Face recognition

Model: FCS10-V3021C

Content

1. Product Descriptions

FCS10-V3021C is a customised face recognition software that works seamlessly with small and medium-sized pedestrian entrance face recognition terminal.

1.1 Software Functionalities

1. Multiple terminals synchronisation mode： Every face recognition terminal can be used as the server unit (server IP is advised to set as static IP), or as a client unit. Under multiple terminals networking mode, server IP address and port number are to be set in client unit. The server database's update of data to the client unit(s) is automatic and real-time. Remark: All related terminals' clock must be synchronised.

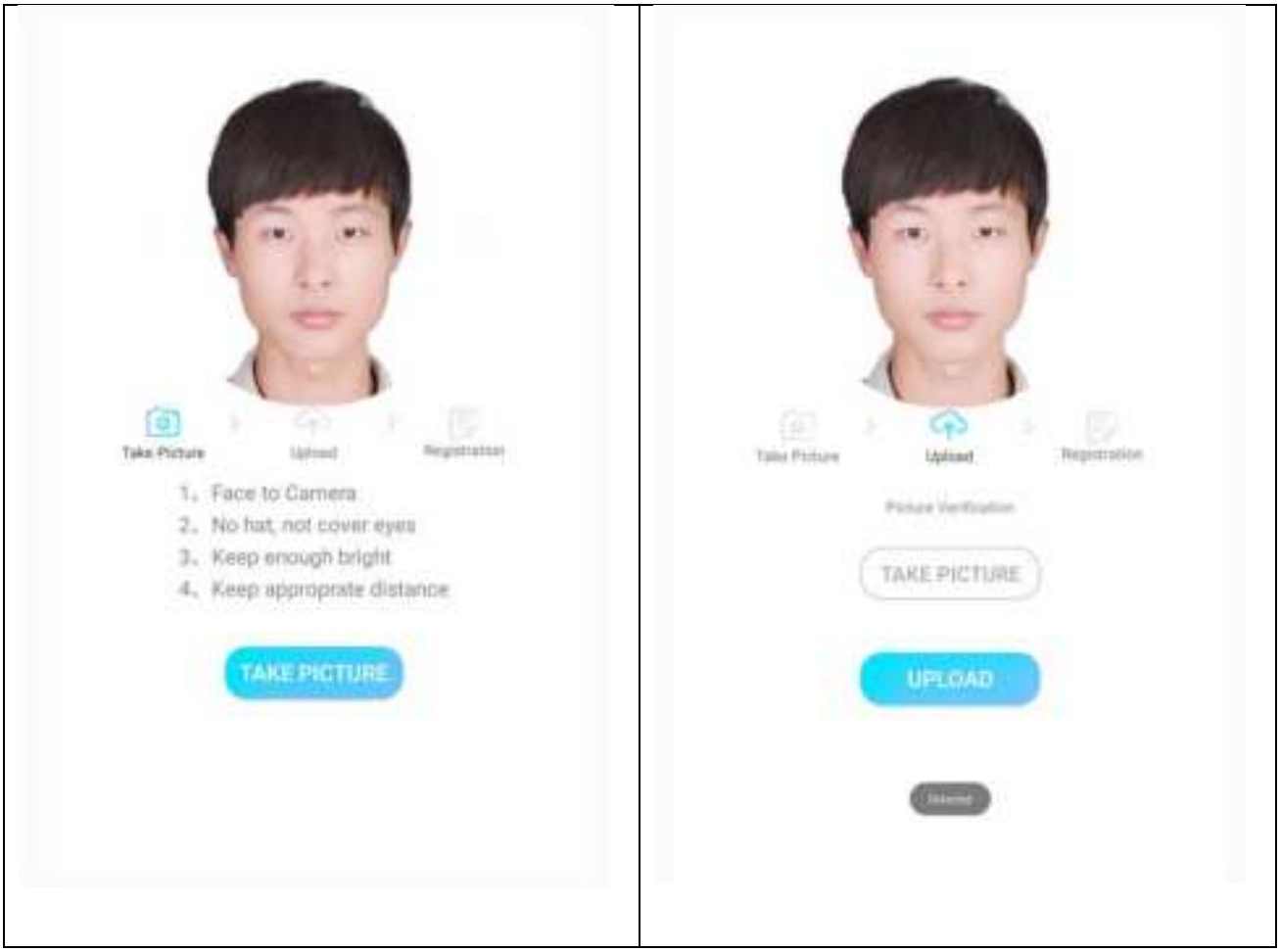
2.Single terminal mode: When used as single device, terminal works without needing any database IP and database is to be loaded directly into the terminal. No synchronising of database even multiple terminals is in operation under single terminal mode.

Details please refer to 2.8.2 Database Settings。

2. Face Recognition Management Centre

2.1 Live Photo

（1）Process：① Take Photo → ②Upload → ③Data Entry（2）Live Photo：Face must be facing the camera. No hat/cap is allowed, no blocking/covering of the eyes, sufficient lighting is required and kindly maintain a certain distance from the camera. Make sure the face is within the face frame and click on the shutter when ready. （3）After taking a photo, the prompted “recognition successful” indicating the photo meets the system requirement. Click upload to enter the information entry page. You may retake photo as shown below if the photoy did not meet the requirement.



（3）Name and Validity Period columns are compulsory when filling in the information. Other

information can be left blank.

- Gender： “Male” is being set by default. May choose “Male” or “Female”.
- Wiegand ID：A non-compulsory column. May choose not to fill.
- Nationality：To choose from 56 nationalities. A non-compulsory column.
- ID no：18 digits column. The “Year” and “month” must be entered correctly. The last digit, can be a number or an alphabet. A non-compulsory column.
- Validity Period：By default, the validity period is from the date of registration until 31 December 2099. Click to modify the validity period.

（4）Re-enter：Click Re-enter if you are unsatisfied with the captured photo or there is any mistake in the information. All current information will be cleared.

（5）Re-enter information and click Save. Upon confirmation of success, all information is recorded and ready for face registration.

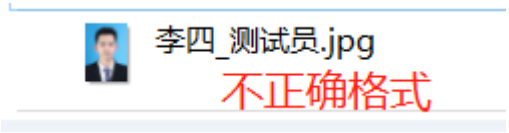
REMARK：Repeat registration of the same person is strictly prohibited

2.2 Batch Import

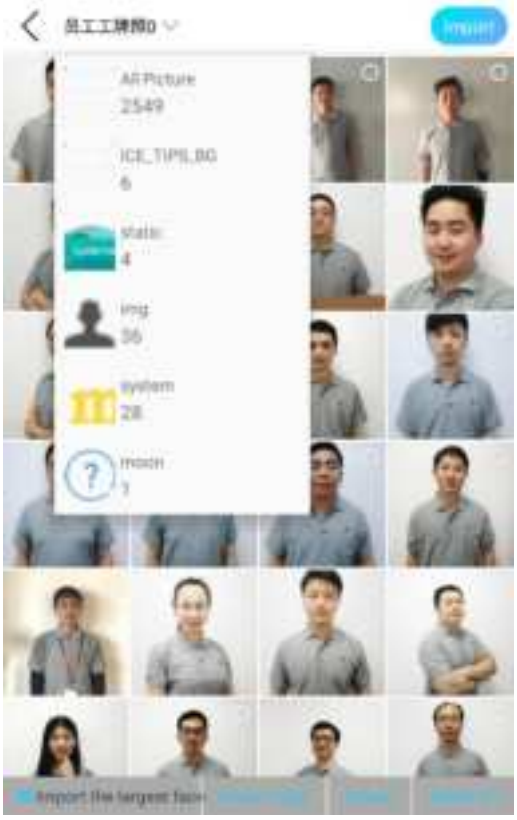
Requirements on batch import：supported format including are .jpg, .png, and .bmp. photo resolution should not exceed 3000 x 3000 pixel, and file size must not be larger than 5MB. The face pixels must be at least 112 x 96 to meet the registration quality threshold. Please refer to 2.8.6 recognition threshold for details. It is recommended to use image of single individual for the process.

Steps：

1. Save edited photo in a pen drive and plug in to the terminal's USB port.



Remark：symbol such as "_" (underscore) is not allowed. It may cause the importing process to fail.



Select “Batch Import” after the pen drive is plugged in to the USB port. The system will automatically load all folders in the pen drive. Select the folder to upload and click on the file to select the photo. Click “Select All” if all files are to be uploaded to the terminal. Click “Import” to confirm. The system will automatically save the selected face information.

Should there are multiple faces in a picture, please select “to import the biggest face”. The system will save the face with the largest proportion. Do not select if this feature is not required. The system will automatically filter the photo of multiple faces when importing.

By default, the validity period for Batch Import is from the date of registration to 31 December 2099. Wiegand ID is “none” and gender is “Male” by default. Click to access “Face Database Management” to change.

Upon completion of data import, the results will be shown in chronological order, indicating whether the entries are successfully or unsuccessfully imported. Reason for unsuccessful entry will be indicated. User may edit the photo accordingly before retrying.

2.3 Visiting Record

The Visiting Record Page will display the personnel's access records in chronological order. Successful record will be shown on the left, indicating live photo, name, gender, nationality, ID card number, reading method, and time of access; whereas unsuccessful record will be shown on the right, indicating avatar and time. Click on "record screening" to access the visiting record of the selected personnel based on name.

Tip：Visiting record will not be deleted before storage is full. By default, the maximum number for storage is 2 million records. System will automatically erase the initial 50% of record when storage is full.

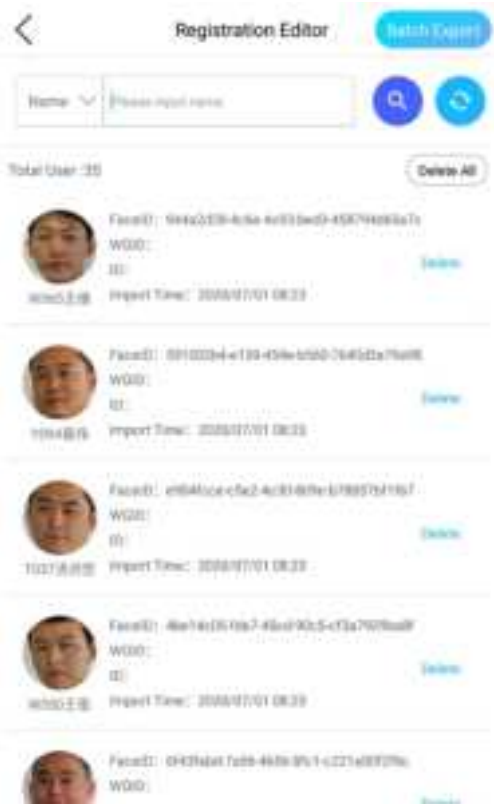
If necessary, set the number of days for record storage manually. Click “Start Setting” at the bottom corner and set the number of days in the pop-up frame.

2.4 Face Database Management

This is the face database of the device. It displays the total number of recorded personnel information. It supports query by name, view and modify as well as single or batch personnel information delete. Refresh record by clicking the button with rotating image.

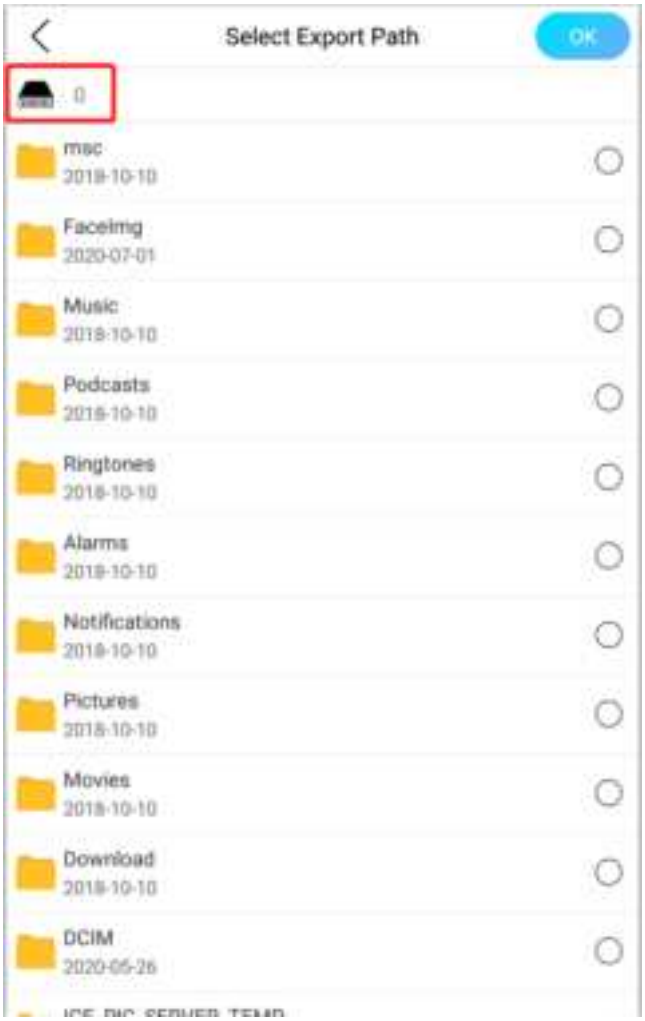
2.4.1 Personnel Information Modification

Click on the avatar to choose preferred photo from the pop-up frame or to take photo.



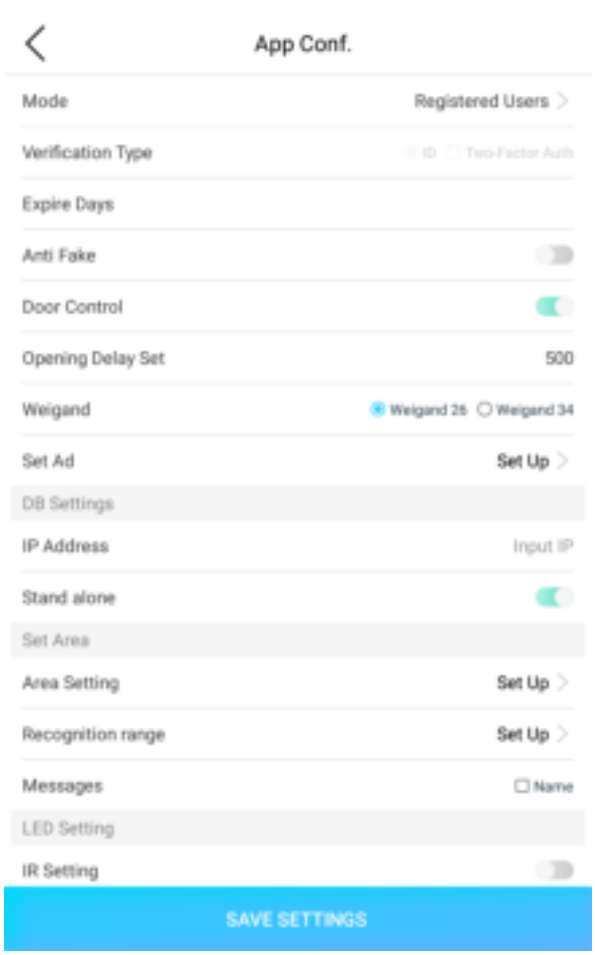
2.4.2 Batch Export Face Information：

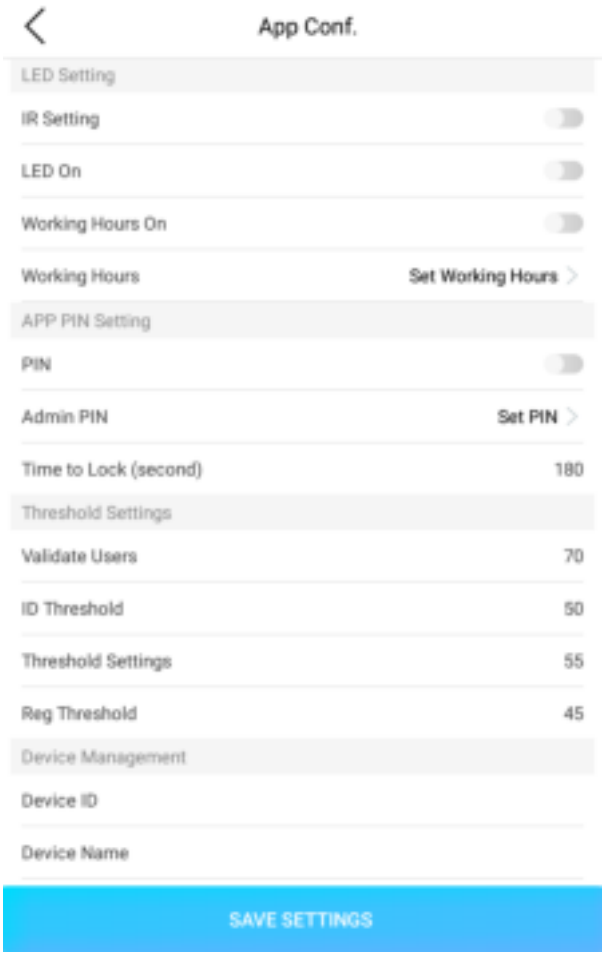
Click Batch Export and choose whether to export the photo information. Select the path to save the exported file.

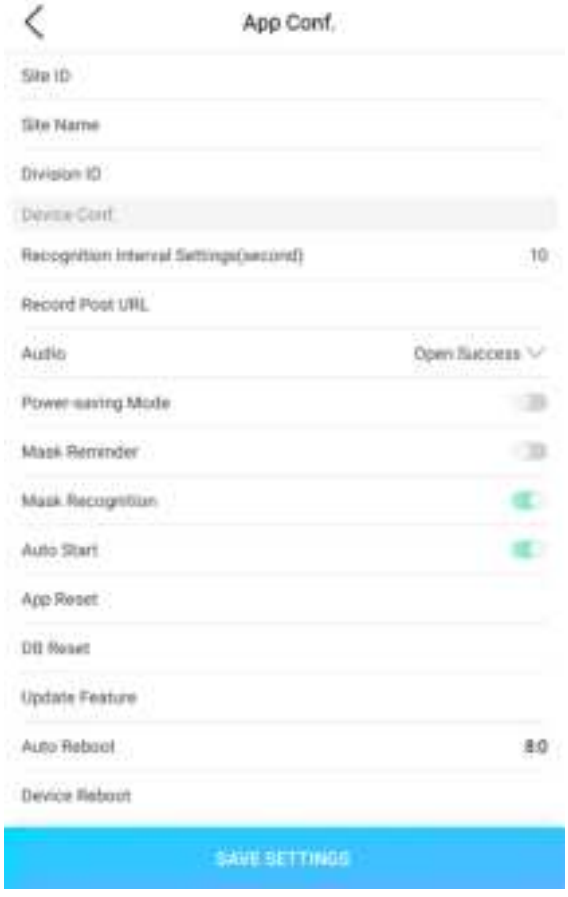


2.8 Application Settings

This is where the settings for face recognition is decided.







2.8.1 Working Mode

1. There are 4 types of Normal Working Mode ①Whitelist Mode ②Visitor Mode ③Hybrid Mode ④ Man-and-Card Mode

① Whitelist Mode - Only database recorded personnel is eligible to access.

② Visitor Mode - Choose either “ID Comparison” or “Double Verification”.

For “ID Comparison” – Stranger may swipe ID card on the spot to complete the process and obtain access. By default, the validity for access is ONE day. Manually changing the valid visiting period is allowed. When the validity for access is set at 0, the visitor will need to verify identity during every visit.

Double Verification：To use with Pre-enter Content. Details please refer 2.4 Pre-enter Content.

③ Hybrid Mode

Under Hybrid Mode, pre-entered face or ID card is authorised to pass.

④ Man-and-Card Mode

Under Man-and-Card mode, face detection must be done with the swiping of ID card.

Access is only granted when face and Wiegand ID in the database match the ID card’s information.

Temperature Check Mode: ① Temperature Check to Access Mode ② Whitelist Temperature Check Mode ③ ID and Temperature Check Mode

① Temperature Check to Access Mode

Under this mode, access is granted to any personnel with normal body temperature.

② Whitelist Temperature Check Mode

Under this mode, access is only granted to personnel with database record and normal body temperature.

③ ID and Temperature Check Mode

Under this mode, access is granted to stranger with ID card (to swipe) and normal body temperature.

2. **Human Recognition**：Activate Human Recognition to prevent non-real person (such as stranger using the photo of recorded personnel) from accessing.

3. Switch On/Off Control：If switched ON, the access is granted automatically after face verification is successful; if switched OFF, the access is manually granted by the direction from the host computer.

4. Access Opening Delay Setting：Calculated in millisecond. By default, the delay is set at 500ms. Manually altering is allowed between 500ms – 5000ms.

5. Wiegand：A Wiegand ID between 26-bit or 34-bit can be generated according to requirement.

6. Full-screen Ads Settings

（1）Fullscreen Ads supports photo (.jpg, .bmp and .png format) and video (.mp4, 3gp and .avi format) playback of file size not exceeding 150MB.

（2）Photo ads is limited to 5sec/image.

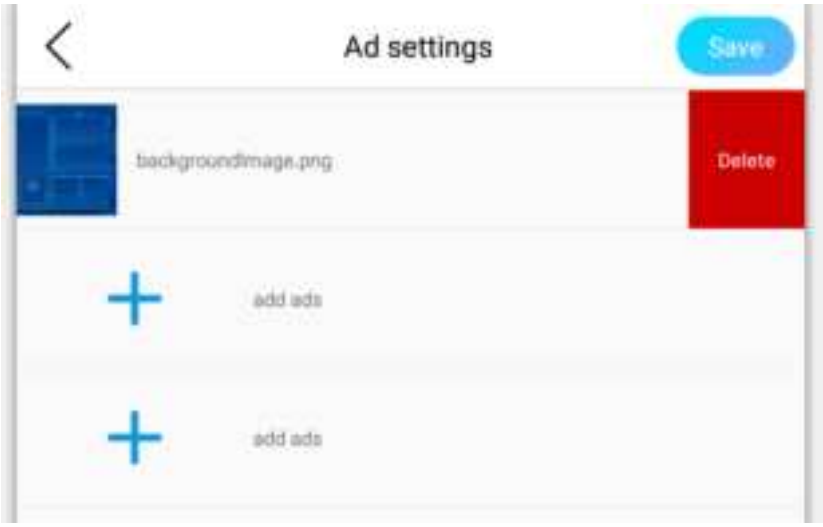
（3）Suggested picture resolution is 800 x 1280.

7. Split-screen Ads Settings

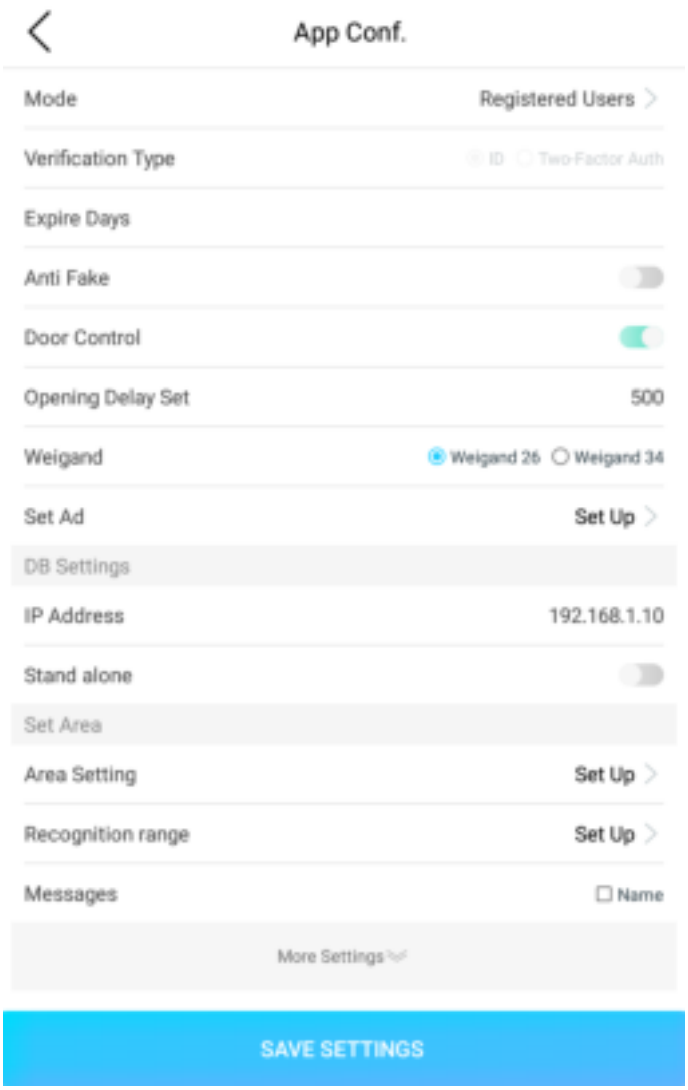
（1）Close the full-screen ads button in the photo/video playback setting to activate split-screen ads. Ads will be played in the advertising area at the bottom of the page. System will reset to default (not playing ads) once image/video is deleted from the system.

（2）Split-screen ads supports photo (.jpg, .bmp and .png format) and video (.mp4, 3gp and .avi format) playback of file size not exceeding 150MB.

（3）Photo ads is limited to 5sec/image at suggested picture resolution of 800 x 260 or the picture appearance may be affected due to cropping or stretching.



2.8.2 Database Settings



1. Switch on to start using the system directly under single terminal mode.

2. Disable “Single Terminal” and enter the server’s IP address in respective devices if using multiple terminals.

2.8.3 Detection Area Settings

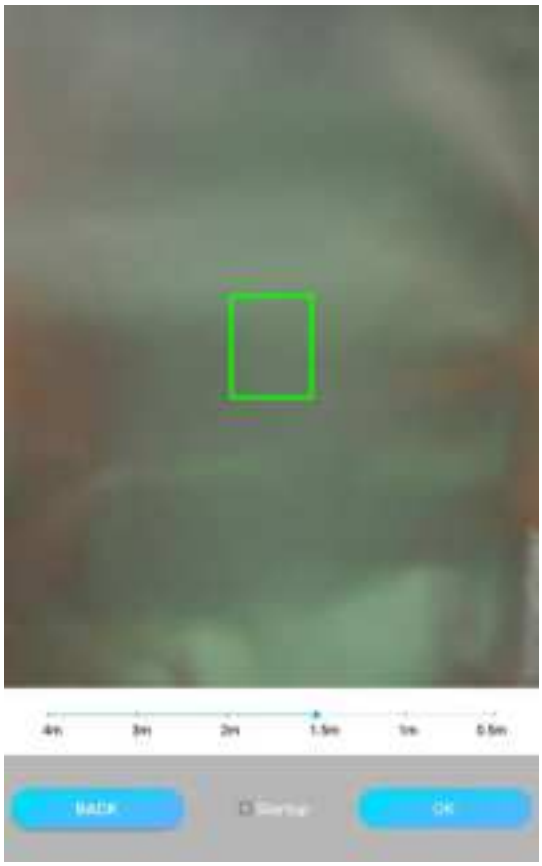
1. Setting Detection Area

This function is used to decide the detection area. The detection area is set based on requirements. Please do not modify this unless necessary.

2. Setting Detection Range

This function is used to modify the detection range (distance). Detection takes place only on face captured within the designated range. Anything beyond the range will be excluded.

Remark: A deviation of 30cm is allowed.



3. Prompt Information Settings

Prompt Information is divided to avatar and name. The system will show the personnel's name and avatar after verification upon selecting this otherwise only the default avatar will be shown.

2.8.4 Additional Lighting Settings

1. Only turn on "Infrared" or "Additional Lighting Stay On" at a time. By turning on the infrared sensor, extra lighting will switch on automatically when there is someone enters the infrared detection range. When "Additional Lighting Stay On" is turned on, the light shall remain on all the time. The additional light can be switched off by turning off the infrared sensor and additional lighting always on.

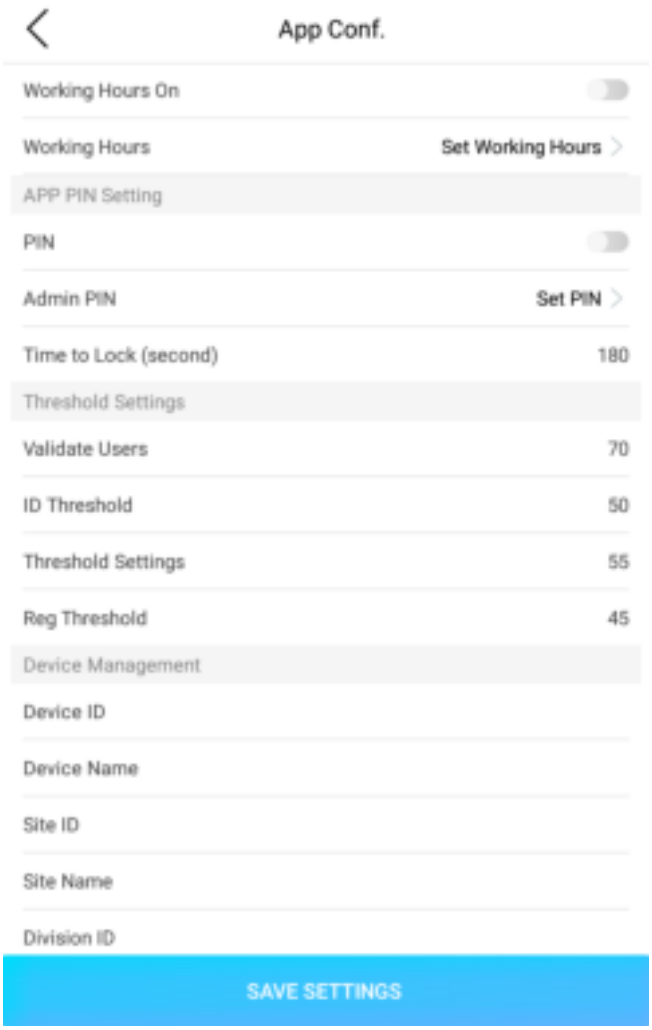
2. Enable “Scheduled Lighting” and set terminal’s working hours. The additional lighting will stay on throughout the working hours and goes off after the working hours.

2.8.5 Password Management Settings

Management Password is disabled be default. The default lock time is 80 seconds (setting range is between 15 to 300 seconds). Exceeding the pre-set lock time will require password. The password is 4 digits number.

Reminder: Remember to click Save Setting after the password setting is completed. The password setting is only valid to Face Verification Management Centre, and nor for other interfaces of the terminal.

2.8.6 Recognition Threshold



The explanation uses default parameters as example. The parameters can be set based on requirement. The maximum point is 100.

1. Whitelist Threshold：Access will only be granted to personnel who meets 70 points (the maximum point for face verification） of similarity between the captured face and the face in the database. Personnel who receives lower than 70 points will be considered as stranger.

2. Personnel Threshold: The face captured by the terminal must reach 55 points of resemblance with the photo on the ID card to be qualified as the same person.

3.Recognition Rating：The system will only activate database face verification when the terminal captured photo reaches 55 points. The rating varies due to factors including clarity, angle, lighting etc.

4.Registration Rating：The face needs to be at least 45 points clear to be qualified to upload to the database, regardless if the photo is an uploaded image or a captured on-the-spot. The objective of the rating system to ensure the quality of face database and improve verification’s accuracy.

Reminder：Avoid modifying the recognition threshold unless it is necessary.

2.8.7 Equipment Management

Name equipment by using equipment ID, nickname, location ID, location name, and area ID for easy management.

2.8.8 System Settings

1. Interval Setting： The interval between the successful face verification and the next verification when the same verified face is yet to leave the screen. By default, it is set at 10 seconds. Available between 0 – 60 seconds.

2. Access Record Backup Address： Set the host computer's URL, save and submit. The system will automatically upload the access record to the host computer.

（1）Image transfer. The transfer of images, including the original image and uploaded image from access record.

（2）Unsuccessful record transfer. The transfer of the record of unsuccessful access.

（3）Retransfer. The transfer of the unsuccessful transferred of access record to host computer.

（4）Synchronisation. Select "Synchronise" on server's setting. Upon submitting the request, all access records from the client terminals will be updated to the host computer.

（5）Stop uploading. Clear the URL and submit to cease the transfer of access records.

3.Voice Announcement： Enable to initiate “Welcome, ***, please enter” after successfully verified. No announcement when disabled. (***the personnel’s name is in the database)

4. Energy Saving Mode： The monitor will automatically dim when no face is detected within 10 seconds. The monitor will resume to normal brightness when a face a detected. This function is disabled by default.

5. Mask Detection： The system automatically reminds the personnel to wear a mask when no mask is detected during face verification.

6. Masked Verification: Enable this function to verify personnel with mask.

7. Auto start upon power on： When enabled, the system automatically enters the face verification interface. Disable this function and the system will enter the main interface and enter the face verification interface manually.

8. System reset： Use this function to restore all configurations to the default values. Database and third-party software will not be deleted.

9. Database reset： Use this function to clear all data in the database. This function cannot be undone. The device will be switched to become single terminal after reset. Third-party software will not be deleted.

10. Schedule Reboot： Schedule an automatic reboot by setting the preferred time for the system restart daily. Reminder: This function cannot be disabled. This function is made to clearing cache, improving the verification efficiency, and extending the terminal's lifespan.

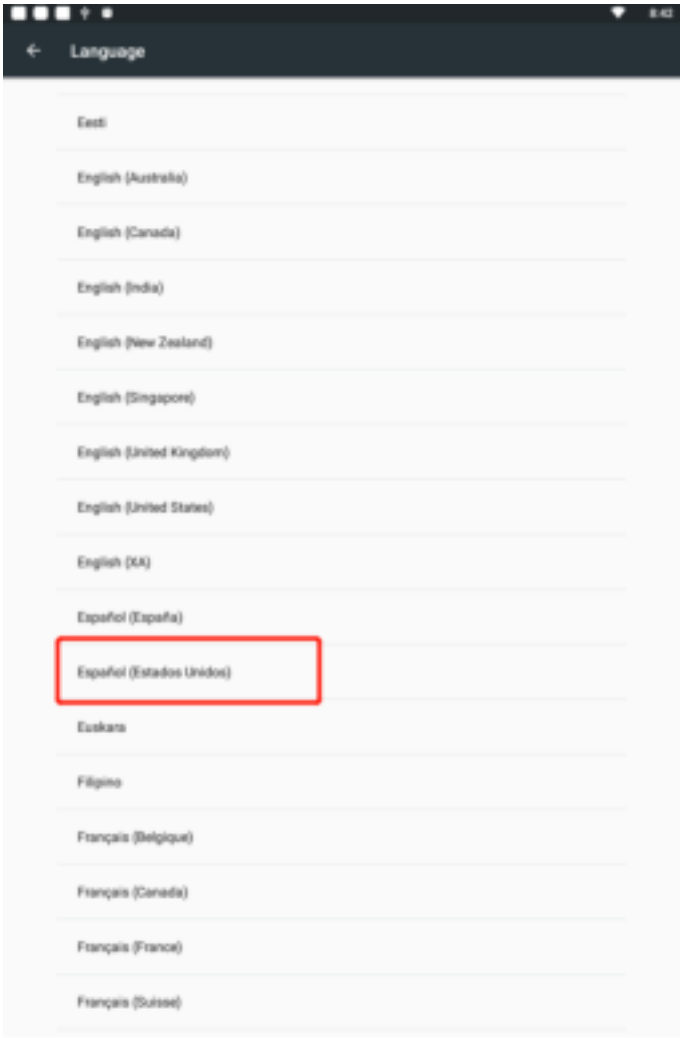
11: System Reboot： Use this function to Reboot the system.

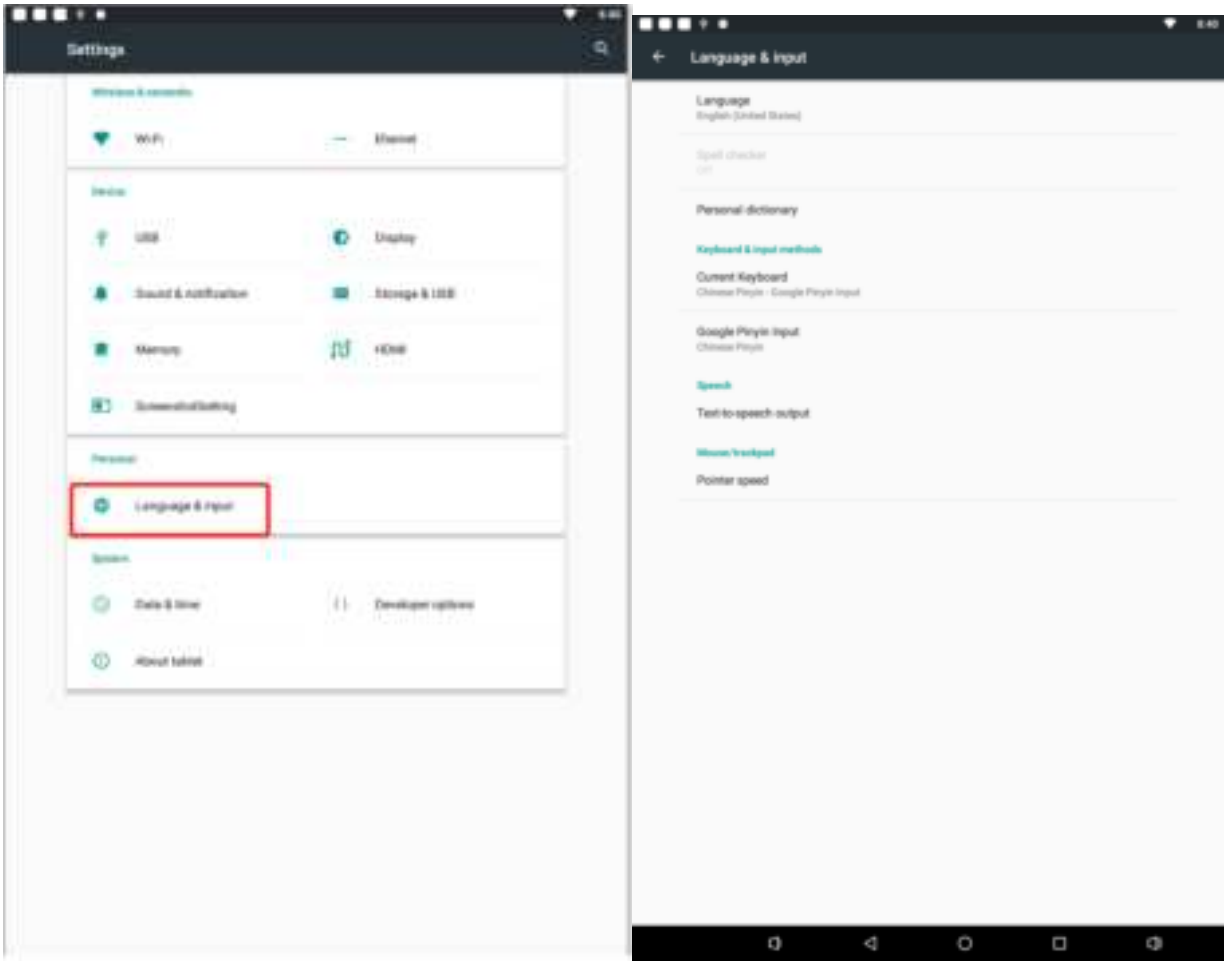
2.9 **Terminal IP**

This is to view terminal's IP address and port number. Reminder: This page cannot modify terminal's IP address. To modify IP address please refer to 3. Network Settings.

3. English Version

Enter System Settings from Control Centre. Click Language and Input Type. Select Language. Select English. The system will be switched to English version.



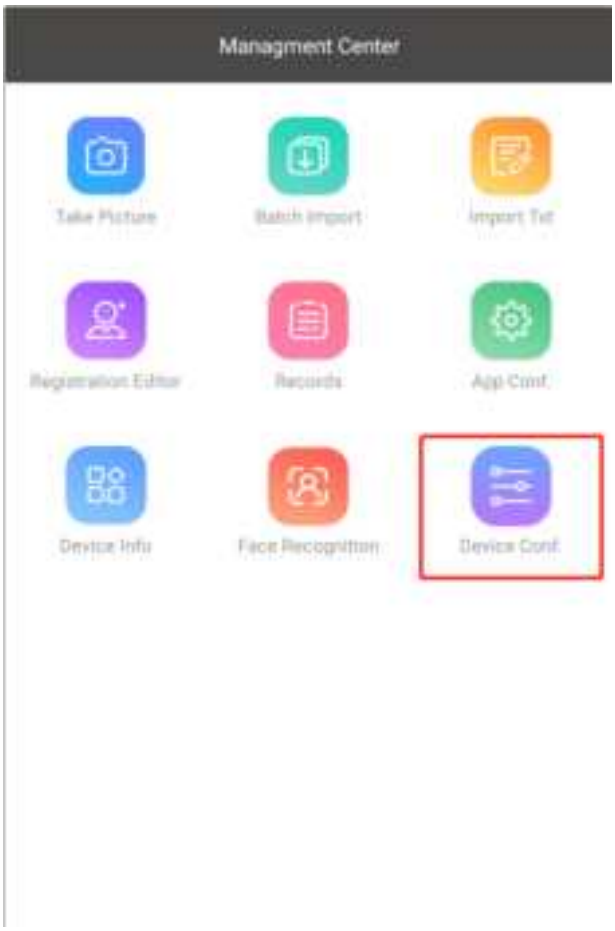


3. Network Settings

This section is for the setup of the terminal's network.

3.1 WLAN Settings

Select WLAN. Choose the preferred WIFI and key in password.


Managment Center
Take Picture
Batch Import
Import Txt
Registration Editor
Records
App Conf
Device Info
Face Recognition
Device Conf


Wi-Fi
On

3.2 Ethernet Settings

Click Ethernet to open the Ethernet connect and set static or dynamic IP.

4. FCC Statement

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this de vice may not cause harmful interference, and (2) this device must accept any interference received, including in terference that may cause undesired operation.
Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not insta lled and used in accordance with the instructions, may cause harmful interference to radio communications. Howe ver, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help important announcement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.