Oracle® Banking APIs Single Sign-on Configuration-SAML



Patchset Release 22.2.5.0.0 G15768-01 October 2024

ORACLE

Oracle Banking APIs Single Sign-on Configuration-SAML, Patchset Release 22.2.5.0.0

G15768-01

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
Critical Patches	vi
Diversity and Inclusion	vii
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
- Critical Patches
- 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.

Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at Critical Patches, Security Alerts and

Bulletins. All critical patches should be applied in a timely manner to ensure effective security, as strongly recommended by Oracle Software Security Assurance.

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 1Acronyms 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.

	ty Cloud Service				
Users	🎰 🍰	Applications and Services		Groups	🍲 🍲
-		-		_	
Total		Total		Total	
		 Created Removed			
Passwords		Logins		All Reports	
-	Ŷ	-	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	н

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		

- 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	e.	
* 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_C	🛛 Activate 🗙 Remove	
Details SSO Configuration Users G App Details	Save	
Application Type	SAML Application	
* Name	OBDX_SAML_CONFIG	
Description	SAML Configuration for OBDX user authentication.	<i>6</i>
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	3			Activate	X Remove
Details SSO Configuration Users Groups			under difference contiference	Developed Identity Developer	Matadat
		Do	ownload Signing Certificate	Download Identity Provider	Metadata
⊿ General					
Use this section to define the required SSO attributes for the appli	cation and to upload the application's signir	ig certificate.			
* Entity ID					
* Assertion Consumer URL					
* NameID Format	Email address 🔹				
* NameID 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_SAML Configuration	SAML on for OBD	CONF X user authentica	IG ition.						Ø Deactivate	🗙 Remove
Details	SSO Configuration	Users	Groups								
		٩	C Select All	🕂 Assign	🗙 Revoke						
							.1.*				
			Νοι	isers 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 Selecti	ion
	First Name	Last Name	Email					
	Super	Admin						
~	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".

ORACLE WebLogic Server Admir	histration Console 14.1.1			õ								
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.	Jummary of Security Realms											
Lock & Edit Release Configuration	A security realm is a container for the mechanisms-including users, groups, security roles, security policles, and security providers-that are used to protect WebLogic resources. You can have multiple active security realms in a WebLogic Server domain, but only one can be set as the default security realm, which is reserved for domain administrative purposes. This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.											
Domain Structure				-								
trunk_dom_repl_domain	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								
Concurrent Templates	🗌 Name 🗞	Default Realm	1									
	myrealm	true										
Bissevices Security Realms	New Delete			Showing 1 to 1 of 1 Previous Next								
How do I												
Configure new security realms												

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

Figure 2-11 Providers

	dministration Console	14.1.1									
Change Center	🔒 Home Log Ou	t Preferences 🔤 Record	d Help		Q				Welcome, weblogic	Connected to: obdx_do	
View changes and restarts	Home >Summary of	f Security Realms >myrealm	>Providers								
Click the Lock & Edit button to modify, add or	Settings for myre	Settings for myrealm									
delete items in this domain.	Configuration U	Jsers and Groups Roles	and Policies C	redential Map	pings Provide	s Migrat	ion				
Domain Structure	Authentication	Password Validation	Authorization	Adjudication	Role Mapping	Auditing	Credential Mapping	Certification Path			
⊕ Environment — Deployments ⊕ Sanites ⊕ Sanites ⊕ Interoperability ⊕ Deprostics	An Authentication Authentication p Customize this Authentication Click the Lock &	n provider allows WebLog :oviders in a security realn : table Providers <i>Edit</i> button in the Chang	iic Server to establ m. Different types e Center to activa	lish trust by va of Authentica te all the butte	alidating a user. Yi tion providers are ons on this page.	ou must hav	ve one Authentication p o access different data	orovider in a securit stores, such as LD/	y realm, and you can c IP servers or DBMS. Showing	onfigure multiple	
	Name			Descrip	tion					Version	
How do I	DefaultAuthentic	ator		WebLog	ic Authentication I	Provider				10	
100 00 1	Default defende			webboy							
 Configure authentication and identity assertion providers 	DeraultidentityA	serter		webLog	ic toenuty Asserti	n provider			Showing	1 to 2 of 2 Previous Next	
Configure the Password Validation provider											
Manage security providers											
 Set the JAAS control flag 											

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	ninistration Console 14.	.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	is >myrealm >Providers >DefaultAuthenticator >Su	mmary of Security Realms >myrealm >Providers						
No pending changes exist. Click the Release	Create a New Authentication Provider									
domain.	OK Cancel									
Lock & Edit	Cranta a rear Arth	antiantian Denviden								
Release Configuration	The following property	tios will be used to identify your	r now Authoritization Dravidor							
Domain Structure	* Indicates required fit	elds	new Addiendcadori Providei.							
trunk_dom_repl_domain										
B-Environment	The name of the auth	entication provider.								
D-Clusters	* Name:	SAML OBDX CON	FIG							
Coherence Clusters Machines										
Virtual Hosts	This is the type of aut	hentication 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	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 Assert	ter,
Domain Structure OBDX21ADMIN	Customize this table	
Environment Deployments	Identity Provider Partners	
B Services	New v Delete	Showing 0 to 0 of 0 Previous Next
Security Realms Interoperability	🖸 Name 🗞	
tit Diagnostics	There are no items to display	
	New - Delete	Showing 0 to 0 of 0 Previous Next
	New Web Single Sign-On Identity Provider Partner	
	New WebService Identity Provider Partner	
Herri de T		

8. Provide the name for the identity partner and select the IDC metadata xml copied to WebLogic server.

Click **OK** button to save.

Entrantil a second of second	
Enter the name or your n Specify the name and loca Indicates required fields	ew Single Sign- on Ldentity Provider partner ation of the SANL 2.0 metadata file that you received from this new partner
Please specify the name of the part	ner. WebSSO-IdP-Partner-0
Please specify the name of the file	containing the partner metadata document.
Path:	/scratch/app/domain/trunk_dom_repl_domain/IDCSMetadata.xml
Recently Used Paths: Current Location:	/scratch/app/domain/trunk_dom_repl_domain 100.76.153.182 / scratch / app / domain / trunk_dom_repl_domain
bin common config	
logs	
 orchestration original servers IDCSMetadata.xml 	
	Specify the name and loc Indicates required fields lease specify the name of the part lease specify the name of the file Path: Recently Used Paths: Current Location: Din common config init-info jms kops ordestration original servers X CK Cancel CK Cancel CK Cancel CK Cancel CK Cancel CK CANCEL CANCEL CK CK CANCEL CK CK CANCEL CK CK CANCEL CK

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 SAME 2.0 Web Single Sign-on Identity Provider partner	Issuer URI:	https://idcs- 02002664422cdcc6857cdd56220cbdf identity.c0dex.0.cc0asdex.com/442/fed	The Issuer URI of this Identity Provider partner. More Info
Configure authentication and identity		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

ORACLE WebLogic Server Ad	ministration Console	14.1.1							Õ			
Change Center	🟦 Home Log C	Out Preferences 🔤 Record	l Help	Q		Welcome,	weblogic Conne	ected to: trunk_dom_repl	_domair			
View changes and restarts	Home >Providers	Home >Providers >SAML_OBDX_IT >IDCS_IT >Summary of Security Realms >myrealm >Providers >SAML_OBDX_IT >Summary of Servers >obdc_server1 >Summary of Servers										
No pending changes exist. Click the Release												
configuration button to allow others to edit the domain.	Configuration Control											
Lock & Edit												
Release Configuration	A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.											
Domain Structure This page summarizes each server that has been configured in the current Weblogic Server domain.												
trunk_dom_repl_domain	2 5											
Environment Servers												
⊞-Clusters	Customize t	his table										
Coherence Clusters	Servers (Filte	ered - More Columns Exis	t)									
Virtual Hosts	New Clor	e Delete					Show	ing 1 to 2 of 2 Previous N	Next			
Work Managers			_									
	□ Name ↔	*	Туре	Cluster	Machine	State	Health	Listen Port				
Deployments	AdminSe	rver(admin)	Configured			RUNNING	🖋 ок	9011				
Services Security Pealms	obdx_se	rver1	Configured	obdx_cluster	obdx_machine	RUNNING	🖋 ок	19003				
Thermerability	New Clor	Delete					Show	ing 1 to 2 of 2 Previous M	Next			
How do I												

- 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

		The organization of a Third Frank
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

- 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

ORACLE WebLogic Server Ad	ministration Console 14.1.1		Q
Change Center	🔒 Home Log Out Preferences 🔤 Record Help	Q	Welcome, weblogic Connected to: trunk_dom_repl_domai
View changes and restarts	Home >Summary of Servers >Summary of Security Res	alms	
Click the Lock & Edit button to modify, add or delete items in this domain.	Summary of Security Realms		
Lock & Edit Release Configuration	A security realm is a container for the mechanisms multiple active security realms in a WebLogic Server This Security Realms page lists each security realm t	including users, groups, security roles, security p domain, but only one can be set as the default s hat has been configured in this Webl onic Server	olicies, and security providersthat are used to protect WebLogic resources. You can have ecurity realm, which is reserved for domain administrative purposes. domain. Click the name of the realm to explore and configure that realm.
Domain Structure	,		
trunk_dom_repl_domain	Customize this table Realms (Filtered - More Columns Exist)		
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
Concurrent Templates	🗆 Name 🗞	Default Realm	
Deployments	myrealm	true	
B Services Security Realms	New Delete		Showing 1 to 1 of 1 Previous Next
How 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 2-20 Providers

	dministration Console 1	4.1.1									Q
Change Center	Home Log Out	Preferences 🔤 Recor	d Help		٩				Welcome, weblogi	Connected to: ob	odx_doma
View changes and restarts	Home >Summary of	Home >Summary of Security Realms >myrealm >Providers									
Click the Lock & Edit button to modify, add or	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	Authentication	Password Validation	Authorization	Adjudication	Role Mapping	Auditing	Credential Mapping	Certification Path			
Deployments Postvices Postvices Postvices Postvices Postvices Postvices Postpostces	An Authentication Authentication pro- Customize this Authentication F Click the Lock & I	n provider allows WebLog oviders in a security real table Providers Edit button in the Chang	iic Server to est m. Different typ e Center to acti	ablish trust by v es of Authentica vate all the butt	alidating a user. Y tion providers are ons on this page.	ou must har designed t	ve one Authentication j o access different data	orovider in a security stores, such as LDA	y realm, and you can o P servers or DBMS. Showing	onfigure multiple	us Next
	Name			Descrip	tion					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 Previou	is Next
Configure the Password Validation provider											
 Manage security providers 											
 Cot the 1AAC control floor 											

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".

,	A		
Change Center	Home Log Out	Preferences 🧰 Record Melp	welcome, weblogic Connected to: test221_domain
View changes and restarts	Home >Summary of	iervers >obdx_server1 >Summary of Servers >Summary of Security Realms >myrealm >Provid	ders >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.	e OK Cancel		
Lock & Edit	OK Caliber		
Palease 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			
E-Environment	The name of the au	hentication provider.	
Clusters	* Name:	001 Auth	
Coherence Clusters		SQLAUN	
Machines	This is the type of a	uthentication provider you wish to create.	
Work Managers			
Concurrent Templates	Type:	ReadOnlySQLAuthenticator ~	
	and langer		
-Services	OK Cancel		
Messaging	-		
1 CTURE SOURCES			
How do I			
Manage security providers			
 Configure authentication and identity assertion providers 			

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	ce	
Lock & Edit Release Configuration	Common Provider Specif	c	
Domain Structure	Click the Lock & Edit butto	n in the Change Center to modify the settings on this page.	
test221_domain	Save		
	This page displays basic info sequence.	ormation about this Read-only SQL Authentication provider. You can	also use this page to set the JAAS Control Flag to control how this provider is used in the login
	街 Name:	SQLAuth	The name of this Read-Only SQL Authentication provider. More Info
Concurrent Templates Startup and Shutdown Classes	ighter the secretary description:	Provider that performs DBMS authentication	A short description of this Read-Only SQL Authentication provider. More Info
Security Realms Therementality	街 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
Configure authentication and identity assertion providers	Save		
Set the JAAS control flag	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 = ?

Deployments Services Security Realms	Data Source Name:	NONXA	The data source used by this Read-Only SQL Authentication provider. More Info
How do I	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 If Group Membership Searching is set to limited. Valid values are 0 and positive integers, for example, 0 inductes only direct group memberships will be found, a positive number indicates the number of levels to go down. More Info
System Status Health 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
Critical (0) Overloaded (0) Warning (0)	SQL User Exists:	SELECT U_NAME FROM I	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
	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
	SQL Is Member:	SELECT G_MEMBER FRO	The SQL statement used to look up members of a group. The SQL statement 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 group 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
	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
	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 most a single record containing the group description. More Info
	Save		
	Click the <i>Lock & Edit</i> button in the Change Center to modify t	he 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

Configuration button to allow others to edit the domain.	Configuration	Users and Groups	Roles and Policies	Credential Map	pings Provider	s Migra	ition			
Lock & Edit	Authentication	n Password Valida	tion Authorization	Adjudication	Role Mapping	Auditing	Credential Mapping	Certification Path		
Release Configuration										
Domain Structure	An Authenticat	ion provider allows V	VebLogic Server to es	tablish trust by va	alidating a user. Yo tion providers are	u must ha	ive one Authentication p to access different data	provider in a security realistores, such as LDAP sen	m, and you can configure m	ultiple
test221_domain	Huttenreuton	providers in a securi	ty reality billerence	pes of Mathematic	uon providers ure	acognea	to access amerene ada	stores, such as core ser	icid of DDHD.	
Environment Servers Clusters	Customize th	is table								
Coherence Clusters	Authenticatio	n Providers								
Machines	New Dolot	Reorder							Chauden 1 ks 4 of 4	Devidence March
Virtual Hosts	101								Showing 1 to 4 of 4	Flevious Next
Concurrent Templates	Name		Description							Version
Startup and Shutdown Classes	SAML_TE	ST	SAML 2.0 Ider	ntity Assertion Pro	wider. Supports Se	curity Ass	ertion Markup Language	e v2.0.		1.0
Services	SQLAuth		Provider that	performs DBMS a	uthentication					1.0
B-Interoperability	DefaultAu	thenticator	WebLogic Aut	hentication Provid	ler					1.0
How do I	DefaultIde	entityAsserter	WebLogic Ide	ntity Assertion pro	ovider					1.0
Configure authentication and identity assertion providers	New Delet	Reorder							Showing 1 to 4 of 4	Previous Next
Configure the Password Validation provider										
Manage security providers										
Set the IAAS control flag										

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	You can reorder your Authentication Providers using the	ist 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 A		
Environment	Authentication Providers:	
Servers	Available:	
Clusters		
Coherence Clusters	SAML_TEST	
Machines	SQLAuth	
Virtual Hosts	DefaultAuthenticator	
Work Managers	DefaultIdentityAsserter	
Concurrent Templates	\bigtriangledown	
Startun and Shutdown Classes	⊻	
Doployments		
Deployments		
Services		
Security Realms		
dr Interoneranility	OK Cancel	
How do I		
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	 .
		- Created	- Removed		
Passwords		Logins		All Reports	
-	Ŷ	-	Я		
	Ŷ	— Total	8		

Figure 2-26 Dashboard

2. In popup window select Confidential Application.



	Identity Cloud Service	License Type :: F	oundation ?	SD
Applicatic	ld Application		<pre>cription, or t</pre>	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.	•	T
- (Confidential Application	Greate a web-server/server-side application that uses OAuth 2.0. These apps application that uses OAuth 2.0. These apps application of their client secret.	0	Ш
	Enterprise Application	Create a web application that is protected by the App Gateway.	0	Ш

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	 — 	2	3		5		Next >
	Details	Client	Resources	Web Tier Policy	Authorization		
	Allowed Grant Types	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	^S 🗆 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	^s 🗌 Introspect 🗌 On behalf	Of				
ID Token Encryption Algorithr	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	 Tagged Specific 			
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 Issuance Polic	cy 🚯	Add App Role		×
Authorized Resources	AllTaggedSpecific	Select All	٩.	
Resources		Selected:	1 Clear Selection	1
+ Add Scope		Identity Domain Administrator		1
Resource No data to dis	splay.			
Grant the clien	t access to Identit			1
+ Add				1
App Roles		Page 1 of 1 (1 of 1 items) K < 1 >	к	
No data to dis	splay.		Ac	bt

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

Figure 2-33 Add Confidential Application

Token Issu	uance Policy	• •			
	Authorized Resources Resources	 All Tagged Specific 			
	+ Add Scope				
	Resource		Protected	Scope	
	No data to displ	lay.			
	Grant the client a	access to Identity Cloud Service	Admin APIs		
	+ Add				
7	App Roles			Protected	
	Identity Domai	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 Grante as Auth	porization U				

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	_CONFIG user details from IDCS	Activate X Remove
Details Configuration Web Tier Policy App Details	Users Groups	Generate Access Token Save
Application Type * Name Description	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	_CONFIG user details from IDCS	🛇 Activate 🛛 🗶 Remove
Details Configuration Web Tier Policy App Details	Confirmation Are you sure that you want to activate the application OBDX_OAUTH_CONFIG?	× Generate Access Token Save
Application Type * Name Description	COBDX_OAUTH_CONFIG OAuth Configuration for fetching user details from IDCS	OK
Application Icon	\frown	

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 ferms in this domain. Configuration Configuration Configuration Demain Structure test221, domain This page displays the list of Java EE applications and standalone application modules installed to this domain. You can update (redeplay) 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 To install a new application or module for deployment to targets in this domain, click Install. Descharms Customize this table Descharms Decomments							s on this page.	
La Diagnosoca		In	stall Update Delete				Showing 1 to 24	of 24 Previous Next
			Name	State	Health	Туре	Targets	Deployment Order
	[0	om.ofss.digx.connector	Active	🖋 ок	Resource Adapter	obdx_server1	0
	ļ		a 🗑 digx-admin	Active	🛩 ок	Web Application	obdx_cluster	100
How do I		O	🗷 🥫 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		0	digx-coherence	Active	🖋 ок	Web Application	obdx_cluster	0
 Monitor the modules of an enterprise application 			B odgx-common	Active	🖋 ок	Web Application	obdx_server1	100
Deploy EJB modules Install a Web application		O	🗄 🗑 digx-corporateloan	Active	🖋 ок	Web Application	obdx_server1	100
Instan a web applied000]		J 🗄 🐻 digx-creditfacility	Active	🖋 ок	Web Application	obdx_server1	100
System Status		C	I 🗄 🐻 digx-edx	Active	🖋 ок	Web Application	obdx_server1	100
Health of Running Servers as of 6:22 AM Failed (0)		C	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	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 Preferen	ces 🔤 Record Help		Q				Welcor	ne, weblogic	Connected to: trunk_	dom_repl_dor
View changes and restarts	Home >Summary of Deployme	nts >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 Pla	n Configuration Securi	ty Targets	Control T	esting	Monitoring	Notes				
Lock & Edit	General Properties	tbound Connection Pools	Admin Objects	Workload	i Instr	umentation					
Release Configuration											
Jomain Structure unk_dom_repl_domain B-Environment Environments	This page displays a table of listed by connection factory connection pool group. Clic	of outbound connection pool g interface and the instances a k the name of a group or insta	roups and instar re listed by their ince to configure	nces for this r JNDI names e it. Automati	esource a . Expand ically gen	adapter. The a group to o erated conne	top level er obtain config ection pools	ntries in the table repr juration information f are not displayed in t	esent outbound or a connection the table below.	d connection pool group pool instance within an	s. Groups are outbound
B-Services Security Realms	New Delete	or configuration rapic								Showing 1 to 1 of 1	Previous Nex
 Interoperability Diagnostics 	Groups and Instan	ces 🊕				Co	onnection I	Factory Interface			
	I javax.resource.cci.	ConnectionFactory				jav	ax.resource	.cci.ConnectionFactor	у		
	New Delete									Showing 1 to 1 of 1	Previous Nex
iow 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_repL_domain ⊕=Environment =Oeployments =Services =Services	Outbound Connection Group @ joxx.resource.cd.ConnectionFoctory 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	he new connection instance	
bomain structure	indicates required netus		
Environment	The Outbound Connection instance represents a connection	ction pool. The JNDI name can be used to obtain the pool at runtime.	
Deployments Services	AT * INDI Name:		
Security Realms	an shor hame.	ra/DIGXConnectorSSOREY	
Interoperability Diagnostics	Back Next Finish Cancel		



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

delete items in this domain. Lock & Edit	Configuration Control Monitoring											
Release Configuration	1	This page displays the list of Jave EE applications and standalone application modules installed to this domain. 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. To install a new application or module for deployment to targets in this domain, click Install .										
ttr Diagnostics		Ins	Install Update Delete				Showing 1 to 24 of 24 Previous Next					
			Name 🚕					State	Health	Туре	Targets	Deployment Order
		O	ocm.ofss.digx.com	nector				Active	🖋 ок	Resource Adapter	obdx_server1	0
			🗈 🦲 digx-admin					Active	🖋 ок	Web Application	obdx_cluster	100
How do I		O	🗉 🥫 digx-auth					Active	🛩 ок	Web Application	obdx_cluster	100
Install an enterprise application			🗄 🐻 digx-cms					Active	🛩 ок	Web Application	obdx_server1	100
Configure an enterprise application Update (redeploy) an enterprise application		0	E adigx-coherence					Active	🖋 ок	Web Application	obdx_cluster	0
 Monitor the modules of an enterprise application 			E adigx-common					Active	🖋 ок	Web Application	obdx_server1	100
Deploy EJB modules		0	E adigx-corporate	loan				Active	🛩 ок	Web Application	obdx_server1	100
Install a Web application		0	E adigx-creditfacil	ity				Active	🖋 ок	Web Application	obdx_server1	100
System Status			E adigx-edx					Active	🖋 ок	Web Application	obdx_server1	100
Health of Running Servers as of 6:22 AM			E adigx-eurekaser	ver				Active	🖋 ок	Web Application	obdx_server1	100

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_repl_domain					
View changes and restarts	Home >Summary of Deployments >com.ofss.digx.connect	tor >Summary of Deployments >com.ofss.di	digx.connector >Summary of Deployments >com.ofss.digx.connector >Roles					
No perding changes edit. Click the Release Configuration button to allow others to edit the domain. Lock & Edit Release Configuration Domain Structures Domain structures	Settings for com.ofss.digs.connector Deerview Deployment Plan Configuration Se Roles Policies Outbound Credential Mappin Cotbound credential mappings let you map Weblog set default outbound credential mappings for all outbound credential bland on thema credential mappings for all outbound	ceutity Targets Control Testing Inbound Principal Mappings Pri pic Server usernames to usernames in th thound connection pools in the resource for this resource advater	Monitoring Notes vincipals					
Benviconnet Benviconnet Deployments Services Services J-Services Interoperability Diagnostics	Customize this table Outbound Credential Mappings Outbound Credential Mappings Outbound Credential Mappings Outbound Credential Mappings	nin unis resource augues.	Showing 0 to 0 of 0 Previous Next.					
	UKLS 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								
Create outbound credential mappings								
 Delete outbound credential mappings 								

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	ctor >Summary of Deployments >com.ofs	s.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.	e	Selecting a pool is required.						
Lock & Edit Release Configuration	1	eate a New Security Credential Mapping						
Domain Structure		Outbound Connection Pool						
rrunk_dom_repl_domain = Environment - Deployments		Which Outbound Connection Pool would you like th Pools in this resource adapter. Each Outbound Con	ne credential map to be associated with nection Pool can then configure thems	P Selecting Resource Adapter Default will configure the credential elves to override these credentials.	mapping for all Outbound Connection			
B-Services Security Realms		Customize this table						
Interoperability Diagnostics		Create a New Security Credential Map Entry I	01:		Showing 21 to 26 of 26 Previous Next			
		🔲 Outbound Connection Pool 🚕						
		ra/DIGXConnectorOBSCF						
		ra/DIGXConnectorOBTFPM_14.3						
		ra/DIGXConnectorOBVAM						
How do I	a /	ra/DIGXConnectorREWARDS						
Create outbound credential mappings		ra/DIGXConnectorSSOKEY						
	-	Resource Adapter Default			Chaudea Of the OC of OC - Devidence Next			
System Status	-				showing 21 to 20 or 20 Previous Next			
Health of Running Servers as of 6:37 AM		Back Next Finish Cancel						
Failed (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	The Home Log Out Preferences Mecord Help Velcome, 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 >Summary of Deployments >com.ofss.digx.connector >Roles
No perding changes edit. Click the Release Configuration button to allow others to edit the domain. Lock & Edit Release Configuration Domain Structure truck dom, repL domain Br Enknoment Deployments Br Searks Br Interoperability Br Deginatics	Create a New Security Credential Mapping
	Wehl onle Server Hear Name
	Back Next Finish Cancel
How do I	
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 >com.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 Noxt Enish Cancel EIS User Name and Password Cancel Cancel Cancel					
	Configure the EIS User Name and Password that you would like to map the WebLogic Server User to:					
Domain Structure	* Indicates required fields					
turk, Gon, repL, Gonain H-Environment H-Deployments H-Sarvices	Enter the EIS User Name: * EIS User Name:	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX				
	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

