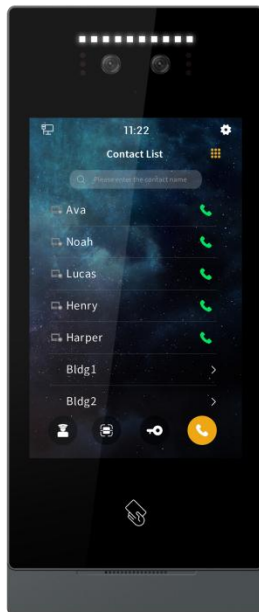


User Manual

Outdoor Station



S Series 8" Facial Recognition Outdoor Station User Manual_V1.3

Model Number:SO801 SO801-P48



Attentions

1、 Please keep devices away from strong magnetic field , high temperature , wet environment ;



2、 Please do not fall the devices to the ground or make them get hard impact ;



3、 Please do not use wet cloth or volatile reagent to wipe the devices ;



4、 Please do not disassemble the devices.

Contents

| | |
|---|-----------|
| Chapter 1 Overview | 1 |
| 1.1 Features | 1 |
| 1.2 Specification | 2 |
| Chapter 2 Appearance and Interface | 3 |
| 2.1 Front View | 3 |
| 2.2 Product Dimension | 4 |
| 2.3 Rear View | 5 |
| 2.3.1 SO801 | 5 |
| 2.3.2 SO801-P48 (48V POE) | 7 |
| Chapter 3 Installation | 9 |
| 3.1 Installation Steps | 9 |
| 3.2 Installation Height | 12 |
| 3.3 Wiring Diagrams | 12 |
| Chapter 4 Basic Functions | 15 |
| 4.1 Call Management Center | 15 |
| 4.2 Face recognition & QR code Unlocking | 16 |
| 4.3 Public password / unlock code unlocking | 16 |
| 4.4 Name List Call & Dial Call | 17 |
| 4.5 Status prompt | 18 |
| Chapter 5 System Setting | 19 |
| 5.1 Sound Setting | 19 |
| 5.2 Time setting | 20 |
| 5.3 Language setting | 21 |
| 5.4 Display settings | 21 |
| 5.4.1 Wallpaper selection | 21 |
| 5.5 Access control setting | 22 |
| 5.5.1 Unlock Setting | 22 |
| 5.5.2 Face management | 23 |
| 5.5.3 Access card management | 24 |
| 5.6 Call Setting | 27 |
| 5.7 Network Setting | 30 |
| 5.8 Alarm Setting | 31 |
| 5.9 Engineering Setting | 32 |

| | |
|---|-----------|
| 5.9.1 Device Name Setting | 33 |
| 5.9.2 Cloud Server Settings | 33 |
| 5.9.3 Engineering Password Setting | 34 |
| 5.9.4 Face recognition Setting | 35 |
| 5.9.5 Motion detection Setting | 36 |
| 5.9.6 Lock 2 Interface Setting | 37 |
| 5.9.7 12V Output Setting | 38 |
| 5.9.8 Wiegand setup | 38 |
| 5.9.9 Video Bit Rate Setting | 39 |
| 5.9.10 Community ID Setting | 39 |
| 5.9.11 RTSP Setting | 40 |
| 5.9.12 Device Lock Setting | 41 |
| 5.9.13 Equipment Self Inspection | 42 |
| 5.10 About | 42 |
| 5.10.1 Device Information | 42 |
| 5.10.2 Restart | 43 |
| 5.10.3 Restoring factory Setting | 43 |
| Chapter 6 Address book configuration | 44 |
| 6.1 Address book generation | 44 |
| 6.2 Address book synchronization | 44 |
| 6.3 Address Book Application | 46 |
| Chapter 7 Web Server | 47 |
| 7.1 Web Server login | 47 |
| 7.2 Time setting | 48 |
| 7.3 Device language setting | 49 |
| 7.4 Network setting | 50 |
| 7.5 Alarm setting | 51 |
| 7.6 Unlock management | 51 |
| 7.6.1 Unlock setting | 51 |
| 7.6.2 Unlock record | 52 |
| 7.7 Access card management | 52 |
| 7.8 Call Setting | 53 |
| 7.8.1 Contact setting | 53 |
| 7.8.2 Contact range setting | 54 |

| | |
|--|----|
| 7.8.3 Management center setting | 55 |
| 7.8.4 Call function switch | 55 |
| 7.9 Engineering setting | 56 |
| 7.10 About | 57 |
| 7.11 Web Login password modification | 58 |

Chapter 1 Overview

This outdoor station is the main component of the S series digital video intercom system. It is connected with indoor stations or guard units for communication and unlocking by standard CAT5 cables.

1.1 Features

- Support SIP protocol
- 8-inch IPS display
- auto fill light with high luminance LED
- Using binocular wide dynamic range + near-infrared camera, Questyle face recognition algorithm, supports multiple face detection, face tracking, liveness detection, mask recognition and other functions. In the standard environment, when there are 10,000 people in the database, the face recognition rate is less than 0.5s, and the false recognition rate is 0.1%;
- Support 9 unlock modes. password unlock, IC card unlock, button unlock, surveillance/call unlock, face recognition unlock, QR code unlock, APP unlock, face recognition+ public password combination unlock, face recognition + IC card combination unlock..
- Compatible with cloud server management, LAN server management, serverless management and multiple server management modes
- Support alarm input, alarm output and support 12V output 250mA MAX
- Support human proximity detection
- Support elevator linkage
- Support Wiegand settings
- Support door status detection and timeout alarm, disconnection alarm and tamper alarm
- Support 2 locks management
- Support OTA online upgrade

1.2 Specification

Operation System: Linux

CPU: 2 x Cortex-A7 1.2GHz 32K

RAM: 512MB

Storage: 4GB

Local face library: 20,000

Working Parameter

Working Voltage: DC 18~30V

Static current: < 150mA (DC24V)

Working Current: < 400mA (DC24V)

Working temperature: -20°C - +70°C

Storage temperature: -30°C - +70°C

Humidity: ≤95%, no condensation

Camera

Type: CMOS

Pixel: 2MP

FOV: H: 61degree、V:35 degree

focal distance: 4.3mm

Light filling mode: infrared 850nm + white light

minimal illumination: ≤0.15Lux/F2.0

Display

Type: LCD

Size: 8"

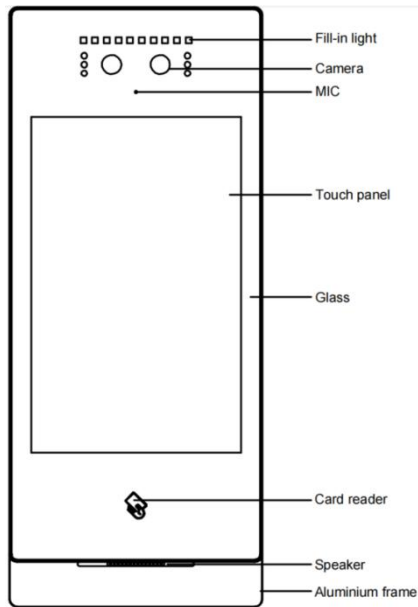
Resolution: 800*1280

Product Dimension

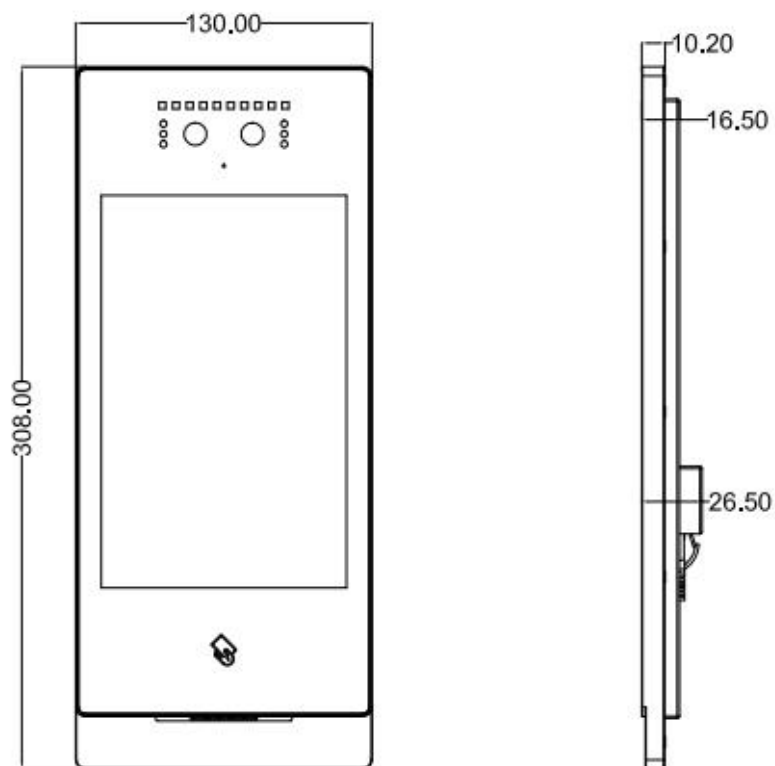
(W/H/D): 130×308×26.50 mm

Chapter 2 Appearance and Interface

2.1 Front View

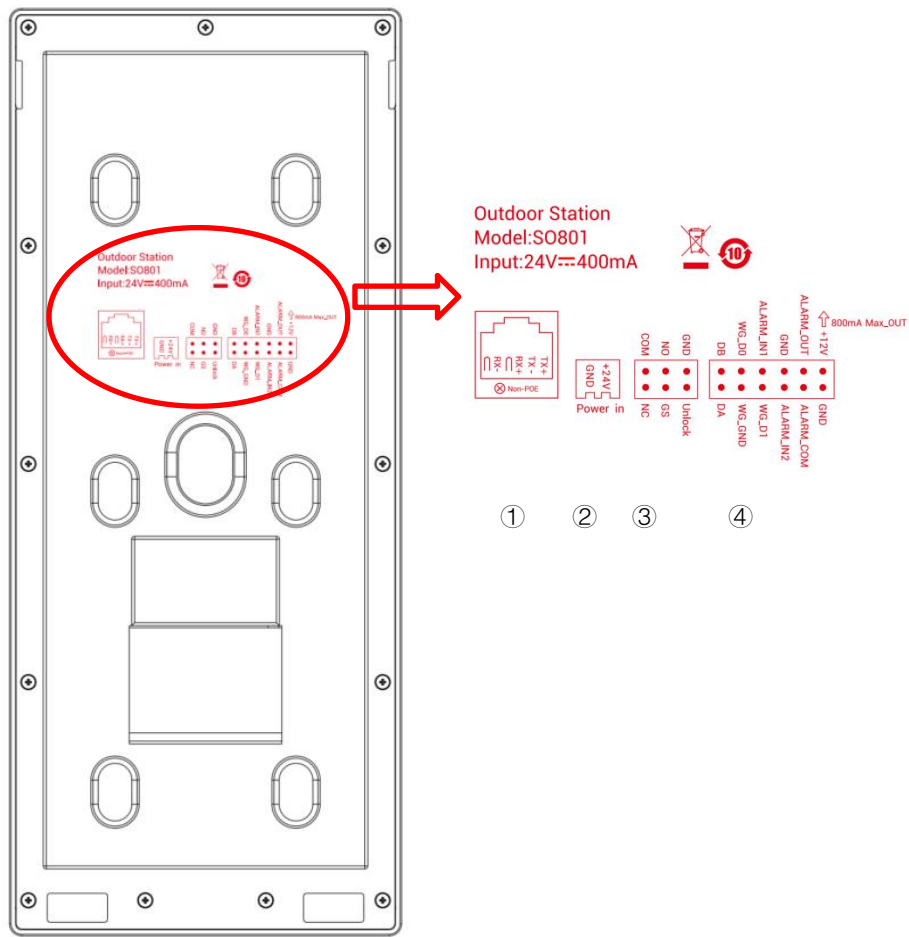


2.2 Product Dimension



2.3 Rear View

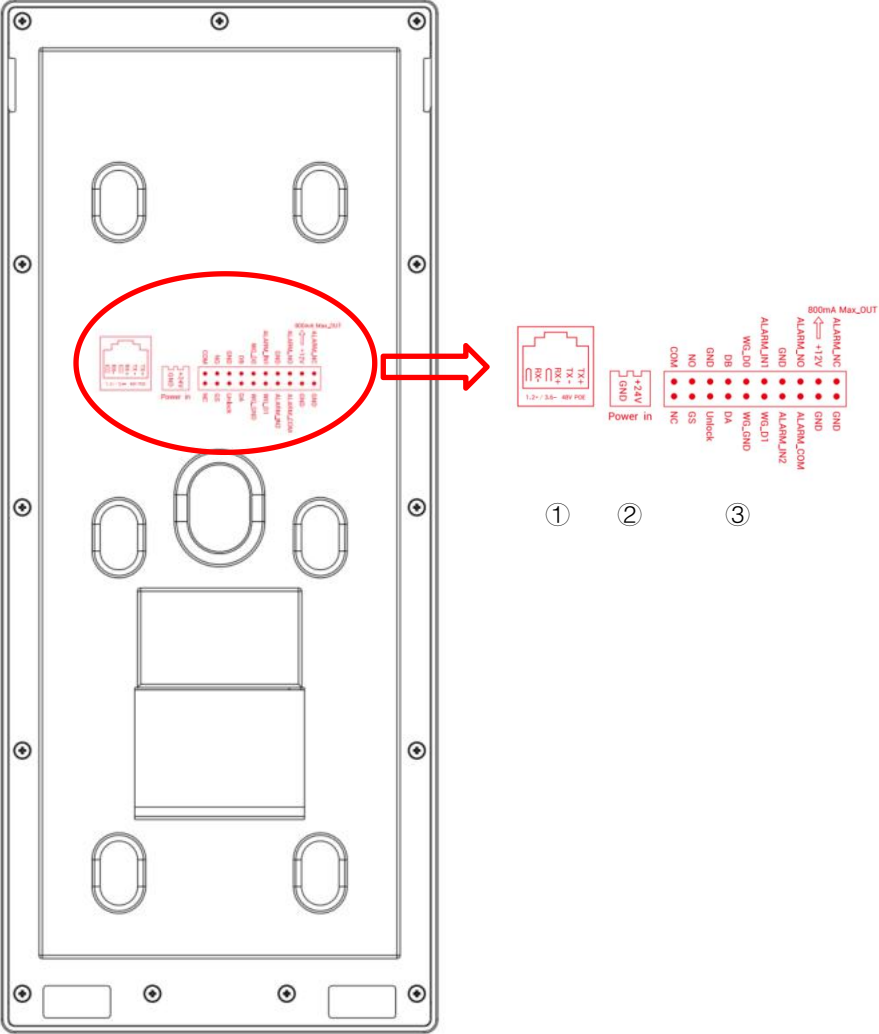
2.3.1 SO801



| | |
|---|---|
| ① | RJ45 network interface |
| ② | Power input interface DC 24V (independent power supply interface, voltage range DC 18-30 V). |
| ③ | COM、NO、NC： Common terminal, normally open terminal and normally closed terminal of the unlocking relay. |

| | |
|---|--|
| | <p>GS: Door state detection input terminal.</p> <p>UNLOCK、GND: Door unlock switch input</p> |
| ④ | <p>WG-GND、WG-D0、WG-D1: Weigen interface</p> <p>DA、DB: 485 communication interface</p> <p>ALARM_IN1: Alarm input 1</p> <p>ALARM_IN2: Alarm input 2</p> <p>GND: GND</p> <p>ALARM_OUT: Lock2 Interface normally open</p> <p>ALARM_COM: Lock2 interface common port</p> <p>GND: GND</p> <p>+12V_OUT: +12V power output</p> |

2.3.2 SO801-P48 (48V POE)



| | |
|---|---|
| ① | RJ45 network interface(Standard 48V PoE power supply) |
| ② | Power input interface DC 24V (independent power supply interface, voltage range DC 18-30 V). |
| ③ | <p>COM、NO、NC: Common terminal, normally open terminal and normally closed terminal of the unlocking relay.</p> <p>GS: Door state detection input terminal.</p> <p>UNLOCK、GND: Door unlock switch input</p> <p>WG-GND、WG-D0、WG-D1: Weigen interface</p> <p>DA、DB: 485 communication interface</p> <p>ALARM_IN1: Alarm input 1</p> <p>ALARM_IN2: Alarm input 2</p> <p>GND: GND</p> <p>ALARM_NO: Lock2 Interface normally open</p> <p>ALARM_COM: Lock2 interface common port</p> <p>ALARM_NC: Lock2 interface common port</p> <p>GND: GND</p> <p>+12V_OUT: +12V power output</p> |

Chapter 3 Installation

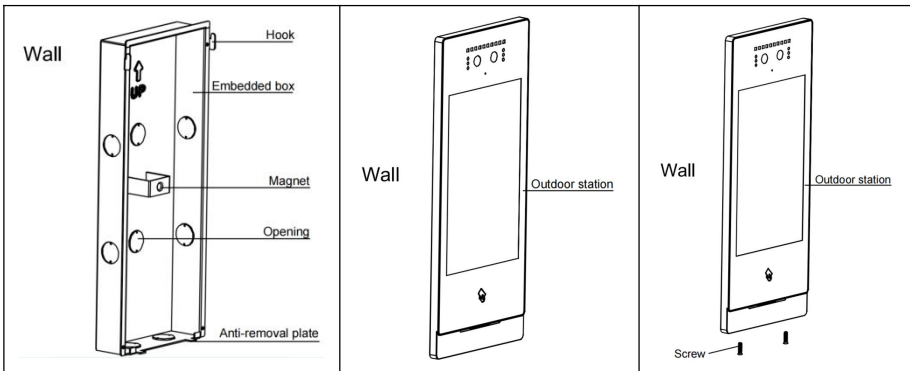
3.1 Installation Steps

(1) Method 1: Embedded in Wall

Step 1: Put embedded box into preformed groove and get cable out through the opening (as shown in Picture 1). Embedded box dimension(W/H/D) is 114 x 292.5 x 38 (mm).

Step 2: After connecting cable to outdoor station, match slot on rear cover of the outdoor station to align with snap on embedded box and snap on the outdoor station (as shown in Picture 2).

Step 3: Fix screws at the bottom of aluminium panel (as is shown in Picture 3).

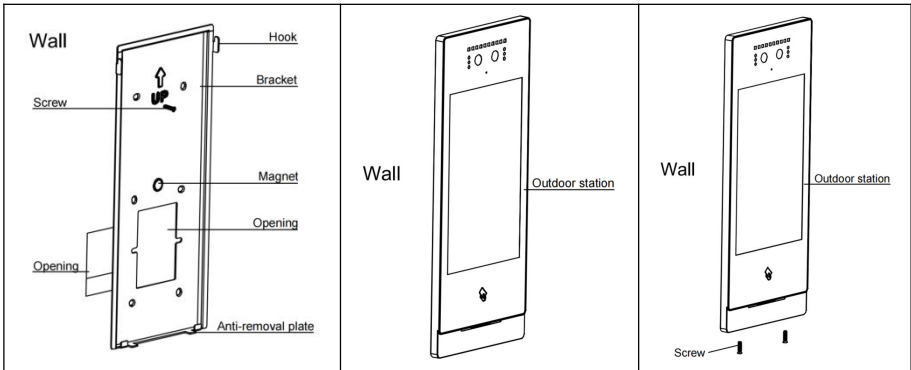


(2) Method 2: Wall-mounted

Step 1: Locate wall bracket according to the opening for cable, match 6 mounting holes on wall bracket, drill corresponding holes in the wall, insert expansion plugs and finally tighten the bracket with screws(as shown in Picture 1).

Step 2: After connecting cable to outdoor station, match slot on rear cover of the outdoor station to align with snap on embedded box and snap on the outdoor station (as shown in Picture 2).

Step 3: Fix screws at the bottom of aluminium panel (as is shown in Picture 3).



(3) Mode 3: Column

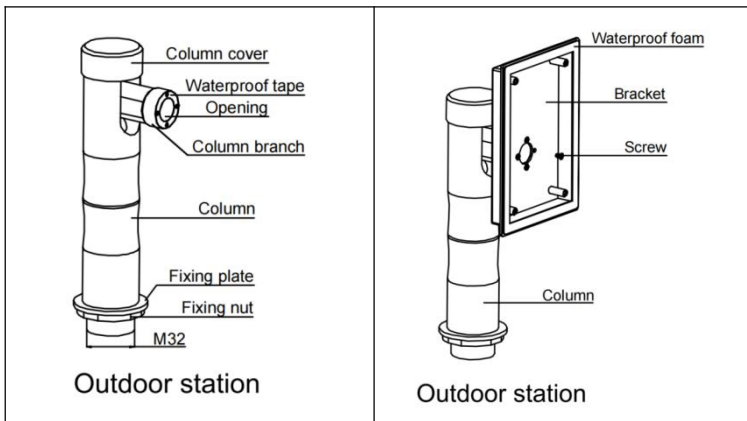
It's required to open a $\Phi 33\text{mm}$ hole in the device that customer provided, get the cable between customer-supplied device and the host out through opening, and then get cable out through the column. Assemble the column and gum a waterproof sticker to the fixed part of the column and column bracket (as shown in Picture 1).

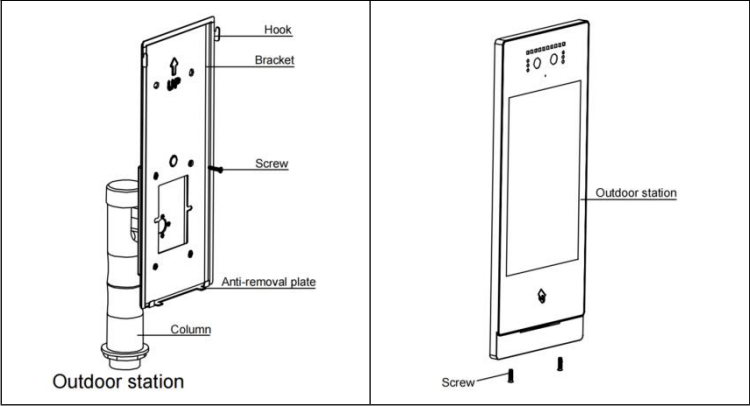
Step 2: Fix column bracket to the column with screws and attach waterproof foam to the end of column bracket (as shown in Picture 2).

Step 3: The wall bracket shall be screwed to column bracket (as shown in Picture 3).

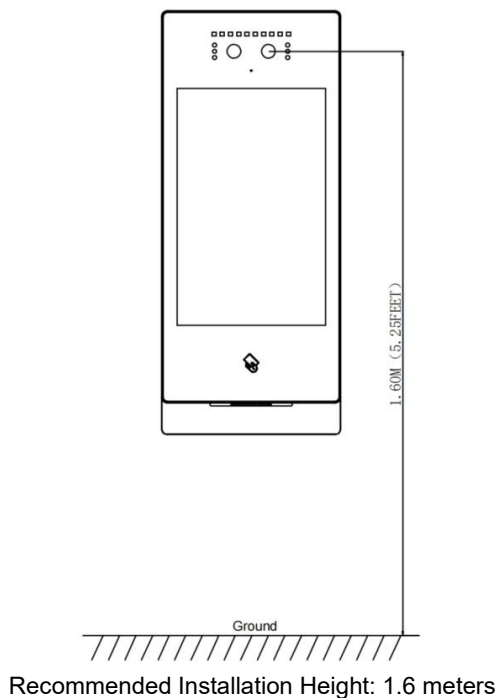
Step 4: Fix screws at the bottom of aluminium panel (as is shown in Picture 4).

Step 5: Pass the column through the hole opened in customer-supplied device and fix the column to it with column fixing nut.



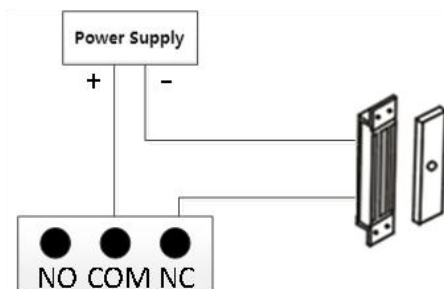


3.2 Installation Height

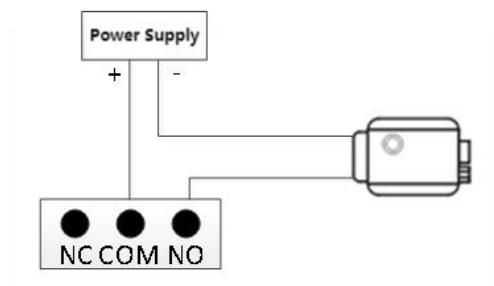


3.3 Wiring Diagrams

(1) Wiring for Signal Unlock Mode



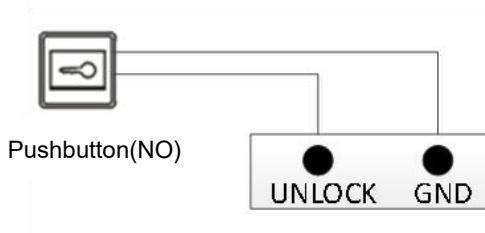
Wiring for normally closed type lock(Magnetic Lock)



Wiring for normally open type lock(Electronic lock)

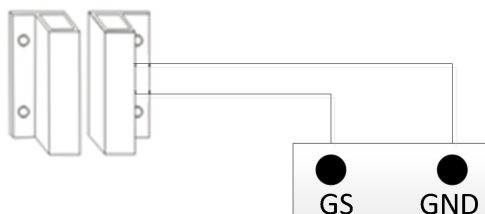
Note: If device is used for power supply under signal unlock mode, the device can only be powered by extra power supply. At the mean time, lock input current shall be less than 800mA, otherwise the equipment may be damaged.

(2) Wiring for Exit Button Unlock Mode



Note: This wiring is not polarised.

(3) Wiring for Door Status Alarm



Normally closed type

Note: The door status alarm function can be switched off in two ways.

- ① Grounding GS port of the host.

- ② Enter "Door Status Alarm" and turn off the door status alarm switch.

Chapter 4 Basic Functions

(1) When the device is powered on for the first time, the user needs to select the language and set up the network.

After restoring the factory settings, the first power on can select language settings, network settings, and automatic configuration mode switch.


Automatic configuration mode: This machine can discover other S-series devices in the same network segment. For small system networking within 16pcs, automatic discovery is preferred. It is a plug and play mode that does not require complicated configuration. Networking requires Router routers to allocate IP addresses to each device, and devices use MDNS protocol to discover each other.

Address book mode: To disable automatic configuration mode, address book mode is required. The devices connected to the address book network need to download a unified address book configuration table, which can be pushed locally by Update&Configuration Tool or pulled online from the intelligent management platform. For detailed functions, please refer to Chapter 5.11 Address Book Configuration and Usage Instructions.

(2) The functions below the main interface can be turned on or off in the system settings.

The homepage management machine, facial recognition unlocking, password unlocking, communication list calling, and dialing call shortcut functions can be turned on or off through engineering settings.

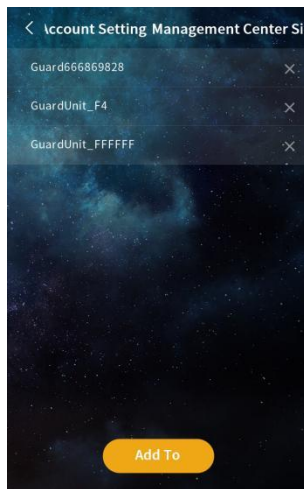
4.1 Call Management Center

Tap icon  to call the SIP account of the management center, and the outdoor station has ring back tones. If there is no answer from the management center within 30s, the call will be ended automatically.

Note: Support calling multiple management center SIP accounts at the same time, set in "Call Settings-Management Center SIP Account".




Call Management Center SIP account



Management center SIP account list


4.2 Face recognition & QR code Unlocking

Tap icon  to scan the face or the QR code for unlocking. Once the face and QR code is recognized as correct, the door will be unlocked.

Note:

- ① When the user whose face has been registered approaches and faces the camera of the outdoor station, the device automatically enters face recognition unlock mode.
- ② The QR code for unlocking is generated by the mobile APP. In the mode of not using the server, there is no QR code unlock function.

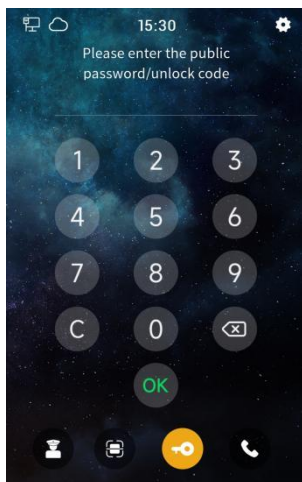
4.3 Public password / unlock code unlocking

Tap icon  to enter the public password/ unlock code to unlock. Once the password/code is recognized as correct, the door will be unlocked.

Note:


- ① The default public password is 666666, which can be modified in "Access Control Settings-Unlock Settings".


- ② The unlock code is generated by the mobile APP. In the mode of not using the server, there is no unlock code function.
- ③ Both public password unlocking and unlock code unlocking can be turned on or off in the system settings.



Public password / lock code unlocking

4.4 Name List Call & Dial Call

Tap icon  to call the corresponding resident through the name list. Click the

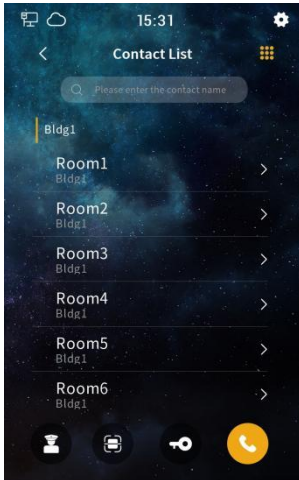
icon  in the upper right corner to switch from the name list call interface to the dial call interface. You can call the corresponding residents by entering the SIP account username corresponding to the device, for example, SIP account "sip: 00010001

1 @ 192.168.150.100:8060 ", enter" 000100011 "to call. When setting up a call and enabling the building dial-up call function, group call functionality can be achieved. For example, in the case of multiple extensions in one household, if there is extension 1 "SIP: 000100011@192.168.150.100 8060 ", extension 2" SIP: 000100012@192.168.150.101 8060 ", extension 3" SIP: 000100012@192.168.150.102 8060 ", extension 4" SIP: 000100012@192.168.150.103 8060 "belongs to Unit 0001 and Unit 0001 indoor units. For calls to the unit's outdoor, you can input 0001 to make group calls to the same indoor unit. For the wall outdoor, it is necessary to input 0001001 the unit number and room

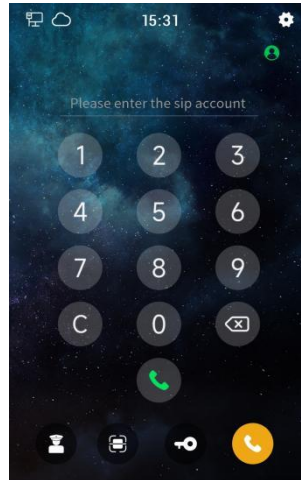
number to achieve group calling of indoor units in the same household.

Note:

- ① The management center or the indoor station can control the unlocking of the outdoor station when they are in communication.
- ② Both name list calling and dial calling can be turned on or off in the system settings.





Name list call




Dail Call

4.5 Status prompt

Network status: The "Computer"  icon indicates the network connection status, no "Computer" icon indicates the network is not connected, and an exclamation mark on the "Computer" icon indicates a network IP conflict.

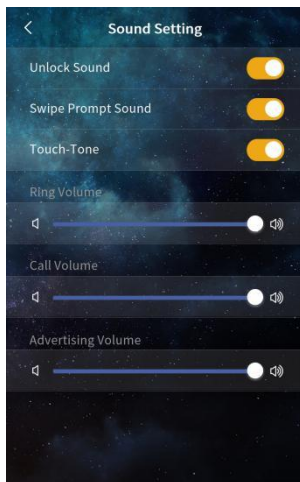
Cloud service status: The "Cloud"  icon indicates that the network is connected to the cloud server, no "Cloud" icon indicates that the cloud service area is not configured, and the blinking exclamation mark of the "Cloud" icon indicates that the cloud service area cannot be connected.

Chapter 5 System Setting

Tap icon  in the upper right corner to enter the system setting interface by inputting the correct engineering password (the default is 801801, which can be modified).

5.1 Sound Setting

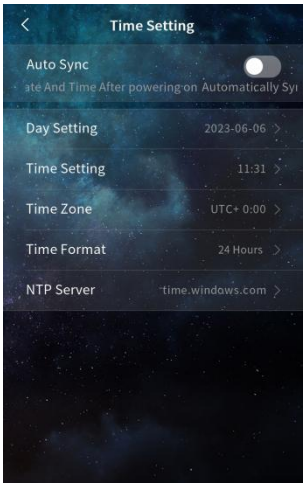
- (1) Unlock prompt sound: After it's enabled, the device will have sound feedback when the door is unlocked.
- (2) Card swiping prompt sound: After it's enabled, the device will have sound feedback when the user swipes the card.
- (3) Touch-Tone: After it's enabled, the device will have sound feedback when user clicks the screen.
- (4) Ringtone volume: The volume of the ringtone can be adjusted.
- (5) Call volume: The volume of the call can be adjusted.
- (6) Advertisement volume: The volume of the advertisement can be adjusted.



Sound setting

5.2 Time setting

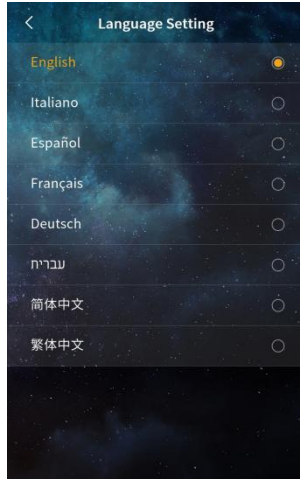
- (1) Automatic synchronization and manual setting: If automatic synchronization is enabled, the device will automatically synchronize the network date and time. If automatic synchronization is disabled, you can manually set the year, month, day, hour and minutes.
- (2) Time zone: Select the corresponding time zone according to the country you are in. After the automatic time synchronization is enabled, the device will convert the local time according to the set NTP server and time zone.
- (3) Time format: 24-hour or 12-hour format can be selected.
- (4) NTP server: Enable the device to obtain accurate clock time from the set NTP server address.



Time setting

5.3 Language setting

Options: English, Italiano, Français, Deutsch, עברית, 简体中文, 繁體中文, Russian, Portuguese, Turkish, Vietnamese.

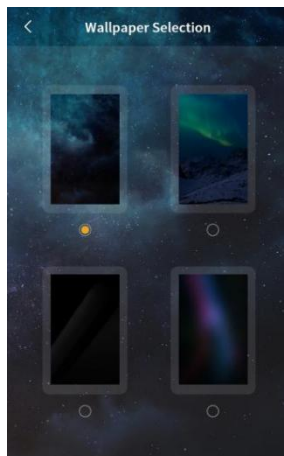


Language setting

5.4 Display settings

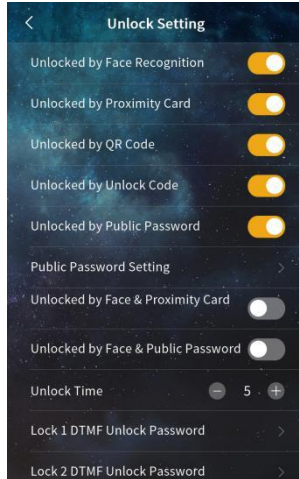
5.4.1 Wallpaper selection

Changeable wallpaper. Custom wallpaper configuration can be done through the Update & Configuration Tool.



5.5 Access control setting

5.5.1 Unlock Setting



Unock setting

(1) Face recognition unlocking: After this option is selected, users with registered faces can unlock the door through the device's camera.

(2) IC card unlocking: After this option is selected, users can unlock the door by putting the registered IC card close to the card swiping area of the outdoor station.

(3) QR code unlocking: After this option is selected, users can unlock the door by scanning the QR code generated by the mobile APP through the device at the "main page - face recognition & QR code unlocking".

Note: When the server mode is not used, there is no QR code unlock function.

(4) Unlock code unlocking: After this option is selected, users can unlock the door by entering the unlock code at the "Main Page-Public Password/Unlock Code".

Note: When the server mode is not used, there is no unlock code function.

(5) Public password unlock: After this option is selected, users can unlock the door by entering the public password at the "main page - public password/unlock code".

(6) Public password setting: The public password can be modified.

(7) Face recognition + IC card combination unlock: After this option is selected, the

device will simultaneously enable face recognition and IC card unlock function. Door will be unlocked only with correct face recognition and IC card.

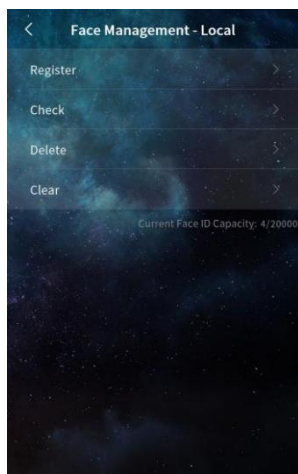
(8) Face recognition+ public password combination unlock: After this option is selected, the device will simultaneously enable face recognition and public password unlock function. Door will be unlocked only with correct face recognition and public password.

(9) Unlocking time: The duration of door unlocking can be modified, and the door will be automatically closed after timeout. The optional range is 1-60s.

(10) Lock 1/Lock 2 DTMF unlock password: Set the DTMF unlock password for Lock 1/Lock 2, the default for Lock 1 is 666666, and the default for Lock 2 is 888888. Only when the DTMF password of the outdoor station and the indoor unit are set consistently, the outdoor station can unlock lock 1/lock 2.

5.5.2 Face management

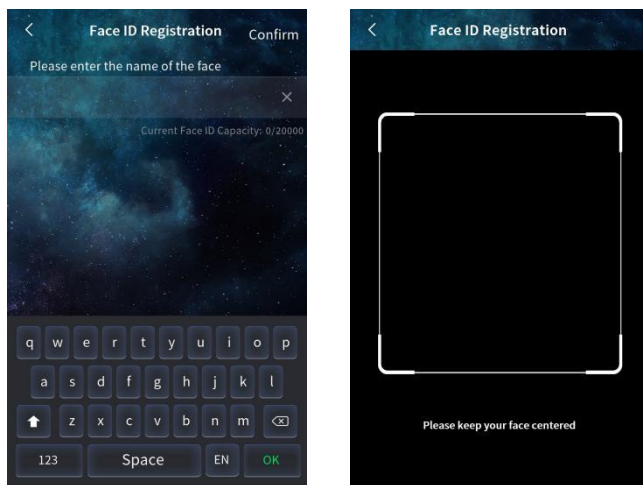
You can register, check, delete and clear face information on the outdoor station. In the default server or custom server mode, the face data of the outdoor station is automatically synchronized with the platform. The maximum face storage capacity is 20,000.



Face management

(1) Register: In the face registration interface, first enter the name of the face, and then click Confirm to register your face by putting your face in front of the camera. When the

outdoor station prompts "registered successfully" means face is registered successfully.

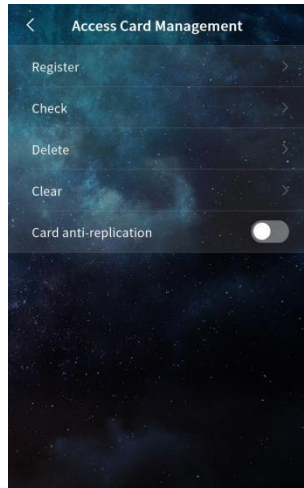


Face registration

- (2) Check: Enter the face name in the search box to check the corresponding face information.
- (3) Delete: Enter the face name in the search box to delete the corresponding face information.
- (4) Clear: The face data of this device can be cleared.
- (5) Face photo saving: When this option is turned off, the outdoor station will not save face photos and delete existing face photos. When this option is turned on, you can view face photos saved on the device.

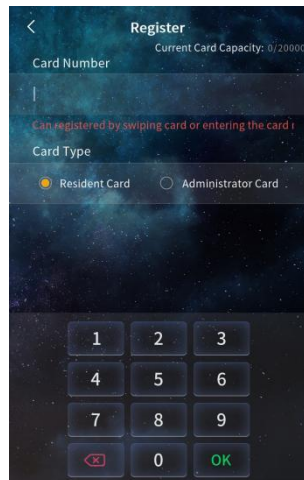
5.5.3 Access card management

You can register, check, delete and clear access card information on the outdoor station. In the default server or custom server mode, the card data of the outdoor station is automatically synchronized with the platform. The maximum card storage capacity is 20,000.



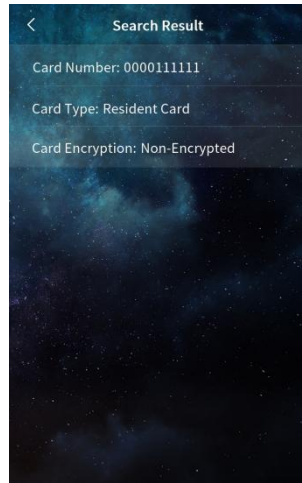
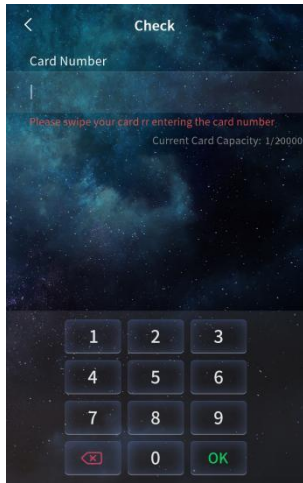
Access card management

(1) Register: In the card registration interface, first swipe the card or enter the card number, select the card type (resident card/administrator card), click OK. When the outdoor station prompts "registered successfully" means card is registered successfully.



Access card registration

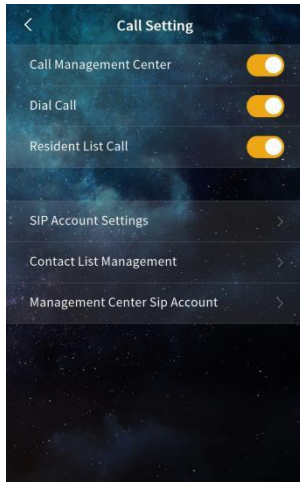
(2) Check: By swiping the card or entering the card number in the search box, you can check the corresponding access card information.



Check access card

- (3) Delete: Swipe the card or enter the card number in the search box then can delete the corresponding access card information.
- (4) Clear: It can erase the user card/ Admin card data of the device
- (5) Card replication prevention: After this option is enabled, the registered card is encrypted and cannot be copied.

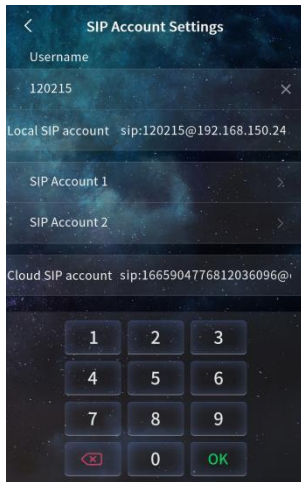
5.6 Call Setting



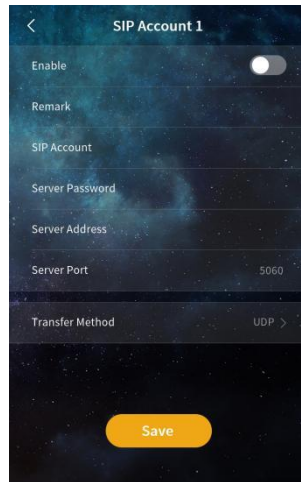
call setting

- (1) Call Management Center: After this function is enabled, the function is enabled on the Mainly Interface , and you can tap to call the management center.
- (2) Dial call: After this item is enabled, the function is enabled on the main screen, and the SIP account can be entered to call the corresponding household.
- (3) Building dial-up call: When enabling dial-up call, building dial-up call will also be selected. After enabling it, regular abbreviated dial-up call will be used, which can achieve group call function. For example, in the case of multiple extensions in one household, if there is extension 1 "SIP: 000100011@192.168.150.100 8060 ", extension 2" SIP: 000100012@192.168.150.101 8060 ", extension 3" SIP: 000100012@192.168.150.102 8060 ", extension 4" SIP: 000100012@192.168.150.103 8060 "belongs to Unit 0001 and Unit 0001 indoor units. For calls to the unit's outdoor, you can input 0001 to make group calls to the same indoor unit. For the wall outdoor, it is necessary to input 00010001 the unit number and room number to achieve group calling of indoor units in the same household. When closing building dial-up calls, only SIP account slips can be entered to call the corresponding devices,For example, input 000100011 to call 1 unit, 1 indoor unit. Rule room number address book mode, detailed functions can be found in the address book configuration and usage instructions.

- (4) Contact list call: After this is enabled, this function is enabled in the main interface, click the contact list to call the corresponding household.
- (5) SIP Account Settings
- User name: Enter the user name to configure the local SIP account for dial-up calls.
Note: It is not allowed to be the same account as another user in the same network.
 - Local SIP account: Displays the local SIP account generated by the local user name and IP address for calling accounts on the same network.
 - SIP Account 1 and 2: Manually configure SIP account information and select whether to enable it. Need to enter the user name, server password, server address and server port, select the transmission mode (UDP, TLS); You can also use the account information of the address book by setting the device name.
 - Cloud intercom SIP account: Displays the cloud intercom SIP account assigned by the server to the device when the device is connected to the cloud server.

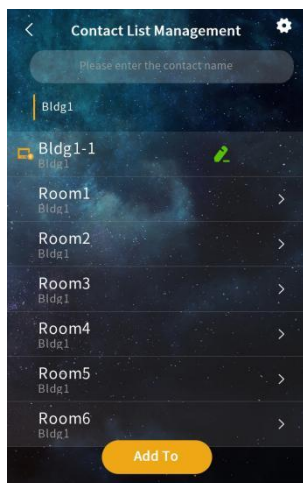


SIP Account Settings



SIP Account 1 & 2

- (6) Contact list management

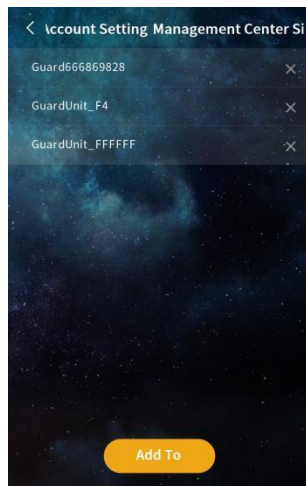


Contact List Management

Displays information about the current contact. Contacts include devices discovered after automatic configuration is enabled, devices imported from the address book, and devices manually added.

- Search: You can fuzzy search for contacts in the list.
- Setting: Select whether to display contact profile pictures. Select whether to set the display range of the communication list. After this item is disabled, all contacts are displayed. After this item is enabled, you can select the same group of contacts to be displayed, or select the contacts to be displayed.
- Add: You can add contacts on the local device by entering remarks, SIP account, and owning group. You can add a group on the local device by setting remarks, group call, and owning group.
- Edit: You can modify the information about the contact.
- Delete: Delete the contact data. Note: Devices discovered by enabling automatic configuration cannot be deleted when they are online. Devices imported through the address book cannot be deleted either.

(7) Account Setting Management Center SIP



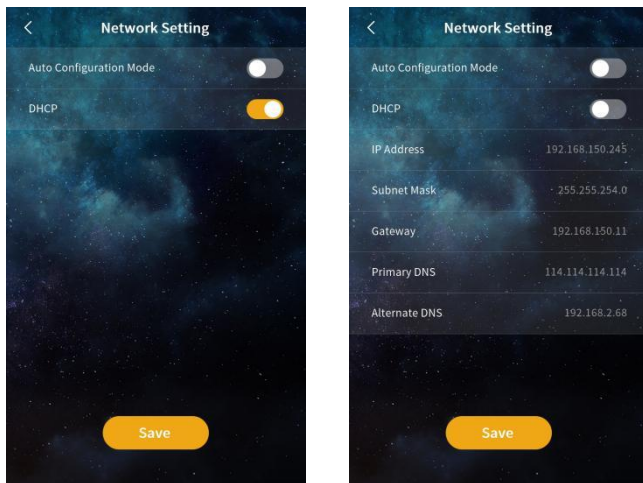
Account Setting Management Center SIP

The SIP account of the selected manager is displayed. When a user clicks the call Manager, the manager SIP account in the list is called simultaneously.

- Add: Click “Add To”, select devices, and add a maximum 10 SIP accounts can be the listed of SIP accounts in the manager.

5.7 Network Setting.

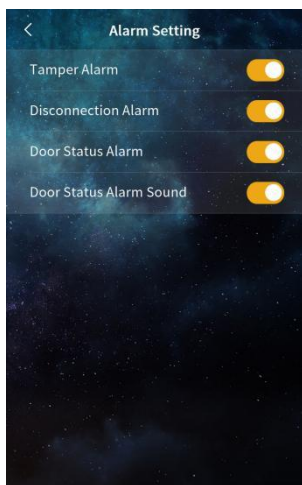
- (1) Automatic configuration mode: After this parameter is enabled, other S-series devices on the same network segment can be discovered.
- (2) DHCP: After disabling the network, it needs manually configuring the network and entering the IP address, sub-netting mask, gateway, and DNS.



Network setting

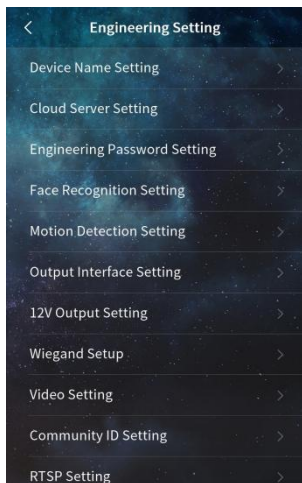
5.8 Alarm Setting.

- (1) Tamper alarm: After this item is turned on, if the device is dismantled by external force, the device will sound an alarm tone.
- (2) Disconnection alarm: After this item is enabled, if the device disconnects, the device will sound an alarm tone and the status bar displays the disconnection icon.
- (3) Door status alarm and door status alarm tone: After opening the door status alarm and door status alarm tone, if the device detects that the door is open for more than 120 seconds, the device will sound the alarm tone.



Alarm setting

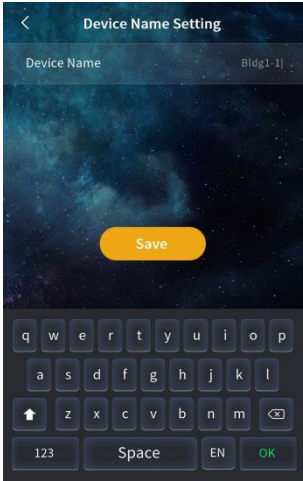
5.9 Engineering Setting



Engineering Setting

5.9.1 Device Name Setting

The device name can be modified. If SIP account information is needed in the address book, the device name needs to be set to the device name corresponding to the account information in the address book. The device will pop up a window prompting whether to use the account information in the address book. Large scale community networking requires the use of address book methods, with unified address book distribution in the community and batch rule generation of address book device information.



Device Name Setting

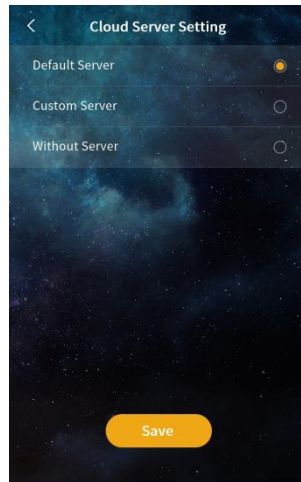
5.9.2 Cloud Server Settings

(1) Default server/Custom server

- Upload the registered face and access control card data of the local computer to the server, and synchronize the data from the server.
- When switching to no server mode, you can choose whether to retain the server data or not. If you select Retain, the device will not clear the data sent by the server. If you select not to retain, the device clears the data.
- The default server refers to a server deployed on the public network. To connect to this default server, the device must be able to access the external network. A custom server can be a locally deployed server or a regional server, and it must also ensure that the device and server network are reachable.

(2) Without server

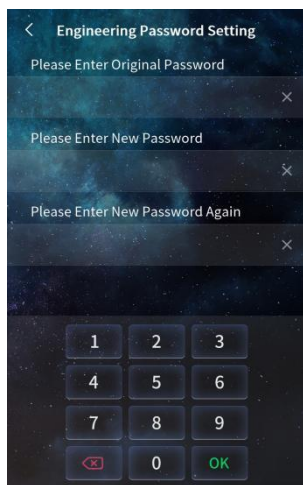
- That is, in the single-machine mode, the face and access card data registered on the machine are saved locally.
- When switching to the default server or a custom server, you can select whether to upload local data. If you select Upload, the local data is uploaded to the server and the server data is synchronized. If you do not select Upload, data on the local server is cleared and data on the server is synchronized.



Cloud server Settings

5.9.3 Engineering Password Setting

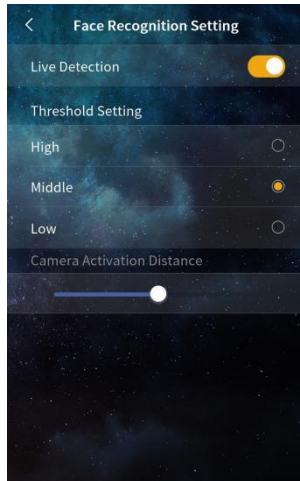
The project password can be changed. The password contains 6 digits.



Engineering Password Setting

5.9.4 Face recognition Setting

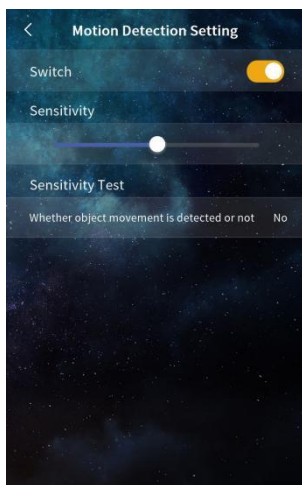
- (1) Live detection switch: After this is turned on, the device conducts live detection, and the non-living registered face cannot be unlocked successfully.
- (2) Threshold: face recognition threshold (high, medium, low), different levels correspond to different face recognition matching degrees. The threshold is high, and the requirements for face similarity are relatively high, requiring the user to be closer to the face recorded during registration.
- (3) Camera wake up distance adjustment: The user can adjust the maximum distance to wake up the camera. The wake-up distance ranges from 0.3 to 2m. If the wake up distance of the camera is set to the maximum, in the screensaver state, the face is within 2m of the device, and the device will enter the face recognition interface.



Face recognition Setting

5.9.5 Motion detection Setting

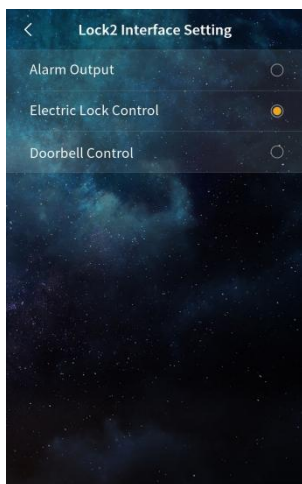
- (1) Switch: When this option is enabled, the device will perform motion detection. If the moving object is near the door machine, the door machine will light up and enter the main screen.
- (2) Sensitivity test: It is for adjusting the sensitivity of the motion, when the sensitivity is low, the visitor shall be more close to the device.
- (3) Sensitivity test: Within the detection range, whether the device detects an object moving. If an object moves, Yes is displayed. If no object moves, None is displayed. Used to view the detection result of the device when adjusting the sensitivity.



Motion detection Setting

5.9.6 Lock 2 Interface Setting

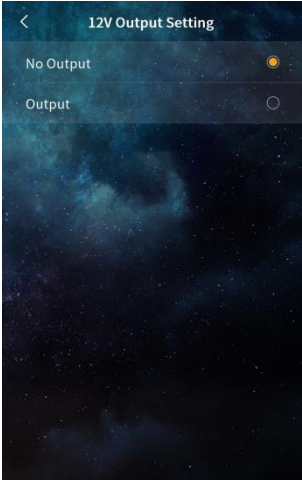
Lock2 interface functions can be selected, including: alarm output, electronic lock control, doorbell control.



Lock 2 Interface Setting

5.9.7 12V Output Setting

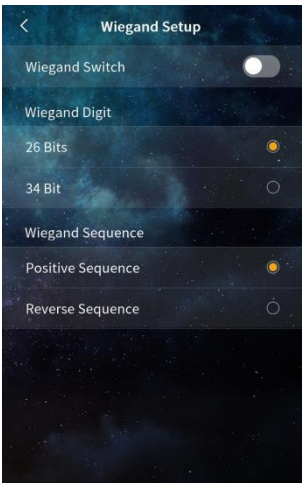
You can choose whether to output 12V voltage.



12V Output Setting

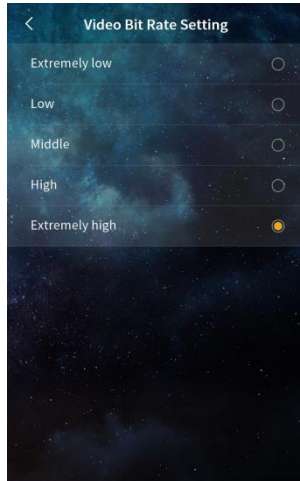
5.9.8 Wiegand setup

Weigen Settings can be performed, including: switch, bit selection (26 bits, 34 bits), and sequence selection (positive order, reverse order). Turn on the Wiegand switch, and when swiping the card, the machine does not perform card verification. Instead, use the Wiegand interface to output the card number to a third party according to the Wiegand digit settings.



5.9.9 Video Bit Rate Setting

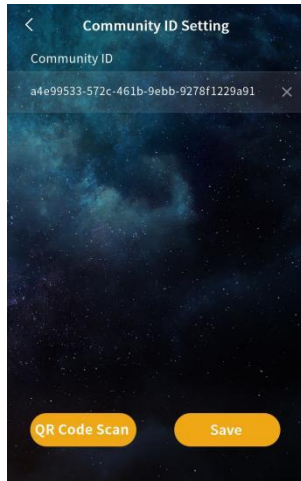
You can set the video bit rate during the call and monitoring.



Video Bit Rate Setup

5.9.10 Community ID Setting

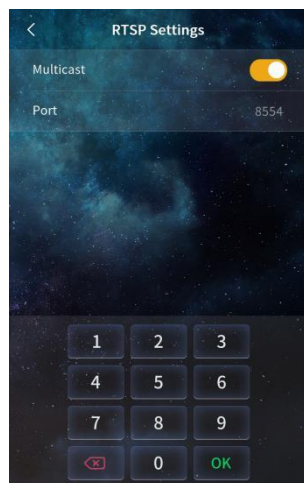
In default server or custom server mode, you can manually enter the cell identification code or click the "Configure" button to scan the QR code of the cell and bind the device to the corresponding cell. After the device is bound to the community, the face management and access card management can be performed on the platform.



Community ID Setting

5.9.11 RTSP Setting

- (1) Multicast: When the multicast switch is enabled, multiple indoor units can receive the video stream from the doorway unit using the multicast address (devices must be connected through a switch). When the multicast switch is disabled, only a maximum of two indoor units can receive the video stream from the doorway unit (devices can be directly connected).
- (2) Port: The default value is 8554. The value ranges from 1 to 65535. If the port of the door unit is inconsistent with that of the indoor unit, the indoor unit cannot monitor the door unit.

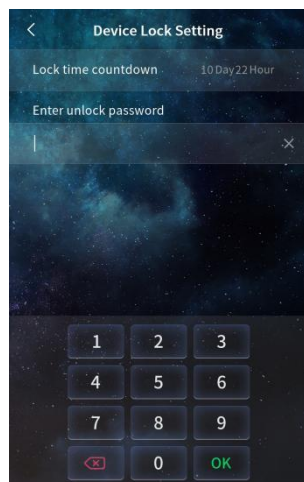


RTSP Setting

5.9.12 Device Lock Setting

Lock time and unlock password can be setting.

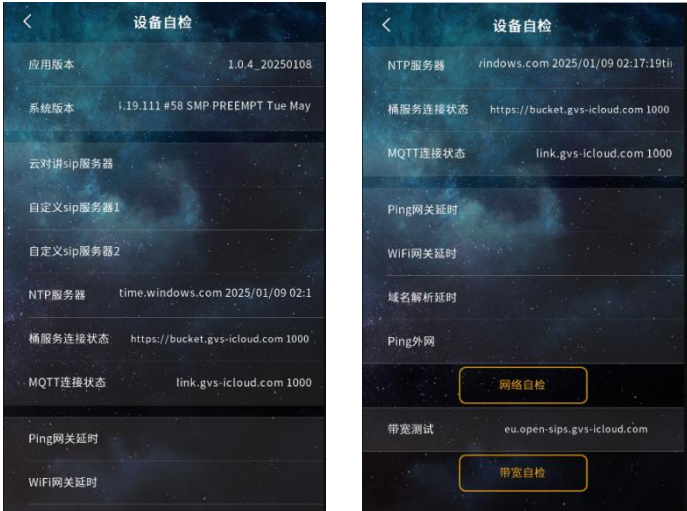
Note: If you forget the unlock password, the device cannot be unlocked and needs to be returned to the factory.



Device Lock Setting

5.9.13 Equipment Self Inspection

The main function of device self-test is to collect device operation data, quickly troubleshoot and locate problems when the device is abnormal, including device version information, server connection status, commonly used network debugging instructions, network status, bandwidth testing data, etc.

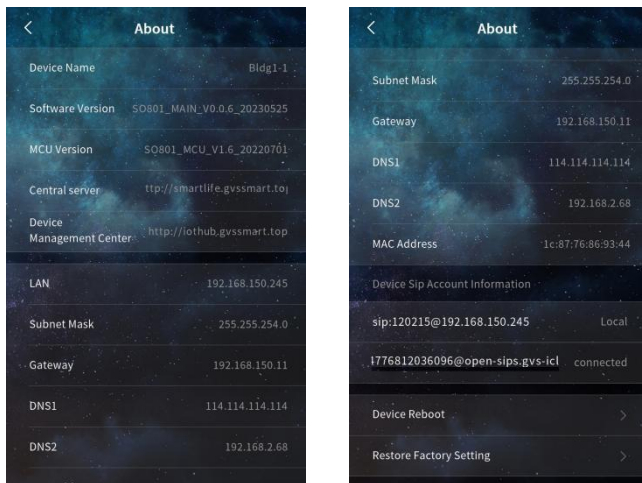


Equipment self-test

5.10 About

5.10.1 Device Information

Displays device information, including device name, software version, MCU version, central server, device manager, LAN, subnet mask, gateway, DNS, MAC address, and SIP account information.



About

5.10.2 Restart

After clicking this item, the device will restart.

5.10.3 Restoring factory Setting

After you click this button, the device will be restored to factory Settings. You need to configure the device again.

Note:

- ① Factory Settings are restored within 60 seconds of power-on. Device Settings are restored to default values, and face and access card data are cleared.
- ② Factory Settings are restored after 60 seconds of power-on. The device Settings are restored to default values, but the face and access card data will not be cleared.

Chapter 6 Address book configuration

Automatic configuration mode: This machine can discover other S-series devices in the same network segment. For small system networking within 16pcs, automatic discovery is preferred. It is a plug and play mode that does not require complicated configuration. Networking requires Router routers to allocate IP addresses to each device, and devices use MDNS protocol to discover each other.

Address book mode: To disable automatic configuration mode, address book mode is required. The devices connected to the address book network need to download a unified address book configuration table, which can be pushed locally by Update&Configuration Tool or pulled online from the intelligent management platform.

6.1 Address book generation

Please refer to Chapter 3.4 Engineering Configuration of the Intelligent Management Platform User Manual for details.

6.2 Address book synchronization

For large-scale community networking systems, devices need to use the address book mode uniformly, and there are two ways to synchronize the address book. Method 1: In Chapter 3.4 of the Intelligent Management Platform User Manual, configure the address book and export the address book configuration file addressBook.xml. Then use the Update&Configuration Tool to locally push to devices. For communities that are not connected to the internet, the tool can only be used to push to all devices.

6.3 Address Book Application

After receiving the address book, the device will automatically restart and update the contact information. Go to Engineering Settings - Device Name Settings, enter the device name and click Save. This will prompt that the device exists in the address book. Do you want to use the address book information? Clicking confirm will prompt that the setting is successful and restarting is in progress. For example, the address book contains the device name "1-1" (device name: 1-1, region: 1Guiding, supported functions: outbound/monitoring/elevator control/access control, gateway: 10.00.100), IP : 192.168.0.20, Mask: 255.0.0.0, DNS1:114.114.114.114, DNS2: 8.8.8.8, SIP Username: 00011, Protocol Type: udp) , After the user inputs "1-1" to save, the IP address information and SIP account information will be automatically updated to the above information. For large-scale community networking systems, after configuring the address book, it is necessary to set the device name for each device separately and apply the address information corresponding to this name. For detailed instructions on setting device names, please refer to section 5.1.14 or section 5.12.10 on setting device names for Web Server.

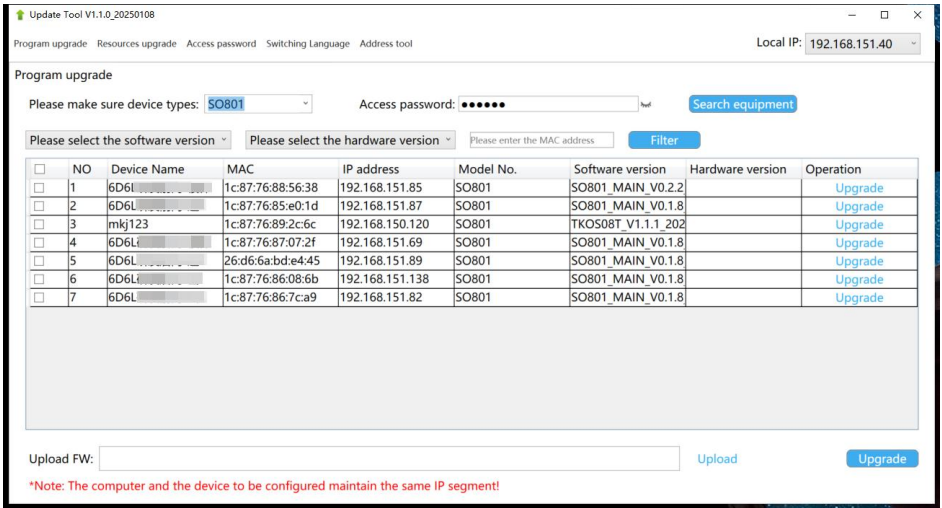
Chapter 7 Web Server

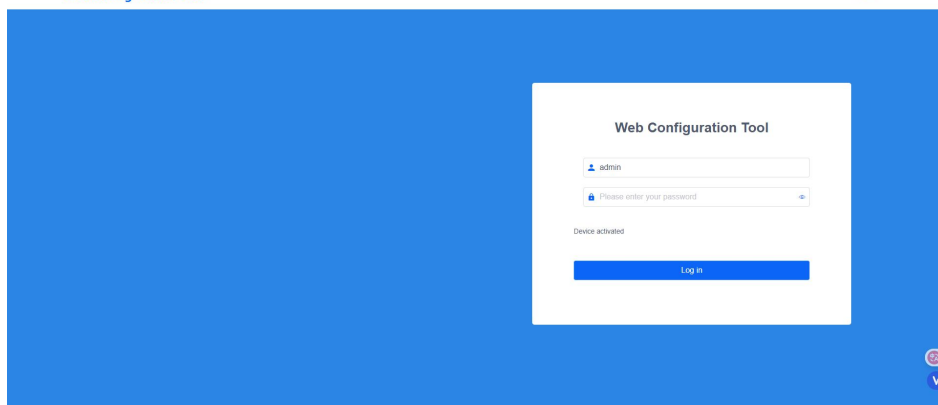
Web Server enables device login through a browser, and its webpage configuration function is similar to device operation function, making it convenient for users to remotely operate. The tedious operations on the device, such as touch screen input methods, can be completed by copying and pasting with a computer keyboard and mouse. Simplify the difficulty of device operation and enhance user convenience.

7.1 Web Server login

Steps for entering the web operation of the entrance machine:

1. Enter the device system configuration with the engineering password and access the About interface to view the device IP address.
2. Run the 'Update&Configuration Tool' program as an administrator and select or enter the device type as 'SO801' or other customized models. Enter the access password as '801801'. Click on 'Search Device' and view the corresponding IP address based on the device's MAC address.





3. Browser input URL `http://ip_address/#/` , such as `http://192.168.151.5/#/` Enter the entrance machine configuration system webpage. The default password is admin.

Attention: Please ensure that the computer IP and the device IP to be configured are in the same network segment.

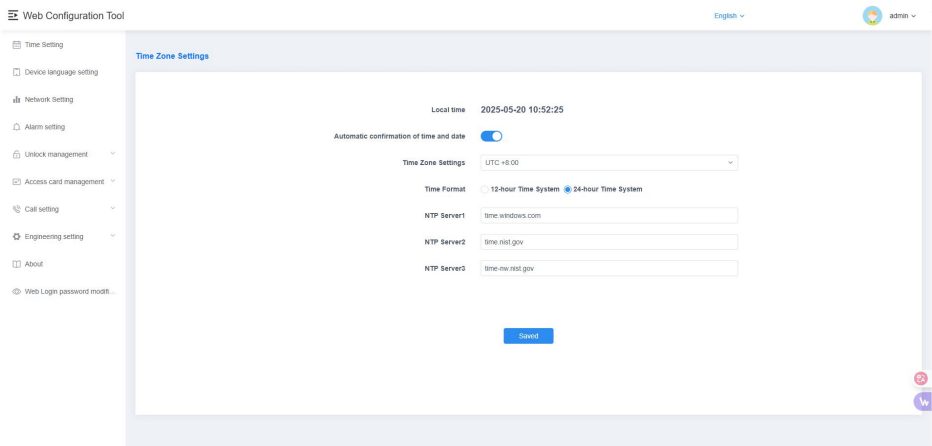
7.2 Time setting

(1) Automatic synchronization, when enabled, automatically synchronizes date and time from the network NTP server according to the set time zone and format.

(2) Turn off automatic synchronization and manually set the date and time.

(3) Time zone setting: Select the corresponding time zone based on the country you are in. This machine will convert the local time based on the set NTP server and time zone.

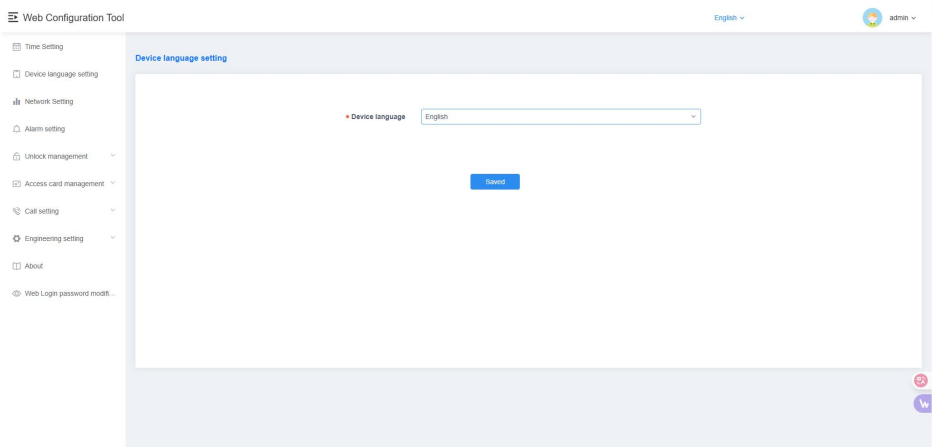
(4) NTP servers: By default, there are 3 built-in NTP servers that users can manually change.

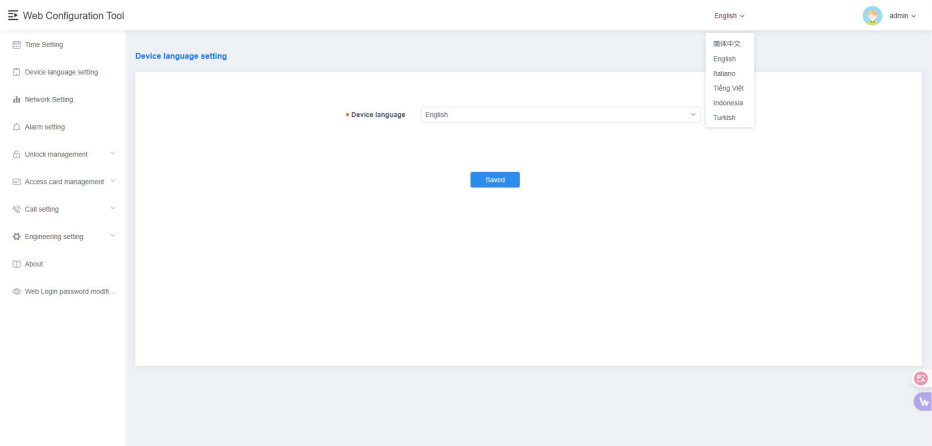


7.3 Device language setting

Device Language: Set the language displayed on the device.

Web language: Set the language of the web page.

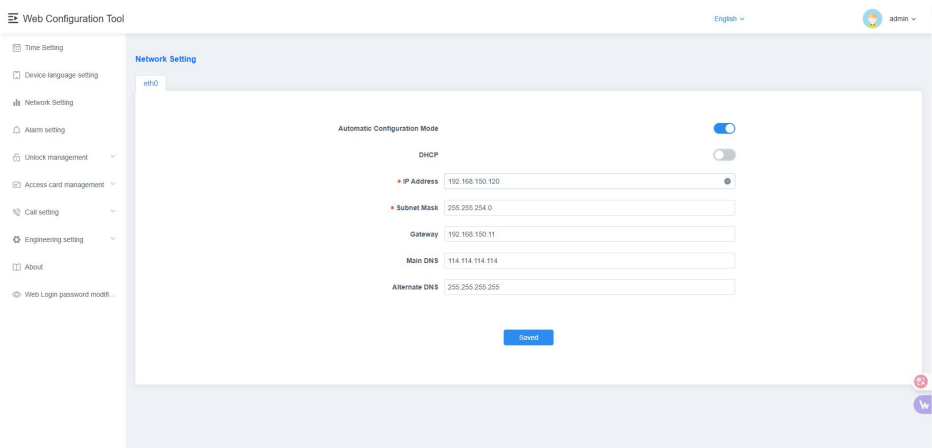




7.4 Network setting

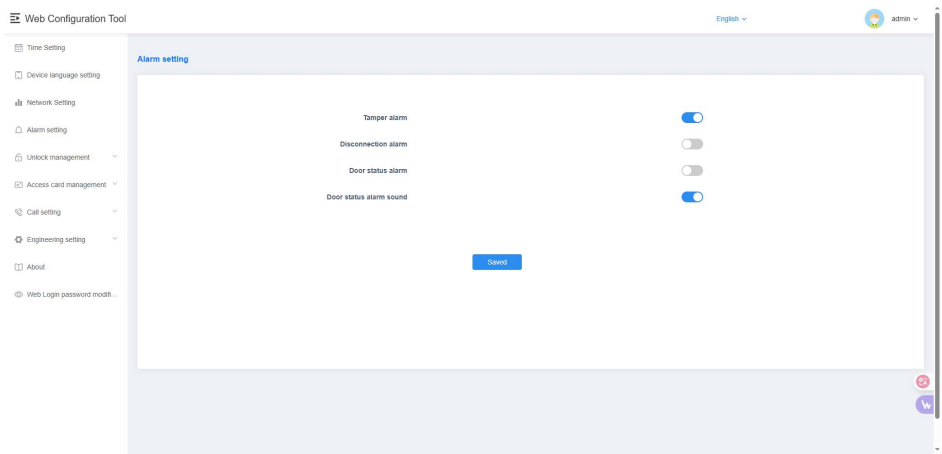
(1) Automatic configuration mode: After enabling this option, this machine can discover other S-series devices in the same network segment.

(2)DHCP: After shutdown, the network needs to be manually configured by entering the IP address, subnet mask, gateway DNS.



7.5 Alarm setting

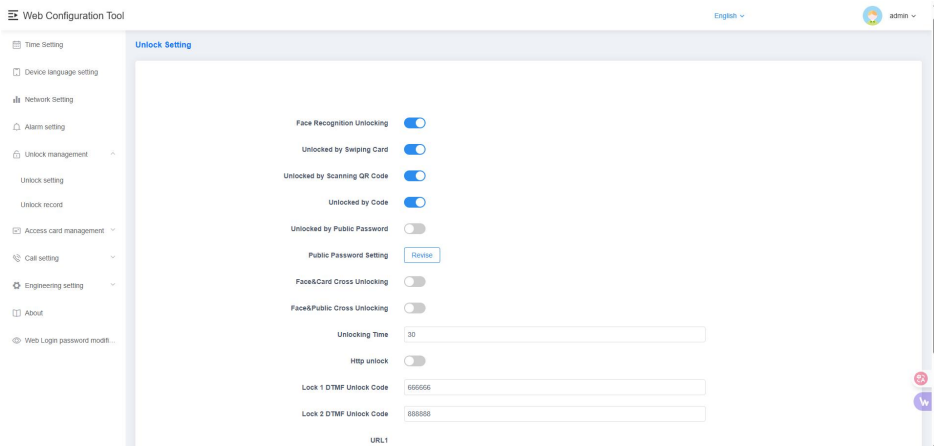
- (1) Anti disassembly alarm: After enabling this option, if the device is disassembled by external force, the device will sound an alarm sound.
- (2) Disconnecting alarm: After enabling this option, if the device is disconnected, the device will sound an alarm sound and the status bar will display a disconnection icon.
- (3) Door status alarm and door status alarm sound: After opening the door status alarm and door status alarm sound, if the device detects that the door is open for more than 120 seconds, the device will sound an alarm sound.



7.6 Unlock management

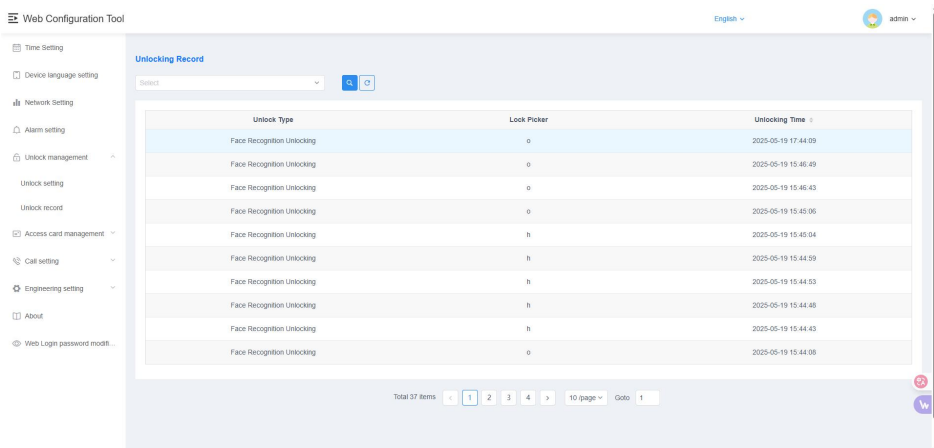
7.6.1 Unlock setting

The web server's webpage feature settings are exactly the same as the local unlock settings in section 5.1.1.



7.6.2 Unlock record

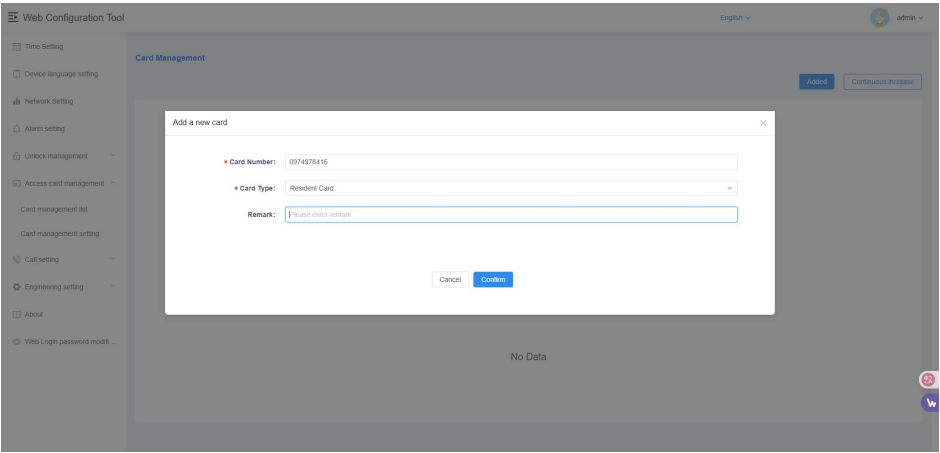
Used to view the unlocking records of this machine, and can also filter the unlocking records of unlocked devices.



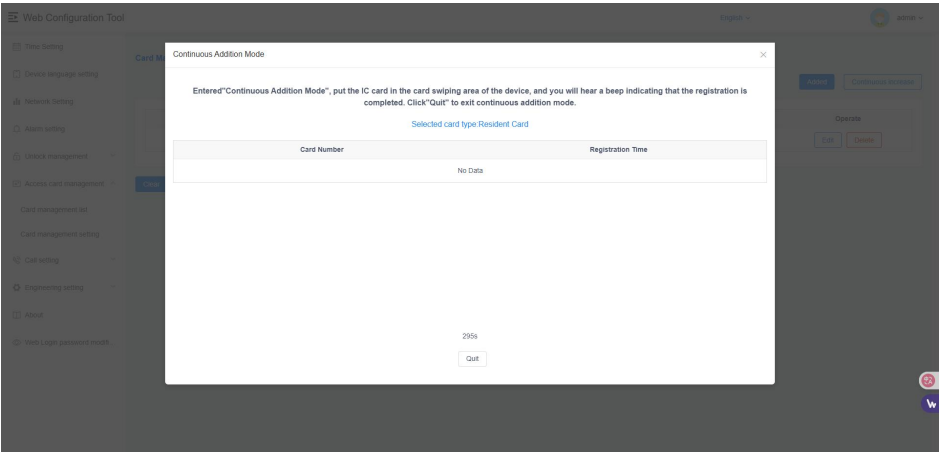
7.7 Access card management

Access card information can be registered, queried, deleted, and cleared on the web. In default server or custom server mode, the card data of this machine is automatically synchronized with the platform. The maximum storage capacity of access cards is 20000

sheets.



Single registration card



Continuous registration card

7.8 Call Setting

7.8.1 Contact setting

Display relevant information of the current contact. The contacts include networked devices discovered after enabling automatic configuration, devices imported from the address book, and devices manually added.

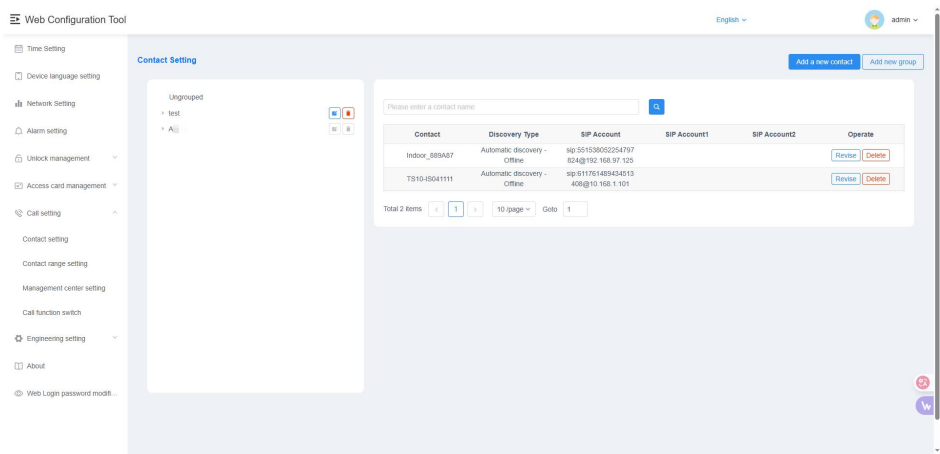
Search: You can vaguely search for contacts in the list.

Add contact person: You can add a contact person in this machine by filling in the remarks, SIP account, and group;

Add group: You can add groups in this machine by filling in the group name, belonging group, and whether group calling is supported;

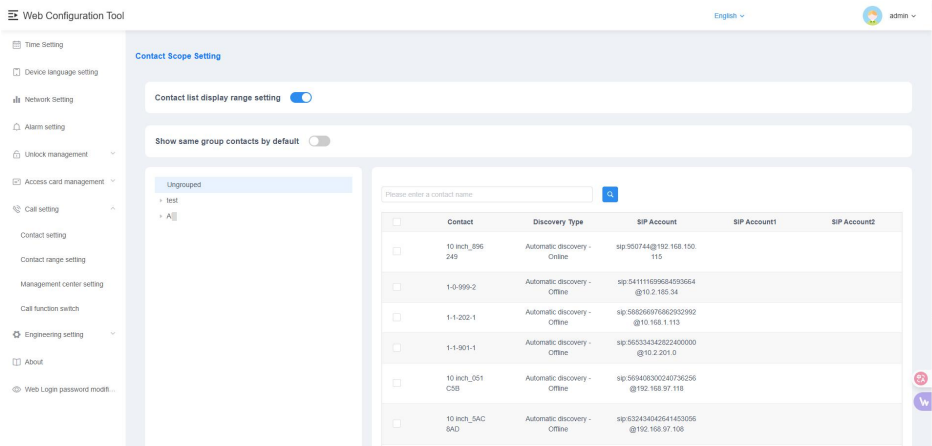
Delete: This contact data can be deleted. Note: Connected devices discovered through enabling automatic configuration cannot be deleted when they are online. Devices imported through the address book cannot be deleted either.

Editor: This contact data can be edited. Note: Address book contacts can only modify notes.



7.8.2 Contact range setting

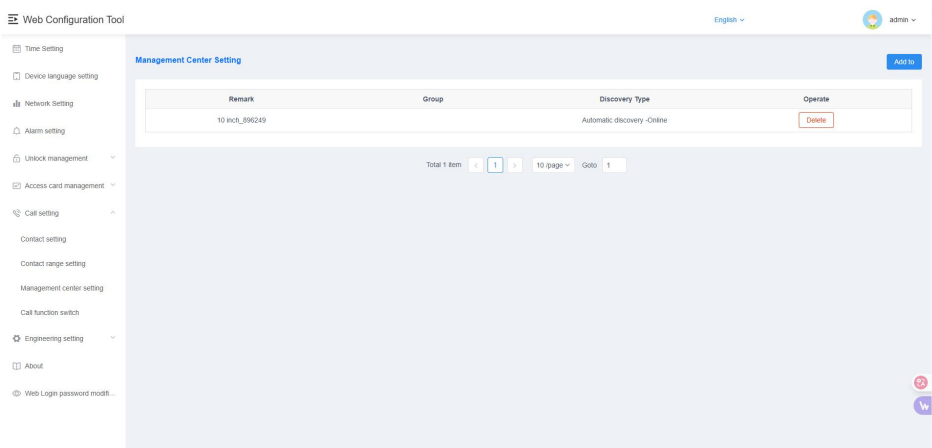
The contact display range of the device itself is available. For large communities, you can choose this unit or customize the continuous person range for easy and quick search during calls.



7.8.3 Management center setting

Display the selected management center SIP account. When the user clicks on the call management center, the SIP accounts of the management center in the list will be called simultaneously.

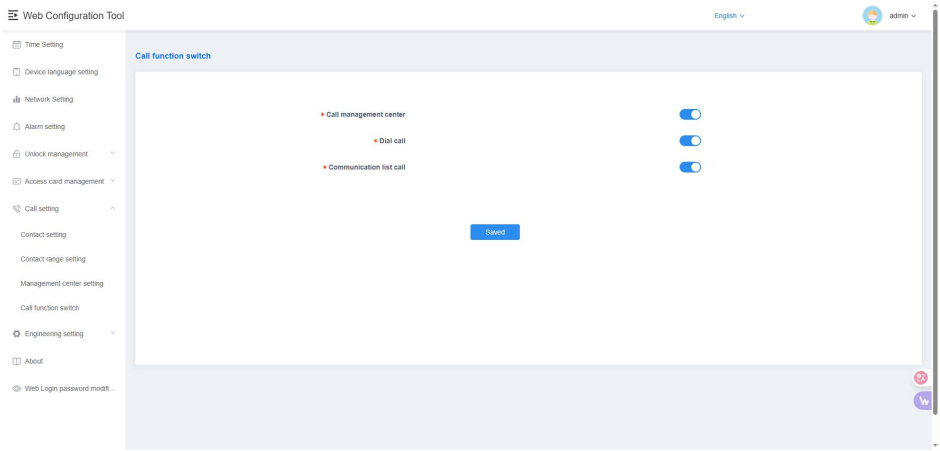
- Add: Click "Add To", select the device, and add the SIP account to the list of SIP accounts in the management center, up to a maximum of 10.



7.8.4 Call function switch

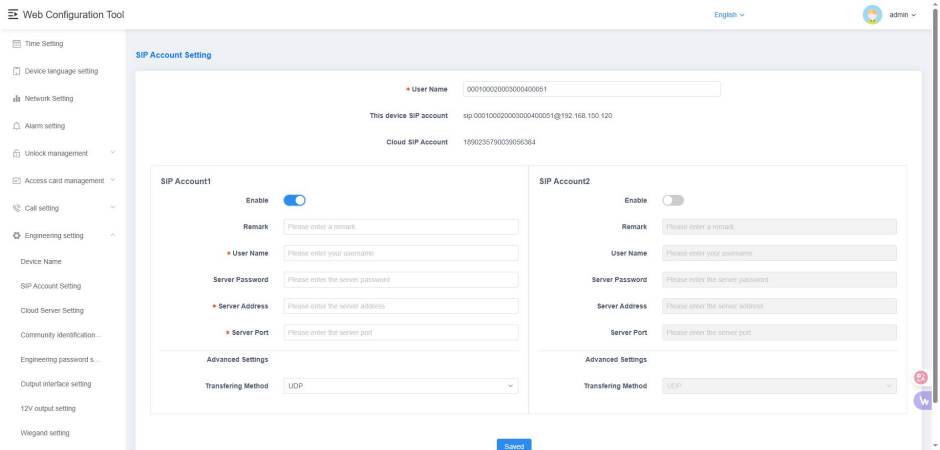
Set whether to enable call management center, dial-up calling, and communication list

calling functions.



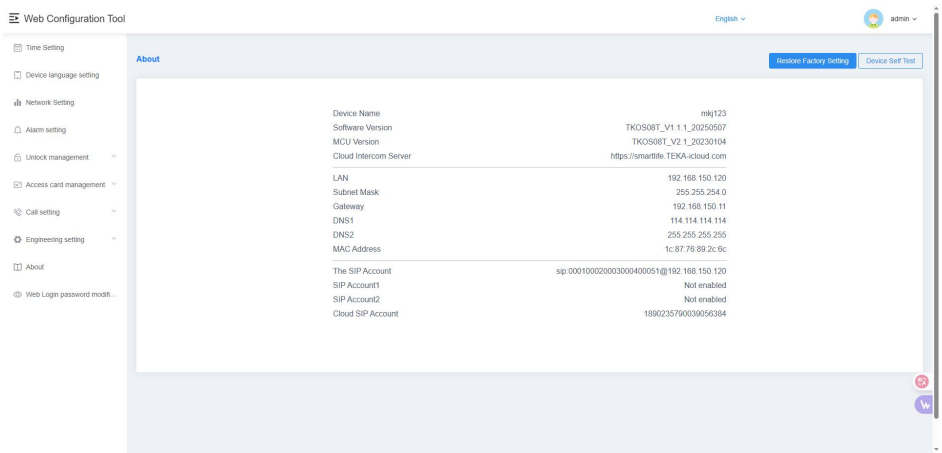
7.9 Engineering setting

The project configuration includes device name settings, SIP account settings, cloud server settings, community identification code settings, project password settings, output interface settings, 12V output settings, Wigan settings, video settings, and RTSP settings. The functions are basically the same as those in Chapter 5.9 of the device side engineering settings.

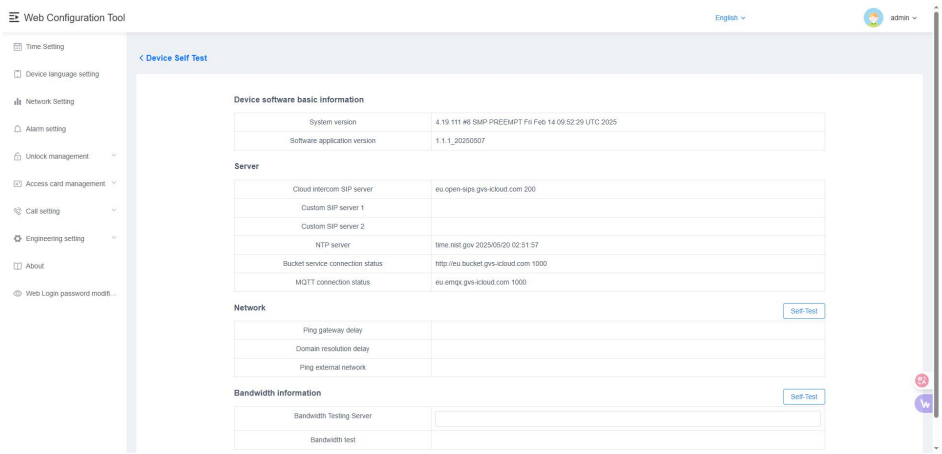


7.10 About

Used to view device related information, including device name, software version, MCU version LAN、Subnet mask, gateway, DNS, MAC address, cloud intercom server, device management center, device SIP account information, factory reset, device self-test.

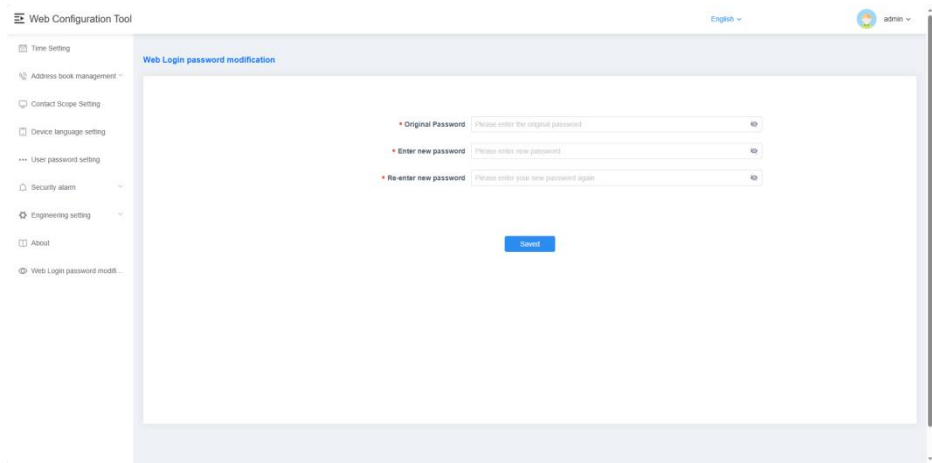


About Information



Equipment self-test information

7.11 Web Login password modification



The screenshot displays the 'Web Configuration Tool' interface. On the left is a sidebar menu with options: Time Setting, Address book management, Contact Scope Setting, Device language setting, User password setting (highlighted), Security alarm, Engineering setting, About, and Web Login password modification. The main content area is titled 'Web Login password modification' and contains three input fields with red asterisks: 'Original Password' (placeholder: 'Please enter the original password'), 'Enter new password' (placeholder: 'Please enter new password'), and 'Re-enter new password' (placeholder: 'Please enter your new password again'). A blue 'Save' button is positioned below the fields. The top right corner shows 'English' and a user profile icon labeled 'admin'.

Users can modify the login password of this Web Server. The initial default password is "admin".

