Access Master Controller

Quick Start Guide

V1.0.1

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 suspect 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.

Foreword

General

This document elaborates on structure, installation, wiring and WEB operation of access master controller.

Safety Instructions

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

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

Privacy Protection Notice

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

About the Manual

- The Manual is for reference only. If there is inconsistency between the Manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Manual.
- The Manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper 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

1 Overview

Access master controller is a controlling device which compensates video monitoring and visual intercom. It has neat and modern design with strong functionality, suitable for commercial building, corporation property and intelligent community.

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 slave 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 and ordinary card.
- Local WEB can add, configure and upgrade the slave 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℃～+60℃ and working humidity: ≤95%.

2 Packing List

Before installation, please check according to Table 2-1.

No.	Name	Quantity
1	Access Controller	1
2	Power Supply Cable	1
3	Storage Battery Cable	1
4	Key	1
5	Accessory Kit (Screw, Expansion Pipe and Wiring Terminal)	1
6	Quick Start Guide	1
7	Certificate of Qualification	1

Table 2-1

3 Installation Guide

3.1 System Structure

Its system structure is shown in Figure 3-1.

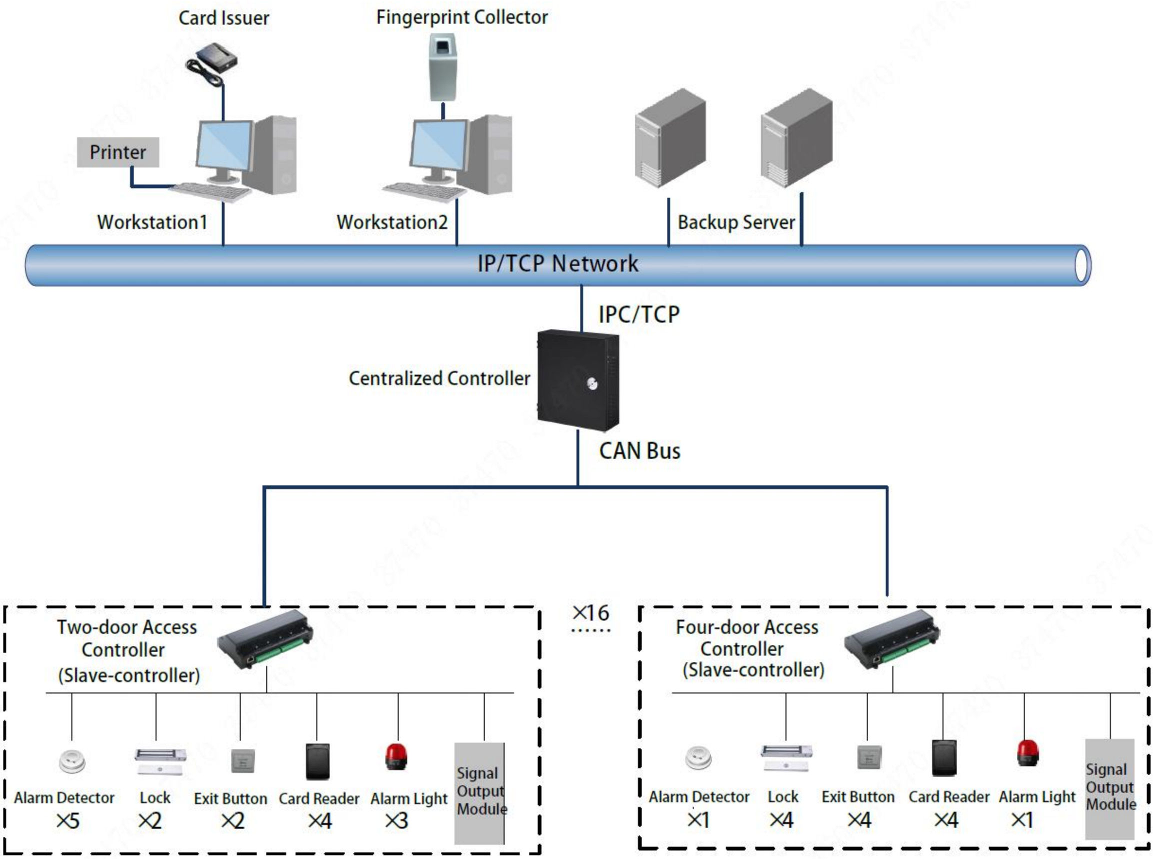


Figure 3-1

3.2 External Dimension

Its appearance and dimension is shown in Figure 3-2. The unit is mm.

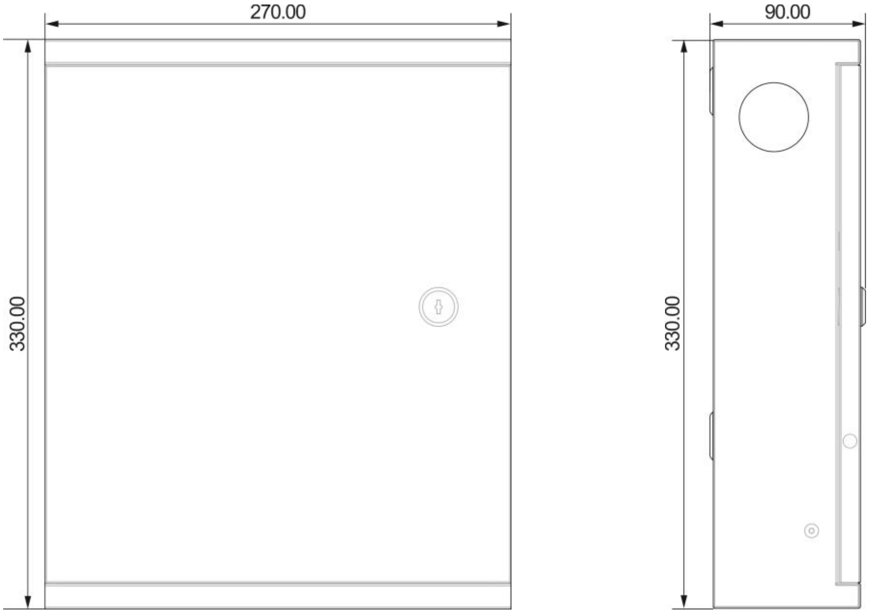


Figure 3-2

3.3 Device Installation

Device installation diagram is shown in Figure 3-3.

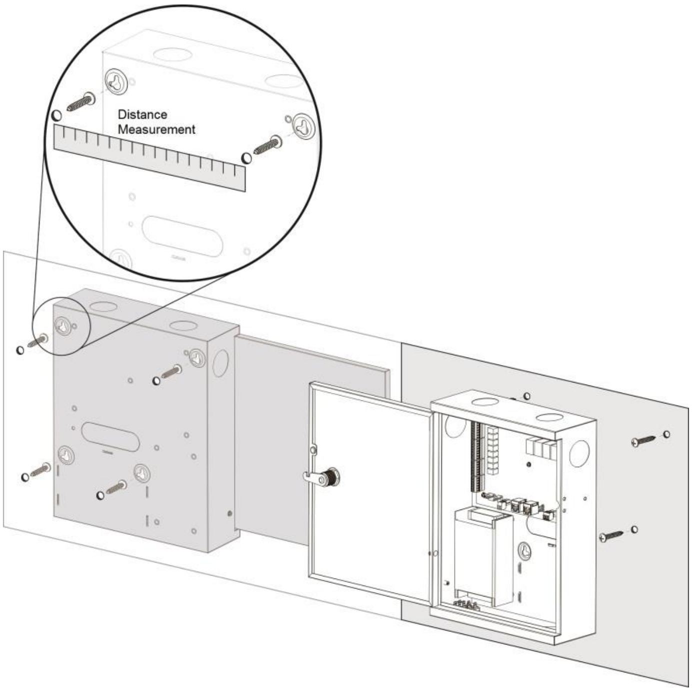


Figure 3-3

Note

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

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.

Embed expansion nuts and fix screws into the wall.

Hang the whole device onto the screws.

3.4 Wiring Diagram

Device wiring diagram is shown in Figure 3-4.

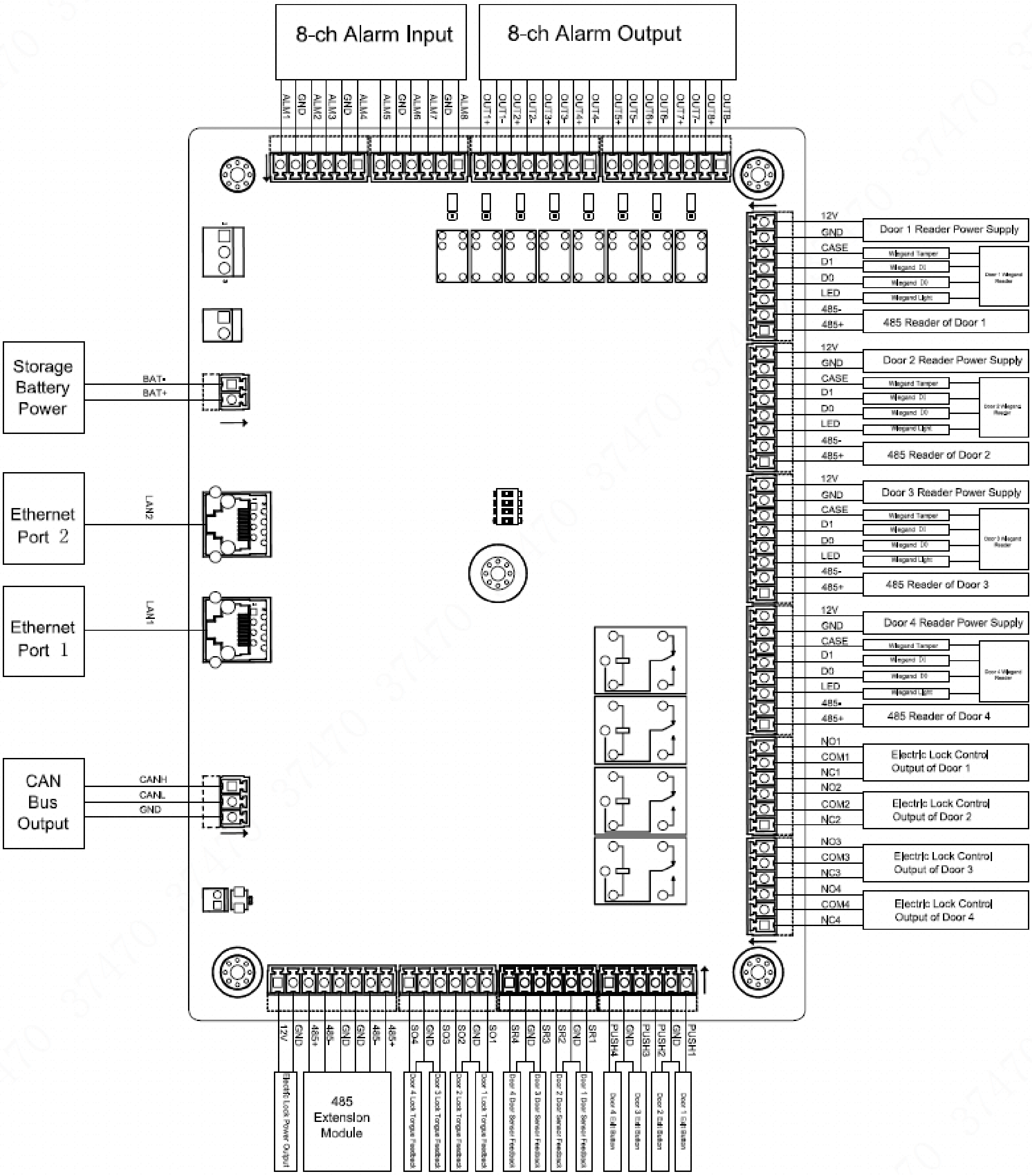


Figure 3-4

3.4.1 Wiring Description of CAN Bus

Access master controller and slave controllers are connected with CAN bus, as shown in Figure 3-5. Please refer to Table 3-1 for descriptions about wiring terminals.

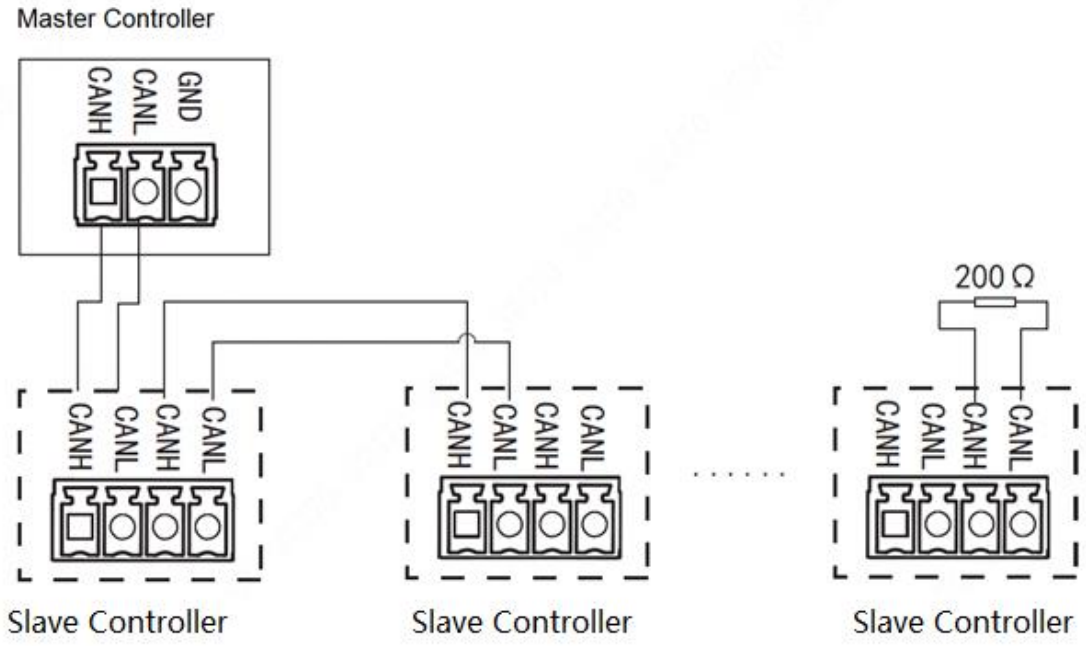


Figure 3-5

Interface	Wiring Terminal	Description
CAN Bus	CANH	CAN bus communication
	CANL	

Table 3-1

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

Table 3-2

3.4.2 Wiring Description of External Alarm Input

Support 8-channel external alarm input, as shown in Figure 3-6. Please refer to Table 3-3 for descriptions about wiring terminals.

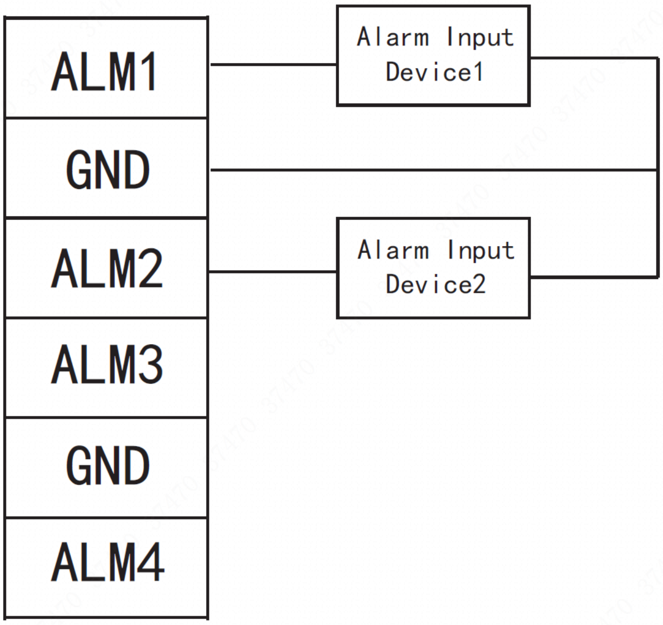


Figure 3-6

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 3-3

3.4.3 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 3-7 and Figure 3-8. Please refer to Table 3-4 for descriptions about wiring terminals.

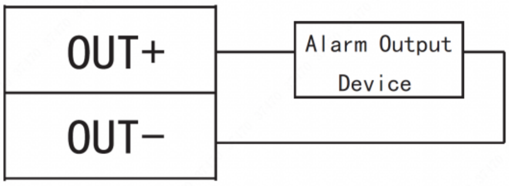


Figure 3-7

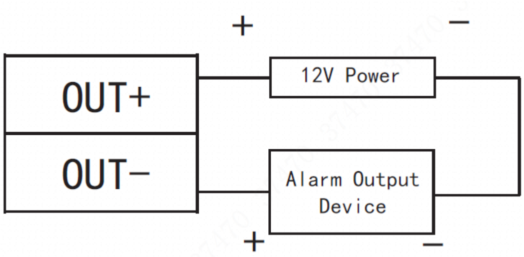


Figure 3-8

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

Table 3-4

3.4.4 Wiring Description of Reader

Note

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

Please refer to Table 3-5 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 3-6 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-	Yellow	485 reader
	485+	Purple	

Table 3-5

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

Table 3-6

3.4.5 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 3-9, Figure 3-10 and Figure 3-11. Please refer to Table 3-7 for descriptions of wiring terminals.

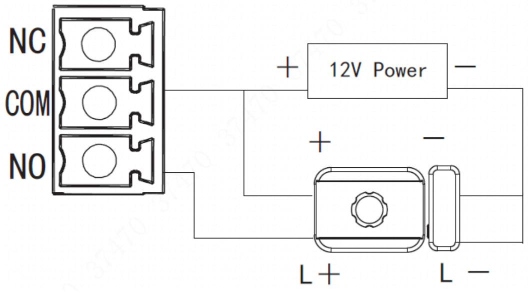


Figure 3-9

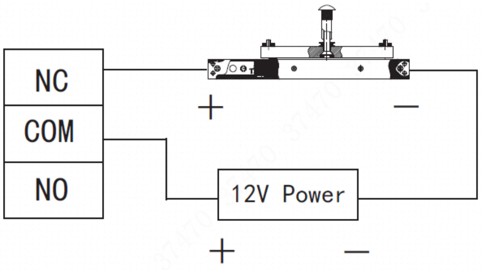


Figure 3-10

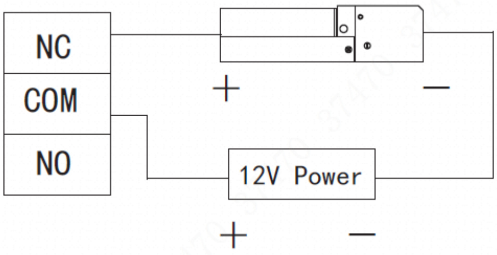


Figure 3-11

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 3-7

3.4.6 Wiring Description of Exit Button

Corresponding wiring terminals of exit button are shown in Figure 3-12. Please refer to Table 3-8 for descriptions of wiring terminals.

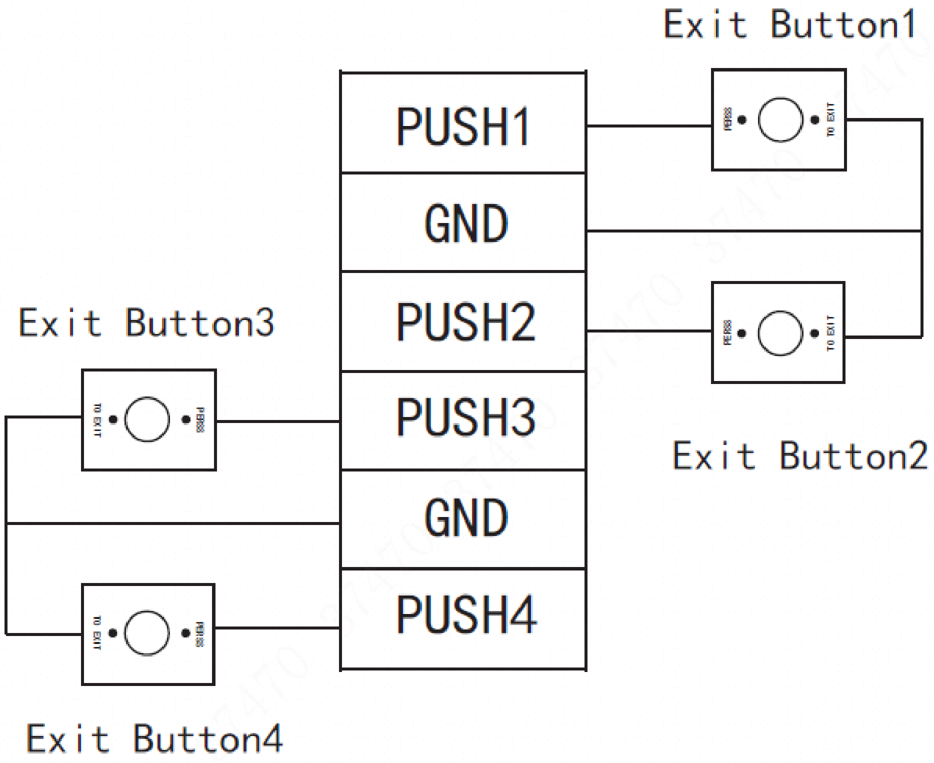


Figure 3-12

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 3-8

3.4.7 Wiring Description of Door Sensor

Corresponding wiring terminals of door sensor are shown in Figure 3-12. Please refer to Table 3-9 for descriptions of wiring terminals.

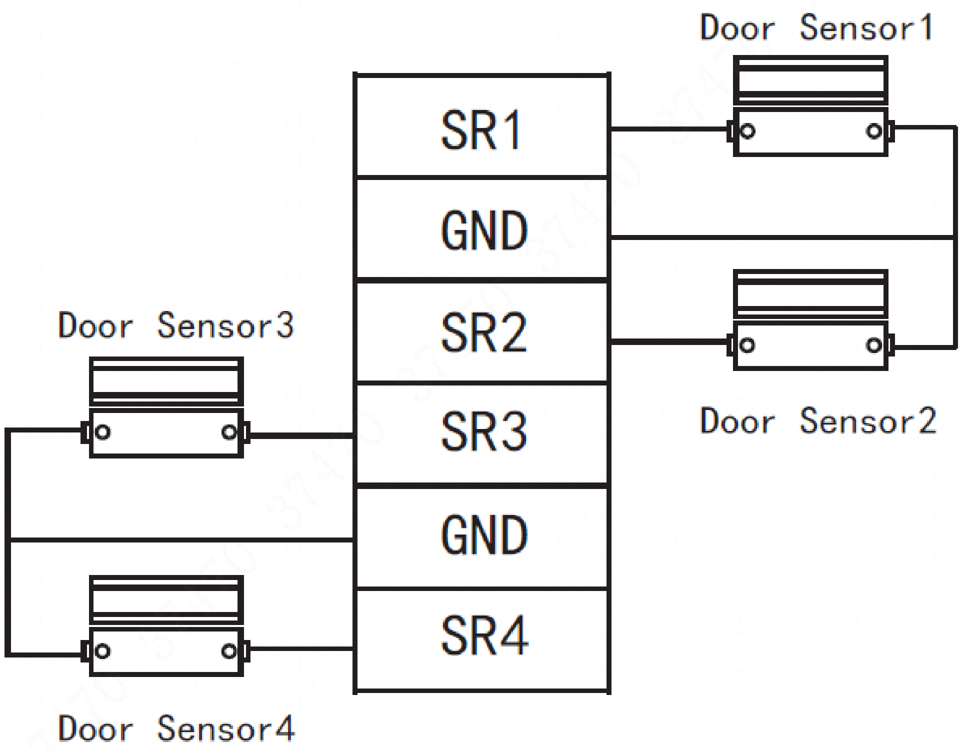


Figure 3-13

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 3-9

3.5 DIP Switch

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

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

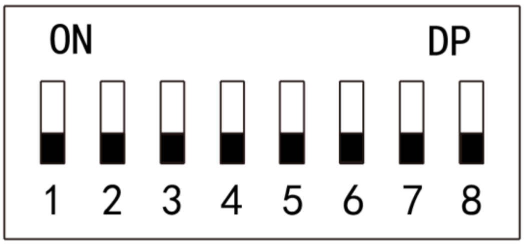


Figure 3-14

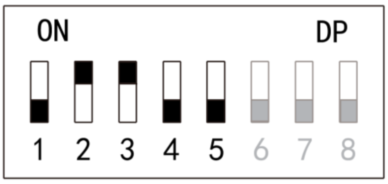
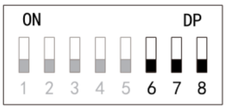
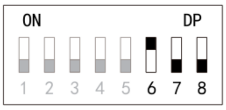
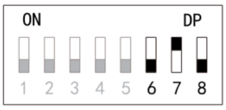
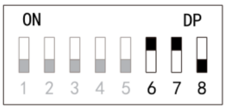
Function	No.	Description
Device Number	1～5	Set device number with binary system. The left is the lowest order. For example:  Binary representation 00110 corresponds to 6 in decimal system.
Speed	6～8	Set the speed. ● All of them are at the bottom  , transmission speed is 50kb/s. ● Only digit 6 is at ON position  , transmission speed is 80kb/s. ● Only digit 7 is at ON position  , transmission speed is 100kb/s. ● Digits 6 and 7 are at ON position  , transmission speed is 125kb/s.

Table 3-10

3.6 Reboot

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

4 WEB Configuration

Default IP address of access master 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.

4.1 Initialization

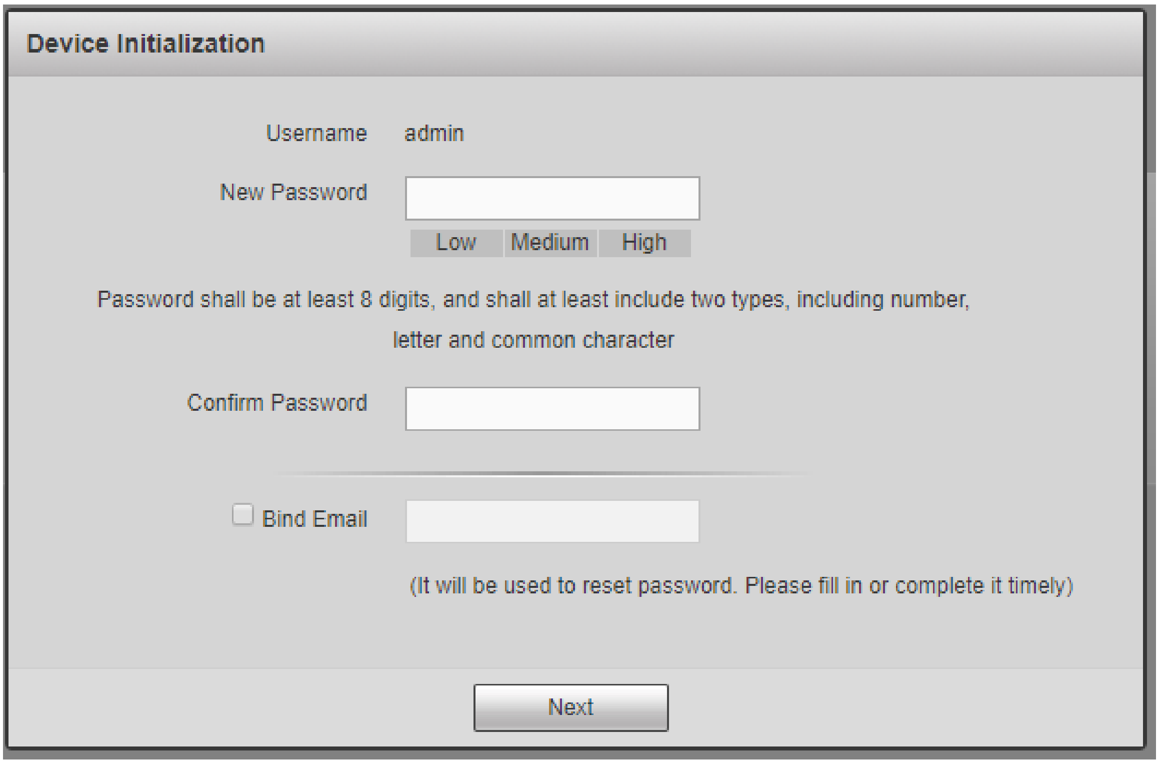
During the first use, please set admin username and password (default administrator username is admin).

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 access master controller in the address bar, and press [Enter] key.

The system displays “Device Initialization” interface, as shown in Figure 4-1.



Device Initialization

Username admin

New Password

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

Confirm Password

□ Bind Email

(It will be used to reset password. Please fill in or complete it timely)

Figure 4-1

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 the user's manual for details.

Step 3 Click "Next".

The system displays "Finish" interface.

Step 4 Click "OK" to complete initialization.

4.2 Login

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

The system displays login interface, as shown in Figure 4-2.

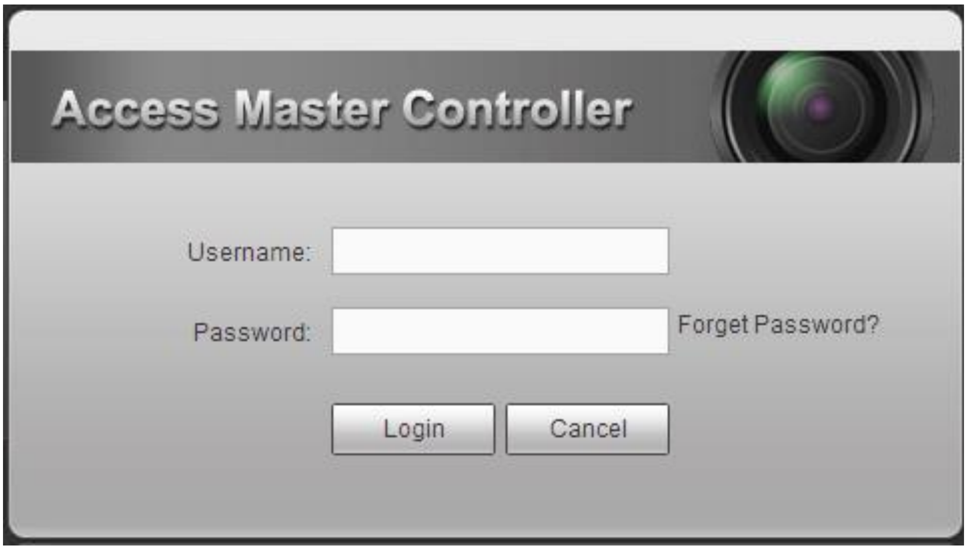


Figure 4-2

Step 2 Input "Username" and "Password".

Note

- Default administrator 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 the user's manual for details.

Step 3 Click "Login".

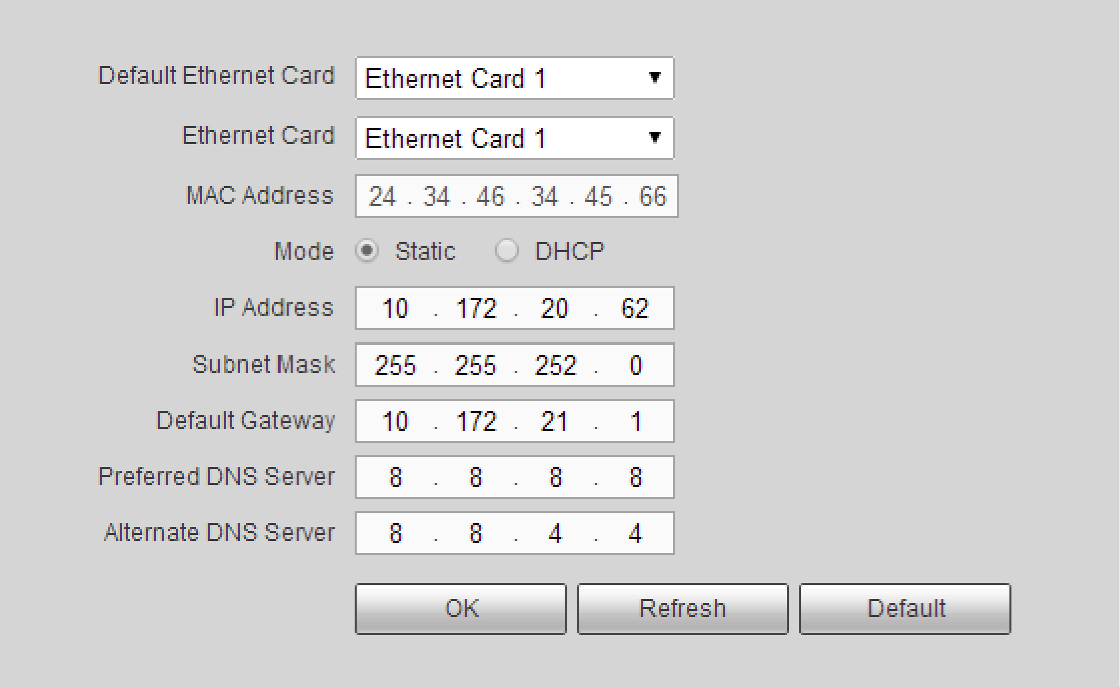
The system displays "Preview" interface.

4.3 Set Network

Set IP address and DNS server of access master controller, in order to connect with other devices in the network.

Step 1 Select "System > Network > TCP/IP".

The system displays “TCP/IP” interface, as shown in Figure 4-3.



Default Ethernet Card: Ethernet Card 1

Ethernet Card: Ethernet Card 1

MAC Address: 24 . 34 . 46 . 34 . 45 . 66

Mode: ● Static ○ DHCP

IP Address: 10 . 172 . 20 . 62

Subnet Mask: 255 . 255 . 252 . 0

Default Gateway: 10 . 172 . 21 . 1

Preferred DNS Server: 8 . 8 . 8 . 8

Alternate DNS Server: 8 . 8 . 4 . 4

Figure 4-3

Step 2 Set TCP/IP parameters. Please refer to Table 4-1 for details.

Parameter	Description
Default Ethernet Card and Ethernet Card	They cannot be modified. Default one is Ethernet Card 1.
MAC Address	Display MAC address of the device.
Mode	● 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. ◇ 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. ◇ When PPPoE is enabled, IP address, subnet mask, default gateway and DHCP cannot be modified.
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	
Preferred DNS Server	IP address of DNS server.
Alternate DNS Server	IP address of alternate DNS server.

Table 4-1

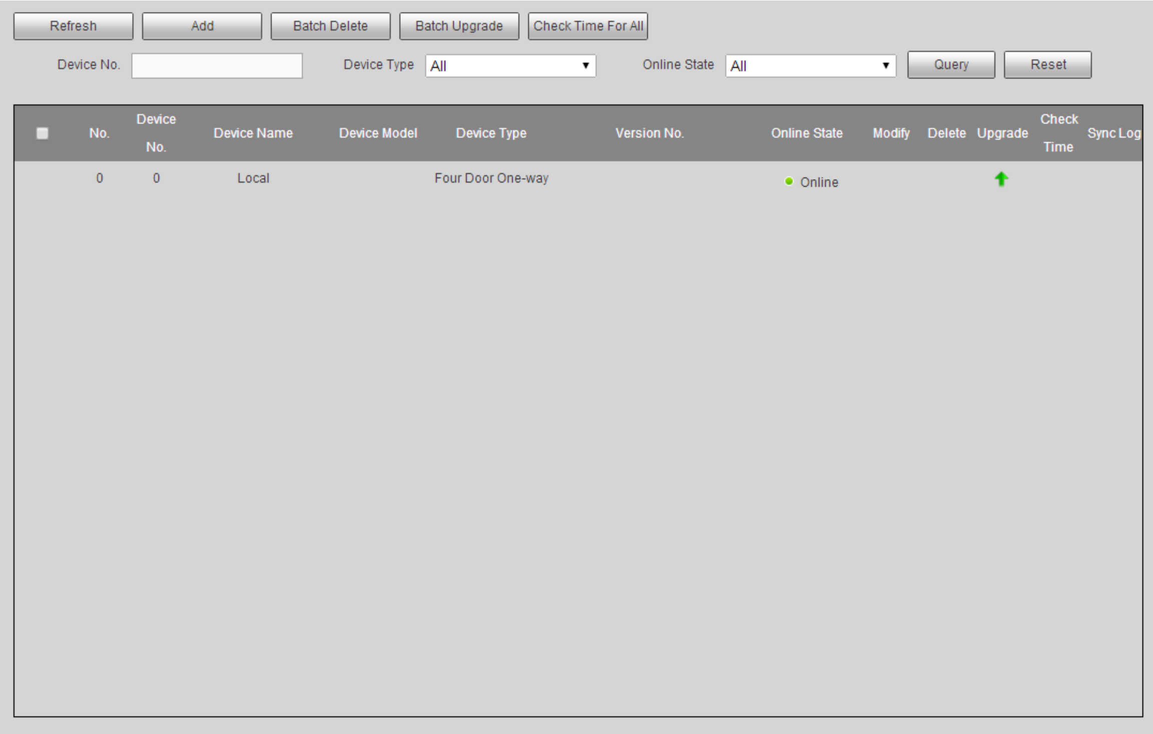
Step 3 Click “OK” to complete setting.

4.4 Add Access Controller

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

Step 1 Select “Access > Device Management”.

The system displays “Device Management” interface, as shown in Figure 4-4.



Device No.:

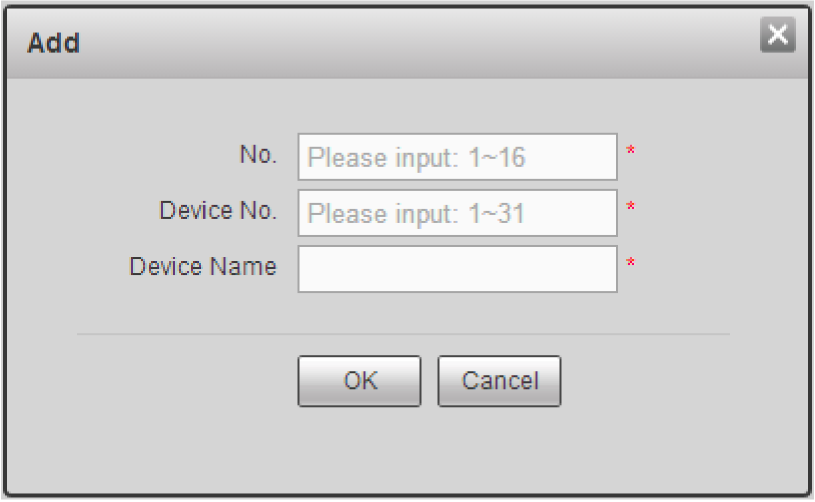
Device Type: All

Online State: All

□	No.	Device No.	Device Name	Device Model	Device Type	Version No.	Online State	Modify	Delete	Upgrade	Check Time	Sync Log
	0	0	Local		Four Door One-way		● Online			↑		

Figure 4-4

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



No. Please input: 1~16 *

Device No. Please input: 1~31 *

Device Name *

Figure 4-5

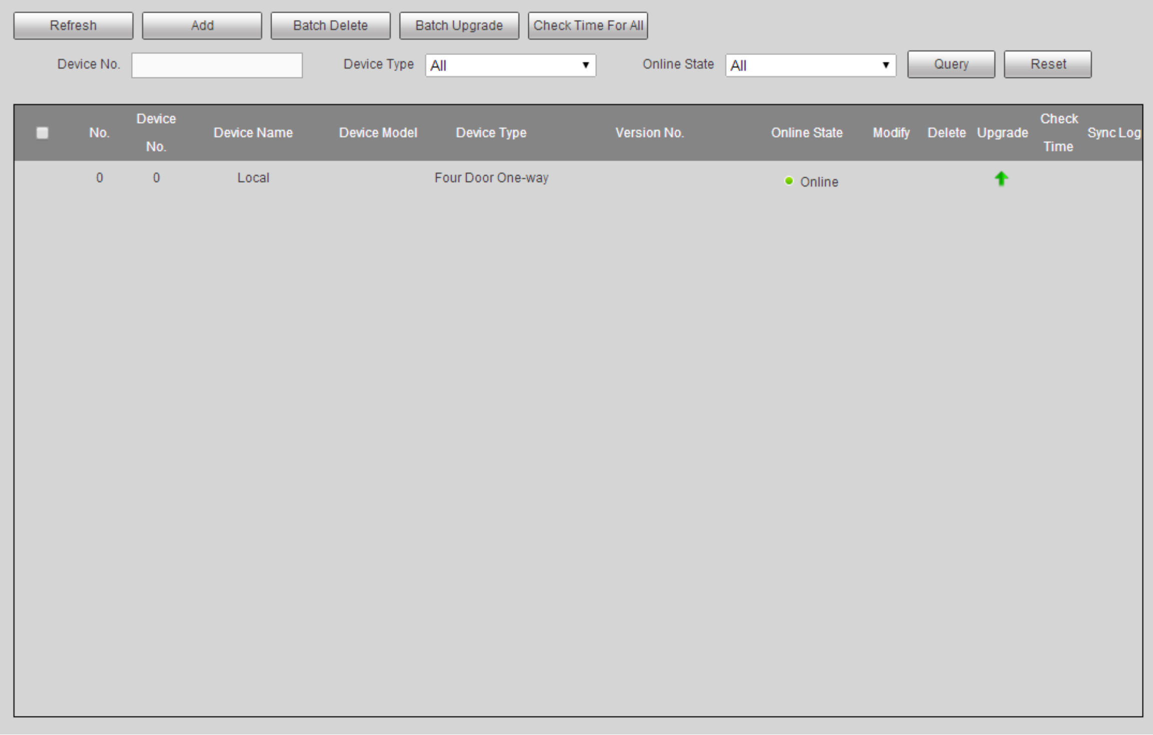
Step 3 Input “No.”, “Device No.” and “Device Name”.

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 slave controller number. Slave controller number is set in DIP switch and can be used after transforming binary encoding to decimal system.
Device Name	Customized slave controller name, in order to facilitate management. The name consists of 16 digits at most, including English letter, number and special character. The name cannot be repeated.

Table 4-2

Step 4 Click “OK”.

After adding, the device is displayed in the list, as shown in Figure 4-6.



Device No.:

Device Type: All

Online State: All

□	No.	Device No.	Device Name	Device Model	Device Type	Version No.	Online State	Modify	Delete	Upgrade	Check Time	Sync Log
	0	0	Local		Four Door One-way		● Online			↑		

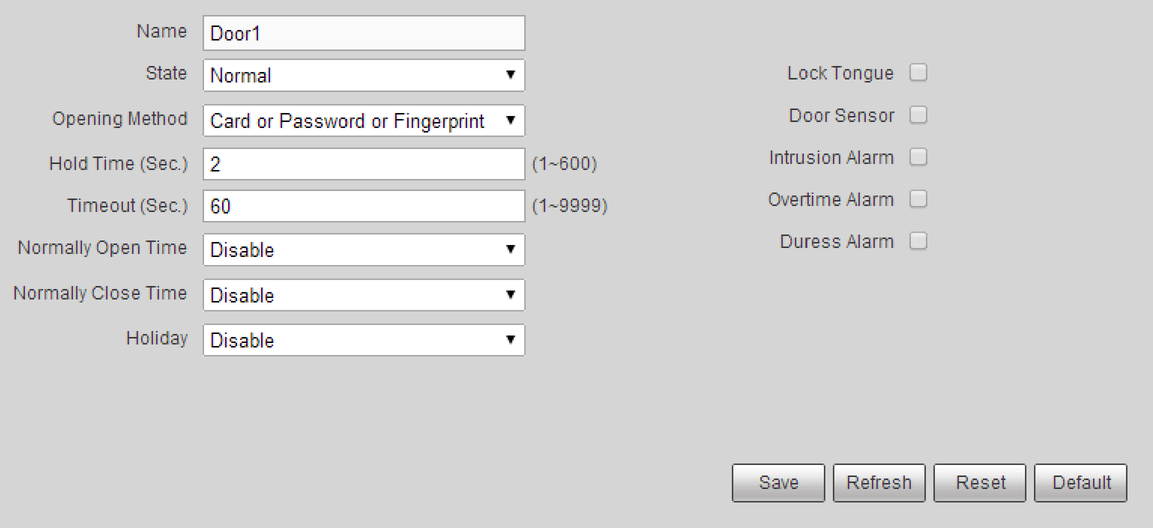
Figure 4-6

4.5 Set Door Parameters

Configure parameters of doors under access controller.

Step 1 Select “Access > Door Parameters”.

The system displays “Door Parameters” interface, as shown in Figure 4-7.



Name	Door1	
State	Normal	
Opening Method	Card or Password or Fingerprint	
Hold Time (Sec.)	2	(1~600)
Timeout (Sec.)	60	(1~9999)
Normally Open Time	Disable	
Normally Close Time	Disable	
Holiday	Disable	

Lock Tongue □
Door Sensor □
Intrusion Alarm □
Overtime Alarm □
Duress Alarm □

Figure 4-7

Step 2 Select a door in the device tree in the left, configure door parameters and refer to Table 4-3 for details.

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>Name</td><td colspan="2">Display the name of present door.</td></tr>
<tr><td>Status</td><td colspan="2">Select door status, which won’t be affected after reboot.
● 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.</td></tr>
<tr><td>Opening Method</td><td colspan="2">Select an opening method. Only the selected method works, while other methods are invalid.
● 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.</td></tr>
<tr><td>Hold Time (Sec.)</td><td colspan="2">Hold time of an open door. The door is closed automatically after hold time.</td></tr>
<tr><td>Timeout (Sec.)</td><td colspan="2">When “overtime alarm” is enabled, upload an alarm if exceeding opening time.</td></tr>
<tr><td>Normally Open Time</td><td>The door is normally open within the set time.</td><td rowspan="3">Note
In the drop-down list, select a synchronously set period in Smart PSS client.
● Disabled: period control is not enabled.
● All day: this setting is executed 24 hours a day.</td></tr>
<tr><td>Normally Close Time</td><td>The door is normally closed within the set time.</td></tr>
<tr><td>Holiday</td><td>It is effective within the selected holiday period, and becomes ineffective after the period.</td></tr>
<tr><td>Lock Tongue</td><td colspan="2">Tick the checkbox to enable lock tongue function. Judge and alarm according to lock tongue status.</td></tr>
</table>

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>Door Sensor</td><td colspan="2">Tick the checkbox to enable door sensor function. Judge and alarm according to door sensor status.</td></tr>
<tr><td>Intrusion Alarm</td><td>Tick the checkbox to enable intrusion alarm function. Upload an alarm in case that door sensor or door tongue is opened when the door is not opened normally.</td><td rowspan="2">Note
While the alarm is enabled, corresponding lock tongue or door sensor shall be enabled. Otherwise, door status cannot be judged.</td></tr>
<tr><td>Overtime Alarm</td><td>Tick the checkbox to enable overtime alarm function. Upload an alarm in case that opening time exceeds "overtime".</td></tr>
<tr><td>Duress Alarm</td><td colspan="2">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.</td></tr>
</table>

Table 4-3

Step 3 Click "Save" to complete parameter setting.

Note

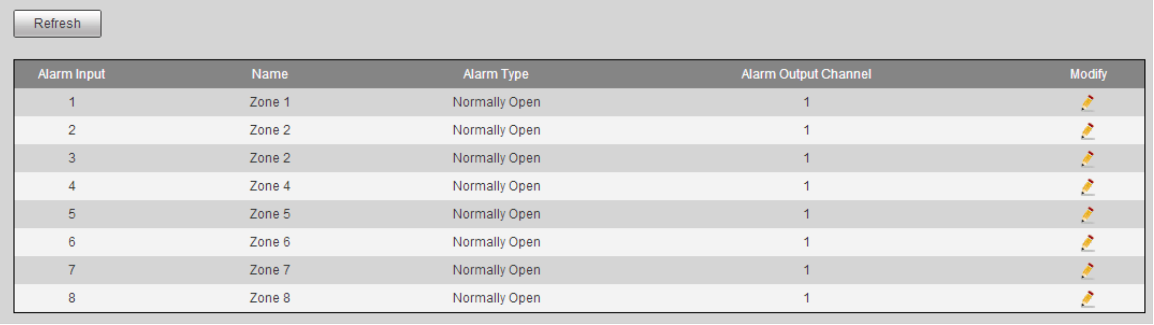
If access master controller connects Smart PSS client, relevant parameters and alarms will be synchronized with the client. Parameters modified in the client will also be synchronized with master controller.

4.6 Set Alarm Linkage

Access master controller supports 8-channel alarm input and output. Set alarm linkage output at this interface.

Step 1 Select "Access > Alarm Linkage".

The system displays "Alarm Linkage" interface, as shown in Figure 4-8.

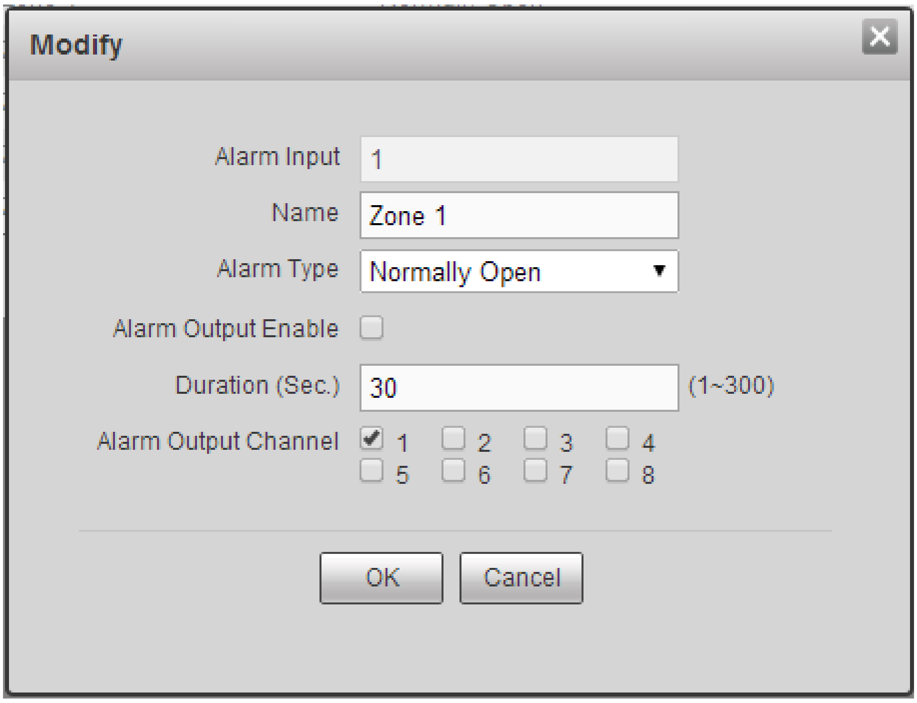


Alarm Input	Name	Alarm Type	Alarm Output Channel	Modify
1	Zone 1	Normally Open	1	✎
2	Zone 2	Normally Open	1	✎
3	Zone 2	Normally Open	1	✎
4	Zone 4	Normally Open	1	✎
5	Zone 5	Normally Open	1	✎
6	Zone 6	Normally Open	1	✎
7	Zone 7	Normally Open	1	✎
8	Zone 8	Normally Open	1	✎

Figure 4-8

Step 2 Click ✎.

The system pops up "Modify" dialogue box, as shown in Figure 4-9.



Modify

Alarm Input 1

Name Zone 1

Alarm Type Normally Open

Alarm Output Enable □

Duration (Sec.) 30 (1~300)

Alarm Output Channel ☑ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8

Figure 4-9

Step 3 Configure parameters and refer to Table 4-4 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.

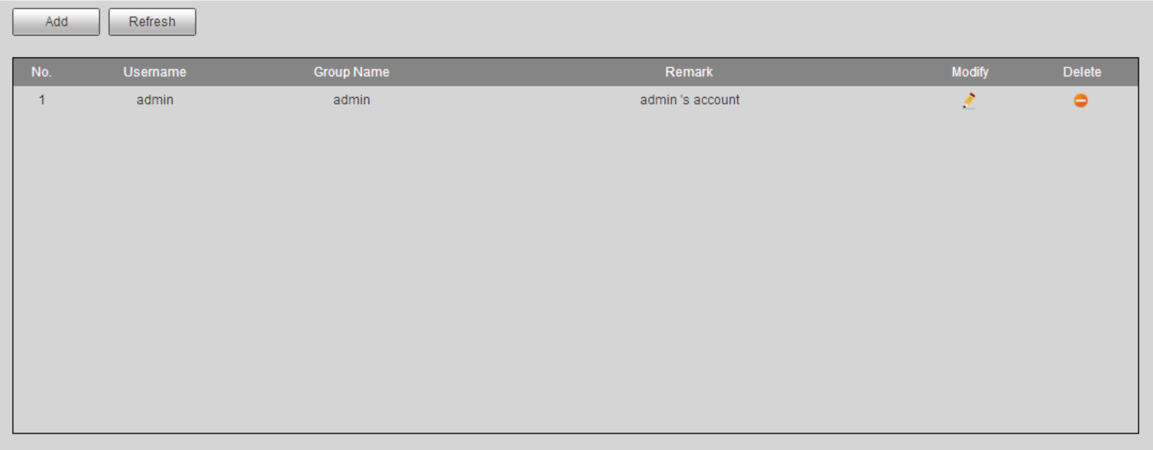
Table 4-4

Step 4 Click “OK” to complete setting.

4.7 Add User

Step 1 Select “System > User Management”.

The system displays “User Management” interface, as shown in Figure 4-10.

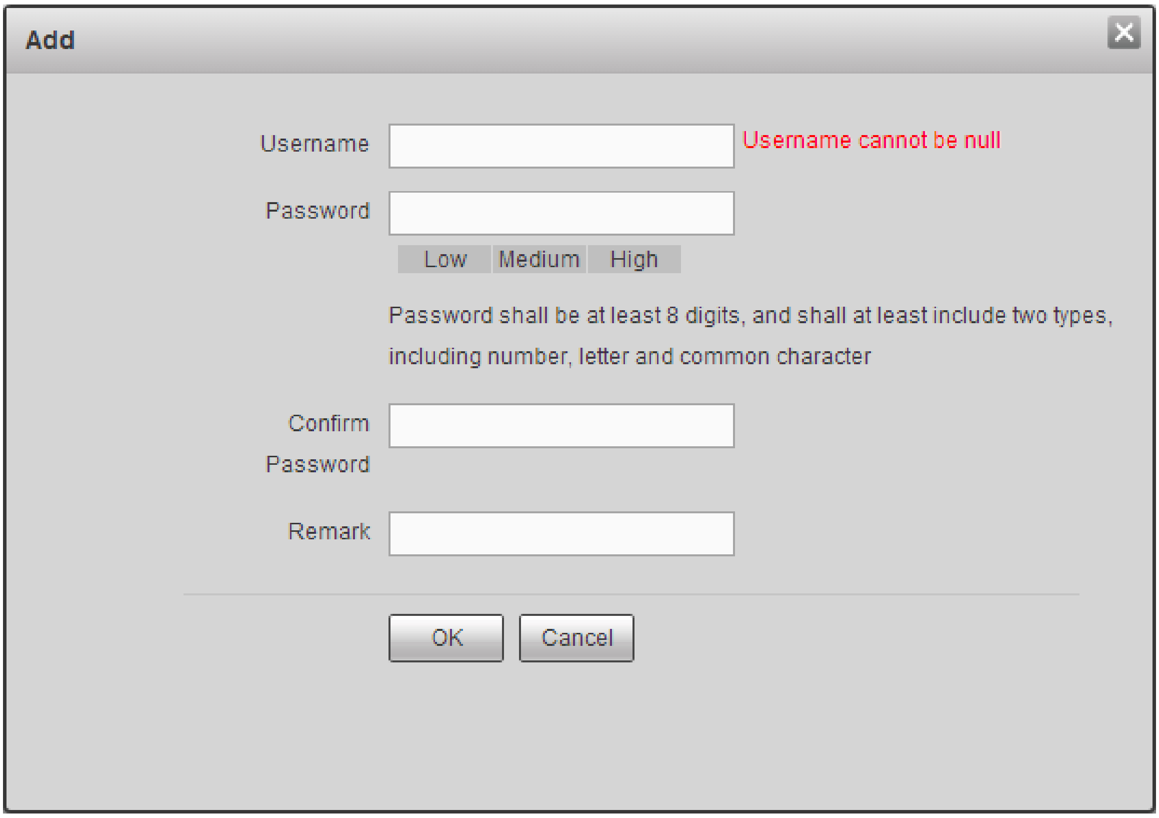


No.	Username	Group Name	Remark	Modify	Delete
1	admin	admin	admin 's account	✎	⊖

Figure 4-10

Step 2 Click “Add”.

Pop up “Add” dialogue box, as shown in Figure 4-11.



Username Username cannot be null

Password

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

Confirm Password

Remark

Figure 4-11

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

Step 4 Click “OK” to complete setting.

5 Smart PSS Configuration

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

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

Note

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

5.1 Login Client

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

5.2 Add Access Controller

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

5.2.1 Auto Search

Devices are required to be in the same network segment.

Step 1 In “Devices” interface, click “Auto Search”, as shown in Figure 5-1.

The system displays “Auto Search” interface, as shown in Figure 5-2.

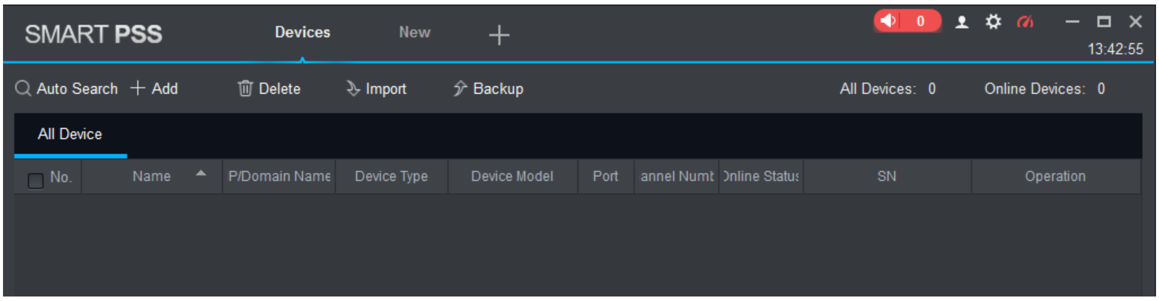
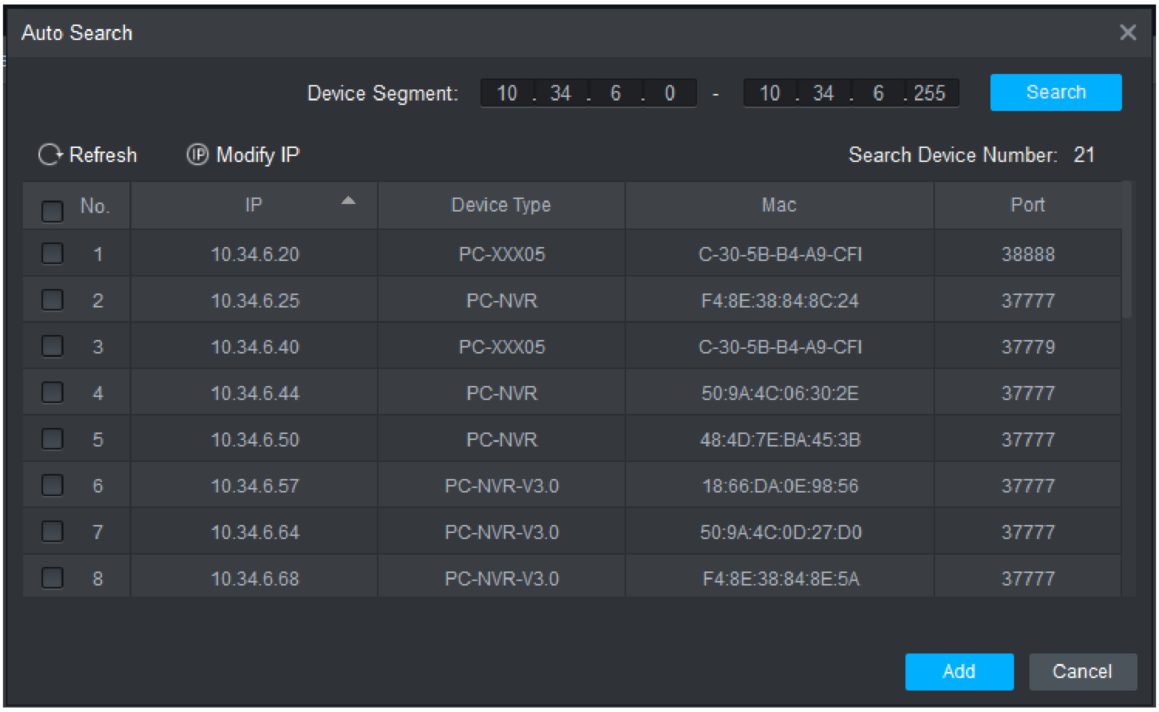


Figure 5-1



Auto Search ✕

Device Segment: 10 . 34 . 6 . 0 - 10 . 34 . 6 . 255 Search

Refresh Modify IP Search Device Number: 21

□ No.	IP	Device Type	Mac	Port
□ 1	10.34.6.20	PC-XXX05	C-30-5B-B4-A9-CFI	38888
□ 2	10.34.6.25	PC-NVR	F4:8E:38:84:8C:24	37777
□ 3	10.34.6.40	PC-XXX05	C-30-5B-B4-A9-CFI	37779
□ 4	10.34.6.44	PC-NVR	50:9A:4C:06:30:2E	37777
□ 5	10.34.6.50	PC-NVR	48:4D:7E:BA:45:3B	37777
□ 6	10.34.6.57	PC-NVR-V3.0	18:66:DA:0E:98:56	37777
□ 7	10.34.6.64	PC-NVR-V3.0	50:9A:4C:0D:27:D0	37777
□ 8	10.34.6.68	PC-NVR-V3.0	F4:8E:38:84:8E:5A	37777

Add Cancel

Figure 5-2

Step 2 Input device segment and click "Search".

The system displays search results.

Note

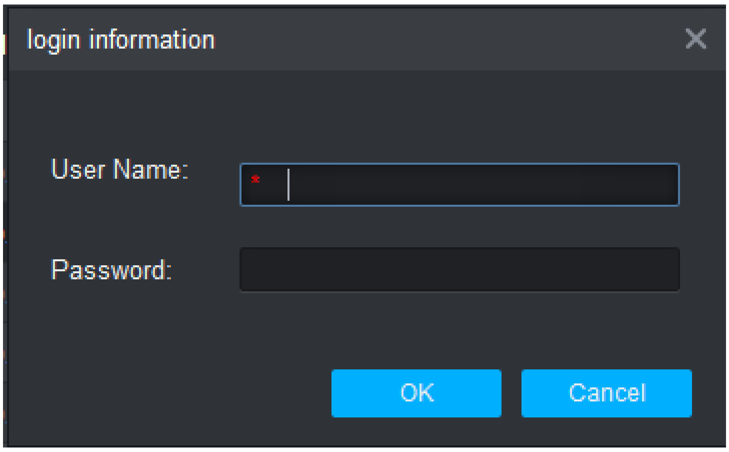
- Click "Refresh" to update device information.
- Select a device, click "Modify IP" to modify IP address of the device. For specific operations, please refer to User's Manual of Smart PSS Client.

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 5-3.



login information ✕

User Name: *

Password:

OK Cancel

Figure 5-3

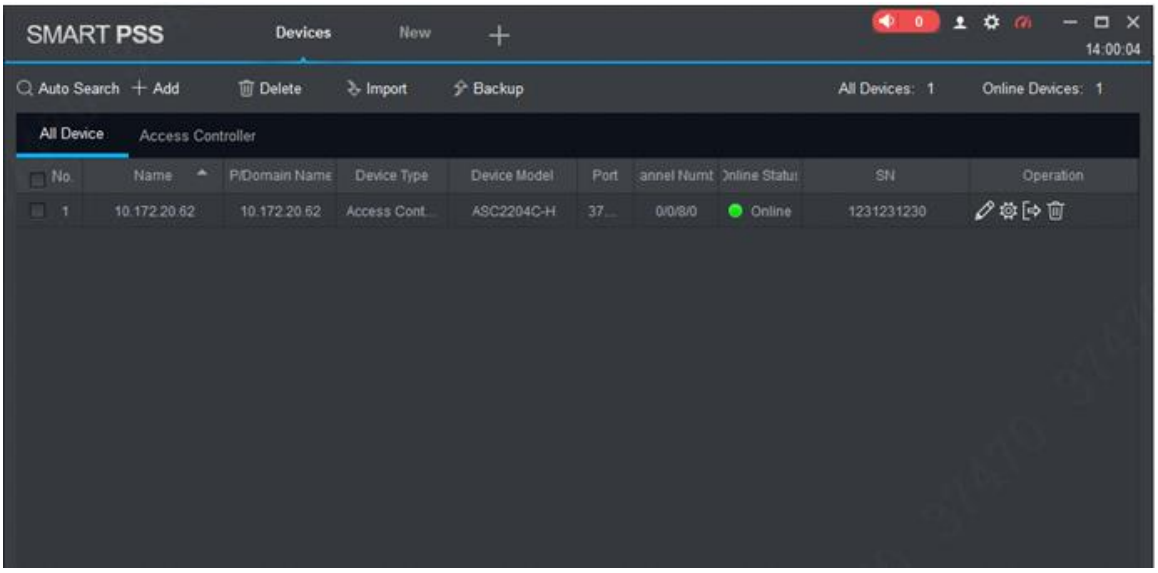
Step 5 Input "User Name" and "Password" to log in the device, and click "OK".

The system displays the added device list, as shown in Figure 5-4. Available operations are shown in Table 5-1.

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”.



No.	Name	P/Domain Name	Device Type	Device Model	Port	annel Numt	Online Statu	SN	Operation
1	10.172.20.62	10.172.20.62	Access Cont...	ASC2204C-H	37...	0/0/8/0	● Online	1231231230	✎ ⚙ ⇨ 🗑

Figure 5-4

Icon	Description
✎	Click this icon to enter “Modify Device” interface. Device info can be modified, 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. Configure device camera, network, event, storage and system info etc.
⇨ and ⇦	● When the device is logged in, the icon displays ⇨. Click the icon to exit, and the icon changes to ⇦. ● When the device is offline, the icon displays ⇦. Click the icon to login the device (device info shall be correct), and the icon changes to ⇨.
🗑	Click this icon to delete a device.

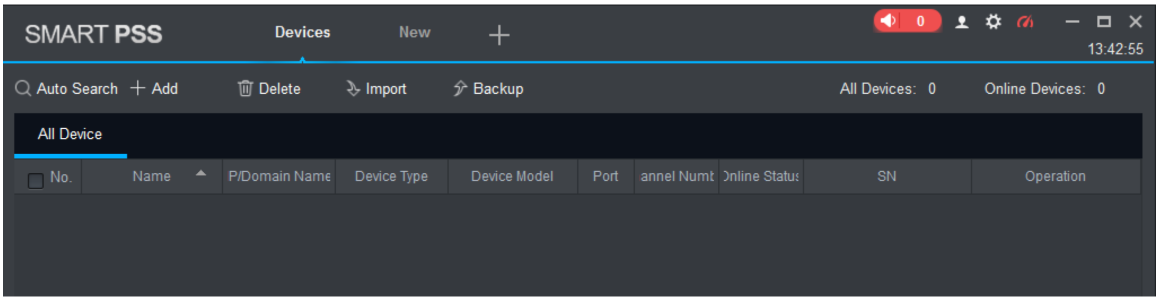
Table 5-1

5.2.2 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 5-5.

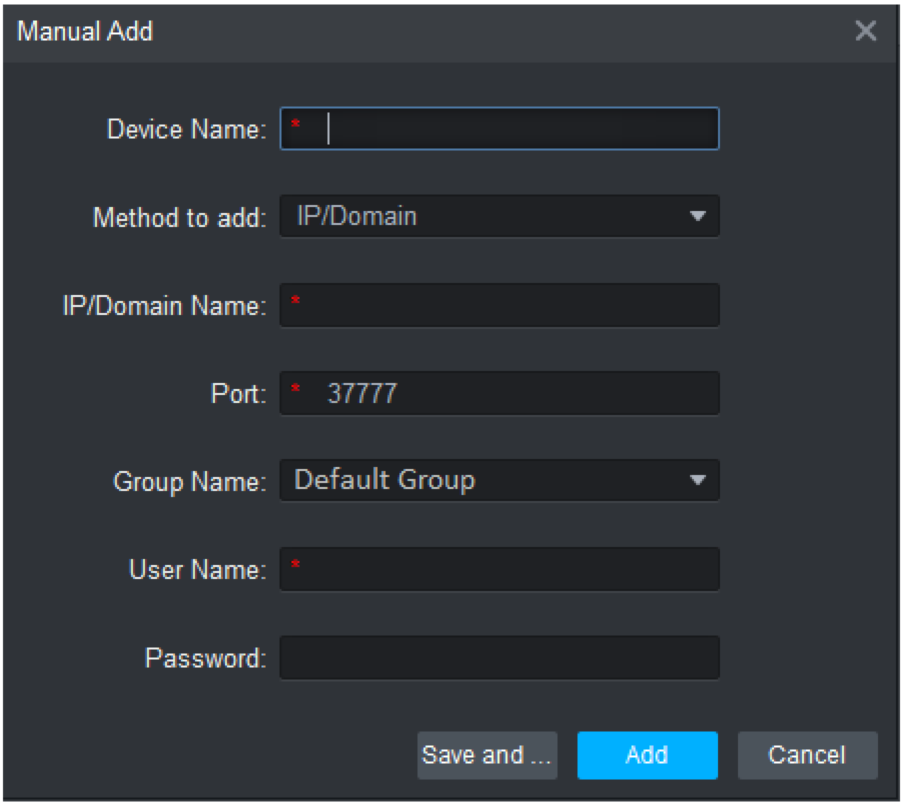
The system pops up “Manual Add” interface, as shown in Figure 5-6.



All Devices: 0

Online Devices: 0

Figure 5-5



Device Name: *

Method to add: IP/Domain

IP/Domain Name: *

Port: * 37777

Group Name: Default Group

User Name: *

Password:

Figure 5-6

Step 2 Set device parameters. For specific parameter descriptions, please refer to Table 5-2.

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 5-2

Step 3 Click “Add” to add a device.

The system displays the added device list, as shown in Figure 5-4. Available operations are shown in Table 5-1. In “Access” tab, display doors under the access controller, as shown in Figure 5-7.

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”.

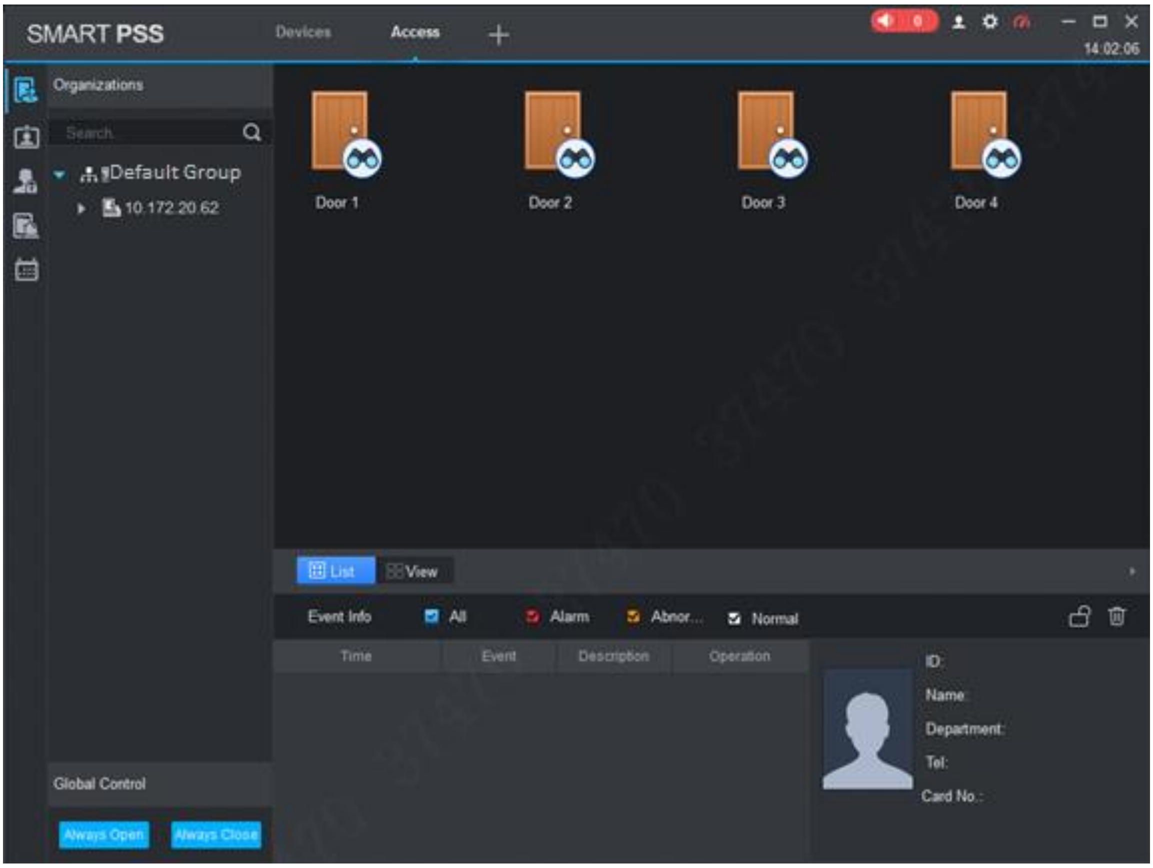


Figure 5-7