Oracle® Banking Digital Experience

Data Protection Guide

Release 25.1.0.0.0
G38588-01
September 2025

Oracle Banking Digital Experience Data Protection Guide, Release 25.1.0.0.0

G38588-01

Contents

Preface

Purpose

This guide is designed to help acquaint you with the Oracle Banking application. This guide provides answers to specific features and procedures that the user need to be aware of the module to function successfully.

Before you Begin

Kindly refer to our **Getting Started User Guide** for common elements, including Symbols and Icons, Conventions Definitions, and so forth.

Pre-requisites

Specify **User ID** and **Password**, and login to **Home** screen.

Audience

This document is intended for the following audience:

- Customers
- Partners

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.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at Critical Patches, Security Alerts and Bulletins. All critical patches should be applied in a timely manner to ensure effective security, as strongly recommended by Oracle Software Security Assurance.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Resources

For more information on any related features, refer to the following documents:

- Oracle Banking Digital Experience Installation Manuals
- Oracle Banking Digital Experience Licensing Manuals

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Convention	Meaning
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes; actual screens that appear in the application may vary based on selected browser, theme, and mobile devices.

Acronyms and Abbreviations

The list of the acronyms and abbreviations used in this guide are as follows:

Table 1 Acronyms and Abbreviations

Abbreviation	Description
OBDX	Oracle Banking Digital Experience

Post-requisites

After finishing all the requirements, please log out from the **Home** screen.

1

Objective and Scope

2

Personally Identifiable Information (PII)

This topic provides information on **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.

OBDX 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 OBDX 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.

For more information on fields, refer to the field description table.

Table 2-1 PII Data Captured

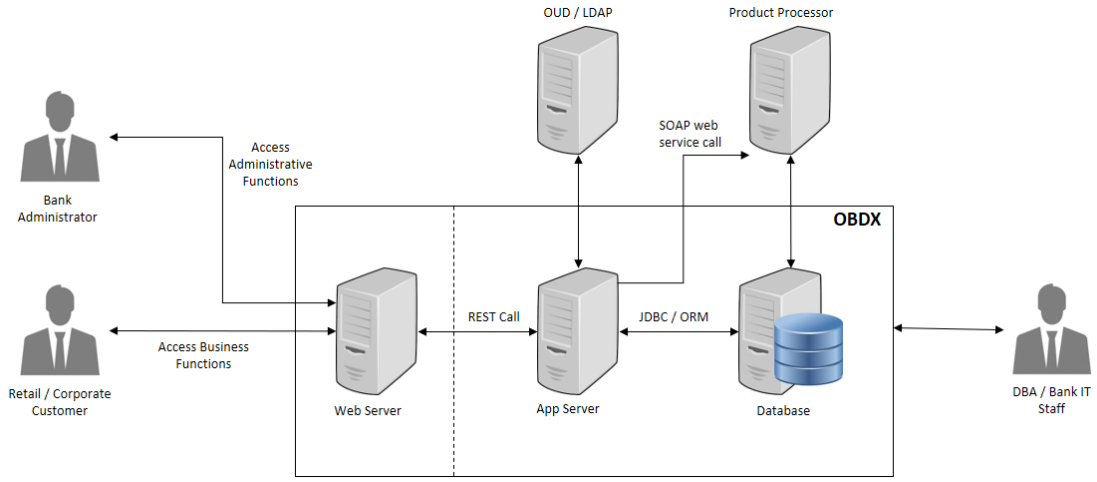
Fields	OBDX 22.2
Bank account information	Yes
Beneficiaries	Yes
Biometric records	No
Birthplace	No
Bonus	No
Country, state, or city of residence	Yes
Credit card numbers	No
Criminal record	No
Date of birth	Yes
Digital identity	No
Disability leave	No
Driver's license number	Yes
Education history	No
Email address	Yes
Emergency contacts	No
Employee ID	Yes
Ethnicity	No
Financial information and accounts	Yes
Fingerprints	No
Full name	Yes
Gender	Yes
Genetic information	No
Health information (including conditions, treatment, and payment)	No
Healthcare providers and plans	No

Table 2-1 (Cont.) PII Data Captured

Fields	OBDX 22.2
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	Yes
PIN numbers	Yes
Political affiliations	No
Property title information	No
Religion	No
Salary	Yes
Screen name	No
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

3
Flow of PII Data

This topic provides information on **Flow of PII Data**. This section depicts the flow **Personally Identifiable Information (PII)** within the OBDX system in the form of a data flow diagram.



The Bank Administrator is Bank's employee who is performing administrative functions using OBDX. As part of these, he will be dealing with PII data. An example is that the Administrator creates Retail and Corporate users in OBDX 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 OBDX 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 OBDX but has access to the database that stores OBDX bank end data or the server environments on which OBDX 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 OBDX 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 OBDX. It can contain primary configuration data, user data and transactional data.

OUD / LDAP represents the external user credentials store. OBDX 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. OBDX 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.

4

Administration of PII Data

This topic provides information on **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.

- Extracting PII data
  This topic provides information on **Extracting PII data**. OBDX 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.
- Deleting or Purging PII data
  This topic provides information on **Deleting or Purging PII data**. There are two ways in which PII data can be deleted or purged from the system.
- Masking of PII data
  OBDX framework provides a facility to mask user sensitive information before showing on the screen.

4.1 Extracting PII data

This topic provides information on **Extracting PII data**. OBDX 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.

- Data stored in OBDX
  This topic provides information on **Data stored in OBDX**. This section provides information about the tables that store PII data. This information is useful for the Bank to extract PII information.
- Data stored outside OBDX
  This topic provides information on **Data stored outside OBDX**. OBDX can store user information in external systems such as OUD or LDAP. OBDX provides screens for fetching this data. Please refer to the **User Management** topic of **User Manual Oracle Banking Digital Experience Core** of OBDX for more details.

4.1.1 Data stored in OBDX

This topic provides information on **Data stored in OBDX**. This section provides information about the tables that store PII data. This information is useful for the Bank to extract PII information.

This table describes PII data stored

> **Note**
>
> The fields which are marked as Required are mandatory.

For more information on fields, refer to the field description table.

Table 4-1 PII Data

PII Data	Table
Bank account information	DIGX_AC_ACCOUNT_NICKNAME
	DIGX_AM_ACCOUNT_ACCESS
	DIGX_AM_ACCOUNT_EXCEPTION
Beneficiaries	DIGX_PY_PAYEE_V3
	DIGX_PY_INTERNAL_PAYEE_V3
	DIGX_PY_DEMANDDRAFT_PAYEE_V3
	DIGX_PY_INTNATNL_PAYEE_BNKDTLS_V3
	DIGX_PY_PEERTOPEER_PAYEE_V3
	DIGX_PY_INTERNATIONAL_PAYEE_V3
	DIGX_PY_GLOBAL_PAYEE_V3
	DIGX_PY_DOMESTIC_PAYEE_V3
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
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

Table 4-1 (Cont.) PII Data

PII Data	Table
	DIGX_AM_ACCOUNT_ACCESS
MAC Address	DIGX_AUDIT_LOGGING
Marital status	DIGX_OR_APPLICANT
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 OBDX 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 OBDX login. For example, an Administrator user can see retail user's profile only if he is entitled by a policy to access this information.

4.1.2 Data stored outside OBDX

This topic provides information on **Data stored outside OBDX**. OBDX can store user information in external systems such as OUD or LDAP. OBDX provides screens for fetching this data. Please refer to the **User Management** topic of **User Manual Oracle Banking Digital Experience Core** of OBDX for more details.

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.

4.2 Deleting or Purging PII data

This topic provides information on **Deleting or Purging PII data**. There are two ways in which PII data can be deleted or purged from the system.

- Using User Interface
  This topic provides information on **Using User Interface**. The information created in (or owned by) OBDX can be deleted from its user interface. For example, a retail user can delete the beneficiaries he/she has maintained. Please refer to the **Manage Payee** topic of **User Manual Oracle Banking Digital Experience Retail Payments** for more details.

- Using purge procedures
  This topic provides information on **Using purge procedures**. OBDX 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.
- Manual truncation of data from backend
  This topic provides information on **Manual truncation of data from backend**. In scenarios where OBDX 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.

4.2.1 Using User Interface

This topic provides information on **Using User Interface**. The information created in (or owned by) OBDX can be deleted from its user interface. For example, a retail user can delete the beneficiaries he/she has maintained. Please refer to the **Manage Payee** topic of **User Manual Oracle Banking Digital Experience Retail Payments** for more details.

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

4.2.2 Using purge procedures

This topic provides information on **Using purge procedures**. OBDX 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 OBDX 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 OBDX.

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.

4.2.3 Manual truncation of data from backend

This topic provides information on **Manual truncation of data from backend**. In scenarios where OBDX 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.

> **Note**
>
> The fields which are marked as Required are mandatory.

For more information on fields, refer to the field description table.

Table 4-2 PII Data

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/office telephone numbers, Login name, Work telephone, First Name, Surname	USERS GROUPMEMBERS DIGX_UM_USERPROFILE DIGX_UM_USERAPPDATA DIGX_UM_USERPARTY_RELATION DIGX_UM_REGISTRATION	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>';

Table 4-2 (Cont.) PII Data

PII Data	Table	Script
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>; 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 fromDIGX_AM_ACCOUNT_ACCESS where ACCESS_LEVEL = 'USER' and USERID = <USER IDENTIFIER>;

Table 4-2 (Cont.) PII Data

PII Data	Table	Script

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_PAY EE
	DIGX_PY_PEERTOPEER_PAYEE
	DIGX_PY_INTERNATIONAL_PAYE E
	DIGX_PY_DOMESTIC_SEPA_PAYE E
		delete from DIGX_PY_INTNATNL_PAYEE_BNK DTLS_V3 where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE_V3 where CREATED_BY = <USER IDENTIFIER>);
		delete from DIGX_PY_INTERNATIONAL_PAYE E_V3 where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE_V3 where CREATED_BY = <USER IDENTIFIER>);
		delete from DIGX_PY_DEMANDDRAFT_PAYEE_ V3 where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE_V3 where CREATED_BY = <USER IDENTIFIER>);
		delete from DIGX_PY_DOMESTIC_PAYEE_V3 where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE_V3 where CREATED_BY = <USER IDENTIFIER>);
		delete from DIGX_PY_INTERNAL_PAYEE_V3 where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE_V3 where CREATED_BY = <USER IDENTIFIER>);
		delete from DIGX_PY_PEERTOPEER_PAYEE_V 3 where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE_V3 where CREATED_BY = <USER IDENTIFIER>);
		delete from DIGX_PY_PAYEE_PARTY_MAP_V3 where PAYEE_ID in (select PAYEE_ID from DIGX_PY_PAYEE_V3 where CREATED_BY = <USER IDENTIFIER>);
		delete from DIGX_PY_PAYEE_V3 where CREATED_BY = <USER IDENTIFIER>;

Table 4-2 (Cont.) PII Data

PII Data	Table	Script
Party/User Information in Originations	DIGX_OR_APPLICANT DIGX_OR_APPLICANT_ADDRESS delete from DIGX_OR_APLT_FIN_EXP where APPLICANT_ID = '<APPLICANT IDENTIFIER>'; DIGX_OR_APLT_IDNT DIGX_OR_APPLICANT_CONTACT DIGX_OR_EMAIL_VERIFICATION DIGX_OR_APLT_EMPT DIGX_OR_APLT_FIN_INCM DIGX_OR_APLT_FIN_AST DIGX_OR_APLT_FIN_EXP DIGX_OR_APLT_FIN_LIB	delete fromDIGX_OR_APLT_FIN_INCM where APPLICANT_ID = '<APPLICANT IDENTIFIER>'; delete from DIGX_OR_APLT_FIN_AST where APPLICANT_ID = '<APPLICANT IDENTIFIER>'; delete from DIGX_OR_APLT_FIN_LIB where APPLICANT_ID = '<APPLICANT IDENTIFIER>'; delete from DIGX_OR_APLT_EMPT where APPLICANT_ID = '<APPLICANT IDENTIFIER>'; delete from DIGX_OR_APLT_IDNT where APPLICANT_ID = '<APPLICANT IDENTIFIER>'; delete fromDIGX_OR_APPLICANT_CONTACT where APPLICANT_ID = '<APPLICANT IDENTIFIER>'; delete fromDIGX_OR_EMAIL_VERIFICATION where SUBMISSION_ID = '<SUBMISSION IDENTIFIER>'; delete fromDIGX_OR_APPLICANT_ADDRESS where APPLICANT_ID = '<APPLICANT IDENTIFIER>'; delete from DIGX_OR_APPLICANT where PARTY_ID = '<PARTY IDENTIFIER>';

4.3 Masking of PII data

OBDX 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 OBDX 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.

OBDX provides masking for following fields out of the box.

For more information on fields, refer to the field description table.

Table 4-3 Table 1

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

OBDX 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 OBDX.
   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', 'xxxxxxxxxxxxNNNN', 'Y',
null, null,
'ofssuser', sysdate, 'ofssuser', sysdate, 'A', 1);
```

With above steps, the OBDX 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

5

Access Control for Audit Information

This topic provides information on **Access Control for Audit Information**.

OBDX 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. OBDX 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.

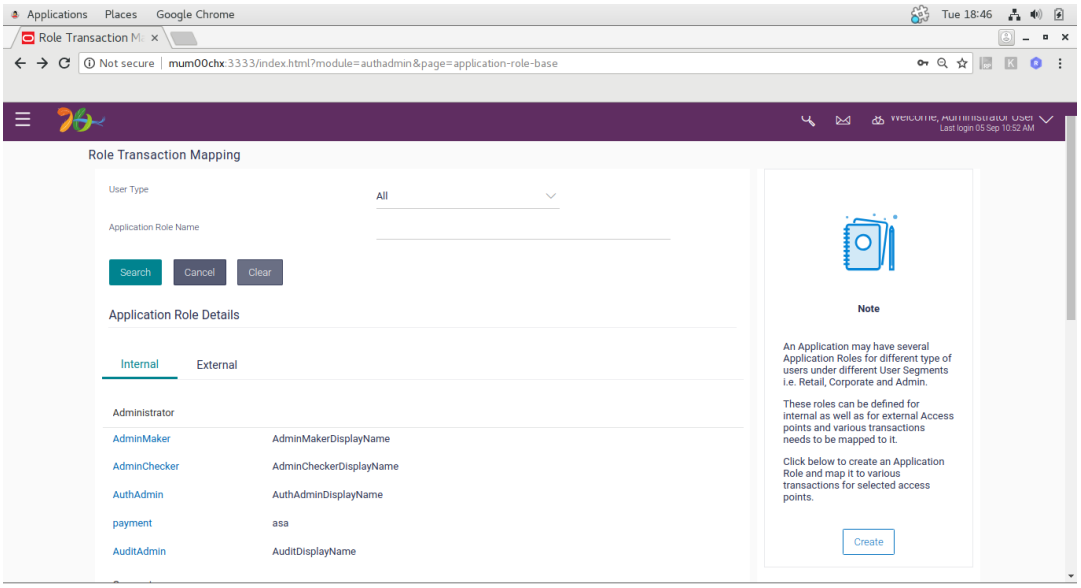
Check the ‘out of box’ access granted

There are two ways to check the Audit Information

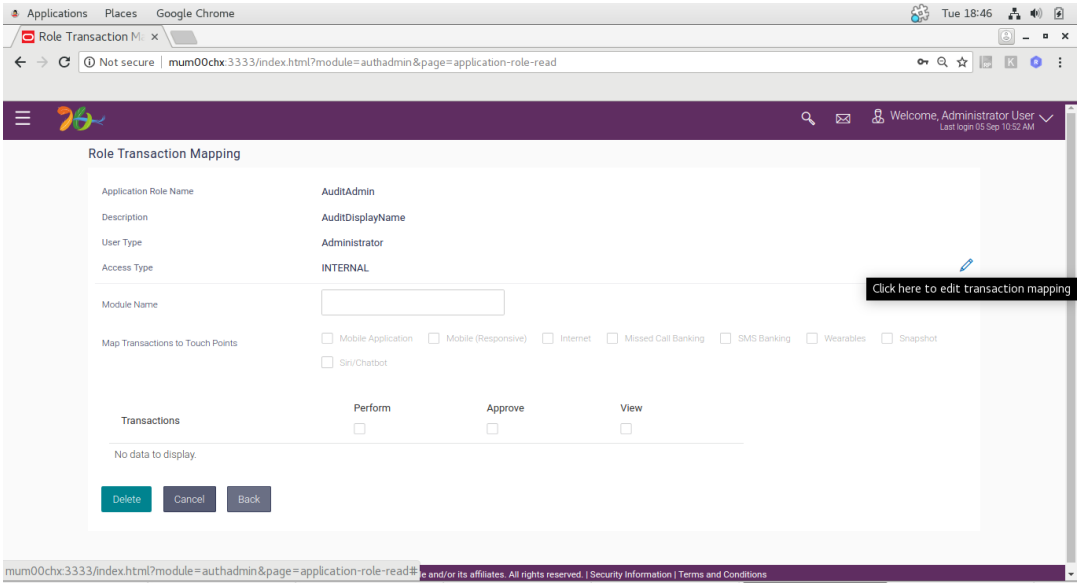
- Maintenance
- Utilization

Maintenance (Performed by system admin)

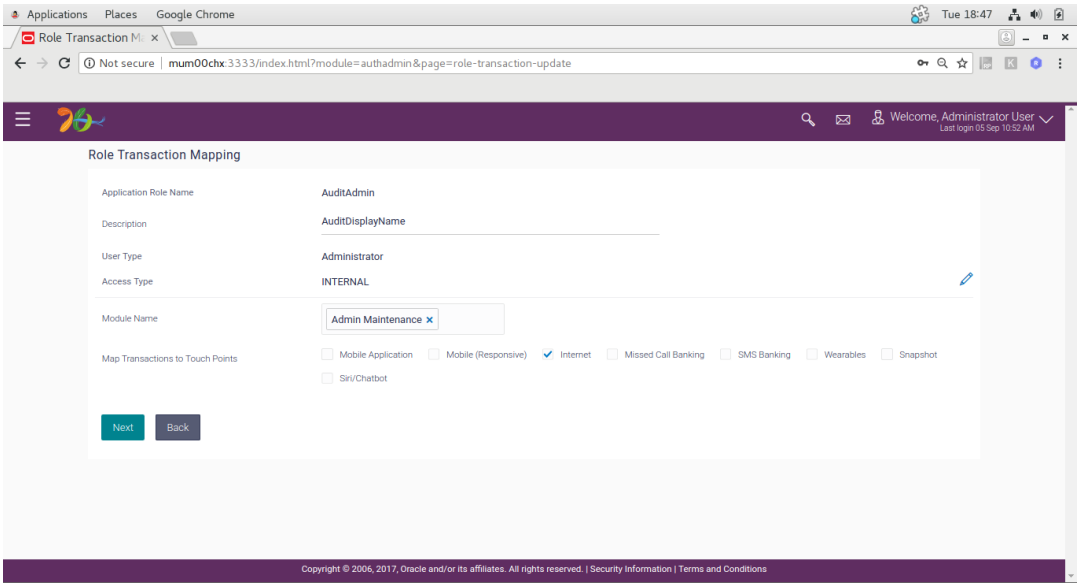
1. Log in using Authadmin credentials.
2. Go to tab **Role Transaction Mapping**.
3. Find application role named **“AuditAdmin”** or **“AuthAdmin”**.



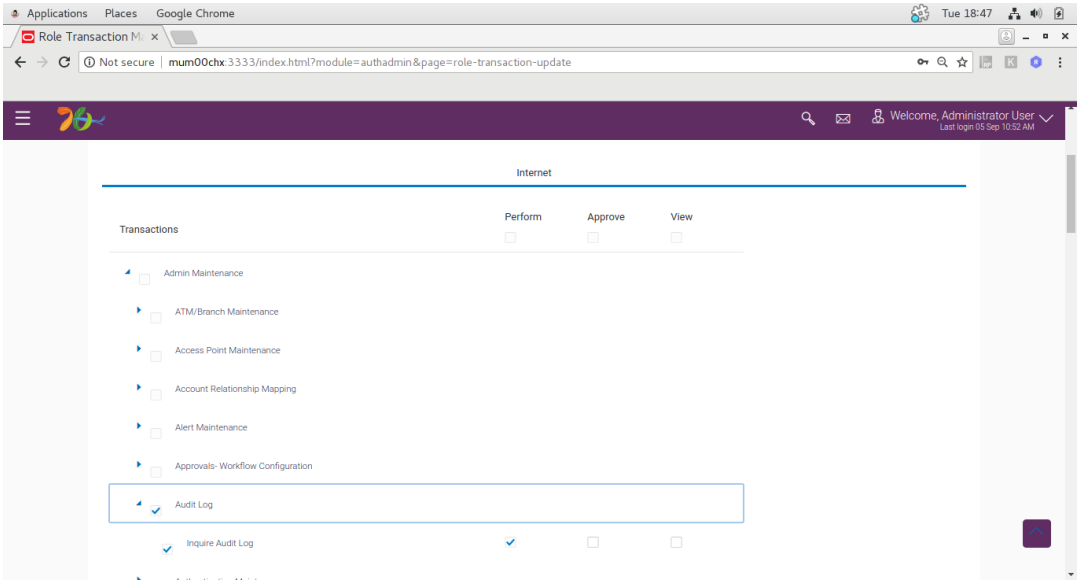
4. Click on **AuditAdmin** and click on edit symbol as shown.



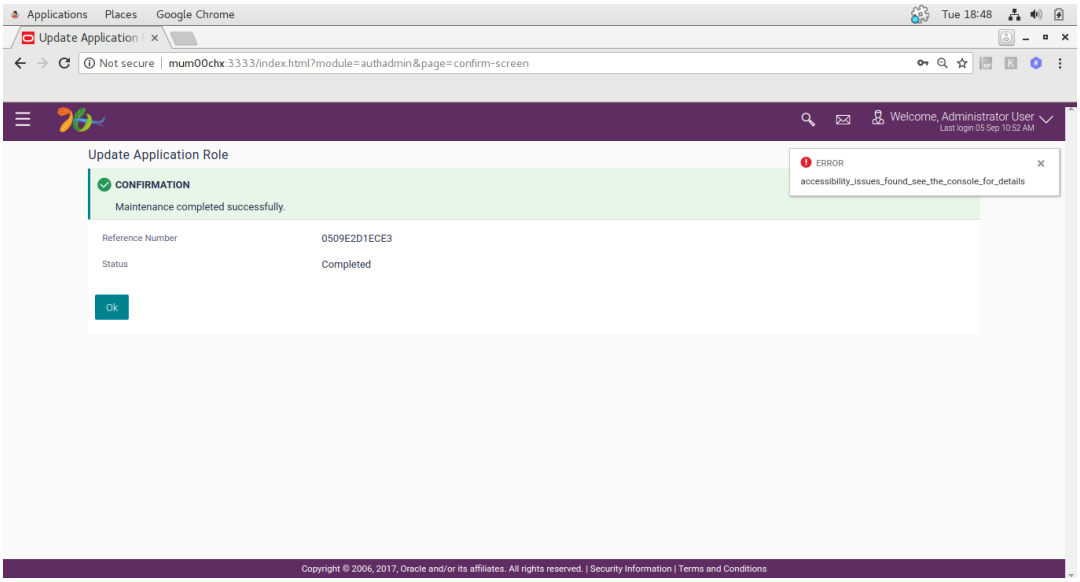
5. Assign module name **“Admin Maintenance”** and check **“Internet”**.



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

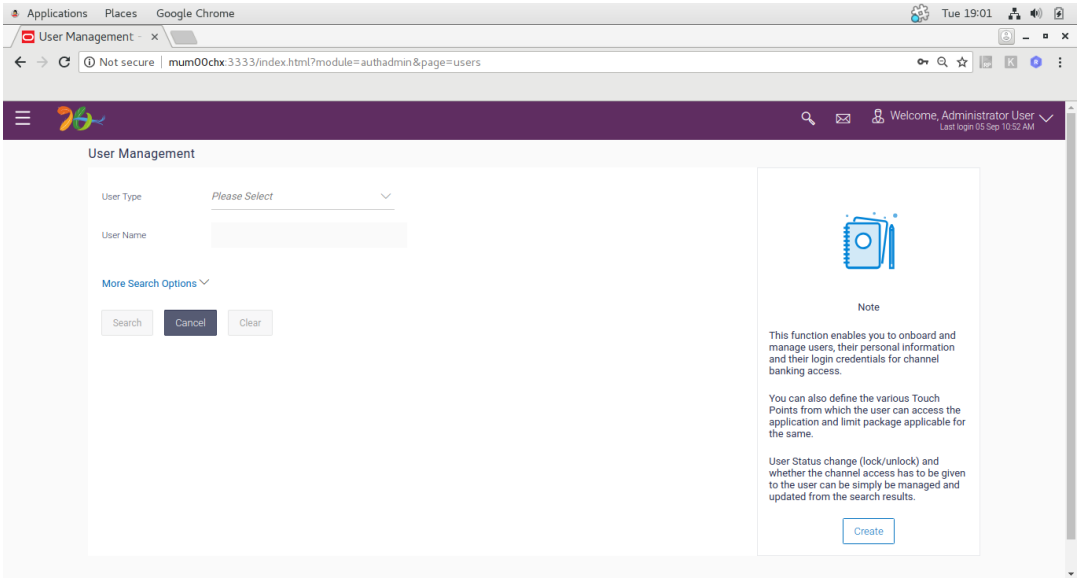


7. Click **Submit**.

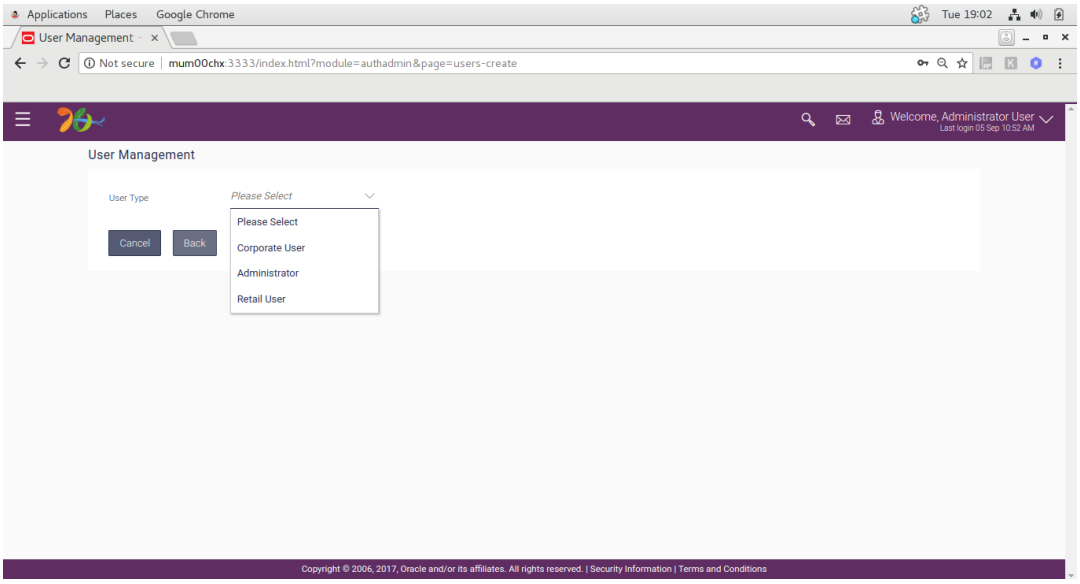


Utilization

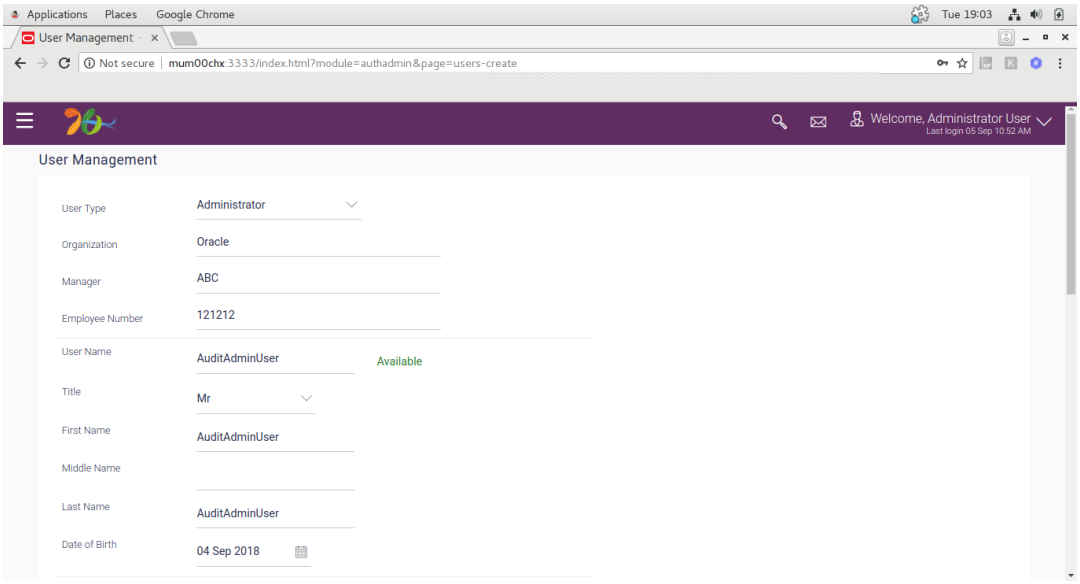
1. Go to **User Management**.
2. Click **Create** user.



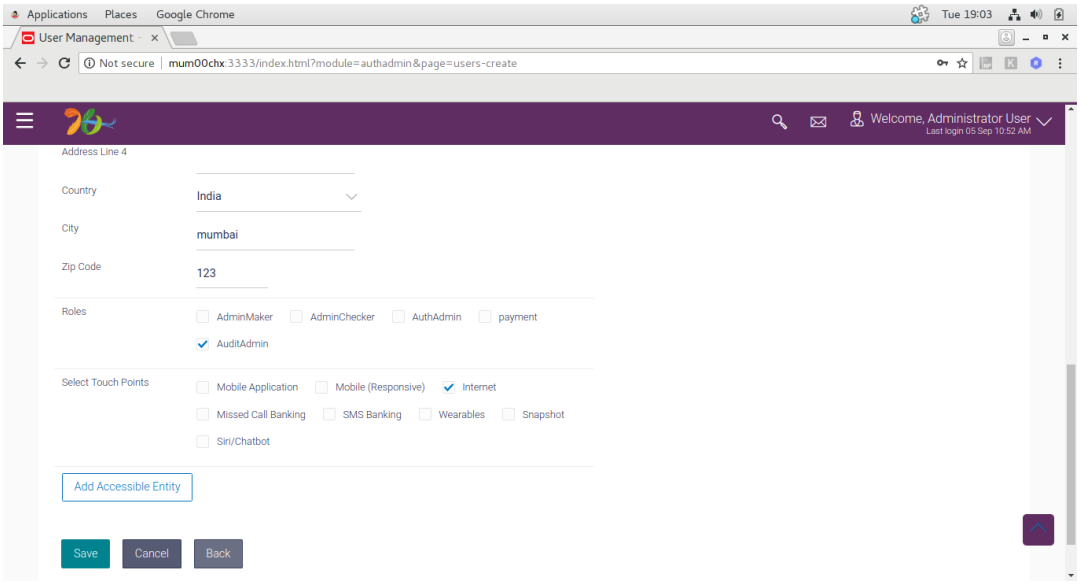
3. Select **Administrator**.



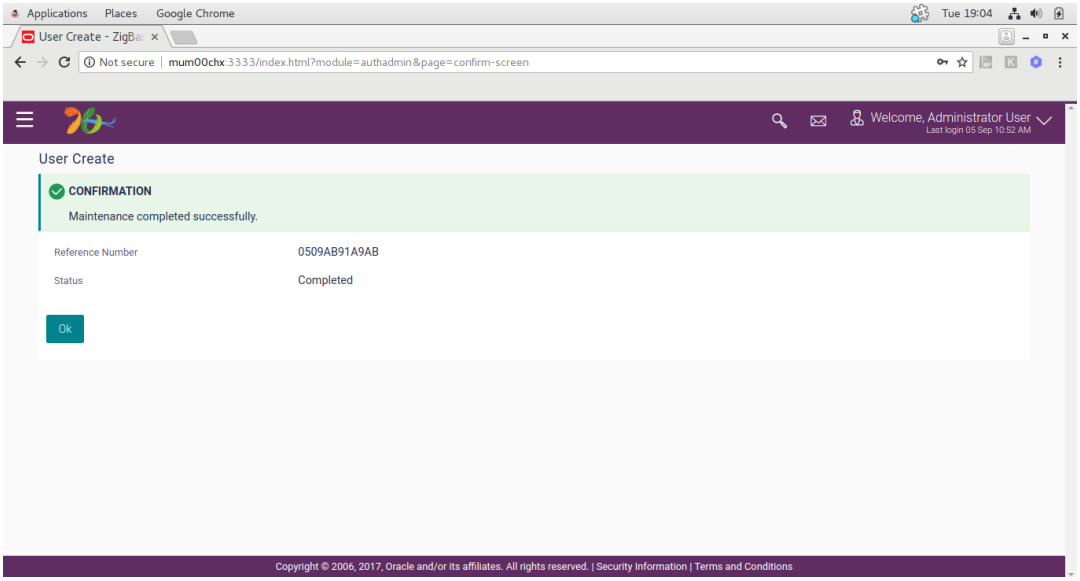
4. Fill necessary details.



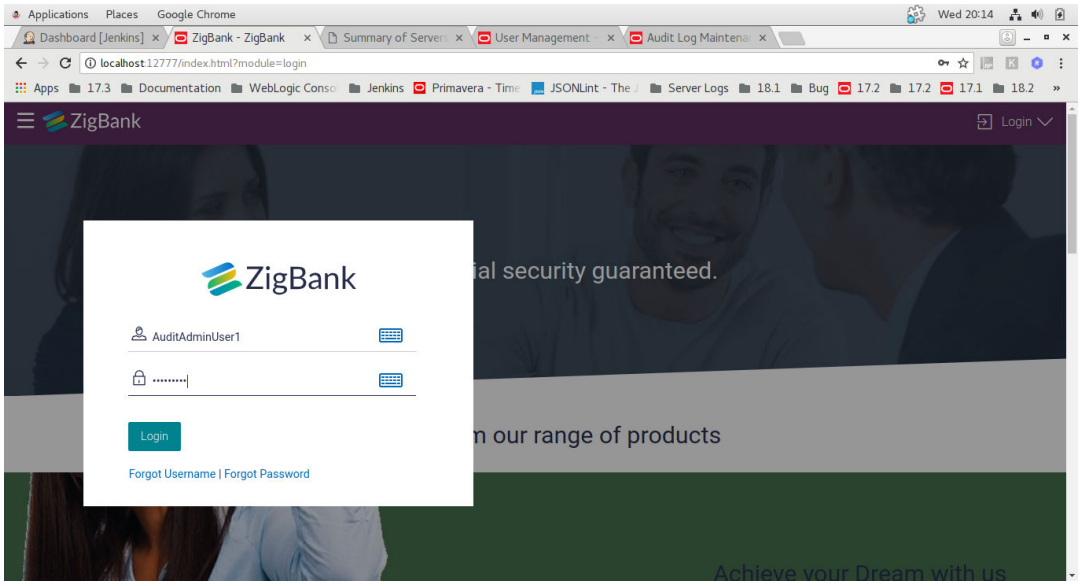
5. Select **AuditAdmin** or **Authadmin** as an application role.



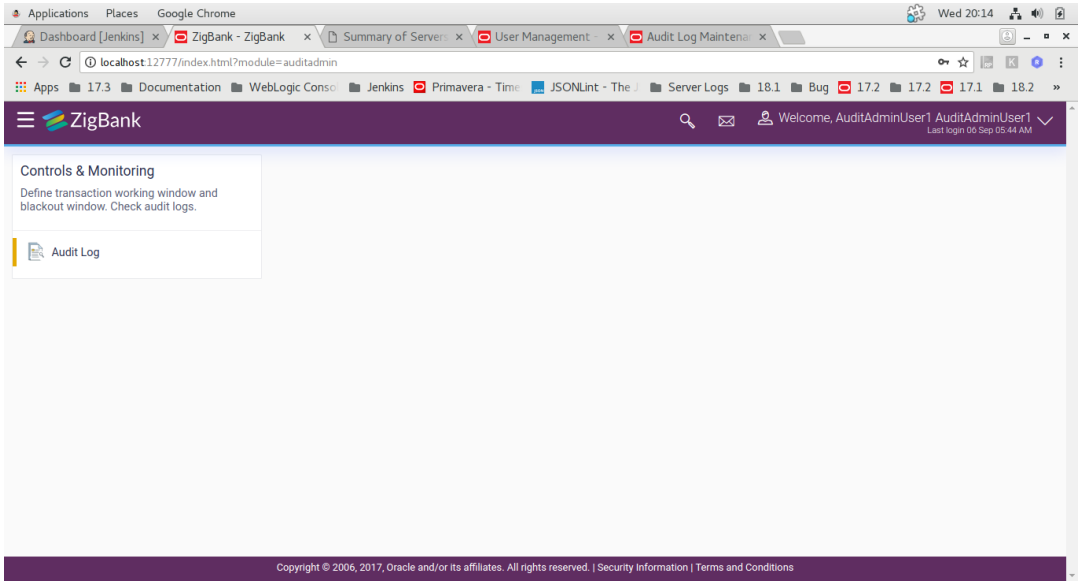
6. Click **Submit**.

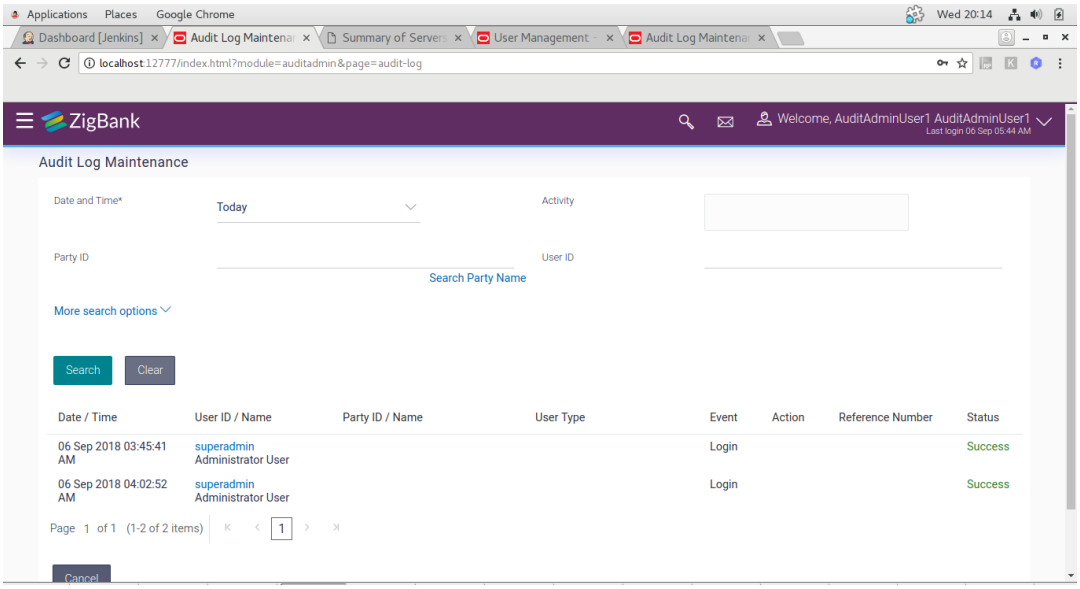


7. Log in using created user.



8. User can access audit log.





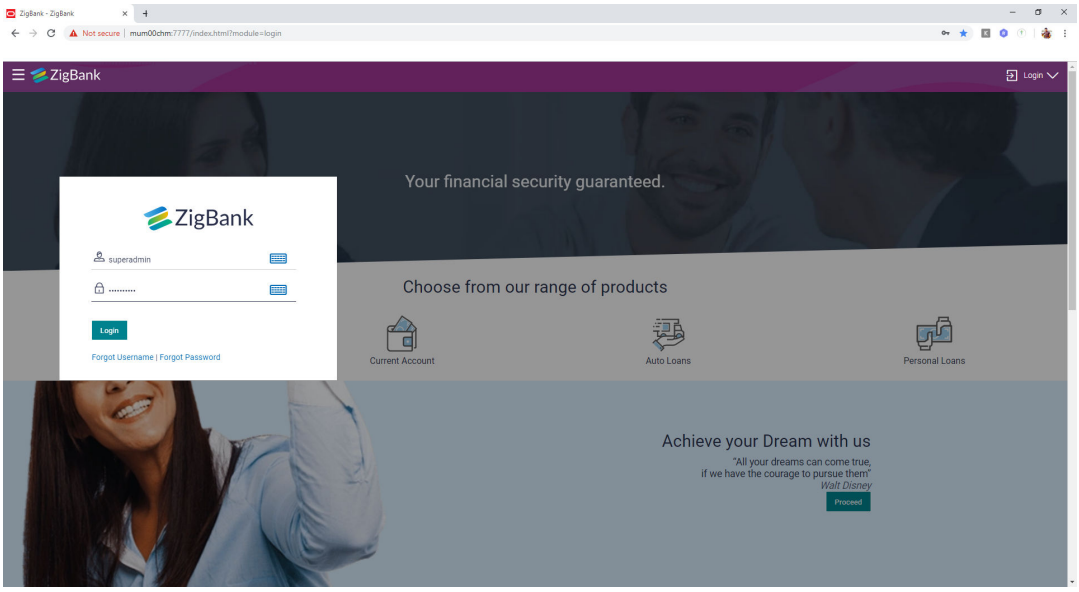
6

User exporting the PII data

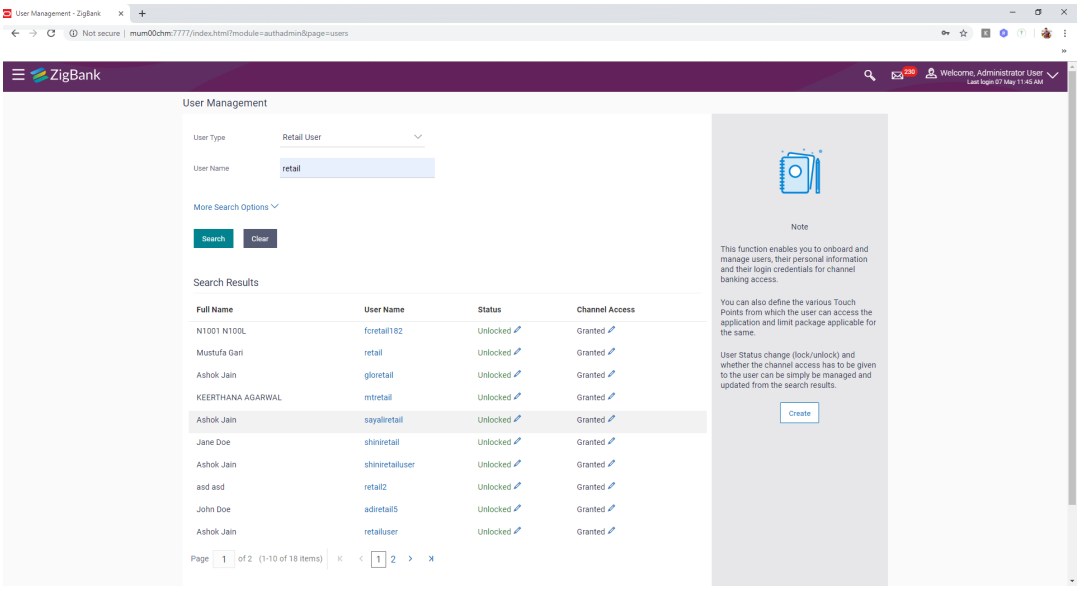
This topic describes the systematic instruction to **User exporting the PII data** option. This functionality will allow to download of user wise PII in CSV formats.

Administrator

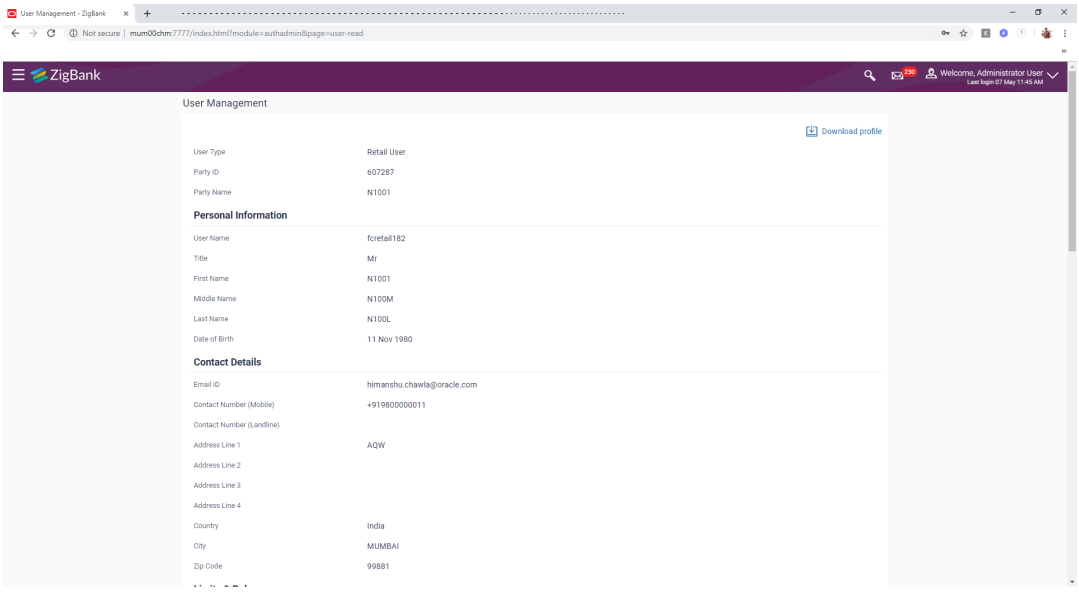
1. Login as administrator.



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.

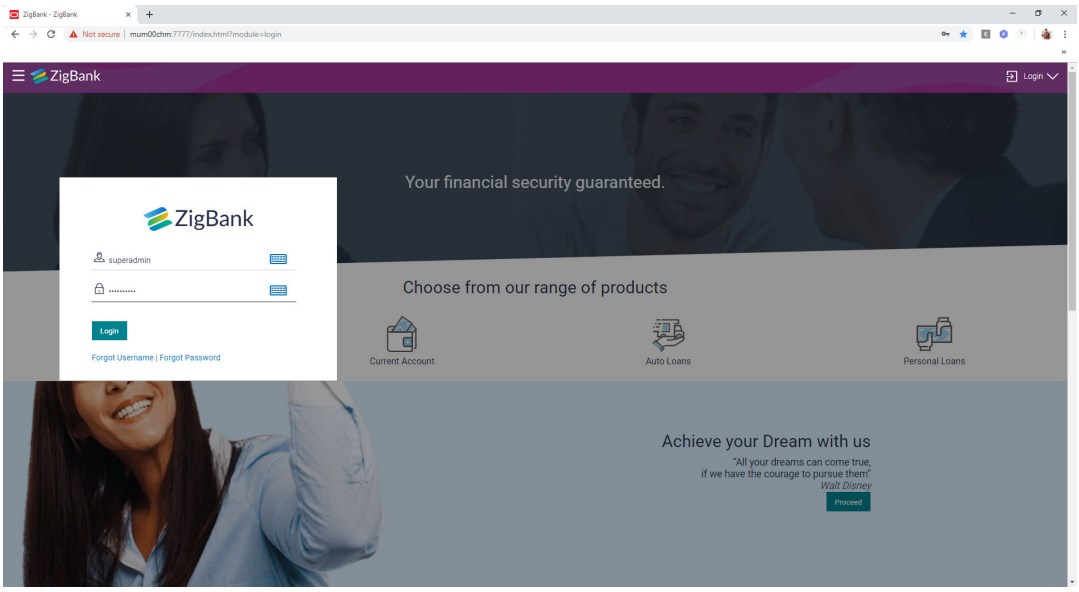


3. Click on the **Download Profile** link.

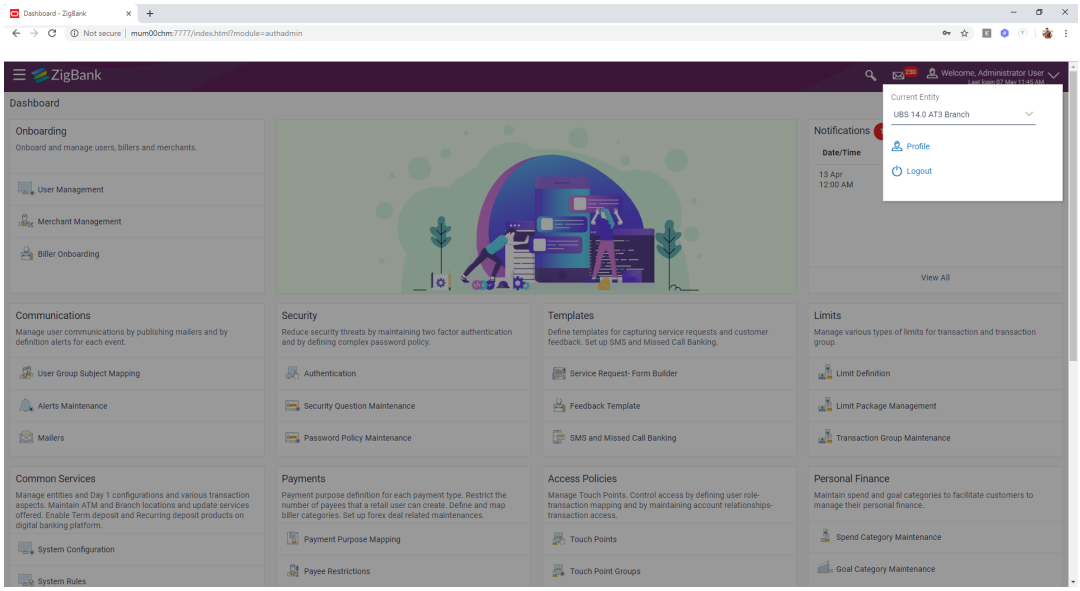


Business User

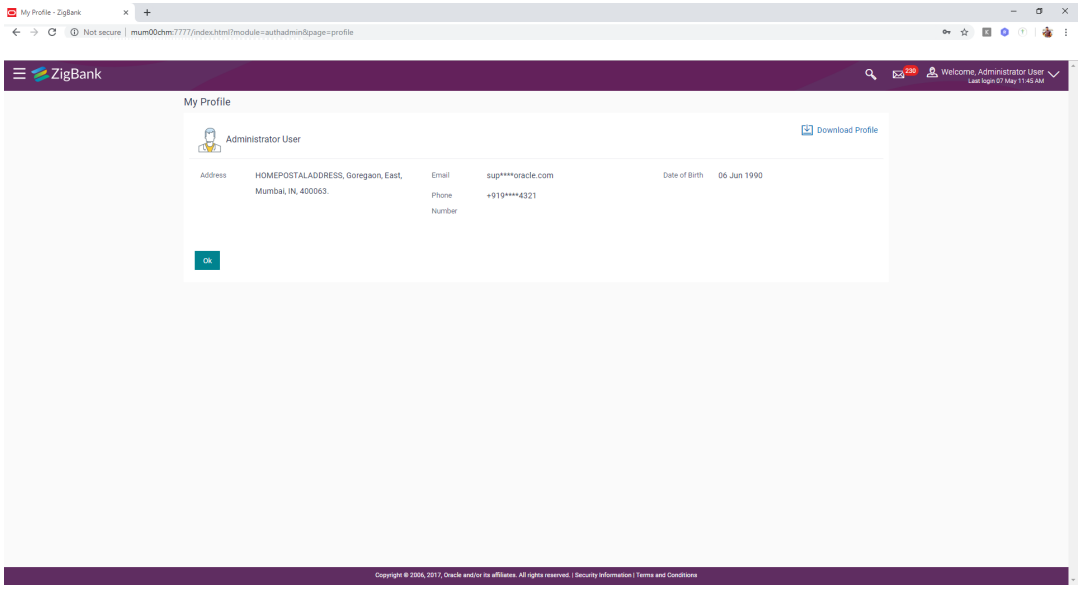
1. Login as Business User (Retail/Corporate/Admin).



2. Click on the **Profile**.



3. Click on the **Download Profile**link.



7

Third Party Consents

This topic provides information on **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.

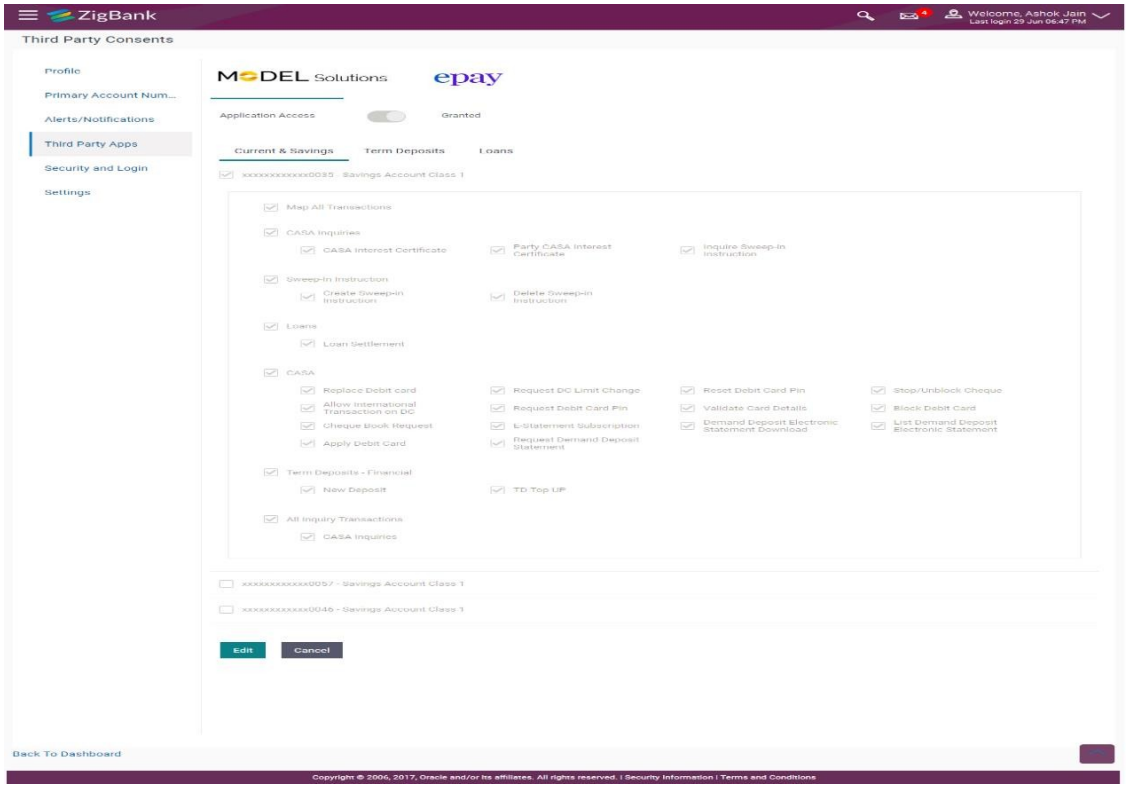
How to reach here:

Dashboard → Toggle Menu → Account Settings → My Preferences → Third Party Application

OR

Dashboard → My Profile → Profile → Third Party Application

Third Party Apps



> **Note**
>
> The fields which are marked as Required are mandatory.

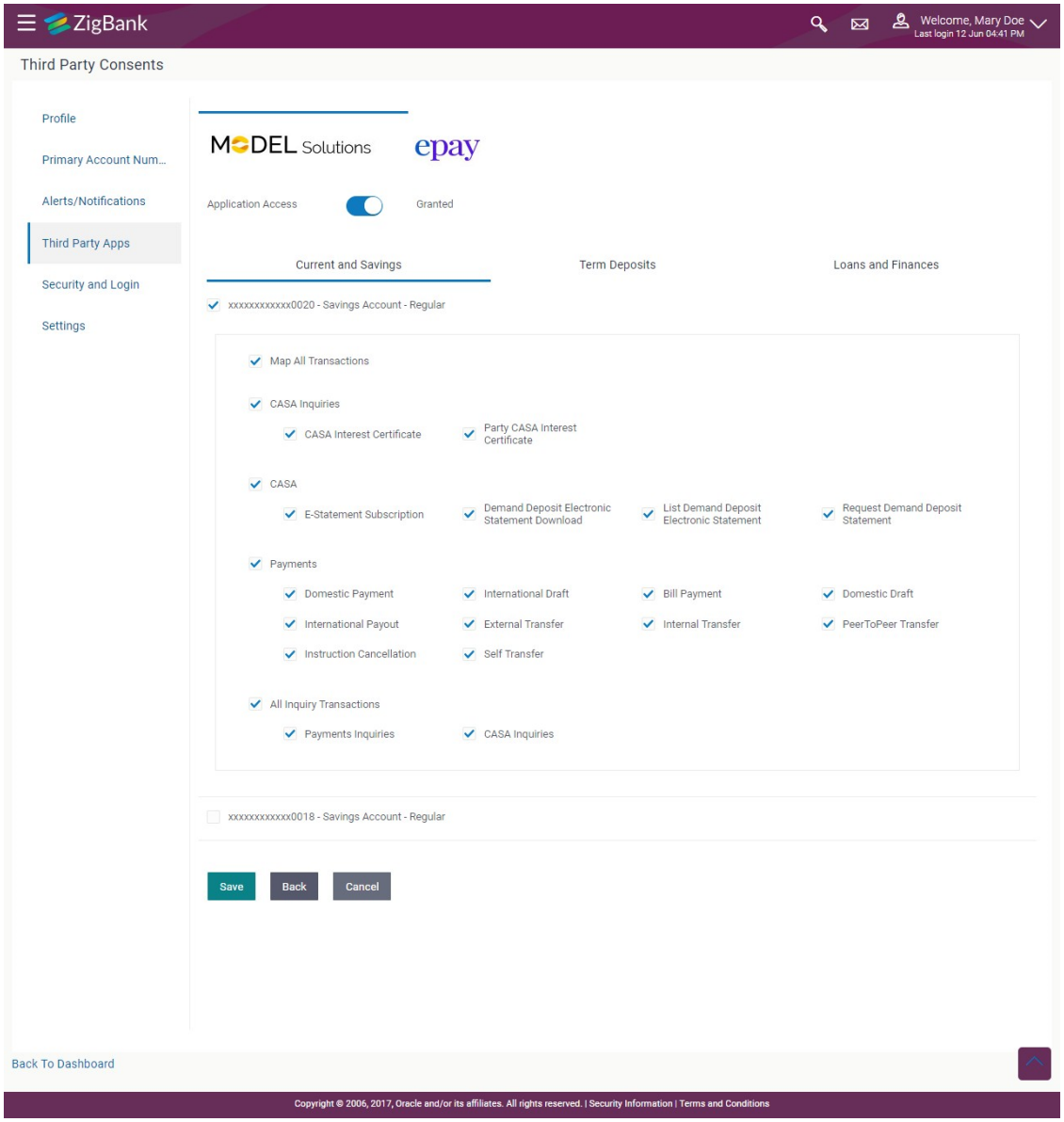
For more information on fields, refer to the field description table.

Table 7-1 Third Party App

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 the application.
Application 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.
Current and Savings/ Term Deposits/ Loans and 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 gain access.
2. The system will display the list of accounts under each of the account types along with the transactions
3. Click **Edit** to modify account and transaction access. The **Third Party Consents –Edit**
4. The screen with values in editable form appears. Perform any one of the following
   - Click **Cancel** to cancel the operation and to navigate back to the Dashboard.
   - Click **Back to Dashboard** to go to the Dashboard.

Third Party Apps - Edit



> **Note**
>
> The fields which are marked as Required are mandatory.

For more information on fields, refer to the field description table.

Table 7-2 Third Party App

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.

Table 7-2 (Cont.) Third Party App

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**,
      i. 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.

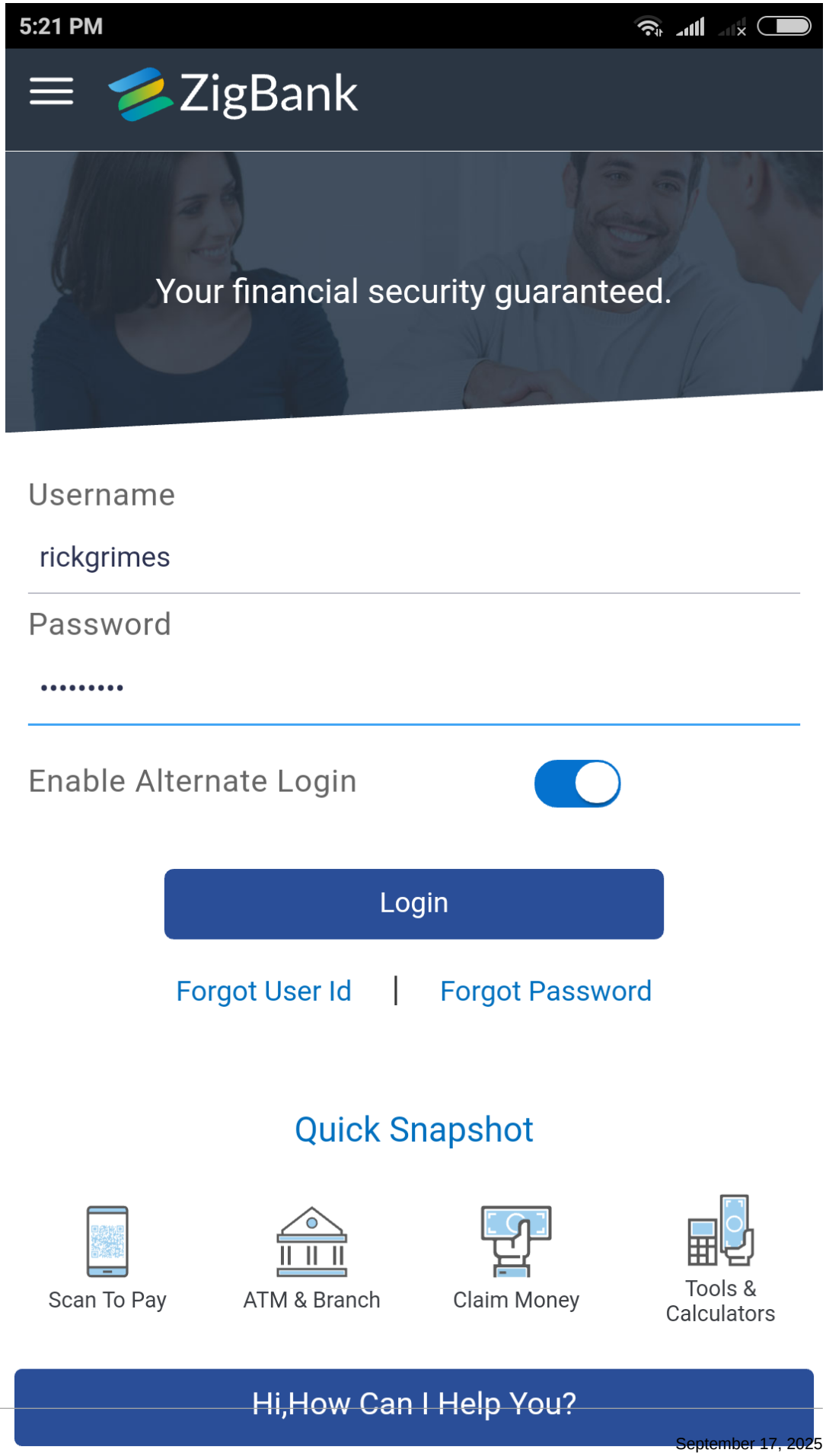
      iii. Select/Deselect all or any of the transaction checkboxes to define the transactions through which the selected account can be accessed.
2. Perform any one of the following:
   - Click **Save** to save the change.
   - Click **Back** to go back to previous screen.
   - Click **Cancel** cancel the operation and navigate back to **Dashboard**.
3. The **Third Party Consents – Review** screen appears. Verify the details, Perform any one of the following:
   - Click **Confirm**.
   - Click **Back** to go back to previous screen.
   - Click **Cancel** 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.

8

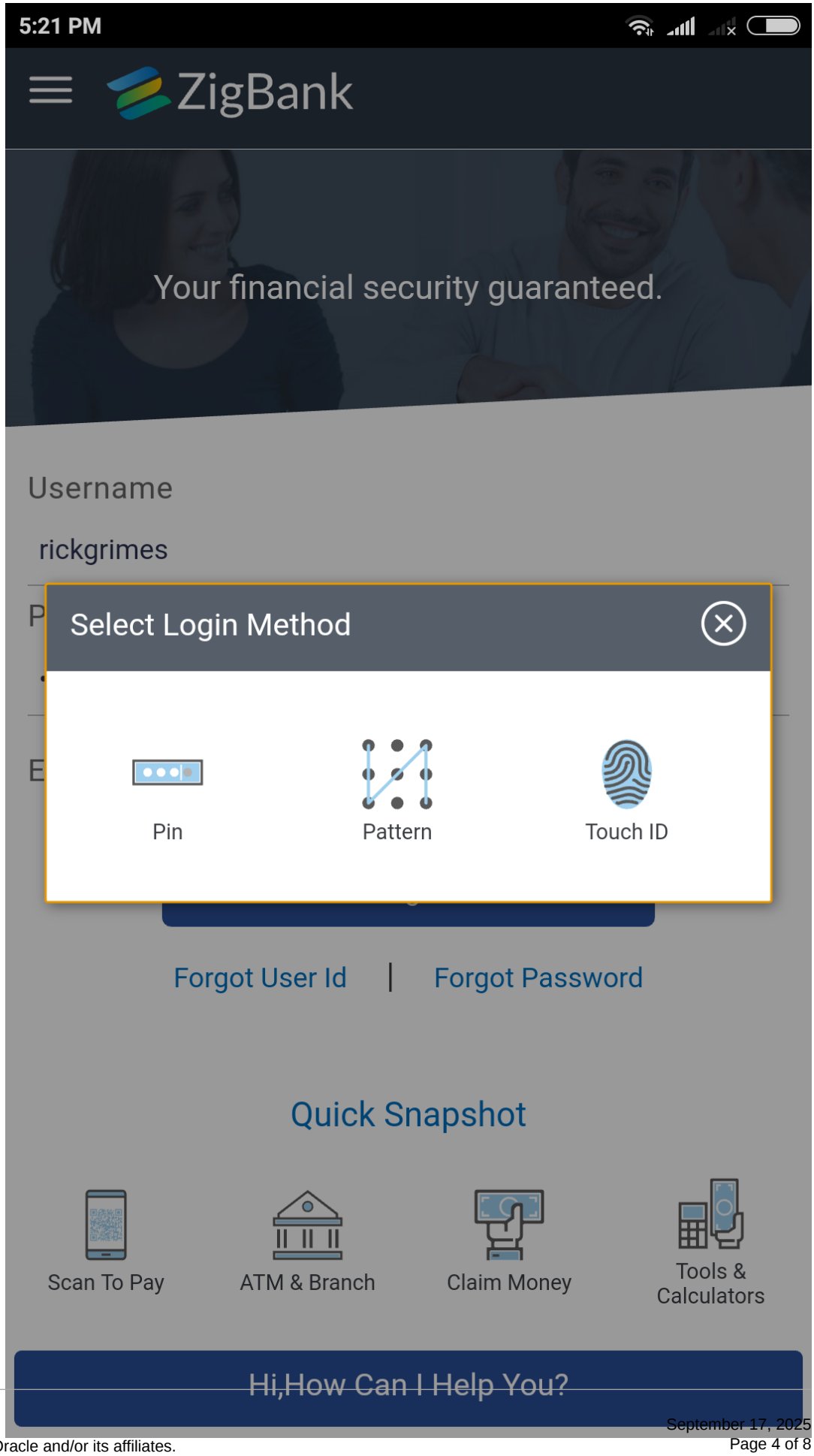
Device ID Consents

This topic describes the systematic instruction to **Device ID Consents** option. OBDX framework provides a facility to enables the alternate login via Pin, pattern or touch ID.

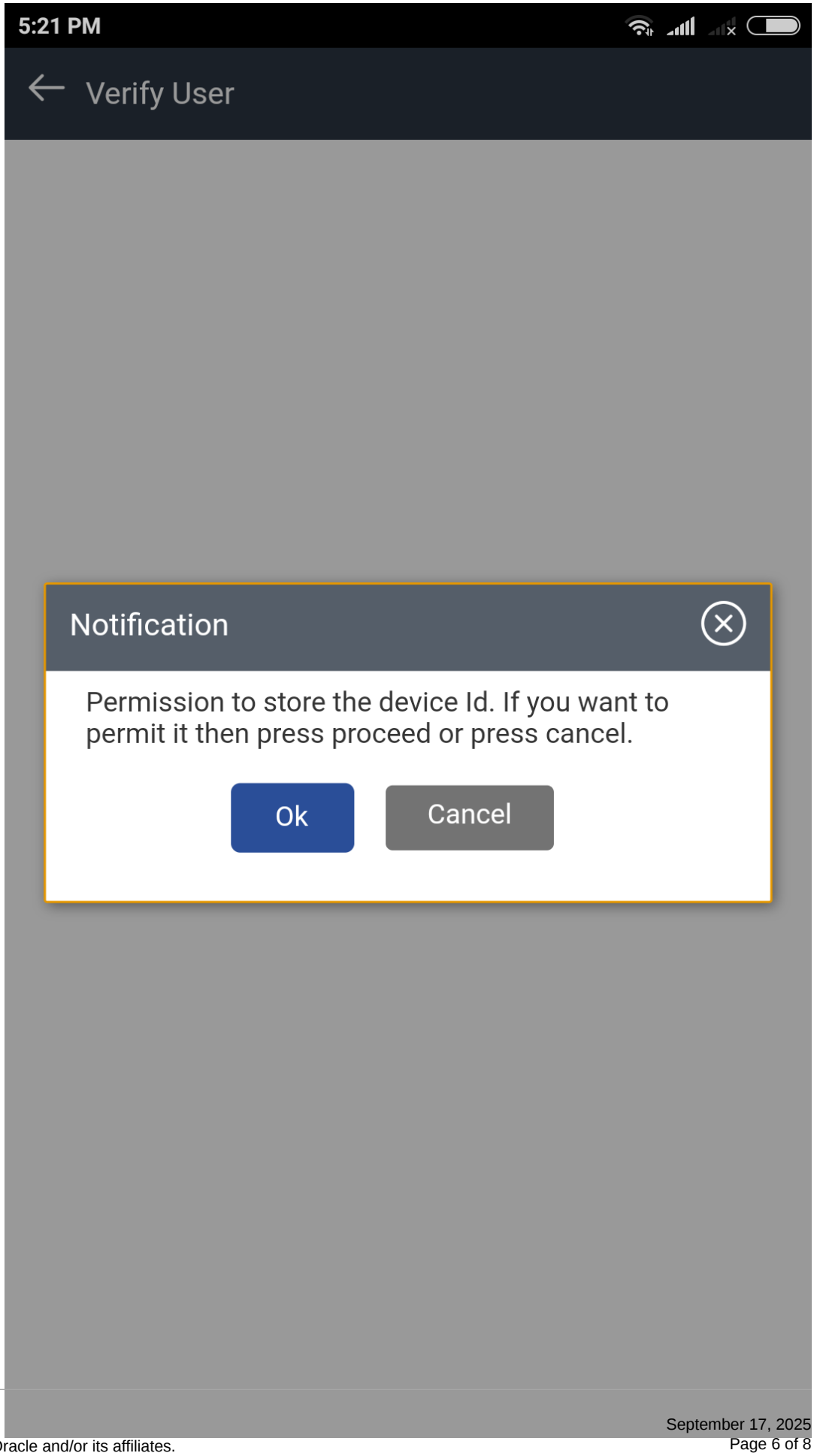
1. On the login page, user will get the **Enable Alternate login** functionality. User needs to enable this for alternate login as pin, pattern or touch ID.



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

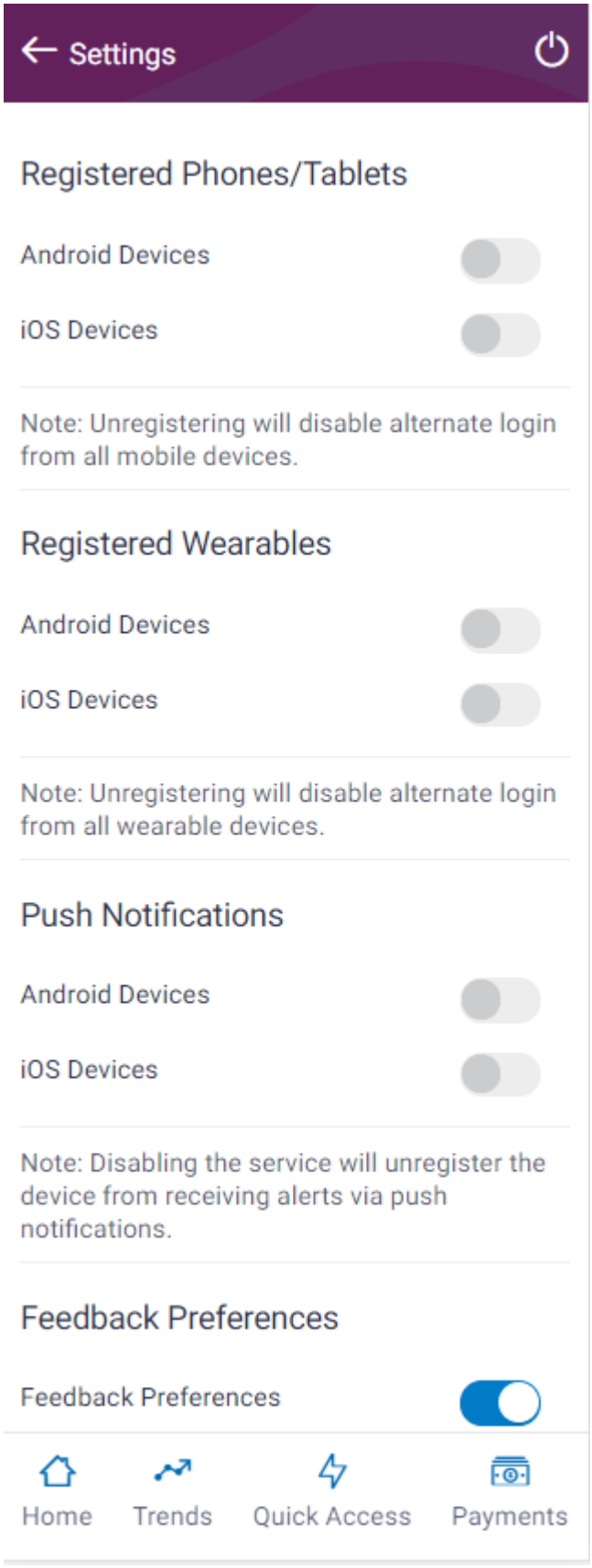


3. Once user will select the appropriate option, Notification of permission to store the device id message will display before setting up the alternate login method.



Unregister the Device ID

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



Index