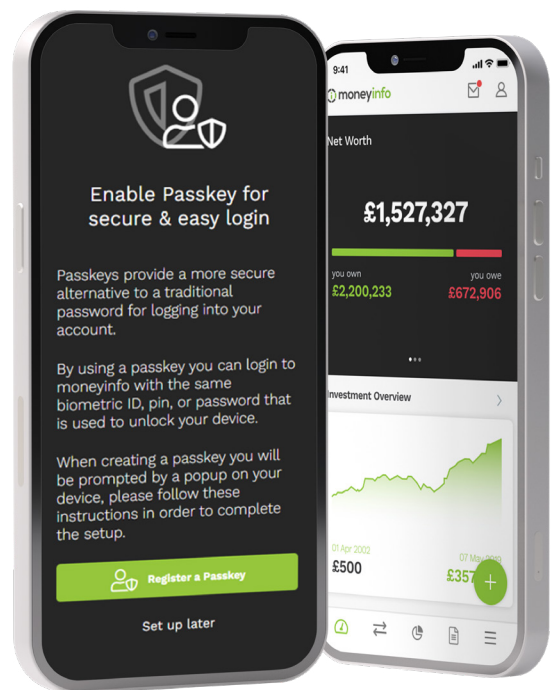




Passkeys User Guide



Document Control	
Document Name	Passkey Guide MI
Document Creation	13 th May 2025
Author/Owner	Alex Fletcher
Document Classification	Client Confidential
Document Last Updated	22 nd May 2025

Revision History			
Version	Date	Comments	Author(s)
1.0	22 nd May 2025	Initial Version	Alex Fletcher

Contents

What are Passkeys?..... 3

Why are we implementing passkeys? 3

Which devices can use passkeys? 3

Setting up passkeys 4

Login in using Passkeys 8

Managing Passkeys 9

FAQs 11

 Passkeys Overview and Security Benefits 11

 Device Setup and Compatibility 11

 User Control and Preferences 12

 Branding, Support and Rollout..... 12

Any Questions? 13

What are Passkeys?

Passkeys are a modern authentication method backed by Apple, Google, and Microsoft. They replace traditional passwords with biometric verification (such as Face ID, fingerprint, or a device PIN), making login faster, easier, and more secure.

Passkeys represent an industry-standard upgrade in login security. Unlike traditional biometrics in apps, Passkeys use public-key cryptography, the private key stays on your device, and only the public key is shared with the server.

Why are we implementing passkeys?

Introducing Passkeys is a step towards smarter, more secure authentication. It allows users to log in with biometrics and simplifies desktop access beyond two-factor authentication.

Unlike passwords, passkeys are resistant to phishing attacks and are not vulnerable to data breaches, as they are not stored on servers.

Passkeys are fast becoming the new standard in authentication. Major technology companies such as Apple and Microsoft have integrated passkey support into their ecosystems. This widespread adoption facilitates a more secure and consistent authentication experience across various platforms and devices.

Passkeys is replacing the current pin code and biometric login methods on the moneyinfo app. Additionally, your clients will be able to login to the app using their username and password, giving them the option to choose their preferred verification method.

Phishing resistance - Passkeys can't be used on fake or malicious websites

No server-side secrets - Nothing sensitive is stored on the server, reducing breach risk

Elimination of weak/reused passwords - Each Passkey is unique, removing human error.

Built-in multi-factor authentication - Your device and biometric ID work together.

Protection against credential theft - They're immune to brute-force and credential stuffing attacks.

Which devices can use passkeys?

Passkeys are compatible with any device using the following operating system versions or above.

- iOS 16
- Android 9
- Windows 10
- MacOS 13

You will have the option to enable Passkeys for desktop/browser-based logins; however, this is not mandatory. If you want more details on the browser version of Passkeys, please contact our support team.

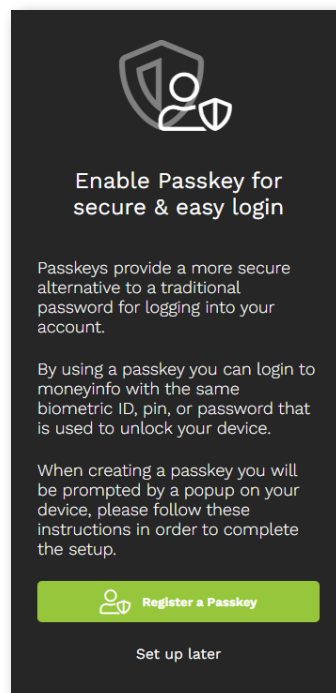
Setting up passkeys

Passkeys can be set up by your clients either by following the prompt displayed during their first login following the app update, or via the new page added to the “My Account” menu. To enhance the security and efficiency of your login process.

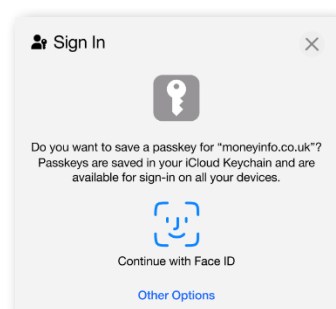
The moneyinfo app supports the use of passkeys. Both setup methods and details on how passkeys can be managed is detailed below.

On first login:

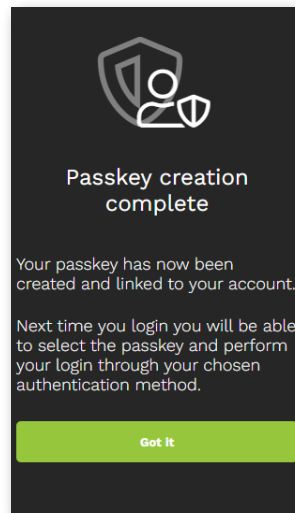
- 1) When the client first launches the app following the update, they will be asked to enter their username and password, followed by their two-factor authentication method if this has been configured.
- 2) After this, the client will be presented with the following prompt that explains what Passkeys are:



- 3) By clicking the “**Register a Passkey**” option, A device specific prompt will appear requesting you to authenticate using your device’s biometric method or PIN:

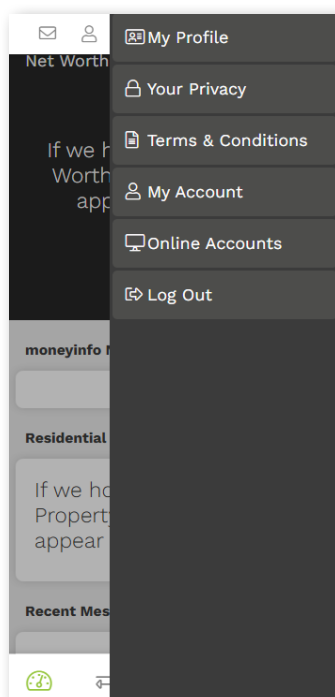


- 4) Once completed, the following confirmation screen will appear. Clicking **“Got It”** will then complete the passkey set up and take the user into their portal.
- 5) If the user instead clicks on the **“Set up later”** button on the initial Passkey prompt, they will skip the setup process, and the login will be completed.

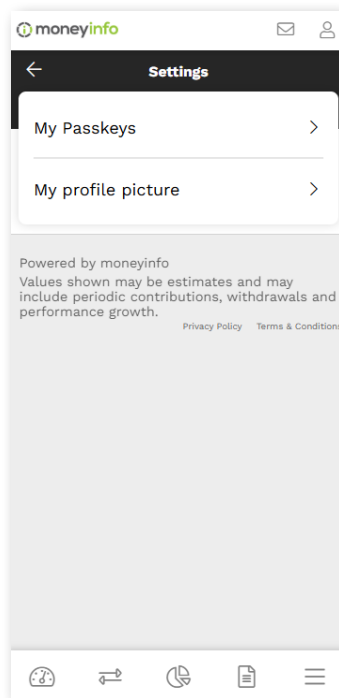


Via the My Account page:

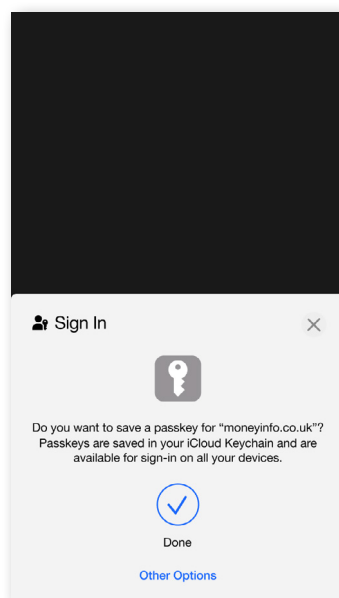
- 1) When logged into the portal, clients can click on the user icon located at the top-right corner of the screen. This will display the following options:



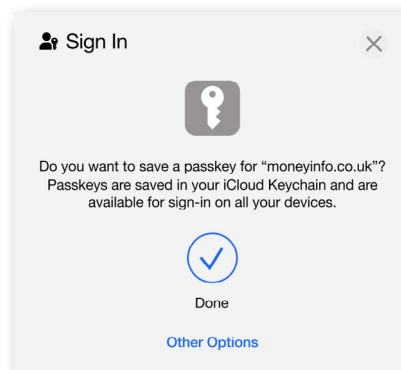
- 2) Click on the **“My Account”** button, then select **“My Passkeys”**.



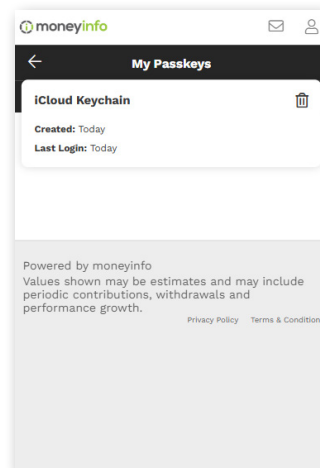
- 3) Click on the **“+”** icon. A prompt will appear requesting you to authenticate using your device's biometric method or PIN.



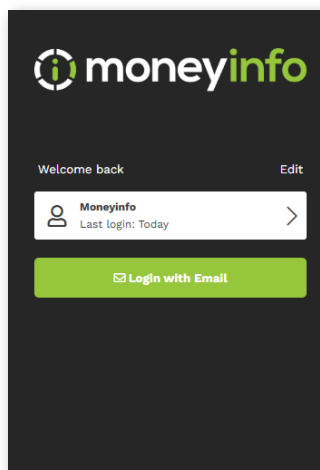
- 4) Upon successful authentication, a confirmation pop up message will appear on your device.



- 5) After confirming the device prompt, the newly created passkey will be displayed on the **"My Passkeys"** screen:

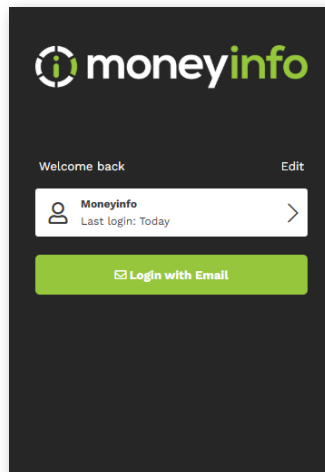


- 6) Following successful setup, the client will have the option to use their passkey upon next login.

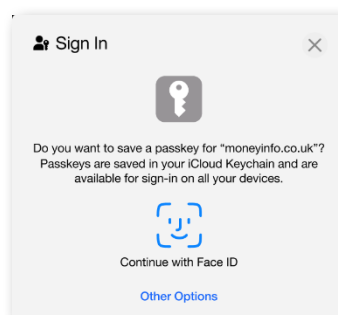


Login in using Passkeys

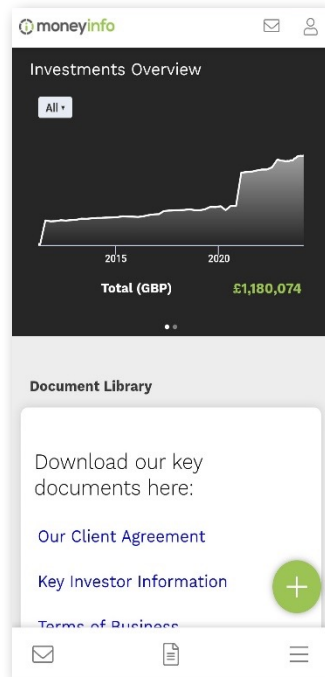
- 1) Click on the passkey on the login page.



- 2) A pop-up with the devices' verification methods will appear on the screen.



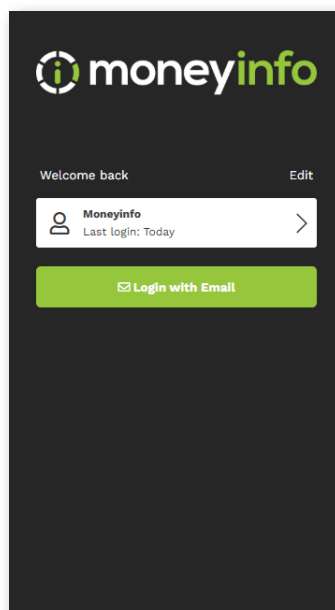
3) Upon successful authentication the client will be logged in.



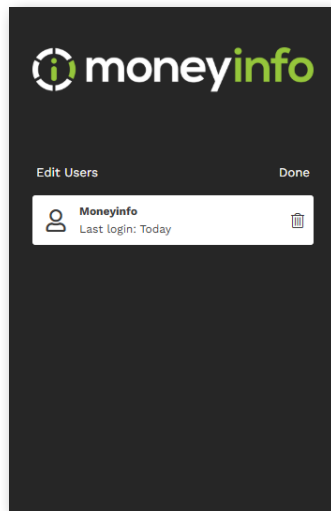
Managing Passkeys

Managing a Passkey from the Login Screen:

1) Open the moneyinfo app and click on the “Edit” option above the passkey.



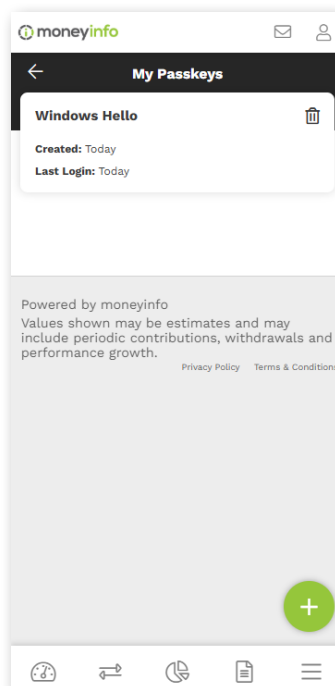
- 2) Click on the “**Bin**” icon next to the passkey you wish to remove.



This will mean that the passkey is no longer registered to the device and cannot be used to login to this account.

Managing Passkeys via the My Account Page:

- 1) Navigate to “**My Account**” and select “**My Passkeys**”.
- 2) Click on the “**Bin**” icon next to the passkey you wish to remove.



This method will allow you to remove the passkey from any device, ensuring that clients can keep their account secure even if they no longer have access to the device that the passkey was created for.

FAQs

Passkeys Overview and Security Benefits

What is the benefit of using Passkeys over the current biometric login?

Passkeys represent an industry-standard upgrade in login security. Unlike traditional biometrics in apps, Passkeys use public-key cryptography, the private key stays on your device, and only the public key is shared with the server.

They are backed by major providers like Apple, Google, and Microsoft, and offer several key benefits:

- **Phishing resistance** - Passkeys can't be used on fake or malicious websites.
- **No server-side secrets** - Nothing sensitive is stored on the server, reducing breach risk.
- **Elimination of weak/reused passwords** - Each Passkey is unique, removing human error.
- **Built-in multi-factor authentication** - Your device and biometric ID work together.
- **Protection against credential theft** - They're immune to brute-force and credential stuffing attacks.

Device Setup and Compatibility

Will clients need to register for a Passkey on every device they use?

Yes, Passkeys are device-specific. If a client uses more than one device, they'll need to register a Passkey on each.

Can the same Passkey be used on all a client's devices?

Not exactly. The Passkey itself is stored securely on each device, but the method of authentication (e.g. Face ID or fingerprint) can remain consistent across devices. Clients will need to set it up separately on each device but can use the same biometric method.

Can multiple clients set up Passkeys on a shared device?

Yes, multiple Passkeys can be created on a single device, so each client can have their own login credentials.

If a client's phone is stolen, can the Passkey be blocked?

Yes, clients can delete their Passkey themselves from the Accounts page in the app. If additional support is needed, your firm can contact moneyinfo support for help.

User Control and Preferences

If a client doesn't want to set up a Passkey, can they stop being asked?

Yes, if a client selects "Set up later" on first prompt, they won't be asked again automatically. They can still enable Passkeys at any time from the Accounts page.

Branding, Support and Rollout

Will the Passkey login appear under my firm's branding or moneyinfo's?

It will appear under your firm's branding. Any use of moneyinfo branding seen during demos is purely for demonstration purposes.

Will this also apply to the MIM app?

Yes, the update will be rolled out to the MIM app once development is complete.

Do you have a one-page guide we can send to clients ahead of launch?

Yes, we already have guidance prepared. This is currently being reviewed and will be distributed before the update goes live.

How will we know when Passkeys will be implemented?

We will communicate with you when you can expect the update to take place. Please look out for an email from us.



Any Questions?

For further guidance with the Passkeys update, please contact our support team. We will be able to answer any further questions you may have related to the app update and can help you set up the optional browser-based Passkey logins too.

Call us on 03303 600 300
or Email us at support@moneyinfo.com
Visit: www.moneyinfo.com

