Face Recognition Terminal User Guide

20260115_V1

1. Product Introduction

1.1 Product Overview 01

1.2 Product Features 01

2. Operating Instructions

2.1 Time and Attendance Machine Installation 01

2.2 Gate Wiring 02

2.2.1 For 5 Inch Plastic Version..... 02

2.2.2 For 5 Inch /8 Inch Metal Version..... 03

3. Product Usage

3.1 Basic Use 03

3.2 Basic Operation of the Identification Interface 03

3.2.1 How to Access the Settings Interface 03

3.2.2 Call interface 04

3.3 System Main Menu Interface 05

3.4 User Management 06

3.4.1 Add User 07

3.4.2 View All users 07

3.4.3 Bulk Import Users 08

3.4.4 Batch Export Users 09

3.4.5 Uploading and Batch Deleting Users via Web Interface 09

3.4.6 Department Management 10

3.5 Record Management 10

3.5.1 View Access Records 10

3.5.2 Delete All Records 12

3.5.3 Record Upload Switch 12

3.5.4 View Operation Logs 12

3.6 Communication Management 12

3.6.1 Wired Settings 12
3.6.2 Wireless Settings 13
3.6.3 Server Settings 14
3.6.4 SIPServer Settings 15
3.6.5 Embedded Web Server 16
3.6.6 OTA Address Setting 17
3.7 Attendance Management 17
3.7.1 Attendance Rule Settings 17
3.7.2 Shift Rules 18
3.7.3 Attendance Sheet Export 19
3.8 SystemSettings 20
3.8.1 Local Settings 20
3.8.2 Advanced Settings 21
3.8.3 Intercom Settings 22
3.8.4 Recognition Settings 23
3.8.5 Access Control Setting 24
3.8.6 Data Management 25
3.9 Device Information 25

1. Product Introduction

1.1 Product Overview

Based on the SV830D chip, this facial attendance motherboard features an Arm Cortex-A7 CPU and + RISC-V CPU architecture, integrated neural network processor supporting up to 0.5 TOPS deep neural network computing power. This binocular facial recognition terminal supports SIP protocol audio/video intercom, enabling one-to-one,one-to-many (group or single call), and optional doodle intercom, The terminal integrates facial recognition, palm vein recognition (optional), fingerprint recognition (optional), ID/IC card recognition, identification record storage, and liveness detection. Equipped with a high-definition facial recognition camera, it adapts to harsh environments like strong or weak light, featuring fast recognition speed, high accuracy, and large list capacity. It can be paired with application management systems such as facial construction site real-name management systems, facial access control attendance management systems, and visitor management systems, making it perfectly suitable for complex application scenarios requiring temperature monitoring, identity recognition, and access control, such as communities, campuses, hospitals, scenic areas, hotels, shopping malls, corporate office buildings, public service venues, and construction sites.

1.2 Product Features

- Dual 100W/200W Cameras, Built-in High-Performance ISP, Auto Exposure
- 3 Serial Ports, Supplementary Lighting, Relays, Wiegand, and Rich Expansion Interfaces
- SIP Protocol Voice and Video Intercom, Supporting One-to-One, One-to-Many (Group or Single Call)
- Tuya WIFI optional, supports video intercom via mobile app (5 inch version)
- Palm vein optional (5 inch version)
- Supports Remote Upgrade via WEB and Local USB Disk Upgrade
- Supports 5,000/20,000 Face, Recognition Rate Over 99.99%, Face Recognition Throughput Less Than 1 Seconds
- Local storage can hold 2 million facial recognition attendance records
- No need to connect to external networks or servers; it independently completes employee attendance records and management
- Provides API integration documentation, supporting custom development

2. Operating Instructions

2.1 Time Attendance Machine Installation

1) The overall bracket effect is shown in Figure 2.1 below.



Figure 2.1

2.2 Gates Wiring

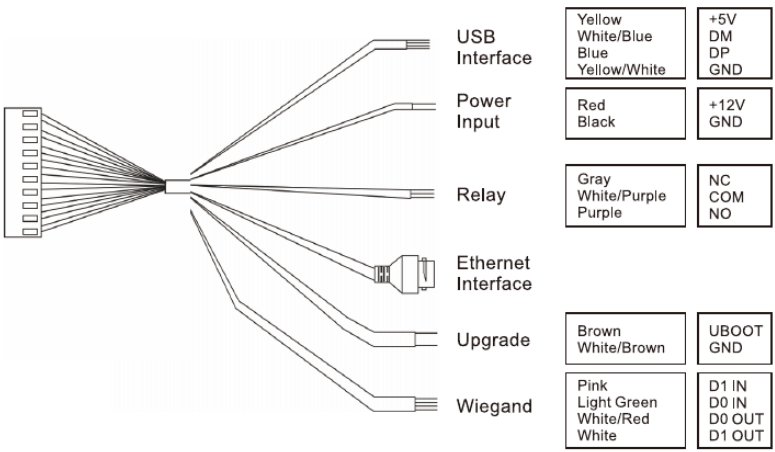
2.2.1 For 5 Inch Plastic Version

Functions	Colors	Function Description
GND	Black	Common Terminal
BUT	Brown	Forced Upgrade Input
ALARM	Gray	Fire Alarm
DOOR	Blue	Door Opening Button
DOOR BELL	Pink	Doorbell Interface
D1	Orange	WG Output Line D1
D0	Purple	WG Output Line DO
NO	Green	Locking signal normally open terminal
COM	White	Locking signal common terminal
NC	Yellow	Locking signal normally closed terminal

Functions	Colors	Function Description
GND	Black	Power -
+12V	Red	Power +

Functions	Colors
RX-	Ethernet interface
RX+	
TX+	
TX-	

2.2.2 For 5 Inch / 8 Inch Metal Version



3. Product Usage

3.1 Basic Usage

After the attendance device is powered on, the screen will display the initialization interface. Once initialization is complete, the device is ready for normal use. The main interface after initialization is shown in Figure 3.1.

3.2 Basic Operations of the Recognition Interface

3.2.1 How to Enter the Settings Interface

Click the leftmost option in the bottom navigation bar. If the device has not set an administrator, it will directly enter the settings interface. If an administrator is set, it will pop up for administrator login, where you can choose to verify with an administrator ID and password or facial verification. After successful verification, enter the system settings, as shown in Figure 3.2.1.

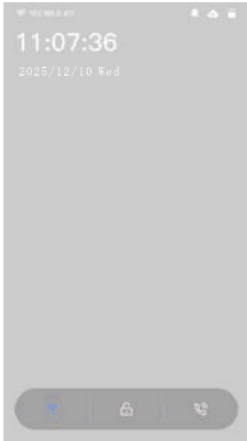


Figure 3.1



Figure 3.2.1

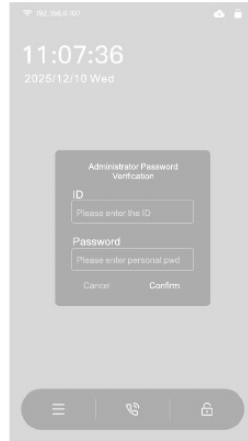


Figure 3.2.2

- IClick "Password Verification" to bring up the administrator login dialog box. Enter the administrator ID and password, as shown in Figure 3.2.2.
- For face verification, the administrator facial verification login interface will pop up. Administrators can directly access the settings interface after completing facial verification.

3.2.2 Call interface

Click the call button in the bottom navigation bar to access the call interface, as shown in Figure 3.2.5.

The intercom call options include: SIP call and Tuya app call.
SIP call is supported by default, while Tuya call is an optional feature.

(1) SIP call: Supports LAN SIP calls or public network SIP calls.

- LAN SIP call: Go to **System Settings > Intercom Settings > Enable LAN IP Call** to enable functions such as intercom, monitoring, and door opening between devices and the indoor unit within the LAN.
- Public network SIP call: Go to **System Settings > Communication Settings > SIP Server Settings**. Register based on the server and account in use. After registration, you can dial calls in the dialing interface to enable functions such as intercom, monitoring, and door opening between devices and the indoor unit over the public network.

(2) Tuya app call: Go to **Device Menu > System Settings > Intercom Settings > Tuya App Binding** (download the Tuya Smart/Smartlife app on your phone, then scan the QR code to bind). Each device call will be directed to the bound Tuya app account.

(3) Call modes: Direct call, Dialing, Contacts (Go to **Device Menu > System Settings > Intercom Settings > Select Call Mode**).

Direct call: Directly call the room number bound to the room.
Dialing: Enter the room number in the dialing interface to call.
Contacts: Select the corresponding person from the added contacts to call the room number.

(4) Monitoring: Go to **Device Menu > System Settings > Intercom Settings > Enable the switch** to allow the indoor unit to perform video monitoring of the door station.

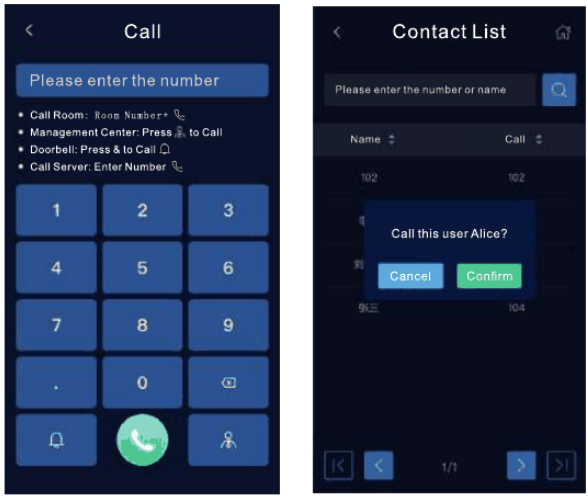


Figure 3.2.5

3.3 System Main Menu Interface

Settings Interface: User Management, Record Management, Communication Management, Attendance Management, System Settings, Device Management. The interface is shown in Figure 3.3.1.

- User Management: Add User, View All Users, Bulk Import Users, Bulk Export Users, Department Management, Delete All Users
- Record Management: View Access Records, Delete All Records, Record Upload Toggle, View Operation Logs;
- Communication Management: Wired Settings, Wireless Settings, Server Settings;
- Attendance Management: Attendance Rules, Shift Rules, AttendanceSheet Export;
- System Settings: Local Settings, Advanced Settings, Recognition Settings, Access Control Settings
- Device Information: Data Capacity Information, About the Device;

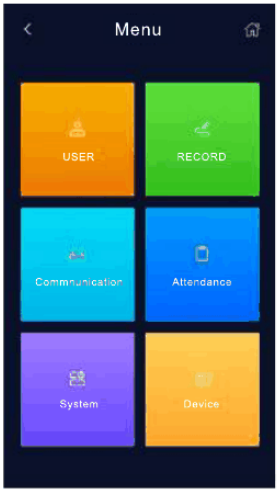


Figure 3.3.1

3.4 User Management

The User Management Interface is shown in Figure 3.4.1

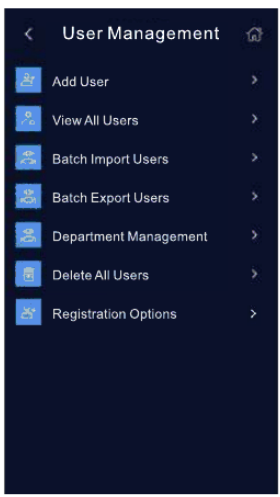


Figure 3.4.1

3.4.1 Add User

Click the Add User option to enter the add interface. Face, palm print, fingerprint, card number, and password can be combined for entry (fingerprint and palm vein options are optional). Click the save icon in the upper right corner to enter the detailed information interface, as shown in Figure 3.4.2 . After successful addition, the corresponding name will be displayed when the face recognition is passed.

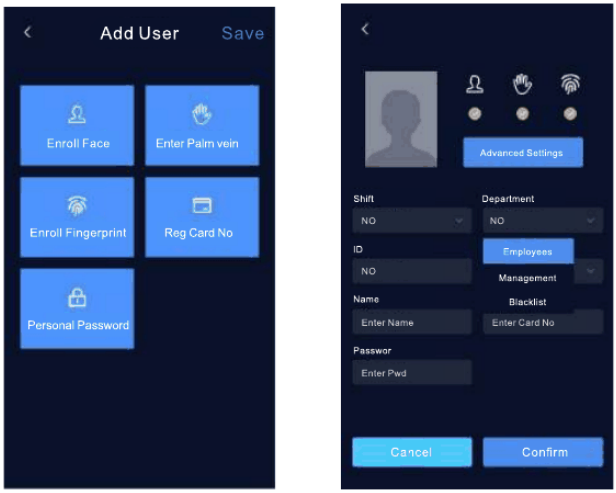


Figure 3.4.2

- **Card Number:** Numbers are entered by default; automatically obtained when swiping the card (optional)
- **User Role:** Regular User, Blacklist, Administrator (required)
- **Name:** Chinese characters or letters are entered by default (optional)
- **Personal ID Number:** Numbers are entered by default; no duplicates allowed (required)
- **ID Card Number:** Numbers or letters are entered by default (optional)
- **Personal Password:** Numbers are entered by default (optional)
- **Department:** Selectable from a list; defaults to the first department on the list (required)
- **Work Shift:** Selectable; defaults to "No" (required)
- **Advanced Settings:** Time periods can be selected (see Weekly Time Period Settings in section 3.8.3); user access start time and user access end time can be set

3.4.2 View all users

Display all user list: Supports searching for users, editing users, deleting users

- Search users: Search and view users by ID and name (Figure 3.4.3)
- Edit User: Modify entered user information; all fields except the ID can be edited
- Delete Users: Click the delete button to remove this user



Figure 3.4.3

3.4.3 Bulk Import Users

The personnel information that needs to be registered into the face recognition machine must be entered into the Excel spreadsheet (person.xlsx) in the specified format, and placed in the REG folder under the root directory of the USB drive, then connect to the device via USB or network to achieve batch import of personnel as shown in Figure 3.4.4

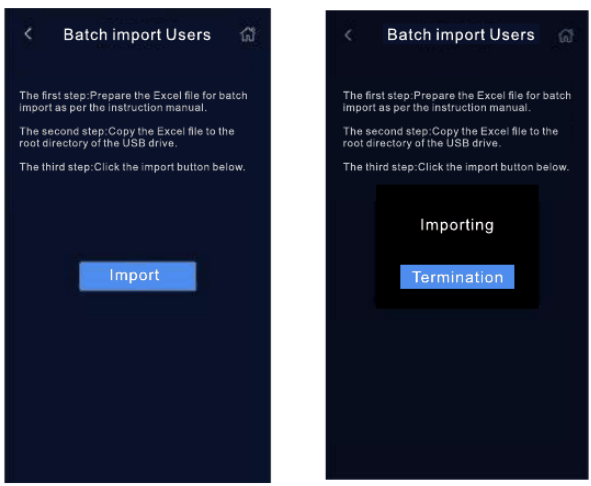


Figure 3.4.4

3.4.4 Batch Export Users

Connect the USB drive, click 'Batch Export Users' to export all personnel from the device. The exported file will be in the REG folder under the root directory of the USB drive (only supports exporting person.xlsx, without personnel photos).

3.4.5 Uploading and Batch Deleting Users via Web Interface

To upload or batch delete users through the web interface, follow these steps:

- IConnect the device to the network via an Ethernet cable or Wi-Fi.
- IAccess the device's web interface by entering its IP address (shown on the top of the device) into a browser.
- ILog in using the default password **123456**. In the left navigation pane, click **Person Info**, then select **Import or Batch delete**. (As shown in Figure 3.4.5)

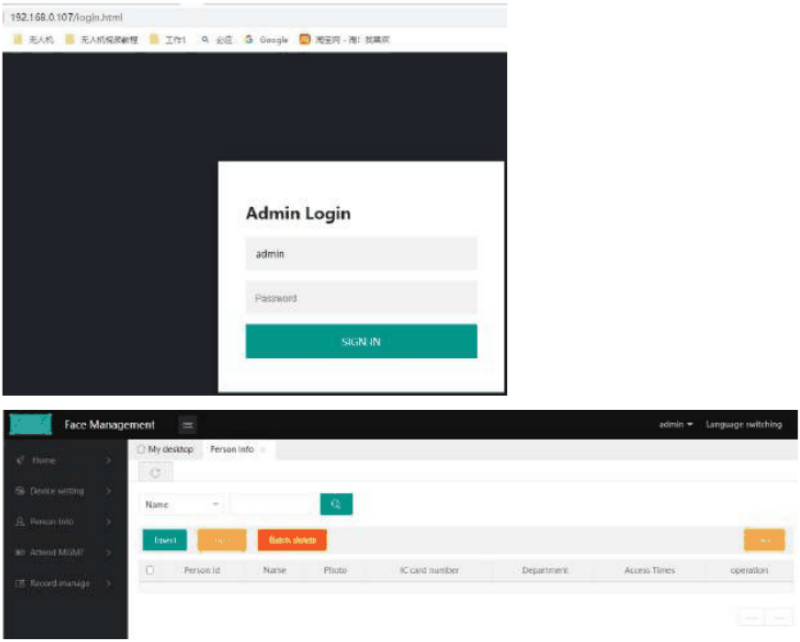


Figure 3.4.5

3.4.6 Department Management

There are ten departments in total, and department names can be edited.
As shown in Figure 3.4.6

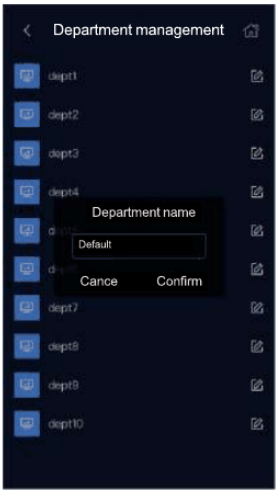


Figure 3.4.6

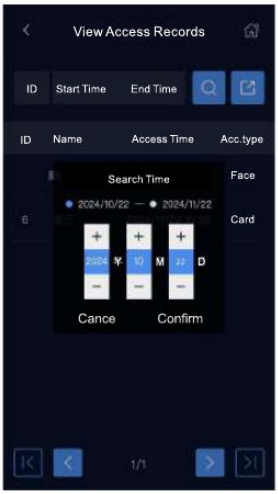
3.4.7 Delete All Users

All users within the device can be deleted with one click.

3.5 Record Management

3.5.1 View Access Records

View the check-in record list, support searching and viewing check-in records by time period or ID; support exporting the corresponding search check-in record list, the exported file is in the root directory of the U disk in the RECG folder as shown in Figure 3.5.1



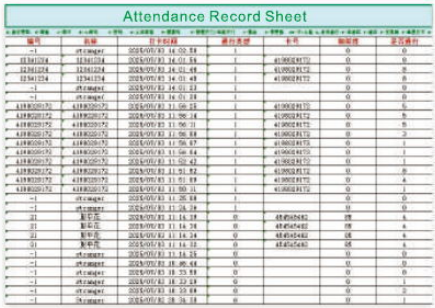


Figure 3.5.1

- Clicking this record can delete the record, as shown in Figure 3.5.2

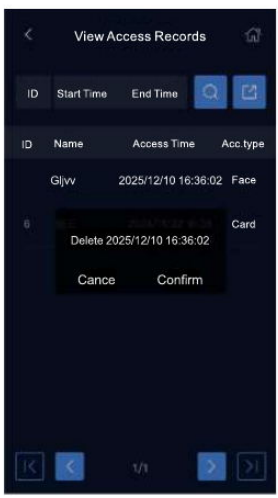


Figure 3.5.2

3.5.2 Delete All Records

Click the button to delete all records in the device

3.5.3 Record Upload Switch

Switches can record uploads to the platform connected to the device, and the local record will be deleted once the upload is completed

3.5.4 View Operation Logs

All operation event information records of the device can be viewed, as shown in Figure 3.5.5.

- Clicking on a record will display its detailed information.
- Click "Export Log Record Data" to export all log records. The exported file will be saved in the RECG folder in the root directory of the USB drive.

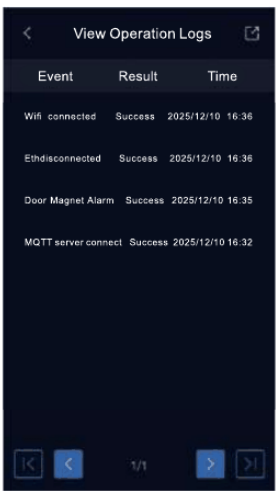


Figure 3.5.5

3.6 Communication Management

Communication Management: Includes wired settings, wireless settings, server address settings, SIP server settings, embedded web server, OTA address settings

3.6.1 Wired Settings

Wired Settings: You can choose to automatically obtain an IP address or statically set an IP address, as shown in Figure 3.6.1



Figure 3.6.1

3.6.2 Wireless Settings

- Check Wi-Fi Switch: The machine turns on Wi-Fi and automatically scans for nearby networks;
- Connect to Wi-Fi: Click the desired network, enter the Wi-Fi password to connect;
- Disconnect Wi-Fi: Click the connected network to disconnect;
- Delete Wi-Fi: Clear the network password for this connection;
- IP Address: View and edit the IP address (Figure 3.6.2)
- Turn off Wi-Fi Switch: The machine turns off Wi-Fi;
- Other: Connect to hidden Wi-Fi, entering the Wi-Fi name and password will automatically connect (Figure 3.6.3)

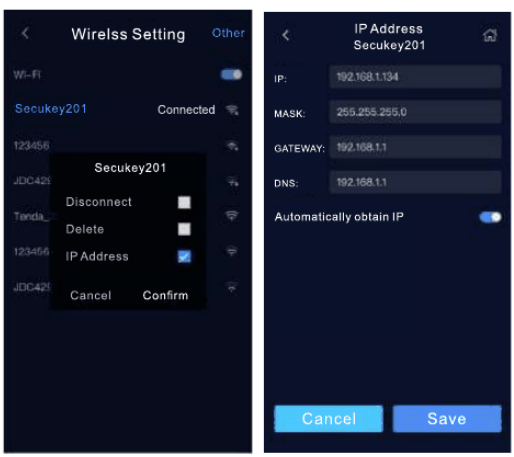


Figure 3.6.2



Figure 3.6.3

3.6.3 Server Settings

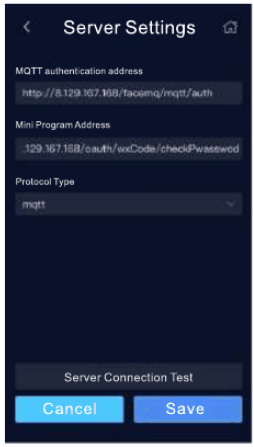
Protocol Type: MQTT/HTTP (Optional)

MQTT Protocol:

- **MQTT Authentication Address:** Enter the client's MQTT authentication address. After successful authentication, the MQTT authentication address returns the information required for the connection, such as IP address, account, password, topic, etc.

HTTP Protocol:

- **HTTP Server Address:** The server address used for heartbeat or record uploads.
- **Heartbeat Packet Interval:** The device sends a heartbeat at regular intervals.
- **Third-Party Record Push:** Enables dual record distribution, pushing data to two platforms.



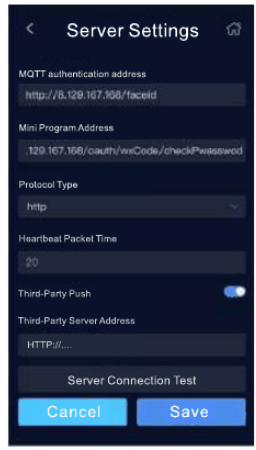


Figure 3.6.4

3.6.4 SIP Server Settings

Includes SIP Server, TURN Server, and STUN Server settings.

(1) SIP Server: The account management platform for SIP users.

- **SIP Server:** Enable this switch when using a public SIP server.
- **Domain:** An SIP domain is an independent VoIP telephony system management unit organized based on a domain name. It manages the registration, authentication, and call routing for all users within the domain through a central server (SIP server), forming the foundational infrastructure for modern IP voice and video communication. The username domain (e.g., sip:1001@company.com). Here, company.com is an "SIP domain" that manages all SIP accounts ending with @company.com.
- **Username:** An available account already created on the server.
- **Password:** The password for the available account already created on the server.
- **Transport:** The transmission method, supporting TCP/UDP.
- **Server Address:** The address of the SIP server.
- **Server Port:** The port number of the SIP server.
- **Proxy Server Address:** The address of the SIP proxy server.
- **Proxy Port:** The port number of the SIP proxy server.

(2) TURN Server: This server is used by SIP for audio/video relay. General SIP servers typically have audio/video relay capability. If not, a TURN server is used.

- **TURN Server:** Enable this switch when in use.
- **Server Address:** The address and port number of the TURN server.
- **Realm:** The server address can be used for this field.
- **Username:** Configure if provided.
- **Password:** Configure if provided.

(3) STUN Server: Used for NAT traversal, generally not used.

- **STUN Server:** Enable this switch when in use.
- **Server Address:** The address of the STUN server.
- **IPv6:** Whether to support using IPv6.

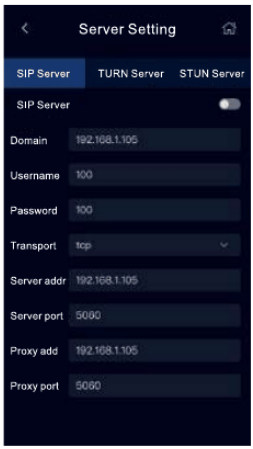


Figure 3.6.5

3.6.5 Embedded Web Server

- Embedded Web Server: Opens to access the device server
- Port Number: Default 80
- Login Password: Default 123456, can be modified manually

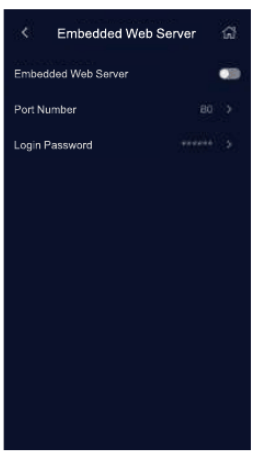


Figure 3.6.6

3.6.6 OTA Address Setting

Set the interface address for automatic device online upgrades



Figure 3.6.7

3.7 Attendance Management

3.7.1 Attendance Rule Settings

Attendance Record Warning: When check-in records reach the upper limit, a warning is displayed on the main interface. For example, if the warning threshold is set to 1,000 and the device's total record capacity is 20,000, a warning will appear on the main interface when locally saved records reach 19,000.

Default Shift: In the new personnel addition interface, the shift will be the pre-set default shift.

Allowed Late Arrival Time: The maximum allowed delay for clocking in at the start of a shift, configurable up to 60 minutes.

Allowed Early Leave Time: The maximum allowed early clock-out at the end of a shift, configurable up to 60 minutes.

Exemption from Check-in: Default is 'No'. Can be set to options such as checking in only for morning shifts or only for evening shifts.

Weekends: Determines whether attendance is counted on weekends. Options include two-day weekends (Saturday & Sunday off), Sunday off only, half-day on weekends, or Friday off.

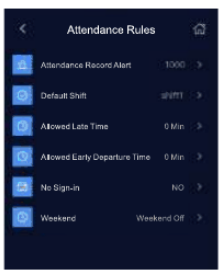


Figure 3.7.1

3.7.2 Shift Rules

- Shift Editing: Shift names, times, and types (attendance or overtime) as well as cross-day times can be edited, with a maximum of 8 shifts (Figure 3.7.2)
- Shift Schedule Import: Enter the required shift schedule information in the specified format into an Excel spreadsheet, and place it in the root directory of the U under the SHIFT folder. Then connect the U to the device to import the shift schedule (Figure 3.7.2)
- Shift Schedule Export: Connect the U, click Shift Schedule Export to export the shift schedule. The exported file is in the root directory of the U under the SHIFT folder. The folder contains shift. xlsx, which includes attendance settings and holidays.
- Holidays: Supports setting holidays on the U, * indicates the lunar calendar. The default is 5 holidays, and up to 30 holidays can be set. The set holidays are not included in the attendance time calculation (Figure 3.7.2)



Holiday

NO.	Name	Start	End
1	New Year's Day	01-01	01-03
2	Spring Festival	01-01*	01-01*
3	Labor Day	05-01	05-03
4	Dragon Boat Festival	05-05*	05-05*
5	Mid-Autumn Festival	08-15*	08-15*
6	National Day	10-01	10-07
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			

Shift Setting

Operation Instructions: Shift name. Maximum length of 16 characters. Type: 0: Normal attendance. 1: Overtime .The ti

NO.	Name	Shift 1			Shift 2			Shift 3			Cross day
		Duty	Off Duty	Type	Duty	Off Duty	Type	Duty	Off Duty	Type	
1	shift1	08:30	12:00	0	13:00	17:30	0	19:00	22:00	0	00:00
2	shift2	00:00	00:00	0	00:00	00:00	0	00:00	00:00	0	00:00
3	shift3	00:00	00:00	0	00:00	00:00	0	00:00	00:00	0	00:00
4	shift4	00:00	00:00	0	00:00	00:00	0	00:00	00:00	0	00:00
5	shift5	00:00	00:00	0	00:00	00:00	0	00:00	00:00	0	00:00
6	shift6	00:00	00:00	0	00:00	00:00	0	00:00	00:00	0	00:00
7	shift7	00:00	00:00	0	00:00	00:00	0	00:00	00:00	0	00:00
8	shift8	00:00	00:00	0	00:00	00:00	0	00:00	00:00	0	00:00

Figure 3.7.2

3.7.3 Attendance Sheet Export

Export the attendance sheet to the ATTEND folder in the U root directory; only export personnel whose shift is not 'no'. The table includes the original record sheet, attendance details sheet, and attendance summary sheet.

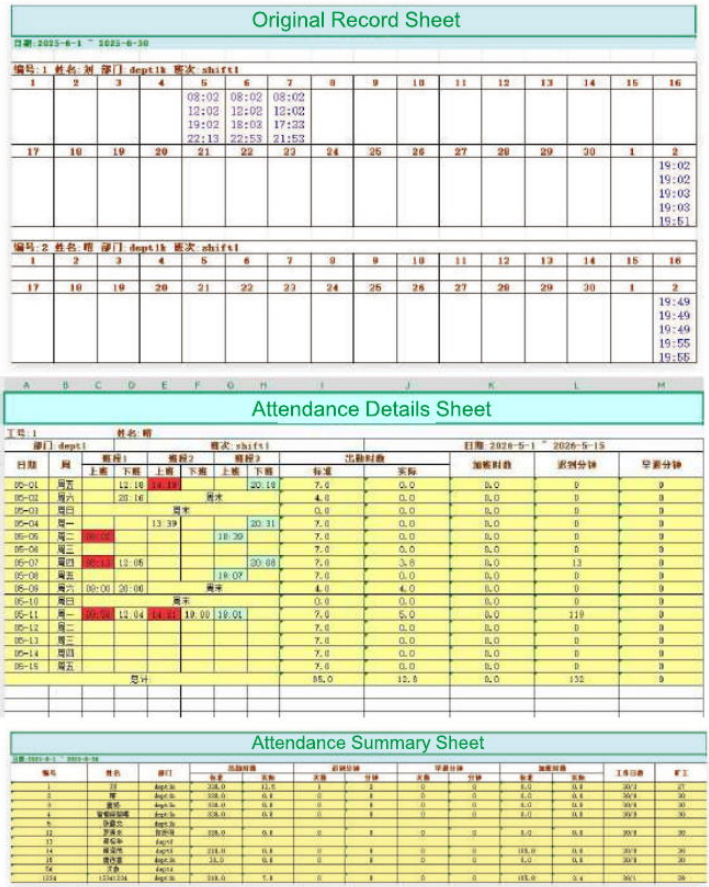


Figure 3.7.3

3.8 SystemSettings

3.8.1 Local Settings

- **Language Settings:** Supports eight languages: Chinese, English, Japanese, Korean, Spanish, Portuguese, Russian, and Arabic. Supports multi-language import, allowing customers to review or add and verify strings for other languages. For specific methods, refer to Chapter 3.9.
- **Time Settings:** When connected to the internet, enabling the "Auto-Settings" button will automatically retrieve the current time. Disabling the button allows for manual time setting. The time zone can also be changed, with the default being UTC+8 (Beijing Time).
- **Screen Settings:** Enabling the "Auto Saver" button and setting a screen saver time will cause the device to enter the screen saver interface after a period of inactivity exceeding the set time. Disabling "Auto Saver" will prevent entering the screen saver interface.Enabling the "Auto Off" button and setting a screen off time will, with "Auto Saver" also enabled, cause the screen to turn off after entering the screen saver interface and a further period of inactivity exceeding the screen off time. With "Auto Saver" disabled, the screen will turn off directly after a period of inactivity exceeding the screen off time.Disabling "Auto Off" prevents the screen from turning off automatically.
- **Magazine Lock Screen:** When disabled, the default screen saver interface is used. When enabled, magazine screen saver pictures will be displayed in a slideshow upon entering the screen saver.
- **Change Magazine Lock Screen:** Imported magazine pictures must be in JPG format with a resolution of 480*853 and a file size less than 100KB. Place the images in the screen folder in the root directory of a USB drive. Then connect the USB drive to the device to change the magazine lock screen pictures.
- **Return to Home Screen:** When enabled, the device will automatically return to the face recognition interface after 30 seconds of inactivity on the settings interface.
- **Home Screen Settings:**
  Face Frame Color: Options include White, Green, and Red. Default is White.
  Show Registered User Count: Selecting "Off" hides the registered user count on the home screen.
  Show IP Address: Selecting "Off" hides the IP address on the home screen.
- **System Maintenance (Scheduled Restart):**
  Monthly: Restarts at the set time on the 1st day of each month.
  Weekly: Restarts at the set time, calculated as 7 days forward from the system time.
  Daily: Restarts at the set time every day.
  None: No scheduled restart operation.
- **Restart System:** Manually restarts the device.
- **Input Method:** 26-key / 9-key.

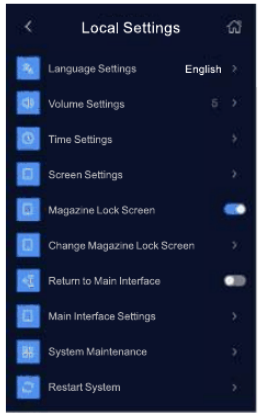


Figure 3.8.1

3.8.2 Advanced Settings

- **Total Administrators:** The maximum number of administrators can be set, up to 255.
- **Verification Mode:** Can be set to any mode, or to a combination of face recognition + card swiping.
- **Disable Face Recognition:** Once enabled, the face recognition function will be deactivated.
- **USB/Wi-Fi Switch:** Turning the switch on activates the external USB port, while turning it off activates the Wi-Fi function.
- **Firmware Upgrade:** Reads the upgrade package from the USB drive to perform a system upgrade.
- **Restore Factory Settings:** Clicking "Confirm" will erase all data and restore the device to its default state.
- **Intercom Icon:** When enabled, the intercom icon will be displayed.

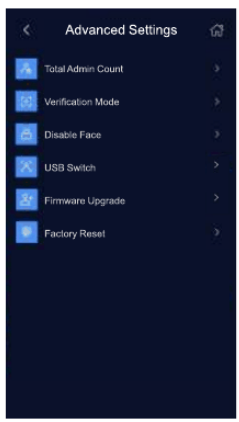


Figure 3.8.2

3.8.3 Intercom Settings

- LAN IP Call: When the switch is turned on, it enables audio and video intercom calls between indoor units within the LAN.
- Router Gateway: After setting this option, the usage range for building number, unit number, and local device number is limited.

(1) Gateway 10.0.0.1 Current Maximum Limit: 10 Buildings, 7 Units, 10 Local Device Numbers. In Normal Mode, the maximum limit can be expanded to: 99 Buildings, 7 Units, 99 Local Device Numbers. In Cross-Zone Mode, the maximum limit can be expanded to: 6 Zones, 63 Buildings, 6 Units, 62 Local Device Numbers.

(2) Gateway 172.16.0.1 Current Maximum Limit: 10 Buildings, 6 Units, 10 Local Device Numbers. The maximum limit can be expanded to: 63 Buildings, 6 Units, 30 Local Device Numbers.

(3) Gateway 192.168.0.1 current maximum limit: 10 buildings, 3 units, 10 local numbers. Maximum limit can be expanded to: 14 buildings, 3 units, 14 local numbers

(4) Gateway 192.168.1.1 current maximum limit: 1 buildings, 1units, 3 local numbers. Maximum limit can be expanded to: 1 buildings 1 units, 3 local numbers

- Building number: The building number where the gate machine is located
- Unit number: The unit number where the gate machine is located
- Local number: The point number of the unit where the gate machine is located
- Call mode: Includes direct call, dialing, and contact list

1. Direct call: Call the room number bound to the room directly
2. Dial: Room number entered on the call dialing interface
3. Contacts: Select the corresponding person to call the room number based on the added contact information

- Sorting Method: This option appears when the call mode is 'Passenger List', with choices including ascending/descending username or call number order
- View Contacts: Add contact persons, up to 500 people
- Monitoring: In LAN IP call mode, when the switch is turned on, indoor units can perform video surveillance on the door unit. In non-LAN IP call mode, when monitoring is enabled, the device displays a third-party SIP server binding on the home screen, allowing video surveillance
- Room Binding: This option appears when the call mode is 'Direct Call', allowing multiple rooms to be called simultaneously after binding. Up to 4 rooms can be supported.
- Central Management Call Number: Set the direct call number for the central management. On the door unit's home screen (in non-direct call mode), click the call button → to dial the interface. The bottom right corner of the interface shows the central management call button, which can be clicked to call the set number. For example: 103 - Call Room 103.
  103: Calling the 103 user on the SIP server side
- Tuya APP binding: Download the Tuya APP on your phone to scan and bind for intercom and door unlocking operations
  Any device call will trigger a call to the Tuya APP

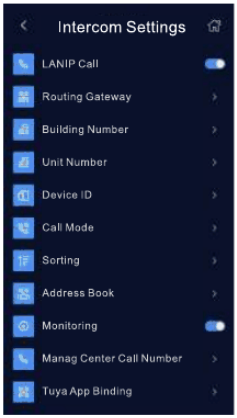


Figure 3.8.3 (1)

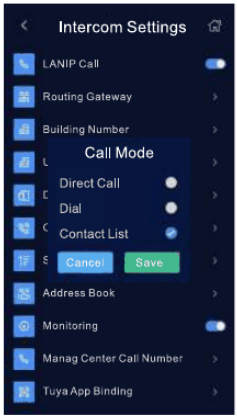


Figure 3.8.4 (2)

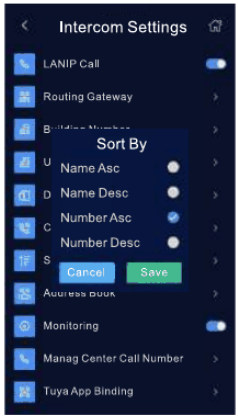


Figure 3.8.5 (3)



Figure 3.8.3 (4)

3.8.4 Recognition Settings

- **Continuous Recognition:** Enables continuous recognition when enabled;
- **Recognition Threshold:** Default value is 54. A higher value indicates a more accurate similarity between the face to be recognized and the saved face image;
- **Liveness Detection:** When checked, detects whether the face is alive;
- **Infrared Image:** When checked, displays an infrared image in a small window in the upper left corner of the face recognition interface;
- **Recognition Level:** High, Medium, and Normal are available. The default is Medium;
- **Recognition Interval:** Default is 1 second. The interval is set to be repeated;
- **Recognition Distance:** Default is 150cm. The setting range is 50cm-150cm;
- **Fill Light Settings:** Default is Automatic. Can be set to Always On, Always Off, or Automatic;
- **Authentication Effects:** Includes options such as name announcement, greeting, avatar display, full name display, ID number display, and stranger voice prompts. These can be combined freely;
- **Stranger Verification:** When enabled, performs stranger recognition;
- **Attendance Mode:** When enabled, successful face recognition does not display a pop-up message, only the name is shown;

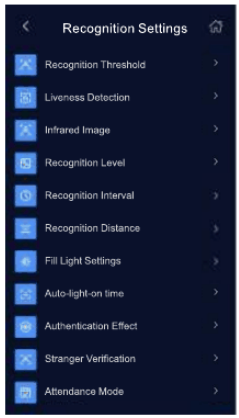


Figure 3.8.4

3.8.5 Access Control Setting

- **Identify door opening:** When enabled, the door will open upon successful identification. When disabled, successful identification will not trigger door opening.
- **Open Door for Strangers:** When enabled, the door will also open for recognized strangers (requires Stranger Verification to be enabled).
- **Manual Door Release:** Click to open the door instantly.
- **Access Type:** Can be set to "Exit" or "Entry".
- **Time Period Settings:**

1. **Daily Period :** Allows editing of up to eight daily period types. Each type can divide a day into up to five time segments.
2. **Weekly Period :** Allows editing of up to eight weekly period types. For each type, you can select the daily period for each day from Monday to Sunday.
3. **Access Time Period Setting:** Allows setting the access time period for each day from Monday to Sunday (default is 24/7 access, or you can select one of the eight daily period types).
4. **Door Always Open Time:** Allows setting the "Door Always Open" time period for each day from Monday to Sunday (default is "No", or you can select one of the eight daily period types).

- **Wiegand Mode:** Can be set to input or output (supports only one channel).
- **Wiegand Format:** Supports Wiegand 26-bit/34-bit/42-bit/50-bit/58-bit/66-bit/37-bit.
- **Card Number Display Format:** Decimal, Wiegand format, or hexadecimal.
- **Card Number Reversal:** The read card number is reversed and displayed according to the selected format.
- **Wiegand Output Reversal:** The output data, such as card number or ID, is reversed.
- **Wiegand Output:** Can be set to output the recognized ID or card number upon successful identification.
- **Door Opening Delay (Relay):** The delay time before the door opens; selectable from 0 to 100 seconds.

- **Door Magnet Alarm:** If a user pushes the door open within the door opening delay time, the door contact alarm timer starts. If the door contact is re-locked within the door contact delay time, no alarm is triggered. If the door remains unlocked after the door contact delay time elapses, a door contact alarm is activated. Check this box to enable the alarm function; leave unchecked to disable it.
- **Device Door Opening Password:** Modify the device's door opening password; the default is 888888. The password can be changed.
- **Door Button Switch:** When enabled, an external button can be used to open the door.
- **Other Door Opening Methods:** By default, the personal door opening password is enabled.

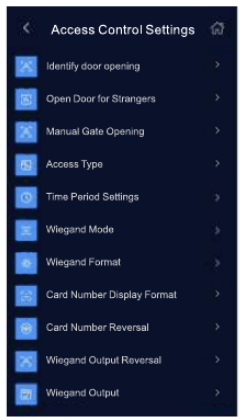


Figure 3.8.5

3.8.6 Data Management

- Revoke administrator Permissions: Restore all administrators in the device to regularusers

3.9 Device Information

- Data capacity information: View the number of administrators, registered users, faces, card numbers, passwords, and attendance records (Figure 3.9.1).

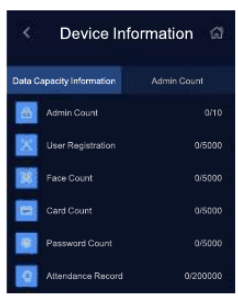


Figure 3.9.1 (5 inch)

- **About the Device:** Displays device information including serial number, MAC address, firmware version, storage capacity, and algorithm version (Figure 3.9.2).
- **Import Language (Test):** This feature allows users to import translated multi-language text strings and audio files for previewing, or to replace the startup logo and screensaver images. Follow these steps:

A. Contact our company to obtain the USB import resource package named "resource_830d" (place this folder in the root directory of your USB drive).

B. Prepare the folder contents for replacement according to the instructions, then connect the USB drive to the device.

C. Click Import Language (Test) to complete the import and immediately view the results. If there is no response after clicking, verify in System Settings > Advanced Settings whether the USB switch is turned ON and that the home screen displays the USB icon.

D. Once successfully imported, the multi-language text strings, startup logo, and screensaver images will take effect immediately. If the translated multi-language text strings are confirmed to be correct, the corresponding files can be provided to our company for updating the multi-language package.

- **Check for Updates:** Checks if a new firmware update is available.



Figure 3.9.2

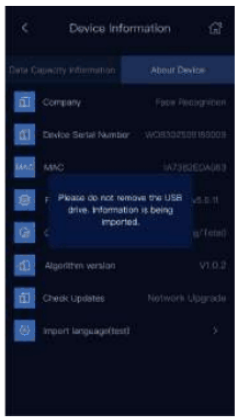


Figure 3.9.3