

Oracle Banking Digital Experience

**PSD2 and Open Banking Guide
Release 18.2.0.0.0**

Part No. E97823-01

June 2018

ORACLE®

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 © 2018, 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
4.1.1 Registering OBDX as an Admin application in IDCS	7
4.2 APICS Configurations	10
5. Third Party Application Registration.....	14
5.1 Registering a Third Party Browser Client in IDCS	14
5.2 Registering a Third Party Mobile Client in IDCS	18
5.3 OBDX Configurations	21
5.3.1 WebLogic Configurations	21
5.3.2 OBDX Configurations (Scope Definition)	27
5.3.3 OBDX Configurations (Touch Point Definition)	28
5.3.4 OBDX Configurations (Role Transaction Mapping)	31
6. View and Manage Consents in OBDX	34
7. PSD2 Offerings and Modules	36

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=acc&id=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=acc&id=info> or visit

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

1.4 Structure

This manual is organized into the following categories:

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

Introduction provides brief information on the overall functionality covered in the User Manual.

The subsequent chapters provide information on transactions covered in the User Manual.

Each transaction is explained in the following manner:

- Introduction to the transaction
- Screenshots of the transaction
- The images of screens used in this user manual are for illustrative purpose only, to provide improved understanding of the functionality; actual screens that appear in the application may vary based on selected browser, theme, and mobile devices.
- Procedure containing steps to complete the transaction- The mandatory and conditional fields of the transaction are explained in the procedure.

If a transaction contains multiple procedures, each procedure is explained. If some functionality is present in many transactions, this functionality is explained separately.

1.5 Related Information Sources

For more information on Oracle Banking Digital Experience Release 18.2.0.0.0, refer to the following documents:

- Oracle Banking Digital Experience Licensing Guide

2. Purpose

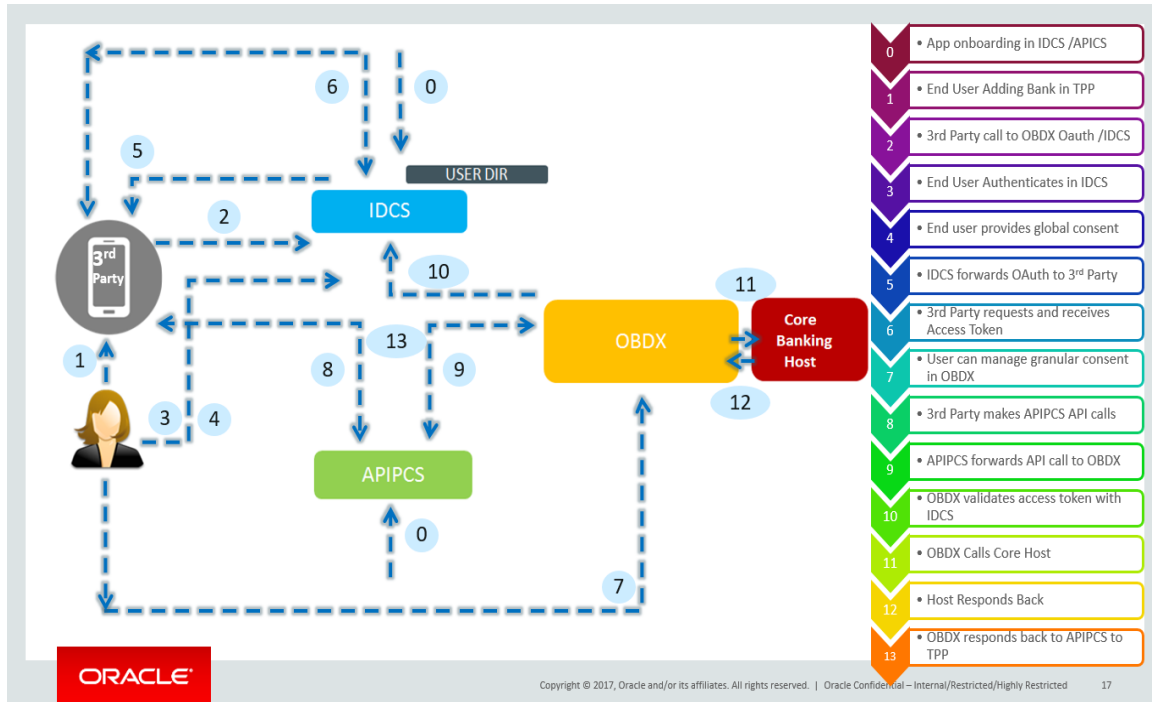
This document provides step by step guide to configure OBDX for PSD2 implementation.

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

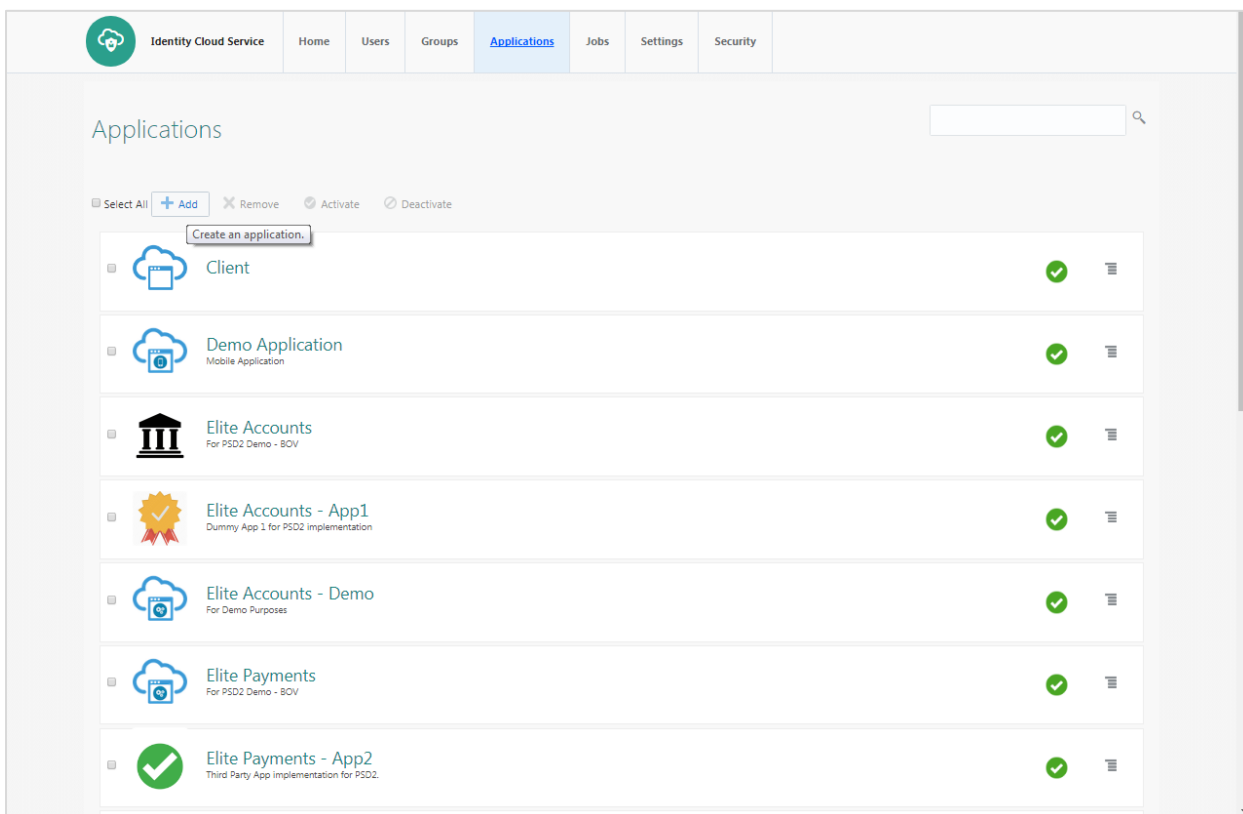

[Home](#)

4. PSD2 Configurations

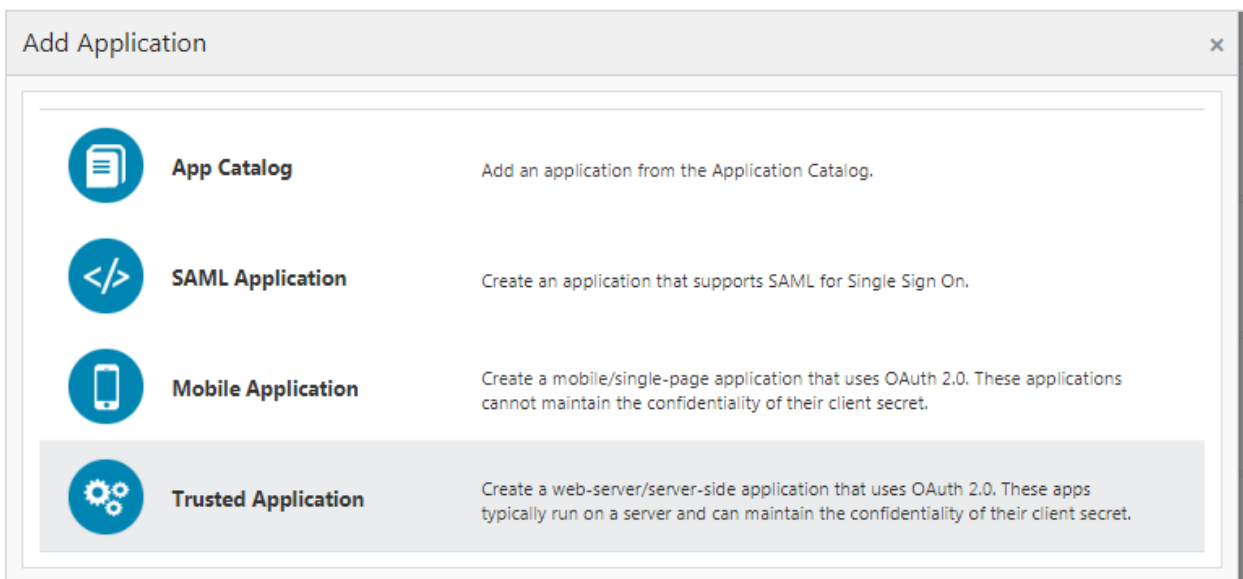
4.1 IDCS Configuration

4.1.1 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”

Identity Cloud Service | Home | Users | Groups | **Applications** | Jobs | Settings | Security


Add Trusted Application

Cancel | Details | Client | Resources | Authorization | Next >

App Details

* Name: Trusted demo

Description: Web Application

Application Icon:  Upload

Application URL:

Login URL:

Logout Page URL:

Tags

Add tags to your applications to organize and identify them. A tag consists of a key-value pair.

+ Add Tag

Display Settings

Display in My Apps ☐

User can request access ☐

- 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 ☐ Device Code

Allow non-HTTPS URLs ☐

Redirect URL:

Logout URL:

Post Logout Redirect URL:

* Client Type: ☐ Trusted ☒ Confidential ☐ Public

Certificate:

Allowed Operations: ☒ Introspect ☐ On behalf Of

- Add Admin Privileges for OBDX Client Configuration

Grant the client access to Identity Cloud Service Admin APIs.

Identity Domain Administrator ✕	User Administrator ✕	Self Registration ✕	Application Administrator ✕	Security Administrator ✕	Me ✕
Signin ✕					

- Application added

The screenshot shows the 'Add Trusted Application' wizard in the 'Authorization' step. A progress bar at the top indicates the steps: Details, Client, Resources, and Authorization (current). A '< Back' button is on the left, and a 'Finish' button is on the right. Below the progress bar, the 'Authorization' section contains a checkbox labeled 'Enforce Grants as Authorization' which is currently unchecked. A tooltip 'Click to add this app' is visible near the 'Finish' button.

The screenshot shows a confirmation dialog titled 'Application Added'. It contains the following text: '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.' Below this text, the Client ID and Client Secret are displayed. A 'Close' button is located at the bottom right.

Client ID	d095c8410e424988829277e998295a9e
Client Secret	fb2a3a1e-726e-4b3b-a310-9d130212e3b9

- 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.

Session Settings

* Session Expiry 480 minutes

Login URL /ui/v1/signin

* Logout URL /ui/v1/myconsole

Allow Cross-Origin Resource Sharing (CORS) ☒

Allowed CORS Domain Names mum00aptin.oracle.com

Save Cancel

- Page to set session token timeout and custom login URL

Session Settings

* Session Expiry 480 minutes

Login URL http://mum00apb.in.oracle.com:7778/p

* Logout URL /ui/v1/myconsole

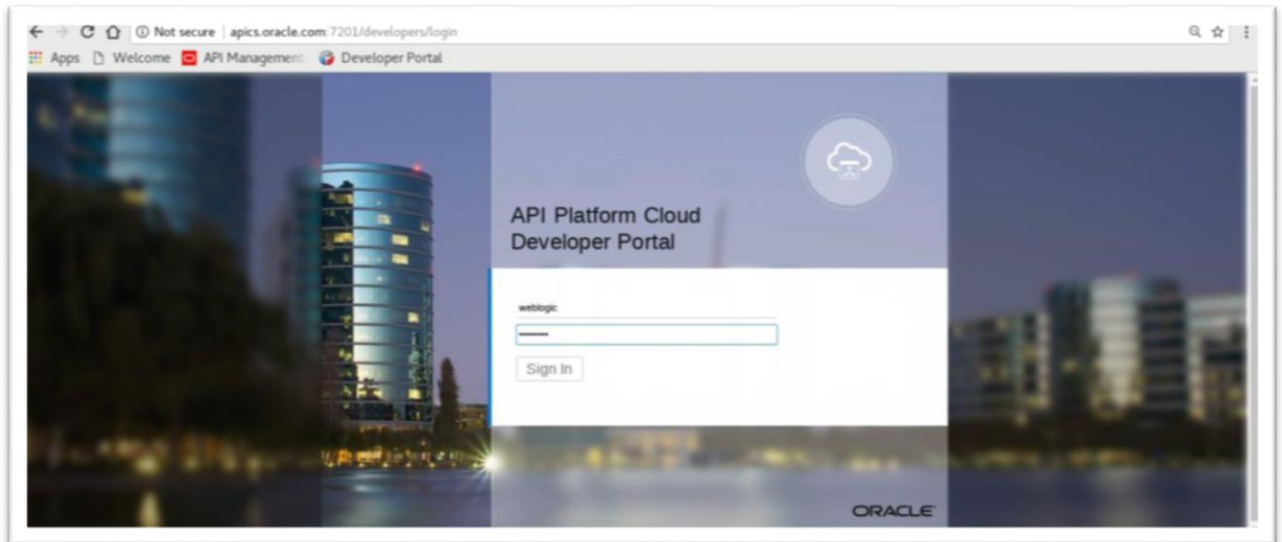
Allow Cross-Origin Resource Sharing (CORS) ☒

Allowed CORS Domain Names mum00apb.in.oracle.com

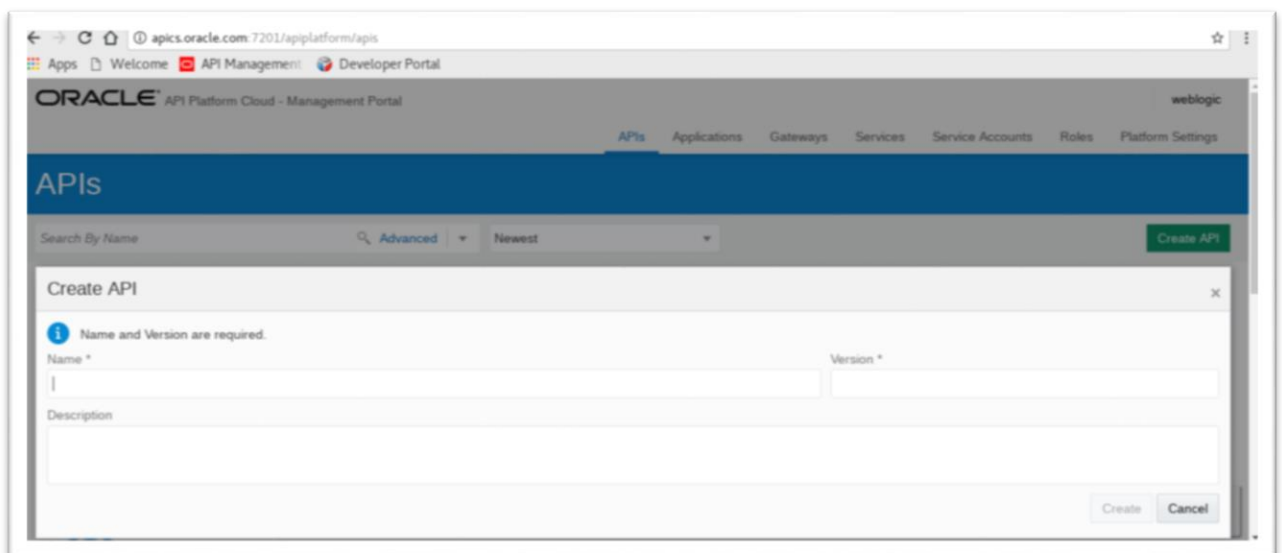
Save Cancel

4.2 APICS Configurations

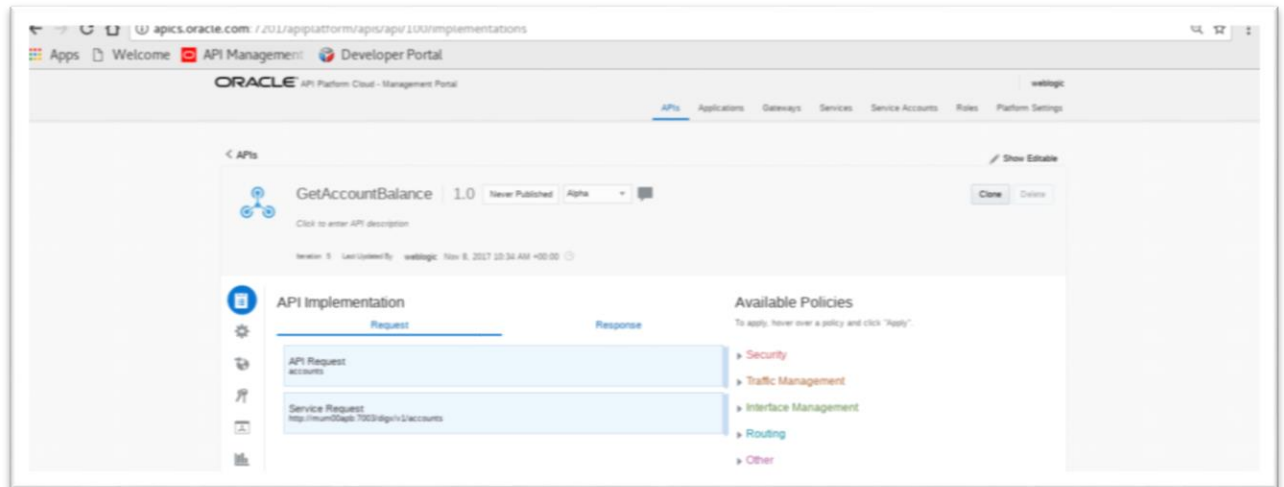
- Login to APICS



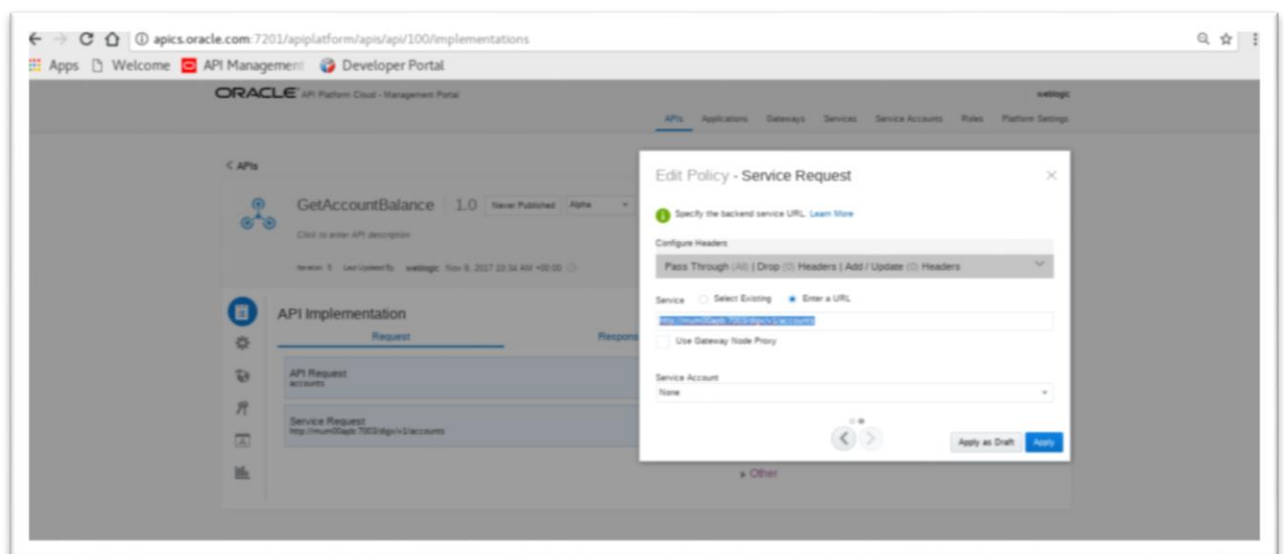
- Create API



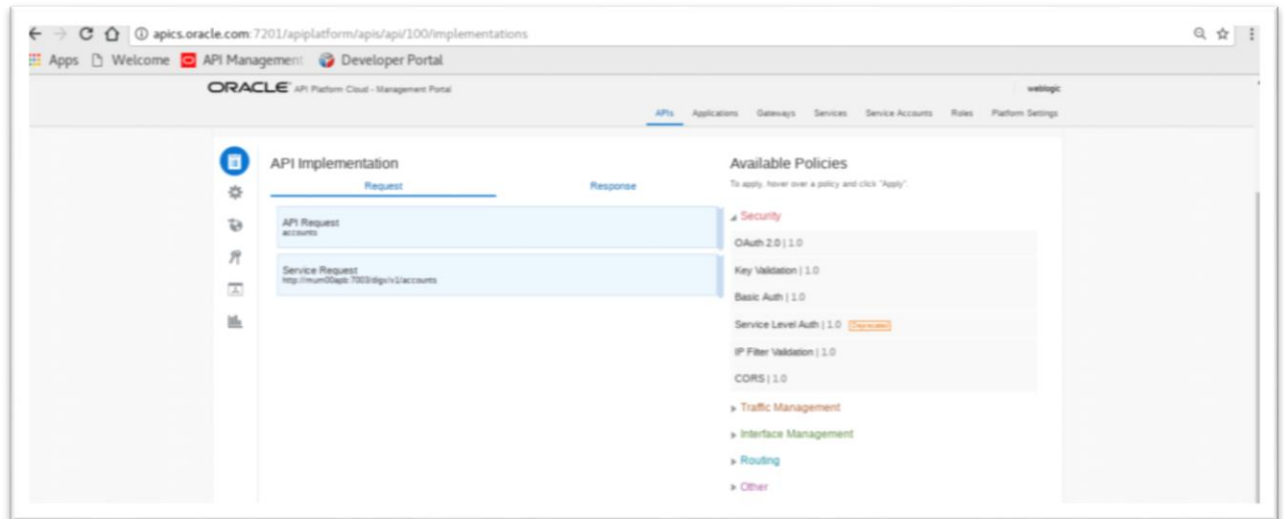
- API Implementation



- Edit Policy



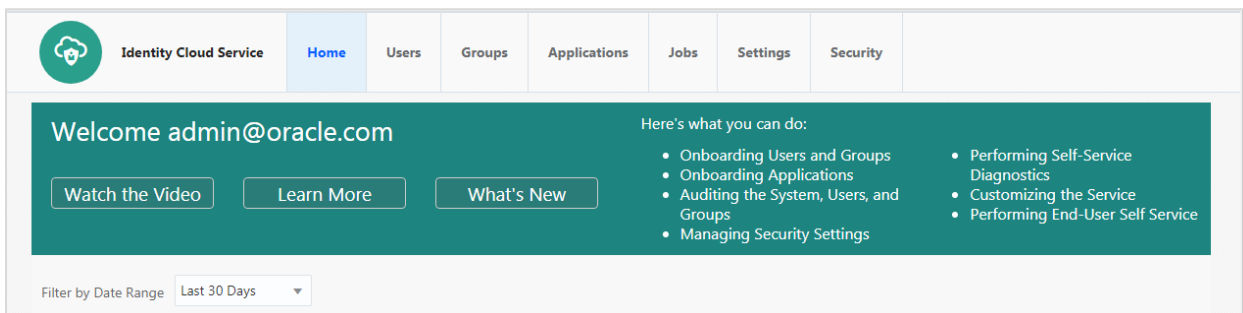
- View API Summarizing



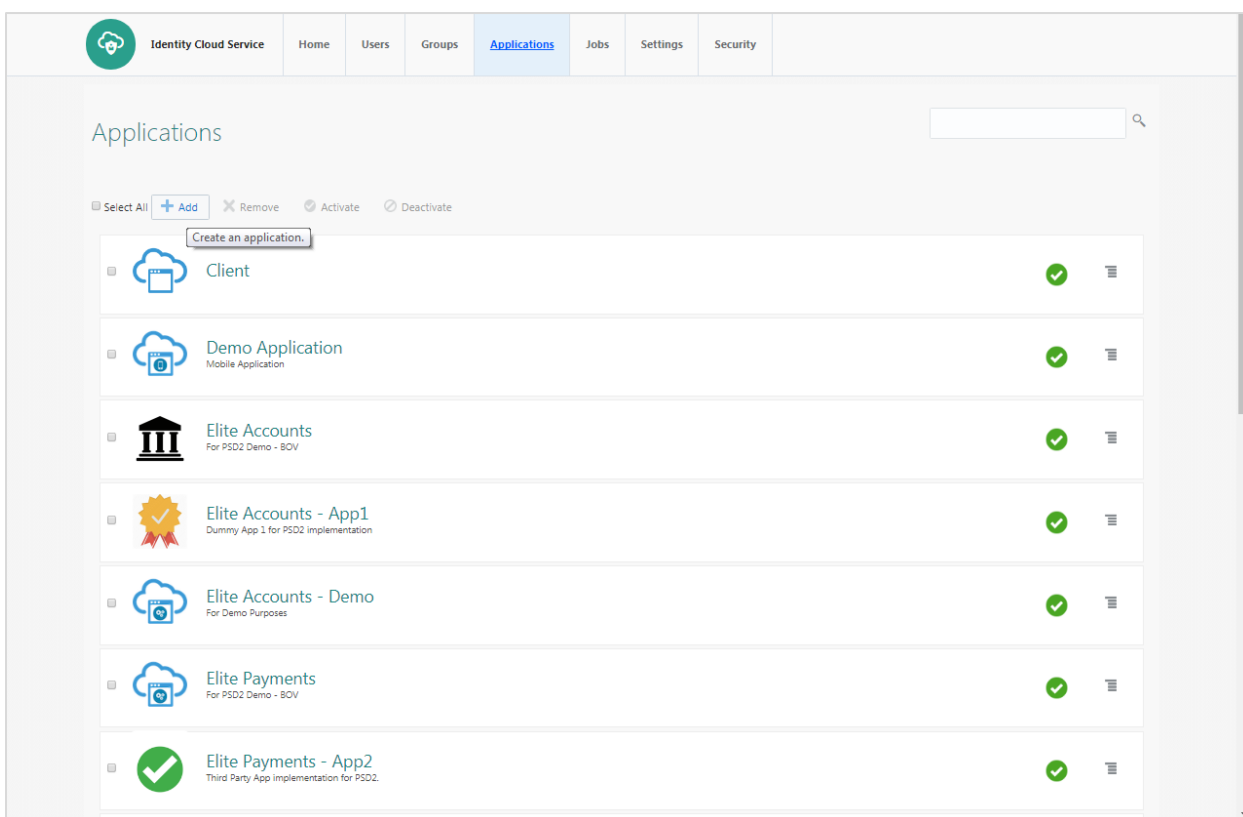
5. Third Party Application Registration

5.1 Registering a Third Party Browser Client in IDCS

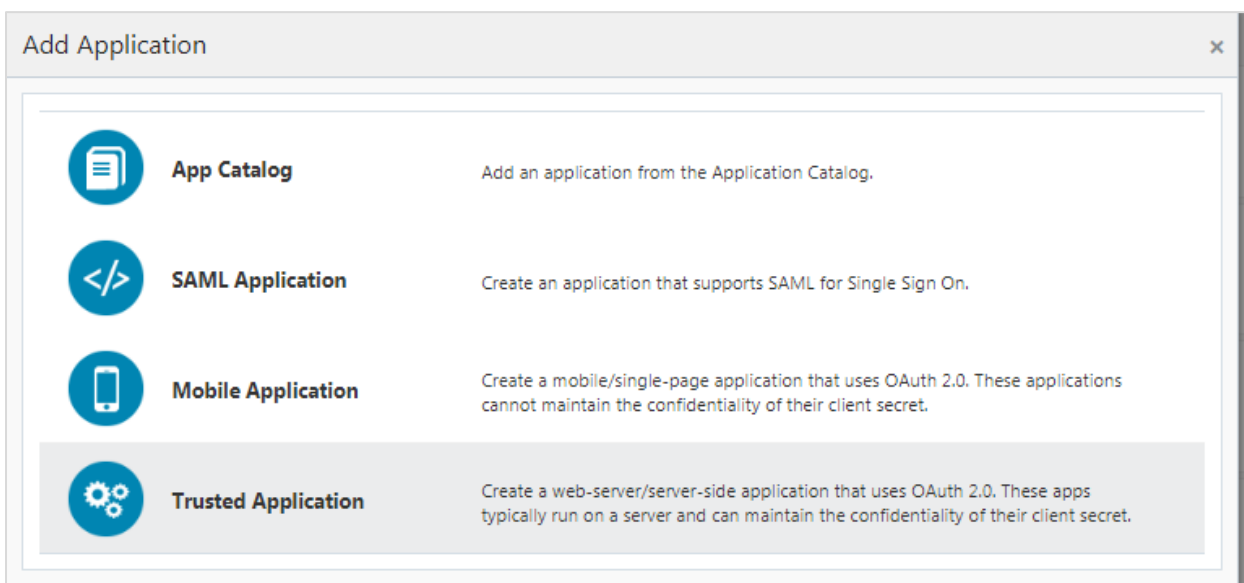
- Log into the IDCS dashboard.
- Click on the “Applications” tab which will list all applications associated with the logged in account.



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



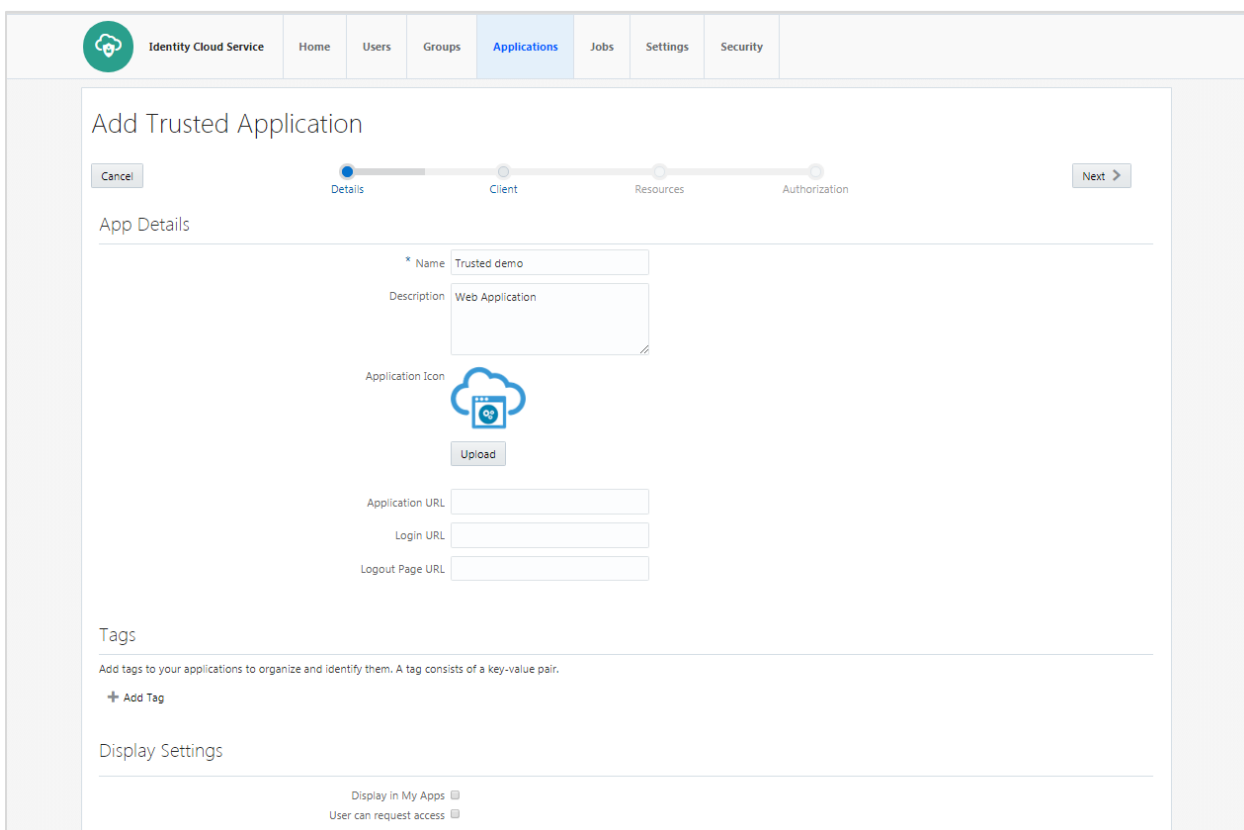
- Select 'Trusted Application'.



The 'Add Application' dialog box shows four options for creating an application. The 'Trusted Application' option is highlighted with a grey background.

Icon	Application Type	Description
	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'.



The 'Add Trusted Application' form is shown in the 'Applications' tab of the Identity Cloud Service. The form is divided into four steps: Details, Client, Resources, and Authorization. The 'Details' step is currently active.

App Details

- Name:** Trusted demo
- Description:** Web Application
- Application Icon:**
- Application URL:**
- Login URL:**
- Logout Page URL:**

Tags

Add tags to your applications to organize and identify them. A tag consists of a key-value pair.

Display Settings

- ☐ Display in My Apps
- ☐ User can request access

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

Add Trusted Application

[< Back](#)
Details
Client
Resources
Authorization
[Next >](#)

☒ Configure this application as a client now
 ☐ Skip for later

Authorization

Allowed Grant Types:
 ☐ Resource Owner
 ☐ Client Credentials
 ☐ JWT Assertion
 ☐ SAML2 Assertion
 ☐ Refresh Token
 ☒ Authorization Code
 ☐ Implicit
 ☐ Device Code

Allow non-HTTPS URLs ☒

* Redirect URL:

Logout URL:

Post Logout Redirect URL:

Security:
 ☐ Trusted Client
 ☐ Certificate

Allowed Operations:
 ☐ Introspect
 ☐ On behalf Of

Accessing APIs from Other Applications

Trust Scope:
 ☐ All resources
 ☐ Allowed tags
 ☒ Allowed scopes

Allowed Tags

[+ Add Tag](#)

Allowed Scopes

[+ Add](#)
[X Remove](#)

Application	Allowed Scope
No data to display.	

- 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: seconds

Is Refresh Token Allowed: ☐

Refresh Token Expiration: seconds

Primary Audience:

Secondary Audiences: [Add](#)

Secondary Audience	Remove
No data to display.	

Allowed Scopes: [Add](#) [Remove](#)

Scope	Description	Requires Consent
No data to display.		

- Application Added.

The screenshot shows the 'Add Trusted Application' form with the 'Authorization' tab selected. The form has a progress bar at the top with four steps: Details, Client, Resources, and Authorization. The 'Authorization' tab is currently active, indicated by a blue dot. Below the progress bar, there is a 'Back' button and a 'Finish' button. The main content area is titled 'Authorization' and contains a checkbox labeled 'Enforce Grants as Authorization' which is currently unchecked. A tooltip 'Click to add this applica' is visible near the 'Finish' button.

The screenshot shows a dialog box titled 'Application Added' with a close button (X) in the top right corner. The dialog contains the following text:

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.

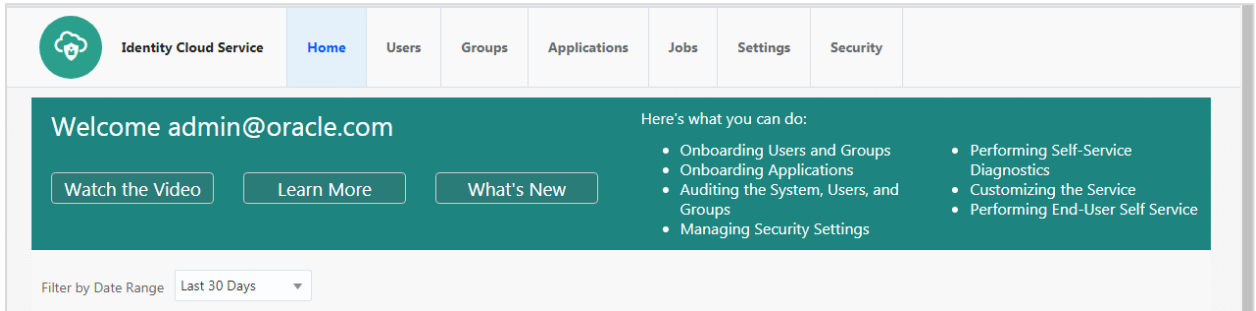
Client ID d095c8410e424988829277e998295a9e
Client Secret fb2a3a1e-726e-4b3b-a310-9d130212e3b9

At the bottom right of the dialog is a 'Close' button.

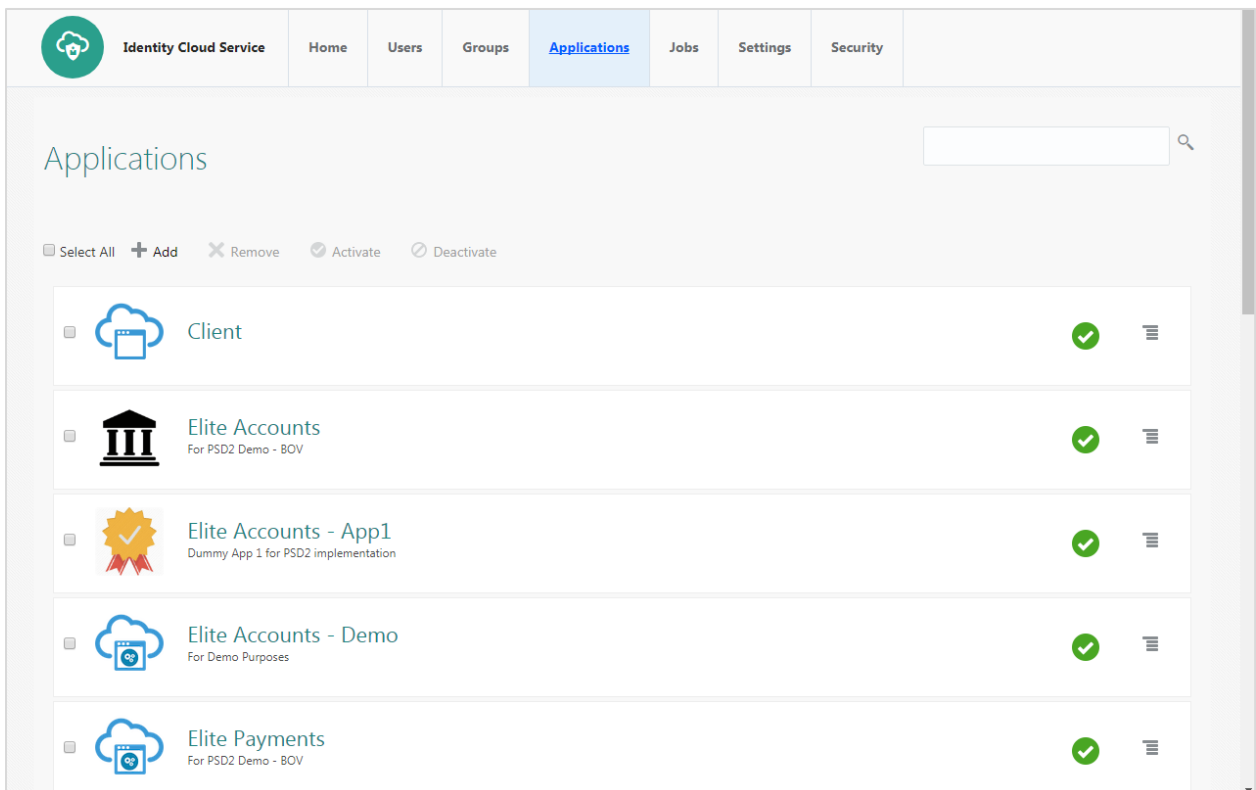
- Click on “Activate” to activate the application.

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


Add Application


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.

Identity Cloud Service
Home
Users
Groups
Applications
Jobs
Settings
Security


Add Mobile Application

Cancel
Details
Client
Authorization
Next >

App Details

* Name
Demo Application

Description
Mobile Application

Application Icon

Upload

Login URL

Logout Page URL

Tags

Add tags to your applications to organize and identify them. A tag consists of a key-value pair.

Add Tag

- 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.

The screenshot shows the 'Add Mobile Application' page in the Identity Cloud Service console. The 'Applications' tab is selected in the top navigation bar. The page has a progress bar with three steps: 'Details', 'Client', and 'Authorization'. The 'Authorization' step is currently active. Below the progress bar, the 'Authorization' section includes options for 'Allowed Grant Types' (Resource Owner, Client Credentials, JWT Assertion, SAML2 Assertion, Refresh Token, and Authorization Code), 'Allow non-HTTPS URLs' (checked), 'Redirect URL' (psd2://redirect), 'Logout URL', 'Post Logout Redirect URL', and 'Allowed Operations' (Introspect and On behalf Of). Below this, there is a section for 'Accessing APIs from Other Applications' with 'Allowed Tags' and 'Allowed Scopes' (Add, Remove). At the bottom, there is a checkbox for 'Grant the client access to Identity Cloud Service Admin APIs'.

- Click on Finish to complete the process.

This screenshot shows the same 'Add Mobile Application' page, but the 'Finish' button is now visible in the top right corner. The progress bar shows that the 'Authorization' step is complete, and the 'Client' step is now active. The 'Authorization' section still shows the same configuration options as the previous screenshot.

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

The screenshot shows a dialog box titled 'Application Added'. It contains the following text: 'Below is the new client ID for your application. This information also appears on the Configuration tab in the Details section for the application.' Below the text, the 'Client ID' is displayed as 'e834413756cd4b578c13c781b0b4e8ab'. There is a 'Close' button in the bottom right corner.

- Click on "Activate" to activate the application.

5.3 OBDX Configurations

5.3.1 WebLogic Configurations

Patch WLS12.2.1.3.

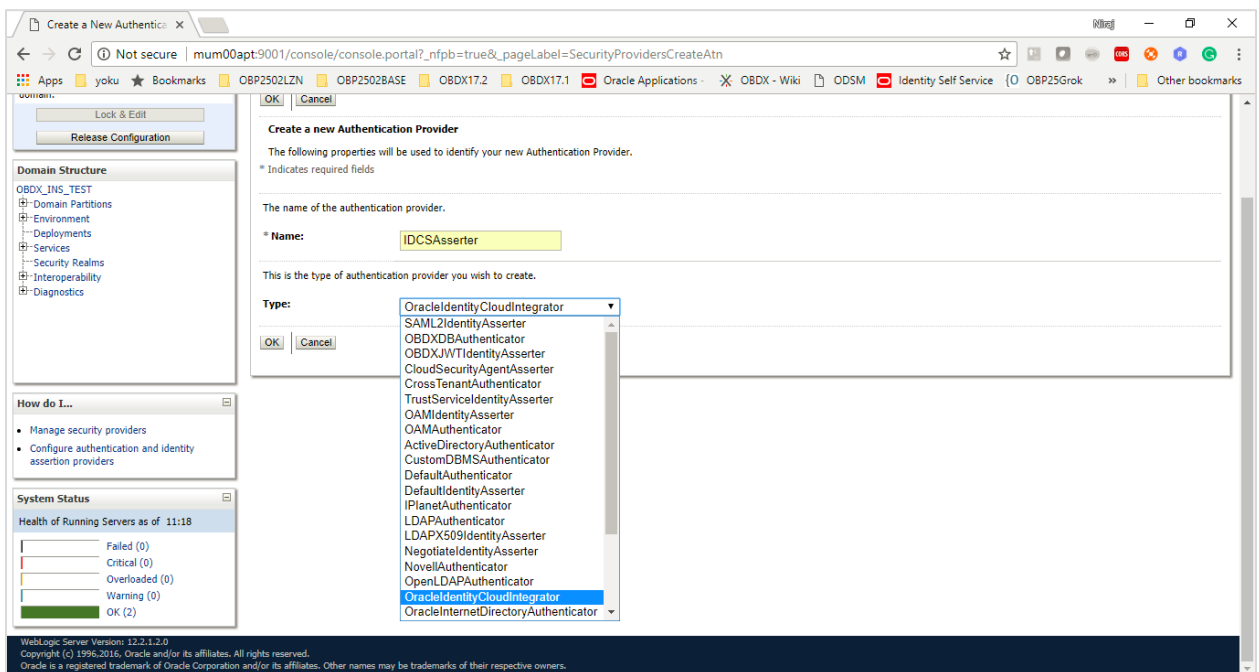
WLS 12.2.1.3.0 Obtain and install the WLS 12.2.1.3.0 kit from OTN:

Download the p27644158_122130_GenericPatch Set Update (PSU) for WebLogic Server 12.2.1.3 from http://aru.us.oracle.com:8080/ARU/ViewPatchRequest/process_form?aru=22260908

Apply the PSU patch following the instructions contained in the README.txt in the p27644158_122130_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'

ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: obdx_domain

Home > obdx_server > Summary of Security Realms > myrealm > Providers

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings **Providers** Migration

Authentication Password Validation Authorization Adjudication Role Mapping Auditing Credential Mapping Certification Path

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS.

Customize this table

Authentication Providers

Click the **Lock & Edit** button in the Change Center to activate all the buttons on this page.

New Delete Reorder Showing 1 to 5 of 5 Previous Next

<input type="checkbox"/>	Name	Description	Version
<input type="checkbox"/>	ODU	Provider that performs LDAP authentication	1.0
<input type="checkbox"/>	OAMIdentityAsserter	Oracle Access Manager Identity Asserter	1.0
<input checked="" type="checkbox"/>	IDCSAsserter	Provider that performs identity assertion for Oracle Identity Cloud Service tokens	1.0
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider	1.0
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

New Delete Reorder Showing 1 to 5 of 5 Previous Next

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

ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: obdx_domain

Home > obdx_server > Summary of Security Realms > myrealm > Providers > IDCSAsserter

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 define the general configuration of this provider.

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

Base64 Decoding Required: false

Save

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:

NORMAL ▾

Port:

443

☒ Cache Enabled

Tenant Names:

obdx-tenant01

Client IDToken Claim:

client_id

Base Path:

Token Clock Skew:

120

Tenant Token Claim:

user_tenantname

Any Identity Domain Enabled:

true

User Name Resource Attribute:

userName

Tenant Host Name Template:

{%tenant}.{%host}

PSD2 and Open Banking Guide

23

<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: <div><div></div></div>	
User IDToken Claim:	<input type="text" value="user_id"/>
User Authentication Assertion Attribute:	<input type="text"/>

<input checked="" type="checkbox"/> Sync Filter Enabled	
Issuer:	<input type="text"/>
<input checked="" type="checkbox"/> Sync Filter Only Client Cert Requests	
Tenant:	<input type="text"/>
Thread Lock Timeout:	<input type="text" value="300"/>
<input type="checkbox"/> Token Virtual User Allowed	
Connect Timeout:	<input type="text" value="300"/>
Response Read Timeout:	<input type="text" value="60"/>
Tenant Data Reload Interval:	<input type="text" value="300"/>
Host:	<input type="text" value="obdx-tenant01.identity.c9dev"/>
App Name Filter Header Name:	<input type="text" value="X-RESOURCE-SERVICE-IN"/>
Client Name Token Claim:	<input type="text" value="client_name"/>
Cache Size:	<input type="text" value="500"/>
<input type="checkbox"/> Client As User Principal Enabled	
<input type="checkbox"/> Sync Filter Prefer Header	
Client Secret:	<input type="password" value="*****"/>
Confirm Credential:	<input type="password" value="*****"/>
Client Tenant Token Claim:	<input type="text" value="client_tenantname"/>
<input checked="" type="checkbox"/> 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

Welcome, weblogic | Connected to: C

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.

Save

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.utils.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.

5.3.2 OBDX Configurations (Scope Definition)

Scopes need to be defined in IDCS and OBDX application as well. It needs to be operationally ensured that the scopes are the same in IDCS as well as OBDX.

The scopes will be seeded in the OBDX application table 'DIGX_FW_ACCESSPOINTSSCOPE' as shown below:

ID	DESCRIPTION
SC01	Account Balance Inquiry
SC02	Account Details Inquiry
SC03	Spends Inquiry
SC04	Domestic Transfers
SC05	Internal Transfers
SC06	International Transfers

Once the scopes are seeded, the same will appear as part of Touch Point Definition as well as in Role to transaction mapping.

5.3.3 OBDX Configurations (Touch Point Definition)

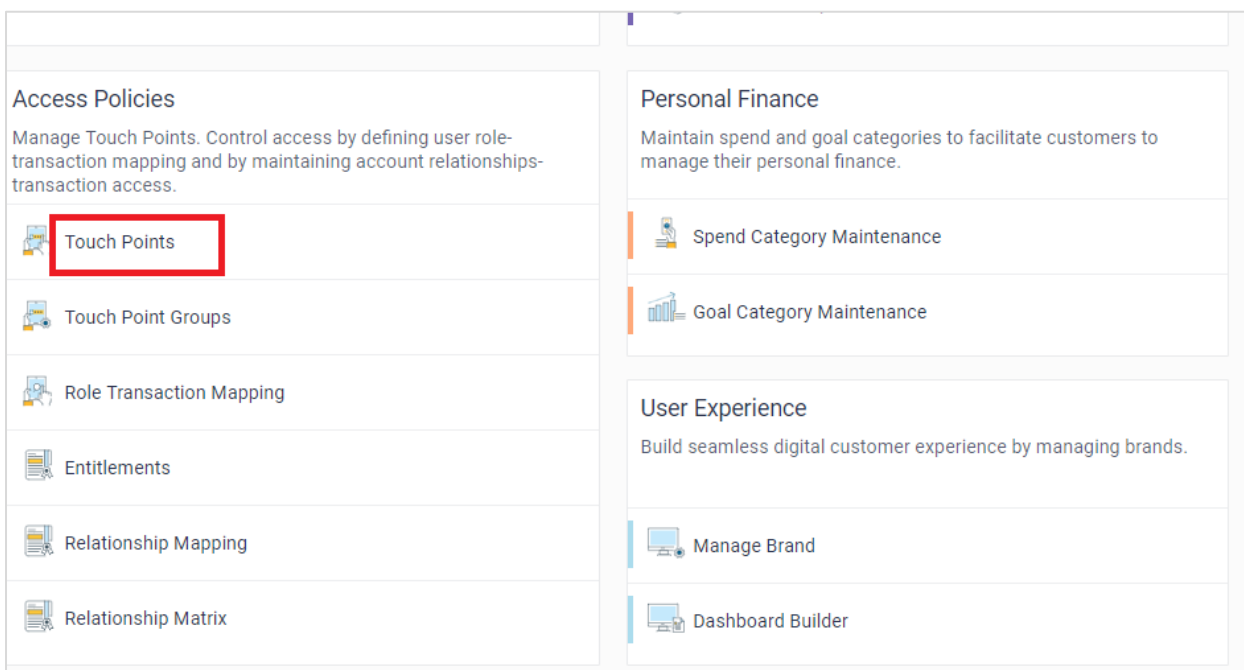
Touch points in OBDX are user agents from which transactions or inquiries can be initiated. Touch points are of 2 types i.e. Internal and External.

Internal Touch Points are shipped from the product i.e. Internet, Mobile Apps, Mobile Responsive, Siri/Chatbot etc.

External Touch Points are typically Third Party Applications that the bank user registers on to inquire and/or transact on bank accounts from third party applications.

To create an external touch point:

1. Login to the system as System Administrator user
2. Navigate to Touch Point Definition option



3. Click on Create option and enter the details required to create the Touch Point as mentioned below

Touch Point Maintenance

Touch Point Id

Touch Point Name


Touch Point Type

☐ INTERNAL
 ☒ EXTERNAL

Client Id

Scope

Upload Logo



Touch Point Status

☐

Headless Mode

☐

Two Factor Authentication

☐

Self On Board Touch Points

☐

Save

Cancel

Back

Description of the fields is mentioned below:

Field Name	Mandatory	Description	Recommended Values
Touch Point Id	Yes	Specify a unique Id to identify the Touch point in the OBDX application	NA
Touch Point Name	Yes	Specify the Touch point name with which the same needs to be identified in the system	NA
Touch Point Type	Yes	Specify the type of Touch Point if it is internal or external. Third party applications are defined as external touch points in the system	External
Client ID	Yes	Specify the same client ID provided to the third party application as part of onboarding in IDCS.	NA

Field Name	Mandatory	Description	Recommended Values
Scopes	Yes	Select the scopes that the Third Party application can access on behalf of the user.	The scopes for the Third Party application should be operationally the same as that defined in IDCS
Upload Logo	Yes	Upload the image of the brand logo of the Third Party Application. This will help the end business user to identify the third party application while managing the Fine Grained Consents	NA
Touch Point Status	Yes	If a particular Touch point is disabled, then any request from Third Party application will not be executed by OBAPI	The default value to will be 'Active' to enable the third party application to access information
Headless Mode	Yes	Select if the Touch Point needs to be enabled in Headless mode. If enabled then masking, indirection of data etc. will be disabled while accessing API from the Third Party	Ideally it should be selected as "YES" so that Third Party apps can access OBAPI in headless mode.
Two Factor Authentication	Yes	Select if two factor authentication needs to be enabled for the third party application.	If disabled, it will override the system level 2FA configuration for the requests from that respective touch point
Self On Board Touch Points	Yes	Select if the touch point will be self onboarded by the user or will be provided by the bank official	Value should be ideally "YES" since the user decides the TPPs on which he/she wishes to register

The above parameters defines the behavior of the third party application when it requests access to OBDX/OBAPI resources. To summarize, any external channel that needs to be given access to OBDX API's, the pre-requisite is that registration need to be done on IDCS and OBDX as well. Client ID is the unique identifier common between the two systems i.e. (IDCS and OBDX)

Post maintenance of touch point, access needs to be defined for the touch point by defining application role for a scope and then associate transactions to the application role.

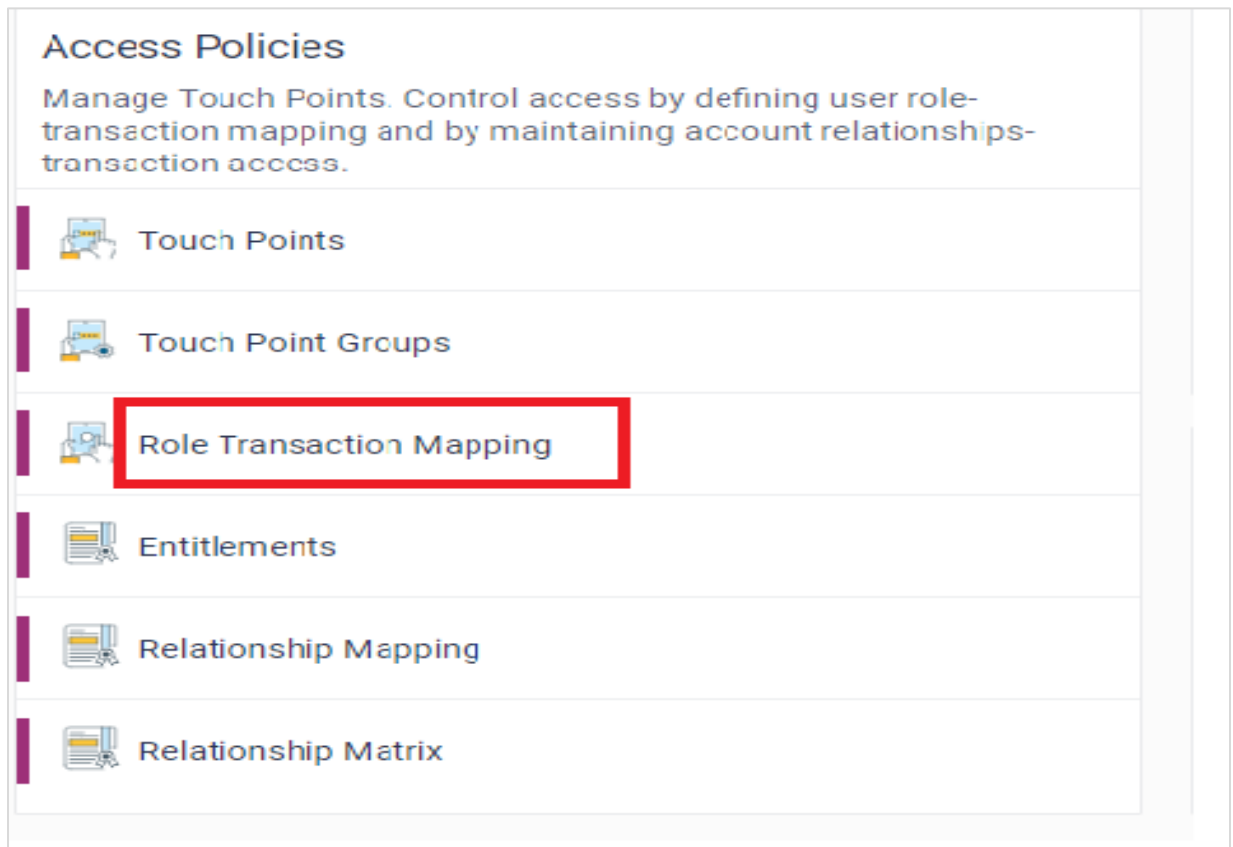
5.3.4 OBDX Configurations (Role Transaction Mapping)

Each scope defined and mapped for a Third Party Application needs an application role to access OBDX/OBAPI resources on behalf of the user.

As part of this maintenance, new application role can be created of type 'External' for each scope and also map transactions to the application role created.

To create new application role and map transactions:

1. Login to the system as System Administrator user
2. Navigate to Role Transaction Mapping maintenance



3. Click on 'Create' option
4. Create New Application Role and select user type i.e. 'Retail' and Access Type as 'External'
5. Select the scope from the list for which this new application role is being created

Role Transaction Mapping

1

2

Application Role Creation
Map Transaction

Application Role Name	Account Balance Inquiry
Description	Account Balance Inquiry
User Type	Retail User
Access Type	EXTERNAL
Scope Name	Account Balance Inquiry

Map Transaction
Cancel
Back

- Now click on Map Transaction to associate transactions to the new application role created
- Select the module(s) in case of specific transactions from the modules need to be mapped
- The selected transactions will be available to the Third Party for access on the basis of the passed scope.
- Click on Save will take to review page
- Confirm the Role Transaction Mapping

Role Transaction Mapping

✓

2

Application Role Creation
Map Transaction

Module Name	Current Account Savings Account
-------------	---------------------------------

Next
Clear
Cancel
Back

Transactions	Perform	Approve	View
<input type="checkbox"/> Current Account Savings Account	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Account Details			
<input type="checkbox"/> Inquire Party CASA Interest Certificate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Account Activity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Account Details	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Inquire CASA Interest Certificate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Calculator			
<input type="checkbox"/> Cheque Book Related			
<input type="checkbox"/> Debit Card			
<input type="checkbox"/> Statement			

Save

Cancel

Back

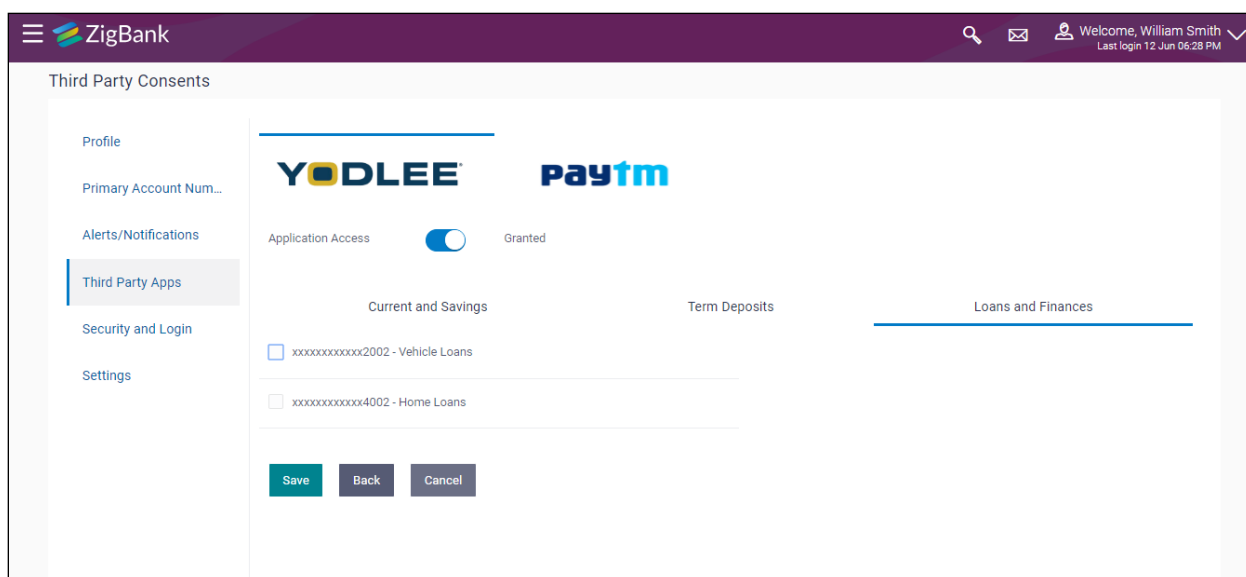
6. View and Manage Consents in OBDX

Business users can manage the consents provided to the third party applications in terms of the accounts on which the third parties can inquire and transact along with the set of transactions for each of the allowed accounts.

To manage fine grained consent business user needs to login with his credentials onto OBDX Internet Banking,

Click Menu -> Preferences -> Third Party Apps

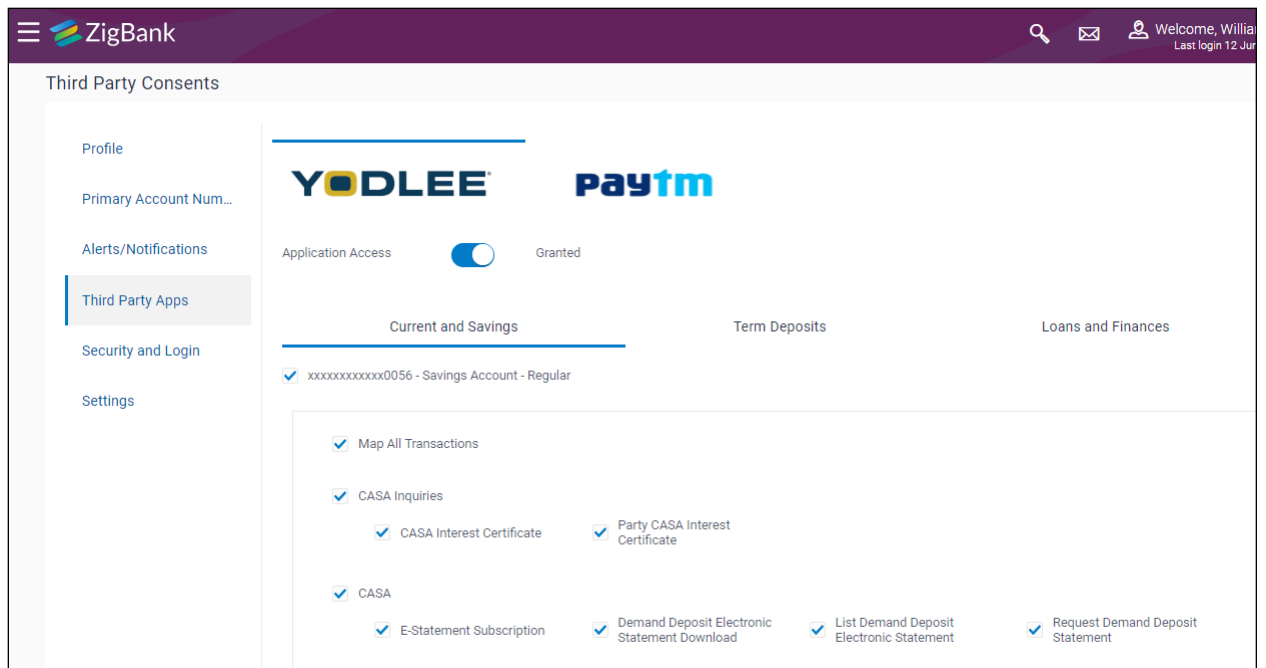
This will display the third party applications that the user has registered on along with the fine grained controls i.e. accounts and transactions for each of these third party applications



The user can revoke complete access to the third party application by turning off the application access

System also displays the accounts that the user has given access to the Third Party Application

Transactions shown for each of the accounts is filtered based on the scopes available to that Third Party application that are internally resolved via the application roles



7. PSD2 Offerings and Modules

The table below describes the PSD2 API Offerings

Sr. No.	Function	Feature
1	Accounts	Fetch account balance
2	Accounts	Validate account balance sufficiency
3	Accounts	Fetch Direct Debits
4	Accounts	Fetch Standing Instructions/orders
5	Accounts	Fetch debit card details
6	Accounts	Fetch product details
7	Deposits	Fetch deposit balance
8	Loans	Fetch drawdown details
9	Loans	Fetch schedule details
10	Credit Cards	Fetch current financial situation of a card
11	Pay to own accounts	Fetch payment details
12	Pay to own accounts	Fetch payment status
13	Pay to own accounts	Make a payment
14	Pay to own accounts	Make mass payment
15	Pay to own accounts	Cancel a payment
16	Pay within the bank	Fetch payment details
17	Pay within the bank	Fetch payment status
18	Pay within the bank	Make a payment
19	Pay within the bank	Make mass payment
20	Pay within the bank	Cancel a payment
21	Pay within EU	Fetch payment details
22	Pay within EU	Fetch payment status
23	Pay within EU	Make a payment

24	Pay within EU	Make mass payment
25	Pay within EU	Cancel a payment
27	Make an international payment	Fetch payment details
28	Make an international payment	Fetch payment status
29	Make an international payment	Make a payment
30	Make an international payment	Make mass payment
31	Make an international payment	Cancel a payment
32	Payment Information (Verify and Confirmation)	Charges
33	Payment Information (Verify and Confirmation)	Exchange Rate
34	Payment Information (Verify and Confirmation)	Initiation and Value Dates
35	Authorization	Add Third Party Access Grants
36	Authorization	Disable Third Party Access Grants
37	Accounts	Show Posting Third Party Details in Narration/Remarks
38	Account	Show Payment delivery time

[Home](#)