# NoahFace

# Facial Recognition Setup Guide

Version 13.0.0

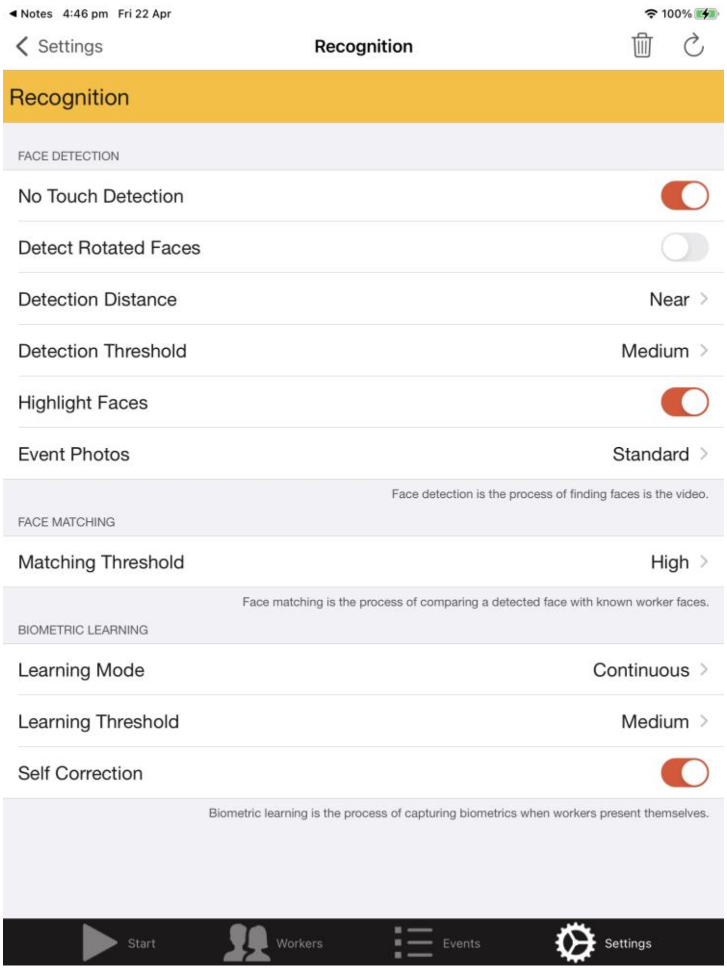
# Introduction

This document is intended to assist with the optimal setup of facial recognition in NoahFace. Reading this document will help you understand how to:

- Configure facial recognition.
- Configure liveness testing.
- Minimise the chances of incorrect matches.
- Resolve issues with detection and recognition.

# Recognition Settings

Under Settings / Facial Recognition you will see the following settings:




Each of these individual settings is explained below.

## No Touch Detection

With this setting turned on, NoahFace constantly scans for faces, and if it sees one, it will attempt to recognise it (ie: compare it with all its known faces). If you turn this setting off, you must first touch the screen before NoahFace will scan for faces.

The default is on. You should consider turning this setting off only if you are mounting NoahFace in a busy thoroughfare, and you don't want it recognising faces that are passing by.

## Detect Rotated Faces

With this setting turned on, NoahFace will recognise faces at up to a 30 degree angle. With this setting tuned off, NoahFace will only recognise faces that are directly facing the iPad screen.

The default is off, which minimises the chances of an incorrect recognition (aka 'false positive'). You should consider turning this setting on if people cannot easily directly face the iPad screen due to its mounting location.

## Detection Threshold

The detection threshold controls the process of finding faces in the video. If it is set to Very Low, if something in the image looks like it could be a face, it starts analysing it.
If it is set to Very High, it needs to be extremely clear that it looks like a face before it will start analysing it.

The default is Medium, which should work well in almost all cases.

You should consider changing this to Low if:

- You have poor lighting conditions.
- You have people with extremely dark skin or thick glasses that you are having trouble detecting.

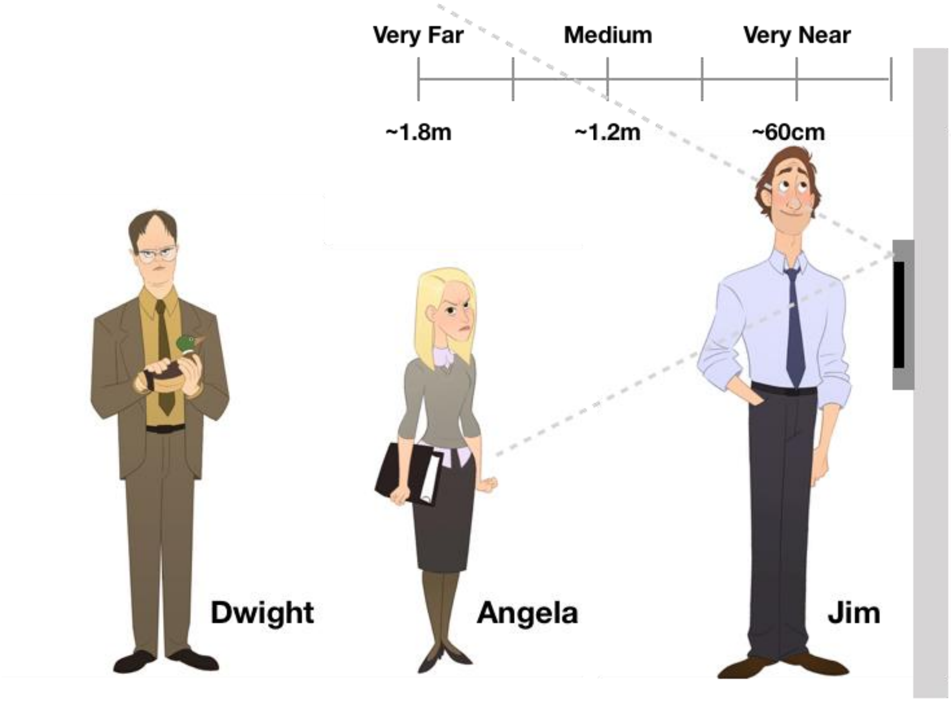
You generally should not change this setting to Very Low – if you find you need this setting at Very Low to detect anyone, you should instead consider adjusting the camera brightness, physical shading, or installing front lighting.

You should consider changing this to High, Very High, or Maximum if:

- You want to take every measure possible to minimise the chances of an incorrect recognition (aka 'false positive').

## Detection Distance

This setting controls the distance at which the NoahFace App will recognise faces. As per the diagram below, this ranges from 'Very Near', which requires you to stand approximately 60cm from the iPad, to 'Very Far', which will detect faces as far away as 1.8 metres.




The default is Near, which will detect faces at approximately 90 cm.

You should consider changing this to Very Near if:

- Your solution requires users to press buttons (eg: for Time and Attendance).
- You are mounting your iPad in a busy thoroughfare, and you don't want it recognising faces that are passing by.
- You want to take every measure possible to minimise the chances of an incorrect recognition (aka 'false positive').

You should note that if you set this to Very Near and your iPad is mounted vertically, it may be difficult for extremely tall or extremely short people to get their faces in camera view.

You should consider changing this to Far or Very Far if:

- You have a door at the end of a long approach, and you want to maximise the chances of the person being recognised before they reach the door.
- You have people who are in wheelchairs.

## Highlight Faces

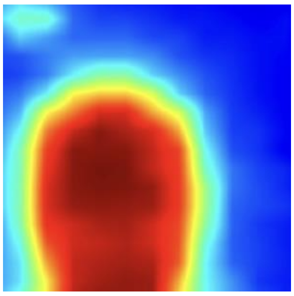
With this setting turned on, NoahFace will draw a box around faces on the video screen.

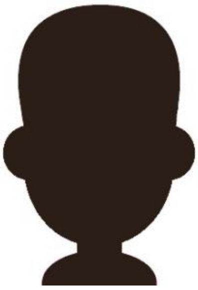
## Event Photos

An image of the user's face is automatically clipped and stored with each event.
The options available are as follows:


Standard


Large

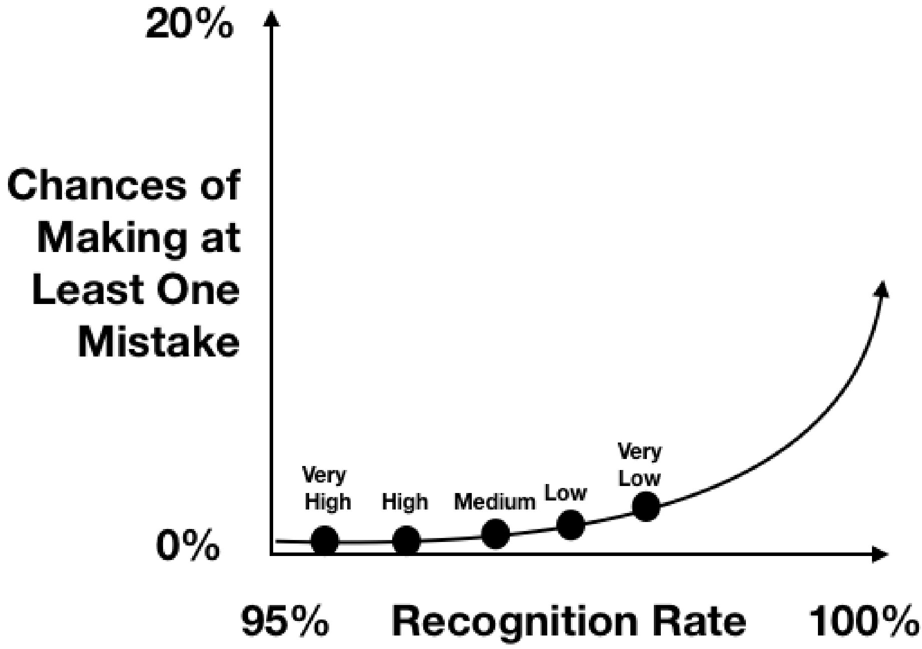

Thermal


None

## Matching Threshold

Once a face is detected, NoahFace compares the face with all the faces of known individuals. This setting controls how confident the software needs to be that a particular face is a known individual before declaring it a match.

When most people hear about this threshold, their immediate response is that they want it set for absolute certainty. Unfortunately, this is not possible: there is a direct tradeoff between recognition rates and the chances of making a mistake. You should instead think of the Matching Threshold using a graph such as the following:




Note that this is no different from human recognition of faces. If you were to look at 1000 images containing faces of people you knew, and had to always declare who each image was, there would be some images where you could not be absolutely certain (eg: because the images were blurry or the person had their face turned to the side), and you could make mistakes. If you are allowed to pass on 20 images, the chances of you making a mistake are less than if you are only allowed to pass on 1 image. The only way to **guarantee** you never make a mistake is to pass on all images (which means you will achieve a 0% recognition rate).

The default setting of Medium is an extremely strong setting, and provides the right balance between excellent recognition and minimal chances of making a mistake in the vast majority of environments.

You should consider changing this to High, Very High, or Maximum if:

- You want to take every measure possible to minimise the chances of an incorrect recognition (aka 'false positive'), and you are happy to live with a lower recognition rate.

## Biometric Learning

Biometric learning is the process of capturing and saving multiple sets of biometrics for the same person. These might be extracted at different distances, different angles, or in different lighting conditions, allowing NoahFace can achieve better recognition results.

NoahFace has three different biometric learning modes as follows:

1. **Registration.** In this mode, biometric learning only happens during the registration process, when people manually identify themselves.
2. **Limited**. In this mode, biometric learning happens automatically each time a person uses NoahFace for up to 10 days after they register.
3. **Continuous**. In this mode, biometric learning happens automatically each time a person uses NoahFace. This is the default.

You should consider changing the Learning Mode to Registration or Limited if:

- You want to take every measure possible to minimise the chances of an incorrect recognition (aka 'false positive'), and you are happy to live with a lower recognition rate.

NoahFace also allows you to change the Learning Threshold, which is how certain it needs to be that a face belongs to a known person before additional biometrics are captured. The default is Medium.

You should consider changing the Learning Threshold to High, Very High, or Maximum if:

- You want to take every measure possible to minimise the chances of an incorrect recognition (aka 'false positive'), and you are happy to live with a lower recognition rate.

## Self Correction

Once a match is determined, the NoahFace App will display the appropriate action screen – for example a Clock In/Out screen. If an individual has been incorrectly matched, they can press the 'Not Me' button so that the biometrics for the matched user are corrected. If you want to hide the 'Not Me' button, you can turn off this switch.

# Liveness Detection

The aim of liveness detection is to differentiate real people from photographs and videos. It is used to avoid fraud / spoofing attempts. NoahFace has three liveness testing algorithms built-in, which can be used independently or together by turning on the appropriate switches on the Settings/Facial Recognition page. Each of these algorithms is explained below:

### Movement Analysis

This algorithm attempts to analyse the movement in the image (frame to frame) to determine if the face is a real face or not. The edges of the face are particularly important to this algorithm, which makes it sensitive to the background. It works exceptionally well if the camera is facing a blank white wall. However, it can be problematic if it is facing a complex background, such as a window, shelving, or even a picture on the wall.

### Constant Background

This algorithm compares the background surrounding a face with the background of the video feed when there are no faces present. If the it differs significantly, then it assumes that someone is attempting to fool the recognition process with a photograph. This test is not at all sensitive to the complexity of the background, <u>as long as it is static</u>. However, this test will ONLY work if:

- You have the iPad mounted on the wall so it cannot move.
- You have consistent lighting and you are using a fixed shutter speed.
- You do NOT have people, cars, or anything else constantly moving in the background.

### Depth Analysis

This algorithm examines the depth of a face at various points to ensure it is three-dimensional. This algorithm relies on the availability of a *TrueDepth* camera, which is currently only available on an iPad Pro 2018 model or later. The *TrueDepth* camera can only accurately determine depth at up to 1.2 meters, so faces further away than this will not be recognised regardless of the Detection Distance and Zoom settings.

If detecting fraud is critical to your application, we strongly recommend considering purchasing an iPad Pro and using the Depth Analysis liveness test.

## Liveness Testing Operation

When NoahFace believes it has detected fraud (ie: not a real person), the recognition process will pause for the configured Lock Time. If this happens you will see that the Enter button on the Welcome screen remains disabled, and the screen will flash red if you have Visual Feedback enabled.


Setting the Lock Time too low can compromise the liveness testing, so we recommend not setting it lower than 3 seconds, which is the default.

## Preparing your Environment

If you plan to use Liveness Testing, please consider:

1. The liveness testing algorithms will **NOT** work reliably if your iPad is not mounted.

2. If you are using the Movement Analysis or Constant Background algorithms, the location you mount your iPad is very important. You will get the best results if your iPad camera is facing a blank wall, and you may get poor results if your iPad camera is facing a complex background (eg: a doorway, a bookcase, or a picture on the wall).

3. When you start the NoahFace App, you **MUST** wait for the message "Preparing liveness detection…" to disappear before it is used. If you do not wait for this message to disappear, then the liveness testing algorithms will **NOT** work reliably.

4. If detecting fraud is critical to your application, we strongly recommend considering purchasing an iPad Pro and using the Depth Analysis liveness test. This is the strongest form of liveness testing – that is, it will detect the most cases.

## Facial Recognition vs. Access Cards

If you are concerned about facial recognition being circumvented using photographs, you should consider the alternative, which is generally access cards. Both technologies provide a simple barrier to access so that only people who should have access get access, and also help you record who has accessed a door and to examine this later by viewing an audit trail.

But neither technology is perfect: access cards are particularly problematic because they can be:

- Lent to friends.
- ‘Borrowed’ from desks.
- Permanently lost or stolen.
- Easily and cheaply duplicated.

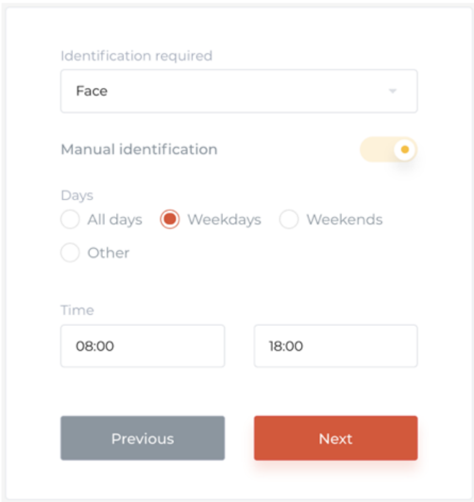
In short, access cards tell you absolutely nothing about who gained access.

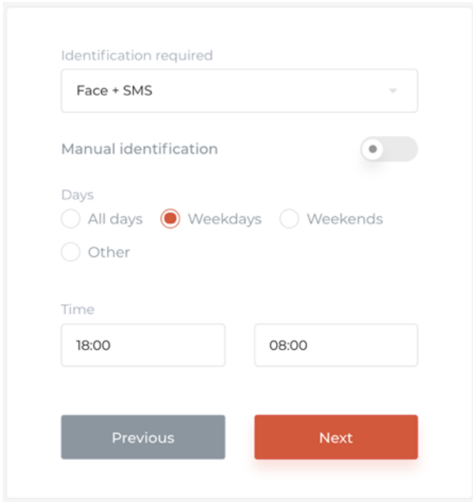
## Access Rules

If you are concerned about facial recognition being circumvented using photographs, you should consider carefully what access rules you have in place.

If you are using NoahFace integrated with an existing access control system, you might choose to use facial recognition for identification only during office hours, and to rely on an alternative identification technology at night and on weekends.

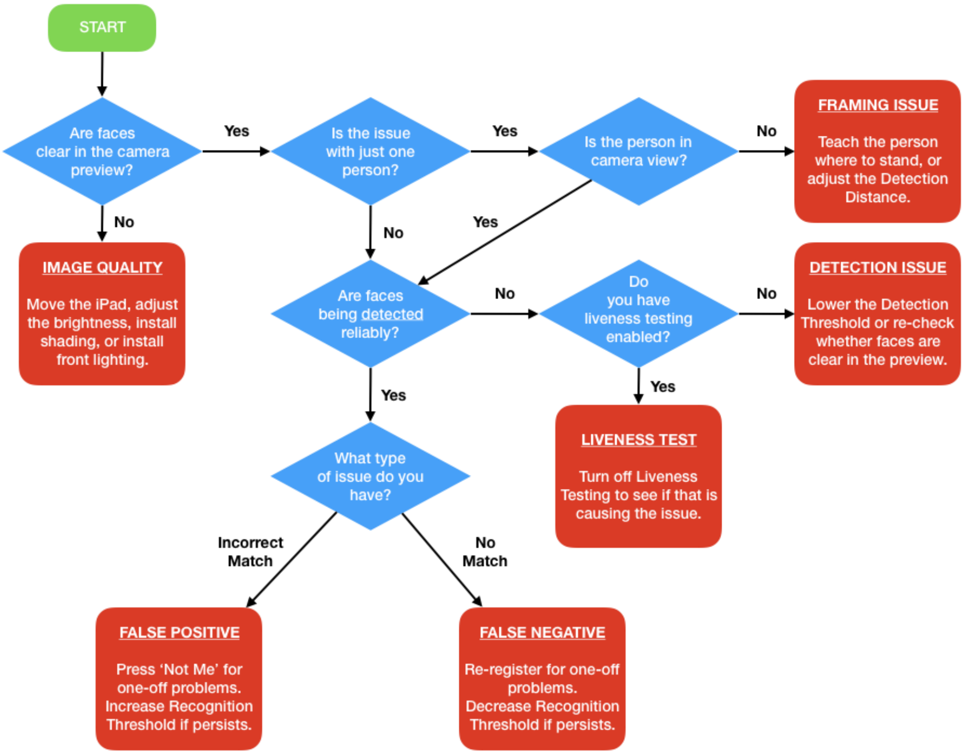
If you are using NoahFace stand-alone, you might consider time of day rules and/or increasing security using two-factor authentication. For example, you might allow access using facial recognition only during office hours, but require the use of facial recognition plus an SMS code outside of these hours. This could be achieved by setting up two rules which are identical except for the identification and timing requirements, as shown below:





# Appendix A: Problem Solving

If you have an issue with facial recognition, use the following flow chart to identify the type of issue you are facing, and what to do about it:




## Are Faces Being Detected Reliably?

To answer the question 'Are faces being detected reliably?', you need to touch the home screen so that the Welcome screen displays. There is a small red progress bar at the top of the video. If this bar quickly progresses from left to right, and the Enter button is enabled, then a face has been detected. If this red bar does not progress, and the Enter button remains disabled, then a face has not been detected.

If you are having issues with an individual, you should ask that individual to stand in front of the iPad and touch the home screen so that the Welcome screen is displayed. If you stand to the side, you will be able to see whether their face is being detected or not by watching the red progress bar and Enter button. Repeat that process a few times, and you should have a good understanding as to what is happening.

## Liveness Testing – Real People Being Detected as Fraud

To verify whether you have a Liveness Testing issue, turn the Visual Feedback switch on. The welcome screen will then flash red when NoahFace believes it has detected fraud. If you determine you definitely have a Liveness Testing issue (ie: you are regularly seeing the screen flash red when real people present themselves), you should consider the following:

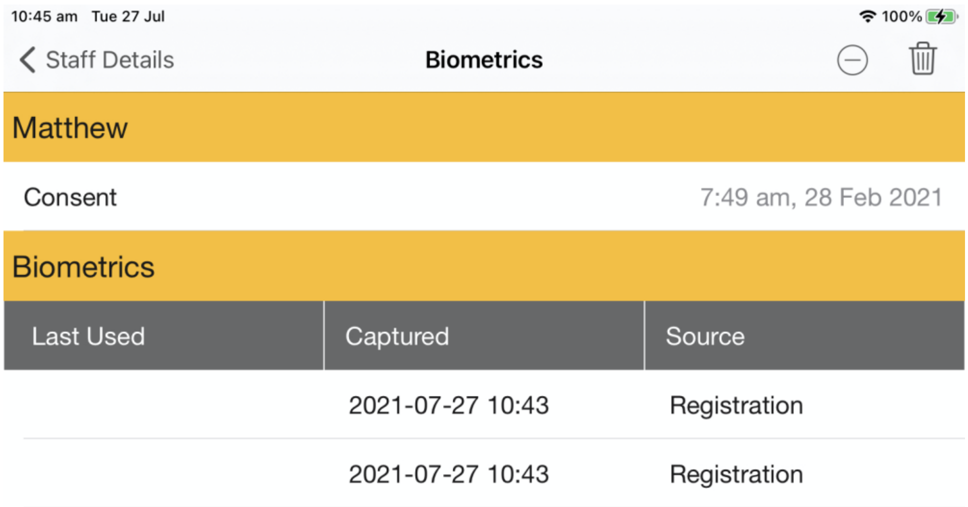
- Firstly, if you have multiple liveness testing algorithms enabled, you should try each algorithm one by one to see which one is causing your issues.
- Is it possible to move anything in the video background (eg: shelving, a picture on the wall, etc)?
- Is it possible to move the iPad to another location with a different background?
- For Access Control solutions, is it possible to angle the iPad slightly (ie: so the left or right vertical edge is further from the wall than the opposite edge). This often changes the camera view sufficiently so that a door frame or window is no longer in view.
- For solutions such as Time and Attendance, is it possible to mount the iPad lower and angle it towards the ceiling (at up to 45 degrees)? This often changes the camera view sufficiently so that a picture, shelving, or a window is no longer in view.
- Is it possible to zoom the image slightly so that a door frame or window is no longer in the video? Note that zooming the video will slow down the recognition process significantly, so this should be done only as a last resort.

Generally, one of the above approaches will work, and will allow you to use liveness testing in almost all environments. However, if you have exhausted all options with both the Movement Analysis and Constant Background algorithms, you should consider the Depth Analysis algorithm. This algorithm is not sensitive to the background at all, and will work well in almost all environments.

## Liveness Testing – Fraud not Detected

If someone has conducted fraud (eg: presented a selfie of someone else which has been recognised as a real person), and you want to try to prevent this happening in the future, you should do the following:

1. Open up the person's user details (in the NoahFace App), and press the right-most toolbar button to view their biometrics. Remove their consent (press the "-" icon) which will cause their biometrics to be deleted from all iPads that are currently active.




It may take up to 5 minutes for the deletions to replicate to other iPads. If you are using Cloud based biometric storage, you should wait for this to complete before proceeding.

2. Ensure the iPad is properly mounted. The liveness testing algorithms will <u>**NOT**</u> work reliably unless the iPad is properly mounted in a fixed location.

3. Re-Read the section on Liveness Detection, and review and adjust your Liveness Testing settings as appropriate.

4. Re-Read the section on Biometric Learning, and consider setting this to ***Registration***. In this mode learning will only take place during the registration process, and certain registration methods (eg: List+Admin) require that a supervisor is present (when fraud is generally easy to prevent). Under most circumstances we recommend leaving this setting at its default of ***Continuous*** (as this results in much more reliable recognition), this is a trade-off you can consider if fraud detection is critical to your application.

5. When you re-start the App, step to the side and wait for the message "Preparing liveness testing…." to disappear. If you start using the App before this message disappears, the liveness testing algorithms will **NOT** work.

6. You are now ready to re-register staff.

Note that the basic Liveness Testing algorithms (eg: Movement Analysis) will detect many, **but not all**, attempts at fraud. If fraud detection is absolutely critical in your environment, we strongly recommend considering purchasing an iPad Pro and using the Depth Analysis liveness test. This is by far the strongest fraud detection algorithm.
You should also consider other, non-technology based, measures – eg: surveillance cameras, employment contract terms, etc. These play a critical role in preventing fraud.

## Detection Issues (False Negatives)

Detection issues can occur on individuals that are extremely tall or short. In such cases, your only real options are:

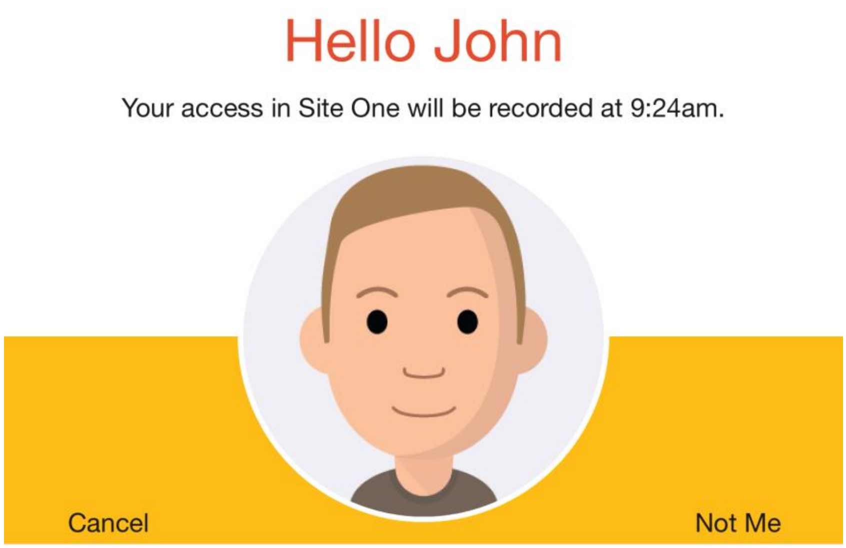
- Increase the Detection Distance setting.
- Make these individuals aware they are out of frame, so they crouch or stand on their toes as needed.
- Ask these individuals to stand further from the iPad.

Detection issues can also occur on people with extremely dark skin (particularly if lighting is poor) or with extremely thick glasses. In such cases, your options are:

- Increase the Brightness/ISO setting (and re-testing with people with fair skin).
- Decrease the Detection Threshold setting (to Low or Very Low).
- Ask an individual to take of their glasses to be recognised.
- Improve the image quality by adding shading or lighting.

## Incorrect Matches (False Positives)

If an individual experiences an incorrect match, it is intended that they should press the 'Not Me' button. This will automatically unlearn the association between their user record and the biometric (or biometrics) that caused the incorrect match.




If users do not press the 'Not Me' button, and instead complete a transaction (such as clocking in) as the wrong user, their biometrics will be recorded against the matched user.

See: 'Appendix B: What do I do if I have an incorrect match?' for more information.

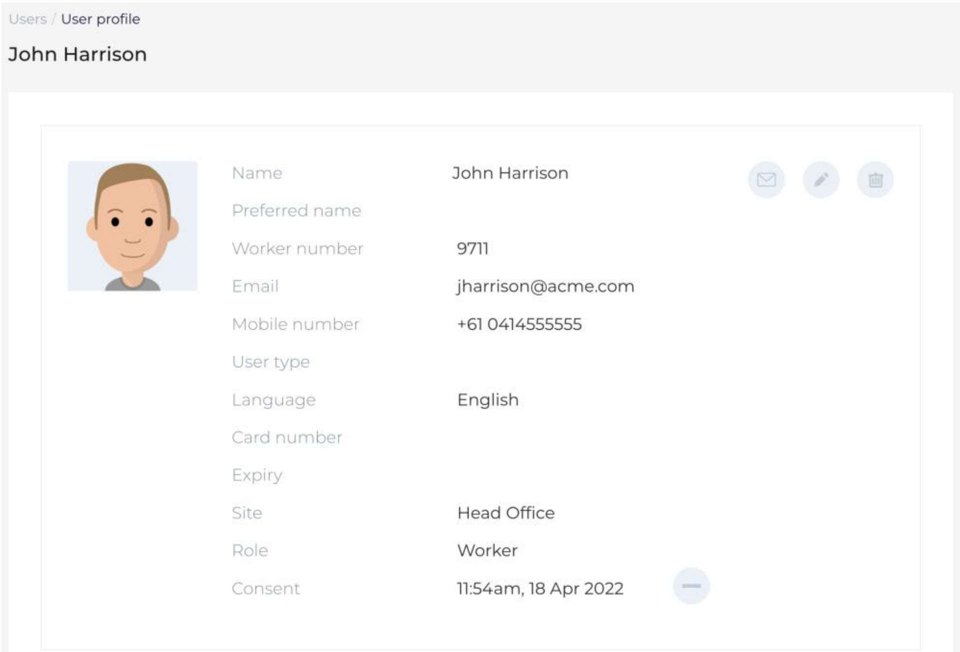
 

# Appendix B: Dealing with Incorrect Matches

If an individual is being incorrectly recognised, you have two options as follows:

1. Ask the individual to present to the App, and if they are incorrectly matched, instruct them to press the 'Not Me' button. NB: It is possible they may need to do this more than once.

2. Login to the NoahFace Dashboard as a System Administrator or Manager, and navigate to the User Details page for the user that is being displayed in the App. For example, if Bill is incorrectly recognised as John, then navigate to the User Details page for **John**. Click on the user's profile picture, and then press the delete icon next to the consent date (to remove their biometrics and consent).



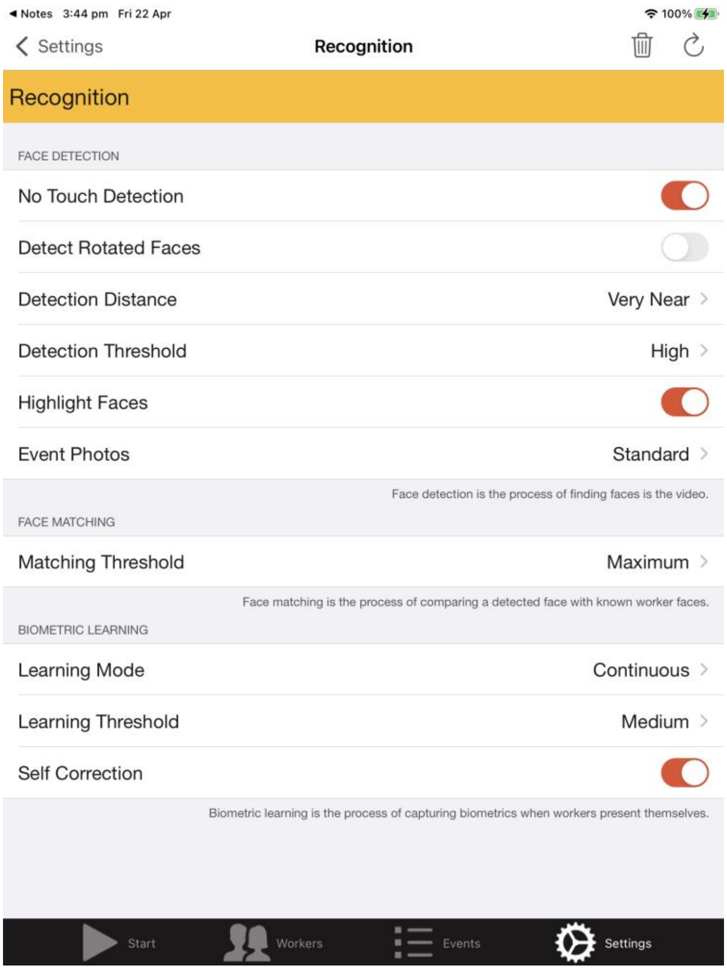

Once you confirm this action, their biometrics will be deleted both in the Cloud and on all iPads. This happens on the next synchronisation, so could take up to five minutes to complete.

Finally, **John** will be required to re-register.

See: 'Appendix C: Minimising Incorrect Matches for more information.'

# Appendix C: Minimising Incorrect Matches

If you want to take every measure possible to minimise the chances of incorrect matches (aka 'false positives') in the future, and you are happy to live with a lower recognition rate, you should adjust your facial recognition settings (on each iPad running the NoahFace App) as follows:




The settings to focus on are:

- The Detection Distance is set to Very Near, which means you have to stand very close to the iPad.
- The Detection Threshold is set to High, which means the image must be extremely clear before face comparisons are attempted.
- The Matching Threshold is set to Maximum, meaning the system must be extremely confident that two faces are identical before declaring a match.
- Biometric Learning has been configured to only take place during registration.

To be absolutely clear: even these settings cannot eliminate the possibility of an incorrect match, it just makes it much less likely than with the default settings. If you cannot accept this in your environment, you should consider using two-factor authentication.

# Version History

| Version | Date | Changes |
|---|---|---|
| **10.11.0** | 23 Jun 2021 | Updated screenshots. |
| **10.13.0** | 26 Jul 2021 | Updated liveness detection sections. |
| **13.0.0** | 22 Apr 2021 | Updated Appendix B and C on incorrect matches. |