

# USER MANUAL



## FCA-3200

Introducing the FCA-3200, a cutting-edge facial recognition system delivering superior accuracy and ultra-fast processing with advanced anti-spoofing technology. The perfect security solution for modern enterprises. Represents the pinnacle of digital access control for the modern era.



FOLLOW US  
[www.iomotech.com](http://www.iomotech.com)

# Foreword

Dear User:

Thank you for choosing and using IOMO products.

In order to make you better use of this product, please read this manual in detail, follow the steps in the manual, and Save it properly for future reference.

The company is committed to continuously improve the product function, improve the quality of service. The contents and pictures in this manual may be different from the actual product, and the function description may be slightly different according to the specific model. If it is different from the actual product, please refer to the actual product.

Some parts, appearance or functions mentioned in this manual may be subject to copyright. Nothing in this instruction manual may be reproduced or transmitted in any form without the written permission of the Company.

The Company reserves the right to modify the contents of this manual and related product specifications. The contents of this manual are subject to change without prior notice. If you have any doubt, please contact us as soon as possible, we will be happy to serve you, thank you again for using our products.

# Contents

<b>Foreword .....</b>	<b>I</b>
<b>Contents.....</b>	<b>II</b>
<b>1 Product Overview .....</b>	<b>1</b>
1.1 Product Overview .....	1
1.2 Appearance Introduction.....	1
<b>2 Installation instructions.....</b>	<b>3</b>
<b>3 Equipment operation Instructions .....</b>	<b>4</b>
3.1 Device activation .....	4
3.1.1 Device power on and activation.....	4
3.1.2 Select the network connection method .....	5
3.1.3 Management method.....	6
3.1.4 Select application scenarios .....	7
3.2 Recognition interface description .....	9
3.2.1 Identification interface .....	9
3.2.2 Standby mode .....	10
3.2.3 Engineering modeEngineering mode.....	10
3.3 Engineering mode .....	12
3.3.1 Personal management .....	12
3.3.2 Time Plan .....	15
3.3.3 Identify Settings.....	17
3.3.4 Passable Settings.....	20
3.3.5 Scene Mode .....	23
3.3.6 Access record .....	30
3.3.7 Data management .....	31
3.3.8 System Settings.....	35
<b>4 Addendum .....</b>	<b>50</b>
4.1 Appendix 1 Enter personnel photos .....	50
4.2 Appendix 2 Enter the card information.....	52
4.3 Save Appendix 4 Customizing the standby screen .....	53

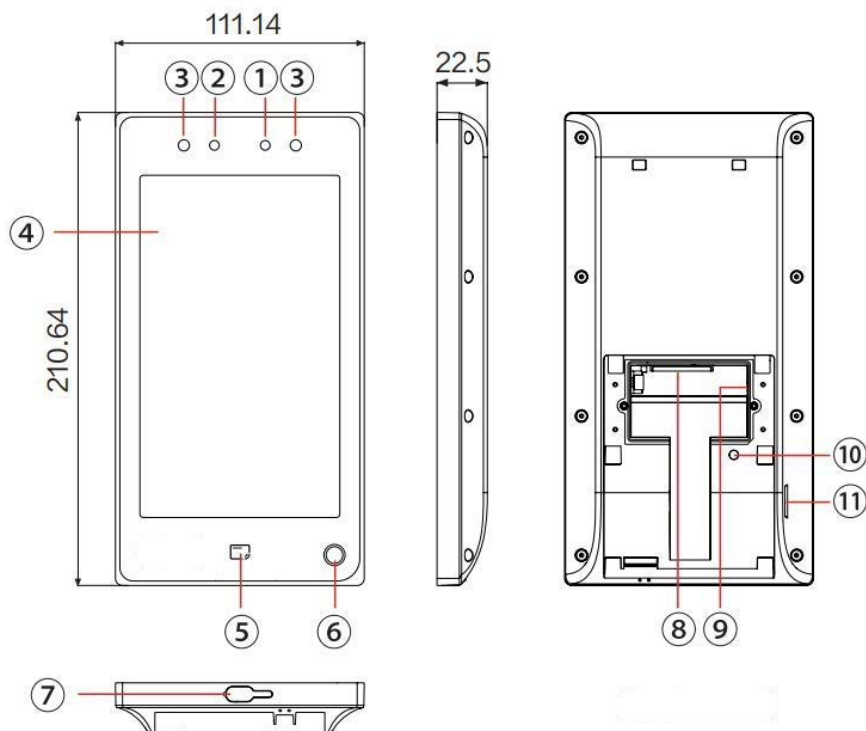
# 1 Product Overview

## 1.1 Product Overview

FCA-3200 is a face recognition class attendance and access control terminal product. There are a variety of models and specifications, and there are differences in temperature measurement, communication methods and so on. The whole series supports face recognition, IC card, password and two-dimensional code and other combination ways for identity verification, can be used in commercial real estate, enterprise building, hotel, government, industrial park, industrial park, campus, small business, construction site, shops and other places.

## 1.2 Appearance Introduction

This section uses the non-temperature measuring model FCA-3200 as an example. The content varies with the model.



No.	Name	Description
1	Visible light camera	Captures visible light images
2	Infrared camera	Captures infrared images
3	Infrared fill light	Provides fill light for the infrared camera
4	Display screen	7-inch multi-touch display screen
5	Card tap area	Users tap their cards here
6	Indicator light	Indicates the access result and power status
7	USB port	A Type C port for connection with USB drives
8	External cable connection	Used for connection to a power source
9	3.5mm headphone jack	Connect external active speakers
10	Tamper prevention button	Prevents disassembly after installation
11	Speaker	Plays audio prompts

# 3 Equipment operation Instructions

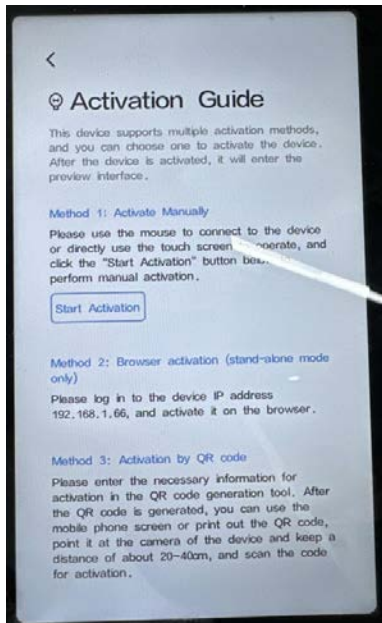
## 3.1 Device activation

### 3.1.1 Device power on and activation

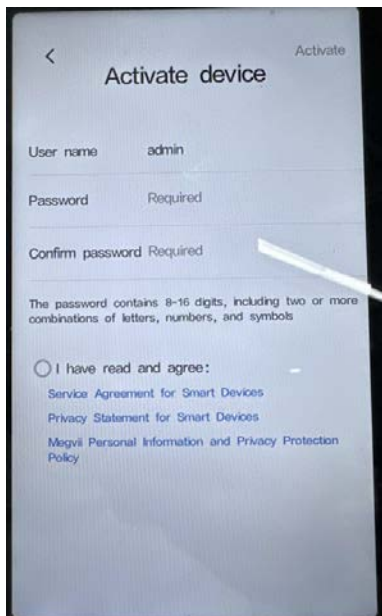
1. The device automatically starts after power-on. The startup screen is as shown in the picture below.



2. Select the device language, support English, simplified Chinese, Traditional Chinese, Thai,Japanese 6 languages.
3. Enter the **【Activation Guide】** nterface, you can choose the activation method according to the wizard prompts.



4. Take **【Method1: Activate Manually】** as an example, click **【Start Activation】**, enter the password, and confirm the password.

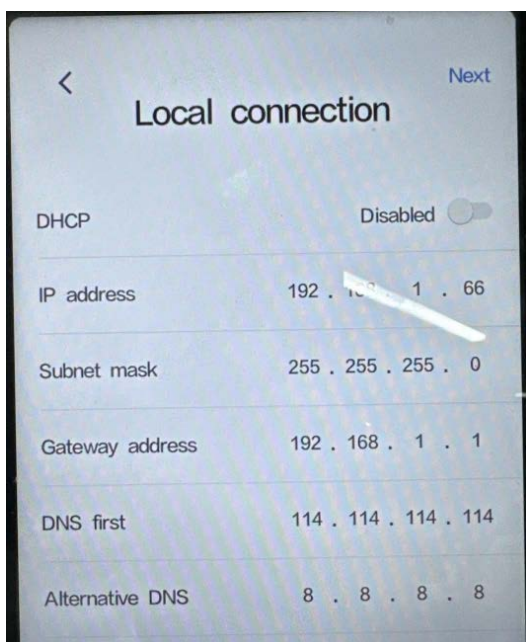


5. Read and check "《Service Agreement for Smart Devices》、《Privacy Statement for Smart Devices》《Megvii Personal information and Privacy Protection》” **【I have read and agree】** .
6. Click **【active】**, to finish creating the password and start setting up the network connection.

### 3.1.2 Select the network connection method

Select **【Local connection】** or **【wifi connection】** as needed.

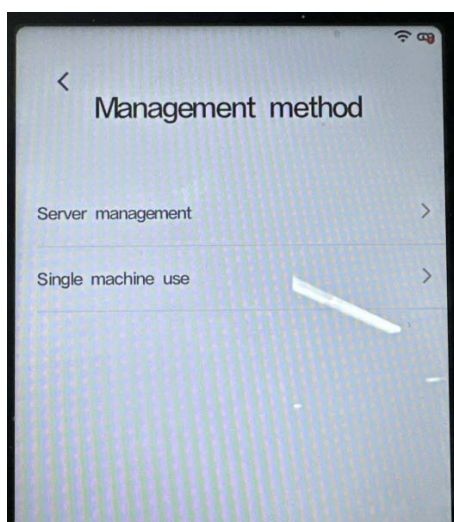
1. If you select **【Local connection】**, click **【Next】**, after the setting is complete to enter the **【wificonnection】** interface, and then click **【Skip】** .



2. If you select [wifi connection], click [Next] on the [Local connection] interface to set wifi.
3. If you select [4G settings], click [Next] on the [wifi connection] interface to perform 4G Settings.
4. After the Settings are complete, start to configure the Management method.

### 3.1.3 Management method

You can choose from Server management【Server management】、【Single machine useSingle machine use】.



**Note:**

If you need to switch the management mode, you need to manually restore factory Settings and then select again, the system will clear all user data, if you need to reuse, please backup in advance.



## Single machine use

If only local Single machine use is required, you can directly click [Single machine use], confirm and set [User authorization], as shown in the figure below. After the authorization is completed, click [Next] to enter the next selection of use scenario.

16:07

< New person Next

---

☐ Consent to Personal Privacy Protection Policy as follows

[Privacy Policy \(Template\)](#)

Company Name:

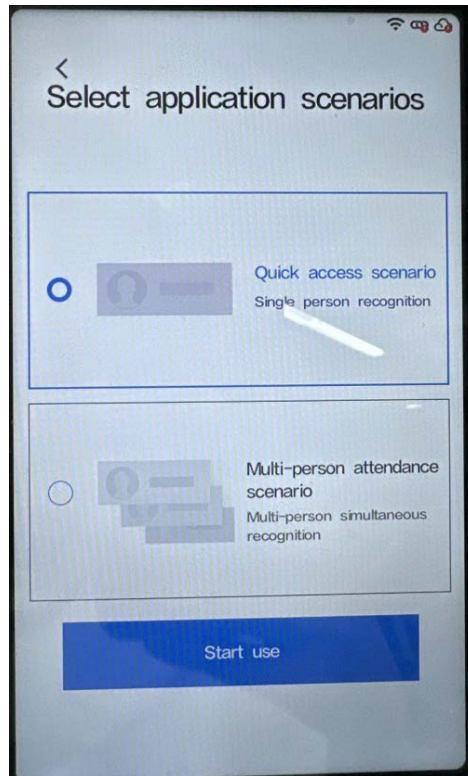
- 1

contact details:

- 1

### 3.1.4 Select application scenarios

Select from: **【Quick access scenario】** or **【Multi-person attendance scenario】**. After the selection is complete, click [Start use] to use the device normally. You can enter [Engineering mode] to set relevant Settings according to your needs.



## Quick access scenario

Single access is recommended. Only one person at a time, often used in gate airport scenery.

## Multi-person attendance scenario

It can meet the large flow of people and fast passage scenario. In the case of multiple people on the same screen, it can be quickly identified, and is mostly used for the attendance clock at the door of the company.

## 3.2 Recognition interface description

### 3.2.1 Identification interface

- Display the current time, real-time picture, personnel identification results, equipment location and other information.



- Click the screen to display the current network connection status, Wi-Fi connection status, server connection status and other information.



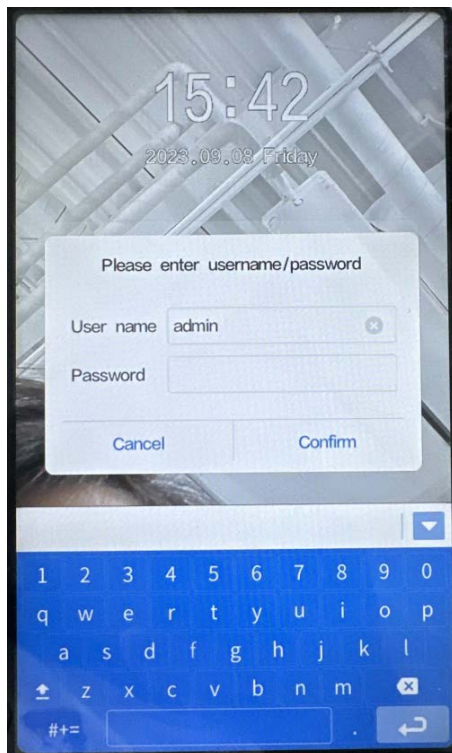
### 3.2.2 Standby mode



- If the standby function is enabled, when the no operation time exceeds the set standby time and no face is detected, it will automatically enter the standby mode
- You can set it in "[Engineering mode] > [System Settings] > [Personality Settings]".

### 3.2.3 Engineering mode

On the screen, press and hold the blank position on the screen and wait for the password prompt box to pop up.



Enter the activation password and confirm the password to enter the Engineering mode.



If the system detects that the operator has administrator permission through face recognition at this time, the system will skip the password input link and enter the Engineering mode directly.

In Engineering mode, you can set the device. For details, see [Engineering mode](#)

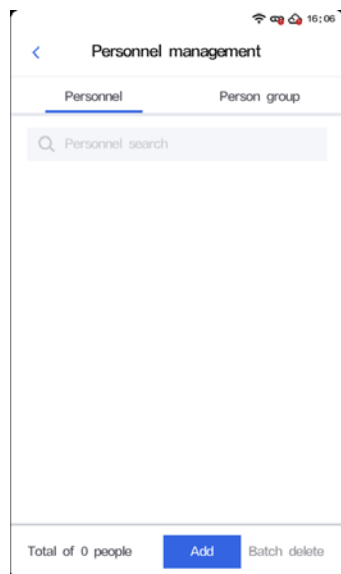
## 3.3 Engineering mode

Engineering mode is mainly for the customer's operation and maintenance management and other technical personnel to configure the face recognition machine.

### 3.3.1 Personal management

If and only if the management mode is [Single machine use], the user can add, remove, modify personnel or personnel groups on the device.

Note: When the device is connected to the cloud or Server management, the data source is delivered from the cloud to ensure data consistency.



#### 3.3.1.1 Creation Personnel

Available only under [Single machine use], with the People management feature, you can add employees and set administrator rights, etc.

#### Steps

1. Go to [Engineering mode] and select [Person management].
2. Select the [Personnel] TAB and click [Add].
3. Read and check the Personal Privacy Protection Policy.

Consent to Personal Privacy Protection Policy as follows

[Privacy Policy \(Template\)](#)

Company Name:  
1

contact details:  
1

4. Click [Next] to start adding people as shown in the picture below.

Name Please enter Required

Serial number Please enter

Photo >

Authentication method: face/card

Set card No. Please set >

Other info

Password Please set >

phone Please enter

Person group 1 groups selected Required >

Admin privileges Close

5. According to the prompts, set the parameter items, see the table below for details.

argument	Instructions
Name	(Required) Repeatable.
Serial number	(optional) Non-repeatable; If you do not fill in, the system will automatically generate.
Photo	(Optional) Click to enter the face photo capture page. For related operations, please refer to “ <a href="#">1.1 Appendix 1 Enter personnel photos</a> ”.
Set card No.	(Optional) cannot be repeated. The user can choose to enter the card number manually or read it automatically after swiping the card in the swipe area at the bottom of the screen. See "Appendix 2 Input Card Information" “ <a href="#">4.2 Appendix 2 Enter the card information</a> ”.
Password	(Optional) Indicates the authentication password. Value: 4-6 digits.
Phone	Enter the person's correct cell phone number.

Person group	(Required) Select a person group to manage people in groups, with "System Default Group" selected by default. For details about how to create a staff group, see <a href="#">3.3.1.2 Create a Personnel Group</a> .
Admin privileges	(Optional) This parameter is enabled, indicating that current personnel have administrator rights on the device and are allowed to enter Engineering mode and set related parameters of the device. Off: indicates that a common user has only access control rights.

- After parameters are configured, click [Save]. The added people are displayed in the people list.
- Optional action.

**Find Personnel:** In the search box on the [Personnel] TAB, enter the initials of the personnel for a quick lookup, with fuzzy search supported.。

**Editing personnel:** Click the personnel name to enter the editing interface to edit.

**delete Personnel:** On the "Personnel" TAB, click "Batch delete", select "personnel", and click "Batch delete" again.

### 3.3.1.2 Create a Personnel Group

Available only under [Single machine use], personnel group management is easy for users to operate.

#### Steps

- Go to [Engineering mode] and select [People Management].
- Select the [Person group] TAB and click [Add]. The following interface is displayed. "System Default Group" has been created by default.

- According to the prompts, set the parameter items, see the following table for details.

Parameters	Instructions
Name	(Required) Enter a person group name.
Default plan	(Optional) Select an access control time plan. By default, the system has created a Default time plan, that is, full time access. If you want to select another time plan, you need to create a time plan. For details, see <a href="#">Time Plan</a>



4. After parameter configuration, click [Save]. The added people group is displayed in the People Group list.
5. Optional action.
6. **Find a Person group:** In the search box of the [Person Group] TAB, enter the name of the person group for quick lookup, fuzzy search is supported  
**Edit staff group:** Click the name of the group, enter the editing interface to edit.  
**delete the personnel group:** On the "Person group" TAB, click "Batch delete", check the "personnel group", and click "Batch delete" again.

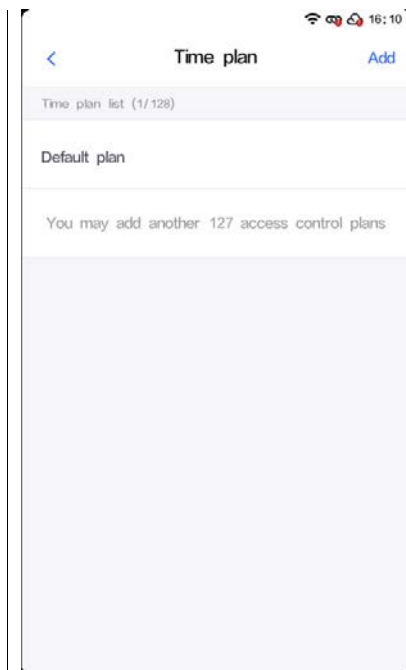
**Please note::**

- The list of people groups is arranged in the order they were added, with the most recently added people group coming last.
- Delete the personnel group. If there are still personnel in the personnel group, it will be automatically transferred to the "System Default Group".

## 3.3.2 Time Plan

If and only if the management mode is [Single machine use], the user can add, remove, or modify a time schedule on the device. When the device is connected to the cloud or Server management, the data source is delivered from the cloud to ensure data consistency.

Add an access control period for the user. During this period, the user's access control permission is valid. The device supports the creation of weekly plans and time plans for special periods. The device supports a maximum of 128 access control time plans (including default time plans).



### 3.3.2.1 Create time plan

#### Steps

1. Enter **【Engineering mode】** and select **【Schedule】**, Default schedule has been created by default, that is, the system uses all time.

2. Click [Add], the following interface is displayed.

3. According to the prompts, set the plan name and set the weekly plan.

Time slot setting instructions:

Set the time period from Monday to Sunday respectively, and click to enter the "Time Period Setting" interface. 8 time slots are supported, and each time slot is off by default.

- Click "On", then the "Edit" button will be displayed under the time period, click to start setting the time plan for the current time period.
- Repeat the above operations to set other time ranges, and click "Save" after the Settings are complete.
- You can select [On] or [off] time schedule as needed.
- The end time of each time segment must be longer than the start time..

For details about how to set a special time schedule, see Creating a Special Time Schedule.

After setting, click [Save] and the schedule will be displayed in the schedule list.

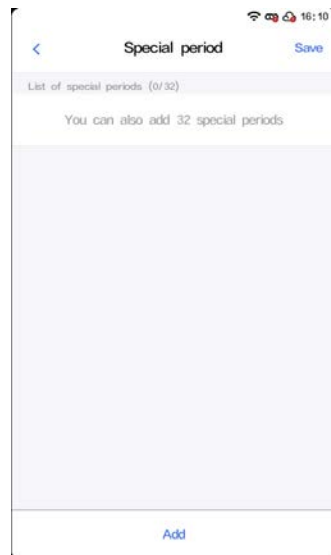
Optional action.

Edit/Delete: On the Schedule screen, click the schedule name to edit/delete the schedule..

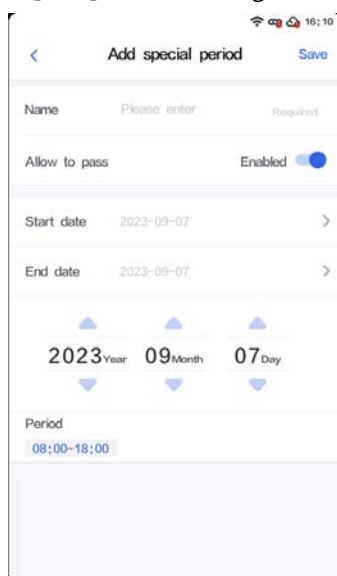
### 3.3.2.2 Create a special time schedule

#### Steps

1. On the "Add Access Control Plan" interface, click "Special Period" and then click "Add" to display the following interface. The system supports 32 holiday plans, and each plan supports 8 holiday periods.



2. Click [Add] to start adding the access control plan for the special period.



3. According to the prompts, enter the name of the special period, choose whether to pass, set the start and end date and related period Settings.
4. After setting, click [Save]. You can return to the interface to check.
5. Optional operation.  
Edit/Delete: Click on the name of a special time period to perform an edit/delete operation.

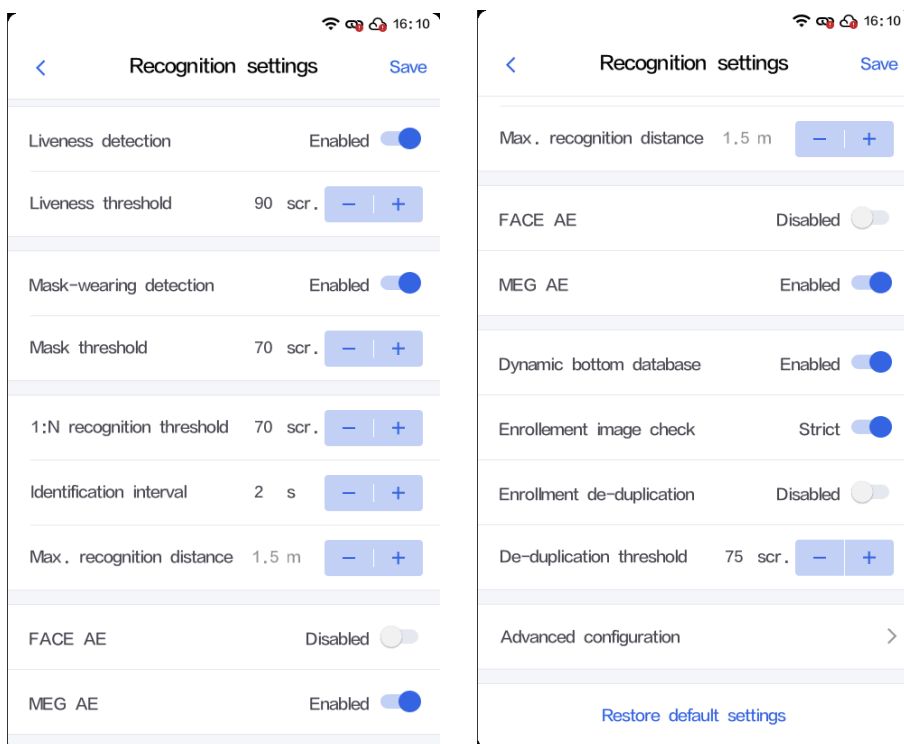
### 3.3.3 Identify Settings

You can configure face recognition parameters here.

#### 3.3.3.1 Basic Configuration

##### Steps

1. Go to [Engineering mode] and select [Recognition Settings].



2. Follow the prompts to set the parameter items, see the table below for details.

Parameters	Instructions
Live testing	On by default. If this function is disabled, the vivisection detection function is not used, and the vivisection threshold cannot be set.
Living body threshold	Can be set when the vivisection switch is on. The default is 90. The selectable range is 0 to 100, the higher the threshold setting, the higher the safety factor (but 100 is not recommended, it may cause unrecognition)
Wear a mask for identification	On by default. If the mask recognition switch is off, the mask recognition threshold cannot be set, and the mask recognition function is not enabled. The higher the threshold, the higher the safety factor.
Mask Threshold	Mask identification switch can be set when turned on. The default is 70. The optional range is 0 to 100. 100 is not recommended as it may cause unrecognition. The higher the threshold, the higher the safety factor.
1:N	The default is 70. The value ranges from 0 to 100. The higher the threshold setting, the higher the safety factor. You are not advised to set the value to 100, which may cause unrecognition.
Recognition interval	Used to set the time interval for the second face recognition. Default 2s.
Maximum recognition distance	Represents the maximum distance the device can recognize. The value ranges from 0.5m to 2m. Note: When the management mode is set to Server management, only 1/1.5/2 m can be set.

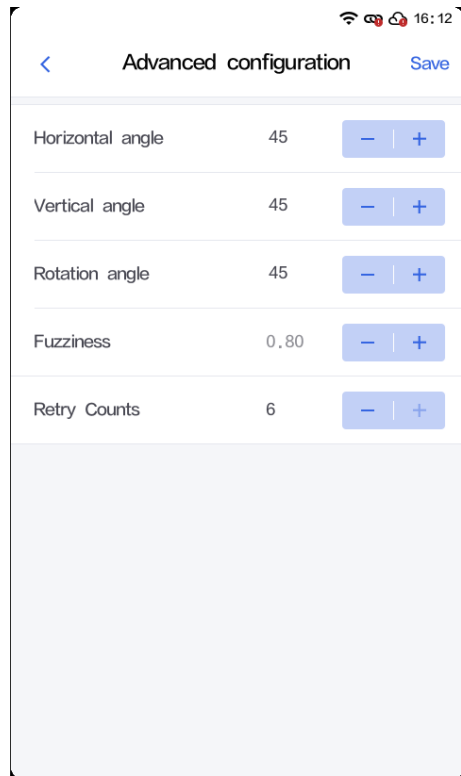
FACE AE	Used for face gain, increase face brightness, mainly solve the problem of face darkening under backlight. [On] : After starting, the device restarts and the function takes effect. [Off] : After the device is turned off, the face gain function is not used.
MEG AE	
Dynamic base library	Set [on] to update the bottom gallery photo based on the captured photo.
Incoming image detection	Loose: the storage image quality requirements are low; Strict: the quality requirements of the stored image are high. Note: The default for Single machine use is "strict"; The default is "loose" when the device is connected to the cloud.
Load the storage to remove the weight	Add personnel, when entering photos, do 1:N check, if there are duplicate personnel in the bottom library, return the error code, if there is no successful storage.
The threshold of reloading in the repository	Default 75. The threshold is modifiable.

3. For Advanced Configuration, refer to Advanced Configuration.
4. Click [Save] when the parameters are configured.
5. Optional action.
  - To restore the default Settings, click Restore Default Settings below.

### 3.3.3.2 Advanced Settings

#### Steps

1. In the "Setup Settings" interface, click "Advanced Configuration" to display the following interface.



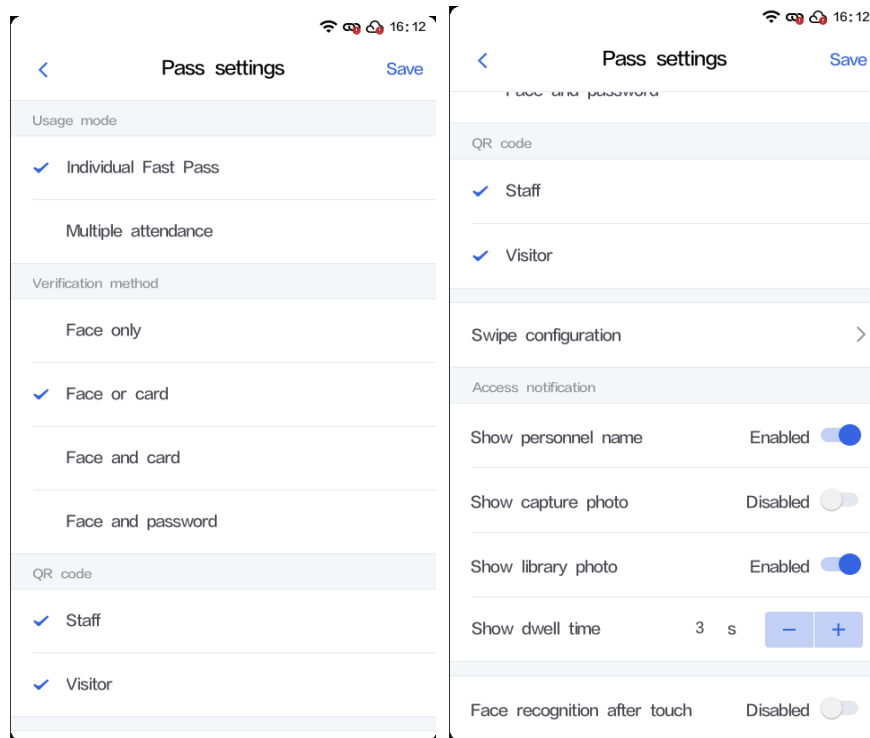
2. According to the prompts, set the parameter items, see the following table for details.

Parameters	Instructions
Horizontal Angle	Optional range is 0~90 (degrees), the higher the value indicates that the face can be recognized under a larger horizontal Angle, the recommended value is: 45.
Vertical Angle	Optional range is 0~90 (degrees), the higher the value indicates that the face can be recognized under a larger Vertical Angle, the recommended value is: 45.
Rotation Angle	Optional range is 0~90 (degrees), the higher the value indicates that the face can be recognized under a larger Rotation Angle, the recommended value is: 45.
Fuzziness	The range of options is 0-1, with higher values indicating more blurred faces, The recommended value is 0.8.
Retry Counts	Default 6, retry times of strangers, supported on demand. The values are: 3,4,5,6.

3. After parameters are configured, click [Save].

### 3.3.4 Passable Settings

You can set the usage mode of the device, the authentication method for personnel passing, whether to use the QR code pass-through function of employees or visitors, and the pass-through prompt setting of the device identification interface when personnel passing.



### 3.3.4.1 Set the usage mode

#### Steps

1. Go to [Engineering mode] and select [Access Settings].
2. Select the usage mode.
3. Click [Save] or make other Settings.

Note:

- Single fast passage: Suitable for fast passage scenes, only one person at a time, often used in gate airport scenes. All authentication modes are supported.
- Multi-person attendance: Suitable for multi-person attendance scenarios, it can meet the large traffic and fast passage scenarios, and can be quickly identified when multiple people are on the same screen. Authentication mode supports [face only] [face or swipe] card.

### 3.3.4.2 Set authentication mode

#### Steps

1. Go to [Engineering mode] and select [Access Settings].
2. Select the authentication mode.
3. Click [Save] or make other Settings.

Note:

- [single quick pass] under the authentication mode is fully supported, the default [face or swipe card], support the choice [face only], [face or swipe card], [face and swipe card],[face and password].

- Under [multi-person attendance], the authentication mode supports [face only], [face or swipe card], and the default is [face or swipe card].

### 3.3.4.3 Configure QR code function

After checking, employees or visitors can pass by QR code.

#### Steps

1. Go to [Engineering mode] and select [Access Settings].
2. Check the user of QR code function, default employees, visitors can use the QR code access.
3. Click [Save] or make other Settings.

### 3.3.4.4 Configure swipe mode

The device supports the use of regular cards (read only physical card numbers), MF cards, and regular CPU cards to encrypt content.

#### Steps

1. Go to [Engineering mode] and select [Access Settings].
2. Click [Swipe Configuration] to enter the swipe configuration interface, select the card reading mode (support read-only physical card number (default), encrypted Mifare, ordinary CPU card encryption content) and read card order (positive order, reverse order (default)).
3. After the configuration is complete, click [Save] or make other Settings.

### 3.3.4.5 Configure Access Tips

Passing prompt: When the face recognition machine is used for face recognition, the recognition result display item displayed on the interface is recognized.

#### Steps

1. Go to [Engineering mode] and select [Access Settings].
2. Set the related function of traffic prompt [on] or [Off].

argument	Instructions
Show person name	<p>[On] : When passing, the identification interface displays the name of the person.</p> <p>[Off] : When passing, the identification interface does not display the name of the person.</p>



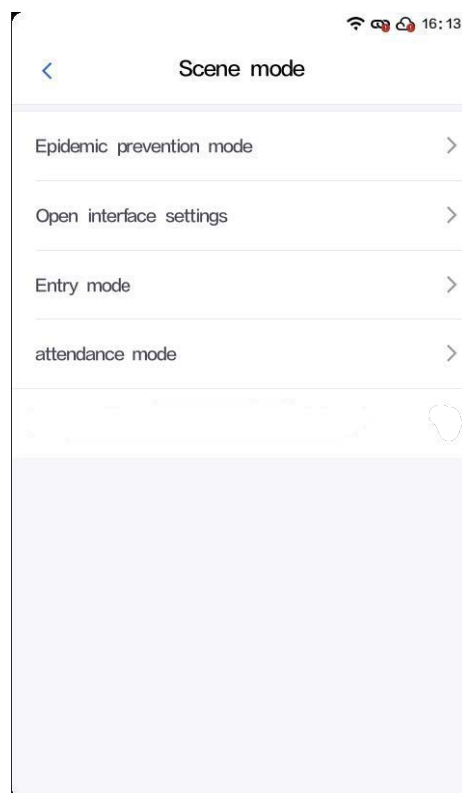
The snap photo is displayed	<p>[On] : When passing, the recognition interface displays the current snap photo.</p> <p>[Off] : The capture image is not displayed on the recognition interface during traffic.</p>
Displays staff library photos	<p>[On] : When passing, the identification interface displays the entered base photo.</p> <p>[Off] : When passing, the identification interface does not display the bottom library picture.</p>
Display residence time	Default 3 seconds.
Face recognition after touch	<p>[Open] : When passing, it is necessary to manually trigger the recognition button, and face recognition is carried out after triggering.</p> <p>[Off] : The face can be recognized without triggering the recognition button.</p>

Note: "Show snap photo" and "show the bottom library photo" function mutually exclusive, if the passable, need to show the face picture, just open a switch can be; If there is no need to display the face picture, the two switches can be [off].

3. Click [Save] or make other Settings.

### 3.3.5 Scene Mode

In scenario mode, you can enable related services and set related parameters based on different scenarios.

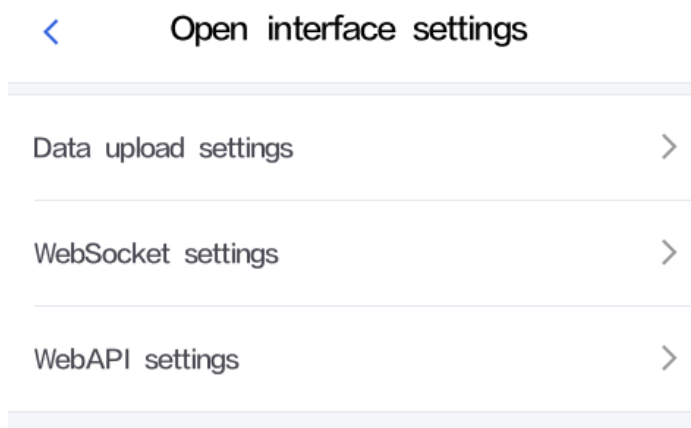


### 3.3.5.2 Open interface Settings

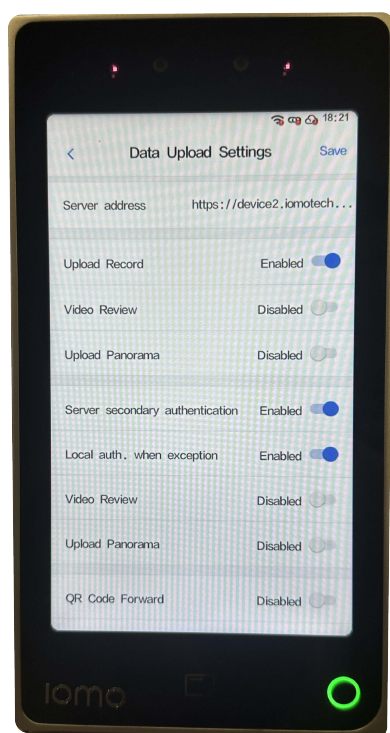
The open interface is used to set the server address for data reporting and WebSocket and WebApi related Settings. If the device management mode is set to Server management, WebSocket is not supported.

#### Steps

1. Enter [Engineering mode] and choose [Scene Mode] > [Open Interface Settings]. The following interface is displayed.



- To configure the data reporting address, select [Data Reporting Settings]. The following interface is displayed.



- Set parameters as prompted. For details, see the following table.

Parameters	Instructions
Server address	IP address of the third-party server. After the IP address is configured, the device uploads all traffic records to the third-party server. (No history will be uploaded, only the records after this service is enabled).
Server secondary authentication	Enable indicates that the secondary authentication function of the server is enabled. You can also set whether to enable Local Authentication when the network is abnormal.
Transparent QR Code transmission	[On] The QR code transparent transmission function is supported.

- To configure WebSocket, select [WebSocket Settings]. The following interface is displayed.

5. According to the prompts, set the parameter items, see the following table for details

Parameters	Instructions
Server address	Please fill in the server address.
SSL Encryption	[Enable] The ssl encryption function takes effect.

6. If you need to configure WebAPI, select [WebApi Settings], the following interface is displayed.

7. Set "Enable HTTPS" to [On]  
8. Click [Save].

### 3.3.5.3 Enter Mode

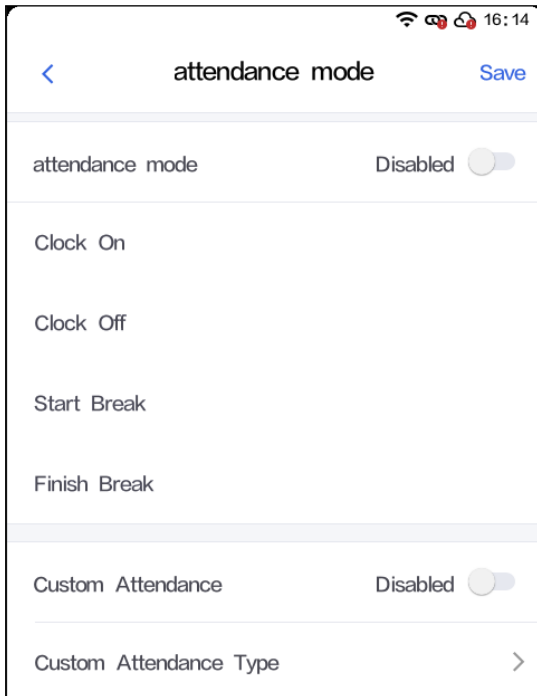
Input mode currently only supports the use of single webapi access to the third-party platform, in this mode, support the face access control integrated machine to obtain personnel photos, personnel information after filling in, report the personnel information to the platform side for storage. It is mainly applicable to the campus, enterprise, office environment, new employees or new employees on the scene to enter the bottom database scene.

Note:

Input server address: The server address reported after manually entering the information of local collection personnel. It can be different from the server address of the data reporting (secondary authentication) interface.


### 3.3.5.4 Attendance mode

Only single mode can be turned on, multiplayer mode attendance mode is not available, automatically deactivated after switching. In the attendance mode, you can record the attendance status of people in different periods. The system supports 4 fixed attendance status and 3 customized attendance status: work, work, start rest, end rest.



### Steps

1. Enter [Engineering mode] and choose [Scene Mode] > [Attendance Mode]. The following interface is displayed.
2. Turn on [Attendance Mode] or customize the attendance type according to the actual scenario.  
Parameter description:

PARAMETERS	Instructions
Attendance mode	<p>[Attendance mode] After the switch is on, enter the attendance mode, which can record the attendance status of people at different times. The system supports the following four attendance status. Function description: The use of this function requires the personnel to enter the warehouse first, after the personnel enter the warehouse, if the system is set to the attendance mode, then when the personnel face recognition, the device identification interface displays the attendance status, you can choose the custom attendance status or the system fixed attendance status, at the same time, the Web side of the access record shows the attendance type.</p>  <p>Go TO Work after work Start taking breaks Ending the Break</p>
Customize your attendance	<p>Customize the type of attendance</p> <p><b>【 Attendance mode 】</b> After the switch is turned on, enter the attendance mode. The system supports custom attendance types, such as afternoon tea, meeting and other attendance types.</p>

3. Click [Save] after the setting is complete.

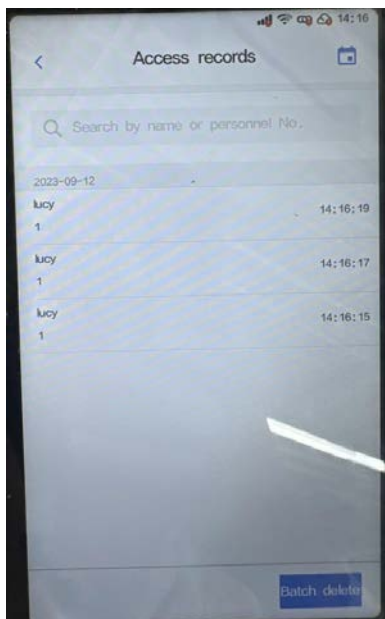
### 3.3.6 Access record

You can search for the personnel log by the personnel name, number, or time, and support the configuration of whether to display the traffic failure record. The traffic records list displays the traffic records of all personnel. Traffic records are arranged in reverse chronological order and displayed separately according to daily records.

#### 3.3.6.1 Manage records

##### Steps

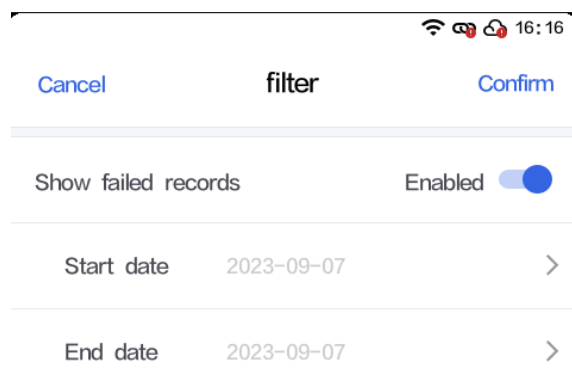
1. Enter [Engineering mode] and select [Traffic Record]. The following interface is displayed.



2. You can query or delete the traffic record. The detailed operation is as follows:

- View access records by name or person number  
Just type in the name or person number in the search box.
- View access records by date

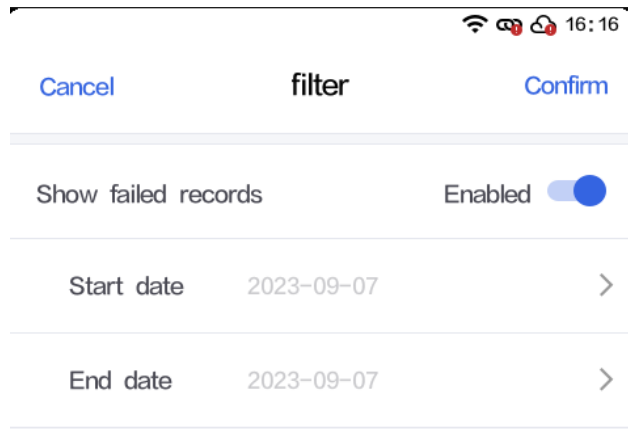
Click the "📅" in the upper right corner of the "Traffic Record" page, set the start and end date, and click "Confirm".



- Set whether to display the traffic failure record

Depending on your needs, you can choose whether the list of traffic records displays traffic failure records.

To display the list of traffic failure, click "  " in the upper right corner of the page of [Traffic record], and then set the switch of [Display traffic failure record] to [On].



- Delete traffic record

In the "traffic record" page, click "Batch selection", then select the traffic record to be deleted, support all selection, after the check is completed, click "Batch delete", after the second confirmation, click "confirm".

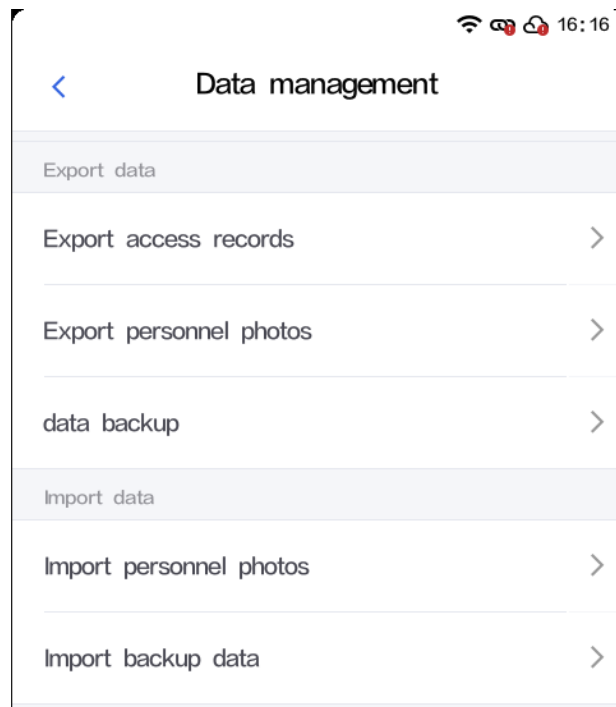
### 3.3.7 Data management

The module implements the import and export function of all user data:

- Export data: support to export access records, export personnel photos, export equipment parameters, data backup.
- Import data: support to import personnel photos, import equipment parameters, import machine data.

Note: When the device management mode is [Server management], only data, and traffic records, and personnel photos can be exported.





### 3.3.7.1 Connect USB flash drive

To import and export data, connect the USB flash drive or other storage device to an external storage device through the USB Type-C port. After the connection is successful, the device detects the USB flash drive or other storage device and can import or export data.

Note:




- If the device is not inserted or fails to read the USB flash drive or other storage device, the font color of the imported data part and the exported data part is gray, indicating that it is unavailable. In this case, you need to click [Redetect] to read the data again.
- After successful detection, all functions of importing and exporting data are available.
- If you use Server management, you cannot export or import personnel photos or backup system data.

### 3.3.7.2 Exporting Data

#### Steps

1. Go to [Engineering mode] and select [Data Management].
2. Connect USB flash drive, refer to Connect USB Flash Drive for details.
3. After the USB drive is successfully connected, select the type of data you want to export.
  1. The device supports the export of traffic records, personnel photos, and data backup.
  2. When you choose to export access records and personnel photos, you need to confirm the privacy security, and export can be supported after confirmation.
  3. Among them, when backing up data, you can select [Device parameters] or [personnel information], and multiple choices are supported.
4. Click [Confirm] to start exporting data. When the export is complete, prompt "Done".

## Instructions for exporting data

Data type	Export content and export path	Remarks
Access records	<ul style="list-style-type: none"> <li>Export contents <ul style="list-style-type: none"> <li>Access record table (named Access record time range, file format is ".xls ");</li> <li>Capture photo (named capture time, file format ".jpg ")</li> </ul> </li> <li>Export path <ul style="list-style-type: none"> <li>The event_log folder in the root directory of the USB flash drive contains the traffic record table and snapshot images.</li> </ul> </li> </ul> <div>  event_log  event_log1 </div>	If the external storage device retains the last exported data, event_log/event_log2 is incremented... .
Personnel photos	<ul style="list-style-type: none"> <li>Export content <ul style="list-style-type: none"> <li>Personnel photo (named as personnel name +personnel number, file format is ".jpg ")</li> </ul> </li> <li>Export path Usb flash drive root →person_pic</li> </ul> <div>  person_pic </div>	<ul style="list-style-type: none"> <li>The last exported data (if any) will be overwritten when exported. Exercise caution when performing this operation.</li> <li>The personnel number must be unique. Otherwise, the import fails.</li> </ul>
Equipment parameters	<ul style="list-style-type: none"> <li>Exported content <ul style="list-style-type: none"> <li>Access control parameters: Related to the configuration of the door lock, door status sensor, and authentication mode.</li> <li>Network parameters: Related to local Ethernet and Wi-Fi configurations.</li> <li>Communication parameters: related configurations of Wiegand.</li> <li>Face parameters: related to binocular, face, recognition threshold, living threshold configuration.</li> </ul> </li> <li>Export path Usb flash drive root →device_data</li> </ul>	The last exported data (if any) will be overwritten when exported. Exercise caution when performing this operation.

### 3.3.7.3 Importing Data

#### Steps

1. Enter Engineering mode and select Data Management.

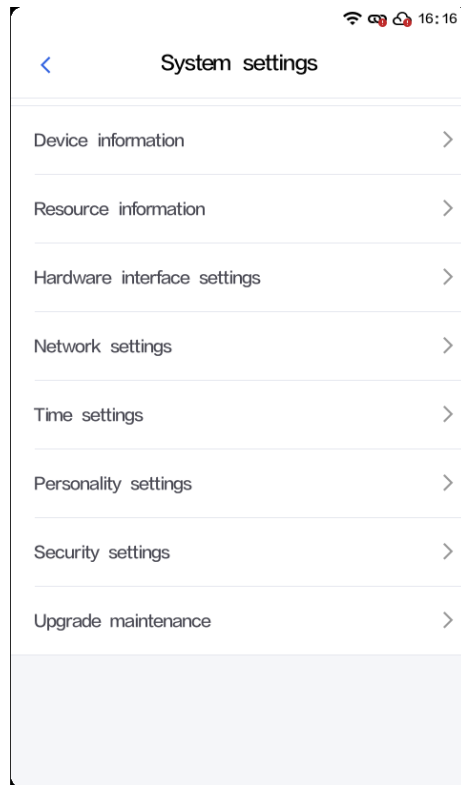
2. Connect USB flash drive, refer to Connect USB Flash Drive for details.
3. After the USB drive is successfully connected, select the type of data you want to import. The device supports the import of personnel photos, device parameters, and machine data.
4. After the privacy security confirmation, the data import begins. When you select [Import Backup data], you do not need to perform the privacy security confirmation.
5. Start importing data. After the import is complete, the prompt "Finish" is displayed, and the device will restart. Click [Cancel] at this time, then the imported data cannot take effect immediately.

Note: When selecting [Import Backup Data], you can select [Device parameters] or [Personnel information] to import. Multiple choices are supported.

## Import data description

Data type	Import content	Remarks
Personnel photos	<ul style="list-style-type: none"> <li>● Import content <ul style="list-style-type: none"> <li>■ Photo naming rules: Person name/person number</li> <li>■ File reading path: USB drive root directory→ person_pic</li> <li>■ Photo format: jpg, png, bmp</li> </ul> </li> </ul>	When there is no matching file to import, the message "Personnel photo folder not detected" is displayed.
Backup data	<ul style="list-style-type: none"> <li>● Import content <ul style="list-style-type: none"> <li>■ device_dataFile reading path: USB flash drive root directory →device_data</li> </ul> </li> </ul>	The device automatically reads the files stored in the USB flash drive or other storage device, imports the files, and deletes the original data.

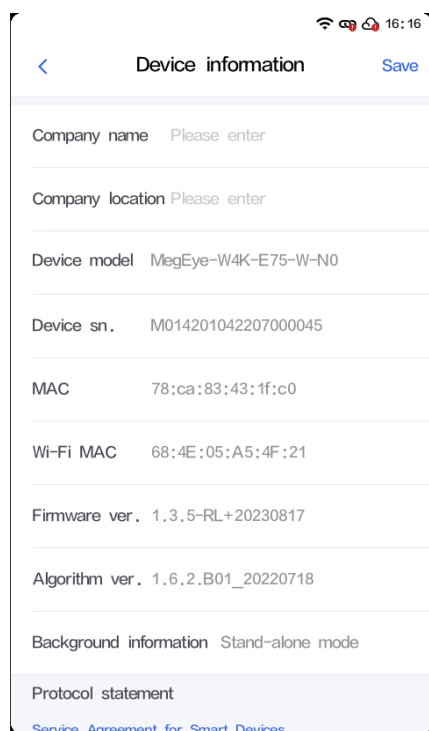
### 3.3.8 System Settings



#### 3.3.8.1 View device information

##### Steps

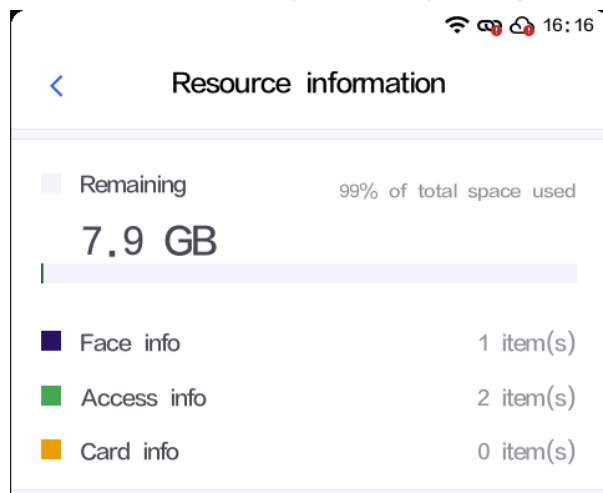
1. Go to [Engineering mode] and choose [System Settings] > [Device Info]. The following page is displayed.



2. You can view the device model, device serial number and other related device information.
3. At the same time, you can also set the [company name] and [company location] displayed on the recognition interface, and click [Save] after setting.

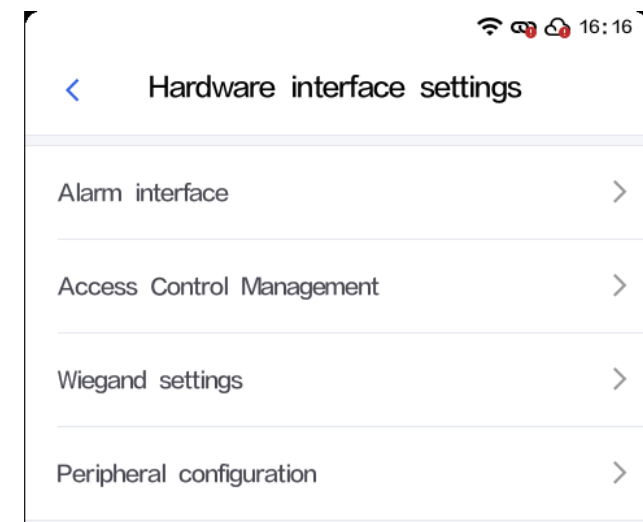
### 3.3.8.2 View the resource usage

To view the resource usage, enter Engineering mode and choose System Settings > Resource Usage.



### 3.3.8.3 Hardware Interface Settings

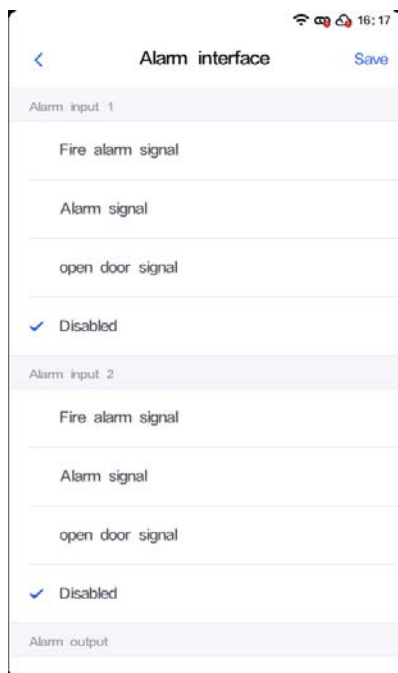
Hardware interface Settings are mainly used to set the Wiegand, alarm interface and access control Settings, and peripheral configuration.



#### Alarm interface

For linkage alarm, follow the steps below:

1. Enter [Engineering mode] and choose [System Settings] > [Hardware Interface Settings] > [Alarm interface]. The system displays the following interface.

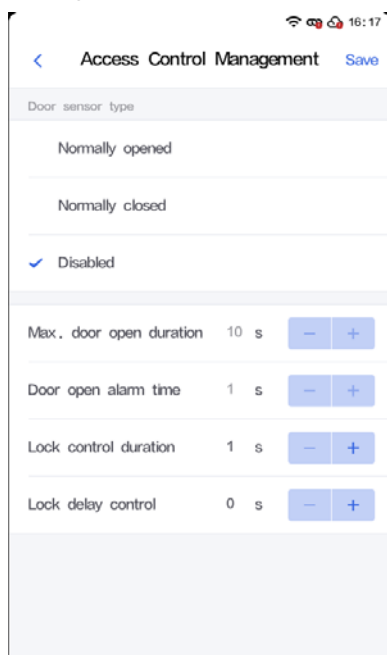


2. Set the [alarm input 1] signal as needed.
3. Set the [alarm input 2] signal as needed.
4. Set the [alarm output] signal as needed.
5. When the Settings are complete, click [Save].

## Access control Settings

The main is to configure the door lock control and door opening.

1. Enter [Engineering mode] and choose [System Settings] > [Hardware Interface Settings] > [Access Control Settings]. The following interface is displayed



2. Set the parameters as required, see the following table for details.

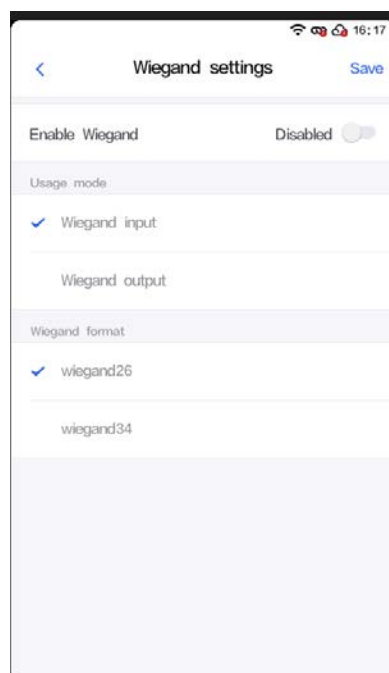
Parameters	Instructions
Type of door magnet	Used to determine the opening and closing state of the door. If the electric lock supports the door status signal, it can be connected to the device. The common type of door status sensor is normally closed. If it is not supported, select Disable (default).
Maximum open time	Indicates the door opening timeout alarm threshold. When the door opening time exceeds the set time, the device will report alarm information and support linkage alarm output. The value ranges from 1 to 255 seconds
Lock control duration	Indicates the operation time of the door unlocking, that is, during this time period, the door is always open. Value: 1 to 60 seconds
Delayed door lock control	After setting the time, after the identification is passed, it will wait for a few hours before opening the door.
Open the door alarm time	If 0s is configured, the alarm signal continues until the access control is closed.

3. After setting, click [Save].

## Wiegand Settings

To use Weigand, follow these steps:

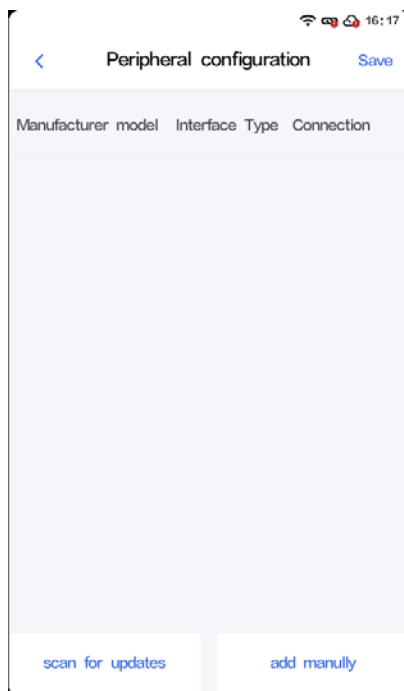
1. Go to [Engineering mode] and select [System Settings] > [Hardware Interface Settings] > [Wiegand Settings]. The following interface is displayed.



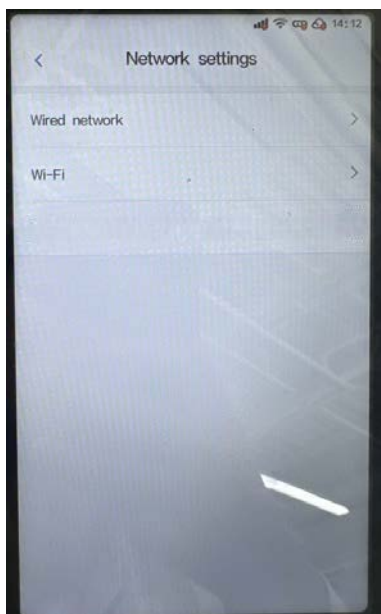
2. Set [On Wiegand] to [On].
3. Select [Use Mode].
4. Select [Wiegand Format].
5. If "Use Mode" is set to [Wiegand Output], you need to set [Output content].
6. After setting, click [Save].

## Peripheral configuration

After inserting the two-dimensional code reading head module, the model can be identified and adapted. You can choose "scan and update" or "manually add" (as shown in the picture on the left), and the picture on the right shows the display result when "manually add".



### 3.3.8.4 Network Settings



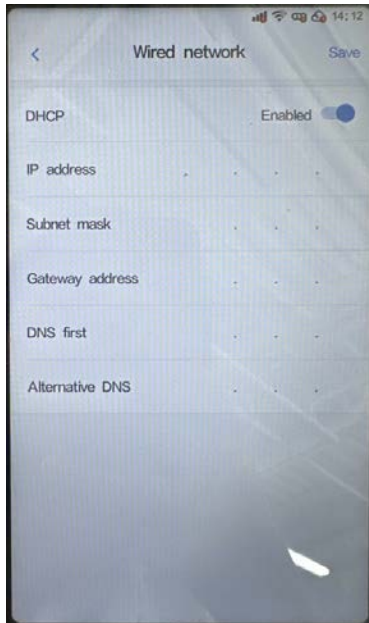
#### 3.3.8.4.1 Configuring Wired network

A local connection requires connecting devices using a network cable.

#### Steps

1. Go to [Engineering mode] and choose [System Settings] > [Network Settings] > [Wired Network]. The following interface is displayed.





2. Set the related parameters as prompted.

Tips:

If the router supports DHCP, you can enable DHCP and the network automatically assigns network information. The default IP address is 192.168.1.66. The default gateway is 255.255.255.0.

3. When the parameters are set, click [Connect].

After the connection is successful, the system prompts "Connection success".

#### 3.3.8.4.2 Configure your WiFi network

Wi-Fi is enabled on your device by default.

#### Steps

1. Enter Engineering mode and choose System Settings > Network Settings > WIFI Network. The following interface is displayed.



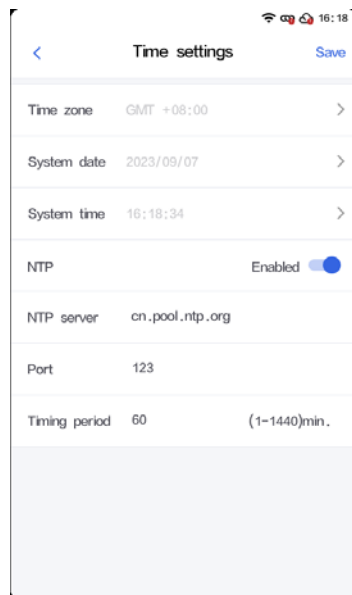
2. Set [Wi-Fi Connection] to [On].
3. Select the available wifi, after entering the Wifi password, click [Join].  
 After the connection is successful, " ✓ " is displayed on the interface for wifi.  
 If you need to view the wifi information, tap the wifi name to view the specific information.  
 If you need to forget the network, long press the wifi name and confirm again to forget the wifi.

### 3.3.8.5 Time configuration

The device supports time configuration, NTP time correction, etc. If the device management mode is Server management, only the time zone can be set. Other parameters are disabled.

#### Steps

1. Go to [Engineering mode] and choose [System Settings] > [Time Configuration]. The following interface is displayed.



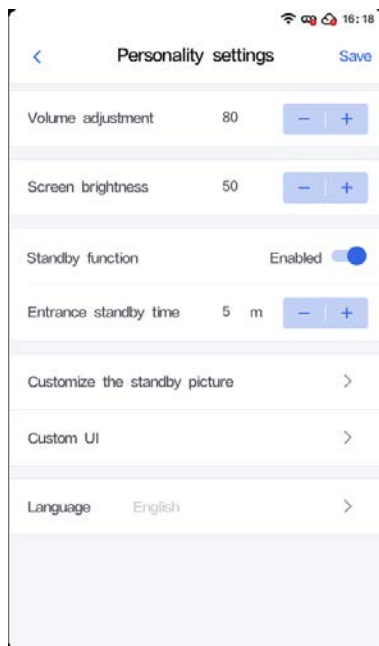
2. Select [Time Zone], [Date], [Time].
3. If NTP calibration is required, set [NTP Settings] to [On], and then set the relevant parameters (NTP server, port, calibration interval).
4. After setting, click [Save].

### 3.3.8.6 Personality Settings

Device supports custom device prompt volume, screen brightness, standby function and standby interface.

#### Steps

1. Enter Engineering mode and choose System Settings > Personality Settings. The following interface is displayed.

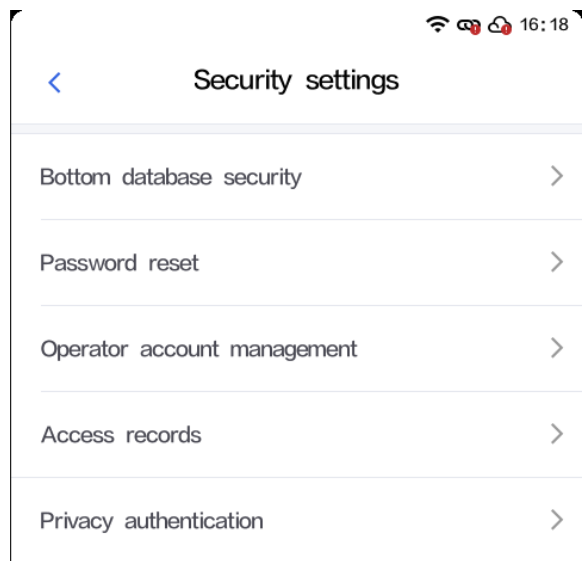


2. For parameter Settings, see the following table.

Parameters	Instructions
Volume adjustment	Used to adjust the volume of the system voice prompt. The value can be 0 to 100
Screen brightness	Value: 0-100
Standby function	It is used to set whether the standby function of the device is enabled. If it is set to [on], the standby function is enabled, and the standby time can be customized. Enter the standby time: 0-30 minutes, select 0 indicates no standby.
Customize the standby picture	Support custom standby interface, please refer to "Appendix 4 Custom standby interface"

### 3.3.8.7 Security Settings

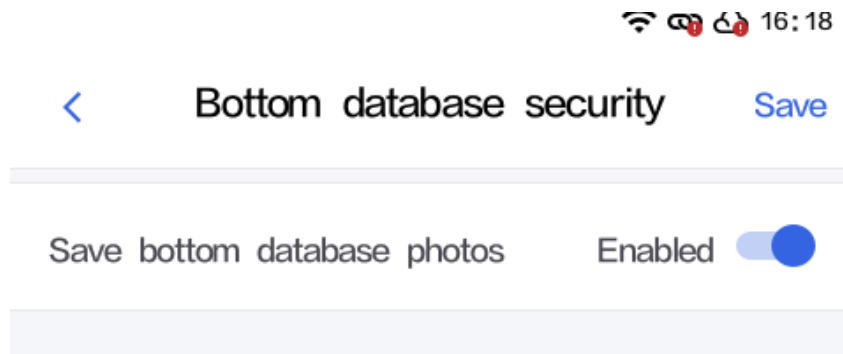
Security Settings are used to change administrator passwords, manage O&M accounts, and set the storage time of access records.



### 3.3.8.7.1 Security of base database

This function is supported only when the device management mode is Server management or MegVII Cloud Management.

The switch of [Save base photo] is enabled by default. After this switch is enabled, the device saves base photo by default.

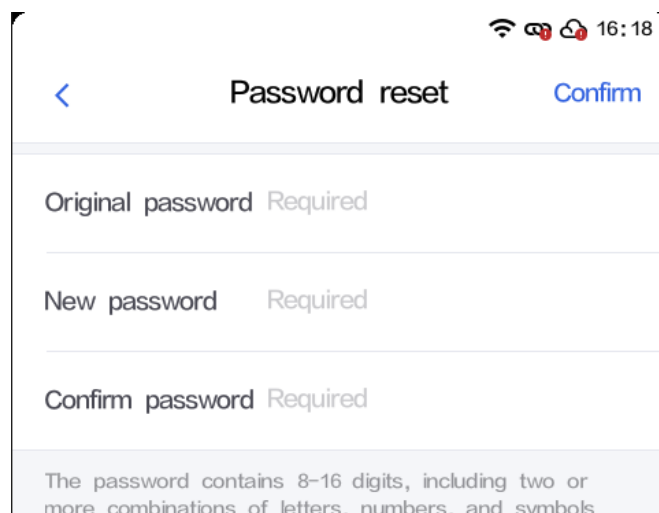


### 3.3.8.7.2 Modify the administrator password (password reset)

If you need to reset your administrator account, follow these steps:

1. Go to [Engineering mode] and select [System Settings] > [Security Settings] > [Password Reset].

The following interface is displayed.



2. Enter the old password, new password and confirm the new password.
3. After setting, click [Save].

### 3.3.8.7.3 Operation and maintenance account management

If you need to reset your O&M account, follow these steps:

1. Go to [Engineering mode] and choose [System Settings] > [Security Settings] > [O&M Account Management] > [Enable O&M Account]. The following interface is displayed.

## Operator account management

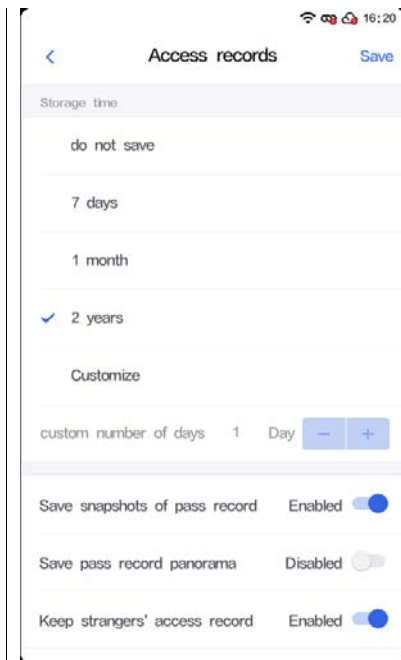
Enable the operator account

2. Enter a new password and confirm it.
3. Click [Save] when the Settings are complete

### 3.3.8.7.4 Access record Settings

If you want to set the storage time and storage type of the access record, please follow the following steps:

1. Enter the "Engineering mode" and choose "[System Settings] > [Security Settings] > [Traffic Record Settings]". The following interface is displayed.



2. For parameter Settings, see the following table.

Parameters	Instructions
Storage time	<p>Select storage time on demand, with the following Settings supported:</p> <ul style="list-style-type: none"> <li>● Not store</li> <li>● Store for 7 days</li> <li>● Store for 1 month</li> <li>● Store for 2 years</li> <li>● Custom <ul style="list-style-type: none"> <li>■ Custom days: Set as needed.</li> </ul> </li> </ul>
Access record Save capture	Open on demand.
Pass-record Save Panorama	Open on demand.
Save stranger access records	Open on demand.

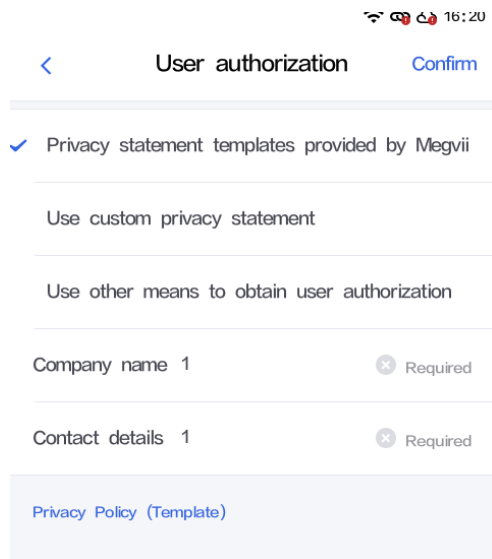
Delete access records synchronously after deleting people	Open on demand.
---	-----------------

- Click [Save] when the Settings are complete.

### 3.3.8.7.5 Privacy authentication

The device allows the user to select the authorization file.

- Go to [Engineering mode] and select [System Settings] > [Security Settings] > [Privacy Authentication]. The following interface is displayed.



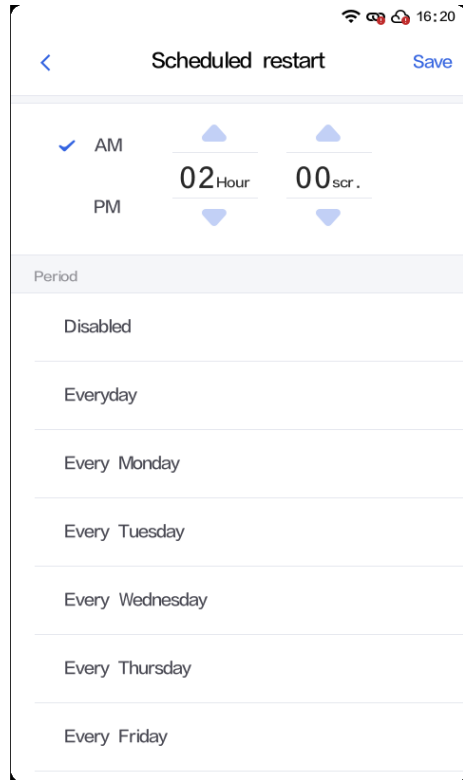
- Select authorization files as required and make related Settings. Only one option is supported.
- After setting, click [Finish].

### 3.3.8.8.2 Device restart

To restart the device, click [Device Restart] to restart the device.

### 3.3.8.8.3 Timed Restart

1. Choose [System Management] > [Upgrade and Maintenance] > [Scheduled Restart]. The following interface is displayed.

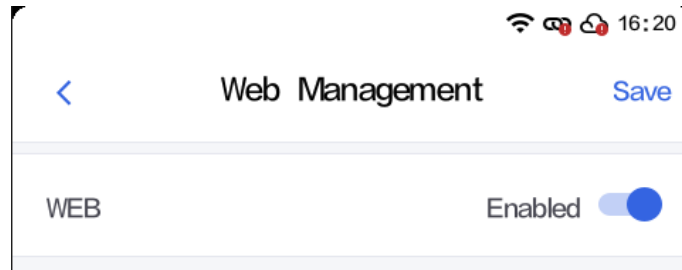


2. Turn on the scheduled restart switch and set the restart time and restart period.
3. After setting, click [Save].

### 3.3.8.8.4 WEB Administration

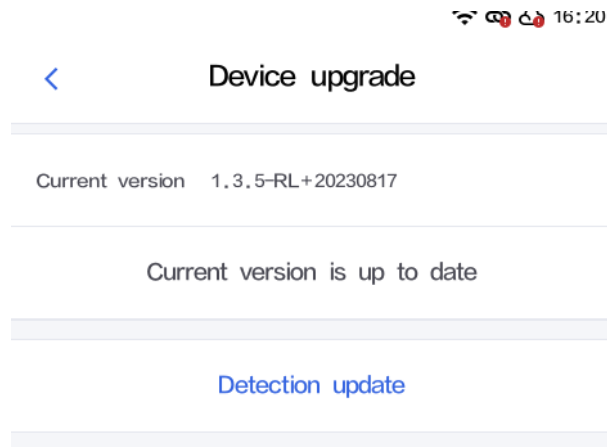
Choose "[System Management] > [Upgrade and Maintenance] > [WEB Management]" and set the [WEB] switch to [On]. After the switch is enabled, users can configure the Settings on the web side. The login address is the ip address of the board, and the user name and password of Engineering mode are used to log in.





#### 3.3.8.8.5 factory data reset

Enter [Engineering mode], choose [System Settings] > [Upgrade and Maintenance] > [Restore factory Settings], confirm the second time, and click [Continue].



#### 3.3.8.9 Equipment debugging

If you need to debug the equipment, you can click [Equipment debugging] to start the equipment debugging function. Support epidemic prevention platform test, ID card service test.

# 4 Addendum

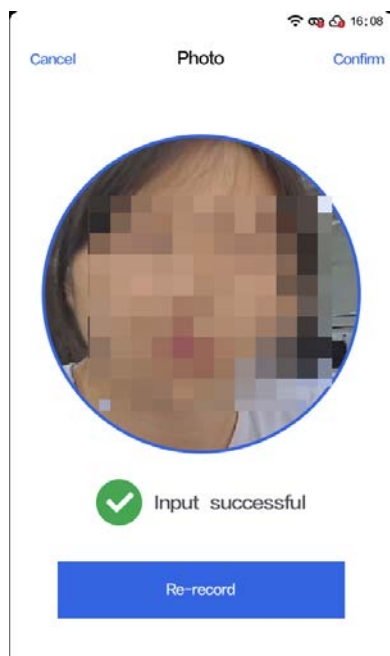
## 4.1 Appendix 1 Enter personnel photos

Follow these steps for face entry:

1. In the "Add personnel" interface, click [face photo] to enter the personnel photo collection page



2. Adjust the pose so that the head is displayed inside the circle and the face is revealed.
3. Click on [Record] and wait 3 seconds for the record to complete.

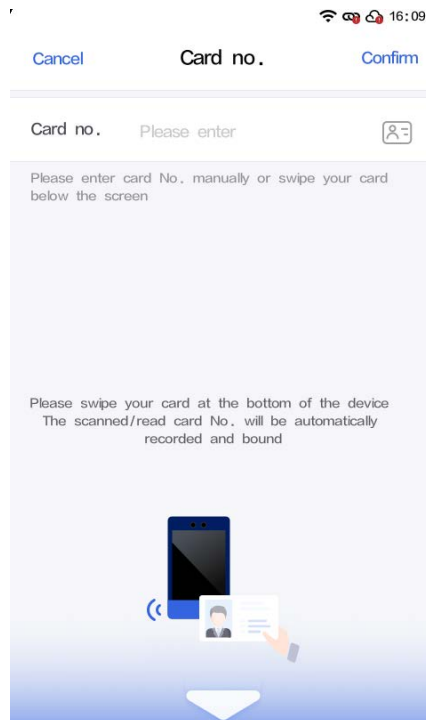


4. Click [Finish], the collection is successful. The photo is used as the face image of the base library.
5. If you need to re-capture the photo, click "re-entry".

## 4.2 Appendix 2 Enter the card information

Follow these steps to enter the card number by swipe:

1. In the "Add personnel" interface, click [card number] to enter the card number collection page.

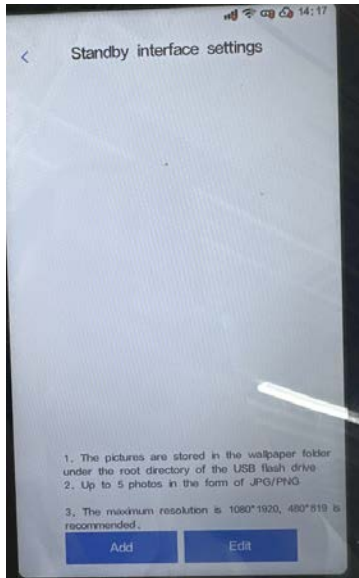


2. Read the card number in the swipe area at the bottom of the screen.
3. Click [Save] when the entry is complete.

## 4.3 Save Appendix 4 Customizing the standby screen

Follow these steps to set up the standby interface:

1. Create a wallpaper folder in the root directory of the USB flash drive and insert the USB flash drive into the device after placing the standby pictures in the folder.
2. Go to [Engineering mode] and select [System Settings] > [Personality Settings].
3. Click the "Custom Standby" interface to enter the setting page.



4. Click [Add], read the u disk picture, the picture support JPG/PNG, the maximum resolution of 1080\*1920, 480\*854 recommended.
5. Set [rotation interval], the default 5s, the maximum 20s, the minimum 3s, the minimum adjustment force is 1s.  
After setting, click [Save].

**Note:**

- When the device is connected to the cloud, the cloud Settings prevail and the local Settings do not take effect. This standby screen replacement function only takes effect when a Single machine is in use.
- When the custom standby picture is enabled (there is a custom picture), when the user picture is displayed in standby mode, the device time/location and other information are not displayed, only the picture uploaded by the user is displayed.
- You can have up to 5 standby pictures built into the device. You can only import them when there is a spare space; If there is no free space, you need to delete the existing image before you can import it.



**Workplace Intelligence**

2525 FYI Center,  
Building 2, Room No. 1203-1205,  
12th Floor, Rama 4 Road, Klong Toei,  
Klong Toei, Bangkok 10110, Thailand  
Tel : (+66) 2 784-5855