

# Two-door Two-way Access Controller

## User's Manual

**V1.0.1**






# Foreword

## General

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

## Safety Instructions

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

Signal Words	Meaning
 <b>DANGER</b>	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 <b>WARNING</b>	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 <b>CAUTION</b>	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 <b>TIPS</b>	Provides methods to help you solve a problem or save you time.
 <b>NOTE</b>	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 User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between paper User's 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 Guide (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

<b>Foreword</b> .....	<b>I</b>
<b>Important Safeguards and Warnings</b> .....	<b>III</b>
<b>1 Overview</b> .....	<b>1</b>
1.1 Functional Feature .....	1
1.2 External Dimension .....	1
<b>2 Installation Guide</b> .....	<b>3</b>
2.1 System Structure.....	3
2.2 Device Installation.....	3
2.3 Disassembly.....	4
2.4 Wiring Diagram .....	5
2.4.1 Wiring Description of Access Controller .....	5
2.4.2 Wiring Description of Exit Button/Door Contact .....	6
2.4.3 Wiring Description of Lock.....	7
2.4.4 Wiring Description of Reader.....	8
2.4.5 Wiring Description of External Alarm Input.....	8
2.4.6 Wiring Description of External Alarm Output.....	9
2.4.7 Wiring Description of Internal Alarm Output .....	10
2.4.8 Description of Alarm Input and Output Rule.....	11
2.5 DIP Switch.....	11
2.6 Restart.....	12
<b>3 Smart PSS Config</b> .....	<b>13</b>
3.1 Login Client .....	13
3.2 Add Access Controller.....	13
3.2.1 Auto Search .....	13
3.2.2 Manual Add.....	15
3.3 Add User .....	17
3.3.1 Card Type .....	18
3.3.2 Single Add.....	19
3.4 Add Door Group .....	21
3.5 Authorize .....	23
3.5.1 Authorize According to Door Group.....	23
3.5.2 Authorize According to User .....	25
<b>4 FAQ</b> .....	<b>27</b>
1. Question: After power on, power indicator doesn't turn on or the buzzer doesn't respond. ....	27
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. ....	27
3. Question: Client software fails to detect the device. ....	27
4. Question: After swiping card, it prompts that card is invalid.....	27
5. Question: Default IP of access controller. ....	27
6. Question: Default port, initial user name and password of access controller. ....	27
7. Question: Online upgrade of the device. ....	27

8. Question: Max. wiring distance and transmission distance of card reader and controller..... 27

**Appendix 1 Cybersecurity Recommendations .....XXVIII**

# 1 Overview

Two-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 commercial building, corporation property and intelligent community.

## 1.1 Functional Feature

Its rich functions are as follows:

- Adopt slide rail and lock-controlled design, convenient installation and maintenance.
- Integrate alarm, access control, video surveillance and fire alarm.
- Support 4 sets of card readers (which can be set as 2 one-door two-way readers).
- Support 8 groups of signal input (exit button\*2, door contact\*2 and intrusion alarm\*4).
- Support 6 groups of control output (electric lock \*2, external alarm output \*2 and internal alarm output \*2).
- With 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 illegal intrusion alarm, unlock timeout alarm, duress card and duress code setup. Also support black-white list 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 and Figure 1-2. The unit is mm.

Figure 1-1

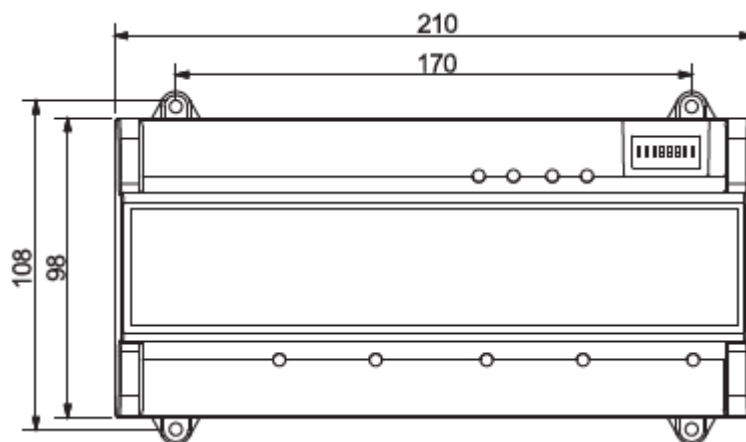
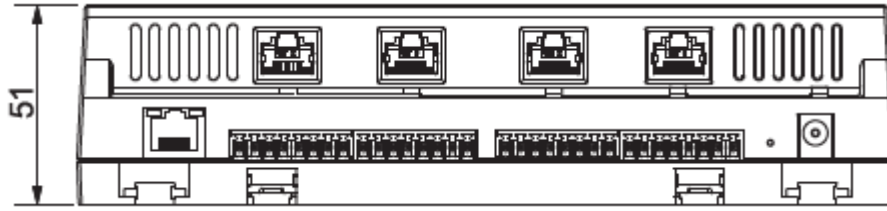


Figure 1-2



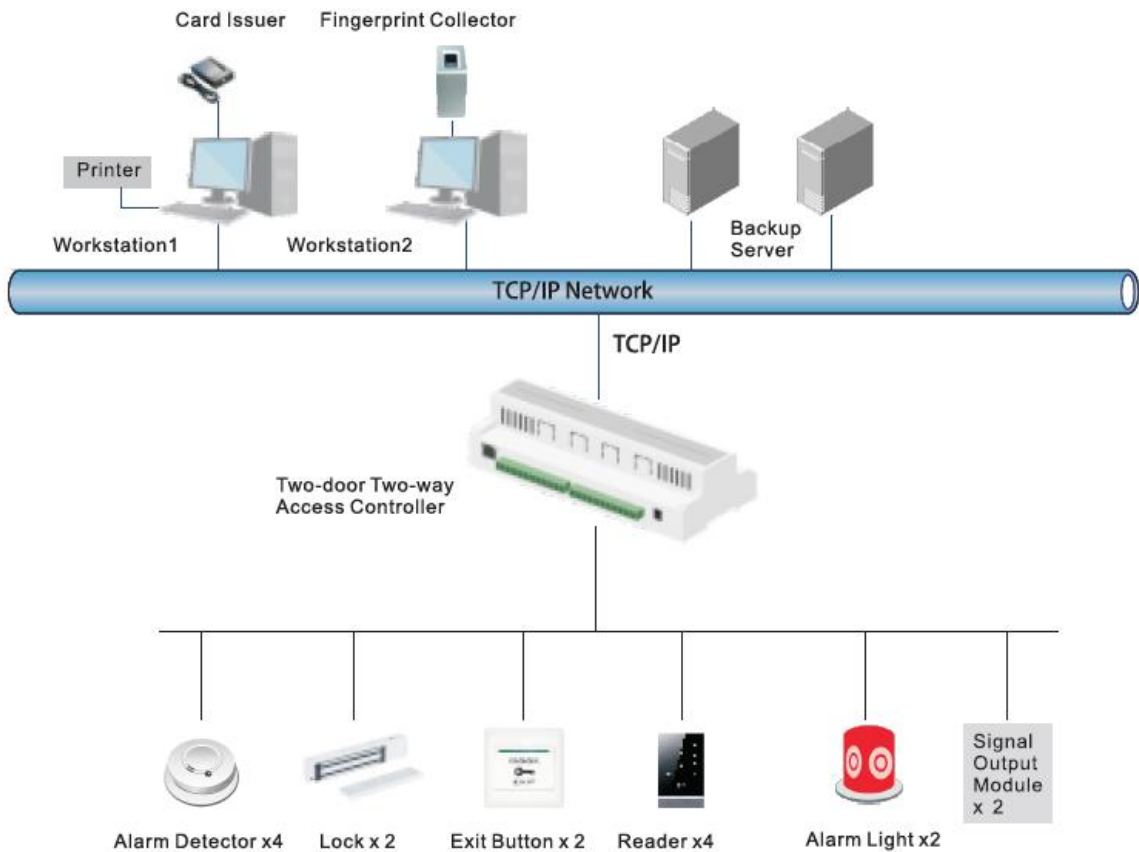


# 2 Installation Guide

## 2.1 System Structure

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

Figure 2-1



## 2.2 Device Installation

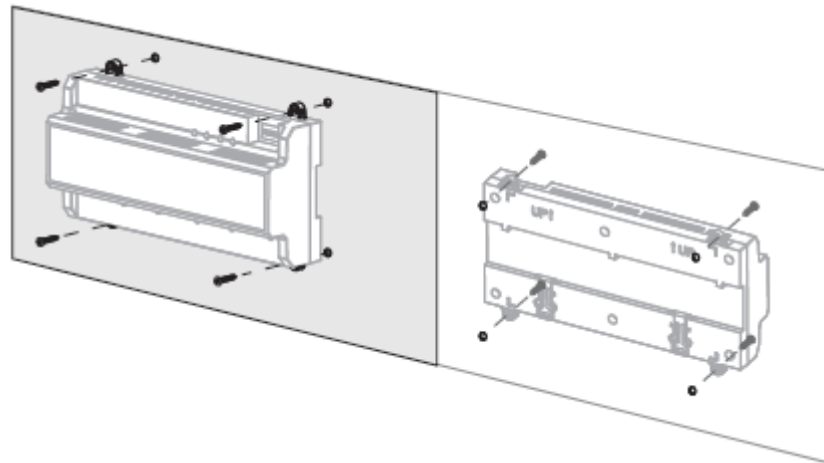
There are two installation modes.

- Mode 1: fix the whole device onto the wall with screws.
- Mode 2: with U-shaped guide rail, hang the whole device onto the wall (the U-shaped guide rail is an optional fitting).

### Mode 1

Installation diagram is shown in Figure 2-2.

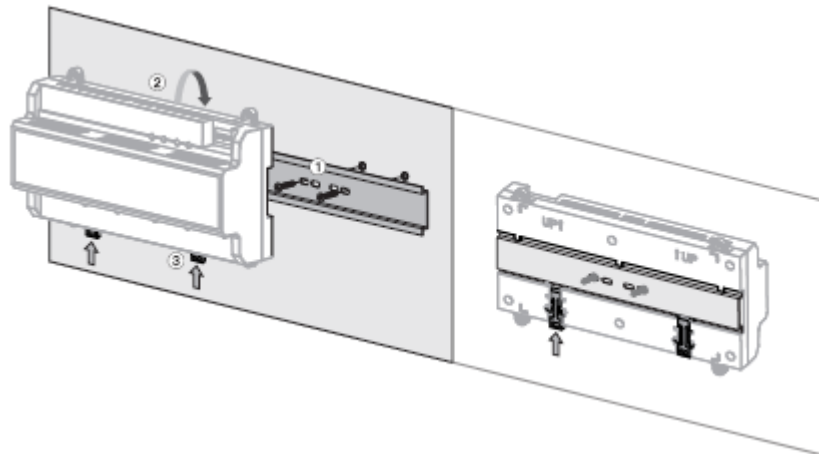
Figure 2-2



## Mode 2

Installation diagram is shown in Figure 2-3.

Figure 2-3



Step 1 Fix the U-shaped guide rail onto the wall with screws.

Step 2 Buckle the upper rear part of the device into upper groove of the U-shaped guide rail.

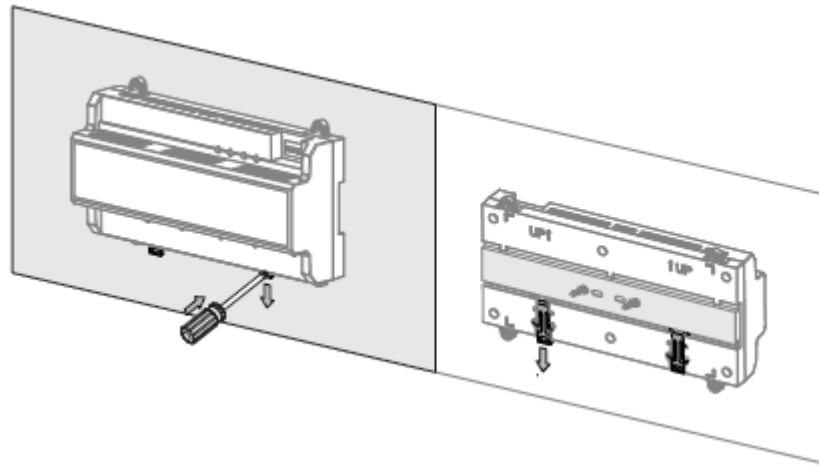
Step 3 Push the snap joint at the bottom of the device upwards. The installation is completed when you hear the fitting sound.

## 2.3 Disassembly

If the device is installed with mode 2, please disassemble it according to Figure 2-4.

Align a screwdriver with the snap joint, press it down and the snap joint will pop up, so the whole device can be disassembled smoothly.

Figure 2-4

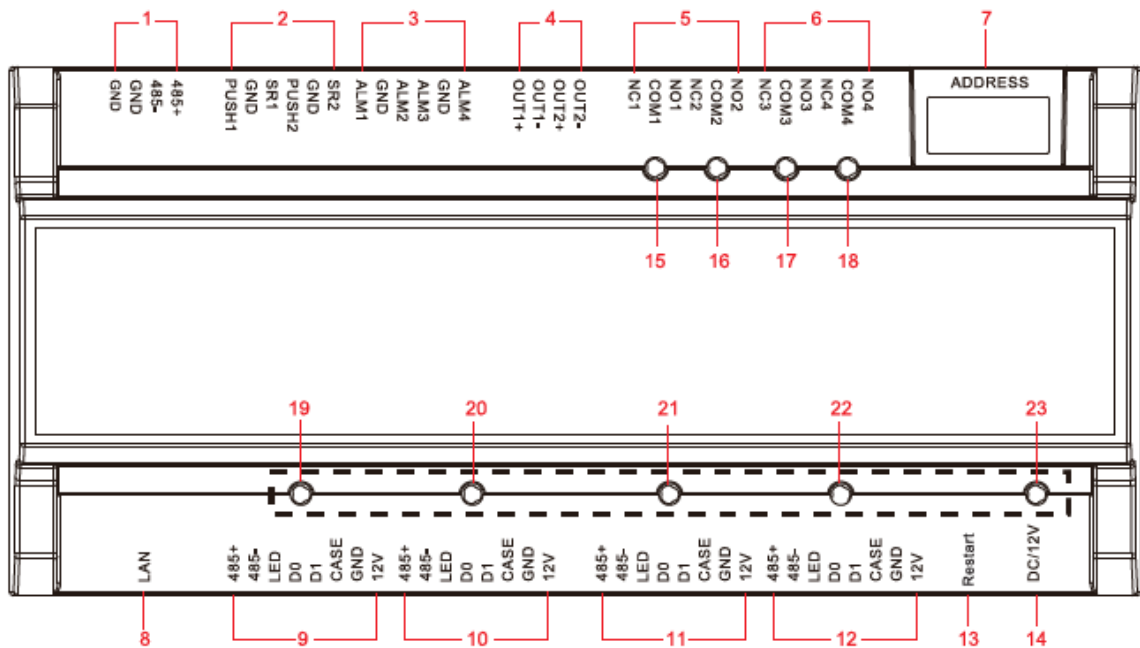


## 2.4 Wiring Diagram

### 2.4.1 Wiring Description of Access Controller

This device supports two-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 2-5.

Figure 2-5



Interfaces are described in Table 2-1.

Table 2-1

No.	Port Description	No.	Port Description
1	RS485 communication	8	TCP/IP, software platform port
2	Exit button and door contact	9	Entry reader of door 1
3	External alarm input	10	Exit reader of door 1
4	External alarm output	11	Entry reader of door 2
5	Lock power output	12	Exit reader of door 2
6	Internal alarm output	13	Restart

No.	Port Description	No.	Port Description
7	DIP switch	14	DC 12V power port

Indicator lights are described in Table 2-2.

Table 2-2

No.	Description
15	Lock status indicator
16	
17	Alarm status indicator
18	
19	Detection indicator of entry reader of door 1
20	Detection indicator of exit reader of door 1
21	Detection indicator of entry reader of door 2
22	Detection indicator of exit reader of door 2
23	Power indicator

## 2.4.2 Wiring Description of Exit Button/Door Contact

Corresponding wiring terminals of exit button and door contact are shown in Figure 2-6. Please refer to Table 2-3 for descriptions of wiring terminals.

Figure 2-6

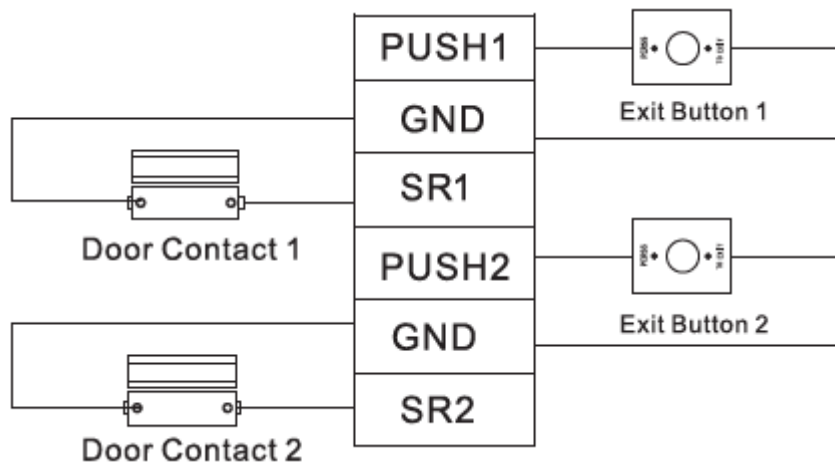


Table 2-3

Port	Wiring Terminal	Description
Exit button+ door contact	PUSH1	Exit button of door 1
	GND	Shared by exit button of door 1 and door contact input of door 1
	SR1	Door contact input of door 1
	PUSH2	Exit button of door 2
	GND	Shared by exit button of door 2 and door contact input of door 2
	SR2	Door contact input of door 2

## 2.4.3 Wiring Description of Lock

Support 4 groups of lock control outputs; serial numbers after the terminals represent corresponding doors. Please choose 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 2-4 for descriptions of wiring terminals.

Figure 2-7

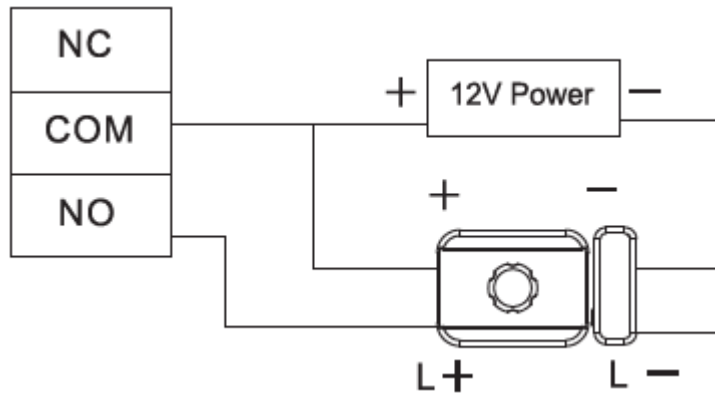


Figure 2-8

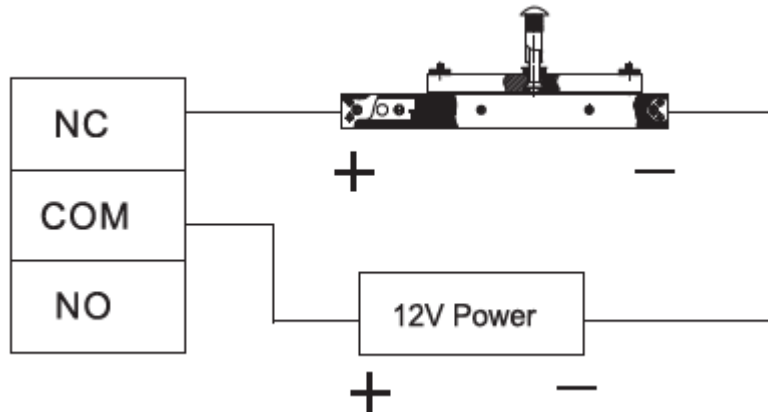


Figure 2-9

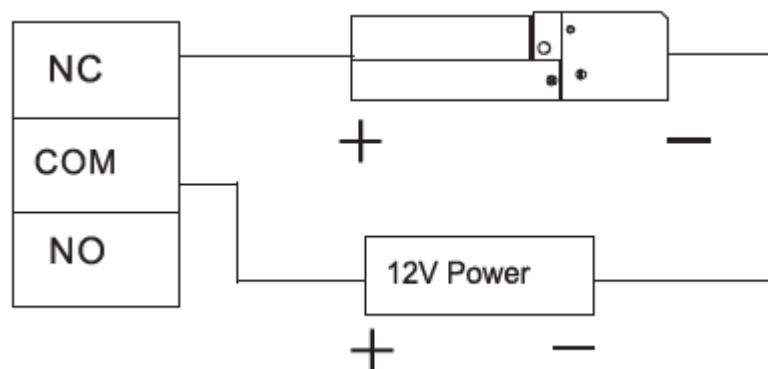


Table 2-4

Port	Wiring Terminal	Description
Lock control output port	NC1	Lock control of door 1
	COM1	
	NO1	
	NC2	Lock control of door 2
	COM2	

Port	Wiring Terminal	Description
	NO2	

## 2.4.4 Wiring Description of Reader

### NOTE

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

Please refer to Table 2-5 for descriptions of wiring terminals corresponding to readers. Take door 1 for example; other readers are the same. Please refer to Table 2-6 for descriptions of reader cable specification and length.

Table 2-5

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	
	GND	Black	Reader power supply
	12V	Red	

Table 2-6

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

## 2.4.5 Wiring Description of External Alarm Input

4-ch external alarm input connection is shown in Figure 2-10. Please refer to Table 2-7 for descriptions of wiring terminals.

Figure 2-10

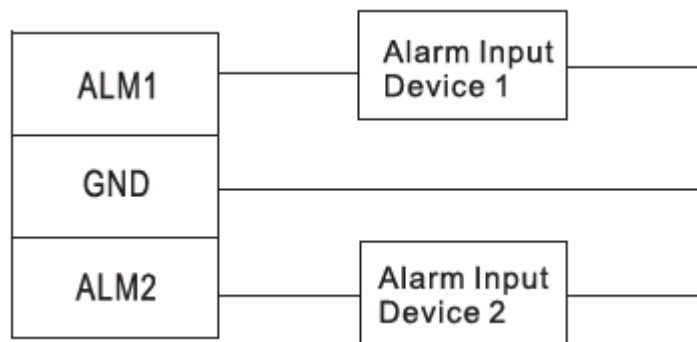



Table 2-7

Port	Wiring Terminal	Description
External alarm input	ALM1	Alarm input port 1
	GND	Shared by alarm input port 1 and 2
		External alarm input ports are able to connect smoke detector and IR detector etc..

Port	Wiring Terminal		Description
	ALM2	Alarm input port 2	 NOTE External alarm can link door open and closed status. <ul style="list-style-type: none"> <li>ALARM1 ~ ALARM2 external alarm links all doors to be normally open.</li> <li>ALARM3 ~ ALARM4 external alarm links all doors to be normally closed.</li> </ul>
	ALM3	Alarm input port 3	
	GND	Shared by alarm input port 3 and 4	
	ALM4	Alarm input port 4	

## 2.4.6 Wiring Description of External Alarm Output

With 2-ch external alarm output, after an alarm is triggered, 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 2-11 and Figure 2-12. Please refer to Table 2-8 for descriptions about wiring terminals.

Figure 2-11

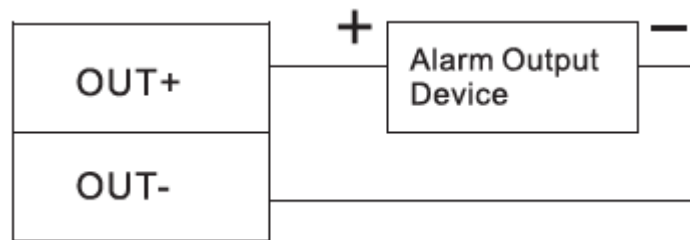


Figure 2-12

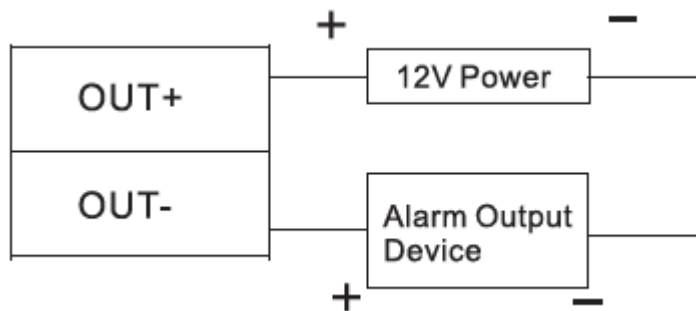


Table 2-8

Port	Wiring Terminal		Description
External alarm output	OUT1+	ALM1/ALM2 triggers alarm output.	External alarm output ports are able to connect audible and visual sirens.
	OUT1-		
	OUT2+	ALM3/ALM4 triggers alarm output.	
	OUT2-		

## 2.4.7 Wiring Description of Internal Alarm Output

With 2-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.

- NC represents normally closed status.
- NO represents 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 2-13 and Figure 2-14. Please refer to Table 2-9 for descriptions about wiring terminals.

Figure 2-13

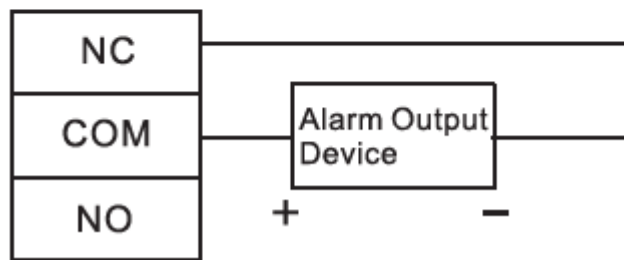
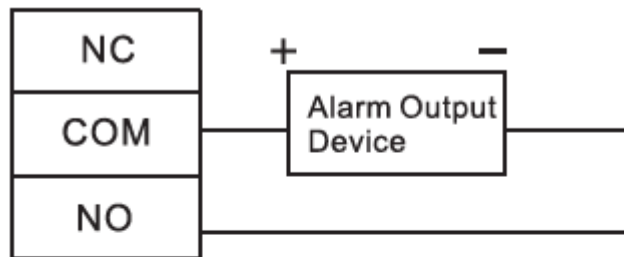


Figure 2-14

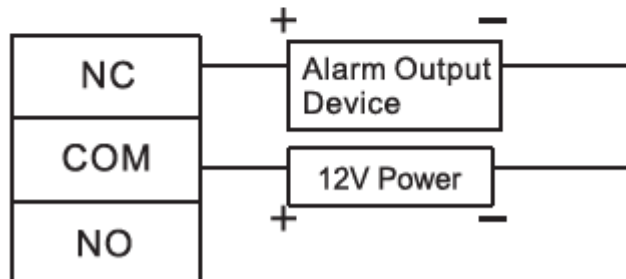
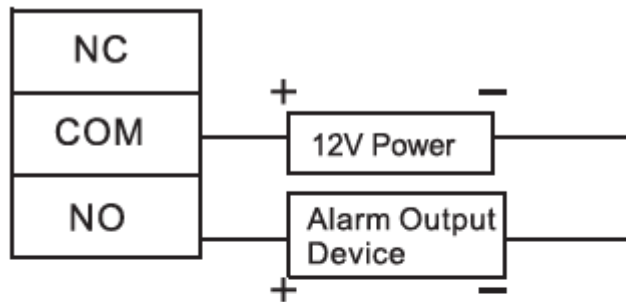




Table 2-9

Port	Wiring Terminal	Description	
Internal alarm output	NC3	<ul style="list-style-type: none"> <li>Tamper alarm output of door 1 entry reader and exit reader</li> <li>Timeout and intrusion alarm output of door 1</li> </ul>	Internal alarm output ports are able to connect audible and visual sirens.
	COM3		
	NO3		
	NC4	<ul style="list-style-type: none"> <li>Tamper alarm output of door 2 entry reader and exit reader</li> <li>Timeout and intrusion alarm output of door 2</li> </ul>	
	COM4		
	NO4		

## 2.4.8 Description of Alarm Input and Output Rule

In case of alarm event, the alarm continues for 15s. Please refer to Table 2-10 for detailed alarm input and output rules.

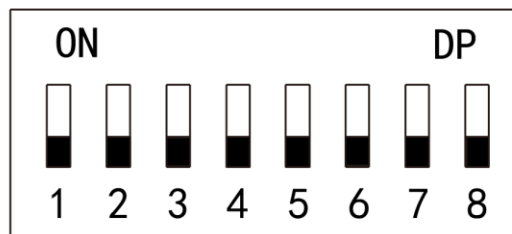
Table 2-10



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 closed.
	ALM4		
Internal alarm input	SR1	OUT1	Door timeout and intrusion alarm trigger external alarm to give an alarm.
	SR2	OUT2	
	RS-485/CASE	OUT1	Tamper alarm of reader triggers external alarm to give an alarm.
	RS-485/CASE	OUT2	

## 2.5 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 restart, the system restores factory defaults.
- 2, 4, 6 and 8 are 1, while others are 0. After restart, the system restores factory defaults, but user info is retained.

## 2.6 Restart

Insert a needle into restart hole, press it once to restart the device.



NOTE

Restart button is to restart 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 ports for different versions. Please refer to actual port.

## 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

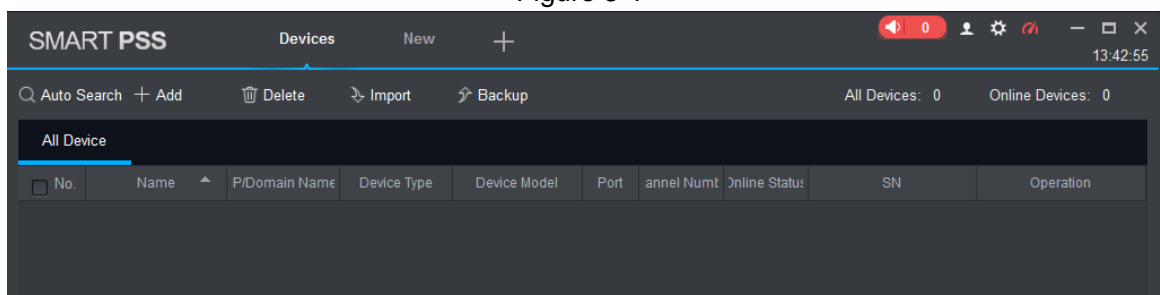
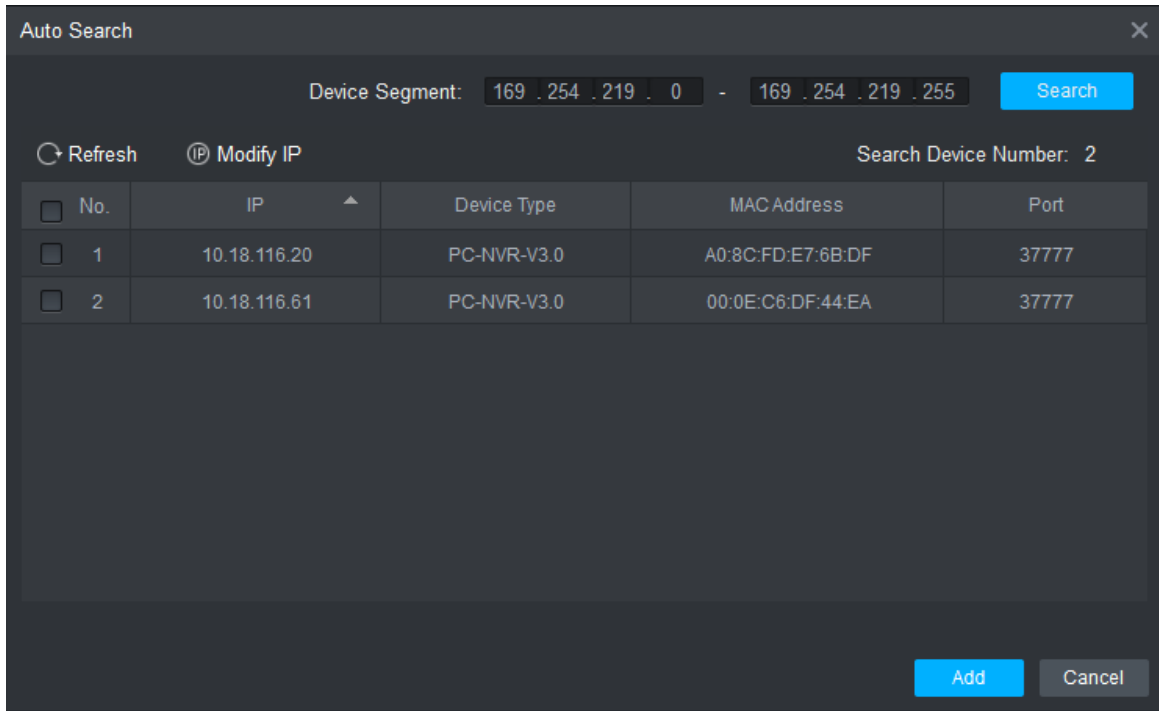


Figure 3-2



**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.

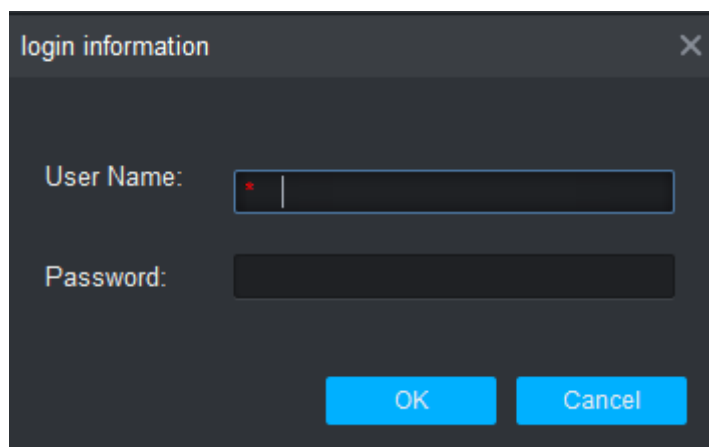
**Step 3** Select the device that needs to be added, and click “Add”.

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

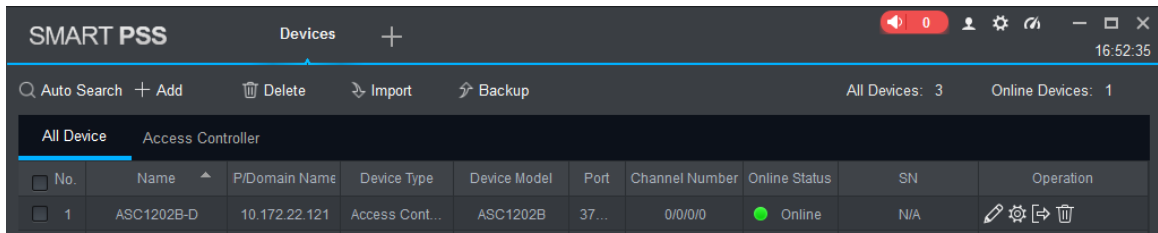


Table 3-1

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	<ul style="list-style-type: none"> <li>• When the device is online, the icon is . Click this icon to exit login, and this icon turns to .</li> <li>• When the device is offline, the icon is . Click this icon to login (with correct device info), and this icon turns to .</li> </ul>
	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

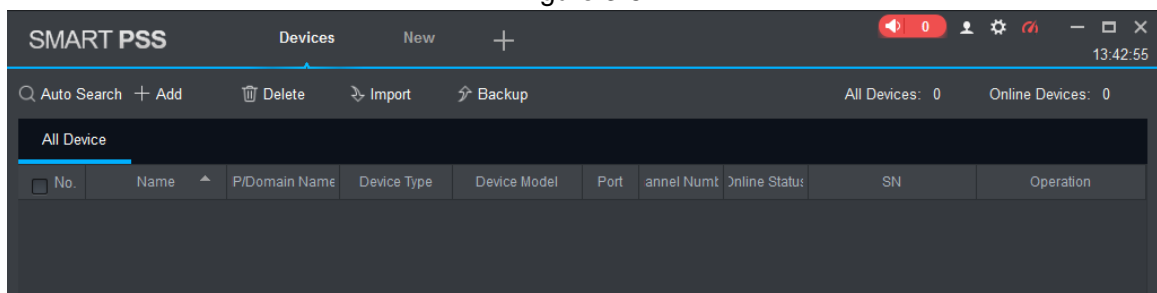


Figure 3-6

**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 name 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.

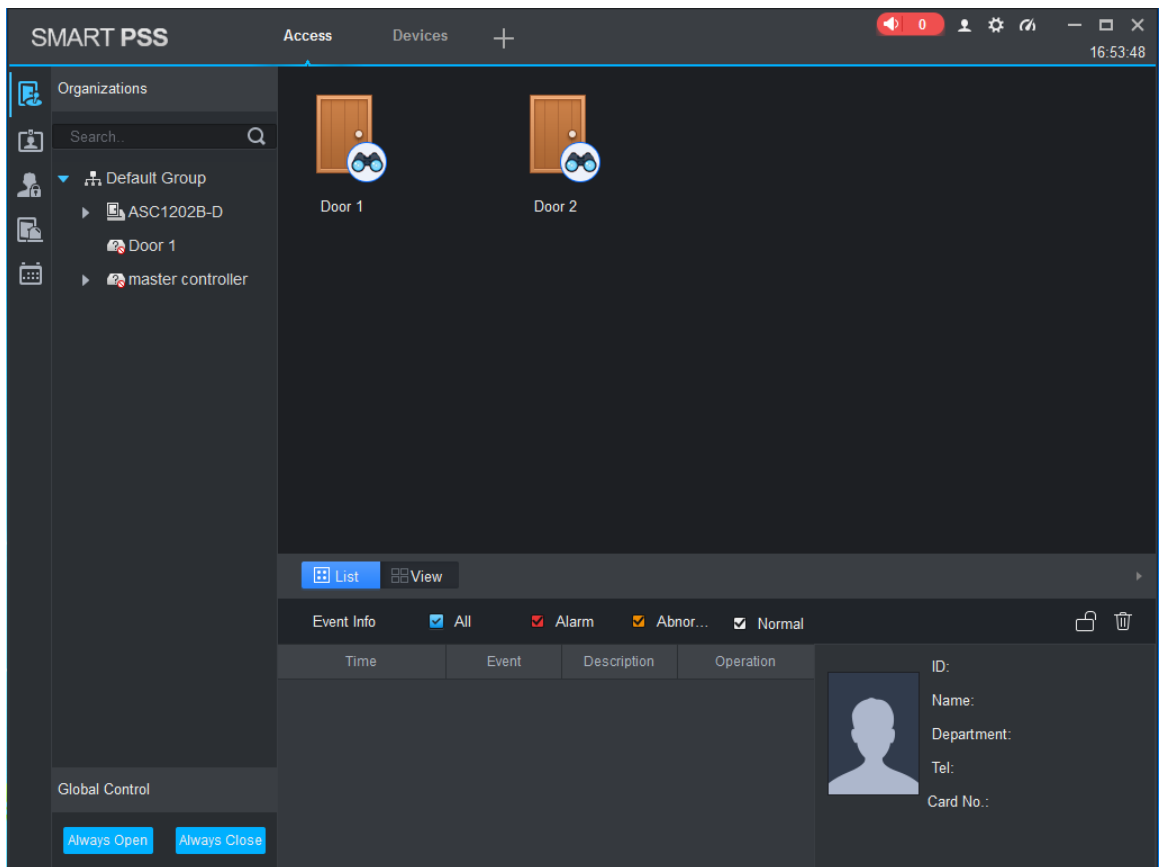
**Step 3** Click “Add” to add a device.

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

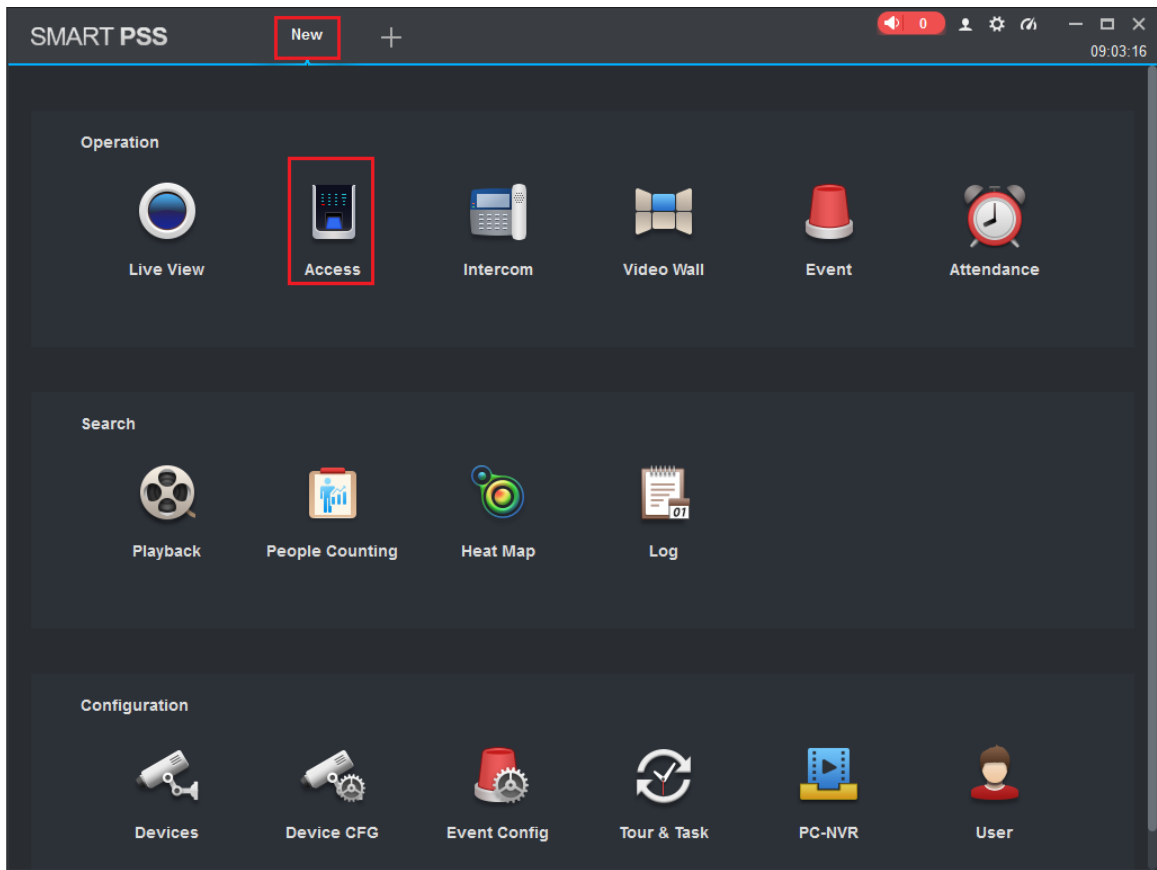


### 3.3 Add User

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

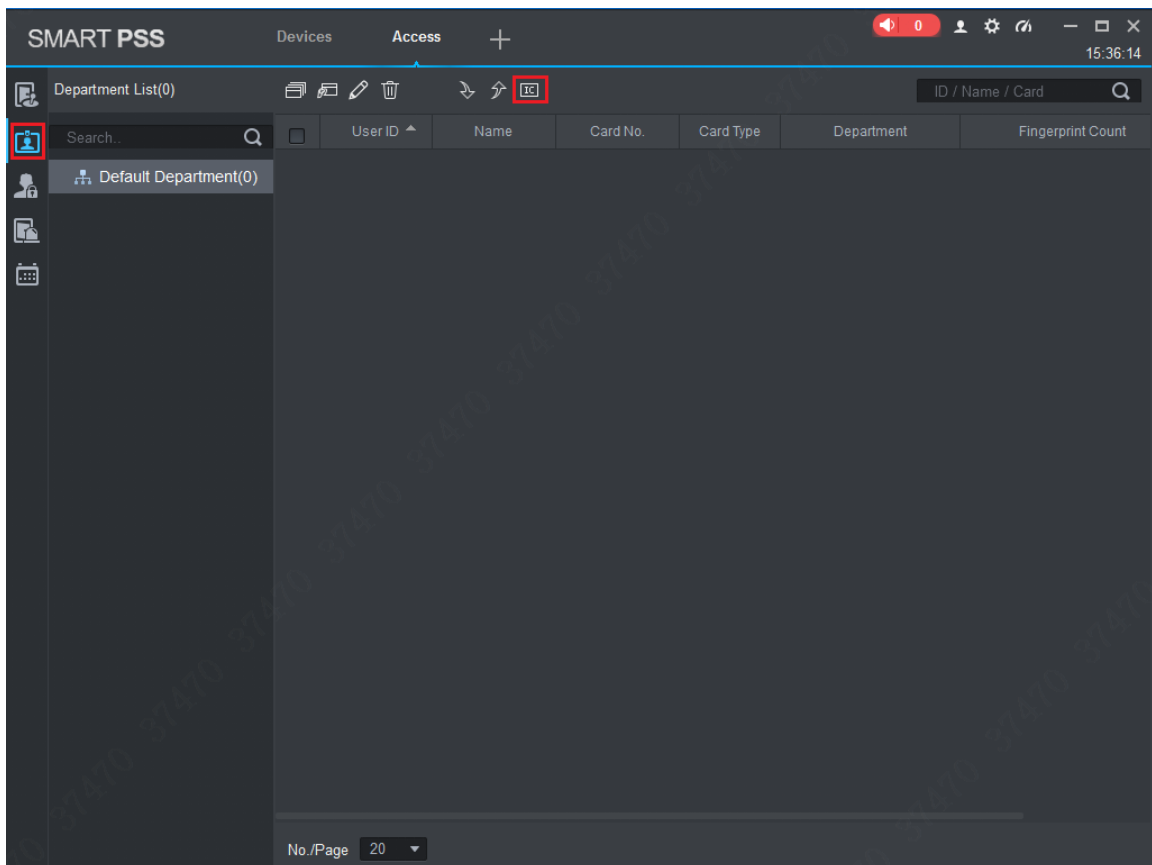
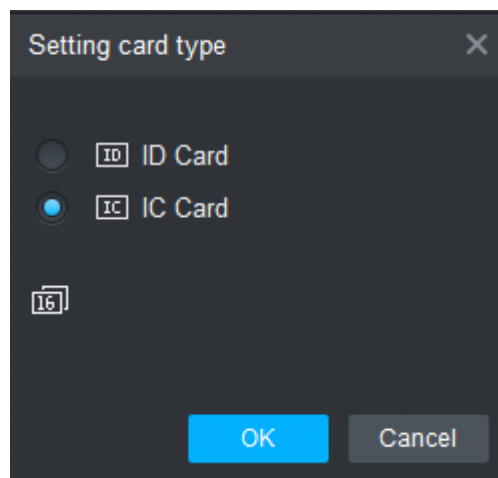


Figure 3-10



### 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

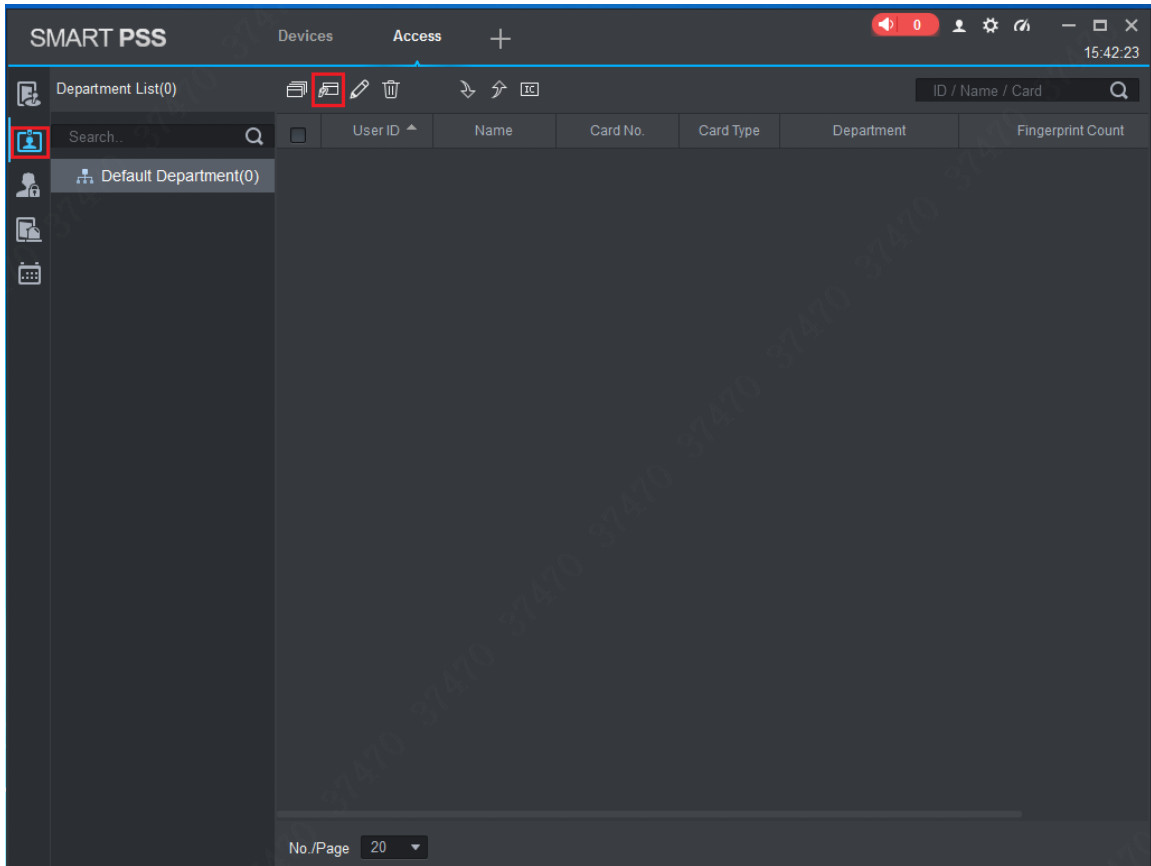
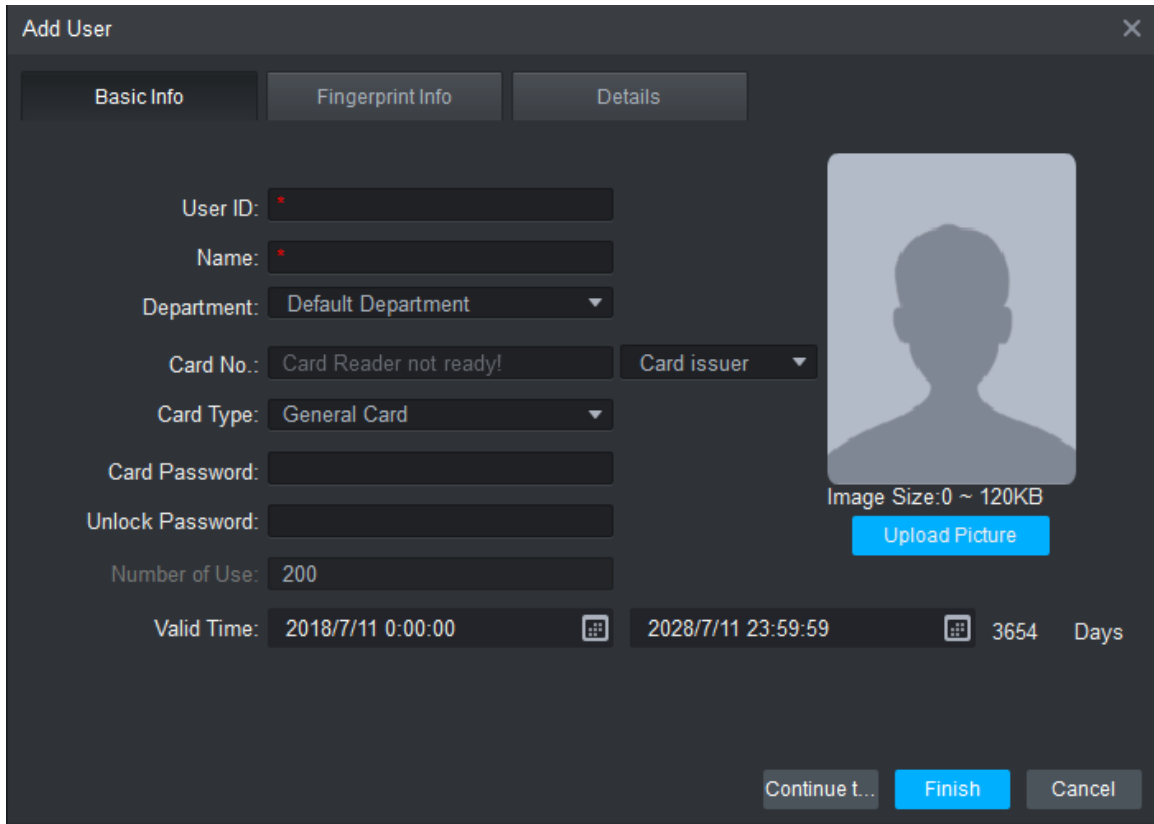



Figure 3-12



**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	<ul style="list-style-type: none"> <li>• User ID (mandatory).</li> <li>• Name (mandatory).</li> <li>• Department (auto association).</li> <li>• Card No.: input by card reader or input manually.</li> <li>• Card type: general card, VIP card, guest card, patrol card, blacklist card and duress card.</li> <li>• Card Password: it is used to open the door with card + password.</li> <li>• Unlock Password: it is used to open the door with password.</li> <li>• Number of Use: it only applies to guest card.</li> <li>• Valid Time: set the valid time of card, which is 10 years by default.</li> <li>• Picture: user picture, max. 120K.</li> </ul> <p> NOTE Card no. and user ID cannot be repeated.</p>
Fingerprint Info	<p>Collect fingerprints with fingerprint reader and access reader.</p> <ul style="list-style-type: none"> <li>• Max. 2 fingerprints for every person.</li> <li>• Support to enter fingerprint name.</li> </ul>
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.


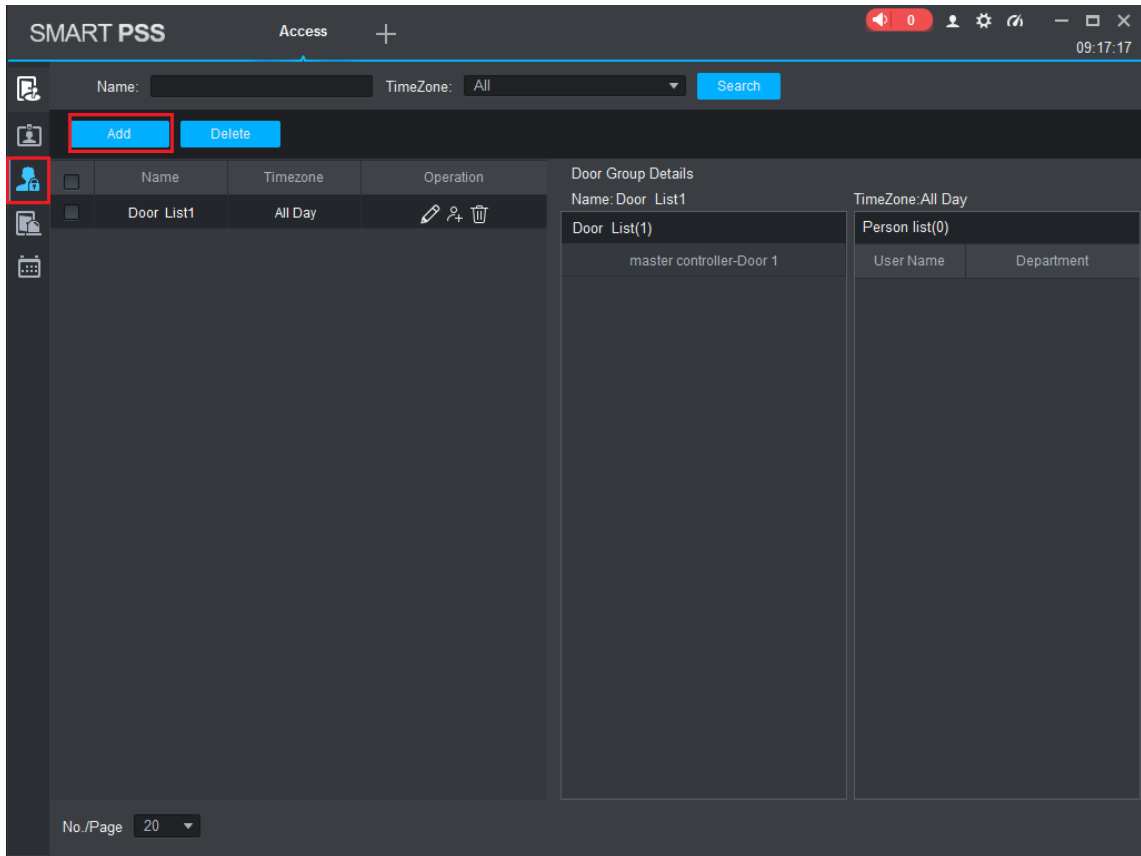
Step 1 In “Access” interface, click , and then click “Access Level”, as shown in Figure 3-13.

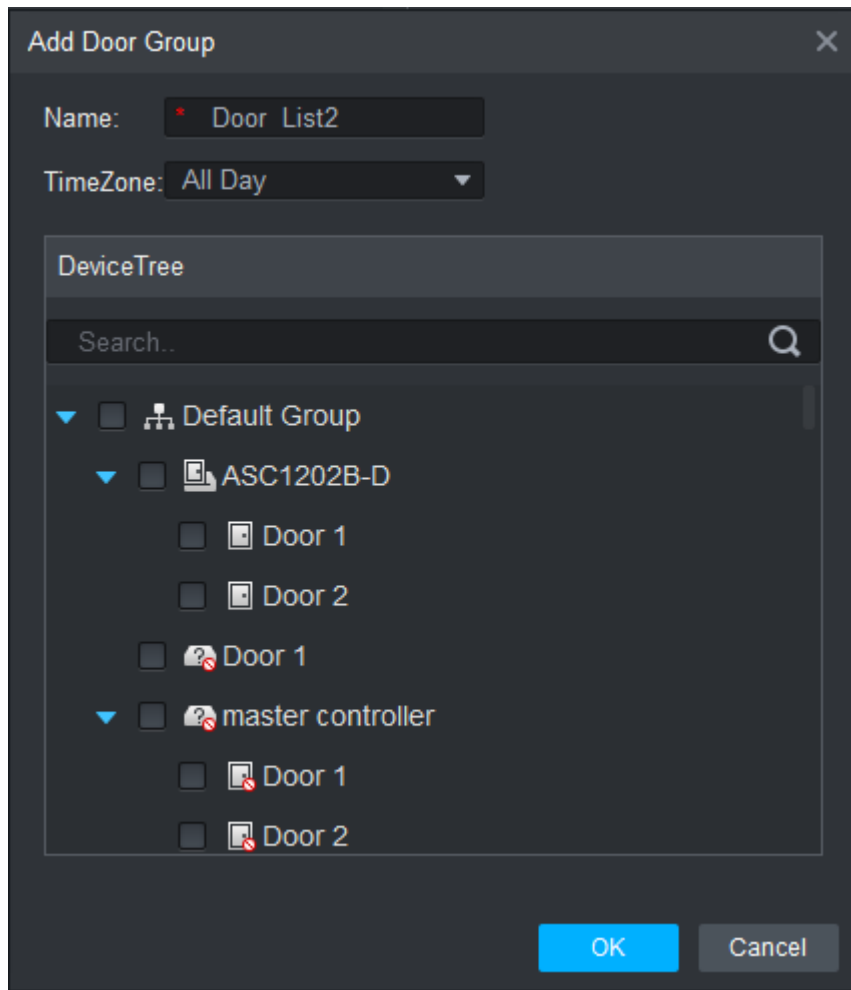
Figure 3-13



**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.


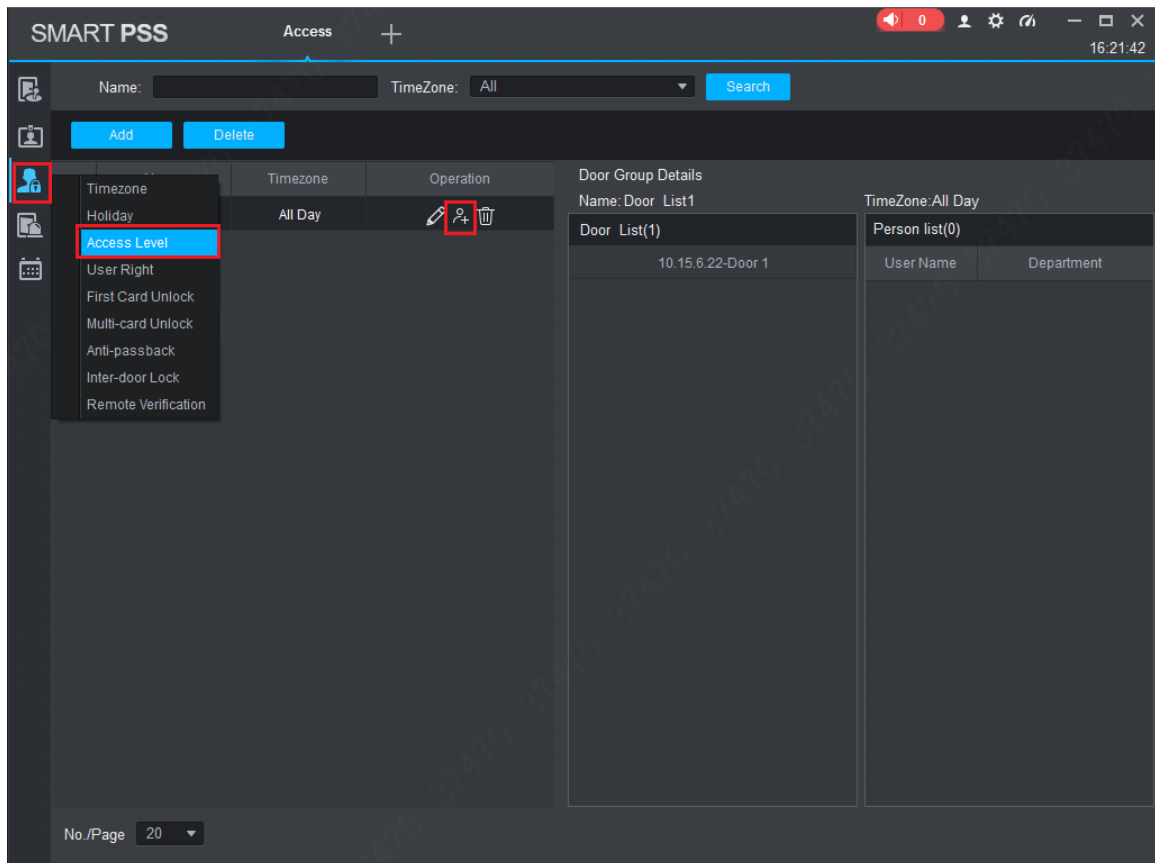

Step 1 In “Access” interface, click , and then click “Access Level”, as shown in Figure 3-15.

Figure 3-15

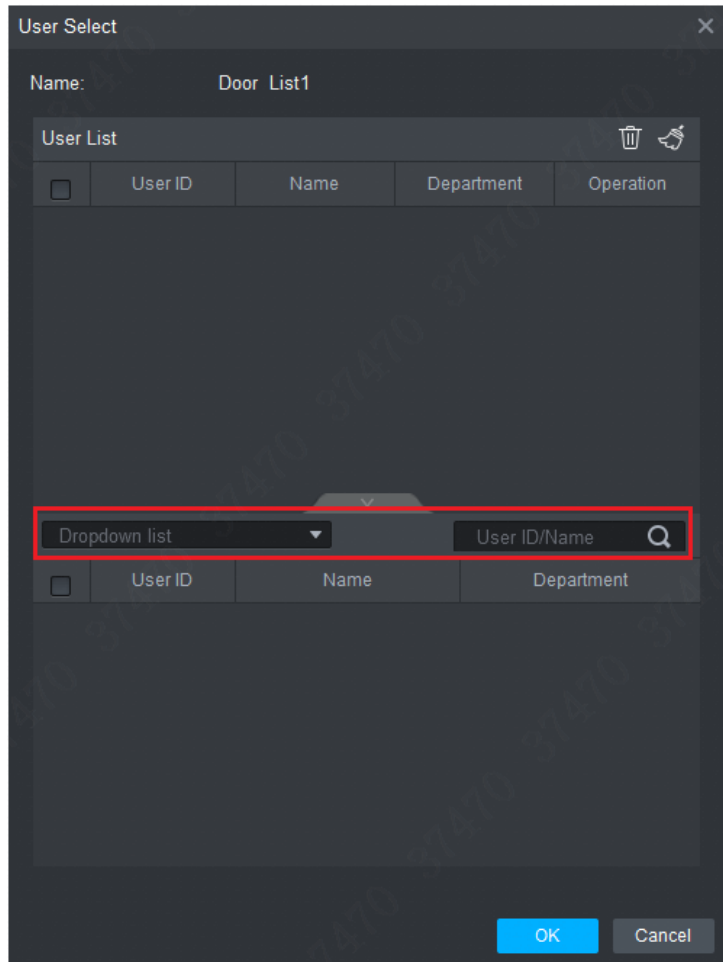


**Step 2** Click .

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, as shown in Figure 3-16.

Figure 3-16



**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.


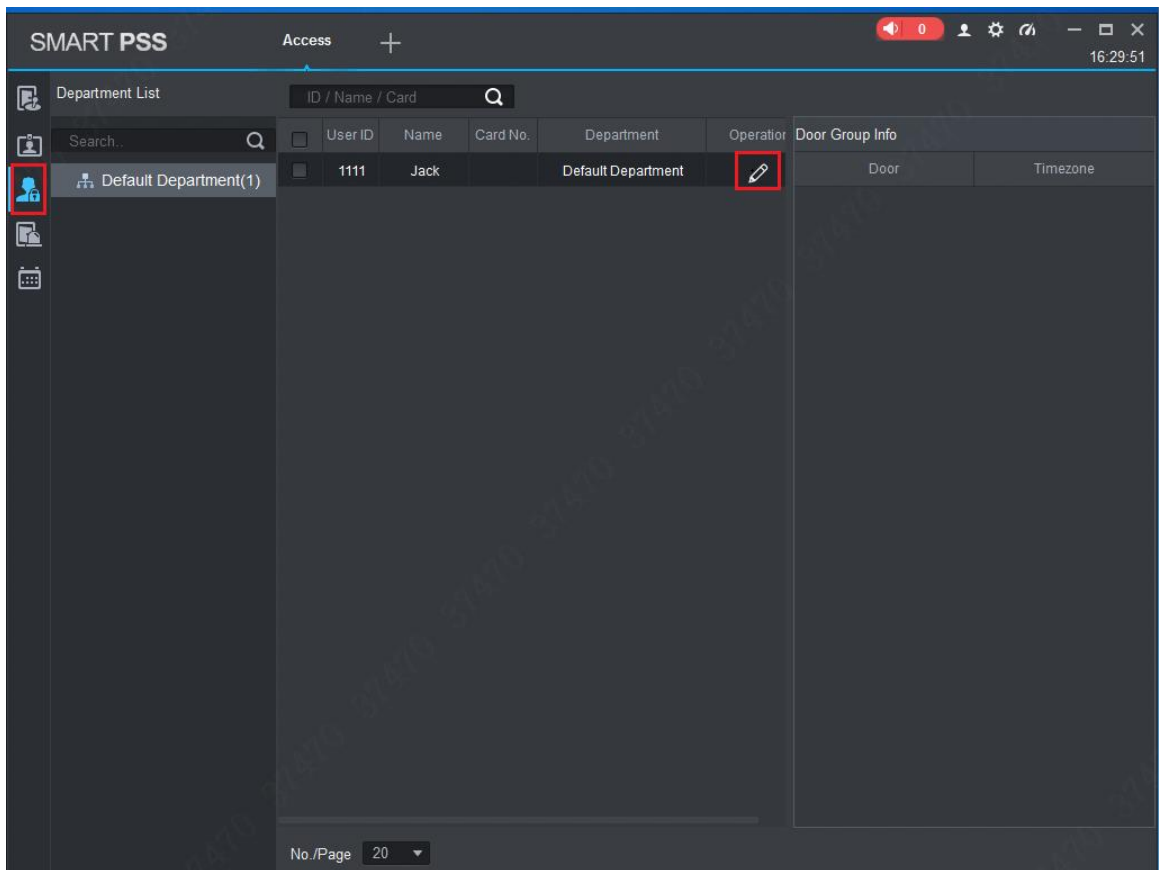

**Step 1** In “Access” interface, click , and then click “User Right”, as shown in Figure 3-17.

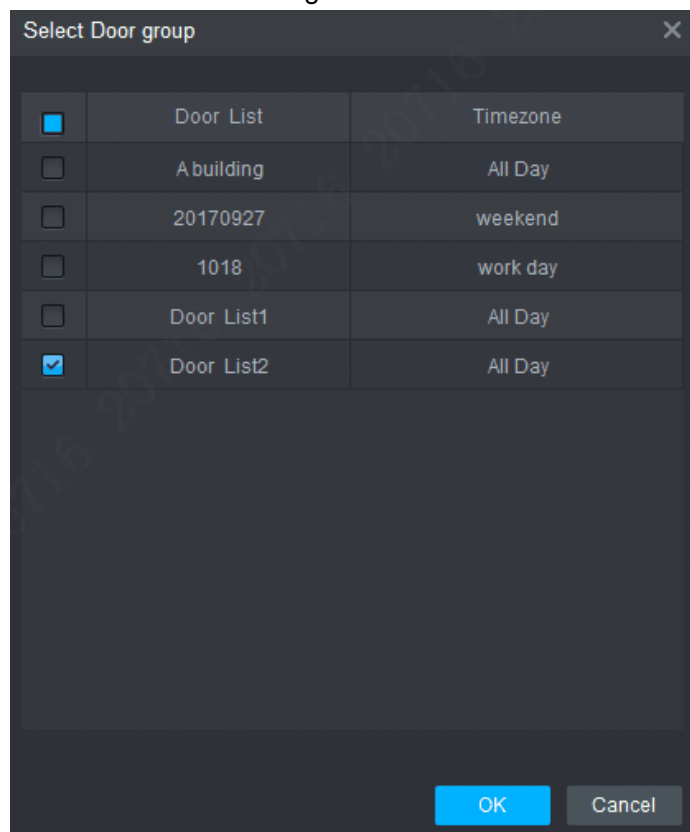
Figure 3-17



**Step 2** Click .

The system pops up “Select Door Group” dialog box, as shown in Figure 3-18.

Figure 3-18



**Step 3** Select the door group and click “OK” to finish authorization.



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

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

## **Mandatory actions to be taken for basic equipment network security:**

### **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. Update Firmware and Client Software in Time**

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

## **"Nice to have" recommendations to improve your equipment network security:**

### **1. Physical Protection**

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

### **2. Change Passwords Regularly**

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

### **3. Set and Update Passwords Reset Information Timely**

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

### **4. Enable Account Lock**

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

## **5. Change Default HTTP and Other Service Ports**

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

## **6. Enable HTTPS**

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

## **7. Enable Whitelist**

We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

## **8. MAC Address Binding**

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

## **9. Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

## **10. Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- **SNMP:** Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- **SMTP:** Choose TLS to access mailbox server.
- **FTP:** Choose SFTP, and set up strong passwords.
- **AP hotspot:** Choose WPA2-PSK encryption mode, and set up strong passwords.

## **11. Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

## **12. Secure Auditing**

- **Check online users:** we suggest that you check online users regularly to see if the device is logged in without authorization.
- **Check equipment log:** By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

## **13. Network Log**

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

## **14. Construct a Safe Network Environment**

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- **Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.**

- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.