Figure 2-28 Add Confidential Application

### Add Confidential Application

Cancel	1 Details	2 Client	Resources	(4) (Web Tier Policy	5 Authorization	Next >
App Details						
	* Nam	OBDX_OAUTH	_CONFIG			
	Descriptic	OAuth Configu details from ID	uration for fetching user DCS			
				4		
	Application Icc		)			
		Upload				

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



Add Confid	ential Applic	cation					
< Back	<ul> <li>—</li> </ul>	2	3		5		Next >
	Details	Client	Resources	Web Tier Policy	Authorization		
Authorization		Resource Owner 🗌 Clien Device Code	t Credentials 🗆 JWT	Assertion SAML2 Ass	ertion 🗆 Refresh Token 🗌	] Authorization Code 🗌 Impl	icit
		TLS Client Authentication					
	Allow non-HTTPS URLs						
	Redirect URL						
	Logout URL						
Po	st Logout Redirect URL						
	Security 🗆 Tr	usted Client Certificate	Import				

#### Figure 2-29 Add Confidential Application

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

### Figure 2-30 Add Confidential Application

< Back	2			5		Next >
Details	Client	Resources	Web Tier Policy	Authorization		
• Configure this application as a client now C Authorization	) Skip for later					
Allowed Grant Type	<sup>S</sup> 🗆 Resource Owner 🗹 Clier	nt Credentials 🗹 🛛 JW	T Assertion 🗆 SAML2 Asse	ertion 🗌 Refresh Token 🗌	Authorization Code 🗌 Implic	it
	Device Code					
	TLS Client Authentication					
Allow non-HTTPS URL	s 🗆					
Redirect UR	L					
Logout UR	L					
Post Logout Redirect UR	L					
Securit	y  Trusted Client Certificate	Import				
Allowed Operation	<sup>s</sup> 🗌 Introspect 🗌 On behalf	Of				
ID Token Encryption Algorithm	None	•				

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



Resources	<ul> <li>Tagged</li> <li>Specific</li> </ul>			
Resources				
+ Add Scope				
Resource		Protected	Scope	
No data to di	splay.			
Grant the clier	it access to Identity Clou	ud Service Admin APIs		
ant the clier	t access to Identity Clou	ud Service Admin APIs		

#### Figure 2-31 Add Confidential Application

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

Figure 2-32 Add App Role

Token Iss	uance Policy		Add App Role			×
	Authorized Resources	<ul><li>All</li><li>Tagged</li><li>Specific</li></ul>	Select All	identity ×	٩	
	Resources			Selected: 1	Clear Selection	
	+ Add Scope		Identity D	omain Administrator		
	Resource					
	No data to disp	olay.				
	Grant the client	access to Identity	,			
	+ Add				-	
	App Roles		Page 1 of 1 (1 o	f 1 items) $\kappa \ll 1 \rightarrow \varkappa$		
	No data to disp	olay.				dd

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

Figure 2-33 Add Confidential Application

Token Iss	uance Policy	0			
		<ul> <li>All</li> <li>Tagged</li> <li>Specific</li> </ul>			
	+ Add Scope				
	Resource		Protected	Scope	
	No data to displ	ay.			
	Grant the client a	access to Identity Cloud Service	Admin APIs		
	+ Add				
7	App Roles			Protected	
	Identity Domain	n Administrator		No	×



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

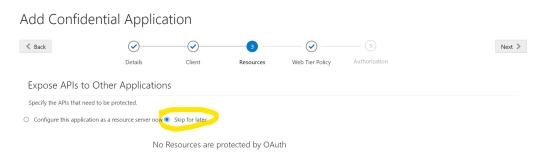
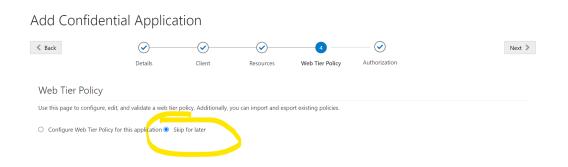


Figure 2-34 Add Confidential Application

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



e. Click on "Finish".

#### Figure 2-36 Add Confidential Application

Figure 2-35 Add Confidential Application

Add Confiden	tial 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".



	License Type :: Foundation ? Cookie Preferences	SD
Applications > OBDX_OAUTH_CONFIG		
OBDX_OAUTH_CONFIG OAuth Configuration for fetching users Application Added ×	Activate	🗙 Remove
Details     Configuration     Web Tier Policy     Us     Below is the new Client ID and Client Secret for your application.       This information also appears on the Configuration tab in the Details section for the application.     This information also appears on the Configuration tab in the Details section for the application.       App Details     Client ID		Save
Application Type Conf Client Secret Client Secret Close * Name OBE Description OAdur consignation for retrining user details from IDCS		
Application Icon		

Figure 2-37 Add Confidential Application

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

Figure 2-38 Edit App	olication	
Applications > OBDX_OAUTH_CONFIG		
OBDX_OAUTH		Activate X Remove
Details Configuration Web Tier Policy App Details	Users Groups	Generate Access Token Save
* Name	Confidential 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.



Applications > OBDX_OAUTH_CONFIG		
OBDX_OAUTH		🛇 Activate 🛛 🗙 Remove
Details Configuration Web Tier Policy App Details	Confirmation Are you sure that you want to activate the application OBDX_OAUTH_CONFIG?	X Generate Access Token Save
	COBDX_OAUTH_CONFIG OAuth Configuration for fetching user details from IDCS	ok
Application Icon	$\sim$	

#### Figure 2-39 Edit Application

9. Logout from IDCS console.

# 2.7 WebLogic configuration for OAuth

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

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

delete items in this domain. Lock & Edit		Confi	guration Control	Monitoring							
Release Configuration		This	page displays the list o	of Java EE app	lications and standalone	application modules installed	d to this domain.				
Domain Structure		You can update (redeploy) or delete installed applications and modules from the domain by selecting the checkbox next to the application name and then using the controls on this page.									
est221_domain Environment Deployments	To install a new application or module for deployment to targets in this domain, click <b>Install</b> .										
Services Security Realms											
Interoperability     Diagnostics		Depl	oyments								
- Digrouto		Inst	tall Update Delet	le						Showing 1 to 24	of 24 Previous   Nex
			Name 🕎				State	Health	Туре	Targets	Deployment Order
			orm.ofss.digx.con	nector			Active	🖋 ок	Resource Adapter	obdx_server1	0
			🗉 🦲 digx-admin				Active	🖋 ок	Web Application	obdx_cluster	100
łow do I 🗉			🗉 🐻 digx-auth				Active	🖋 ок	Web Application	obdx_cluster	100
Install an enterprise application     Configure an enterprise application			🗄 👩 digx-cms				Active	🖋 ок	Web Application	obdx_server1	100
Update (redeploy) an enterprise application			E odigx-coherence				Active	🛩 ок	Web Application	obdx_cluster	0
<ul> <li>Monitor the modules of an enterprise application</li> </ul>			E 👩 digx-common				Active	🖋 ок	Web Application	obdx_server1	100
Deploy EJB modules     Install a Web application		0	E adigx-corporatel	oan			Active	🖋 ок	Web Application	obdx_server1	100
<ul> <li>moran a web appread01</li> </ul>			E odigx-creditfacili	ty			Active	🖋 ок	Web Application	obdx_server1	100
ystem Status		0	E adigx-edx				Active	🖋 ок	Web Application	obdx_server1	100
Health of Running Servers as of 6:22 AM Failed (0)			E adigx-eurekasen	/er			Active	🛩 ок	Web Application	obdx server1	100

Figure 2-40 Deployments

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

Change Center	🙆 Home Log Out Preference	is 🔤 Record Help	Q			Welcome, weblog	gic Connected to: trunk_dom_repl_d		
View changes and restarts	Home >Summary of Deployment	s >com.ofss.digx.connector							
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 Security Targets	Control T	esting Monitoring	Notes				
Lock & Edit	General Properties Out	ound Connection Pools Admin Ob	ects Workload	I Instrumentatio	n				
Release Configuration									
omain Structure unk_dom_repl_domain	listed by connection factory i	outbound connection pool groups and in Iterface and the instances are listed by t the name of a group or instance to confi	neir JNDI names	. Expand a group to	obtain configurat	ion information for a connec	tion pool instance within an outbound		
Deployments	Outbound Connection Poo	Configuration Table							
B-Services Security Realms	New Delete		Showing 1 to 1 of 1 Previous   N						
<ul> <li>Interoperability</li> <li>Diagnostics</li> </ul>	Groups and Instances 🖘 Connection Factory Int								
	javax.resource.cci.C	onnectionFactory		ţ	avax.resource.ccl.0	ConnectionFactory			
	New Delete						Showing 1 to 1 of 1 Previous   N		
low do I 🖂									
Configure outbound connection pool     properties									
System Status									
Health of Running Servers as of 6:26 AM									
=									

Figure 2-41 Outbound Connection Pools Configuration

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

Figure 2-42 Outbound Connection Group Configuration

Change Center	🙆 Home Log Out Preferences 🔤 Record Help	Welcome, weblogic Connected to: trunk_dom_repl_domain
View changes and restarts	Home >Summary of Deployments >com.ofss.digx.connector	
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           Eack         Next         Finish         Cancel           Outbound Connection Group         In which outbound connection group do you want to create an instance?	
Domain Structure	Outbound Connection Groups	
trunk_dom_repLdoman ⊕=Environment ⊨⊃eployments ⊕=Services ⊨=Security Realms ⊨=Intercopresality ⊕=Diagnostics	Outbound Connection Group @           prex_resource.cd.ConnectionFactory           Back         Next           Finish         Cancel	Showing 1 to 1 of 1 Previous   Next 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**.

### Figure 2-43 JNDI Configuration for Outbound Connection

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.connector >	Summary of Deployments >com.ofss.digx.connector	
No pending changes exist. Click the Release	Create a New Outbound Connection		
Configuration button to allow others to edit the domain.	Back Next Finish Cancel		
Lock & Edit			
Release Configuration	JNDI name for Outbound Connection Instance		
	Enter the JNDI name that you want to use to obtain the * Indicates required fields	new connection instance	
Domain Structure trunk_dom_repl_domain	- Indicates required news		
Environment	The Outbound Connection instance represents a connection	on pool. The JNDI name can be used to obtain the pool at runtime.	
Deployments     Services	4 * JNDI Name:		
Security Realms	age - SNDI Name:	ra/DIGXConnectorSSOKEY	
Interoperability     Diagnostics	Back Next Finish Cancel		
- Originated			



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

delete items in this domain. Lock & Edit	Co	nfiguration Control	Monitoring					
Release Configuration	т	his name displays the list (	of Java EE applications and standalone application	modules installed to this dom	main.			
Domain Structure		This page usplays the list of page 22 applications and isolations and modules from the domain by selecting the checkbox next to the application name and then using the controls on this page.						
est221_domain			n or module for deployment to targets in this doma					o orrono poger
Services     Services     Services     Services     Services     Thereperability		Customize this table						
		ployments nstall Update Dele	te				Showing 1 to 24	of 24 Previous   Ne
	(	Name 🐟		Sta	ate He	alth Type	Targets	Deployment Order
		) 👼 com.ofss.digx.com	nector	Act	tive 🖋 (	K Resource Adapter	obdx_server1	0
	0	) 🗄 🦲 digx-admin		Act	tive 🗸	OK Web Application	obdx_cluster	100
How do I	C	) 🗄 🥫 digx-auth		Act	tive 🖌	OK Web Application	obdx_cluster	100
Install an enterprise application	C	] 🗄 🥫 digx-cms		Act	tive 🖌	OK Web Application	obdx_server1	100
Configure an enterprise application     Update (redeploy) an enterprise application	C	) 🗄 🐻 digx-coherence	9	Act	tive 🖌	OK Web Application	obdx_cluster	0
Monitor the modules of an enterprise     application	C	) 🗄 🐻 digx-common		Act	tive 🖋	OK Web Application	obdx_server1	100
Deploy EJB modules	C	) 🗄 🐻 digx-corporatel	loan	Act	tive 🖌	OK Web Application	obdx_server1	100
Install a Web application	C	) 🗄 🐻 digx-creditfacili	ity	Act	tive 🖌	OK Web Application	obdx_server1	100
System Status	C			Act	tive 🖌	OK Web Application	obdx server1	100
Health of Running Servers as of 6:22 AM								

Figure 2-44 Deployments

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

#### Figure 2-45 Outbound Credentials Mappings

Change Center	🔒 Home Log Out Preferences 🔤 Record Help	Q	Welcome, weblogic Connected to: trunk_dom	n_repl_domain		
View changes and restarts	Home >Summary of Deployments >com.ofss.digx.conner	tor >Summary of Deployments >com.ofss.di	digx.connector >Summary of Deployments >com.ofss.digx.connector >Roles			
No preding danges edd. Click the Release Configuration button to allow others to edit the domain. Lock & Edit Release Configuration Domain Structure Uruni, donrepLomain Previorments	Settings for com.ofss.digx.connector           Overview         Deployment Plan         Configuration         Security         Targets         Control         Testing         Monitoring         Notes           Roles         Publicies         Outbound Credential Mappings         Inbound Principal Mappings         Principals           Outbound credential mappings let you map         WebLogic Server usernames to usernames in the Enterprise Information System (EIS) to which you want to connect using a resource adapter. You can use default uctuational correction pools in the resource adapter, or specify particular outbound credential mappings for individual connection pools. This page contains the table of outbound credential mappings for this resource adapter.					
Services     Security Realms     Interoperability	Vuscomize this table Outbound Credential Mappings					
■-Diagnostics	Delete Showing 0 to 0 of 0 Previo					
	🗌 WLS User 🗠	EIS User	Outbound Connection Pool			
		There are	re no items to display			
	New Delete		Showing 0 to 0 of 0 Pre	vious   Next		
How do I 😑						
Create outbound credential mappings						
<ul> <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	Q	Welcome, weblogic	Connected to: trunk_dom_repl_domain	
View changes and restarts	Ι.	Home >Summary of Deployments >com.ofss.digx.conne Messages	ctor >Summary of Deployments >com.c	fss.digx.connector >Summary of Deployments >com.ofss.digx.connector	>Roles	
No pending changes exist. Click the Release Configuration button to allow others to edit the domain.		Selecting a pool is required.				
Lock & Edit Release Configuration	1	Create a New Security Credential Mapping           Back         Next.         Finish         Cancel				
Domain Structure	1	Outbound Connection Pool				
trunk_dom_repl_domain  -Environment -Deployments		Which Outbound Connection Pool would you like the Pools in this resource adapter. Each Outbound Connection		th? Selecting Resource Adapter Default will configure the credentia iselves to override these credentials.	I mapping for all Outbound Connection	
Services     Security Realms		Customize this table				
Interoperability     Diagnostics		Create a New Security Credential Map Entry f	or:		Showing 21 to 26 of 26 Previous Next	
		Outbound Connection Pool 🚕				
		ra/DIGXConnectorOBSCF				
		ra/DIGXConnectorOBTFPM_14.3				
		ra/DIGXConnectorOBVAM				
How do I	1 /	ra/DIGXConnectorREWARDS				
Create outbound credential mappings	٦N	ra/DIGXConnectorSSOKEY     Resource Adapter Default				
System Status	1				Showing 21 to 26 of 26 Previous   Next	
Health of Running Servers as of 6:37 AM		Back Next Finish Cancel				
Called (0)						

#### Figure 2-46 Create New Security Credentials Mappings

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

Figure 2-47 Create New Security Credentials Mappings

Change Center	🔟 Home Log Out. Preferences 🗠 Record. Help
View changes and restarts	Home >Summary of Deployments >com.ofss.digr.connector >Summary of Deployments >com.ofs
No pending drange exist. Click the Release Configuration button to allow others to edit the domain. Lock & Edit Release Configuration Domain Structure Uruk, donrepi.domain # Enknorments - Socurty Realms # Interopenshilly - Socury Realms	Create a New Security Credential Mapping
	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.
  - a. EIS User Name: Client ID save in txt file generated from IDCS in section 3.5, step 6.
  - EIS Password: Client Secret save in txt file generated from IDCS in section 3.5, step 6.
  - c. EIS User Name: Client Secret save in txt file generated from IDCS section 3.5, step 6.



ORACLE WebLogic Server Adr	ministration Console 14.1.1		Q			
Change Center	🏠 Home Log Out Preferences 🔤 Record Help	٩	Welcome, weblogic Connected to: trunk_dom_repl_domai			
View changes and restarts	Home >Summary of Deployments >com.ofss.digx.connector >	Summary of Deployments Scom.ofss.digx.connector Summary	of Deployments >com.ofss.digx.connector >Roles			
No pending changes exist. Click the Release Configuration button to allow others to edit the domain. Lock & Edit Release Configuration	Create a New Security Credential Mapping           Back         Next         Finish         Cancel           EIS User Name and Password         Cancel         Cancel         Cancel					
Holdase conliguration	Configure the EIS User Name and Password that you would like to map the WebLogic Server User to:					
Domain Structure	* Indicates required fields					
tunk_dom_yepi_domain H=Environment H=Deployments H=Services H=	Enter the EIS User Name: *EIS User Name:	xxxxxxxxxxxxxxx				
	Enter the EIS Password: * EIS Password:					
	* Confirm Password::					
How do I	Back Next Finish Cancel					
Create outbound credential mappings						
System Status						
Health of Running Servers as of 6:39 AM						
Failed (0)						

#### Figure 2-48 Configure EIS UIS Username / Password

12. Click on **Finish** to save the configuration.

## 2.8 OBAPI configuration for OAuth

To enable IDCS out of the box support for OAuth follow below mentioned steps.

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

- 1. Replace <SSO\_PROVIDER\_URL> with respective SSO provider URL.
- 2. 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';
```

5. Restart all the servers in domain.

# 2.9 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.

## 2.10 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,SUMMARY_TEXT,CREATED_BY,CREATION_DATE,
LAST_UPDATED_BY,LAST_UPDATED_DATE,OBJECT_STATUS,OBJECT_VERSION_NUMBER,
EDITABLE,CATEGORY_DESCRIPTION)
```

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.



# 3 List of Topics

This user manual is organized as follows:

### Table 3-1 List of Topics

Topics	Description
Preface	This topic provides information on the introduction, intended audience, list of topics, and acronyms covered in this guide.
Introduction	This topic explains step-by-step details on configuration required at IDCS side (Application and User) and WebLogic console configurations for SAML and SQL Authentication Providers.
Configuration	This topic explains steps to enable SAML authentication which involves configuration at WebLogic server (console) and IDCS console.



# Index

### С

Configuration, 2-1

### D

Database Configuration, 2-14 Default Admin Configuration, 2-26

l

IDCS OAuth Integration, 2-15 Identity Provider Configuration at IDCS, 2-1

### L

Logout Configurations, 2-26

### 0

OBAPI configuration for OAuth, 2-25 OHS Configuration, 2-13

### S

SAML Authentication Provider configuration, 2-5 SQL Authentication Provider configuration, 2-9

### W

WebLogic configuration for OAuth, 2-21

