

Oracle Banking Digital Experience

PSD2 Guide

Release 18.1.0.0.0

Part No. E92727-01

January 2018

ORACLE®

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. Preface	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. Purpose	5
3. Topology	6
4. PSD2 Configurations	7
4.1 IDCS Configuration	7
4.2 APICS Configurations	11
4.3 OBDX Configurations	14
5. Third Party Application Registration	26
5.1 Registering a Third Party Browser Client in IDCS	26
5.2 Registering a Third Party Mobile Client in IDCS	30
5. View and Manage Consents in OBDX	34
5.3 Manage Consent in OBDX.....	34
5.4 PSD2 Offerings and Modules.....	35

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

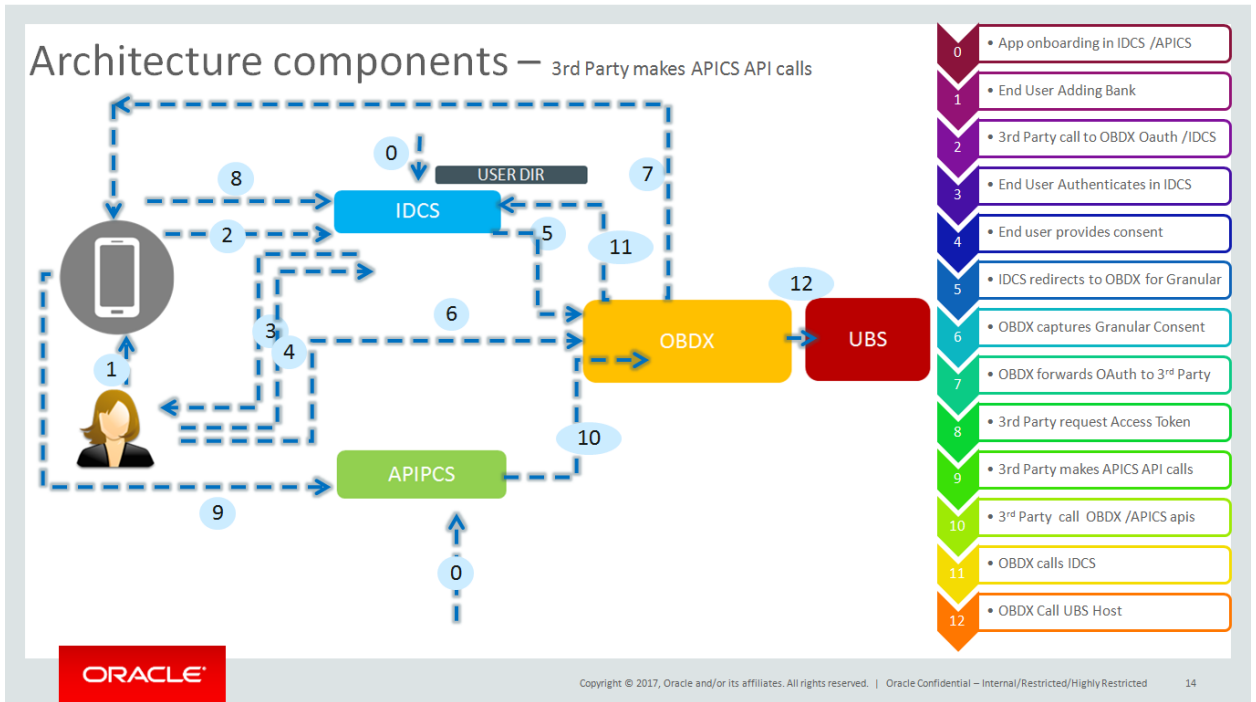
This document provides step by step guide to configure OBDX for PSD2 implementation.

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



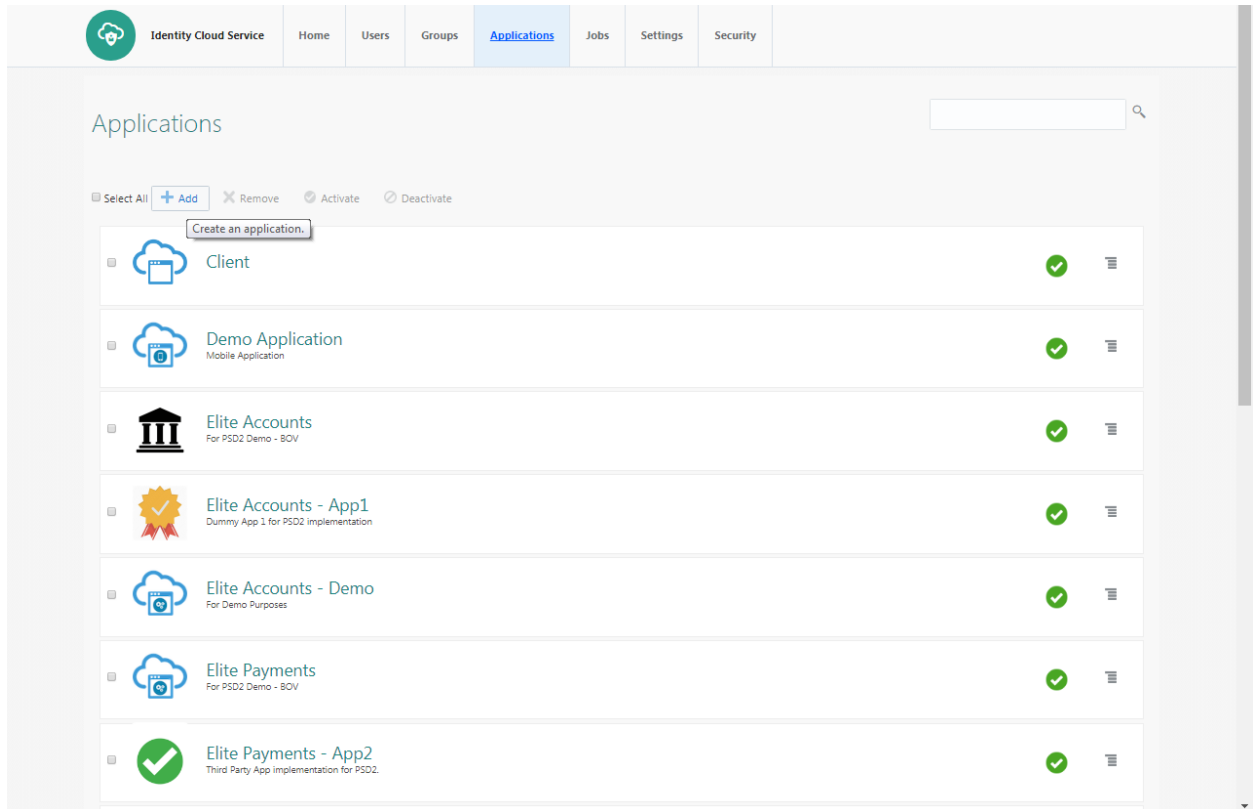
[Home](#)

4. PSD2 Configurations

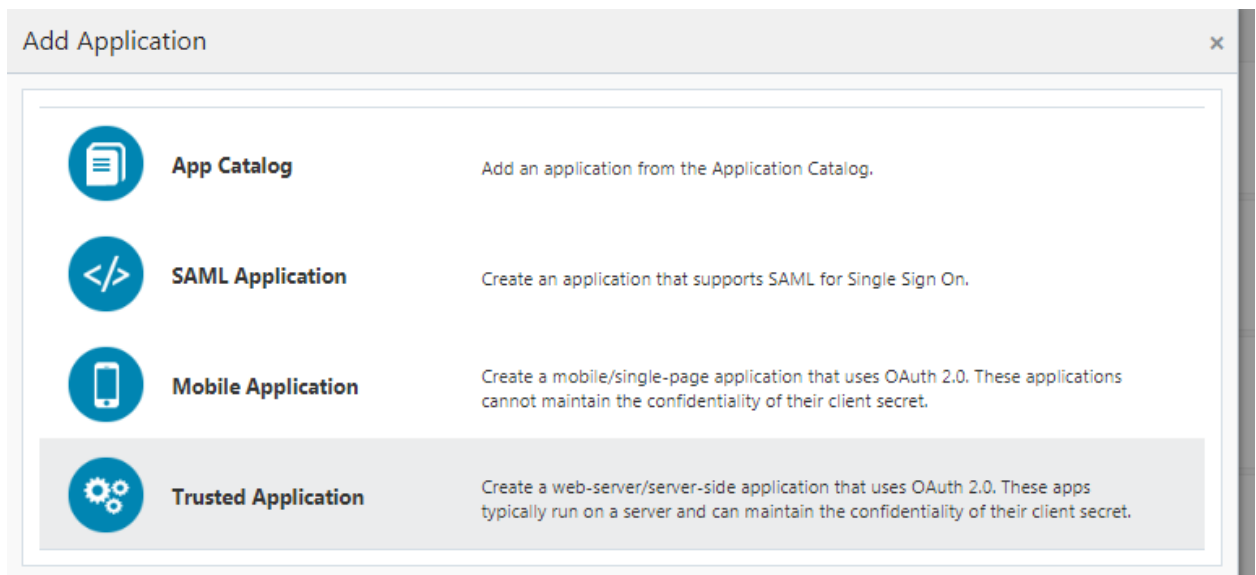
4.1 IDCS Configuration

a) Registering OBDX as an Admin application in IDCS

- Click add in the application tab to register OBDX Admin application.



- Select trusted application



- Add “name” and “description”

The screenshot shows the 'Add Trusted Application' wizard in the Identity Cloud Service console. The wizard is currently on the 'App Details' step, which is highlighted in the progress bar. The 'App Details' section contains the following fields:

- Name:** A text input field containing 'Trusted demo'.
- Description:** A text area containing 'Web Application'.
- Application Icon:** A preview of a blue cloud icon with a white 'X' and a blue 'X' inside, with an 'Upload' button below it.
- Application URL:** An empty text input field.
- Login URL:** An empty text input field.
- Logout Page URL:** An empty text input field.

The 'Tags' section below the 'App Details' section contains the text: 'Add tags to your applications to organize and identify them. A tag consists of a key-value pair.' and a '+ Add Tag' button.

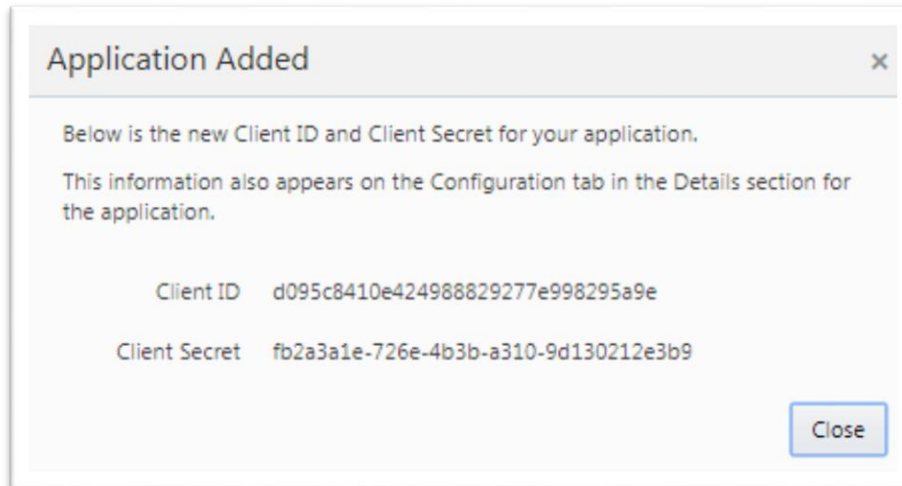
The 'Display Settings' section at the bottom contains two checkboxes:

- Display in My Apps
- User can request access

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

- Add Admin Privileges for OBDX Client Configuration

- Application added



- 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.

The screenshot shows the 'Session Settings' configuration page in the ZigBank Identity Cloud Service. The page includes the following fields and controls:

- Session Expiry:** A numeric input field containing '480' with up and down arrow icons and the unit 'minutes'.
- Login URL:** A text input field containing '/ui/v1/signin'.
- Logout URL:** A text input field containing '/ui/v1/myconsole'.
- Allow Cross-Origin Resource Sharing (CORS):** A toggle switch that is currently turned on (blue).
- Allowed CORS Domain Names:** A text area containing 'mum00apt.in.oracle.com'.

Buttons for 'Save' and 'Cancel' are located in the top right corner.

- Page to set session token timeout and custom login URL

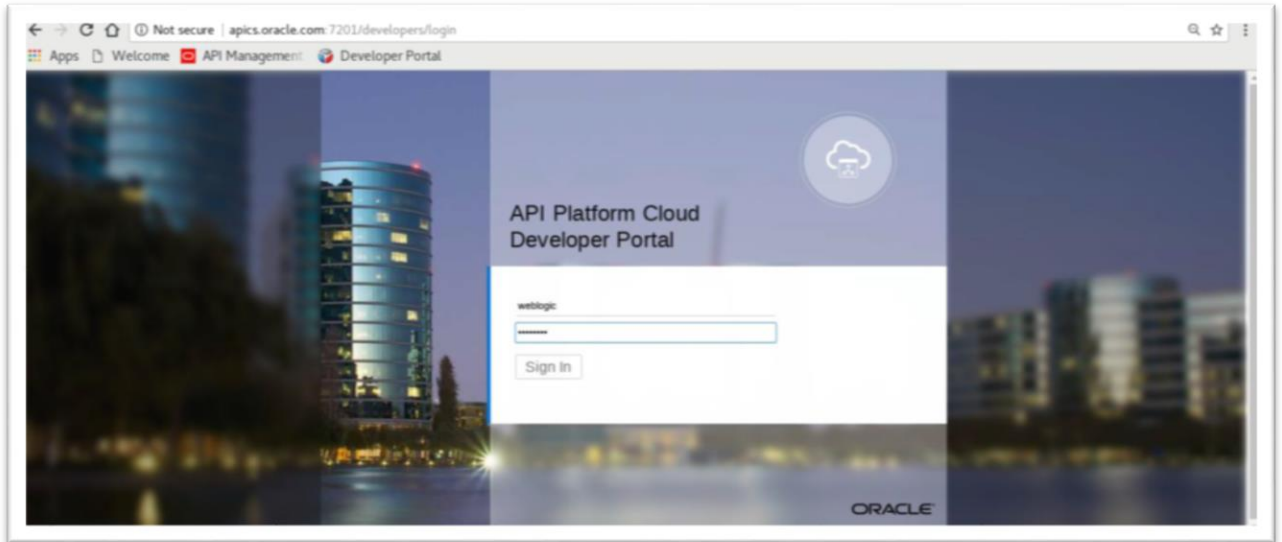
This screenshot shows the 'Session Settings' page with a custom Login URL. The fields and controls are:

- Session Expiry:** 480 minutes.
- Login URL:** http://mum00apb.in.oracle.com:7778/p
- Logout URL:** /ui/v1/myconsole
- Allow Cross-Origin Resource Sharing (CORS):** Toggle is on.
- Allowed CORS Domain Names:** mum00apb.in.oracle.com

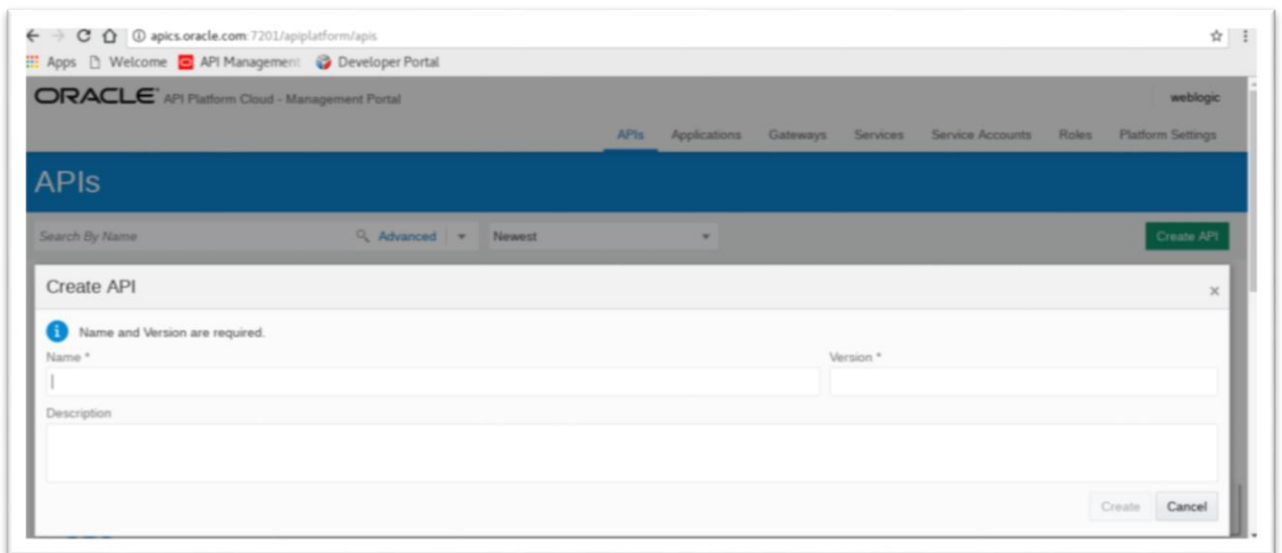
'Save' and 'Cancel' buttons are present in the top right.

4.2 APICS Configurations

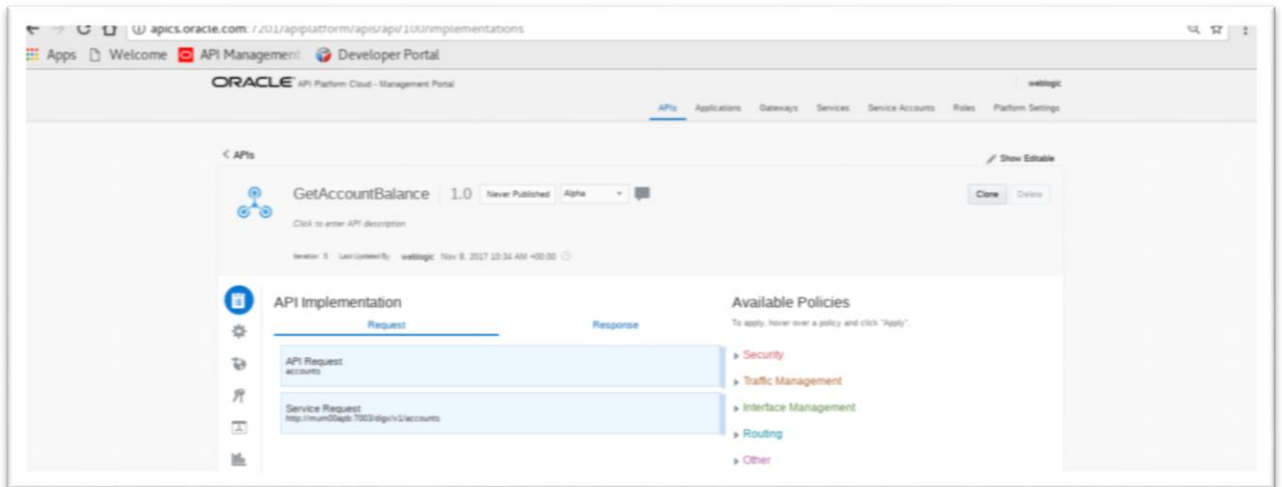
- Login to APICS



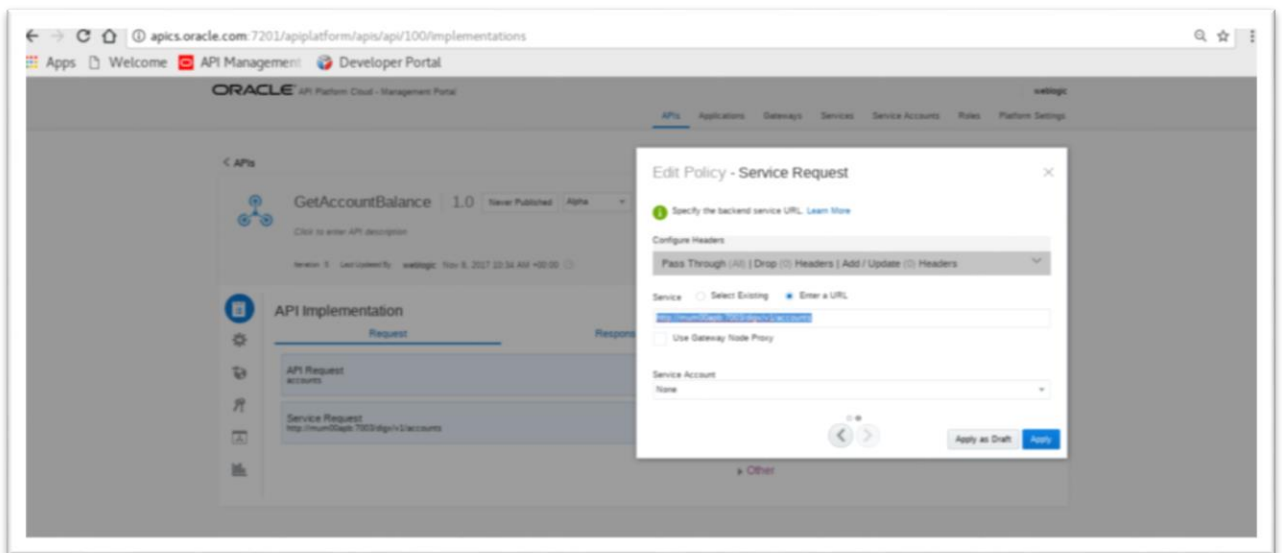
- Create API



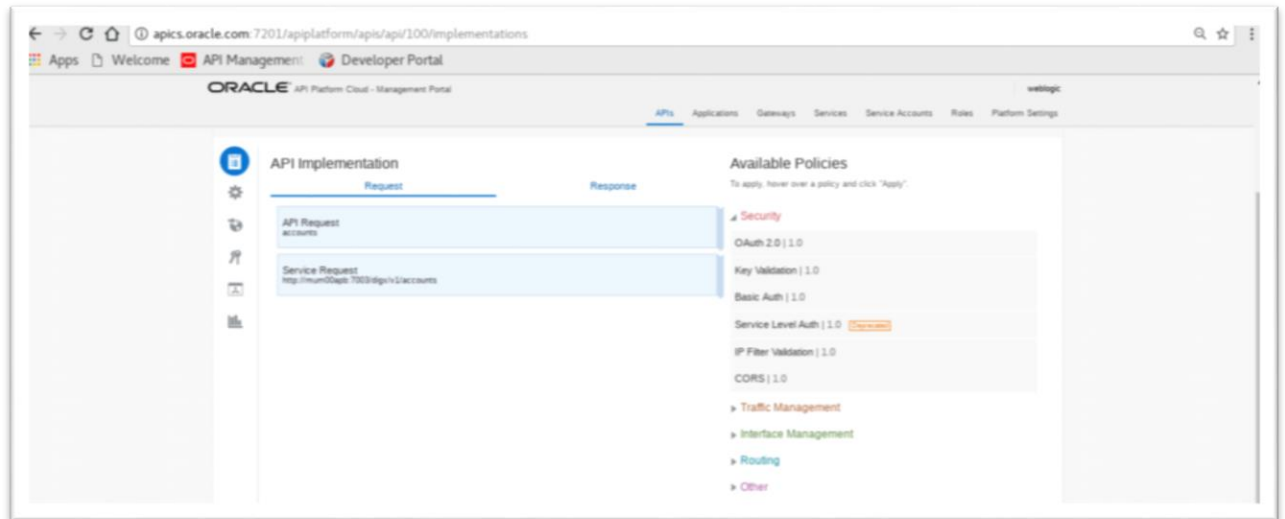
- API Implementation



- Edit Policy



- View API Summarizing



4.3 OBDX Configurations

4.3.1 WebLogic Configurations

Patch WLS12.2.1.2.

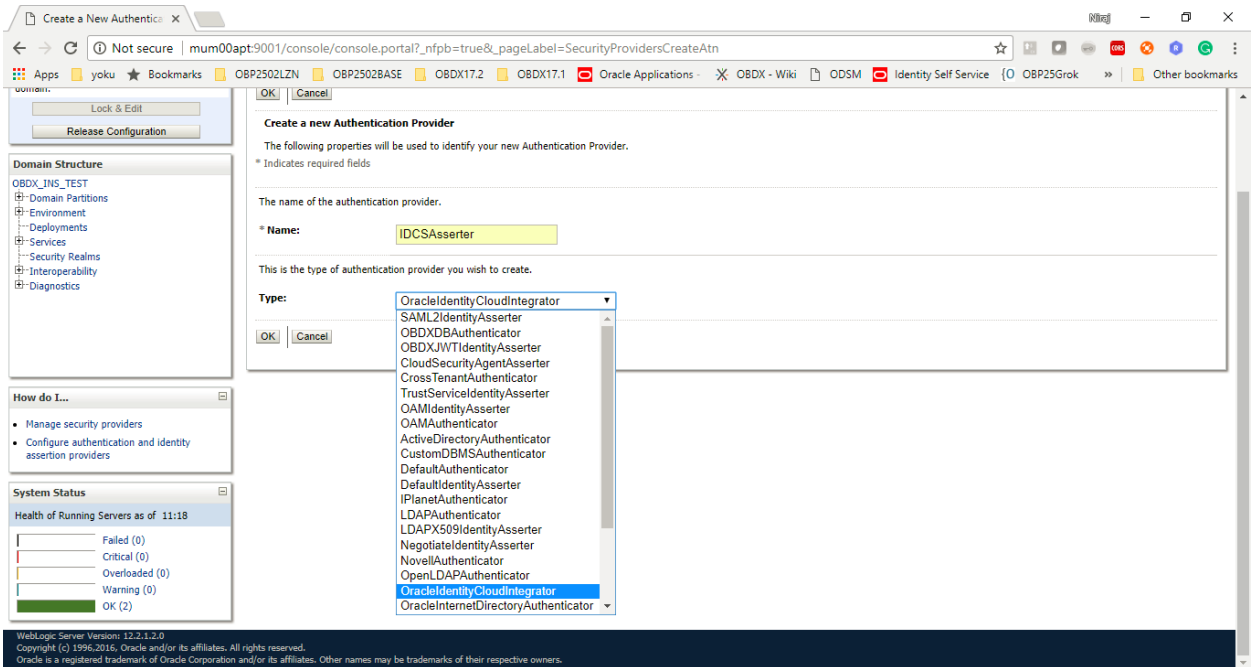
- WLS 12.2.1.2.0 (PS2 PSU) Obtain and install the WLS 12.2.1.2.0 kit from OTN:

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 asseter

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



- Click 'OK'



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

The screenshot displays the Oracle WebLogic Server Administration Console interface. The top navigation bar includes 'ORACLE WebLogic Server Administration Console 12c' and user information 'Welcome, weblogic Connected to: obdx_domain'. The left sidebar contains several panels: 'Change Center' with 'Lock & Edit' and 'Release Configuration' buttons; 'Domain Structure' showing a tree view of the domain hierarchy; 'How do I...' with 'No task help found.'; and 'System Status' showing the health of running servers with a bar chart for Failed (1), Critical (0), Overloaded (0), Warning (0), and OK (1) states.

The main content area is titled 'Settings for IDCSAsserter' and is divided into 'Configuration' and 'Provider Specific' tabs. The 'Configuration' tab is active, showing a 'Save' button at the top. Below it, a message states: 'Click the *Lock & Edit* button in the Change Center to modify the settings on this page.' This is followed by another 'Save' button and a note: 'This page allows you to define the general configuration of this provider.'

The configuration details include:

- Name:** IDCSAsserter
- Description:** Provider that performs identity assertion for Oracle Identity Cloud Service tokens
- Version:** 1.0
- Active Types:**
 - Available:** Idcs_user_assertion, REMOTE_USER, idcs_user_assertion
 - Chosen:** Authorization (highlighted in yellow)
- Base64 Decoding Required:** false

 At the bottom of the configuration section, there is another 'Save' button and a final message: '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 [Step 4.1.a](#) in fields Client Id and Client Secret & Confirm Credentials. Fill in other marked properties as per the IDCS host.

Settings for IDCSasserter

Configuration

Common **Provider Specific**

Click the *Lock & Edit* button in the Change Center to modify the settings on this page.

Save

This page allows you to configure additional attributes for this security provider.

Audience Enabled

JSONWeb Key Set URI:

Sync Filter Match Case

Token Validation Level:

Port:

Cache Enabled

Tenant Names:

Client IDToken Claim:

Base Path:

Token Clock Skew:

Tenant Token Claim:

Any Identity Domain Enabled:

User Name Resource Attribute:

Tenant Host Name Template:

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

Sync Filter Enabled

Issuer:

Sync Filter Only Client Cert Requests

Tenant:

Thread Lock Timeout:

Token Virtual User Allowed

Connect Timeout:

Response Read Timeout:

Tenant Data Reload Interval:

Host:

App Name Filter Header Name:

Client Name Token Claim:

Cache Size:

Client As User Principal Enabled

Sync Filter Prefer Header

Client Secret:

Confirm Credential:

Client Tenant Token Claim:

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 > Summary of Servers > OBDX_INS1

Settings for OBDX_INS1

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services **Keystores** SSL Federation Services Deployment Migration Tuning Overload Concurrency Health Monitoring Server Start Web Services

Click the *Lock & Edit* button in the Change Center to modify the settings on this page.

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help manage the security of message transmissions.

Keystores:	Demo Identity and Demo Trust	Change	Which configuration rules should be used for finding the server's identity keystores? More Info...
Identity			
Demo Identity Keystore:	kss://system/demoidentity		The location of the demo identity keystore. More Info...
Demo Identity Keystore Type:	kss		The type of the demo identity keystore. Generally, this is JKS or KSS.
Demo Identity Keystore Passphrase:		The demo identity keystore's encrypted passphrase. This is read only and will not be applied. More Info...
Trust			
Demo Trust Keystore:	kss://system/trust		The location of the demo trust keystore. More Info...
Demo Trust Keystore Type:	kss		The type of the demo trust keystore. Generally, this is JKS or KSS. More Info...
Demo Trust Keystore Passphrase:			The demo trust keystore's encrypted passphrase. This is read only and not be applied. More Info...
Java Standard Trust Keystore:	/home/devops/jdk18/jre/lib/security/cacerts		The location of the java standard trust keystore. More Info...
Java Standard Trust Keystore Type:	jks		The type of the java standard trust keystore. Generally, this is JKS. More Info...
Java Standard Trust Keystore Passphrase:			The password for the Java Standard Trust keystore. This password is c

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

Dweblogic.security.SSL.hostnameVerifier=weblogic.security.util.SSLWLSWildcardHostnameVerifier

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload Concurrency Health Monitoring **Server Start** Web Services Coherence

Save

Node Manager is a WebLogic Server utility that you can use to start, suspend, shut down, and restart servers in normal or unexpected conditions. Use this page to configure the startup settings that Node Manager will use to start this server on a remote machine.

Java Home: The Java home directory (path on the machine running Node Manager) to use when starting this server. [More Info...](#)

Java Vendor: The Java Vendor value to use when starting this server. [More Info...](#)

BEA Home: The BEA home directory (path on the machine running Node Manager) to use when starting this server. [More Info...](#)

Root Directory: The directory that this server uses as its root directory. This directory must be on the computer that hosts Node Manager. If you do not specify a Root Directory value, the domain directory is used by default. [More Info...](#)

Class Path: The classpath (path on the machine running Node Manager) to use when starting this server. [More Info...](#)

Arguments: The arguments to use when starting this server. [More Info...](#)

- Restart OBDX Managed as well as Admin Server.

Enable Headless Mode

- Add the following property to enable Headless mode
-Dobdx.headless.mode.enabled=true

The screenshot shows the 'Settings for obdx_server' page in the Oracle WebLogic Administration Console. The 'Server Start' tab is selected, and the 'Arguments' field contains the following text:

```
Dweblogic.Stdout=/scratch/obdx/wls/logs/obdx-err.log -
Dobdx.security.disabled=true -Dfcacat.jvm.id=1 -Xdebug -
Xnoagent -
Xrunidup:transport=dt_socket,server=y,address=3320,suspend=n
-Dobdx.headless.mode.enabled=true
```

The 'Health of Running Servers' section shows the following status:

Health	Count
Failed	1
Critical	0
Overloaded	0
Warning	0
OK	1

- Restart OBDX Managed Server.

4.3.2 OBDX Configurations

Enabling PSD2 on OBDX entity

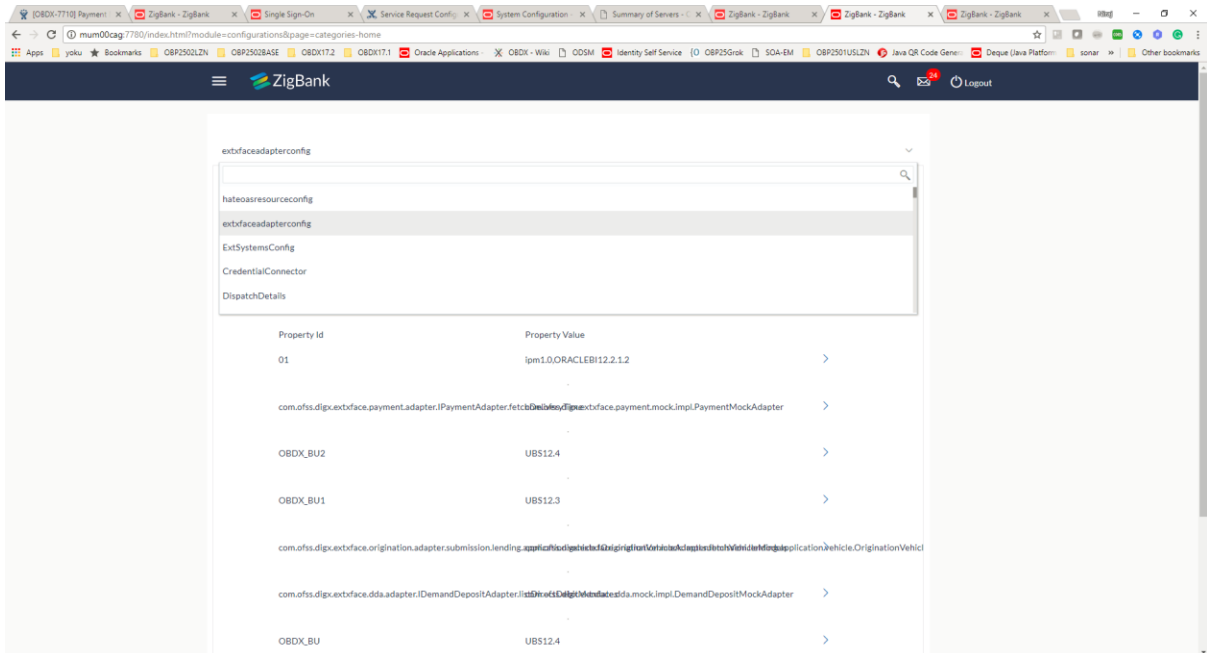
- Add IDCS Host details in Day-1 Configurations for that entity – (in Other Modules section)

The screenshot shows the ZigBank configuration interface for OBDX. The header includes the ZigBank logo, a search icon, a notification icon with '25', and a Logout button. The main content area is a configuration form with the following fields:

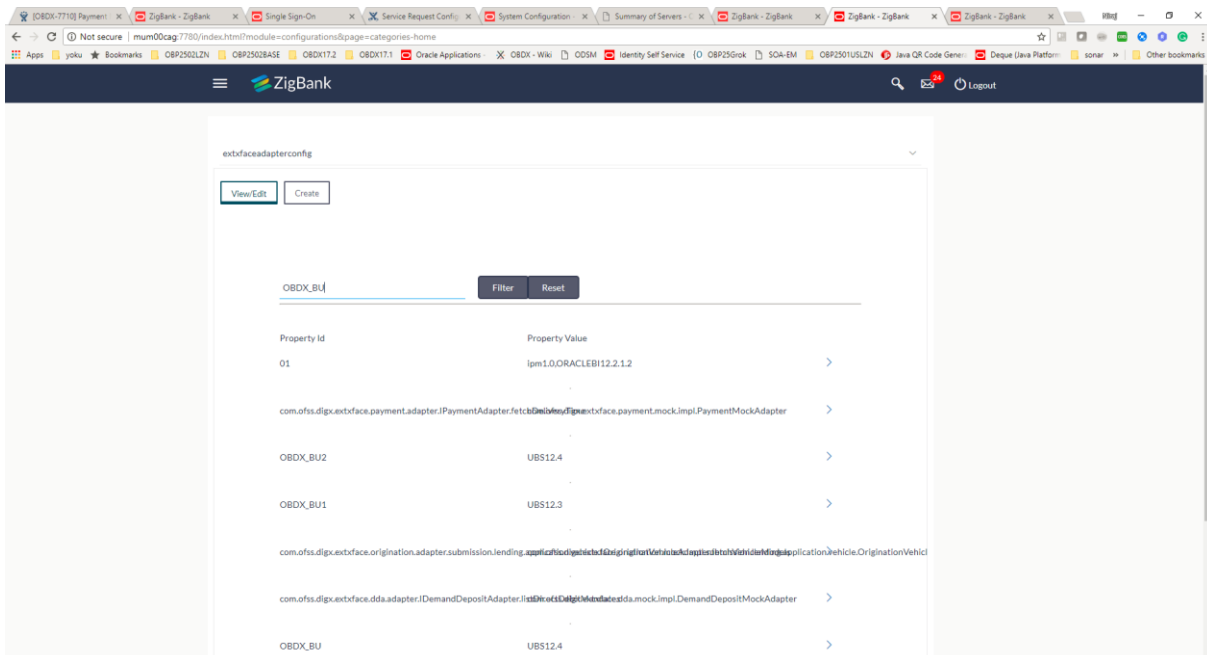
Limits Effective from Same Day (Y/N)	Y	Bank Code	
Host Name	UBS	Branch Code	
Currency Support In Approval	true	Region	INDIA
Rules			
Flag to enable SSL	false	Anonymous Security Policy	oracle/wss_username_tol
Anonymous Security Key Name	origination_owsm_key	IDCS Host IP	obdx-tenant01.identity.c
IDCS Host 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			

At the bottom of the form, there are three buttons: Previous, Next, and Cancel.

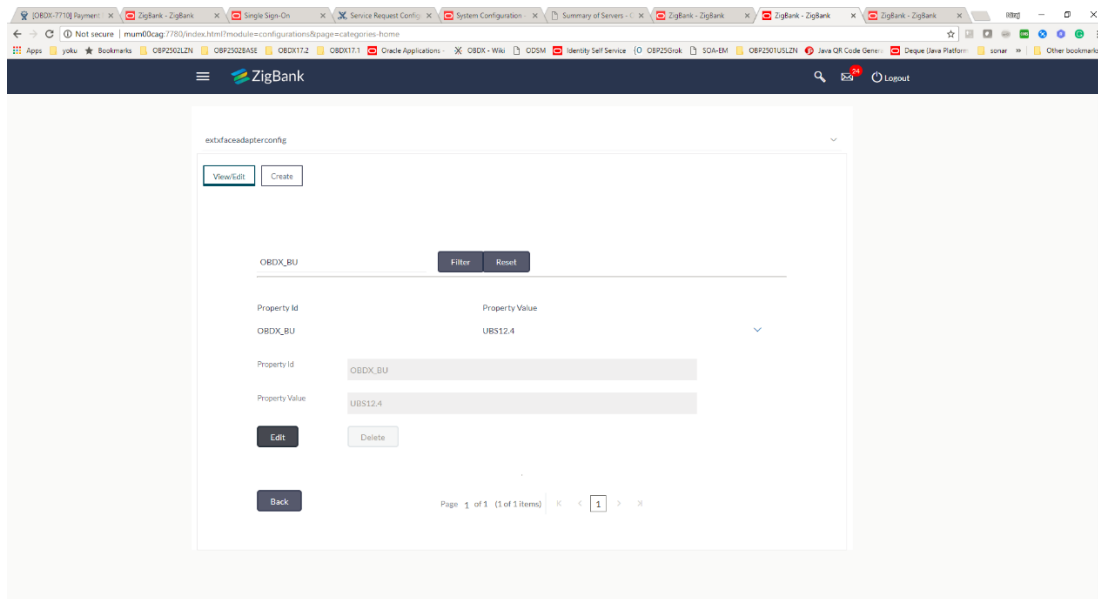
- In Configurations, navigate to Base Configurations. Search Category: 'extxfaceadapterconfig'



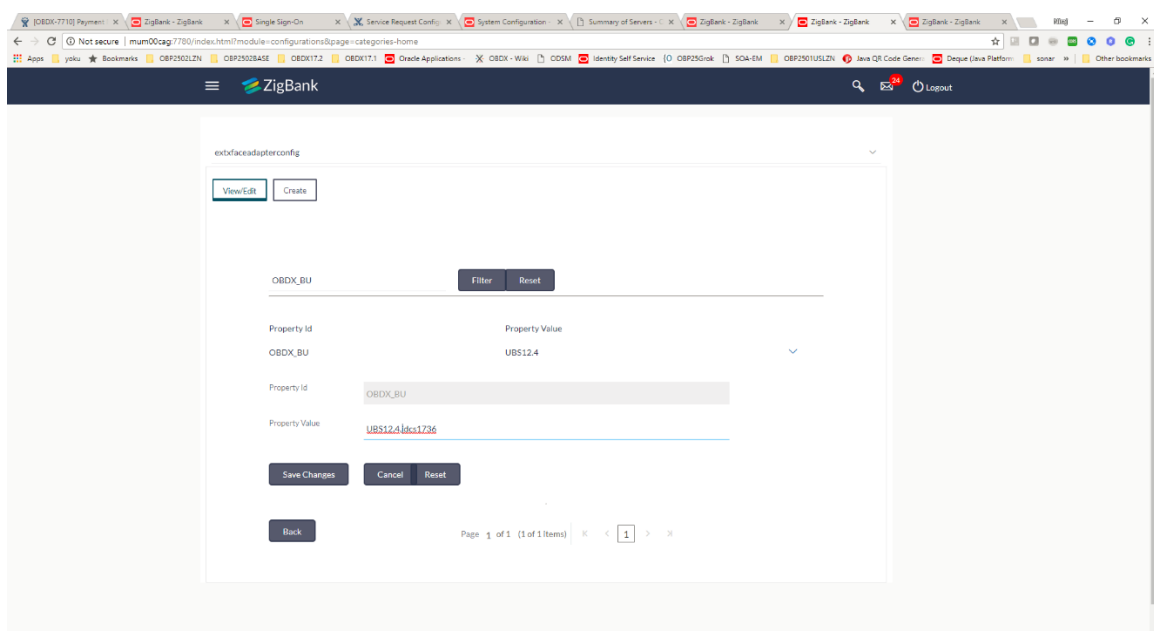
- Search for the entity to enable IDCS adapters



- View the existing property for editing the same



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



- Restart OBDX Managed Server.

[Home](#)

5. Third Party Application Registration

5.1 Registering a Third Party Browser Client in IDCS

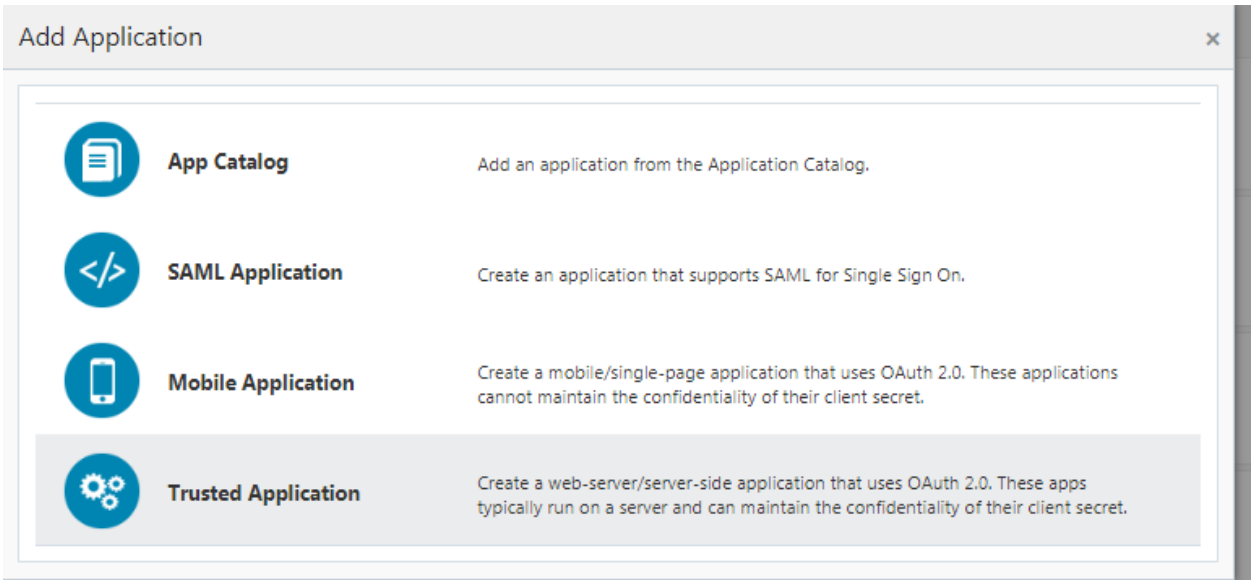
- Log into the IDCS dashboard.
- Click on the “Applications” tab which will list all applications associated with the logged in account.

The screenshot shows the Identity Cloud Service dashboard. The top navigation bar includes the Oracle logo, 'Identity Cloud Service', and tabs for 'Home', 'Users', 'Groups', 'Applications', 'Jobs', 'Settings', and 'Security'. The 'Home' tab is selected. Below the navigation bar is a green banner with the text 'Welcome admin@oracle.com'. To the right of the banner, it says 'Here's what you can do:' followed by a list of actions: 'Onboarding Users and Groups', 'Onboarding Applications', 'Auditing the System, Users, and Groups', 'Managing Security Settings', 'Performing Self-Service Diagnostics', 'Customizing the Service', and 'Performing End-User Self Service'. Below the banner are three buttons: 'Watch the Video', 'Learn More', and 'What's New'. At the bottom left, there is a 'Filter by Date Range' dropdown menu set to 'Last 30 Days'.

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

The screenshot shows the 'Applications' page in the Identity Cloud Service dashboard. The top navigation bar is the same as in the previous screenshot, but the 'Applications' tab is selected. Below the navigation bar, the page title is 'Applications' with a search bar on the right. Below the title, there are controls: 'Select All', '+ Add', 'Remove', 'Activate', and 'Deactivate'. A tooltip 'Create an application.' is visible over the '+ Add' button. The main content area displays a list of applications, each with a checkbox, an icon, the application name, a description, a status indicator (green checkmark), and a menu icon. The applications listed are: 'Client', 'Demo Application (Mobile Application)', 'Elite Accounts (For PSD2 Demo - BOV)', 'Elite Accounts - App1 (Dummy App 1 for PSD2 implementation)', 'Elite Accounts - Demo (For Demo Purposes)', 'Elite Payments (For PSD2 Demo - BOV)', and 'Elite Payments - App2 (Third Party App Implementation for PSD2)'.

- Select 'Trusted Application'.

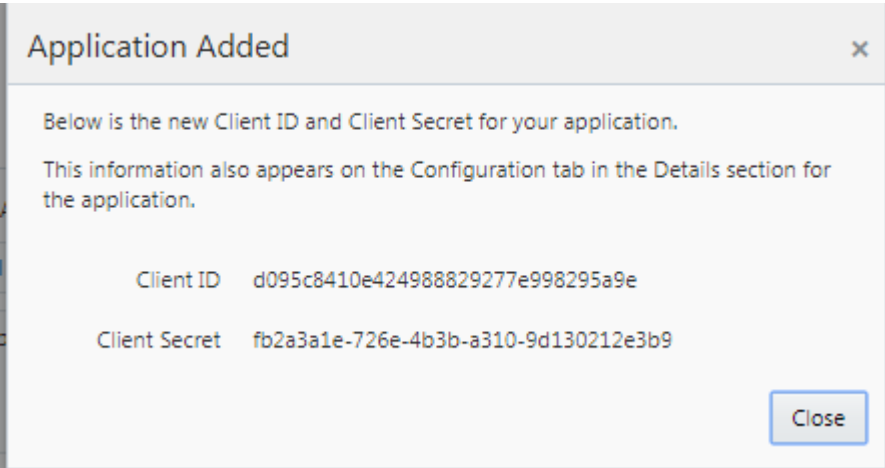
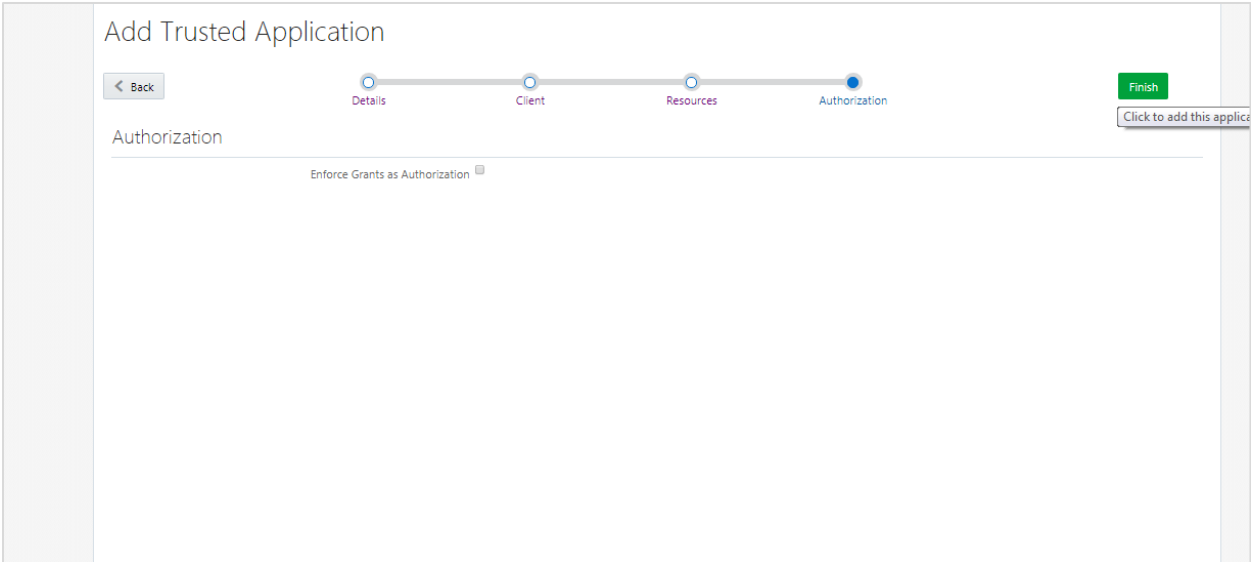


- Add 'Name' and 'Description'.

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

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

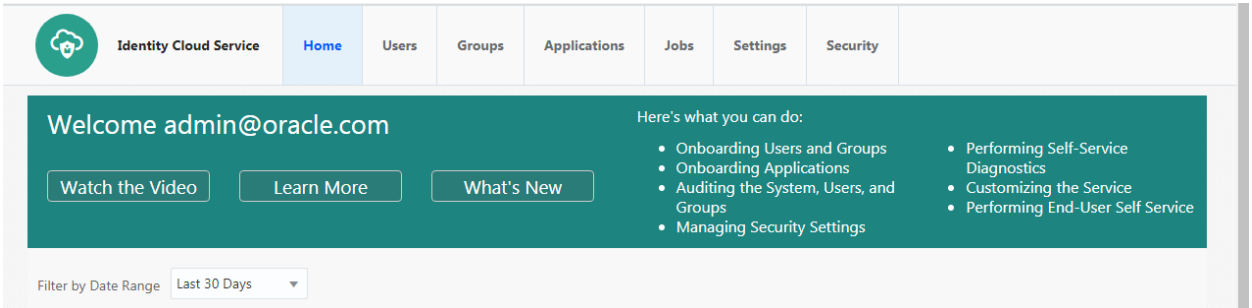
- Application Added.



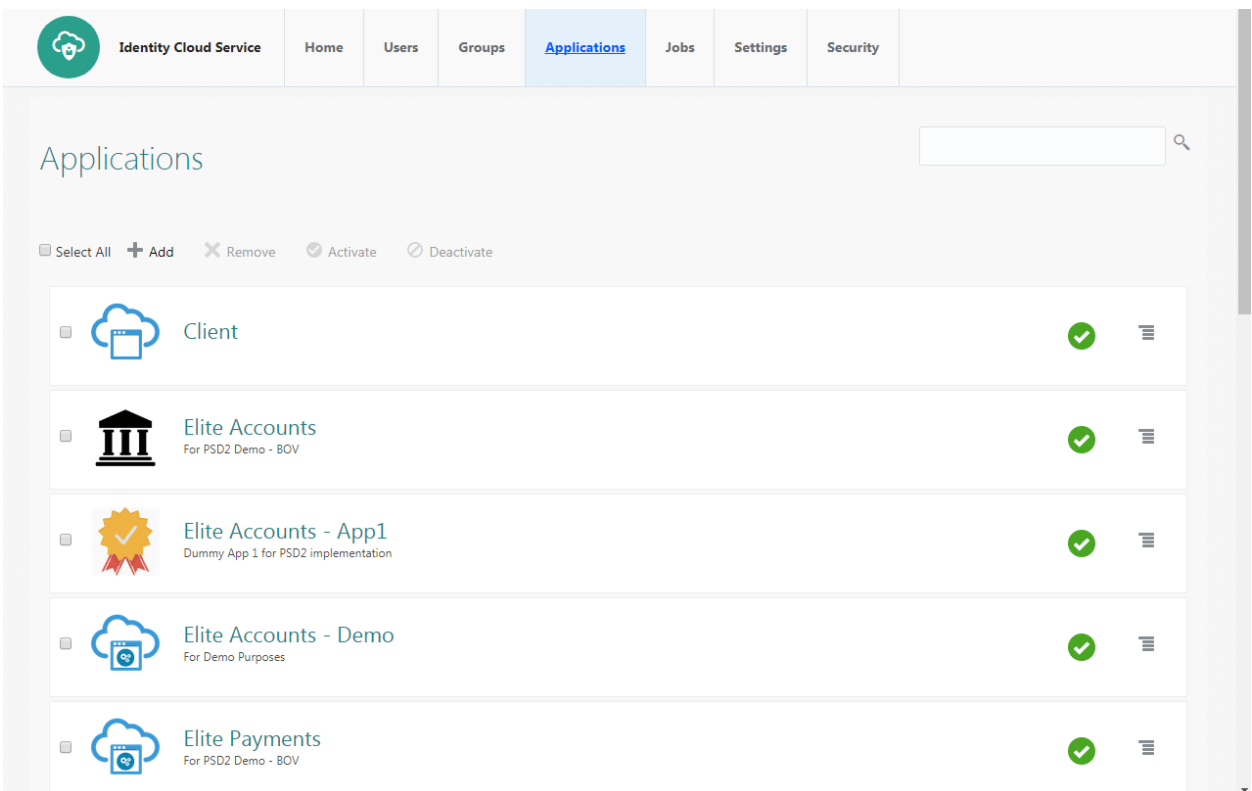
- Click on "Activate" to activate the application.

5.2 Registering a Third Party Mobile Client in IDCS

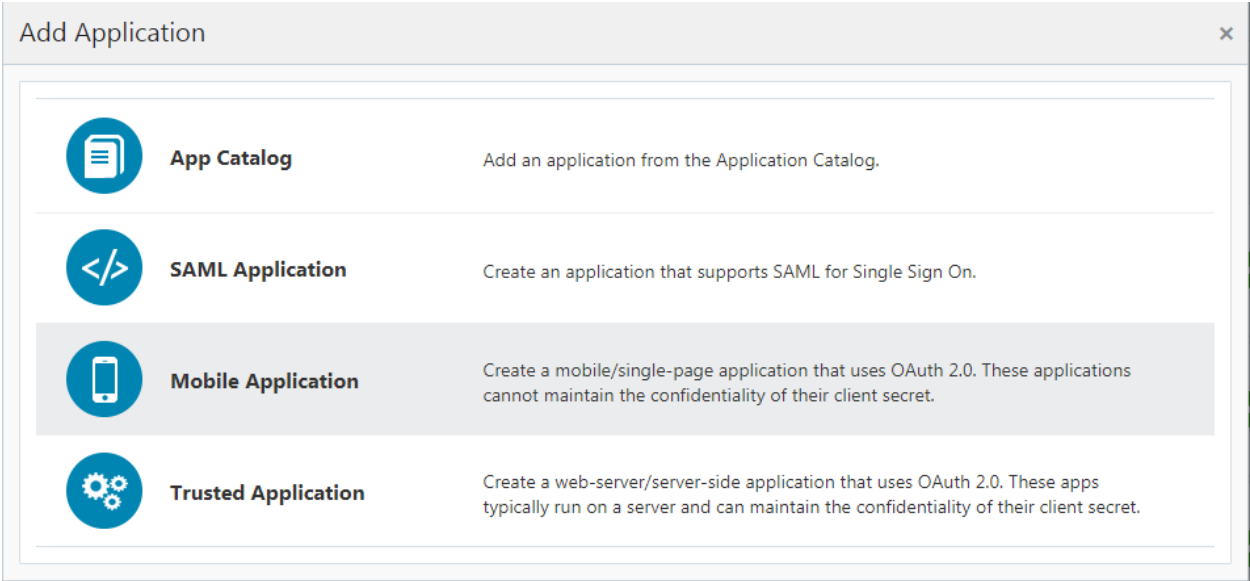
- Log into the IDCS dashboard.
- Click on the “Applications” tab which will list all applications associated with the logged in account.



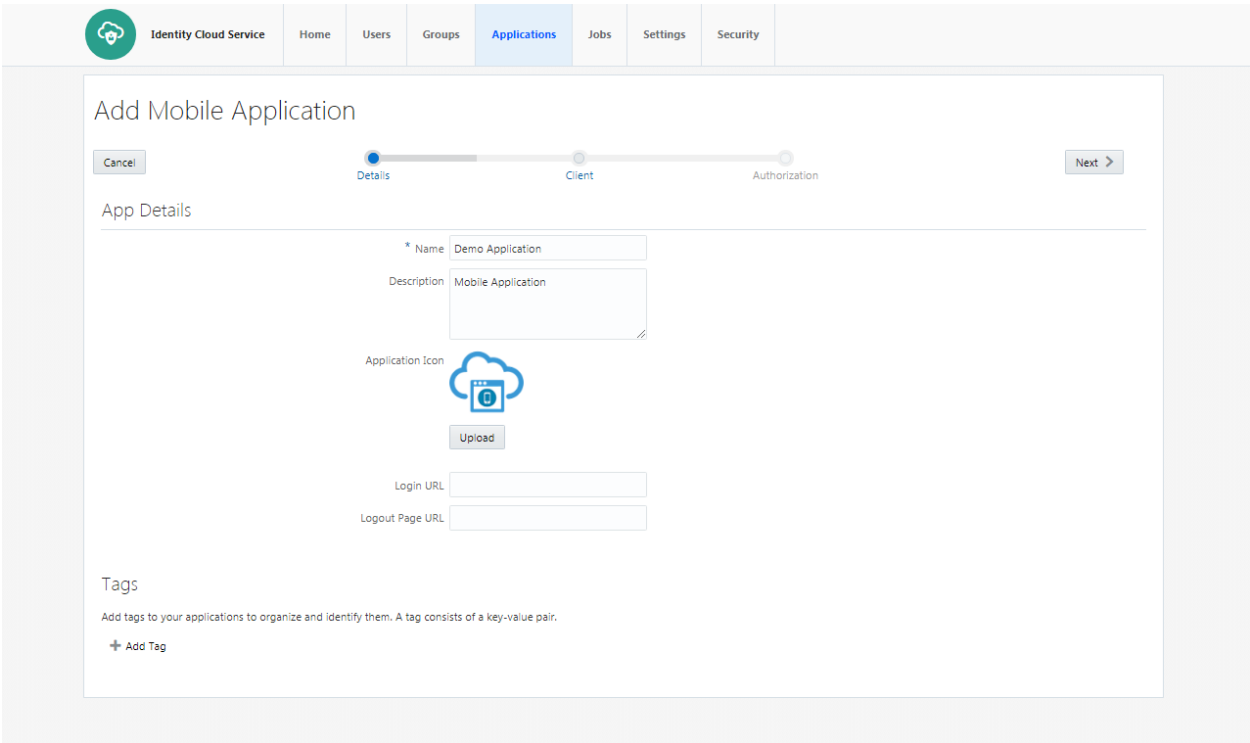
- Click on the “Add” button to create a new application



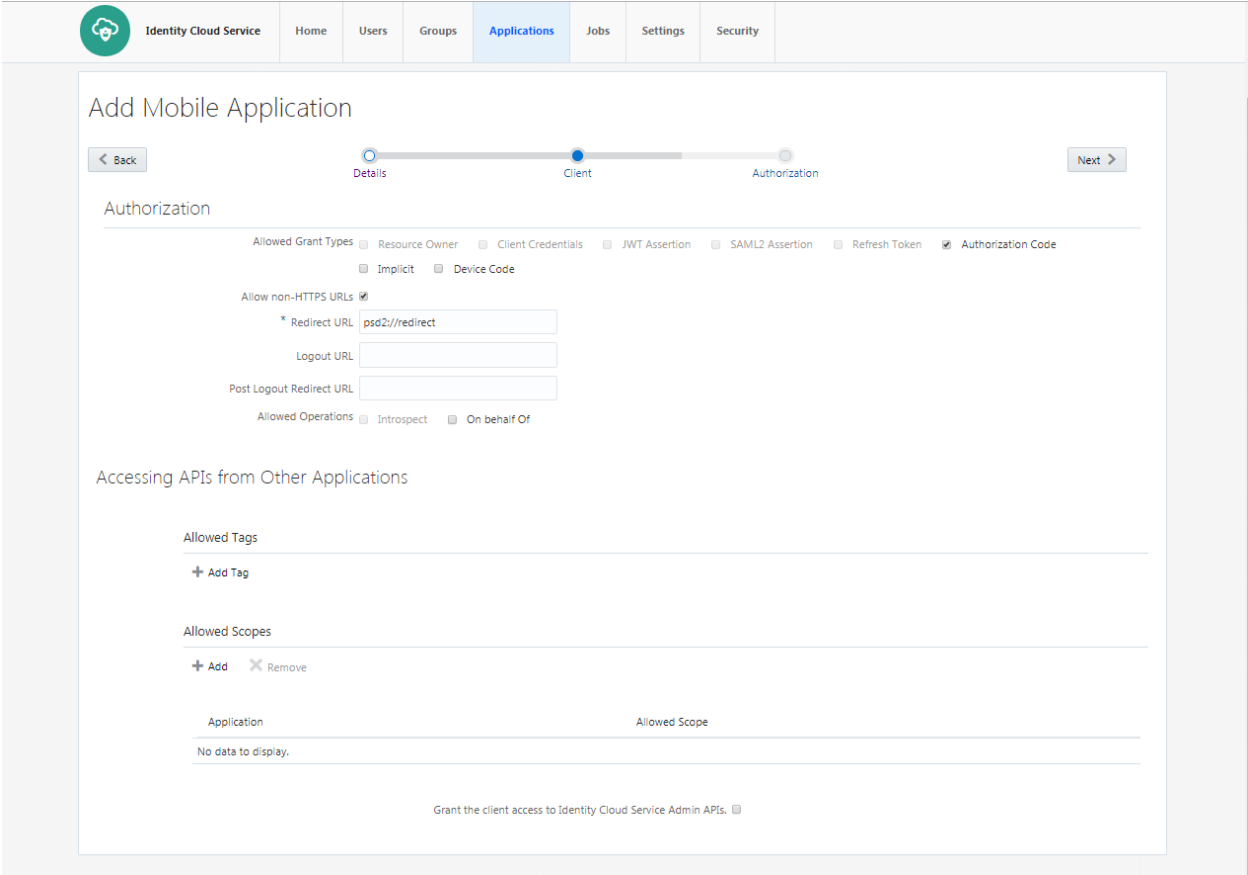
- Select Mobile Application



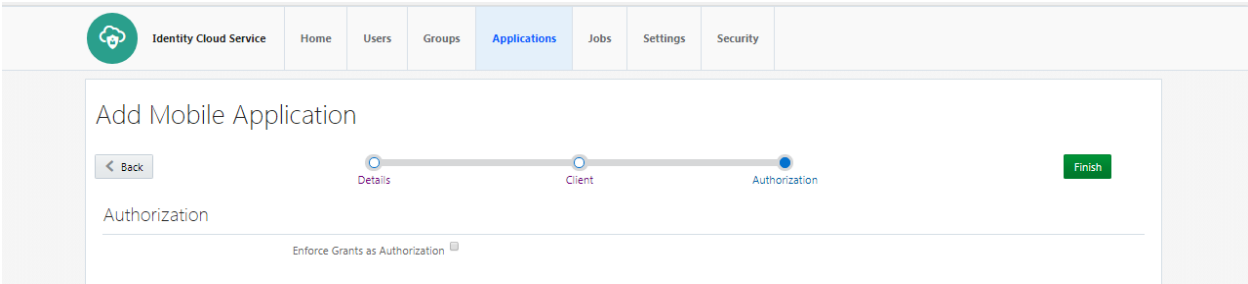
- Enter the name and description.



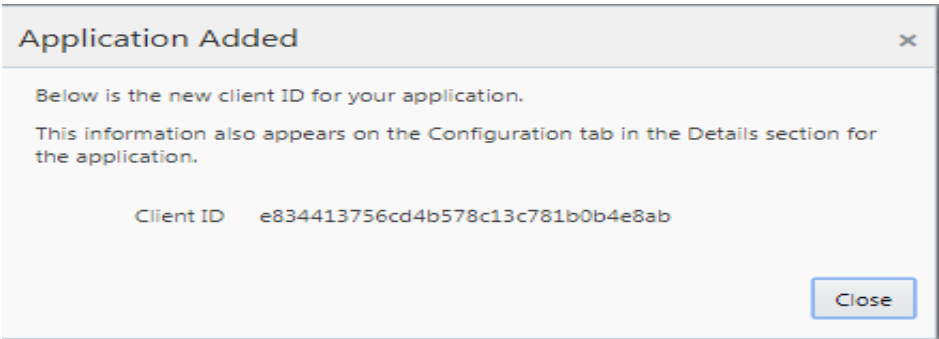
- Select 'Authorization Code' as Allowed Grant Types. Configure Redirect-URL as per your choice. The client application should listen to this URL when IDCS redirects on this URL with Authorization code.



- Click on Finish to complete the process.



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

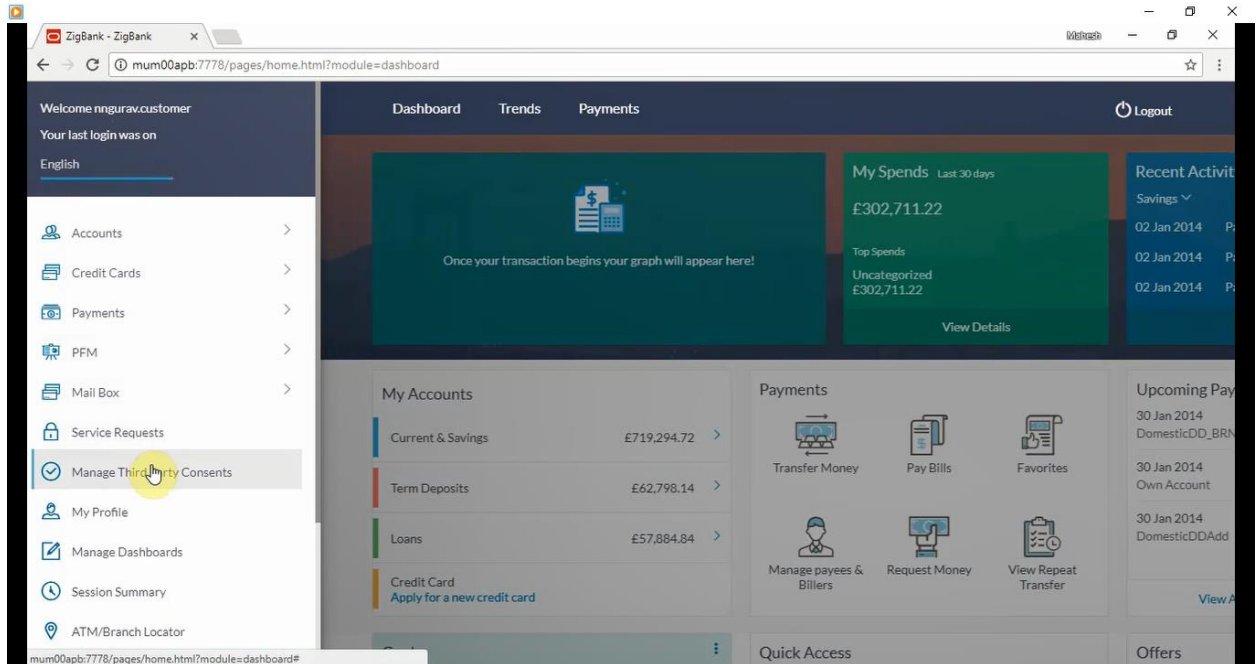


- Click on “Activate” to activate the application.

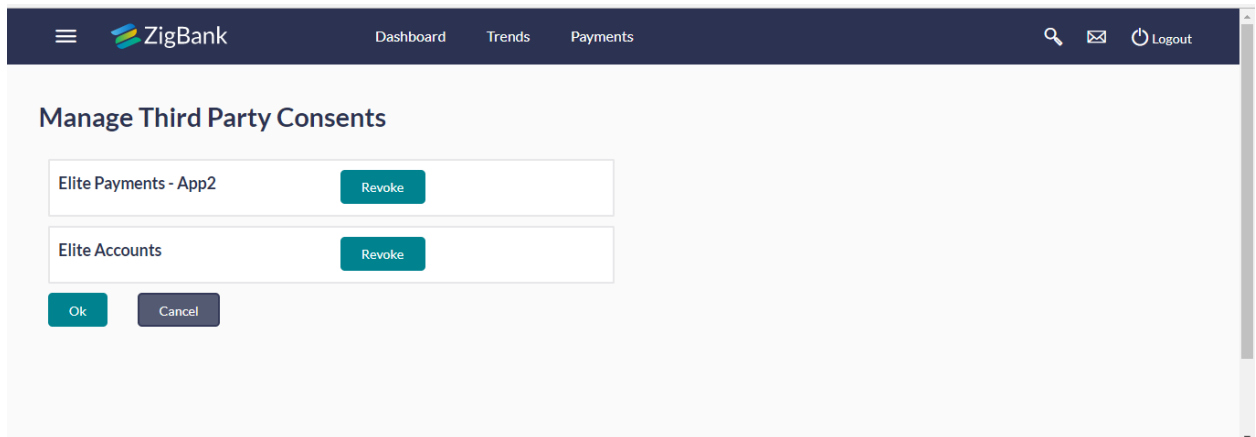
5. View and Manage Consents in OBDX

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



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

API USAGE	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

API USAGE	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

[Home](#)