

University of Pretoria
Software Engineering – COS 301

A-Recognition User Manual



Team Singularity
August 22, 2019

In association with the Advance.io group, a subdivision of the EPI-USE Group.











Contents

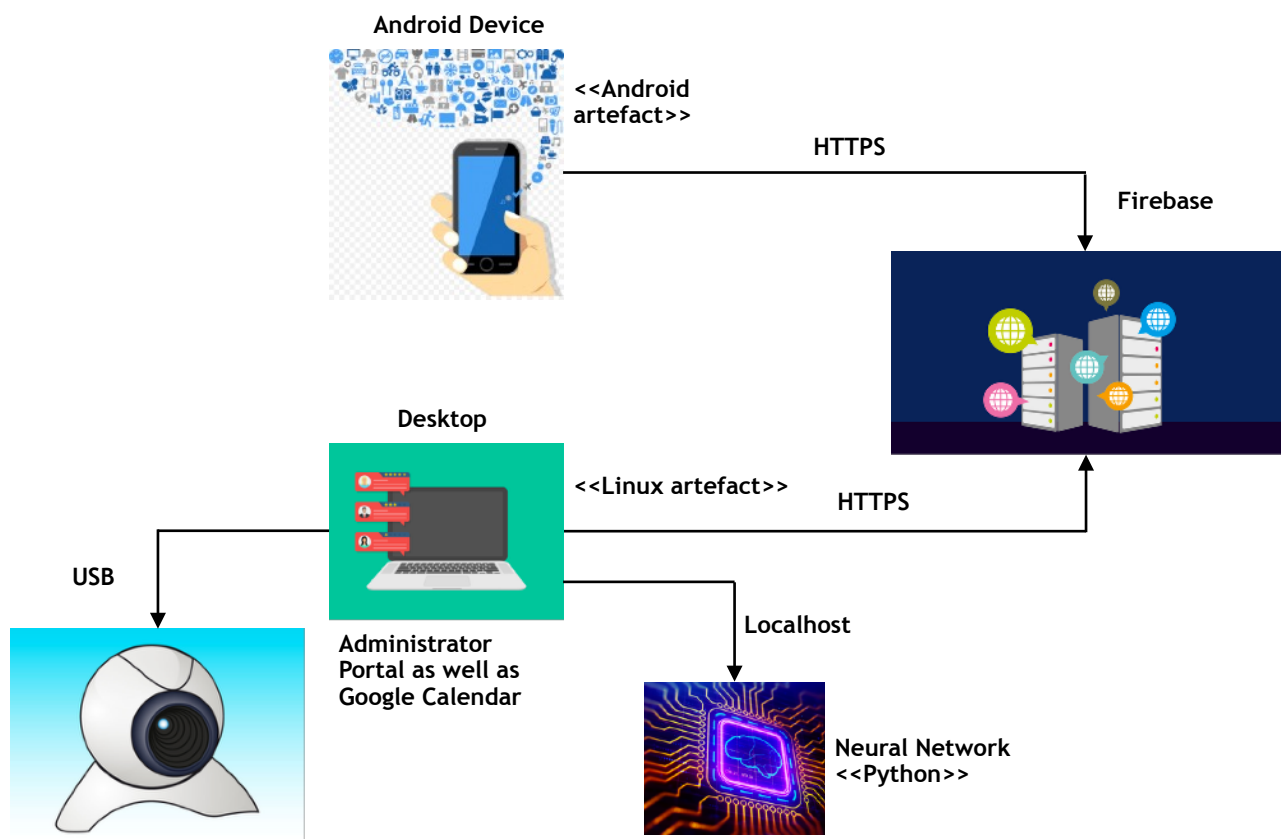
1.	Glossary	2
2.	Domain Model	2
3.	A-Recognition, what is it?	3
4.	Mobile Application	5
5.	Web Application.....	6
	5.1. Logging in	7
	5.2. Dashboard	7
	5.3. Administrator Ribbon	8
	5.4. Adding an Employee	8
	5.5. Generating OTP	10
	5.6. View employees	11
6.	Camera Capture Process	12
7.	Errors.....	12
	7.1. Unable to login as Administrator	12
	7.2. Unable to add employee	13
	7.2.1.Via live photo and Upload image.....	13
8.	Troubleshooting.....	13
	8.1. No Internet Connection	13
	8.1.1.Mobile	13
9.	Feedback and Enquiries	14

Figure 1 Glossary Figure	2
Figure 2 Google Home	3

1. Glossary

OTP		One Time Pin, a 6 digit number generated to access a board room if facial recognition fails or for guest use
App		Referencing the mobile application
WebApp		Referencing to the web application, opening the application in a browser
Admin Portal		The administrators working screen to perform operations after login
Calendars		Reference to Google Calendar to make the bookings for the meetings
Android		An operating system for mobile phones
GDPR		General Data Protection Regulation
POPI		Protection Of Personal Information Act

2. Domain Model

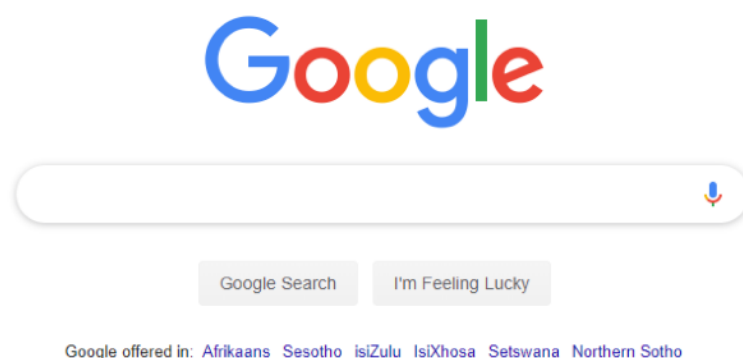


The Deployment model depicts a simple and easy to follow structure of how A-Recognition works. Simply put, both the Mobile Application **A-Recognition** as well as the Web Application both send messages over the internet to the hosted site, found at . These messages are then processed and certain actions and operations are taken once these messages have been processed.

3. A-Recognition, what is it?

A-Recognition as a whole system is a facial recognition access control system, simply put. But it is more than that, it is the amalgamation of various security and ethical concepts that are enforced to ensure that the system does its job, and does it right. It involves certain aspects of Artificial Intelligence (AI) to ensure that it cannot be fooled by an image or photograph. The system is far more in depth in that it can dynamically generate a manual OTP to a user that may have lost or forgotten their own, and we have ensured it enforces the ethical concepts of GDPR and POPI.A-Recognition is a facial recognition access control system that has a primary roll to control access to meeting or boardrooms. The system as a whole will have three major users to partake within it, namely an Administrator (will be responsible for registering new employees as well as overseeing any problems in the future), Employees (personnel within the company that will be registered by an administrator) and Guests or Clients (users that are not registered onto the system by an administrator. The system comes in two parts for a user, namely the Mobile Application(INSERT APP NAME) (See Section 1.5 Mobile Application for more) and a Web Application (See Section 1.6 Web Application for more).The application currently only runs on Android Devices and will require internet connection via mobile data or via WI-FI. To check your internet connectivity, follow the below steps:

1. Go to settings on your cell phone, often depicted by a gear symbol.
2. Select the Connections option and inspect whether Wi-Fi is on
 - a. If Wi-Fi is not on, select the option to turn it on
 - b. Connect to a Wi-Fi network that you trust and that is in range of your device by selecting it. Ensure that you trust the network you are attempting to
3. To test if you have internet connection, via mobile data or via Wi-Fi, a simple measure is to attempt to open your web browser on your cell phone and enter Google.com into the search bar. After loading, if the screen shows an output similar to Figure 1.1, you have internet connection.



A similar process could be followed for ensuring that there is internet connection to either

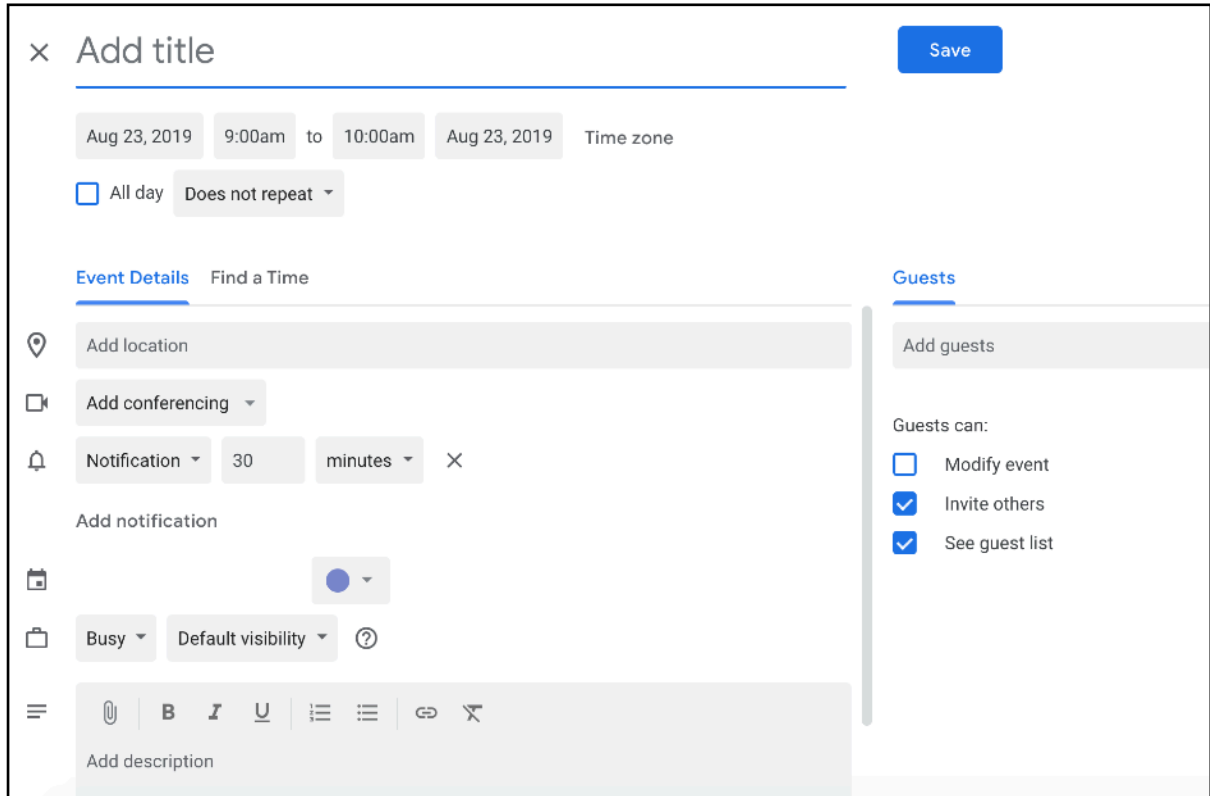
The image shows the Google Calendar 'Add event' interface. At the top, there is a title field with a placeholder 'Add title' and a blue 'Save' button. Below the title, the date and time are set to 'Aug 23, 2019' from '9:00am' to '10:00am' in the 'Time zone'. There are checkboxes for 'All day' and a dropdown for 'Does not repeat'. The interface is divided into two main sections: 'Event Details' and 'Guests'. The 'Event Details' section includes fields for 'Add location', 'Add conferencing', 'Notification' (set to 30 minutes), 'Add notification', a color picker, 'Busy' status, 'Default visibility', and a description field with a rich text editor. The 'Guests' section has an 'Add guests' field and a list of permissions: 'Modify event' (unchecked), 'Invite others' (checked), and 'See guest list' (checked).

Figure 3 - Google Calendar interface

a desktop computer or a laptop to access the Web Application. To ensure internet connection is present, you may open any web browser on your desktop computer or laptop and once again attempt to open Figure 1.1. If an error occurs, please see Section 1.9 Troubleshooting.

In order to make use of the A-Recognition system, bookings for events will be made through Google Calendar. Simply, a person can make a booking upon a specific day for a meeting in which the system will be able to gather that information at hand. Employees will be able to use their facial data to gain access while any guests being added to the meeting or booking will be sent an OTP to gain access.

The user will input all relevant information regarding the booking in the above Figure.

- A Title
- Start date
- Start time
- Any guests required for OTP generation

4. Mobile Application

The Mobile Application used for the A-Recognition acts as a virtual keypad, that allows a user to essentially carry their very own keypad around with them. It has the functionality of being able to input the OTP that a guest or client has received and being able to scan a QR code to identify the particular room that a person is attempting to enter. When first launching the A-Recognition mobile application, you will be greeted by the following screen:

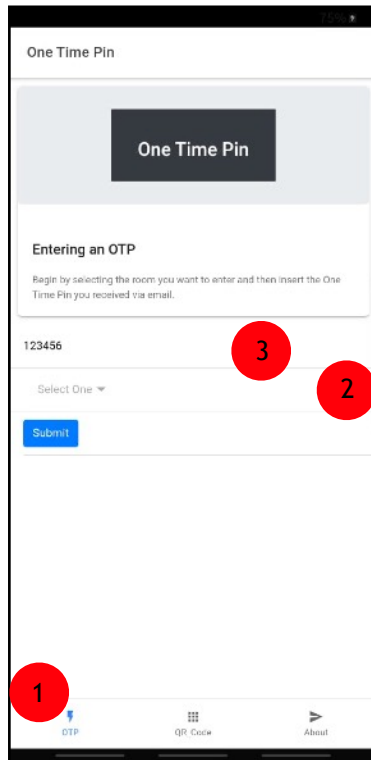


Figure 4 - OTP Input Mobile Application

Figure 3 Depicts the Applications home landing screen. This screen in particular will be used to input the OTP that a client may have received or for an employee to use if they would like to make use of an OTP they have received.

In order to make use of the mobile application as a keypad, the following steps will be taken:

1. Ensure that you are on the OTP tab
2. By using the dropdown menu, select the room you would like to access
3. Finally input your 6-digit OTP and click submit.

A message such as Figure 6 will pop up if access has been granted or such as Figure 7 if access was denied.

As mentioned above, the application may also be used to scan a QR code to make the process of room identification simpler for users that may not be aware of room names or identities. In order to make use of the QR scanner that can pull the room name from a QR code, simply access the QR Code tab within the application, as depicted by figure 4.

1. Once the tab has been selected, select the scan code option to make use of your camera. (Take notice, the first time you attempt to scan a QR code, you will have to grant permission to the camera as shown in figure 7).
2. Place your camera over the QR code and scan it.
3. Input your OTP and click submit to submit your OTP
4. The same success or error messages as above will appear.

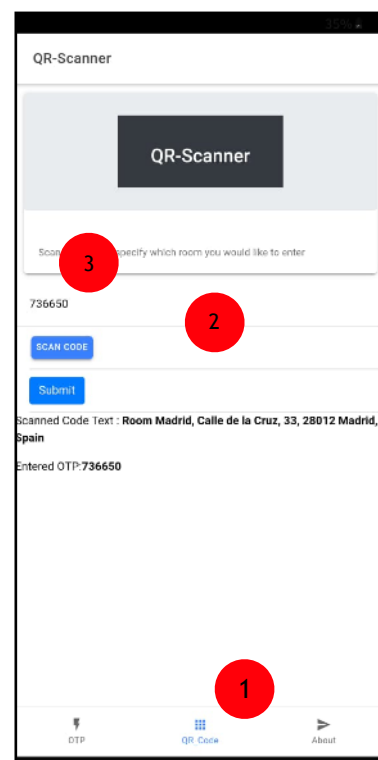


Figure 5 - QR Code OTP Input Mobile Application

The message that will pop up when you first make use of your camera from your Android device to scan a QR code.

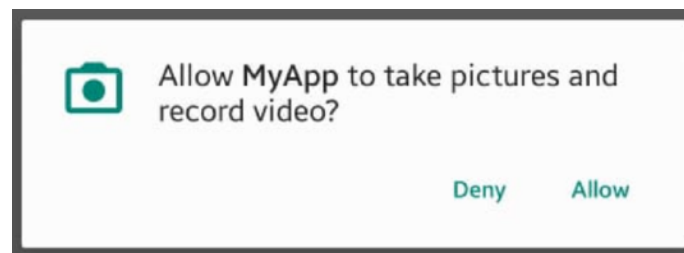


Figure 6 - Permissions pop up to make use of Android Camera

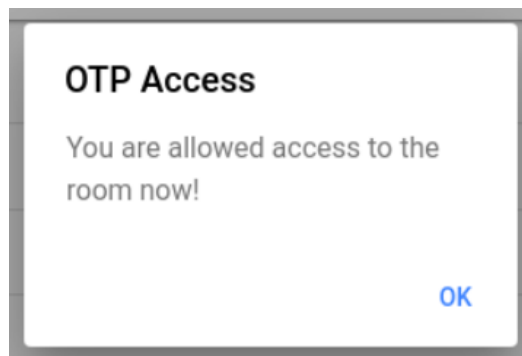


Figure 7 - Example of the response output from the application when the correct OTP has been used.

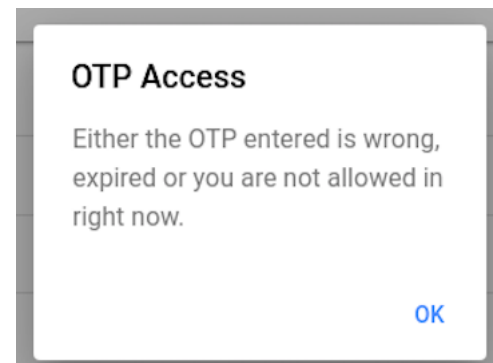


Figure 8 - Example of the response output from the application when the incorrect or expired OTP has been used.

5. Web Application

The web application, which is based on the new age of making use of applications that can be available on many different devices and not only limited to just websites, is where the administrator functionality lives.

The web application provides many tools that an administrator user may make use of which may include, but not limited to, adding new employees to the companies database and even sending broadcast OTP's in certain scenario's.

The initial screen that a user, an administrator privileged user in this case, is greeted with, will look like Figure 8 below:

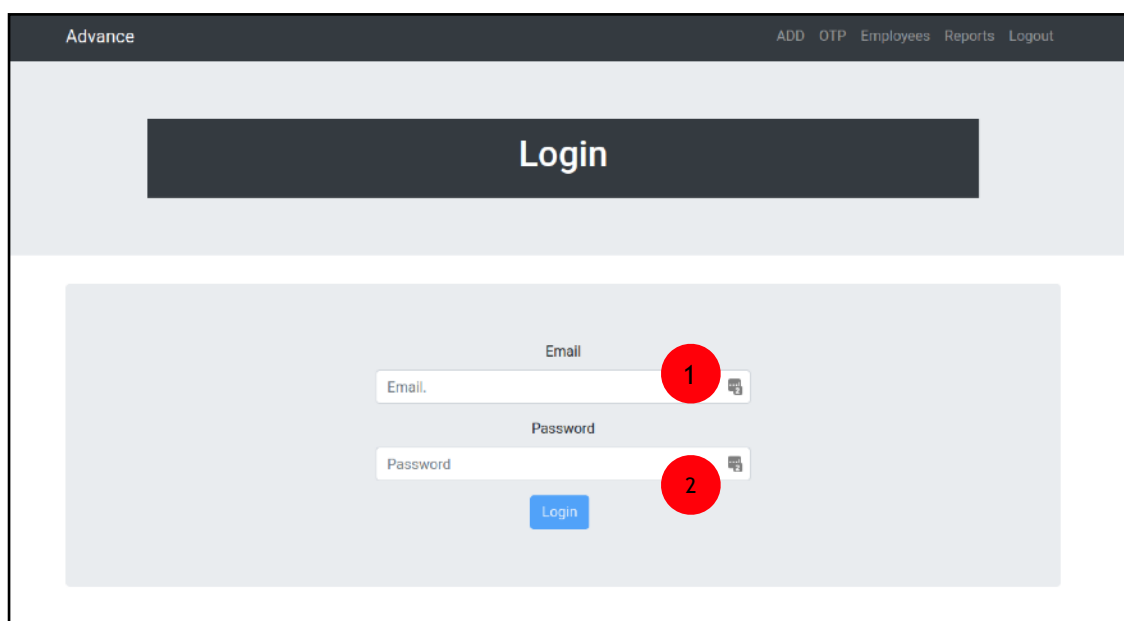


Figure 9 - Login Screen web application

5.1. Logging in

Figure 8 provides a clean interface to login to the web application for administrators and holds the functionality and operations within. The portal, the application that becomes available to the administrator on login can only be accessed by administrator privileged users that have valid login credentials.

These credentials are namely an email address associated with the administrator as well as a password linked to that email address.

To login as an administrator;

- Firstly ensure that you are an administrator user yourself.
- Secondly, simply input your email address and password that was used to register for the administrator role.

If any errors occur, please see Section 7.1 of the Errors Section under the heading of Unable to login as Administrator. A troubleshoot guide will accompany the above mentioned section to ensure the error is resolved.

5.2. Dashboard

Once a user has successfully logged in, via the login page (Figure 8 above), a number of options are available to the user. These will appear via the dashboard page which hosts some essential operations and commands. Some of the options that will appear on the dashboard page will appear as:

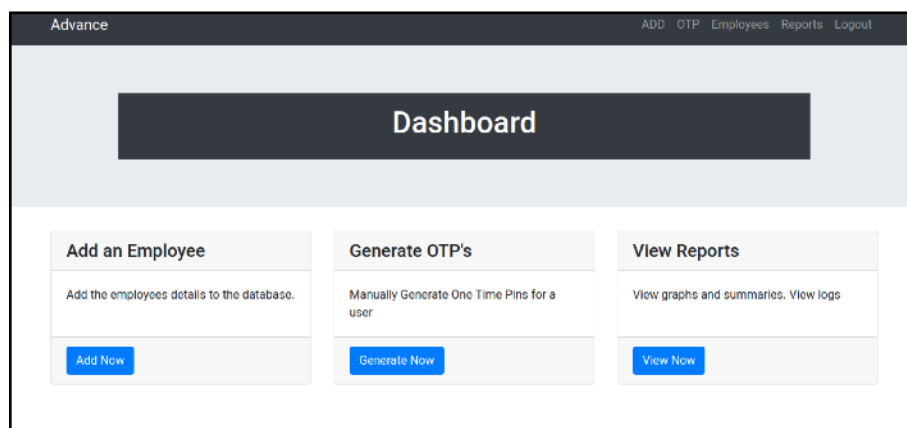


Figure 10 - Administrator Dashboard

The following operations will be possible to an Administrator upon successfully logging in:

- **Add an Employee** - (Adding a new employee to the organisation)
- **Generate OTP's** - Submit a request to generate a new OTP for either an entire room or a new OTP for a client.

5.3. Administrator Ribbon

Some extra options appear on the top of the screen, within what is known as a ribbon. These options may be viewed and seen by the top most ribbon bar that signifies what the administrator is capable of. This ribbon will always be present on every screen throughout the web application.

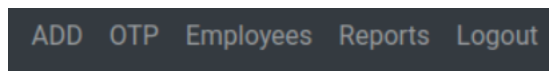


Figure 11 - Administrator control ribbon

The options, reading from left to right are as follows:

- **ADD** - Add an employee to the database to make use of facial recognition
- **OTP** - Manually generate OTP's for a single user or broadcasted
- **Employees** - View a list of all registered employees to edit
- **Reports** - Access reports from logs generated from each room
- **Logout** - Log the current administrator out of their current session

5.4. Adding an Employee

In order to add or register a new employee, the following process is followed (Please take note that when registering an employee, a number of details about the said employee will be required. It is advised that the employee be seated with an administrator during this process to simplify the process overall).

When registering an employee, two options of facial data submission are available, namely taking a live photo at that very moment, or uploading a photo of the employee with a clear defined face within the image. Both methods will involve the employees face to be completely shown in order for the A-Recognition system to correctly generate a stored image for the employee.

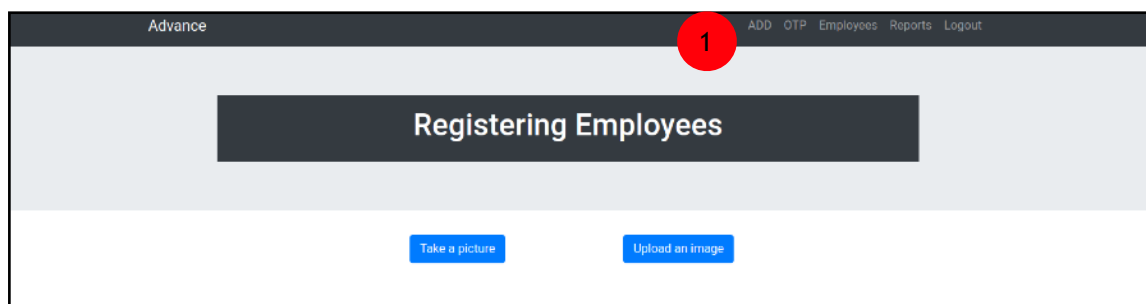


Figure 12 - Register a new employee

Adding an employee involves the following steps:

1. Select the ADD option in the administrator operations ribbon
2. Select the method of image submission you would like to use (Taking a live photo or uploading an image)
 - 2.1. If the option to **take a picture** was selected, Figure 11 will show, allowing you to fill in their
 - 2.1.1. Name
 - 2.1.2. Surname
 - 2.1.3. As well as their email address

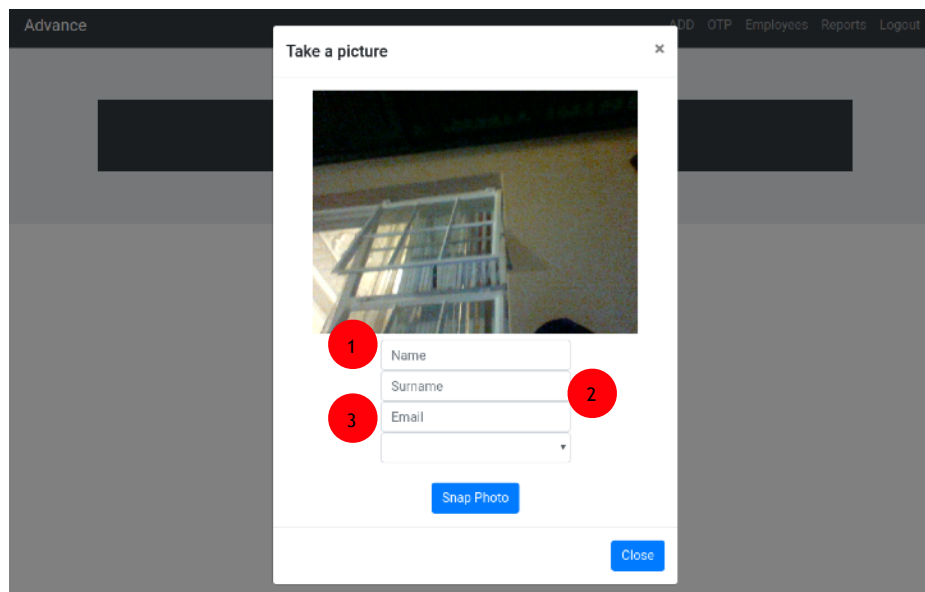


Figure 14 - Register a new employee via taking a live photo

- 2.2. If the option to **upload an image** from a local source has been selected, Figure 12 will show, and the required fields to fill in will be their
 - 2.2.1. Name
 - 2.2.2. Surname
 - 2.2.3. As well as their email address
 - 2.2.4. Take note that an image of 720px minimum will suffice for the system to process

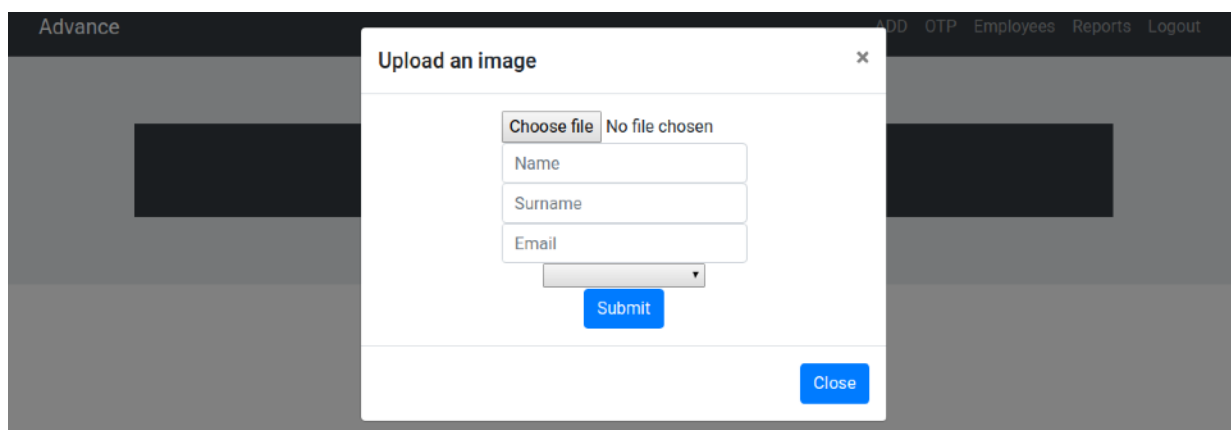


Figure 13 - Register a new employee via uploading an image

If any errors occur during the employee registration, please see Section 7.2 Unable to add Employee within Section 7 Errors.

2.5. Generating OTP

The generating OTP function may be used to generate an OTP for two scenario's,

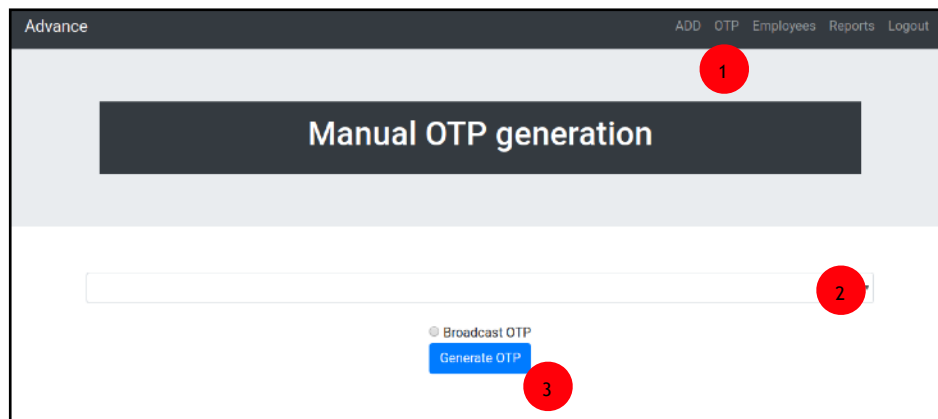


Figure 14 - Manual OTP Generation

- The first being to generate an OTP that can be broadcasted to all users under a specific event to use the same OTP
- The second is to generate an OTP for a specific user that may have lost their own OTP or it may have timed out (By missing the meeting).

In order to begin generating the OTP's, simply select the OTP option within the Administrator Ribbon which will show the page depicted in Figure 13 above (Noted by number 1 above).

Upon this screen, the drop down menu offers a list of events that an OTP could be generated for (Noted by number 2 above). This allows the administrator to select a specific event that an OTP could be generated for, as well as event and broadcasted OTP's.

Finally, select the Generate OTP button to create a new OTP that will be stored for that specific event (Noted by number 3 above).

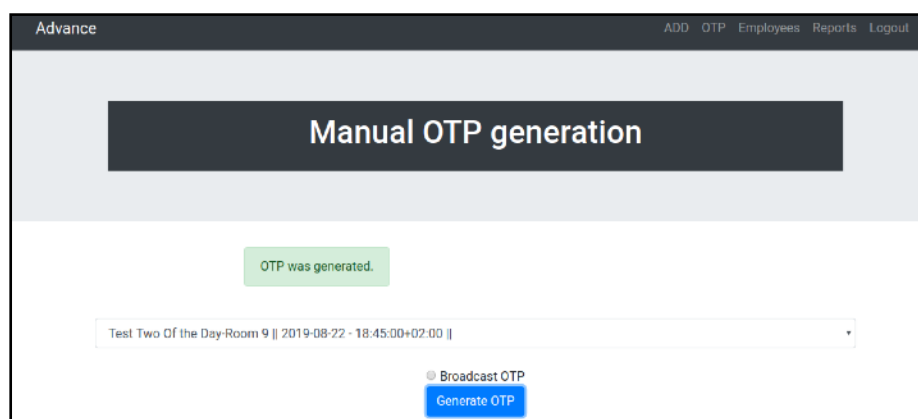
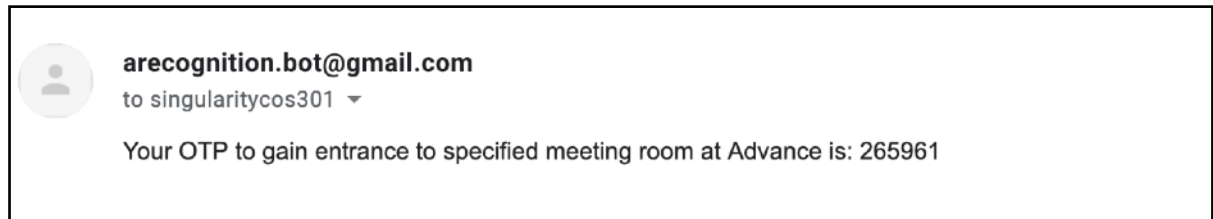


Figure 15 - Manual OTP Generation Success

Once an OTP has successfully been generated, A screen output similar to Figure 14 will show. This new OTP will be available until the end of the booking time for any person that may have a valid OTP at hand.

A employee or client that receives an OTP will receive an email in the form of:



This allows the user to have a clear indication of the OTP as well as the company available.

2.6. View employees

Administrators are also able to view all current employees in the case of updating certain information about an employee. This enables an administrator to make use of tools available to ensure information has been captured correctly as well as any errors that have to be corrected. In order to make use of viewing employees and possibly updating their information, the following steps will be followed:

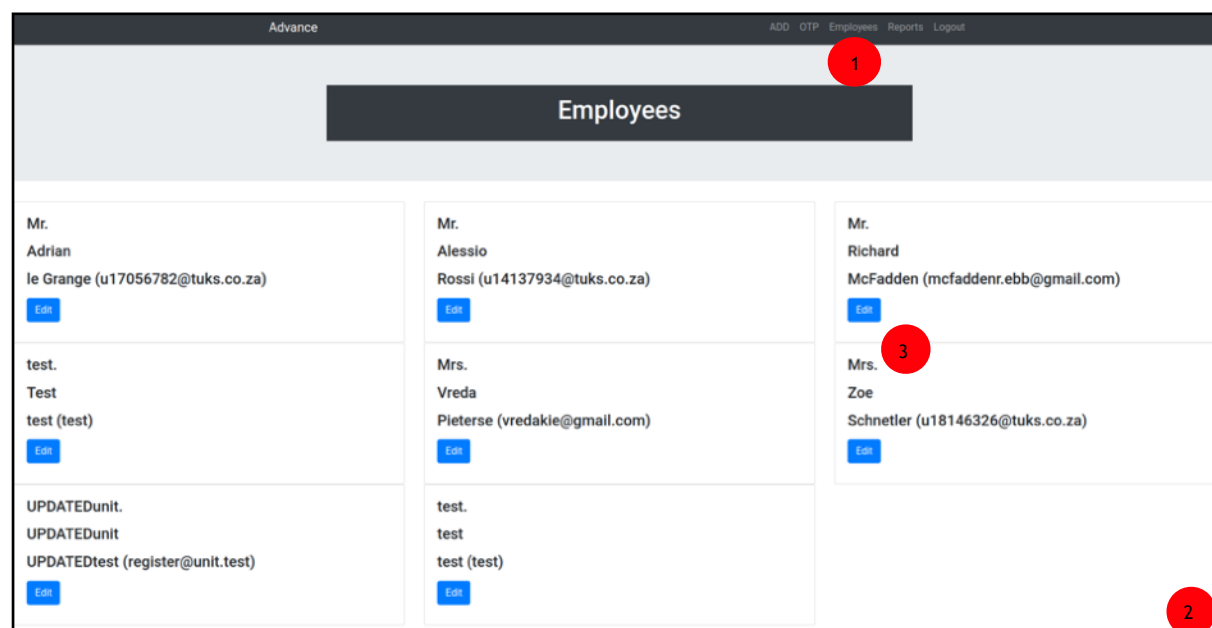


Figure 16 - View Employee Output

1. Select the Employee option from the Administrator Ribbon
2. Figure 16 will appear with a list of all employees currently registered
3. In order to edit an employee, select the edit option which will allow the administrator to update any relevant information regarding the employee

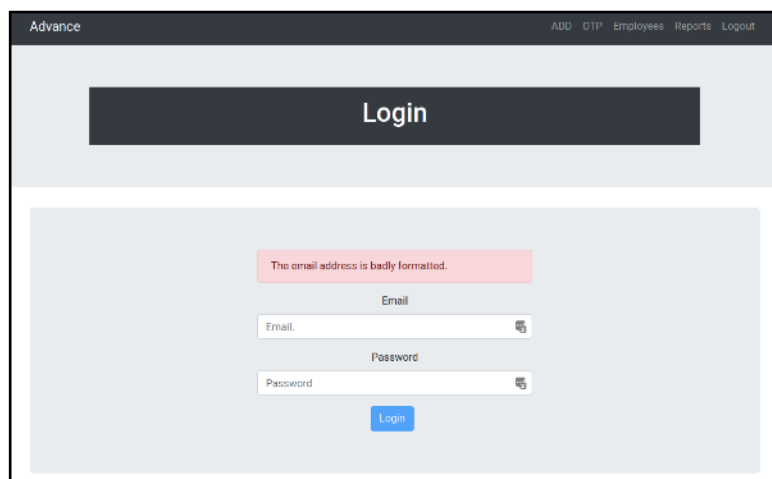
6. Camera Capture Process

In order to make correct and proper use of the Facial Recognition, an employee will place themselves directly in front of the camera. Two boxes will appear over the employees eyes which will be available to track the persons eyes which is used to test liveliness (Whether a person is real or a photo was being used).

The person will position themselves with their face fitted within the border. A user will then blink to notify the system that the user is a real person, and the comparison will be made and access will be granted if matches are present or denied if there is no match.

7. Errors

7.1. Unable to login as Administrator

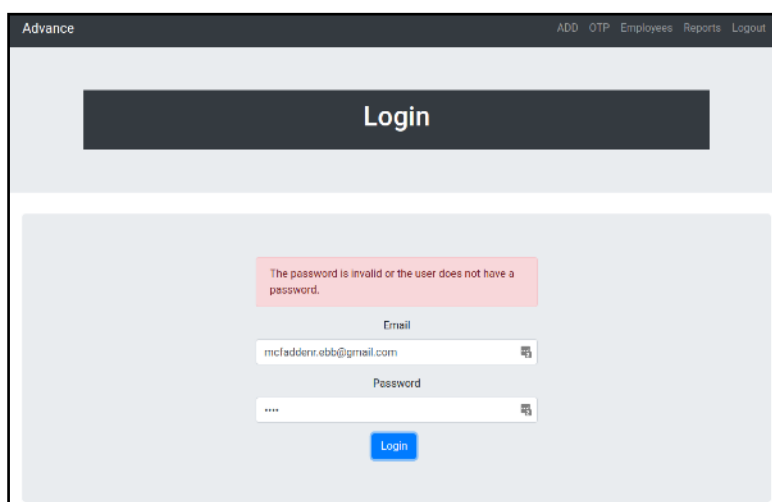


The screenshot shows a web application interface for a login page. At the top, there is a dark header bar with the word "Advance" on the left and navigation links "ADD", "OTP", "Employees", "Reports", and "Logout" on the right. Below the header, there is a large dark gray button labeled "Login". Underneath the button, there is a light gray rectangular area containing a red error message box that says "The email address is badly formatted." Below the error message, there are two input fields: "Email" and "Password". The "Email" field contains the text "Email." and the "Password" field contains the text "Password". Both fields have a small icon to the right of the input area. Below the input fields, there is a blue "Login" button.

Figure 17 - Email Error

In the case of an email being badly formatted, which includes an incorrectly configured email, an invalid email or emails that don't follow a specific template, an error similar to Figure 17 will appear.

Troubleshooting for this error will be available in Section 8.2 within the Troubleshooting Section (Section 8).



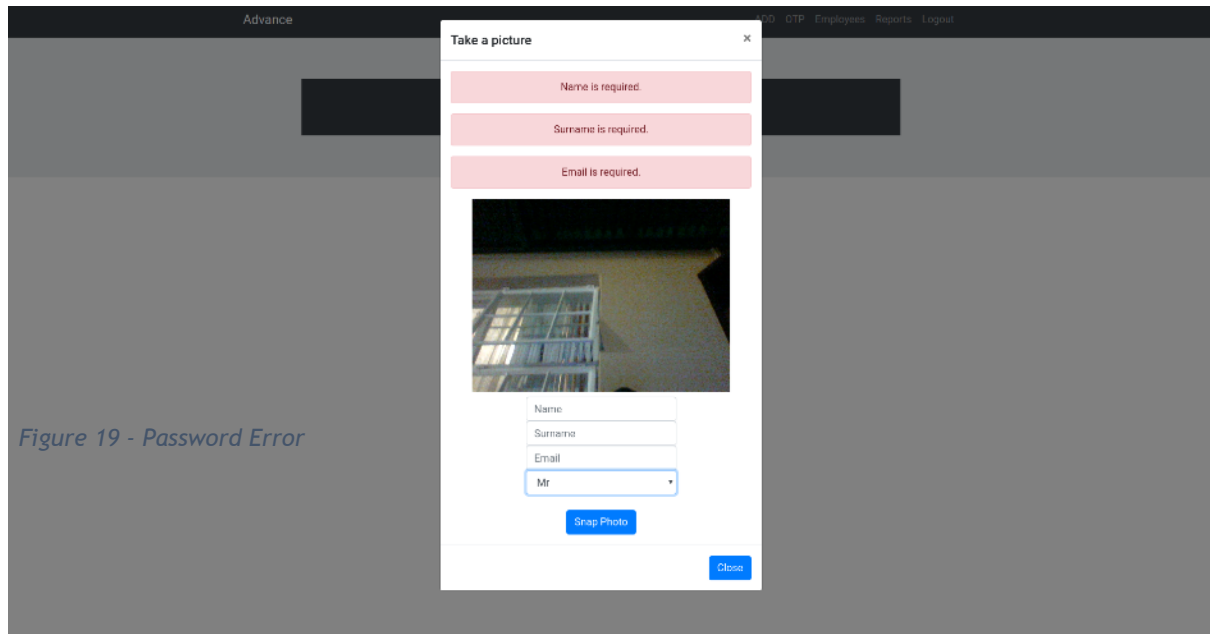
The screenshot shows the same web application interface as Figure 17. The "Email" field now contains the text "mcladdenr.ebb@gmail.com". The "Password" field contains the text "****". The red error message box now says "The password is invalid or the user does not have a password." Below the input fields, there is a blue "Login" button.

Figure 18 - Password Error

If an error in the shape of figure 18 appears, a mismatch between the user email as well as the password has arisen. This is often an error if a typo has arisen when a user has attempted to put their email or password in or when a capital letter has been input within the password which does not match.

7.2. Unable to add employee

7.2.1.Via live photo and Upload image



If errors such as required fields appear, the administrator has forgotten to fill in specific fields regarding the information for the employee.

In order to fix these errors, an administrator will have to return to the error fields and fill in the areas that seem to be required for future use.

8. Troubleshooting

8.1. No Internet Connection

8.1.1.Mobile

1. Go to settings on your cell phone, often depicted by a gear symbol.
2. Select the Connections option and inspect whether Wi-Fi is on
 - a. If Wi-Fi is not on, select the option to turn it on
 - b. Connect to a Wi-Fi network that you trust and that is in range of your device by selecting it. Ensure that you trust the network you are attempting to
3. To test if you have internet connection, via mobile data or via Wi-Fi, a simple measure is to attempt to open your web browser on your cell phone and enter Google.com into the search bar.

9. Feedback and Enquiries

For any feedback or enquiries regarding the system in terms of improvements or assistance, please see:

singularitycos301@gmail.com

with a clearly stated Subject about whether feedback is being supplied or enquiries are being made.