Oracle® Banking Digital Experience

Passwordless Login through Passkeys User Manual

Release 25.1.0.0.0
G38563-01
September 2025

Oracle Banking Digital Experience Passwordless Login through Passkeys User Manual, Release 25.1.0.0.0

G38563-01

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

Basic Actions

Most of the screens contain icons to perform all or a few of the basic actions. The actions which are called here are generic, and it varies based on the usage and the applicability. The table below gives a snapshot of them:

Table 2 Basic Actions and Descriptions

Action	Description
Back	In case you missed to specify or need to modify the details in the previous segment, click **Back** to navigate to the previous segment.
Cancel	Click **Cancel** to cancel the operation input midway without saving any data. You will be alerted that the input data would be lost before confirming the cancellation.
Next	On completion of input of all parameters, click **Next** to navigate to the next segment.
Save	On completion of input of all parameters, click **Save** to save the details.
Save & Close	Click **Save & Close** to save the data captured. The saved data will be available in **View Business Product** with *In Progress* status. You can work on it later by picking it from the **View Business Product**.
Submit	On completing the input of all parameters, click **Submit** to proceed with executing the transaction.
Reset	Click **Reset** to clear the data entered.
Refresh	Click **Refresh** to update the transaction with the recently entered data.
Download	Click **Download** to download the records in PDF or XLS format.

Symbols and Icons

The following are the symbols/icons you are likely to find in this guide:

Table 3 Symbols and Icons

Symbols and Icons	Description
	Add data segment
	Close
	Maximize
	Minimize
	Open a list
	Open calendar
	Perform search
	View options
	View records in a card format for better visual representation.
	View records in tabular format for better visual representation.

Post-requisites

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

1

Passwordless Login through Passkeys

This topic describes the process of passwordless login using passkeys.

A passkey can meet multifactor authentication requirements in a single step. Usernames are often easy to discover; sometimes they're just your email address. Since passwords can be hard to remember. A passkey is an alternative method of user authentication that eliminates the need for usernames and passwords. Passkeys are end-to-end encrypted and stored securely either on your device locally or in a vault, such as your device's keychain or password manager.

Passkeys **protect users from phishing attacks**. Passkeys work only on their registered websites and apps; a user cannot be tricked into authenticating on a deceptive site because the browser or OS handles verification. Passkey are more secure because every passkey is unique, passkeys tend to be more secure than passwords. That means passwords will no longer be reused across multiple sites and platforms. And because passkeys are generated automatically, users won't need to rely on passwords that are either easy to remember and unfortunately, easy for others to guess or so complicated that they're easily forgotten and also passkey protects from server leaks.

When you attempt to log in to a site that uses passkey technology, the site will send a push notification to the smartphone you used when you registered the account. When you use your face, fingerprint or personal identification number (PIN) to unlock the device, it will create a unique passkey and communicate it to the website you are attempting to access and to give the site or app permission to grant the login request.

- Setting up Passkey
  This topic provides the systematic instructions for setting up Passkey.
- Authentication Using Passkey
  This topic provides the systematic instructions for implementing Passkey authentication.

1.1 Setting up Passkey

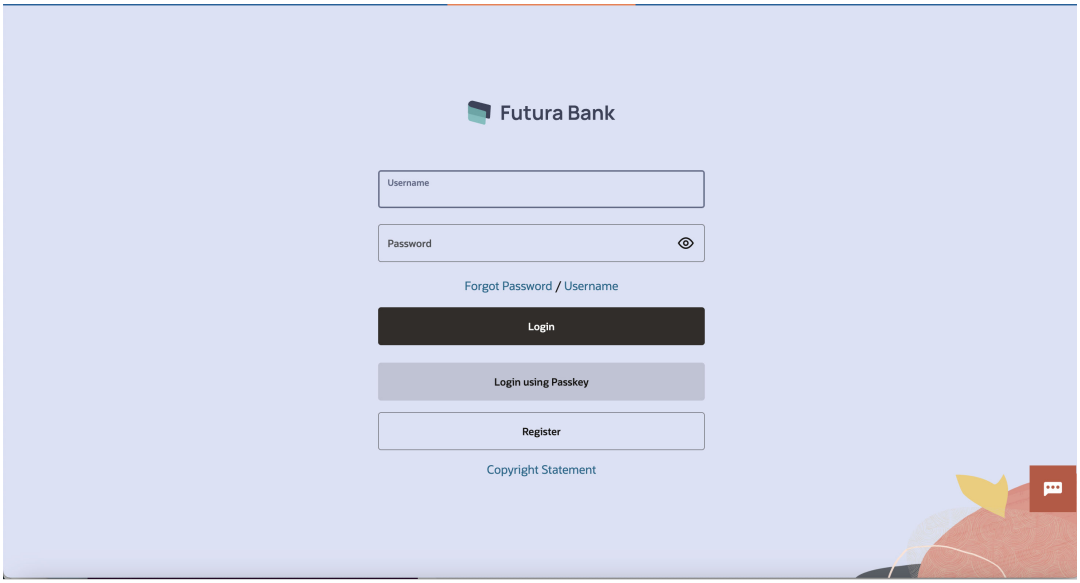
This topic provides the systematic instructions for setting up Passkey.

How to setup a passkeys on another device:

1. Launch the **Futura Bank** App.

   The Futura Bank pre-login screen appears.

Figure 1-1 Futura Bank pre-login page

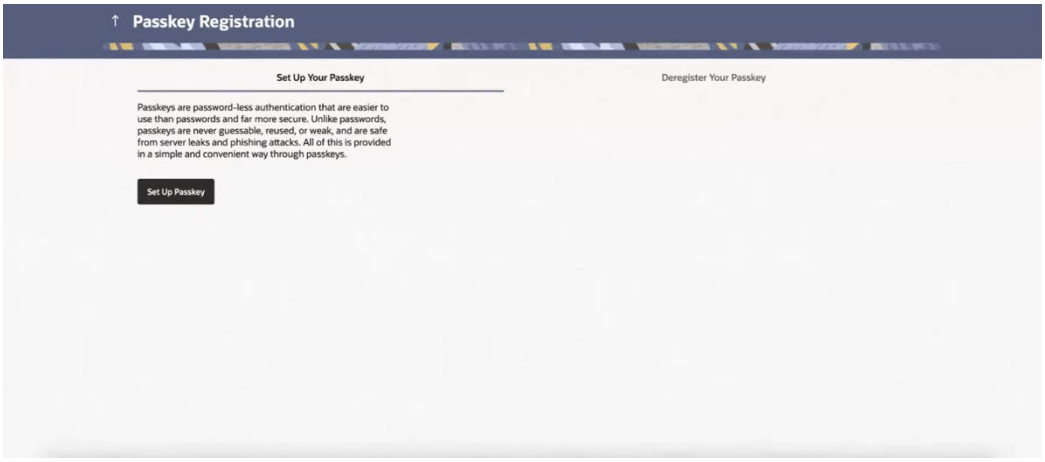


2. In the **Username** field, enter the user ID.
3. In the **Password** field, enter the password.
4. Click **Login**.

   The **Dashboard** screen appears.
5. From the toggle menu, click **Account Settings**, and then click **Setup Passwordless Authentication**.

   The **Passkey Registration** screen appears.

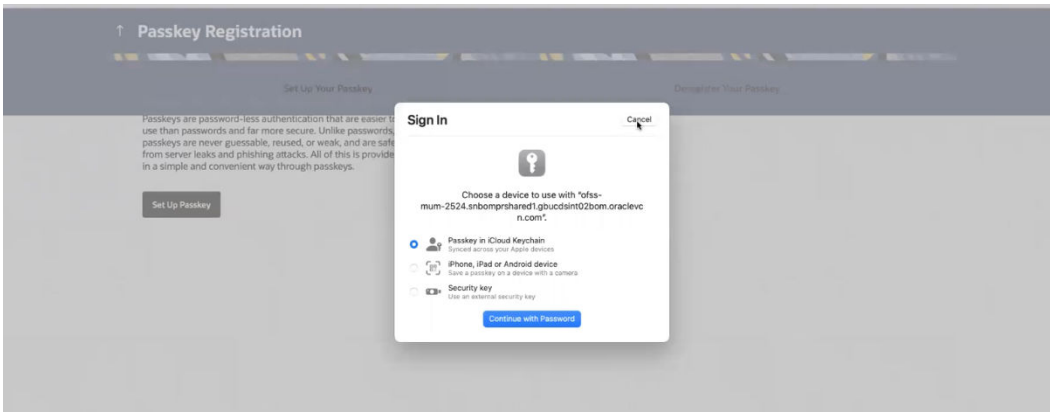
Figure 1-2 Passkey Registration screen



6. Click on the **Setup Passkey**.

   System prompts the user to save passkey in the device itself or in other mobile or table device with camera or in any security key.

Figure 1-3 Selection of device for Setup Passkey

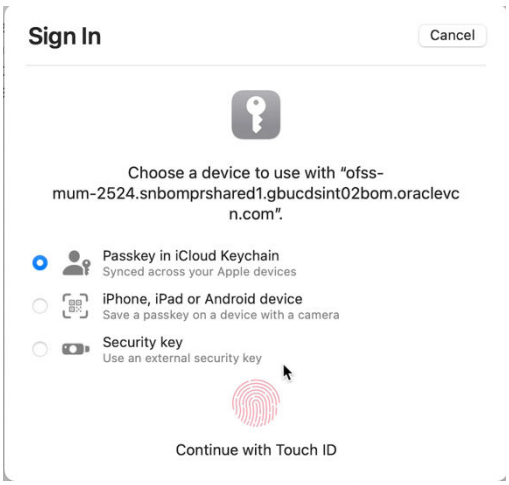


7. Select a desired device.
8. Perform one of the following actions:
   - Click **Continue** with Password.

     > **Note**
     >
     > The first priority to register the password is the biometrics (fingerprint or Face ID), then if they are not available, it asks for the device password.

   - On a device with biometric functionality, continue with biometric.

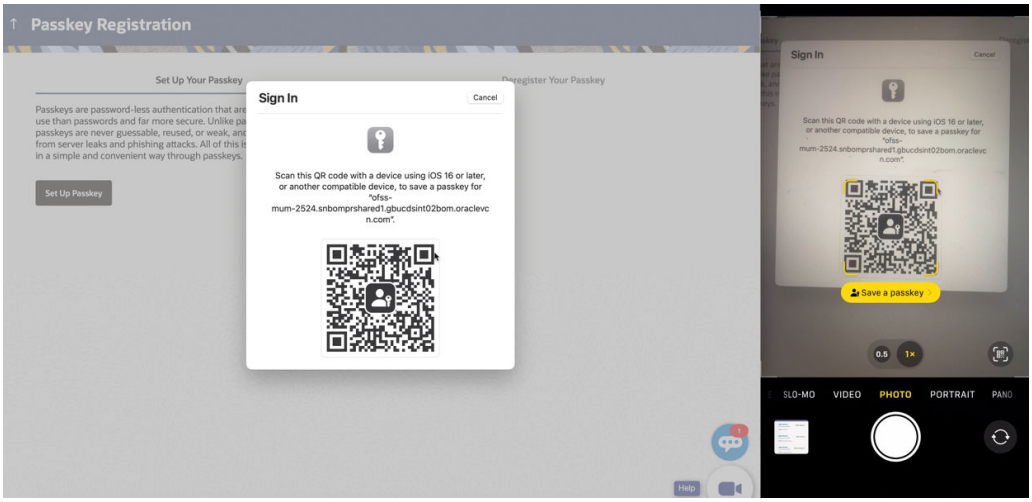
Figure 1-4 Sign In to device



   - You can select **Security Key** or select **Save a passkey on a device with a camera**.

     1) The device displays a **QR** code; use a camera on a device that supports passkey authentication to scan it.

Figure 1-5 Scanning QR Code to save passkey



2) To scan the QR code, open your Camera app and hold it up to the QR code on the connecting device's screen.

9. Click **Save Passkey**.
10. Click **Continue** on the device.
11. The operating system may require an authentication step, such as Face ID, fingerprint, or device password verification, before registering a passkey.

    The same mechanism will be used during login through stored passkey.

> **Note**
>
> This feature requires Bluetooth to be enabled on both devices.

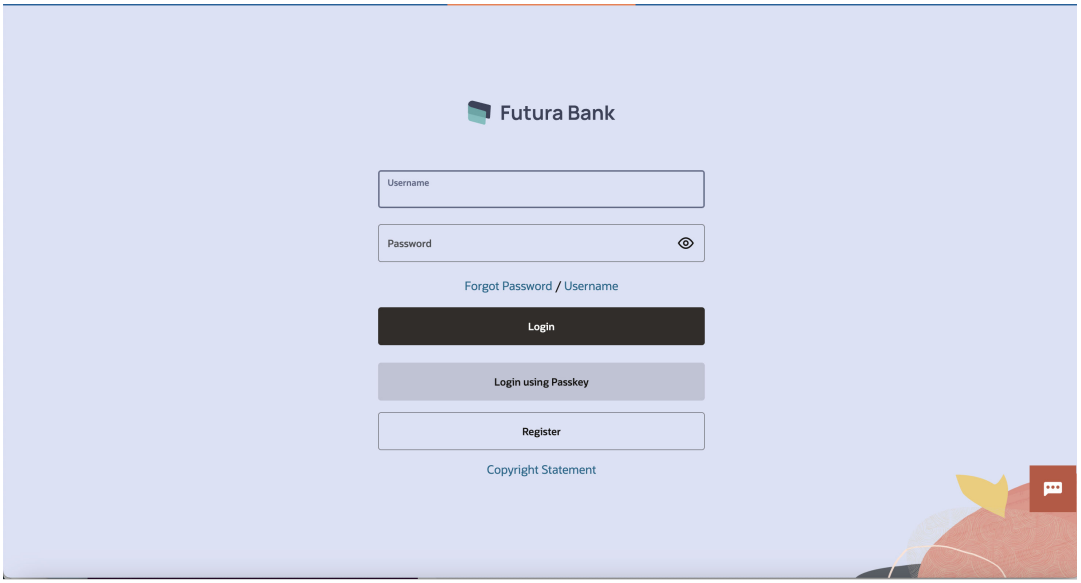
The passkey will be securely saved after successful registration.

1.2 Authentication Using Passkey

This topic provides the systematic instructions for implementing Passkey authentication.

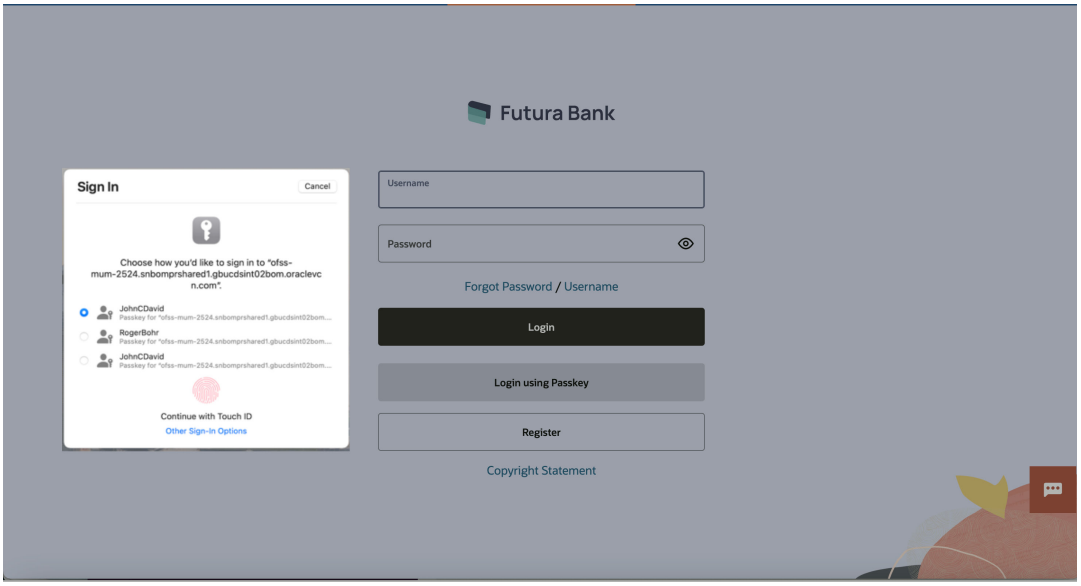
1. On **Login Page**, click on **Passwordless Login**.

Figure 1-6 Futura Bank pre-login page



2. User will be prompted to authenticate using stored passkeys on his device.

Figure 1-7 Prompt to authenticate using stored passkeys



3. User can also authenticate using a **security key** or **use passkey from a device with camera**.

> **Note**
>
> If the user selects passkey from a device with camera option, he will be shown a QR code which he can scan using a mobile device and login using saved passkey on that device by undergoing same passkey authentication mechanism as was used during passkey registration.

4. Click **Allow**, then **Allow again** to use your passkeys to sign in future.

   The system displays the success message of allowing you to use your passkeys to sign in future.

5. Click **OK**.

   a. Goto **Deregister your Passkey** section to deregister the passkey set for a devices.

   b. You can log into your account using the biometric data, PIN, or whatever method you use to sign in to your Android phone/web browser/iOS devices.

2 FAQ

1. **Does deregister passkey remove passkey from device?**
   No. When you deregister the passkey it only gets removed from server and not from device or your device's keychain or password manager. Since passkey works on public-private key infrastructure, and deregistering the passkey removes public key from server , the device's private key cannot be used to authenticate and access login to the application or for any other use.
2. **Does the user need to re-register for passkey after certain time duration?**
   No. Passkeys have no expiry. Hence the passkey created once does not require any re-registration.
3. **Is there support for cross-platform application for passkey?**
   No. As of May'23, cross platform support for passkeys is not enabled. So a passkey created for android device cannot be used to authenticate an iPhone device and same is for similar other cross channel cases.
4. **Can I still use "alternate login" for application login?**
   No. If the bank provides option for passkey login then alternate login cannot be used for application login on mobile devices. It's an either "Passkey" or "Alternate Login" option.
5. **Can I use passkey for siri/iMessage type payments?**
   No. Passkeys can only be used for application login.
6. **What versions of Android and iOS are supported for passkeys?**
   Android 9 and higher. iOS/iPad OS 16 and higher.

   For more on info on passkey support for chrome and android refer to this link : https://developers.google.com/identity/passkeys/supported-environments#chrome-passkey-support-summary

Index