Oracle Banking Digital Experience

Soft Token Application User Manual
Release 18.3.0.0.0

Part No. F12056-01

December 2018

ORACLE®

Soft Token Application User Manual

December 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/

Table of Contents

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
- Pre-requisite for 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 18.3.0.0.0, 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	Oracle FLEXCUBE Core Banking 11.7.0.0.0	Oracle FLEXCUBE Universal Banking 14.0.0.0.0	Oracle FLEXCUBE Universal Banking 14.1.0.0.0
1	Soft Token Application	**NH**	**NH**	**NH**

3. Soft Token Application

Security tokens are generally used in environments with higher security requirements as part of a multifactor authentication system. Soft tokens give the same security advantages of multifactor authentication, while simplifying distribution and lowering costs.

A Soft token app is a two - factor authentication based on Passcode or PIN and something you have (an authenticator such as smartphone), protecting your sensitive networked information and data. A soft token is a software-based security token that generates a single-use 6 digit login PIN or passcode.

Features Supported In Application

- Online registration
- OTP generation

3.1 Registration

Business users can register on soft token application (PaySecure Application) using their Digital Banking login credentials. Post validating the credentials, user has to set the new PIN to login into the PaySecure application for generating OTP.

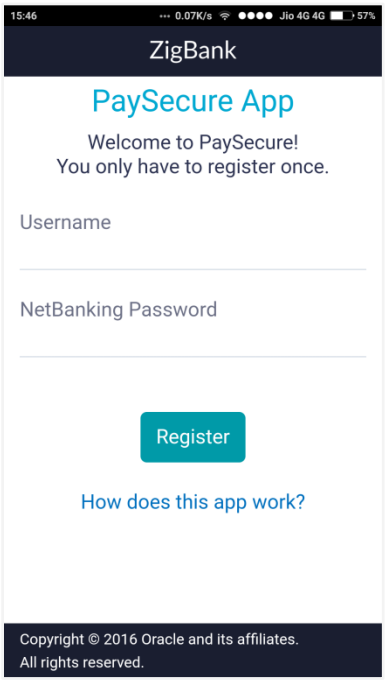
Pre-Requisites

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

To generate a single-use login PIN:

1. Launch **PaySecure** App.
2. In the **Bank Username** field enter the username.
3. In the **Password** field enter the password.

Register page

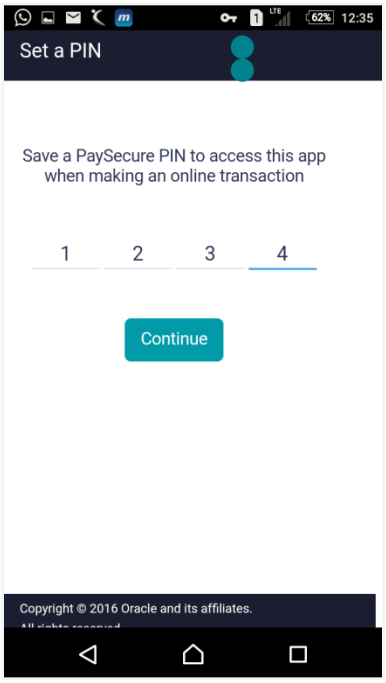


Field Description

Field Name	Description
Username	Login id provided by the bank.
Net Banking Password	The password for channel access.

4. Click **Register** to register on the app. The **Set a PIN** screen appears with prompt to select a new PIN.

Set a PIN



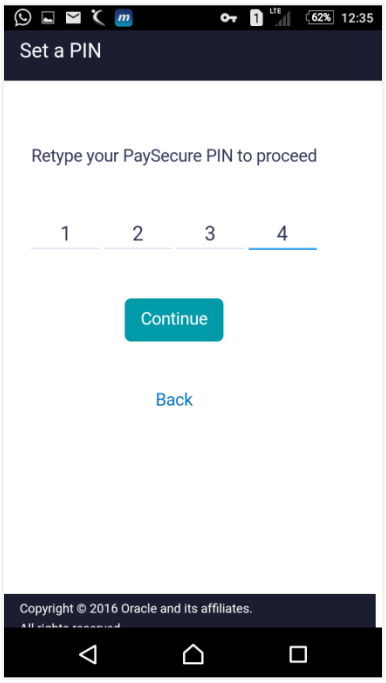
Field Description

Field Name	Description
PaySecure PIN	The PIN to be set for the PaySecure.

6. In the **PaySecure PIN** field, enter the PIN to be set.

   Click **Continue** to proceed to the next screen.

Set a PIN- Re enter PIN



Field Description

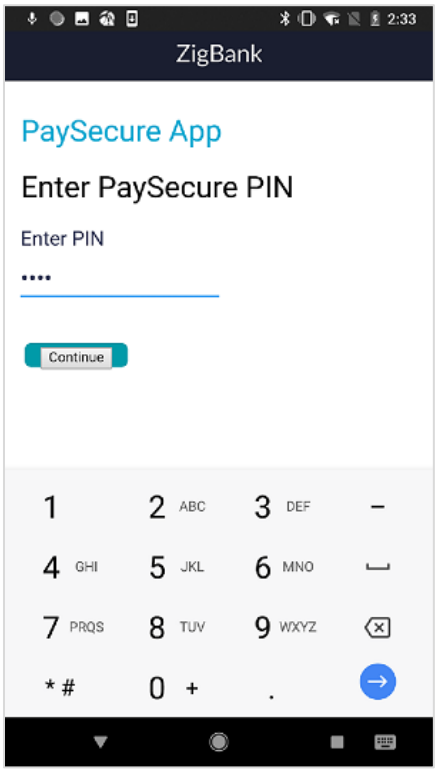
Field Name	Description
Retype PaySecure PIN	Retype PIN number to be set for the PaySecure.

7. In the PaySecure PIN field, re-enter a PIN.
8. Click Continue to proceed to next screen. User will be directed to the screen to generate an OTP.
   OR
   Click **Back** to go back to previous screen.

3.2 Login & OTP Generation

Once the registration is successful, from the subsequent logins user has to use the PIN to login into the PaySecure application. Post authentication, user will be provided with an option to either select the user for which OTP is to be generated (if multiple users are registered using same application) or to register another user on same device and application.

PaySecure PIN

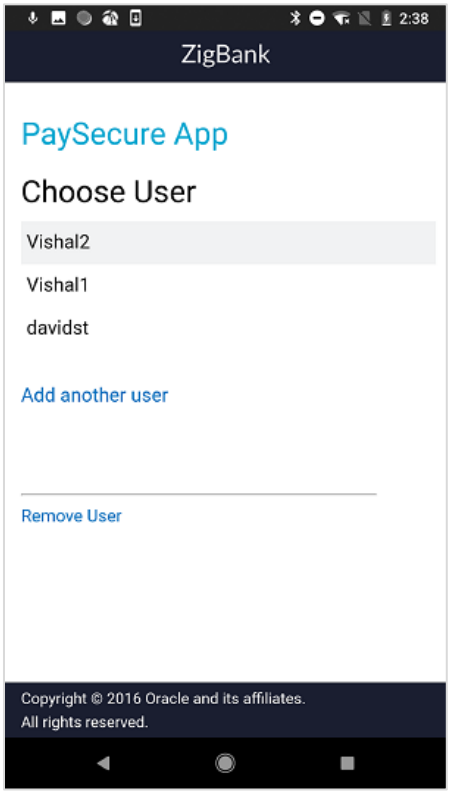


Field Description

Field Name	Description
Enter PIN	Enter the PIN to login into the application.

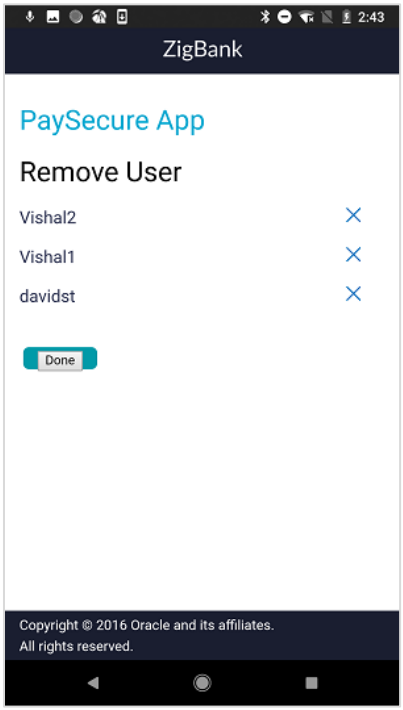
1. Enter the **PIN**, and click **Continue**.
   The **Choose User** screen appears.

Choose User



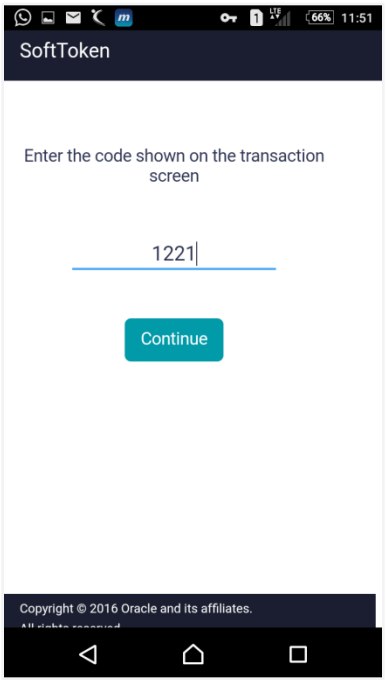
2. Select the user. The user is prompted to enter the code.
   OR
   Click **Add Another User** to add another account. For more information refer Registration section.
   OR
   Click **Remove User**.

Remove User



3. Click  against a user to remove a user. A popup message appears prompting to confirm the user deletion.
4. Click **Yes** to delete the user. User deleted message is displayed.
   OR
   Click **No** to navigate back to the **Remove User** screen.
5. Click **Done.**

Soft Token Code

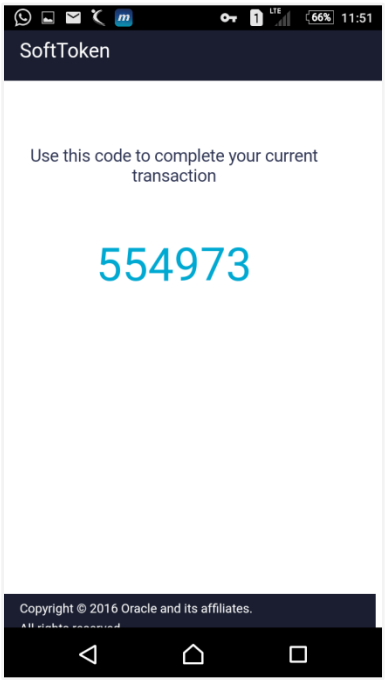


Field Description

Field Name	Description
Enter the code	The Soft Token code displayed on transaction screen.

6. In the **Enter the code** field, enter the code appear on transaction screen.
7. Click **Continue** to proceed to next screen. The **Soft Token** code generated successfully.

Generated Soft Token Code (HOTP based)

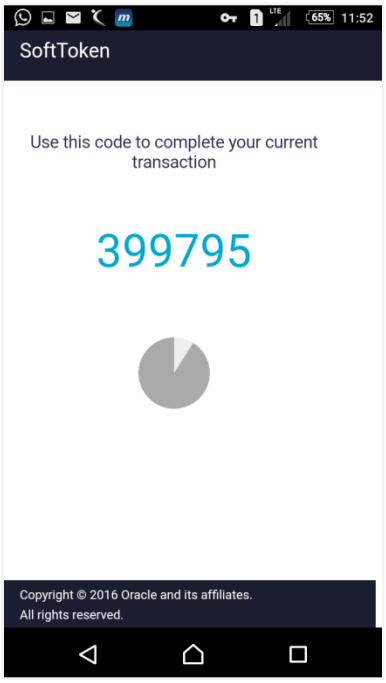


8. Use the generated Soft Token PIN to complete the current transaction.

Note:
For the Time based Soft Token Code, the code dynamically changes after every 30 sec. User has to configure App while installing and choose TOTP (Time-based one-time password) option which is a temporary passcode.

By default HOTP (HMAC-based one-time password (OTP) algorithm) is selected, which is internet based.

Generated Soft Token Code (TOTP based)



FAQs

1. **While setting up secure PIN in application can 2FA be introduced post login with credentials and before setting up PIN?**

   Yes, this is supported in the product. (Only OTP).

2. **What other options are available other than PIN to setup in application like Fingerprint, Eye, pattern, etc. In addition, can we change/switch to other options after login to App?**

   Only PIN is supported out of box.

3. **How can I reset the PIN if I forget the PIN?**

   Currently, forgot PIN is not supported. Incase if user enters the incorrect PIN for more than 'N' times, then the user will need to re-register in the app using his internet banking credentials and redefine the PIN.

4. **If incorrect PIN is entered formore than maximum allowed failure attempts then what are consequences?**

   User/App will not get locked but will be forced to re-register in the app using his internet banking credentials and redefine the PIN.

5. **This APP is supported in Android/IOS with which version. In addition, is it supported by other Platform like blackberry/Windows/etc. and with which respective version?**

No, only iOS (11, 12) and android (six and above) are supported out of box.

6. **Can this App be installed in rooted device?**

   Before the soft token app installation there will be a check if a device is rooted. Whereas, post app installation, if a device is rooted, there will be no change since this is an offline app.

7. **Is internet is required to use this App post first time login to use or can be used without internet?**

   Internet is required during app installation and for first time login. Post that internet is not required.

8. **Will time difference of mobile device in terms of time zone and with different timings set to phone (i.e. 15 min early) and OBDX server will cause any problem?**

   HOTP does not have any impact. In case of TOTP, the time zone offsets are already handled. However, in case of a device time mismatching with the server time, in that case there will be issue.

9. **If a person changes mobile device or if a person uninstall and install the App in same device, is activation again required?**

   User will need to re-register in the app using his internet banking credentials and redefine the PIN.

10. **What are all the use cases where App gets locked?**

    User/App will not be locked but will be forced to re-register in the app using his internet banking credentials and redefine the PIN. There are no use cases for app lock.

11. **If App gets lock, can Admin unlock the APP or assist customer to unlock it?**

    Not applicable.

12. **Can language translation can be done for this App?**

    Yes.

13. **What is the Length of token or otp?**

    6 digits.

14. **What is the maximum time of code to validate TOTP and HOTP?**

    Maximum time to validate TOTP is n buckets of 30 seconds, wherein n (TOKEN_TIME_WINDOWS_ALLOWED) is configurable and default value is six. As far as HOTP is, concerned expiry is configurable.

15. **After how many number if invalid attempts of pin the app will be locked?**

    Number of allowed invalid attempts are configurable as a part of app build max_no_attempts in (app.properties.xml/app.plist). Data in the app is reset if attempts are exhausted.

16. **Currently OTP and Token is supported from this APP or only Token?**

A token, which will be generated by an app, is a onetime password (OTP) to be used to authenticate the transaction.

17. Is Self-registration is available for user without admin intervention. Currently bank is live with customer and has one maintenance i.e. checkbox to tick for soft app registration can these be short-circuited and user himself register for this?

There is no admin intervention required for app registration; the user himself will register for the app.

18. Can I register PaySecure app on multiple devices for same user?

No, registering PaySecure application on multiple devices for the same user is not allowed. The token generated from the latest installed mobile app would be valid.

19. Can I register multiple user ids using one PaySecure application installed on one device?

Yes, you can register multiple users on PaySecure application installed on one device.

Home