

swidch

OTAC auth Mobile App User Manual



V 1.0.4

swidch Ltd.

swidch
Address: 1st floor, 3 More London Pl, London SE1 2RE
Tel: +44 (0) 2032834081
Mail : developer@swidch.com

Contents	
Introduction	3
Download the App	3
Initial PIN Setup	4
Account Registration	6
Settings - Edit Account	10
Settings - Security Features (PIN/Biometric)	13
Settings - Security Features (Use both)	15
Settings – Security Features (Enable Biometric Authentication)	17
Settings – Security Features (Disable Biometric Authentication)	19
Settings – Security Features(Change PIN)	21
Terms of Use	23

Introduction

This document is intended for end user's who will be using the OTAC auth app available on Google Play store and Apple App store. This mobile app works together with the backend OTAC service that typically protects web applications such as a PLC application. The mobile app generates a One Time Authentication Code (OTAC) which is the world's first one-way dynamic authentication technology that enables users to authenticate to PLC devices via their phone.

- **App Details:** Experience rapid and secure user/device authentication through OTAC's 8-character code.
- **Quick and Easy, No Registration:** Streamlined authentication without the hassle of sign-up or login processes. Your privacy is paramount; no personal information required.
- **Secure Authentication with OTAC Code:** Ensure robust security with time-sensitive OTAC codes. Safely access your accounts using a code that expires after a specific duration.
- **Manage Multiple Accounts Easily:** Effortlessly authenticate multiple accounts using a single OTAC auth app. Register and manage up to 20 accounts securely.

Once a PLC is protected with our solution, the user can authenticate to PLC utilizing our dynamic 'one-time authentication code' (OTAC) technology. The code is generated on our mobile app (available on Google Play and Apple App store), is valid for a short period of time and even works offline. OTAC combined with device biometrics and/or PIN provides a highly optimized and secure authentication solution specifically for ICS/OT security challenges.

Download the App

You can download the OTAC auth app from the respective Google and Apple app stores:



Initial PIN Setup

Launch the app After Installation

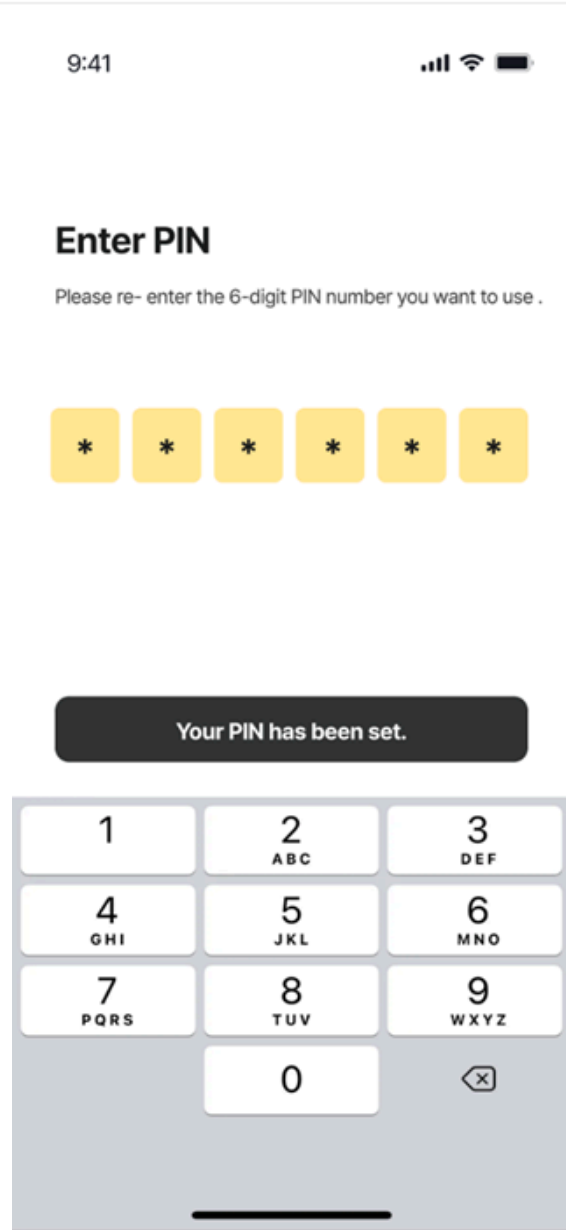
Install app, tap [Getting started] onboarding button.



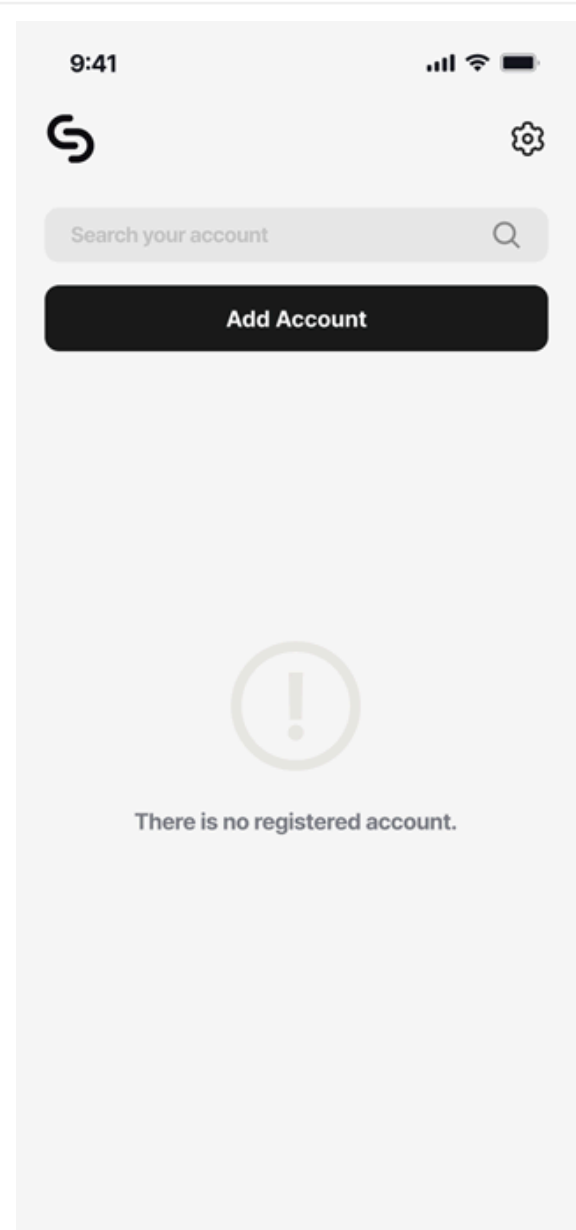
Enter a 6-digit PIN for app security.
- Enter it twice (App reset after 5 unsuccessful attempts).



PIN setup is complete.



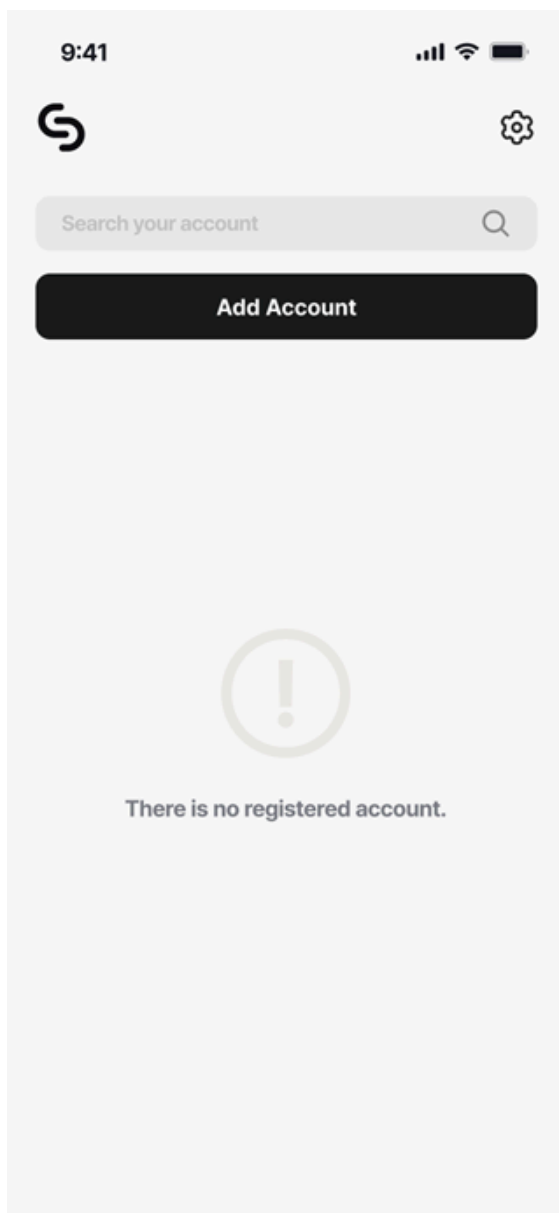
Navigate to the main screen.



Account Registration

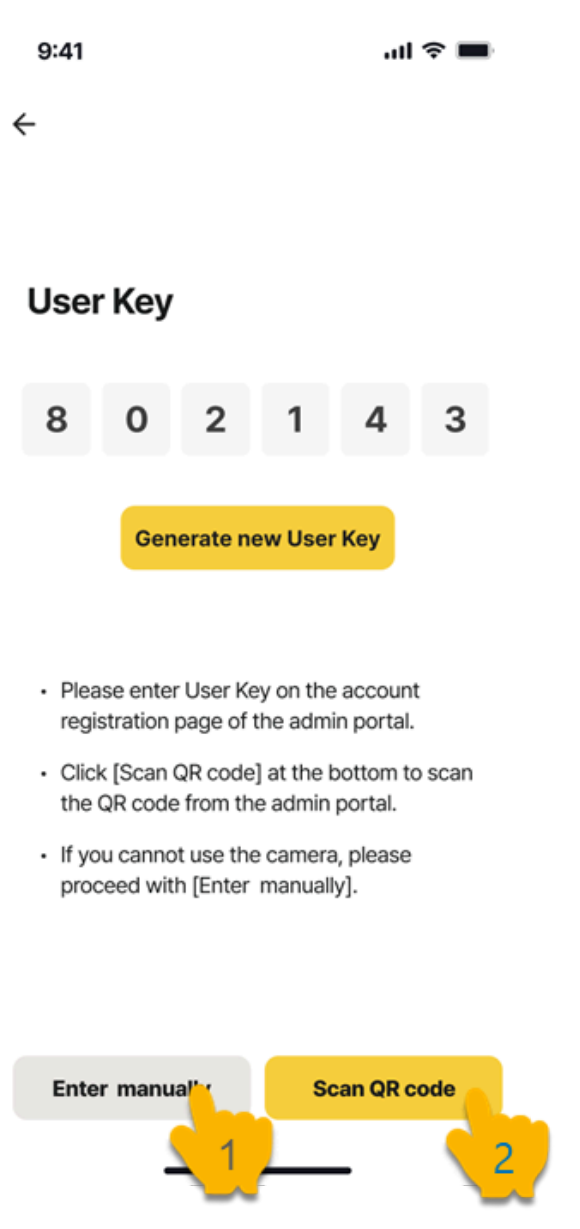
Now that the initial security PIN is set, you are ready to use the app. The first thing to do is to register for an account. The account registration happens in tandem with the administrator doing the same on the admin portal. For this you need your administrator to login to the admin portal simultaneously.

Select the [Add Account] button on the main screen.



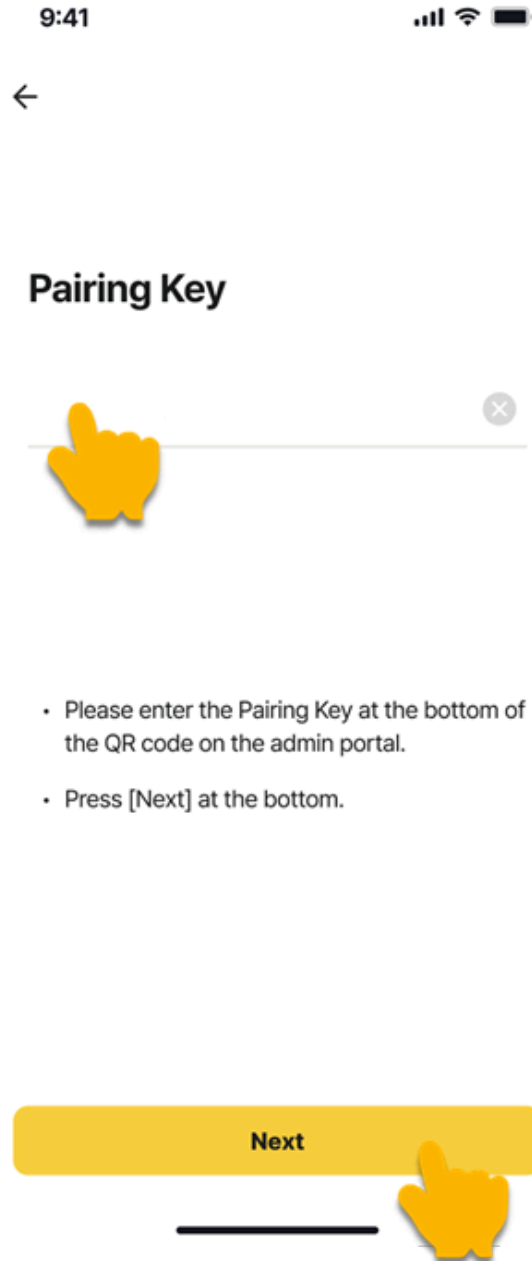
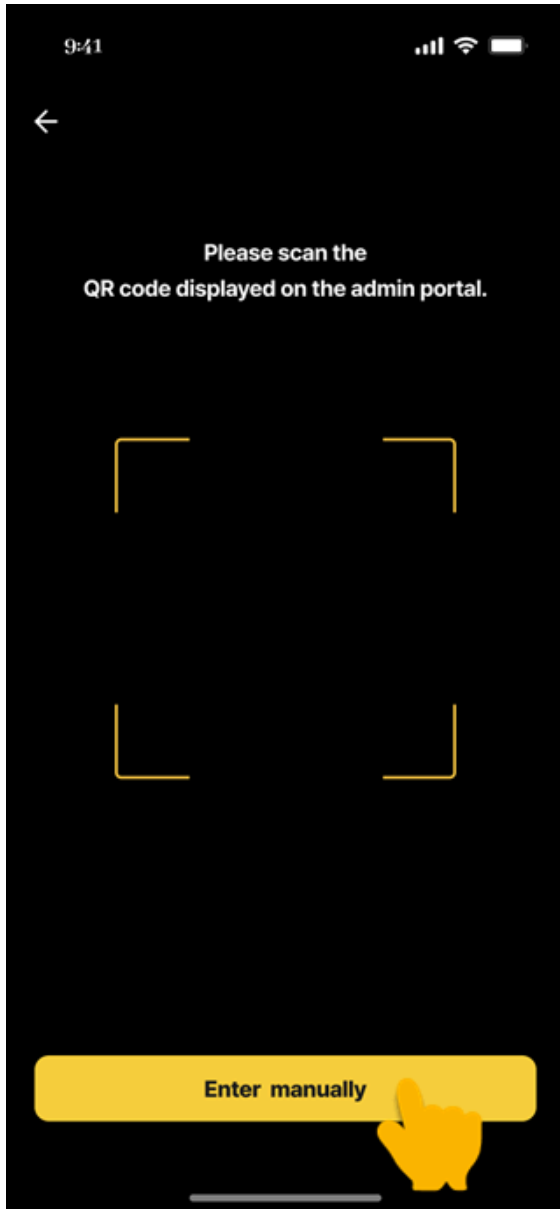
Enter the 6-digit User key on the admin portal.

1. If camera access is allowed select the "Scan QR Code"
2. If camera access is denied, select the "Enter manually"



If camera access is allowed Capture the QR code(Pairing Key) generated on the admin portal or enter it manually.

If camera access is denied, manually enter the QR code(Pairing Key) displayed on the admin website.
-If an error occurs, request a new User Key

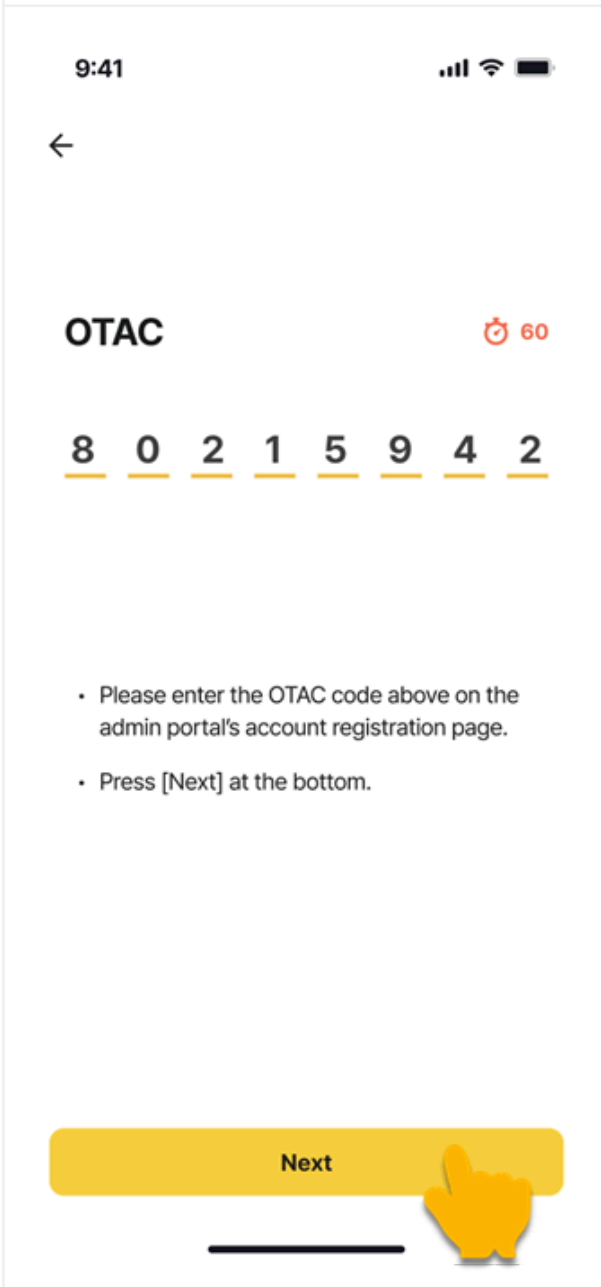
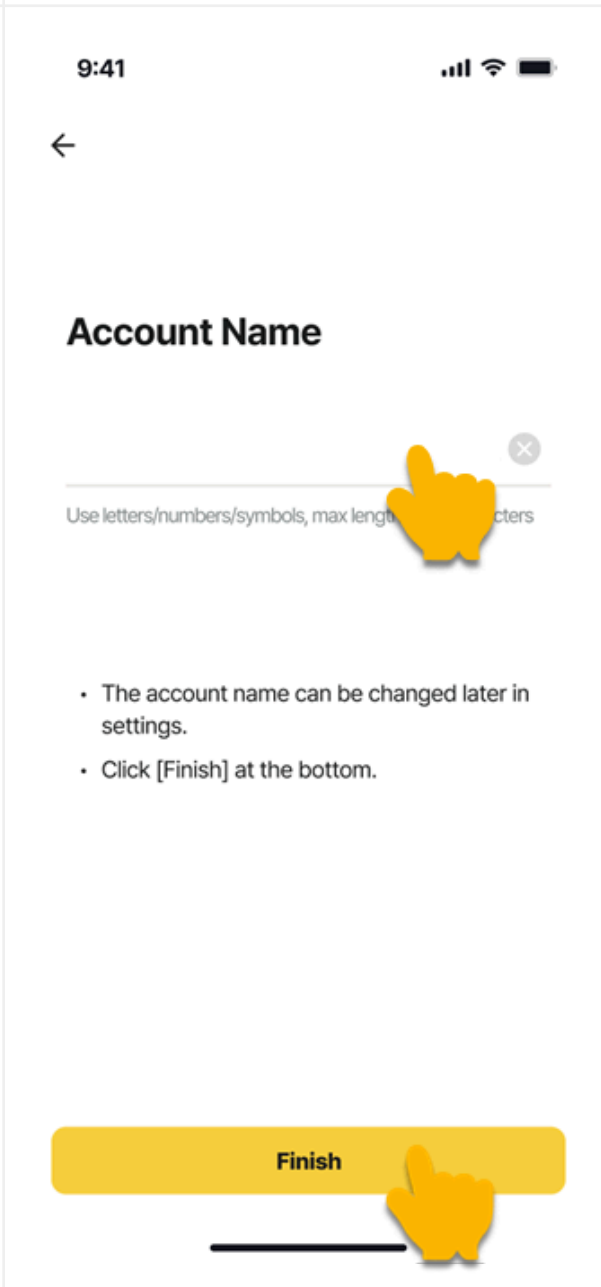


Enter the displayed OTAC on the screen into the admin portal.
-It 's valid for 60 seconds and

Set the name for the registered account.
- Up to 20 characters, including letters, numbers, and symbols.

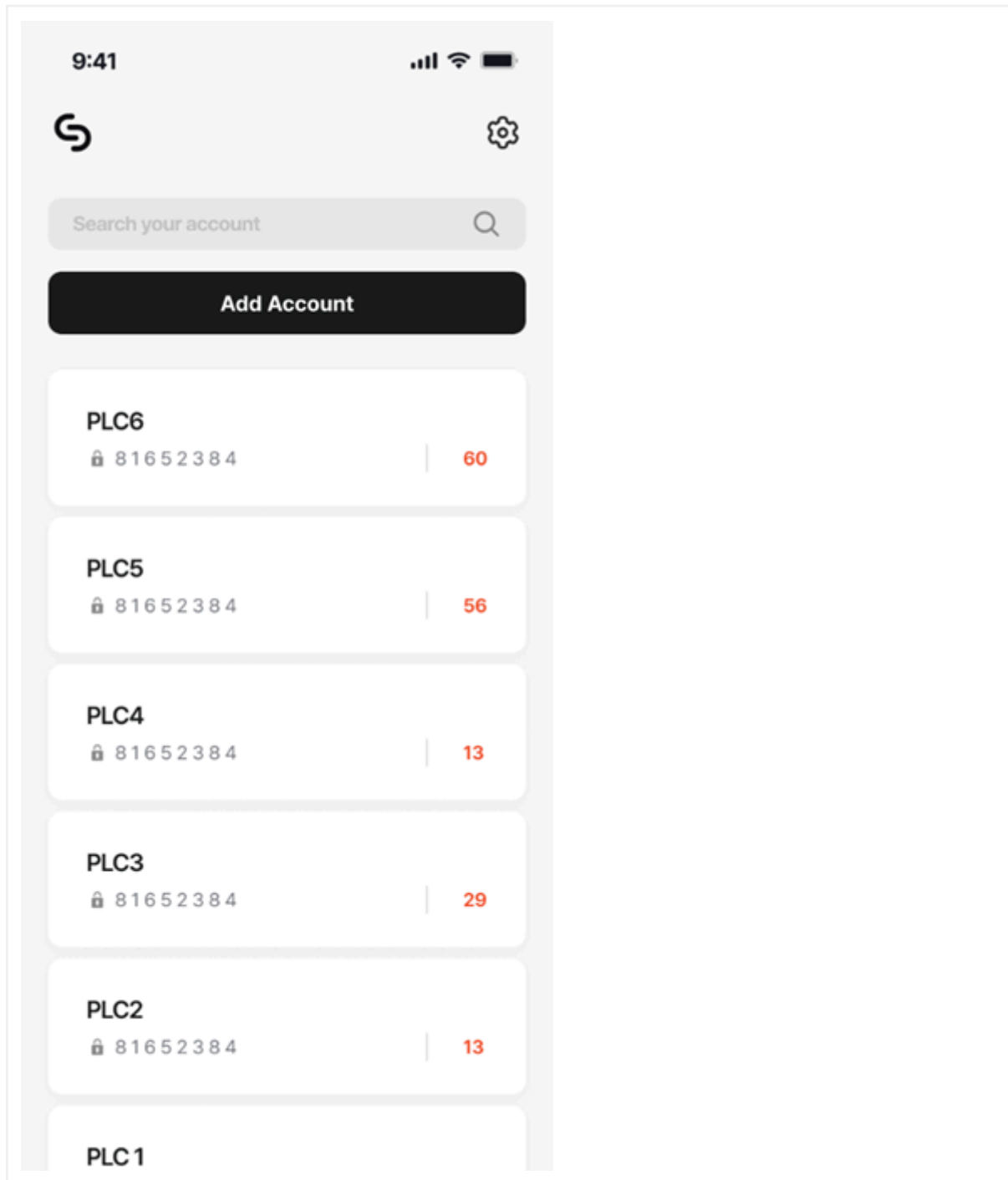
auto-refreshes.

- Cannot use duplicate account names.
- If the administrator has set an account name, it will be displayed.

 <p>The screenshot shows a mobile app interface for entering an OTAC code. At the top, the time is 9:41 and there are signal, Wi-Fi, and battery icons. A back arrow is on the left. The title 'OTAC' is centered, with a red timer icon and '60' on the right. Below the title, the code '8 0 2 1 5 9 4 2' is displayed in a row of eight yellow boxes. Below the code, there are two bullet points: 'Please enter the OTAC code above on the admin portal's account registration page.' and 'Press [Next] at the bottom.' At the bottom, there is a yellow 'Next' button with a hand icon pointing to it.</p>	 <p>The screenshot shows a mobile app interface for entering an account name. At the top, the time is 9:41 and there are signal, Wi-Fi, and battery icons. A back arrow is on the left. The title 'Account Name' is centered. Below the title, there is a text input field with a hand icon pointing to it. Below the input field, there is a small grey 'x' icon and a line of text: 'Use letters/numbers/symbols, max length 30 characters'. Below this, there are two bullet points: 'The account name can be changed later in settings.' and 'Click [Finish] at the bottom.' At the bottom, there is a yellow 'Finish' button with a hand icon pointing to it.</p>
---	---

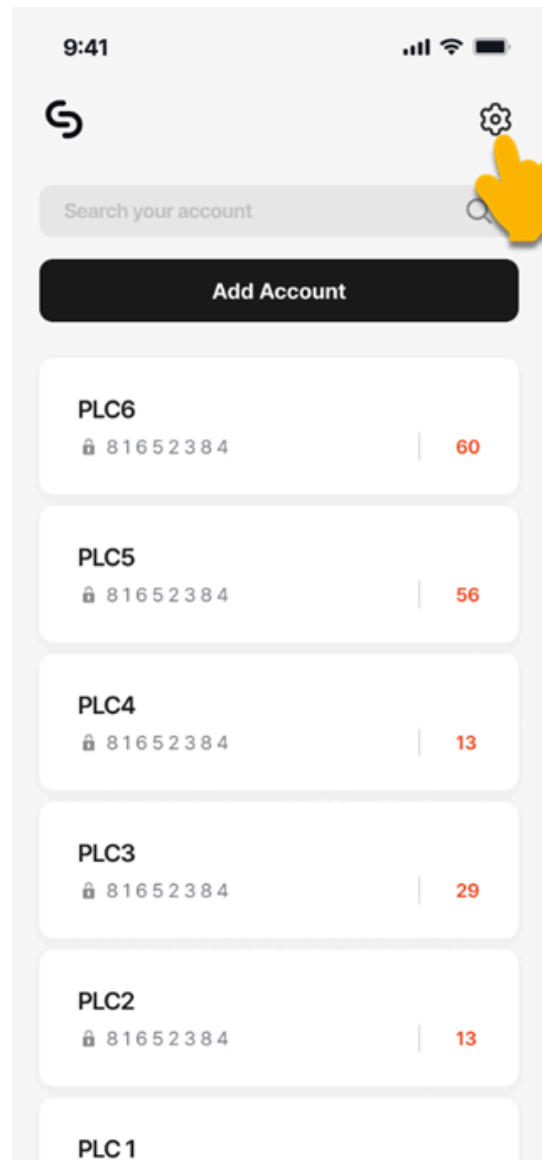
Account registration is complete.

- Registered accounts are sorted by the most recent.

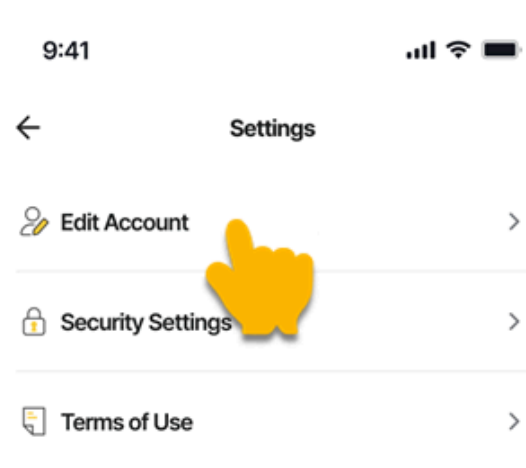


Settings - Edit Account

Select the [Settings] icon on the main screen.



Choose [Edit Account].

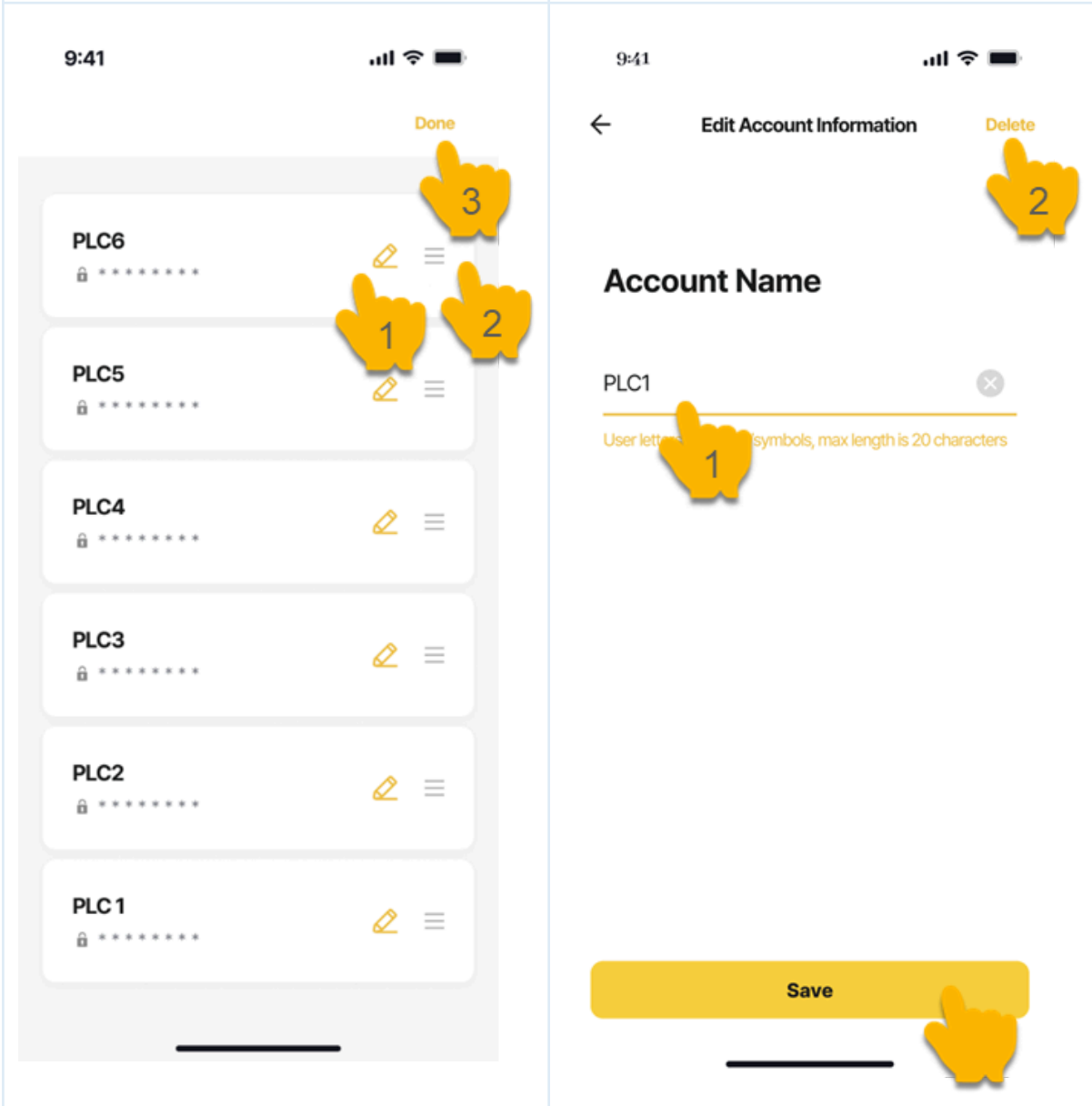


1. Click the [pencil] icon to edit account information.

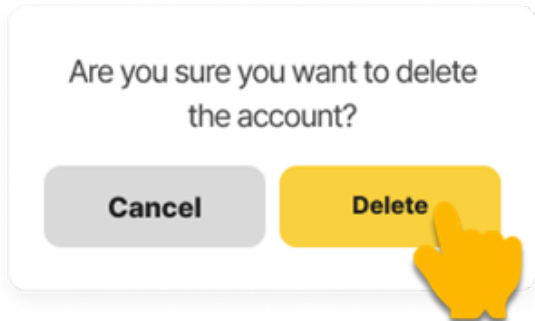
You can edit or delete the account name.

2. Use the [=] icon to Rearrange the order.
3. Click [Done] to Return to the main screen.

1. Use up to 20 characters, including letters, numbers, and symbols. Duplicate account names are not allowed.
2. Click [Delete] > Confirm in the popup dialog.



Clicking [Delete] will remove the account information from the app.
Click [Cancel] > Exit the delete popup.

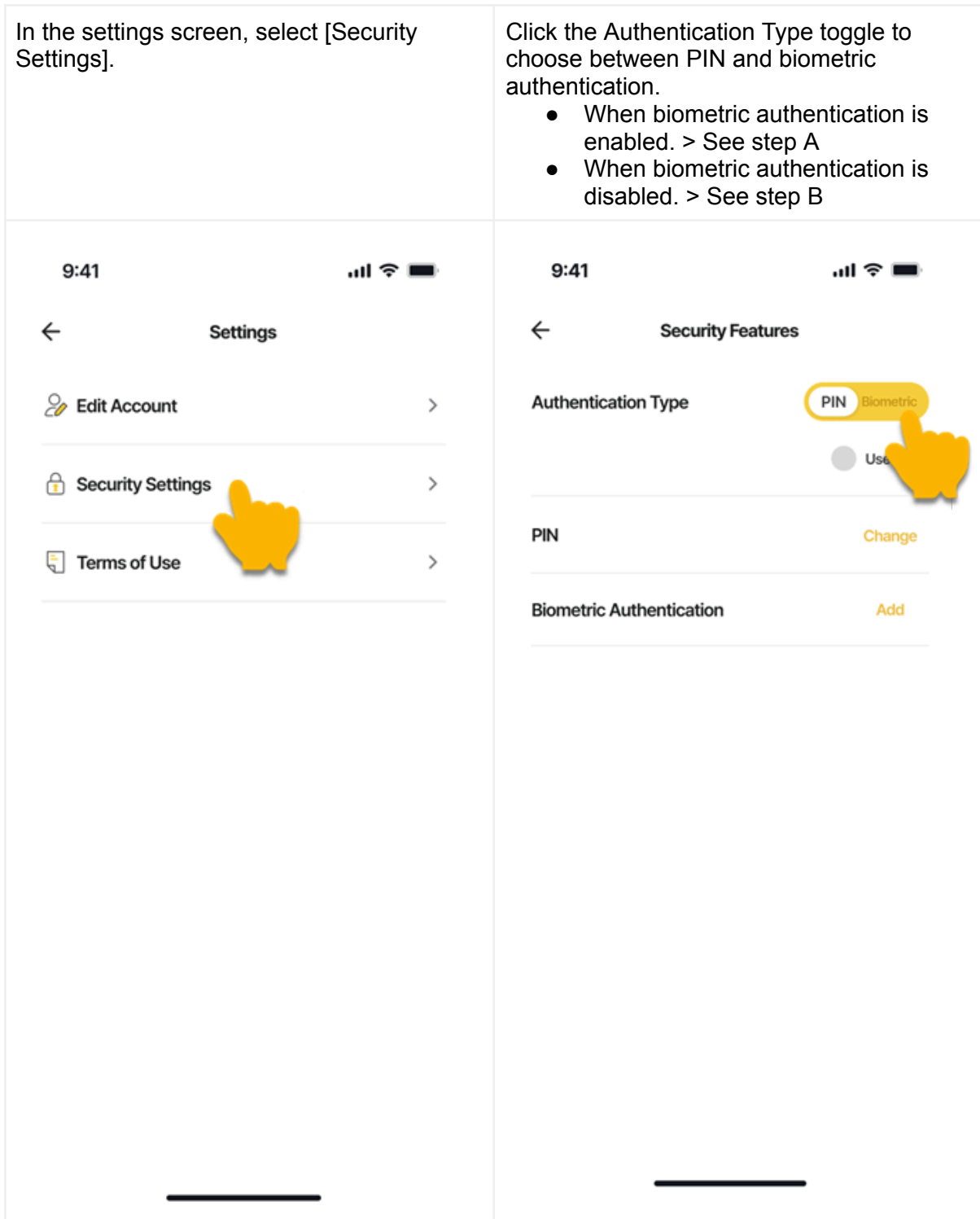


Settings - Security Features (PIN/Biometric)

In the settings screen, select [Security Settings].

Click the Authentication Type toggle to choose between PIN and biometric authentication.

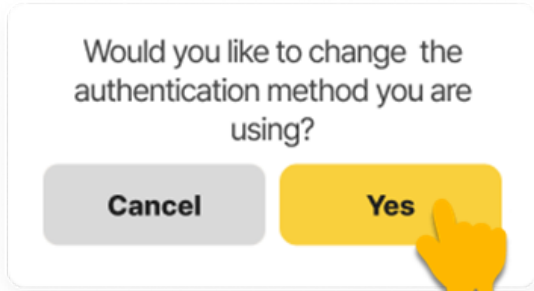
- When biometric authentication is enabled. > See step A
- When biometric authentication is disabled. > See step B



Step A

Click [Yes] in the popup to change the authentication method.

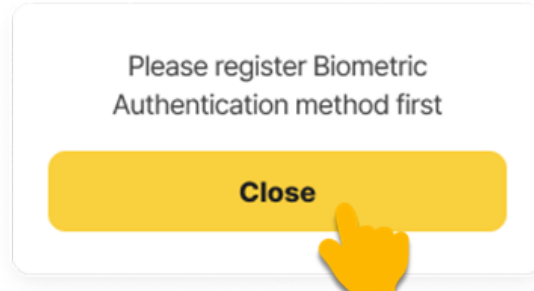
- Select [Yes] > Complete the change.
- Select [Cancel] > keep the current method.



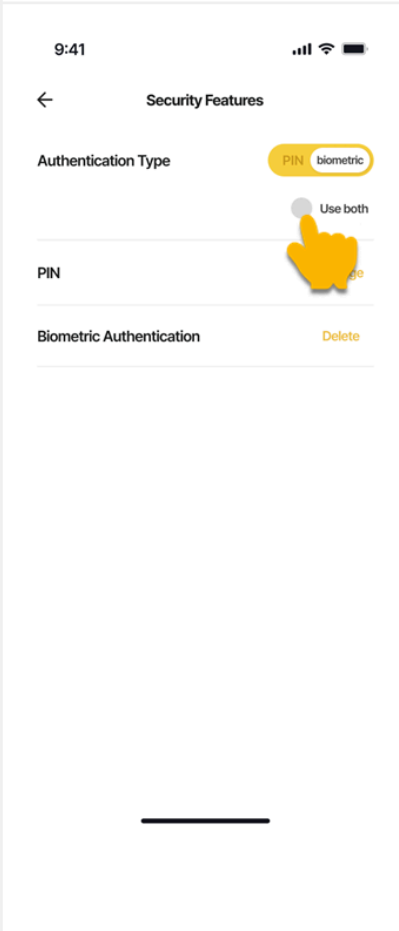

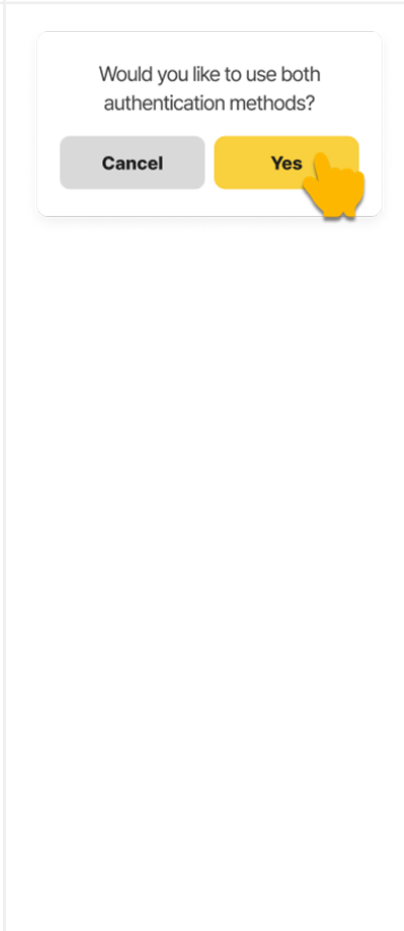
Step B

Biometric authentication inactive. Popup says to add a biometric method.

- Choose [OK]

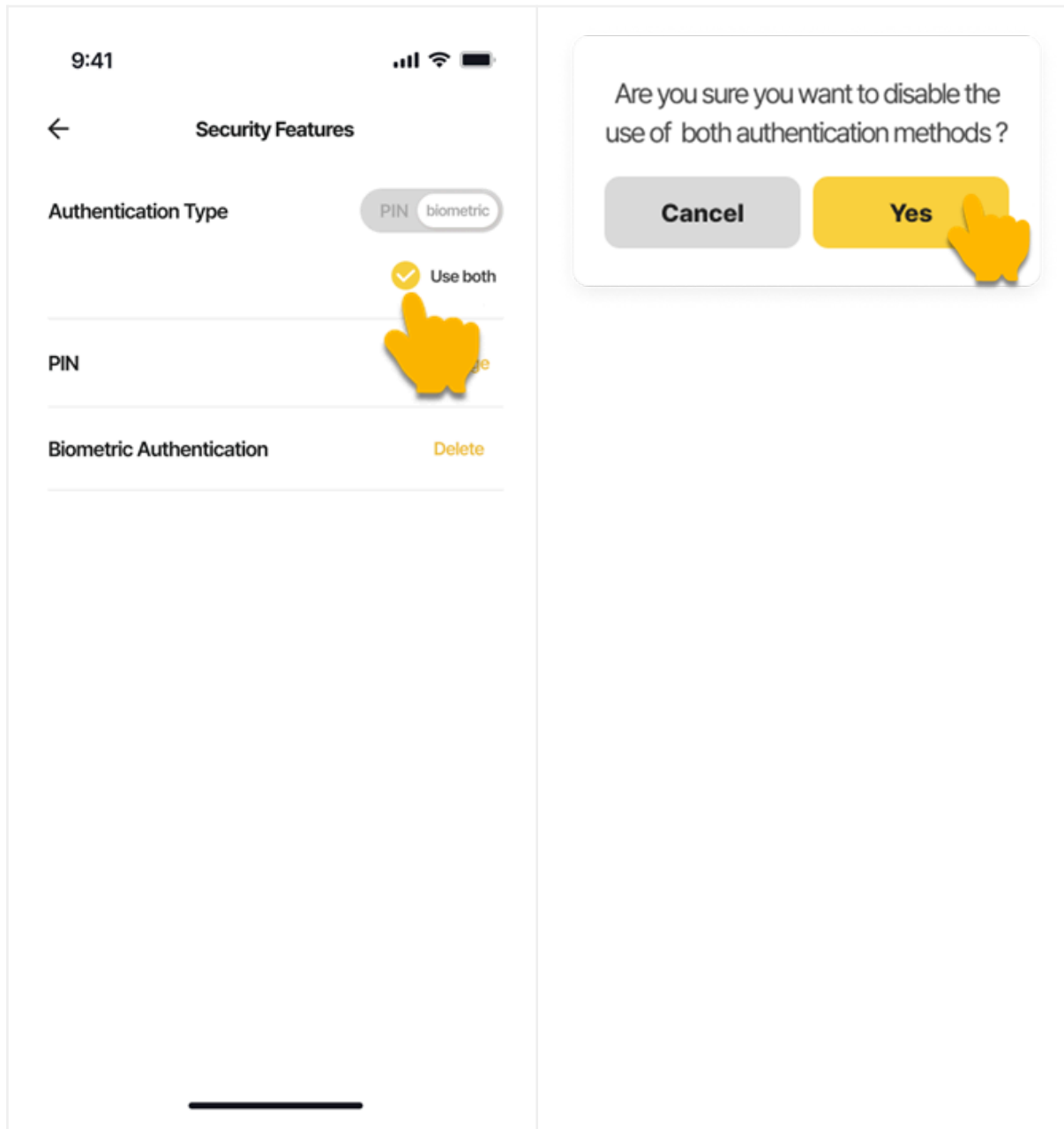


Settings - Security Features (Use both)

<p>In the security features screen, click the [Use both] button for authentication methods.</p> <ul style="list-style-type: none"> - Biometric authentication is disabled. > - Biometric authentication is enabled. > 	<p>When biometric authentication is disabled, an alert popup is displayed.</p> <ul style="list-style-type: none"> • Click [Close] > Close the popup. 	<p>When biometric authentication is enabled, a Confirm popup appears.</p> <ul style="list-style-type: none"> • Click [Yes] > Enable "Use both" • Click [Cancel] > Maintain the existing authentication method.
		

To deactivate the "Use both" feature, click the [Use both] button.

- A Confirm popup appears for deactivation.
- Click [Yes] > Switch to using only the authentication methods toggled ON.
 - Click [Cancel] > Maintain the "Use both" feature.



Settings – Security Features (Enable Biometric Authentication)

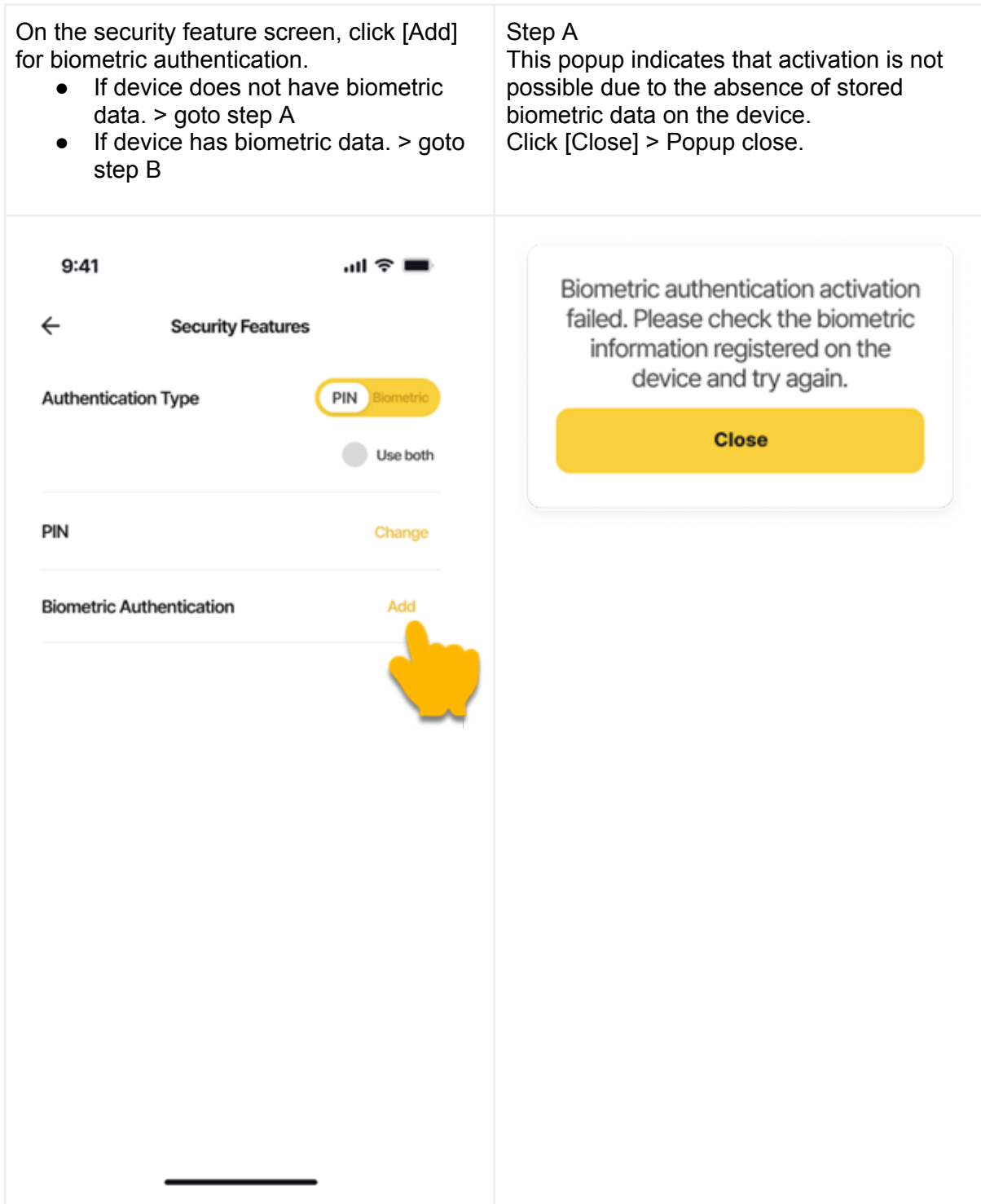
On the security feature screen, click [Add] for biometric authentication.

- If device does not have biometric data. > goto step A
- If device has biometric data. > goto step B

Step A

This popup indicates that activation is not possible due to the absence of stored biometric data on the device.

Click [Close] > Popup close.

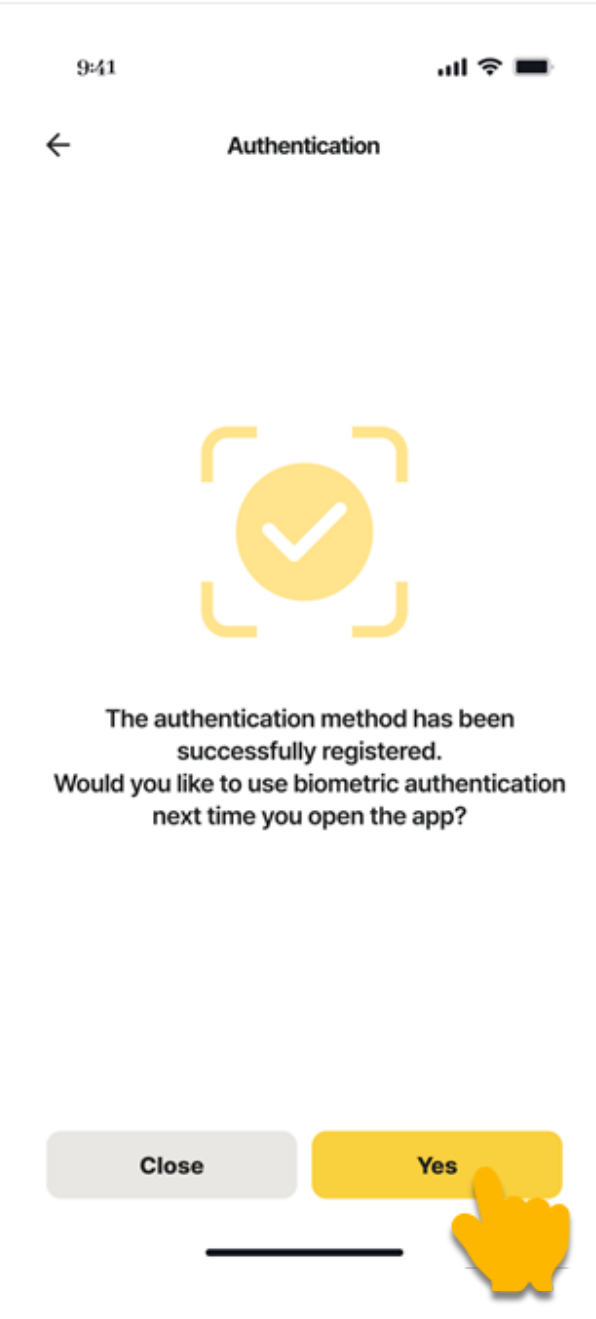
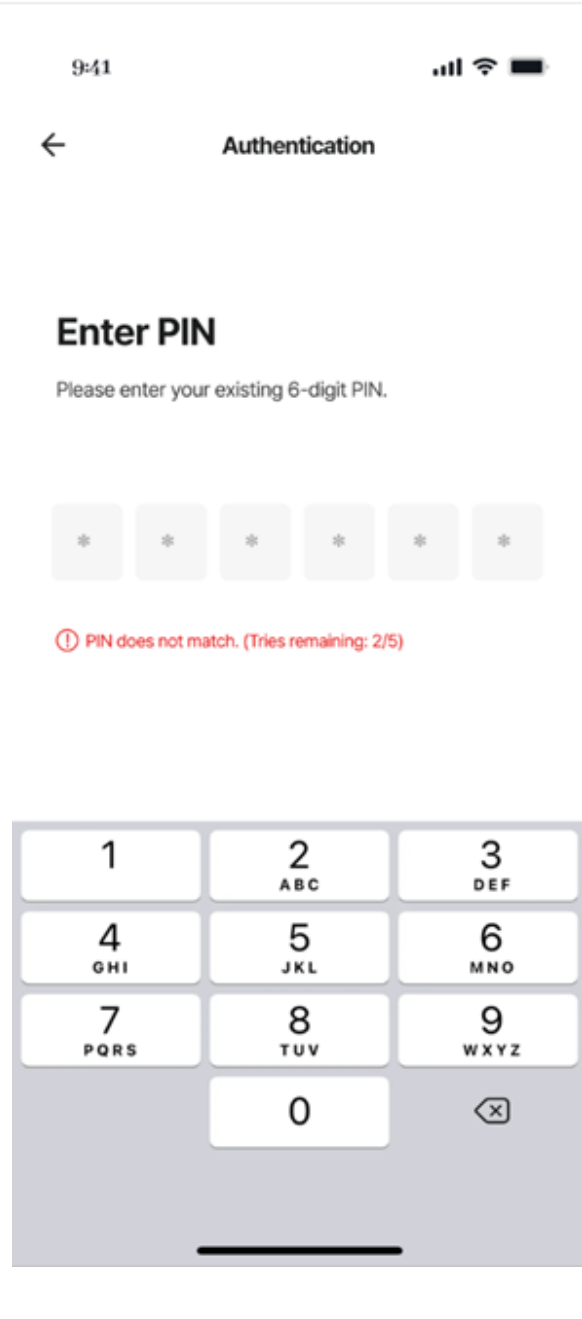


Step B

If the device has biometric data, enter the registered PIN.

Starting from the next login, you can choose whether to use biometric authentication.

- Click [yes] > Switch to biometric authentication
- Click [Close] > Continue using PIN



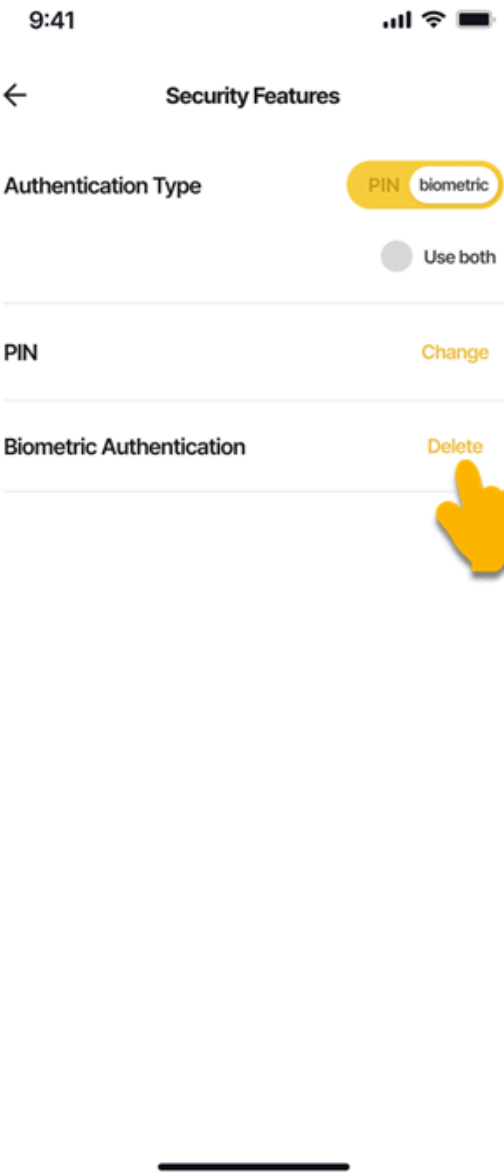
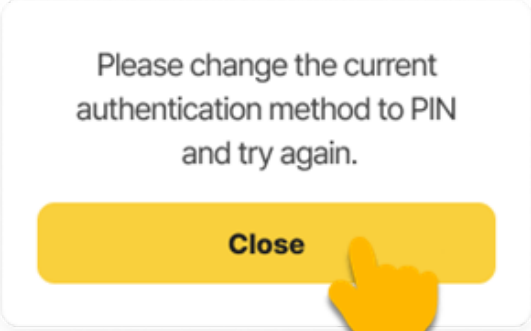
Settings – Security Features (Disable Biometric Authentication)

On the security features screen, select the [Delete] button for biometric authentication.

- When the authentication method is set to PIN > goto step A
- When the authentication method is set to biometric or “Use both” > goto step B

Step A

Authentication set to biometric or “Use both“, a popup prompts PIN method change.

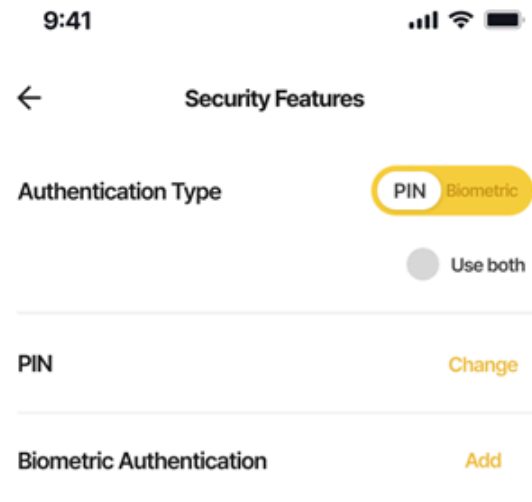
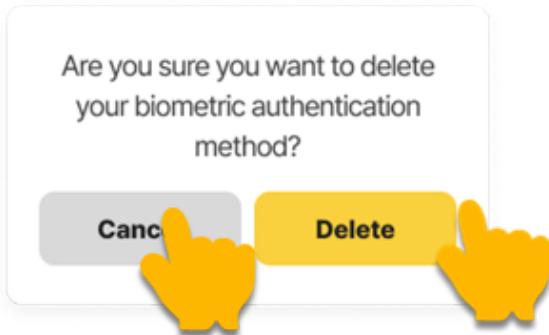
<p>On the security features screen, select the [Delete] button for biometric authentication.</p> <ul style="list-style-type: none"> • When the authentication method is set to PIN > goto step A • When the authentication method is set to biometric or “Use both” > goto step B 	<p>Step A Authentication set to biometric or “Use both“, a popup prompts PIN method change.</p>
	

Step B

Popup asks to deactivate authentication.

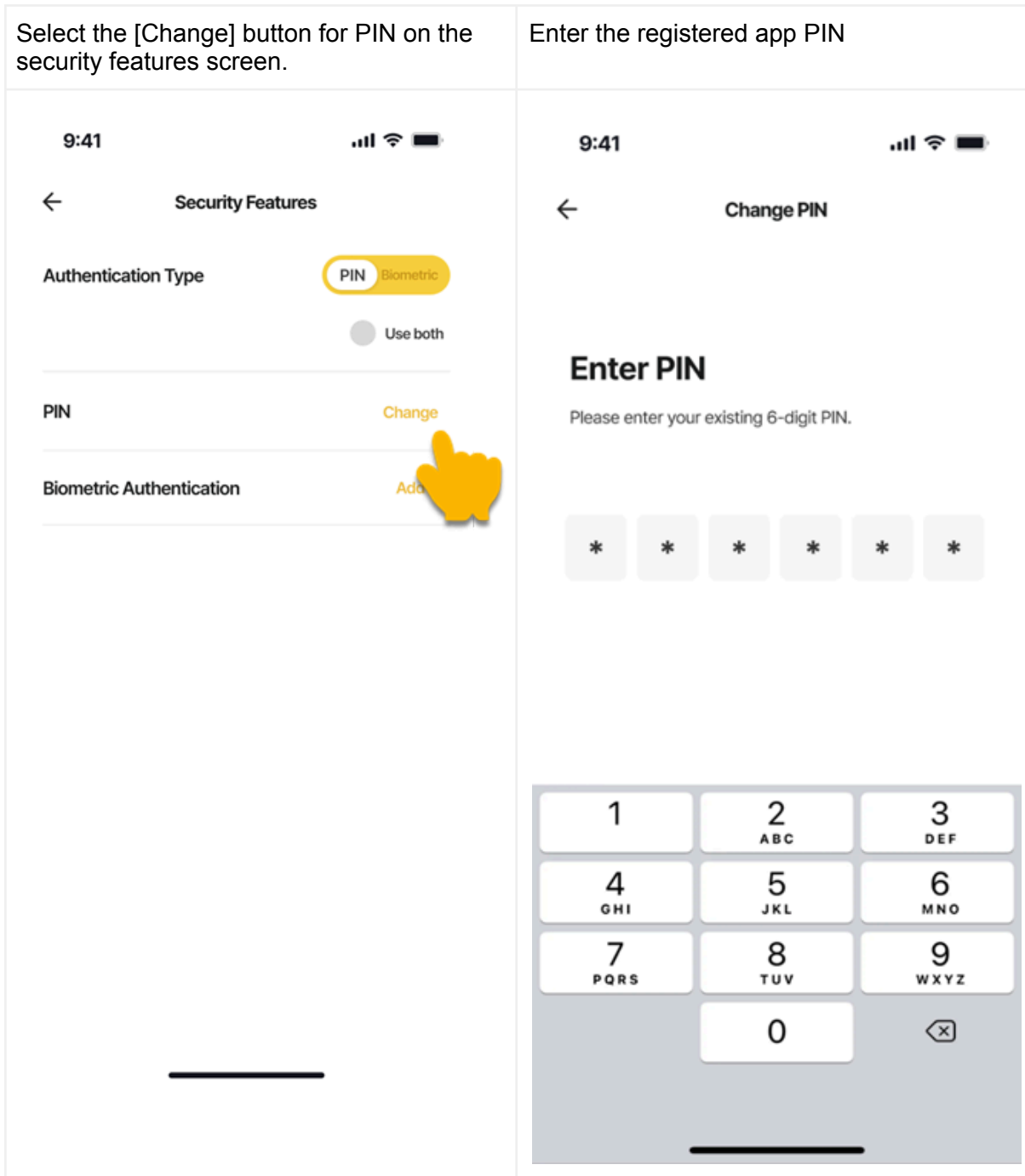
- Click [Delete] > Disable biometric.
- Click [Cancel] > Keep biometric enabled.

Biometric authentication has been deactivated.



Settings – Security Features(Change PIN)

Select the [Change] button for PIN on the security features screen.

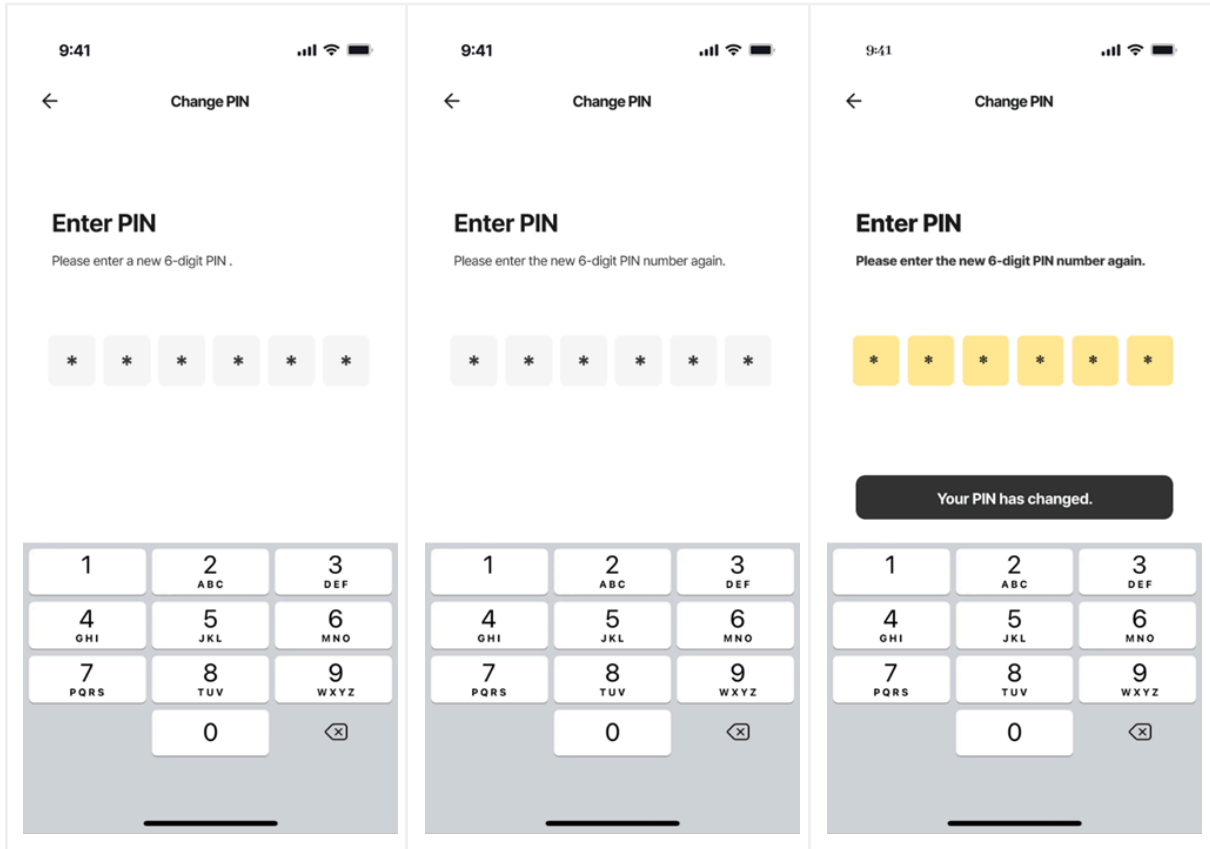


Enter the registered app PIN

Enter a new 6-digit PIN number.

Enter the new 6-digit PIN number again.

PIN change is complete.



Terms of Use

<p>In the settings screen, select [Terms of use].</p>	<p>Clicking on [Terms of Service] will take you to the full-screen agreement. Version information is displayed at the bottom.</p>	<p>You can review the full Terms of Service agreement.</p>
