Four-door Two-way Access Controller

User's Manual

V1.0.2

Foreword

General

This document elaborates on structure, installation and wiring of four-door two-way access controller.

Safety Instructions

The following categorized signal words with defined meaning might appear in the Manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: Providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product

updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.

- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

The following description is the correct application method of the device. Please read the manual carefully before use, in order to prevent danger and property loss. Strictly conform to the manual during application and keep it properly after reading.

Operating Requirement

- Please don't place and install the device in an area exposed to direct sunlight or near heat generating device.
- Please don't install the device in a humid, dusty or fuliginous area.
- Please keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Please don't drip or splash liquids onto the device; don't put on the device anything filled with liquids, in order to prevent liquids from flowing into the device.
- Please install the device at well-ventilated places; don't block its ventilation opening.
- Use the device only within rated input and output range.
- Please don't dismantle the device arbitrarily.
- Please transport, use and store the device within allowed humidity and temperature range.

Power Requirement

- Please make sure to use batteries according to requirements; otherwise, it may result in fire, explosion or burning risks of batteries!
- To replace batteries, only the same type of batteries can be used!
- The product shall use electric cables (power cables) recommended by this area, which shall be used within its rated specification!
- Please use standard power adapter matched with the device. Otherwise, the user shall undertake resulting personnel injury or device damage.
- Please use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, please refer to device labels.
- Products with category I structure shall be connected to grid power output socket, which is equipped with protective grounding.
- Appliance coupler is a disconnecting device. During normal use, please keep an angle that facilitates operation.

Table of Contents

1 Overview

Four-door two-way access controller is a controlling device which compensates video surveillance and visual intercom. It has neat and modern design with strong functionality, suitable for high-end commercial building, bank, government and enterprise.

1.1 Functional Feature

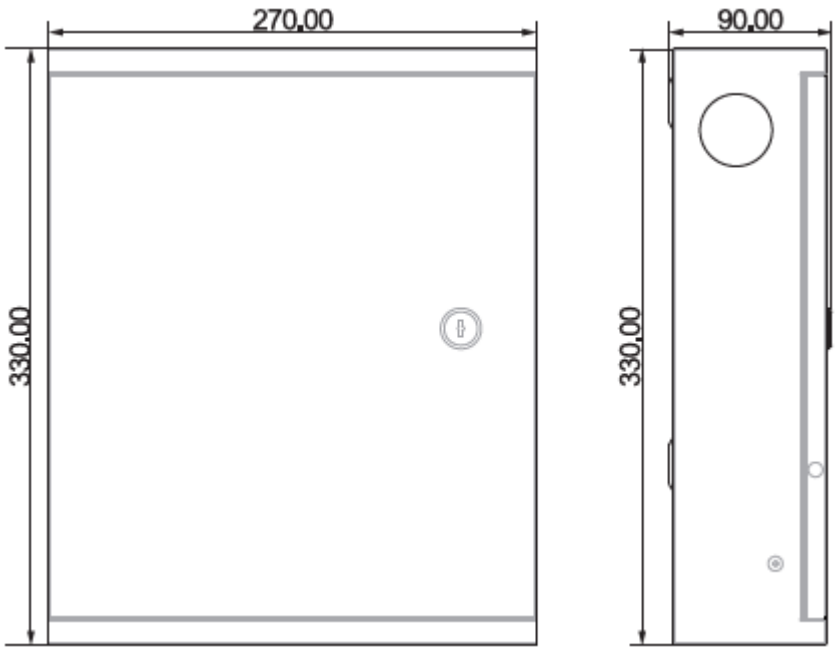
Its rich functions are as follows:

- Professional industrial design, lock and hinge rotational structure, able to bear 80kg force, with excellent vandal-resistant performance.
- Integrate alarm, access control, video surveillance and fire alarm.
- Support 8 sets of card readers (which can be set to 4 one-door two-way readers, with RS485 or Wiegand input).
- Support 21 groups of signal input (exit button*4, door contact*4, lock bolt*4, local tamper alarm*1 and alarm input*8).
- Support 12 groups of control output (electric lock *4 and external alarm output *8).
- Support audio module output (with external amplifier and speaker).
- Support extended GSM module.
- With 2 groups of RS485 port, it may extend to connect control module.
- FLASH storage capacity is 16M (which may extend to 32M). Support max. 100,000 card holders and 150,000 card reading records.
- Support tamper alarm, illegal intrusion alarm, unlock timeout alarm, duress card and duress code setup. Also support blocklist and allowlist and patrol card setup.
- Support valid time period setting, password setting and expiration date setting of cards. Regarding guest card, its time of use can be set.
- Support 128 groups of schedules and 128 groups of holiday schedules.
- Permanent data storage during outage, built-in RTC (support DST), online upgrade.

1.2 External Dimension

Its appearance and dimension is shown in Figure 1-1. The unit is mm.

Figure 1-1

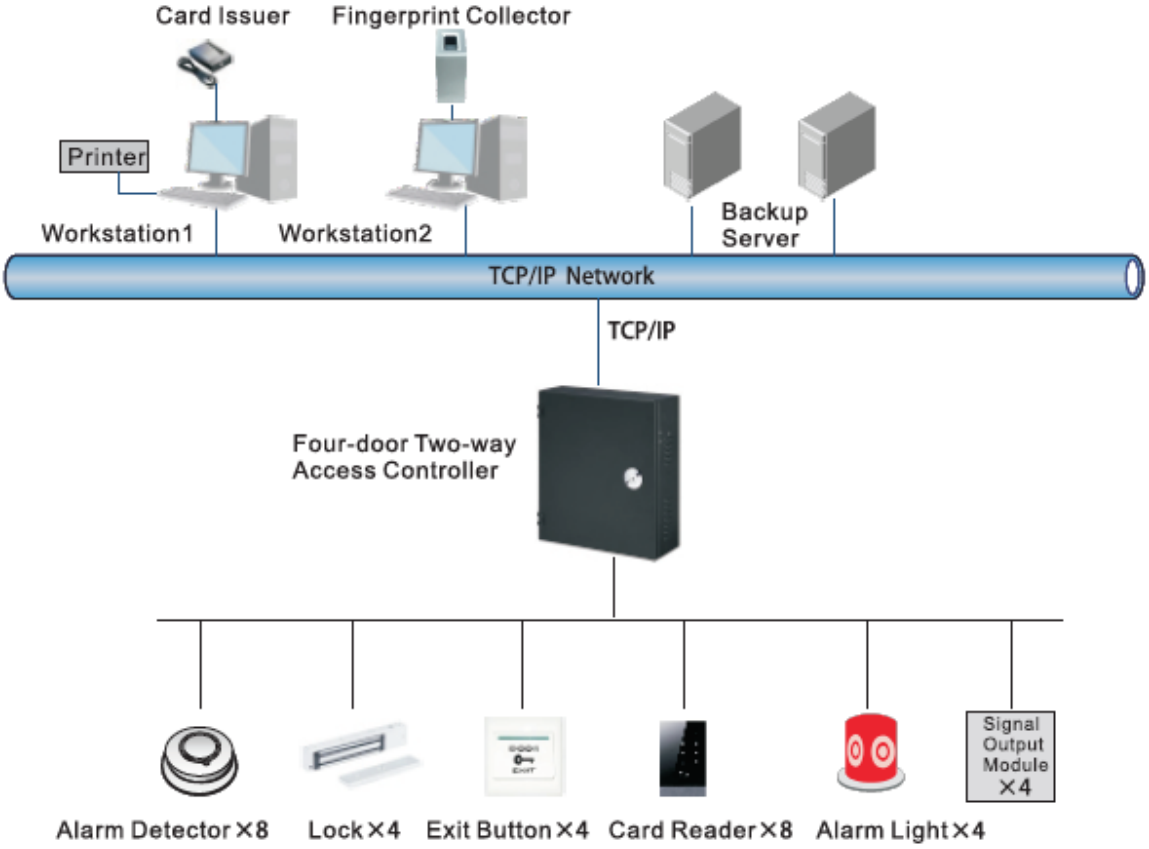


2 Installation Guide

2.1 System Structure

System structure of four-door two-way access controller, door lock and reader is shown in Figure 2-1.

Figure 2-1



2.2 Device Installation

Device installation diagram is shown in Figure 2-2 and Figure 2-3. The unit is mm.

Figure 2-2

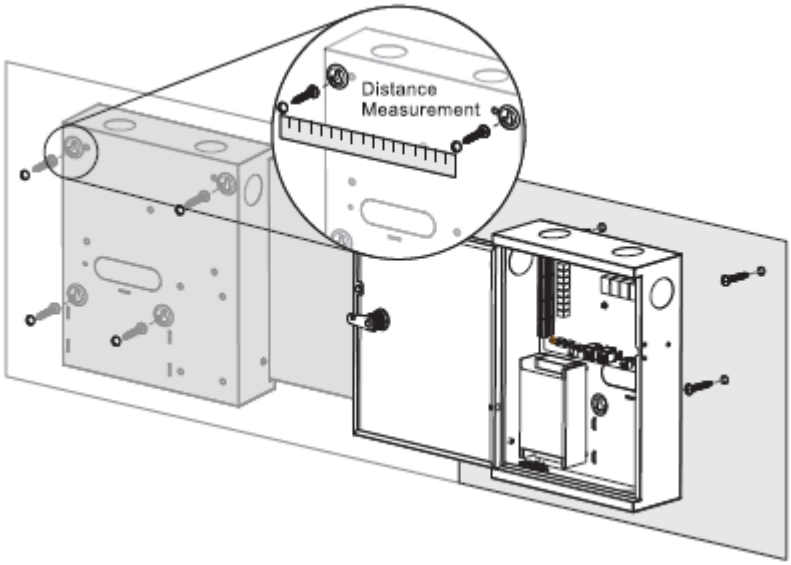
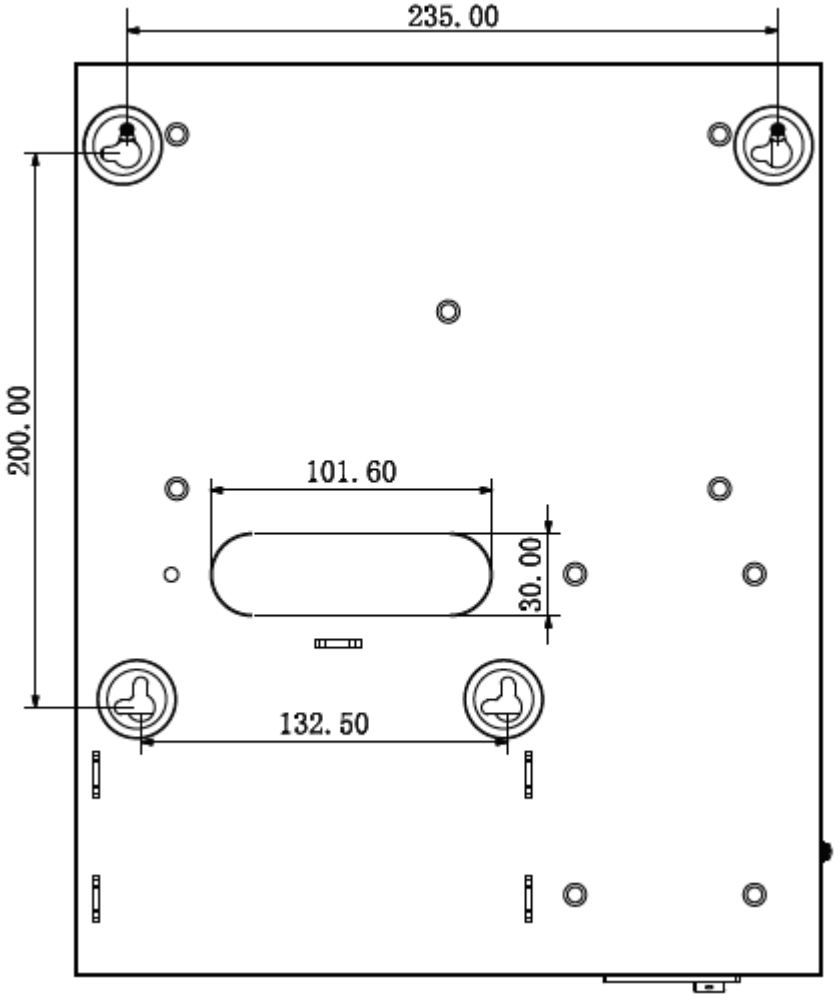


Figure 2-3



NOTE

Please ensure that device mounting surface is able to bear 3 times as many as the total weight of the device, bracket and accessories.

Step 1 Measure every hole distance and position according to holes at rear shell of the device, as shown in Figure 2-3; drill holes in the wall according to the measured positions.

Step 2 Embed expansion nuts and fix screws into the wall.

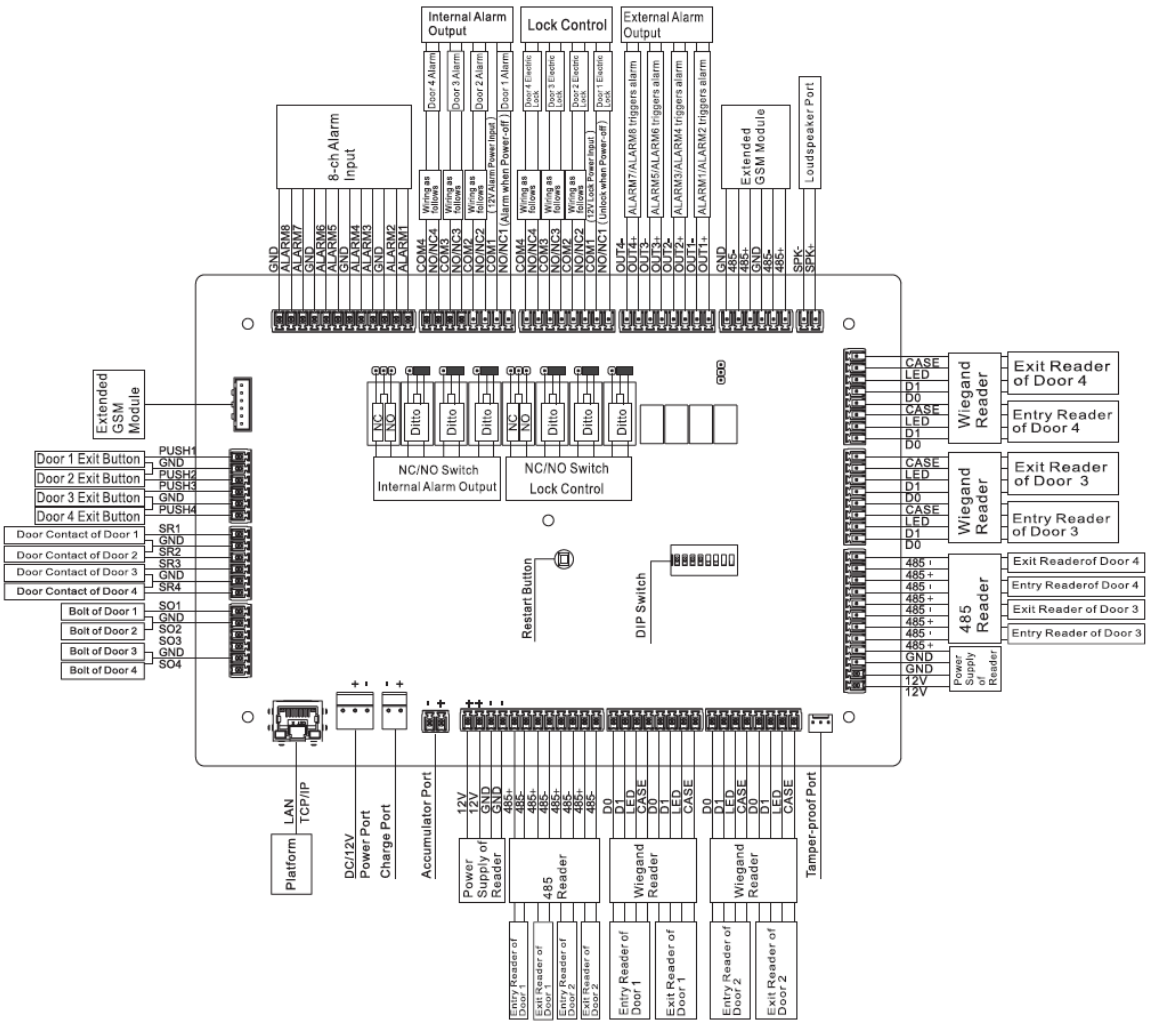
Step 3 Hang the whole device onto the screws.

2.3 Wiring Diagram

2.3.1 Wiring Description of Access Controller

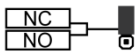
This device supports four-door two-way in or out. In case of alarm input, trigger external alarm output device to give an alarm. Device wiring diagram is shown in Figure 2-4.

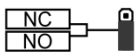
Figure 2-4



2.3.2 NC/NO Switching Description

During connection of internal alarm output and lock control, it is necessary to switch NC/NO with jumper cap.

- 

means to switch to NC (normally closed).
- 

means to switch to NO (normally open).

2.3.3 Wiring Description of Exit Button

Corresponding wiring terminals of exit button are shown in Figure 2-5. Please refer to Table 2-1 for descriptions of wiring terminals.

Figure 2-5

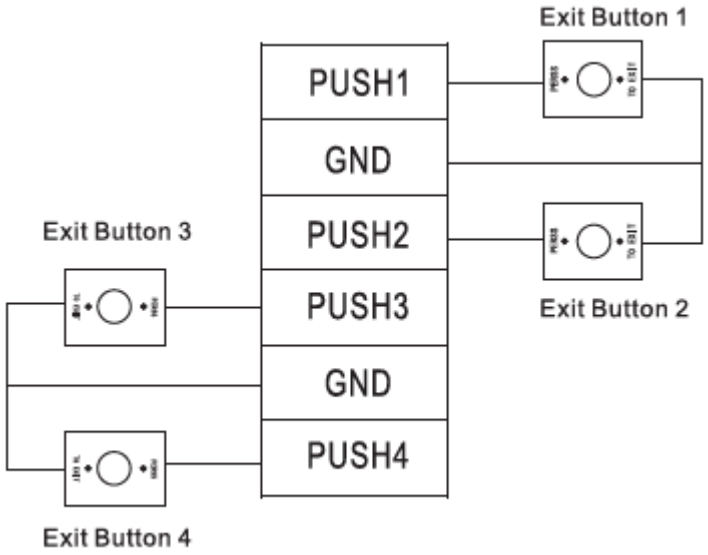


Table 2-1

Port	Wiring Terminal	Description
Exit button Control Port	PUSH1	Exit button of door 1
	GND	Shared by door 1 and door 2
	PUSH2	Exit button of door 2
	PUSH3	Exit button of door 3
	GND	Shared by door 3 and door 4
	PUSH4	Exit button of door 4

2.3.4 Wiring Description of Door Contact

Corresponding wiring terminals of door contact are shown in Figure 2-6. Please refer to Table 2-2 for descriptions of wiring terminals.

Figure 2-6

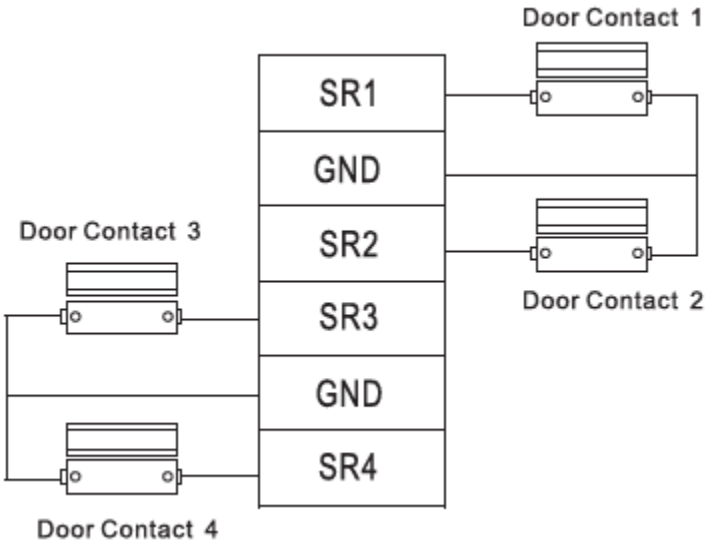


Table 2-2

Port	Wiring Terminal	Description
Door contact feedback port	SR1	Door contact feedback of door 1
	GND	Shared by door 1 and door 2
	SR2	Door contact feedback of door 2
	SR3	Door contact feedback of door 3
	GND	Shared by door 3 and door 4
	SR4	Door contact feedback of door 4

2.3.5 Wiring Description of Lock

Support 4 groups of lock control outputs; serial numbers after the terminals represent corresponding doors. Please choose NC/NO and a proper connection mode according to lock type, as shown in Figure 2-7, Figure 2-8 and Figure 2-9. Please refer to Table 2-3 for descriptions of wiring terminals.

Figure 2-7

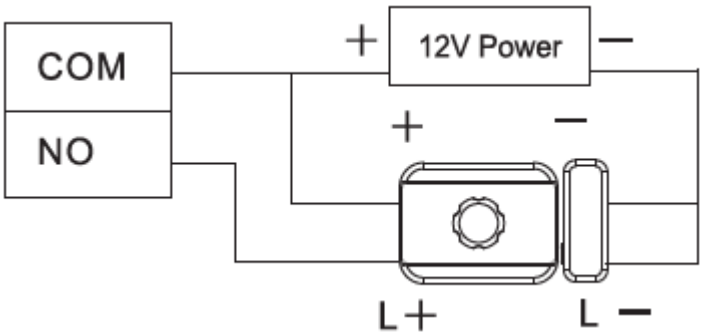


Figure 2-8

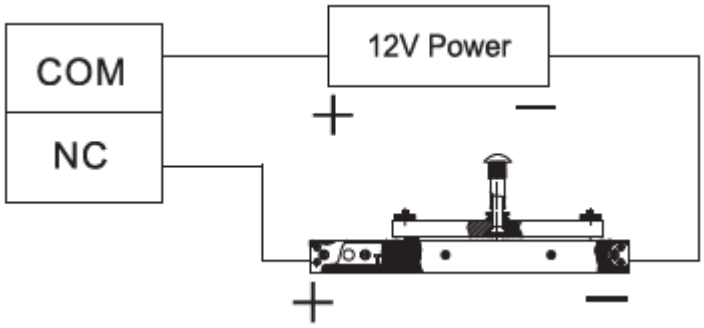


Figure 2-9

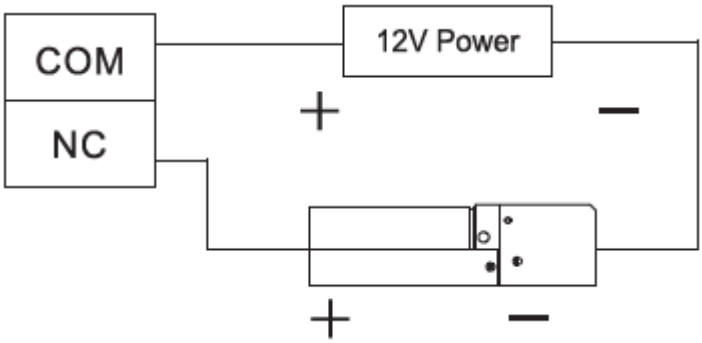


Table 2-3

Port	Wiring Terminal	Description
Lock control output port	COM1	Lock control of door 1
	NO1/NC1	
	COM2	Lock control of door 2
	NO2/NC2	
	COM3	Lock control of door 3
	NO3/NC3	
	COM4	Lock control of door 4
	NO4/NC4	

2.3.6 Wiring Description of Reader

NOTE

1 door only supports to connect one type of reader—485 or Wiegand.

Please refer to Table 2-4 for descriptions of wiring terminals corresponding to readers. Take door 1 for example; other readers are the same. Please refer to Table 2-5 for descriptions of reader cable specification and length.

Table 2-4

Port	Wiring Terminal	Cable Color	Description
Entry Reader of Door 1	485+	Purple	485 reader
	485-	Yellow	
	LED	Brown	Wiegand reader
	D0	Green	
	D1	White	
	CASE	Blue	

Port	Wiring Terminal	Cable Color	Description
	GND	Black	Reader power supply
	12V	Red	

Table 2-5

Reader Type	Connection Mode	Length
485 Reader	CAT5e network cable, 485 connection	100m
Wiegand Reader	CAT5e network cable, Wiegand connection	100m

2.3.7 Wiring Description of External Alarm Input

8-ch external alarm input connection is shown in Figure 2-10. Please refer to Table 2-6 for descriptions of wiring terminals.

Figure 2-10

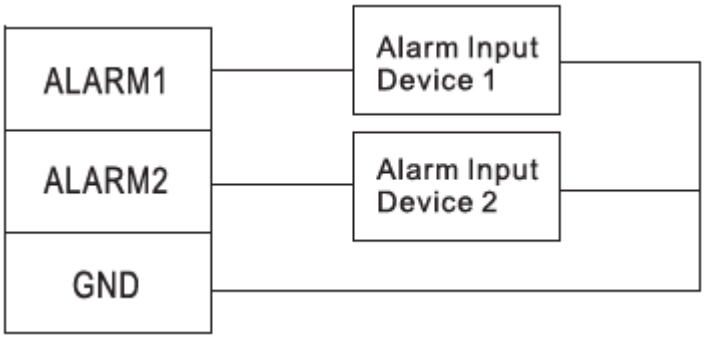


Table 2-6

Port	Wiring Terminal		Description
External alarm input	ALARM1	Alarm input port 1	External alarm input ports are able to connect smoke detector and IR detector etc.. NOTE External alarm can link door open and closed status. ● ALARM1～ALARM2 external alarms link all doors to be normally open. ● ALARM3 ~ ALARM4 external alarms link all doors to be normally closed.
	ALARM2	Alarm input port 2	
	GND	Shared by alarm input port 1 and 2	
	ALARM3	Alarm input port 3	
	ALARM4	Alarm input port 4	
	GND	Shared by alarm input port 3 and 4	
	ALARM5	Alarm input port 5	
	ALARM6	Alarm input port 6	
	GND	Shared by alarm input port 5 and 6	
	ALARM7	Alarm input port 7	
	ALARM8	Alarm input port 8	
	GND	Shared by alarm input port 7 and 8	

2.3.8 Wiring Description of Internal Alarm Output

With 4-ch internal alarm output, after internal alarm input (such as door timeout) triggers an alarm, the alarm output device gives an alarm for 15s.

During connection of alarm output device, please select NC/NO according to normally closed or normally open status.

There are two connection modes of internal alarm output, depending on alarm device. For example, IPC can use Mode 1, whereas audible and visual siren can use Mode 2, as shown in Figure 2-11 and Figure 2-12. Please refer to Table 2-7 for descriptions about wiring terminals.

Figure 2-11

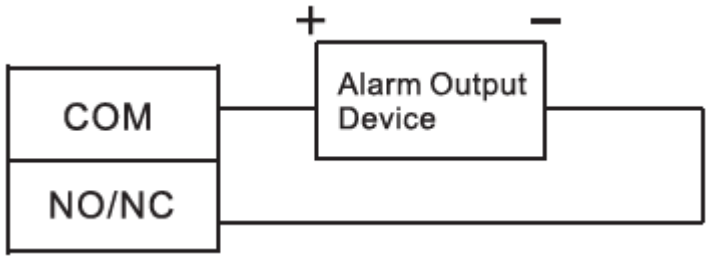


Figure 2-12

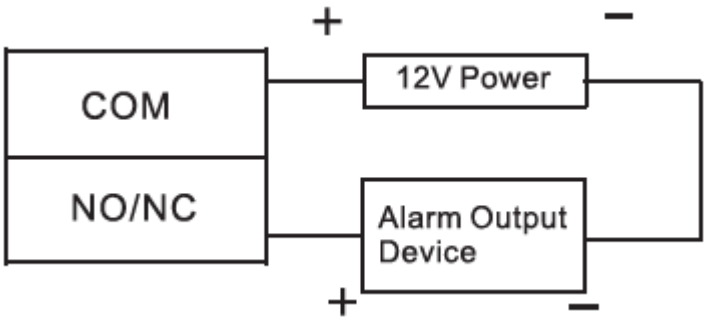


Table 2-7

Port	Wiring Terminal		Description
Internal alarm output	COM1	● Tamper alarm output of door 1 entry reader and exit reader ● Timeout and intrusion alarm output of door 1	Internal alarm output ports are able to connect audible and visual sirens.
	NO1/NC1		
	COM2	● Tamper alarm output of door 2 entry reader and exit reader ● Timeout and intrusion alarm output of door 2	
	NO2/NC2		
	COM3	● Tamper alarm output of door 3 entry reader and exit reader ● Timeout and intrusion alarm output of door 3	
	NO3/NC3		
	COM4	● Tamper alarm output of door 4 entry reader and exit reader ● Timeout and intrusion alarm output of door 4	
	NO4/NC4		

2.3.9 Wiring Description of External Alarm Output

With 4-ch external alarm output, after external alarm input triggers an alarm, the alarm output device gives an alarm for 15s.

There are two connection modes of external alarm output, depending on alarm device. For example, IPC can use Mode 1, whereas audible and visual siren can use Mode 2, as shown in Figure 2-13 and Figure 2-14. Please refer to Table 2-8 for descriptions about wiring terminals.

Figure 2-13

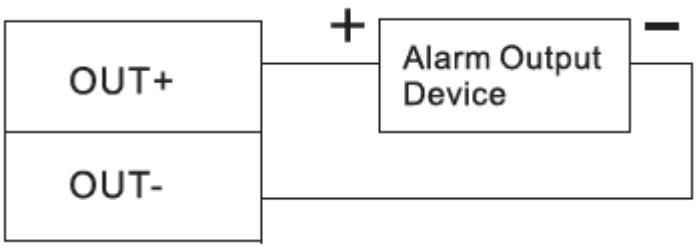


Figure 2-14

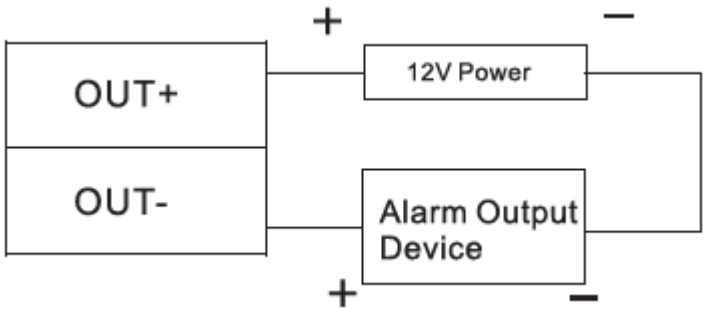


Table 2-8

Port	Wiring Terminal		Description
External alarm output	OUT1+	ALARM1/ALARM2 triggers alarm output.	External alarm output ports are able to connect audible and visual sirens.
	OUT1-		
	OUT2+	ALARM3/ALARM4 triggers alarm output.	
	OUT2-		
	OUT3+	ALARM5/ALARM6 triggers alarm output.	
	OUT3-		
	OUT4+	ALARM7/ALARM8 triggers alarm output.	
	OUT4-		

2.3.10 Description of Alarm Input and Output Rule

In case of alarm event, the alarm continues for 15s. Please refer to Table 2-9 for detailed alarm input and output rules.

Table 2-9

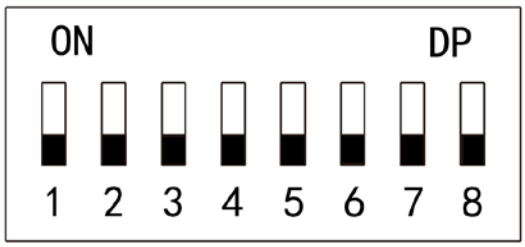
Alarm Type	Alarm Signal Input Port	Alarm Signal Output Port	Alarm Status
External alarm input	ALM1	OUT1	Link all doors to be normally open.
	ALM2		
	ALM3	OUT2	Link all doors to be normally open.
	ALM4		
	ALM5	OUT3	Link all doors to be normally closed.
	ALM6		
	ALM7	OUT4	Link all doors to be normally closed.
	ALM8		
Internal alarm input	SR1	Internal alarm output COM1	Door timeout and intrusion alarm trigger external alarm to give an alarm.
	SR2	Internal alarm output COM2	
	SR3	Internal alarm output COM3	

Alarm Type	Alarm Signal Input Port	Alarm Signal Output Port	Alarm Status
	SR4	Internal alarm output COM4	
	RS-485/CASE	Internal alarm output COM1	Tamper alarm of reader triggers external alarm to give an alarm.
	RS-485/CASE	Internal alarm output COM2	
	RS-485/CASE	Internal alarm output COM3	
	RS-485/CASE	Internal alarm output COM4	

2.4 DIP Switch

Operate with DIP switch.

Figure 2-15



-  the switch is at ON position, meaning 1.
-  the switch is at the bottom, meaning 0.
- 1～8 are all 0; the system is started normally.
- 1～8 are all 1; the system enters BOOT mode after start.
- 1, 3, 5 and 7 are 1, while others are 0. After reboot, the system restores factory defaults.
- 2, 4, 6 and 8 are 1, while others are 0. After reboot, the system restores factory defaults, but user info is retained.

2.5 Reboot

Press reboot button (as shown in Figure 2-4) to reboot the device.

NOTE

Reboot button is to reboot the device, rather than modifying configuration.

3 Smart PSS Config

Access controller is managed with Smart PSS client, so as to realize control and right configuration of one door and door groups.

This chapter mainly introduces quick configuration. For specific operations, please refer to User's Manual of Smart PSS Client.

NOTE

Smart PSS client offers different interfaces for different versions. Please refer to actual interface.

3.1 Login Client

Install the matching Smart PSS client, and double click 

to run. Carry out initialization configuration according to interface prompts and complete login.

3.2 Add Access Controller

Add access controller in Smart PSS; select "Auto Search" and "Add".

3.2.1 Auto Search

Devices are required to be in the same network segment.

Step 1 In "Devices" interface, click "Auto Search", as shown in Figure 3-1.

The system displays "Auto Search" interface, as shown in Figure 3-2.

Figure 3-1

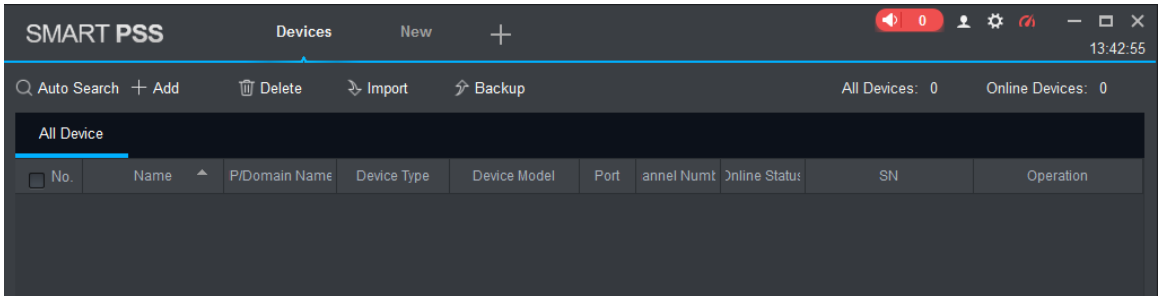
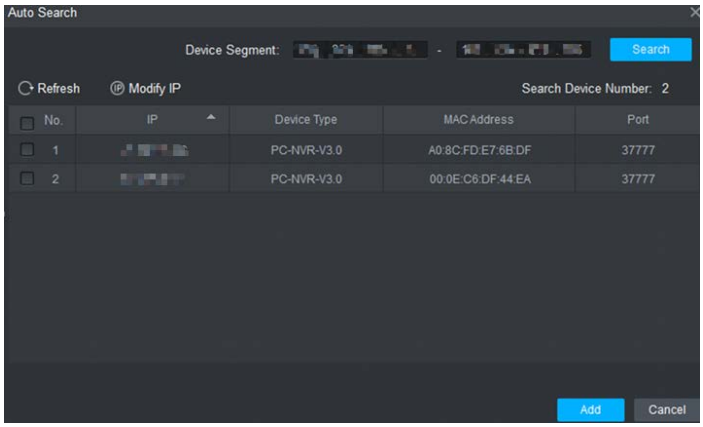


Figure 3-2



Step 2 Input device segment and click "Search".

The system displays search results.

NOTE

- Click "Refresh" to update device information.
- Select a device, click "Modify IP" to modify IP address of the device. For specific operations, please refer to User's Manual of Smart PSS Client.

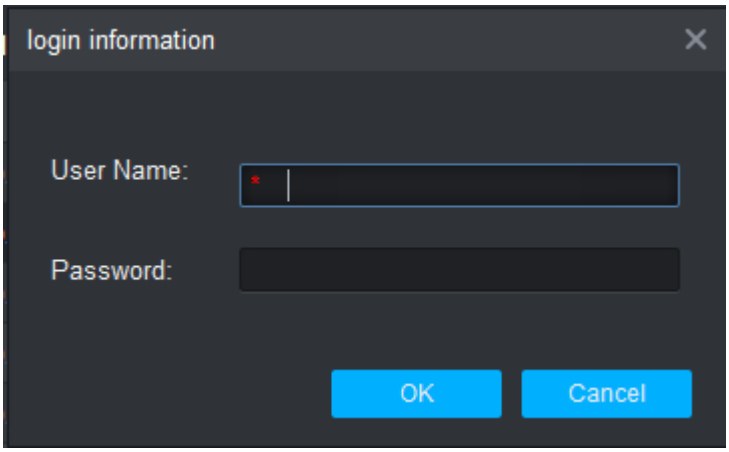
Step 3 Select the device that needs to be added, and click "Add".

The system pops up "Prompt".

Step 4 Click "OK".

The system displays "Login Information" dialogue box, as shown in Figure 3-3.

Figure 3-3



Step 5 Input "User Name" and "Password" to log in the device, and click "OK".

The system displays the added device list, as shown in Figure 3-4. Please refer to Table 3-1 for details.

NOTE

- After completing adding, the system continues to stay at "Auto Search" interface. You can continue to add more devices, or click "Cancel" to exit "Auto Search" interface.
- After completing adding, Smart PSS logs in the device automatically. In case of successful login, online status displays "Online". Otherwise, it displays "Offline".

Figure 3-4

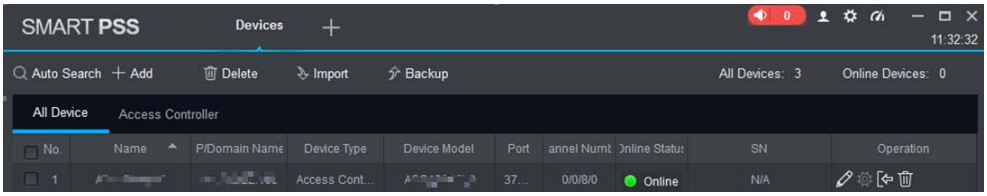


Table 3-1

Icon	Description
	Click this icon to enter "Modify Device" interface and modify device info, including device name, IP/domain name, port, user name and password. Alternatively, double click the device to enter "Modify Device" interface.
	Click this icon to enter "Device Config" interface and configure device camera, network, event, storage and system info.
and	• When the device is online, the icon is . Click this icon to exit login, and this icon turns to . • When the device is offline, the icon is . Click this icon to login (with correct device info), and this icon turns to .
	Click this icon to delete the device.

3.2.2 Manual Add

To add devices, device IP address or domain name shall be known first.

Step 1 In "Devices" interface, click "Add", as shown in Figure 3-5.

The system pops up "Manual Add" interface, as shown in Figure 3-6.

Figure 3-5

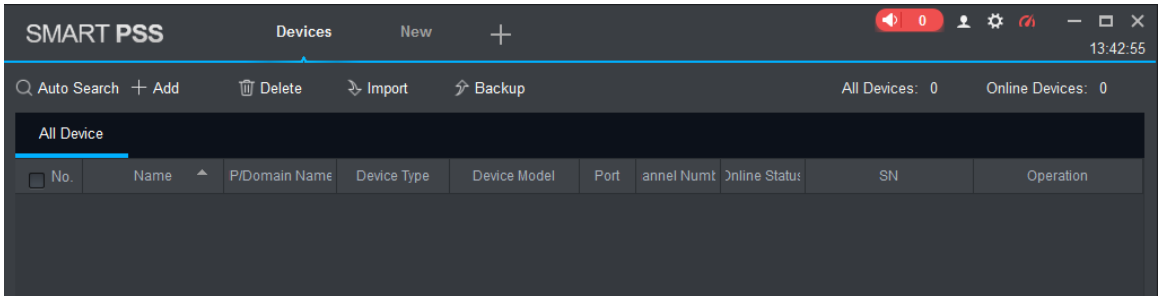
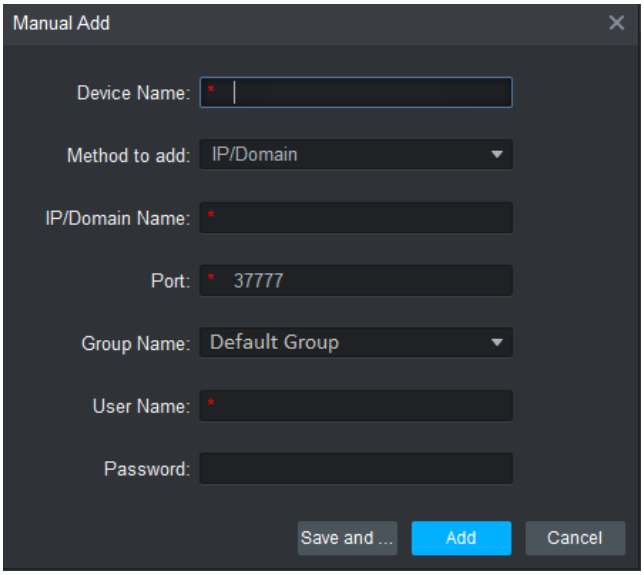


Figure 3-6



Step 2 Set device parameters. For specific parameter descriptions, please refer to Table 3-2.

Table 3-2

Parameter	Description
Device Name	It is suggested that device should be named by the monitoring zone, so as to facilitate maintenance.
Method to add	Select "IP/Domain Name". Add devices according to device IP address or domain name.
IP/Domain Name	IP address or domain name of the device.
Port	Port number of the device. Default port number is 37777. Please fill in according to actual conditions.
Group Name	Select the group of the device.
User Name and Password	User name and password of the device.

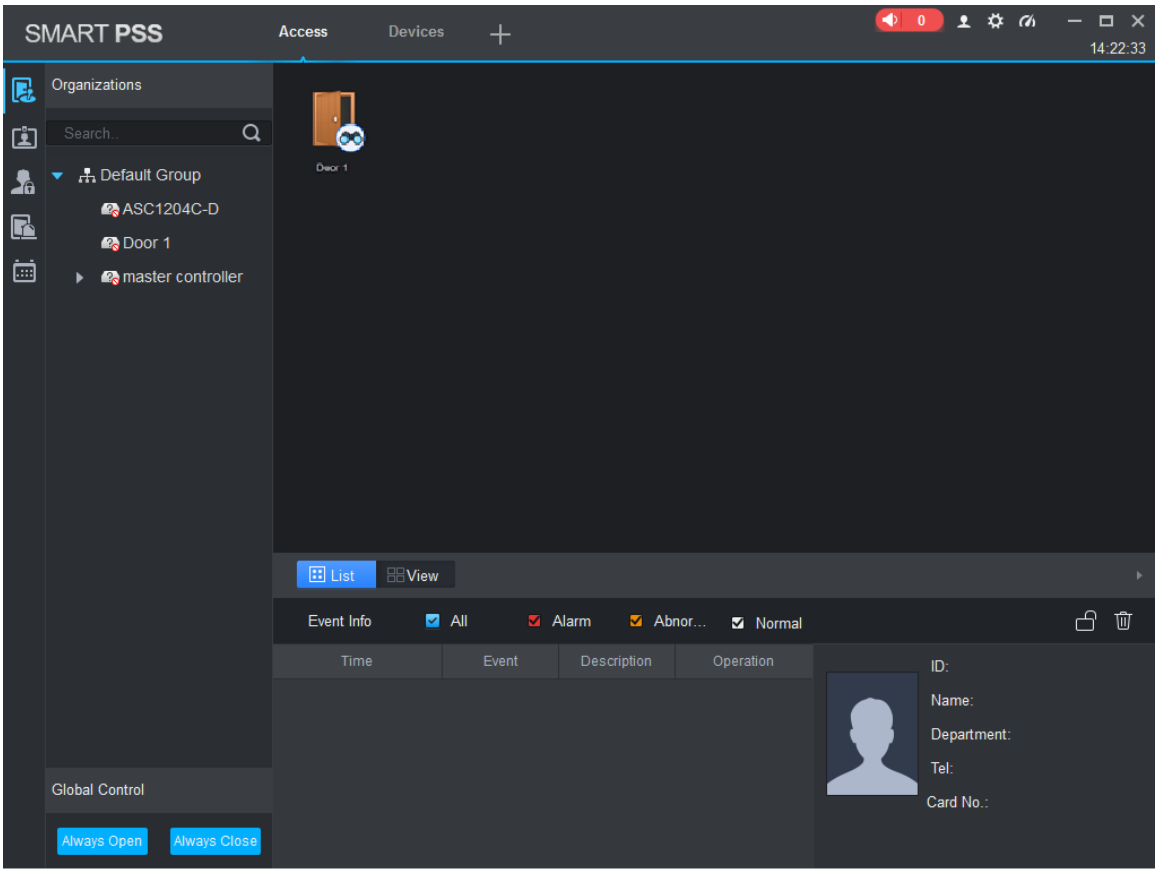
Step 3 Click "Add" to add a device.

The system displays the added device list, as shown in Figure 3-4. Please refer to Table 3-1 for operation interface. Doors of the added controller are displayed under "Access" tab, as shown in Figure 3-7.

NOTE

- To add more devices, click "Save and Continue", add devices and stay at "Manual Add" interface.
- To cancel the adding, click "Cancel" and exit "Manual Add" interface.
- After completing adding, Smart PSS logs in the device automatically. In case of successful login, online status displays "Online". Otherwise, it displays "Offline".

Figure 3-7

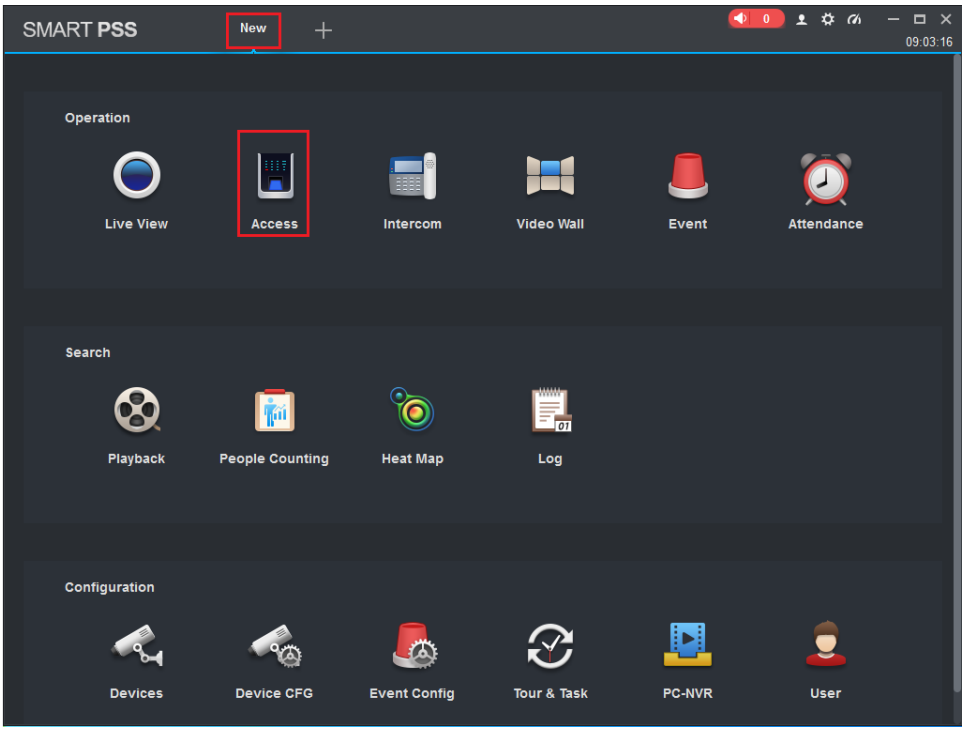


3.3 Add User

Add users and bind with cards, so as to distribute authority.

In "New" interface, click "Access" to enter "Access" interface, and complete access config here.

Figure 3-8



3.3.1 Card Type

CAUTION

Card type shall be the same with card issuer; otherwise, it fails to read card number.

In "Access" interface, click  and then click  to set the card type, as shown in Figure 3-9 and Figure 3-10.

Figure 3-9

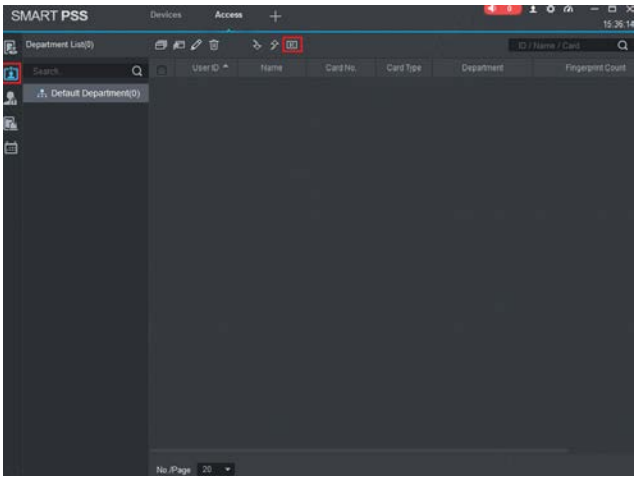
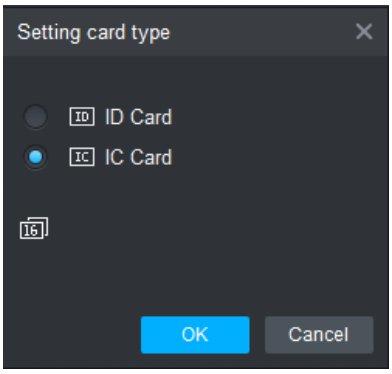


Figure 3-10



3.3.2 Single Add

Add a single user, send a card and input user info.

Step 1 In "Access" interface, click  , and then click  , as shown in Figure 3-11.

The system pops up "Add User" dialog box, as shown in Figure 3-12.

Figure 3-11

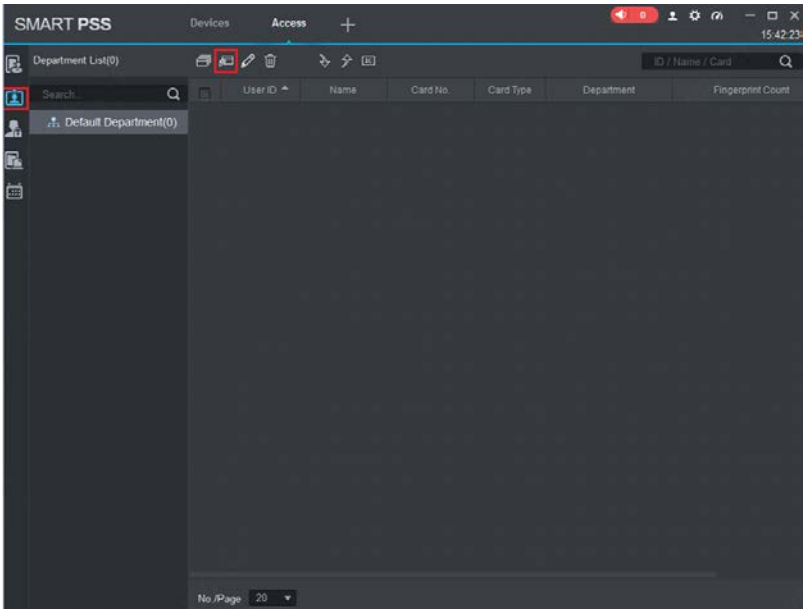
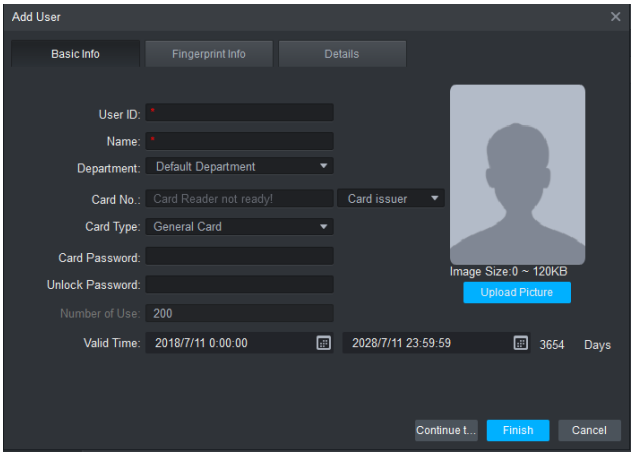


Figure 3-12



Step 2 Add user info manually, including basic info, fingerprint info and details. Please refer to Table 3-3 for details.

Table 3-3

Parameter	Description
Basic Info	• User ID (mandatory). • Name (mandatory). • Department (auto association). • Card No.: input by card reader or input manually. • Card type: general card, VIP card, guest card, patrol card, blocklist card and duress card. • Card Password: it is used to open the door with card + password. • Unlock Password: it is used to open the door with password. • Number of Use: it only applies to guest card. • Valid Time: set the valid time of card, which is 10 years by default. • Picture: user picture, max. 120K. NOTE Card no. and user ID cannot be repeated.

Parameter	Description
Fingerprint Info	Collect fingerprints with fingerprint reader and access reader. ● Max. 2 fingerprints for every person. ● Support to enter fingerprint name.
Details	Fill in detailed user info according to interface parameters.

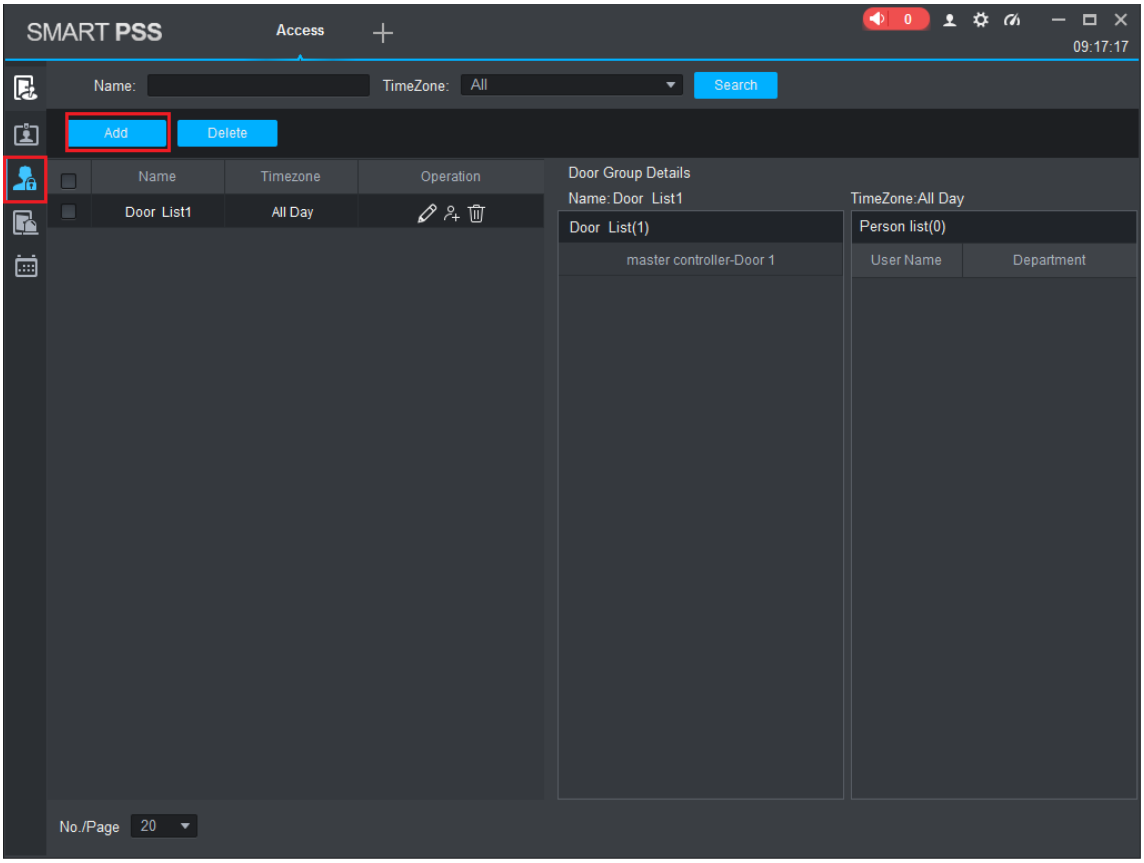
Step 3 Click "Finish" to finish adding the users.

3.4 Add Door Group

Divide doors into groups and manage them together.

Step 1 In "Access" interface, click  , and then click "Access Level", as shown in Figure 3-13.

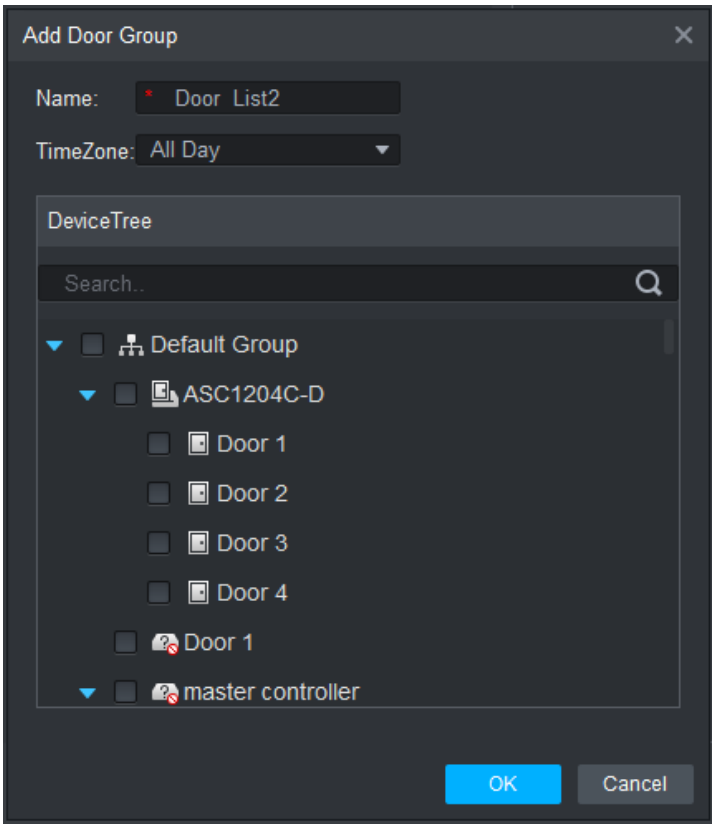
Figure 3-13



Step 2 Click "Add".

The system pops up "Add Door Group" dialog box, as shown in Figure 3-14.

Figure 3-14



Step 3 Enter "Name"; select "Time Zone" and doors to be managed.

Step 4 Click "OK" to complete adding.

3.5 Authorize

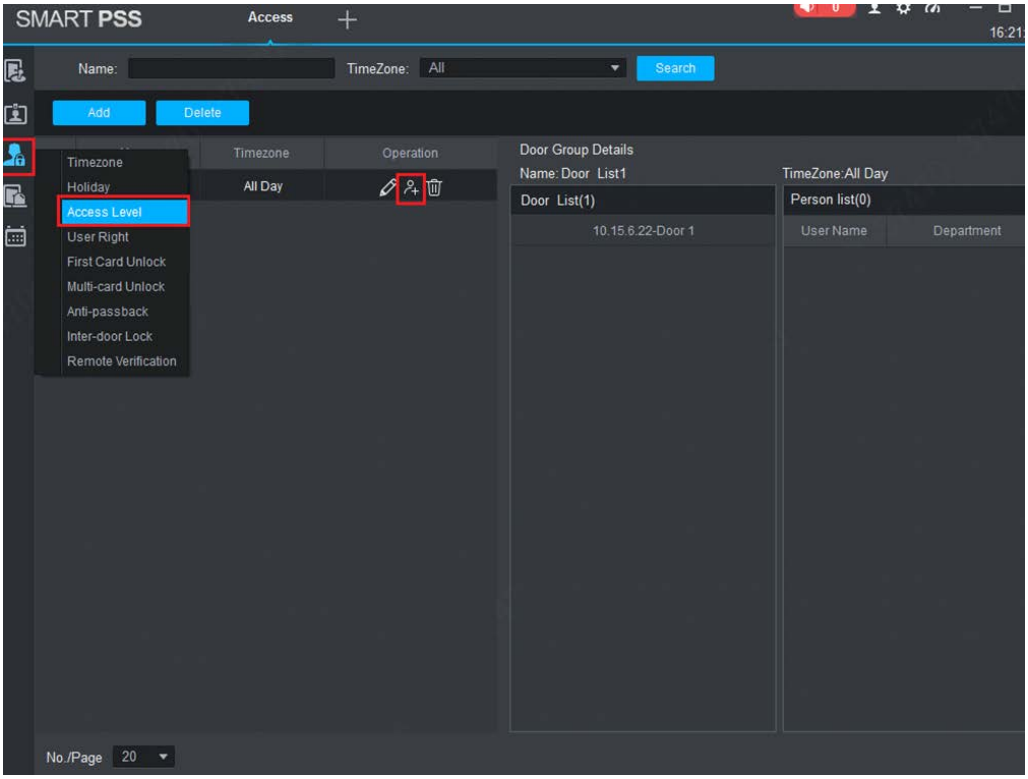
Grant users authorities according to door group and user.

3.5.1 Authorize According to Door Group

Select a door group, add corresponding users to the group, so all users in the group obtain authority of all doors in the group.

Step 1 In "Access" interface, click  , and then click "Access Level", as shown in Figure 3-15.

Figure 3-15



Step 2 Click .

The system pops up "User Select" dialog box.

Step 3 Select the user's department from dropdown list, or enter the user's ID or name directly.

Step 4 In the search list, select the user and add to user list.

Step 5 Click "OK" to finish authorization.

NOTE

- The search list filters user info without card number.
- In the user list, cancel the added user and delete the user's authority.

3.5.2 Authorize According to User

Select a user, distribute door group and grant door group authority to the user.

Step 1 In "Access" interface, click , and then click "User Right".

Step 2 Click .

Step 3 Select the door group and click "OK" to finish authorization.

4 FAQ

For problems not included hereinafter, please contact local customer service personnel or consult headquarter customer service personnel. We will be always at your service.

1. **Question: After power on, power indicator doesn't turn on or the buzzer doesn't respond.**

Answer: Please check whether power plug is inserted in place. Please pull it out and insert it again.

2. **Question: After the reader is connected with the device, card swiping light doesn't turn on, and it doesn't respond after swiping a card.**

Answer: Please check whether reader connector is inserted in place. Please pull it out and insert it again; check whether reader contact light turns on.

3. **Question: Client software fails to detect the device.**

Answer: Please check whether TCP/IP connector is connected properly, and whether device IP is in the same network segment.

4. **Question: After swiping card, it prompts that card is invalid.**

Answer: Please check whether this card number has been added in the controller.

5. **Question: Default IP of access controller.**

Answer: Default IP address is 192.168.0.2.

6. **Question: Default port, initial user name and password of access controller.**

Answer: Default port is 37777, initial user name is admin and password is 123456.

7. **Question: Online upgrade of the device.**

Answer: Connect the device and platform through network, and upgrade it at the platform.

8. **Question: Max. wiring distance and transmission distance of card reader and controller.**

Answer: It depends on network cable type and whether it needs power supply of control relay.

Connected with CAT5E network cable, typical value is:

- RS485, 100m.
- Wiegand, 100m.

Appendix 1 Cybersecurity Recommendations

The necessary measures to ensure the basic cyber security of the platform:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

2. **Customize the Answer to the Security Question**

   The security question setting should ensure the difference of answers, choose different questions and customize different answers (all questions are prohibited from being set to the same answer) to reduce the risk of security question being guessed or cracked.

Recommendation measures to enhance platform cyber security:

1. **Enable Account Binding IP/MAC**

   It is recommended to enable the account binding IP/MAC mechanism, and configure the IP/MAC of the terminal where the commonly used client is located as an allowlist to further improve access security.

2. **Change Password Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Turn On Account Lock Mechanism**

   The account lock function is enabled by default at the factory, and it is recommended to keep it on to protect the security of your account. After the attacker has failed multiple password attempts, the corresponding account and source IP will be locked.

4. **Reasonable Allocation of Accounts and Permissions**

   According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.

5. **Close Non-essential Services and Restrict the Open Form of Essential Services**

   If not needed, it is recommended to turn off NetBIOS (port 137, 138, 139), SMB (port 445), remote desktop (port 3389) and other services under Windows, and Telnet (port 23) and SSH (port 22) under Linux. At the same time, close the database port to the outside or only open to a specific IP address, such as MySQL (port 3306), to reduce the risks faced by the platform.

6. **Patch the Operating System/Third Party Components**

   It is recommended to regularly detect security vulnerabilities in the operating system and third-party components, and apply official patches in time.

7. **Security Audit**

   - Check online users: It is recommended to check online users irregularly to identify whether there are illegal users logging in.
   - View the platform log: By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

8. The Establishment of a Secure Network Environment

In order to better protect the security of the platform and reduce cyber security risks, it is recommended that:

- Follow the principle of minimization, restrict the ports that the platform maps externally by firewalls or routers, and only map ports that are necessary for services.
- Based on actual network requirements, separate networks: if there is no communication requirement between the two subnets, it is recommended to use VLAN, gatekeeper, etc. to divide the network to achieve the effect of network isolation.