Banno Digital Platform

device-level authentication for iOS

first vs. subsequent app launch

First App Launch, Existing User Upgrading From 3.31.1 or Earlier

- Instead of the normal lock screen, user sees the Unlock Setup Screen.
- Go to Unlock Setup Screen.

First App Launch, Not Upgrading

- This is the very first launch after downloading the app, so there is no existing profile.
- User proceeds through the normal process to add a profile (login/enrollment/recovery flow).
- At the end of that profile process, before being taken to the dashboard, the user sees the Unlock Setup Screen.
- Go to Unlock Setup Screen.

Subsequent App Launch

- The user has already been obligated to select an unlock method during a previous app session. The lock screen they see now depends upon which unlock method they chose.
  - Selected unlock method: Passcode / biometrics (go to App Lock Screen: Passcode / Biometrics)
  - Selected unlock method: In-app PIN (go to App Lock Screen: In-App PIN)
  - Selected unlock method: Don't lock app (go to App Lock Screen: Automatically Unlocked (Don't Lock App))

A Helpful Reminder to the Reader

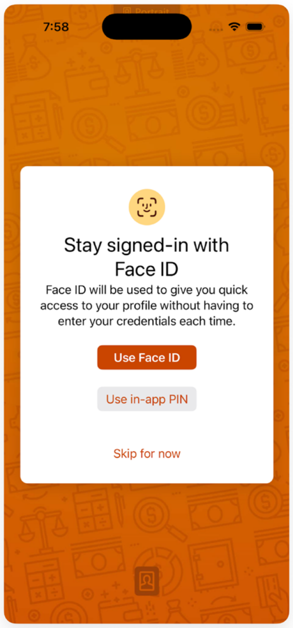
- Don't use "passcode" and "PIN" as synonyms.
  - » **Passcode** in this document specifically refers to a device-level passcode managed by the iOS operating system, which is associated with Touch ID and Face ID when those are in use.
  - » **In-app PIN** or **application PIN** in this document refers to a four-digit PIN managed by the app.

unlock setup screen

General Notes

The user is obligated to select one of the three app unlock options:

1. Device passcode / biometrics
2. In-app PIN
3. Don't use a lock screen ("Skip for now")



Stay signed-in with Face ID

Face ID will be used to give you quick access to your profile without having to enter your credentials each time.

Unlock Setup Screen on a device with Face ID enabled

Device biometrics availability differs from device to device:

- There are two different kinds of biometrics: Touch ID and Face ID.

- The user may have disabled biometrics on the device (or never enabled it in the first place).

Device passcode availability differs from device to device:

- Most users have a device passcode; the iOS operating system strongly encourages users to have one, and make it difficult not to have one without acknowledging several security warnings.
- Some users still do not have a device passcode. If they do not have a device passcode, they cannot enable Touch ID or Face ID.

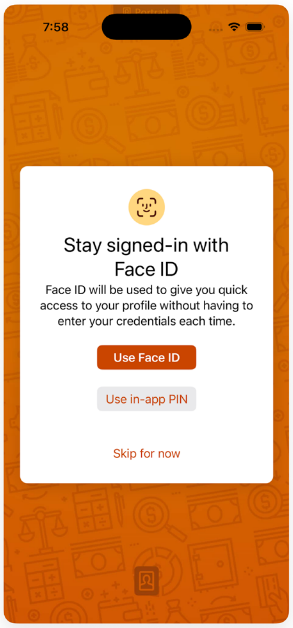
The availability of biometrics and passcode determine which Unlock Setup Screen content the user will see.

The scenarios that follow show different variations of the Unlock Setup Screen.

Sceario 1: User Has a Passcode and Face ID is Enrolled

The user is obligated to select one of the three app unlock options:

1. Face ID / device passcode ("Use Face ID")
2. In-app PIN ("Use in-app PIN")
3. Don't use a lock screen ("Skip for now")



Stay signed-in with Face ID

Face ID will be used to give you quick access to your profile without having to enter your credentials each time.

Unlock Setup Screen on a device with Face ID enabled

Option 1: User taps the "Use Face ID" button

- The user will be prompted by the operating system to authenticate with Face ID (system Face ID dialogs not pictured here).
- After Face ID authentication succeeds, the user's choice to biometrics / passcode is saved by the app and will be used in the future (see App Lock Screen).
- If Face ID authentication fails, the user will remain on the Unlock Setup screen.

Option 2: User taps the "Use in-app PIN" button

- What happens next depends upon whether or not the user is upgrading to this experience from a previous app version where they had selected an in-app PIN using the previous experience.
- If the user is upgrading from an earlier app version where they had provided an in-app PIN for their user profile, see Unlock Setup Screen: Verifying Previous App Pin.
- If the user is **not** upgrading from an earlier app version and so there is no previous app PIN to verify against, see Unlock Setup Screen: Registering New App Pin.

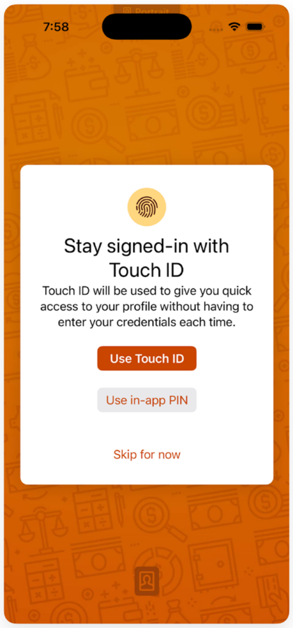
Option 3: User taps the "Skip for now" button

- What happens next depends upon whether or not the user is upgrading to this experience from a previous app version where they had selected an in-app PIN using the previous experience.
- If the user is upgrading from an earlier app version where they had provided an in-app PIN for their user profile, see Unlock Setup Screen: Verifying Previous App PIN.
- If the user is **not** upgrading from an earlier app version and so there is no previous app PIN to verify against, the user's preference to not use a lock screen is saved by the app. The Unlock Setup Screen is dismissed and the user proceeds with normal app use.
- For information about how the app operates when no lock screen is selected, see App Lock Screen: Automatically Unlocked (Don't Lock App) Special Restrictions.

Scenario 2: User Has a Passcode and Touch ID is Enrolled

The user is obligated to select one of the three app unlock options:

1. Touch ID / device passcode ("Use Touch ID")
2. In-app PIN ("Use in-app PIN")
3. Don't use a lock screen ("Skip for now")



7:58

Stay signed-in with Touch ID

Touch ID will be used to give you quick access to your profile without having to enter your credentials each time.

Unlock Setup Screen on a device with Touch ID enabled

Option 1: User taps the "Use Touch ID" button

- The user will be prompted by the operating system to authenticate with Touch ID (system Touch ID dialogs not pictured here).
- After Touch ID authentication succeeds, the user's choice to biometrics / passcode is saved by the app and will be used in the future (see App Lock Screen).
- If Touch ID authentication fails, the user will remain on the Unlock Setup Screen until they make another choice or successfully choose Touch ID.

Option 2: User taps the "Use in-app PIN" button

- What happens next depends upon whether or not the user is upgrading to this experience from a previous app version where they had selected an in-app PIN using the previous experience.
- If the user is upgrading from an earlier app version where they had provided an in-app PIN for their user profile, see Unlock Setup Screen: Verifying Previous App Pin.
- If the user is **not** upgrading from an earlier app version and so there is no previous app PIN to verify against, see Unlock Setup Screen: Registering New App Pin.

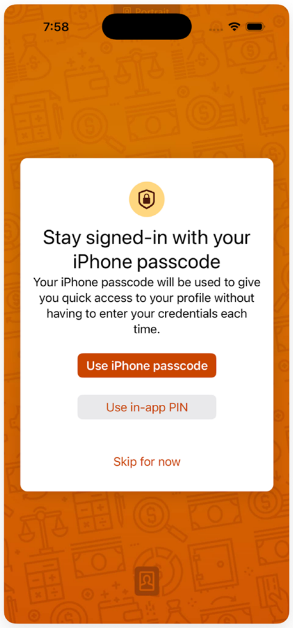
Option 3: Users taps the "Skip for now" button

- What happens next depends upon whether or not the user is upgrading to this experience from a previous app version where they had selected an in-app PIN using the previous experience.
- If the user is upgrading from an earlier app version where they had provided an in-app PIN for their user profile, see Unlock Setup Screen: Verifying Previous App Pin.
- If the user is **not** upgrading from an earlier app version and so there is no previous app PIN to verify against, the user's preference to not use a lock screen is saved by the app. The Unlock Setup Screen is dismissed and the user proceeds with normal app use.
- For information about how the app operates when no lock screen is selected, see App Lock Screen: Automatically Unlocked (Don't Lock App) Special Restrictions.

Scenario 3: User Has a Passcode but Is Not Enrolled in Biometrics

The user is obligated to select one of the three app unlock options:

1. Device passcode ("Use iPhone passcode" or "Use iPad passcode")
2. In-app PIN ("Use in-app PIN")
3. Don't use a lock screen ("Skip for now")



Stay signed-in with your iPhone passcode

Your iPhone passcode will be used to give you quick access to your profile without having to enter your credentials each time.

Unlock Setup Screen on a device where no biometrics are enrolled (no Face ID, no Touch ID) but there is a device passcode

Option 1: User taps the "Use iPhone passcode" or "Use iPad passcode" button

- The user will be prompted by the operating system to authenticate with their device passcode (system passcode dialogs not pictured here).
- After device passcode authentication succeeds, the user's choice to biometrics / passcode is saved by the app and will be used in the future (see App Lock Screen).

  Note: The preference being saved here is "biometrics / passcode," not merely passcode. If the user later enables Touch ID or Face ID on their device, the app will automatically prefer biometrics for future app unlocks, falling back to a device passcode only if the biometric attempt unlock fails.

- If device passcode authentication fails during the Unlock Setup Screen, the user will remain on the Unlock Setup Screen until they make another choice or successfully choose to use a passcode.

Option 2: User taps the "Use in-app PIN" button

- What hapens next depends upon whether or not the user is upgrading to this experience from a previous app version where they had selected an in-app PIN using the previous experience.
- If the user is upgrading from an earlier app version where they had provided an in-app PIN for their user profile, see Unlock Setup Screen: Verifying Previous App PIN.
- If the user is **not** upgrading from an earlier app version and so there is no previous app PIN to verify against, see Unlock Setup Screen: Registering New App PIN.

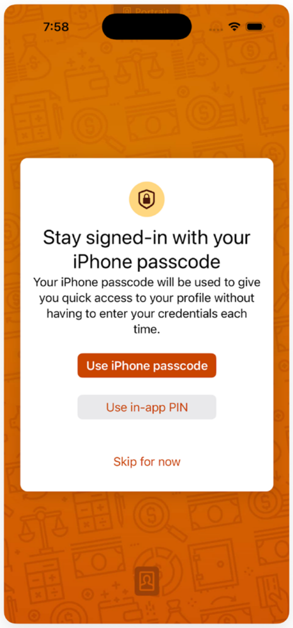
Option 3: User taps the "Skip for now" button

- What happens next depends upon whether or not the user is upgrading to this experience from a previous app version where they had selected an in-app PIN using the previous experience.
- If the user is upgrading from an earlier app version where they had provided an in-app PIN for their user profile, see Unlock Setup Screen: Verifying Previous App PIN.
- If the user is **not** upgrading from an earlier app version and so there is no previous app PIN to verify against, the user's preference to not use a lock screen is saved by the app. The Unlock Setup Screen is dismissed and the user proceeds with normal app use.
- For information about how the app operates when no lock screen is selected, see App Lock Screen: Automatically Unlocked (Don't Lock App) Special Restrictions.

Scenario 4: User Does Not Have a Passcode Set Up and Therefore No Biometrics Are Available Either

The user is obligated to select one of the three app unlock options:

1. Device passcode ("Use iPhone passcode" or "Use iPad passcode")
2. In-app PIN ("Use in-app PIN")
3. Don't use a lock screen ("Skip for now")



Stay signed-in with your iPhone passcode

Your iPhone passcode will be used to give you quick access to your profile without having to enter your credentials each time.

Unlock Setup Screen on a device where there is no device passcode set at all (and therefore no biometrics are available either).

Option 1: User taps the "Use iPhone passcode" or "Use iPad passcode" button

- The button still uses the term "passcode" here because this is the intent of the button, and we strongly encourage all users to set a device passcode on all their devices.
- When the user taps this button, the app will show an alert, letting the user know that they do not have a device passcode set. The alert has only one button "OK" which dismisses the alert and does nothing else; they will remain here on the Unlock Setup Screen.
- If the user wants to use a device passcode option, they will need to navigate to the device passcode section of the system Settings app. This will either be named "Face ID & Passcode" or "Touch ID & Passcode" depending on which of the biometric types are available on the user's device.

Note: It is **strongly** recommended that **all** users have a device passcode on their iPhone or iPad. A device without a device-level passcode is very insecure.

- If the user sets up a device passcode and then returns to the app, the Unlock Setup Screen will update to reflect the availability of a passcode (Stay signed-in with your iPhone/iPad passcode).

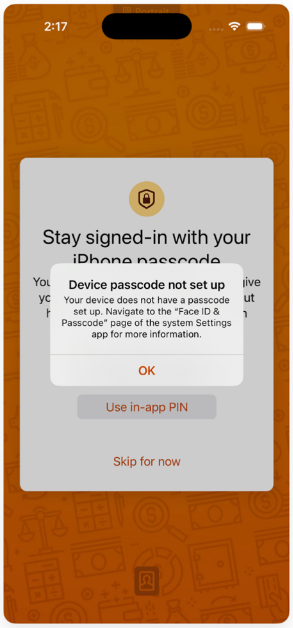
Option 2: User taps the "Use in-app PIN" button

- What happens next depends upon whether or not the user is upgrading to this experience from a previous app version where they had selected an in-app PIN using the previous experience.
- If the user is upgrading from an earlier app version where they had provided an in-app PIN for their user profile, see Unlock Setup Screen: Verifying Previous App PIN.
- If the user is **not** upgrading from an earlier app version and so there is no previous app PIN to verify against, see Unlock Setup Screen: Registering New App PIN.

Option 3: User taps the "Skip for now" button

- What happens next depends upon whether or not the user is upgrading to this experience from a previous app version where they had selected an in-app PIN using the previous experience.
- If the user is upgrading from an earlier app version where they had provided an in-app PIN for their user profile, see Unlock Setup Screen: Verifying Previous App PIN.
- If the user is **not** upgrading from an earlier app version and so there is no previous app PIN to verify against, the user's preference to not use a lock screen is saved by the app. The Unlock Setup Screen is dismissed and the user proceeds with normal app use.
- For information about how the app operates when no lock screen is selected, see App Lock Screen: Automatically Unlocked (Don't Lock App) Special Restrictions.

The following alerts are shown after the user taps (option 1) "Use iPhone/iPad passcode" on a device that does not have a passcode set.

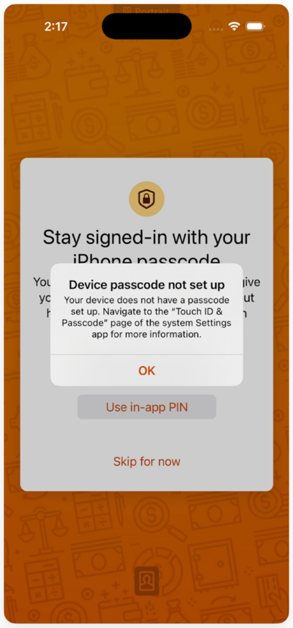


2:17

Stay signed-in with your iPhone passcode

Device passcode not set up

Your device does not have a passcode set up. Navigate to the "Face ID & Passcode" page of the system Settings app for more information.



2:17

Stay signed-in with your iPhone passcode

Device passcode not set up

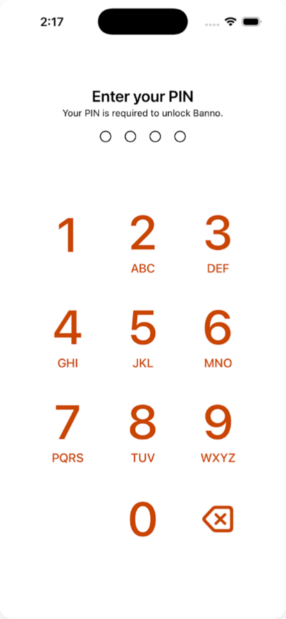
Your device does not have a passcode set up. Navigate to the "Touch ID & Passcode" page of the system Settings app for more information.

Alert with instructions on where to find the Face ID & Passcode settigns in the system Settings app.

Alert with instructions on where to find the Touch ID & Passcode settings in the system Settings app.

Scenario 5: Verifying Previous App PIN

This screen requires the user to verify their previous in-app PIN from an earlier version of the app.



2:17

Enter your PIN

Your PIN is required to unlock Banno.

○ ○ ○ ○

Unlock Setup Screen after the user taps "Use in-app PIN" on a device that had a previous in-app PIN from version 3.31.1 or earlier.

This screen is reached if the following criteria are met:

- The user has just upgraded to version 3.31.2 or later from app version 3.31.1 or earlier.
- The app has one or more user profiles on it already.
- This is the first time the user is launching the upgraded app version and therefore has only just now been asked to select an app unlock method.
- From the Unlock Setup Screen, the user tapped on either "Use in-app PIN" or "Skip for now."

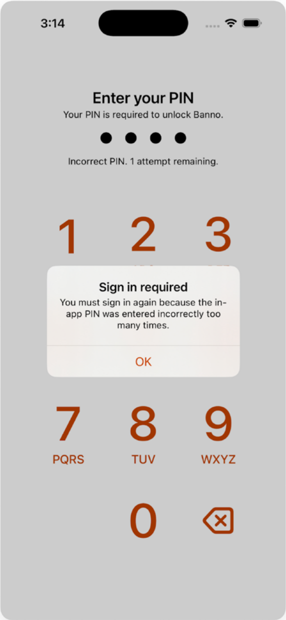
Expected interaction:

- The user has to enter their existing PIN that they created with app version 3.31.1 or earlier.
- They have up to five attempts to enter this PIN.
- If they enter it incorrectly five times, they will see an alert that they will have to sign in again on this device.
- If they enter the PIN correctly, the Unlock Setup Screen is dismissed and the app will proceed normally.

Successful outcome:

After entering the correct PIN, the user's selected app unlock settings will be saved. If they tapped "Use in-app PIN" their existing PIN will continue to be used. If they tapped "Skip for now" the app will not require an unlock method in the future.

The user will see the following alert after entering the wrong in-app PIN five times.



Enter your PIN

Your PIN is required to unlock Banno.

●●●●

Incorrect PIN. 1 attempt remaining.

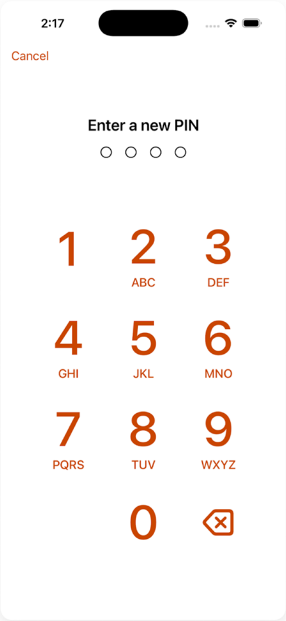
Sign in required

You must sign in again because the in-app PIN was entered incorrectly too many times.

Unlock Setup Screen after the user taps "Use in-app PIN" on a device that had a previous in-app PIN from version 3.31.1 or earlier, but the user fails to verify the correct PIN after five times.

Scenario 6: Registering a New App PIN

This screen allows the user to enter a new app PIN.



Enter a new PIN

○○○○

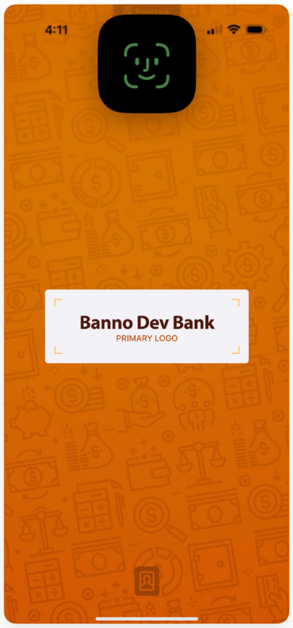
The user enters a new in-app PIN using this screen.

- The user chooses a new PIN.
- They enter it two times in a row.
- If they don't enter it correctly two times in a row, they will have to start over and repeat this process until they do.
- After repeating the new PIN twice in a row, the PIN is saved and this screen is dismissed, and the app proceeds normally.
- At any time the user can press a "Cancel" button dismiss this PIN pad and return to the previous screen that brought them here.

app lock screen

Passcode / Biometrics

This lock screen is used when the user has selected device passcode / biometrics as their preferred unlock method.

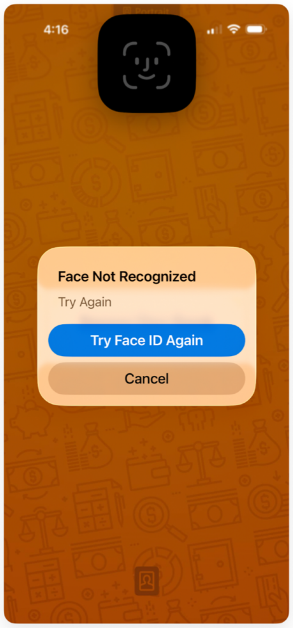


The App Lock Screen when Face ID is enrolled.

There are three ways the screen can be unlocked:

- **Face ID:** If the device uses Face ID and it is enrolled, this will trigger first, falling back to a device passcode UI only if it fails (see description below).

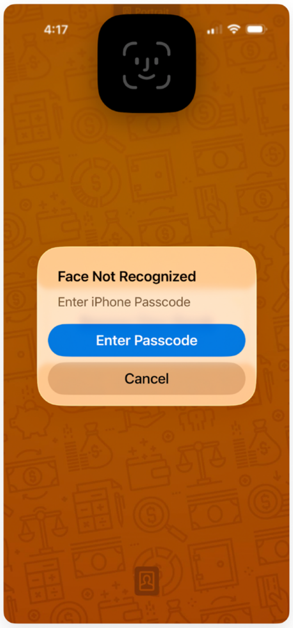
- **Touch ID:** If the device uses Touch ID and it is enrolled, this will trigger first, falling back to a device passcode UI only if it fails (see description below).
- **Device passcode:** If the device uses either Face ID or Touch ID, the passcode entry UI will not appear until Face ID / Touch ID fail twice and the user is given the option to try a device passcode. If the device does not have either Face ID or Touch ID (or they are not enrolled), then device passcode will be the first and only option that appears.



Face Not Recognized

Try Again

The system Face ID alert that appears when Face ID fails the first attempt.



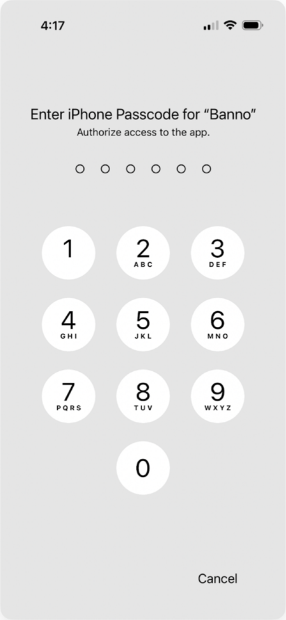
Face Not Recognized

Enter iPhone Passcode

The system Face ID alert that appears when Face ID fails twice in a row.

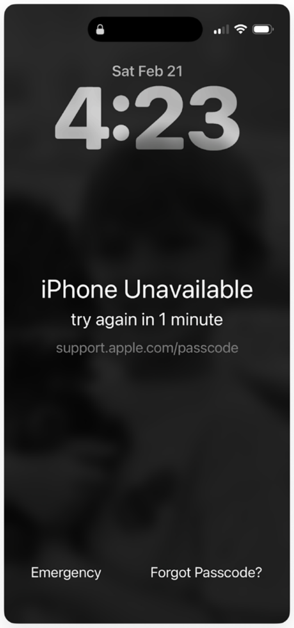
If the user fails to pass biometric scans, and also fails to enter their device passcode correctly, the operating system will start imposing timed lock-outs of exponentially increasing length, starting with one minute. For more information, consult Apple's public documentation.

Screenshots for Touch ID are not pictured here, but it follows the same overall flow as the Face ID experience, with the experience being that a fingerprint sensor UI is shown instead of a Face ID scanning interface.



Enter iPhone Passcode for "Banno"
Authorize access to the app.

The system device passcode entry screen.

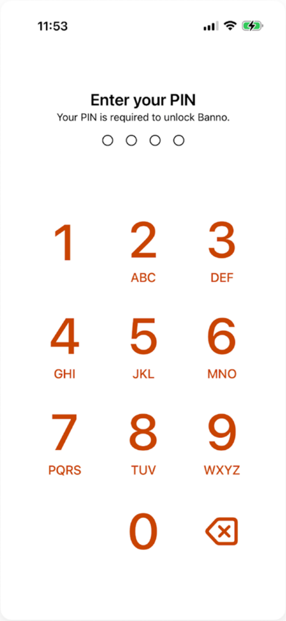


iPhone Unavailable
try again in 1 minute
support.apple.com/passcode

The device will eventually become locked for increasingly longer time-outs if the user enters the passcode incorrectly too many times.

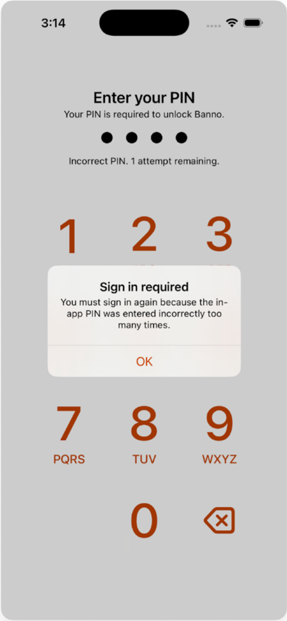
In-App PIN

This lock screen is used when the user has selected an in-app PIN as their preferred unlock method.



Enter your PIN
Your PIN is required to unlock Banno.

The App Lock Screen that appears when the user has opted to use an in-app PIN as their unlock method.



Enter your PIN
Your PIN is required to unlock Banno.

Incorrect PIN. 1 attempt remaining.

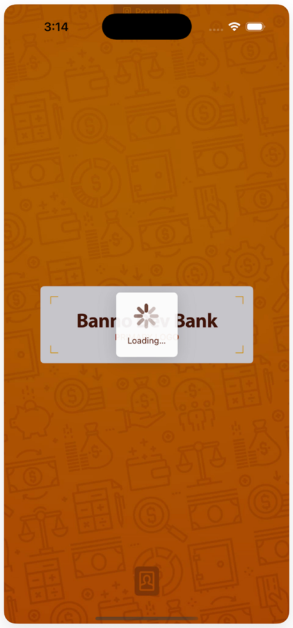
Sign in required
You must sign in again because the in-app PIN was entered incorrectly too many times.

An alert appears after the fifth consecutive failed PIN attempt.

- The user has up to five tries to enter the correct PIN.
- After the fifth failure, the user will be shown an alert indicating that they will be signed out and must sign in again.
- The number of PIN attempts is tracked consecutively; force-quitting the app will not reset the attempt count.
- If the user enters the PIN correctly, the tracked number of failed attempts is reset to zero, the lock screen is dismissed, and the app proceeds normally.

Automatically Unlocked (Don't Lock App)

This placeholder lock screen is used when the user has selected not to require an unlock method. When the app is launched or brought to the foreground, the user will briefly see this placeholder lock screen. It will be automatically dismissed without the user having to take any action.



The placeholder lock screen briefly during app launch.

Automatically Unlocked (Don't Lock App) Special Restrictions

When the user opts out of using a lock/unlock method, there are some special restrictions that apply.

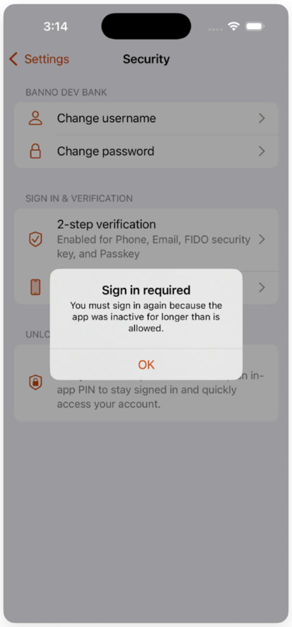
Inactivity time-out:

- If the user leaves the app, and the operating system keeps it suspended (does not terminate it), the user has five minutes to return to the app and continue using it.

- If they return to the app after five minutes (and the operating system kept it suspended), the user will see an alert indicating that they have to be signed out and must sign back in again.

Cold launch always requires a sign-in:

- If the app is launching "cold" (i.e. either the phone was rebooted, or the operating system terminated the app while it was in the background in order to free up memory for other active apps), then the user must sign in again.



3:14

Settings — Security

BANNO DEV BANK

Change username

Change password

SIGN IN & VERIFICATION

2-step verification
Enabled for Phone, Email, FIDO security key, and Passkey

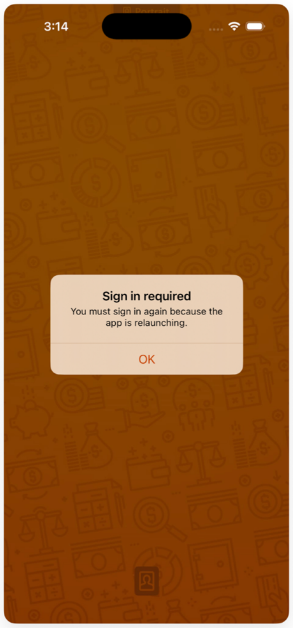
UNLC

n in-app PIN to stay signed in and quickly access your account.

Sign in required

You must sign in again because the app was inactive for longer than is allowed.

OK



3:14

Sign in required

You must sign in again because the app is relaunching.

OK

The alert shown when the user returns to the app after it has been suspended (but not terminated) for more than five minutes, and the user has opted out of using an app lock method like passcode, biometrics, or an in-app PIN.

The alert shown when the user launches the app "cold" (e.g. after a device reboot) and the user has opted out of using an app lock method like passcode, biometrics, or an in-app PIN.

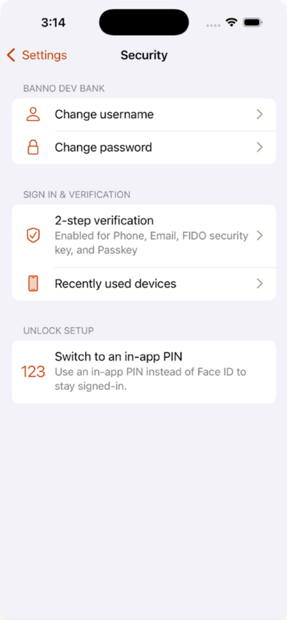
security settings

Current Unlock Method: Passcode / Biometrics

On the Security page of the in-app settings screen, the user can find options to adjust their preferred app unlock method under the "Unlock Setup" section.

- If the user's current method is passcode / biometrics, they will see a button titled "Switch to an in-app PIN."

- Pressing this button will show an alert indicating that, in order to make this change, they will first have to sign out and then back in again, clearing all app data.



3:14

< Settings Security

BANNO DEV BANK

Change username >

Change password >

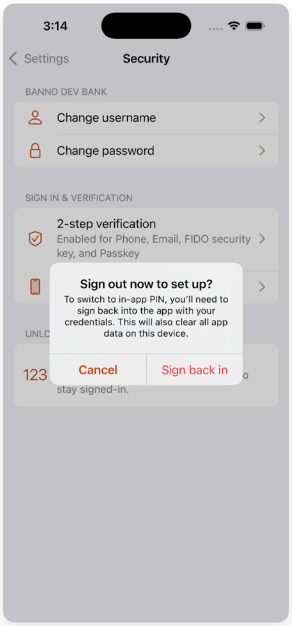
SIGN IN & VERIFICATION

2-step verification
Enabled for Phone, Email, FIDO security key, and Passkey >

Recently used devices >

UNLOCK SETUP

123 Switch to an in-app PIN
Use an in-app PIN instead of Face ID to stay signed-in.



3:14

< Settings Security

BANNO DEV BANK

Change username >

Change password >

SIGN IN & VERIFICATION

2-step verification
Enabled for Phone, Email, FIDO security key, and Passkey >

Sign out now to set up?

To switch to in-app PIN, you'll need to sign back into the app with your credentials. This will also clear all app data on this device.

Cancel | Sign back in

Security settings page when the current unlock method is passcode / biometries (in this example it's Face ID).

The alert shown when the user taps "Switch to an in-app PIN."

Current Unlock Method: In-App PIN

On the Security page of the in-app settings screen, the user can find options to adjust their preferred app unlock method under the "Unlock Setup" section.

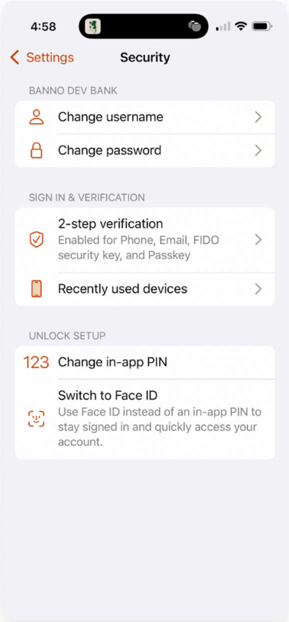
- If the user's current method is an in-app PIN, they will see two buttons:

1. Change in-app PIN

- This button shows a PIN pad screen that asks them first to confirm their existing PIN, then asks them to change their PIN.
- If they fail to enter their PIN five times in a row, they will be forced to be signed out.
- This PIN pad is the same one seen during Unlock Setup and App Unlock.

2. Switch to passcode / biometrics

- The button title depends upon what is available: "Switch to Face ID" or "Switch to Touch ID" or "Switch to iPhone passcode" etc.
- Pressing this button will immediately trigger a system UI for local authentication (Face ID scan, Touch ID fingerprint scan, or device passcode, whichever is available). Upon a successful authentication, the user's preference will be updated to use passcode / biometrics for the app's lock screen going forward.



4:58

Settings Security

BANNO DEV BANK

Change username

Change password

SIGN IN & VERIFICATION

2-step verification
Enabled for Phone, Email, FIDO security key, and Passkey

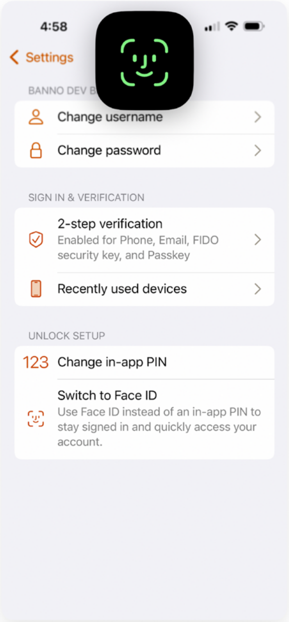
Recently used devices

UNLOCK SETUP

123 Change in-app PIN

Switch to Face ID
Use Face ID instead of an in-app PIN to stay signed in and quickly access your account.

Security settings page when the current unlock method is an in-app PIN.



4:58

Settings

BANNO DEV B

Change username

Change password

SIGN IN & VERIFICATION

2-step verification
Enabled for Phone, Email, FIDO security key, and Passkey

Recently used devices

UNLOCK SETUP

123 Change in-app PIN

Switch to Face ID
Use Face ID instead of an in-app PIN to stay signed in and quickly access your account.

Biometric scanning starts when the user presses the button to switch to passcode / biometrics instead of an in-app PIN.

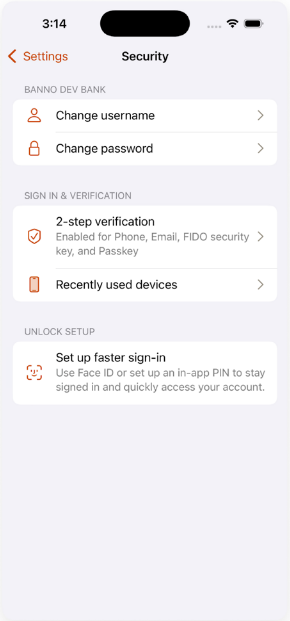
Current Unlock Method: Don't Lock App

On the Security page of the in-app settings screen, the user can find options to adjust their preferred app unlock method under the "Unlock Setup" section.

- If the user's current method is to not use a lock screen at all, they will see one button:

Set up faster sign-in

- This button shows the user the familiar Unlock Setup Screen described elsewhere in this document.



BANNO DEV BANK

Change username

Change password

SIGN IN & VERIFICATION

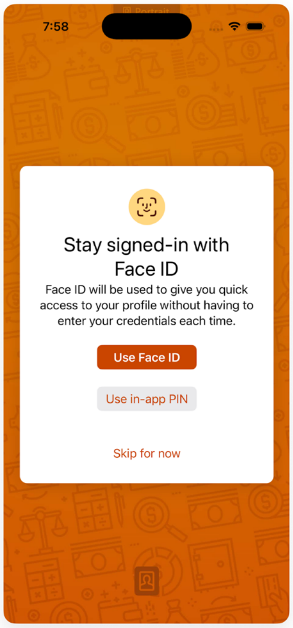
2-step verification
Enabled for Phone, Email, FIDO security key, and Passkey

Recently used devices

UNLOCK SETUP

Set up faster sign-in
Use Face ID or set up an in-app PIN to stay signed in and quickly access your account.

Security settings page when the current unlock method is to not lock the app at all.



Stay signed-in with Face ID

Face ID will be used to give you quick access to your profile without having to enter your credentials each time.

Pressing "Set up faster sign-in" will show the Unlock Setup Screen.