Data Protection Guide Oracle Banking APIs Patchset Release 21.1.5.0.0

Part No. F40802-01

May 2022

ORACLE

Data Protection Guide May 2022

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, 2022, 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.	Pro	reface	
	1.1	Intended Audience	
	1.2	Documentation Accessibility	
	1.3	Access to Oracle Support	1–1
	1.4	Structure	
	1.5	Related Information Sources	
2.	Ob	bjective and Scope	2-1
2	2.1	Background	2-1
2	2.2	Objective	2-1
2	2.3	Scope	2-1
3.	3. Personally Identifiable Information (PII)		
4. Flow of PII DataError! Bookmark no			
₹.	Flo	low of PII Data	.Error! Bookmark not defined.
. 5.		low of PII Data	
5.			Error! Bookmark not defined.
5.	Ad	dministration of PII Data	Error! Bookmark not defined.
5.	Ad 5.1	dministration of PII Data	Error! Bookmark not defined. rror! Bookmark not defined. rror! Bookmark not defined.
5.	Ad 5.1 5.2 5.3	dministration of PII DataE Extracting PII dataE Deleting or Purging PII dataE	Error! Bookmark not defined. rror! Bookmark not defined. rror! Bookmark not defined. rror! Bookmark not defined.
5. !	Ad 5.1 5.2 5.3 Ac	dministration of PII DataE Extracting PII dataE Deleting or Purging PII dataE Masking of PII dataE	Error! Bookmark not defined. rror! Bookmark not defined. rror! Bookmark not defined. rror! Bookmark not defined. 6–1
5. { { { {	Ad 5.1 5.2 5.3 Ac Us	dministration of PII DataE Extracting PII dataE Deleting or Purging PII dataE Masking of PII dataE ccess Control for Audit Information	Error! Bookmark not defined. rror! Bookmark not defined. rror! Bookmark not defined. rror! Bookmark not defined. 6–1

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 21.1.5.0.0, refer to the following documents:

Oracle Banking APIs Installation Manuals



2. Objective and Scope

2.1 Background

OBAPI is designed to help banks respond strategically to today's business challenges, while also transforming their business models and processes to reduce operating costs and improve productivity across both front and back offices. It is a one-stop solution for a bank that seeks to leverage Oracle Fusion experience across its core banking operations across its retail and corporate offerings.

OBAPI provides a unified yet scalable IT solution for a bank to manage its data and end-to-end business operations with an enriched user experience. It comprises pre-integrated enterprise applications leveraging and relying on the underlying Oracle Technology Stack to help reduce inhouse integration and testing efforts.

In order to provide these services OBAPI needs to acquire, use or store personally identifiable information (PII). In some cases, OBAPI may be owner of the PII data and in some other cases OBAPI might just acquire and use this data for providing required services to the customer.

2.2 Objective

By the very nature of PII data, it is necessary for the Bank to be aware of the information being acquired or used or stored by OBAPI. This knowledge will enable the Bank to take necessary measures and put apt policies and procedures in place to deal with PII data. In some of the geographies Bank might need to comply with local laws and regulations for dealing with PII data. This document attempts to provide necessary information so as to enable the Bank to do so.

2.3 <u>Scope</u>

This document is intended for technical staff of the Bank as well as administration users of the Bank and provides information about following aspects of the PII data.

- Identifies what PII data is acquired, used or stored in OBAPI
- Process to extract PII data from OBAPI
- Process to purge and delete the PII data from OBAPI

Out of scope

This document does not intend to suggest that OBAPI is out of box compliant with any local laws and regulations related to data protection. The purpose of this document is to provide information about PII data dealt with in the system so that the Bank can put in place appropriate processes to comply with laws and regulations of the land.



3. Personally Identifiable Information (PII)

Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used to de-anonymizing anonymous data can be considered PII.

OBAPI needs to acquire, use or store some PII data of the customers of the Bank in order to perform its desired services. This section declares the PII data captured by OBAPI so that the Bank is aware of the same and adopts necessary operational procedures and checks in order to protect PII data in the best interest of its customers.

Fields	OBAPI 21.1
Bank account information	Yes
Beneficiaries	Yes
Biometric records	No
Birthplace	No
Bonus	No
Country, state, or city of residence	Yes
Credit card numbers	No
Criminal record	No
Date of birth	Yes
Digital identity	No
Disability leave	No
Driver's license number	Yes
Education history	No
Email address	Yes
Emergency contacts	No
Employee ID	Yes
Ethnicity	No
Financial information and accounts	Yes
Fingerprints	No



Fields	OBAPI 21.1
Full name	Yes
Gender	Yes
Genetic information	No
Health information (including conditions, treatment, and payment)	No
Healthcare providers and plans	No
Personal/office telephone numbers	Yes
IP address	No
Job title	Yes
Login name	Yes
MAC address	Yes
Marital status	Yes
Military rank	No
Mother's maiden name	No
National identification number	Yes
Passport number	Yes
Performance evaluation	No
Personal phone number	Yes
Photographic images	No
PIN numbers	Yes
Political affiliations	No
Property title information	No
Religion	No
Salary	Yes
Screen name	No

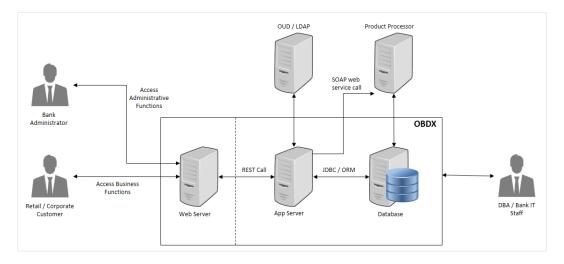


Fields	OBAPI 21.1
Sexual life	No
Social security number	Yes
Taxpayer information	Yes
Union membership	No
Vehicle registration number	Yes
Work telephone	Yes
Citizenship Number	No
Geo-Location	No
Product has Customer defined fields	No
Mobile Subscriber Identifier (IMSI)	No
Surname	Yes
First name	Yes



4. Flow of PII Data

This section depicts the flow 'personally identifiable information' (PII) within the OBAPI system in the form of a data flow diagram.



The Bank Administrator is Bank's employee who is performing administrative functions using OBAPI. As part of these, he will be dealing with PII data. An example is that the Administrator creates Retail and Corporate users in OBAPI and while creating users he/she enters user information such as first name, last name, email address, mobile number, correspondence address etc.

Retail / Corporate Customer is Bank's customer who is accessing the online banking features. As part of this he/she will be able to see his/her accounts, balances, beneficiaries, transactions, profile details etc. Note that OBAPI also supports onboarding of new users. The system captures some user information such as first name, last name, email address, mobile number, correspondence address and financial information such as income profile.

DBA / Bank IT Staff is Bank's employee who is not a user of OBAPI but has access to the database that stores OBAPI bank end data or the server environments on which OBAPI is deployed.

Web server typically contains static web content such as styling information (CSS), Javascript resources, images, static HTMLs etc. Web server passes the REST service calls to Application server.

Application (App) Server is the server on which OBAPI services are deployed. This server performs required processing on the service calls. It does use the database for retrieval or storage of data. It can also connect to external user credential store (such as OUD or Open LDAP). It can also connect to core product processor to enquiring CIF or Account related data or for posting any transactions initiated by the Retail or Corporate customer.



Database is the persistence store for OBAPI. It can contain primary configuration data, user data and transactional data.

OUD / LDAP represents the external user credentials store. OBAPI does not maintain user credentials locally but depends on external specialized software to do that. An example can be Oracle Unified Directory (OUD) or Open LDAP.

Product Processor is the core banking solution which actually processes actual banking transactions. OBAPI connects to the product processor to fetch data such as CIFs or Accounts or transactions. It also connects to the product processor to post new transaction initiated by Retail or Corporate customer.



5. Administration of PII Data

This section provides information about doing administrative tasks on PII data. This includes retrieval, modification, deletion or purging of such data.

5.1 Extracting PII data

OBAPI stores some PII data in its database and it also accesses data stored or owned by external systems such as OUD / LDAP or product processor.

5.1.1 Data stored in OBAPI

This section provides information about the tables that store PII data. This information is useful for the Bank to extract PII information.

PII Data	Table
Bank account information	DIGX_AC_ACCOUNT_NICKNAME DIGX_AM_ACCOUNT_ACCESS DIGX_AM_ACCOUNT_EXCEPTION
Beneficiaries	DIGX_PY_PAYEEGROUP DIGX_PY_PAYEE DIGX_PY_DOMESTIC_UK_PAYEE DIGX_PY_INTERNAL_PAYEE DIGX_PY_DEMANDDRAFT_PAYEE DIGX_PY_DOMESTIC_INDIA_PAYEE DIGX_PY_PEERTOPEER_PAYEE DIGX_PY_INTERNATIONAL_PAYEE DIGX_PY_DOMESTIC_SEPA_PAYEE DIGX_PY_GLOBAL_PAYEE
Country, state, or city of residence	DIGX_OR_APPLICANT, DIGX_OR_APPLICANT_ADDRESS DIGX_UM_USERPROFILE
Date of birth	DIGX_OR_APPLICANT DIGX_UM_USERPROFILE
Driver's license number	DIGX_OR_APLT_IDNT



PII Data	Table
Email address	DIGX_OR_APPLICANT_CONTACT DIGX_OR_EMAIL_VERIFICATION (used only for email verification, data is purged once email is verified) DIGX_UM_USERPROFILE
Email ID	DIGX_AP_TRANSACTION
Employee ID	DIGX_OR_APLT_EMPT
Financial information and accounts	Only financial information(Income, Asset, expense, Liability) DIGX_OR_APLT_FIN_INCM, DIGX_OR_APLT_FIN_AST, DIGX_OR_APLT_FIN_EXP, DIGX_OR_APLT_FIN_LIB
Full name	DIGX_OR_APPLICANT DIGX_UM_USERPROFILE DIGX_AP_TRANSACTION
Gender	DIGX_OR_APPLICANT
Personal/office telephone numbers	DIGX_OR_APPLICANT_CONTACT DIGX_UM_USERPROFILE DIGX_AP_TRANSACTION
Job title	DIGX_OR_APLT_EMPT DIGX_UM_USERPROFILE
Login name	DIGX_UM_USERAPPDATA DIGX_UM_USERPARTY_RELATION USERS GROUPMEMBERS DIGX_UM_USERPROFILE DIGX_AM_ACCOUNT_ACCESS
MAC Address	DIGX_AUDIT_LOGGING
Marital status	DIGX_OR_APPLICANT



PII Data	Table
National identification number	DIGX_OR_APLT_IDNT
Passport number	DIGX_OR_APLT_IDNT
Personal phone number	DIGX_OR_APPLICANT_CONTACT
PIN numbers	DIGX_OR_APPLICANT_ADDRESS
Salary	DIGX_OR_APLT_FIN_INCM, DIGX_OR_APLT_EMPT
Social security number	DIGX_OR_APLT_IDNT
Taxpayer information	DIGX_OR_APLT_IDNT
Vehicle registration number	DIGX_OR_APLT_IDNT
Work telephone	DIGX_OR_APPLICANT_CONTACT
Surname	DIGX_OR_APPLICANT DIGX_UM_USERPROFILE DIGX_AP_TRANSACTION
First name	DIGX_OR_APPLICANT DIGX_UM_USERPROFILE DIGX_AP_TRANSACTION

Please note that OBAPI provides user interface to access most of this data. The data will be accessible to you only if you have required roles and policies mapped to your OBAPI login. For example, an Administrator user can see retail user's profile only if he is entitled by a policy to access this information.

5.1.2 Data stored outside OBAPI

OBAPI can store user information in external systems such as OUD or LDAP. OBAPI provides screens for fetching this data. Please refer to the 'User Management' section of the Core user manual of OBAPI.

https://docs.oracle.com/cd/F30659_01/um_docs/User%20Manual%20Oracle%20Banking%20Dig ital%20Experience%20Core.pdf

Also note that the data can be accessed directly from the external system i.e. OUD, Open LDAP or the Product Processor. These details are outside the scope of this document. Please refer to the manual of corresponding software for more details.



5.2 **Deleting or Purging Pll data**

There are two ways in which PII data can be deleted or purged from the system.

5.2.1 Using User Interface

The information created in (or owned by) OBAPI can be deleted from its user interface. For example, a retail user can delete the beneficiaries he/she has maintained. Please refer to 'Manage Payee' section of following user manual for more details.

https://docs.oracle.com/cd/F30659_01/um_docs/User%20Manual%20Oracle%20Banking%20Dig ital%20Experience%20Retail%20Payments.pdf

Note that user's data such as CIF or account number is not owned by OBAPI and hence it cannot be deleted from OBAPI. However information such as account access granted to a particular user can be modified or deleted by the bank administrator. Please refer to 'Party Account Access' and 'User Account Access' sections of the Core user manual for more details.

https://docs.oracle.com/cd/F30659_01/um_docs/User%20Manual%20Oracle%20Banking%20Dig ital%20Experience%20Core.pdf

5.2.2 Using purge procedures

OBAPI provides some out of the box purge procedure that can be used to purge the data. Otherwise the DBA / IT staff can prepare similar procedures to purge required data. However note that it is not recommended to purge or delete any data stored in OBAPI tables without doing detailed impact analysis. Please also note that the purge jobs are useful typically for purging old data. They may not be useful for purging data of a specific customer.

Procedure name –

DIGX_USER_PII_DATA_PURGE.sql

Procedure input parameter -

User Id (unique identifier of user) which is to be purged.

Description -

DIGX_USER_PII_DATA_PURGE will permanently purge the user and all the PII data associated with the user from all the database tables of OBAPI.

It must be noted that once user is purged then associated PII data and user cannot be retrieved under any circumstances.

Associated table –

This table holds data of table names and field names of tables containing User Id. Procedure fetches data from table DIGX_UM_USERS_ASSOCIATIONS and deletes all the PII data related to the provided User Id



Steps to run -

Run the procedure with providing User Id as input parameter.

5.2.3 Manual truncation of data from backend

In scenarios where OBAPI does not have user interface to remove customer data and scheduled purge option is not useful, then data needs to be purged using SQL scripts. Below section provides some queries that can be used for such a purging. This option must be used with utmost care and proper impact analysis must be done before using these scripts.

PII Data	Table	Script
For modules other than Origination: Personal information of user including Country, state, or city of residence, Date of birth, Email address, Employee ID, Full name, Gender, Personal/offi ce telephone numbers, Login name, Work telephone, First Name, Surname	USERS GROUPMEMBERS DIGX_UM_USERPROFILE DIGX_UM_USERPARTY_RELATIO N DIGX_UM_REGISTRATION	<pre>delete from digx_um_userparty_relation where user_id = '<user identifier="">'; delete from digx_um_userappdata where id = '<user identifier="">'; delete from DIGX_UM_USERPROFILE where U_NAME = '<user identifier="">'; delete from GROUPMEMBERS where G_MEMBER = '<user IDENTIFIER>'; delete from USERS where U_NAME = '<user identifier="">';</user></user </user></user></user></pre>
Bank Account Information	DIGX_AC_ACCOUNT_NICKNAME DIGX_AM_ACCOUNT_ACCESS DIGX_AM_ACCOUNT_EXCEPTION	delete from DIGX_AC_ACCOUNT_NICKNAME where USER_ID = <user IDENTIFIER>;</user



PII Data	Table	Script
		delete from DIGX_AM_ACCOUNT_EXCEPTION where ACCOUNT_ACCESS_ID in (select ACCOUNT_ACCESS_ID from DIGX_AM_ACCOUNT_ACCESS where ACCESS_LEVEL = 'USER' and USERID = <user IDENTIFIER>); delete from DIGX_AM_ACCOUNT_ACCESS where ACCESS_LEVEL = 'USER' and USERID = <user IDENTIFIER>;</user </user
Beneficiaries	DIGX_PY_PAYEEGROUP DIGX_PY_PAYEE DIGX_PY_DOMESTIC_UK_PAYEE DIGX_PY_INTERNAL_PAYEE DIGX_PY_DEMANDDRAFT_PAYEE DIGX_PY_INTNATNL_PAYEE_BNK DTLS DIGX_PY_DOMESTIC_INDIA_PAYE E DIGX_PY_PEERTOPEER_PAYEE DIGX_PY_INTERNATIONAL_PAYE E DIGX_PY_DOMESTIC_SEPA_PAYE E	delete from DIGX_PY_INTERNAL_PAYEE where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE where CREATED_BY = <user IDENTIFIER>); delete from DIGX_PY_DOMESTIC_UK_PAYEE where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE where CREATED_BY = <user IDENTIFIER>); delete from DIGX_PY_DEMANDDRAFT_PAYEE where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE where CREATED_BY = <user IDENTIFIER>); delete from DIGX_PY_INTNATNL_PAYEE_BNK DTLS where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE where CREATED_BY = <user IDENTIFIER>); delete from DIGX_PY_INTNATNL_PAYEE_BNK DTLS where CREATED_BY = <user IDENTIFIER>); delete from DIGX_PY_INTERNATIONAL_PAYE E</user </user </user </user </user



PII Data	Table	Script
		where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE where CREATED_BY = <user IDENTIFIER>);</user
		delete from DIGX_PY_DOMESTIC_INDIA_PAYE E
		where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE where CREATED_BY = <user IDENTIFIER>);</user
		delete from DIGX_PY_PEERTOPEER_PAYEE
		where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE where CREATED_BY = <user IDENTIFIER>);</user
		delete from DIGX_PY_DOMESTIC_SEPA_PAYE E
		where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE where CREATED_BY = <user IDENTIFIER>);</user
		delete from DIGX_PY_PAYEE where CREATED_BY = <user IDENTIFIER>;</user
		delete from DIGX_PY_PAYEEGROUP where CREATED_BY = <user IDENTIFIER>;</user



PII Data	Table	Script
Party/User Information in Originations	DIGX_OR_APPLICANT DIGX_OR_APPLICANT_ADDRESS	delete from DIGX_OR_APLT_FIN_INCM where APPLICANT_ID = ' <applicant IDENTIFIER>';</applicant
	DIGX_OR_APLT_IDNT DIGX_OR_APPLICANT_CONTACT DIGX_OR_EMAIL_VERIFICATION	delete from DIGX_OR_APLT_FIN_AST where APPLICANT_ID = ' <applicant IDENTIFIER>';</applicant
	DIGX_OR_APLT_EMPT	delete from DIGX_OR_APLT_FIN_EXP where APPLICANT_ID = ' <applicant IDENTIFIER>';</applicant
	DIGX_OR_APLT_FIN_INCM DIGX_OR_APLT_FIN_AST DIGX_OR_APLT_FIN_EXP	delete from DIGX_OR_APLT_FIN_LIB where APPLICANT_ID = ' <applicant IDENTIFIER>';</applicant
	DIGX_OR_APLT_FIN_LIB	delete from DIGX_OR_APLT_EMPT where APPLICANT_ID = ' <applicant identifier="">';</applicant>
		delete from DIGX_OR_APLT_IDNT where APPLICANT_ID = ' <applicant identifier="">';</applicant>
		delete from DIGX_OR_APPLICANT_CONTACT where APPLICANT_ID = ' <applicant identifier="">';</applicant>
		delete from DIGX_OR_EMAIL_VERIFICATION where SUBMISSION_ID = ' <submission identifier="">';</submission>
		delete from DIGX_OR_APPLICANT_ADDRESS where APPLICANT_ID = ' <applicant identifier="">';</applicant>
		delete from DIGX_OR_APPLICANT where PARTY_ID = ' <party IDENTIFIER>';</party



5.3 Masking of PII data

OBAPI framework provides a facility to mask user sensitive information before showing on the screen. Masking is a process in which only some portion of the data is displayed to the user while remaining portion of the data is either skipped or is replaced with hash characters such as '*'. Main purpose of masking is to avoid a possibility of 'over the shoulder' stealing of sensitive information. However it is also used so that the clear text sensitive information is not logged in system logs.

A typical example of masking is the account numbers. When OBAPI API is invoked that contains Account number is the response, the API will always give masked value. So complete clear text account number is never displayed on the screen.

Sr. No	Field Name
1	Party Identifier
2	Account Number (Includes current account, saving account, deposit, loan account)
3	Mobile/phone number
4	E-mail ID
5	Social Security Number
6	Submission Identifier
7	Application Identifier

OBAPI provides masking for following fields out of the box.



OBAPI framework also provides a provision in which any field other can the ones mentioned in above table can also be masked as per the requirement. This can be achieved by following steps:

- 1. Create a complex datatype in OBAPI. This datatype must extend com.ofss.digx.datatype.complex. MaskedIndirectedObject
- 2. Define a 'masking qualifier' and a 'masking attribute'
- 3. Configure this masking qualifier and masking attribute in DIGX_FW_CONFIG_ALL_B. An example of the configurations for account number mask is given below

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 ('*.account_id', 'Masking', 'AccountNumberMasking<', 'Y', null, null, 'ofssuser', sysdate, 'ofssuser', sysdate, 'A', 1);

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 ('AccountNumberMasking', 'MaskingPattern', 'xxxxxxxxNNNN', 'Y', null, null, 'ofssuser', sysdate, 'ofssuser', sysdate, 'A', 1);

With above steps, the OBAPI framework will make sure to mask the data of this data type during serialization phase in the REST tier.

The masking pattern can contain following characters

- 1. N Original character in the data will be retained
- 2. H Original character in the data will be skipped
- 3. * (Or any other placeholder character) Original character in the data will be replaced with this character



6. Access Control for Audit Information

OBAPI provides mechanism for maintaining audit trail of transactions / activities done by its users in the system. This audit trail is expected to be used for customer support, dispute handling. It can also be used for generating some management reports related to feature usage statistics etc.

From a data protection perspective it is worth noting that the audit trail contains

PII data in the form of transactional data as well as usage trends or statistics. Hence it is necessary for the Bank to put in place appropriate access control mechanisms so that only authorized Bank employees get access to this data. OBAPI provides comprehensive access control mechanism that the Bank can leverage to achieve this.

This access control can be achieved using the role based transaction mapping. This section focuses specifically from data protection aspect. You are requested to go through the user manual for 'Role Transaction Mapping' before reading further in this section. As an example, we have considered a use case where the Bank wants to restrict access to 'Audit Log' feature so that only the permitted set of administration users will be able to access audit of the users. Please note that same process can be applied to other services that deal with PII data. For example, same process can be used for restricting access to user management functions.

Check the 'out of box' access granted

There are two ways to check the Audit Information

- Maintenance
- Utilization

Maintenance (Performed by system admin)

- 1. Log in using Authadmin credentials.
- 2. Go to tab Role Transaction Mapping.
- 3. Find application role named "AuditAdmin" or "AuthAdmin".

Applications Place	ces Google Chrome					🖧 Tue	18:46 🗳 🐠 🕖
Role Transaction	n Ma 🗙 🔪						🕒 _ = ×
← → C ③ Not s	secure mum00chx:3333/in	dex.html?module=authadmin	&page=application-rol	e-base		o , Q 3	🏠 🔝 🔝 🏮 🗄
👯 Apps 🖿 17.3 🖡	Documentation 🖿 Web	DLogic Consol 🖿 Jenkins	Primavera - Time	🔜 JSONLint - The J	Server Logs 🖿 18	8.1 🖿 Bug 🖸 17.2 🖿 17.2 🖸 1	17.1 🖿 18.2 »
≡ 7⁄6≁						🔍 🖂 🌡 Welcome, Adn	ninistrator User 🗸 🍵
Role T	Transaction Mapping						
Use	er Type	All		\sim			
Арр	plication Role Name						
1	Search Cancel Clea					₹/	
Ap	oplication Role Details					Note	
	Internal External					An Application may have several Application Roles for different type of users under different User Segments	
Ad	dministrator					i.e. Retail, Corporate and Admin. These roles can be defined for internal as well as for external Access	
Ad	dminMaker	AdminMakerDisplayName				points and various transactions needs to be mapped to it.	
Ad	dminChecker	AdminCheckerDisplayName				Click below to create an Application Role and map it to various	
Au	uthAdmin	AuthAdminDisplayName				transactions for selected access points.	
ра	ayment	asa					
Au	uditAdmin	AuditDisplayName				Create	
Slack - Oracle-Deve	elo 🛛 🧐 [Inbox - Mozilla Thu	nd 🕷 [trunk - com.ofss.c	liqx 📴 middleware	e 🔝 [Or	acle SQL Developer	Role Transaction Mapp 🔚 harshal@	harshal-linux:~ 1/4



4. Click on AuditAdmin and click on edit symbol as shown.

Applications	Places Google Chrome							<u> </u>	Tue 18:46		ø
Role Trans	saction Ma ×									8 -	• ×
$\boldsymbol{\epsilon}$ \rightarrow C () Not secure mum00chx:3333/index.htm	nl?module=authadmin&pag	e=application-role-	read				0- G	1 🖈 📑	K O	:
🔛 Apps 🖿 1	.7.3 🖿 Documentation 🖿 WebLogic	Consol 🖿 Jenkins 🖸 Pr	rimavera - Time 🚦	🔜 JSONLint - The J	Server Logs	18.1	Bug 🖸 17	.2 🖿 17.2 🕻	17.1	18.2	»
≡ 76	~					(२, 🖂	& Welcome, /	Administrat ast login 05 Sep	or User 10.52 AM	*
F	Role Transaction Mapping										
	Application Role Name	AuditAdmin									
	Description	AuditDisplayName									. 1
	User Type	Administrator									. 1
	Access Type	INTERNAL							1		_
	Module Name							Click here to e	edit transa	ction ma	apping
	Map Transactions to Touch Points	Mobile Application	Mobile (Responsive)	Internet Misse	ed Call Banking	SMS Banking	Wearables	Snapshot			
		Perform	Approve	View							
	Transactions										. 1
	No data to display.										
											. 1
	Delete Cancel Back										. 1
											- 1
											_1
mum00chx:3333	/index.html?module=authadmin&page=a	application-role-read# <mark>e and</mark>			mation Terms and Co :le SQL Developer		ansaction Mapp		al@harshal-li		▼ 1/4
Stack - Oraci	le-Develo	w [trunk - com.orss.digx	[Pictures]	[Orac	te suit Developer	Role In	ansaction Mapp	harsha	auconarshal-li	nux:~	1/4

5. Assign module name "Admin Maintenance" and check "Internet".

Applications	Places Google Chrome		🚱 Tue 18:47 📫 🐠 🗹
Role Tran	saction Ma ×		() _ • ×
\leftrightarrow \Rightarrow G (Not secure mum00chx:3333/index.htm	l?module=authadmin&page=role-transaction-update	🕶 ९ 🛧 🐻 🔣 🧯 :
👯 Apps 🖿 1	17.3 🖿 Documentation 🖿 WebLogic	Consol 🖿 Jenkins 🧧 Primavera - Time 🔜 JSONLint - The J 🖿 Server Logs 🖿 18.1 🖿 Bug 🥃	17.2 🖿 17.2 🖸 17.1 🖿 18.2 »
= 76	ĸ	٩, 🖂	B Welcome, Administrator User V Last login 05 Sep 10.52 AM
1	Role Transaction Mapping		
	Application Role Name	AuditAdmin	
	Description	AuditDisplayName	
	User Type	Administrator	
	Access Type	INTERNAL	1
	Module Name	Admin Maintenance ×	
	Map Transactions to Touch Points	Mobile Application Mobile (Responsive) Internet Missed Call Banking SMS Banking Weare Siv/Chatbot	ibles Snapshot
	Next Back		
	(opyright © 2006, 2017, Oracle and/or its affiliates. All rights reserved. Security Information Terms and Conditions	
Slack - Oraci	le-Develo 🧐 [Inbox - Mozilla Thund	🏽 [trunk - com.ofss.digx] 📄 [Pictures]	Mapp 📔 harshal@harshal-linux:~ 1/4



6. Under Admin maintenance give access of Module name Audit log to it and click save.

Applications	Places Google Chrome						🖧 Tue 18:47 🛔	4 0) 🗐
	action Ma ×							
€ → C 0	Not secure mum00chx:3333/index.h	tml?module=authadmin&page	e=role-transaction-update				• Q 🕁 📑 K	0 :
🔛 Apps 🖿 17	.3 🖿 Documentation 🖿 WebLogi	c Consol 🖿 Jenkins 🖸 Pri	imavera - Time 🛛 🔜 JSO	NLint - The J	Server Logs	🖿 18.1 🖿 Bug 🖸 17.2	🖿 17.2 🖸 17.1 🖿 18.2	? »
≡ 🏷	2					୯ ଅଧି	Welcome, Administrator Use Last login 05 Sep 10:52 AM	r₄∨ Î
			Internet					1
	Transactions		Perform	Approve	View			
	Admin Maintenance							
	ATM/Branch Maintenance							
	Access Point Maintenance							
	Account Relationship Mapping							
	Alert Maintenance							
	Approvals- Workflow Configure	ation				7		
	Audit Log							.
	Inquire Audit Log		×					
🛐 [Slack - Oracle	-Develo (3) [Inbox - Mozilla Thund	🐲 [trunk - com.ofss.digx	[Pictures]	🔋 [Orac	le SQL Developer	Role Transaction Mapp	harshal@harshal-linux~	1/4

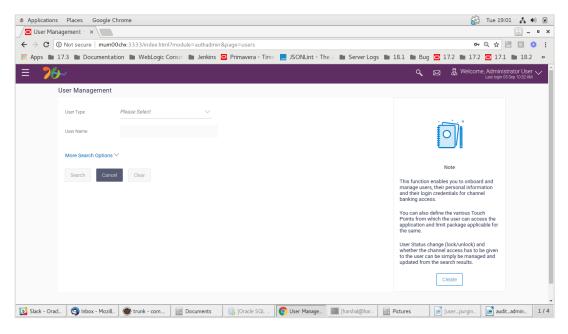
7. Submit.

Applications	Places Google Chrome					🚱 Tue 18:48 🔥	(I) 🗲
🖉 Update A	pplication (×					3 -	• ×
← ⇒ C (D Not secure mum00chx:3333/index.ht	ml?module=authadmin&pag	e=confirm-screen			॰ ९ ☆ 🗷 🔣	9 🗄
👯 Apps 🖿 🗄	17.3 🖿 Documentation 🖿 WebLogi	: Consol 🖿 Jenkins 🖸 Pr	imavera - Time 🛛 🔜 JSONL	int - The J 💼 Server Logs 🛛	🖿 18.1 🖿 Bug 🖸 17.2	🖿 17.2 🖸 17.1 🖿 18.2	»
= 76	×				9、⊠ &	Welcome, Administrator User Last login 05 Sep 10:52 AN	└ Î
	Update Application Role				ERROR		×
	CONFIRMATION				accessibility_issues	found_see_the_console_for_details	
	Maintenance completed successfully.						_
	Reference Number	0509E2D1ECE3					
	Status	Completed					
	Ok						
							_
		c0a.		Security Information Terms and Con			-
[🛐 [Slack - Orac	:le-Develo 🧐 [Inbox - Mozilla Thund	🐲 [trunk - com.ofss.digx	[Pictures]	🜏 [Oracle SQL Developer	🜔 Update Application Rol	🔚 harshal@harshal-linux:~	1/4



Utilization

- 1. Go to user management.
- 2. Click "Create" user.



3. Select Administrator.

Applications	Places Google Ch	rome						\$	Tue 19:02	(t)
🖉 User Manage	ement - ×								8 -	• ×
← → C () ►	lot secure mum00	chx:3333/index.html	module=authadmin	&page=users-create				07	Q 🕁 🗟 K	0 :
🚻 Apps 🖿 17.	3 🖿 Documentatio	on 🖿 WebLogic Co	onsol 🖿 Jenkins	Primavera - Time	🤜 JSONLint - The	🛛 🖿 Server Logs	5 🖿 18.1 🖿 Bug	17.2 17.2	🖸 17.1 🖿 18.3	2 »
≡ 78~	i -						٩	🖂 🤱 Welcom	e, Administrator Use Last login 05 Sep 10:52 Al	er 🗸 🌔
Us	er Management									
	User Type	Please Select	~							
	Cancel Back	Please Select Corporate User Administrator Retail User								
	Copyright @ 2006, 2017; Oracle and/or its affiliates. All rights reserved. Security Information Terms and Conditions									
🛐 Slack - Oracl	Inbox - Mozill	💮 trunk - com	🗑 Documents	[Oracle SQL	O User Manage	[harshal@har	Pictures	[user_purgin	audit_admin	1/4



4. Fill necessary details.

Applications Places Good	gle Chrome	🚱 Tue 19:03 🛔 🐠 🕢
User Management - 🗙 🛛		8 – • ×
← → C ③ Not secure m	num00chx:3333/index.html?module=authadmin&page=users-create	아 ☆ 🐻 🔣 🔇 🗄
🔛 Apps 🖿 17.3 🖿 Docum	entation 🖿 WebLogic Consol 🖿 Jenkins 🖸 Primavera - Time 🔜 JSONLint - The J 🖿 Server Logs 🖿 18.1 🖿 Bug	■ 17.2 ■ 17.2 ■ 17.1 ■ 18.2 »
≡ 🎾 🗧	√ ⊠	& Welcome, Administrator User 🗸
User Management		
User Type	Administrator \checkmark	
Organization	Oracle	
Manager	ABC	
Employee Number	121212	
User Name	AuditAdminUser Available	
Title	Mr \checkmark	
First Name	AuditAdminUser	
Middle Name		
Last Name	AuditAdminUser	
Date of Birth	04 Sep 2018	Ţ
🛐 Slack - Oracl 🧐 Inbox - M	tozil 🐲 trunk - com 🔄 Documents 🛛 🙀 [Oracle SOL 💽 User Manage 🔟 [harshal@har] 🚟 Pictures	user_purgin addit_admin 1/4

5. Select AuditAdmin or Authadmin as an application role.

Applie	cations Places Googl	e Chrome						8		4 () 🗲
🖉 🖸 Usi	er Management - 🛛 🗙 🔪									- • ×
\leftarrow \rightarrow	C 🛈 Not secure mu	m00chx:3333/index.html	?module=authadmir	&page=users-create					or 🕁 📑 K	0 :
👯 App	s 🖿 17.3 🖿 Documer	itation 🖿 WebLogic C	onsol 🖿 Jenkins	Primavera - Time	🤜 JSONLint - Th	e 💷 🖿 Server Logs	s 🖿 18.1 🖿 Bu	ig 🖸 17.2 🖿 17.3	2 🖸 17.1 🖿 18	.2 »
≡	76~						9, E	🛛 🔱 Welcome,	Administrator Use Last login 05 Sep 10:52 A	er 🗸 📍
	Address Line 4									
	Country	India	\sim							
	City	mumbai								
	Zip Code	123								
	Roles	AdminMaker	AdminChecker	AuthAdmin 📄 payn	nent					
		✓ AuditAdmin								
	Select Touch Points	Mobile Application	Mobile (Respons	ive) 🖌 Internet						
		Missed Call Banking	SMS Banking	Wearables	Snapshot					
		Siri/Chatbot								
	Add Accessible Entity]								
										_ I
										\frown
	Save Cancel	Back								
🛐 Slack	: - Oracl 🧐 Inbox - Mo:	zill 🔅 trunk - com	Documents	👸 [Oracle SQL	O User Manage	🔚 [harshal@har	Pictures	[user_purgin	audit_admin	1/4



6. Submit

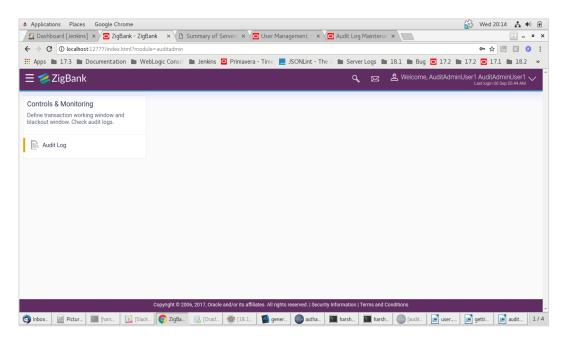
Applications	Places Google Ch	nrome						6	Tue 19:04 🛔	()
User Create	e - ZigBar × 🔪									• ×
← → C ①	Not secure mum00	chx:3333/index.html	module=authadmin	&page=confirm-scree	n				ማ 🕁 📑 K	0 :
🔡 Apps 🖿 17	7.3 🖿 Documentati	on 💼 WebLogic Co	onsol 🖿 Jenkins	Primavera - Time	JSONLint - The J	Server Logs	🖿 18.1 🖿 E	Bug 🖸 17.2 🖿 17.3	2 🖸 17.1 🖿 18.2	»
= 76	⊬						Q I	🖂 🐰 Welcome,	Administrator User Last login 05 Sep 10.52 AM	Ŷ
User Crea	ate									
	IRMATION									
Maint	tenance completed su	ccessfully.								
Reference	e Number	05	09AB91A9AB							
Status		Co	mpleted							
Ok										
										_
					ights reserved. Security i	_				-
🛐 Slack - Oracl	🔄 🗐 Inbox - Mozill	💮 trunk - com	Documents	[[Oracle SQL	🧿 User Create 📗	[harshal@har	Pictures	[user_purgin	audit_admin	1/4

7. Log in using created user.

Applications	Places Google Chrome							1	分 Wed 20:1	14	()
🗕 Dashboard [[Jenkins] 🗙 🧧 ZigBank - ZigBank	× 🖉 🗅 Summary of Serv	rers 🗙 🧧 User Mana	gement ×	Audit Log	Maintenar ×					- "
← → C ()	localhost 12777/index.html?module=logir	1							야 ☆	B K	0 :
🛄 Apps 🖿 17	.3 🖿 Documentation 🖿 WebLogic	Conso 🖿 Jenkins 🖸	Primavera - Time 🔜	JSONLint - Th	e J 🖿 Serve	er Logs 🖿 🛙	8.1 🖿 Bug	17.2 17.2	L7.2 🧧 17.1	18	.2 »
≡ 🥏 ZigB	Bank										
	1										
ų	ZigB		ial secu	irity gua	arantee	ed.					
	AuditAdminUser1										
	۵ا										
	Login		n our ra	inge of	produc	ots					
	Forgot Username Forgot Passwor	d					_				
3 Inbox 🗐 F	Pictur 🔚 [hars 🛐 [Slack 🚺	ZigBa 📙 [Oracl	💓 [18.1 🛛 🚺 gener	autha	🔚 harsh	harsh	Caudit	user	📄 getti	audit	. 1/



8. User can access audit log.



Applications Places Good	gle Chrome						Wed 20:14	•) 🚱		
😰 Dashboard [Jenkins] 🗴 🖉 Audit Log Maintenar 🗴 🕐 Summary of Servers 🗴 🔁 User Management - 🗴 🔁 Audit Log Maintenar 🗴 👘										
← → C (0) localhost12777/index.html?module=auditadmin&page=audit-log ◆ ☆ C										
🗰 Apps 🖿 17.3 🖿 Docume	ntation 🖿 WebLogic Co	nso 🖿 Jenkins 🖸 Primaver	a - Time 🔜 JSONLint - The J	🖿 Server Logs 🖿	18.1 🖿 Bug	O 17.2 D 17.2	🖸 17.1 🖿 18.2	»		
Ξ 💋 ZigBank				9, 🖂	2 Welcome	, AuditAdminUser1 . La	AuditAdminUser1 Ist login 06 Sep 05:44 AM	\checkmark		
Audit Log Maintenanc	e							- 1		
Date and Time*	Today	~	Activity							
Party ID		Search P	User ID							
More search options >> Search Clear										
Date / Time	User ID / Name	Party ID / Name	User Type	Event	Action	Reference Number	Status	- 1		
06 Sep 2018 03:45:41 AM	superadmin Administrator User			Login			Success	- 1		
06 Sep 2018 04:02:52 AM	superadmin Administrator User			Login			Success	- 1		
Page 1 of 1 (1-2 of 2 items) K < 1 > X										
🌍 Inbox 🚊 Pictur 🔳 [ha	ırs 🛐 [Slack 🚺 💽 Ai	ıdit 🔋 [Oracl	. 🚺 gener 🍥 autha 🔳	harsh 🔚 harsh	audit	📑 user 💽 g	etti 💽 audit	1/4		

7. User exporting the PII data

This functionality will allow to download of user wise PII in CSV formats.

7.1 Administrator

1. Login as administrator

🏓 Bug 29720615 - OBDX MAILBOX 🛪 🛛 🏓 Summary Report 🛛 🛪	🏓 Bug 29722265 - CAN'T MODEFI 🛪 🖪 Advait Dighe - Aria People	🗴 📄 New Service Creation. 🛛 🗴 💽 ZgBank - ZgBank	x + - σ ×
← → C ▲ Not secure mum00chm:7777/index.html?module=io	gin		🕶 ★ 🔟 🔕 🐑 🖓 E
🗮 Apps 🧿 Oracle 🧧 https://eeho.fa.us2 🖻 Fusion 💽 ZigBank - Zig	Bank 🕲 Payvoll (O OBP GROC 🌱 SonarQube 🔮 OTE TIME SHEET	💷 😇 IIT 18.3 😇 OlM 🔮 WLS Docker 🌘 Swagger UI 🗶 V2 🚊 Trunk	Jenkins (O OBDX_GROC 🥃 IT 18.1 🌲 BUGDB 属 18.1 Logs 🚥
≡ 💋 ZigBank			j Login ∨
ALC: NO DECIDENT			THE REPORT OF THE REPORT OF
			and the second
	Vourfinancial	accurity guaranteed	A CONTRACTOR OF A CONTRACTOR A
	Four Infancial	security guaranteed.	
💋 💋 🌽 ZigBank			
A superadmin			
£	Choose from o	ur range of products	
	~		-
Login	ra .	79	
Forgot Username Forgot Password	Current Account	Auto Loans	Personal Loans
	-		
THE REAL PROPERTY OF		Achieve your Dre	
	A IN	"All your drea if we have the coura	ams can come true, ge to pursue them*
			Walt Disney
	1		
	Come of the second		

2. Click on "User Management" and search for any user (Corporate User/ Administrator / Retail User)

then clicked on the any "User Name" from the list of search users.

🏓 Bug 29720615 - OBDX MAILBOX 🗙 🛛 🏓 Summ	ary Report 🛛 🗙 🛛 🙀 Bug 29722265 - CA	AN'T MODIFY L 🗙 📔 Advait Digh	e - Aria People 🛛 🗙 🛛 🔁	New Service Creation. 🗙 💽 User	Management - ZigBank × +	– a ×
← → C (1) Not secure mum00chm:77	77/index.html?module=authadmin&page=users					🕶 🚖 🔟 🧔 🕐 🛛 🍓 🗄
👯 Apps 🚍 Oracle 🚍 https://eeho.fa.us2	Fusion 🥃 ZigBank - ZigBank 🚷 Payroll { 0	OBP GROC 🤺 SonarQube 🚷 (OTE TIME SHEET E 🧧 IT 18	3 🧧 CIM 🚷 WLS Docker 🌒 Swagger	UI 🗶 V2 🧕 Trunk Jenkins {0 OBDX_GROC 🖻	IT 18.1 🍌 BUGDB 🖂 18.1 Logs 🛛 😕
≡ 🥏 ZigBank					٩	Last login 07 May 11:45 AM
	User Management					
	Lose Type Retail User User Name retail More Search Optious ~ Search Results	~			Note This function enables you to onboard and manage users, there personal information and their login credentials for channel andming access.	
	Full Name	User Name	Status	Channel Access	You can also define the various Touch Points from which the user can access the	
	N1001 N100L	foretail182	Unlocked 🖉	Granted 🖉	application and limit package applicable for the same.	
	Mustufa Gari	retail	Unlocked 🖉	Granted 🥒	User Status change (lock/unlock) and	
	Ashok Jain	gloretail	Unlocked 🥒	Granted 🖉	whether the channel access has to be given to the user can be simply be managed and	
	KEERTHANA AGARWAL	mtretail	Unlocked 🖉	Granted 🥒	updated from the search results.	
	Ashok Jain	sayaliretail	Unlocked 🥒	Granted 🖉	Create	
	Jane Doe	shiniretail	Unlocked 🖉	Granted 🖉		
	Ashok Jain	shiniretailuser	Unlocked 🖉	Granted 🖉		
	asd asd	retail2	Unlocked 🖉	Granted 🖉		
	John Doe	adiretail5	Unlocked 🥒	Granted 🖉		
	Ashok Jain	retailuser	Unlocked 🥒	Granted 🖉		
	Page 1 of 2 (1-10 of 18 items) K	< <u>1</u> 2 → X				

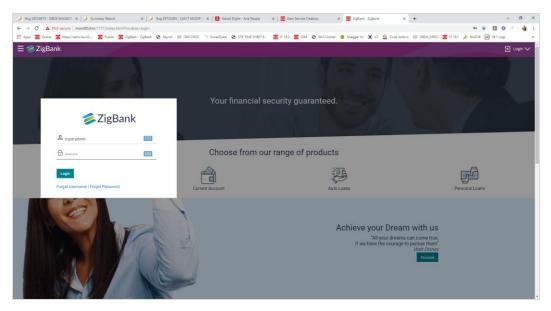


3. Clicked on the "Download profile" link.

lug 29720615 - OBOX MAILBOX 🗙 📔 🍌	Summary Report 🛛 🗙 🛛 😼 Bug 29723	2265 - CAN'T MODIFY L 🗙 🛛 🖪 Advait Dighe - Aria People	X Service Creation. X User Management - ZigBank	× +	- a
C Not secure mum00d		=user-read			er 🖈 🔟 🧿 🕐 🕴
os 🖻 Oracle 🗃 https://eeho.fa.us2	🖻 Fusion 🧧 ZigBank - ZigBank 🔇 Payro	al (O OBP GROC 🦄 SonarQube 😵 OTE TIME SHEET E	🖻 IT 18.3 📮 OlM 🔗 WLS Docker 🌐 Swagger Ul 🗶 V2 🧕 Trunk Je	nkins {0 OBDX_GROC 🖻	IT 18.1 🍌 BUGDB 🛃 18.1 Logs
ZigBank				٩	230 & Welcome, Administrator User Last login 07 May 11:45 AM
	User Management				
				Download profile	
	User Type	Retail User			
	Party ID	607287			
	Party Name	N1001			
	Personal Information				
	User Name	fcretail182			
	Title	Mr			
	First Name	N1001			
	Middle Name	N100M			
	Last Name	N100L			
	Date of Birth	11 Nov 1980			
	Contact Details				
	Email ID	himanshu.chawla@oracle.com			
	Contact Number (Mobile)	+919800000011			
	Contact Number (Landline)				
	Address Line 1	WQA			
	Address Line 2				
	Address Line 3				
	Address Line 4				
	Country	India			
	City	MUMBAI			
	Zip Code	99881			

7.2 Business User

1. Login as Business User (Retail/Corporate/Admin)





2. Clicked on "Profile"

🍌 Bug 29720615 - OECK MAILECH 😠 🛛 🖽 Summary Report	🛪 📔 🏄 Bug 29722265 - CAN'T MCDIFY 🛛 🗙 📔 Ádvalt Dighe - Aria People	X 🛛 😇 New Service Creation. X 😇 Dashboard - ZigBank	x + - 0
← → C () Not secure mum00chm:7777/index.html?module=	authadmin		er 🕁 🔟 0 🕐 诸
🗄 Apps 🔄 Oracle 🥃 https://eeho.fa.us2 💽 Fusion 🕃 ZigBank - 1	tigBank 🚱 Payroll { O OBP GROC 🦳 SonarQuibe 🧿 OTE TIME SHEET E	😇 IIT 18.3 🥃 DIM 🔇 WLS Docker 🐠 Swagger UI 🗶 V2 🚊 Trunk	lenkins 🔞 OBDIC_GROC 🧧 IT 18.1 🏓 BUGDB 📓 38.1 Logs
≡ 🤣 ZigBank			Q 😡 🚧 & Welcome, Administrator User 🔪
ashboard			Current Entity UBS 14.0 AT3 Branch 🗸
Onboarding			Notifications
Onboard and manage users, billers and merchants.			Date/Time Profile
			13 Apr 🕐 Logout
User Management			12.00 AM
By Merchant Management	° .		
Biller Onboarding			
			View All
Communications	Security	Templates	Limits
Manage user communications by publishing mailers and by definition alerts for each event.	Reduce security threats by maintaining two factor authentication and by defining complex password policy.	Define templates for capturing service requests and customer feedback: Set up SMS and Missed Call Banking.	Manage various types of limits for transaction and transaction group.
🗿 User Group Subject Mapping	Authentication	Service Request-Form Builder	Limit Definition
Alerts Maintenance	Security Question Maintenance	🚔 Feedback Template	Limit Package Management
Mallers	Password Policy Maintenance	SMS and Missed Call Banking	Transaction Group Maintenance
Common Services	Payments	Access Policies	Personal Finance
Anage entities and Day 1 configurations and various transaction spects. Maintain ATM and Branch locations and update services (fered. Enable Term deposit and Recurring deposit products on spital banking platform.	Payment purpose definition for each payment type. Restrict the number of payees that a retail user can create. Define and map biller categories. Set up forex deal related maintenances.	Manage Touch Points. Control access by defining user role- transaction mapping and by maintaining account relationships- transaction access.	Maintain spend and goal categories to facilitate customers to manage their personal finance.
System Configuration	Payment Purpose Mapping	Touch Points	Spend Category Maintenance
System Rules	Payee Restrictions	Touch Point Groups	Goal Category Maintenance

3. Clicked on "Download Profile"

🍌 Bug 29720615 - OBDX MAILBOX 🗙 🍌 Sum	ary Report 🛛 🗙 🛛 🕺 Bu	g 29722265 - CAN'T MODIFY X	Advait Dighe - Ar	ia People 🛛 🗙 🛛 🗖	lew Service Creation.	🗙 🔁 Му Р	rofile - ZigBank	×	+			-	a ×
← → C () Not secure mum00chm	77/index.html?module=authadmin8	Stpage=profile									07 🕁) i 🍲 🗄
👯 Apps 🖸 Oracle 🧧 https://eeho.fa.us2	🖸 Fusion 🧧 ZigBank - ZigBank 🔇	Payroll (O OBP GROC 🦄	SonarQube 🚷 OTE TI	ME SHEET E 📴 IT 18.3	B 🧧 OIM 😵 WLS Docke	Smagger	UI 🗶 V2 🧕 Tru	ink Jenkins	{O OBDX_GROC	🖸 IT 18.1	🍌 BUGDB 🛃	18.1 Logs	30
≡ 🥩 ZigBank									٩	⊠ ²³⁰	& Welcome	, Administrato et login 07 Mey 11	User 🗸 🍐
	My Profile												
	Administrator User							¥	Download Profile				
	Address HOMEPOSTAI Mumbai, IN, 4	LADDRESS, Goregaon, East, 00063.	Email Phone Number	sup****oracle.com +919****4321		Date of Birth	06 Jun 1990						
	Ok												
		Copyright	© 2006, 2017, Oracle and/or	its affiliates. All rights reserve	s. Security Information Terms an	d Conditiona							

<u>Home</u>



8. Third Party Consents

This option enables the user to manage the access provided to third party application(s). The user can define the fine-grained entitlements i.e. account level access along with a set of transactions for the third party. The user can disable the access for a specific third party application whenever required.

Note: Only those third party applications for which the user has registered and given rights to access his/her accounts for inquiries and transactions, will appear on this page.

How to reach here:

Dashboard > Toggle Menu > Account Settings > My Preferences > Third Party Application OR

Dashboard > My Profile > Profile > Third Party Application

Third Party Apps

≡ 💋 ZigBank				🔍 🖂 🚨 Welcome, Ashok Jain 🧹 Last login 29 Jun 06:47 PM
Third Party Consents				
Profile Primary Account Num Alerts/Notifications	Application Access	_		
Third Party Apps	Current & Savings Term Deposits	Loans		
Security and Login	Concentration (Concentration of Concentration of Concentr			
Settings	Map All Transactions CASA Inquiries CASA Inquiries CASA interest Certificate	Party CASA Interest Certificate	Inquire Sweep-in Instruction	
	Sweep-In Instruction	Delete Sweep-in Instruction		
	🕑 Loana 🖂			
	🖉 CASA			
	Replace Debit card	Request DC Limit Change	Reset Debit Gard Pin	Stop/Unblock Cheque
	Allow International Transaction on DC	C Request Debit Card Pin	Validate Card Details	Plock Debit Card
	Cheque Book Request	E-Statement Subscription	Demand Deposit Electronic Statement Download	List Demand Deposit Electronic Statement
	Apply Debit Gard	III Request Demand Deposit Statement		
	🗭 Term Deposits - Financial			
	🐼 New Deposit	IV TD TOP UP		
	All Inquiry Transactions CASA Inquiries			
	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx			
	Edit Cancel			
	Cancer			
Back To Dashboard				-



Field Description

Fie	eld Name	Description				
Third Party Application Name		The names of the third party applications are displayed. Select a third party application to define access to the application.				
Fie	eld Name	Description				
Ap	plication Access	The option to define whether access for the application is to be provided or not. If access is granted, then the user can revoke access and if it was revoked, then the user can grant access whenever required.				
Те	rrent and Savings/ rm Deposits/ Loans d Finances	Select a product to define account and transaction level access to the third party.				
1.	Select the third party	application for which you wish to define fine grained access.				
2.	The system will displa transactions	ay the list of accounts under each of the account types along with the				

- 3. Click Edit to modify account and transaction access. The Third Party Consents Edit
- 4. Screen with values in editable form appears. OR

Click $\ensuremath{\textbf{Cancel}}$ to cancel the operation and to navigate back to the Dashboard. OR

Click **Back** to Dashboard to go to the Dashboard.



Third Party Apps – Edit

Profile	MODEL Solutions	av	
Primary Account Num	op	ay .	
Alerts/Notifications	Application Access Grante	d	
hird Party Apps			
Security and Login	Current and Savings	Term Deposits	Loans and Finances
Settings	 xxxxxxxxxx0020 - Savings Account - Regular 		
	Map All Transactions		
	CASA Inquiries		
	 CASA Interest Certificate 	Party CASA Interest Certificate	
	✓ CASA		
	 E-Statement Subscription 	Demand Deposit Electronic Statement Download Electronic Statement	 Request Demand Deposit Statement
	 Payments 		
	Domestic Payment	✓ International Draft ✓ Bill Payment	 Domestic Draft
	 International Payout 	✓ External Transfer ✓ Internal Transfer	✓ PeerToPeer Transfer
	 Instruction Cancellation 	✓ Self Transfer	
	✓ All Inquiry Transactions		
	 Payments Inquiries 	CASA Inquiries	
	xxxxxxxxxxx0018 - Savings Account - Regular		
	Save Back Cancel		

Field Description

Field Name	Description
Third Party Application Name	The names of the third party applications are displayed. Select a third party application to define access to accounts and transactions.
Application Access	The option to define whether access for the application is to be provided or not.
Field Name	Description



Current and Savings/ Term Deposits/ Loans and Finances	Select a product to define account level access to the third party.
Accounts	All the accounts of the user are displayed under the respective account type.
Transactions	Once you select an account, all the transactions through which the account can be accessed are displayed. Select any or all transactions to provide account access for the transactions to the third party application.

- 1. Click the **Application Access** button to enable / disable access for the third party application.
 - a. If you select Enable,
 - Click an account type.
 The account check boxes are enabled and you can select/deselect any check box to edit access of these accounts to the third party application
 - ii. Select an account check box. The transactions for which the selected account can be accessed appear.
 - iii. Select/Deselect all or any of the transaction checkboxes to define the transactions through which the selected account can be accessed.
- 2. Click **Save** to save the changes.
 - OR Click **Back** to go back to previous screen. OR

Click **Cancel** to cancel the operation and navigate back to 'Dashboard.

3. The Third Party Consents – Review screen appears. Verify the details, and click Confirm. OR

Click Back to go back to the previous screen.

OR

Click Cancel to cancel the operation and navigate back to Dashboard.

- 4. The success message of third party consent setup appears along with the transaction reference number.
- 5. Click **OK** to complete the transaction and to navigate back to the Dashboard.



9. Device ID Consents

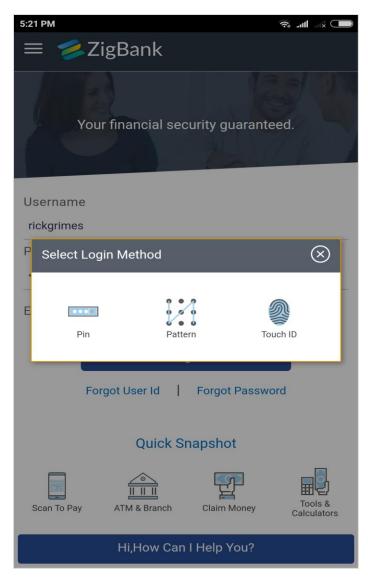
OBAPI framework provides a facility to enables the alternate login via Pin, pattern or touch ID.

1. On the login page, user will get the "Enable Alternate login" functionality. User needs to enable this for alternate login as pin, pattern or touch ID.

5:21 PM 🙃 att att 🗰
≡ 💋 ZigBank
Your financial security guaranteed.
Username
rickgrimes
Password
Enable Alternate Login
Login
Forgot User Id Forgot Password
Quick Snapshot
Scan To Pay ATM & Branch Claim Money
Hi,How Can I Help You?



2. Once user enables the functionality then, "Select Login Method" pop up will come from which user can select the alternate login method.





3. Once user will select the appropriate option, Notification of permission to store the device id message will display before setting up the alternate login method.

5:21 PM	
← Verify User	
Notification	\otimes
Permission to store the device Id. If you wa permit it then press proceed or press cance	nt to el.
Ok Cancel	_
-	_



Unregister the Device ID

In the Settings page, user can disable the alternate login from all mobile devices.

