Access Main Controller

Quick Start Guide

V1.0.0

Foreword

General

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

Version	Revision Content	Release Time
V1.0.0	First release.	March 2020

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 jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.

- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

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

Operating Requirement

- Do not place and install the device in an area exposed to direct sunlight or near heat generating device.
- Do not install the device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device; don’t put on the device anything filled with liquids to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- The device must be used with screened network cables.

Power Requirement

- Use electric wires (power wires) recommended by this area, which must be used within its rated specification!
- 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, refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.
- Do not cut off power supply during device upgrade. Power supply can be cut off only after the device has completed upgrade and has rebooted.

Table of Contents

1 Overview

Access main 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).

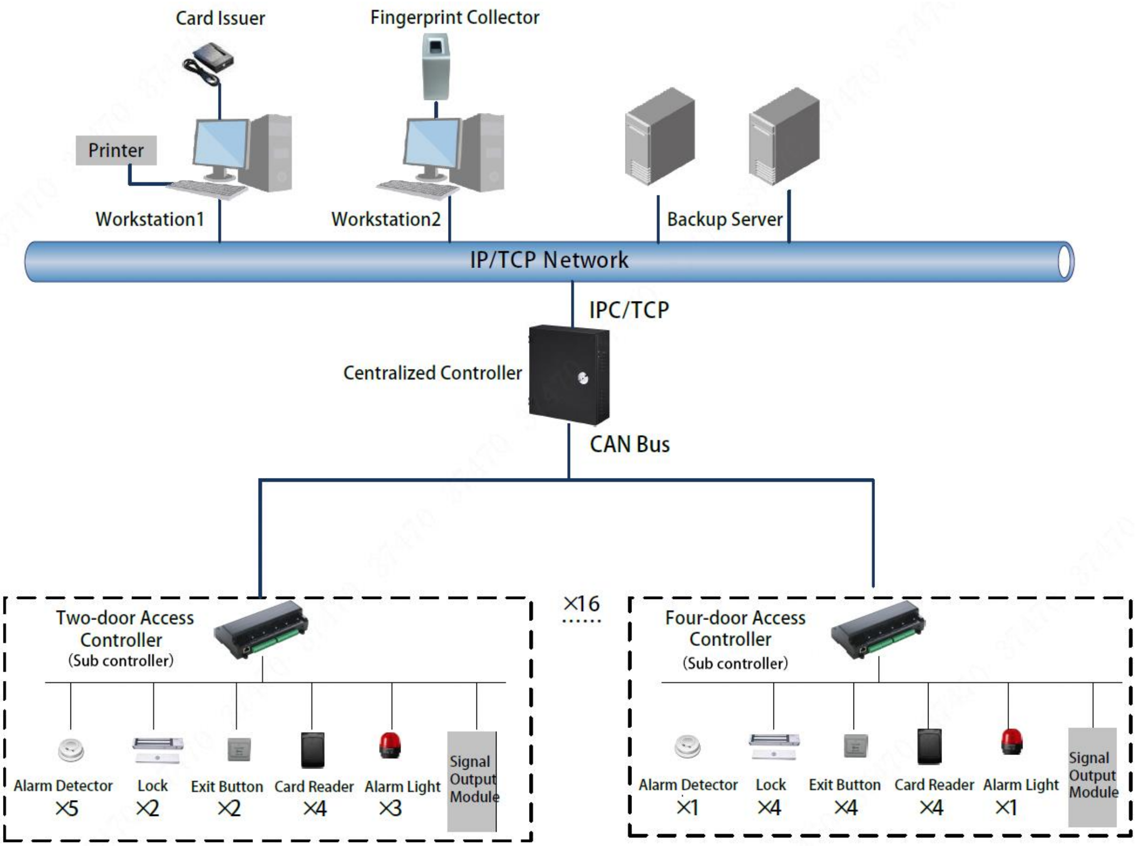
Controller Parameter

- Support three-level network mode of CAN bus, support max. 16 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 and ordinary 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°C to +60°C and working humidity: ≤95%.

2 Installation Guide

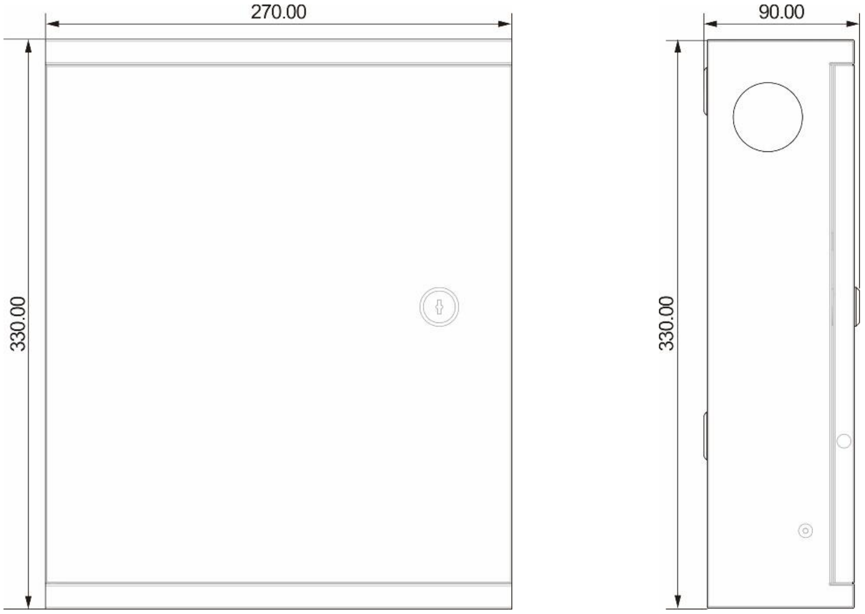
2.1 System Structure

Figure 2-1 System structure



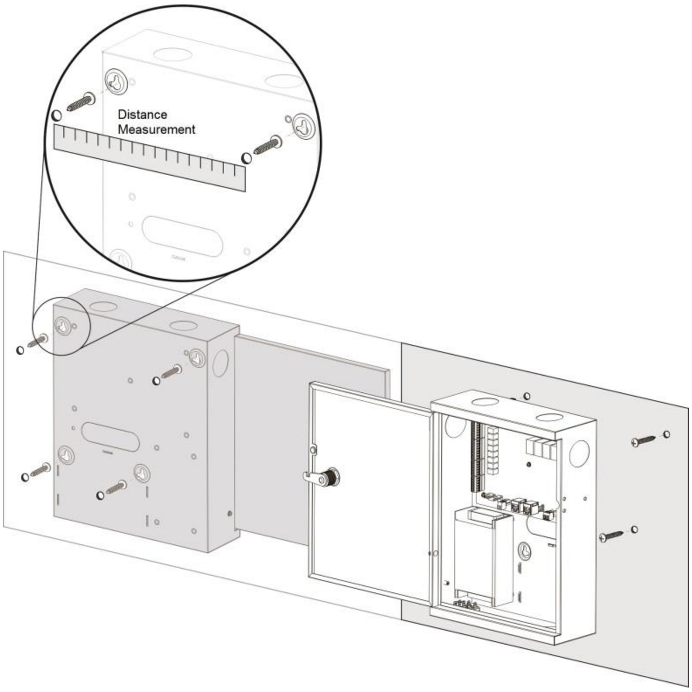
2.2 External Dimension

Figure 2-2 Dimensions (mm)



2.3 Device Installation

Figure 2-3 Installation



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

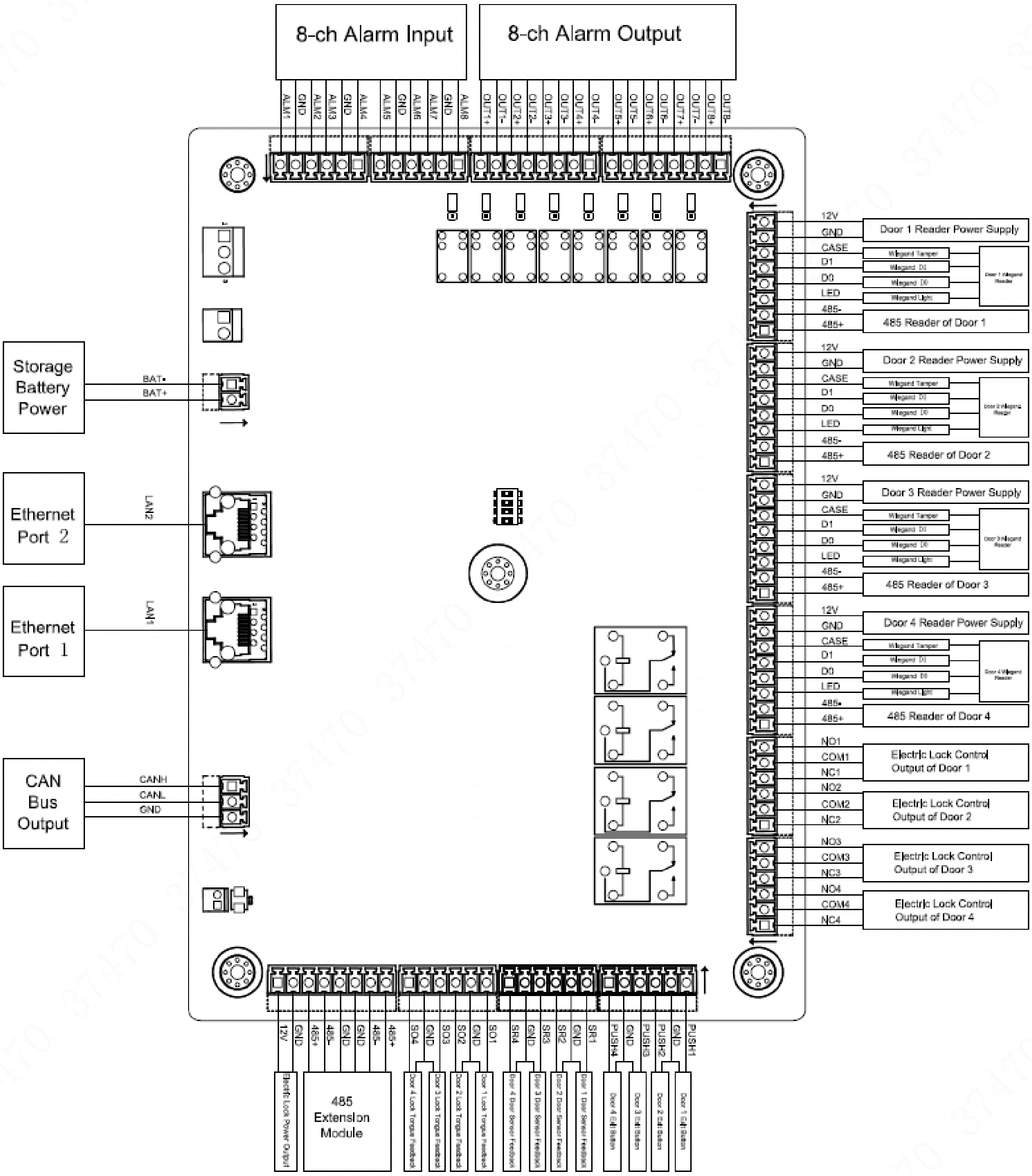
Step 1 Measure every hole distance and position according to holes at rear shell of the device; drill holes in the wall according to the measured positions.

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

Step 3 Hang the whole device onto the screws.

2.4 Wiring Diagram

Figure 2-4 Wiring diagram



2.4.1 Description of CAN Bus Wiring

Cable Requirement

- Shielded twisted pair cables (AWG20 or AWG18) are recommended. See Table 3-1 for details.

- If network cable is used, oxygen-free copper cable whose resistance is less than 10 Ω is needed.

Table 2-1 Cable requirement

Cable length	Resistance	Cable cross section area	Cable type
300 m–600 m	<40 mΩ/m	0.5 mm^2–0.6 mm^2	AWG20
600 m–1000 m	<20 mΩ/m	0.75 mm^2–0.8 mm^2	AWG18

Access main controller and sub controllers are connected by CAN bus, see Figure 2-5. For descriptions about wiring terminals, see Table 2-2. For communication distance, see Table 2-1. Data transfer rate can be set through DIP switch, for details, see "2.5 DIP Switch."

Figure 2-5 Use CAN bus to connect main and sub controllers

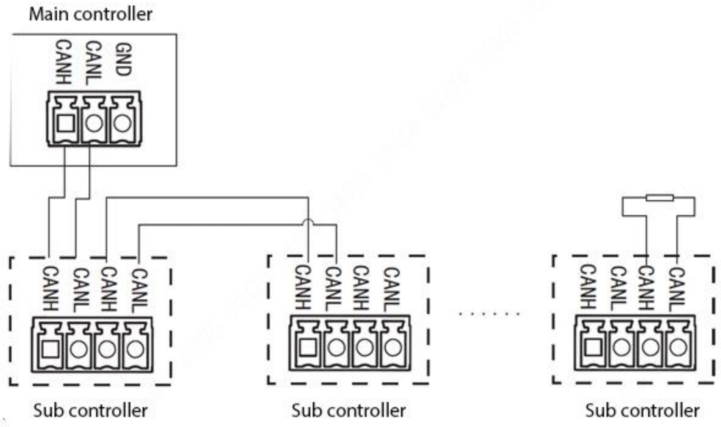


Table 2-2 Communication distance

Interface	Wiring Terminal	Description
CAN Bus	CANH	CAN bus communication
	CANL	

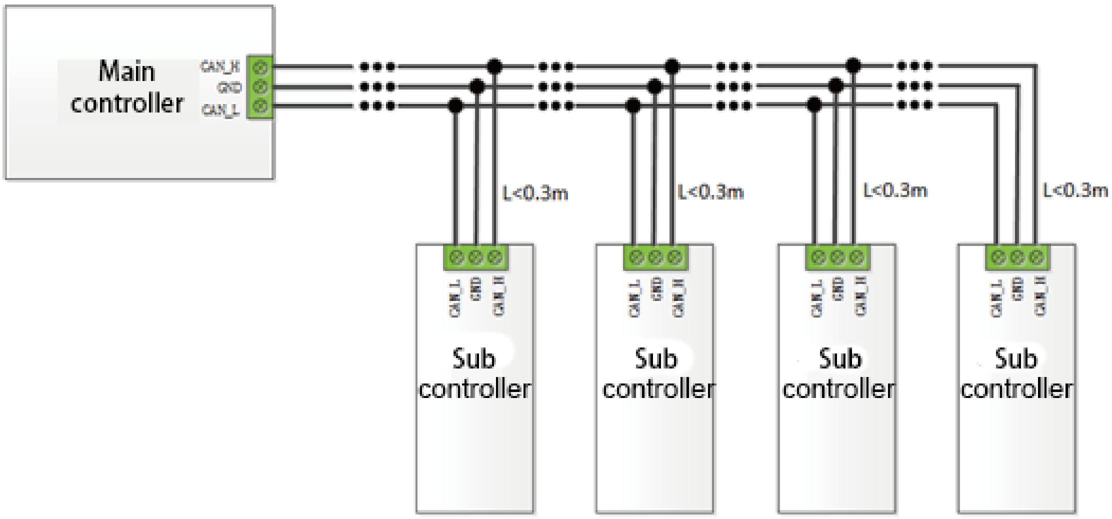
Table 2-3 Data transfer rate

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

CAN Connection Mode

"Hand-in-Hand" Connection

Figure 2-6 Hand-in-hand connection



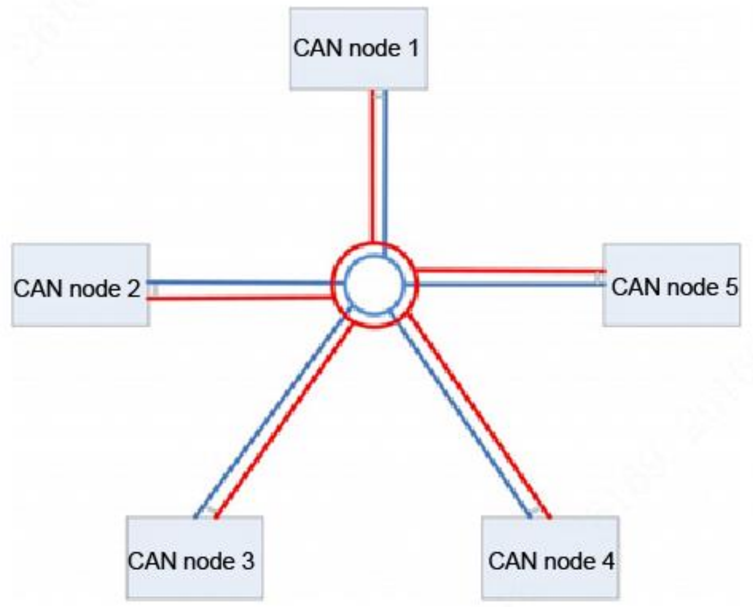
- Connect main controllers and sub controllers by terminal resistance, and 200Ω or 220Ω resistances are recommended. Do not connect peripheral terminal resistances to the main controller because there are already resistances integrated in the main controller. In certain cases, peripheral terminal resistances are needed to do minor adjustment.
- When connecting cables, if T-shaped branch cable layout appears, the T-shaped cable length is not allowed to exceed 0.3 m.
- If network cables are used to transmit data, the cables not used in the network must be all connected to ground cables (no less than two cores). When using one-layer network cable, the shielded layer can be connected to the GND.

- When the distance between main controller and sub controllers is too short, and if there is great common-mode voltage difference and common-mode interference, you can only use CANL and CANH to transfer data without connecting GND.
- When the distance between main controller and sub controllers is far and power supply mode is complex, GND cable must be connected and the GND cable resistance should be as low as possible.

"Non-Hand-in-Hand" Connection

- For the star-shaped cable connection, if the cable lengths are equal, concentrators are not necessary. You just need to adjust terminal resistance.
- R=n×60Ω (R refers to terminal resistance of each branch, and n refers to branch number).

Figure 2-7 Non-hand-in-hand connection



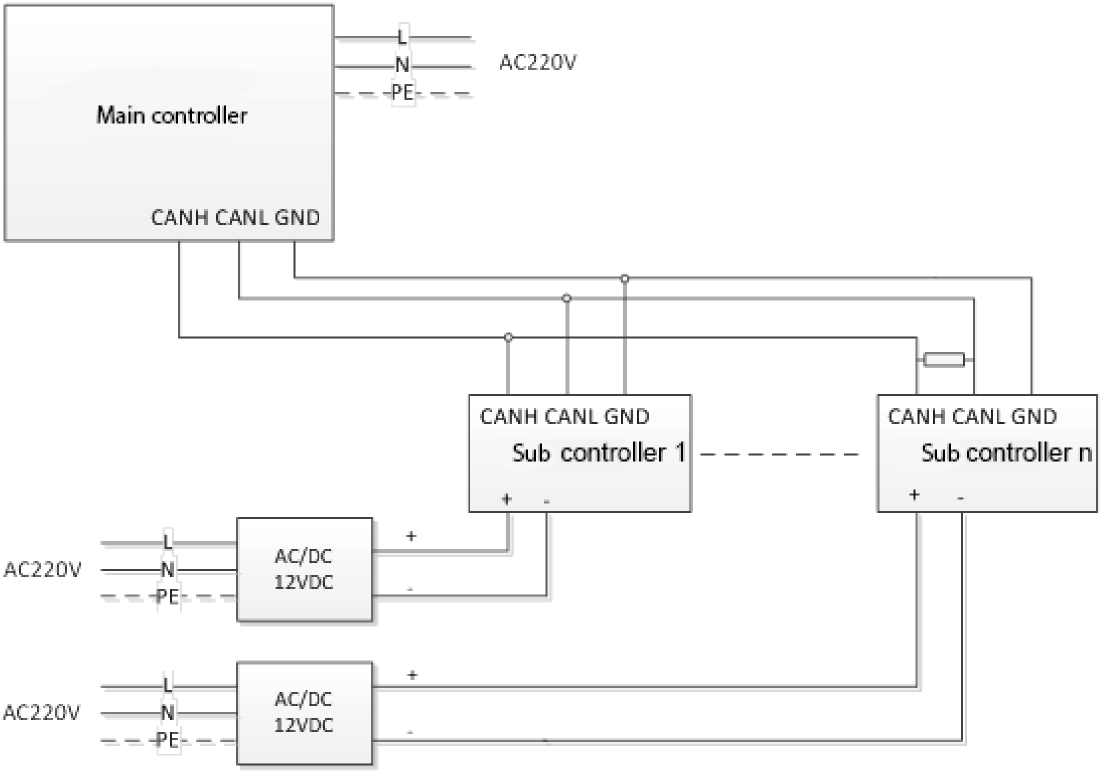
Power Cable Connection

There is a power adapter within the main controller. To provide power for the main controller, connect the main controller to 220V AC power source. Sub controllers are without power adapters. You need to connect them to 12V DC power source.

- In the CAN bus, there must be only one power negative GND connected to PE; otherwise electrical ground loop might occur.
- Currently, PE and GND of the main controller are connected, but PE and GND of sub controllers cannot be connected. When earth leakage protection occurs, you must disconnect the main controller from the PE cable.

- Use a multimeter to test whether there is electric current between negative electrode of the main controller and power adapter cover. If there is no electric current between them, power negative GND was not connected to PE.
- Generally, earth leakage will not occur to the main controller because the current of the main controller is low. You need to pay attention to earth leakage when the main controller and peripheral devices share the GND.

Figure 2-8 Power cable connection



After connecting the CAN bus, stability test must be done for each device. The stability test period must not be less than three days.

2.4.2 Wiring Description of External Alarm Input

Support 8-channel external alarm input ports.

Figure 2-9 External alarm input

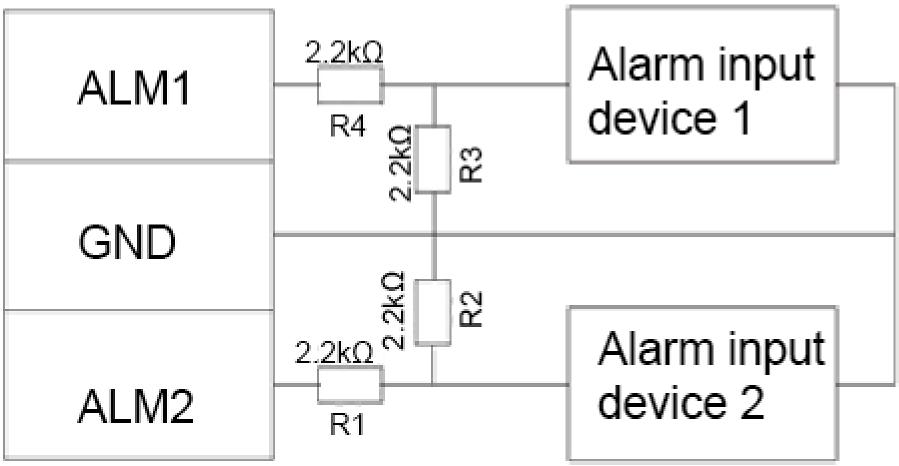


Table 2-4 Terminal description

Interface	Wiring Terminal		Description
External Alarm Input	ALM1	Alarm input port 1	External alarm input ports connect smoke detectors, and
	GND	Alarm input port 1 and 2	

Interface	Wiring Terminal		Description
	ALM2	Alarm input port 2	IR detectors, and more.
	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 2-5 Connection troubleshooting

Status	ALMIN Value	Description
Open Circuit	ALMIN=3.0V	The cable connected to peripheral alarm input devices is not connected.
	ALMIN=0V	The cable connected to peripheral alarm input devices is in short circuit.
Normal	ALMIN=1.5V	Peripheral alarm input devices are correctly connected, and there are no alarm events.
Alarm	ALMIN=1.0V	Peripheral alarm input devices are correctly connected, and there are alarm events.

2.4.3 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.

Figure 2-10 External alarm output (1)

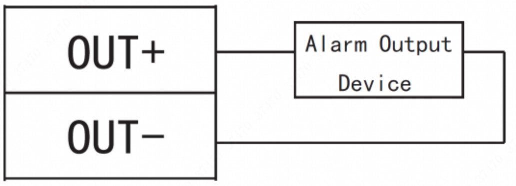


Figure 2-11 External alarm output (2)

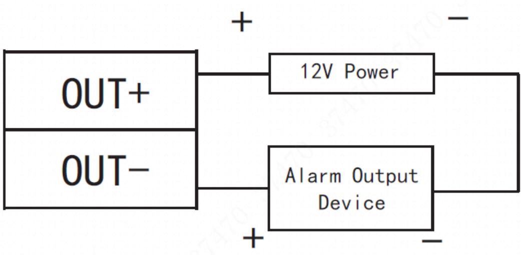


Table 2-6 Terminal description

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

2.4.4 Wiring Description of Reader

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

Refer to Table 2-7 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 2-8 for descriptions of video cable specification and length.

Table 2-7 Terminal description

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 2-8 Cable specification and length

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

2.4.5 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 2-12, Figure 2-13, and Figure 2-14. Please refer to Table 2-9 for descriptions of wiring terminals.

Figure 2-12 Connection mode (1)

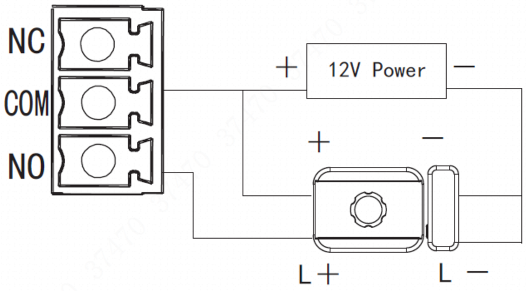


Figure 2-13 Connection mode (2)

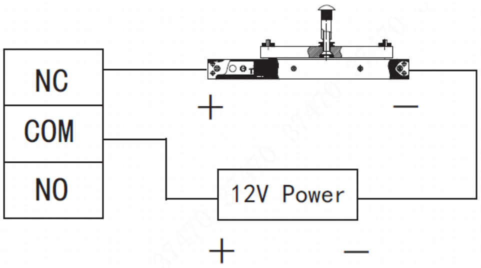


Figure 2-14 Connection mode (3)

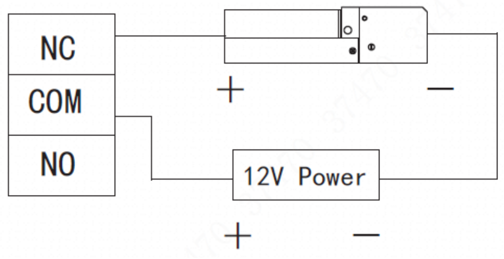


Table 2-9 Terminal description

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	

2.4.6 Wiring Description of Exit Button

Corresponding wiring terminals of exit button are shown in Figure 2-15.

Figure 2-15 Wiring exit button terminals

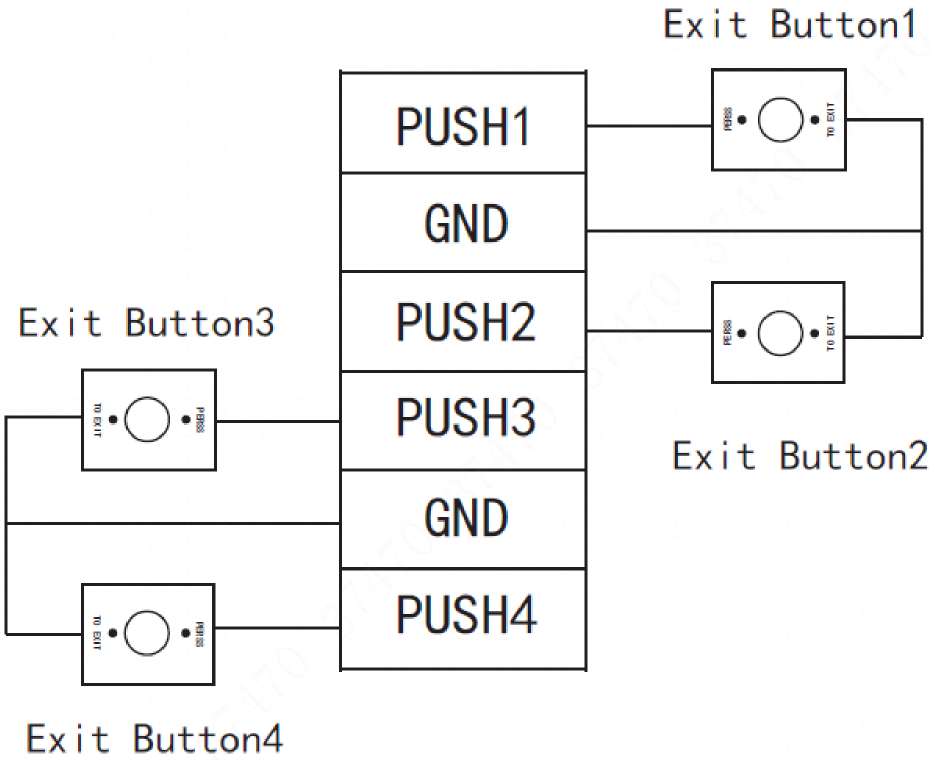


Table 2-10 Terminal description

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

2.4.7 Wiring Description of Door Sensor

See the figure below for wiring terminals of door sensor.

Table 2-11 Wiring door sensor terminals

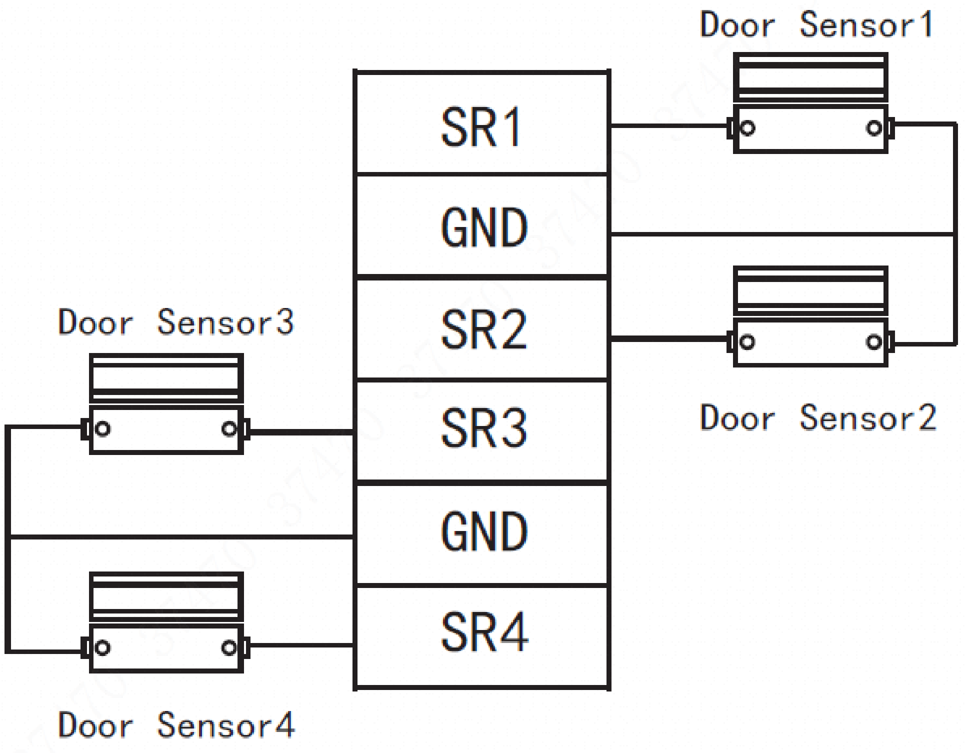


Table 2-12 Terminal description

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

2.5 DIP Switch

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

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

Figure 2-16 DIP switch

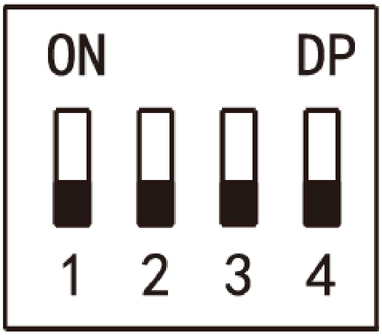
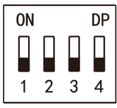
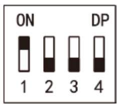
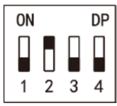
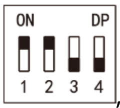


Table 2-13 Function description

Function	No.	Description
Speed	1–4	Set the speed. ● All of them are at the bottom , transmission speed is 50 kb/s. ● Only digit 6 is at ON position , transmission speed is 80 kb/s. ● Only digit 7 is at ON position , transmission speed is 100 kb/s. ● Digits 6 and 7 are at ON position , transmission speed is 125 kb/s.

2.6 Reset

Insert a needle into RESET hole, and press and hold for a few seconds to restart the controller.

3 Web Configuration

Default IP address of access main 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.

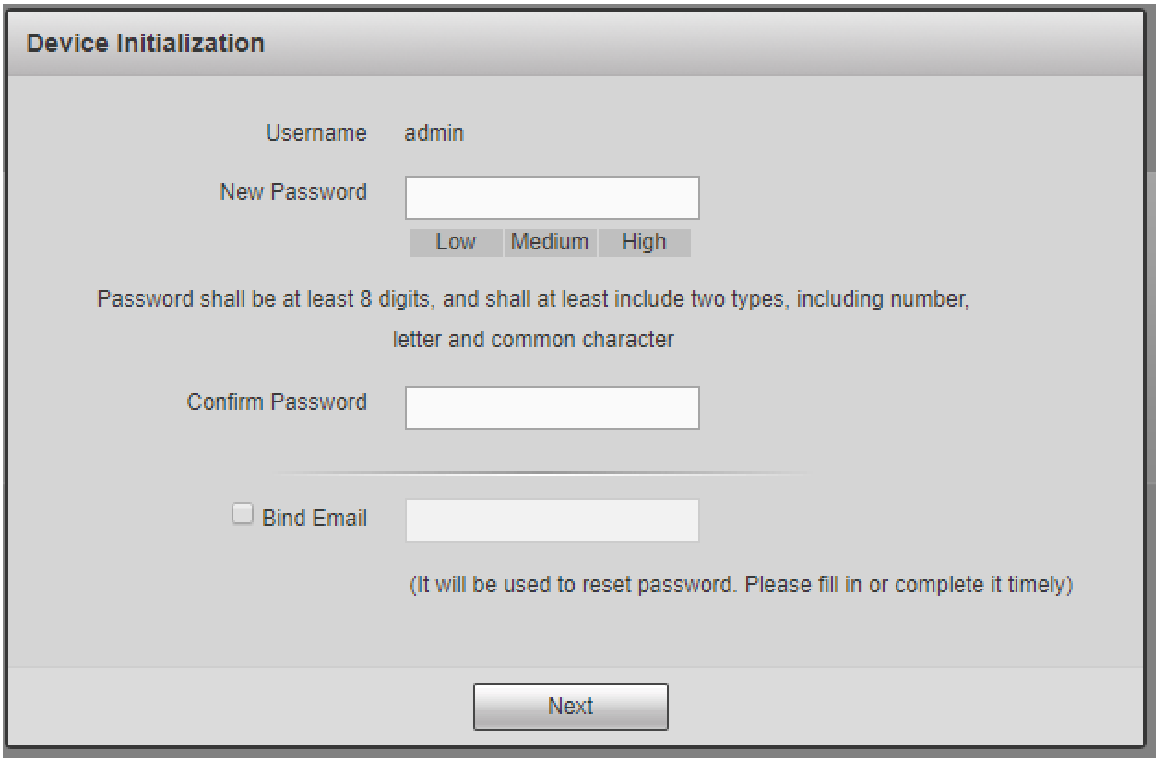
3.1 Initialization

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

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 main controller in the address bar, and press Enter.

Figure 3-1 Device initialization



Device Initialization

Username admin

New 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

□ Bind Email

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

Next

Step 2 Set admin login password and Email.

- The password can be set with 8–32 digits of characters, and must 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**.

Step 4 Click **OK**.

3.2 Login

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

Step 2 Input username and password.

- 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**.

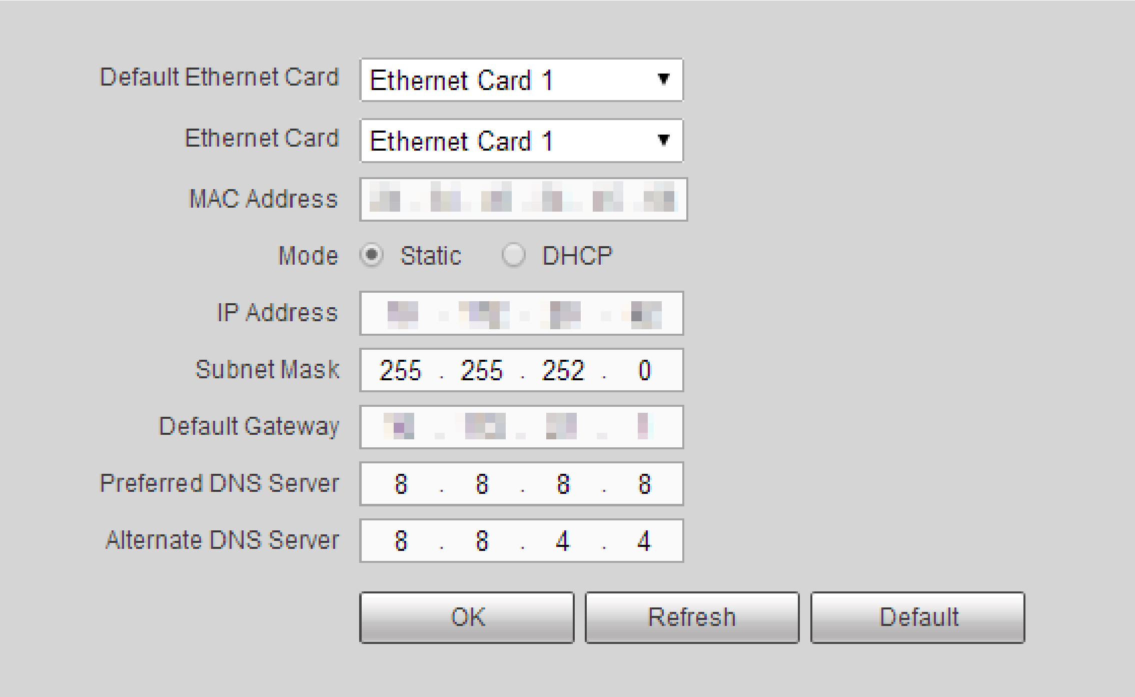
The **Preview** interface is displayed.

3.3 Set Network

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

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

Figure 3-2 TCP/IP



Default Ethernet Card	Ethernet Card 1 ▼
Ethernet Card	Ethernet Card 1 ▼
MAC Address	[redacted]
Mode	● Static ○ DHCP
IP Address	[redacted]
Subnet Mask	255 . 255 . 252 . 0
Default Gateway	[redacted]
Preferred DNS Server	8 . 8 . 8 . 8
Alternate DNS Server	8 . 8 . 4 . 4

Step 2 Set TCP/IP parameters.

Table 3-1 Parameter description

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 must 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. 📖 IP address and default gateway must 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.

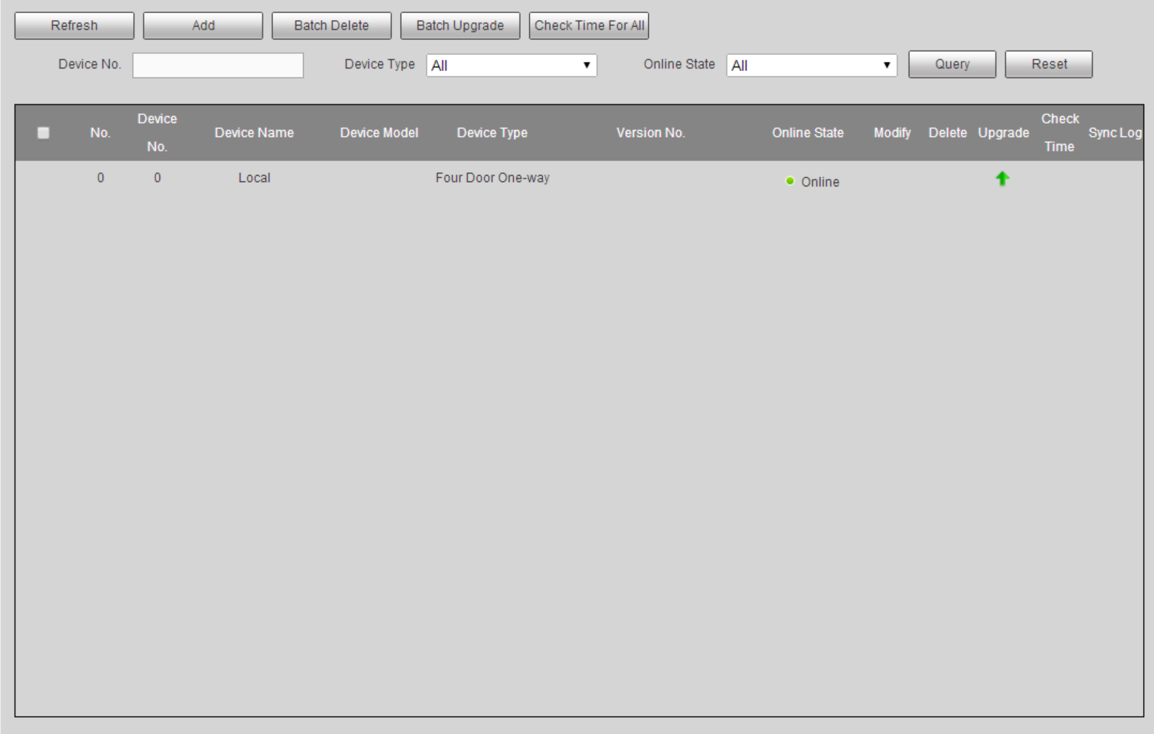
Step 3 Click **OK** to complete setting.

3.4 Add Access Controller

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

Step 1 Select **Access** > **Device Management**.

Figure 3-3 Device management



Device No.:

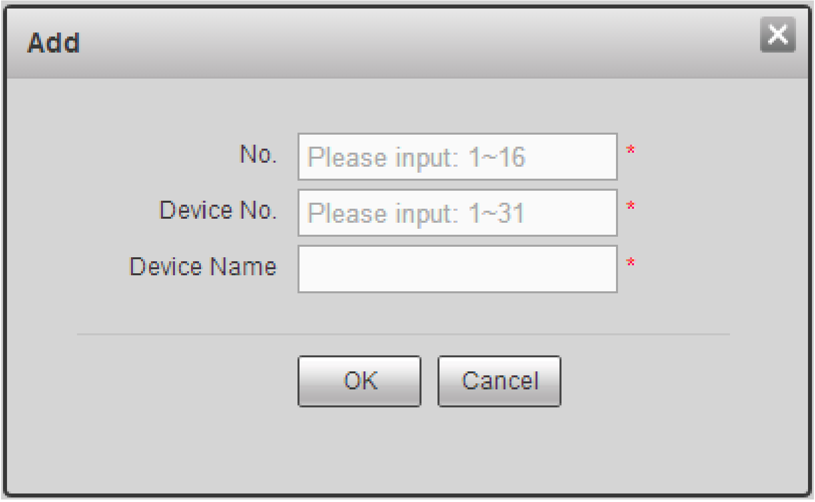
Device Type: All

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			↑		

Step 2 Click **Add**.

Figure 3-4 Add a device



No.: Please input: 1~16 *

Device No.: Please input: 1~31 *

Device Name: *

Step 3 Input No., device No., and device name.

Table 3-2 Parameter description

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.
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. The name cannot be repeated.

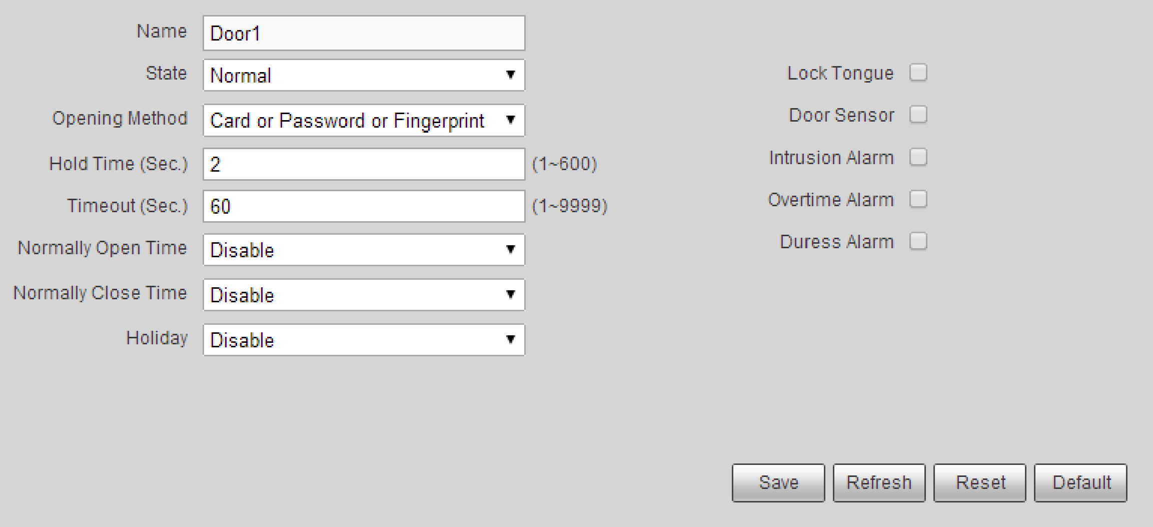
Step 4 Click **OK**.

3.5 Set Door Parameters

Configure parameters of doors under access controller.

Step 1 Select **Access > Door Parameters**.

Figure 3-5 Door parameter



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 □

Step 2 Select a door in the device tree in the left, and configure the door parameters.

Table 3-3 Parameter description

<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">In the drop-down list, select a synchronously set period in Smart PSS client.
● Disabled: period control is not</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</td></tr>
</table>

Parameter	Description	
	holiday period, and becomes ineffective after the period.	enabled. ● All day: this setting is executed 24 hours a day.
Lock Tongue	Tick the checkbox to enable lock tongue function. Judge and alarm according to lock tongue status.	
Door Sensor	Tick the checkbox to enable door sensor function. Judge and alarm according to door sensor status.	
Intrusion Alarm	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.	🕮 While the alarm is enabled, corresponding lock tongue or door sensor must 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".	
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.	

Step 3 Click **Save**.

🕮

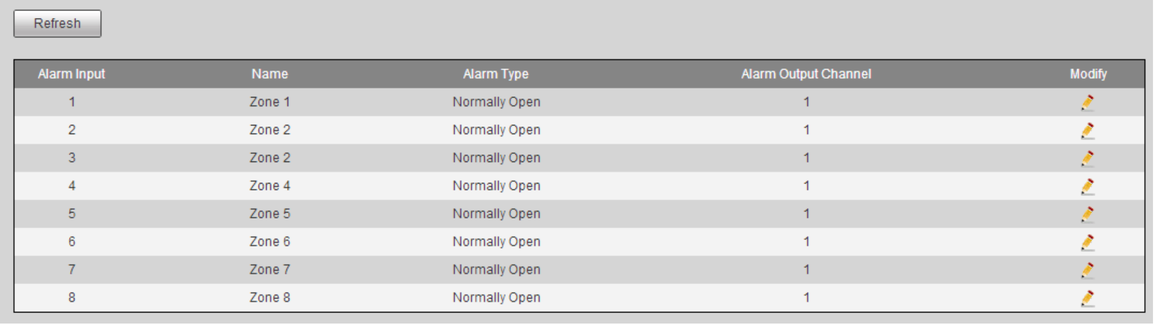
If access main controller connects Smart PSS client, relevant parameters and alarms will be synchronized with the client. Parameters modified in the client will also be synchronized with main controller.

3.6 Set Alarm Linkage

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

Step 1 Select **Access** > **Alarm Linkage**.

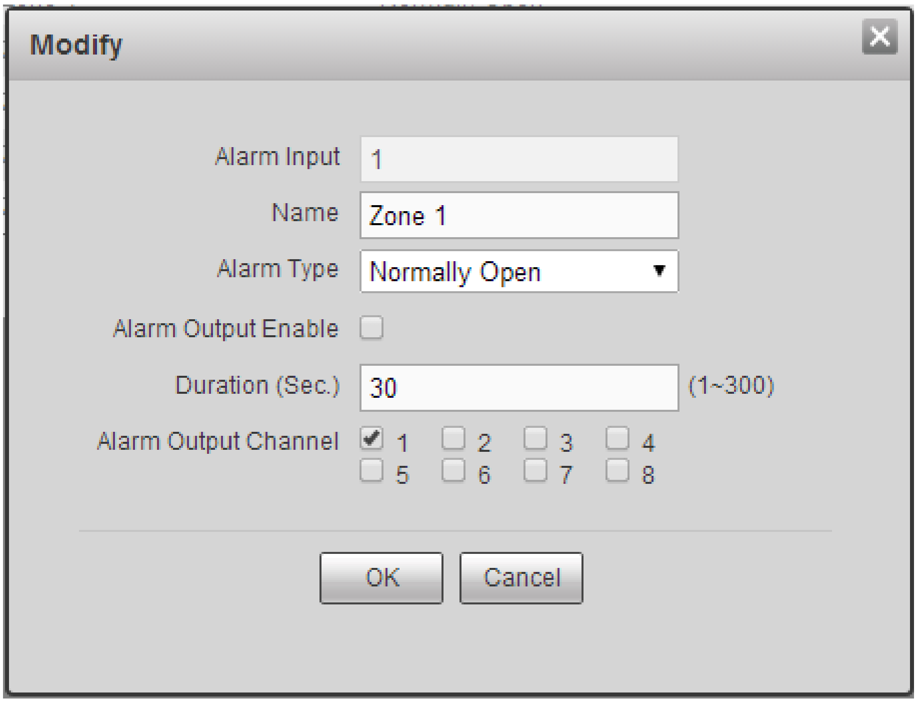
Figure 3-6 Alarm linkage



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	✎

Step 2 Click ✎.

Figure 3-7 Modify alarm information



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

Step 3 Configure parameters.

Table 3-4 Parameter description

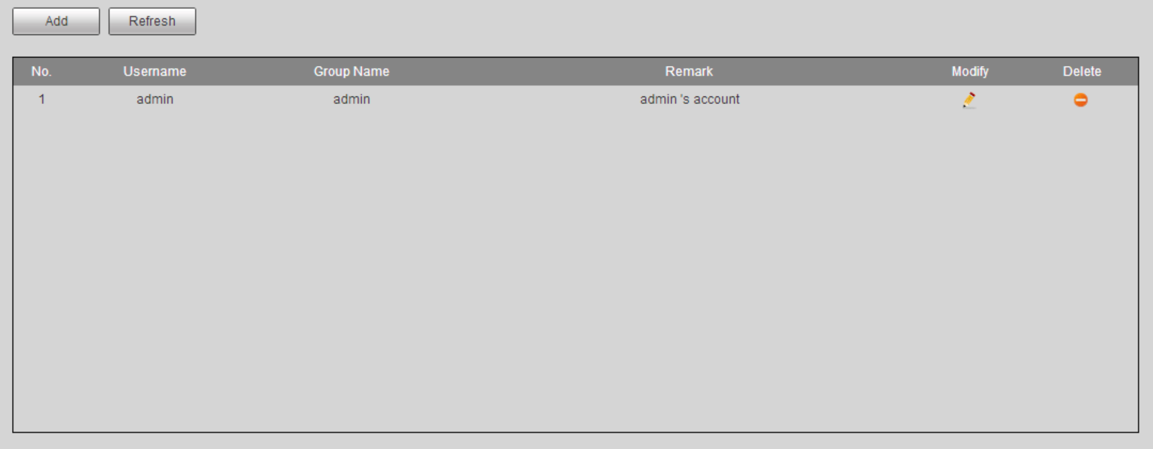
Parameter	Description
Alarm Input	Display the present alarm input.
Name	Customize alarm input name.
Alarm Type	Alarm type is consistent with the terminal.
Alarm Output Enable	Tick the checkbox to enable alarm output, so as to upload alarm to the platform synchronously.
Duration (Sec.)	Alarm duration.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

Step 4 Click **OK**.

3.7 Add User

Step 1 Select **System** > **User Management**.

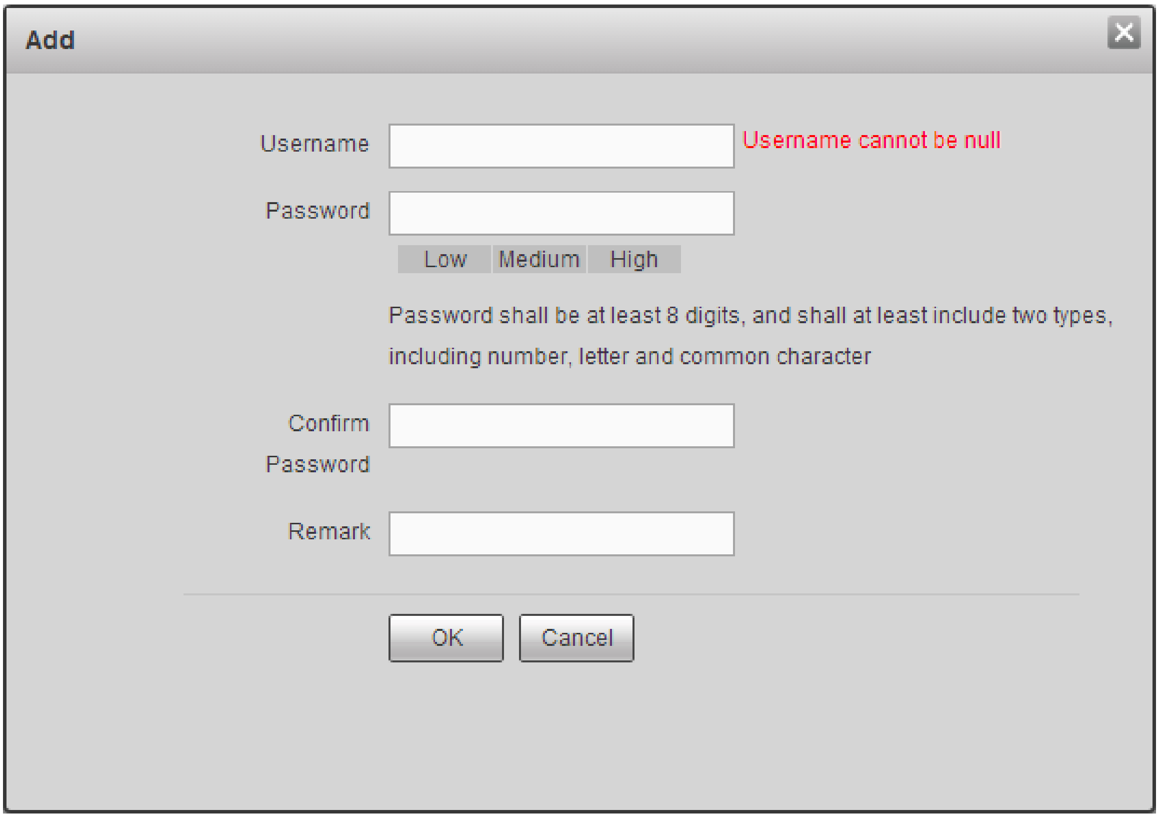
Figure 3-8 User management



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

Step 2 Click **Add**.

Figure 3-9 Add a user



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

Step 3 Input username, password, confirm password, and remark.

Step 4 Click **OK**.

4 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.

Smart PSS client offers different interfaces for different versions. The actual interface must prevail.

4.1 Login Client

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

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**.

Figure 4-1 Auto search

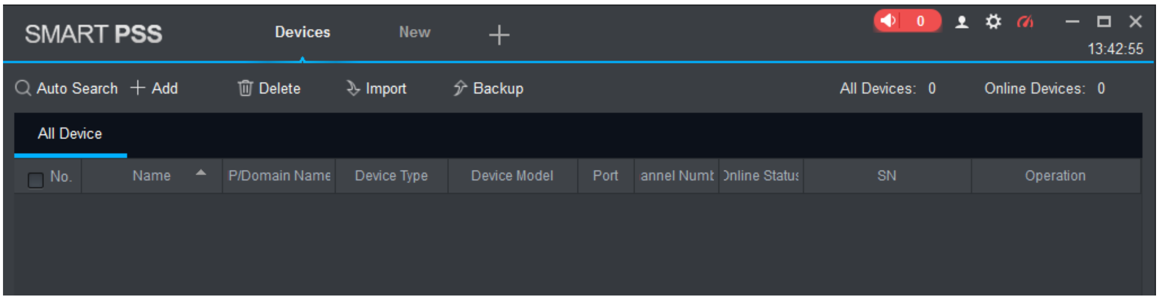
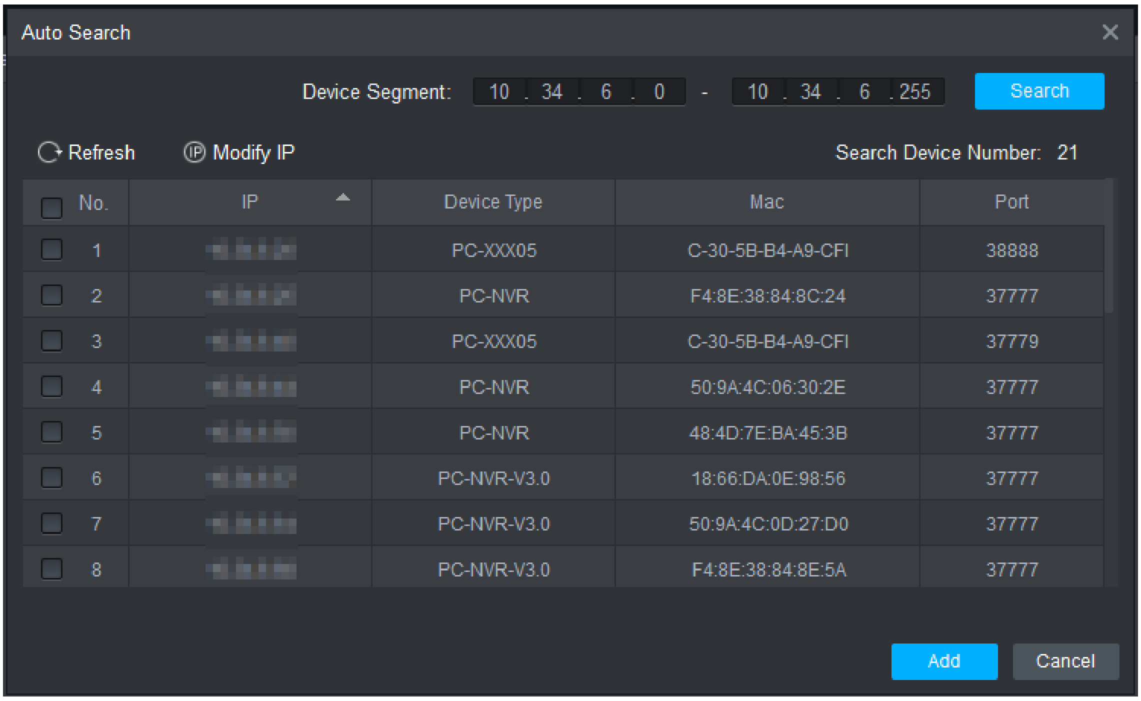


Figure 4-2 Search results



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

Search Device Number: 21

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

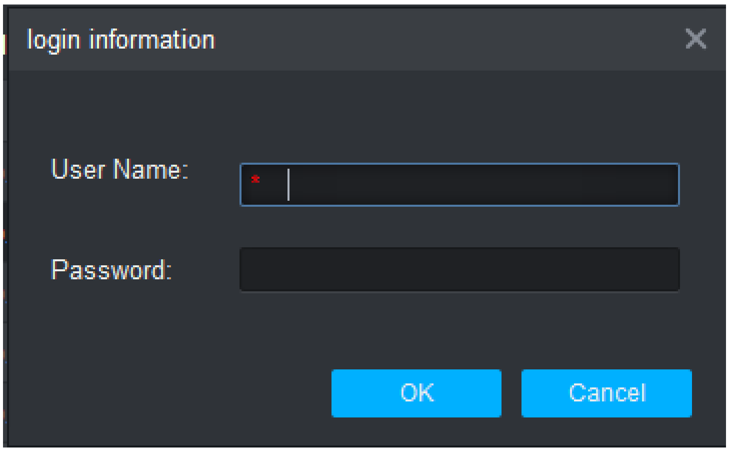
Step 2 Input device segment and click **Search**.

- 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**.

Step 4 Click **OK**.

Figure 4-3 Login information



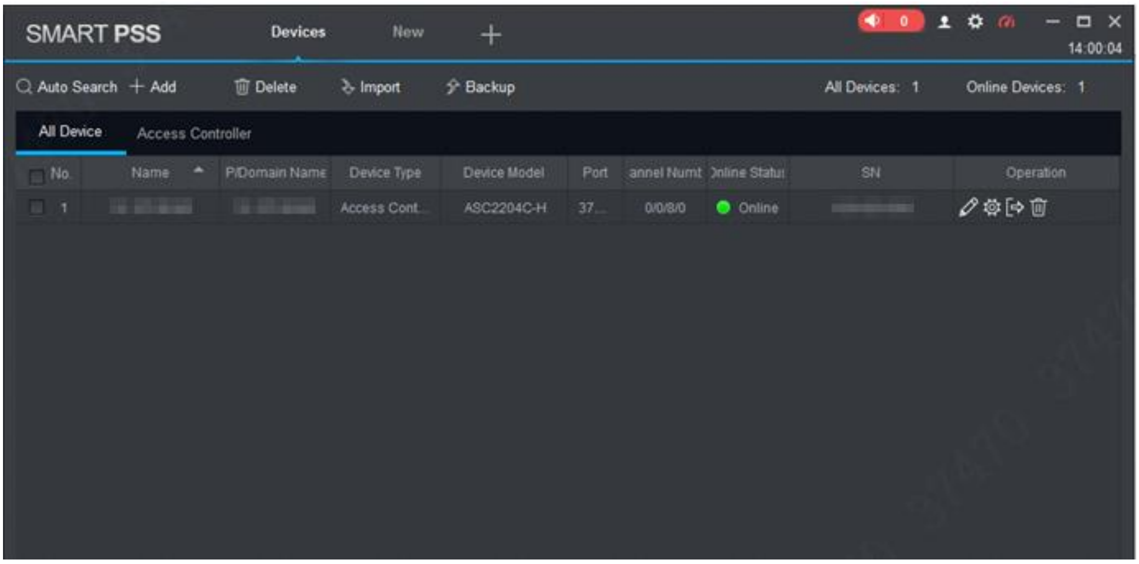
User Name: *

Password:

Step 5 Input user name and password to log in the device, and click **OK**.

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

Figure 4-4 Login



No.	Name	P/Domain Name	Device Type	Device Model	Port	annel Numb	Online Status	SN	Operation
1	[redacted]	[redacted]	Access Cont...	ASC2204C-H	37...	0/0/8/0	● Online	[redacted]	✎ ⚙ ⇨ 🗑

Table 4-1 Icon description

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 must be correct), and the icon changes to ⇨.
🗑	Click this icon to delete a device.

4.2.2 Manual Add

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

Step 1 On the **Devices** interface, click **Add**.

Figure 4-5 Manually add a device

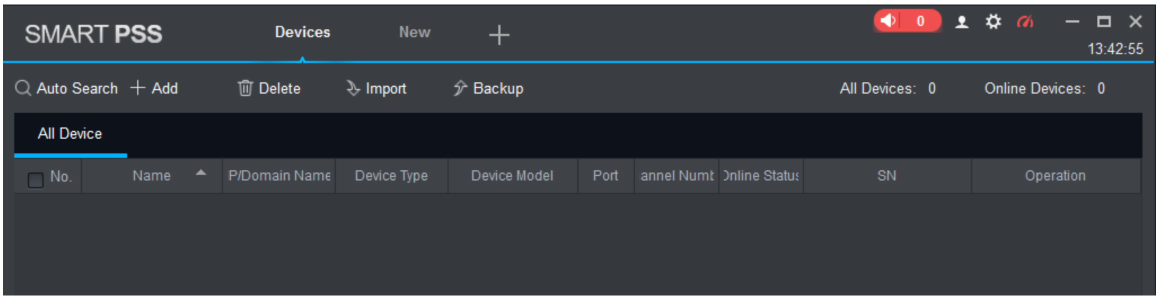
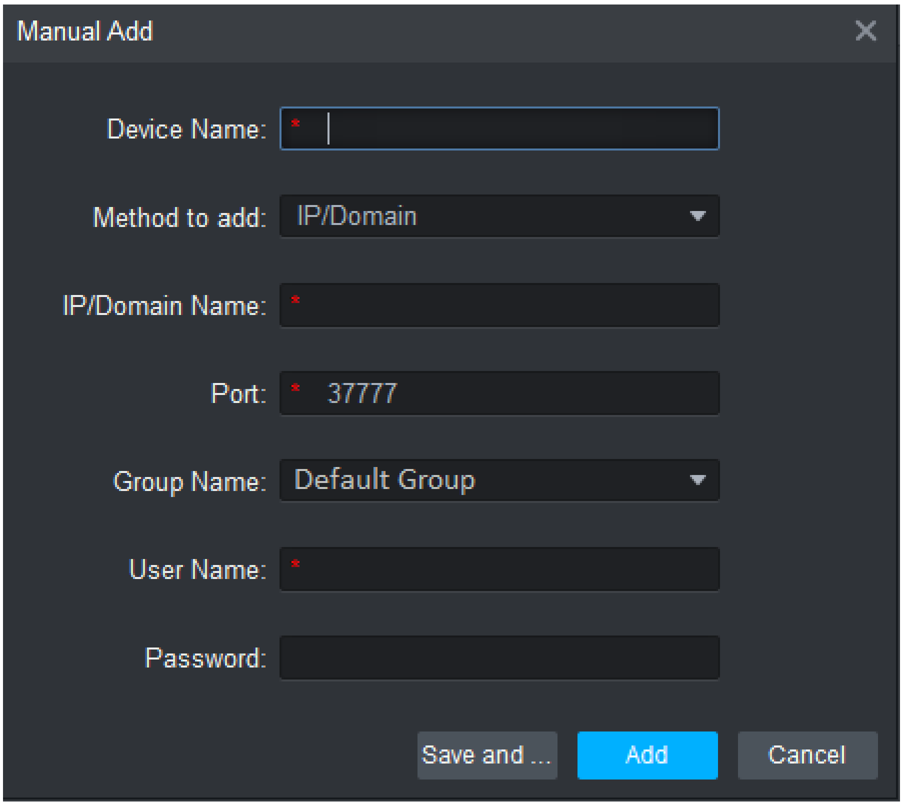


Figure 4-1 Enter information



Device Name: *

Method to add: IP/Domain

IP/Domain Name: *

Port: * 37777

Group Name: Default Group

User Name: *

Password:

Step 2 Set device parameters.

Table 4-2 Parameter description

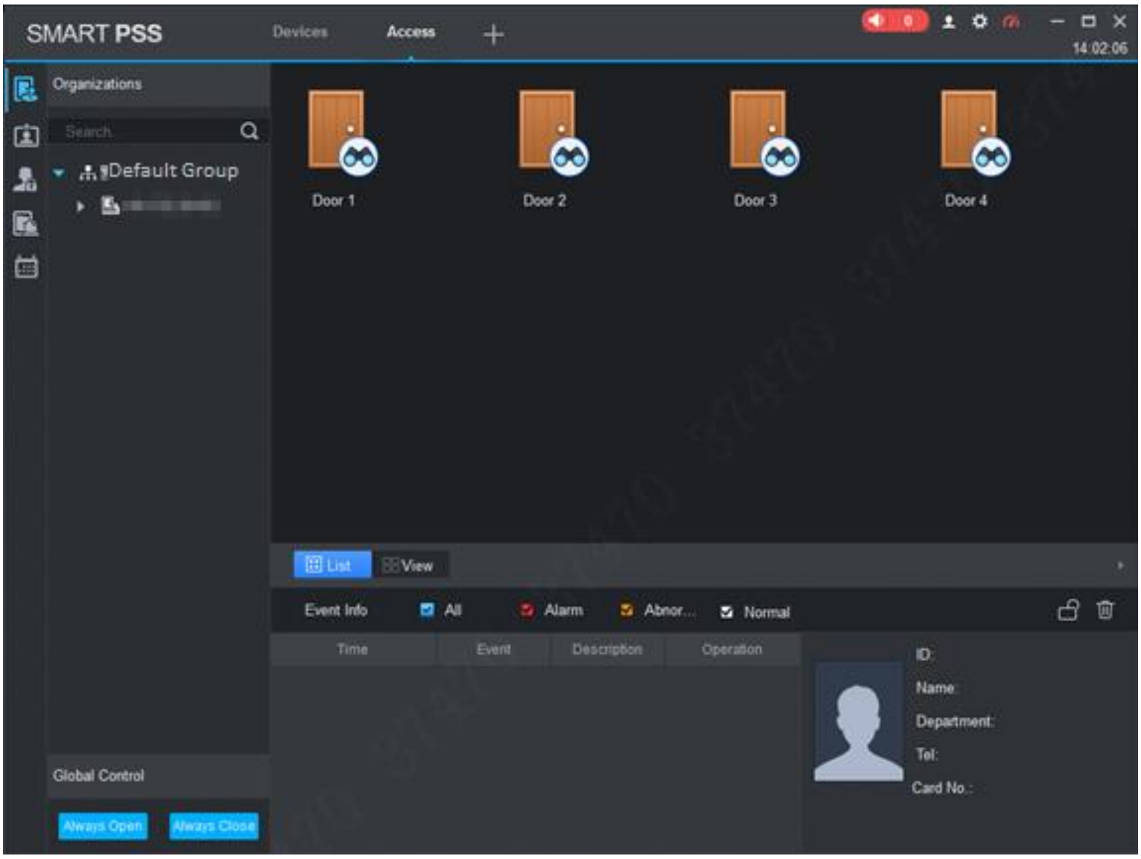
Parameter	Description
Device Name	It is suggested that device name should be named by the monitoring zone, so as to facilitate maintenance.
Method to add	Select **IP/Domain Name**. Add devices according to device IP address or domain name.
IP/Domain Name	IP address or domain name of the device.
Port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

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

- To add more devices, click **Save and Continue** to add devices.

- To cancel the adding, click **Cancel** to exit **Manual Add** interface.
- After completing adding, Smart PSS logs in to the device automatically. In case of successful login, online status is **Online**. Otherwise, **Offline** will be displayed.

Figure 4-6 Automatically log in to the device



Appendix 1 Packing List

Appendix Table 1-1 Packing list

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

Appendix 2 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

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

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

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

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

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

4. **Enable Account Lock**

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

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

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

6. **Enable HTTPS**

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

7. **MAC Address Binding**

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

8. **Assign Accounts and Privileges Reasonably**

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

9. **Disable Unnecessary Services and Choose Secure Modes**

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

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

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

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

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

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.