Panasonic

Installation and Operating Instructions

Video Intercom System — Lobby Display Station

Model No. **VL-VQ9000SX**

Thank you for purchasing a Panasonic product.
Please follow all instructions in this document and save it for future reference.
Carefully read the information found in the section titled "Important safety information" in particular.
The terms Entrance panel, Building panel, and Door panel used in this document refer to the Lobby Display Station.

This system is not designed to provide complete protection from property loss. To the maximum extent permitted by applicable law, Panasonic will not be held responsible for any damage incurred as a result of property loss.

Note to the installer

- **This document includes instructions for both installation and operation. See the section titled "Installation" for installation instructions.**
- Please read this document carefully, and install the product safely and correctly by following the instructions.
- Only use attachments/accessories specified by the manufacturer.
- The installation shall be carried out in accordance with all applicable installation rules.

Table of Contents

1. Technical Specifications 1
2. Packing Contents 1
3. Name and Functions of Each Part 3
   3.1 Front and Rear Part 3
4. Connection Diagram 4
   4.1 System Layout 4
   4.2 Wiring Diagram 5
   4.3 Relay Lock Connection 6
5. Installation 6
6. Operation Description 7
   6.1 Call Page 7
   6.2 PIN unlock 8
   6.3 Contact page 9
   6.4 Face Recognition unlock 9
   6.5 QR code unlock 9
   6.6 IC card unlock 10
   6.7 Setting Page 10
      6.7.1 Device Information 10
      6.7.2 Access 11
      6.7.3 System 12
      6.7.4 Password 13
      6.7.5 About 14
      6.7.6 Contact 14
7. Web Client Operation 15
   7.1 Login The Client 15
   7.2 Local Configuration Page 16
   7.3 SIP Configuration Page 16
   7.4 RTSP Configuration Page 17
   7.5 DTMF Configuration Page 17
   7.6 Address Book Configuration Page 18
      7.6.1 Add Site Camera 18
      7.6.2 Site Camera Authorize 19
      7.6.3 Add Sip Device 20
   7.7 User Management Page 20
   7.8 Maintenance Page 20
   7.9 Access Manage 21

Important safety information

To prevent severe injury or loss of life or property, and to ensure proper and safe operation of your product, read this section carefully before using the product.

⚠ WARNING

Preventing fire, electric shock, and short circuits

- **Leave installation work to the dealer. Installation work requires technical knowledge and experience. Electrical connection work should be performed by certified personnel only. Failure to observe this may cause fire, electric shock, injury, or damage to the product. Consult the dealer.**
- Follow the below instructions about the power supply.
  - —Use only the ethernet (LAN) cable (Cat-5e or higher). <*>

  <*> This product complies with the IEEE 802.3af Power-over-Ethernet (PoE) standard. If PoE is available on your network, this product can receive the necessary power from the network through the ethernet cable and no DC adaptor is needed. If PoE is not available, you will need to connect a DC adaptor to the product.

  Recommended PoE-connected devices (user supplied) specifications

  - A switching hub or power supply device that supports PoE (compliant with IEEE 802.3af)
  - Complies with safety standard IEC60950-1 or BIS certification

  Refer to the documentation included with the PoE-connected device for details.

  If unsure whether it complies with safety standards, please contact the manufacturer of the switching hub or power supply device.

  Recommended DC adaptor (user supplied) specifications

  - Complies with safety standard IEC60950-1 or BIS certification
  - INPUT: AC 100 V-240 V, 50/60 Hz, 0.8 A Max.
  - OUTPUT: DC 12 V, 1.5 A, 18 W

  Refer to the documentation included with the DC adaptor for details.

  If unsure whether it complies with safety standards, please contact the manufacturer of the DC adaptor.

  If devices other than above are connected, safety and performance cannot be guaranteed.
- Do not place objects on the cables. Install the product where no one can step or trip on the cables.
- Do not allow the cables to be excessively pulled, bent or placed under heavy objects.
- Insert the DC cable plug or DC adaptor firmly all the way into the terminals or power outlet. If they are not inserted all the way, heat may be generated.
- Never touch the DC cable plug or DC adaptor with wet hands.
- Do not disassemble or modify the product. Refer servicing to an authorised service centre when service is required. Disassembling the product or manipulating the product in a way not described in the documentation may expose you to dangerous voltages and other risks.
- Do not touch the product, cables, DC cable plug or DC adaptor during an electrical storm. There may be remote risk of electric shock from lightning.
- Never install wiring during a lightning storm.
- Do not connect non-specified devices.

- Do not connect a cable to a terminal that is not specified in this document.
- When opening holes in walls for installation or wiring, or when securing the cable, make sure you do not damage existing wiring and ductwork.
- Do not make any wiring connections when the power outlet is turned on.
- Do not install the product in the following places:
  - Places where the product may be splashed with water or chemicals
  - Places where there is a high concentration of dust or high humidity
- Do not expose the product to direct sunlight.
- Do not push any objects through the openings of the product.
- If any of the following conditions occur, disconnect the Ethernet (LAN) cable from the product, disconnect the DC adaptor from the power outlet, and then refer servicing to an authorised service centre.
  - The product emits smoke, an abnormal smell or makes unusual noise
  - The cables are damaged or frayed
  - Metal objects have been dropped inside the product
- When existing wires are used, it is possible that they contain AC voltage. Contact an authorised service centre.

⚠ CAUTION

Preventing accidents, injuries, and property damage

- Do not use the product in unstable areas or areas prone to strong vibrations. This may cause the product to fall, resulting in damage to the product or injury.
- If the wiring passes outdoors, use a conduit and a surge protector.
- If the wiring passes underground, use a conduit, and do not make any connections underground.
  Install the product securely with screws according to the instructions in this document to prevent it from falling off the wall. Avoid installing onto low-strength walls, such as gypsum board, ALC (autoclaved lightweight concrete), concrete block, or veneer (less than 18 mm thick) walls.
- The DC adaptor is used as the main disconnect device. Ensure that the power outlet is installed near the product and is easily accessible. Ensure that the power supply of PoE hub is connected to a breaker in an easily accessible distribution board.
- Do not put your ear(s) near the speaker, as loud sounds emitted from the speaker may cause hearing impairment.
- To prevent serious injuries due to the product unexpectedly falling, the product with a wall mount feature must be installed at a height of 2 m or lower.

Important safety instructions

When using this product, basic safety precautions should always be followed to reduce the risk of fire, electric shock, or personal injury.

Follow the power supply instructions indicated in this document.

1. Use only the ethernet (LAN) cable or DC adaptor indicated in this document.

SAVE THESE INSTRUCTIONS

Privacy and rights of portrait

When installing or using the product, please take into consideration the rights of others with regard to privacy and rights of portrait.

- It is generally said that "privacy" means the ability of an individual or group to stop information about themselves from becoming known to people other than those whom they choose to give the information. "Rights of portrait" means the right to be safe from having your own image taken and used indiscriminately without consent.
- Please observe the legal regulations (data protection, video surveillance) in your country during use.

Data security

In order to use the system safely and correctly, the data security guidelines (listed below) must be observed.

Failure to do so may result in the following.

- Loss, leakage, falsification or theft of user information.
- Unauthorised or illegal use of the system by a third party.
- Interference or suspension of service caused by a third party.

What is user information?

User information is defined as the following types of information.

- Information stored in the product
  - System event information
  - Resident names and room numbers
  - System and device settings
  - QR code for unlocking
  - Face recognition data for unlocking
- Information stored on the computer that is used by the setup tool (CMS)
  - Resident names and room numbers
  - System and device settings

Data security guidelines

- **Observe proper management of passwords.**
  - Passwords can be used to program the system, open doors, etc. Select passwords that are difficult to guess, change them regularly, and keep them secret. Assign a unique password to each device.
  - You will never receive enquires about passwords from Panasonic.
- **Use caution when entering or saving contact information for use by the system.**
  - When configuring email addresses, room numbers, or other contact information, make sure all information is entered correctly. Incorrect information could cause user information to be disclosed to unintended recipients.
- **Protect user information when sending the product to be repaired, or when handing it over to a third party.**
  - Use the product‘s reset function to initialise the product before when sending the product to be repaired or handing it over to a third party.
  - Note that user information may be deleted or initialised when the product is repaired.
  - Refer all repairs to a trusted Panasonic service centre.
- **Protect user information stored on the computer used to configure the system.**
  - When user information is stored on a computer, the confidentiality of that information becomes the responsibility of the installer. Take precautions to prevent the unauthorized use of the computer and the setup tool (SCS and CMS) used for performing system configuration or maintenance.

- Connect the computer to the network only when performing system configuration or maintenance, and disconnect the computer from the network as soon as the work is complete.
- Use a secure network that is protected by a firewall, etc.
- To prevent the leaking of personal information, enable a screensaver for the computer that uses a password.
- Before disposing of the computer, ensure that data cannot be retrieved from it by formatting the hard disk and/or rendering it physically unusable.

- **Protect user information when disposing of the product.**
  - Use the product‘s reset function to initialise the product before disposing of the product.

Disclaimer

- Recorded data may be altered or deleted as a result of incorrect operations, exposure to static electricity, accidents, malfunction, repairs or other operations.

  To the maximum extent permitted by applicable law, Panasonic assumes no liability for any direct or indirect damages resulting from the loss or alteration of recorded data.
- To the maximum extent permitted by applicable law, Panasonic assumes no responsibility for injuries or property damage resulting from failures arising out of improper installation or operation inconsistent with this document.
- To the maximum extent permitted by applicable law, Panasonic will not be held responsible for any damage or loss due to non-performance or delay in performance, error or failure of network and/or any products.

Other important information

- Before attempting to connect or operate this product, please read the nameplate on the bottom or rear of the product.
- When you leave the product unused for a long period of time, consult the installer regarding unplugging the product from the power outlet.
- If you stop using this product, remove it from the walls to prevent it from falling off.
- When power fails, this product cannot be used.
- Panasonic may not be liable for damages due to external factors such as power failures.

General information

- In the event of problems, you should contact your equipment supplier in the first instance.
- After removing the product and any included items from the packaging, store, dispose, or recycle the packaging as necessary. Note that certain types of packaging may be a suffocation or choking hazard.

Cleaning

Wipe the product with a soft, dry cloth.

- For excessive dirt, wipe the product with a cloth slightly dampened with fresh water.
- When the product is installed near ocean coasts, wipe the product with a cloth slightly dampened with fresh water once every 2 to 3 months.

Important:

- **DO NOT USE ANY SOLVENTS CONTAINING CHLORINE. This causes the product to rust.**
- **Do not use any cleaning products that contain alcohol, polish powder, powder soap, benzine, thinner, wax, petroleum, or boiling water. Also do not spray the product with insecticide, glass cleaner, hair spray or wall paint. This may cause a change in colour or quality of the product.**

Open source software notice

Parts of this product use open source software supplied based on the relevant conditions of the Free Software Foundation's GPL and/or LGPL and other conditions. Please read all licence information and copyright notices related to the open source software used by this product.

This information is available at the following web page:

https://security.in.panasonic.com/products/vl-vq9000sx

At least three (3) years from delivery of this product, Panasonic Corporation will give to any third party who contacts us at the contact information provided below, for a charge of no more than the cost of physically distributing source code, a complete machine-readable copy of the corresponding source code and the copyright notices covered under the GPL and the LGPL. Please note that software licensed under the GPL and the LGPL is not under warranty.

https://security.in.panasonic.com/products/vl-vq9000sx

Graphical symbols for use on equipment and their descriptions

Symbol	Explanation
	Alternating current (A.C.)
	Direct current (D.C.)
	Caution: risk caused by visible radiation
	For indoor use only
	Class Ⅱ equipment (equipment in which protection against electric shock relies on Double Insulation or Reinforced Insulation)

Terms and illustrations

- Design and specifications are subject to change without notice.
- Illustrations may vary slightly from the actual product

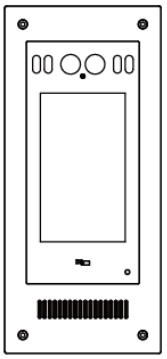
Trademarks

- Android is trademark of Google LLC.
- MIFARE is a registered trademark of NXP B.V. and is used under license.
- The word "QR Code" is a registered trademark of DENSO WAVE INCORPORATED in Japan and other countries.
- All other trademarks identified herein are the property of their respective owners.

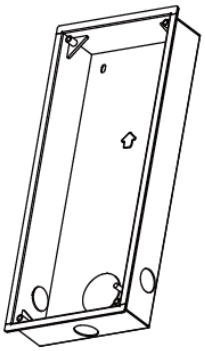
1. Technical Specifications

- 7 inches IPS LCD screen, 1024 x 600 resolution
- Face recognition to unlock, dual cameras enable liveliness check
- White LED for night vision, light adjustable and automatic for dark environment
- Viewing angle: H116° V62° D132°
- Operating system: Android™ 12
- Network Connection: Ethernet (PoE)
- Operating Voltage: 48 V (PoE), 12 V (DC)
- Operation temperature: -10 ℃ to +55 ℃
- Dust-proof and water-proof (IP65)
- Flush mounted
- Anti-vandal (IK07) and tamper alarm
- 2 relay outputs
- Wiegand input and output
- Dimensions (mm): Approx. 355(H) x 160(W) x 58(D)
- Mass(weight): Approx. 1423 g
- IC card frequency: 13.56 MHz (ISO/IEC 14443 Type A (MIFARE®)),
  Transmission power: 6.9dBμV/ m (max.) @10 m

2. Packing Contents



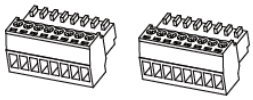
Main body



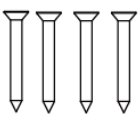
Metal embedded wall bracket

2 pin DC power connector

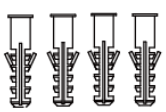
4 pin connector



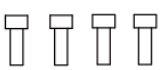
8 pin connector



Screw
(4 mm x 35 mm)

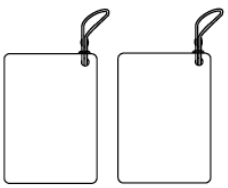


Plastic expansion pipe
(4 mm x 35 mm)



Hex screw
(5 mm x 13 mm)

Screws driver tool
(Wrench)



RFID card

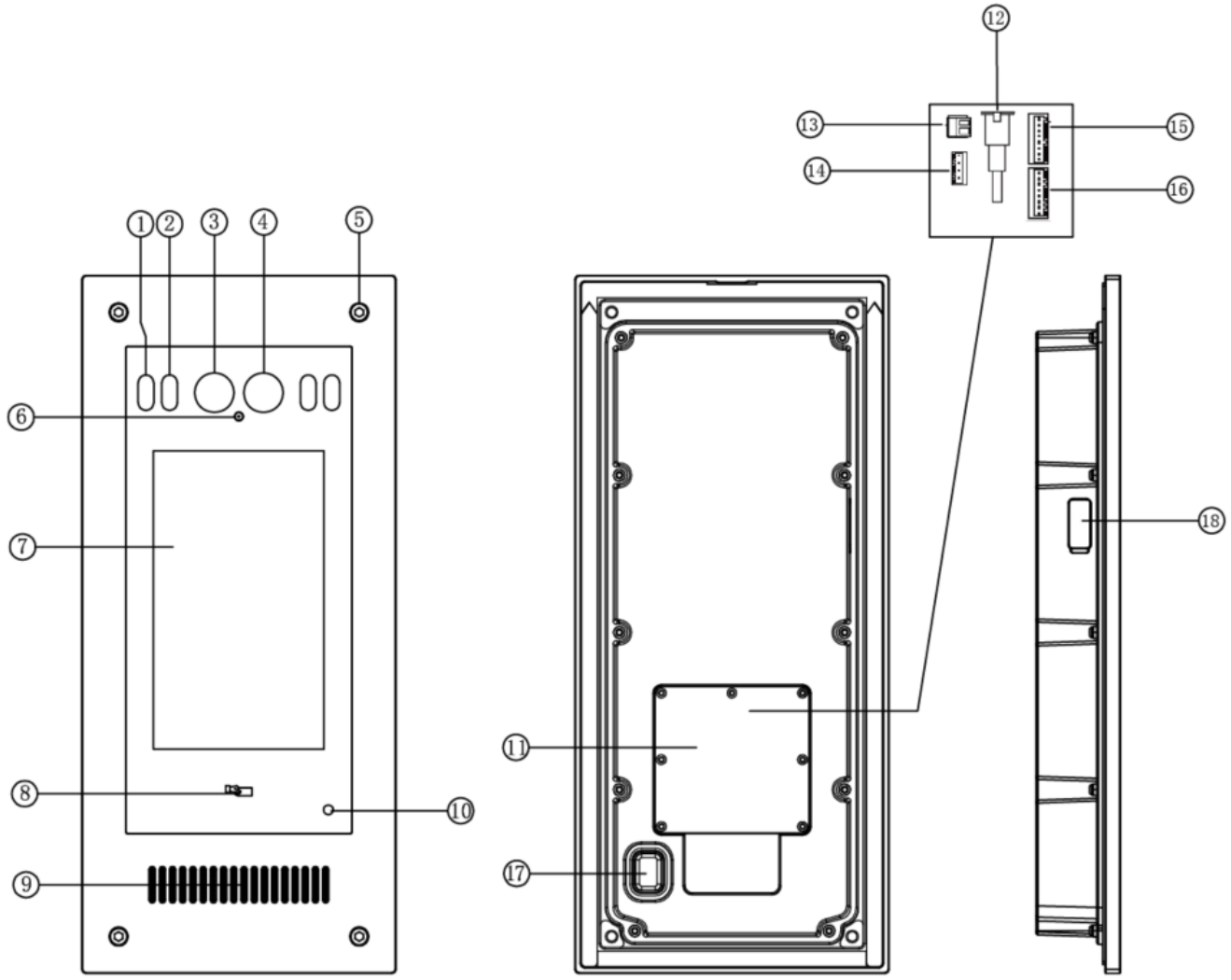
Plastic packaging materials information for this product

Plastic packaging material	Recycling mark	Thickness	Importer EPR number
Left cushion		50 Microns or more	Panasonic Life Solutions India Pvt. Ltd. EPR number : 2023030608544812298
Right cushion		50 Microns or more	
Bag for Main body		50 Microns or more	
Protective film for Main body		50 Microns or more	
Bag for Connector / Screw / Expansion pipe / Wrench		50 Microns or more	
Bag for consolidating RFID cards		50 Microns or more	
Bag for a single RFID card		50 Microns or more	

This information is prepared in accordance with India / Plastic Waste Management (Amendment) Rules.

3. Name and Functions of Each Part

3.1 Front and Rear Part



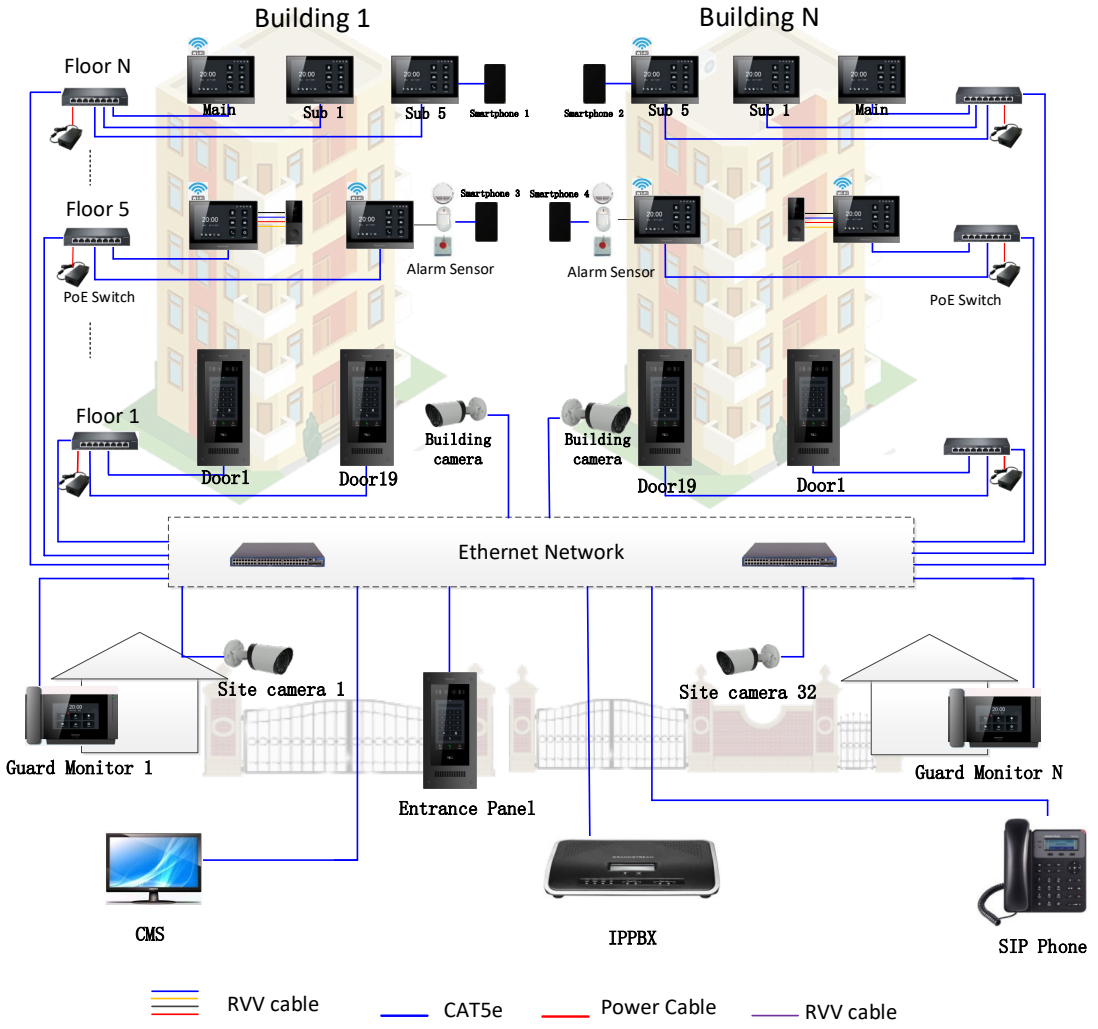
NO.	Part Name	NO.	Part Name
1	White LED for night vision	10	Light sensor
2	IR light	11	Cover for cables
3	Main camera	12	RJ45 connector
4	Auxiliary camera	13	DC power
5	Screws for fixing hood cover	14	Relay release connector
6	Microphone	15	Wiegand connector
7	7 inches LED	16	Relay lock connector
8	Card-read area	17	Tamper alarm button
9	Speaker	18	Micro SD card slot

4. Connection Diagram

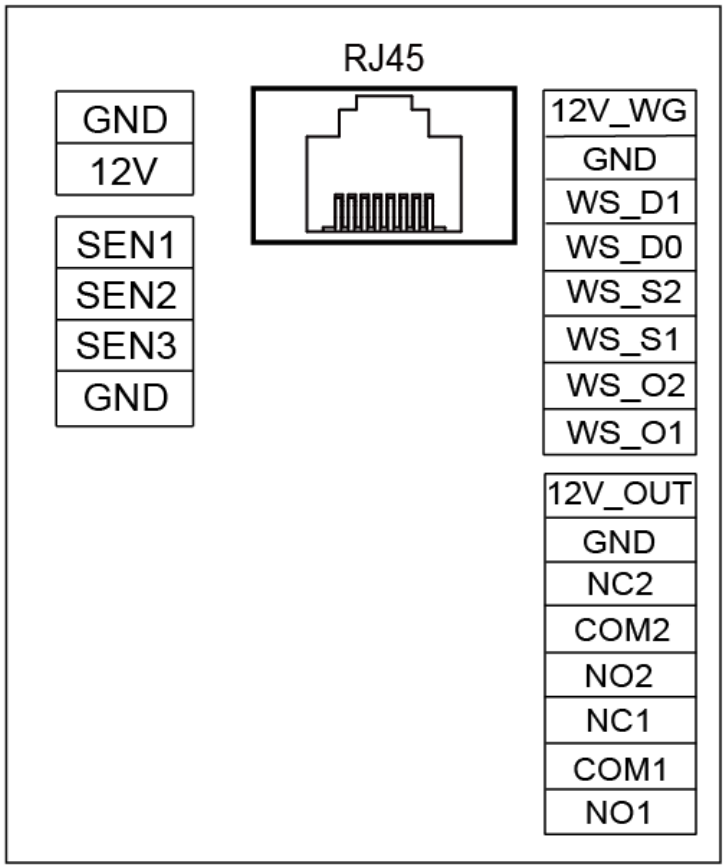
4.1 System Layout

Remark:

- The distance between other devices (indoor monitor, door panel, network switch, guard unit, and PoE Switch) and PoE Switch is limited to 70 meters.
- The system supports up to 98 buildings.
- The system supports up to 32 IP cameras.
- One room supports up to 6 monitors.
- Door panels can be classified into entrance panels and building panels. Entrance panel can talk with all indoor monitors in the site and unlock locks of the site. Building panel can talk with all indoor monitors in the building and unlock locks of the building.
- Guard units have authority to talk, send messages, receive SOS calls and receive alarms. Guard units can be classified into site guards and building guards. Site guards have authority of the site. Building guards have authority of the building.
- The system supports two Network configurations (Auto and Manual).
- The encode type and network configuration must keep up with first building panel.
- The address of other devices can be successfully set only after the first Building panel (4-digit: 0181; 5-digit: 01801; 6-digit: 019001) in the system is set.



4.2 Wiring Diagram



RJ45：Connect PoE port to the system.

12V/GND: Supply power when PoE is not in use. *1

SEN1/SEN2/SEN3/GND: Signal input to release relay, input for exit buttons.

12V WG/GND: Wiegand device power supply.

WS_D1/0: Wiegand input interface for Wiegand access control.

WS_S1/2: Wiegand common interface for Wiegand access control, can be configured as output/input.

WS_O1/2: Wiegand output interface for Wiegand access control.

12V OUT/GND: 12 V power output for lock.

NO2/COM2/NC2: NO/NC relay terminal 2.

NO1/COM1/NC1: NO/NC relay terminal 1.

*1 If PoE is not available, connect the DC adaptor to the product as follows:

1) Strip the remaining end of the DC wire of DC adaptor.
2) Insert the end of the DC wire into the 2 pin DC power connector (included) and secure it with a minus screwdriver.

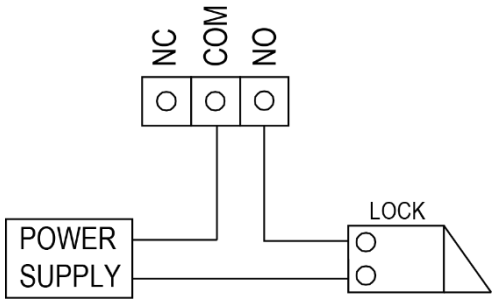
   (Connect ensuring that the polarity of DC+ and DC- is correct.)
3) Connect the 2 pin DC power connector to the product.

4.3 Relay Lock Connection

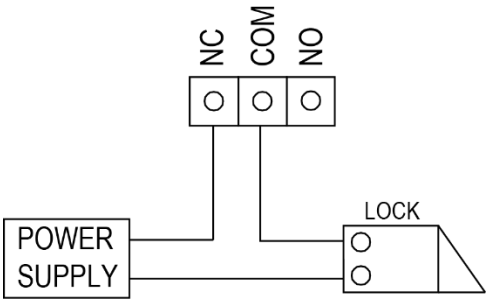
Note:

1. The external power supply must be used according to the lock.
2. The door lock is limited to 30 V, 2 A.
3. There are two unlock types as the follows:
4. Both entrance panel and building panel support 2 NO/NC locks.

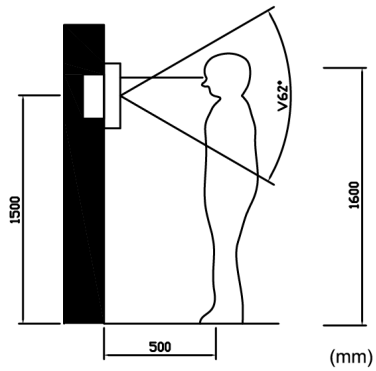
Type 1: Power-on-to-unlock



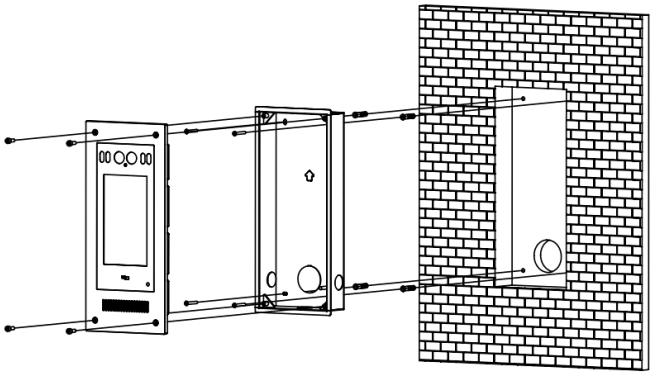
Type 2: Power-off-to-unlock



5. Installation



Camera installation location
Standard installation height of door panel: lens's height is about 1,600 mm above the floor.



Wiring and installation of door panel

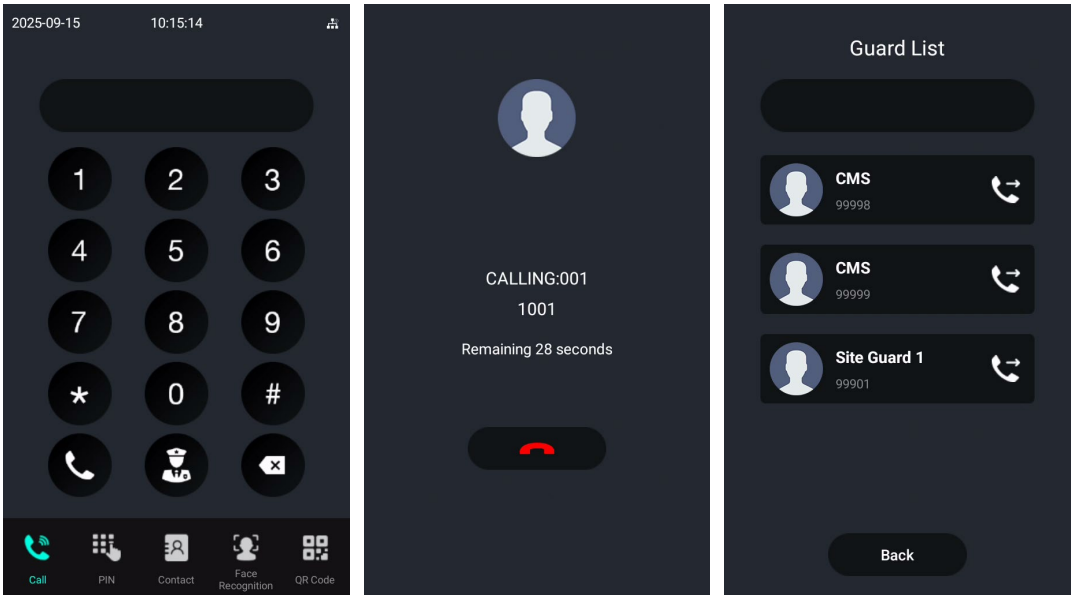
1) Prepare a niche in the wall measuring 355 mm x 160 mm x 58 mm for installation of embedded box.
2) Remove embedded box behind door panel and fix it on the wall with screw;
3) Pull the cable out and connect the system according to 4.1 and 4.2;
4) Fix the swipe card panel on the door panel with screw;
5) Fix the door panel onto the embedded box and fasten it with screws.

6. Operation Description

6.1 Call Page

Remark:

- Once a human face is detected, the white LED will be lit up, if the LED is enabled.
- Once a human face is detected, the screen will also be lit up.
- The device screen will go back to black screen, if not detecting a human face or not receiving any operations for 150 seconds.



You can input the room number you want to call and then press  to start the call. In the call page, you can press  to delete the number. During the call and the talk, you can press  to end.

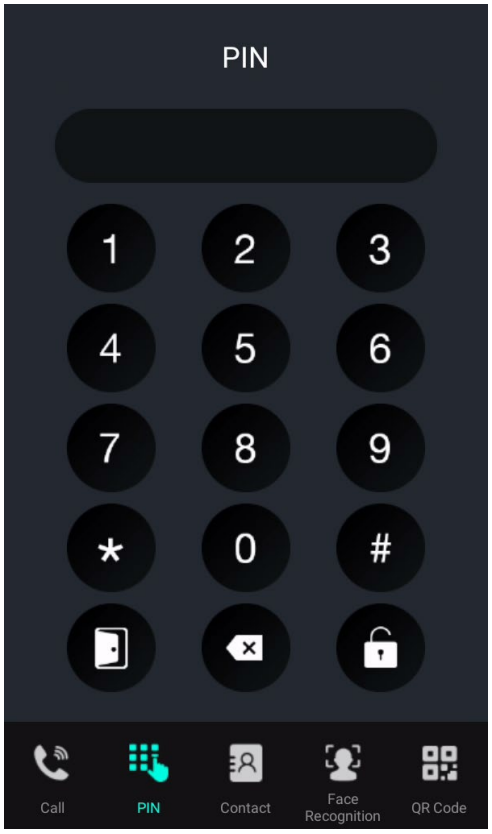
Press  to enter the guard list page, you can search for devices or select the device you want to call and then press the nameplate to start the call; when there is only one Guard in the system, press  , it will call that Guard directly.

Remark:

- The call rings for 30 seconds, and the talk can last for 2 minutes.
- The way to input the address: for Building Panel,
  4-digit: call room 1--dial 01 or 1; call room 12--dial 12.
  5-digit: call room 1--dial 001 or 01 or 1; call room 12--dial 012 or 12.
  6-digit: call floor 1 room 1--dial 0101 or 101 (only call flats belong to this Building).
- The way to input the address: for Entrance Panel,
  4 digits: call Building 1 Room 1--dial 01 01.
  5 digits: call Building 1 Room 1--dial 01 001.
  6 digits: call Building 1 floor 1 room 1--dial 01 01 01.

6.2 PIN unlock

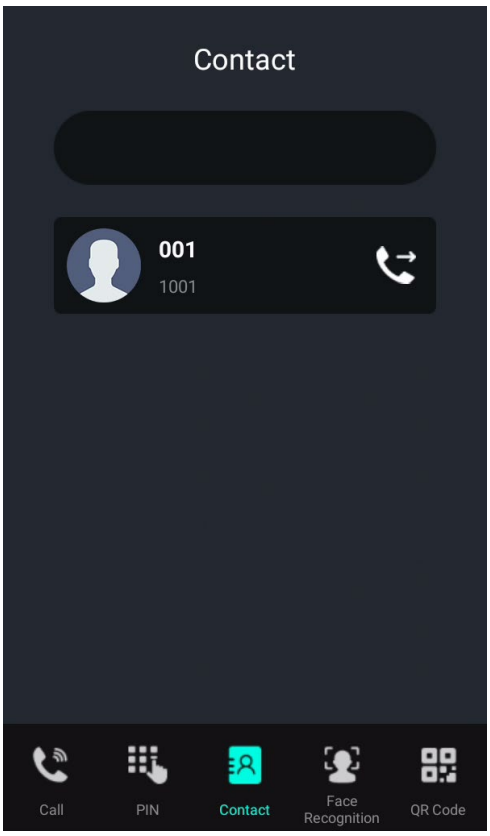
Click  and input password then press  to open relay lock 1 (usually used as door lock), or press  to open relay lock 2 (usually used as garage lock), if password is correct, there will be a prompt voice ‘Door open’. If the password is incorrect, the screen will pop up ‘Invalid password’.

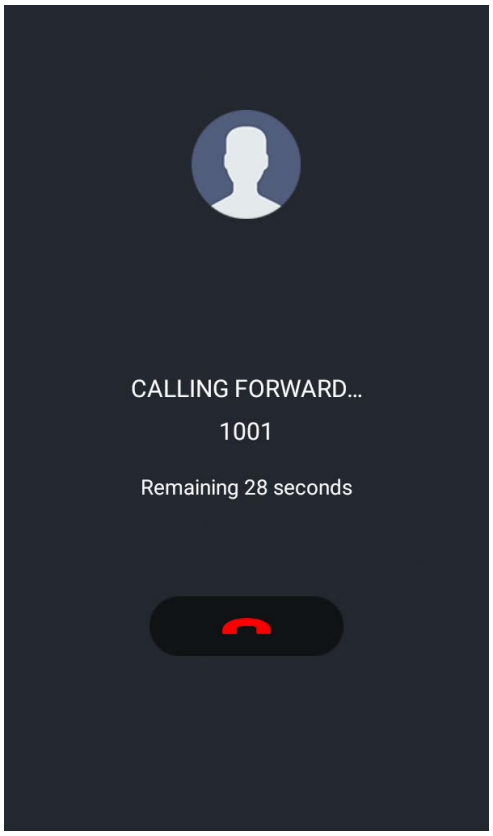


Remark:

- The unlock functions can be enabled/disabled in the access settings.
- Swipe card distance ≤ 20 mm.

6.3 Contact page



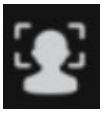


In contact page, you can search for devices or select the device you want to call and then press the nameplate to start the call.

Remark:

The call rings for 30 seconds, and the talk can last for 2 minutes.

6.4 Face Recognition unlock

Click  to use Face Recognition to unlock. Stand before the lobby display station within 1 meter and make sure only one face is in the recognize area. If the face is already added in the [Access] page, after successful recognition, it will show and prompt voice ‘Door Open’. Otherwise, it will pop up ‘Recognize Failed’. Face Recognition can be added in [Contact] or CMS software.

Remark:

- The face recognition can last for 15 seconds.
- Face Recognition unlock supports one face at a time.
- Face Recognition capacity max 10,000.

6.5 QR code unlock

You can press  to use QR code to unlock. QR code can be added in CMS software. If an added QR code is recognized, it will show and prompt voice ‘Door Open’. Otherwise it will pop up ‘Incorrect QR code’.

6.6 IC card unlock

You can swipe IC cards to open the lock, in the default setting, short swipe will unlock electric lock, long swipe will unlock garage lock. IC cards can be added in [Access] or CMS software. Card reader is at the lower area of the device.

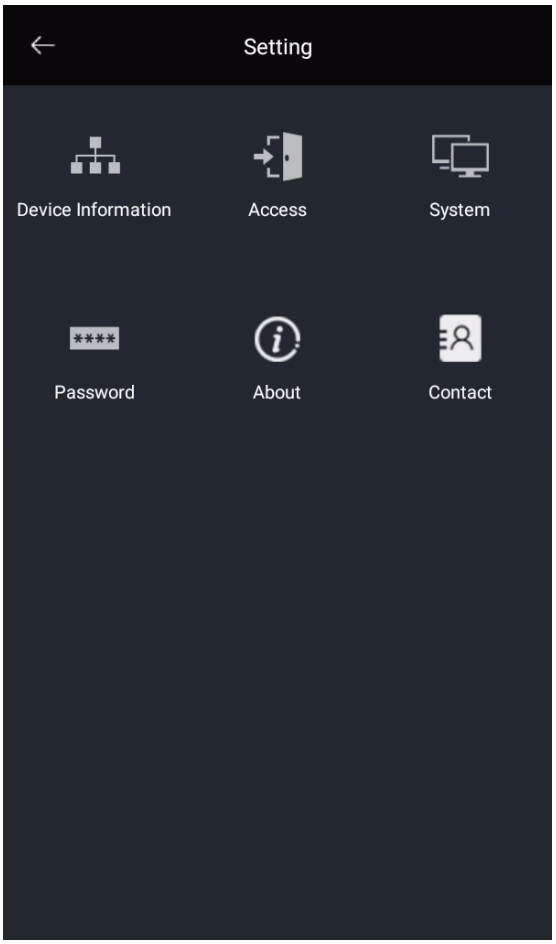
Remark:

- IC card capacity max 10,000.

6.7 Setting Page

Press * → 📞 → 99 → input the engineer password → Confirm, the screen will enter the setting page.

- **Please refer to the included important information leaflet for details about the default password.**



6.7.1 Device Information

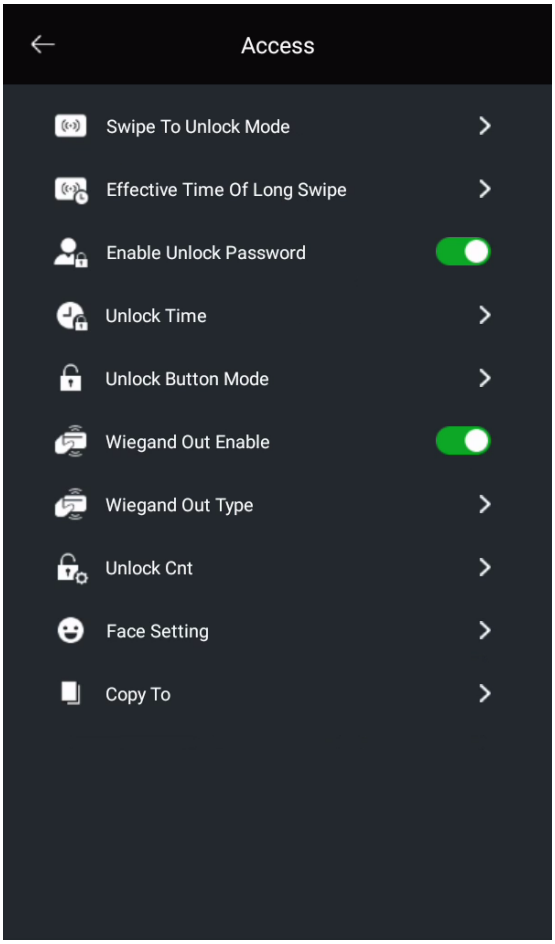
In [Device Information] setting page, you can set the Building NO. / Device Id and configure device IP address. After the setting is completed, the device will reboot automatically.

Remark:

- It supports three encode types (6-digit encoding: **Building No.** + **Floor No.** + **Flat No.** ; 5-digit encoding: **Building No.** + **Room No.** ; 4-digit encoding: **Building No.** + **Room No.**)

- It supports two Network configurations (Auto and Manual) whatever encoding type you choose.
- 4-digits encoding for Building Panel, Building number range: 1 to 98; Device Id range: 81 to 85.
- 4-digits encoding for Entrance Panel, Building number range: 99; Device Id range: 81 to 85;
- 5-digits encoding for Building Panel, Building number range: 1 to 98; Device Id range: 801 to 819.
- 5-digits encoding for Entrance Panel, Building number range: 99; Device Id range: 801 to 819;
- 6-digits encoding for Building Panel, Building number range: 1 to 98; Device Id range: 9001 to 9019.
- 6-digits encoding for Entrance Panel, Building number range: 99; Device Id range: 9001 to 9019.

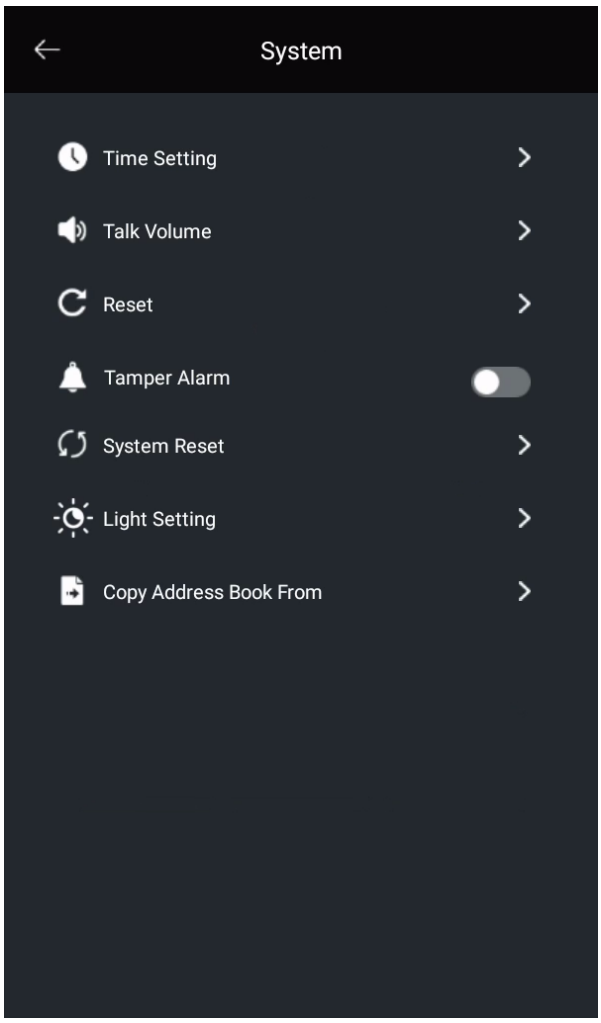
6.7.2 Access



- In [Swipe To Unlock Mode], you can choose 2 modes, short swipe to open electric door and long swipe to open garage door, or long swipe to open electric door and short swipe to open garage door.
- In [Effective Time Of Long Swipe], you can set the time length for long swipe (default time is 5 seconds).
- In [Enable Unlock Password], if this function is disabled, all the unlock passwords will all be not available. When you input the password to unlock, it will show ‘Function is disabled!’
- In [Unlock Time], you can set the opening time for both electric door and garage door. Time range is 1-15 seconds (default time is, electric door:1 second; garage door:5 seconds).
- In [Unlock Button Mode], you can choose normal open type lock or normal close type lock.

- In [Wiegand Out Enable], you can enable or disable Wiegand out port.
- In [Wiegand Out Type], you can choose the type of Wiegand between Wiegand 26 and Wiegand 34.
- In [Unlock Cnt], if you set to 1, only the electric lock can be unlocked. If you set to 2, both the electric and the garage lock can be unlocked.
- In [Face Setting], you can enable the Face Recognition function. Set the environment mode between indoor and outdoor, according to your installation, this setting will control the brightness parameter of face scanning. And enable the liveliness check, set the liveliness level sensitivity.
- In [Copy To], you can copy the Face Recognition data/ IC&ID card data/ address book data/ password data to other lobby display station.

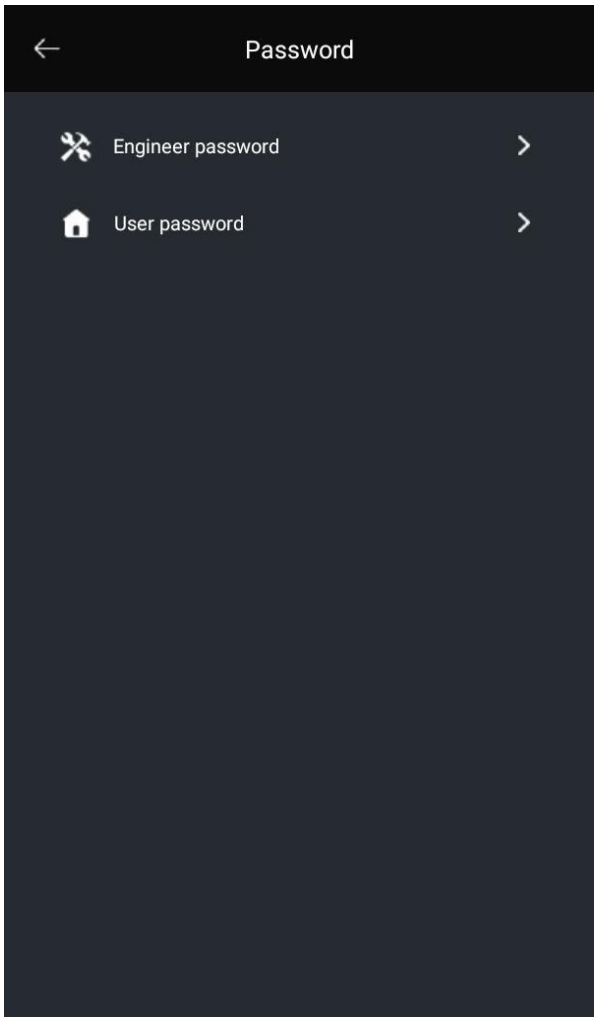
6.7.3 System



- In [Time Setting], you can set the date (Year-Month-Day), and time (Hour: Minute : Second) displayed on the device.
- In [Talk Volume], you can adjust the talking volume from 1-10 (default is 7).
- In [Reset], if you press ‘Yes’, all settings will be set to default, except for the [Device Information].
- In [Tamper Alarm], if enable, the alarm will go off when the tamper alarm button is released. And the CMS and guard units will receive this alarm.
- In [System Reset], if you press ‘Yes’, all settings will be set to default, including the [Device Information].

- In [Light Setting], you can set the corresponding LED lightness for day (default:1) and night (default:10). Set the lightness of the screen (default:100). The door panel can recognize day and night according to the environment lightness.
- In [Copy Address Book From], you can copy the address book from other lobby display station or Micro SD card which stores address book data.

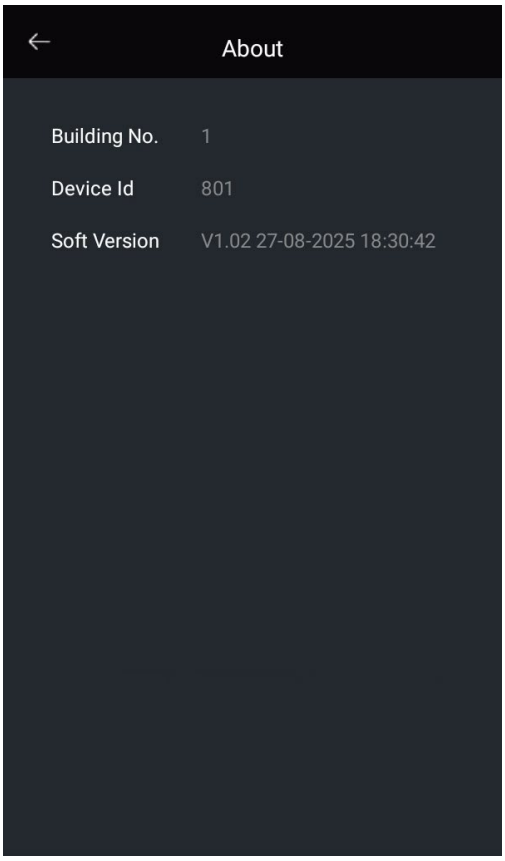
6.7.4 Password



- In [Engineer password], you can change the engineer password.
- In [User password], you can change the user password of Contact.

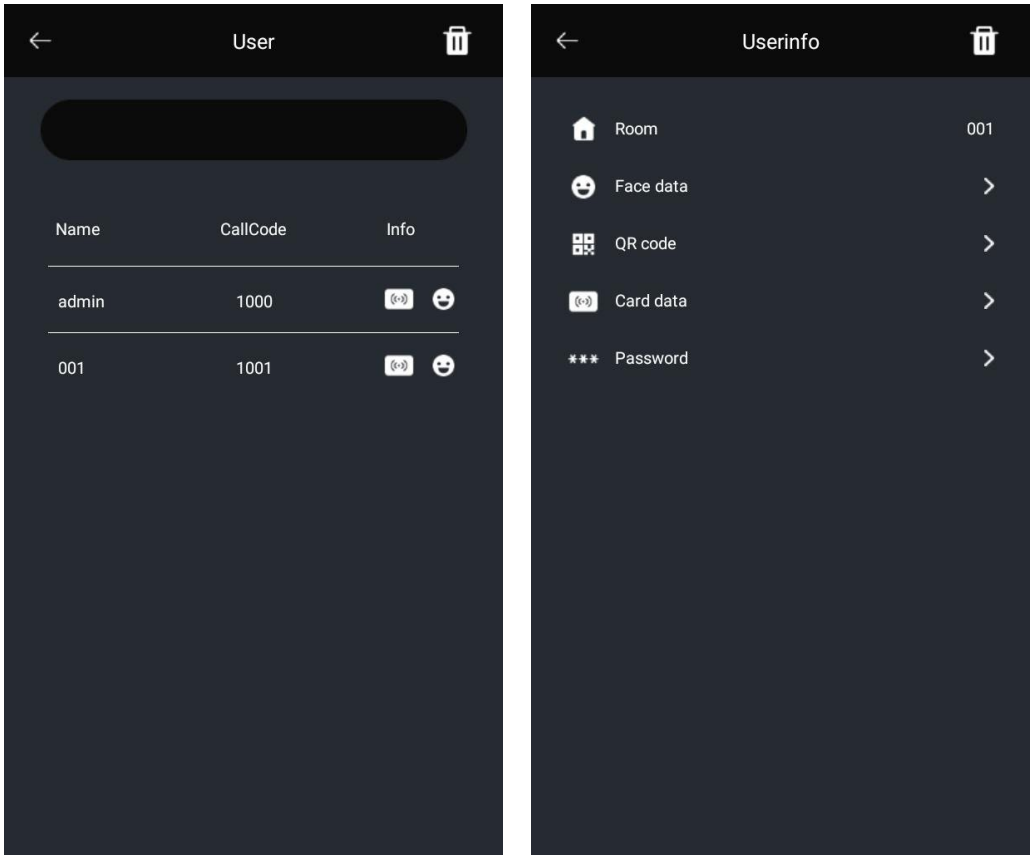
- **Please refer to the included important information leaflet for details about the default password.**

6.7.5 About



In [About], you can check the device information and check the firmware version.

6.7.6 Contact



- In [Contact], you can authorize unlock function to the admin account or the registered indoor monitors. Choose a user you want to add. You can press the upper right delete icon to delete all the access information, or get into user page delete access information accordingly.
- In [Face data], you can add or delete Face Recognition. To add Face Recognition, stand 1 meter before the lobby display station, press the camera icon, and name the Face Recognition, it will pop up ‘add face successfully!’. If failed, you need to modify the face position and angle according to the prompt. You can delete the Face Recognition data by pressing the delete icon.
- In [QR code], you can manage and delete the existing QR code.
- In [Card data], you can add and delete the IC/ID card. To add card, press ‘Add card’, and swipe the IC or ID card at the lower card-read area of the device. You can delete the cards by pressing the delete icon.
- In [Password], you can set password for user to open the electric and garage door. To add password, press ‘Add password’, type the password and retype to confirm. One user account only supports one password.

Remark:

- You can also add Face Recognition in CMS software.
- You can add QR code in both CMS software and mobile APP.
- You can authorize which lock to open with the Face Recognition/QR code/IC&ID card/password in the CMS
- If [Unlock Cnt] is set to 1, long swipe or short swipe will only open the authorized lock.

7. Web Client Operation

In the web client, you can review all the successful configuration of the device; you can also update the software version.

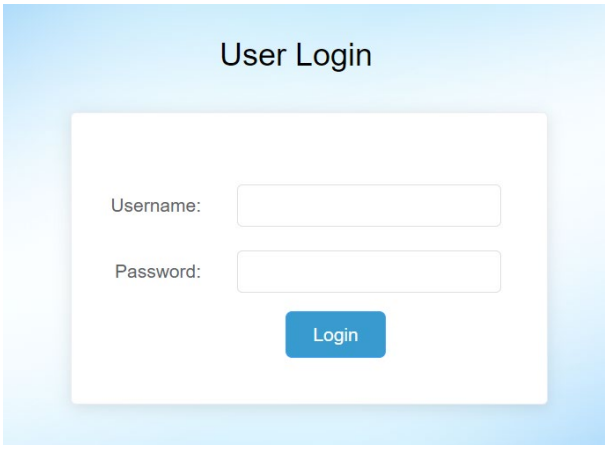
7.1 Login The Client

>> Connect your computer and device network with a network cable，then modify computer IP address to the same network segment of the system.

>> Open web browser, input the IP address of the device and press the “Enter” button to enter the login page;

>> You need to input user name & password, then click “Login” item to enter the local configuration page.

- **Please refer to the included important information leaflet for details about the default user name and password.**



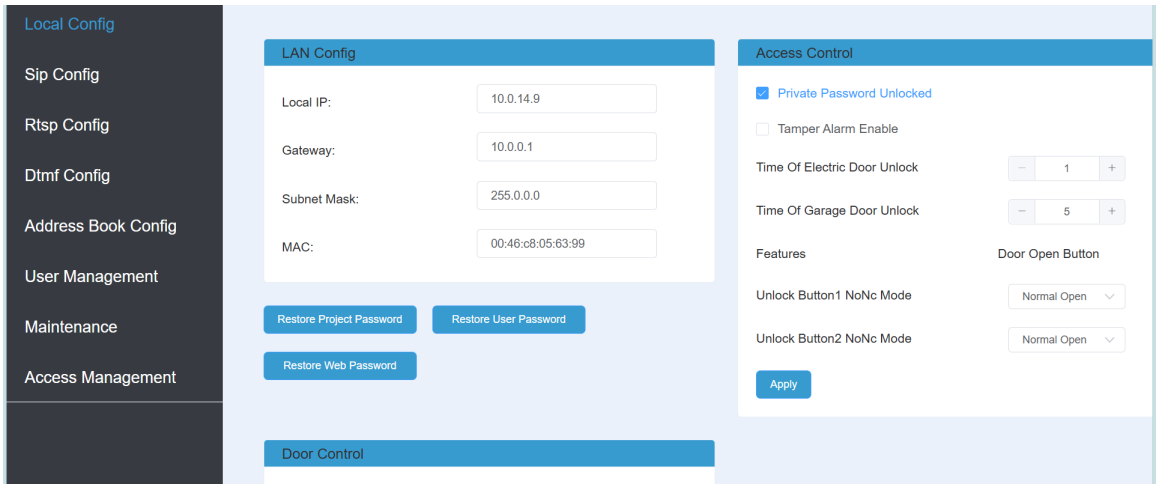
Remark:

- The computer and the device need to be on the same network segment, otherwise the login will fail.

7.2 Local Configuration Page

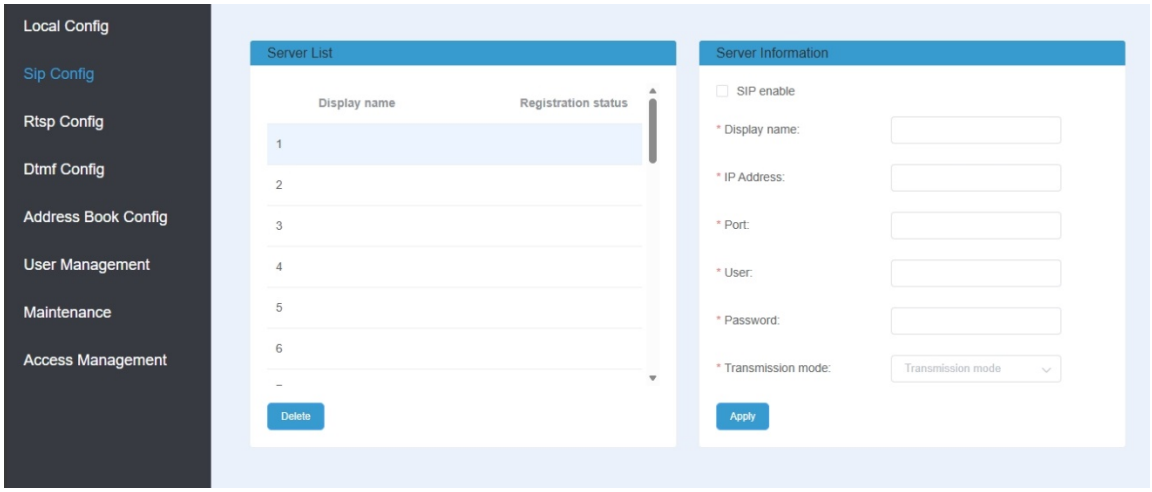
In the local configuration page, you can review the IP address of device, enable/disable the password unlocks function, enable/disable the tamper alarm function and set the unlock time. And you can set the mode of swipe card to unlock (default short swipe to unlock electric lock/lock 1, long swipe to unlock garage door/lock 2). You can also select the unlock button mode: Normal Open/Normal Close.

In [Restore Project Password], you can change the engineer password to default.



7.3 SIP Configuration Page

In the SIP configuration page, you can register the door panel to the SIP servers.

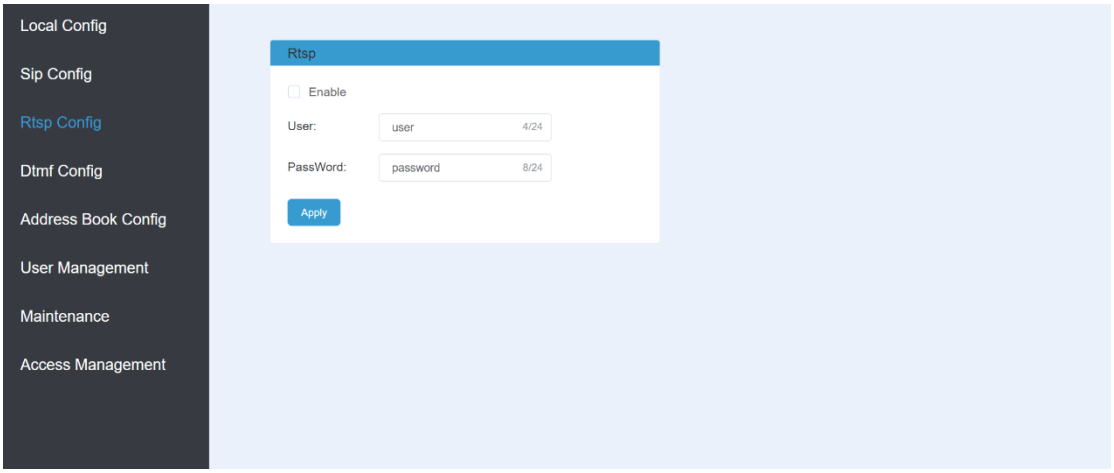


Remark:

- The door panel support 30 SIP accounts, corresponding to 30 SIP servers.
- SIP server should be in the same network segment with the door panel.

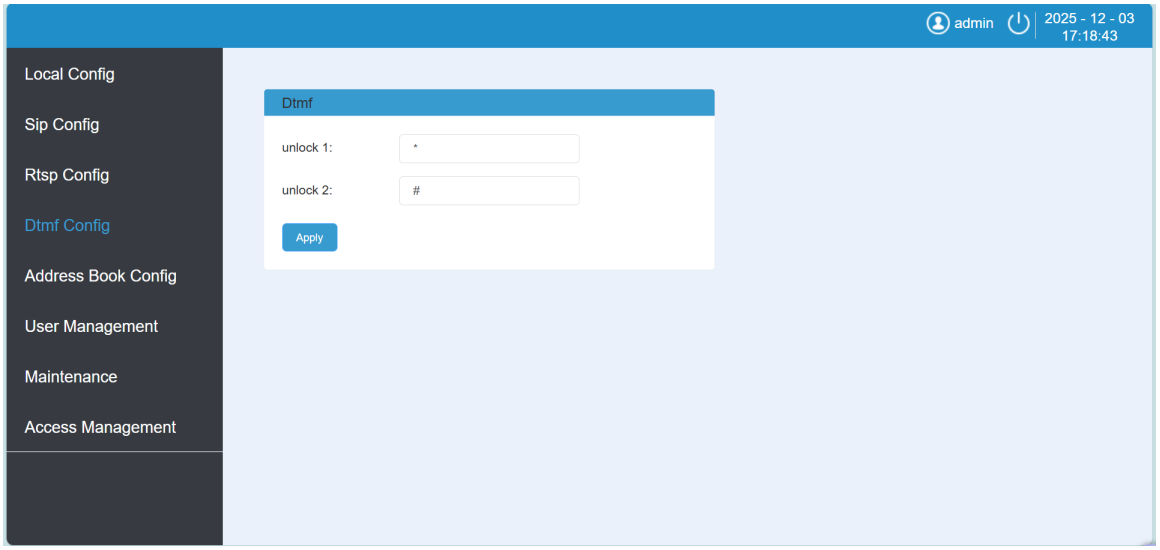
7.4 RTSP Configuration Page

In the RTSP configuration page, you can enable the RTSP function (default is OFF). You can also check and change the user name and password of RTSP. (Default user name: user, default password: password)



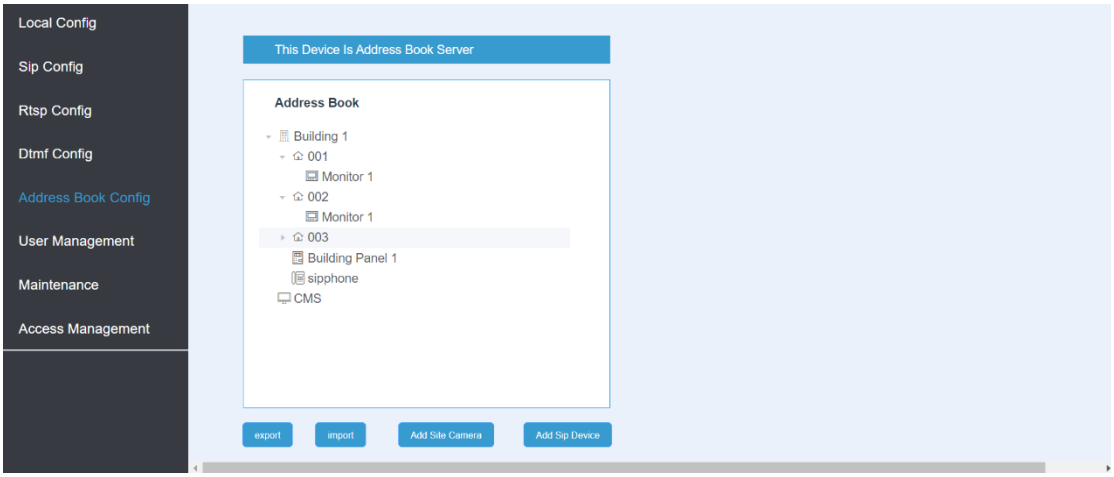
7.5 DTMF Configuration Page

In the address book configuration page, you can check and change the unlock code. Unlock 1 refers to relay 1. Unlock 2 refers to relay 2.



7.6 Address Book Configuration Page

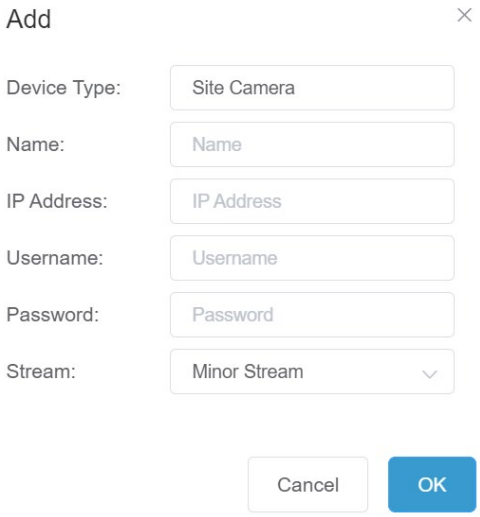
In the address book configuration page; you can review all the successful configuration of the devices in the system. Click the device name, you can review the ID code, IP address and MAC address, you can also modify the name of the devices. You can click the [Delete] item, and delete the device information (Building 1 can't be deleted).



Click the [export] item and then export address book to local PC. Click the [import] item and then import the local address book to the door panel.

7.6.1 Add Site Camera

You can click the [Add Site Camera] item; the screen will be show as follows:

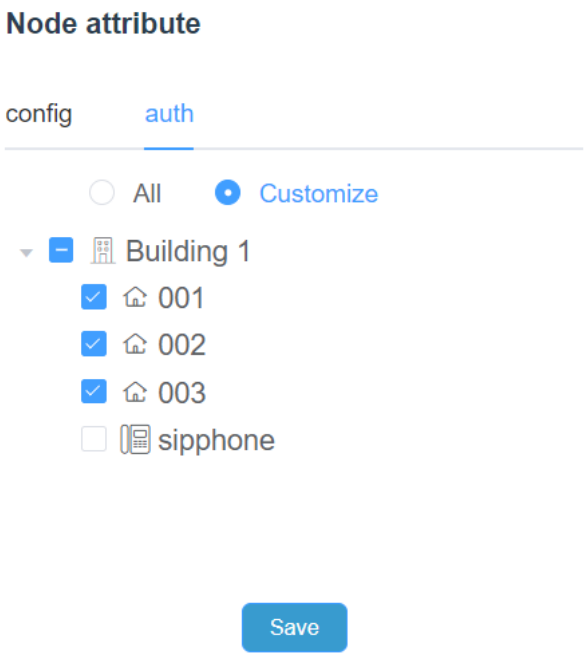


You can input the Name, IP address (the IPC and the device need to be on the same network segment), Username, Password and select the Stream mode: major stream/ minor stream, then click [OK] item to confirm it.

You can click the [delete] item, and delete the device information (Building 1 can't be deleted).

7.6.2 Site Camera Authorize

You can click the [auth] item; the screen will be show as follows:



You can click the [All] item and then click the [save] item, all the devices in the system can review the IPC monitoring image.

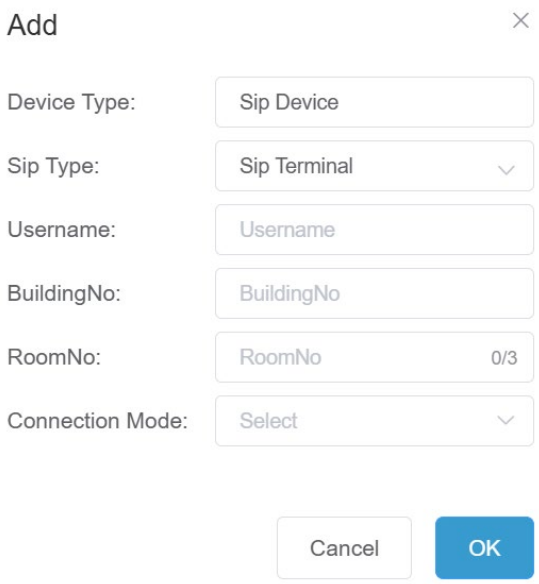
You can click the [Customize] item, select the one or more devices and then click the [save] item, only the selected devices can review the IPC monitoring image.

You can click the [closet] item and then lock the address book (add, delete and save the address book function are disabled).

Remark: It supports IPC with main stream and sub stream coding complexity.

7.6.3 Add Sip Device

You can click the [Add Sip Device] item; the screen will be show as follows:

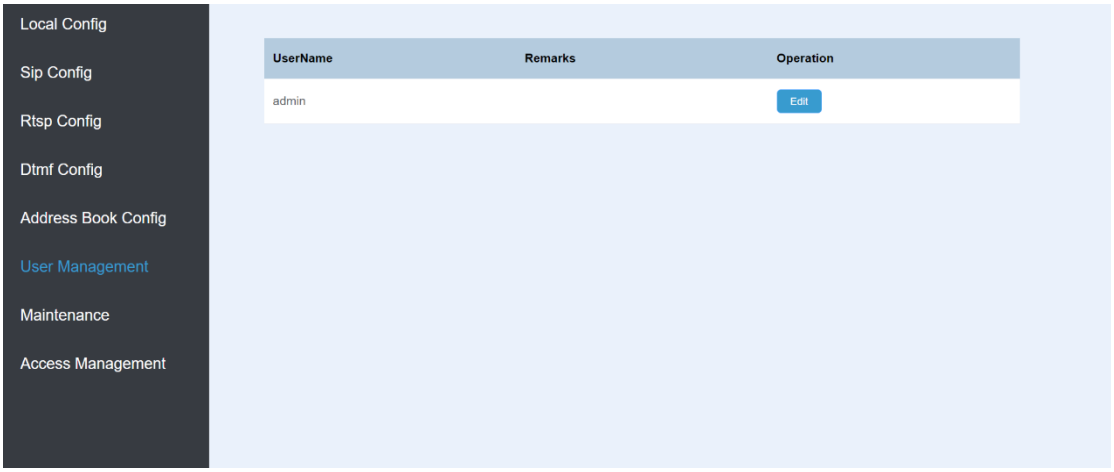


You can select Sip Type, input the Username, BuildingNo, RoomNo and Connection Mode, and then click [OK] item to confirm it.

Click [Connection Mode], then choose Through IP or Through Sip Server. If your Sip device is connected to the system by IP directly, you can use Through IP and input the IP Address. If your Sip device is connected to the system by Sip server, you can use Through Sip Server and choose the target Sip server which has the registration of both the door panel and the Sip device.

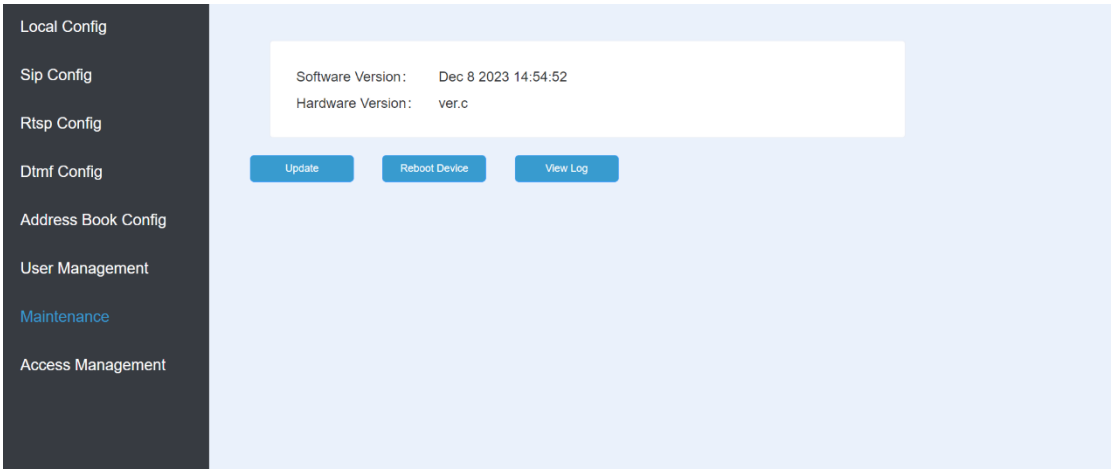
7.7 User Management Page

In the user management page, you can click the [Edit] item to set the login password and remarks.



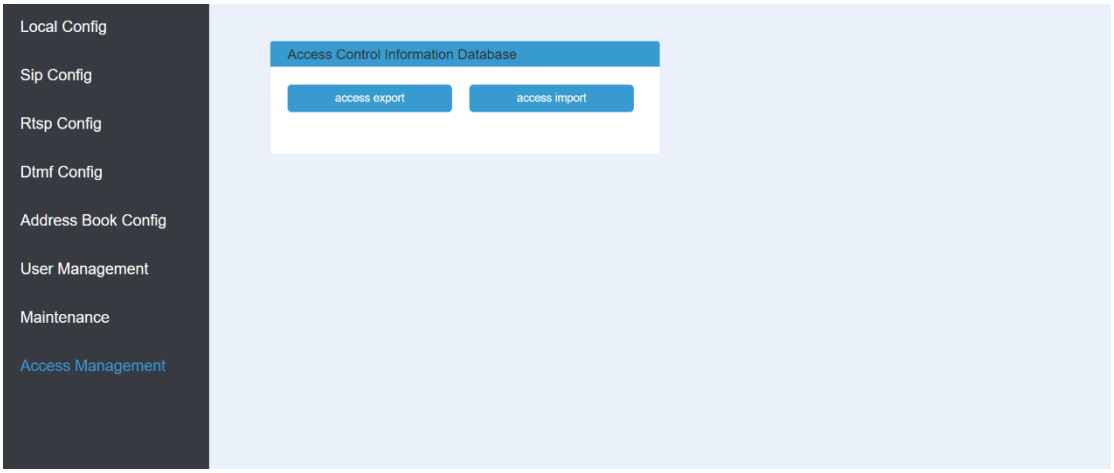
7.8 Maintenance Page

In the maintenance page, you can update the software version; you can also reboot the device.



7.9 Access Manage

In the Access manage page, you can import/export the information about the door panel (card information and unlock password).



When the door panel is reset, you can click the [access import] item to import the card information and unlock password into the door panel.

Panasonic Corporation
1006 Kadoma, Kadoma City, Osaka 571-8501, Japan
http://www.panasonic.com

PNQP2042ZA P0126MG0