Access Controller

User Manual

V1.0.0

Foreword

General

This manual introduces the installation and detailed operations of the Access Controller (hereinafter referred to as "the Device").

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.	September 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 regions. For detailed information, see 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, please refer to our 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 occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

This chapter describes the contents covering proper handling of the access controller, hazard prevention, and prevention of property damage. Read these contents carefully before using the access controller, comply with them when using, and keep the manual well for future reference.

Operation Requirements

- Do not place or install the device in a place exposed to sunlight or near the heat source.
- Keep the device away from dampness, dust or soot.
- Keep the device installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into the device.
- Install the device in a well-ventilated place, and do not block the ventilation of the device.
- Operate the device within the rated range of power input and output.
- Do not dissemble the device randomly.
- Transport, use and store the device under the allowed humidity and temperature conditions.

Electrical Safety

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the device; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

Table of Contents

1 Overview

1.1 Introduction

The Device is a controlling device which compensates video surveillance and visual intercom. It has neat and modern design with strong functionality, suitable for high-end commercial building, group properties and smart communities.

1.2 Features

- Using PC+ABS as material, the appearance is high-end and neat.
- Support TCP/IP network communication, communication data is encrypted for security.
- Support OSDP protocol.
- Support PoE function.
- Support card, password and fingerprint unlock.
- Support 100,000 users, 100,000 cards, 3,000 fingerprints, and 500,000 records.
- Support interlock, anti-passback, multi-user unlock, first card unlock, admin password unlock, remote unlock, and more.
- Support tamper alarm, intrusion alarm, door sensor timeout alarm, duress alarm, blocklist alarm, illegal card exceeding threshold alarm, incorrect password alarm and external alarm.
- Support user types such as general users, VIP users, guest users, blocklist users, patrol users, and other users.
- Support built-in RTC, NTP time calibration, manual time calibration, and automatic time calibration functions.
- Support offline operation, event record storage and upload functions, data can be stored locally after the network is disconnected, and continue to upload after the network is restored.
- Support 128 periods, 128 holiday plans, 128 holiday periods, normally open periods, normally closed periods, remote unlock periods, first card unlock periods, and support unlock in periods.
- Support watchdog guard mechanism to ensure the operation stability.

1.3 Dimensions

Two-door One-way Access Controller

Figure 1-1 Dimensions (two-door one-way) (mm [inch])

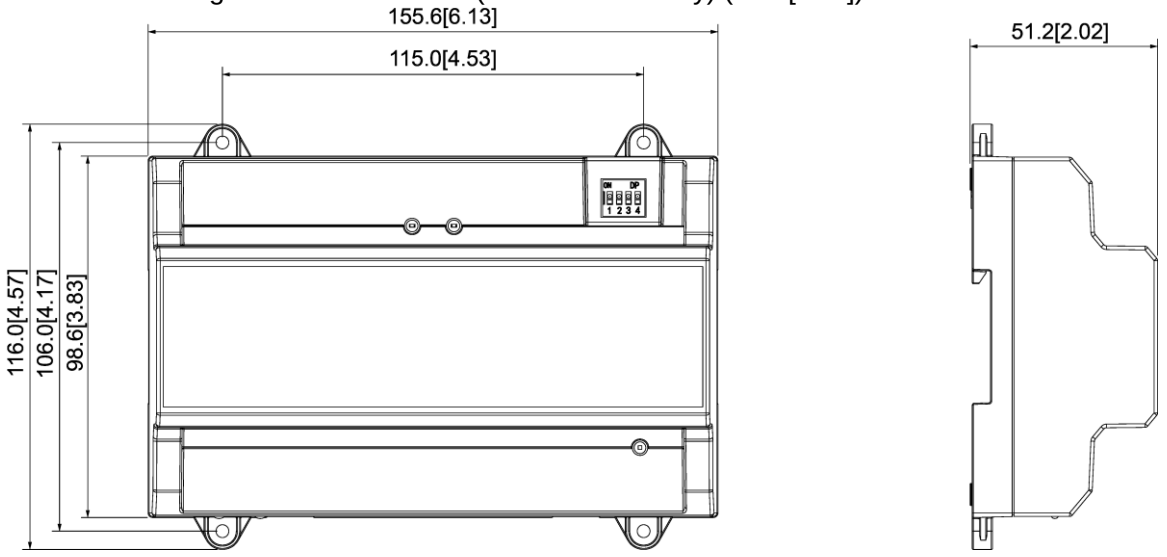
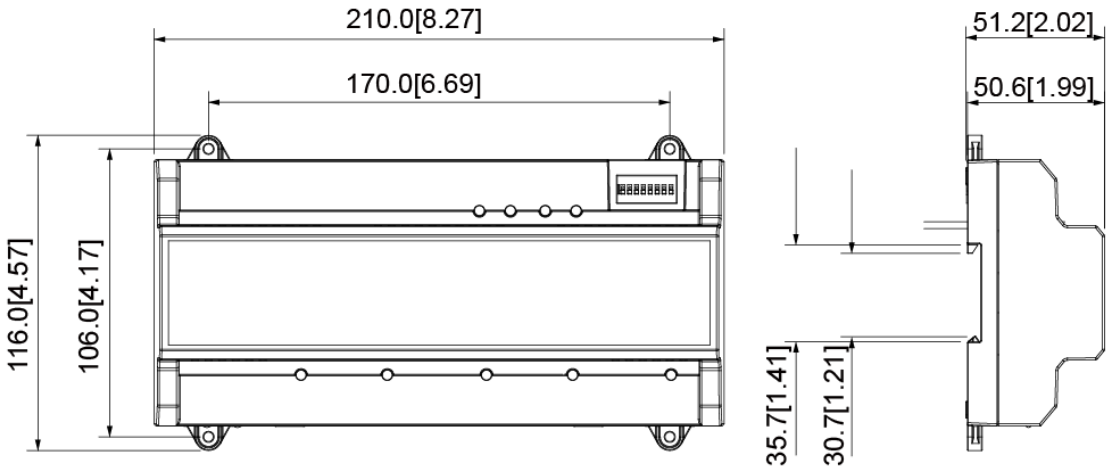


Figure 1-2 Dimensions (two-door two-way/four-door one-way) (mm [inch])



1.4 Components

Two-door One-way Access Controller

Figure 1-3 Components (two-door one-way)

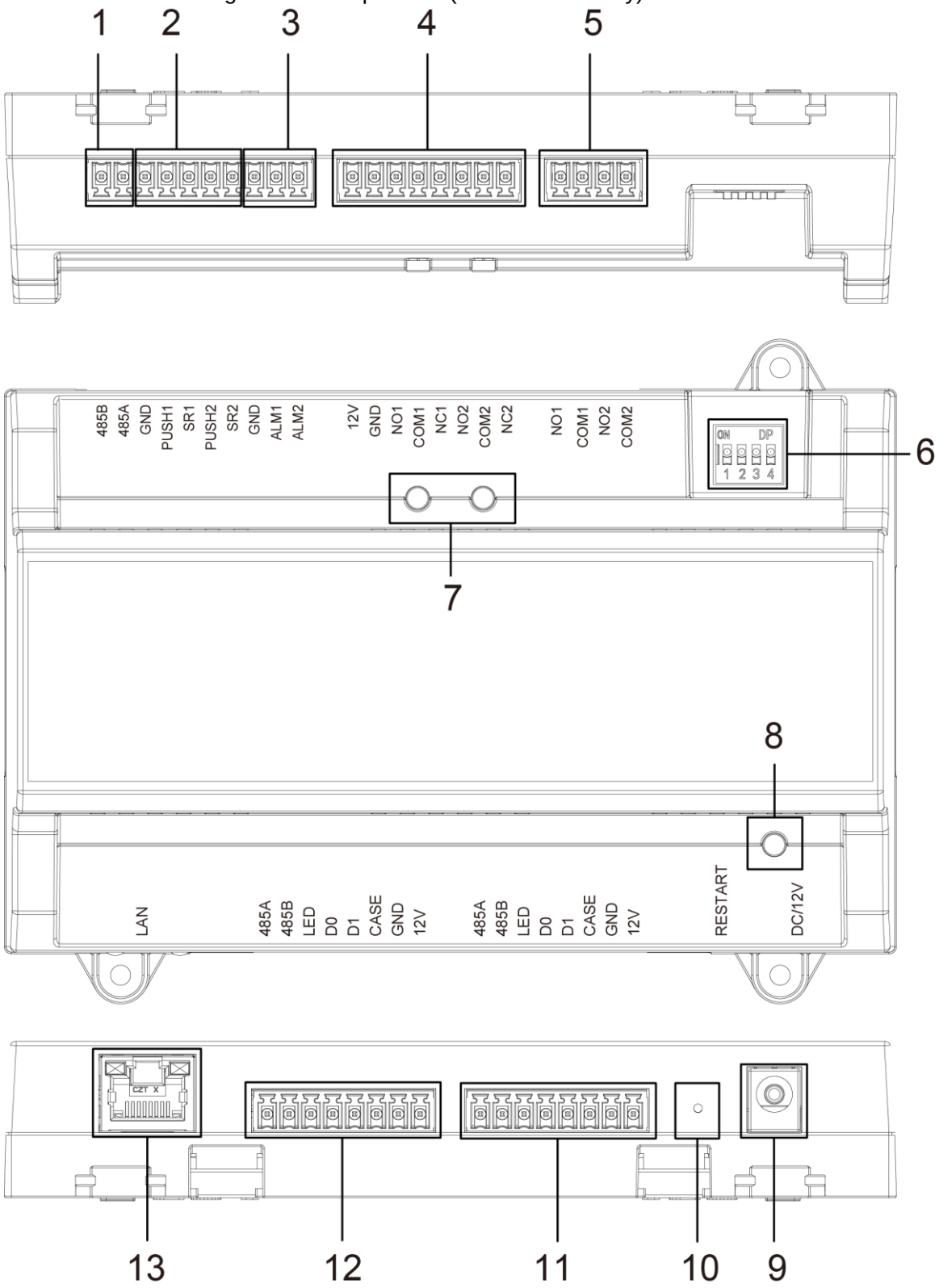


Table 1-1 Component description (two-door one-way)

No.	Name	No.	Name
1	RS-485 port	8	Power indicator light
2	Exit button/door contact port	9	Power port

3	Alarm IN port	10	Restart button
4	Door lock OUT port	11	Entrance card reader port of No.2 door
5	Alarm OUT port	12	Entrance card reader port of No.1 door
6	DIP switch	13	Network port
7	Indicator light of door lock	14	—

Two-door Two-way Access Controller

Figure 1-4 Components (two-door two-way)

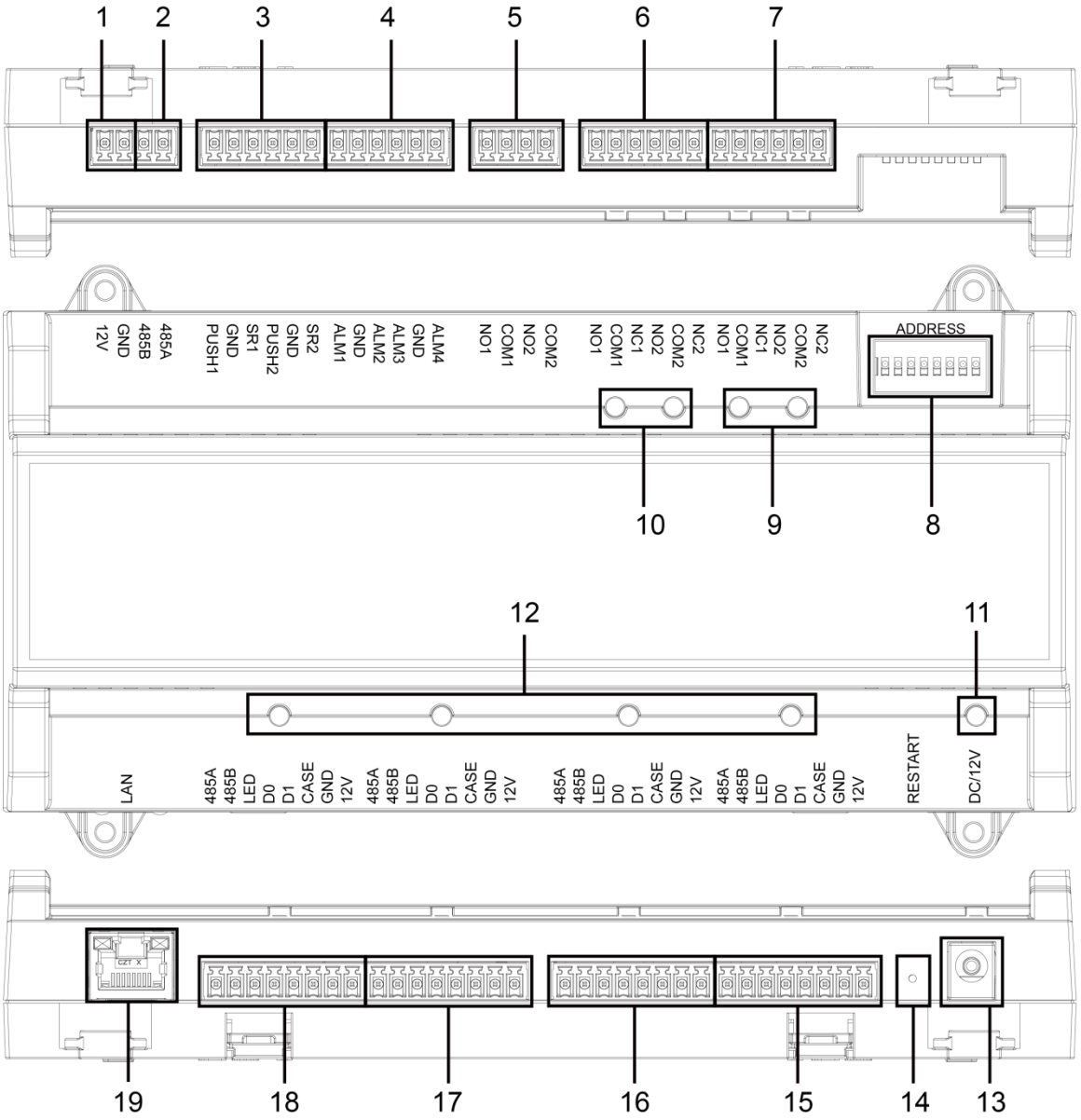


Table 1-2 Component description (two-door two-way)

No.	Name	No.	Name
1	Door lock power port	11	Power indicator light
2	RS-485 port	12	Card reader indicator light
3	Exit button/door contact port	13	Power port
4	External alarm IN port	14	Restart button
5	External alarm OUT port	15	Exit card reader port of No.2 door
6	Door lock control OUT port	16	Entrance card reader port of No.2 door

7	Internal alarm OUT	17	Exit card reader port of No.1 door
8	DIP switch	18	Entrance card reader port of No.1 door
9	Alarm indicator light	19	Network port
10	Door lock indicator light	—	—

Four-door One-way Access Controller

Figure 1-5 Components (four-door one-way)

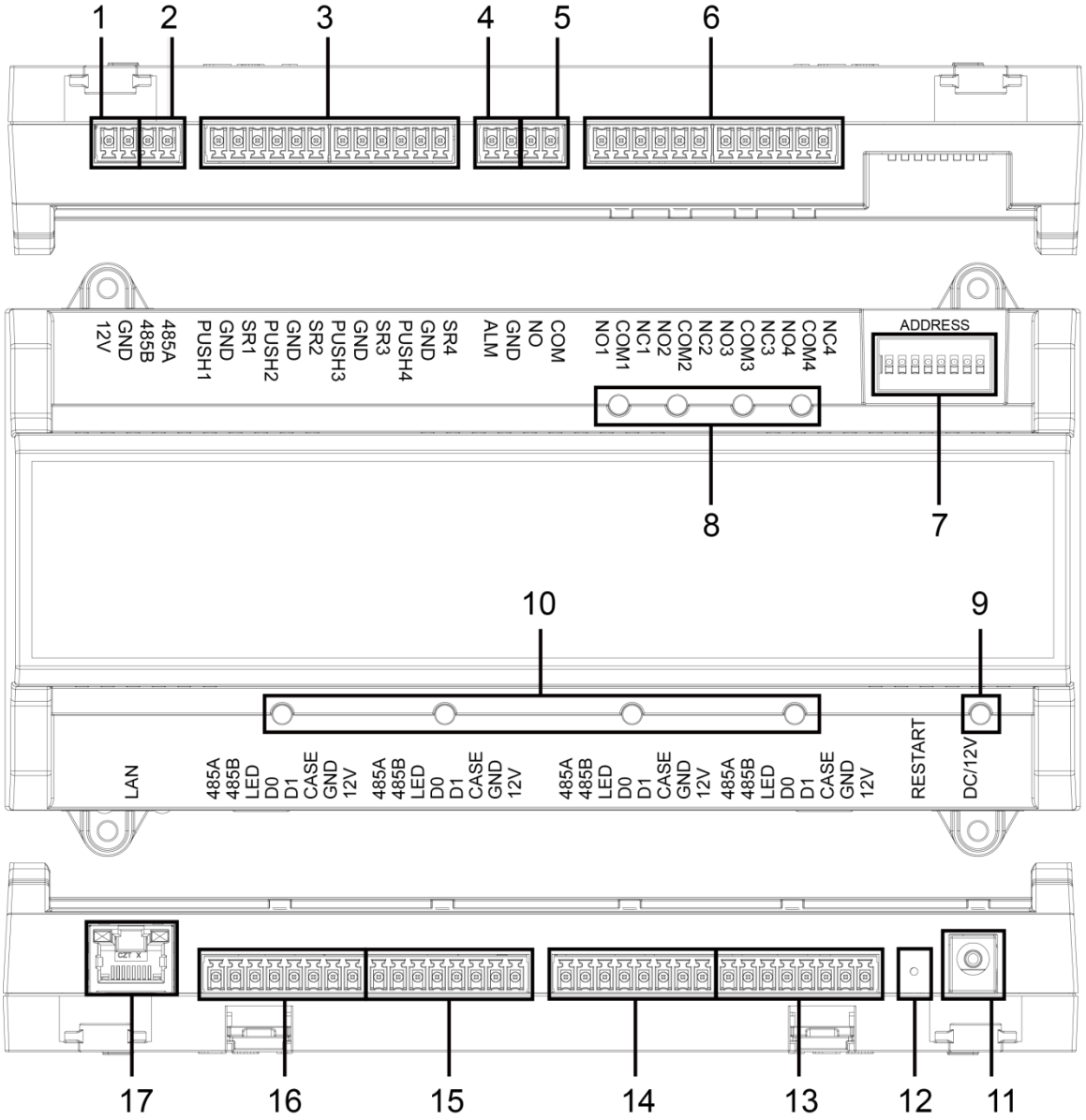


Table 1-3 Component description (four-door one-way)

No.	Name	No.	Name
1	Door lock power port	10	Card reader indicator light
2	RS-485 port	11	Power port
3	Exit button/door contact port	12	Restart button
4	Alarm IN port	13	Entrance card reader port of No.4 door
5	Alarm OUT port	14	Entrance card reader port of No.3 door
6	Door lock control OUT port	15	Entrance card reader port of No.2 door

7	DIP switch	16	Entrance card reader port of No.1 door
8	Door lock indicator light	17	Network port
9	Power indicator light	—	—

Port

10/100 Mbps self-adaptive port, and it supports PoE power supply.

Indicator Light

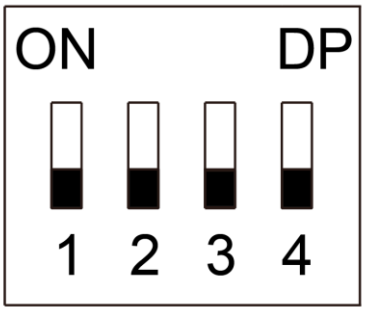
- Power indicator light
  - ◇ Green: Working normally.
  - ◇ Red: Power anomaly.
  - ◇ Blue: Upgrading.
- Alarm indicator light
  - ◇ On: Alarm is triggered.
  - ◇ Off: Alarm is not triggered.
- Door lock Indicator light
  - ◇ On: Door lock is connected.
  - ◇ Off: Door lock is not connected.
- Card reader Indicator light
  - ◇ On: Card reader is connected.
  - ◇ Off: Card reader is not connected.

DIP Switch

Perform corresponding operation through DIP switch.

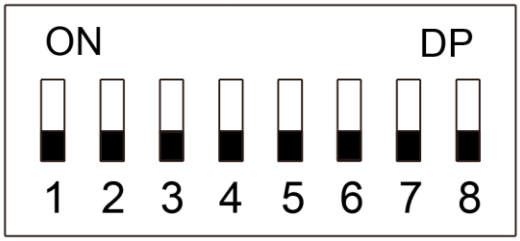
 Means 1;  means 0.

Figure 1-6 DIP switch (two-door one-way access controller)



- 1–4 are all 0, the Device starts normally after power-on.
- 1–4 are all 1, the Device enters to boot mode after power-on.
- 1 and 3 are 1, 2 and 4 are 0, the Device restores to factory defaults after restart.
- 2 and 4 are 1, 1 and 3 are 0, the Device restores to factory defaults after restart. But user information will be retained.

Figure 1-7 DIP switch (two-door two-way/four-door one-way access controller)



- 1–8 are all 0, the Device starts normally after power-on.
- 1–8 are all 1, the Device enters to boot mode after power-on.
- 1, 3, 5 and 7 are 1, 2, 4, 6 and 8 are 0, the Device restores to factory defaults after restart.
- 1, 2, 4, 6 and 8 are 1, 1, 3, 5 and 7 are 0, the Device restores to factory defaults after restart. But user information will be retained.

Restart

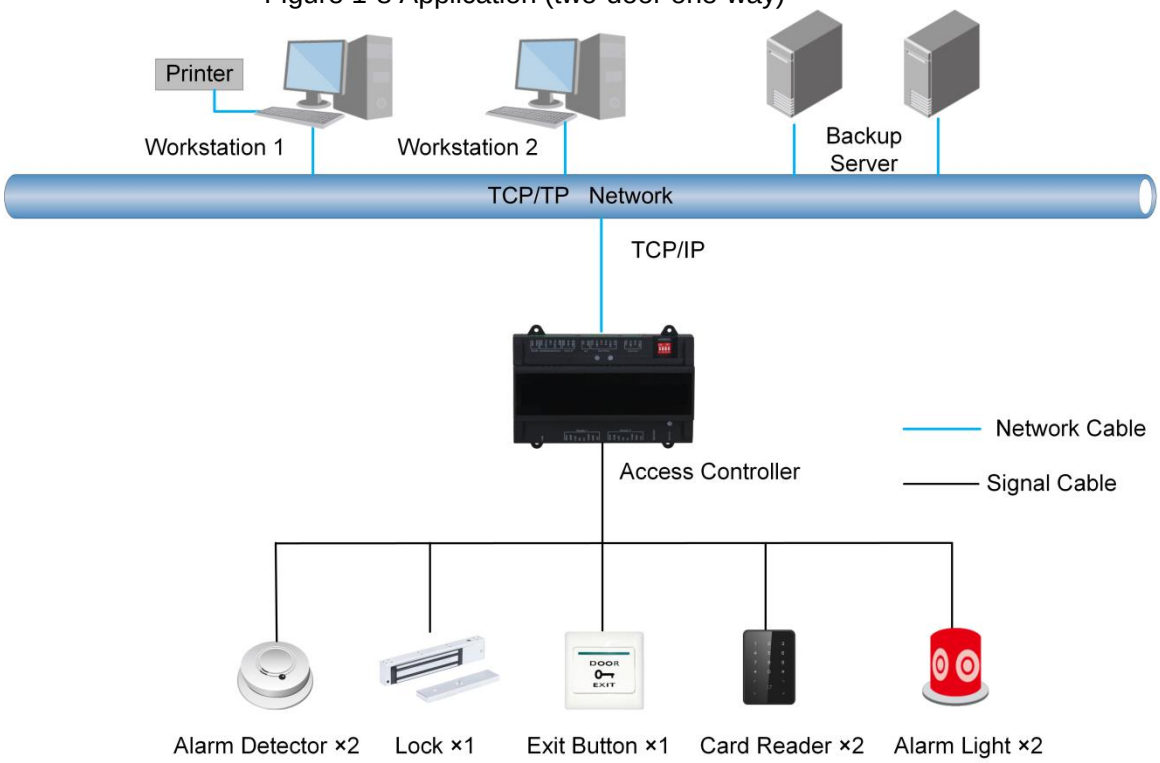
Insert a needle into the RESTART hole and press it to restart the Device.

Restart button is to restart the Device, rather than modifying configuration.

1.5 Application

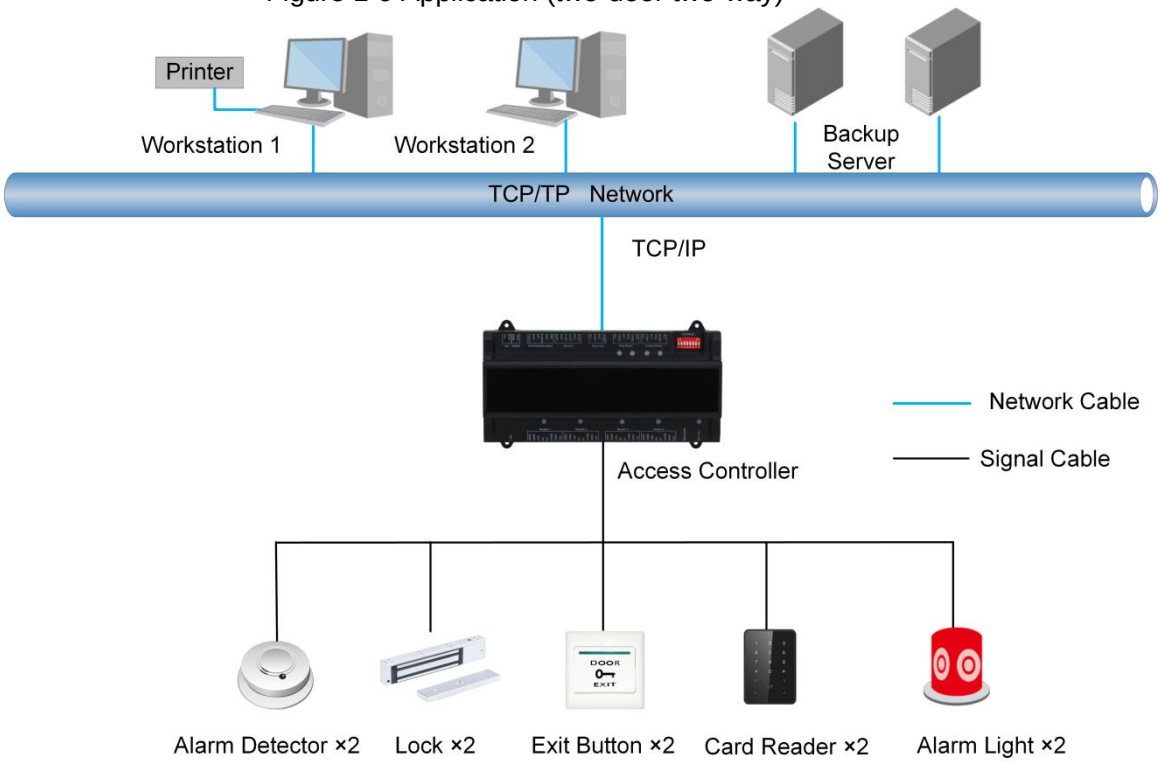
Two-door One-way Access Controller

Figure 1-8 Application (two-door one-way)



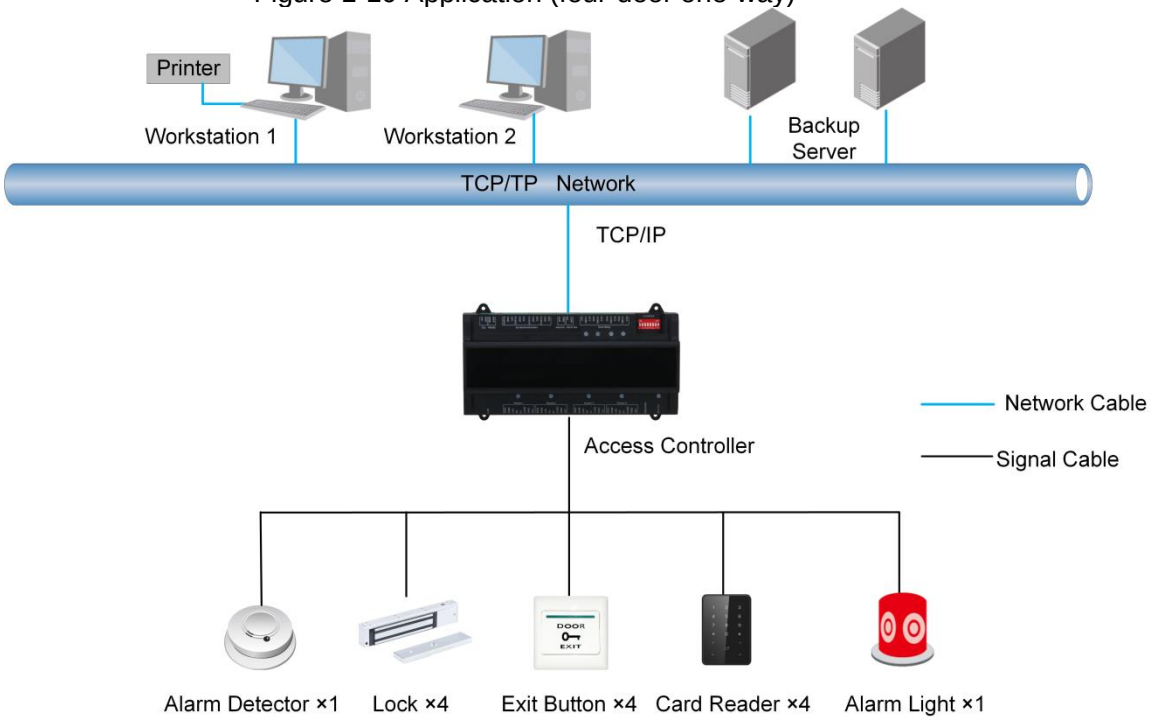
Two-door Two-way Access Controller

Figure 1-9 Application (two-door two-way)



Four-door One-way Access Controller

Figure 1-10 Application (four-door one-way)

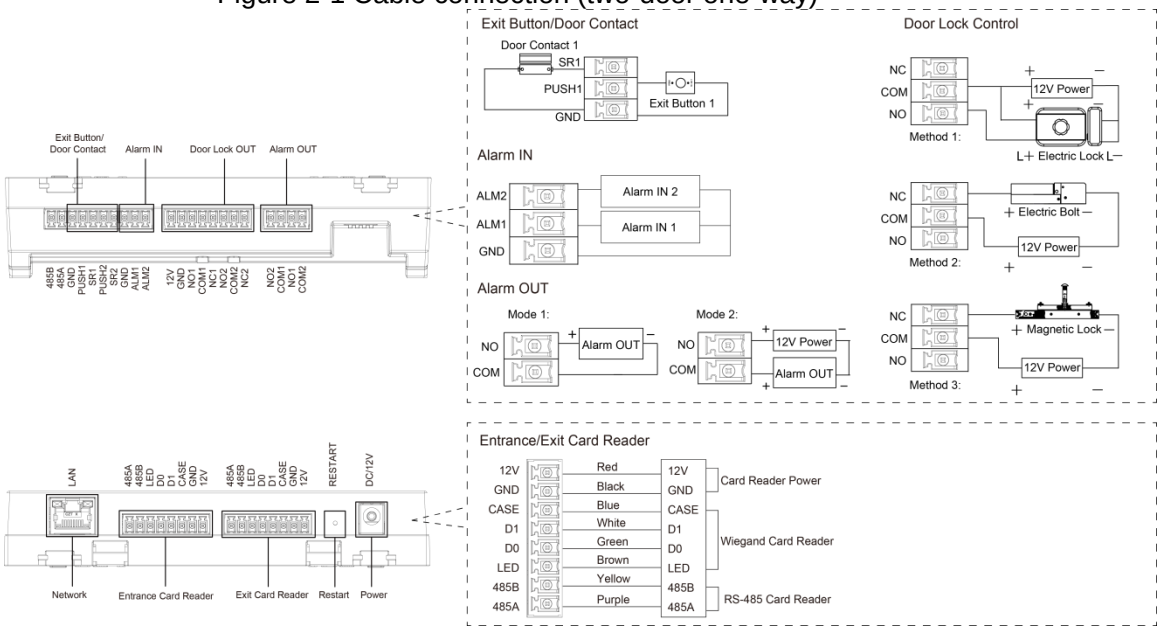


2 Installation

2.1 Cable Connection

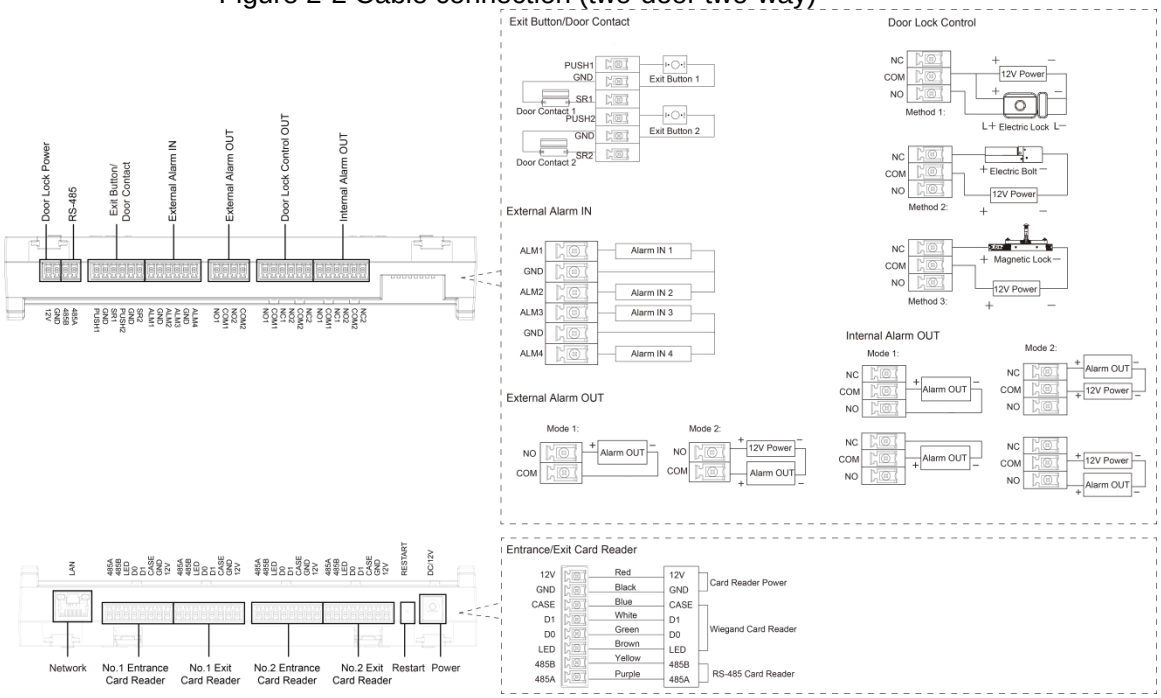
Two-door One-way Access Controller

Figure 2-1 Cable connection (two-door one-way)



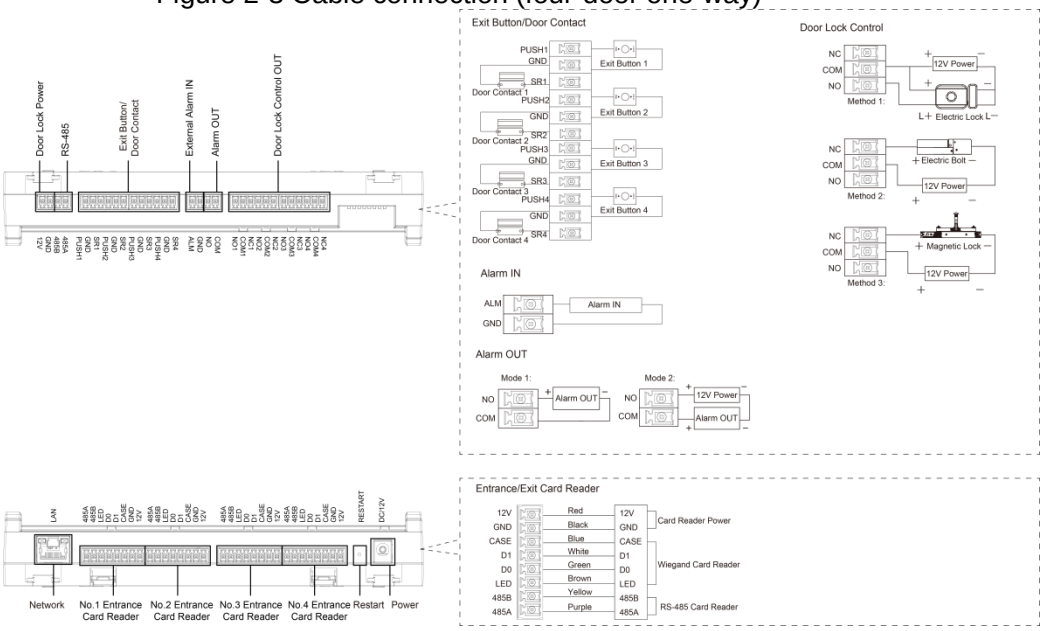
Two-door Two-way Access Controller

Figure 2-2 Cable connection (two-door two-way)



Four-door One-way Access Controller

Figure 2-3 Cable connection (four-door one-way)



2.1.1 Cable Connection of Alarm Input

The external alarm input port can be connected to smoke detectors, infrared detectors, and more.

Table 2-1 Cable connection of alarm input

Model	Alarm Input Channel	Description
Two-door one-way	2-channel alarm input.	The external alarm can be linked to the state of the door lock/unlock. ● ALM1 external alarm links all doors to be normally open. ● ALM2 external alarm links all doors to be normally closed.
Two-door two-way	4-channel alarm input.	The external alarm can be linked to the state of the door lock/unlock. ● ALM1–ALM2 external alarm links all doors to be normally open. ● ALM3–ALM4 external alarm links all doors to be normally closed.
Four-door one-way	1-channel alarm input.	When the external alarm is triggered, all the doors are normally open.

2.1.2 Cable Connection of Alarm Output

Internal or external alarm input triggers an alarm, and the alarm output device gives an alarm for 15 s.

There are two connection modes of alarm output. Select the connection mode depending on alarm device. For example, IPC can use mode 1, and sound and light device can use mode 2.

When two-door two-way access controllers are connected to the internal alarm output device, select NC/NO according to the normally open or normally closed state.

Table 2-2 Cable connection of alarm output

Model	Alarm Output Channel	Port	Description
Two-door	2-channel alarm	NO1	● ALM1 triggers alarm output.

Model	Alarm Output Channel	Port	Description
one-way	output.	COM1	● Door contact timeout alarm and intrusion alarm. ● Tamper alarm output of No.1 door entrance card reader.
		NO2	● ALM2 triggers alarm output. ● Tamper alarm output of No.2 door entrance card reader.
		COM2	
Two-door two-way	2-channel external alarm output.	NO1	ALM1/ALM2 trigger alarm output.
		COM1	
		NO2	ALM3/ALM4 trigger alarm output.
		COM2	
	2-channel internal alarm output.	NC1	● Tamper alarm output of No.1 door entrance and exit card readers. ● Door contact timeout alarm and intrusion alarm of No.1 door.
		COM1	
		NO1	
		NC2	● Tamper alarm output of No.2 door entrance and exit card readers. ● Door contact timeout alarm and intrusion alarm of No.2 door.
		COM2	
		NO2	
Four-door one-way	1-channel alarm output.	NO	● ALM triggers alarm output. ● Door contact timeout alarm and intrusion alarm. ● Tamper alarm output of card reader.
		COM	

2.1.3 Cable Connection of Card Reader

One door only supports one type of card reader: RS-485 or Wiegand.

Table 2-3 Cable specification and length of card reader

Card Reader Type	Connection mode	Length
RS-485 Card Reader	CAT5e network cable, RS-485 connection	100 m
Wiegand Card Reader	CAT5e network cable, Wiegand connection	30 m

2.2 Device Installation

There are two installation methods.

- Directly fix the Device on wall with screws.
- Install U-shaped guide rail (not provided) on wall, and then hang the Device to the guide rail.

Figure 2-4 Installation (1)

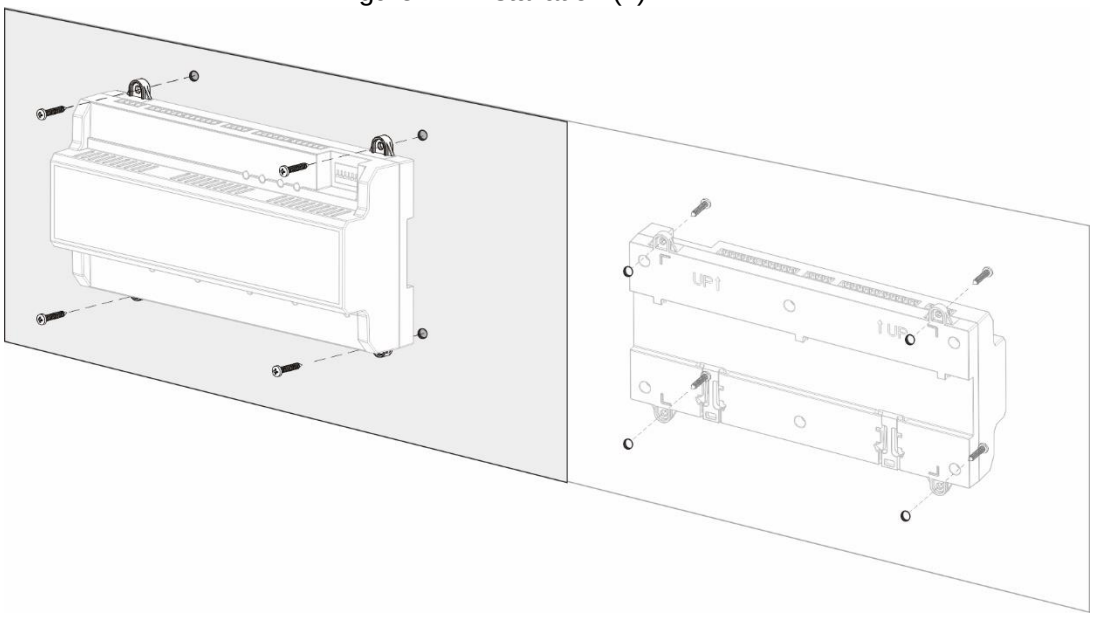
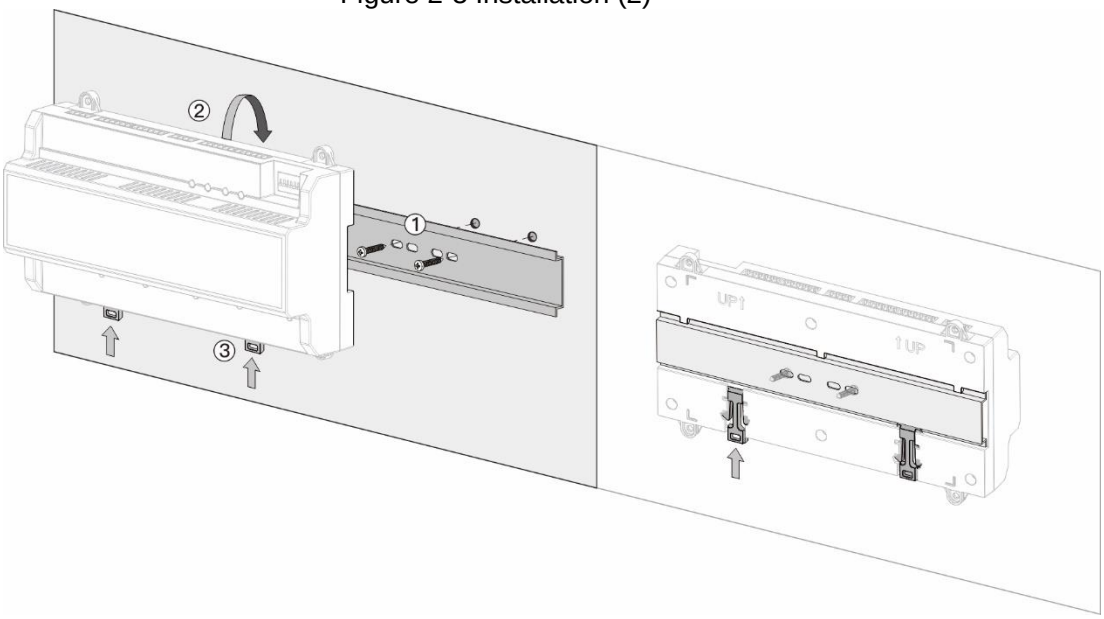


Figure 2-5 Installation (2)



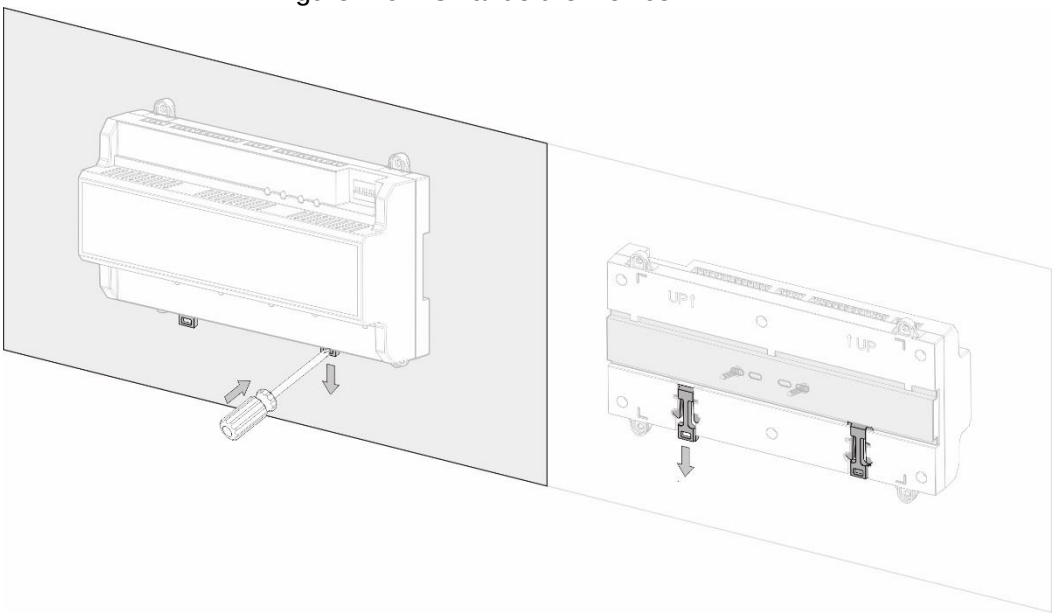
Step 1 Fix the U-shaped guide rail on wall with screws.
Step 2 Buckle the upper back part of the Device into the U-shaped guide rail.
Step 3 Push up the buckle on the lower part of the Device until hearing a click sound.

2.3 Demounting the Device

If you use installation method two to install the Device, please refer to Figure 2-6.

Use a screwdriver to press down the buckle firmly, and then bounce the buckle to remove the Device.

Figure 2-6 Dismantle the Device



3 SmartPSS AC Configuration

You can remotely manage the Device through SmartPSS AC. This chapter mainly introduces quick configuration. For detailed operations, please refer to SmartPSS AC user manual.

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

3.1 Login

Step 1 Install the SmartPSS AC.

Step 2 Double-click  , and then follow the instructions to finish the initialization and log in.

3.2 Adding Devices

You need to add the Device to SmartPSS AC. You can click Auto Search to add and click Add to manually add devices.

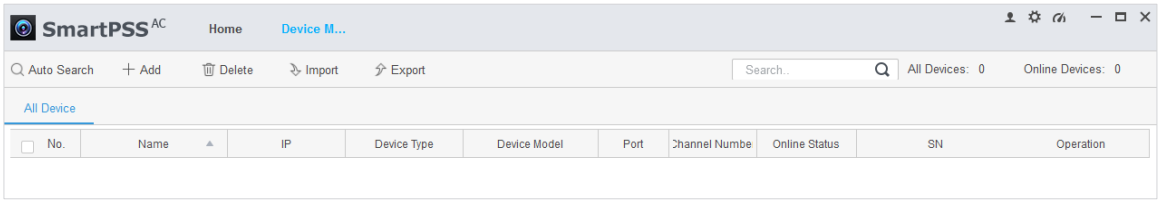
3.2.1 Auto Search

It is recommended to add devices by auto search when you need to add devices in batches within the same network segment, or when the network segment is clear but the device IP address is unclear.

Step 1 Log in to SmartPSS AC.

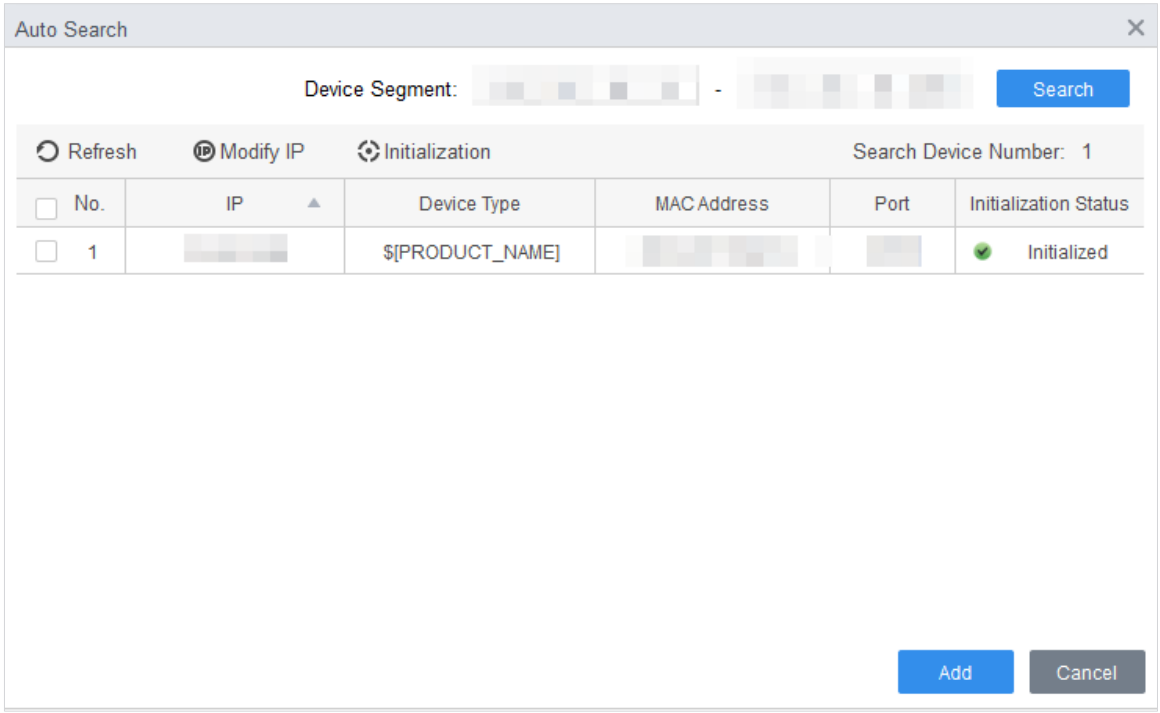
Step 2 Click **Device Manager** at the lower left corner, and the **Device Manager** interface is displayed.

Figure 3-1 Devices



Step 3 Click **Auto Search**, and the **Auto Search** interface is displayed.

Figure 3-2 Auto search



Step 4 Enter the network segment, and then click **Search**.

A search result list will be displayed.

- Click **Refresh** to update device information.
- Select a device, click **Modify IP** to modify IP address of the Device.

Step 5 Select devices that you want to add to the SmartPSS AC, and then click **Add**.

The Login information dialog box will be displayed.

Step 6 Enter the username and the login password to login.

You can see the added devices on the **Devices** interface.

- The username is admin and password is admin123 by default. It is recommended to modify the password after login.
- After adding, SmartPSS AC logs in to the Device automatically. In case of successful login, status displays Online. Otherwise, it displays Offline.

3.2.2 Manual Add

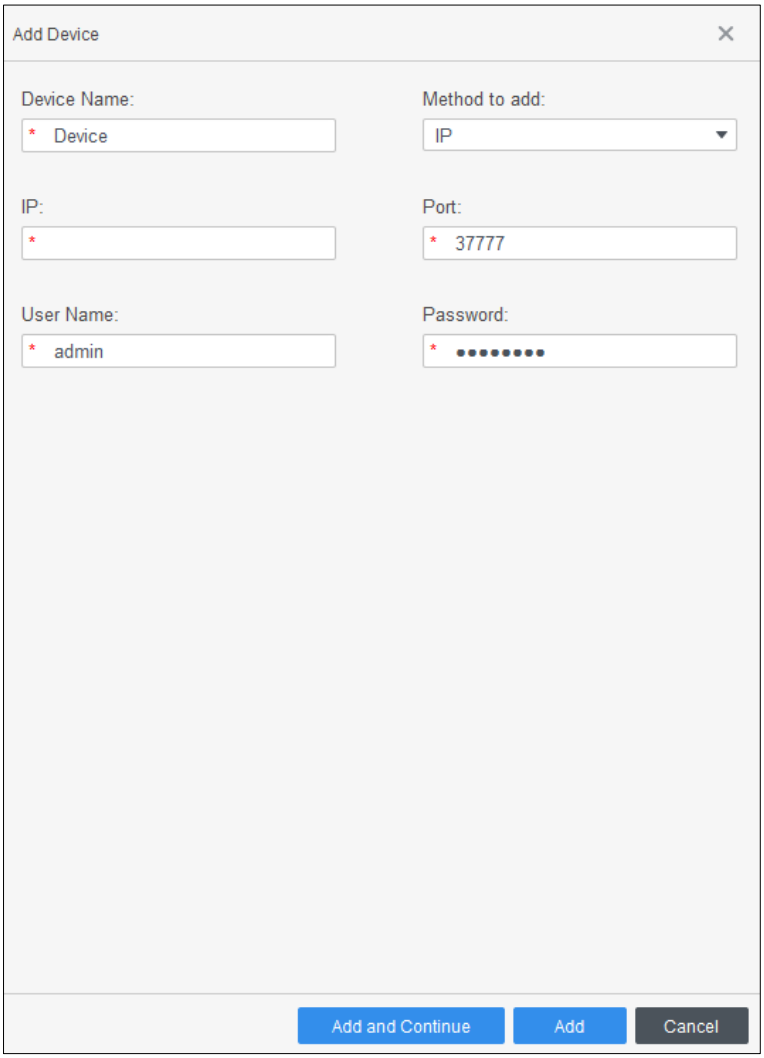
You can add devices manually. You need to know IP addresses and domain names of access controllers that you want to add.

Step 1 Log in to SmartPSS AC.

Step 2 Click **Device Manager** at the lower left corner, and the **Device Manager** interface is displayed.

Step 3 Click **Add** on the **Device Manager** interface, and the **Manual Add** interface will be displayed.

Figure 3-3 Manual add



Step 4 Enter detailed information of the Device.

Table 3-1 Parameters

Parameter	Description
Device Name	Enter a name of the Device. It is recommended to name the Device with installation area for easy identification.
Method to add	Select **IP** to add the Device through IP address.
IP	Enter IP address of the Device. It is 192.168.1.108 by default.
Port	Enter the port number of the Device. Default port number is 37777.
User Name, Password	Enter the username and password of the added device. The username is admin and password is admin123 by default. It is recommended to modify the password after login.

Step 5 Click **Add**, and then you can see the added device on the **Devices** interface.

After adding, SmartPSS AC logs in to the Device automatically. In case of successful login, status displays Online. Otherwise, it displays Offline.

3.3 User Management

3.3.1 Card Type Setting

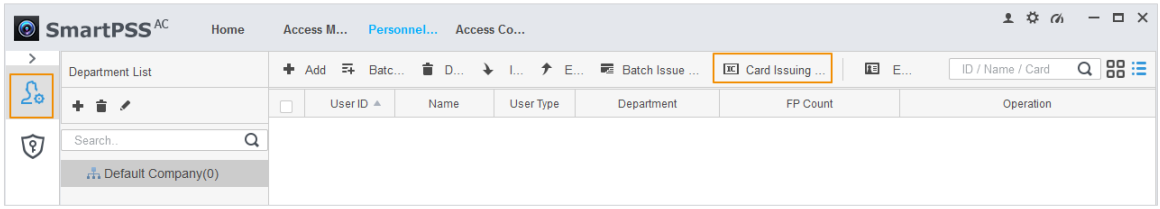
Before issuing card, set card type first. For example, if the issued card is ID card, select type as ID card.

Card types must be the same as card issuer types; otherwise card numbers cannot be read.

Step 1 Log in to SmartPSS AC.

Step 2 Click **Personnel Manager**, and the **Personnel Manager** interface is displayed.

Figure 3-4 Personnel manager

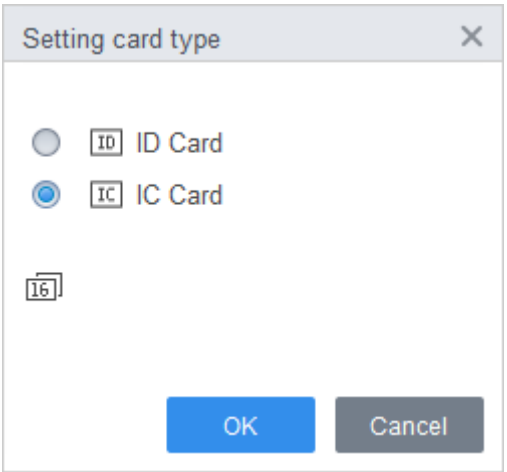


Step 3 On the **Personnel Manager** interface, click  , then click  .

Step 4 On the **Setting Card Type** interface, select a card type.

Step 5 Click  to select display method of card number in decimal or in hex.

Figure 3-5 Setting card type



Step 6 Click **OK**.

3.3.2 Adding User

3.3.2.1 Manual Add

You can add user one by one manually.

Step 1 Log in to SmartPSS AC.

Step 2 Click **Personnel Manger > User > Add**.

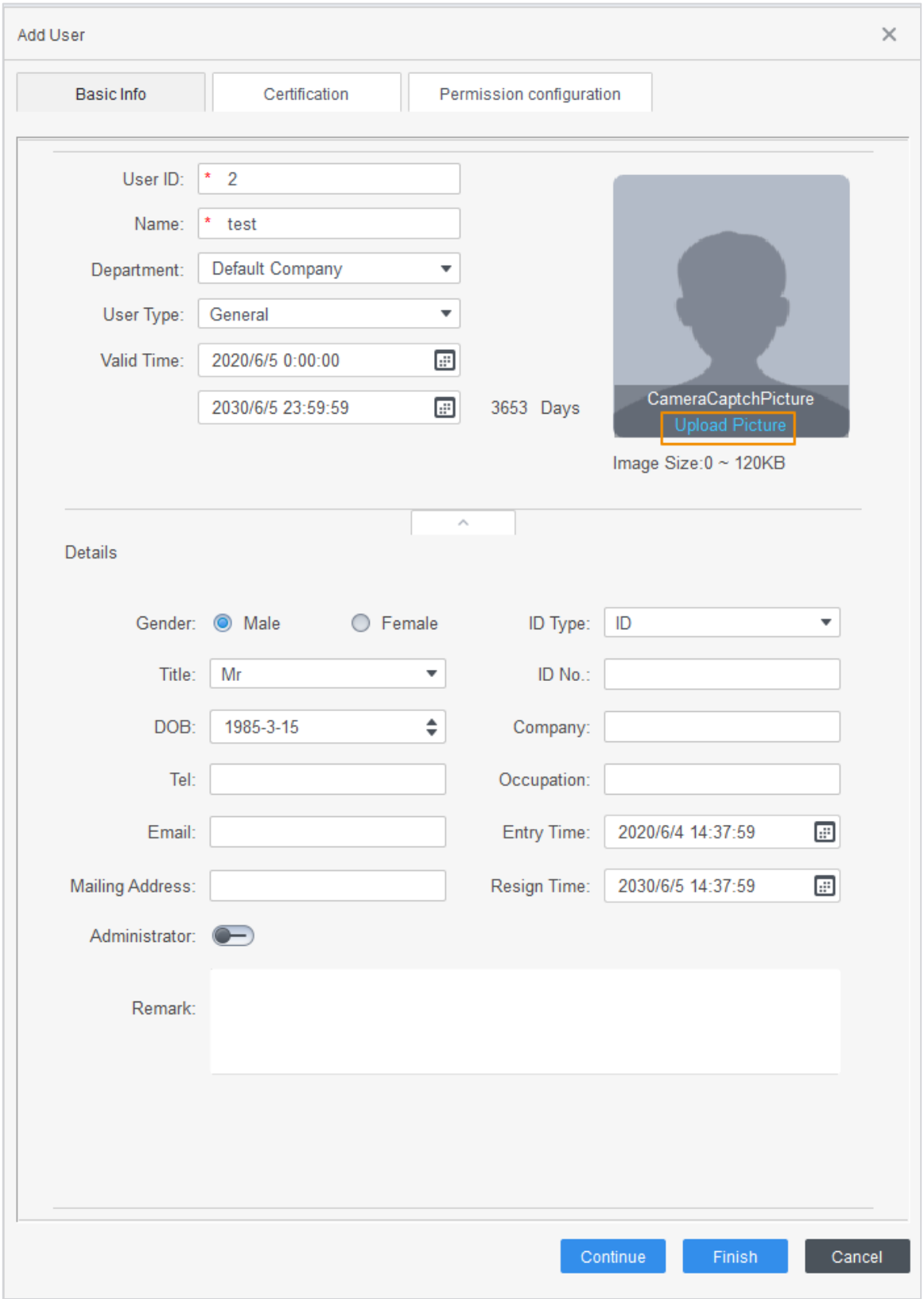
Step 3 Add basic information of the user.

1) Click the **Basic Info** tab on the **Add User** interface, and then add basic information of the user.
2) Click the image, and then click **Upload Picture** to add a face image.

   The uploaded face image will display on the capture frame.

   Make sure that the image pixels are more than 500 × 500; image size is less than 120 KB.

Figure 3-6 Add basic information



Step 4 Click the **Certification tab** to add certification information of the user.

- Configure password.
  Set password. For the second generation access controllers, set the personnel password; for other devices, set the card password. The new password must consist of 6 digits.
- Configure card.

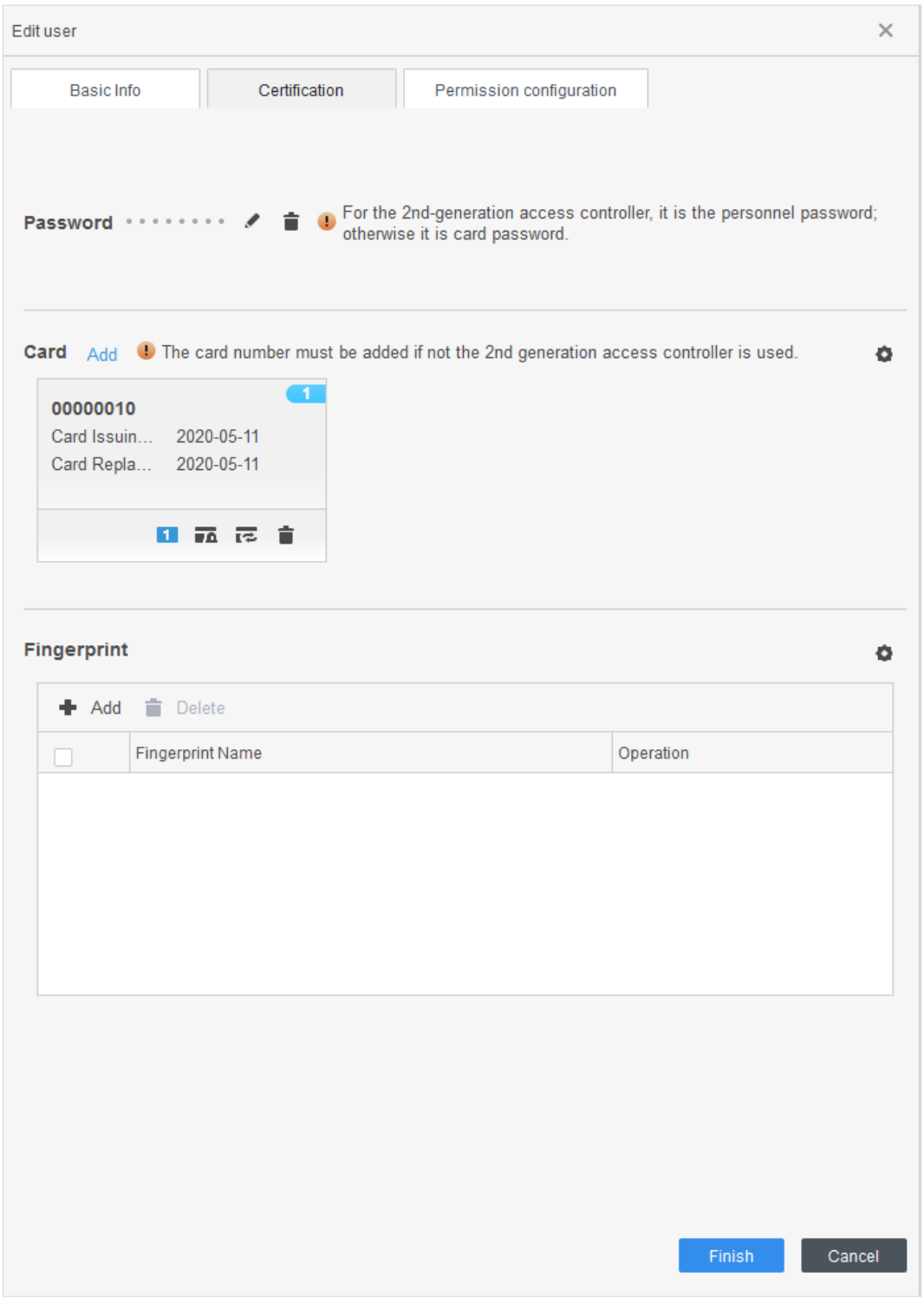
The card number can be read automatically or filled in manually. For automatically read, select a card reader, and then place the card on the card reader. The card number is read automatically after that.

1) Click to select **Device** or **Card issuer** as card reader.
2) Add card. The card number must be added if the non-second generation access controller is used.
3) After adding, you can select the card as main card or duress card, or replace the card with new one, or delete the card.

- Configure fingerprint.

1) Click to select **Device** or **Fingerprint Scanner** as fingerprint collector.
2) Add fingerprint. Click **Add Fingerprint** and press finger on the scanner three times continuously.

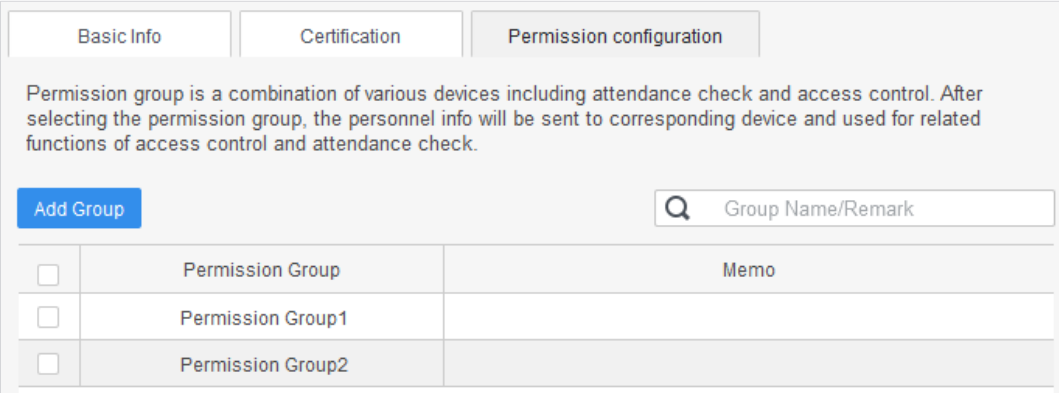
Figure 3-7 Configure certification



Step 5 Configure permission for the user.

For details, see "3.4 Permission Configuration".

Figure 3-8 Permission configuration



Step 6 Click **Finish**.

3.3.2.2 Batch Add

You can add users in batches.

Step 1 Log in to SmartPSS AC.

Step 2 Click **Personnel Manger > User > Batch Add**.

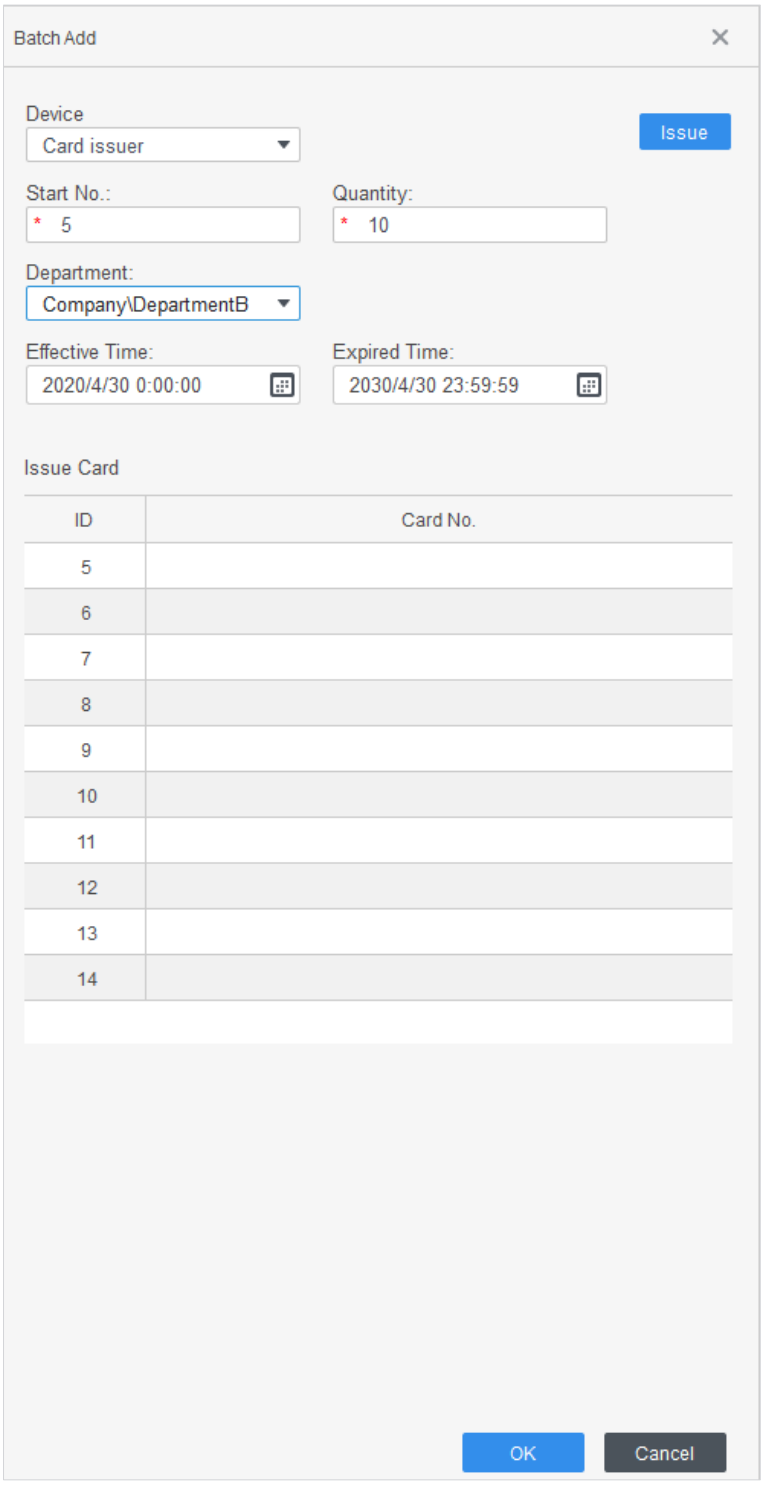
Step 3 Select card reader and the department of user. Set the start number, card quantity, effective time and expired time of card.

Step 4 Click **Issue** to start issuing cards**.**

The card number will be read automatically.

Step 5 Click **Stop** after issuing card, and then click **OK**.

Figure 3-9 Add user in batches



Step 6 In the list of user, click to modify information or add details of users.

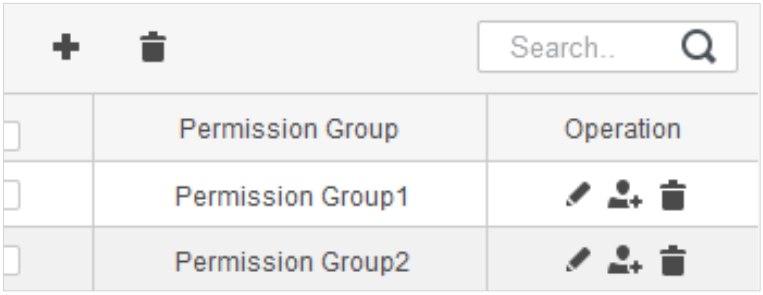
3.4 Permission Configuration

3.4.1 Adding Permission Group

Step 1 Log in to SmartPSS AC.

Step 2 Click **Personnel Manger > Permission Configuration**.

Figure 3-10 Permission group list



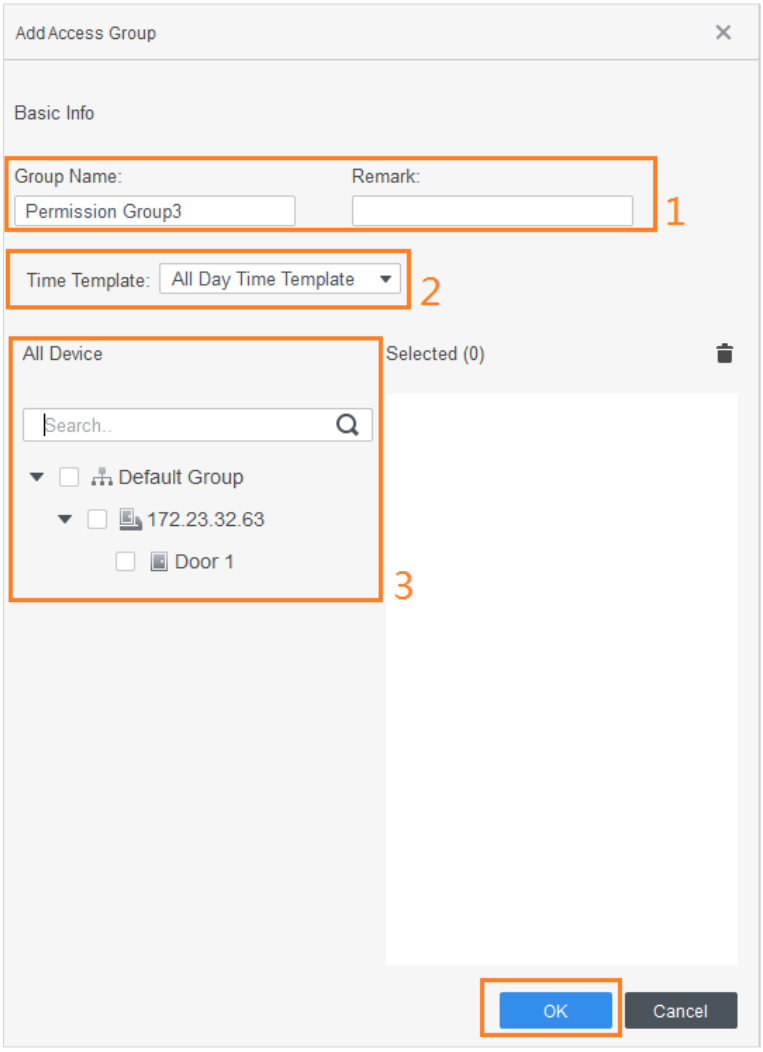
Step 3 Click to add a permission group.

Step 4 Set permission parameters.

1) Enter group name and remark.
2) Select the needed time template.

   For details of time template setting, see SmartPSS AC user manual.
3) Select the corresponding device, such as door 1.

Figure 3-11 Add permission group



Step 5 Click **OK**.

On the **Permission Group List** interface, you can do:

- Click to delete group.
- Click to modify group info.
- Double-click permission group name to view group info.

3.4.2 Configuring Permission

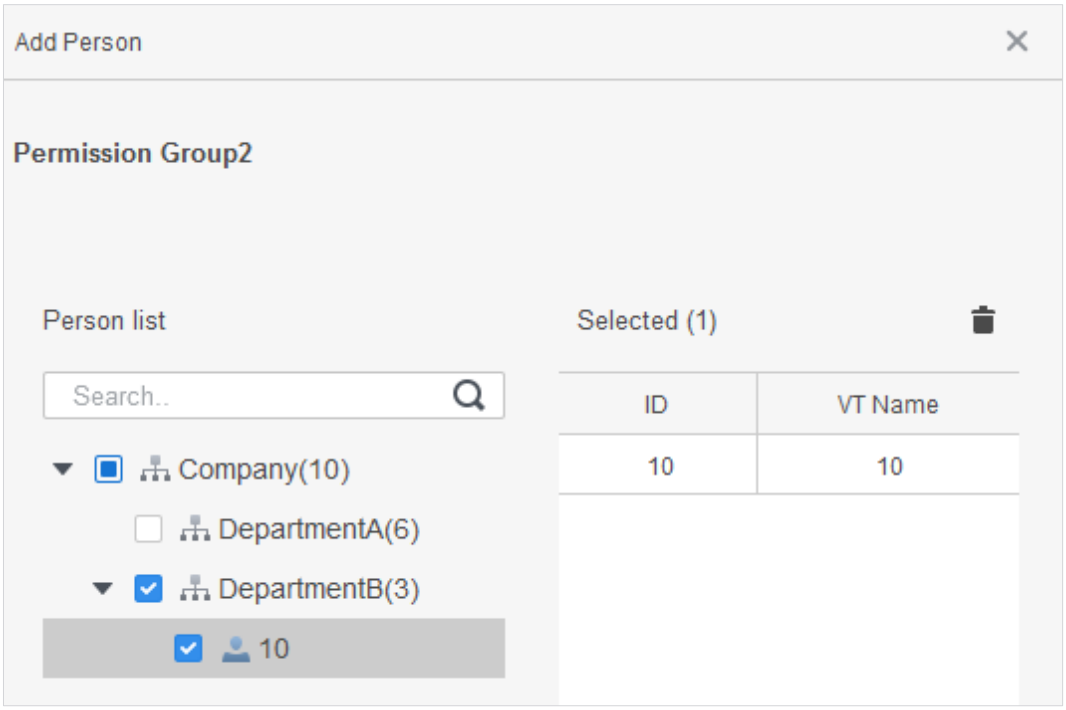
The method to configure permission for department and for users is similar. This section takes users as an example.

Step 1 Log in to SmartPSS AC.

Step 2 Click **Personnel Manger > Permission Configuration**.

Step 3 Select the target permission group, and then click .

Figure 3-12 Configure permission



Step 4 Select the user need to be configured permission.

Step 5 Click **OK**.

3.5 Access Controller Configuration

3.5.1 Advanced Functions Configuration

3.5.1.1 First Card Unlock

Only after the specified first-card user swipes the card every day can other users unlock the door with their cards. You can set multiple first cards. Only after any one of the users swipes the first card can other users without first cards unlock the door with their cards.

- The person to be granted with the first card unlock permission should be the **General** user type and have permission of the certain door. Set the type when adding. For details, see “3.3.2 Adding User.”
- For details of permission assignment, see "3.4 Permission Configuration."

Step 1 Select **Access Configuration > Advanced Config**.

Step 2 Click the **First Card Unlock** tab.

Step 3 Click **Add**.

Step 4 Configure the **First Card Unlock** parameters and click **Save**.

Figure 3-13 First card unlock configuration

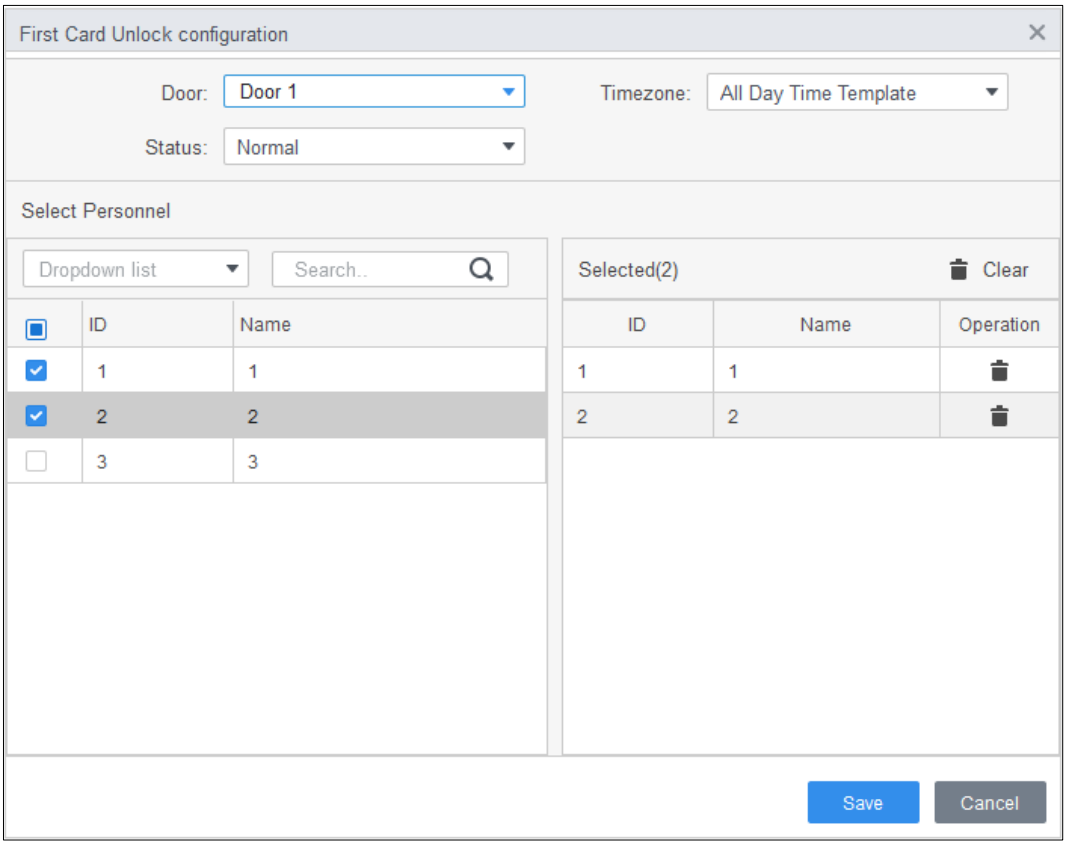


Table 3-2 Parameters of first card unlock

Parameter	Description
Door	Select the target access control channel to configure the first card unlock.
Timezone	First Card Unlock is valid in the time period of the selected time template.
Status	After First Card Unlock is enabled, the door is in either the **Normal mode** or **Always Open mode**.
User	Select the user to hold the first card. Supports selecting a number of users to hold first cards. Any one of them swiping the first card means first card unlock is done.

Step 5 (Optional) Click  . The icon changing into  indicates **First Card Unlock** is enabled.

The newly added **First Card Unlock** is enabled by default.

3.5.1.2 Multi Card Unlock

In this mode, one or multiple groups of users have to swipe cards for an access control channel in an established sequence to unlock the door.

- One group can have up to 50 users, and one person can belong to multiple groups.
- With Multi-Card Unlock enabled for an access control channel, there can be up to four groups of users being on site at the same time for verification. The total number of users can be 200 at most, with up to 5 valid users.

- First card unlock has higher priority than multi-card unlock, which means if the two rules are both enabled, the system performs first card unlock first.
- You are recommended to add people with first card unlock permission to the multi-card Unlock group.
- Do not set the **VIP** or **Patrol** type for people in the user group. For details, see “3.3.2 Adding User.”
- For details of permission assignment, see "3.4 Permission Configuration."

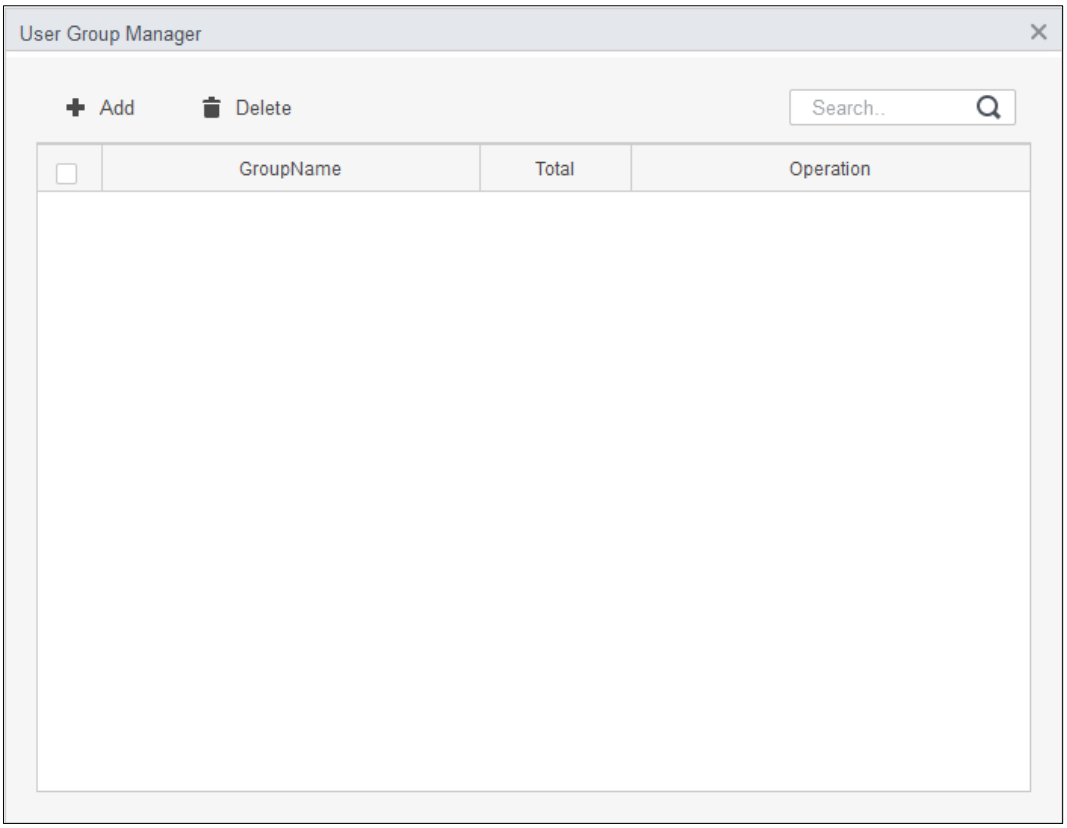
Step 1 Select **Access Configuration > Advanced Config**.

Step 2 Click the **Multi Card Unlock** tab.

Step 3 Add user group.

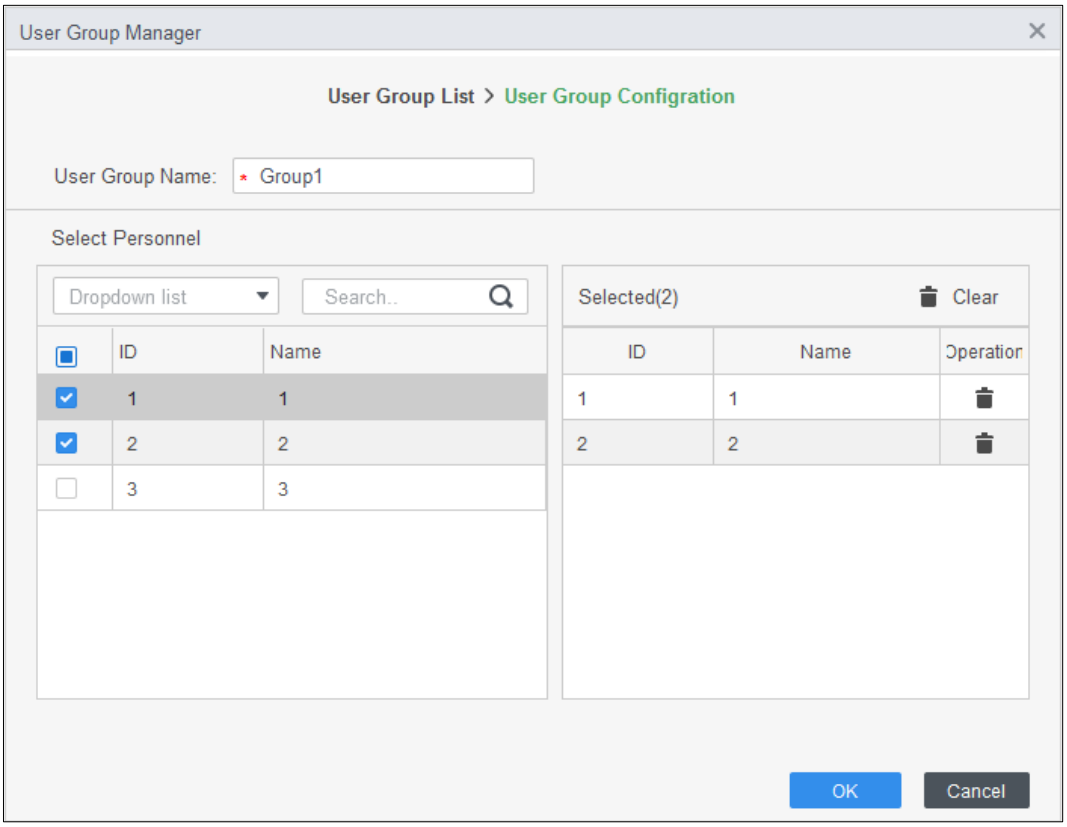
1) Click **User Group**.

Figure 3-14 User group manager



2) Click **Add**.

Figure 3-15 User group configuration



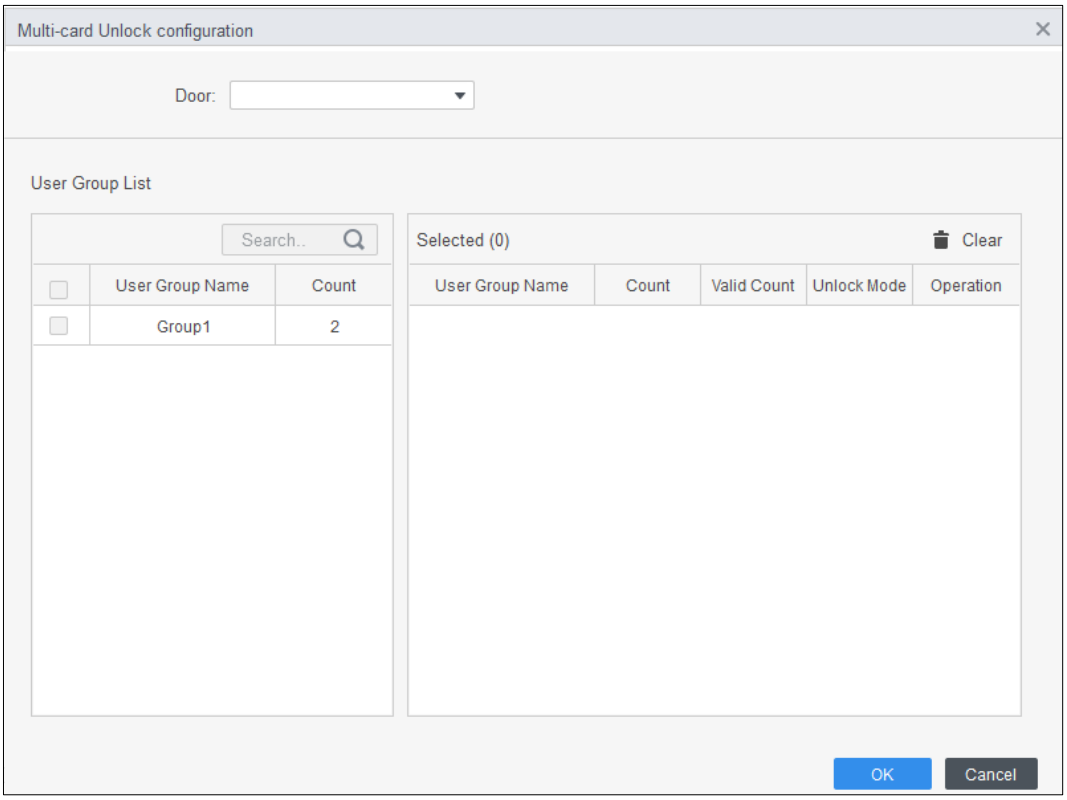
3) Set up **User Group Name**. Select users from **User List** and click **OK**. You can select up to 50 users.

4) Click ☒ at the upper-right corner of the **User Group Manager** interface.

Step 4 Configure parameter of multi card unlock.

1) Click **Add**.

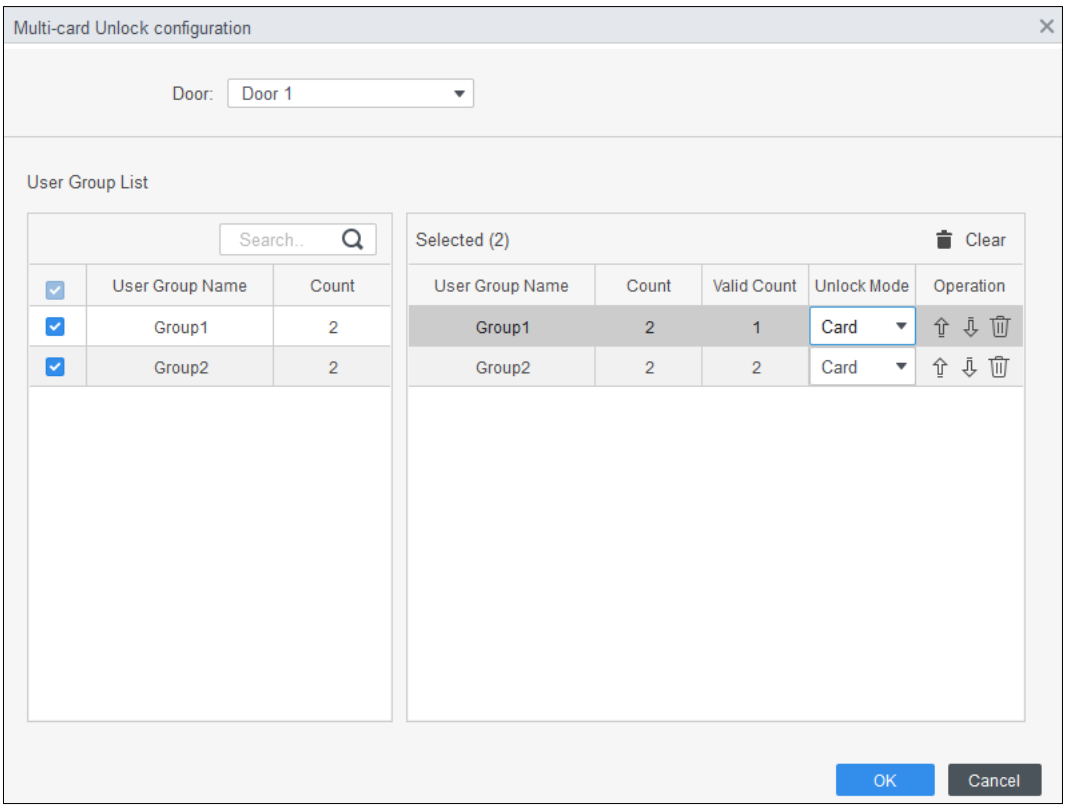
Figure 3-16 Multi card unlock configuration (1)



2) Select the door.

3) Select the user group. You can select up to four groups.

Figure 3-17 Multi card unlock configuration (2)



4) Fill in the **Valid Count** for each group to be on site and the **Unlock Mode**. Click  or  to adjust the group sequence to unlock the door.

The valid count refers to the number of users in each group that must be on site to swipe their cards. Take Figure 3-17 as an example. The door can be unlocked only if it swiped by any person of group 1 and 2 persons of group 2.

Up to five valid users are allowed.

5) Click **OK**.

Step 5 (Optional) Click  . The icon changing into  indicates **Multi Card Unlock** is enabled.

The newly added **Multi Card Unlock** is enabled by default.

3.5.1.3 Anti-passback

The Anti-passback feature requires a person to exit from the specific doors. For the same person, an entry record must pair with an exit record. If someone has entered by tailing someone else, which means there is no entry record, this person cannot unlock the door for exit.

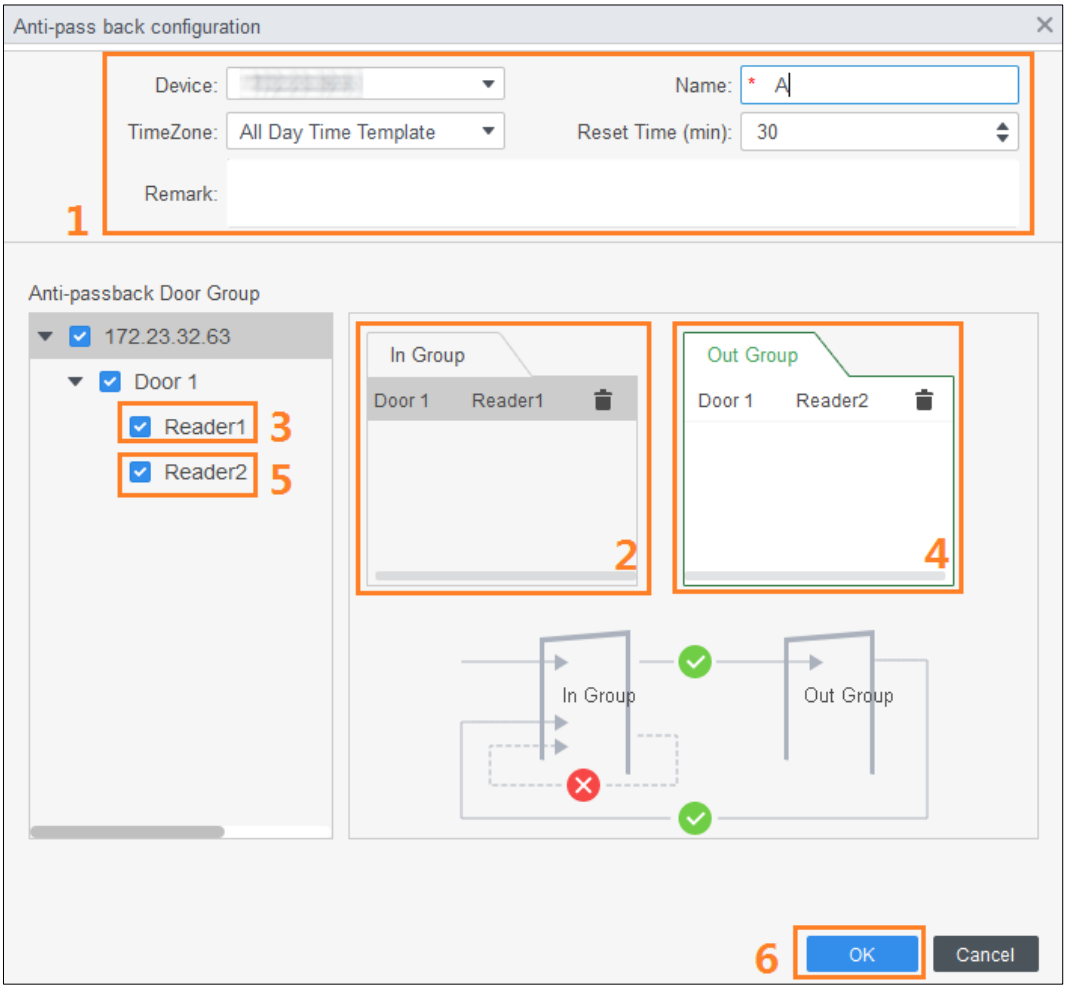
Step 1 Select **Access Configuration > Advanced Config**.

Step 2 Click **Add**.

Step 3 Configure parameters.

1) Select device and enter device name.
2) Select time template.
3) Set rest time and the unit is minute. For example, set the reset time as 30 minutes. If one staff has swiped in but not swiped out, the anti-pass back alarm will be triggered when this staff tends to swipe in again within the 30 minutes. The second swipe-in of this staff is only valid after 30 minutes later.
4) Click **In Group** and select the corresponding reader. And then click **Out Group** and select the corresponding reader.
5) Click **OK**. And then the configuration will issue to device and take effect.

Figure 3-18 Anti-pass back configuration



Step 4 (Optional) Click . The icon changing into indicates **Anti-passback** is enabled.

The newly added **Anti-passback** is enabled by default.

3.5.1.4 Inter-door Lock

One A&C central controller supports two groups of inter-door unlock, and each door group can add up to 4 doors.

Step 1 Select **Access Configuration > Advanced Config**.

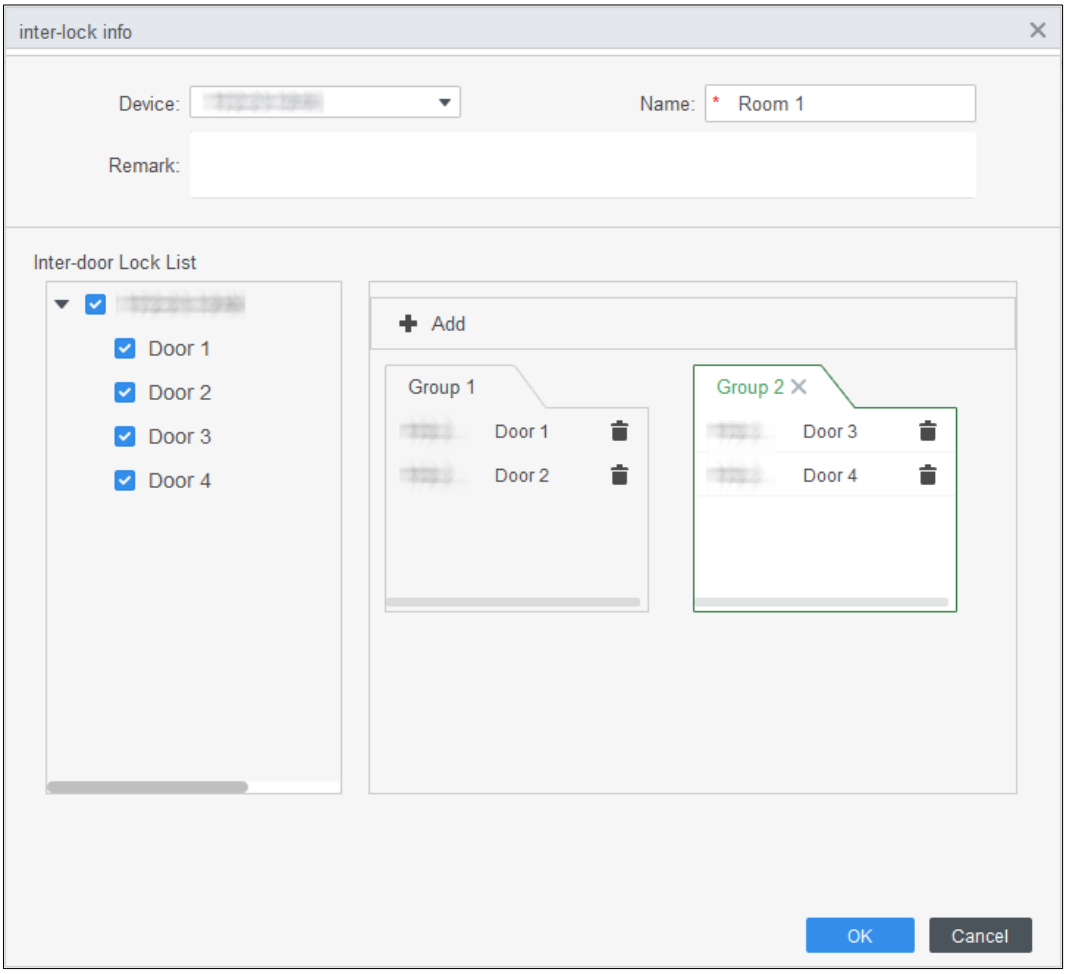
Step 2 Click the **Inter-Lock** tab.

Step 3 Click **Add**.

Step 4 Configure parameters and click **OK**.

1) Select device and enter device name.
2) Enter remark.
3) Click **Add** twice to add two door groups.
4) Add doors of the access controller to the needed door group. Click one door group and then click doors to add.
5) Click **OK**.

Figure 3-19 Inter-door lock configuration



Step 5 (Optional) Click . The icon changing into indicates **Inter-door Lock** is enabled.

The newly added **Inter-door Lock** is enabled by default.

3.5.2 Access Controller Configuration

You can configure access door, such as reader direction, door status and unlock mode.

Step 1 Select **Access Configuration > Access Config**.

Step 2 Click the door needs to be configured.

Step 3 Configure parameters.

Figure 3-20 Configure access door

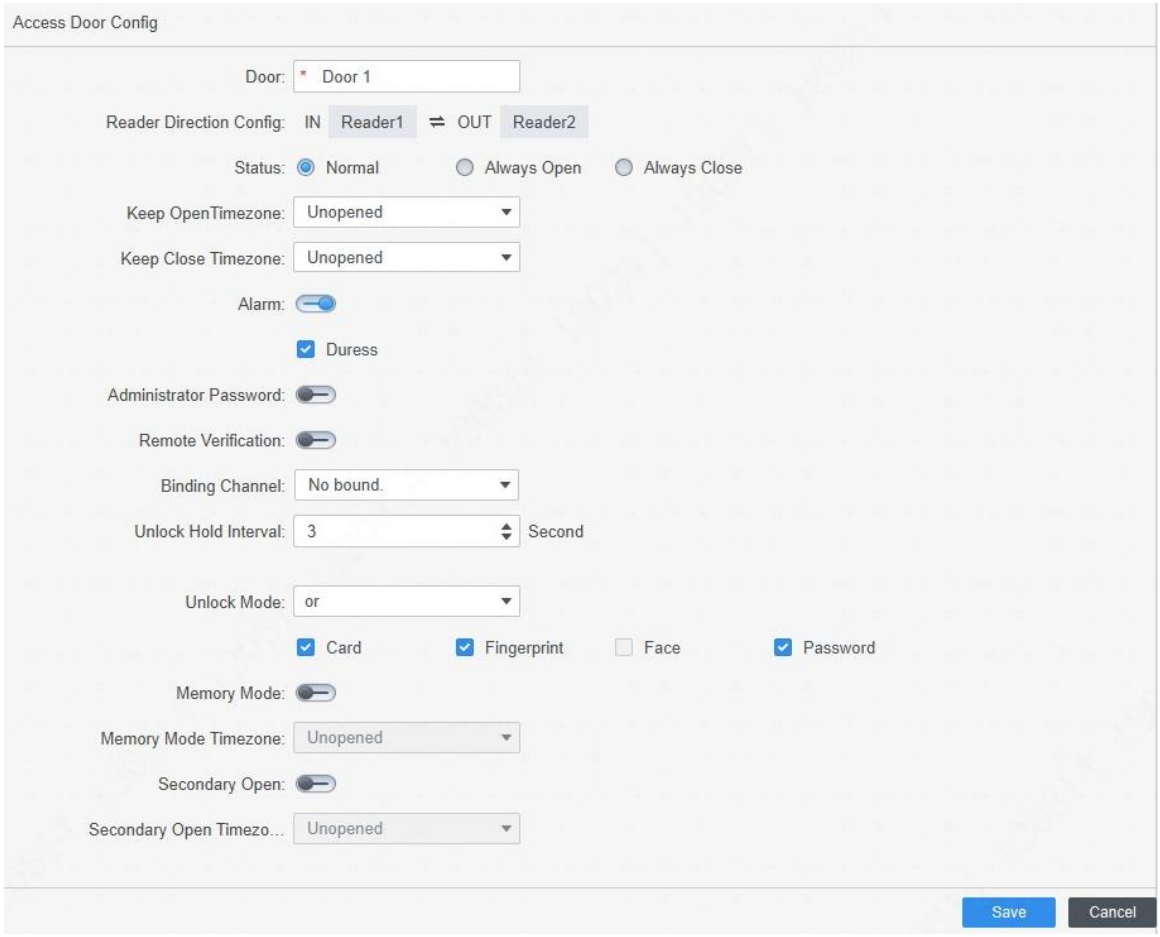


Figure 3-21 Unlock by time period

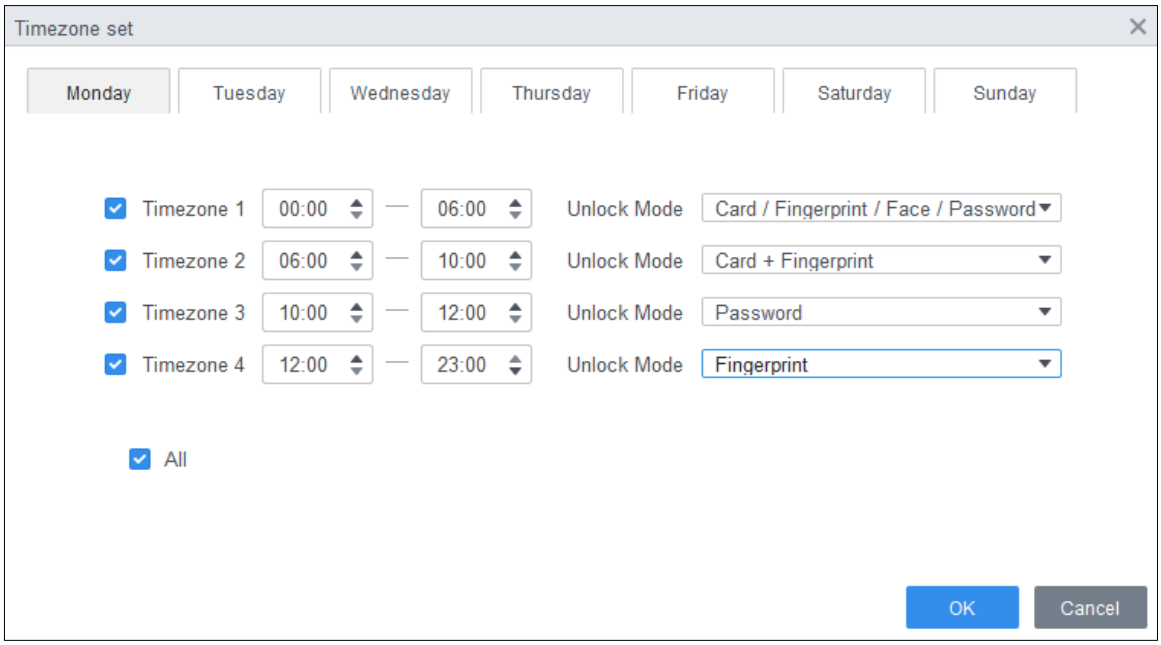


Table 3-3 Parameters of access door

Parameter	Description
Door	Enter door name.
Reader Direction	Click ⇌ to set reader direction according to actual situations.
Status	Set door status, including **Normal**, **Always Open** and **Always Close**. 📖 It is not the actual door status because the SmartPSS-AC can only send commands to the device. If you want to know the actual door status, enable door sensor.
Keep Open Timezone	Select time template when door is always opened.
Keep Close Timezone	Select time template when door is always closed.
Alarm	Enable alarm function and set alarm type, including intrusion, overtime and duress. When alarm enabled, the SmartPSS-AC will receive uploaded message when the alarm is triggered.
Door Sensor	Enable door sensor so that you can know the actual door status. You are recommended to enable the function.
Administrator Password	Enable and set the administrator password. You can access by entering the password.
Remote Verification	Enable the function and set the time template, and then the access of personnel have to be verified remotely through the SmartPSS-AC during the template periods.
Remote Channel	Set the linked video channel of access controllers. After setting, when viewing the video of access controller, the real-time video

Parameter	Description
	of the pre-defined video channel will be displayed.
Unlock Hold Interval	Set the unlock holding interval. The door will auto close when time is over.
Close Timeout	Set the timeout for alarm. For example, set close timeout as 60 seconds. If the door is not closed for more than 60 seconds, the alarm message will be uploaded.
Unlock Mode	Select unlock mode as needed. ● Select **And** and select unlock methods. You need to satisfy all the configured methods at the same time to open the door. ● Select **Or** and select unlock methods. You can open the door in any way you configured.. ● Select **Unlock by time period** and select unlock mode for each time period. The door can only be opened when you satisfy the unlock methods during the period.
Memory Mode	After swiping card once, more than one person can pass the turnstile. There are two modes: Off (default) and On. ● If several people are permitted to pass the turnstile, and one of them did not start to pass the turnstile in 5 seconds, or the one did not pass the turnstile within specified duration and stayed overtime between the turnstiles, the swing barriers will be locked. At this time, you need to swipe cards several times to allow several people pass the turnstile continuously. ● In the memory mode, if card swiping interval exceeds single person passing duration, the memory function will not be triggered. ● The interval between two identity verifications must be longer than the unlock duration of the access controller or the face recognitions access controller; otherwise, only one identity verification will be counted. The recommended identity verification interval is 2 s to 5 s. ● In the memory mode, at most 255 people can pass the turnstile continuously.
Second Unlock	After people entered the turnstile and triggered alarms, they do not need to step backwards and can get identities verified directly.  Memory mode and second unlock functions are only available for turnstiles.

Step 4 Click **Save** and then the configuration will issue to device and take effect.

3.5.3 Viewing Historical Event

Historical door events include those happened on the SmartPSS-AC and door devices. Before viewing, extract historical events on the door devices to ensure that all events are searched.

Step 1 Add the needed personnel to the SmartPSS-AC.

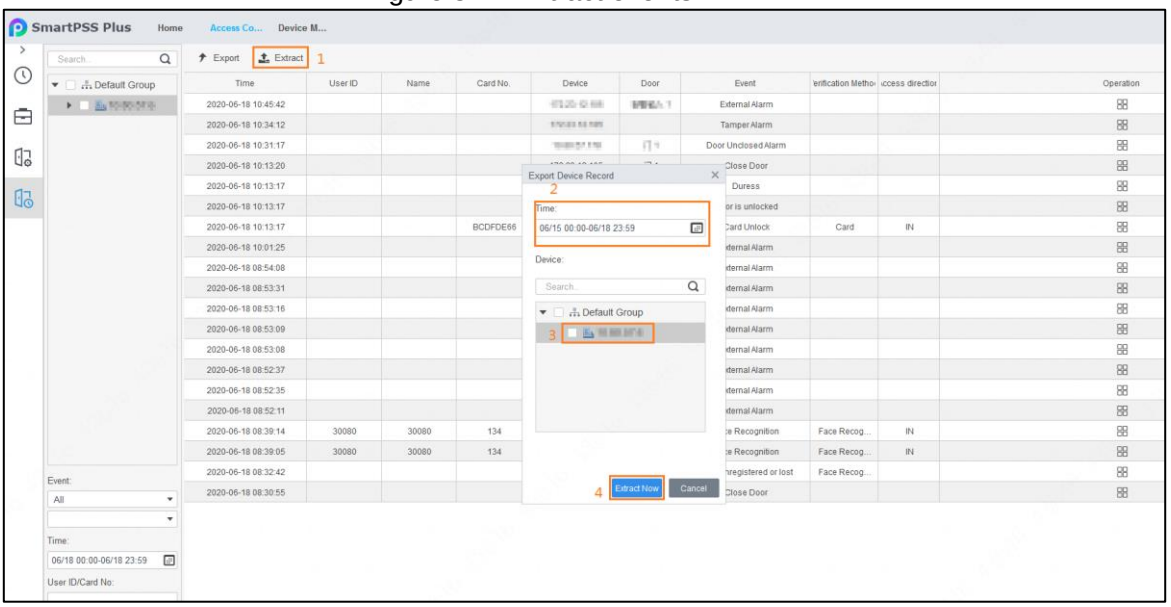
Step 2 Click **Access Configuration > History Event** on the homepage.

Step 3 Click on the **Access Manager** interface.

Step 4 Extract events from door device to the local. Click **Extract**, set the time, select the door device, and then click **Extract Now**.

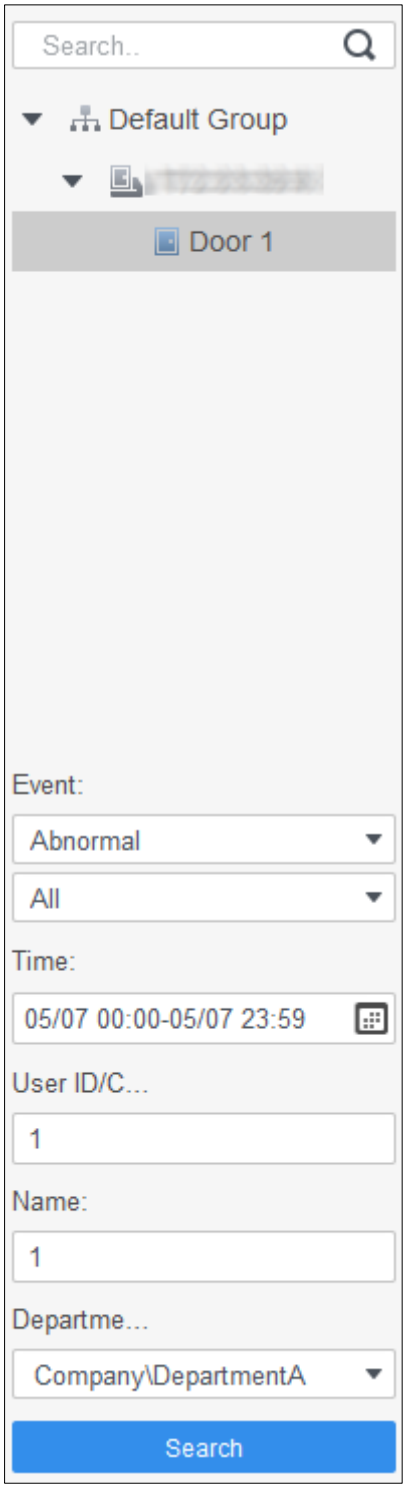
You can select multiple devices at one time to extract events.

Figure 3-22 Extract events



Step 5 Set filtering conditions, and then click **Search**.

Figure 3-23 Search for events by filtering conditions



Step 6 (Optional) Click **Export**, and then operate according to instructions to save the searched door events to the local.

3.6 Access Management

3.6.1 Remotely Opening and Closing Door

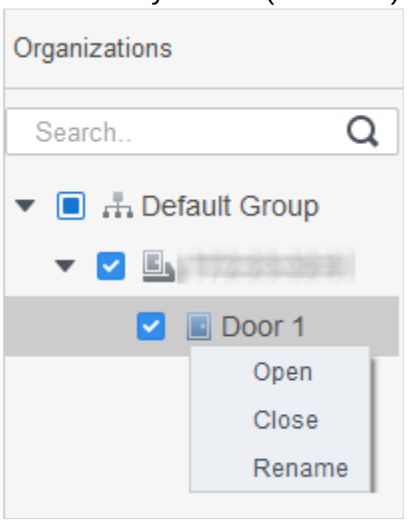
After access configuration, you can remotely control door through SmartPSS AC.

Step 1 Click **Access Manager** on the homepage. (Or click **Access Guide >**).

Step 2 Remotely control the door. There are two methods.

- Method 1: Select the door, right click and select **Open**.

Figure 3-24 Remotely control (method 1)



- Method 2: Click or to open or close the door.

Figure 3-25 Remotely control (method 2)

Step 3 View door status by **Event Info** list.

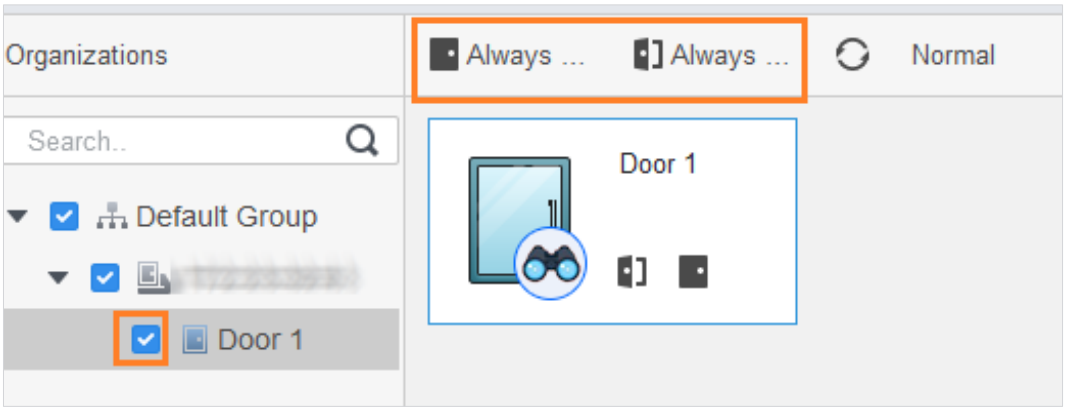
- Event filtering: Select the event type in the **Event Info**, and the event list displays events of the selected types. For example, select **Alarm**, and the event list only displays alarm events.
- Event refresh locking: Click to the right of **Event Info** to lock or unlock the event list, and then the real-time events cannot be viewed.
- Event deleting: Click to the right of **Event Info** to clear all events in the event list.

3.6.2 Setting Always Open and Always Close

After setting always open or always close, the door is open or closed all the time and cannot be controlled manually. If you want to manually control the door again, click **Normal** to reset the door status.

Step 1 Click **Access Manager** on the homepage. (Or click **Access Guide >**).
Step 2 Select the needed door, and then click **Always Open** or **Always Close**.

Figure 3-26 Set always open or always close



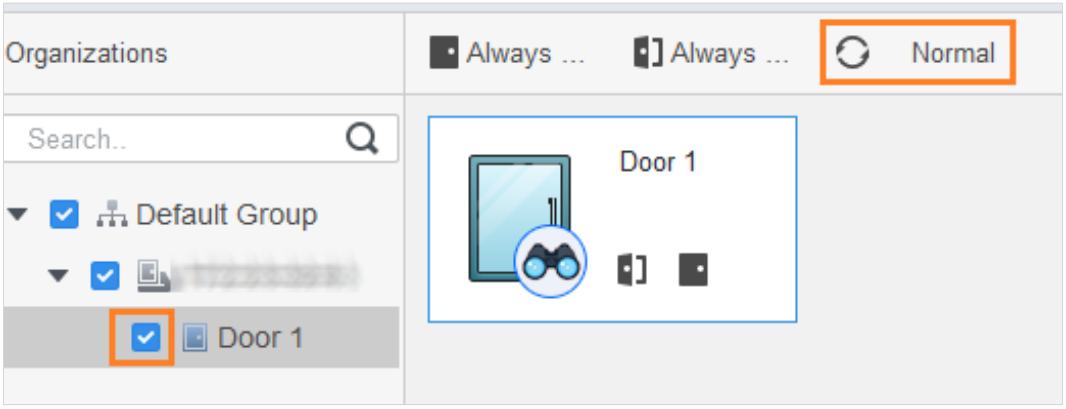
3.6.3 Resetting Door Status

Click **Normal** to reset the door status, if you want to manually control the door again when you have clicked **Always Open** or **Always Close**.

Step 1 Click **Access Manager** on the homepage. (Or click **Access Guide >**).

Step 2 Select the needed door, and then click **Normal**. And then follow the on-screen instructions to operate.

Figure 3-27 Reset door status



3.7 Event Configuration

By event configuration, you can make software linkages, such as alarm sound, mail sending and alarm linkages.

- Configure external alarm linkages connected to the access controller, such as smoke alarm.
- Configure linkages of access controller events.
  - ◇ Alarm event
  - ◇ Abnormal event
  - ◇ Normal event

For anti-pass back function, set the anti-pass back mode in **Abnormal** of **Event Config**, and then configure the parameters in **Advanced Config**. For details, see "3.5.1 Advanced Functions Configuration."

Step 1 Click **Event Config** on the homepage.

Step 2 Select the needed door and select **Alarm Event > Intrusion Event**.

Step 3 Click to the right of **Intrusion Alarm** to enable the function.

Step 4 Configure intrusion alarm linage actions as needed.

- Enable alarm sound.

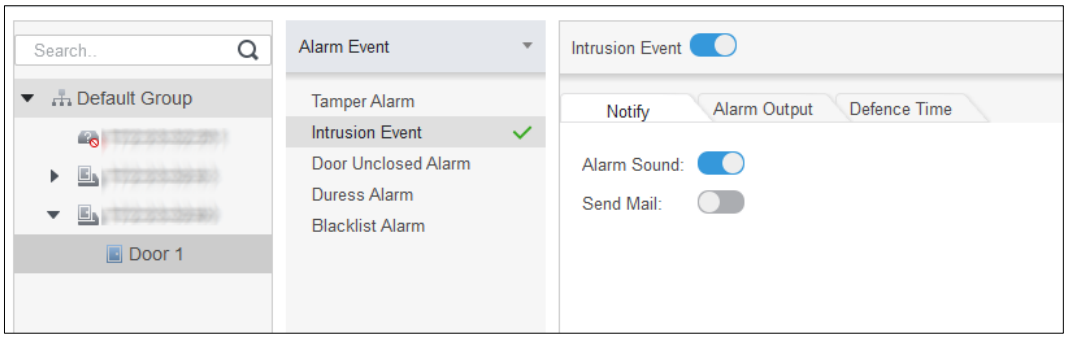
  Click the **Notify** tab, and click to the right of **Alarm Sound**. When intrusion event happens, the access controller warns by alarm sound.

- Send alarm mail.

1) Enable **Send Mail** and confirm to set SMTP, you will automatically go to the **System Settings** interface.
2) Configure SMTP parameters, such as server address, port number, and encrypt mode.

   When intrusion event happens, the system automatically sends alarm mails to the specified receiver.

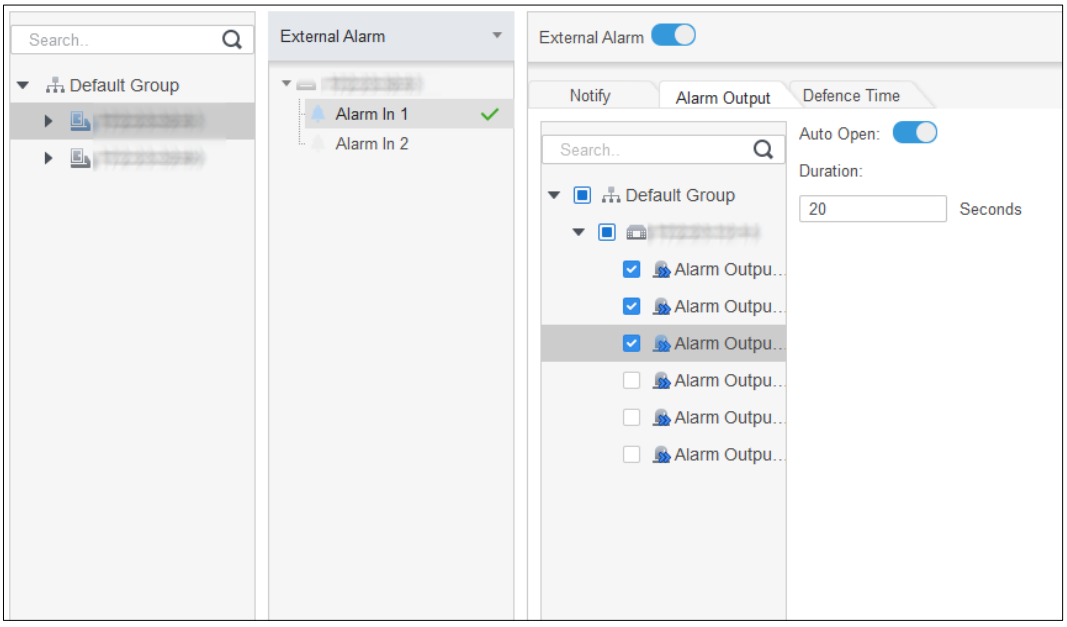
Figure 3-28 Configure intrusion alarm



- Configure alarm I/O.

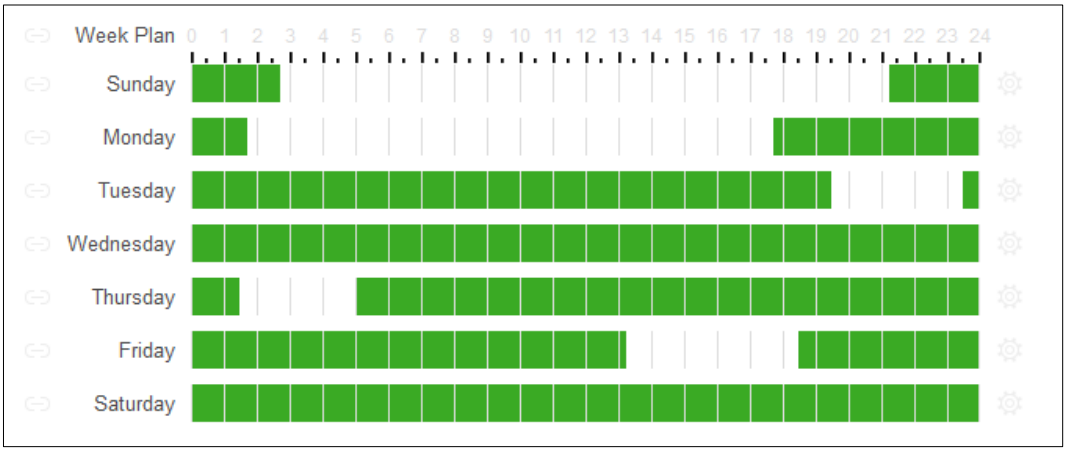
3) Click Alarm Output tab.
4) Select the device which supports alarm in, then select alarm-in interface, and then enable **External Alarm**.
5) Select the device which supports alarm out, then select alarm-out interface.
6) Enable **Auto Open** for the alarm linkage.
7) Set the duration.

Figure 3-29 Configure alarm linkage



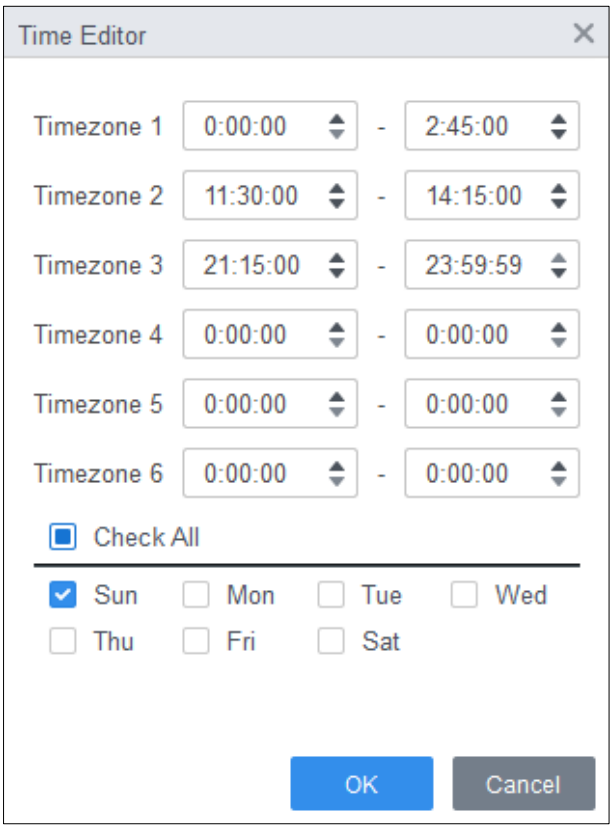
- Set defence time. There are two methods.
  - ◇ Method 1: Move the cursor to set time periods. When the cursor is pencil, click to add periods; when the cursor is eraser, click to minus periods. The green area is the periods with defence.

Figure 3-30 Set defence time (method 1)



  - ◇ Method 2: Click  to set periods, and then click **OK**.

Figure 3-31 Set defence time (method 2)



Step 5 (Optional) Click **Copy To**, select the access controller to be applied on, and then click **OK**.

Step 6 Click **Save**.

4 ConfigTool Configuration

ConfigTool is mainly used to configure and maintain the Device.

Do not use ConfigTool and SmartPSS AC at the same time, otherwise it may cause abnormal device search.

4.1 Adding Devices

You can add one or multiple devices according to your actual needs.

Make sure that the Device and the PC where the ConfigTool is installed are connected; otherwise the tool cannot find the Device.

4.1.1 Adding One Device

Step 1 Click .

Step 2 Click Manual Add.

Step 3 Select IP Address or Device SN from Add Type list.

Figure 4-1 Manual add (IP address)

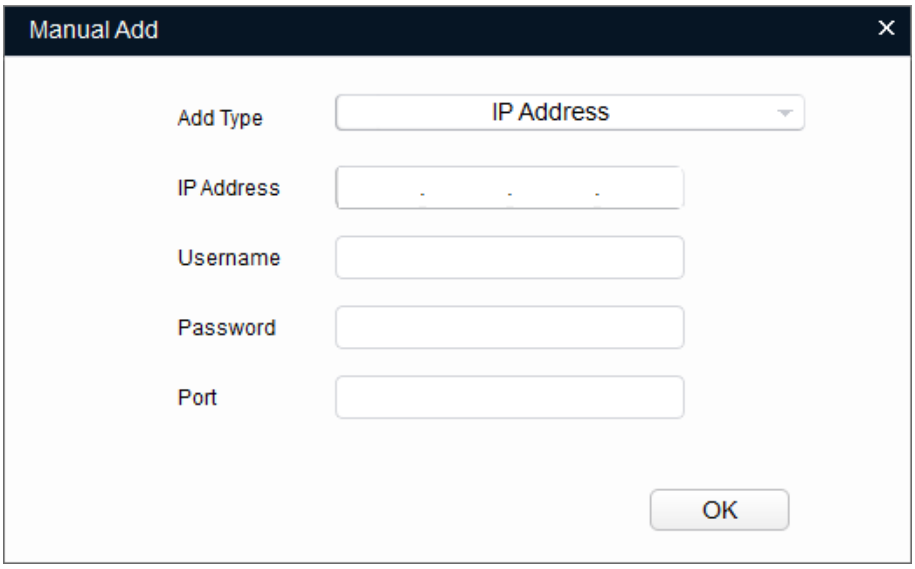


Figure 4-2 Manual add (Device SN)

Step 4 Set the device parameters.

Table 4-1 Manual add parameters

Add Method	Parameter	Description
IP Address	IP Address	The IP address of the device. It is 192.168.1.108 by default.
	Username	The user name and password for device login.
	Password	
	Port	The device port number.
Device SN (Device support P2P only)	SN	The serial number of the device.
	Username	The user name and password for device login.
	Password	

Step 5 Click **OK**.

The newly added device appears in the device list.

4.1.2 Adding Multiple Devices

You can add multiple devices through searching devices or importing the template.

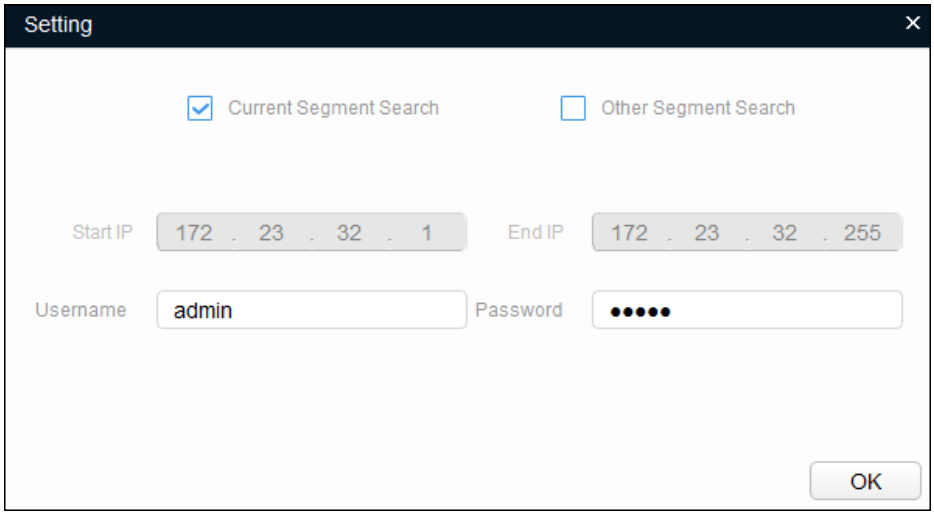
4.1.2.1 Adding by Searching

You can add multiple devices through searching the current segment or other segment.

You can set the filtering conditions to search the wanted device quickly.

Step 1 Click Search setting.

Figure 4-3 Setting



Step 2 Select the searching way. Both the following two ways are selected by default.

- Current Segment Search

Select the **Current Segment Search** check box. Enter the user name in the **Username** box and the password in the **Password** box. The system will search the devices accordingly.

- Other Segment Search

Select the **Other Segment Search** check box. Enter the IP address in the **Start IP** box and **End IP** box respectively. Enter the user name in the **Username** box and the password in the **Password** box. The system will search the devices accordingly.

- If you select both the **Current Segment Search** check box and the **Other Segment Search** check box, the system searches devices under the both conditions.
- The username and the password are the ones used to log in when you want to modify IP, configure the system, update the device, restart the device, and more.

Step 3 Click **OK** to start searching devices.

The searched devices will appear in the device list on the main user interface.

- Click to refresh the device list.
- The system saves the searching conditions when exiting the software and reuses the same conditions when the software is launched next time.

4.1.2.2 Adding by Importing Device Template

You can add the devices by filling in and importing an Excel template. You can import 1000 devices at most.

Close the template file before importing the devices; otherwise the import will fail.

Step 1 Export device template. Click , select one device, click **Export**, and then follow the on-screen guide to save the template file locally.

Step 2 Fill in the template. Open the template file, follow the existing device info to fill in the info of devices you want to add.

Step 3 Import the template. Click **Import**, select the template and click **Open**.
The system starts importing the devices details. After the importing is completed, a success notice is displayed.

Step 4 Click **OK**.
The newly imported devices appear in the device list.

4.2 Configuring Access Controller

The interface and parameters might vary depending on the device type and model, and the actual interface shall prevail.

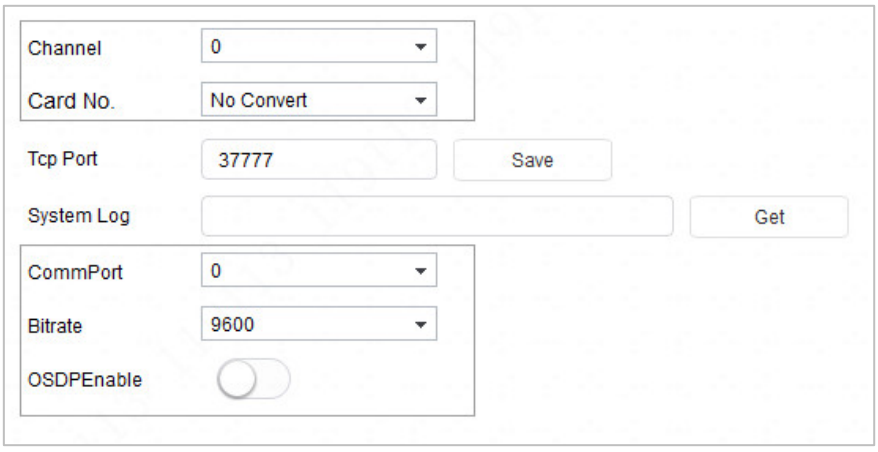
Step 1 Click on the menu bar.

Step 2 Click the access controller that you want to configure in the device list, and then click **Get Device Info**.

Step 3 (Optional) If the Login interface prompts, enter the username and password, and then click **OK**.

Step 4 Set access controller parameters.

Figure 4-4 Configure access controller



- Channel: Select the channel to set the parameters.
  Card No.: Set the card number processing rule of the access controller. It is **No Convert** by default. When the card reading result does not match the sent card No., select **Byte Revert** or **HIDpro Convert**.
  - ◇ Byte Revert: When access controller works with third-party readers, and the card reading result does not match the sent card No. for example, the card reading result is hexadecimal 12345678 while the sent card No. is hexadecimal 78563412, you can select **Byte Revert** to match them.

◇ HIDpro Convert: When access controller works with HID Wiegand readers, and the card reading result does not match the sent card No., for example, the card reading result is hexadecimal 1BAB96 while the sent card No. is hexadecimal 78123456, you can select **HIDpro Revert** to match them.

- TCP Port: Modify TCP port number of the Device.
- SysLog: Click **Get** to select a storage path for system logs.
- CommPort: Select the reader to set bitrate and enable OSDP.
- Bitrate: If card reading is slow, you can increase bitrate. It is 9600 by default.
- OSDPEnable: When access controller works with third-party readers through ODSP protocol, enable ODSP.

Step 5 (Optional) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**.

If succeeds, ✓ is displayed on the right side of the Device; if fails, ⚠ is displayed. You can click the icon to view detailed information.

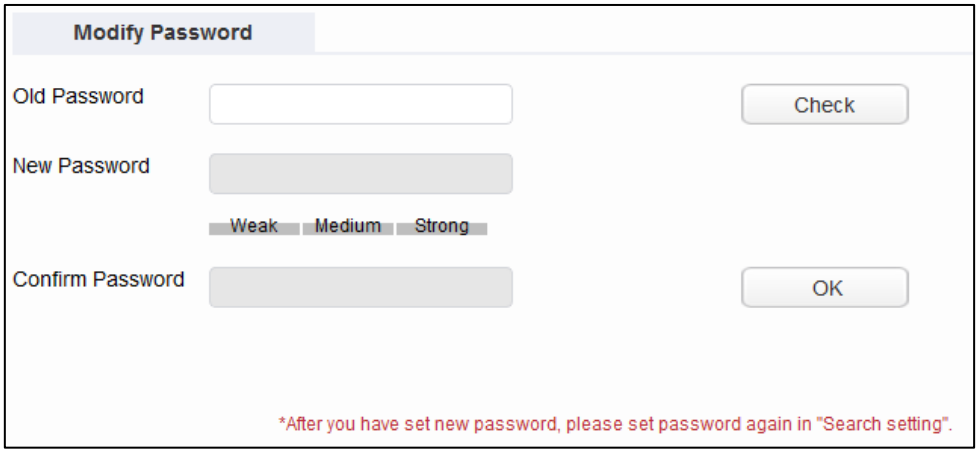
4.3 Modifying Device Password

You can modify the device login password.

Step 1 Click  .

Step 2 Click the **Device Password** tab.

Figure 4-5 Device password



Step 3 Click ▶ next to the device type, and then select one or multiple devices.

If you select multiple devices, the login passwords must be the same.

Step 4 Set the password.

Follow the password security level hint to set a new password.

Table 4-2 Password parameters

Parameter	Description
Old Password	Enter the device old password. To make sure that the old password is entered correctly, you can click **Check** to verify.

New Password	Enter the new password for the device. There is an indication for the strength of the password. The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
Confirm Password	Confirm the new password.

Step 5 Click **OK** to complete modification.

Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

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

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

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

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

4. **Enable Account Lock**

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

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

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

6. **Enable HTTPS**

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

7. **MAC Address Binding**

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

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 equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

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

- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.