

Two-door Access 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 Optiview VMS:

Those using the VMS 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 Optiview VMS:

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.

General

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

Safety Instructions

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

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

Privacy Protection Notice

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

About the Manual

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



Caution

- Please change default password timely after deployment, so as not to be stolen.
- 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.



Warning

- 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 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.

Special Announcement

- This manual is for reference only. Please refer to the actual product for more details.
- This manual and program will be regularly updated according to product changes, and the updated contents will be added into the new version without prior announcement.
- The user shall undertake any losses resulting from violation of guidance in the manual.
- The manual may include technically inaccurate contents, inconsistencies with product functions and operations, or misprint. Final explanations of the company shall prevail.

Table of Contents

Cybersecurity Recommendations	2
Foreword	I
Important Safeguards and Warnings	III
Table of Contents	V
1 Overview	1
2 Appearance and Dimension	2
3 Assembly and Disassembly	3
3.1 Assembly.....	3
3.2 Disassembly.....	4
4 Interface Description	6
4.1 Interface Diagram.....	6
4.2 Wiring Description	7
4.3 Wiring Description of Peripheral Device	10
4.3.1 Wiring Description of Card Reader.....	10
4.3.2 Wiring Description of Exit Button/Door Sensor	10
4.3.3 Wiring Description of Lock.....	11
5 Client Configuration	12
5.1 Log in Client	12
5.2 Add Access Controller.....	12
5.2.1 Auto Search	12
5.2.2 Manual Add.....	14
5.3 Add Persons.....	15
5.3.1 Setting Card Type	15
5.3.2 Add User	16
5.4 Add Groups	17
5.5 Right Distribution.....	17
5.5.1 Right of Door Group.....	17
5.5.2 User Right.....	18
6 Technical Parameters	20

The two-door access 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.

Its rich functions are as follows:

- Adopt sliding rail type and lock type installation, convenient installation and maintenance.
- Integrate alarm, access control, video monitoring, fire alarm and control module input.
- Support 4 sets of card readers (may set 2 as bidirectional card readers).
- Support 9 groups of input signal (unlock button *2, door sensor *2, vandal-proof alarm *1, intrusion alarm *4).
- Support 6 groups of output control (electric lock *2, alarm output *2, device control *2).
- With RS485 port, it may extend to connect lift control module, alarm or household control module.
- FLASH storage capacity is 16M (which may extend to 32M), max supports 100,000 card holders and 150,000 records.
- Support illegal intrusion alarm, unlock overtime alarm, duress card alarm and duress code setup. It also supports black-white list and patrol card setup.
- Support setup of valid card period, password and validity. Guest card has setup of times of use.
- Support 128 groups of schedules, 128 groups of periods and 128 groups of holiday schedule.
- Data storage during outage, built-in RTC (support DST), online upgrading.

2 Appearance and Dimension

Appearance and dimension of two-door access controller is shown in Figure 2-1 and Figure 2-2. The unit is mm.

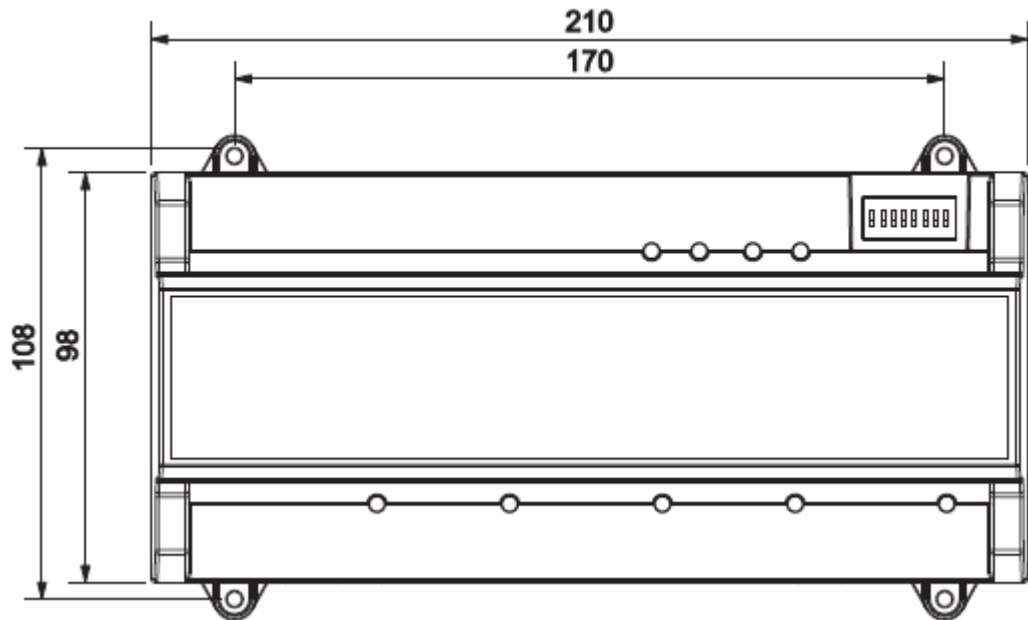


Figure 2-1

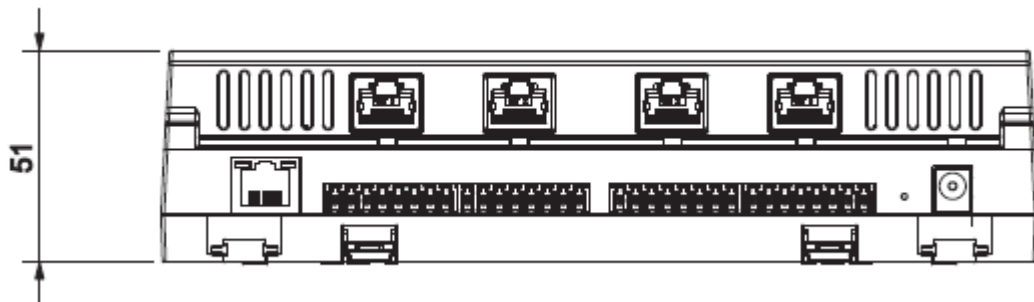


Figure 2-2

3

Assembly and Disassembly

3.1 Assembly

There are two assembly types:

- Assembly type 1: fix the whole device onto the wall with screws.
- Assembly type 2: fix the whole device onto the wall with a bracket.

Assembly type 1: fix the whole device onto the wall with screws, as shown in Figure 3-1.

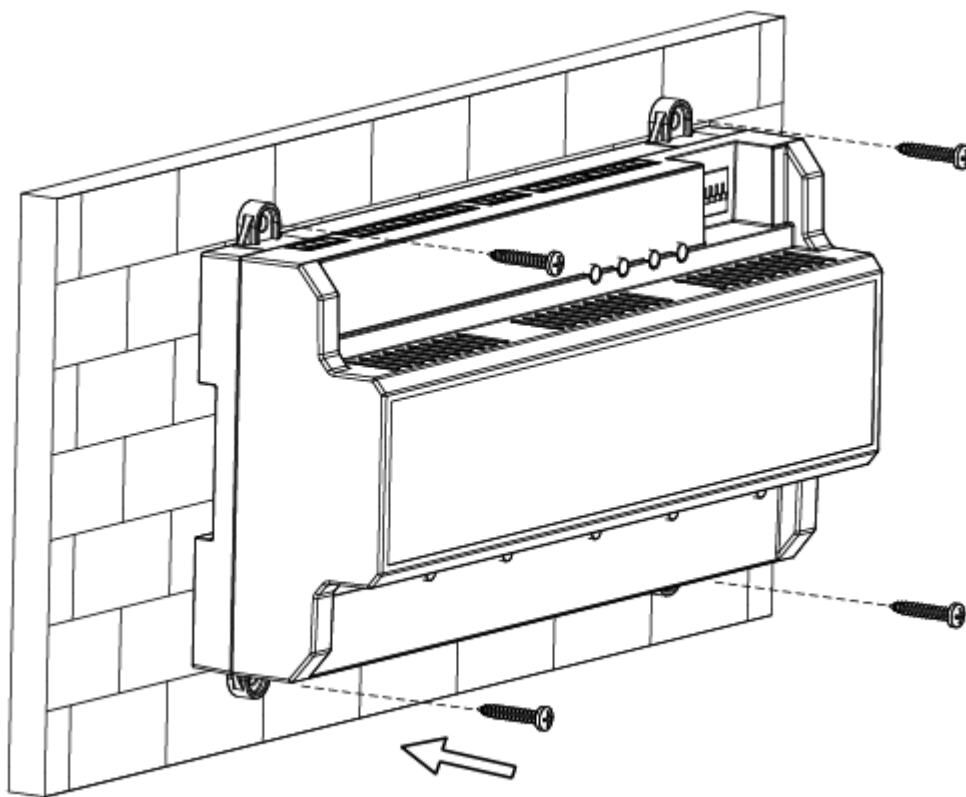


Figure 3-1

Assembly type 2 is shown in Figure 3-2.

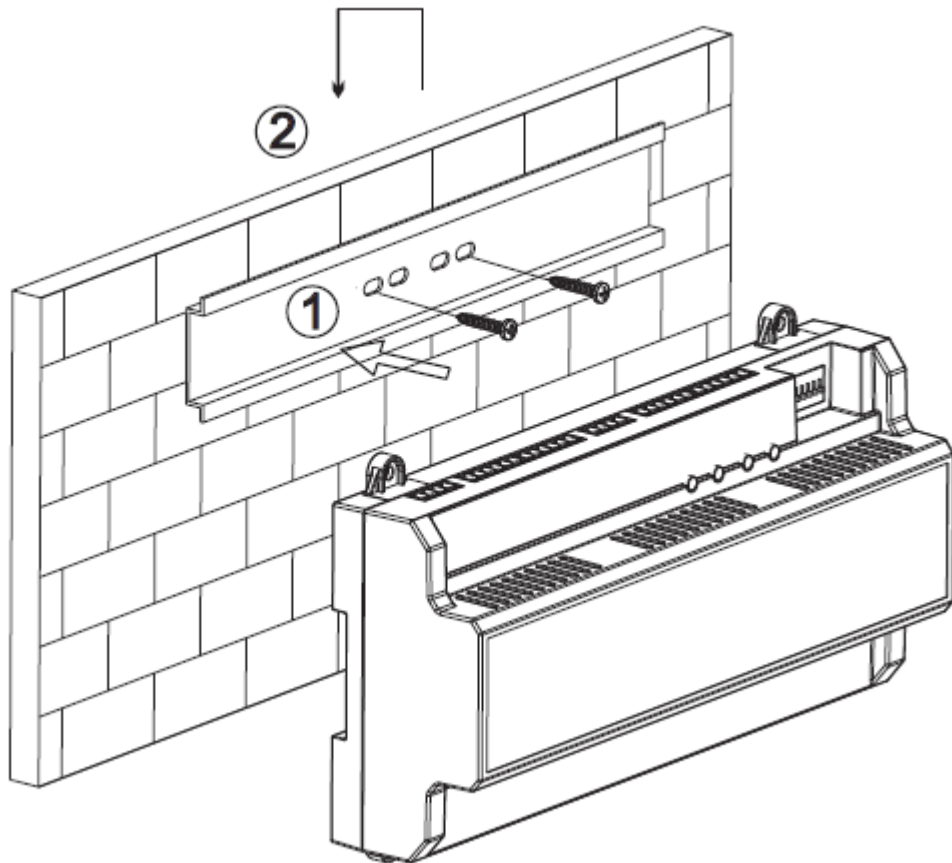


Figure 3-2

Steps of assembly type 2 are as follows:

Step 1 Fix the bracket onto the wall with screws.

Step 2 Put the upper part of rear side of the device into upper groove of the bracket, and press the lower part of the device to the bracket.

Step 3 Installation is completed when hearing that snap joint at rear side of the device is pushed in place.

3.2 Disassembly

Disassembly steps of assembly type 2 are as follows:

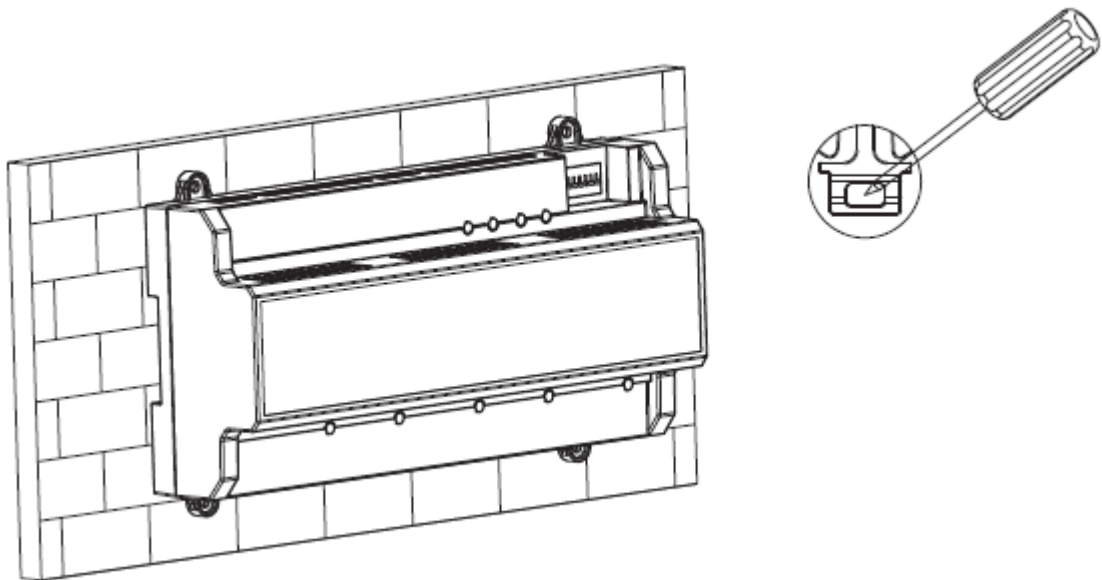


Figure 3-3

Disassembly steps:

Step 1 Point a screwdriver to the snap joint, and press it downwards hard. The snap joint will pop open.

Step 2 Open the second snap joint in the same way, so the whole device will be disassembled smoothly.

4 Interface Description

4.1 Interface Diagram

Interface diagram is shown in Figure 4-1.

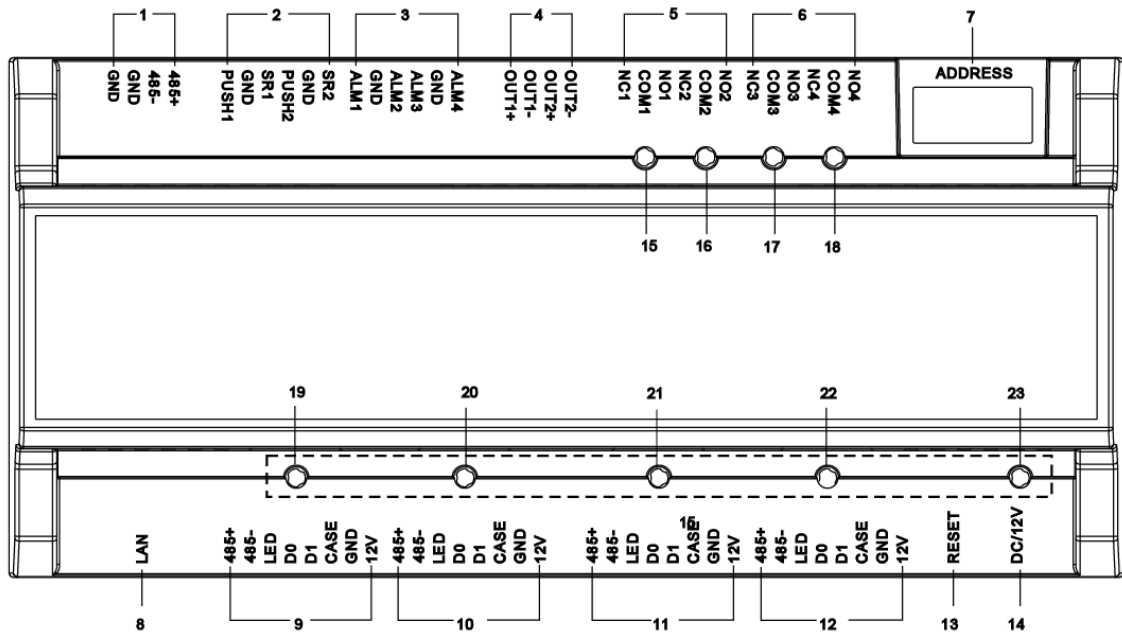


Figure 4-1

Interface description is shown in Table 4-1.

No.	Interface Description	No.	Interface Description
1	RS485 communication	8	TCP/IP, software platform interface
2	Unlock button + door sensor	9	No. 1 entry reader
3	4-ch signal alarm input	10	No. 1 exit reader
4	2-ch control output	11	No. 2 entry reader
5	Lock control output	12	No. 2 exit reader
6	Alarm control output	13	Reset switch
7	Toggle switch	14	DC 12V power interface

Table 4-1

Indicator light is described in Table 4-2.

No.	Description
15	Lock status indicator light
16	
17	Alarm status indicator light
18	

No.	Description
19	Detection indicator light of no. 1 entry reader
20	Detection indicator light of no. 1 exit reader
21	Detection indicator light of no. 2 entry reader
22	Detection indicator light of no. 2 exit reader
23	Power indicator light

Table 4-2

Note: status indicator light of reader is not available in some versions.

4.2 Wiring Description

No. 1~7 wiring terminals are shown in Figure 4-2.

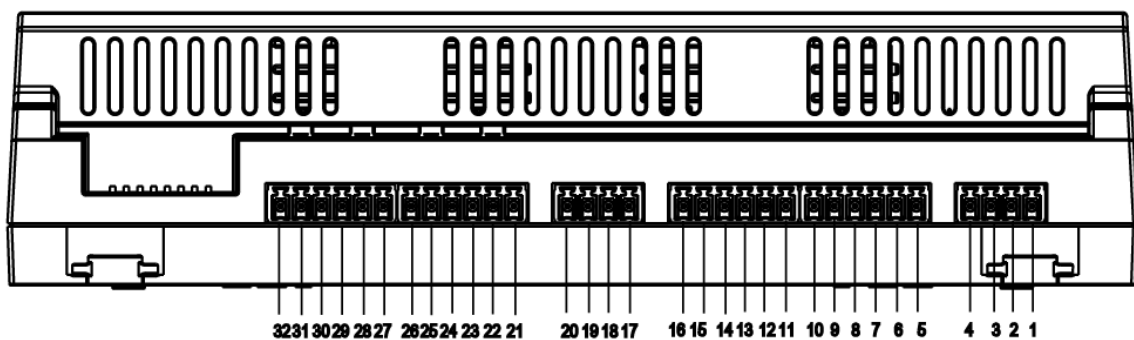


Figure 4-2

Wiring terminals corresponding to “RS485 communication” are shown in Table 4-3.

Interface	No.	Wiring Terminal
485 communication	1	GND
	2	GND
	3	485-
	4	485+

Table 4-3

Wiring terminals corresponding to “unlock + door sensor” are shown in Table 4-4.

Interface	No.	Wiring Terminal	Description
Unlock + door sensor	5	PUSH1	No. 1 exit button
	6	GND	Shared by no. 1 exit button and no. 1 door sensor input
	7	SR1	No. 1 door sensor input
	8	PUSH2	No. 2 exit button
	9	GND	Shared by no. 2 exit button and no. 2 door sensor input
	10	SR2	No. 2 door sensor input

Table 4-4

Wiring terminals corresponding to “4-ch signal alarm input” are shown in Table 4-5.

Interface	No.	Wiring Terminal	Description
4-ch signal alarm input	11	ALM1	It may connect smoke detector, sound and light alarm etc.
	12	GND	-
	13	ALM2	-
	14	ALM3	-
	15	GND	-
	16	ALM4	-

Table 4-5

Wiring terminals corresponding to “control output” are shown in Table 4-6.

Interface	No.	Wiring Terminal	Description
Control output	17	OUT1+	Signal output of no. 1 dry contact
	18	OUT1-	
	19	OUT2+	Signal output of no. 2 dry contact
	20	OUT2-	

Table 4-6

Wiring terminals corresponding to “lock control output” are shown in Table 4-7.

Interface	No.	Wiring Terminal	Description
Lock control output	21	NC1	No. 1 power-off unlocking
	22	COM1	12V power input of no. 1 lock
	23	NO1	No. 1 power-off locking
	24	NC2	No. 2 power-off unlocking
	25	COM2	12V power input of no. 2 lock
	26	NO2	No. 2 power-off locking

Table 4-7

Wiring terminals corresponding to “alarm control output” are shown in Table 4-8.

Interface	No.	Wiring Terminal	Description
Alarm control output	27	NC3	No. 1 power-off unlocking alarm
	28	COM3	12V power input of no. 1 door alarm
	29	NO3	No. 1 power-off locking alarm
Alarm control output	30	NC4	No. 2 power-off unlocking alarm
	31	COM4	12V power input of no. 2 door alarm
	32	NO4	No. 2 power-off locking alarm

Table 4-8

Wiring terminals corresponding to card readers are shown in Figure 4-3.

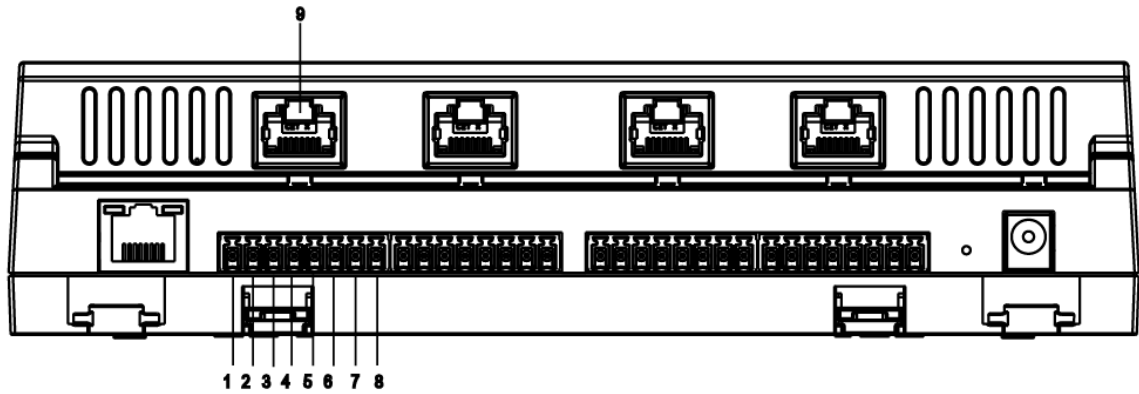


Figure 4-3

Wiring terminals corresponding to “no. 1 entry reader” are shown in Table 4-9. “No. 1 exit reader” and “no. 2 entry reader” are the same as “no. 2 exit reader” and “no. 1 entry reader”.

Interface	No.	Wiring Terminal	Description
No. 1 entry card reader	1	485+	485 card reader
	2	485-	
	3	LED	Wiegand card reader
	4	D0	
	5	D1	
	6	CASE	
	7	GND	Power supply of card reader
	8	12V	

Table 4-9

Colors of four RJ45 are shown in Table 4-10 (Not standard).

No.	Wiring Terminal	Color
9	485+	White and orange
	485-	Orange
	LED	White and green
	D0	Blue
	D1	White and blue
	CASE	Green
	GND	White and brown
	12V	Brown

Table 4-10

4.3 Wiring Description of Peripheral Device

4.3.1 Wiring Description of Card Reader

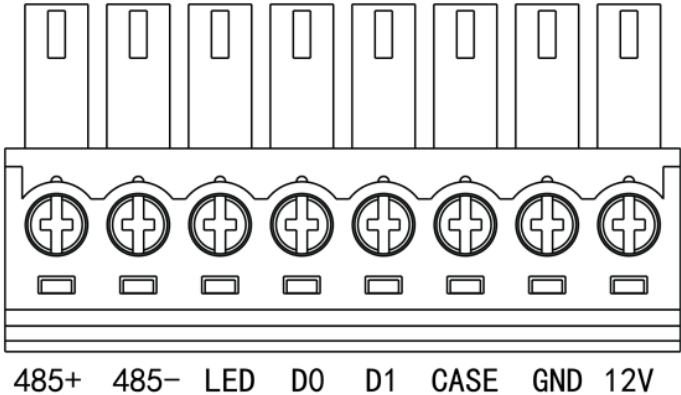


Figure 4-4

4.3.2 Wiring Description of Exit Button/Door Sensor

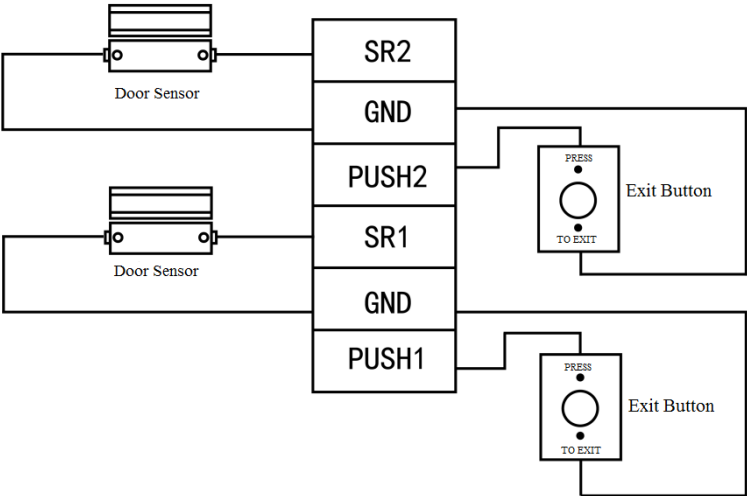


Figure 4-5

4.3.3 Wiring Description of Lock

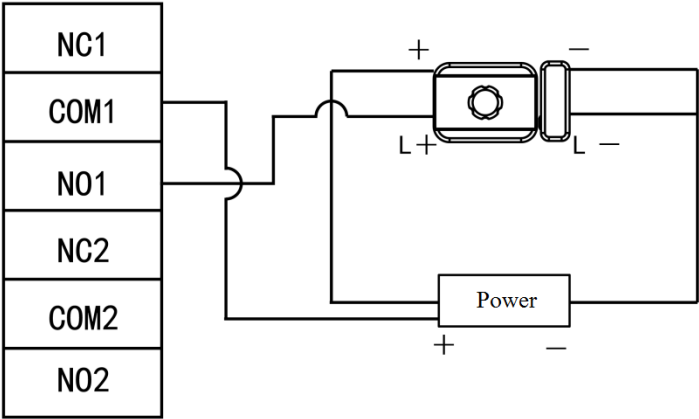


Figure 4-6

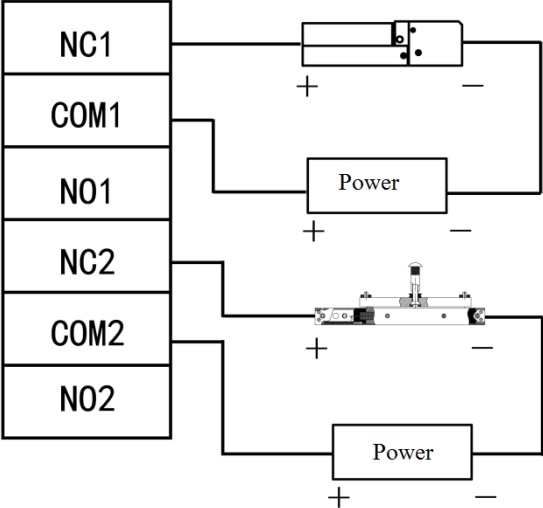


Figure 4-7

5

Client Configuration

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

5.1 Log in Client

Install the matching the Optiview VMS 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 the VMS; select “Auto Search” and “Add”.

5.2.1 Auto Search

Devices are required to be in the same network segment.

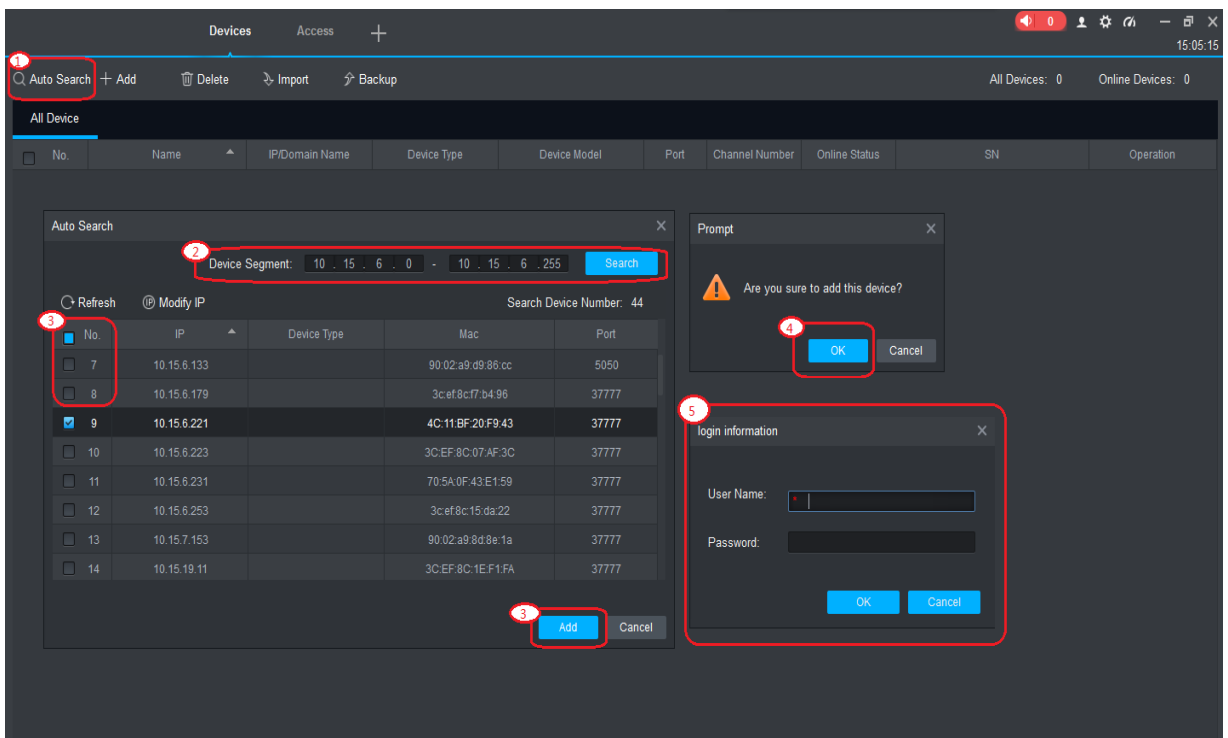


Figure 5-1

Step 1 In “Devices” interface, click “Auto Search”. The system displays “Auto Search” interface.

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 the VMS Client.

Step 3 Select the device that needs to be added, and click “Add”. The system pops up “Prompt”.

Step 4 Click “OK”, and the system displays “Login Information” dialog box.

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 5-2. 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, the VMS logs in the device automatically case of successful login, online status displays “Online”. Otherwise, it displays “Offline”.

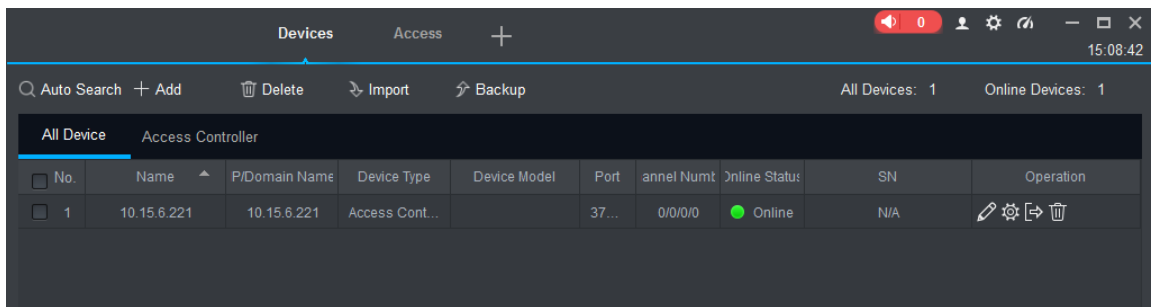











Figure 5-2

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 	<ul style="list-style-type: none"> • When the device is logged in, the icon displays . Click the icon to exit logging, and the icon changes to . • When the device is offline, the icon displays . Click the icon to log in the device (device info shall be correct), and the icon changes to .
	Click this icon to delete a device.


Icon	Description
	When choosing “Display Device ID” in system setting, operation bar displays this icon. Click this icon to customize device code, so as to operate the device when keyboard is connected.

Table 5-1

5.2.2 Manual Add

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

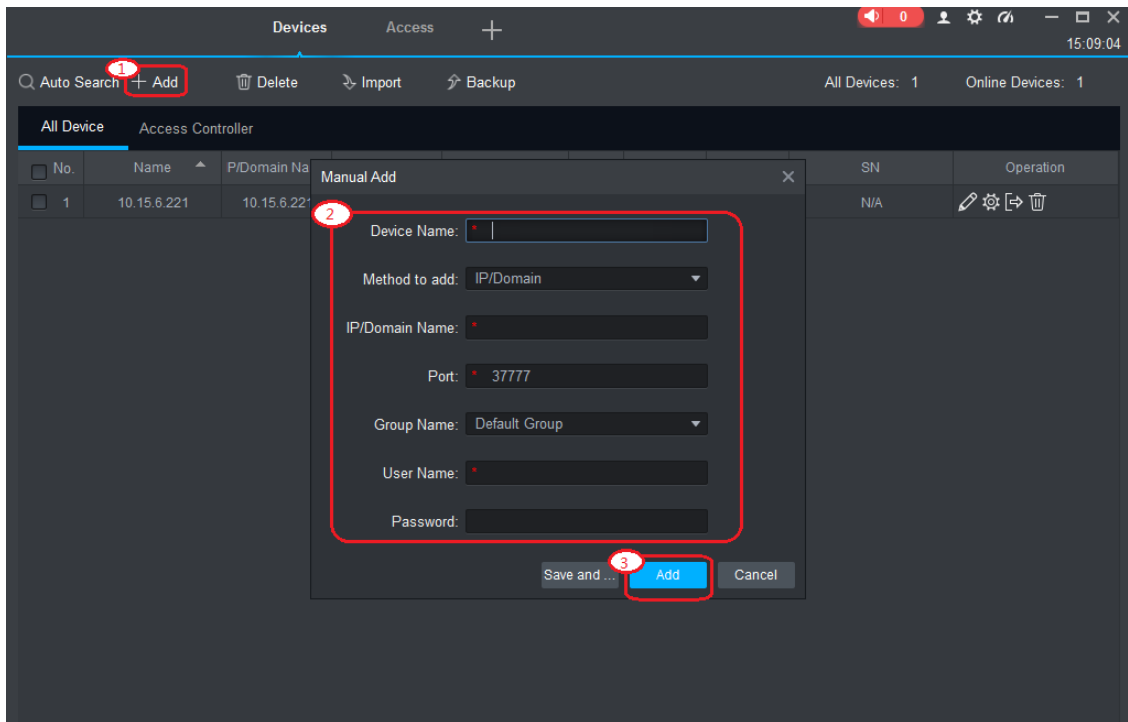


Figure 5-3

Step 1 In “Devices” interface, click “Add”. The system pops up “Manual Add” interface.

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. Available operations are shown in Table 5-1.

 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, the VMS logs in the device automatically. In case of successful login, online status displays “Online”. Otherwise, it displays “Offline”.

5.3 Add Persons

Added persons correspond to cards, so as to distribute right.



In “New” interface, click , enter “Access” interface and complete relevant configurations of access.

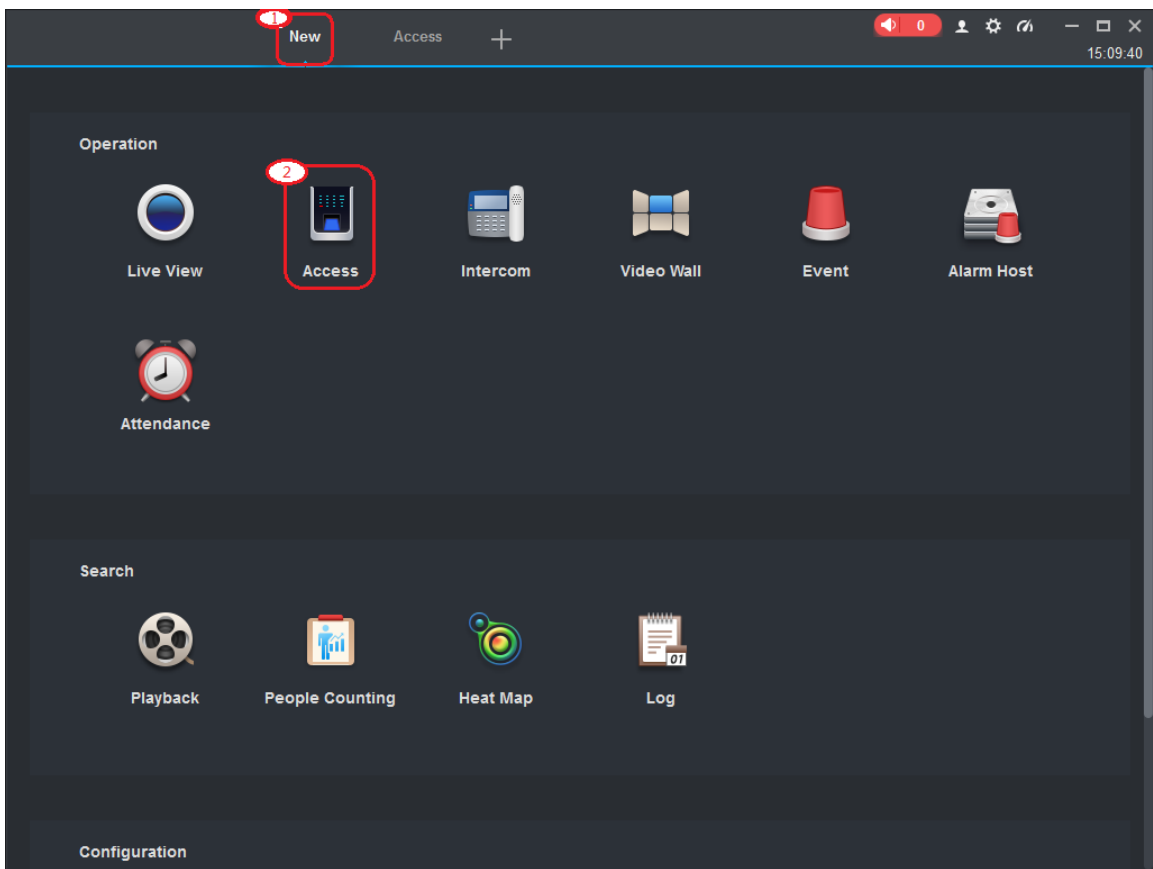


Figure 5-4

5.3.1 Setting Card Type



Caution

Card type shall be consistent with card sender. Otherwise, card number cannot be read.

In “Access” interface, select “User”; click  to set the card type, as shown in Figure 5-5.

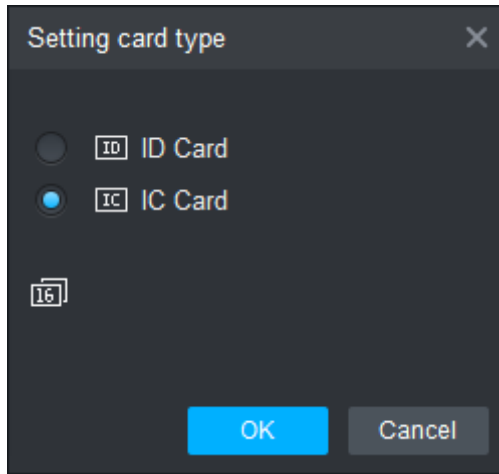



Figure 5-5

5.3.2 Add User

Add one user, issue one card and input user info.

In "Access" interface, select "User", click  to add user info manually, including basic info, fingerprint info and details. Click "Finish" to finish the adding, as shown in Figure 5-6.

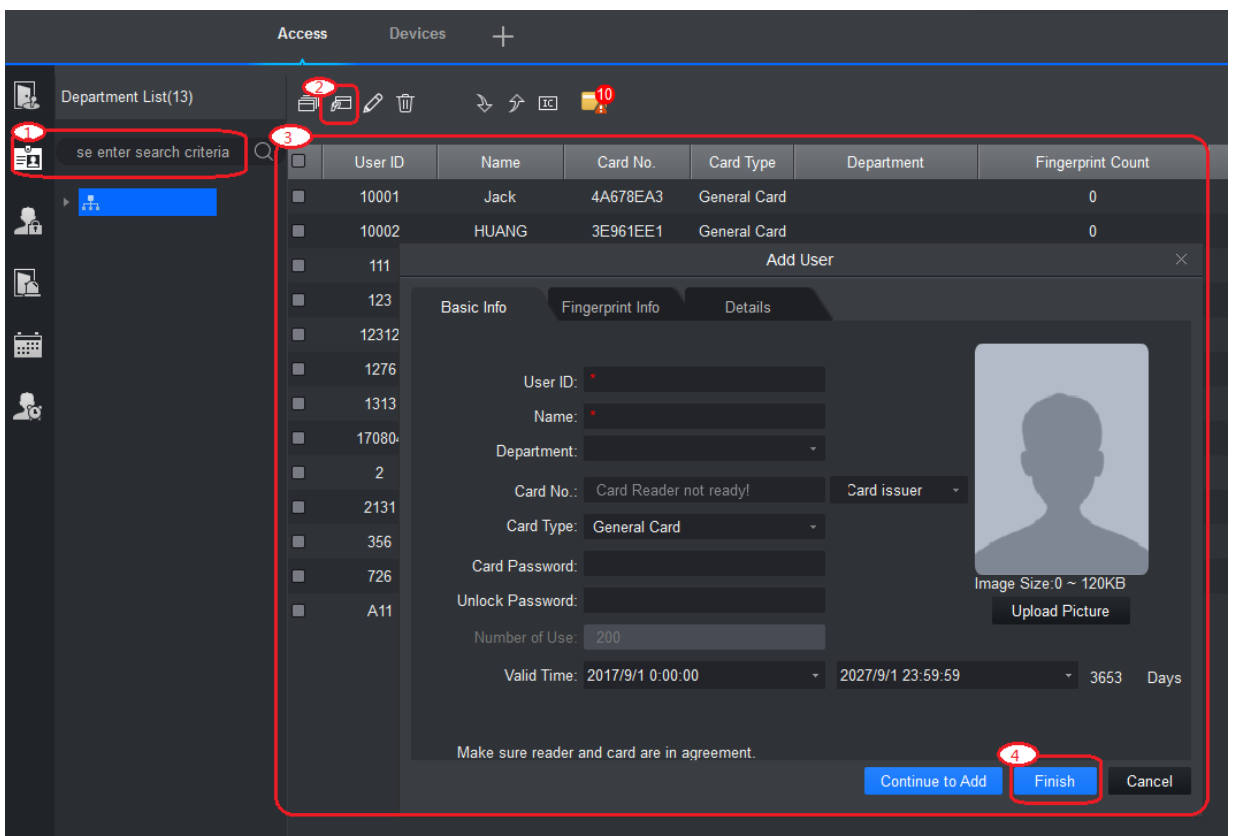


Figure 5-6

5.4 Add Groups

Divide the access into groups, and carry out combined management.

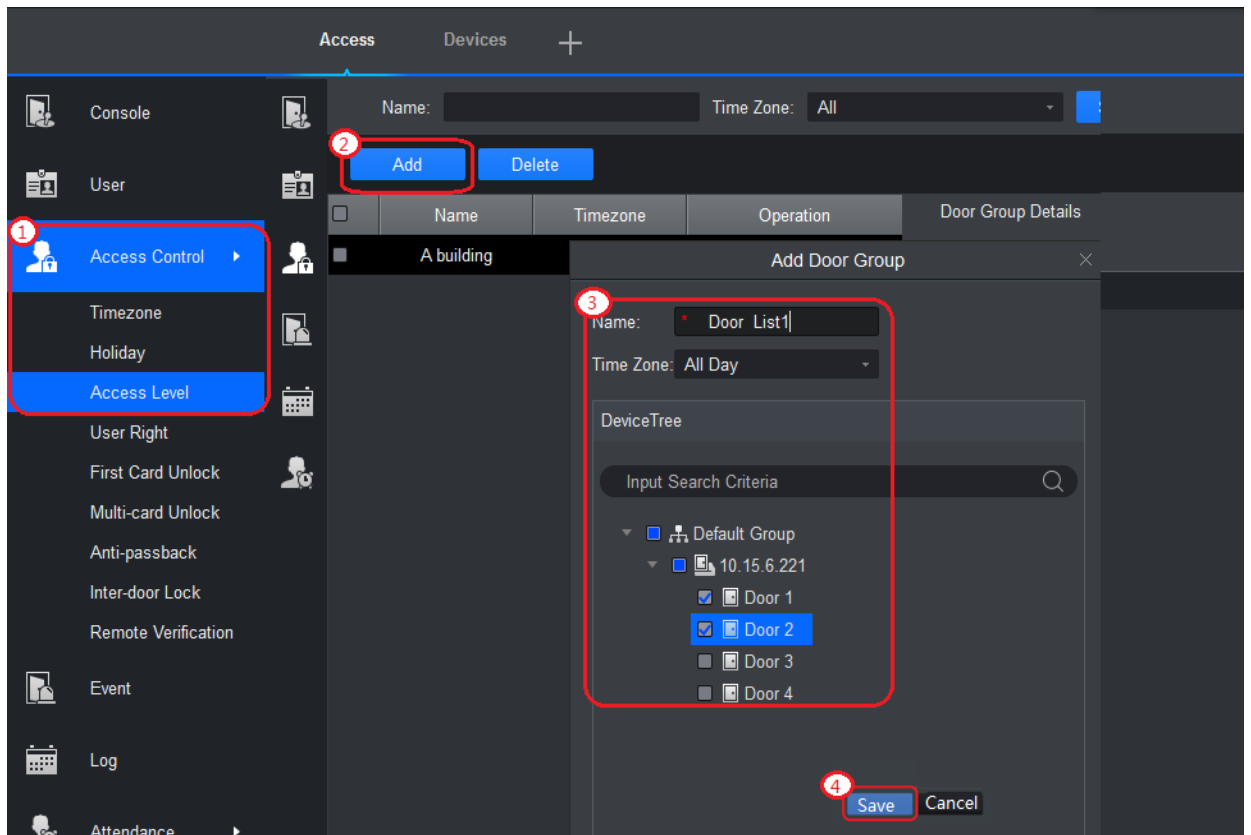


Figure 5-7

- Step 1 In "Access" interface, select "User > Access Control".
- Step 2 Click "Add". The system pops up "Add Door Group" dialog box.
- Step 3 Input "Name", select "Time Zone" and doors to be managed by the group.
- Step 4 Click "Save" to complete adding.

5.5 Right Distribution

There are two types of right: right is distributed according to door group and user.

5.5.1 Right of Door Group

Select door group, add users to the door group. In this way, users in the door group enjoy right of all doors in the group.

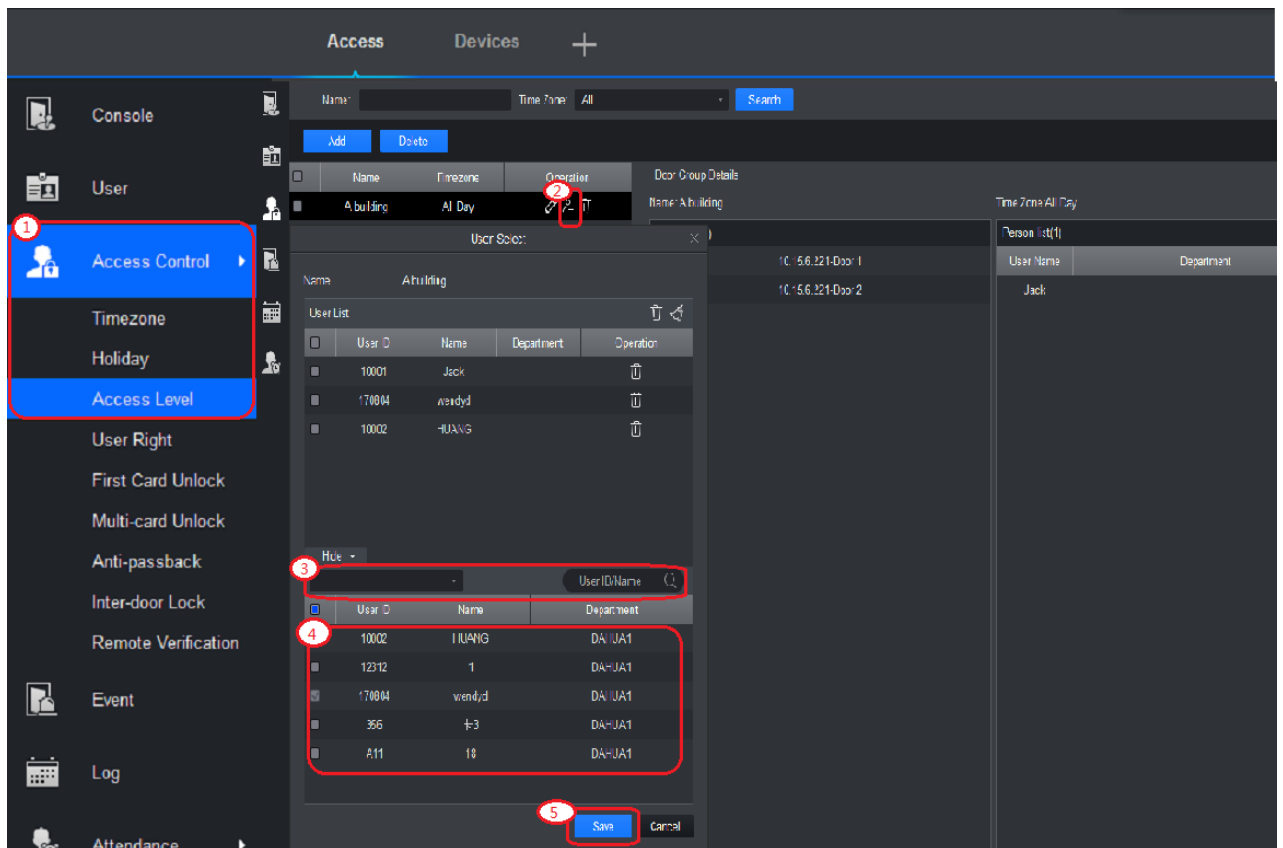



Figure 5-8

- Step 1 In "Access" interface, select "User > Access Control".
- Step 2 Click . The system pops up "User Select" dialog box.
- Step 3 In the pull-down list, select user department or input the user ID or name.
- Step 4 Select users from search list, and add them to user list.
- Step 5 Click "Save" to complete distribution of right.

5.5.2 User Right

Select one user, distribute door groups to the user. In this way, the user enjoys the right of all doors in the selected door groups.

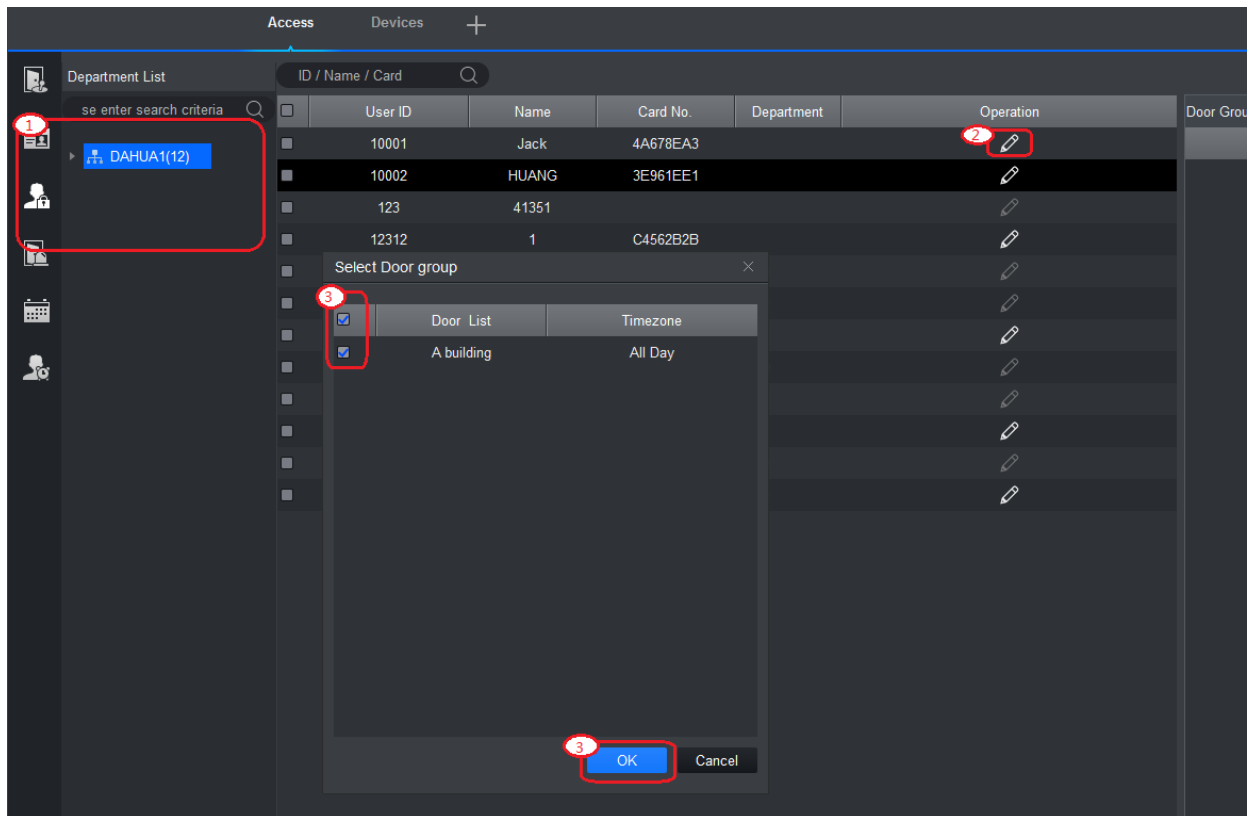


Figure 5-9

Step 1 In "Access" interface, select "User > Access Control".

Step 2 Click . The system pops up "Select Door Group" dialogue box.

Step 3 Select door groups that will be authorized, click "OK" to complete the authorization.

6

Technical Parameters

Parameter	Specification
Processor	32-bit ARM processor
Storage Capacity	16M
Max User	100,000
Max Record	150,000
Communication Port of Reader	Wiegand,RS485
Communication Port of platform	TCP/IP
Quantity of Connected Reader	4 groups
Working Power	Rated power 10V~15V DC, rated current 0.75A
Schedule	128
Period	128
Holiday	128
Unlock Mode	Card, card+ password, password, card or password, card+ fingerprint, fingerprint+ password, fingerprint or card or password, by period.
Cross-segment Network	Support
Dual-door Lock	Support
Single-door bidirectional swiping	Support
Real-time Monitoring	Support
Alarm Activation	Support
Vandal-proof Alarm	Support
Illegal Intrusion Alarm	Support
Unlock Overtime Alarm	Support
Duress Card and Password Setup	Support
DST and Time Sync	Support
Online Upgrading	Support