



FCA-2300



Face Recognition Access Control Terminal (3.5")

Fast, accurate face recognition that works in any light, with liveness detection and face, QR, or Mifare card access.

Foreword

Dear User:

Thank you for choosing and using our products.

To ensure you use this product effectively, please read this instruction manual carefully, follow the steps outlined in the manual, and keep it safe for future reference.

Our company is committed to continuously improving product functionality and service quality.

The content and images in this manual may differ from the actual product, and functional descriptions may vary slightly depending on the specific model. If there are any discrepancies with the actual product, please refer to the actual product.

Certain components, appearances, or functions mentioned in this manual may be copyrighted.

No part of this manual may be reproduced or distributed in any form without the prior written permission of the company.

Our company reserves the right to modify the contents of this instruction manual and related product technical specifications. Changes to the contents of this instruction manual will be made without separate notice. If you have any questions, please contact us as soon as possible. We will be happy to assist you. Thank you again for using our products.

Chapter 1 Product Overview

1.1 Product Introduction

The FCA-2300 is a facial recognition-based time and attendance/access control terminal product. It supports facial recognition, Mifare cards, passwords, and QR codes, and can be used in commercial real estate, corporate buildings, hotels, government agencies, industrial parks, factories, campuses, small businesses, construction sites, shops, and other similar locations.

This product features a 3.5-inch touchscreen display with a vertical screen design, a high-quality, highly reliable chassis built with graphene technology, and IOMO technology.

With world-leading AI deep learning algorithms, mature and reliable technical solutions, and multi-field application experience, we meet the facial recognition needs of our customers in various scenarios.

1.2 Appearance Introduction

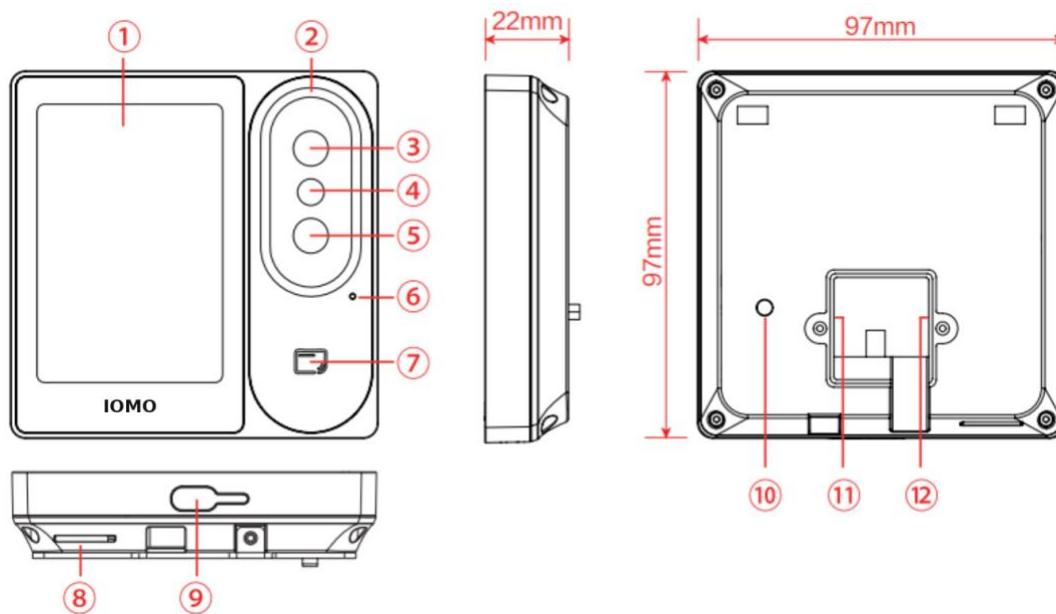


Figure 1.2-1 Product appearance drawing

No.	Name	Description
1	Display	3.5-inch multi-touch display
2	white light fill light	Fill light for RGB camera
3	Infrared camera	Take an infrared image
4	Infrared fill light	Fill in light for infrared camera
5	visible light camera	Take visible light images
6	microphone	sound collection

Note ② White light fill light: Face and hand models supported
FCA-2300 Series: Face + Hand Design
FCA-2300F Series: Face Only Model

No.	Name	Description
7	Swipe area	Cards can be swiped here
8	speaker	Play voice prompts
9	Type C interface	Supports connecting USB flash drives via Type-C port
10	Anti-tamper button	To prevent the equipment from being dismantled after installation
11	External cable	Connect power via cable
12	reset button	Long press to restore to factory settings

Figure 1.2-2 Appearance Description

Chapter 2 Installation Instructions

2.1 Installation Environment

The FCA-2300 can be installed indoors, supporting wall mounting and 86-type junction box installation. A height of 1.4 meters is recommended, but it can be adjusted according to the actual usage scenario.

During installation, avoid placing the device directly opposite windows, doors, or light sources, and prevent direct sunlight or light exposure.

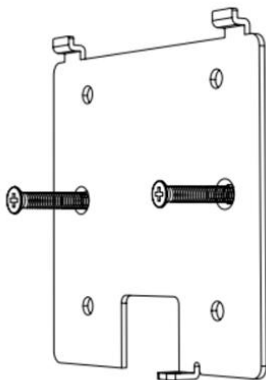
Note: Prolonged power outages may cause time inaccuracies. The device will automatically synchronize its time after powering on and connecting to the network. The time will be corrected within 72 hours of power-on.

The battery will be fully charged and can maintain normal operation for approximately 20 days in the event of a power outage. Furthermore, to ensure accurate recognition, the lens surface must be kept clean and free of dirt or fingerprints.

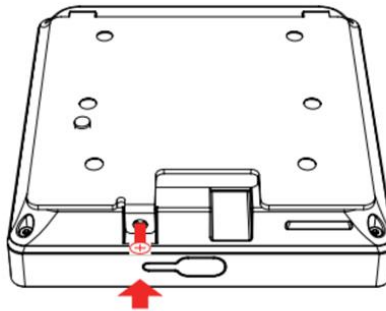
2.2 Installation Methods

2.2.1 86-Type Junction Box Installation

1. Secure the bracket to the 86 box with two machine screws.

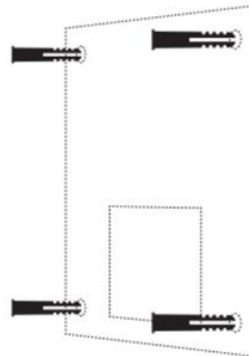
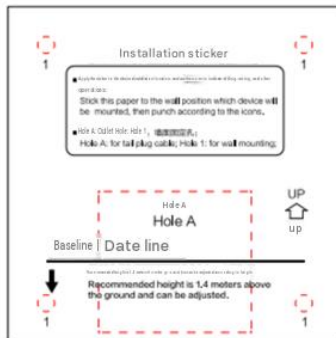


2. After connecting the wires, assemble the bracket with the panel and tighten the screws provided with the bracket. Installation complete.

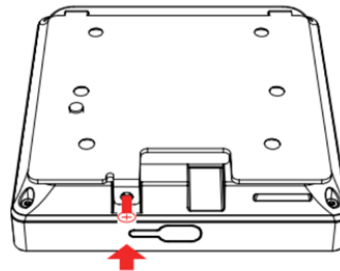
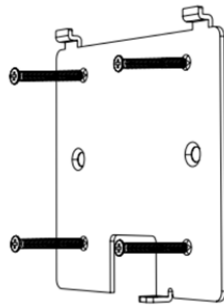


2.2.2 Wall Mounting

1. Attach the mounting sticker to the wall according to the baseline on the mounting sticker, and drill four holes in the wall according to hole 1.
2. Insert expansion tubes into each of the four holes and peel off the installation sticker.

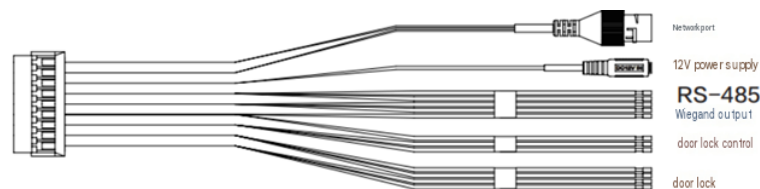


3. Align the quick-release bracket with the holes on the wall and use four self-tapping screws to fix it to the wall.

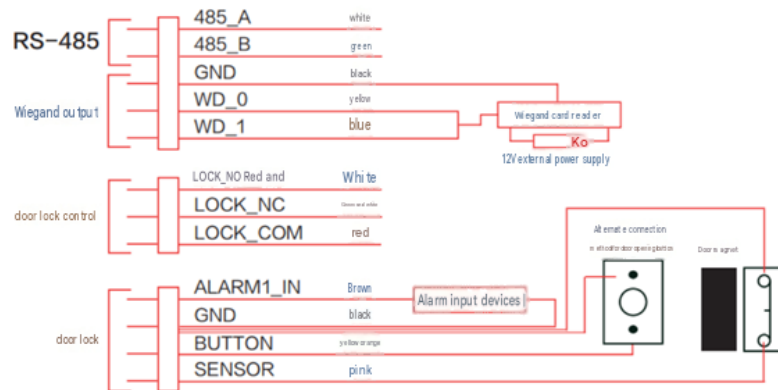


Chapter 3 Equipment Wiring

3.1 Terminal Block Description



3.2 Equipment Wiring Instructions



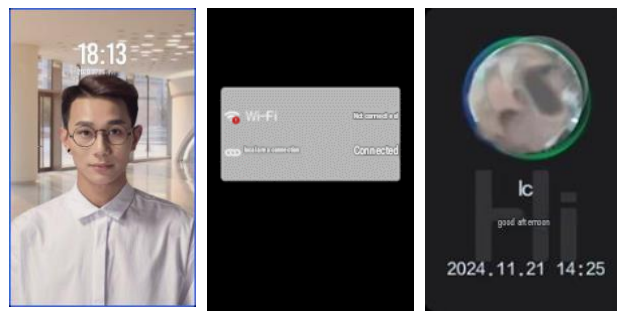
Note: When communicating with other devices, it is recommended to connect the GND of the panel device to the GND of the other device to enhance communication stability.

Chapter 4 Basic Operations of the Local Interface

4.1 Recognition Interface Description

4.1.1 Recognition Interface

- The recognition interface can display information such as the current time and real-time video.
- Tapping the screen displays the current network connection status, Wi-Fi
- connection status, and server connection status. After verification, the pass result,

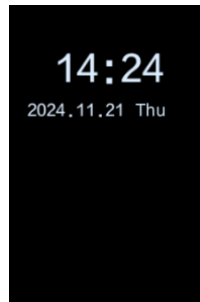


Recognition interface diagram

4.1.2 Standby Mode

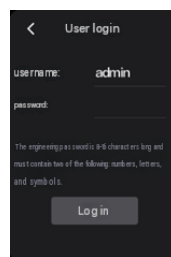
If there is no operation for longer than the set standby time and no face is detected in the access preview interface or system configuration interface, the device will automatically enter standby mode.

Standby mode will exit when a face is detected. This can be configured in the device's web interface or in the admin settings under "Personalized Settings".



4.1.3 Engineering Mode

Step 1 : Long press on an empty area of the screen to bring up the [User Login] prompt box.



Step 2 Enter the username and engineering password you set during activation, then click "Login" to enter engineering mode. For instructions on operating the engineering mode interface, please refer to Section 4.2 Engineering Mode.

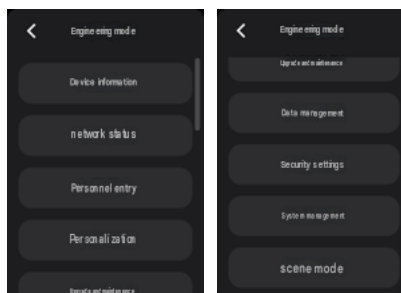
Note: If the system detects that the operator has administrator privileges through facial recognition, the system will skip the password input step and directly enter engineering mode.

Click the "<" button in the upper left corner to exit engineering mode.

Note: If the password is entered incorrectly 5 times within 5 minutes, the device will be locked for 10 minutes.

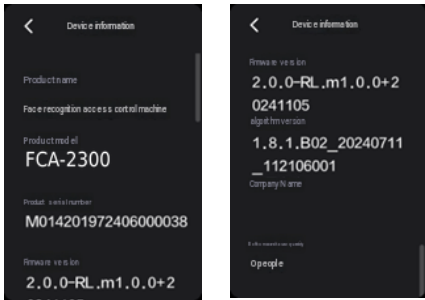
4.2 Engineering Mode

In engineering mode, you can query information and perform related configurations. The available operation modules are shown in the image below:



4.2.1 Viewing Device Information

In the [Engineering Mode] interface, click "Device Information" to jump to the device information page, which displays information such as "Product Name", "Product Model", "Product Serial Number", "Firmware Version", and "Base Library Quantity".



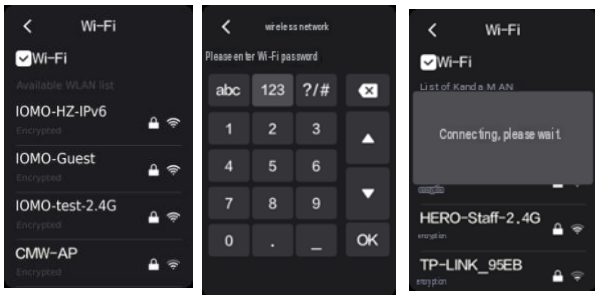
4.2.2 Network Status

In the [Engineering Mode] interface, click "Network Status" to jump to the network status page, as shown in the figure below.



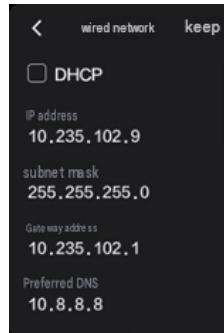
4.2.2.1 Viewing Wi-Fi

Clicking "Wi-Fi" will take you to the Wi-Fi information page, which displays a list of available Wi-Fi networks and their connection statuses. Clicking on a Wi-Fi name allows you to enter the password to connect. Once connected, clicking on the connected Wi-Fi name will display detailed information.



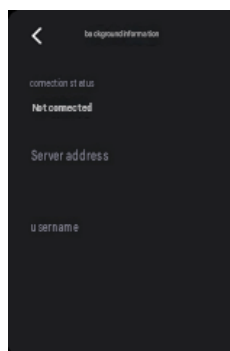
4.2.2.2 Viewing Wired Networks

Clicking "Wired Network" will take you to the wired network information page, which displays information such as "DHCP" switch, "IP address", "subnet mask", "gateway address", and "DNS", as shown in the image below.



4.2.2.3 Viewing Backend Information

Clicking "Backend Information" will take you to the backend information page, which displays "Connection Status", "Server Address", and "Username".

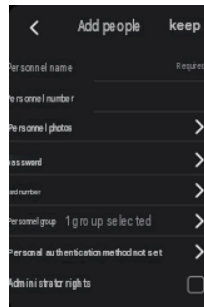


4.2.3 Personnel Entry

The device supports local personnel entry. To enter personnel information locally, please follow these steps. This feature is only available in standalone mode. Through the personnel management function, you can add employees, set administrator permissions, and more.

Operating Steps

- Step 1 In the [Engineering Mode] interface, click "Personnel Entry" to start adding personnel information



- Step 2 : Enter the information according to the on-screen prompts.

Parameter description:

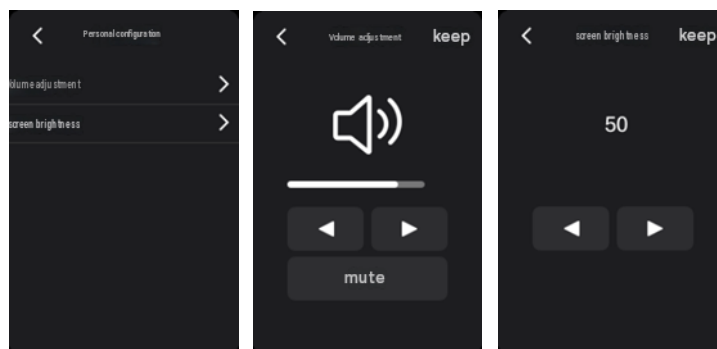
Parameter	Description
Personnel	(Required) Can be repeated.
Personnel	(Optional) No duplicates allowed; if left blank, the system will generate one
Personnel	(Optional) Click to enter the personnel photo collection page. Please refer to
Password	(Optional) This is the authentication password for access. Please use a 6-digit
Card Number	(Optional) No duplicate entries allowed. Users can choose to manually enter the card number or swipe their card in the card swiping area at the top right of the screen, and the card number will be read automatically.
Personnel	(Required) Select a personnel group to manage personnel in groups. The default
Administrator Privileges	(Optional) Enabled means the current user will have administrator privileges for the device and can enter [Engineering Mode] to configure device parameters. "Off" indicates a regular user with only access control privileges.

- Step 3: When the message "Entry successful" appears, click "Save".

4.2.4 Personalized Settings

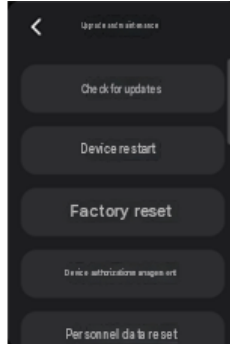
In the [Engineering Mode] interface, click "Personalized Settings" to enter the personalized configuration page, where you can adjust the device's prompt voice volume and screen brightness.

See the figure below.



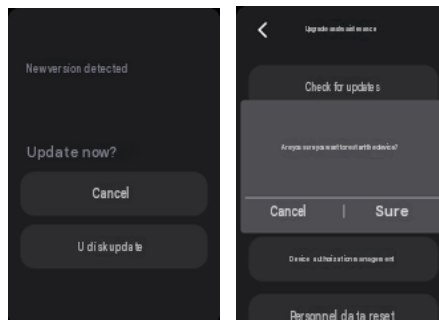
4.2.5 Upgrade and Maintenance

In the [Engineering Mode] interface, click "Upgrade and Maintenance" to enter the upgrade and maintenance page, which supports device upgrades, restarts, factory resets, Lua plugin authorization management, personnel data reset, and other operations.



4.2.5.1 Checking for Updates

- Step 1 Place the upgrade file (upgrade.bin) in the root directory of a FAT32-formatted USB flash
- Step 2 drive and insert it into the USB port of the control panel. Click "Check for Updates," then click
- Step 3 "Update from USB."
- Step 4 The device will automatically check the upgrade files on the USB drive and perform the update.



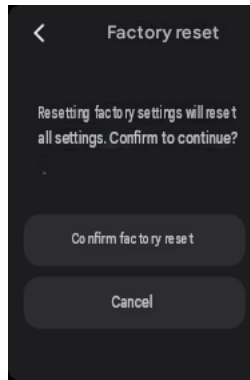
4.2.5.2 Device Restart

Click "Restart Device" and confirm. The device will then perform a soft reboot.

4.2.5.3 Restoring Factory Settings

Click "Restore Factory Settings," and the device will be restored to factory settings after confirmation.

Note: Restoring factory settings will delete all data on the device and reset the configuration.



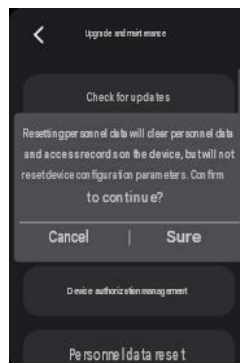
4.2.5.4 Device Authorization Management

Click "Device Authorization Management" to enter the authorization code manually or obtain it automatically via USB drive.



4.2.5.5 Personnel Data Reset

Clicking "Reset Personnel Data" and confirming will clear personnel data and access records on the device, but will not reset the device settings or configuration parameters.

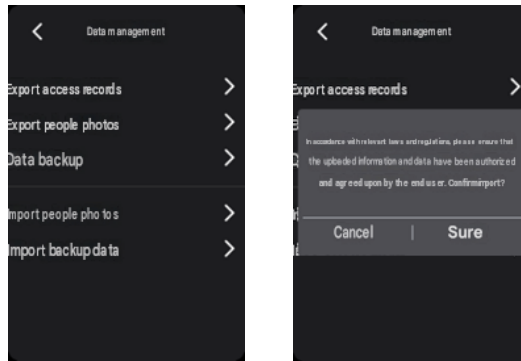


4.2.6 Data Management

This module enables the import and export of device and user data:

- Export Data: Supports exporting access records, personnel photos, and data backups.
- Import Data: Supports importing personnel photos and backup data.

When exporting access records and personnel photos, please ensure the data is used in compliance with applicable regulations and kept secure.



4.2.6.1 Connecting a USB Flash Drive

If users need to perform data import and export operations, they must first connect an external storage device, such as a USB flash drive or other storage device, via a USB Type-C interface. Once the connection is successful, the device will detect the USB flash drive or other storage device, and then data import/export operations can be performed.

Note:

- If no USB flash drive or other storage device is inserted, or the device fails to read it, the import and export data options will turn gray, indicating that they are unavailable.
- Once the storage device is detected, all import and export functions will be available.

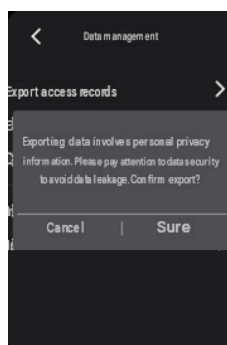
4.2.6.2 Exporting Data

Step 1 : Enter [Engineering Mode] and select [Data Management].

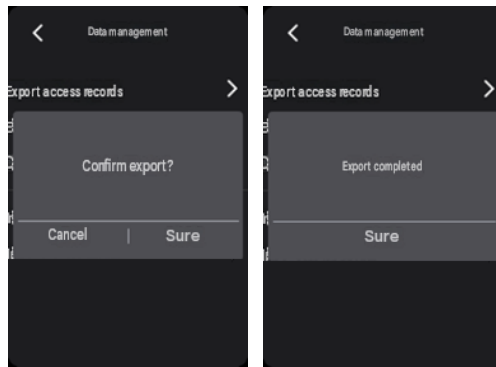
Step 2: Connect the USB flash drive.

Step 3: After successfully connecting the USB drive, select the data type you want to export.

1. The device supports exporting access records, personnel photos, and data backups.
2. When selecting to export access records and personnel photos, privacy and security confirmation is required. Export starts after confirmation, as shown in the figure below.



3. During data backup, users can select either "Device Parameters" or "Personnel"
- Step 4 Click "Confirm" to begin exporting data. Once the export is complete, a "Finish" message will



Export Data Description

Data Type	Export content and export path	Remark
Access Records	● Export content ■ Access record table (named after the access record time range, file format ".xls"); ■ Captured photo (named with the capture time, file format ".jpg") ● Export path ■ The folder named "event_log" in the root directory of the USB drive contains the access record table and captured images. event_log event_log1	If the external storage device retains the data from the previous export, the folder name will be incremented to "event_log1" / "event_log2"... during the export process.
Personnel Photos	● Export content ■ Personnel photos (named with personnel name + personnel number, file format ".jpg") ● Export path ■ USB drive root directory → person_pic person_pic	● The export process will overwrite the previous exported data (if it exists), so please proceed with caution. ● Personnel numbers cannot be duplicated; otherwise, the import will fail.

Device Parameters	● Export content ■ Access control parameters: These involve the configuration of the device's door locks, door sensors, and authentication methods . ■ Network parameters: This involves the configuration of local Ethernet and Wi-Fi. ■ Communication parameters: This involves the Wiegand configuration. ■ Face parameters: This involves the configuration of the binocular camera, face, recognition threshold, and liveness threshold. ● Export path ■ USB drive root directory → device_data	The export process will overwrite the previous exported data (if it exists), so please proceed with caution.
-------------------	--	--

4.2.6.3 Importing Data

Step 1 : Enter [Engineering Mode] and select [Data Management].

Step 2: Connect the USB flash drive.

Step 3: After the USB flash drive is successfully connected, select the data type to import. The device supports importing personnel photos and backup data.

Step 4: After confirming privacy and security, begin importing data. Note that no privacy and security confirmation is required when selecting "Import Backup Data."

Step 5: The data import begins. Once the import is complete, a "Complete" message will appear, and the device will restart. If you click "Cancel" at this point, the imported data will not take effect immediately.

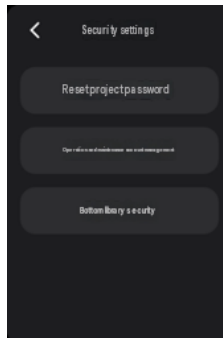
Note: When selecting "Import Backup Data", you can choose to import either "Device Parameters" or "Personnel Information", and multiple selections are supported.

Import Data Description

Data Type	Import content	Remark
Personnel Photos	● Import content ■ Photo naming rule: personnel name/personnel number ■ File read path: USB drive root directory → person_pic ■ Photo formats: jpg, png, bmp	If no matching file is found to import, the message "No people photos folder detected" will be displayed.
Backup data	● Import content ■ File read path: USB drive root directory → device_data	The device automatically reads and imports files stored on a USB flash drive or other storage device, and will overwrite the original data.

4.2.7 Security Settings

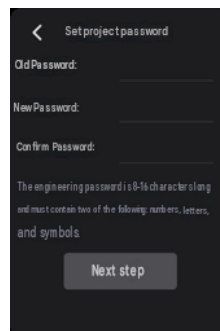
Security settings are used to reset the engineering password, manage operations and maintenance accounts, and configure database security settings.



4.2.7.1 Reset Engineering Password

To reset the engineering password, please follow these steps:

Step 1 : Enter [Engineering Mode], select [Security Settings] > [Reset Engineering Password]. The system will display the following interface.



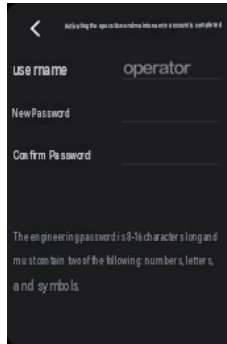
Step 2: Enter the old password, enter the new password, and confirm the new password.

Step 3: Click "Save".

4.2.7.2 Operations and Maintenance Account Management

To set up the operations and maintenance account, please follow these steps:

Step 1 Enter [Engineering Mode], select [Security Settings] > [Operations Account Management] > [Enable Operations Account]. The system will display the following interface.



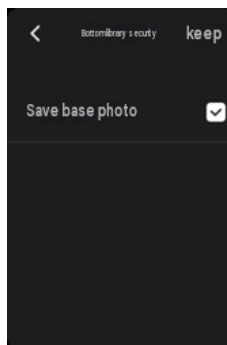
Step 2 : Enter and confirm the new password.

Step 3: Click "Save".

4.2.7.3 Database Security

To configure whether base photos are saved, please follow these steps:

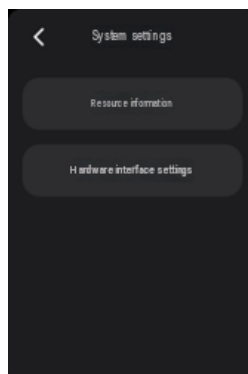
Step 1 : Enter [Engineering Mode], select [Security Settings] > [Database Security]. The system will display the following interface.



Step 2 : Enable or disable "Save base photo" as needed; it is on by default. When off, the device will delete the original photo after extracting facial feature values.

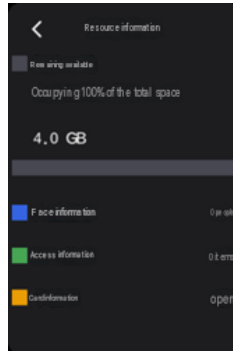
4.2.8 System Management

System management allows you to view device resource information and configure hardware interfaces. Enter [Engineering Mode], select [System Settings], and the system will display the following interface.



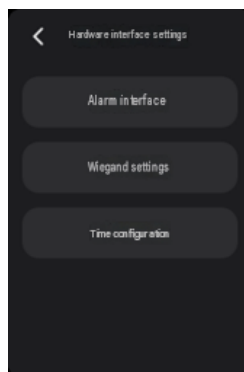
4.2.8.1 Resource Information

Click "Resource Information" to enter the resource viewing interface. It shows the device storage space, number of personnel information records, number of access records, and number of card information records.



4.2.8.2 Hardware Interface Settings

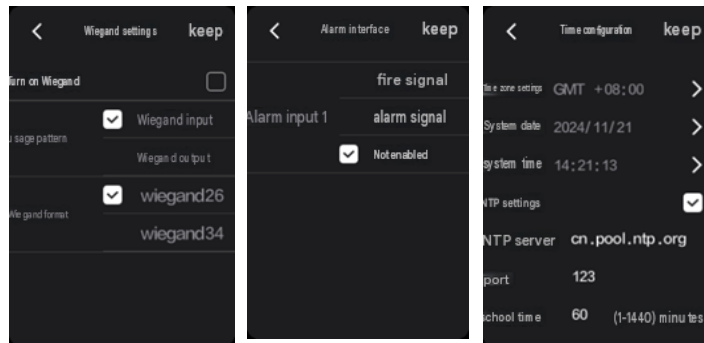
Click "Hardware Interface Settings" to configure the alarm interface, Wiegand settings, and time configuration. See the image below.



Alarm Interface: This product supports one alarm input interface. After correct wiring, this alarm input can be configured as a fire alarm signal, or the alarm signal can be disabled. The default is disabled.

Wiegand Settings: This product supports one Wiegand interface. After enabling the Wiegand function, the Wiegand interface can be configured as a Wiegand input or output, and the Wiegand protocol can be configured as Wiegand26 or Wiegand34.

Time configuration: Configure time zone, system date, system time, NTP server, port, etc.



Appendix 1: Entering Personnel Photos

Please follow the steps below to enter personnel photos.

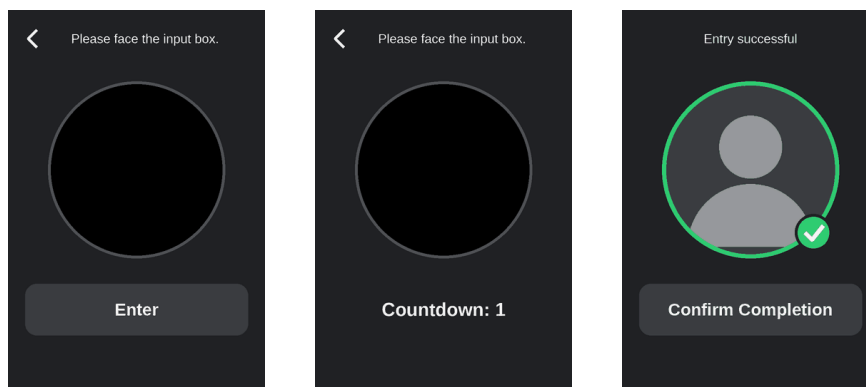
Operating Steps

Step 1 : On the "Personnel Entry" interface, click on [Personnel Photo] to enter the personnel photo collection page.

Step 2: Click on [Enter], adjust your pose so that your face is displayed within the circle, and wait 3 seconds for the entry to complete.

Step 3: Click "Confirm Completion" to complete the photo entry. This photo will be used as the base image.

If the data entry fails, the system will display the message "[Data Entry Failed]". Click "[Re-enter]" to capture the photo again.



Appendix 2: Safety Precautions

To reduce the risk of fire or electric shock, do not expose the product to rain or moisture.

An easily accessible power disconnect device should be incorporated into the building's wiring installation.



Warning:

During product installation and use, all national and regional electrical safety regulations must be strictly followed. Please use a power adapter provided by a

ensure the product is securely fastened.

If the product malfunctions, please contact the service provider where you purchased it. Do not disassemble or modify the product in any way. (Our company is not responsible for any problems caused by unauthorized modifications or repairs.)

When installing on a wall or ceiling,



Avoid

installing the product in environments with vibration or shock, and keep it away from locations with electromagnetic interference. (Ignoring this may

Do not touch the heat dissipation components of the product directly to avoid burns.

Do not install indoor products in environments where they may come into contact with water or other liquids.

Do not use the product in extremely hot, extremely cold, dusty, corrosive, or high humidity environments. Please refer to the product's parameter table for specific temperature and humidity requirements.

Avoid pointing the lens at strong light (such as artificial lighting, sunlight, or laser beams), as this may damage the image sensor.

To prevent heat buildup, ensure good ventilation around the product.

Do not touch the image sensor directly. If cleaning is necessary, gently wipe away dust and dirt with a soft, clean cloth slightly dampened with alcohol. When the product is not in use, cover it to protect the image sensor.

Connecting your device to the internet may pose cybersecurity risks. Please strengthen the protection of your personal information and data. If you discover any potential cybersecurity vulnerabilities in your device, please contact us immediately.

Please understand that you are responsible for configuring all passwords and other related product security settings properly, and for keeping your username and password safe.

Please keep all original packaging materials of the device. In case of any problems, use these materials to properly repackage the device and send it to the distributor or return it to the manufacturer for processing. The user is responsible for any accidental damage during transportation caused by materials other than the original packaging materials.



Note

Requirements for the qualifications of installation and maintenance

Possess basic knowledge and installation skills of access control systems and their components.

Possess basic knowledge and operational skills in low-voltage wiring and low-voltage electronic circuit connection.

Possess basic cybersecurity knowledge and skills, and be able to understand the contents of this manual.

