UK Open Banking Configuration Guide Oracle Banking Digital Experience Release 21.1.0.0.0

Part No. F40800-01

May 2021

ORACLE

UK Open Banking Configuration Guide May 2021

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 © 2006, 2021, 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	eface	. 1–1		
1	.1	Intended Audience	. 1–1		
1	.2	Documentation Accessibility	. 1–1		
1	.3	Access to Oracle Support	. 1–1		
1	.4	Structure	. 1–1		
1	.5	Related Information Sources	. 1–1		
2.	Ob	jective and Scope	. 2–1		
3.	Тес	chnology Stack	. 3–1		
4.	4. Pre-requisites				
5.	5. Headers Configuration				
6.	6. Properties				
7.	SA	ML	.7–1		
7	7.1	SAML Setup	.7–1		
7	7.2	SAML Integration	. 7–1		
8.	OA	uth Configuration	. 8–1		
8	3.1	UI configuration	. 8–1		
8	3.2	Weblogic configuration	. 8–1		
9.	Ext	ensibility and Code Conventions	.9–1		

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.

The subsequent chapters describes following details:

- Introduction
- Preferences & Database
- Configuration / Installation.

1.5 Related Information Sources

For more information on Oracle Banking Digital Experience Release 21.1.0.0.0, refer to the following documents:

Oracle Banking Digital Experience Installation Manuals



2. Objective and Scope

Background

Open Banking Configuration Document provides the various configurations required to enable UK Open Banking in OBAPI

Scope

- Headers Configuration
- Properties
- SAML Integration
- OAuth Configuration
- Code Convention and Extensibility



3. Technology Stack

Software	Version
Java	Java JDK or JRE version 8
OBDX/OBAPI	20.1.0.0.0
OAuth	OBDX Internal OAuth

Abbreviations

ООТВ	Out of the Box
TPP	Third Party Providers
ASPSP	Account Servicing Payment Service Provider
SAML	Security Assertion Markup Language

<u>Home</u>



4. Pre-requisites

- Java JDK or JRE version 7 or higher must be installed. For installation of Java please refer installation guide.
- OAuth Setup
- Weblogic Server with SAML Assertion capability



5. Headers Configuration

There are two types of headers configuration available for UK Open Banking.

- System Headers (i.e. Mandatory Headers and its respective value validation)
- Configuration Headers (i.e. Mandatory Headers).

Below are the configuration steps and Out of the box header already configured in the system.

System Headers:- As of now in OOTB one header has been added as mandatory "x-fapi-financialid" with value as "491308330388688" (This is a random value and can be changed. This value is issued by OBIE and corresponds to the Organization Id of the ASPSP in the Open Banking Directory). This value needs to be configured by Bank or ASPSP. This header needs to be sent by the TPP to the ASPSP mandatorily with the same value. Both Header name and Header value are validated for System Headers.

For configuring more system headers, below script is to be executed in the OBAPI Admin schema.

Insert into DIGX_FW_CONFIG_ALL_B (PROP_ID, CATEGORY_ID, PROP_VALUE, FACTORY_SHIPPED_FLAG, PROP_COMMENTS, SUMMARY_TEXT, CREATED_BY, CREATION_DATE, LAST_UPDATED_BY, LAST_UPDATED_DATE, OBJECT_STATUS, OBJECT_VERSION_NUMBER) values ('uk%%**HEADER NAME**%%','OpenbankingSystemHeaders','%%**HEADERVALUE**%%','N',null,'Open Banking','ofssuser',sysdate, 'ofssuser',sysdate, 'Y',1);

Below Query is used to check the System Headers in the system

select * from digx_fw_config_all_b where category_id = 'OpenbankingSystemHeaders';

Configuration Headers :- As of now in OOTB one header has been added as mandatory - "x-fapi-interaction-id". This header is required to be sent by the TPP to the ASPSP mandatorily with any value.

Only header name is validated in case of Configuration Headers.

For configuring more config headers, below script is to be executed in the OBDX/OBAPI Admin schema.

Insert into DIGX_FW_CONFIG_ALL_B (PROP_ID, CATEGORY_ID, PROP_VALUE, FACTORY_SHIPPED_FLAG, PROP_COMMENTS, SUMMARY_TEXT, CREATED_BY, CREATION_DATE, LAST_UPDATED_BY, LAST_UPDATED_DATE, OBJECT_STATUS, OBJECT_VERSION_NUMBER) values ('uk%%**HEADER NAME**%%',' OpenbankingConfigHeaders',null,'N',null,'Open Banking','ofssuser',sysdate,'ofssuser',sysdate,'Y',1);



Below Query is used to check the System Headers in the system

select * from digx_fw_config_all_b where category_id = 'OpenbankingConfigHeaders';



6. Properties

Below are the properties required to be updated in the UK Open Banking. Please find the below properties, its purpose and OOTB values.

Table:- DIGX_FW_CONFIG_ALL_B

Category-Id :- OpenBankingConfig

Property Id	Property Value (Out of the Box)	Purpose
CONSENT_EXPIRY DAYS	90	This value is used to check if expiry date send by TPP for the Account Access Consent is not more than 90 days and if it is more than 90 days then ASPSP will reject this value
CONSENT_HANDLE R	com.ofss.digx.app.openbanking .consent.handler.uk.UKConsent Handler	Handler defines the Region specific behavior of the Open Banking framework. By default UK Consent Handler is used for UK Open Banking compatibility

Token Settings

Category-Id :- SecurityConstants

Property Id	Property Value	Purpose
SIGNER	MAC/no row – MAC Signer X509RS256 – x509 signed token with RS256 algorithm X509PS256 - x509 signed token with PS256 algorithm	The algorithm used to generate JWT token.



Client Authentication

Property File Path :- /core/auth/com.ofss.digx.oauth.rest/src/common_rest.properties

Property Id	Property Value	Purpose
clientAuthenticationM ethod	1. client_secret_basic - Clients that have received a client_secret value from the Authorization Server authenticates with the Authorization Server in accordance with OAuth 2.0 using the HTTP Basic authentication scheme. This is the default value.	A set of Client Authentication methods that are used by Clients to authenticate to the Authorization Server when using the Token Endpoint.
	2. private_key_jwt - Clients that have registered a public key sign a JWT using that key. The Client authenticates in accordance with OAuth.JWT and OAuth.Assertions.	

Code Challenge

Property File Path :- /core/auth/com.ofss.digx.oauth.rest/src/common_rest.properties

Property Id	Property Value	Purpose
isCodeChallengeEna bled	 false – this is the default value true 	Property to enable/disable code challenge mechanism as per the FAPI requirements.

<u>Home</u>

7. SAML

7.1 SAML Setup

SAML Setup is required for propagating User Identification for account selection as part of consent authorization. Follow this section of the document available at below location for SAML setup:

0

7.2 SAML Integration

SAML Integration is required for asserting User Identification for account selection as part of consent authorization. Steps to be followed for SAML Integration are as below.

URL for SAML Account Rest should be as :- http://<host>:<port>/ob/saml/accounts

One default Internal Touch Point configuration will be required to handle Access to FETCH and POST Accounts through SAML.

Create a new TouchPoint for SAML services Access and configure in the web.xml of **obdx.app.rest.idm.ear** for the URL "**ob/saml/accounts**" as "**init-param** :- **obdx.saml.accesspoint**". So through Role Transaction Mapping of the newly created touchpoint, the access would be provided for the SAML services of Open Banking FETCH and POST account.

As part of User Onboarding in OBAPI, the created touchpoint needs to be associated to the user being onboarded.

Home



ORACLE

SAML

8. OAuth Configuration

8.1 UI configuration

OAuth Identity Domain Maintenance will require below maintenance to configure UI Component for Authorizing consent.

The value of Consent Page URL (Menu -> OAuth -> Identity Domain Maintenance) is configured as http://host:port?homeComponent=authorize-consent&homeModule=open-banking&applicationType=digx-auth.

8.2 Weblogic configuration

OAuth Maintenance will require below maintenance in weblogic to configure an URL.

Step 1: Login to weblogicStep 2: Go to Security Realms

ORACLE WebLogic Server Administration Console 12c 🏦 Home Log Out Preferences 🔤 Record Help Q Welcome, weblogic Connected to: obdx_d Change Center Home View changes and restarts Click the Lock & Edit button to modify, add or delete items in this domain. Home Page - Information and Resources -Lock & Edit General Information Common Administration Task Descripti Read the documentation Ask a question on My Oracle Support Helpful Tools Release Configuration Helpful Tools Configure applications Configure GridLink for PAC Data Source Configure a Dynamic Cluster Recent Task Status S Et your console preferences Oracle Enterprise Manager Domain Structure domain main Partitions - Domain Configuration Resource Group Template Domain Domain Intero Resource Group Templates WTC Servers Jolt Connection Pools Domain Partition Resource Grou Domain Partitions Partition Work Managers Resource Groups Diagnostics Log Files Ξ How do I... Diagnostic Modules Built-in Diagnostic Modules Diagnostic Images Request Performance Deployed Re Search the configuration Use the Change Center Deployments Servers Record WLST scripts Clusters Services Change Console preferences Manage Console extensions Monitor servers Messaging JMS Servers Store-and-Forward Agents W/S Modules Server Templates Migratable Targets Archives Context SNMP Coherence Clusters Interce Machines



ORACLE WebLogic Server Administration Console 12c				
Change Center	🏦 Home Log Out Preferences 🔤 Record Help	Welcome, weblogic Connected to: obdx_domain		
View changes and restarts	Home >Summary of Security Realms			
Click the Lock & Edit button to modify, add or delete items in this domain.	Summary of Security Realms			
Lock & Edit Release Configuration Domain Structure	A security realm is a container for the mechanisms-including users, groups, security security realms in a WebLogic Server domain, but only one can be set as the default : This Security Realms page lists each security realm that has been configured in this V	roles, security policies, and security providers-that are used to protect WebLogic resources. You can have multiple active security realm, which is reserved for domain administrative purposes. HebLogic Server domain. Click the name of the realm to explore and configure that realm.		
obdx_domain II-Domain Partitions III-Environment Deployments				
- Services	Click the Lock & Edit button in the Change Center to activate all the buttons on this page.			
Becurity Realms	New Delete	Showing 1 to 1 of 1 Previous Next		
Diagnostics	🔲 Name 🏟	Default Realm		
	myrealm	true		
	New Delete	Showing 1 to 1 of 1 Previous Next		
How do I				
Configure new security realms				
Enable automatic realm restart				
Delete security realms				
Change the default security realm				
System Status				
Models of Dunning Conservation of 40404 DM				



Step 4: Go to Providers

DRACLE WebLogic Server Administration Console 12c				
Change Center	🙆 Home Log Out Preferences 🔤 Record Help	٩	Welcome, weblogic Connected to: obdx_domain	
View changes and restarts	Home >Summary of Security Realms >myrealm			
Click the Lock & Edit button to modify, add or delete items in this domain. Lock & Edit Release Configuration	Settings for myrealm Configuration Users and Groups Roles and Policies General RDBMS Security Store User Lockout Per	Credential Mapping Providers Agration		
Domain Structure	Click the Lock & Edit button in the Change Center to mo	dify the settings on this page.		
obdy_domain @: Domain Partitions @: Environment :: Dopployments B: Serucks :: Security Realms B: Interoperability B: Diagnostics	Save Use this page to configure the general behavior of this security realm. Note: If you are implementing security using JACC (Dava Authorization Contract for Containers as defined in 35R 115), you must use the DD Only security model. Other WebLogic Server more and the security functions for Web applications and EDBs in the Administration Console are disabled. Name: myrealm The name of this security realm. More Info			
	Ecurity Model Default:	DD Only *	Specifies the default security model for Web applications or EIBs that are secured by this security realm. You can override this default during deployment. More Info	
How do I • Configure new security realms			Determines how the role mappings in the Enterprise Application, Web application, and EIB containers interact. This setting is valid only for Web applications and EIBs that use the Advanced security model and that initialize roles from deployment descriptors. More Info	
Enable automatic realm restart Manage security for Web applications and EJBs	Use Authorization Providers to Protect JMX /	Access	Configures the WebLogic Server MBean servers to use the security realm's Authorization providers to determine whether a JMX client has permission to access an MBean atthibute or invoka an MBean operation. More Info	
 Set the default security model Delegate MBean authorization to the realm 	Automatically Restart After Non-Dynamic Chang	jes	Specifies whether the Realm will be auto-restarted if non-dynamic changes are made to the realm or providers within the realm. More Info	

Step 5: Go to OBDXJWT

ORACLE WebLogic Server Adm	inistration Console 12c		Q
Change Center	🏦 Home Log Out Preferences 🔤 Record Help	9	Welcome, weblogic Connected to: obdx_domain
View changes and restarts	Home >Summary of Security Realms >myrealm >Providers		
Click the Lock 5 defortution to modify, add or delet terms in this domain. Lock & Edit defortution to modify, add or delet terms in this domain. Release Configuration Domain Structure ocks, domain P-Dealphometis —Deelphometis —Services —Security Realms —Structures	Settings for myrealm Configuration Users and Groups Roles and Polices Authentication Pessword Validation Authorization An Authentication provider allows WebLogic Server to es a security realm. Different types of Authentication provide science and the set of the se	Credential Mappings Providers Migration Adjudication Role Mapping Auditing Credential Mapping Certification Path tablish trust by validating a user. You must have one Authentication provider in a security realm, and you ors are designed to access different data stores; such as LDAP servers or DBMS.	can configure multiple Authentication providers in
L±Diagnostics	New Delete Reorder		Showing 1 to 5 of 5 Previous Next
	Name	Description	Version
	DBAuthenticator	OBDX - DB Authenticator	18.3.2.2.0,956
Hann de T	SQLAuth	Provider that performs DBMS authentication	1.0
How do 1	OBDXJWT	OBDX Identity Assertion Provider (JWT and OAuth)	18.3.2.2.0,956
 Configure authentication and identity assertion providers 	DefaultAuthenticator	WebLogic Authentication Provider	1.0
Configure the Password Validation provider	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
Kanage security providers Set the JAAS control flag Re-order authentication providers		Showing 1 to 5 of 5 Previous Next	

Step 6: Go to Provider Specific

ORACLE WebLogic Server Administration Console 12c				
Change Center	🔒 Home Log Out Preferences 🔤 Record Help	Welcome, weblogic Connected to: obdx_domain		
View changes and restarts	Home >Summary of Security Realms >myrealm >Providers >OBDXJWT			
Click the Lock & Edit button to modify, add or delete items in this domain. Lock & Edit Release Configuration	Settings for OBDXIWT Configuration Common Provider Sectors Common Provider Sectors			
Domain Structure	Circk the Lock a Lan button in the Change Center to mouny the settings on this page.			
Domain Partitions Environment	This page allows you to define the general configuration of this provider.			
Deployments B-Services	d			
Security Realms Interoperability Diagnostics	Bescription: OBDX Identity Assertion Provider (JWT and OAuth)			
	الله Version: 18.3.2.2.0,956			
How do I	Ative Types: Available: Cossen: Authorization			
No task help found.	30			
System Status Health of Running Servers as of 12:25 PM				
Failed (0) Critical (0)	Base64 Decoding Required: true			
Overloaded (0)	Save			



Step 7: Edit Oauth URL and add the following url and save. "http://{{host}}:{{manage-server-port}/digx-auth/v1/token/info"

ORACLE WebLogic Server Administration Console 12c			
Change Center	🏦 Home Log Out Preferences 🔐 Record Help		
View changes and restarts	Home >Summary of Security Realms >myrealm >Providers >OBDXJWT		
Click the Lock & Edit button to modify, add or	Settings for OBDXJWT		
delete items in this domain.	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		
B-Environment	This page allows you to configure additional attributes for this security provider.		
Deployments	OAuth URL: http://obdow/s.in.oracle.com		
Security Realms			
B-Diagnostics	SLEnabled		
	Save		
	Click the Lock & Edit button in the Change Center to modify the settings on this page.		
How do I			
No task help found.			
System Status 🗉			
Health of Running Servers as of 12:25 PM			
Failed (0)			
Critical (0)			
Uverloaded (0)			



9. Extensibility and Code Conventions

Code Convention of Account API's

Accounts related API should use below arguments and return type for working with UK Open Banking

Arguments

SessionContext sessionContext

 $com.ofss.digx.app.openbanking.dto.accounts.uk.AccountRequest DTO\\accountRequest DTO$

Return Type

BaseResponseDTO<T>

Where T extends DataTransferObject

Any service implemented with the above type of argument will be compatible with UK Open Banking.

Code Convention of Payment API's

Payment related API should use below arguments and return type for working with UK Open Banking

Arguments

Create and Read Method

SessionContext sessionContext

Any DTO Object which extends com.ofss.digx.app.openbanking.dto.consent.uk.UKPaymentDTO

Any service implemented with the above type of argument will be compatible with UK Open Banking.

Error Message Framework

The Error Message Framework helps convert the OBAPI error response according to the UK Open Banking Specifications.

The error response structure for Open Banking Read/Write APIs is as follows:



The UK Open Banking specified error response is handled using DIGX_OB_UK_OBDX_ERROR_MAP table.

The contents of the table are as follows:

Column Name	Description
DIGX_ERROR_CODE	Represents the OBAPI error codes. This is a Primary and Unique Key
UK_ERROR_CODE	Represents the Open Banking specified error code
PATH	Represents the reference to the JSON Path of the field with error. Can be null.
URL	Represents the URL to help remediate the problem, or provide more information etc. Can be null.



For mapping OBAPI error codes with UK Open Banking specified codes below script can be used:

Insert into DIGX_OB_UK_OBDX_ERROR_MAP (DIGX_ERROR_CODE,UK_ERROR_CODE,PATH,URL) values ('%%OBDX Error Code%%',%%Open Banking specified error code%%', '%%Path%%', '%%URL%%');

For example -

Insert into DIGX_OB_UK_OBDX_ERROR_MAP (DIGX_ERROR_CODE,UK_ERROR_CODE,PATH,URL) values ('DIGX_OB_0010','UK.OBIE.Field.Missing', 'Data.Initiation ',null);

Below Query is used to check the OBAPI errors mapped with UK Open Banking specified error codes in the system

select * from DIGX_OB_UK_OBDX_ERROR_MAP;

For configuring HTTP status codes with custom message, below script can be used:

Insert into DIGX_FW_CONFIG_ALL_B (PROP_ID, CATEGORY_ID, PROP_VALUE, FACTORY_SHIPPED_FLAG, PROP_COMMENTS, SUMMARY_TEXT, CREATED_BY, CREATION_DATE, LAST_UPDATED_BY, LAST_UPDATED_DATE, OBJECT_STATUS, OBJECT_VERSION_NUMBER)

values ('%%HTTP Status code%%','OpenBankingErrorConfig','%%Error Message%%','N',null,'OpenBanking Error Message','ofssuser',sysdate,'ofssuser',sysdate,'Y',1);

Below Query is used to check the Open Banking HTTP status codes in the system

select * from digx_fw_config_all_b where category_id = ' OpenBankingErrorConfig';

Permission Response Handler

Permissions is used in only Account API's. Based on Permissions, Response is generated based on permissions.

OBAPI consists of Permission Handler against each type of permissions. This configuration is available in the table DIGX_OB_UK_PERMISSIONS_PRIMARY



The contents of the table are as follows:

Column Name	Description
SERVICEID	Represents the OBAPI Service Id for which the permission and its handler is available
PERMISSION	Represents Permission
RESPONSEHANDLER	Represent Permission Handler

Permission Handler can be overriden or can be newly introduced. This will be required for additional fields mapping which is not available OOTB. Steps for the same are as follows

Introducing Permission Handler

New Permisison Handler should implement interface IResponseHandler

New Permission Handler should have below methods

public static <T implements IResponseHandler> getInstance()

public <T extends DataTransferObject> assembleResponse(DataTransferObject object, List<String> permissions) – This method assembles response from object to the require response object which needs shown in the API response. Object is the response got from base sevice and T will be the response object require by API specifications. Assembling of the values will be done this method

public int getPriority() – This defines the high priority of the handler to be applied for assembling response in case of permissions and its handler has been consented by the user i.e. Basic and Detail permission will have different handlers but if the consent is both the permission the priority of the handler will decide which needs to be executed on high priority.

