Passwordless Login through Passkeys User Manual
Oracle Banking Digital Experience
Patchset Release 22.2.5.0.0

Part No. F72987-01

October 2024

Passwordless Login through Passkeys User Manual

October 2024

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 Purpose

Welcome to the User Guide for Oracle Banking Digital Experience. This guide explains the operations that the user will follow while using the application.

1.2 Audience

This manual is intended for Customers and Partners who setup and use Oracle Banking Digital Experience.

1.3 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 customers that have purchased support 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 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.

1.5 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.

1.6 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.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1.7 Screenshot Disclaimer

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.

1.8 Acronyms and Abbreviations

The list of the acronyms and abbreviations that you are likely to find in the manual are as follows:

Abbreviation	Description
OBDX	Oracle Banking Digital Experience

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 11.10.0.0.0	Oracle FLEXCUBE Universal Banking 14.7.4.0.0
1	Multifactor Authentication through Passkeys	**NH**	**NH**

3. Passwordless Login through 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.

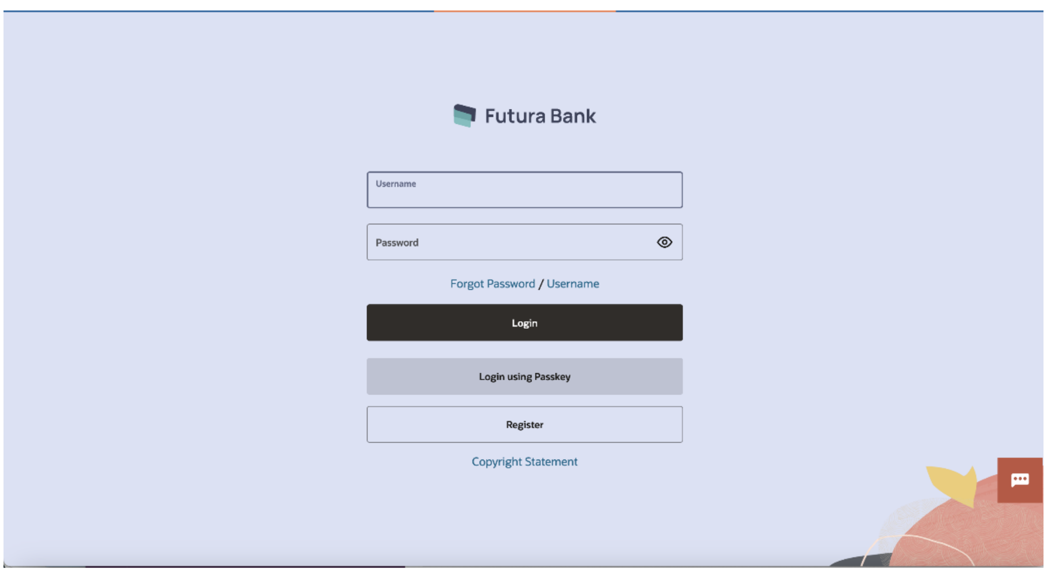
When you attempt to log in to a site that uses passkey technology, the site will send a push notification to the smartphone you used when you registered the account. When you use your face, fingerprint or personal identification number (PIN) to unlock the device, it will create a unique passkey and communicate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

3.1 Setting up Passkey

How to setup a passkeys on another device:

1. Launch the **futura bank App.** The **futura bank** pre-login screen appears.

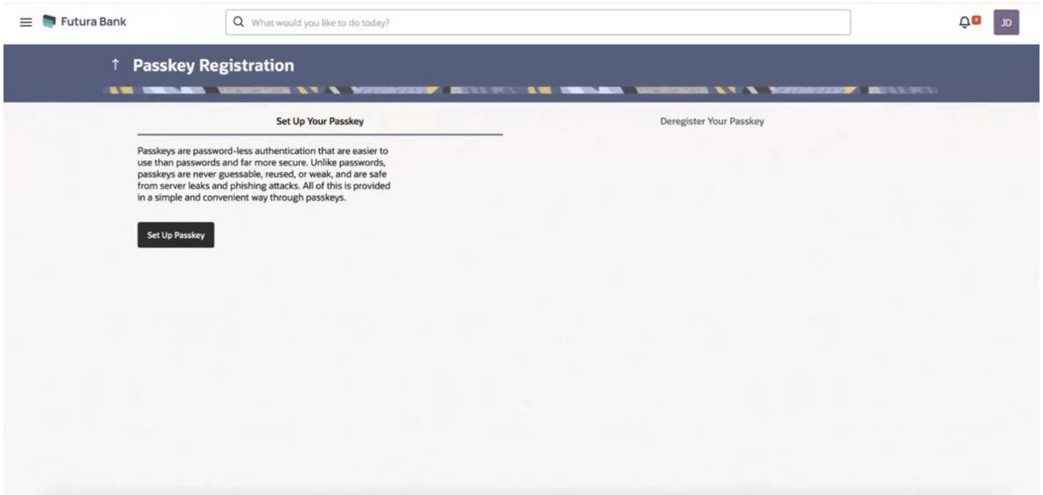
futura bank pre-login page



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

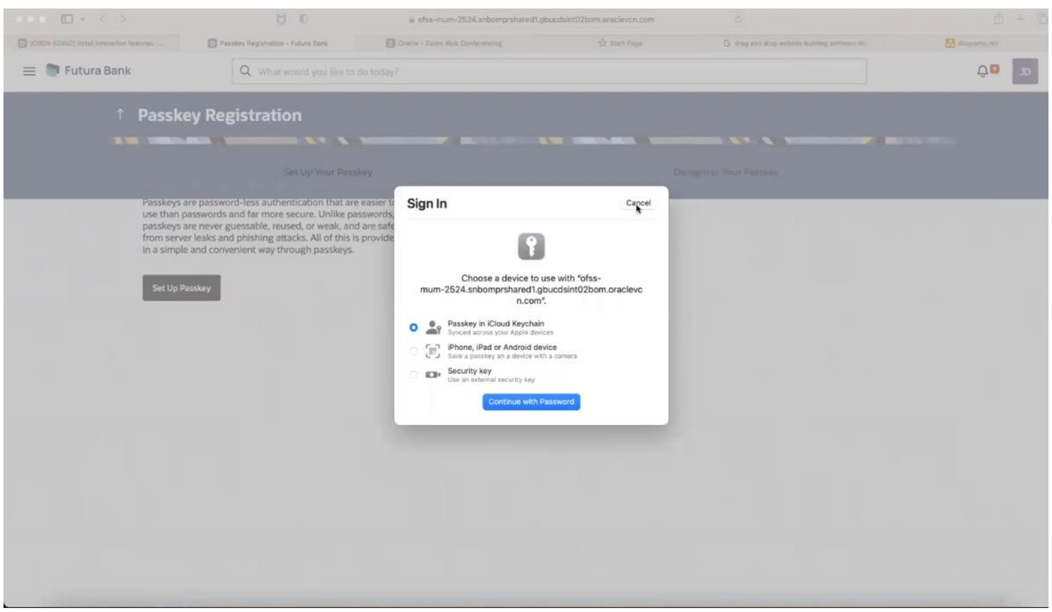
5. From the toggle menu, click **Account Settings**, and then click **Setup Passwordless Authentication**. The **Passkey Registration** page appears.

Passkey Registration screen



6. Click on the **Setup Passkey**.
7. 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.

Selection of device for Setup Passkey

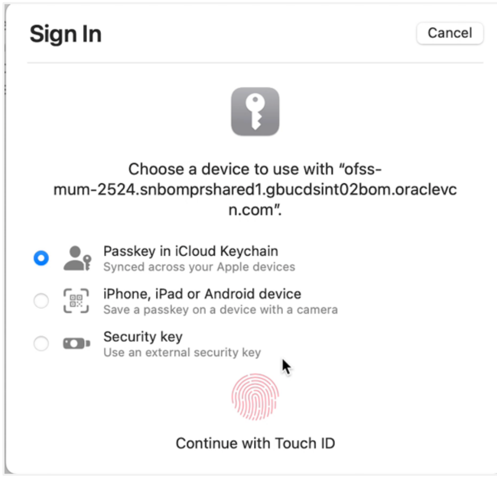


8. Select a desired device.
9. Click **Continue with Password**.

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.

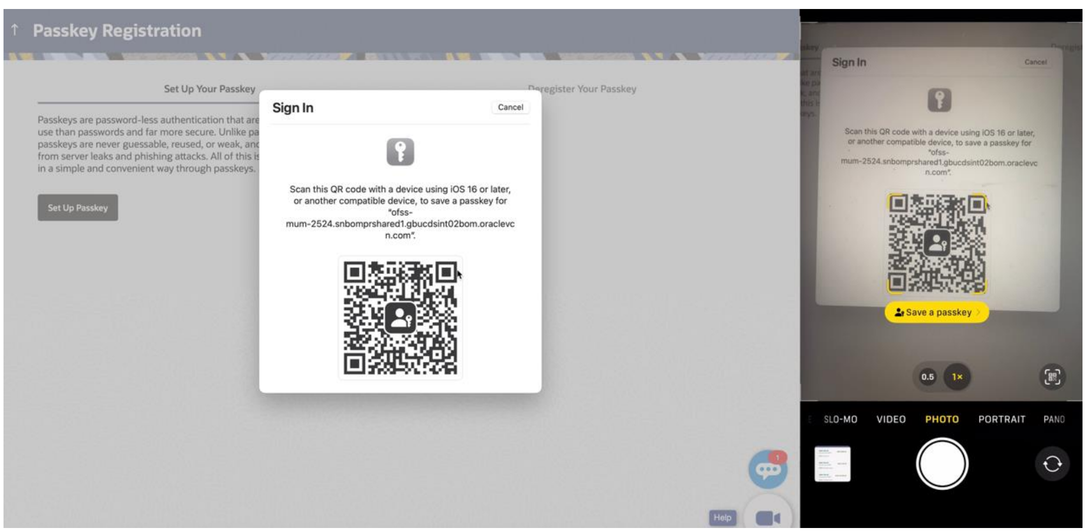
OR
On a device with biometric functionality, continue with biometric.

Sign In to device



OR
You can select **Security Key** or select **Save a passkey on a device with a camera**.
1) **QR Code** is displayed on the device, and it needs to be scanned with a device with camera that supports passkey authentication.

Scanning QR Code to save passkey



2) Open the Camera app on your device. Point the camera at the QR code on the screen of the device you want to connect to.

10. Click **Save Passkey**.
11. Click **Continue** on the device.
12. The operating system may ask for authentication mechanism such as Face ID/Fingerprint/device password for registering passkey. The same mechanism will be used during login through stored passkey.

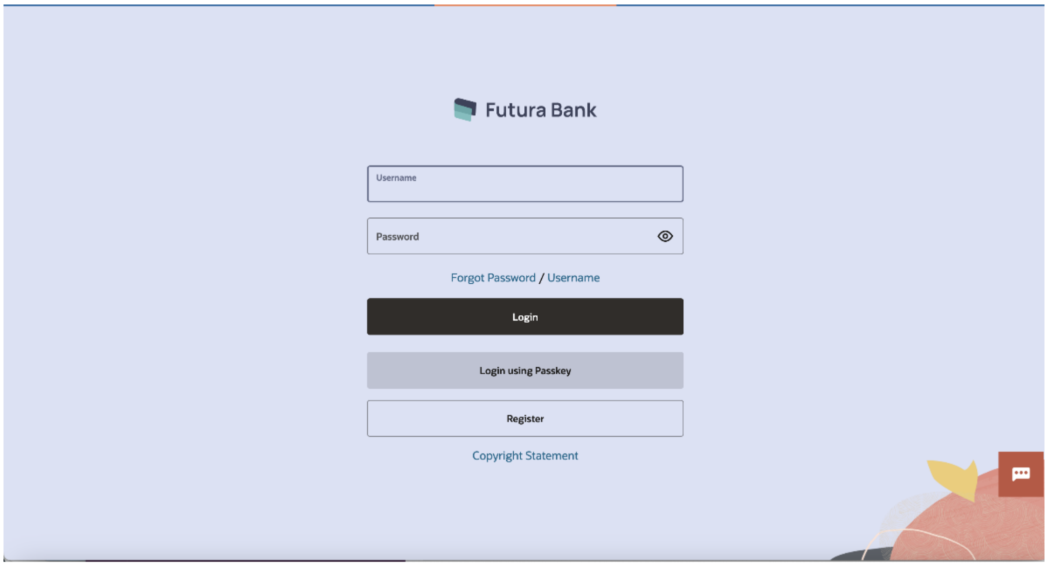
Note : For this feature to work, Bluetooth on both the devices needs to be turned ON.

13. On successful registration, passkey will be saved.

3.2 Authentication Using Passkey

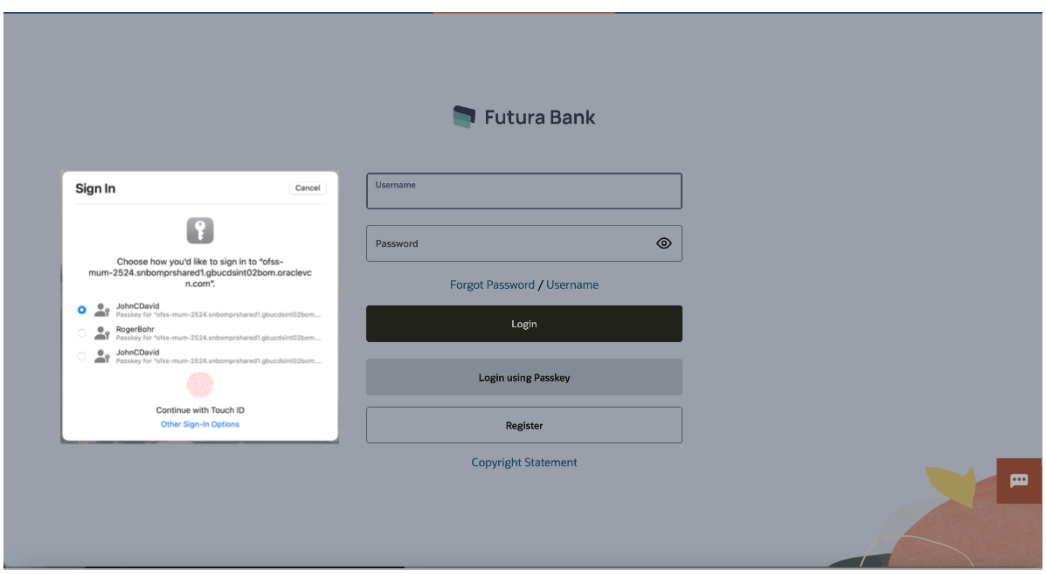
1. On Login Page, click on **Passwordless Login**.

futura bank pre-login page



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

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.
5. The system displays the success message of allowing you to use your passkeys to sign in future**.**
6. Click **OK**.

Note:
1.Goto **Deregister your Passkey** section to deregister the passkey set for a devices.
2. 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.

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

   .