Oracle Banking Digital

Experience

PSD2 Guide Release 18.1.0.0.0

Part No. E92727-01

January 2018



PSD2 Guide January 2018

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

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

Table of Contents

1. Pre	face	4
1.1	Intended Audience	4
1.2	Documentation Accessibility	4
1.3	Access to Oracle Support	4
1.4	Structure	4
1.5	Related Information Sources	4
2. Pu	pose	5
3. Тор	oology	6
4. PS	D2 Configurations	7
4.1	IDCS Configuration	7
4.2	APICS Configurations1	1
4.3	OBDX Configurations	4
5. Thi	rd Party Application Registration2	6
5.1	Registering a Third Party Browser Client in IDCS2	6
5.2	Registering a Third Party Mobile Client in IDCS	0
5. Vie	w and Manage Consents in OBDX3	4
5.3	Manage Consent in OBDX	4
5.4	PSD2 Offerings and Modules	5

1. Preface

1.1 Intended Audience

This document is intended for the following audience:

- Customers
- Partners

1.2 Documentation Accessibility

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

1.3 Access to Oracle Support

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

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

http://www.oracle.com/pls/topic/lookup?ctx=accandid=trs if you are hearing impaired.

1.4 Structure

This manual is organized into the following categories:

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

The subsequent chapters describes following details:

- Purpose
- Configuration / Installation.

1.5 Related Information Sources

For more information on Oracle Banking Digital Experience Release 18.1.0.0.0, refer to the following documents:

• Oracle Banking Digital Experience Licensing Guide

2. Purpose

This document provides step by step guide to configure OBDX for PSD2 implementation.

The actual steps will vary based on actual implementation depending on bank infrastructure and enablement of use cases out of OBDX PSD2 list of offerings.

For Example, bank may choose to configure mobile client or browser client or mix of both and accordingly the implementation steps will vary. Though, this document covers steps required for all the scenarios.

Home

3. Topology



Home

4. PSD2 Configurations

4.1 IDCS Configuration

- a) Registering OBDX as an Admin application in IDCS
- Click add in the application tab to register OBDX Admin application.

Identity Cloud Service	Home User:	Groups	Applications	Jobs	Settings	Security			
Applications									٩
Select All + Add X Remove Create an applica Client	C Activate	Deactivate						0	Т
Demo Ap Mobile Application	plication							0	Ξ
Elite Acco	unts ^{BOV}							0	Ξ
Elite Acco Dummy App 1 for	unts - App1 PSD2 implementation							0	Ξ
Elite Acco For Demo Purpos	unts - Demo							0	Ξ
Elite Payn For PSD2 Demo-	nents BOV							0	т
Elite Paym Third Party App in	nents - App2 aplementation for PSD2.							0	т

• Select trusted application

Add App	lication		×
E	App Catalog	Add an application from the Application Catalog.	-
.</td <th>SAML Application</th> <td>Create an application that supports SAML for Single Sign On.</td> <td></td>	SAML Application	Create an application that supports SAML for Single Sign On.	
C	Mobile Application	Create a mobile/single-page application that uses OAuth 2.0. These applications cannot maintain the confidentiality of their client secret.	
•	Trusted 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.	

• Add "name" and "description"

Add Trusted A	oplication				
Cancel	Details	Client	Resources	Authorization	Next >
App Details					
	*	Name Trusted demo			
	Desc	ription Web Application			
			h		
	Applicatio	on Icon			
		Upload			
	Applicatio	on URL			
	Log	jin URL			
	Logout Pa	ge URL			
Tags					
Add tags to your applications to	organize and identify them. A t	ag consists of a key-value pair.			
T Add lag					
Display Settings					

• Check 'Client Credentials' option as the 'Allowed Grant Type'. Check 'Introspect' as 'Allowed Operations'.

✓ Client Configuration
Register Client No Client
Allowed Grant Types 📄 Resource Owner 😨 Client Credentials 📄 JWT Assertion 📄 SAML2 Assertion 📄 Refresh Token 📄 Authorization Code 📄 Implicit
Allow non-HTTPS URLs
Redirect URL
Logout URL
Post Logout Redirect URL
* Client Type 🔘 Trusted 💿 Confidential 💿 Public
Certificate Import
Allowed Operations 🗷 Introspect 💿 On behalf Of

Add Admin Privileges for OBDX Client Configuration

Grant the client access to Identity Clou	d Service Admin APIs.				
Identity Domain Administrator 🗙	User Administrator 🗙	Self Registration $ imes$	Application Administrator ×	Security Administrator 🗙	Me ×
Signin ×					

Application added

Add Trustee	d Application				
< Back	Details	Client	Resources	Authorization	Finish
Authorization					Click to add this appre
	Enforce Grants as Authorizat	ion			

Ap	plication Ad	ded	×
Be	low is the new Cli	ent ID and Client Secret for your application.	
Th the	is information als e application.	o appears on the Configuration tab in the Detail	s section for
	Client ID	d095c8410e424988829277e998295a9e	
	Client Secret	fb2a3a1e-726e-4b3b-a310-9d130212e3b9	
			Ciose

• Application added. We shall need the Client-Id and Client-Secret to configure OBDX Admin application in OBDX and WLS. (Refer "Enabling PSD2 on OBDX Entity" & "Set up IDCS Asserter" sections)

Setting up login page

• Set Login URL to '/ui/v1/signin' if something else. '/ui/v1/signin' is the default login page provided by IDCS.

≡ ≱ ZigBank Identity Cloud Service	
Session Settings	Save Cancel
* Session Expiry	480 v n minutes
Login URL	/ui/v1/signin
* Logout URL	/ui/v1/myconsole
Allow Cross-Origin Resource Sharing (CORS)	
Allowed CORS Domain Names	mum00apt.in.orade.com

• Page to set session token timeout and custom login URL

Session Settings	Save Cancel
* Session Expi	y 480 🗸 ninutes
Login UI	L http://mum00apb.in.oracle.com:7778/p
* Logout U	L /ui/v1/myconsole
Allow Cross-Origin Resource Sharir (COR	g C
Allowed CORS Domain Nam	s mum00apb.in.orade.com
	i.

4.2 APICS Configurations

Login to APICS



Create API

← → C û ① apics.oracle.com:7201 Apps ▷ Welcome API Managen	L/apiplatform/apis nent 🛛 🌍 Developer Portal							\$
	- Management Portal							weblogic
		APIs	Applications	Gateways	Services	Service Accounts	Roles	Platform Settings
APIs								
Search By Name	Advanced * Newest		*					Create API
Create API								×
Name and Version are required.								
Name *					Version *			
Description								
								Create Cancel

• API Implementation

reaconite 🖸	Art Hanagement 😈 Developer Foldat		
	ORACLE API Platern Cloud - Management Potal	eshige APis Applications Gateways Services Service Accounts Roles Plathon Service	
	< APIs	/ Stev Edualie	
	GetAccountBalance 1.0 New Published Apta • Cick to entry API description Institu 5 Loci logeneity weakings Nov 8, 2017 10 34 AM +00.00 ③	Data Data	
	API Implementation API Implementation Request	Available Policies To apply, here new a policy and click "Apply".	
	API Request accounts	Security Traffic Management	
	P Service Request Http://www00apti?003vdgv/s2iscouvts	Interface Management Routing	

• Edit Policy

ORACLE API Parton Coul - Management Portal	setings
	Ma Applications Damong's Devices Service Accounts Rober Partner Detrops
Caris	Edit Policy - Service Request ×
GetAccountBalance 1.0 New Patrice Groot	Apra * SpecTy the factional service URL, Learn More
Char to ense API description	Configure Headers
Memory 1 Carroyamently waitings: from 8, 2017 10 34 AM 4010	Company (c) Present (c) P
API Implementation	Server O seek strategy a strategy and a server of the strategy and a serve
Preparat	Respons Use Gateway Node Pory
API Request accord	Service Account
R Service Request	
Inclusion Couple Tricing in Line County	Anty as Dati Anny
11 III III III III III III III III III	s Other

• View API Summarizing

) Welcome 🖸 A	Pl Management 🛛 🌍 Developer Portal			
(DRACLE API Platform Cloud - Management Portal		weblogic	
	•	APts	Agglications Gateways Services Service Accounts Roles Planform Settings	
	API Implementation	Resources	Available Policies To applic, how your a policy and click 'Apply'.	
	÷		- Security	
	API Request accounts		QA(m 2.0)10	
	R Service Request		Key Valdation 1.0	
	Ang. Trium Obagit: 7003 idge/v1/accounts		Basic Auth 1.0	
	if.		Service Level Auth 1.0 Service	
			IP Filter Validation 1.0	
			CORS 10	
			 Traffic Management 	
			 Interface Management 	
			» Routing	
			Other	

4.3 **OBDX Configurations**

4.3.1 WebLogic Configurations

Patch WLS12.2.1.2.

• WLS 12.2.1.2.0 (PS2 PSU) Obtain and install the WLS 12.2.1.2.0 kit from OTN:

Download the 12.2.1.2.171017 Patch Set Update (PSU) for WebLogic Server 12.2.1.2 from https://support.oracle.com/epmos/faces/PatchDetail?patchId=26485996

Apply the PSU patch following the instructions contained in the README.txt in the p26485996_122120_Generic.zip patch file.

Set up IDCS asserter

- Login to WLS console using admin credentials.
- Navigate to Security Realms →myrealm →Providers
- Click on New
- Name the asserter. Select 'OracleIdentityCloudIntegrator' as the provider type.

Create a New Authentica 🗙												Niej	-	ć	1	×
← → C ③ Not secure mum00a	apt:9001/conso	e/console.porta	I?_nfpb=true&_	pageLabel=	SecurityProvidersCreate	Atn			☆			-0	0	8	G	:
👖 Apps 📙 yoku ★ Bookmarks 📙 🤇	OBP2502LZN	OBP2502BASE	OBDX17.2	OBDX17.1	Oracle Applications	🔆 OBDX - Wiki	D ODSM	Identity Self Servic	e {0	OBP	25Grok	**		Other I	ookm	irks
Lock & Edit Release Configuration	OK Canc Create a ne The following	el w Authentication	Provider used to identify your	new Authentica	ation Provider.											-
Domain Structure	* Indicates req	uired fields														11
OBDX_INS_TEST	The name of t	he authentication p	rovider.													l
Deployments E-Services	* Name:	IC	CSAsserter													Ш
Security Realms Triteroperability Diagnostics	This is the typ	e of authentication	provider you wish to	create.												Ш
	Type:	0	racleIdentityClou AML2IdentityAss	dIntegrator erter	T											Ш
	OK Canc		BDXDBAuthentic BDXJWTIdentity	ator Asserter												I
		č	rossTenantAuthe	nticator												1
How do I 😑		Ti	rustServiceIdentit	yAsserter or												
Manage security providers		ŏ	AMAuthenticator	61												
 Configure authentication and identity assertion providers 		AC	ctiveDirectoryAut ustomDBMSAuth	henticator enticator												
System Status		D	efaultIdentityAss PlanetAuthenticat	erter or												
Health of Running Servers as of 11:18		L	DAPAuthenticato													
Failed (0) Critical (0) Overloaded (0) Warning (0) OK (2)		N N O O	DAPX509Identity. egotiateIdentityA ovellAuthenticato penLDAPAuthen racleIdentityClou racleInternetDire	Asserter sserter r ticator dintegrator ctoryAuthenti	icator 👻											
WebLogic Server Version: 12.2.1.2.0 Copyright (c) 1996,2016, Oracle and/or its affiliates. Al Oracle is a registered trademark of Oracle Corporation	ll rights reserved. and/or its affiliates. (Other names may be t	rademarks of their res	pective owners.												Ļ

Click 'OK'

	ministration Console	12c									õ	
Change Center	🙆 Home Log Ou	it Preferences 🔯 Rec	cord Help		Q				Welcon	ne, weblogic Conne	ected to: obdx_domain	
View changes and restarts	Home >obdx_serve	er >Summary of Security F	Realms >myrealm >	Providers								
Click the Lock & Edit button to modify, add or delete items in this domain	Settings for myre	alm										
Lock & Edit	Configuration Users and Groups Roles and Policies Credential Mappings Providers Migration											
Release Configuration	Authentication	Password Validation	Authorization	Adjudication	Role Mapping	Auditing	Credential Mapping	Certification Path				
Domain Structure obdr_domain ⊕ Domain Partitions ⊕ Townorment → Deployments ⊕ Security Realms ⊕ Interopenability ⊕ Diagnostics	An Authenticatio a security realm.	on provider allows WebL . Different types of Auth s table Providers <i>B Edit</i> button in the Char Reorder	u must haı data store	re one Authentication p s, such as LDAP server	rovider in a security s or DBHS.	realm, and you can confi	igure multiple Authen Showing 1 to 5 o	tication providers in f 5 Previous Next Version				
			Provider	that performs LD/	AP autnentication						1.0	
How do I	OAMIdenti	tyAsserter	Oracle A	ccess Manager Ide	entity Asserter						1.0	
Configure Authentication and Identity Assertion providers	IDCSAsserter Provider that performs identity assertion for Oracle Identity Cloud Service tokens 1.0 Identity DefaultAuthenticator WebLogic Authentication Provider 1.0											
Configure the Password Validation provider	DefaultIder	ntityAsserter	WebLogi	c Identity Assertio	n provider						1.0	
Manage security providersSet the JAAS control flag	New Delete	Reorder								Showing 1 to 5 o	f 5 Previous Next	
 Re-order Authentication providers 												

- Click on 'IDCSAsserter'
- Choose 'Authorization' property as Active Type

	ninistration Console 12c		Q
Change Center	🏠 Home Log Out Preferences 🔤	Record Help	Welcome, weblogic Connected to: obdx_domain
View changes and restarts	Home >obdx_server >Summary of Secu	rity Realms >myrealm >Providers >IDCSAsserter	
Click the Lock & Edit button to modify, add or delate items in this domain	Settings for IDCSAsserter		
Lock & Edit	Configuration		
Release Configuration	Common Provider Specific		
Domain Structure	Click the Lock & Edit button in the	Change Center to modify the settings on this page.	
obdx_domain	Save		
E - Environment	This page allows you to define the	eneral configuration of this provider.	
Deployments Services	個 Name:	IDCSAsserter	
Security Realms Transport	Description:	Provider that performs identity assertion for Oracle Identity Cloud Service tokens	
	👍 Version:	1.0	
How do I	Active Types: Available: Idcs_user_assertion REMOTE_USER Idcs_user_assertion	Chosen: Authorization	
No task help found.			
System Status		22	
Health of Running Servers			
Failed (1) Critical (0)	Base64 Decoding Required:	false	
Overloaded (0) Warning (0)	Save		
OK (1)	Click the Lock & Edit button in the	Change Center to modify the settings on this page.	

• Click on Provider Specific and configure IDCSAsserter properties. Provide Client Id and Client secret of OBDX Admin Application; created in <u>Step 4.1.a</u> in fields Client Id and Client Secret & Confirm Credentials. Fill in other marked properties as per the IDCS host.

aungs for fDC-SASSerter	
onfiguration	
Common Provider Specific	
Click the Lock & Edit button in the Change Center to modify the settings	s on this page.
Save	
This page allows you to configure additional attributes for this security pr	rovider.
Audience Enabled	
ISONWeb Key Set URI:	
Sync Filter Match Case	
Token Validation Level:	NORMAL 🔻
Port:	443
🗹 Cache Enabled	
Fenant Names:	
lient IDToken Claim:	client_id
Base Path:	
oken Clock Skew:	120
enant Token Claim:	user_tenantname
ny Identity Domain Enabled:	true
Jser Name Resource Attribute:	userName
Jenant Host Name Template:	{%tenant}.{%host}

SSLEnabled	
Access Token Timeout Window:	300
User IDResource Attribute:	id
Client IDResource Attribute:	
App Roles Token Claim:	appRoles
Client Id:	00fa15d18cd147398ca4b53f
Tenant Data Flush Interval:	0
Only User Token Claims Enabled	
User Name Token Claim:	
Signature Prefer X509 Certificate	
Token Secure Transport Required	
Cache TTL:	300
Groups Token Claim:	groups
🖉 Token Cache Enabled	
Client Tenant:	obdx-tenant01
Resource Tenant Token Claim:	tenant
Sync Filter User Header Names:	
User IDToken Claim:	user_id
User Authentication Assertion Attribute:	

✓ Sync Filter Enabled	
Issuer:	
Sync Filter Only Client Cert Requests	
Tenant:	
Thread Lock Timeout:	300
Token Virtual User Allowed	
Connect Timeout:	300
Response Read Timeout:	60
Tenant Data Reload Interval:	300
Host:	obdx-tenant01.identity.c9dev
App Name Filter Header Name:	X-RESOURCE-SERVICE-IN
Client Name Token Claim:	client_name
Cache Size:	500
Client As User Principal Enabled	
Sync Filter Prefer Header	
Client Secret:	
Confirm Credential:	
Client Tenant Token Claim:	client_tenantname
🗹 Tenant Data Reload Enabled	
Tenant Header Names: X-USER-IDENTITY-SERVICE-GUID X-USER-IDENTITY-DOMAIN-NAME X-RESOURCE-IDENTITY-SERVICE-GUID X-RESOURCE-IDENTITY-DOMAIN-NAME	

• Restart the OBDX Managed as well as Admin Server.

Configuring TLS for IDCS.

 Download Certificate from IDCS Host. Add the certificate to a custom keystore and add it to the WebLogic server.

🛍 Home	Log Out	t Preferenc	es 🚵 Rec	ord Help			Q					Welo	ome, weblogic	Connected to:
Home >Su	mmary of	f Servers >0	BDX_INS1											1
Settings fo	r OBDX	(_INS1												
Configura	ation	Protocols	Logging	Debug	Monitoring	Control	Deployments	Services	Security	Notes				
General	Cluster	r Service	s Keysto	ores S	L Federatio	n Services	Deployment	Migration	Tuning	Overload	Concurrency	Health Monitoring	Server Start	Web Services
Click the	Lock &	Edit button	in the Char	nge Cente	r to modify the	e settings o	n this page.							
Save				-		-								
<i>Keystore</i> manage	s ensure the secu	the secure wity of mess	storage and sage transm	d manage issions.	ment of private	e keys and	trusted certificat	e authorities	(CAs). This	page lets y	ou view and defi	ne various keystore c	onfigurations. T	hese settings help
Keystore	5:					Der	no Identity and	Demo Trust	Change		Which configure keystores? Mo	ation rules should be ore Info	used for finding	the server's iden
— Identit	у ——													
Demo Ide	entity K	(eystore:				kss	://system/demoi	dentity			The location of	the demo identity ke	ystore. More I	nfo
Demo Ide	entity K	(eystore Ty	ype:			kss					The type of the	e demo identity keysto	ore. Generally, t	his is JKS or KSS.
Demo Ide	entity K	Ceystore Pa	assphrase:			•••	•••••				The demo iden will not be appl	tity keystore's encryp lied. More Info	ted passphrase.	This is readonly
Demo Tru	ust Keys	store:				kss	://system/trust				The location of	the demo trust keyst	ore. More Info	
Demo Tri	ust Keys	store Type				kss					The type of the	e demo trust keystore	Generally, this	is JKS or KSS. 🕴
Demo Tri	ust Key	store Pass	phrase:								The demo trust not be applied.	t keystore's encrypted More Info	passphrase. Th	is is read only an
Java Star	ndard Ti	rust Keyst	ore:			/ho	me/devops/jdk1	8/jre/lib/seci	urity/cacerts	5	The location of	the java standard tru	st keystore. M	ore Info
Java Star	ndard Ti	rust Keyst	ore Type:			jks					The type of the	: java standard trust k	eystore. Genera	Illy, this is JKS.
Jawa Star	dand T	wet Kourt	oro Daccol								The paramord f	for the Java Standard	Truct keyetore	This password is

Java Standard Trust Keystore Passphrase:

• Add the following property in WLS managed server start configuration.

 ${\sf Dweblogic.security.SSL.hostnameVerifier = weblogic.security.utils.SSLWLSWildcardHostnameVerifier = weblogic.security.utils.security.utils.SSLWLSWildcardHostnameVerifier = weblogic.security.utils.security.security.utils.security.utils.security.securits.security.security.security.security.security.security.securit$

Configura	tion	Protocols	Logging	Debug	Monitoring	Control	Deployments	Services	Security	Notes					
General	Cluste	r Service:	s Keystor	res SSL	Federation	Services	Deployment	Migration	Tuning	Overload	Concurrency	Health Monitoring	Server Start	Web Services	Coherence
Save															
Node Ma Manager	nager is will use	a WebLogic to start this	Server utili server on a	ity that you a remote n	u can use to s nachine.	tart, susper	nd, shut down, a	and restart s	ervers in no	ormal or une	xpected conditio	ons. Use this page to o	configure the star	tup settings that	Node
Java Hon	ie:										The Java hom starting this se	e directory (path on t erver. More Info	he machine runni	ing Node Manage	r) to use when
Java Ven	dor:										The Java Vend	dor value to use when	starting this serv	ver. More Info	
BEA Hom	e:										The BEA home starting this se	e directory (path on th erver. More Info	ne machine runni	ng Node Manager) to use when
Root Dire	ctory:										The directory the computer the domain di	that this server uses a that hosts Node Mana rectory is used by def	as its root directo ager. If you do no ault. More Info.	ry. This directory ot specify a Root I 	must be on Directory value,
Class Pat	h:										The classpath	(path on the machine	running Node M	anager) to use w	hen starting
/scrate	ch/obc	dx/config	3:				//				this server.	NOTE INTO			
Argumen	ts:										The argument	s to use when starting	g this server. M	ore Info	
Dobdx.	securi Jwp:tr	ity.disat	oled=tru =dt_sock	e -Dfc et.serv	at.jvm.id	=1 -Xde	bug -Xnoage 9.suspend=r	ent 🔺							
Dobdx.1	neadle	ess.mode	enabled	=true -			s,saspend-r								
Dweblog	<u>sic.se</u> SWildo	ecurity. ardHostr	SSL.host nameVeri	nameVer fier	ifier=web	logic.s	ecurity.uti	lls -							

• Restart OBDX Managed as well as Admin Server.

Enable Headless Mode

• Add the following property to enable Headless mode

-Dobdx.headless.mode.enabled=true

view changes and restarts	L														
Click the Lock & Edit button to modify, add or	Settings for o	odx_server													
Lock & Edit	Configuratio	n Protocols	Logging	Debug	Monitoring	Control	Deployments	Services	Security	Notes					
Release Configuration	General Cl	uster Service	s Keystor	res SSL	. Federation	n Services	Deployment	Migration	Tuning	Overload	Concurrency	Health Monitoring	Server Start	Web Services	Coherence
Domain Structure	Click the Loc	k & Edit button	in the Char	nge Cente	r to modify th	e settings o	on this page.								
bbdx_domain B-Domain Partitions B-Environment D-Deployments B-Services	Save Node Manag Manager wil	er is a WebLogi use to start this	: Server utili server on a	ity that yo a remote i	u can use to : machine.	start, suspe	end, shut down,	and restart s	ervers in no	ormal or une	expected condition	ons. Use this page to	configure the star	rtup settings that	Node
Security Realms Diagnostics	Java Home:										The Java hom starting this s	e directory (path on erver. More Info	the machine runn	ing Node Manage	er) to use whe
	Java Vendor	:									The Java Ven	dor value to use when	n starting this ser	ver. More Info	
	BEA Home:										The BEA hom starting this s	e directory (path on t erver. More Info	he machine runni	ing Node Manage	r) to use whe
How do I Configure startup arguments for Managed	Root Directo	ry:									The directory the computer the domain di	that this server uses that hosts Node Man rectory is used by de	as its root directo ager. If you do no fault. More Info.	ry. This directory ot specify a Root	must be on Directory valu
Servers Start Managed Servers from the Administration Console Shut down a server instance System Status	Class Path: /scratch/	obdx/wls/c	onfig								The classpath this server.	(path on the machin More Info	e running Node M	lanager) to use w	/hen starting
Health of Running Servers							11								
Failed (1) Critical (0) Overloaded (0) Warning (0) OK (1)	Arguments: Dweblogic Dobdx.sec Xnoagent Xrunjdwp: d=n -Dobc	.Stderr=/s urity.disal - transport= x.headless	cratch/o bled=tru dt_socke .mode.en	bdx/wl: e -Dfo t,serve abled=1	s/logs/obc cat.jvm.ic er=y,addre <mark>true</mark>	dx-err.l d=1 -Xde ≳ss=3320	og - Bug - , suspen v				The argument	ts to use when startin	g this server. M	ore Info	
	Security Pol	cy File:									The security p Manager) to u	oolicy file (directory a use when starting this	nd filename on th server. More In	e machine runnin 1fo	ig Node
	User Name:										The user nam	e to use when bootin	g this server. M	ore Info	

• Restart OBDX Managed Server.

4.3.2 OBDX Configurations

Enabling PSD2 on OBDX entity

• Add IDCS Host details in Day-1 Configurations for that entity – (in Other Modules section)

≡ 💋 ZigBank				٩	⊠ ²⁵ () Logout
	Limits Effective from Same Day (Y/N)	Υ	Bank Code		-
	Host Name	UBS	Branch Code		
	Currency Support In Approval Rules	true	Region	INDIA ~	
	Flag to enable SSL	false	Anonymous Security Policy	oracle/wss_username_tol	
	Anonymous Security Key Name	origination_owsm_key	IDCS Host IP	obdx-tenant01.identity.c	
	IDCS Host Port	443	IDCS OBDXClient Id	00fa15d18cd147398ca4	
	IDCS OBDXClient Secret	••••••	IDCS Connection Scheme	https	
	IPM Host password		IPM Host IP address		
	IPM Host application name		IPM Host port		
	IPM Host username				
Previous Next Can	cel				

• In Configurations, navigate to Base Configurations. Search Category: 'extxfaceadapterconfig'

PSD2 Configurations

😤 [OBDX-7710] Payment 🛛 🗙 🔁 ZigBank - ZigBank	x 🗙 🔁 Single Sign-On 🛛 🗙 Service Requ	uest Config: 🗙 🔁 System Configuration - 🗙 🎦 Summary of Servers - 🛇 💆 ZigBank - ZigBank	× ZigBank - ZigBank × 🔁 ZigBank - ZigBank × Ritzgi -	o ×
← → C ③ mum00cag:7780/index.html?mod	dule=configurations&page=categories-home		x 💷 🖬 😁 🚾 📀 🕻	
👯 Apps 📙 yoku 🚖 Bookmarks 📒 OBP2502LZN	08P2502BASE 📃 OBDX17.2 📃 OBDX17.1 🖸 O	racle Applications - 💥 OBDX - Wiki 🗋 ODSM 🥃 Identity Self Service {O OBP25Grok 🗋 SOA-EM	📙 OBP2501USLZN 🌍 Java QR Code Generi 😇 Deque (Java Platform 📙 sonar 🔅 📒 Othe	r bookmarks
	≡ 💋 ZigBank		🔍 🖂 🕫 🔿 Lagout	
	expraceadaptercomig			
			٩.	
	hateoasresourceconfig			
	extxfaceadapterconfig			
	ExtSystemsConfig			
	CredentialConnector			
	DispatchDetails			
	Property Id	Property Value		
	01	ipm1.0,ORACLEBI12.2.1.2	>	
	com.ofss.digx.extxface.payment.ada	$pter. IP ayment Adapter. fetch \\ Deliver Mignex \\ tx face. payment. mock. \\ impl. Payment \\ Mock \\ Adapter \\ mock \\ Mock \\ Adapter \\ mock \\ $	>	
	OBDX_BU2	UB512.4	>	
	OBDX_BU1	UB512.3	>	
	com.ofss.digx.extxface.origination.a	dapter.submission.lending.apphia/Nadigatein/Angigingting/Angiona/Angipasibtah/Angingingingi	ication≱ehicle.OriginationVehicl	
	com ofss digx extyface dda adanter.	DemandDenositAdanter.li ttDire/tDdiritMdmlater. ida.mork.imni.DemandDenositMorkAdanter.	>	
	ORDX RU	118512.4		
	0007_00	VUJ107		

• Search for the entity to enable IDCS adapters

😤 [OBDX-7710] Payment 🛛 🗙 🔁 ZigBank - ZigBank	× Single Sign-On ×	🗶 Service Request Config: 🗙 🧿 System Configuration - 🗴	🕒 Summary of Servers - 🖂 🗙 🔁 ZigBank - ZigBank	× ZigBank - ZigBank	× ZigBank - ZigBank ×	Mind - D X
← → C (i) Not secure mum00cag:7780/inde	ex.html?module=configurations&page	=categories-home			☆ 🔛	🖬 🐵 🖬 🔕 🌼 🗄 E
👯 Apps 📃 yoku 🚖 Bookmarks 📙 OBP2502LZN	CBP2502BASE CBDX17.2	18DX17.1 🧧 Oracle Applications - 🔆 OBDX - Wiki 🗋 ODSI	M 🔁 Identity Self Service {0 OBP25Grok 🗋 SOA-EM	🧧 OBP2501USLZN 🍈 Java QR Co	ode Genera 🧧 Deque (Java Platform	📙 sonar 👒 📔 🛄 Other bookmarks
:	≡ 💋 ZigBank			۹ 🛛	9 ²⁴ O Logout	
	extxfaceadapterconfig			~		
	View/Edit Create					
		Filter Deret				
	0607.60	Pilter Keset				
	Property Id	Property Value				
	01	ipm1.0,ORACLE	BI12.2.1.2	>		
	com.ofss.digx.extxfac	e.payment.adapter.IPaymentAdapter.fetc bDieiUvie ovd ign eev	txface.payment.mock.impl.PaymentMockAdapter	>		
	OBDX_BU2	UBS12.4		>		
	OBDX_BU1	UBS12.3		>		
	com.ofss.dlgx.extxfac	e.origination.adapter.submission.lending.application.dignetic	bd Beigington Vehiolaet epticabrohvehiderbeige pl	ication wehicle. Origination Vehicl		
	com.ofss.digx.extxfac	e.dda.adapter.IDemandDepositAdapter.Ii stEPixo£\$DabgitHe	${\bf txdiatext}$ da.mock.impl.DemandDepositMockAdapter	>		
	OBDX_BU	UB512.4		>		

• View the existing property for editing the same

😤 (OBDX-7710) Payment I 🗙 🧔 Zig8ank - Zig8ank	X 🖸 Single Sign-On X	🗶 Service Request Config: 🗙 🔪 📼 System Configuration - 🙁 🔨 🖺 Summary of Servers - 🗇 🗙 📿 Zigt	Bank - ZigBank 🛛 🗙 🔁 ZigBank - ZigBank 🛛 🗙 🔁	ZigBank - ZigBank 🗙 Nitzij — 🗗 🗙
← → C O Not secure mum00cag:7780/inde	x.html?module=configurations&page=	categories-home		🖈 💷 🗖 😁 🖬 🔕 🔕 😗 🗄
👬 Apps 🧧 yoku 🚖 Bookmarks 📙 OBP2502LZN	🗌 OBP2502BASE 📙 OBDX17.2 📃 OB	DX17.1 🖸 Oracle Applications - 💥 OBDX - Wiki 🗅 ODSM 🥃 Identity Self Service { O OSP25Gro	k 🕒 SDA-EM 📙 OBP2501USLZN 🌍 Java QR Code Gener	🖸 Deque (Java Platform 📒 sonar 🔅 📙 Other bookmarks
:	≡ 💋 ZigBank		ዓ <mark>8</mark> ኛ ሮ	Logout
	extxfaceadapterconfig		~	
	View/Edit Create			
	OBDX_BU	Filter Reset		
	Property Id OBDX_BU	Property Value UBS12.4	~	
	Property Id	OBDX, BU		
	Property Value	UB\$12.4		
	Edit	Delete		
	Back	Page 1 of1 (lof1Rems) $K \in 1$ > 3		

• Edit the property. Add appropriate IDCS Adapters. - 'idcs1736' for OBDX 18.1

> C () Not secure mum00cag:7780/index.html?module=	=configurations&page=categories-home E 📙 OBDX17.2 📙 OBDX17.1 🔁 Oracle Application	ns - 💥 OBDX - Wiki 🎦 ODSM 🥃 Identity Self Service [O OBP25Grok []) SOA-EM 📙 OBP2501USLZN 🌒 Java QR C	ode Genera 😇 Deque (Java Platform 📒 sonar 😕 📋 Other bookma
≡ 💋	ZigBank		ଦ୍ ଜ	e O Logout
extxfaceadapt	terconfig		~	
View/Edit	Create			
	OBDX_BU	Filter Reset		
	Property Id	Property Value		
	OBDX_BU	UBS12.4	~	
	Property Id OBDX_BU			
	Property Value UBS12.4.dcs1736			
	Save Changes Cancel Reset	l		
,	Back	Page 1 of 1 (lofiltems) K < 1 > X		

• Restart OBDX Managed Server.

<u>Home</u>

5. Third Party Application Registration

5.1 Registering a Third Party Browser Client in IDCS

- Log into the IDCS dashboard.
- Click on the "Applications" tab which will list all applications associated with the logged in account.

Identity Cloud Service	Home	Users	Groups	Applications	Jobs	Settings	Security	
Welcome admin@o	racle.cc	e e	What's	New	Here's wha Onbo Onbo Audit Grou Mana	t you can do: parding Users parding Appli ing the Syste ps nging Security	and Groups cations m, Users, and [,] Settings	 Performing Self-Service Diagnostics Customizing the Service Performing End-User Self Service
Filter by Date Range Last 30 Days	•							

• Click add in the application tab to register a browser client.

Identity	Cloud Service	Home	Users	Groups	<u>Applications</u>	Jobs	Settings	Security			
Applicatio	ons										Q
Select All + Ac	dd X Remove Create an applica Client	Activa tion.	ate 🖉 D	leactivate						0	Ξ
	Demo App Mobile Application	plication								Ø	Ξ
• <u>m</u>	Elite Acco For PSD2 Demo -	unts ^{BOV}								Ø	Ξ
• 👷	Elite Acco Dummy App 1 for	unts - Ap PSD2 implement	p1 tation							Ø	Ξ
	Elite Acco For Demo Purpose	unts - De	mo							0	Ξ
	Elite Paym For PSD2 Demo -	nents BOV								Ø	Ξ
•	Elite Paym Third Party App in	nents - Ap	op2 or PSD2.							Ø	Ξ

• Select 'Trusted Application'.

Add Applic	ation		×
0	App Catalog	Add an application from the Application Catalog.	-
	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.	
•	Trusted 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.	

• Add 'Name' and 'Description'.

Cancel	C	• Details	-	Client	Re	esources	Authorization	Next 📏
App Details								
			* Name Tru:	sted demo				
		De	cription We	b Application				
						4		
		Applicat	ion Icon	3				
			C	0				
			Up	bload				
		Applica	ion URL					
		Lo	gin URL					
		Logout P	age URL					
Tags								
	ins to organize and id	entify them. A	tao consists o	f a key-value pair.				

• Check 'Authorization Code' option as the 'Allowed Grant Type'. Configure the 'Redirect URL' of the application.

< Back	Details Client Resources Authorization
	Configure this application as a client now O Skip for later
Authorization	n
	Allowed Grant Types 📄 Resource Owner 📄 Client Credentials 📄 JWT Assertion 📄 SAML2 Assertion 📄 Refresh Token 📝 Authorization Code
	Implicit Device Code
	Allow non-HTTPS URLs 🗹
	* Redirect URL http://www.example.com/redirect
	Logout URL
	Post Logout Redirect URL
	Security Trusted Client Certificate Import
	Allowed Operations Interconect On hebalf Of
Accessing API	is from Other Applications
	Trust Scope 0 All resources
	Allowed tags Allowed scopes
Allo	wed Tags
+	Add Tag
Allo	wed Scopes
+	Add X Remove
	Application Allowed Scope

• Configure Access Token Expiration, Refresh Token properties as per bank policy

Register Resources	No resources
Configure application APIs that	need to be OAuth protected.
Access Token Expiration	n 3,600 v A seconds
Is Refresh Token Allowed	d 🖬
Refresh Token Expiration	n 604,800 v 🔨 seconds
Primary Audience	e http://mum00apb:7771/digx/v1/
Secondary Audiences	s Add
Secondary	Audience Remove
No data to di	isplay.
Allowed Scope:	s Add Remove
Scope	Description Requires Consent
No data to di	isplay.

Application Added.

Add Truste	ed Application				
< Back	O Details	Client	Resources	Authorization	Finish
Authorization					Click to add this applica
	Enforce Grants as Authorizati	on 🗆			

Application Added									
Below is the new CI This information als the application.	ient ID and Client Secret for your application. o appears on the Configuration tab in the Details section for								
Client ID	d095c8410e424988829277e998295a9e								
Client Secret	fb2a3a1e-726e-4b3b-a310-9d130212e3b9								
	Close	2							

• Click on "Activate" to activate the application.

5.2 Registering a Third Party Mobile Client in IDCS

- Log into the IDCS dashboard.
- Click on the "Applications" tab which will list all applications associated with the logged in account.

Identity Cloud Service	Home	Users	Groups	Applications	Jobs	Settings	Security	
Welcome admin@o	r acle.co earn More	e e	What's	H	lere's wha • Onbo • Onbo • Audit Grou • Mana	t you can do: parding Users parding Applid ing the Syste ps nging Security	and Groups cations m, Users, and ^y Settings	 Performing Self-Service Diagnostics Customizing the Service Performing End-User Self Service
Filter by Date Range Last 30 Days	•							

• Click on the "Add" button to create a new application

6	Identity Cloud Service	Home	Users	Groups	Applications	Jobs	Settings	Security			
Applic	cations									٩	
Select All	+ Add X Remove	Activa	te 🖉 🛙	Deactivate							
• <[Client								0	Ξ	
• <u>I</u>	Elite Accou	ints ov							•	Ξ	
	Elite Accou	I <mark>nts - Ap</mark> SD2 implement	p1 ation						•	Ξ	
• 4	Elite Accou	ints - De	mo						•	Ξ	
• 4	Elite Payme	ents ov							Ø	Ξ	

Select Mobile Application

Add Applic	ation		×
0	App Catalog	Add an application from the Application Catalog.	
	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.	
•	Trusted 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.	

• Enter the name and description.

	-			
Cancel	Details	Client	Authorization	Next >
App Details				
	* Name	Demo Application		
	Description	Mobile Application		
	Application Icon			
		Upload		
	Login URL			
	Logout Page URL			

• Select 'Authorization Code' as Allowed Grant Types. Configure Redirect-URL as per your choice. The client application should listen to this URL when IDCS redirects on this URL with Authorization code.

< Back	O Deta	ils	Cli	ent .	Authorization			Next >
Authorization								
А	Allowed Grant Types	Resource Owner	Client Credentia	ils 🔲 JWT Assertio	SAML2 Assertion	Refresh Token	 Authorization Code 	
Allo		Implicit 🔲 Dev	ce Code					
	* Redirect URL ps	d2://redirect						
	Logout URL							
Post L								
	Logout Redirect URL							
	Allowed Operations	Introspect 🔲 C	n behalf Of					
Accessing APIs from	Allowed Operations	Introspect 🛛 C	n behalf Of					
Accessing APIs from	Allowed Operations	Introspect 🛛 C	n behalf Of					
Accessing APIs from Allowed Tags	Allowed Operations	Introspect C	n behalf Of					
Accessing APIs from Allowed Tags + Add Tag	Allowed Operations	introspect 🛛 C	n behalf Of					
Accessing APIs from Allowed Tags + Add Tag	Allowed Operations	Introspect C	n behalf Of					
Accessing APIs from Allowed Tags + Add Tag Allowed Scop	Allowed Operations	Introspect C	n behalf Of					
Accessing APIs from Allowed Tags + Add Tag Allowed Scop + Add	Allowed Operations	Introspect C	n behalf Of					
Accessing APIs from Allowed Tags + Add Tag Allowed Scop + Add	Allowed Operations	introspect C	n behalf Of	Allowed S	00e			

• Click on Finish to complete the process.

Identity Cloud Service	Home	Users	Groups	Applications	Jobs	Settings	Security		
Add Mobile App	licatio	n							
< Back		O Details		(O Ilient		Auti	• thorization	Finish
Authorization									
	Enforce Gra	ints as Autho	rization 🗐						

• Client ID is generated for the application. As this application is not a 'Trusted Application', Client-Secret is not generated for the application.



• Click on "Activate" to activate the application.

5. View and Manage Consents in OBDX

5.3 Manage Consent in OBDX

• Login with Channel User. Select 'Manage Third Party Consents' from the menu.



Consent Management Screen for Third party Consents

≡ 💋ZigBank	Dashboard	Trends	Payments	٩	
Manage Third Party Con	sents				
Elite Payments - App2	Revoke				
Elite Accounts	Revoke				
Ok					

5.4 PSD2 Offerings and Modules

Bellow describes the PSD2 API Offerings and Modules

Modules: Below are the modules on which OPEN APIs are being build

Customer	Accounts	Deposits
Loans	Credit Cards	Pay to own accounts
Pay within the bank	Pay within EU	Make an international payment
Trusted beneficiaries	Payment Information (Verify and Confirmation)	Authentication

APIS, Usage and Module

APIUSAGE	Module		
Show Payment debit and delivery time	Account		
Fetch account balance	Accounts		
Validate account balance sufficiency	Accounts		
Fetch account financial summary	Accounts		
Fetch account movements	Accounts		
Fetch Direct Debits	Accounts		
Fetch Standing Instructions/orders	Accounts		
Fetch debit card details	Accounts		
Fetch debit card details	Accounts		
Show Posting Third Party Details in Narration/Remarks	Accounts		
Mutual TLS, OAuth 2.0 and Open ID Connect	Authentication		
Add Third Party Access Grants	Authorization		
Delete Third Party Access Grants	Authorization		
Disable Third Party Access Grants	Authorization		
Fetch current financial situation of a card	Credit Cards		

APIUSAGE	Module			
Fetch card status	Credit Cards			
Fetch party information	Customer			
Fetch party to party relationship	Customer			
Fetch all accounts of the party and nick name	Customer			
Fetch deposit balance	Deposits			
Fetch deposit financial summary	Deposits			
Fetch movements in the deposit	Deposits			
Fetch loan financial summary	Loans			
Fetch schedule details	Loans			
Fetch payment details	Make an international payment			
Fetch payment status	Make an international payment			
Make a payment	Make an international payment			
Make mass payment	Make an international payment			
Cancel a payment	Make an international payment			
Fetch payment details	Pay to own accounts			
Fetch payment status	Pay to own accounts			
Make a payment	Pay to own accounts			
Make mass payment	Pay to own accounts			
Cancel a payment	Pay to own accounts			
Fetch payment details	Pay within EU			
Fetch payment status	Pay within EU			
Make a payment	Pay within EU			
Cancel a payment	Pay within EU			
Fetch payment details	Pay within the bank			
Fetch payment status	Pay within the bank			

API USAGE	Module
Make a payment	Pay within the bank
Make mass payment	Pay within the bank
Cancel a payment	Pay within the bank
Unique Identifier	Payment Information (Verify and Confirmation)
Charges	Payment Information (Verify and Confirmation)
Exchange Rate	Payment Information (Verify and Confirmation)
Payment reference	Payment Information (Verify and Confirmation)
Amount	Payment Information (Verify and Confirmation)
Initiation and Value Dates	Payment Information (Verify and Confirmation)
Fetch beneficiaries by account	Trusted beneficiaries
Fetch beneficiaries by type of payment	Trusted beneficiaries

<u>Home</u>