

Main Access Controller

User's Manual

V1.0.2

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

- Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
- These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system’s credentials. You will need to either update the camera’s firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

- Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.
- You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on Smart PSS:

Those using Smart PSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for Smart PSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

- UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.
- If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you think that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network






The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

General

This document elaborates on structure, installation, wiring and WEB operation of the main 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.

Revision Record

No.	Version No.	Revision Content	Release Date
1	V1.0.2	Updated the manual.	2022.10.19
2	V1.0.1	Add privacy protection notice.	2018.05.23

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 resulting personal injury or device damage shall be borne by the user.
- 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

Cybersecurity Recommendations	II
Foreword	V
Important Safeguards and Warnings	VII
1 Overview	10
1.1 Functional Feature	10
1.2 External Dimension	11
2 Installation Guide	12
2.1 System Structure.....	12
2.2 Device Installation	13
2.3 Wiring Diagram	13
2.3.1 Wiring Description of CAN Bus.....	14
2.3.2 Wiring Description of External Alarm Input.....	15
2.3.3 Wiring Description of External Alarm Output.....	16
2.3.4 Wiring Description of Reader.....	17
2.3.5 Wiring Description of Lock.....	17
2.3.6 Wiring Description of Exit Button	18
2.3.7 Wiring Description of Door Sensor	19
2.4 DIP Switch.....	20
2.5 Reboot.....	21
3 WEB Configuration	22
3.1 Initialization	22
3.2 Login.....	23
3.3 Reset Password.....	23
3.4 Manage Access Controller	25
3.4.1 Add.....	25
3.4.2 Modify	27
3.4.3 Delete.....	27
3.4.4 Upgrade	27
3.4.5 Check Time	28
3.4.6 Synchronize Log	28
3.4.7 Query	28
3.5 Set Door Parameters	28
3.6 Set Alarm Linkage	30
3.7 Set Network.....	31
3.7.1 TCP/IP	31
3.7.2 Port	33
3.7.3 DDNS.....	33
3.7.4 Register.....	34
3.7.5 P2P	35
3.7.6 HTTPS	36
3.8 User Management	42

3.8.1 Add User	42
3.8.2 Modify Password	43
3.8.3 Set Email.....	44
3.8.4 Delete User	44
3.9 Safety Management.....	44
3.9.1 IP Authority.....	44
3.9.2 SSH.....	45
3.10 Maintenance.....	46
3.10.1 Date Setting	46
3.10.2 Maintenance	47
3.10.3 Config Management	47
3.10.4 Default Setting	48
3.10.5 System Upgrade	48
3.11 Information	49
3.11.1 Version Info	49
3.11.2 Online User	50
4 Smart PSS Config.....	51
4.1 Log in Client	51
4.2 Add Access Controller.....	51
4.2.1 Auto Search	51
4.2.2 Manual Add.....	53
4.3 Add User	55
4.3.1 Card Type	56
4.3.2 Single Add.....	57
4.4 Add Door Group.....	59
4.5 Authorize	61
4.5.1 Authorize According to Door Group.....	61
4.5.2 Authorize According to User	63
5 FAQ	66
1. Question: After power on, power indicator doesn't turn on or the buzzer doesn't respond.	66
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.	66
3. Question: Client software fails to detect the device.	66
4. Question: After swiping card, it prompts that card is invalid.....	66
5. Question: How can I deal with problems that are not confirmed or cannot be solved?.....	66
6 Technical Parameters.....	67

Main access controller is a controlling device which compensates access control system. It has neat and modern design with strong functionality, suitable for commercial building, corporation property and intelligent community.

1.1 Functional Feature

Product Highlight

- Support cascade design of CAN bus.
- Overall planning and design of entire route.
- Overall multi-door interlocking.
- Support to connect card readers in the form of fingerprint, IC and password.

Controller Interface

- Locally support 4 groups of lock control output.
- Locally support 8 groups of alarm input and 8 groups of alarm output.
- Locally support 4 groups of exit buttons, 4 groups of door sensor feedback and 4 groups of locking tongue feedback.
- Locally support 4 groups of card readers (four-door one-way 4 groups of RS485 readers or 4 groups of Wiegand readers).

Controller Parameter

- Support three-level network mode of CAN bus, support max. 16 sub controllers and centralized management of 64+4 doors.
- Support max. 200,000 card holders, 150,000 records and 3,000 fingerprints.
- Support illegal intrusion alarm, unlock overtime alarm, tamper alarm, duress alarm and local unlocked alarm.
- Support regional anti-passback and regional AB door.
- Support unlock with multi-card and remote authentication.
- Support VIP card, guest card, patrol card, ordinary card, blocklist card and duress card.
- Local WEB can add, configure and upgrade the sub controllers.
- Support Onvif Profile C/ CGI /SDK and third-party platform connection.
- All ports have overcurrent and over-voltage protection.
- Support 128 groups of schedules, 128 groups of periods and 128 groups of holiday schedules.
- Support valid time period setting, password setting and expiration date setting of cards. Regarding guest card, its time of use can be set.

- Permanent data storage during outage, built-in RTC (support DST), online upgrading, NTP (network time protocol) and active registration.
- Working temperature: $-30^{\circ}\text{C} \sim +60^{\circ}\text{C}$ and working humidity: $\leq 95\%$.

1.2 External Dimension

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

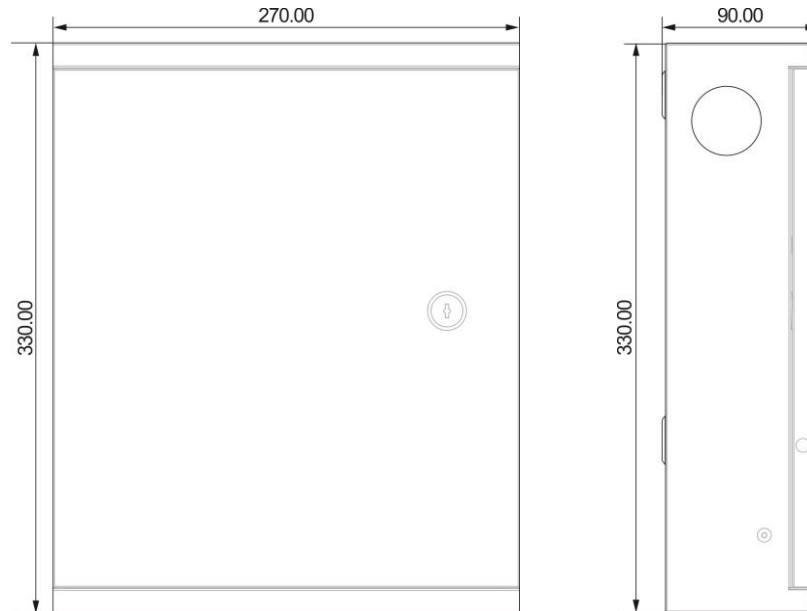


Figure 1-1

2.1 System Structure

Its system structure is shown in Figure 2-1.

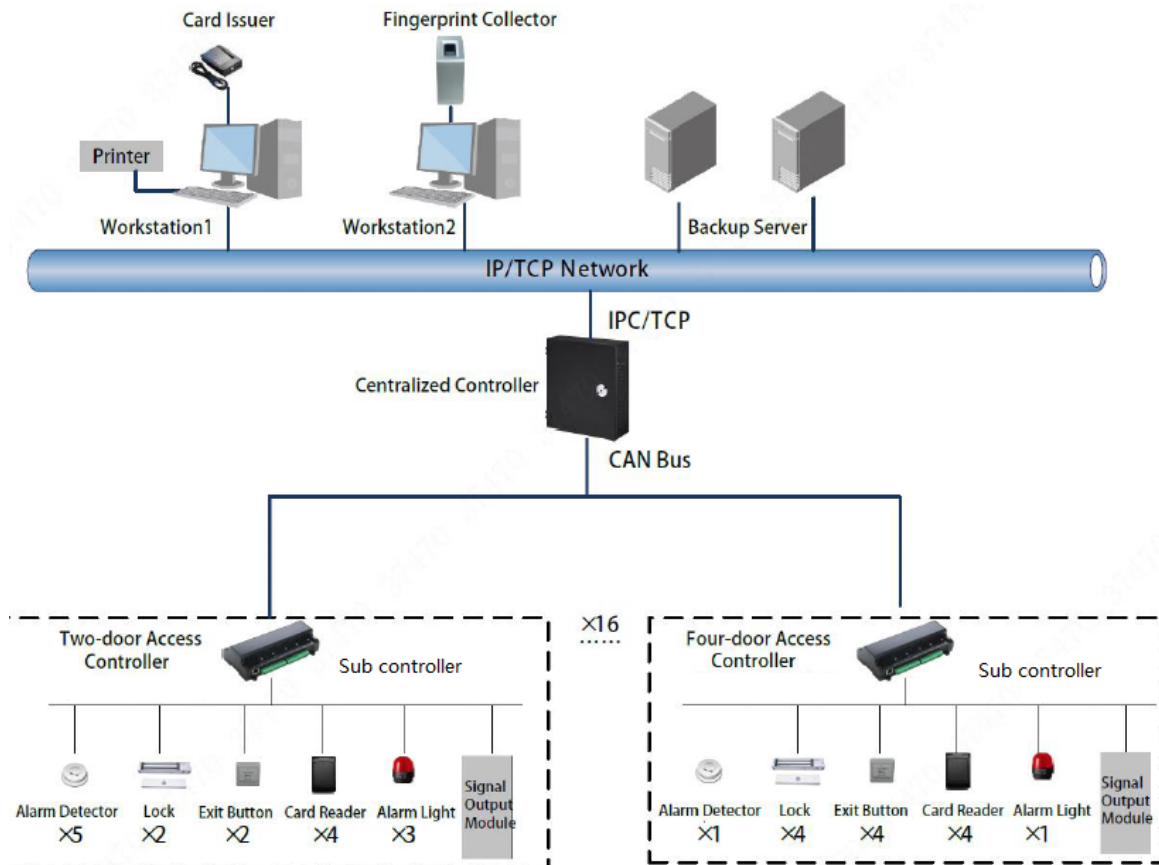


Figure 2-1

2.2 Device Installation

Device installation diagram is shown in Figure 2-2.

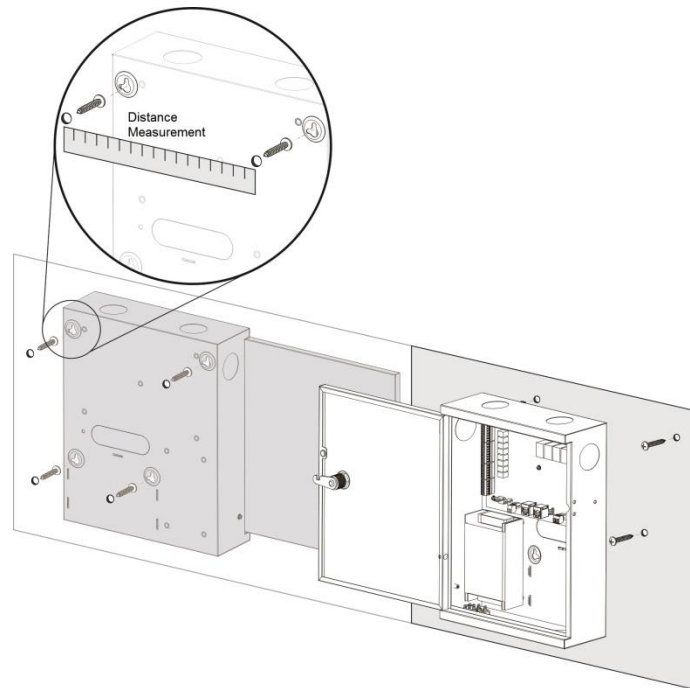


Figure 2-2

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; 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

Device wiring diagram is shown in Figure 2-3.

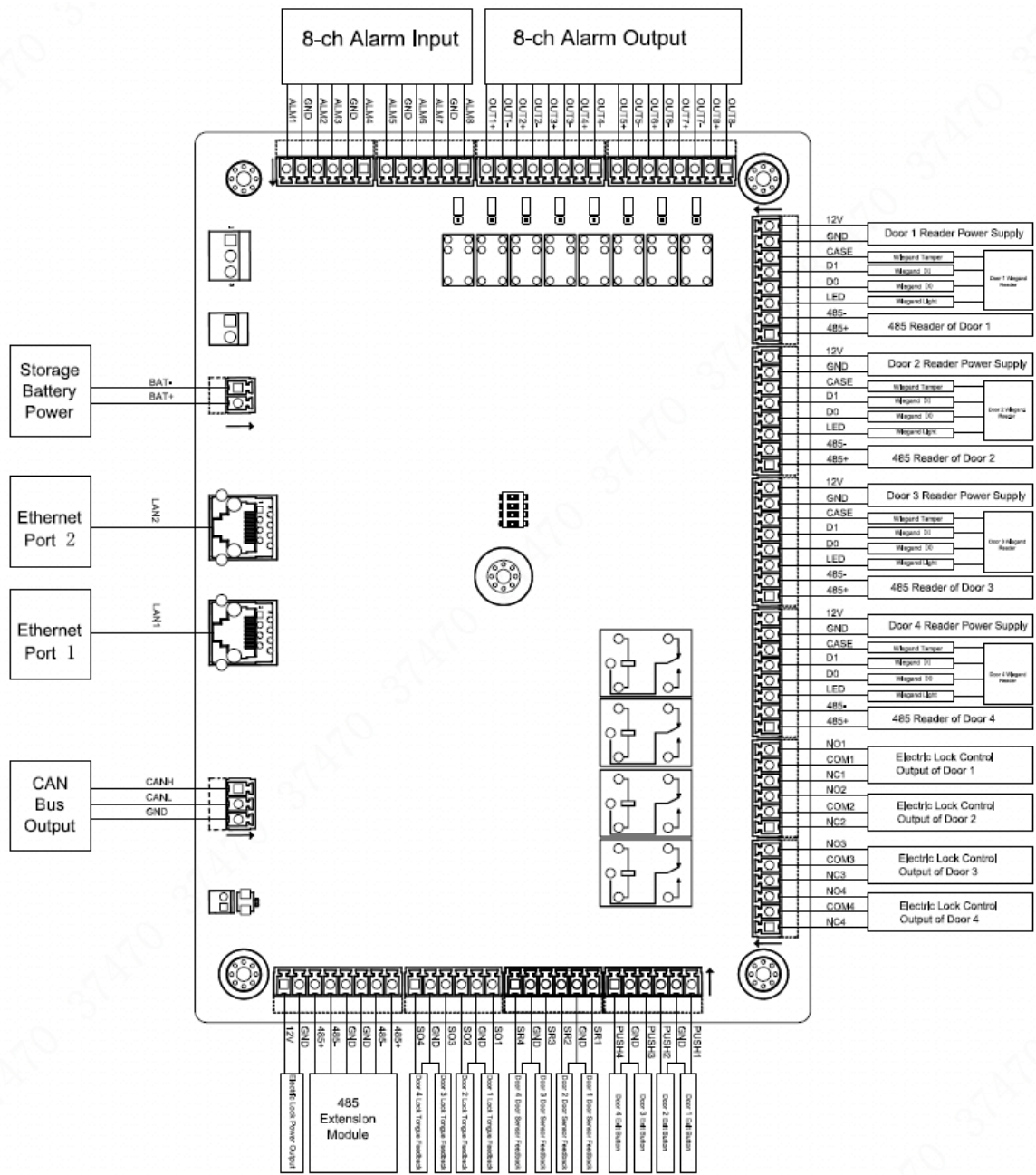


Figure 2-3

2.3.1 Wiring Description of CAN Bus

Main access controller and sub controllers are connected with CAN bus, as shown in Figure 2-4. Please refer to Table 2-1 for descriptions about wiring terminals, and refer to Table 2-2 for communication distance. Speed is set with dip switch. Please refer to “2.4 DIP Switch” for details.

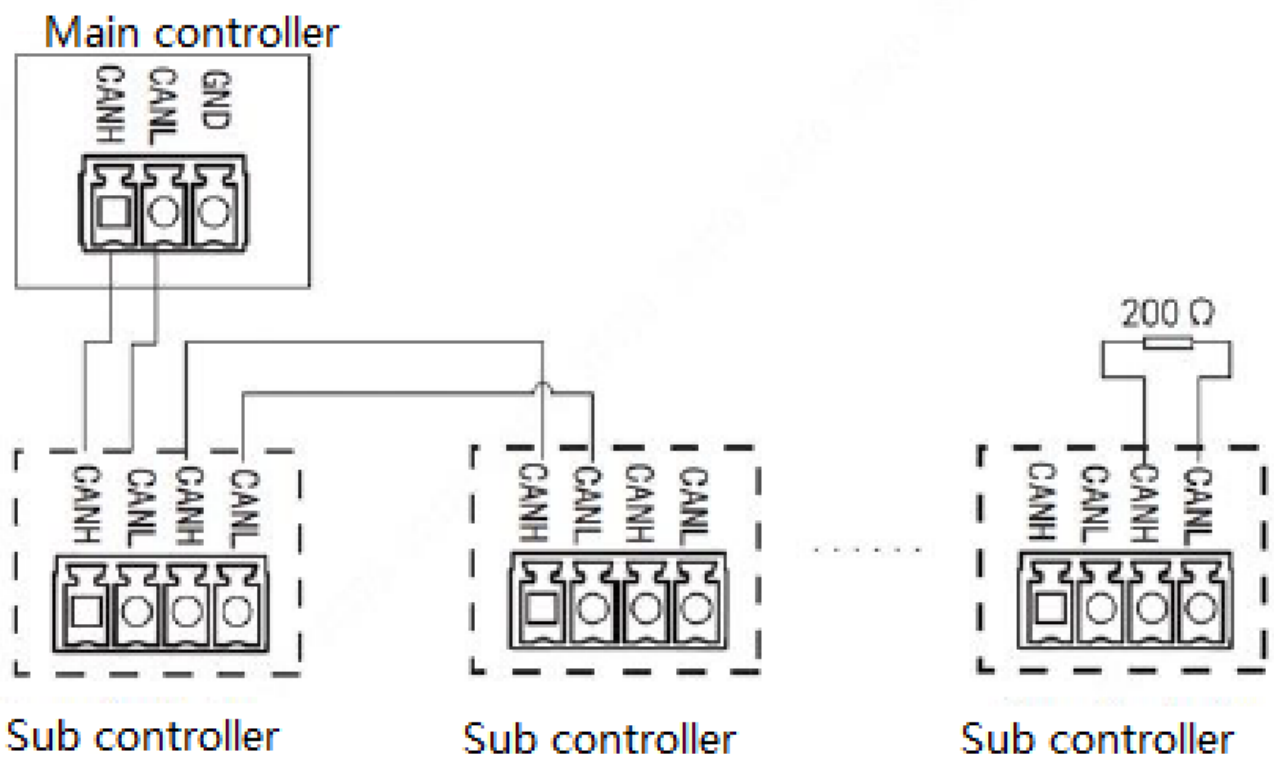


Figure 2-4

Interface	Wiring Terminal	Description
CAN Bus	CANH	CAN bus communication
	CANL	

Table 2-1

Speed	Distance
50kb/s	600m
80kb/s	400m
100kb/s	400m
125kb/s	200m

Table 2-2

2.3.2 Wiring Description of External Alarm Input

Support 8-channel external alarm input, as shown in Figure 2-5. Please refer to Table 2-2 for descriptions about wiring terminals.

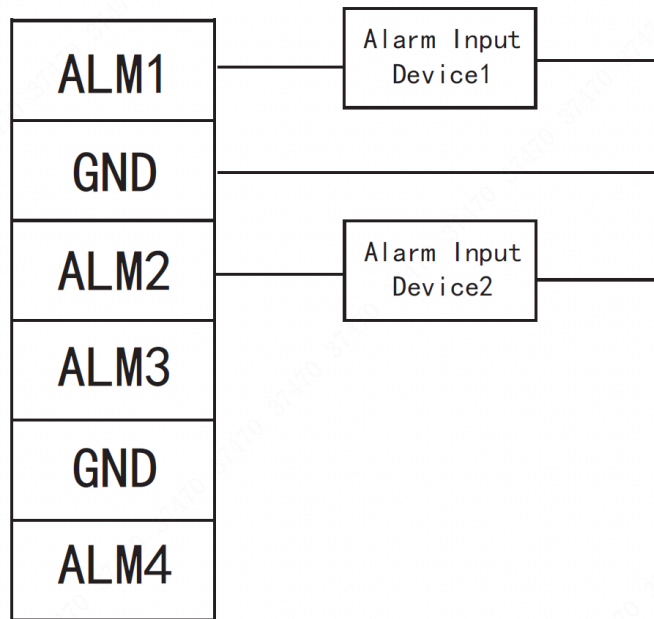


Figure 2-5

Interface	Wiring Terminal		Description
External Alarm Input	ALM1	Alarm input port 1	External alarm input ports connect smoke detector and IR detector etc..
	GND	Alarm input port 1 and 2	
	ALM2	Alarm input port 2	
	ALM3	Alarm input port 3	
	GND	Alarm input port 3 and 4	
	ALM4	Alarm input port 4	
	ALM5	Alarm input port 5	
	GND	Alarm input port 5 and 6	
	ALM6	Alarm input port 6	
	ALM7	Alarm input port 7	
	GND	Alarm input port 7 and 8	
	ALM8	Alarm input port 8	

Table 2-3

2.3.3 Wiring Description of External Alarm Output

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 2-6 and Figure 2-7. Please refer to Table 2-3 for descriptions about wiring terminals.

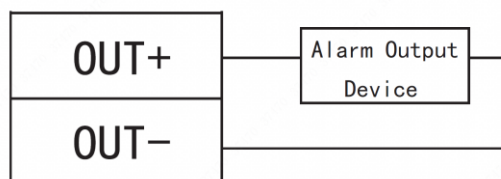


Figure 2-6

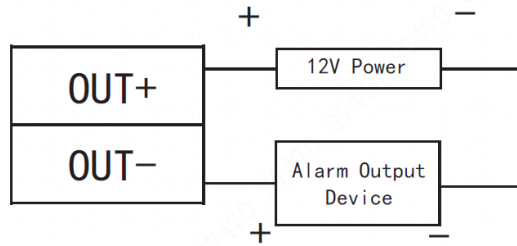


Figure 2-7

Interface	Wiring Terminal	Description
External Alarm Output	OUT1+	External alarm output ports connect audible and visual siren etc..
	OUT1-	

Table 2-4

2.3.4 Wiring Description of Reader



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, and other readers are the same as Door 1. Please refer to Table 2-5 for descriptions of video cable specification and length.

Interface	Wiring Terminal	Cable Color	Description
Entry Reader of Door 1	12V	Red	Reader power supply
	GND	Black	
	CASE	Blue	Wiegand reader
	D1	White	
	D0	Green	
	LED	Brown	485 reader
	485-	Yellow	
485+	Purple		

Table 2-5

Reader Type	Connection Mode	Length
485 Reader	CAT5e network cable, 485 connection	100m
Wiegand Reader	CAT5e network cable, Wiegand connection	30m

Table 2-6

2.3.5 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 2-8, Figure 2-9 and Figure 2-10. Please refer to Table 2-6 for descriptions of wiring terminals.

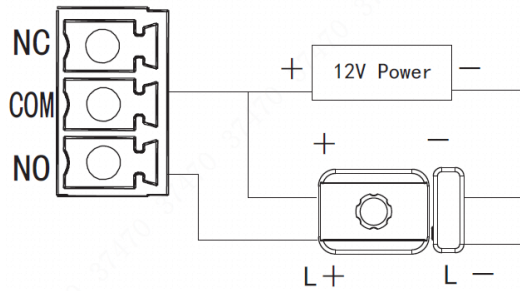


Figure 2-8

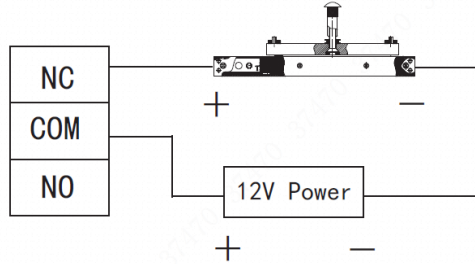


Figure 2-9

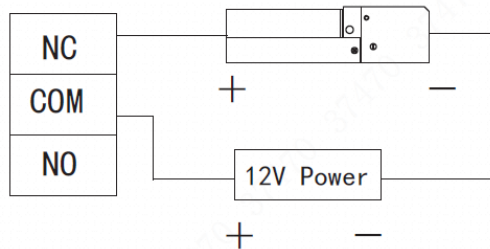


Figure 2-10

Interface	Wiring Terminal	Description
Lock Control Output Interface	NC1	Lock control of door 1
	COM1	
	NO1	
	NC2	Lock control of door 2
	COM2	
	NO2	
	NC3	Lock control of door 3
	COM3	
	NO3	
	NC4	Lock control of door 4
	COM4	
	NO4	

Table 2-7

2.3.6 Wiring Description of Exit Button

Corresponding wiring terminals of exit button are shown in Figure 2-11. Please refer to Table 2-7 for descriptions of wiring terminals.

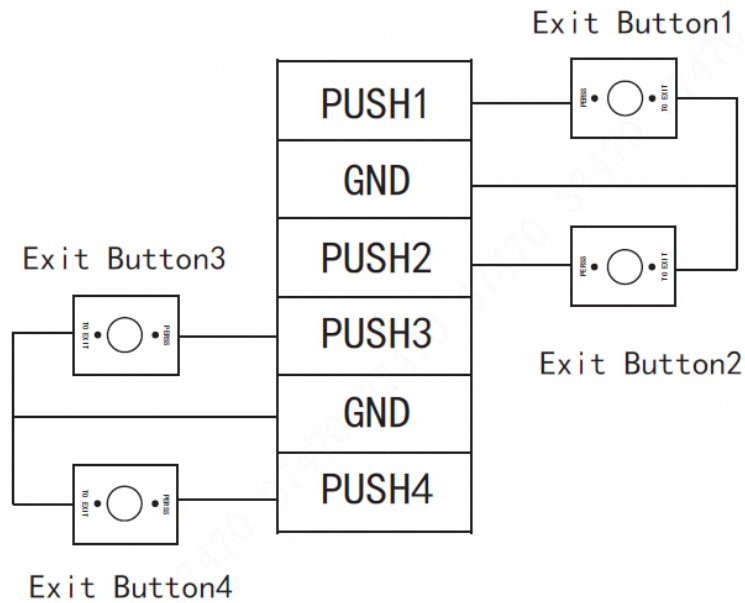


Figure 2-11

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

Table 2-8

2.3.7 Wiring Description of Door Sensor

Corresponding wiring terminals of door sensor are shown in Figure 2-12. Please refer to Table 2-8 for descriptions of wiring terminals.

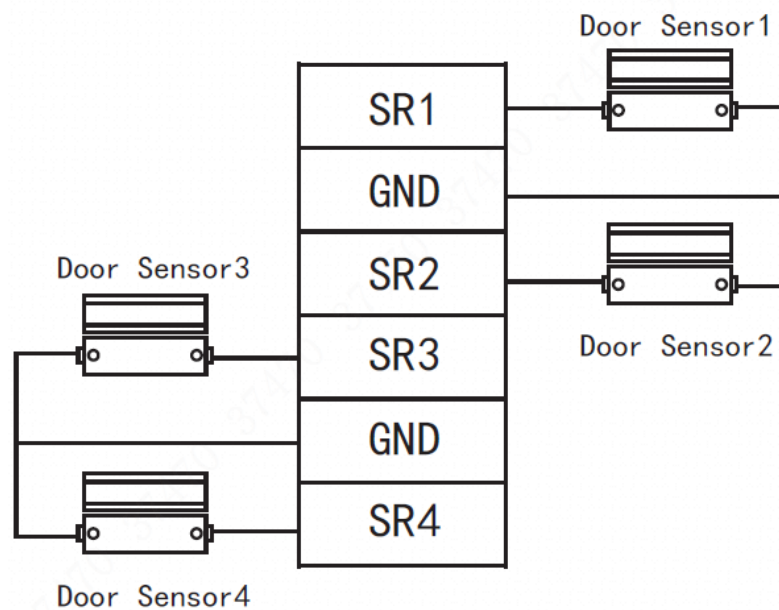




Figure 2-12

Interface	Wiring Terminal	Description
Door Sensor Feedback Interface	SR1	No. 1 door sensor feedback
	GND	Shared by door 1 and 2
	SR2	No. 2 door sensor feedback
	SR3	No. 3 door sensor feedback
	GND	Shared by door 3 and 4
	SR4	No. 4 door sensor feedback

Table 2-9

2.4 DIP Switch

Set device number and speed with DIP switch. Speed of main access controller shall be consistent with sub access controller.

-  the switch is at ON position, meaning 1.
-  the switch is at the bottom, meaning 0.

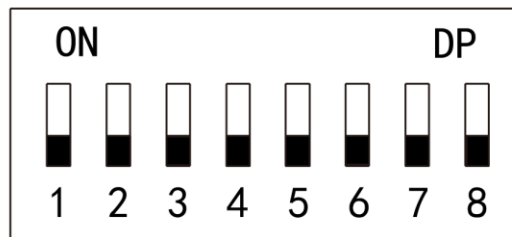
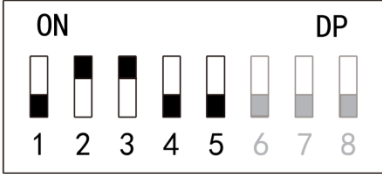
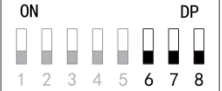


Figure 2-13

Function	No.	Description
Device Number	1~5	Set device number with binary system. The left is the lowest order. For example:  Binary representation 00110 corresponds to 6 in decimal system.
Speed	6~8	Set the speed.  <ul style="list-style-type: none"> All of them are at the bottom, transmission speed is 50kb/s.

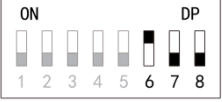
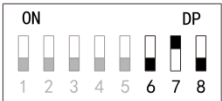
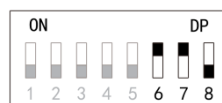
Function	No.	Description
		<ul style="list-style-type: none"> Only digit 6 is at ON position transmission speed is 80kb/s. 
		<ul style="list-style-type: none"> Only digit 7 is at ON position transmission speed is 100kb/s. 
		<ul style="list-style-type: none"> Digits 6 and 7 are at ON position transmission speed is 125kb/s. 

Table 2-10

2.5 Reboot

Insert a needle into RESET hole, and long press to reboot controller.

3 WEB Configuration

Default IP address of main access controller is 192.168.1.109. During the first use, connect PC with the device directly, modify and ensure that IP address of PC and IP address of the device are in the same network segment, in order to login WEB for operations.

3.1 Initialization

During the first use, please set admin username and password (default administrator username is admin).

 Note

To ensure device safety, please keep admin login password properly after device initialization, and modify it regularly.

Step 1 Open IE explorer, input IP address of main access controller in the address bar, and press [Enter] key.

The system displays “Device Initialization” interface, as shown in Figure 3-1.

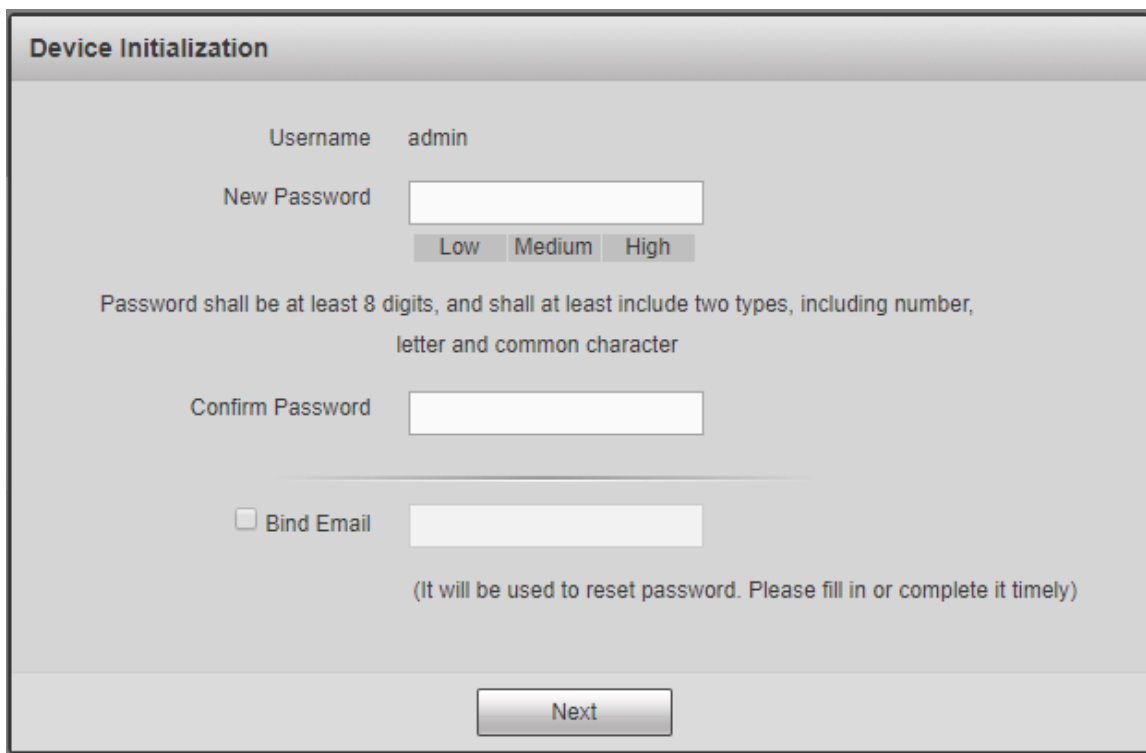


Figure 3-1

Step 2 Set admin login password and Email.

 Note

- The password can be set with 8~32 digits visible characters, and shall include at least two types of number, letter and ordinary character (expect “” , “!” , “,” , “.” and

“&”).

- Bind Email. Scan QR code, input the reserved Email to receive a security code, and thus reset admin password.
- Without reserved Email or in order to modify the Email, please set at “System > User Management” interface. Please refer to “3.8.3 Set Email” for details.

Step 3 Click “Next”.

The system displays “Finish” interface.

Step 4 Click “OK” to complete initialization.

3.2 Login

Step 1 Open IE explorer, input IP address of main access controller in the address bar, and press [Enter] key.

The system displays login interface, as shown in Figure 3-2.



Figure 3-2

Step 2 Input “Username” and “Password”.

 Note

- Default admin username is admin, whereas password is the login password set during device initialization. For the sake of safety, it is suggested that you modify admin password regularly and keep it properly.
- If you forget the login password, click “Forget Password” to reset it. Please refer to “3.3 Reset Password” for details.

Step 3 Click “Login”.

The system displays “Preview” interface.

3.3 Reset Password

If you forget login password of admin user, please reset the password with Email.

Step 1 With the browser, login WEB interface of main access controller.



Figure 3-3

Step 2 Click “Forgot Password”.

The system displays “Reset the password” dialog box, as shown in Figure 3-4.



Figure 3-4

Step 3 Scan the QR code according to interface prompts and obtain security code.



Caution

- Two security codes can be obtained by scanning the same QR code. To obtain security code again, please refresh QR code.
- After receiving security code in your Email, please reset the password with the security code within 24 hours. Otherwise, the security code will become invalid.
- If wrong security code is entered for 5 times continuously, this account will be locked for 5 min.

Step 4 Please enter the received security code in the dialog box.

Step 5 Click “Next”.

The system displays “Reset the password” interface, as shown in Figure 3-5.



Figure 3-5

Step 6 Set “New Password” and “Confirm”.



Note

Password can be 8 to 32 visible characters; it consists of at least 2 types among letters, numbers and symbols (except “'”, “'””, “,””, “.”, and “&”).

Step 7 Click “OK” to complete resetting.

3.4 Manage Access Controller

Add and manage sub access controller; upgrade, check time and synchronize log.

3.4.1 Add

After connecting sub access controller with main access controller, add the sub controller to main controller management system, in order to realize unified management. Maximum 16 controllers can be added.

Step 1 Select “Access Control > Device Management”.

The system displays “Device Management” interface, as shown in Figure 3-6.

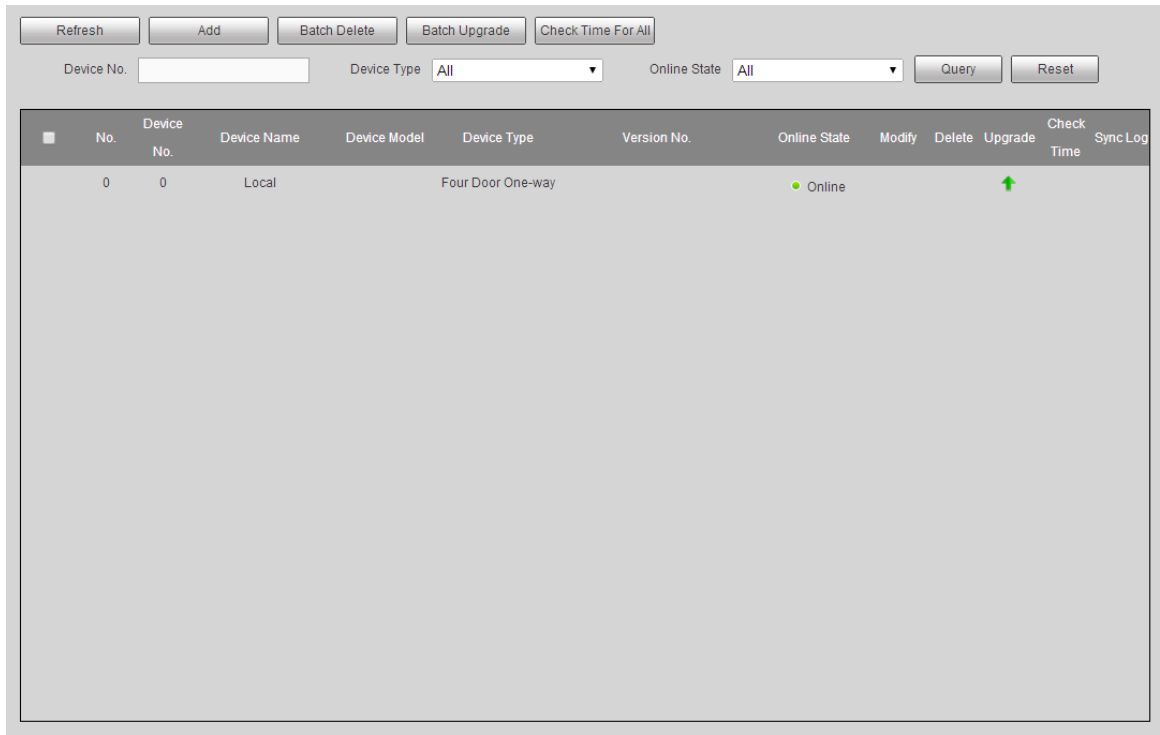


Figure 3-6

Step 2 Click “Add”. The system pops up “Add” dialogue box.

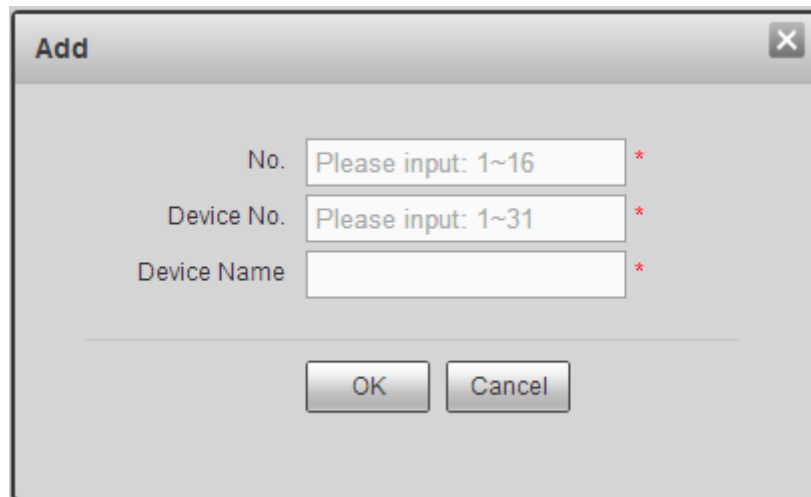


Figure 3-7

Step 3 Input “No.”, “Device No.” and “Device Name”.

Parameter	Description
No.	A customized number ranging from 1 to 16. The number cannot be repeated.
Device No.	It is the same as the added sub controller number. Sub controller number is set in DIP switch and can be used after transforming binary encoding to decimal system. During setting of sub controller, ensure that device no. is not repeated.
Device Name	Customized sub controller name, in order to facilitate management. The name consists of 16 digits at most, including English letter, number and special character.

Table 3-1

Step 4 Click “OK”.

After adding, the device is displayed in the list, as shown in Figure 3-8.

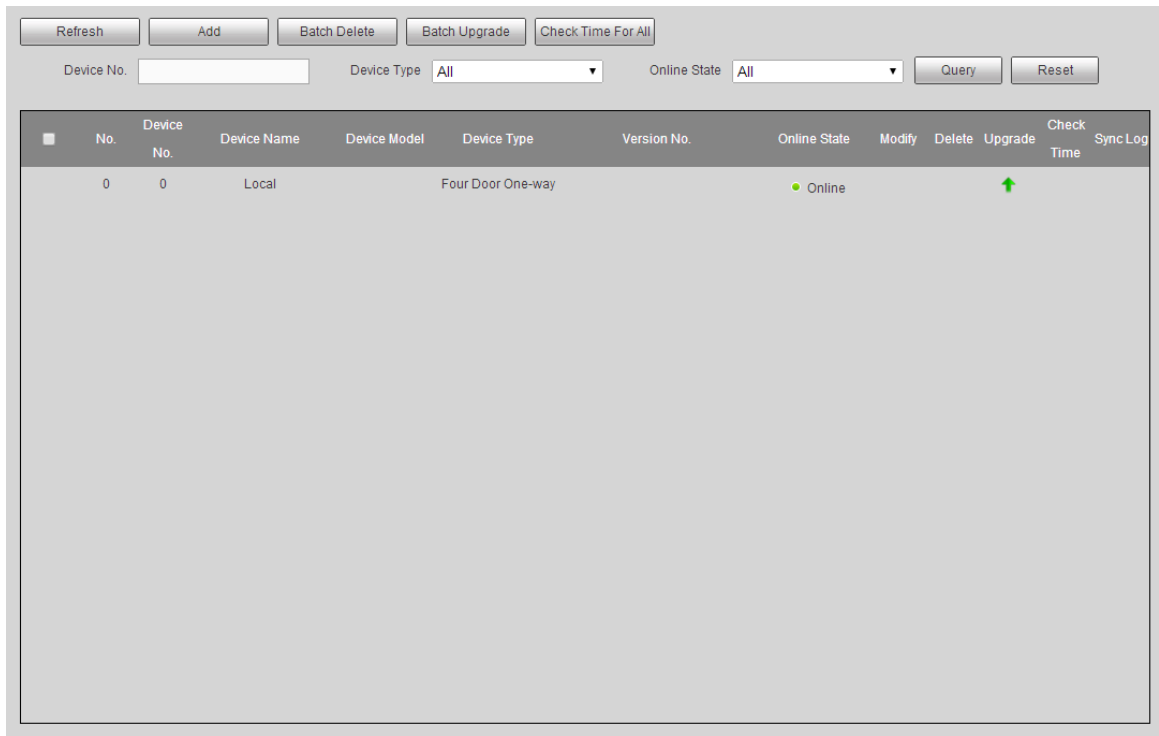




Figure 3-8

3.4.2 Modify

Click  to modify device name of the access controller.


3.4.3 Delete

The access controller can be deleted in two ways.

- Delete: click  to delete it.
- Batch delete: tick the checkboxes before the ones that shall be deleted, and then click “Batch Delete”.

3.4.4 Upgrade

Upgrade online access controllers.


- Upgrade: click  to upgrade the access controller.
- Batch upgrade: tick the checkboxes before the ones that shall be upgraded, and then click “Batch Upgrade”.

 Note


If main access controller is selected, only the reader can be upgraded. To upgrade main program, please select “Setting > System > System Upgrade”. Please refer to “3.10.5 System Upgrade” for details.

3.4.5 Check Time

Check the time of online access controllers and ensure that it is consistent with the time of main access controller.

- Check time: click , in order that the time of this access controller synchronizes with the time of main access controller.
- Check time for all: click “Check Time for All”. The time of all online access controllers synchronizes with the time of main access controller.

3.4.6 Synchronize Log

Click , in order that offline log info of access controller is synchronized to main access controller.

3.4.7 Query

Query access controllers according to device no., device model and online status.

Input query conditions; click “Query” to display results.

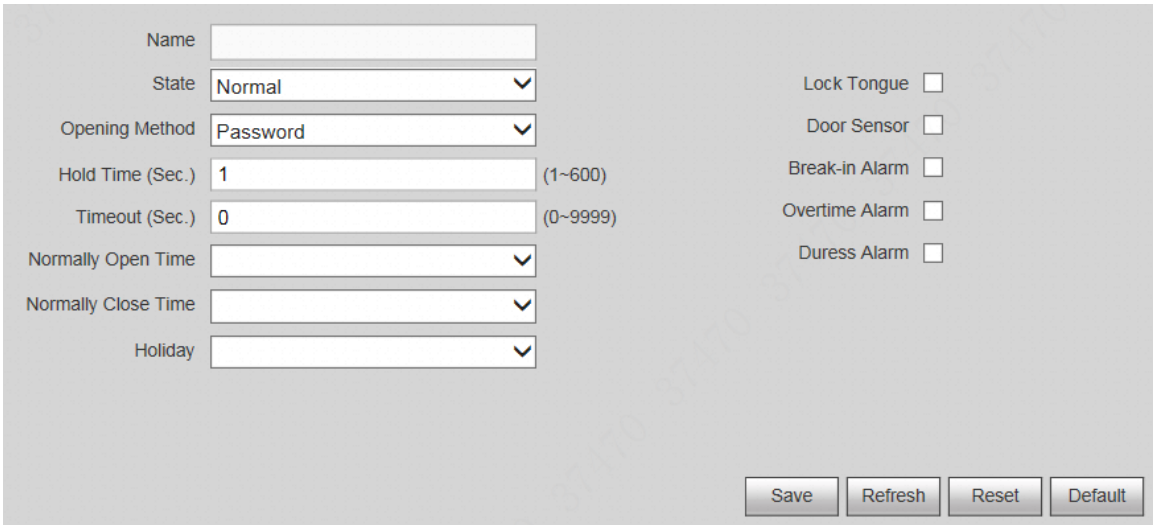
Click “Reset”; display results according to default condition value of the system.

3.5 Set Door Parameters

Configure parameters of doors under access controller.

Step 1 Select “Access Control > Door Parameters”.

The system displays “Door Parameters” interface, as shown in Figure 3-9.





Name	<input type="text"/>	
State	Normal	Lock Tongue <input type="checkbox"/>
Opening Method	Password	Door Sensor <input type="checkbox"/>
Hold Time (Sec.)	1 (1~600)	Break-in Alarm <input type="checkbox"/>
Timeout (Sec.)	0 (0~9999)	Overtime Alarm <input type="checkbox"/>
Normally Open Time	<input type="text"/>	Duress Alarm <input type="checkbox"/>
Normally Close Time	<input type="text"/>	
Holiday	<input type="text"/>	

Save Refresh Reset Default

Figure 3-9

Step 2 Select a door in the device tree in the left, configure door parameters and refer to Table 3-2 for details.

Parameter	Description	
Name	Display the name of present door.	
State	Select door state, which won't be affected after reboot. <ul style="list-style-type: none"> • Normal: open the door in a preset way. • Normally closed: the door is normally closed and cannot be opened in any way. • Normally open: the door is normally open and can be entered directly. 	
Opening Method	Select an opening method. Only the selected method works, while other methods are invalid. <ul style="list-style-type: none"> • Password: open the door with password only. • Card: open the door with card. • Card and password: open the door with card plus password. • Period: open the door with corresponding methods within the preset period. • Fingerprint: open the door with fingerprint only. • Card or password or fingerprint: open the door with one of the three methods. • Card and fingerprint: open the door with card plus fingerprint. 	
Hold Time (Sec.)	Hold time of an open door. The door is closed automatically after hold time.	
Timeout (Sec.)	When "overtime alarm" is enabled, upload an alarm if exceeding opening time.	
Normally Open Time	The door is normally open within the set time.	 Note In the drop-down list, select a synchronously set period in Smart PSS client. Disabled: period control is not enabled.
Normally Close Time	The door is normally closed within the set time.	
Holiday	Holiday period has the highest priority. During holiday after selection, it is valid to swipe card during holiday. Beyond this period, it is valid to swipe card according to normal rules.	
Lock Tongue	Tick the checkbox to enable lock tongue function.	
Door Sensor	Tick the checkbox to enable door sensor function. Judge and alarm according to door sensor status.	
Break-in Alarm	Tick the checkbox to enable break-in alarm function. Upload an alarm in case that door sensor is opened when the door is not opened normally.	 Note While the alarm is enabled, corresponding door sensor shall be enabled. Otherwise, door status cannot be judged.
Overtime Alarm	Tick the checkbox to enable overtime alarm function. Upload an alarm in case that opening time exceeds "overtime".	

Parameter	Description
Duress Alarm	Tick the checkbox to enable duress alarm function. In case of duress, open the door with duress card, duress password or duress fingerprint. The door will be opened normally, but the system will upload alarm info to management center.

Table 3-2

Step 3 Click “Save” to complete parameter setting.

 Note

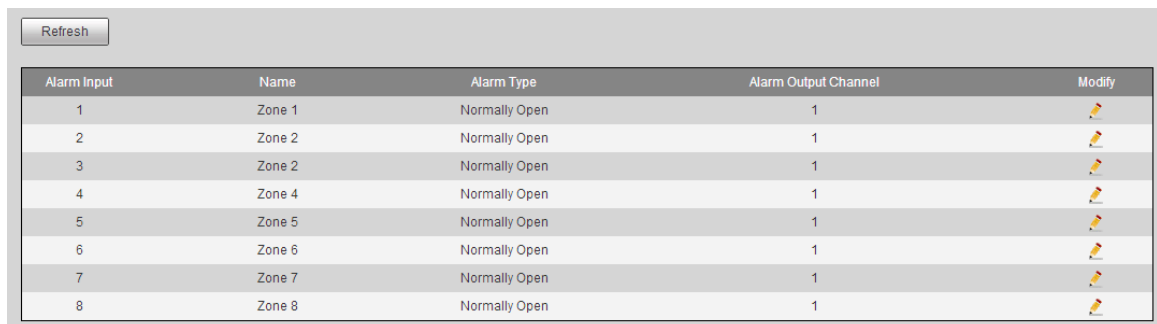
If main access controller connects Smart PSS client, relevant parameters will be synchronized with the client. Parameters modified in the client will also be synchronized with main controller.

3.6 Set Alarm Linkage

Main access controller supports 8-channel alarm input and output. Set alarm linkage output at this interface.

Step 1 Select “Access Control > Alarm Linkage”.

The system displays “Alarm Linkage” interface, as shown in Figure 3-10.












Alarm Input	Name	Alarm Type	Alarm Output Channel	Modify
1	Zone 1	Normally Open	1	
2	Zone 2	Normally Open	1	
3	Zone 2	Normally Open	1	
4	Zone 4	Normally Open	1	
5	Zone 5	Normally Open	1	
6	Zone 6	Normally Open	1	
7	Zone 7	Normally Open	1	
8	Zone 8	Normally Open	1	

Figure 3-10

Step 2 Click  .

The system pops up “Modify” dialogue box, as shown in Figure 3-11.

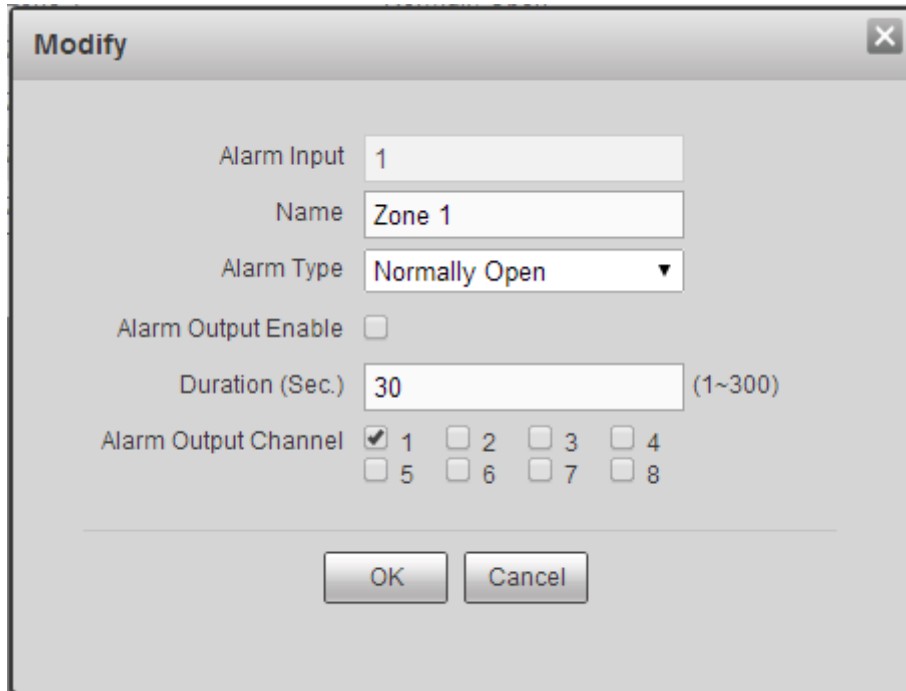


Figure 3-11

Step 3 Configure parameters.

Step 4 Parameter	Description
Alarm Input	Display the present alarm input.
Name	Customize alarm input name.
Alarm Type	Alarm type is consistent with the terminal.
Alarm Output Enable	Tick the checkbox to enable alarm output, so as to upload alarm to the platform synchronously.
Duration (Sec.)	Alarm duration. The alarm will disappear after this duration.
Alarm Output Channel	Select alarm output channel, so as to output the alarm in designated channel.

Step 5 Table 3-3 for details.

Parameter	Description
Alarm Input	Display the present alarm input.
Name	Customize alarm input name.
Alarm Type	Alarm type is consistent with the terminal.
Alarm Output Enable	Tick the checkbox to enable alarm output, so as to upload alarm to the platform synchronously.
Duration (Sec.)	Alarm duration. The alarm will disappear after this duration.
Alarm Output Channel	Select alarm output channel, so as to output the alarm in designated channel.

Table 3-3

Step 6 Click "OK" to complete setting.

3.7 Set Network

3.7.1 TCP/IP

Set IP address and DNS server of main access controller; ensure that it is interconnected with other devices in the network.

Step 1 Select “System Setup > Network Setting > TCP/IP”.

The system displays “TCP/IP” interface, as shown in Figure 3-12.

The screenshot shows a network configuration window with the following fields and values:


- Default NIC: NIC 1
- NIC: NIC 1
- MAC Address: 3c...
- Mode: Static, DHCP
- IP Address: [Empty]
- Subnet Mask: [Empty]
- Default Gateway: [Empty]
- First DNS Server: 8 . 8 . 8 . 8
- Second DNS Server: 8 . 8 . 4 . 4

Buttons at the bottom: OK, Refresh, Default.


Figure 3-12

Step 2 Set TCP/IP parameters.

Parameter	Description
Default NIC	They cannot be modified. Default one is NIC 1.
MAC Address	Display MAC address of the device.

Step 3 Parameter	Description
Mode	<ul style="list-style-type: none"> ● Static Set IP address, subnet mask and gateway manually. ● DHCP Obtain IP function automatically. When DHCP is enabled, IP address, subnet mask and gateway cannot be set. <ul style="list-style-type: none"> ◇ If present DHCP takes effect, IP/subnet mask/gateway displays the value obtained by DHCP. Otherwise, they display 0. ◇ To view the manual set IP, if DHCP is not effective, please disable DHCP; display IP info that is not obtained by DHCP. If DHCP takes effect, previous IP info cannot be displayed by disabling DHCP, but IP parameters shall be set again.
IP Address	Input numbers to modify IP address; set subnet mask and default gateway corresponding to IP address.  Note IP address and default gateway shall be in the same network segment.
Subnet Mask	
Default Gateway	
First DNS Server	IP address of DNS server.
Second DNS Server	IP address of alternate DNS server.

Step 4 Table 3-4 for details.

Parameter	Description
Default NIC	They cannot be modified. Default one is NIC 1.
MAC Address	Display MAC address of the device.
Mode	<ul style="list-style-type: none"> ● Static Set IP address, subnet mask and gateway manually. ● DHCP Obtain IP function automatically. When DHCP is enabled, IP address, subnet mask and gateway cannot be set. <ul style="list-style-type: none"> ◇ If present DHCP takes effect, IP/subnet mask/gateway displays the value obtained by DHCP. Otherwise, they display 0. ◇ To view the manual set IP, if DHCP is not effective, please disable DHCP; display IP info that is not obtained by DHCP. If DHCP takes effect, previous IP info cannot be displayed by disabling DHCP, but IP parameters shall be set again.
IP Address	Input numbers to modify IP address; set subnet mask and default gateway corresponding to IP address.  Note IP address and default gateway shall be in the same network segment.
Subnet Mask	
Default Gateway	
First DNS Server	IP address of DNS server.

Parameter	Description
Second DNS Server	IP address of alternate DNS server.

Table 3-4

Step 5 Click “OK” to complete setting.

3.7.2 Port

Set the max. connection and every port to visit main access controller through WEB client.

Step 1 Select “System Setup > Network Setting > Port”.

The system displays “Port” interface, as shown in Figure 3-13.

Figure 3-13

Step 2 Configure every port value of the device. Please refer to Table 3-5 for details.

Note

Except “Max Connection”, if other parameters are modified, it shall be rebooted to put them into effect.

Parameter	Description
Max Connection	Max. quantity of users who are allowed to login WEB client and visit main controller at the same time.
TCP Port	Communication port of TCP protocol, to be set according to the user’s actual needs. It is 37777 by default.
UDP Port	User datagram protocol port, to be set according to the user’s actual needs. It is 37778 by default.
HTTP Port	Communication port of HTTP, to be set according to the user’s actual needs. It is 80 by default. To set other numbers, please add the modified port number to the address during login with the browser.
HTTPS Port	Communication port of HTTPS, to be set according to the user’s actual needs. It is 443 by default. Tick “Enable”, representing that HTTPS function is available.

Table 3-5

Step 3 Click “OK” to complete setting.

3.7.3 DDNS

In case of frequent changes in IP address of the device, DDNS (Dynamic Domain Name Server)

dynamically updates the relation between domain name and IP address on DNS server, and ensures that users are able to visit the device through domain name.

Step 1 Select “System Setup > Network Setting > DDNS”.

The system displays “DDNS” interface, as shown in Figure 3-14.

Figure 3-14

Step 2 Tick “Enable”, and configure DDNS parameters according to actual conditions. Please refer to Table 3-6 for details.

Parameter	Description
DDNS Type	Name and address of DDNS server provider. Corresponding relation is as follows:
Host IP	<ul style="list-style-type: none"> • Dyn dns DDNS address is: members.dyndns.org • NO-IP DDNS address is: dynupdate.no-ip.com • CN99 DDNS address is: members.3322.org
Domain Name	Domain name registered by the user at the website of DDNS server provider.
Username	User name and password obtained from DDNS server provider. The user needs to register (including user name and password) at the website of DDNS server provider.
Password	
Update Cycle	The time interval to raise update request after designated DDNS update is enabled. The unit is minute.

Table 3-6

Step 3 After filling in, click “OK”.

Step 4 Enter domain name in PC browser and press [Enter] key.

Configuration is successful if WEB interface is displayed; otherwise, configuration fails.

3.7.4 Register

Register actively. When connecting WAN, report current position to the server designated by the user, so client software visits the device through the server, in order to preview and monitor.

Step 1 Select “System Setup > Network Setting > Register”.

The system displays “Register” interface, as shown in Figure 3-15.

Figure 3-15

Step 2 Tick “Enable”, and enter server address, port and sub-device ID. Please refer to Table 3-7 for details.

Parameter	Description
Host IP	IP address or domain name of the server to be registered.
Port	Auto registration port number of the server.
Sub-device ID	Device ID allocated by the server side.

Table 3-7

Step 3 Click “OK” to complete setting.

3.7.5 P2P

P2P is a private network traversal technology. Scan the QR code, download mobile phone APP, register an account, and thus manage multiple controllers. During easy and convenient use, it is unnecessary to apply for dynamic domain name, carry out port mapping or deploy relay server.



Caution

To use this function, the device shall be connected with WAN, in order to use it normally.

Step 1 Select “System Setup > Network Setting > P2P”.

The system displays “P2P” interface, as shown in Figure 3-16.

Figure 3-16

Step 2 Tick “Enable” to enable P2P function.

Step 3 Click “OK” to complete setting.

After the setting has been completed, “State” becomes “Online”, representing successful P2P registration. Scan QR code with the platform or mobile client, or enter the serial number directly to add the device to the client, in order to manage and operate it.

3.7.6 HTTPS

At HTTPS setting interface, create server certificate or download root certificate, so PC is able to login through HTTPS. In this way, ensure communication data security; guarantee user info and device security with reliable stable technology.

Select “System Setup > Network Setting > HTTPS”. The system displays “HTTPS” interface, as shown in Figure 3-17.

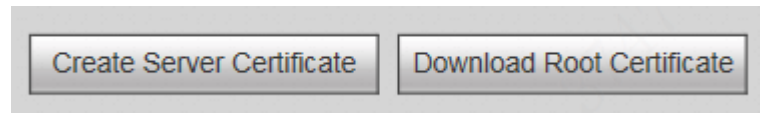


Figure 3-17

 Note

- If you use this function for the first time or change device IP, execute “Create Server Certificate” again.
- If you use HTTPS for the first time after changing computer, execute “Download Root Certificate” again.

Create Server Certificate

Step 1 Click “Create Server Certificate”.

Pop up “Create Server Certificate” dialog box, as shown in Figure 3-18.



Figure 3-18

Step 2 Fill in “Country”, “Province” and relevant info; and then click “OK”.

The system displays “Created successfully”, which means that server certificate has been created successfully, as shown in Figure 3-19.

 Note

“IP or Domain Name” shall be consistent with device IP or domain name.

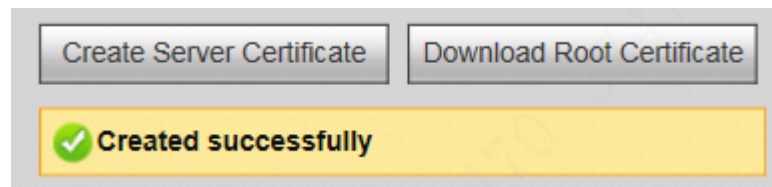


Figure 3-19

Download Root Certificate

Step 1 Click “Download Root Certificate”.

Pop up “File Download” dialog box, as shown in Figure 3-20.

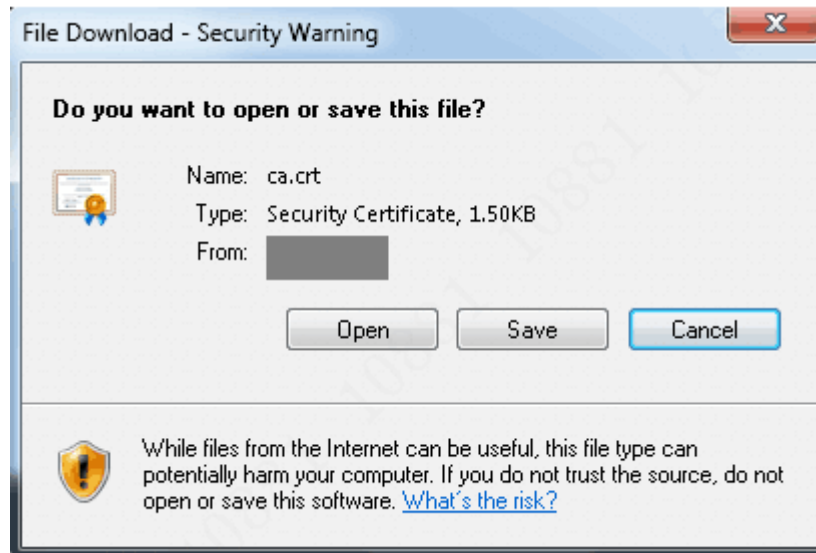


Figure 3-20

Step 2 Click “Open”.

Pop up “Certificate” dialog box, as shown in Figure 3-21.

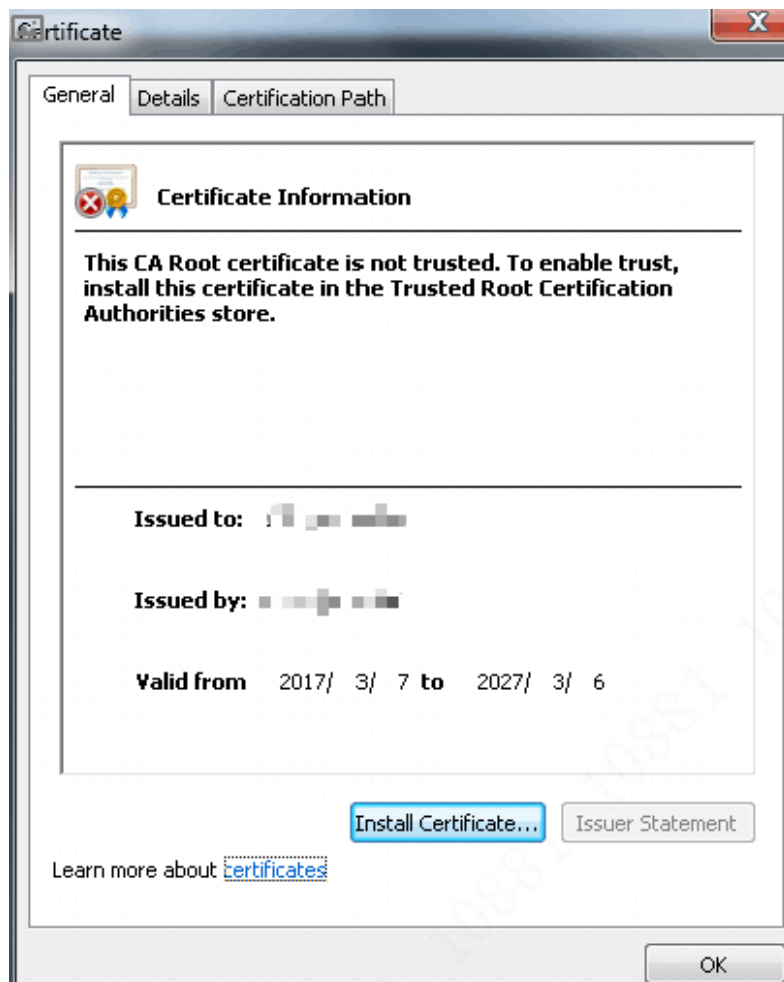


Figure 3-21

Step 3 Click “Install Certificate”.

Pop up “Certificate Import Wizard” dialog box, as shown in Figure 3-22.



Figure 3-22

Step 4 Click "Next".

The system displays "Certificate Store" interface, as shown in Figure 3-23.

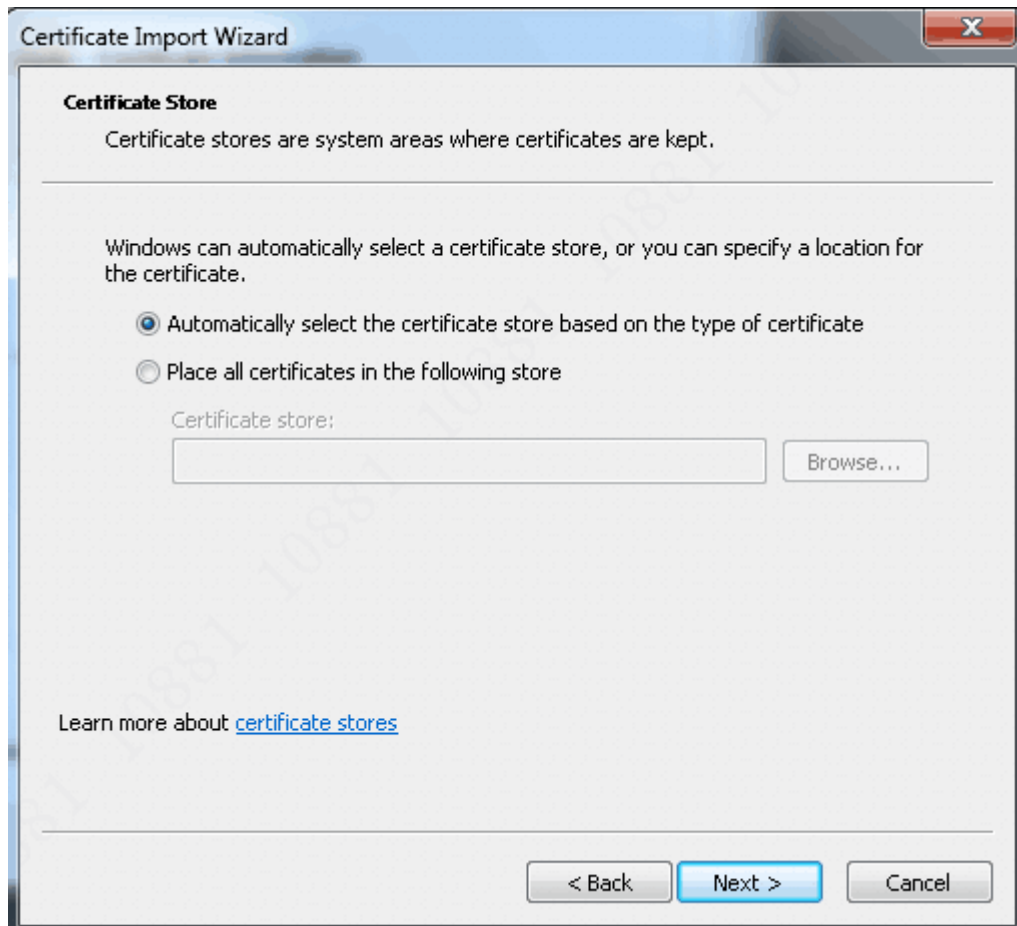


Figure 3-23

- Step 5 Select "Automatically select the certificate store based on the type of certificate", and click "Next". The system displays "Completing the Certificate Import Wizard" interface, as shown in Figure 3-24.

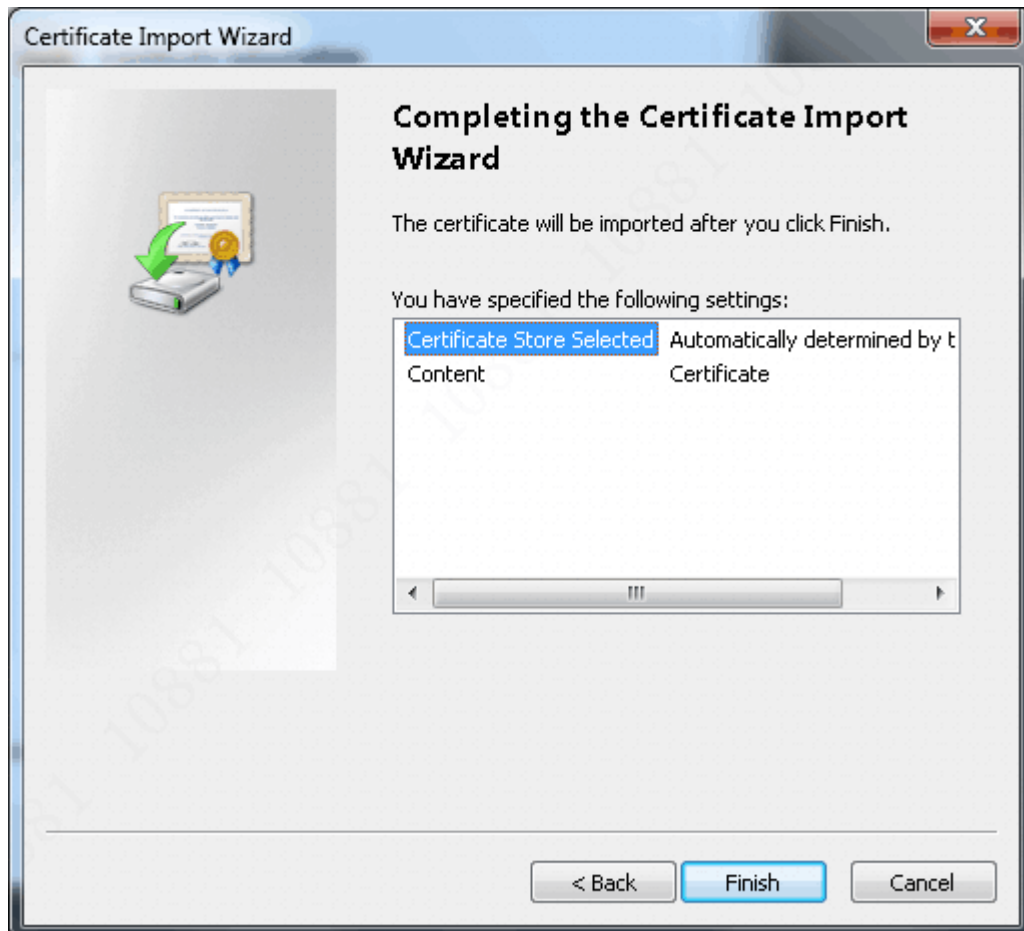


Figure 3-24

Step 6 Click “Finish”.

Pop up “The import was successful” dialog box, and the certificate downloading has been finished, as shown in Figure 3-25.

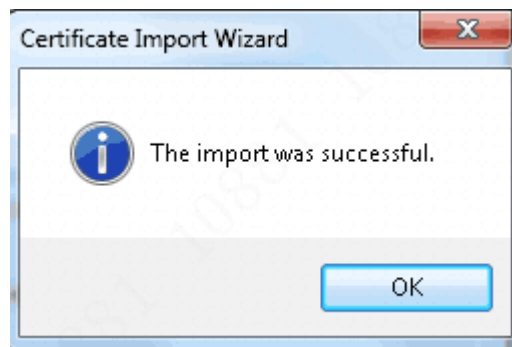


Figure 3-25

Set HTTPS Port No.

Create server certificate or download root certificate and set port number.

Step 1 Select “System Setup > Network Setting > Port”.

The system displays “Port” interface, as shown in Figure 3-26.

Max Connection	<input type="text" value="20"/>	(1~999)
TCP Port	<input type="text" value="37777"/>	(1025~65535)
UDP Port	<input type="text" value="37778"/>	(1025~65535)
HTTP Port	<input type="text" value="80"/>	(1~65535)
HTTPS Port	<input type="text" value="443"/>	(1~65535) <input type="checkbox"/> Enable
<input type="button" value="OK"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>		


Figure 3-26

Step 2 Enter “HTTPS Port”, which is “443” by default, select “Enable” and click “OK”.

Use HTTPS

Use HTTPS to login.

Enter <https://xx.xx.xx.xx:port> in the browser, and pop up login interface.

 Note

- “xx.xx.xx.xx” corresponds to your IP or domain name.
- “Port” corresponds to HTTPS port. In case of default port 443, it is unnecessary to add “.port”, just use <https://xx.xx.xx.xx>.

3.8 User Management

Add and delete users, modify password and set the Email to retrieve admin password.

3.8.1 Add User

Step 1 Select “System Setup > User Management”.

The system displays “User Management” interface, as shown in Figure 3-27.

No.	Username	Group Name	Remark	Modify	Delete
1	admin	admin	admin's account		

Figure 3-27

Step 2 Click “Add”.

Pop up “Add” dialog box, as shown in Figure 3-28.

Add

Username

Password

Low Medium High

Password shall be at least 8 digits, and shall at least include two types, including number, letter and common character

Confirm Password

Remark

OK Cancel

Figure 3-28

Step 3 Enter “Username”, “Password”, “Confirm Password” and “Remark”.

Step 4 Click “OK” to complete adding.

3.8.2 Modify Password

Modify password of corresponding user.

Step 1 At “User Management” interface, click .

Pop up “Modify” dialog box, as shown in Figure 3-29.

Modify

Username

Remark

Bind Email

Modify Password

OK Cancel

Figure 3-29

Step 2 Tick “Modify Password”, and enter “Old Password”, “New Password” and “Confirm

Password”.

Step 3 Click “OK” to complete modification.

3.8.3 Set Email

Set the reserved Email to reset admin password.

 Note

Only admin user supports this function.


Step 1 At “User Management” interface, click .

Pop up “Modify” dialog box, as shown in Figure 3-29.

Step 2 Tick “Bind Email” and enter the Email.

Step 3 Click “OK” to complete setting.

3.8.4 Delete User

At “User Management” interface, click  to delete ordinary users.

3.9 Safety Management

3.9.1 IP Authority

In order to strengthen device network security and protect device data, set IP authority of other devices to visit main access controller. IP authority strategy includes allowlist and blocklist.

Step 1 After allowlist is enabled, only devices in the allowlist can login WEB interface successfully.

Step 2 After blocklist is enabled, devices in the blocklist will fail to login WEB interface.

Step 3 Select “System Setup > Safety Management > IP Authority”.

The system displays “IP Authority” interface, as shown in Figure 3-30.

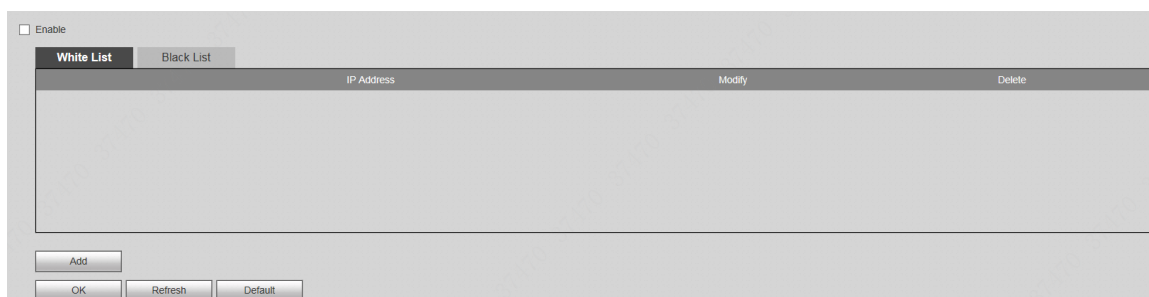


Figure 3-30

Step 4 Tick “Enable”.

The system displays allowlist and blocklist checkboxes.

Step 5 Add allowlist or blocklist.

1. Select “Allow List” or “Block List”.
2. Click “Add”.

The system displays “Add” interface, as shown in Figure 3-31.

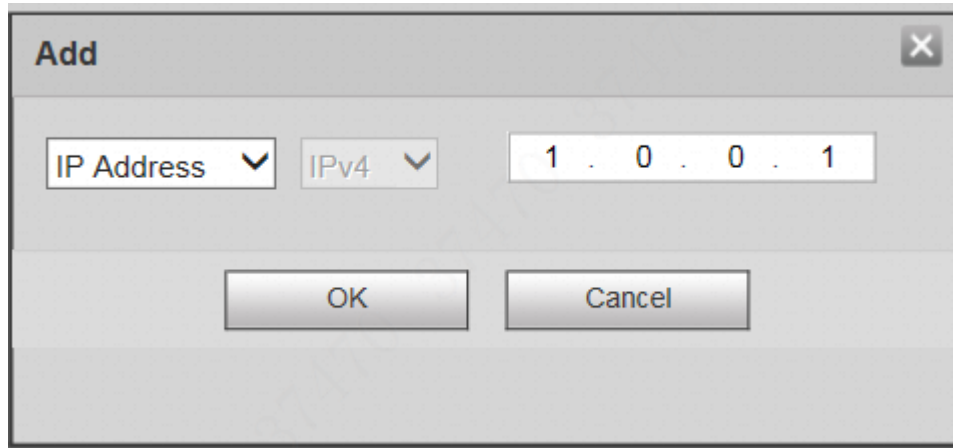


Figure 3-31

- Configure IP address info. Please refer to Table 3-8 for details.



The system supports max. 64 IP addresses.

Parameter	Description
IP Address	Click dropdown list, and select the mode of adding. <ul style="list-style-type: none"> IP address: enter IP address of blocklist or allowlist. IP segment: enter IP segment range of blocklist or allowlist. Multiple IP hosts can be added simultaneously.
IPv4	IP address adopts IPv4 format, such as 172.16.5.10.

Table 3-8

- Click “OK”.

The system returns to “IP Authority” interface.

Step 6 Click “OK” to complete setting.

- IP host in the allowlist can login WEB interface of the device successfully.
- If IP host in the blocklist logs in the WEB interface, the system shows that it has been added to blocklist and login fails.

3.9.2 SSH

For the purpose of network safety, by default, prohibit visiting the device through SSH protocol. Please enable it when necessary.

Step 1 Select “System Setup > Safety Management > SSH”.

The system displays “SSH” interface, as shown in Figure 3-32.

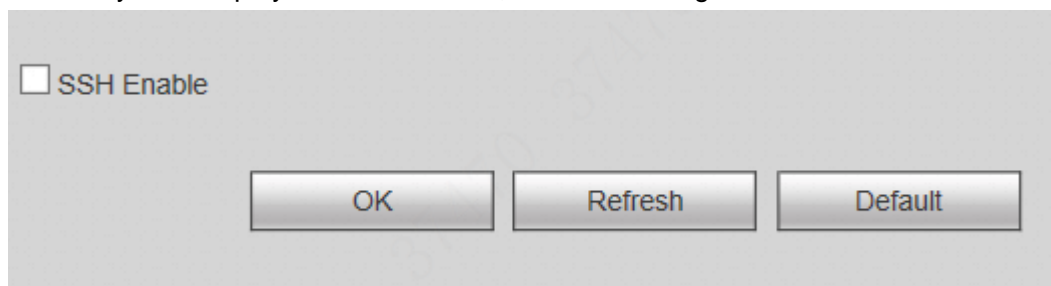


Figure 3-32

Step 2 Tick “SSH Enable” to enable SSH.

Step 3 Click “OK” to complete setting.

3.10 Maintenance

This part introduces date setting, maintenance, config management, default setting and system upgrade.

3.10.1 Date Setting

Set date format, DST and other parameters of the device.

Step 1 Select “System Setup > Date Setting”.

The system displays “Date Setting” interface, as shown in Figure 3-33.

The screenshot shows the 'Date Setting' configuration page. At the top, there are four dropdown menus: 'Date Format' set to 'Year Month Day', 'Time Format' set to '24-Hour system', 'Date Separator' set to '-', and 'Time Zone' set to 'GMT+08:00'. Below these is the 'System Time' section with input fields for year (2000), month (01), day (31), hour (18), minute (30), and second (10), and a 'Sync with PC' button. A 'DST' checkbox is present and unchecked. Under 'DST', there are radio buttons for 'Date' (selected) and 'Week'. Below are 'Starting Time' (2017 - 01 - 01 00 : 00) and 'Ending Time' (2017 - 01 - 02 00 : 00) input fields. An 'NTP Setting' checkbox is also present and unchecked. Under 'NTP Setting', there are input fields for 'Server' (clock.isc.org), 'Port' (123), and 'Update Cycle' (10), along with a 'Manual Update' button. At the bottom, there are 'OK', 'Refresh', and 'Default' buttons.

Figure 3-33

Step 2 Configure date parameter. Please refer to Table 3-9 for details.

Parameter	Description
Date Format	Set date display format, including Year Month Day, Month Day Year and Day Month Year.
Time Format	Set time display format, including 12-hour system and 24-hour system.
Date Separator	Set date format separator.
Time Zone and System Time	Set present system date, time and time zone of access controller. Click “Save”.
DST	Tick “DST” to enable it; select “Date” or “Week”.
Starting Time	Set starting time of DST.
Ending Time	Set ending time of DST.
NTP Setting	Tick “NTP Setting” to enable NTP update function.

Parameter	Description
Server	Enter domain name or IP address of NTP server; click “Manual Update” to synchronize the time of the device and NTP server.
Port	Set port no. of NTP server.
Update Cycle	The time interval of updating time between device and NTP server. Maximum update cycle is 65,535 minutes.

Table 3-9

Step 3 Click “OK” to complete setting.

3.10.2 Maintenance

When the device has been working for a long time, set the device to reboot automatically within an idle time period, in order to improve its operating speed.

Step 1 Select “System Setup > Maintenance”.

The system displays “Maintenance” interface, as shown in Figure 3-34.

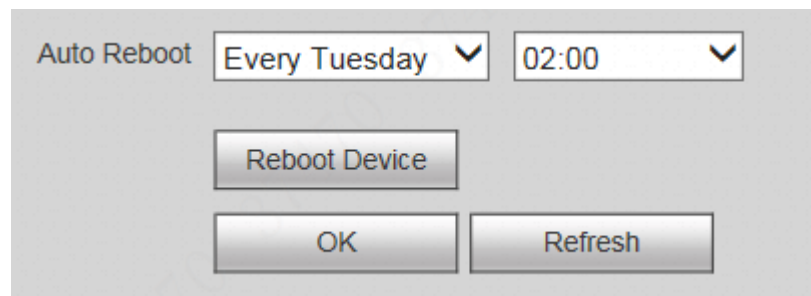


Figure 3-34

Step 2 Select “Auto Reboot” time.

 Note

Default “Auto Reboot” time is 02:00 every Tuesday.

Step 3 Click “OK” to complete auto maintenance setting.

 Note

Click “Reboot Device” to reboot the device.

3.10.3 Config Management

Import or export system config files. When multiple devices need the same parameter setting, use the config backup file.

Select “System Setup > Config Management”. The system displays “Config Management” interface, as shown in Figure 3-35.

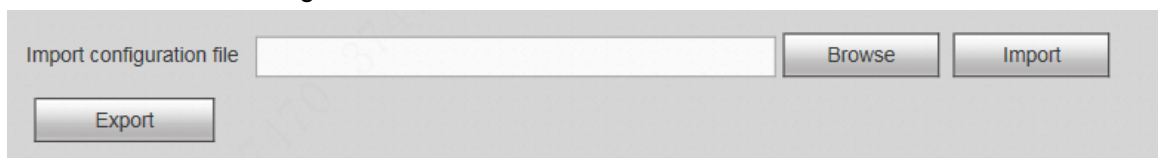


Figure 3-35

Config Export

Step 1 Click “Export”.

Pop up “File Downloading” dialog box.

Step 2 Click “Save”, select a path and save all config files of WEB interface.

Config Import

Step 1 Click “Browse” to select the needed config file.

Step 2 Click “Import” to import system config of backup data.

3.10.4 Default Setting

The system restores default config status which is set when leaving the factory (specific items can be selected on the menu).

Select “System Setup > Default”, as shown in Figure 3-36.

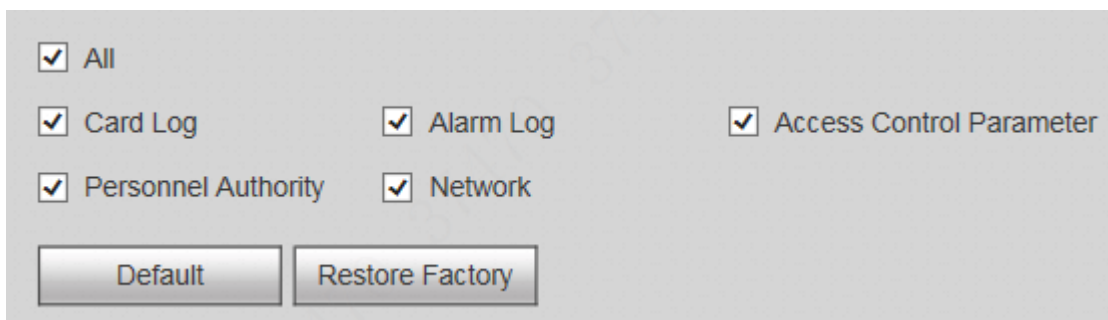


Figure 3-36

- Tick the items that shall be restored to default, and click “Default”.
- Click “Restore Factory”, so all system parameters are restored to factory defaults.

3.10.5 System Upgrade



Caution

- During upgrade, please don't cut off power supply or network; don't reboot or turn off the device.
- Please select the correct upgrade file. Wrong program may lead to failure of the device.

Select “System Setup > Upgrade”. The system displays “System Upgrade” interface, as shown in Figure 3-37.

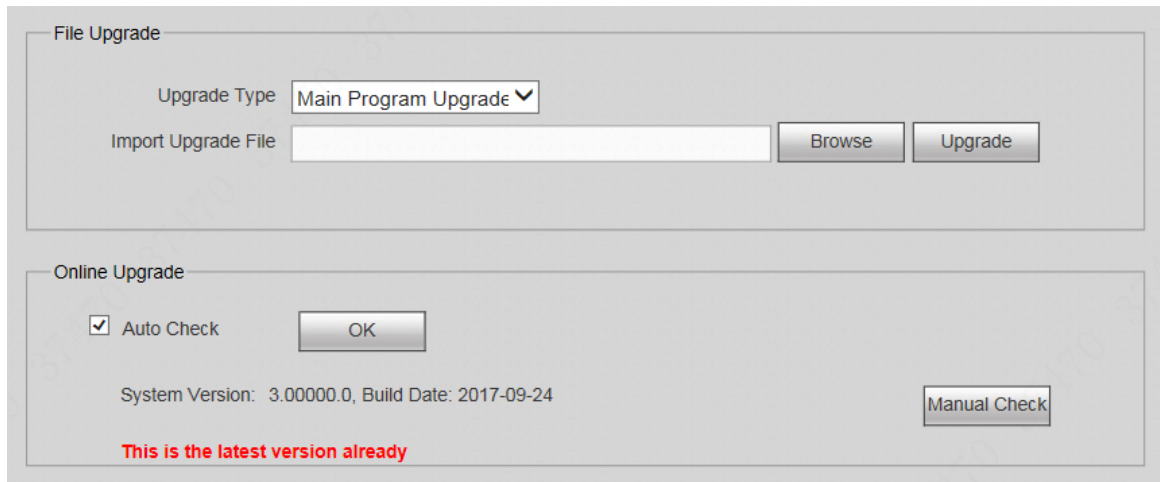


Figure 3-37

3.10.5.1 File Upgrade

Upgrade the system with *.bin file.

Step 1 Select “Upgrade Type”, click “Browse” and select upgrade file.

Step 2 Click “Upgrade” to start to upgrade.

After completing upgrade, the device reboots automatically.

3.10.5.2 Online Upgrade

Through interaction with the cloud, check the latest version and realize online upgrade.

Step 1 Check version.

- Tick “Auto Check”, click “OK” to enable auto check, so the device interacts with the cloud regularly and checks whether there is a new version. In case of new version, “System Setup” tab at WEB interface shows red point, and “System Setup > System Upgrade” tab shows the quantity of upgradable files.
- Click “Manual Check” to view the latest version of this device on the cloud in a real-time way.
 - ◇ If this is the latest version already, the interface prompts “This is the latest version already”.
 - ◇ If a new version is found, the system will prompt new version info, release date and relevant modifications.

Step 2 In case of new version, click “Upgrade Now” to upgrade.

After completing upgrade, the device reboots automatically.

3.11 Information

3.11.1 Version Info

Select “Information > Version Info”. The system displays “Version Info” interface, to show “Model”, “Name”, “MAC Address”, “S.N.”, “Web Version No.” and “System Version No.”.

3.11.2 Online User

Select "Information > Online User". The system displays "Online User" interface, to show the info about current user who has logged into WEB, including "Username", "User Group", "IP Address" and "User Login Time".

4

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 part mainly introduces quick configuration. For details, please refer to matching Smart PSS user's manual.

 Note

Smart PSS client has different interfaces depending on the versions. Please refer to actual interface.

4.1 Log in Client

Install the matching Smart PSS client, and double click  to run. Carry out initialization configuration according to interface prompts and complete login.

4.2 Add Access Controller

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

4.2.1 Auto Search

Devices are required to be in the same network segment.

Step 1 In “Devices” interface, click “Auto Search”, as shown in Figure 4-1.

The system displays “Auto Search” interface, as shown in Figure 4-2.

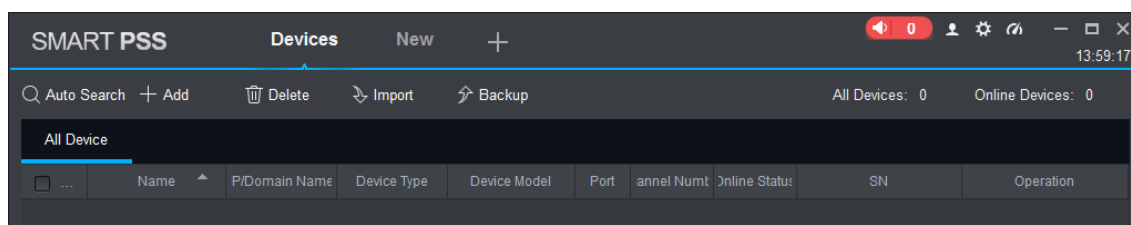


Figure 4-1

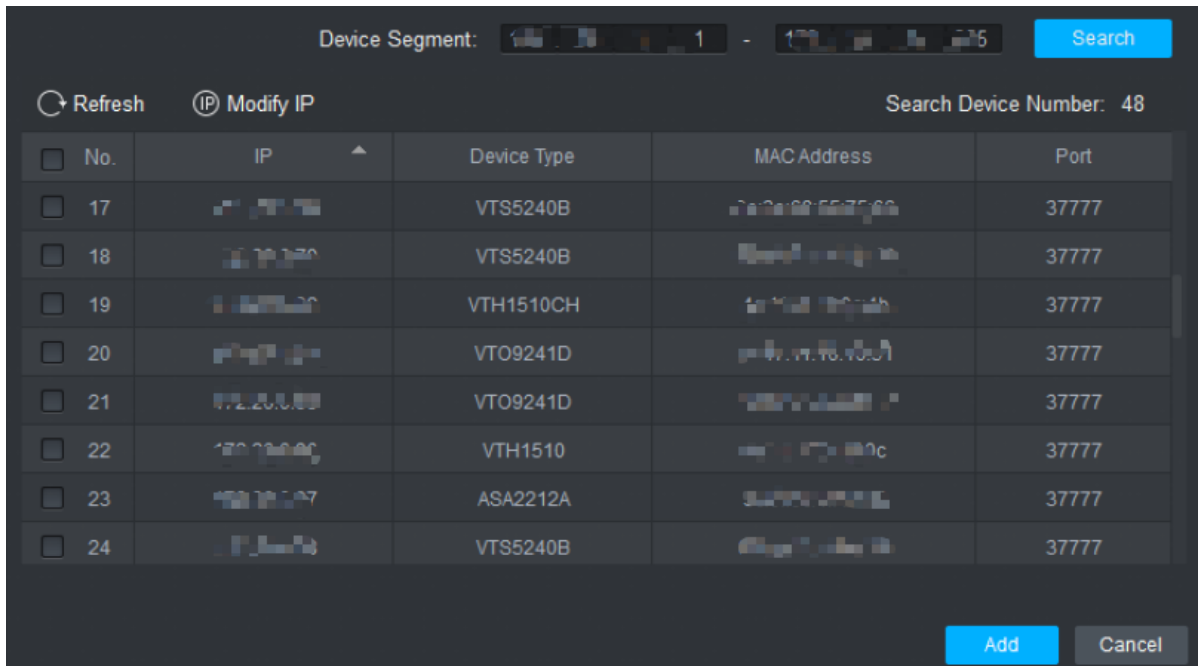


Figure 4-2

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” dialog box, as shown in Figure 4-3.

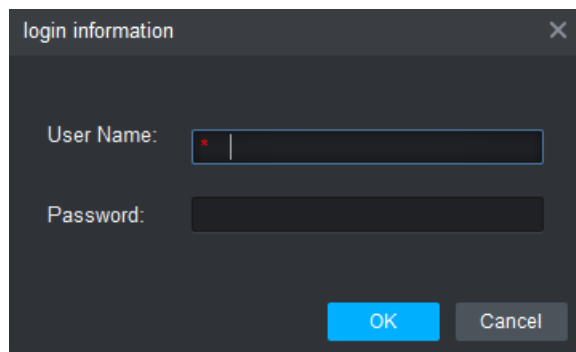


Figure 4-3

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 4-4. Please refer to Table 4-1 for operations.

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”.

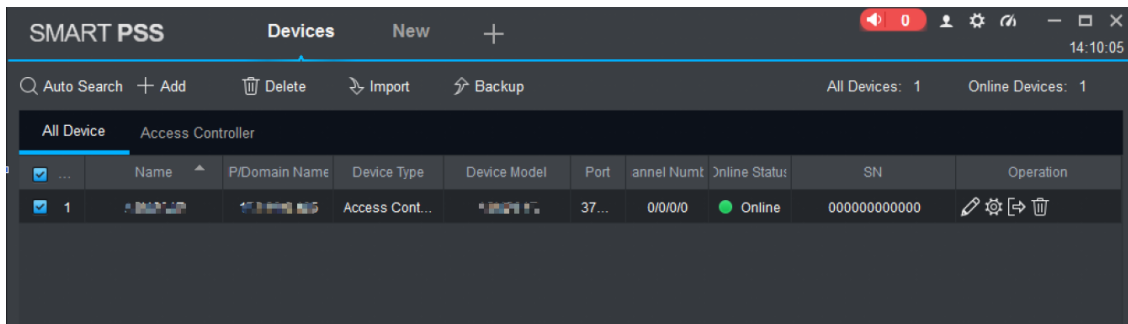


Figure 4-4

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"> 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.

Table 4-1

4.2.2 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 4-5.

The system pops up “Manual Add” interface, as shown in Figure 4-6.

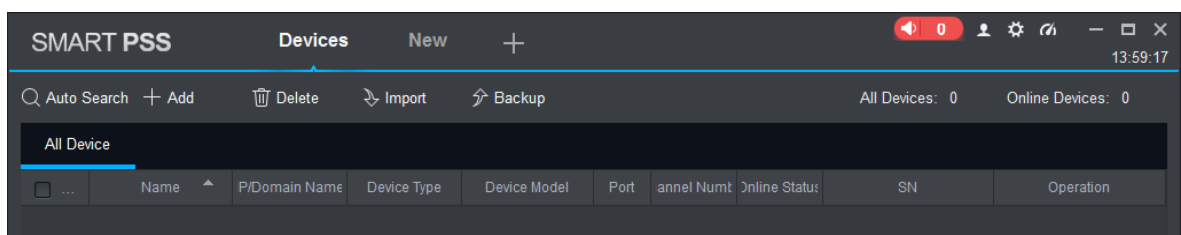


Figure 4-5

Figure 4-6

Step 2 Set device parameters.

Step 3 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.

Table 4-2.

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.

Table 4-2

Step 3 Click "Add" to add a device.

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

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”.

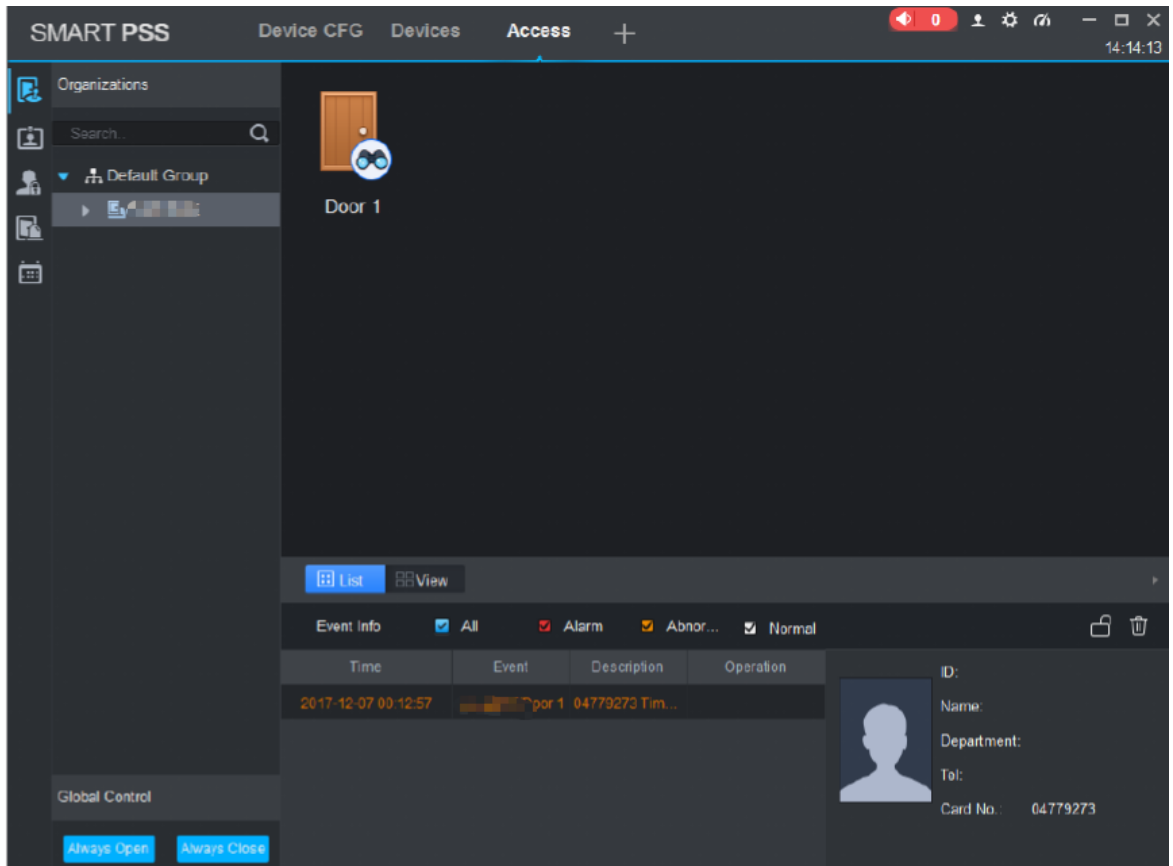


Figure 4-7

4.3 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.

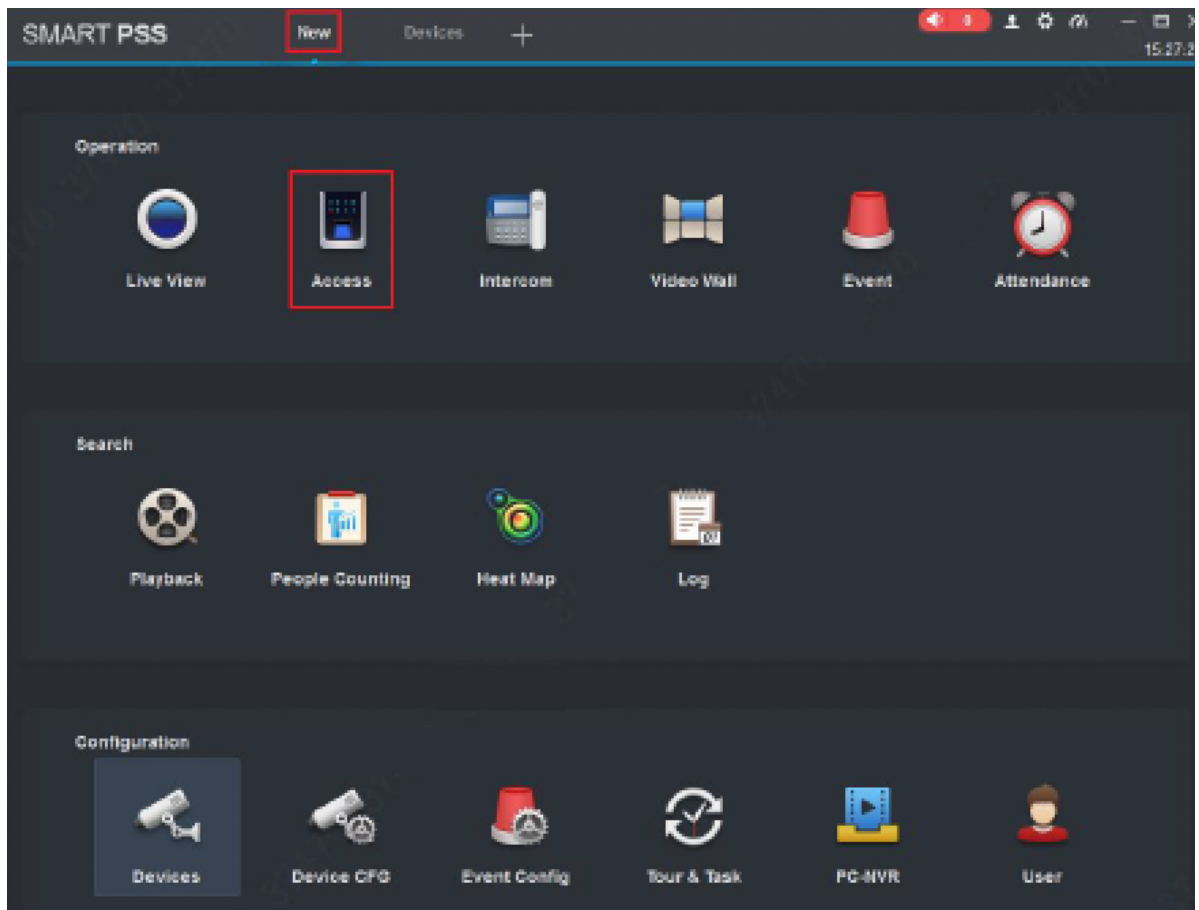


Figure 4-8

4.3.1 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 4-9 and Figure 4-10.

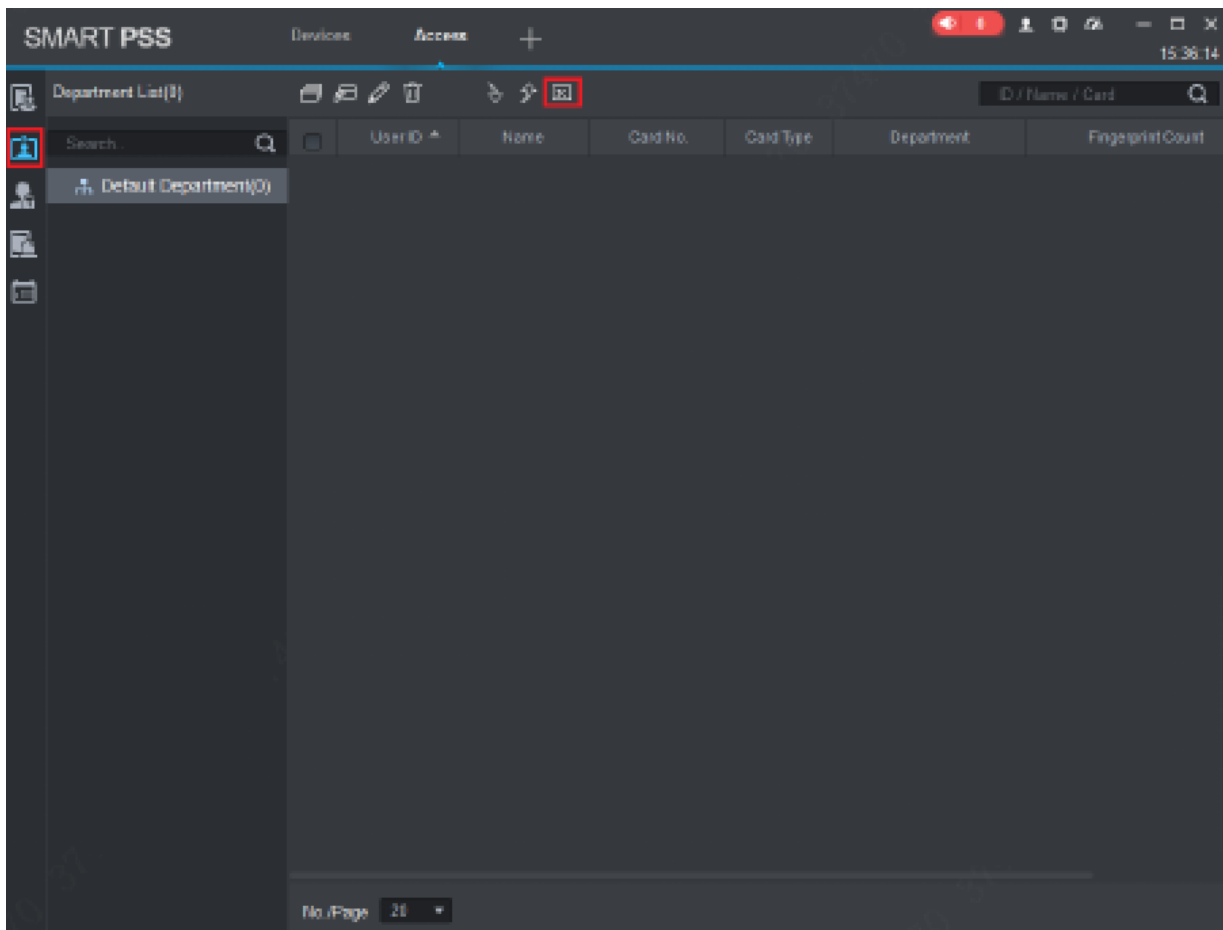


Figure 4-9

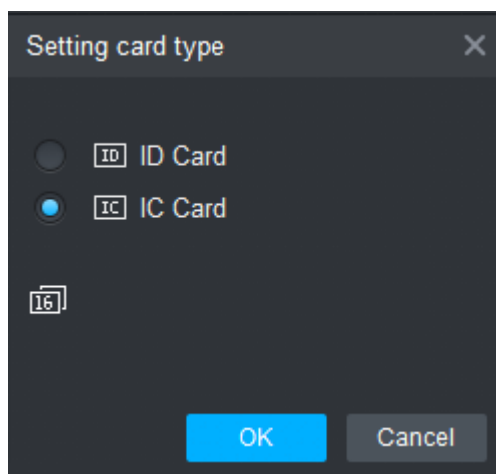




Figure 4-10

4.3.2 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 4-11. The system pops up “Add User” dialog box, as shown in Figure 4-12.

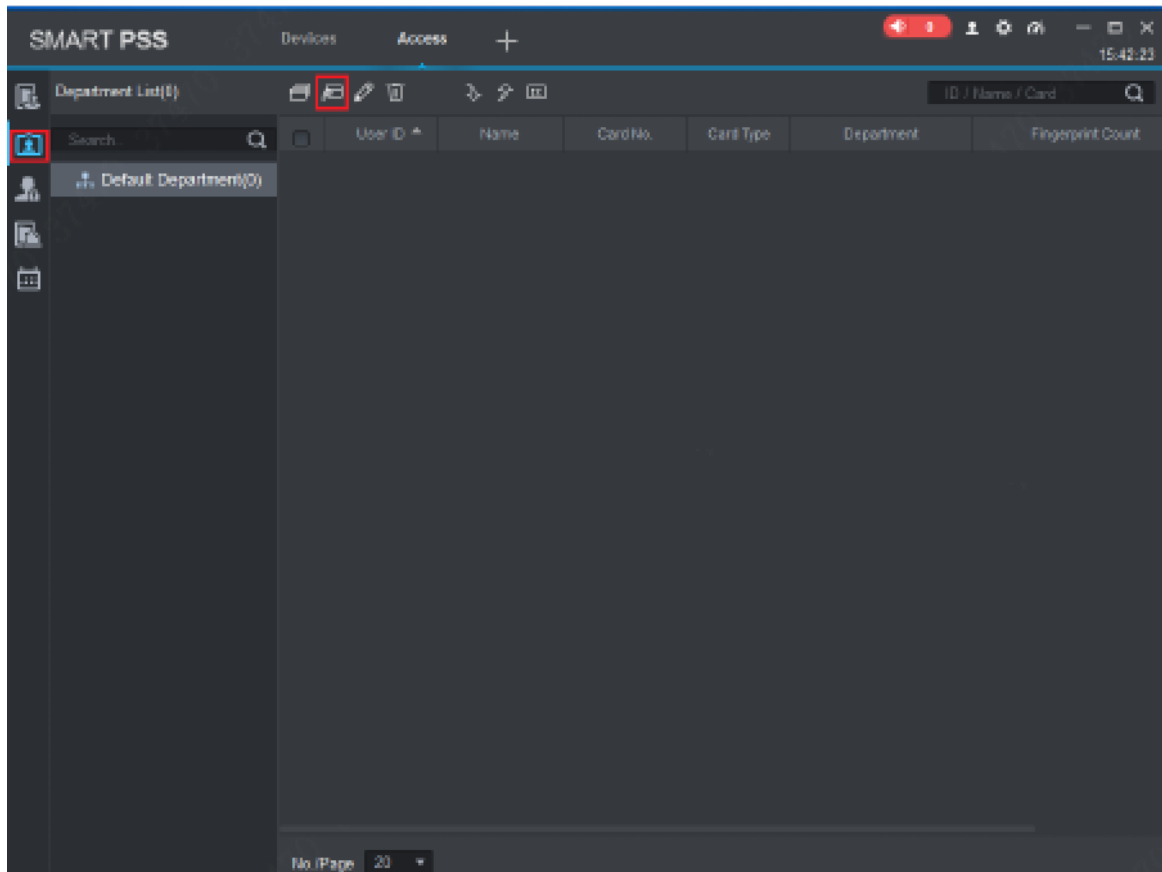


Figure 4-11

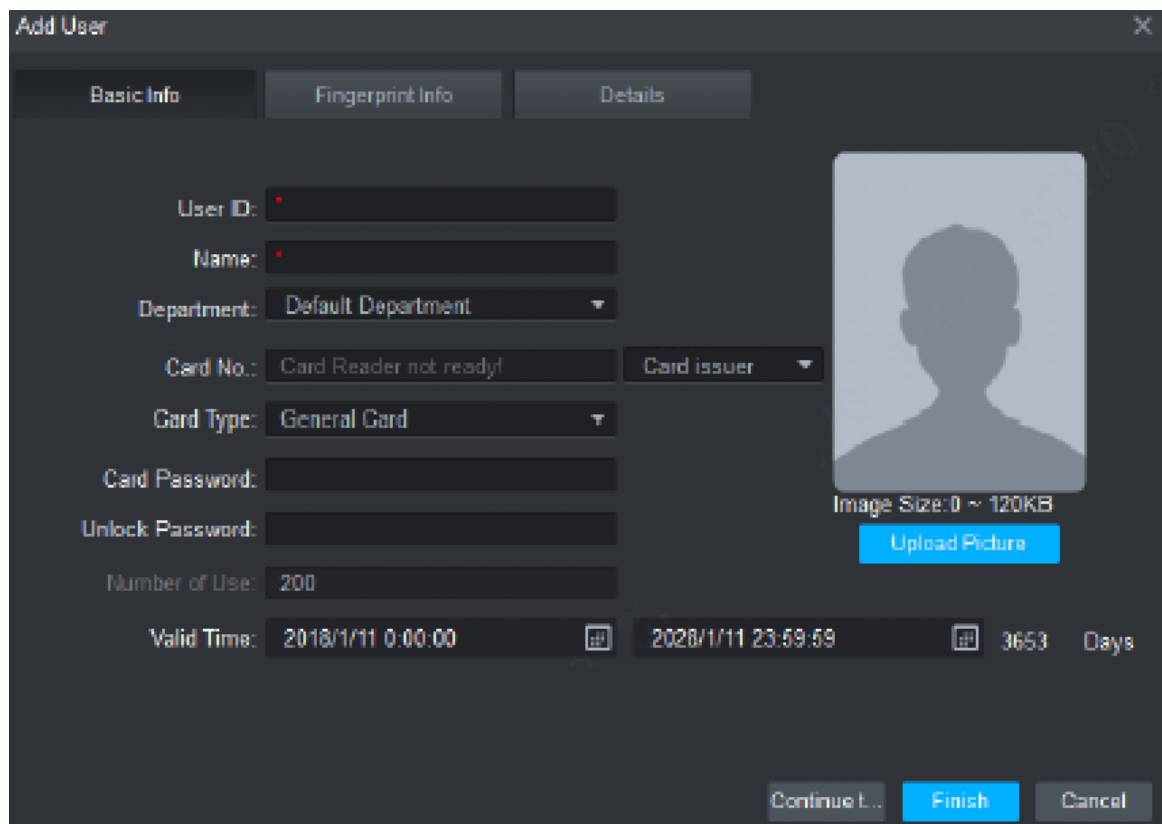


Figure 4-12

Step 2 Add user info manually, including basic info, fingerprint info and details.



Parameter	Description
Basic Info	<ul style="list-style-type: none"> • 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, blacklist 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. <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"> • Max. 2 fingerprints for every person. • Support to enter fingerprint name.
Details	Fill in detailed user info according to interface parameters.

Table 4-3

Step 3 Click “Finish” to finish adding the users.

4.4 Add Door Group

Divide doors into groups, combine and manage them together.

Step 1 In “Access” interface, click , and then click “Access Level”, as shown in Figure 4-13.

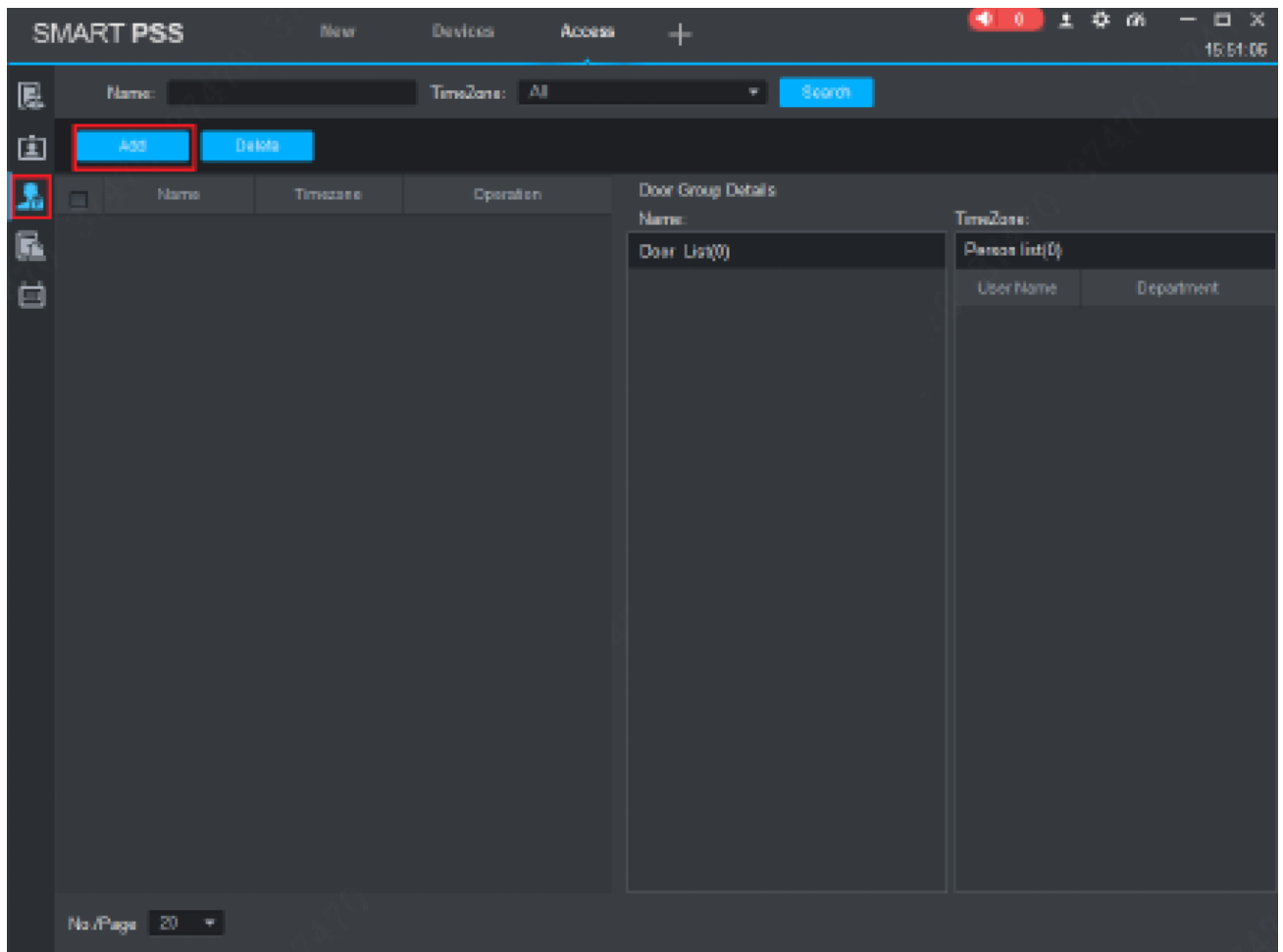


Figure 4-13

Step 2 Click “Add”.

The system pops up “Add Door Group” dialog box, as shown in Figure 4-14.

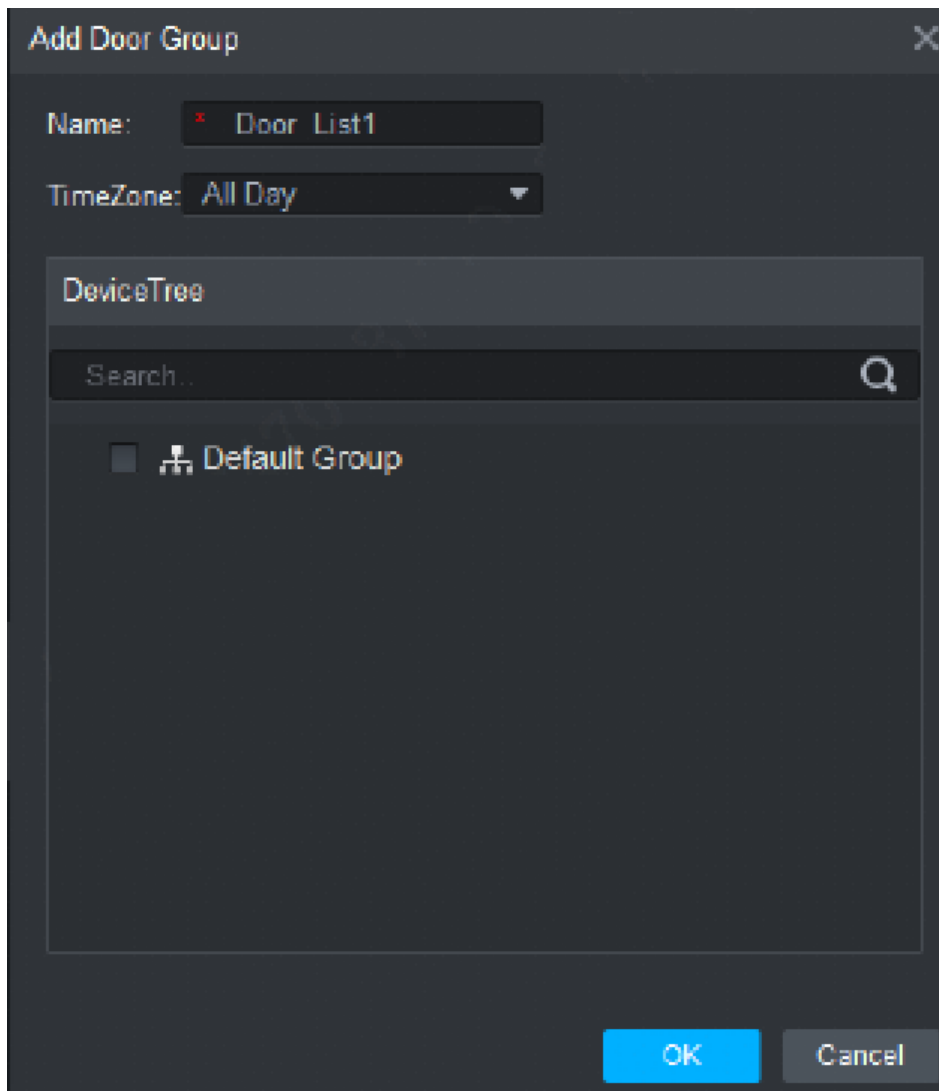


Figure 4-14

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


Step 4 Click "OK" to complete adding.

4.5 Authorize

Grant users authorities according to door group and user.

4.5.1 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 4-15.

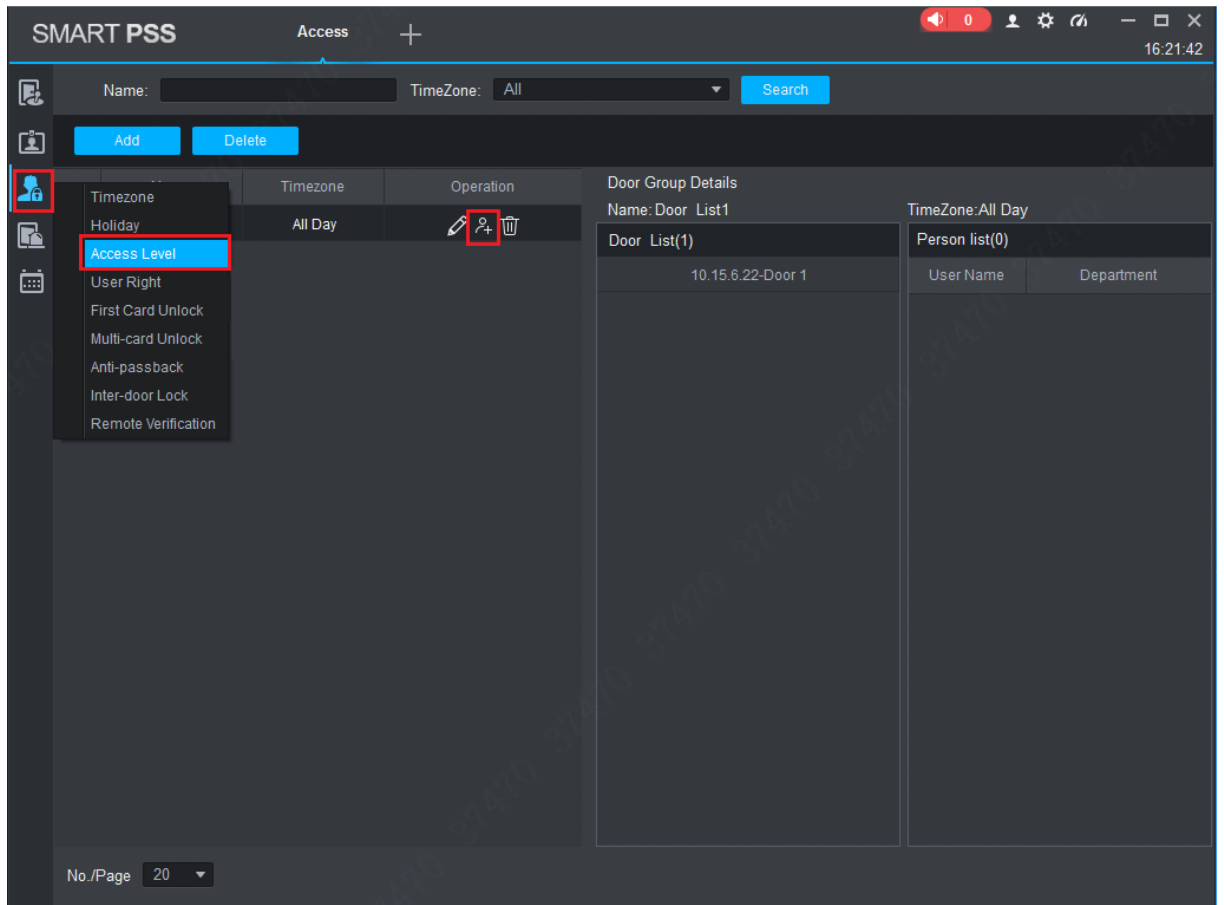


Figure 4-15

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 4-16.

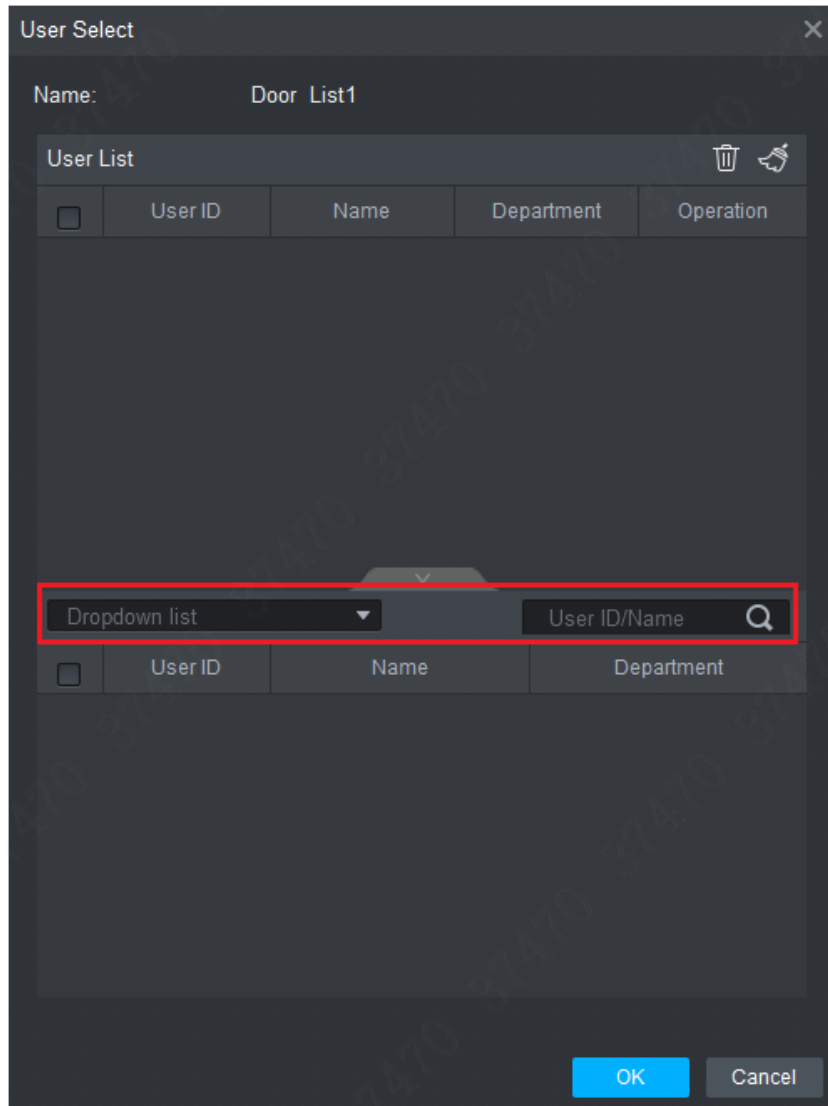


Figure 4-16

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.

4.5.2 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 4-17.

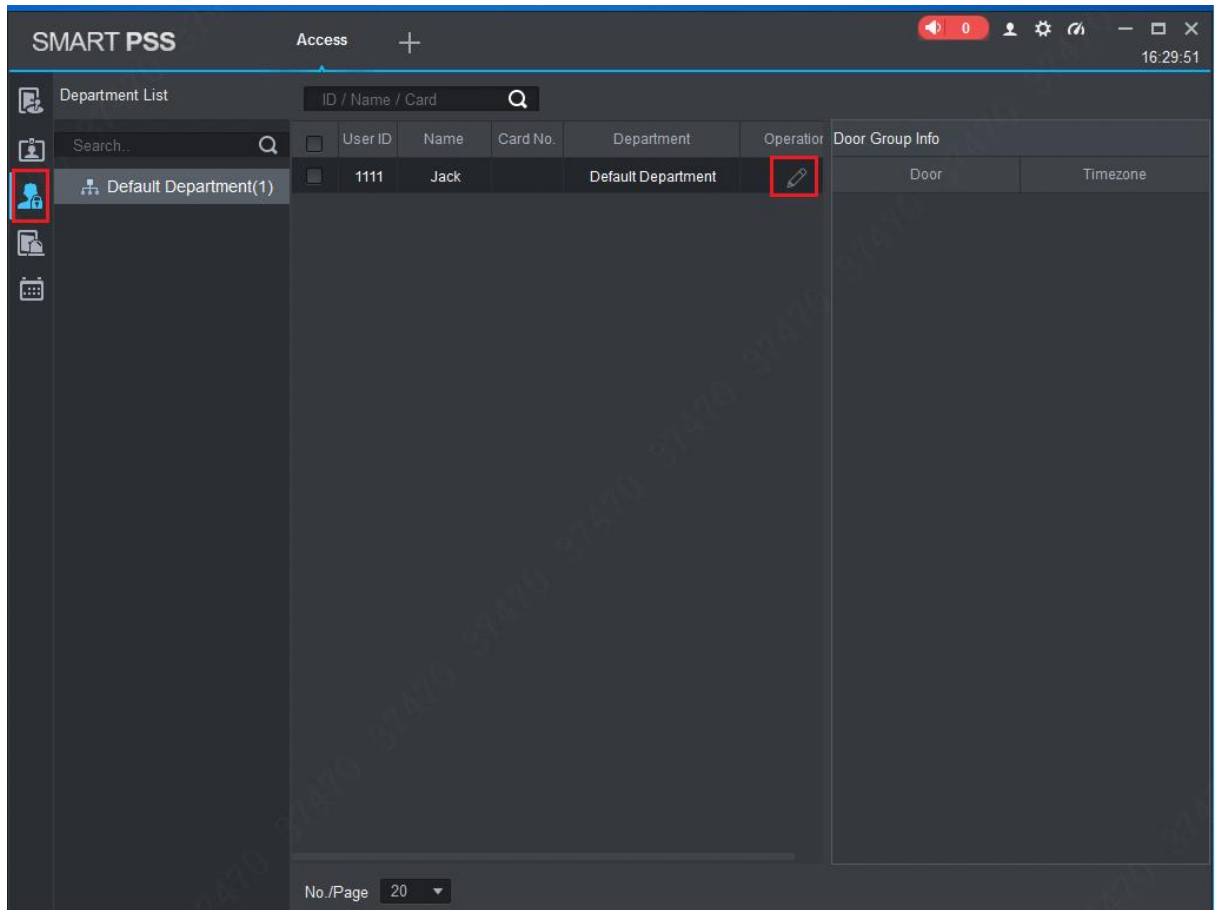



Figure 4-17

Step 2 Click .

The system pops up “Select Door Group” dialog box, as shown in Figure 4-18.

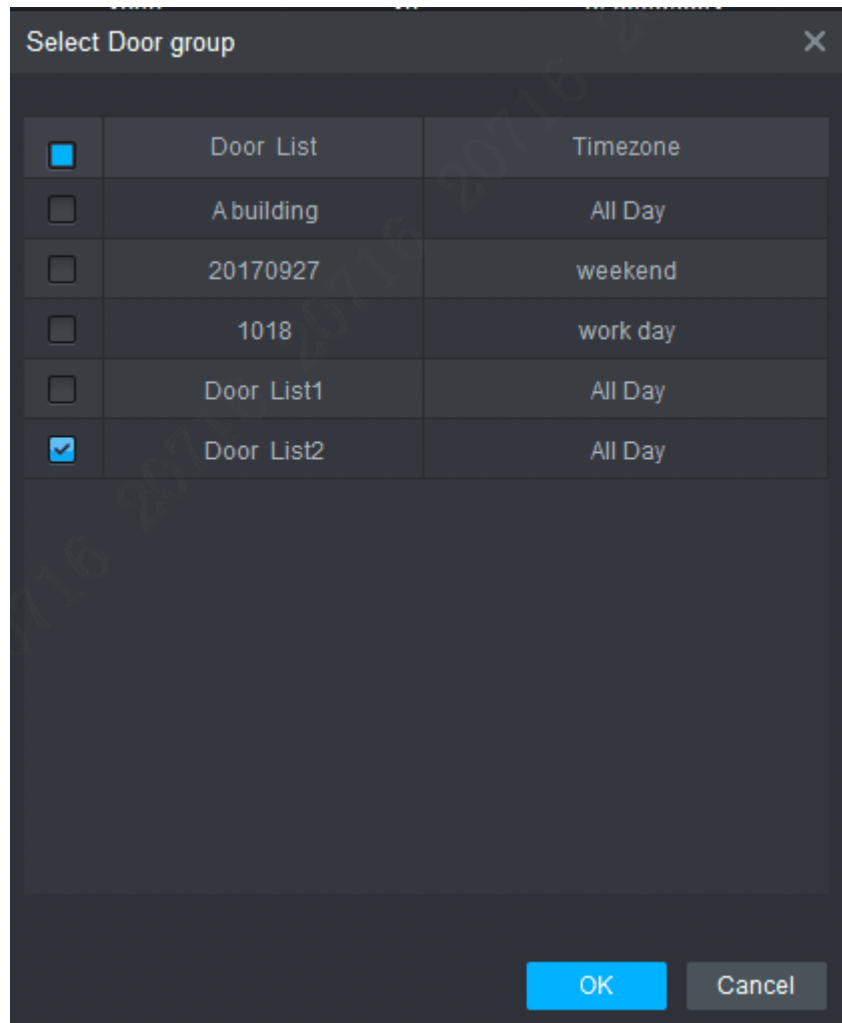


Figure 4-18

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: How can I deal with problems that are not confirmed or cannot be solved?

Answer: Please consult professional technical support.

6

Technical Parameters

Classification	Name	Parameter Value
System parameter	Main processor	Dual 32-bit ARM processor
	Memory capacity	2G
Door control parameter	Lock control	4-channel
	Door sensor	4-channel
	Locking tongue sensor	4-channel
	Exit button	4-channel
	External reader	8-channel (4-channel RS485, 4-channel Wiegand)
Alarm parameter	Alarm input	8-channel
	Alarm output	8-channel
Function	Door overtime alarm	Give an overtime alarm when door opening time exceeds "door overtime". This function shall be set.
	Intrusion alarm	Give an intrusion alarm if someone intrudes without swiping card or inputting password.
	Duress alarm	Give a duress alarm if you enter with duress card.
	Tamper alarm	Tamper alarm button will give a tamper alarm if the access control device is tampered.
	Unlocking mode	Support card, password and fingerprint.
	Remote verification	Support bonding with period.
	Schedule	128 groups
	Period	128 groups
	Holiday	128 groups
	Network upgrade	Upgrade the device through network.
	Patrol card	Patrol card can be swiped and recorded at patrol points. Patrol card cannot unlock the door.
	Guest card	Set the use times of the card. The card will lose effect in case of exceeding the use times.
	Multi-door interlocking	Support arbitrary interlocking of 64+4 doors.
	Anti-passback	Support anti-passback of arbitrary 64+4 readers.
Work in case of power interruption	12V storage battery can be configured to supply power to doors and controllers in case of power interruption.	
Interface parameter	Network interface	2
	RS485 interface	2
General parameter	Power supply	AC 80–260V
	Power consumption	≤5W (excluding reader)
	Working temperature	-30℃~+60℃
	Working humidity	5%~95%
	Atmospheric pressure	86kPa~106kPa
	Dimension	320mm×280mm×114mm

Classification	Name	Parameter Value
	Weight	2.0kg
	Mounting mode	Wall-mounted