



Access Control Device User Manual



CONTENT

1. INSTALLATION DIAGRAM	1
2. OPERATION INSTRUCTIONS	3
2.1. CONFIGURATION INSTRUCTIONS	4
2.1.1. SET NETWORK PARAMETERS	4
2.2. OPENING INSTRUCTIONS	5
2.2.1. SWIPE CARD TO OPEN THE DOOR	5
2.2.2. PASSWORD TO OPEN THE DOOR	6
2.2.3. FACE RECOGNITION OPENS THE DOOR	7
3. SYSTEM SETTINGS	8
3.1. USER MANAGEMENT	9
3.2. ACCESS CONTROL SETTINGS	10
3.3. SYSTEM MAINTENANCE	11
3.4. FACIAL RECOGNITION	11
3.5. COMMUNICATION SETTINGS	12
3.6. SYSTEM SETTINGS	12

1. Installation diagram

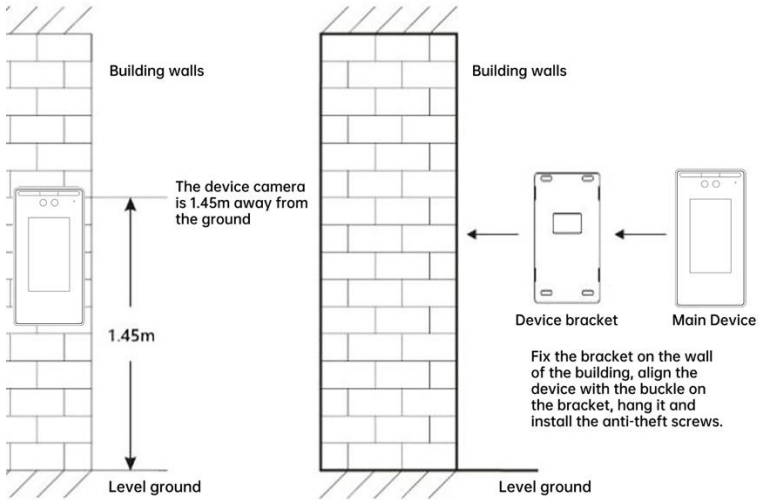


Image 1-1 Installation diagram

The device is installed at a height of about 1.45 meters from the ground. Fix the bracket on the wall. Align the device with the bracket buckle and use anti-theft screws to install it.

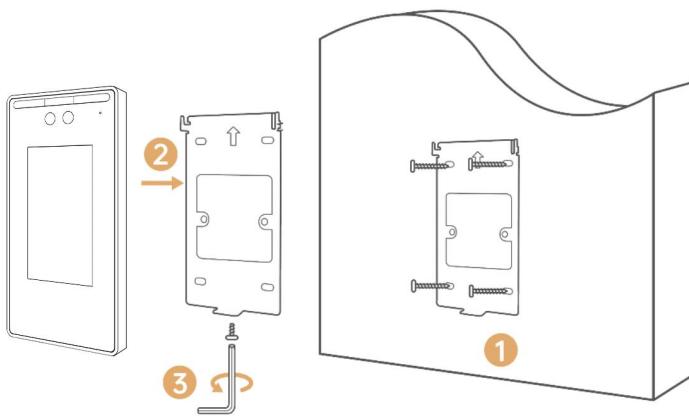


Image 1-2 Installation steps

Installation steps:

1. After determining the installation height, use screws to fix the bracket on the wall.
2. Align the device with the mounting buckle of the bracket and pull it down into the installation position.
3. Install anti-theft screws on the bottom of the device to fix the device and the bracket.

Notice:

1. Do not expose device to wind and rain. If it cannot be avoided, please install a rain cover.
2. Do not expose the camera to direct sunlight or strong light.
3. Try to keep the light of the camera even.
4. Do not install near strong magnetic fields.
5. Do not install it where the background noise is greater than 70dB.
6. Non-professionals are not allowed to disassemble the equipment for maintenance.

2. Operation Instructions

Main UI:

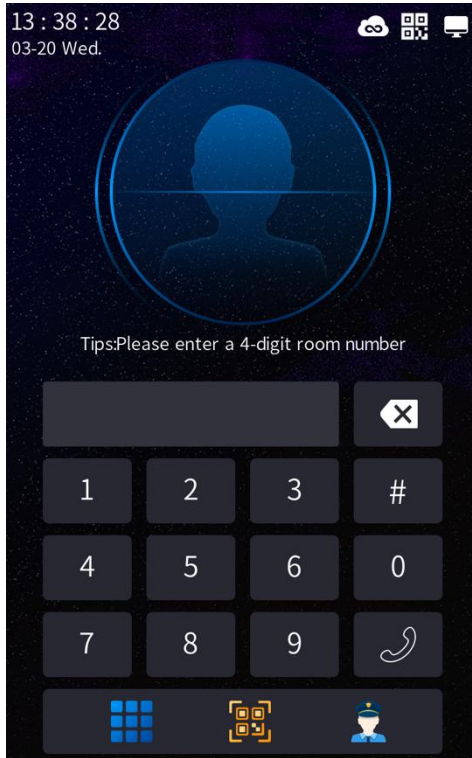




Image 2-1 Main UI

1. Displayed in the upper right corner  of the main interface, indicating that the cloud intercom server has been connected.
2. Displayed in the upper right corner  of the main interface, indicating that the network is connected.

Steps to connect to the network:

- ① Connect the network cable to the network interface on the back of the device, and the other end to the network device interface in the LAN to ensure that the network connection of the device is ok.
- ② Configure network parameters. For specific operations, see [2.1.1](#)

Setting Network Parameters.

2.1. Configuration instructions

2.1.1. Set network parameters

When using it for the first time, you need to configure the network parameters of the device. If the device room number is set successfully, the device will obtain the corresponding IP address according to the configuration table. The network parameters of the device can also be set through Set it up as follows.

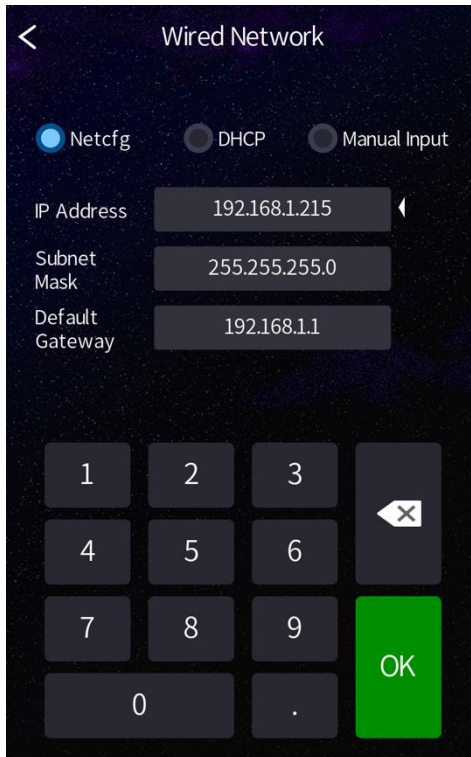



Image 2-2 Set network parameters

Steps:

④ Click on the main interface , Enter the password unlock interface

and click on the interface  , Enter the administrator password (initial password: 666666)。

② Click "Communication Settings" - "Wired Network", you can choose to obtain according to the configuration table, obtain automatically or enter manually to set the relevant parameters of the door station: IP address, subnet mask and gateway address.

③ After the setting is successful, a prompt box indicating successful setting will pop up at the door along with a voice prompt.

2.2. Opening instructions

The device supports a variety of door opening methods: card opening, password opening, face recognition opening and remote opening. After the door is opened successfully, the door station will display a prompt box indicating that the door is opened successfully and accompanied by a voice prompt.

2.2.1. Swipe card to open the door

Place the added legal IC card in the card swiping area of the door machine to open the door. For the operation of adding a card, see [3.6 System Settings - Card Management](#).

2.2.2. Password to open the door

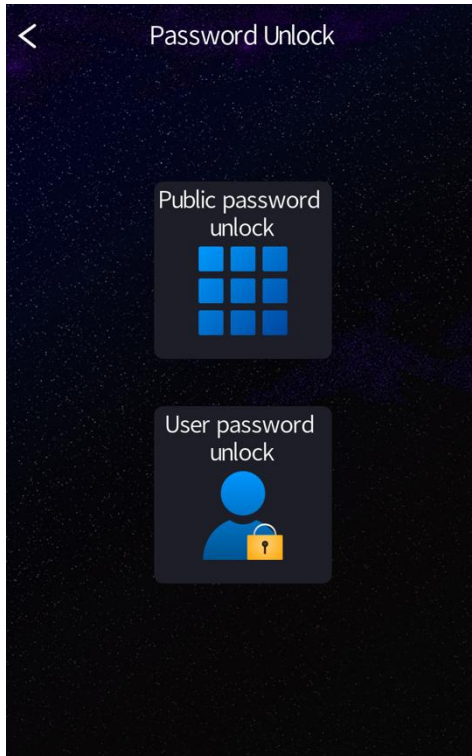





Image 2-3 Password to open the door

Click on the main interface  ,Enter the password unlock interface. In this interface, click  ,Can perform public password unlocking and public hijacking password unlocking ; Click  ,User password unlocking and user hijacking password unlocking can be performed. When the entered password is correct, the door lock opens and the door station captures a picture and uploads it to the management center. When the entered password is incorrect, it will prompt that the password is incorrect, and the door station will capture a picture and upload it to the management center.

➤ **Explanation:**

Public password unlocking

Enabled by default, initial password: 668899.

The public hijacking password to unlock the door

The public hijacking password (initial password: 998866) is in reverse order of the public password. No settings are required. It is automatically generated and can only be used when the public password unlocking is enabled.

For example: the public unlocking password is 123456, and the hijacking unlocking password is 654321. When the hijacking password is used to unlock, the door machine will alarm the management center and notify the management center that someone is being held hostage at the door.

User password to unlock

It is closed by default, and the administrator needs to enable the permission through system settings. For specific operations, see [3.6 System Settings - Advanced Settings](#), and the resident needs to set it on the indoor unit before it can be used. After enabling it, just enter the corresponding room number and password. The user password can be unlocked with the public password unlocking is used at the same time.

User hijacking password to unlock the door

User hijacking password unlocking is related to the authority of user password unlocking. When user password unlocking is set, the user hijacking password is automatically generated in reverse order.

2.2.3. Face recognition opens the door

Face registration:


1. Management center entry:

① Local upload: Open the management center, click "Owner Management" - "Enter Face", select local upload (image format: jpg, resolution 640*480, less than 500k), and follow the prompts to complete the registration.

② Take pictures with camera: Open the management center, click "Owner Management" - "Enter Face", select the camera to take pictures, and follow the prompts to complete the registration.

2. Enter the face when adding a user to the device. For specific operations, see [3.1 User Management](#).

Face recognition opens the door:

The automatic face recognition permission is turned on by default. When it is turned on, whether the screen is on or in standby mode, the device will automatically wake up the face recognition door opening interface when passing the door. If the automatic face recognition permission is turned off, you need to manually click the face recognition icon  on the main interface to start face recognition to open the door. For specific operations on turning on/off automatic face recognition permissions, see [3.6 System Settings - Advanced Settings](#).

3. System settings

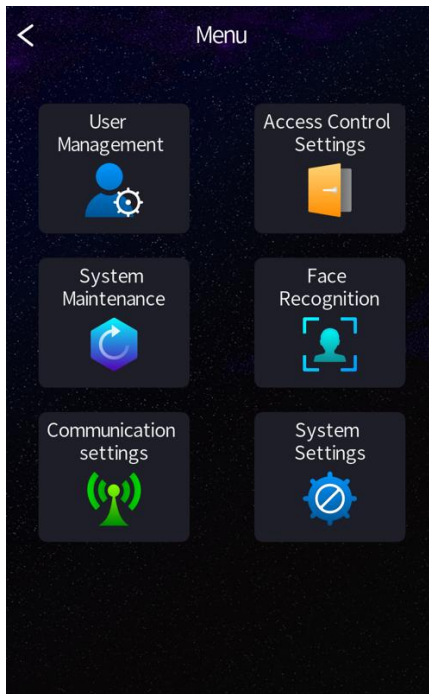




Image 3-1 System settings

Click the  on the main interface, enter the password unlocking interface, then click the  on this interface, input the administrator password (default password: 666666) to enter the system settings.

3.1. User Management

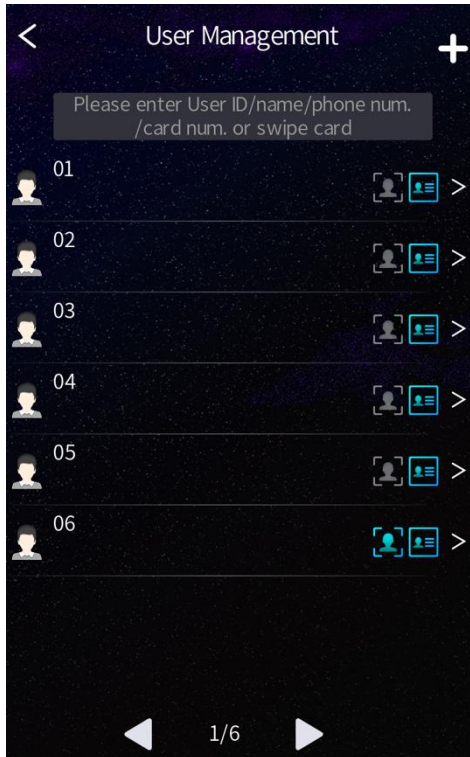



Image 3-2 User Management


 : Click the "+" in the upper right corner to add a user, input the user number, mobile phone number, name, card number, face and select the user type.

➤ Explanation:

Add user:

① Add card: Manually input the card number or swipe the card in the card reading area of the device to automatically obtain the card number.

The card type can be chosen as common card or management card.

② Enter face: Look directly at the screen and make sure your face is not blocked, then click .

③ User type: You can choose common user or administrator.

Search for user:

Click the input box on the user management interface to search for user based on their user number/name/mobile phone number/card number or by swiping their card.

Delete user:

Click the user to be deleted in the user management interface, enter the user information interface, and click .

3.2. Access Control Settings



Access Control Settings: Set the card recognition verification, door sensor status (normally open/normally closed), door sensor delay time (S), door sensor action time (S), repeat authentication interval time (S), access control authority, sector number and sector password.

➤ Explanation:

① Card recognition verification: Turned off by default. The administrator can enable this function. After it is enabled, the device can be unlocked based on the card number.

② Door sensor status: Normally closed by default, here you can set the normally open/normally closed status of the door sensor.

③ Door sensor delay time (S): The default time is 30S, which can be set as needed, ranging from 1 to 99.

④ Door sensor action time (S): The default time is 5S, which can be set as needed. There are 1s, 2s, 5s, 10s, 30s, 50s and 200s available.

⑤ Repeat authentication interval time (S): The default time is 0S, which can be set as needed, ranging from 0 to 60.

⑥ Access control authority number setting: Each unit has an access control number, which needs to correspond to the access control authority value of the "Management Center → Terminal Management →

Outdoor Station Access Control Permission Setting".

⑦ Access control sector number and sector password settings: :

Sector number: same to the sector number (01~15) of the unit access control card set by the administrator when issuing the card.

Sector password: same to the password (12 digits) of the unit access control card set by the administrator when issuing the card.

Note: In order to facilitate management, it is recommended that the same community use a unified sector number and sector password, which can be set by manually input, management card swipe, management center platform or background remote control. Access control authority needs to be set by manually input. Both management card and user access control card can be issued on the management center PC terminal. For detailed operations, please refer to the Management Center PC Terminal Usage Instructions.

3.3. System Maintenance



: Check the system information, address information, serial number and restart the system.

➤ **Explanation:**

① System information: Check the machine number, MAC address, local IP address, local subnet mask, local gateway, server address, machine location information, software version number, network configuration table version, serial number and system version.

② Address information: Check and set the address information. After successful setting, the device will restart.

③ Serial number setting: The serial number of this machine is the unique number of the device. It is set by default and cannot be modified without authorization.

3.4. Facial Recognition



: Face data synchronization, face data management and face

threshold setting.

➤ **Explanation:**

- ① Face data synchronization: Check the face data synchronization information of this machine. Including local faces, backed up faces, faces to be backed up, downloaded faces, invalid faces and the time of the last successful synchronization.
- ② Face data management: Manage local face data, including all local face data and unbacked up face data.
- ③ Face threshold setting: Set the on/off of liveness detection, on by default. Set the face recognition threshold, which is used to determine the pass rate of face recognition. The default is 80 and the setting range is 61~90.

3.5. Communication Settings



: Set up the wired network and download the network configuration table.

➤ **Explanation:**

- ① Wired network: You can choose to set the IP address, subnet mask and default gateway by the configuration table, automatic acquisition or manual input.
- ② Download the network configuration table: When you need to update the network configuration table, enter the IP address of the management center and press "OK" to download the network configuration table.

3.6. System Settings



: Including volume settings, advertising settings, time settings, password settings, advanced settings and supplementary functions.

1. Volume settings: Adjust the volume for ringtones, calls, button pressing, and ads.
2. Advertising settings: on/off. When it's turned on, the device can play advertisements, and the advertisement content is set by the property

management.

3. Time setting: Set the on/off of automatic time acquisition. If it is turned off, you need to manually set the time and date of the device. After the settings are completed, click "Save".

4. Password setting: Set the door opening password and administrator password.

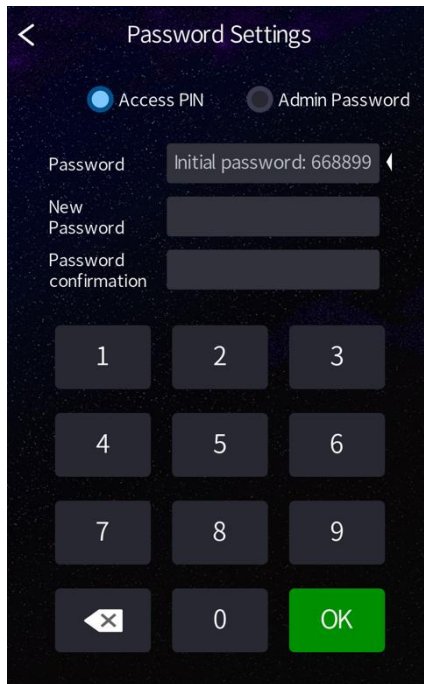


Image 3-3 Password setting

➤ **Explanation:**

The door opening password is the public unlocking password. The public hijacking unlocking password is the reverse order of the public unlocking password, no setting is required and it is automatically generated. The two unlocking passwords cannot be the same. The default public unlocking password is 668899, and the public hijacking unlocking password is 998866.

If the public unlocking password is set as 666666 or 121121, the public

hijacking unlocking password is the same as the public unlocking password, which violates the setting rules and prompts failed setting.

5. Advanced settings::

- ① Hang up after door unlocked: Off by default. When turned on, during intercom, the call will automatically be hang up after door unlocked.
- ② Facial recognition: On by default. When turned on, the device can be unlocked by face.
- ③ Automatic facial recognition: On by default. When turned on, the device will enter the automatic facial recognition statue.
- ④ Unlocked by user password: Off by default. When turned on, the device can be unlocked by the user password.
- ⑤ Unlocked by public unlocking password: On by default. When turned on, the device can be unlocked by the public unlocking password.
- ⑥ Anti-tamper: Off by default. When turned on, when someone maliciously dismantles the device, the device will sound an alarm and report to the management center.
- ⑦ Save logs: On by default. When turned on, the device operation logs will be uploaded to the cloud.
- ⑧ Unlocked by QR code scan: On by default. When turned on, the device can be unlocked by QR code scan.
- ⑨ Screen on all-day, animation mode, full face: Off by default, can be turned on if necessary.
- ⑩ Set the call time: Slide to set the call time of the device. The default time is 60S and the setting range is 10~120S.
- ⑪ Set the standby time: Slide to set the standby time of the device. The default time is 30S and the setting range is 10~300S.

6. Auxiliary functions:

- ① Call settings: Set the permissions to turn on/off of "Call Management Center", "Call Cloud Management Center", "Call Security Extension", "Call Indoor Monitor" and "Call Cloud Indoor Monitor", set the call duration time of indoor monitor, mobile phone and cloud indoor monitor. The permissions for "Call Cloud Management Center" and "Call Cloud

Indoor Monitor" are turned off by default. They can be turned on if necessary. After the settings are completed, click the "Save" button on the bottom of the interface to save.

➤ **Explanation:**

Call refers to the function of initiating an intercom to a designated device or user through the outdoor station. For example: Call an indoor monitor refers to the function of the outdoor station initiating an intercom to the indoor monitor. It is usually used to talk to the resident before the visitor enters the access control area to confirm the visitor identity or the purpose of the visit.

- ② Server settings: Set the IP address and port number of the server.
- ③ Card management: add card and delete card.

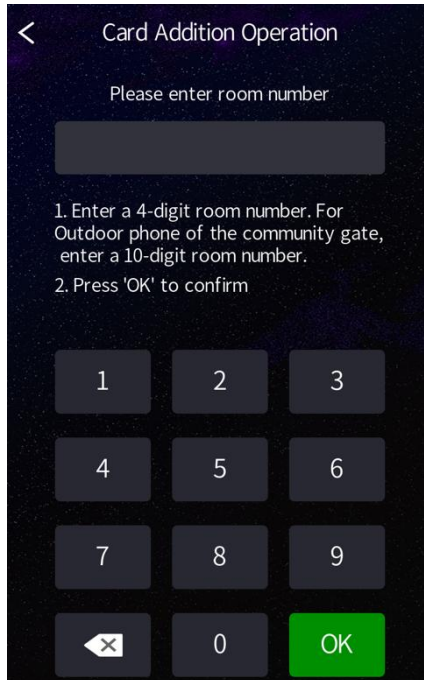


Image 3-4 Card management

➤ **Explanation:**

Add card: After inputting the room number where the card needs to be

added, place the card in the card reading area of the device to add the card. Multiple cards can be added continuously.

Delete card: Place the card to be deleted in the card reading area of the device to delete the card. Multiple cards can be deleted continuously.

- ④ Hardware test: Choose to test camera, speaker, microphone, card swiping, others, screen, network, restart and enter test mode.
- ⑤ Aging test: Choose to test the aging of camera, screen and speakers of the device.
- ⑥ Language setting: Set the language of the device, you can choose Simplified Chinese, English and Russian.
- ⑦ Elevator settings: Set the on/off of elevator calling and manage the elevator server.

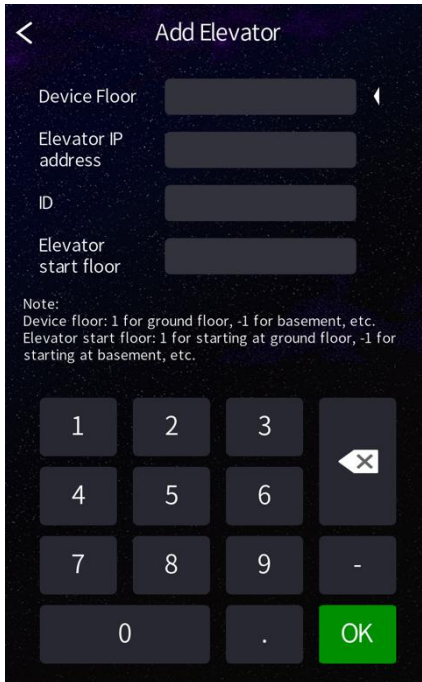


Image 3-5 Elevator settings

➤ **Explanation:**



Add elevator: Select elevator server management, click "Add Elevator",

and input the device located floor number, the elevator IP address, number and starting floor.

Delete elevator: Select elevator server management, select the elevator to be deleted and delete it according to the prompts.

7. Restore factory settings: After clicking to restore factory settings, the device will clear all settings.

➤ **Explanation:**

Click the  on the main interface, then click the  on this interface, input the super password (if necessary, you can contact the device dealer or after-sales service to obtain the super password) to enter the system settings, click "System Maintenance", then click "restore factory settings".

