

Oracle Banking Digital Experience

PIN / Pattern Authentication User Manual
Release 18.1.0.0.0

Part No. E92727-01

January 2018

ORACLE®

PIN / Pattern Authentication User Manual

January 2018

Oracle Financial Services Software Limited

Oracle Park

Off Western Express Highway

Goregaon (East)

Mumbai, Maharashtra 400 063

India

Worldwide Inquiries:

Phone: +91 22 6718 3000

Fax: +91 22 6718 3001

www.oracle.com/financialservices/

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Table of Contents

1. Preface.....	4
1.1 Intended Audience	4
1.2 Documentation Accessibility	4
1.3 Access to Oracle Support	4
1.4 Structure.....	4
1.5 Related Information Sources.....	4
2. Transaction Host Integration Matrix.....	5
3. Pattern / PIN Authentication.....	6
3.1 Pattern based authentication	6
3.1.1 Set pattern.....	6
3.1.2 Manage pattern	10
3.1.3 Pattern Visibility.....	11
3.2 PIN based Authentication.....	12
3.2.1 Set PIN.....	12
3.2.2 Manage PIN	16
3.3 Using Alternate Login Method.....	17

1. Preface

1.1 Intended Audience

This document is intended for the following audience:

- Customers
- Partners

1.2 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

1.3 Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit

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

1.4 Structure

This manual is organized into the following categories:

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

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

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

Each transaction is explained in the following manner:

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

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

1.5 Related Information Sources

For more information on Oracle Banking Digital Experience Release 18.1.0.0.0, refer to the following documents:

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

2. Transaction Host Integration Matrix

Legends

NH	No Host Interface Required.
✓	Pre integrated Host interface available.
✗	Pre integrated Host interface not available.

Sr No	Transaction / Function Name	FCR 11.7.0.0.0	UBS 12.3.0.0.0	UBS 12.4.0.0.0
1	Definition of Pattern	NH	NH	NH
2	Pattern based Authentication	NH	NH	NH
3	Manage Pattern	NH	NH	NH
5	Definition of PIN	NH	NH	NH
6	PIN Based Authentication	NH	NH	NH
7	Manage PIN	NH	NH	NH
8	Alternate login through PIN/Pattern	NH	NH	NH

3. Pattern / PIN Authentication

3.1 Pattern based authentication

Pattern based authentication allows user to login to Zig bank mobile application by drawing a pattern on screen rather than entering his user id and password. User can define a pattern for authentication and same needs to be drawn every time for login.

Note: Pattern based Authentication is available for ZigBank application for Android and iOS.

Features Supported In Application

- Set Pattern
- Manage Pattern
- Pattern Visibility
- Login using pattern

Pre-Requisites

The user must download **ZigBank** application and have a valid account with bank with online banking enabled.

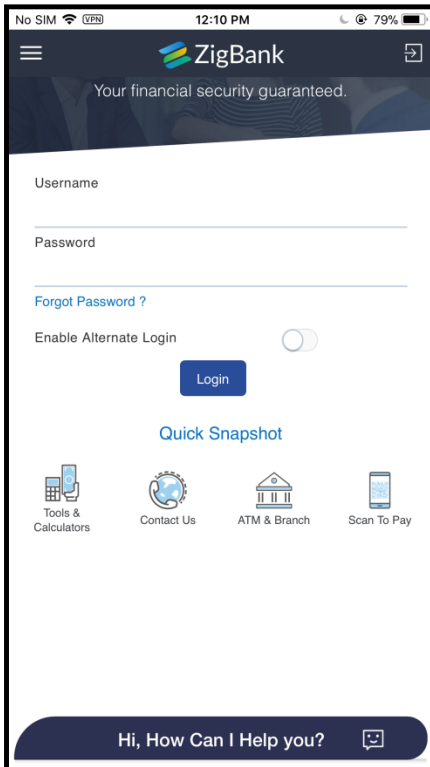
3.1.1 Set pattern

User can define a pattern for login using his ZigBank login credentials from Zig Bank mobile application.

To set pattern for login:

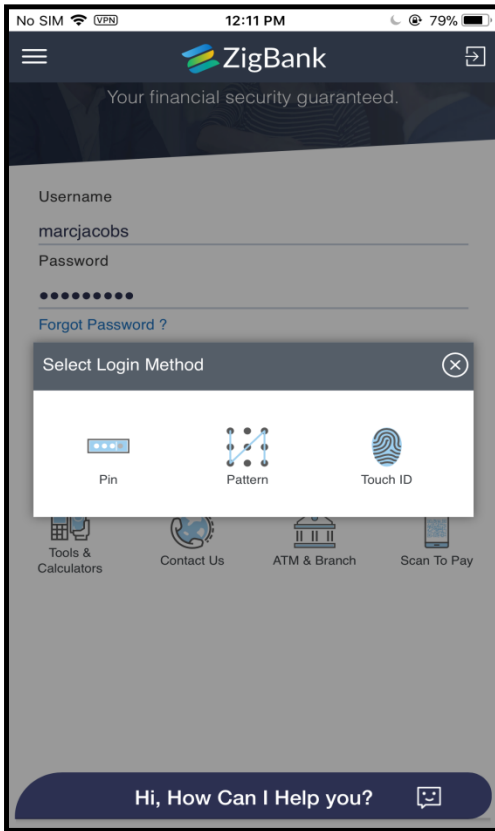
1. Launch the **Zigbank Application** Page. The **Zigbank** login page appears.

Zigbank Login Page



2. In the **Username** field, enter the user ID.
3. In the **Password** field, enter the password.
4. Select the **Enable Alternate Login** option.
5. Click **Login**. The **Select Login Method** screen appears.

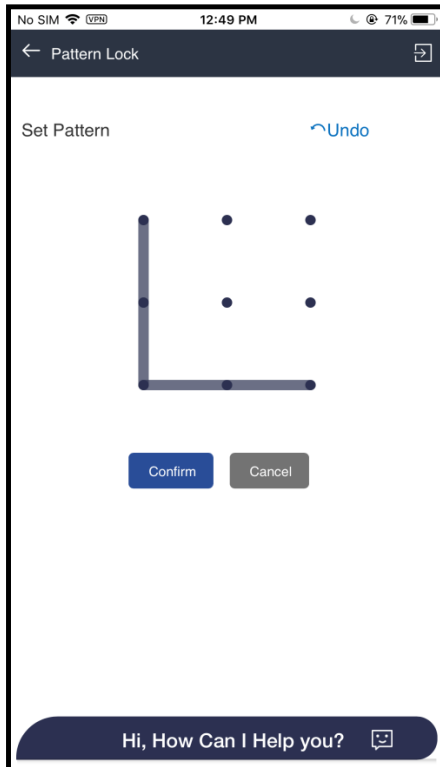
Select Login Method screen- Pattern



6. Select **Pattern** based authentication for login. The **Set Pattern** screen appears.

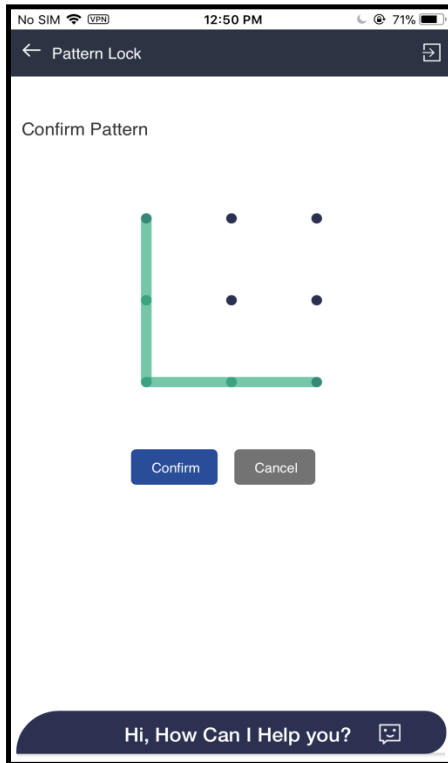
7. **Note:** User needs to provide the permission to application to set the pattern to perform the transaction.

Set Pattern screen



8. Setup desired pattern. Draw a pattern connecting minimum of 4 dots.
9. Click **Confirm**. The **Confirm Pattern** screen appears.
OR
Click **Undo** to reset the pattern and redraw it again.
OR
Click **Cancel** to cancel the transaction.

Confirm Pattern screen



10. Redraw the same pattern to confirm the pattern.
11. Click **Confirm**. The pattern gets set and user is redirected to Dashboard.
OR
Click **Cancel** to cancel the transaction.

Note: Once the pattern is set, system will prompt user to draw the pattern at the time of login.

3.1.2 Manage pattern

Using this option user can change or reset the login pattern defined.

In case the user wants to change the alternate login from Pattern to any other method (for example from PIN to Pattern) or if it has got locked by reaching the maximum number allowed for drawing an incorrect pattern, user can reset it using this option.

To reset the pattern for login transaction:

1. Click on toggle menu on **Zigbank Application**.
2. Click **Security Setting**, and then **Manage Pattern**. The **Verify User** screen appears.
3. In **Enter Password** field, enter the password to login application.
4. Click **Proceed**. **Set Pattern** screen appears.
5. Now setup desired pattern. Draw a pattern connecting minimum of 4 dots. The **Confirm Pattern** screen appears.
6. Redraw the same pattern for confirmation.

7. Click **Confirm**. The **Confirm Pattern** screen appears.
OR
Click **Cancel** to cancel the transaction.
8. The success message for new pattern being set will get displayed.
Click **Go to Dashboard**, to navigate to the dashboard.
OR
Click **More Security Options** to go to other security options.

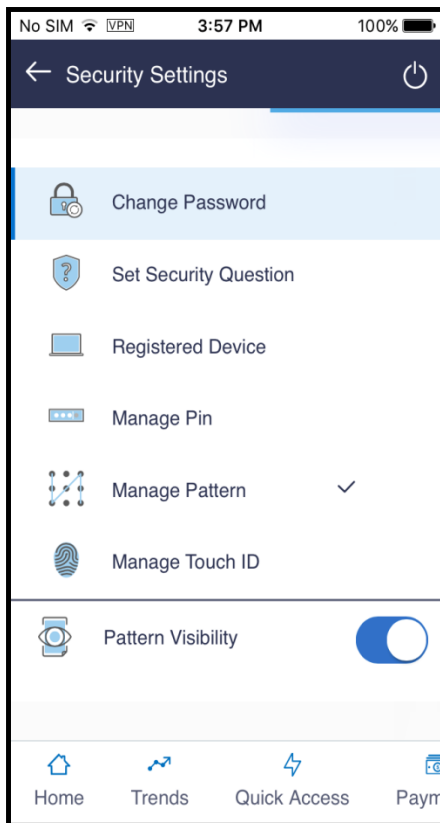
3.1.3 Pattern Visibility

Using this option user can define if the pattern has to be kept visible or invisible at the time of drawing the same for logging into the application.

To pattern visible:

1. Launch the **Zigbank App** Page. The **Zigbank** login page appears.
2. Enter login credentials and log into **Zigbank** application.
3. Click toggle menu, and then click **Security Settings** option.

Security Settings options



4. Click **Pattern Visibility** to make pattern visible.
Next times when user draw pattern at the time of login, he will able to see it on the screen.
This way user can see the pattern as drawing it with finger to make it easier to unlock application.

Note: By default the **Pattern Visibility** option is off. If the user keeps the pattern visibility as switched off, user will not be able to see the pattern that he is drawing at the time of login and this will prevent any unauthorized access to the application.

3.2 PIN based Authentication

This option allows user to login to ZigBank Application using a PIN instead of user id and password. User can define a 4 or 6 digit numeric PIN for login. User also has the option of resetting his PIN and changing his alternate login method from PIN to any other method.

Features Supported In Application

- Set PIN
- Manage PIN
- Login using PIN

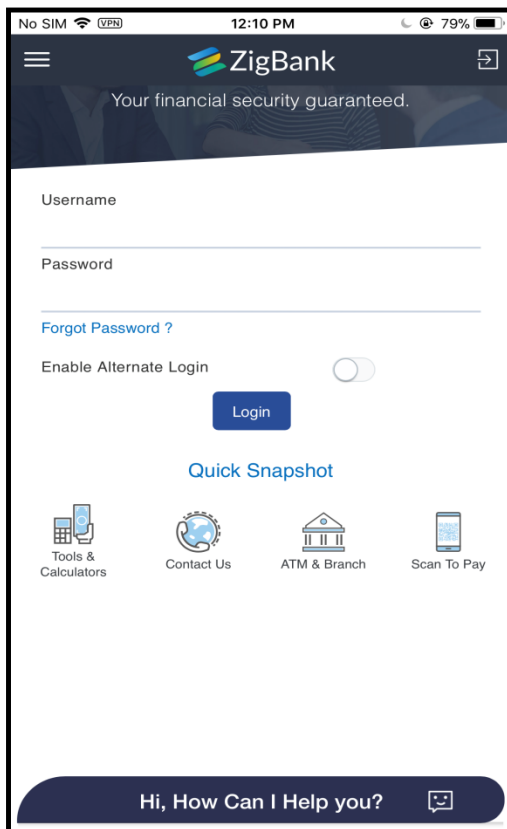
3.2.1 Set PIN

User can define a PIN for login using his Zig Bank login credentials from ZigBank Application.

To set PIN for login transaction:

1. Launch the **Zigbank** application page. The **Zigbank** login page appears.

Zigbank login

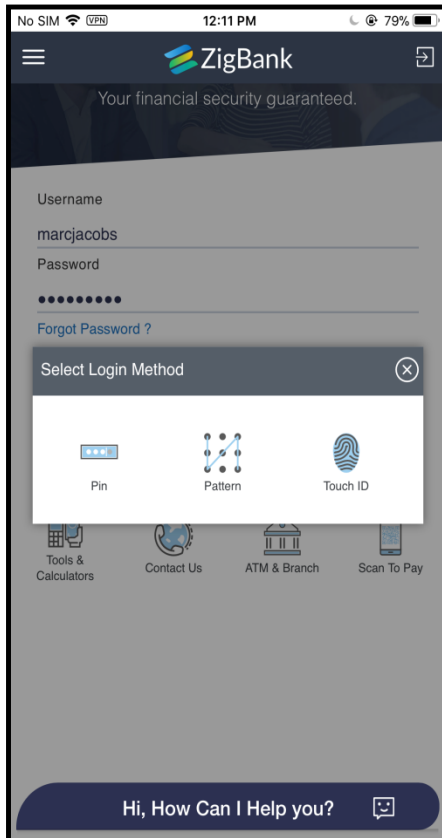


2. In the **Username** field, enter the user ID.
3. In the **Password** field, enter the password.

4. Select **Enable Alternate Login** option.
5. Click **Login**. The **Select Login Method** screen appears.

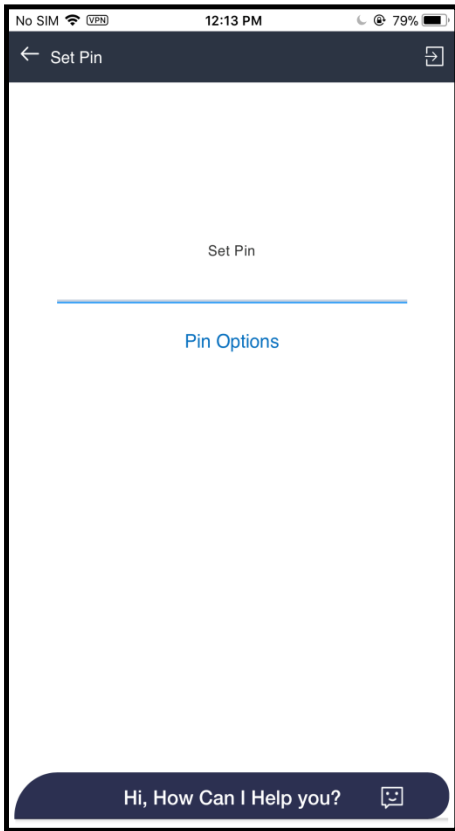
Note: User needs to provide the permission to application to set the pattern to perform the transaction.

Select Login Method screen



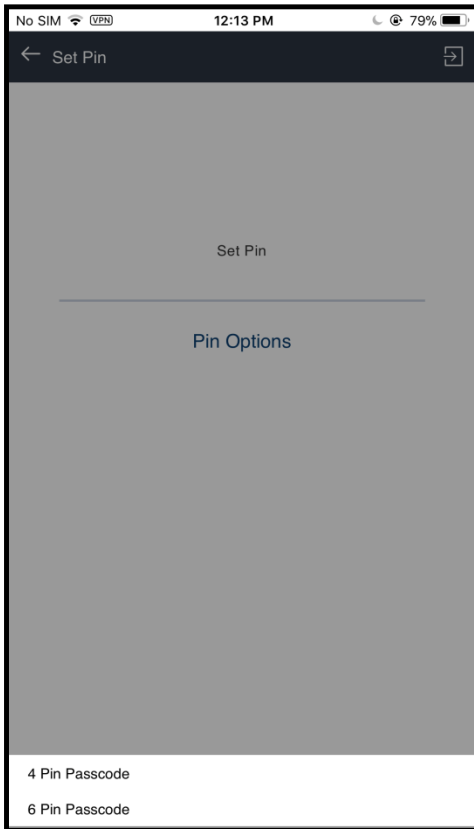
6. Select **PIN** based authentication. **Set PIN** screen will get displayed.

Set PIN screen



8. Click **PIN Option** to choose the pin length.

PIN options screen



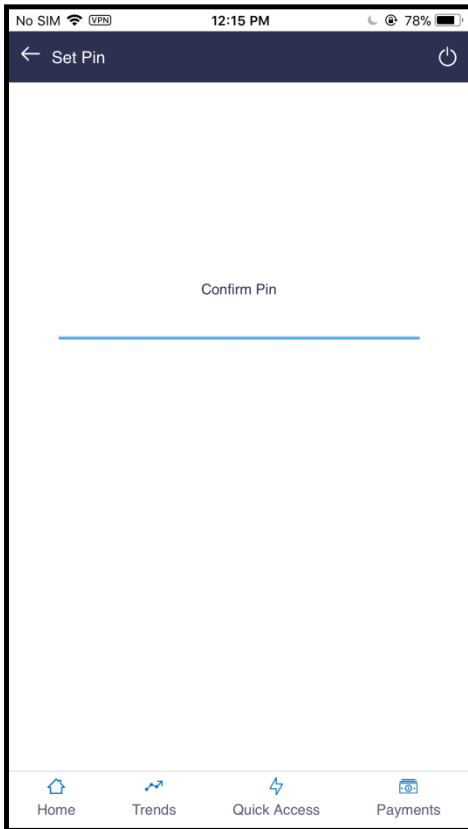
8. Select the desired PIN option.

Field Description

Field Name	Description
PIN Options	<p>This option lets the user to decide the length of the PIN.</p> <p>The options are:</p> <ul style="list-style-type: none"> • 4 PIN Passcode: Set the 4 digit PIN for login transaction. • 6 PIN Passcode: Set the 6 digit PIN for login transaction.

9. In the **Set PIN** field, enter PIN that needs to be set for login. The **Confirm PIN** screen appears.

Confirm screen



10. In the **Confirm PIN** field, re-enter the pin for confirmation.

Field Description

Field Name	Description
Confirm PIN	Re-enter the PIN to confirm.

11. PIN will get set and user will be redirected to dashboard.

Note: Once the PIN is set system will prompt user to enter the PIN at the time of login.

3.2.2 Manage PIN

Using this option user can change or reset the login PIN defined.

In case the user wants to change the alternate login from PIN to any other method (for example from Pattern to PIN) or if it has got locked by reaching the maximum number allowed for drawing an incorrect PIN, user can reset it using this option.

To reset the PIN for login transaction:

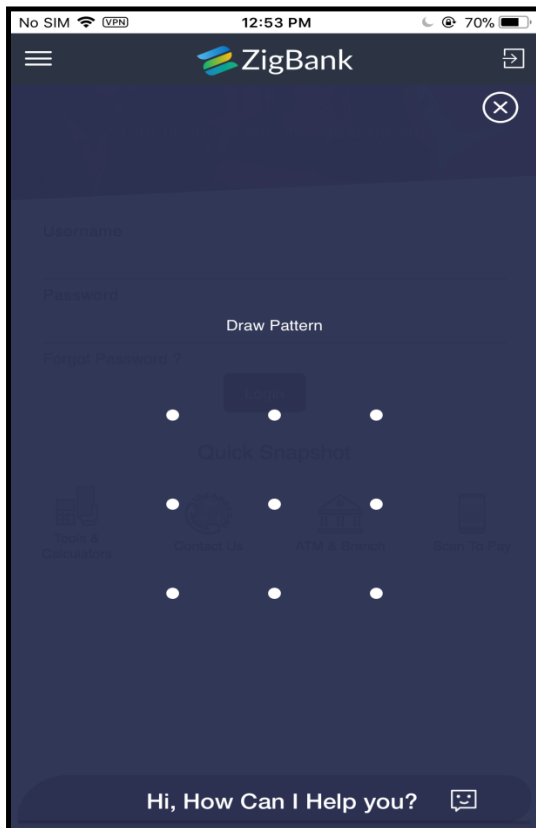
1. Click on toggle menu on **Zigbank Application**.
2. Click **Security Setting**, and then **Manage PIN**. The **Verify User** screen appears.
3. In **Enter Password** field, enter the password to login application.

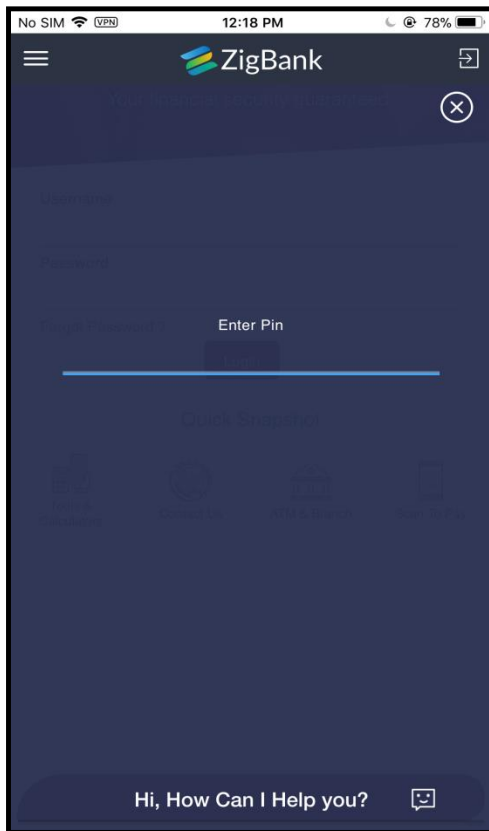
4. Click **Proceed**. The **Set PIN** screen appears.
5. In the **Set PIN** field, enter PIN to be set for login. The **Confirm PIN** screen appears.
6. In the **Confirm PIN** field, re-enter the pin for confirmation.
7. The success message of request submission appears.
Click **Go to Dashboard**, to navigate to the dashboard.
OR
Click **More Security Options** to go to other security options.

3.3 Using Alternate Login Method

1. Launch the **Zigbank Application** page.
2. The system prompts user to enter a PIN / Pattern appears.

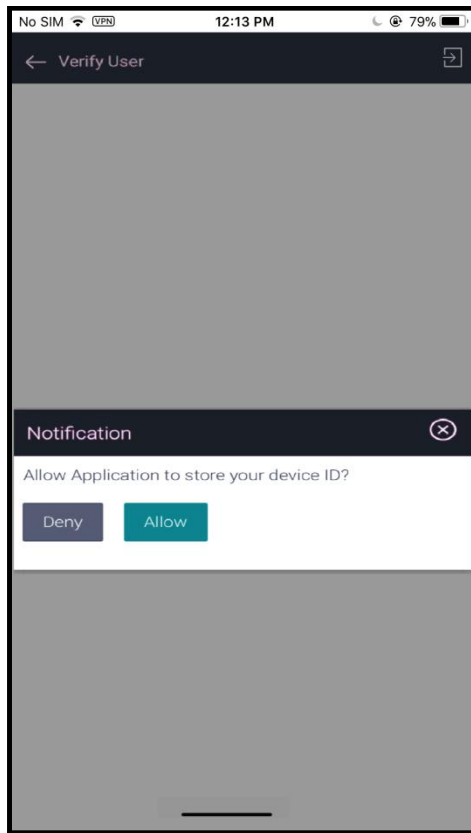
Login Method screen- Pattern




Login Method screen- PIN

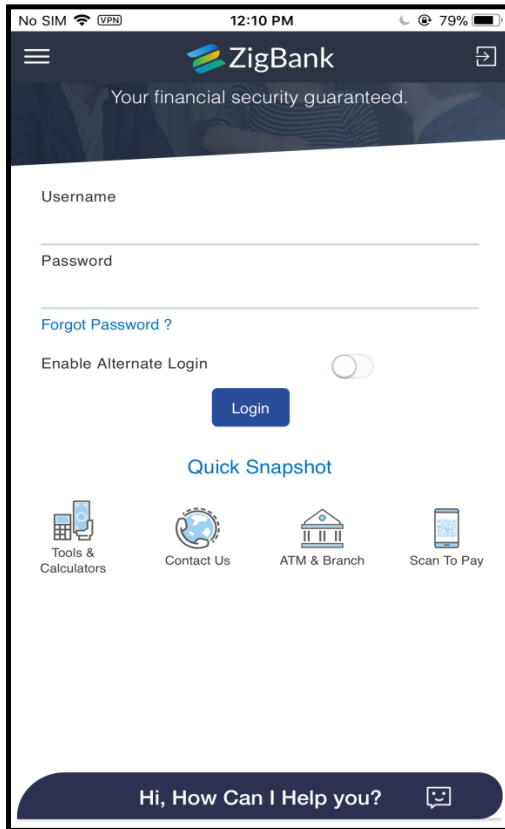
3. If **PIN** is set as authentication;
 - a. Enter **PIN** defined for login.
4. If **Pattern** is set as authentication;
 - a. Draw **Pattern** defined for login.
5. The system prompt user for permission to store the device ID.

Prompt to store Device ID



6. Click **Allow**, if the user wish to store the device ID.
OR
Click **Deny**, if the user do not wish application to store the device ID.
7. On successful authentication, user gets logged in to the **Zigbank** application.
8. If user clicks , user is redirected to the login page.

Zigbank pre-login



If using OAM as identity provider for OBDX mobile application, add below property on DIGX 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,EDITABLE,CATEGORY_DESCRIPTION) values ('AUTH_PROVIDER','mobileconfig','OAM','N',null,'configuraion for mobile uid in OUD','ofssuser',sysdate,'ofssuser',sysdate,'Y',1,'N',null);
```

FAQs

1. What are the alternate login methods used in Mobile?

In mobile banking PIN, Pattern, and Finger print are used for alternate login method for logging into Zigbank Mobile Application.

Note: User needs to provide the permission to application to set the PIN/ Pattern / Finger Print/ Device ID to perform the transaction.

2. How to change the PIN or Swipe Pattern?

Click on toggle menu on Zigbank mobile application, then click Security Setting, and then Manage PIN/Pattern.

3. User's mobile number is not registered with the bank? Can he/she use the mobile application?

No, user has to register his/her mobile number with his/her account with the bank to use this feature.

4. If user re-installs the mobile application on a new phone, is it required to register the alternate login again?

No, user can login with his/her existing alternate login defined.

5. Can user have two authentications for login?

No, user can only set one type of PIN/Pattern method for login..

6. What if user forget the PIN or Swipe Pattern?

To reset the PIN/Pattern, click on toggle menu on Zigbank mobile application, then click Security Setting, and then Manage PIN/Pattern.

[Home](#)