

Berlin Open Banking Configuration Guide
Oracle Banking APIs
Patchset Release 21.1.1.0.0

Part No. F40802-01

June 2021

ORACLE®

Berlin Open Banking Configuration Guide

June 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. Preface	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. Objective and Scope.....	2-1
2.1 Background.....	2-1
3. Technology Stack	3-2
4. Pre-requisites	4-3
5. Headers Configuration	5-4
6. Properties	6-1
7. OAuth Configuration	7-1
7.1 UI configuration.....	7-1
7.2 Weblogic configuration	7-1
7.3 Code_challenge and Code_verifier configuration	7-3
8. Extensibility and Code Conventions	8-1

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 APIs Patchset Release 21.1.1.0.0, refer to the following documents:

- Oracle Banking APIs Installation Manuals

2. Objective and Scope

2.1 Background

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

Scope

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

3. Technology Stack

Software	Version
Java	Java JDK or JRE version 8
OBDX/OBAPI	21.1.0.0.0
OAuth	OBAPI Internal OAuth

Abbreviations

OOTB	Out of the Box
TPP	Third Party Providers
ASPSP	Account Servicing Payment Service Provider

4. Pre-requisites

- Java JDK or JRE version 7 or higher must be installed. For installation of Java please refer **Installation Guide**.
- OAuth Setup

5. Headers Configuration

There are three types of headers configuration available for Berlin Open Banking.

- System Headers (i.e. Mandatory Headers and its respective value validation)
- Configuration Headers (i.e. Mandatory Headers).
- API Configuration Headers (i.e. Mandatory Headers of a specific API)

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

System Headers:- 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 ('berlin.%%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-Request-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 ('berlin.%%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';
```

API Configuration Headers :- As of now in OOTB multiple headers have been added as mandatory. This header is required to be sent by the TPP to the ASPSP mandatorily with a corresponding suitable value.

Header name is validated if the entry is made for requested API only in case of API Configuration Headers.

For configuring more api 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 ('%%API_PATH%%.%%HTTP_METHOD%%','
OpenbankingApiConfigHeaders',%%HEADER NAME%%,'N',null,'Open
Banking','ofssuser',sysdate,'ofssuser',sysdate,'Y',1);
```

Example : Insert into DIGX_FW_CONFIG_ALL_B (PROP_ID, CATEGORY_ID, PROP_VALUE, FACTORY_SHIPPED_FLAG, PROP_COMMENTS, SUMMARY_TEXT, CREATED_BY, CREATION_DATE, LAST_UPDATED_BY, LAST_UPDATED_DATE, OBJECT_STATUS, OBJECT_VERSION_NUMBER) values ('accounts/{account-id}/balances.GET','OpenbankingApiConfigHeaders','Consent-ID','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 = 'OpenbankingApiConfigHeaders';
```

6. Properties

Below are the properties required to be updated in the Berlin 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_EXPIRYDAYS	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

Table:- AUTH_CONFIG

Category-Id :-AuthServerConfig

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
OAUTH_REDIRECT_HOST_PORT	http://{HOST}:{PORT}	'HOST' refers to the hostname/IP of the application 'PORT' refers to the application's port

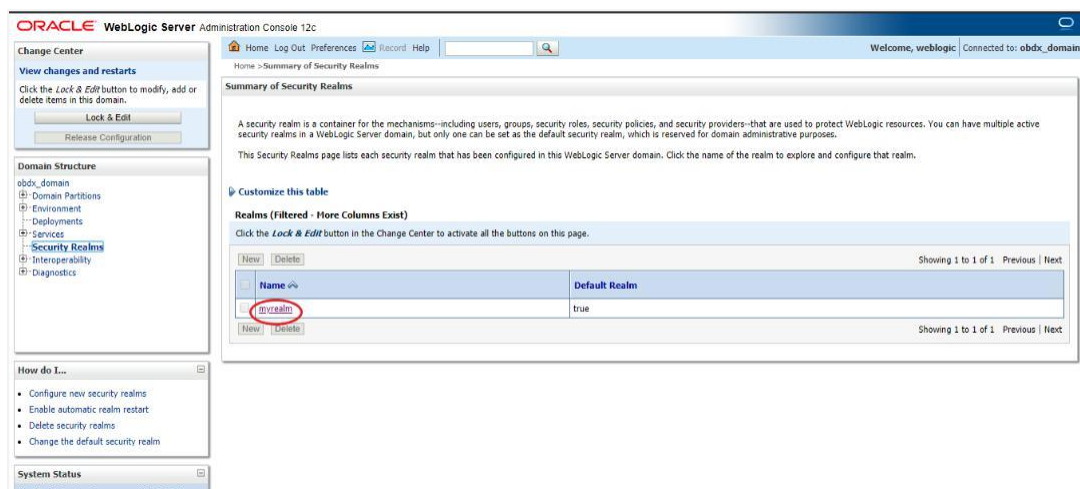
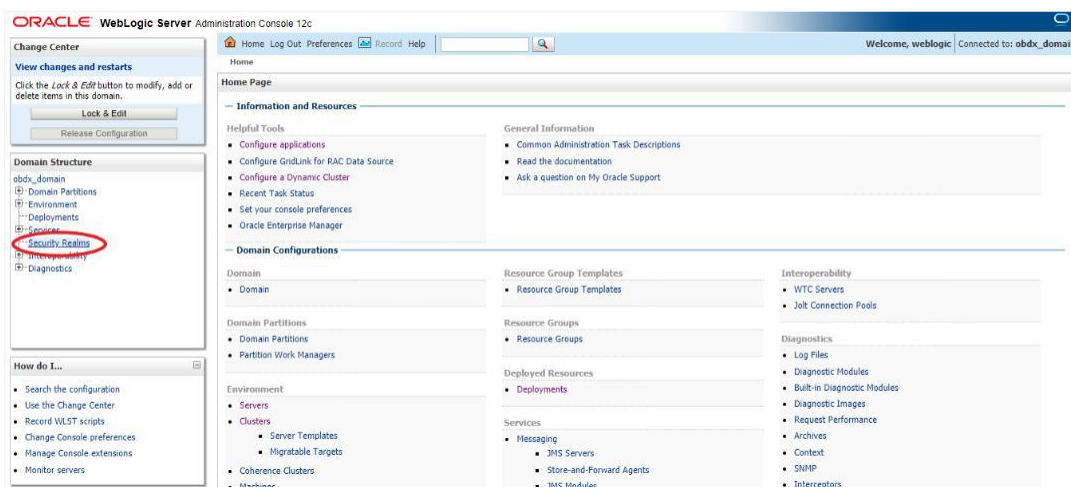
7. OAuth Configuration

7.1 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-berlin&homeModule=open-banking&applicationType=digx-auth&menuNavigationAvailable=false`.

7.2 Weblogic configuration



ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: obdx_domain

Home > Summary of Security Realms > myrealm

Settings for myrealm

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

General RDBMS Security Store User Lockout Performance

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

Save

Use this page to configure the general behavior of this security realm.

Note: If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.

Name: myrealm The name of this security realm. More Info...

Security Model Default: DD Only Specifies the default security model for Web applications or EJBs that are secured by this security realm. You can override this default during deployment. More Info...

Combined Role Mapping Enabled Determines how the role mappings in the Enterprise Application, Web application, and EJB containers interact. This setting is valid only for Web applications and EJBs that use the Advanced security model and that initialize roles from deployment descriptors. More Info...

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 attribute or invoke an MBean operation. More Info...

Automatically Restart After Non-Dynamic Changes Specifies whether the Realm will be auto-restarted if non-dynamic changes are made to the realm or providers within the realm. More Info...

ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: obdx_domain

Home > 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

Name	Description	Version
DBAuthenticator	OBOX - DB Authenticator	18.3.2.2.0.956
SQLAuth	Provider that performs DBMS authentication	1.0
OBDXJWT	OBOX Identity Assertion Provider (JWT and OAuth)	18.3.2.2.0.956
DefaultAuthenticator	WebLogic Authentication Provider	1.0
DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

New Delete Reorder Showing 1 to 5 of 5 Previous Next

ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: obdx_domain

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

Settings for OBDXJWT

Configuration **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: OBDXJWT

Description: OBOX Identity Assertion Provider (JWT and OAuth)

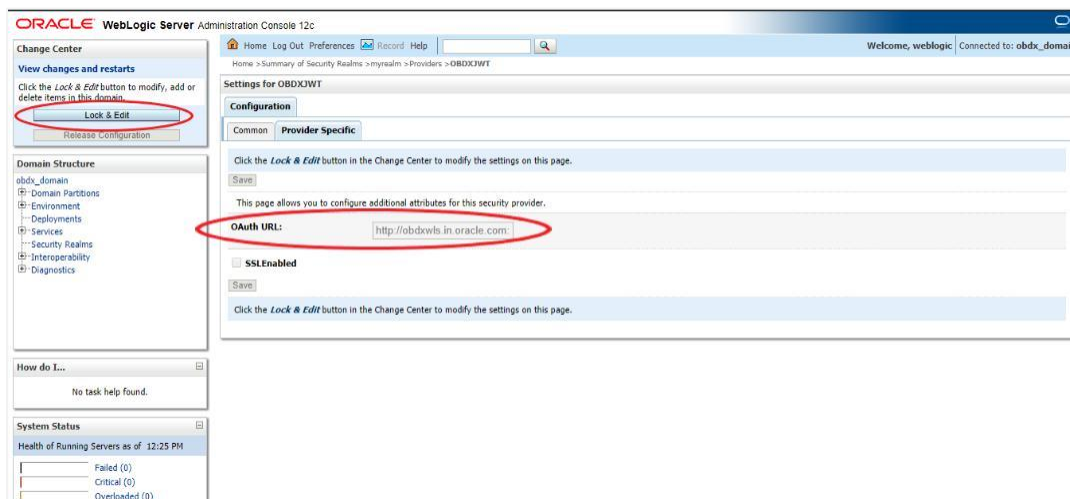
Version: 18.3.2.2.0.956

Active Types:

Available: [] Chosen: [x] Authorization

Base64 Decoding Required: true

Save



7.3 Code challenge and Code verifier configuration

Table: AUTH_CONFIG

Category-Id : AuthServerConfig

Property Id	Property Value	Purpose
isCodeChallengeEnabled	true/false	To enable/disable code_challenge and code_verifier functionality. The default value is 'false'.

8. Extensibility and Code Conventions

Error Message Framework

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

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

```

{ "tppMessages" :[
  {
    "category" : "",
    "path" : "",
    "code" : "",
    "text" : ""
  }
]
}

```

The Berlin Open Banking specified error response is handled using DIGX_OB_BERLIN_OBAPI_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
BERLIN_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 Berlin Open Banking specified codes below script can be used:

```
Insert into DIGX_OB_BERLIN_OBAPI_ERROR_MAP
(DIGX_ERROR_CODE,BERLIN_ERROR_CODE,PATH,URL) values ('%%OBAPI Error
Code%%','%%Open Banking specified error code%%', '%%Path%%', '%%URL%%');
```

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

```
select * from DIGX_OB_BERLIN_OBAPI_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';

[Home](#)