Access Controller (C)

User's Manual

V1.0.3

Foreword

General

This manual introduces the structure, functions and operations of the access controller (hereinafter referred to as "the 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, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.3	Updated the format.	July 2024
V1.0.2	Updated wiring image.	June 2022
V1.0.1	Added initialization process.	December 2021
V1.0.0	First release.	March 2021

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the Controller.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Controller, hazard prevention, and prevention of property damage. Read carefully before using the Controller, comply with the guidelines when using it, and keep the manual safe for future reference.

Transportation Requirement

Transport the Controller under allowed humidity and temperature conditions.

Storage Requirement

Store the Controller under allowed humidity and temperature conditions.

Installation Requirements

- Do not connect the power adapter to the Controller while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Controller.
- Do not connect the Controller to two or more kinds of power supplies, to avoid damage to the Controller.
- Improper use of the battery might result in a fire or explosion.

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Controller in a place exposed to sunlight or near heat sources.
- Keep the Controller away from dampness, dust, and soot.
- Install the Controller on a stable surface to prevent it from falling.
- Install the Controller in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.

- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the Controller label.
- The Controller is a class I electrical appliance. Make sure that the power supply of the Controller is connected to a power socket with protective earthing.
- The Controller must be grounded when it is connected to 220 V mains electricity.

Table of Contents

1 Overview

1.1 Introduction

The Controller is an access control panel 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.

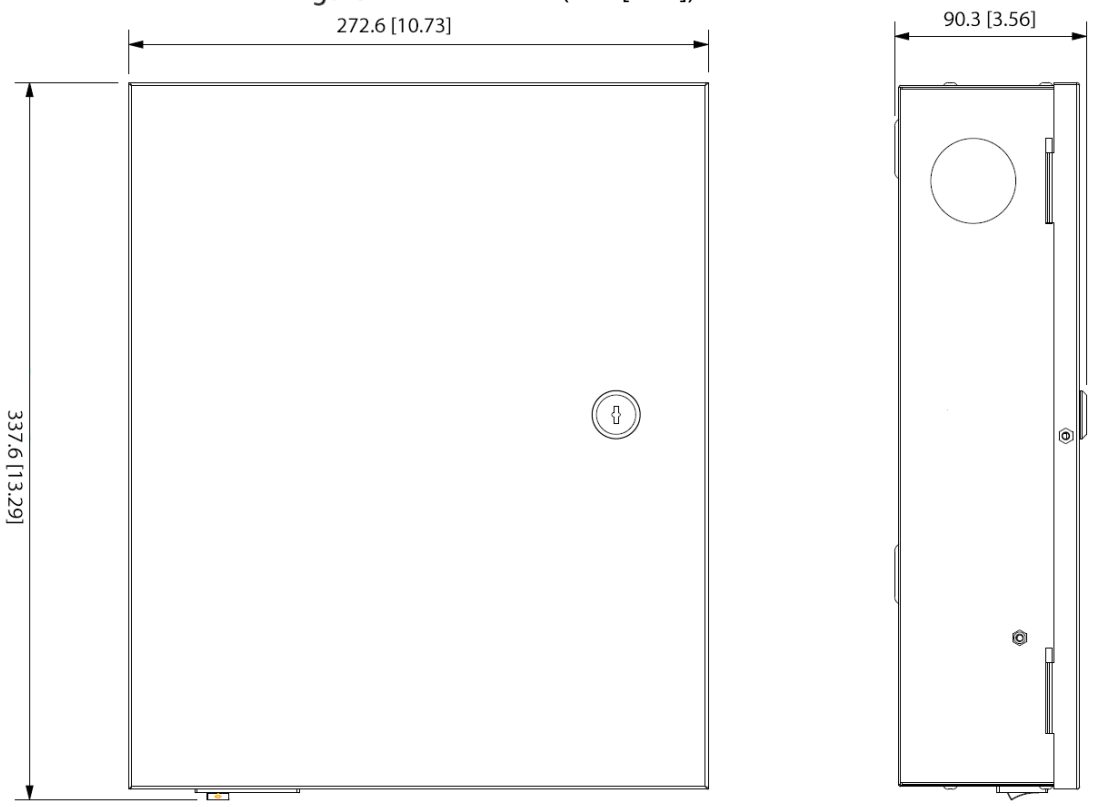
1.1 Features

- Adopts SEEC steel board to deliver a high-end appearance.
- Supports TCP/IP network communication. Communication data is encrypted for security.
- Auto registration.
- Supports OSDP protocol.
- Supports card, password and fingerprint unlock.
- Supports 100,000 users, 100,000 cards, 3,000 fingerprints, and 500,000 records.
- Supports interlock, anti-passback, multi-user unlock, first card unlock, admin password unlock, remote unlock, and more.
- Supports tamper alarm, intrusion alarm, door sensor timeout alarm, duress alarm, blocklist alarm, invalid card exceeding threshold alarm, incorrect password alarm and external alarm.
- Supports user types such as general users, VIP users, guest users, blocklist users, patrol users, and other users.
- Supports built-in RTC, NTP time calibration, manual time calibration, and automatic time calibration functions.
- Supports offline operation, event record storage and upload functions, and automatic network replenishment (ANR).
- Support 128 periods, 128 holiday plans, 128 holiday periods, normally open periods, normally closed periods, remote unlock periods, first card unlock periods, and unlock in periods.
- Supports watchdog guard mechanism to ensure the operation stability.

1.2 Dimensions

There are five kinds of access controllers, including two-door one-way, two-door two-way, four-door one-way, four-door two-way, and eight-door one-way. Their dimensions are the same.

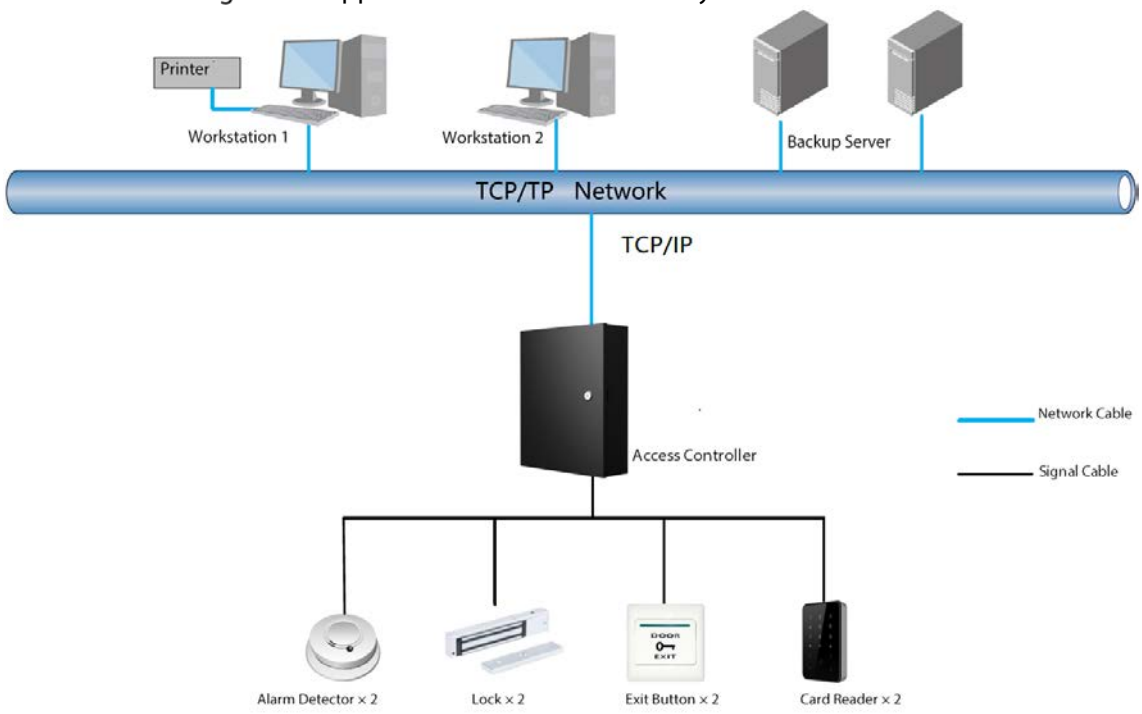
Figure 1-1 Dimensions (mm [inch])



1.3 Application

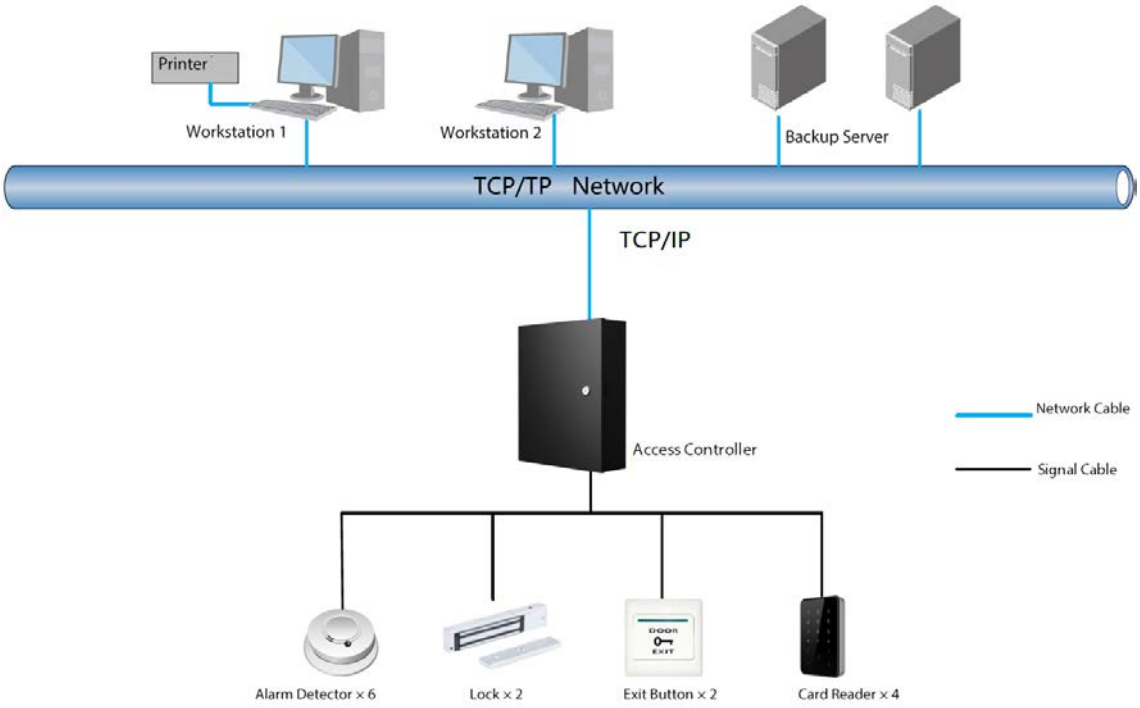
1.3.1 Two-door One-way

Figure 1-2 Application of two-door one-way controller



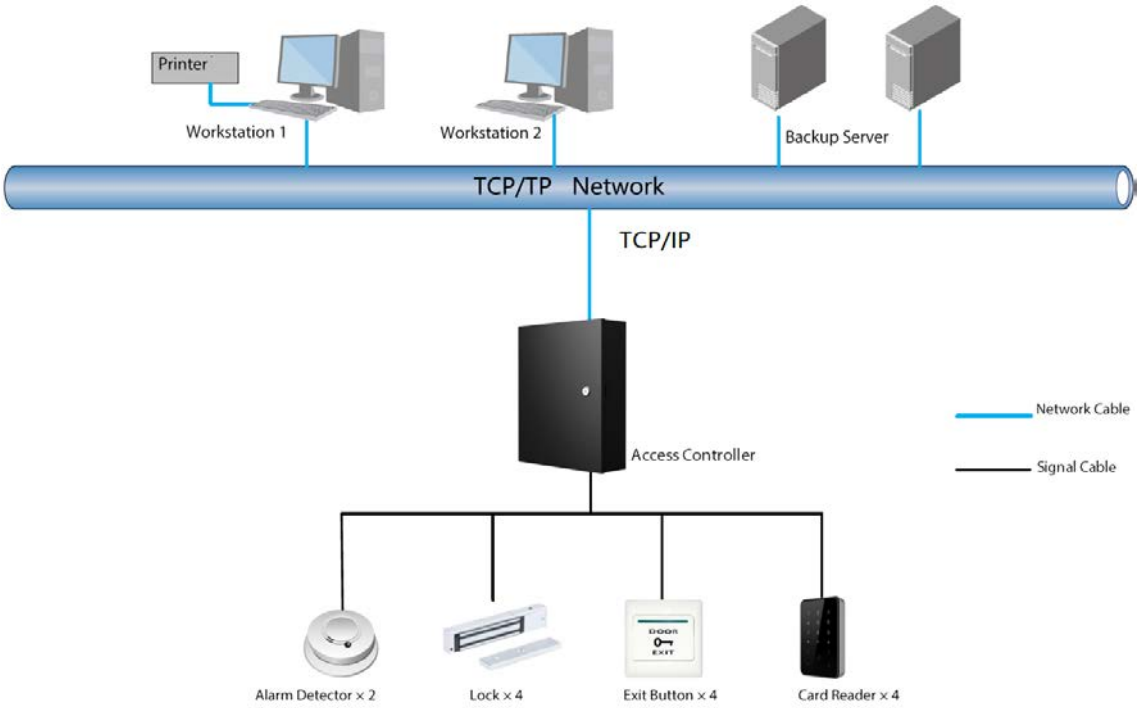
1.3.2 Two-door Two-way

Figure 1-3 Application of two-door two-way controller



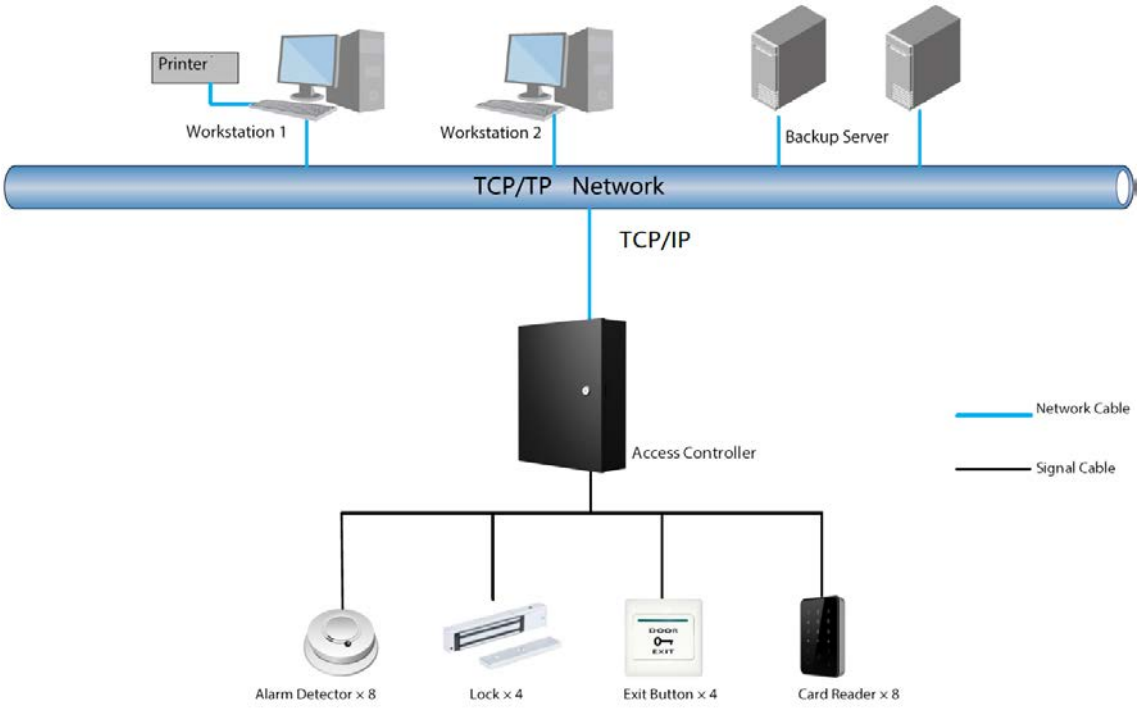
1.3.3 Four-door One-way

Figure 1-4 Application of four-door one-way controller



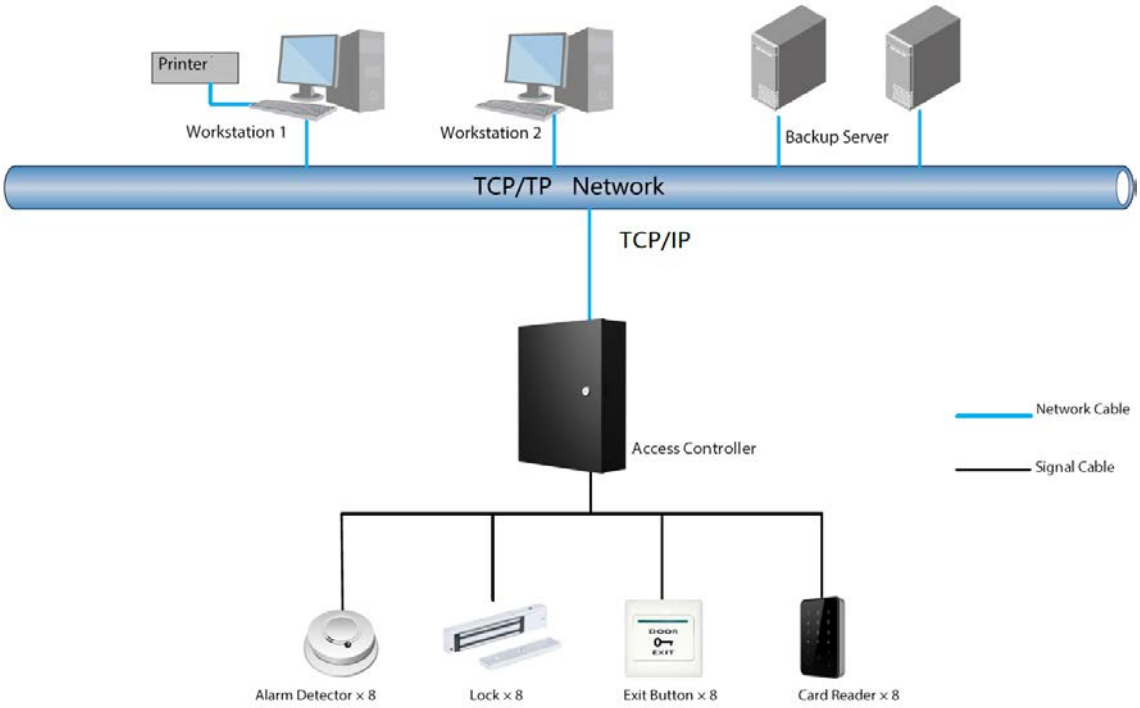
1.3.4 Four-door Two-way

Figure 1-5 Application of four-door two-way controller



1.3.5 Eight-door One-way

Figure 1-6 Application of eight-door one-way controller



2 Structure

2.1 Wiring

⚠

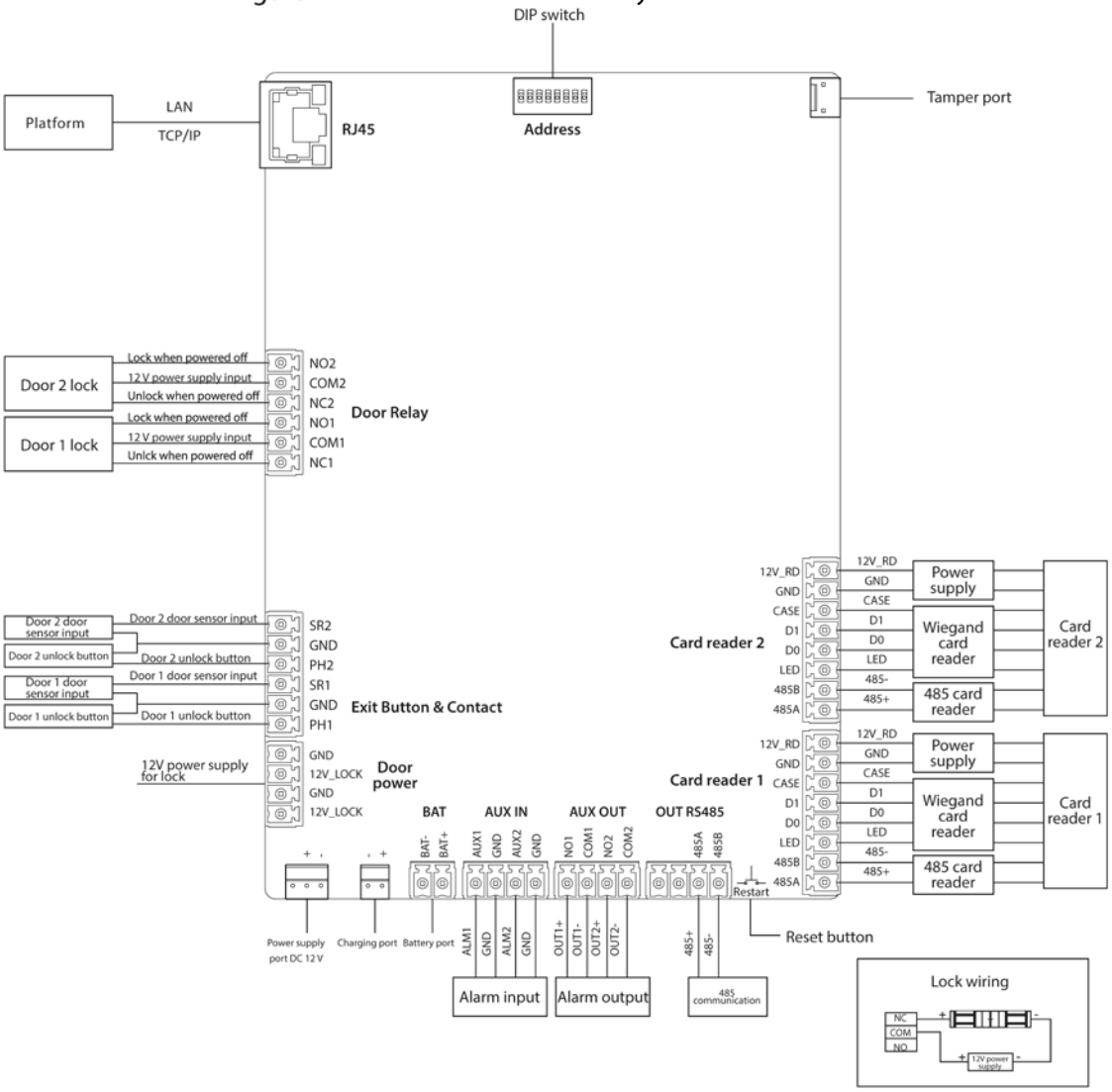
- Connect the wires only when powered off.
- Make sure that the plug of the power supply is grounded.
- 12 V: Maximum current for an extension module is 100 mA.
- 12 V_RD: Maximum current for a card reader is 2.5 A.
- 12 V_LOCK: Maximum current for a lock is 2 A.

Table 2-1 Wire specification

Device	Cable	Cross-sectional Area of Each Core	Remarks
Card reader	Cat5 8-core shielded twisted pair	≥ 0.22 mm^2	Suggested ≤ 100 m
Ethernet cable	Cat5 8-core shielded twisted pair	≥ 0.22 mm^2	Suggested ≤ 100 m
Button	2-core	≥ 0.22 mm^2	–
Door contact	2-core	≥ 0.22 mm^2	–

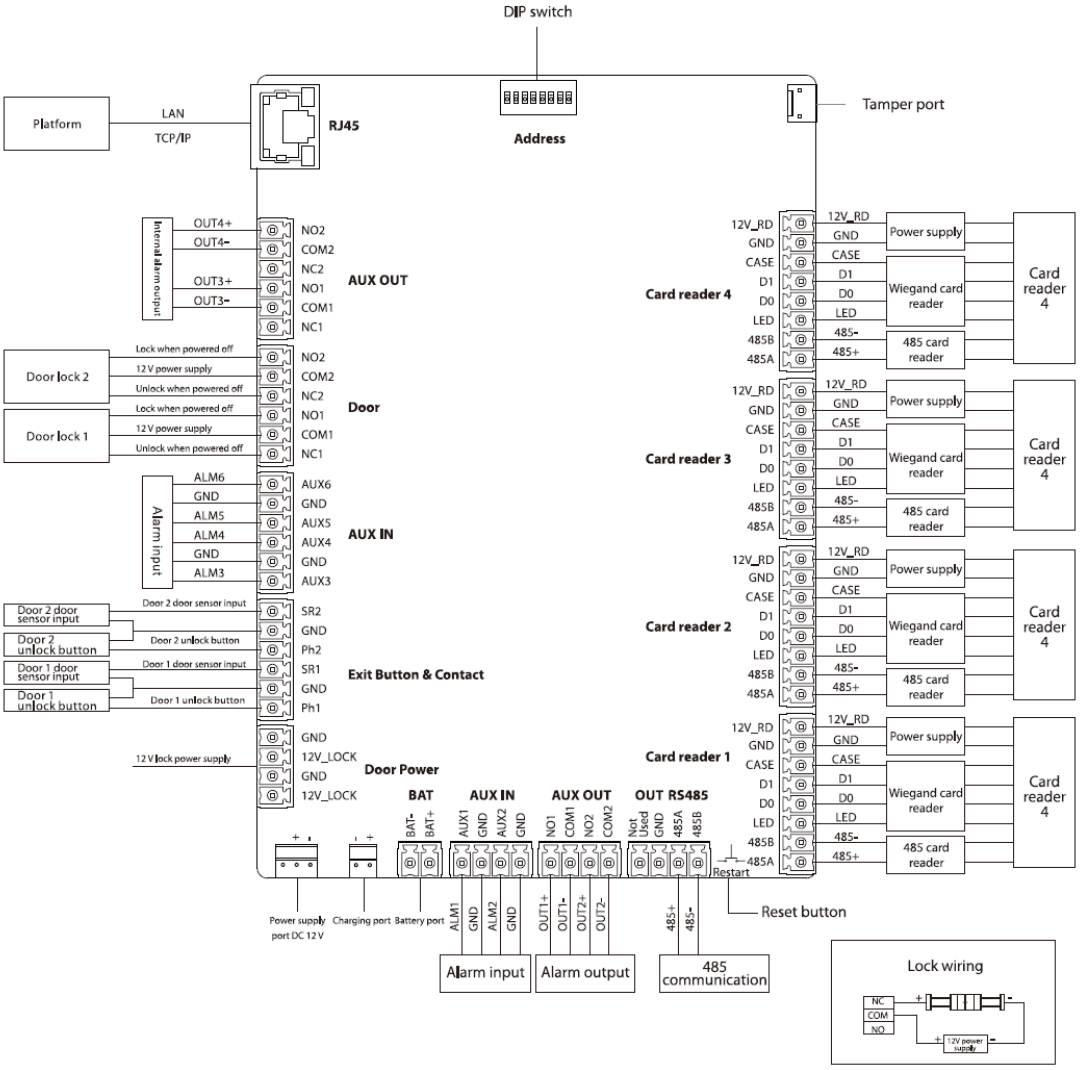
2.1.1 Two-door One-way

Figure 2-1 Wire a two-door one-way controller



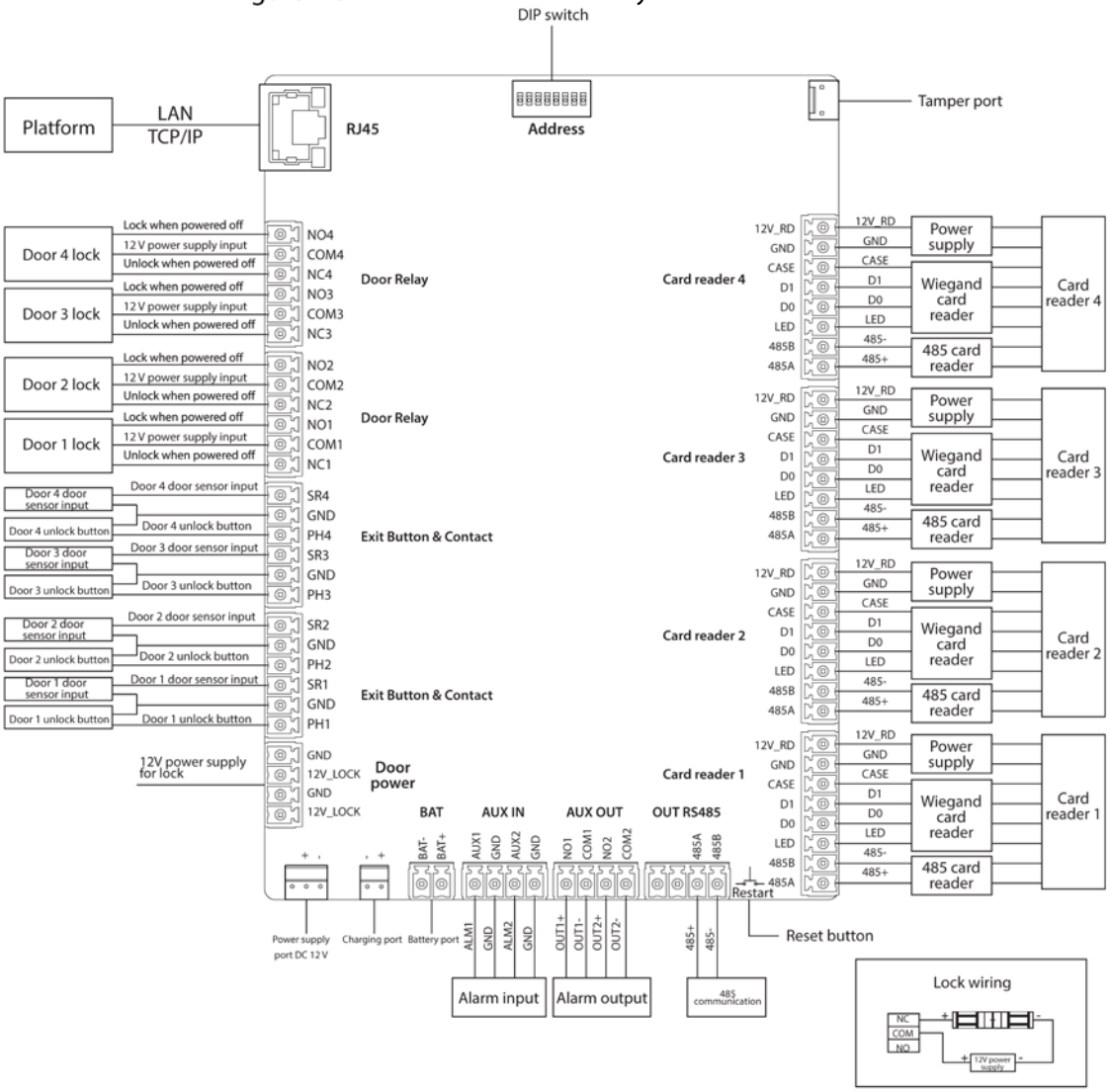
2.1.2 Two-door Two-way

Figure 2-2 Wire a two-door two-way controller



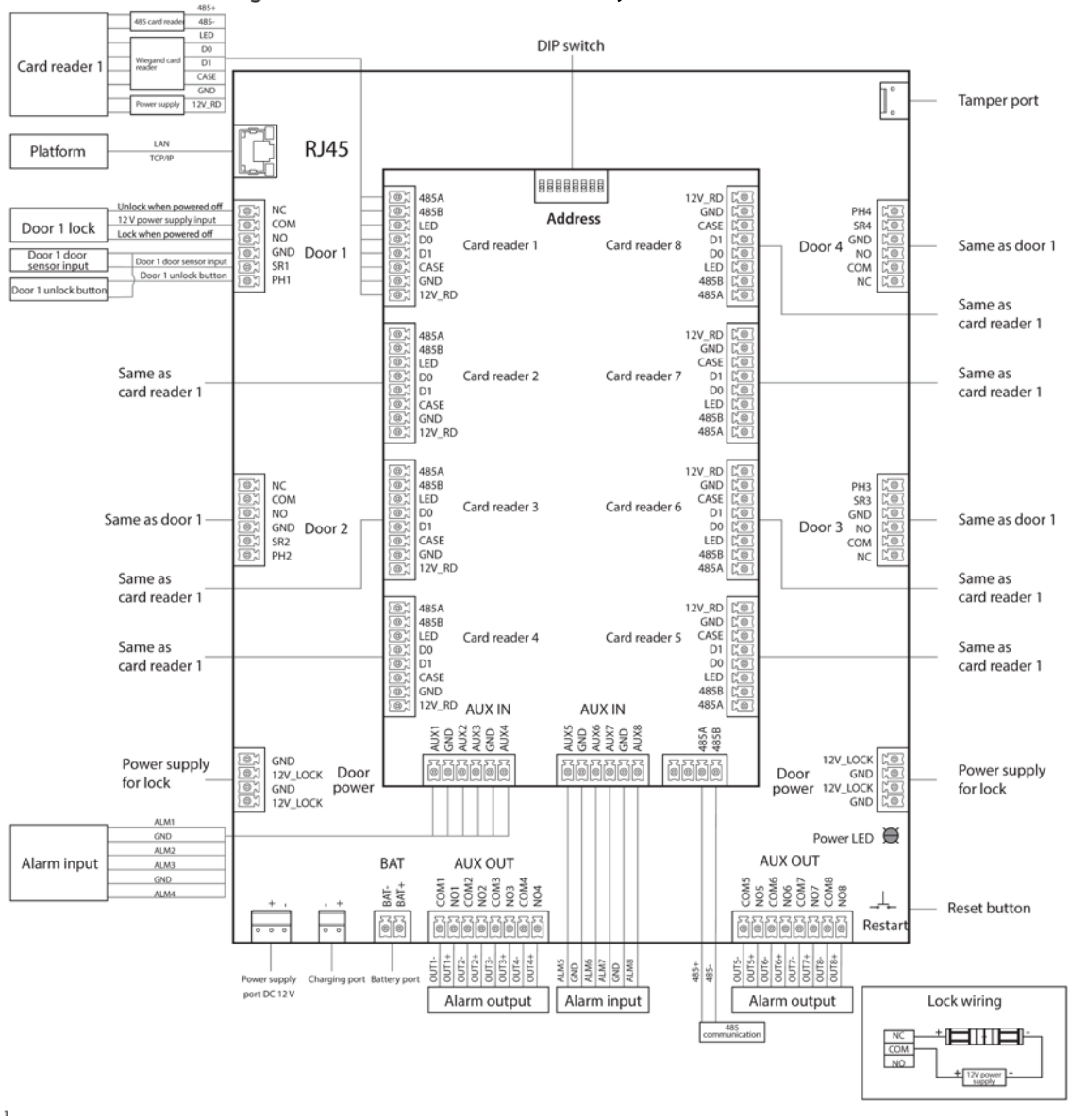
2.1.3 Four-door One-way

Figure 2-3 Wire a four-door one-way controller



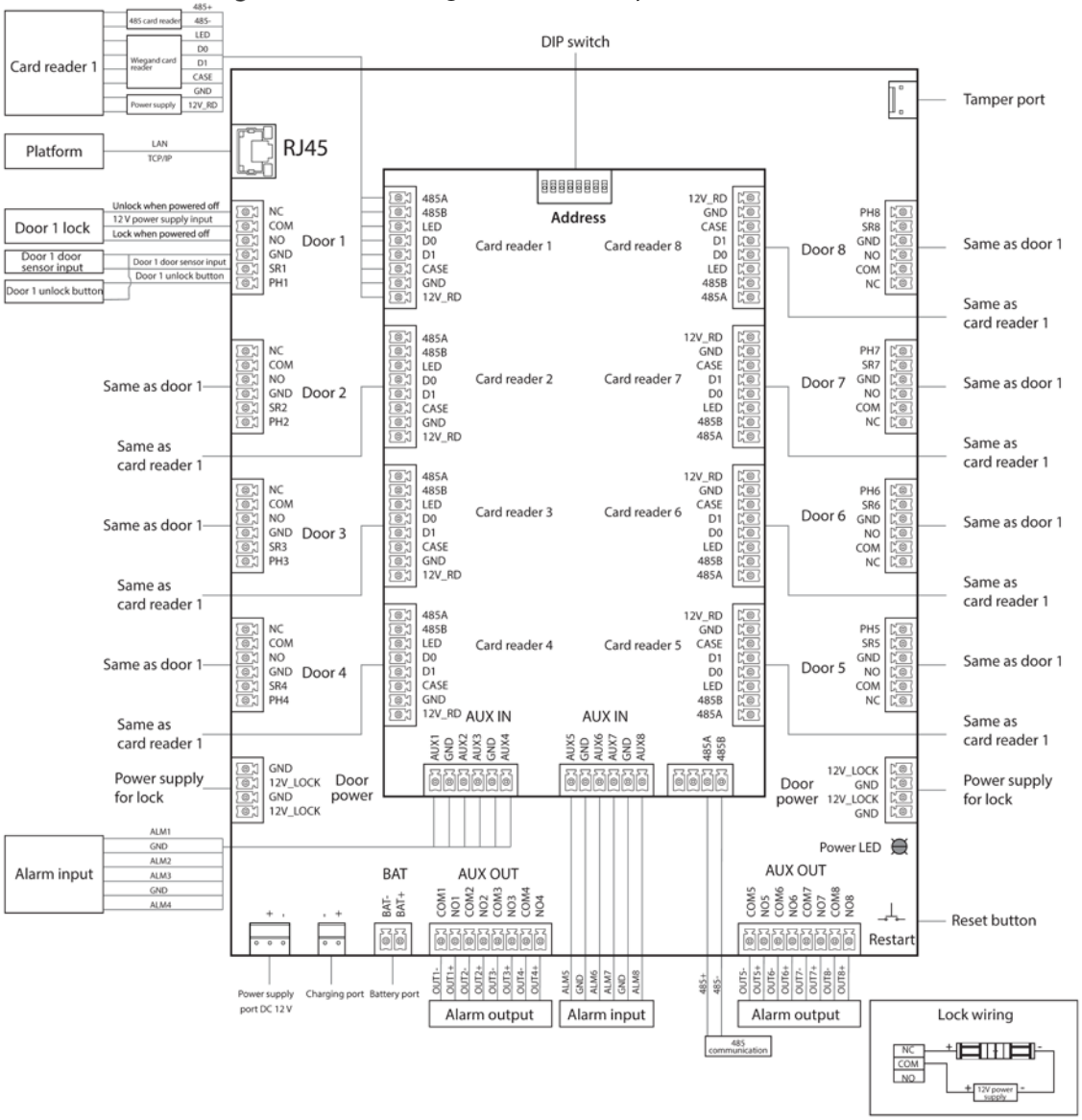
2.1.4 Four-door Two-way

Figure 2-4 Wire a four-door two-way controller



2.1.5 Eight-door One-way

Figure 2-5 Wire an eight-door one-way controller



2.1.6 Lock

Select the wiring method according to your lock type.

Figure 2-6 Electric lock

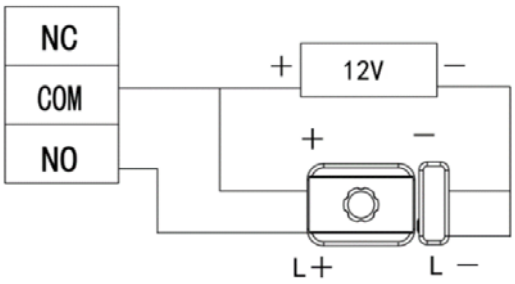


Figure 2-7 Magnetic lock

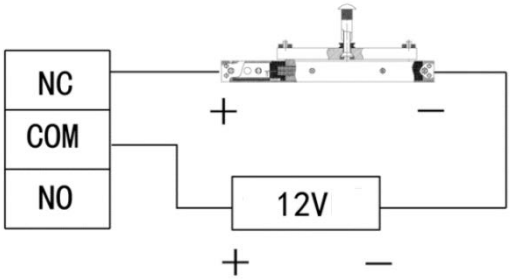
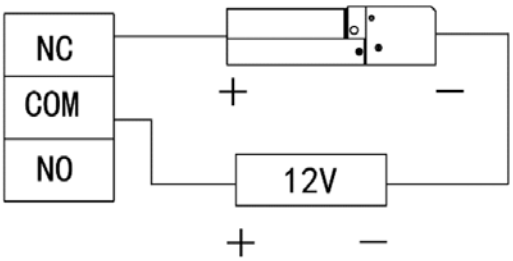


Figure 2-8 Electric bolt



2.1.7 Alarm Input

The alarm input port connects to external alarm devices, such as smoke detector and IR detector. Some alarm in ports can link door open/close status.

Table 2-2 Wiring alarm input

Type	Number of Alarm Input Channels	Description
Two-door One-way	2	Linkable door status: ● AUX1 external alarm links Normally Open for all doors. ● AUX2 external alarm links Normally Closed for all doors.
Two-door Two-way	6	Linkable door status: ● AUX1–AUX2 external alarm links Normally Open for all doors. ● AUX3–A UX4 external alarm links Normally Closed for all doors.
Four-door One way	2	Linkable door status: ● AUX1 external alarm links Normally Open for all doors. ● AUX2 external alarm links Normally Closed for all doors.
Four-door Two-way	8	Linkable door status: ● AUX1–AUX2 external alarm links Normally Open for all doors. ● AUX3–A UX4 external alarm links Normally Closed for all doors.
Eight-door One-way	8	Linkable door status: ● AUX1–AUX2 external alarm links Normally Open for all doors. ● AUX3–A UX4 external alarm links Normally Closed for all doors.

2.1.8 Alarm Output

When an alarm is triggered from the internal or external alarm input port, the alarm output device will report the alarm, and the alarm will last for 15 s.

When wiring the two-way dual-door device to the internal alarm output device, select NC/NO according to the Always Open or Always Close status.

- NC: Normally Closed.
- NO: Normally Open.

Table 2-3 Wiring alarm output

Type	Number of Alarm Output Channels	Description	
Two-door One-way	2	NO1	● AUX1triggers alarm output. ● Door timeout and intrusion alarm output for door 1. ● Card Reader 1 tamper alarm output.
		COM1	
		NO2	● AUX2 triggers alarm output. ● Door timeout and intrusion alarm output for door 2. ● Card Reader 2 tamper alarm output.
		COM2	
Two-door Two-way	2	NO1	AUX1/AUX2 triggers alarm output.
		COM1	
		NO2	AUX3/AUX4 triggers alarm output.
		COM2	
	2	NC1	● Card Reader 1/2 tamper alarm output. ● Door 1 timeout and intrusion alarm output.
		COM1	
		NO1	
		NC2	● Card Reader 3/4 tamper alarm output. ● Door 2 timeout and intrusion alarm output.
		COM2	
		NO2	
Four-door One way	2	NO1	● AUX1 triggers alarm output. ● Door timeout and intrusion alarm output. ● Card Reader tamper alarm output.
		COM1	
		NO2	AUX2 triggers alarm output.
		COM2	
Four-door Two-way	8	NO1	● AUX1 triggers alarm output. ● Card Reader 1/2 tamper alarm output. ● Door 1 timeout and intrusion alarm output. ● Device tamper alarm output.
		COM1	
		NO2	● AUX2 triggers alarm output. ● Card Reader 1/2 tamper alarm output. ● Door 2 timeout and intrusion alarm output.
		COM2	
		NO3	● AUX3 triggers alarm output. ● Card Reader 5/6 tamper alarm output. ● Door 3 timeout and intrusion alarm output.
		COM3	
		NO4	● AUX4 triggers alarm output. ● Card Reader 7/8 tamper alarm output. ● Door 4 timeout and intrusion alarm output.
		COM4	
		NO5	AUX5 triggers alarm output.
		COM5	
		NO6	AUX6 triggers alarm output.
		COM6	
		NO7	AUX7 triggers alarm output.
		COM7	
		NO8	AUX8 triggers alarm output.
		COM8	

Type	Number of Alarm Output Channels	Description	
Eight-door One-way	8	NO1	• AUX1 triggers alarm output. • Card Reader 1 tamper alarm output. • Door 1 timeout and intrusion alarm output. • Device tamper alarm output.
		COM1	
		NO2	• AUX2 triggers alarm output. • Card Reader 2 tamper alarm output. • Door 2 timeout and intrusion alarm output.
		COM2	
		NO3	• AUX3 triggers alarm output. • Card Reader 3 tamper alarm output. • Door 3 timeout and intrusion alarm output.
		COM3	
		NO4	• AUX4 triggers alarm output. • Card Reader 4 tamper alarm output. • Door 4 timeout and intrusion alarm output.
		COM4	
		NO5	• AUX5 triggers alarm output. • Card Reader 5 tamper alarm output. • Door 5 timeout and intrusion alarm output.
		COM5	
		NO6	• AUX6 triggers alarm output. • Card Reader 6 tamper alarm output. • Door 6 timeout and intrusion alarm output.
		COM6	
		NO7	• AUX7 triggers alarm output. • Card Reader 7 tamper alarm output. • Door 7 timeout and intrusion alarm output.
		COM7	
		NO8	• AUX8 triggers alarm output. • Card Reader 8 tamper alarm output. • Door 8 timeout and intrusion alarm output.
		COM8	

2.1.9 Card Reader

One door can only connect card readers of the same type, either RS-485 or Wiegand.

Table 2-4 Card reader wire specification description

Card Reader Type	Wiring Method	Length
RS-485 card reader	RS-485 connection. The impedance of a single wire must be within 10Ω.	100 m
Wiegand card reader	Wiegand connection. The impedance of a single wire must be within 2Ω.	80 m

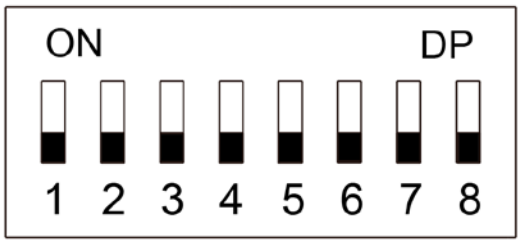
2.2 Power Indicator

- Solid green: Normal.
- Red: Abnormal.
- Flashes green: Charging.
- Blue: The Controller is in the Boot mode.

2.3 DIP Switch

 (ON) indicates 1;  indicates 0.

Figure 2-9 DIP switch



- When 1–8 are all switched to 0, the Controller starts normally after power-on.
- When 1–8 are all switched to 1, the Controller enters the BOOT mode after it starts.
- When 1, 3, 5 and 7 are switched to 1 and the others are 0, the Controller restores to factory defaults after it restarts.
- When 2, 4, 6 and 8 are switched to 1 and the others are 0, the Controller restores to factory defaults but keeps user information after it restarts.

2.4 Power Supply

2.4.1 Door Lock Power Port

The rated voltage of the door lock power port is 12 V, and the maximum current output is 2.5 A. If the power load exceeds the maximum rated current, provide extra power supply.

2.4.2 Card Reader Power Port

- Two-door one-way, two-door two-way, four-door one-way controllers: The rated voltage of the card reader power port (12V_RD) is 12 V, and the maximum current output is 1.4 A.
- Four-door two-way and eight-door one-way controllers: The rated voltage of the card reader power port (12V_RD) is 12 V, and the maximum current output is 2.5 A.

3 SmartPSS AC Configuration

You can manage the Controller through SmartPSS AC. This section mainly introduces quick configurations of the Controller. For details, refer to SmartPSS AC user manual.

The screenshots of Smart PSS AC client in this manual are only for reference, and might differ from the actual product.

3.1 Login

Step 1 Install the SmartPSS AC.

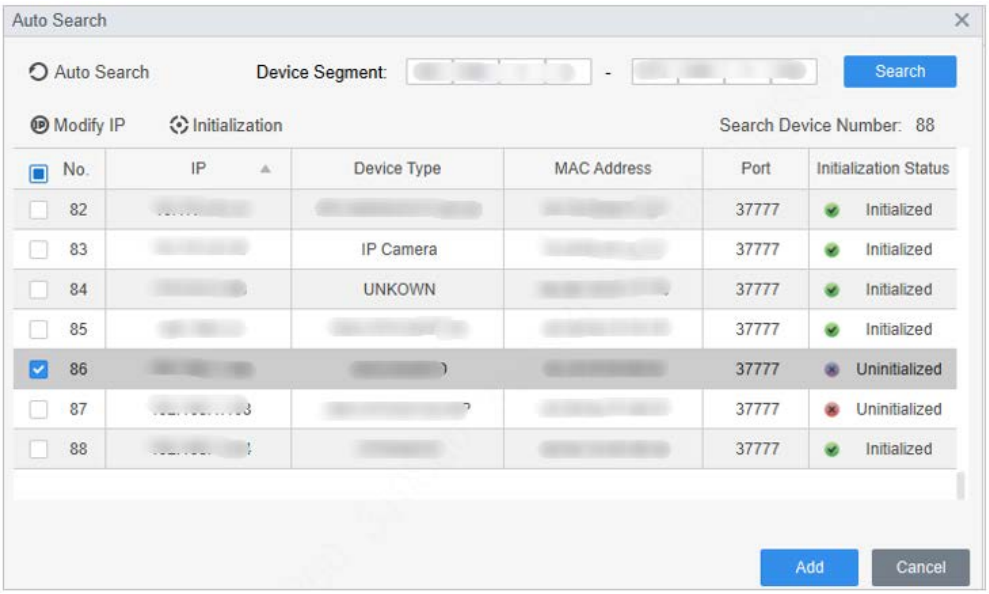
Step 2 Double-click , and then follow the instructions to finish the initialization and log in.

3.2 Initialization

Before initialization, make sure the Controller and the computer are on the same network.

Step 1 On the home page, select **Device Manager**, and then click **Auto Search**.

Figure 3-1 Auto search



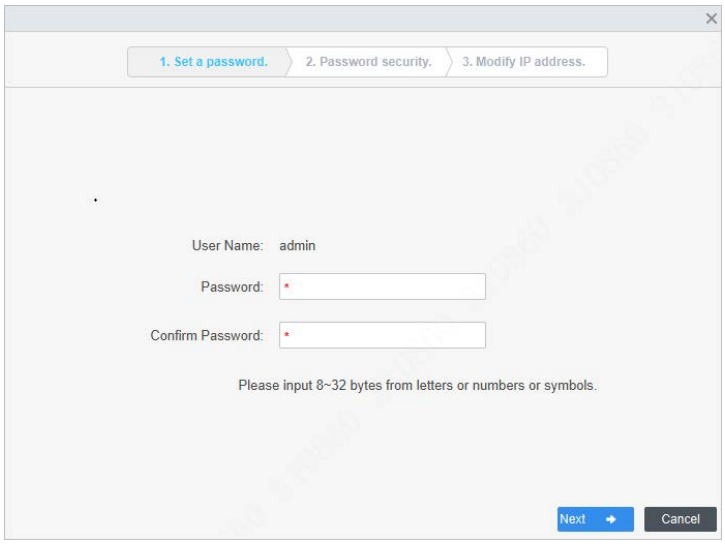
Step 2 Enter a network segment range, and then click **Search**.

Step 3 Select the device, and then click **Initialization**.

Step 4 Set the admin password, and then click **Next**.

If you forget the password, use the DIP switch to restore factory defaults.

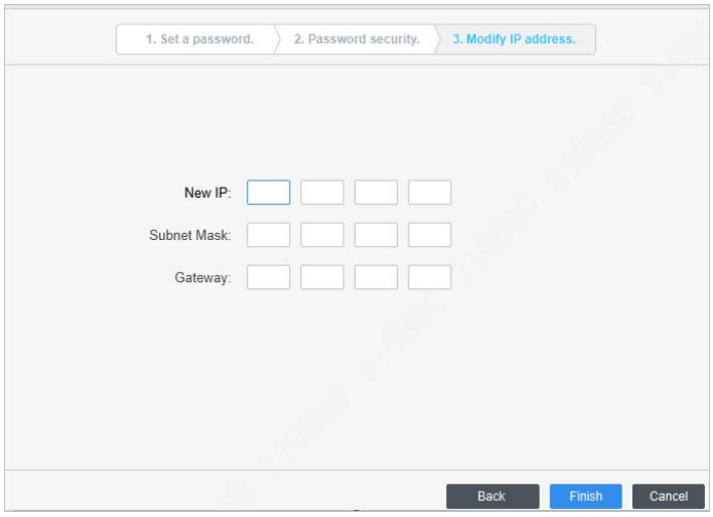
Figure 3-2 Set password



Step 5 Associate the phone number, and then click **Next**.

Step 6 Enter new IP, subnet mask and gateway.

Figure 3-3 Modify IP Address



Step 7 Click **Finish**.

3.3 Adding Devices

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

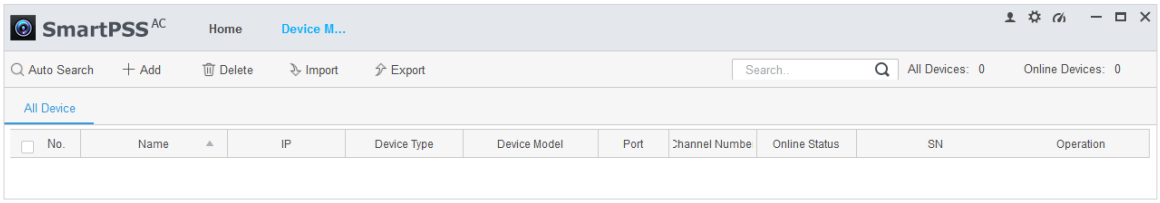
3.3.1 Auto Search

We recommend adding 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.

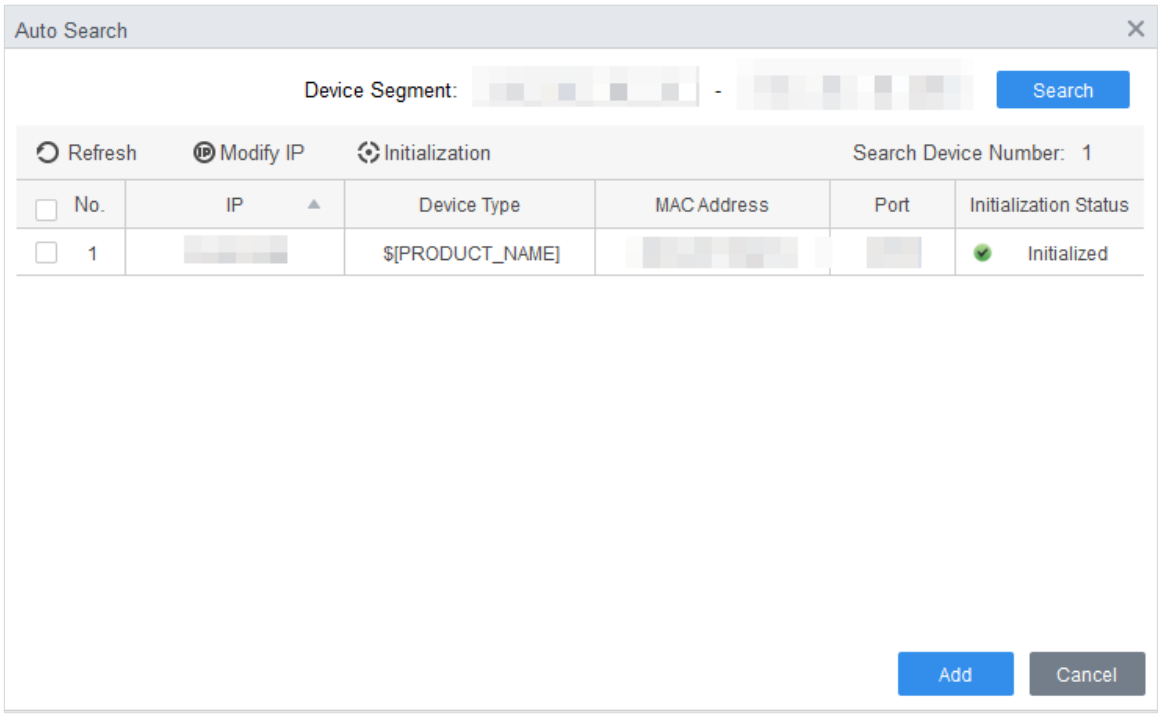
Step 2 Click **Device Manager** on the lower-left corner.

Figure 3-4 Devices



Step 3 Click **Auto Search**.

Figure 3-5 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**.

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

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

- The username is admin and password is admin123 by default. We recommend changing the password after login.
- After adding, SmartPSS AC logs in to the device automatically. After successful login, the status displays **Online**. Otherwise, it displays **Offline**.

3.3.2 Manual Add

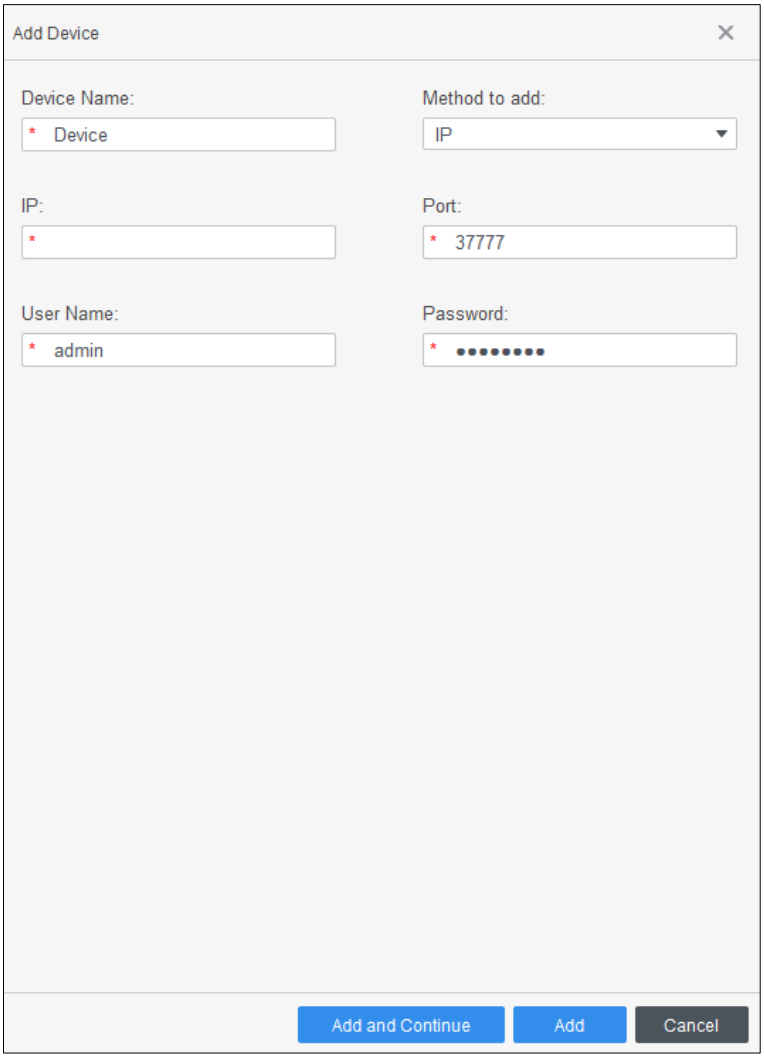
You can add devices manually. You need to know IP addresses and domain names of access controllers that you want to add.

Step 1 Log in to SmartPSS AC.

Step 2 Click **Device Manager** on the lower-left corner.

Step 3 Click **Add** on the **Device Manager** page.

Figure 3-6 Manual add



Step 4 Enter detailed information of the Controller.

Table 3-1 Parameters

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

Step 5 Click **Add**.

The added device is on the **Devices** page.

After adding, SmartPSS AC logs in to the device automatically. After successful login, the status displays **Online**. Otherwise, it displays **Offline**.

3.4 User Management

Add users, assign cards to them, and configure their access permissions.

3.4.1 Setting Card Type

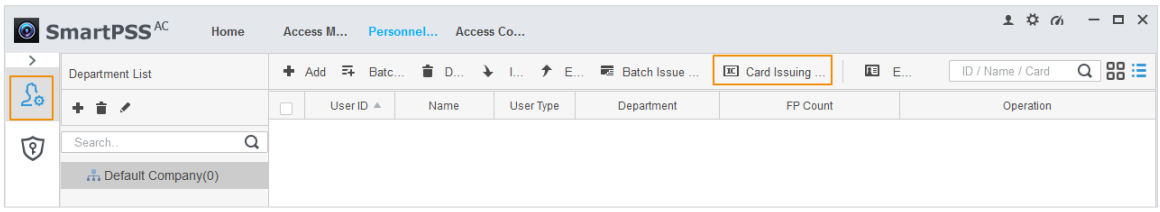
Before assigning card, set card type first. For example, if the assigned card is ID card, select type as ID card.

The selected card type must be the same as the actual assigned card type; otherwise card numbers cannot be read.

Step 1 Log in to SmartPSS AC.

Step 2 Click **Personnel Manager**.

Figure 3-7 Personnel manager

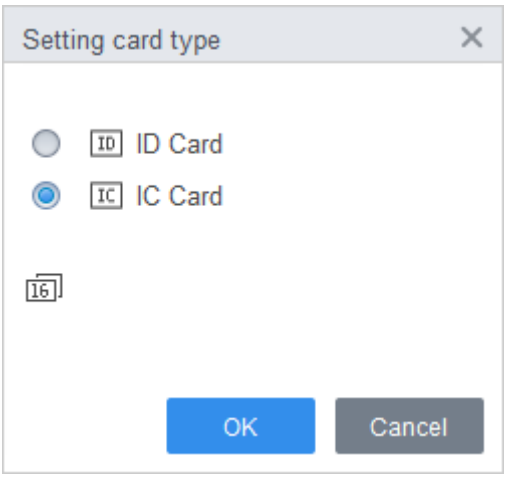


Step 3 On the **Personnel Manager** page, click , then click .

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

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

Figure 3-8 Setting card type



Step 6 Click **OK**.

3.4.2 Adding User

3.4.2.1 Adding Individually

You can add users individually.

Step 1 Log in to SmartPSS AC.

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

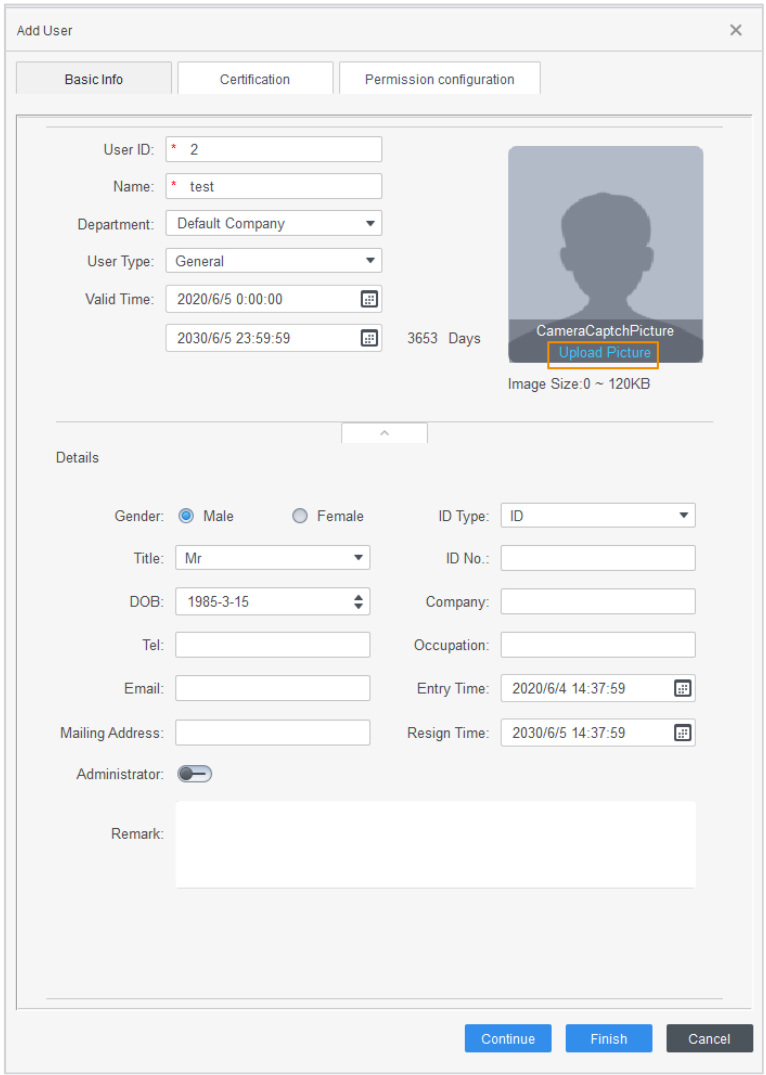
Step 3 Add basic information of the user.

1) Click the **Basic Info** tab on the **Add User** page, 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 3-9 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.

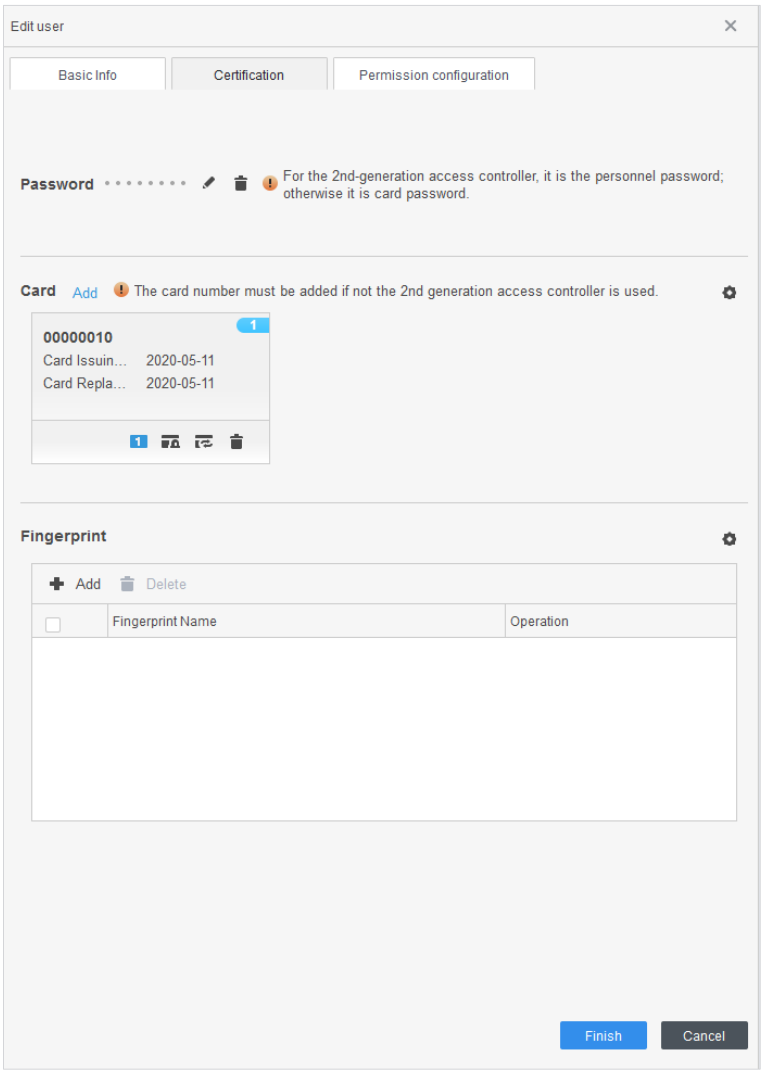
The card number can be read automatically or entered manually. To read the card number automatically, select a card reader, and then place the card on the card reader.

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

- Configure fingerprint.

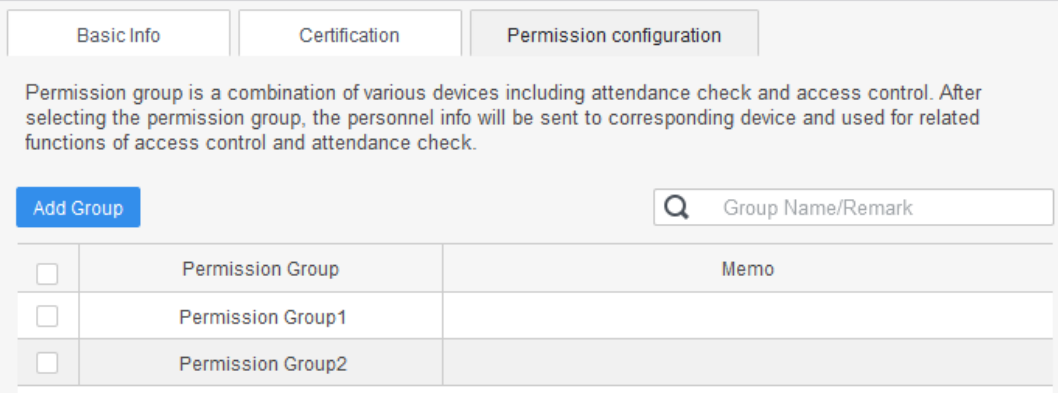
1) Click to set **Device** or **Fingerprint Scanner** to fingerprint collector.
2) Click **Add Fingerprint** and press your finger on the scanner three times continuously.

Figure 3-10 Configure certification



Step 5 Configure permissions for the user.
For details, see "3.5 Configuring Permission".

Figure 3-11 Permission configuration



Step 6 Click **Finish**.

3.4.2.2 Adding in Batches

You can add users in batches.

Step 1 Log in to SmartPSS AC.

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

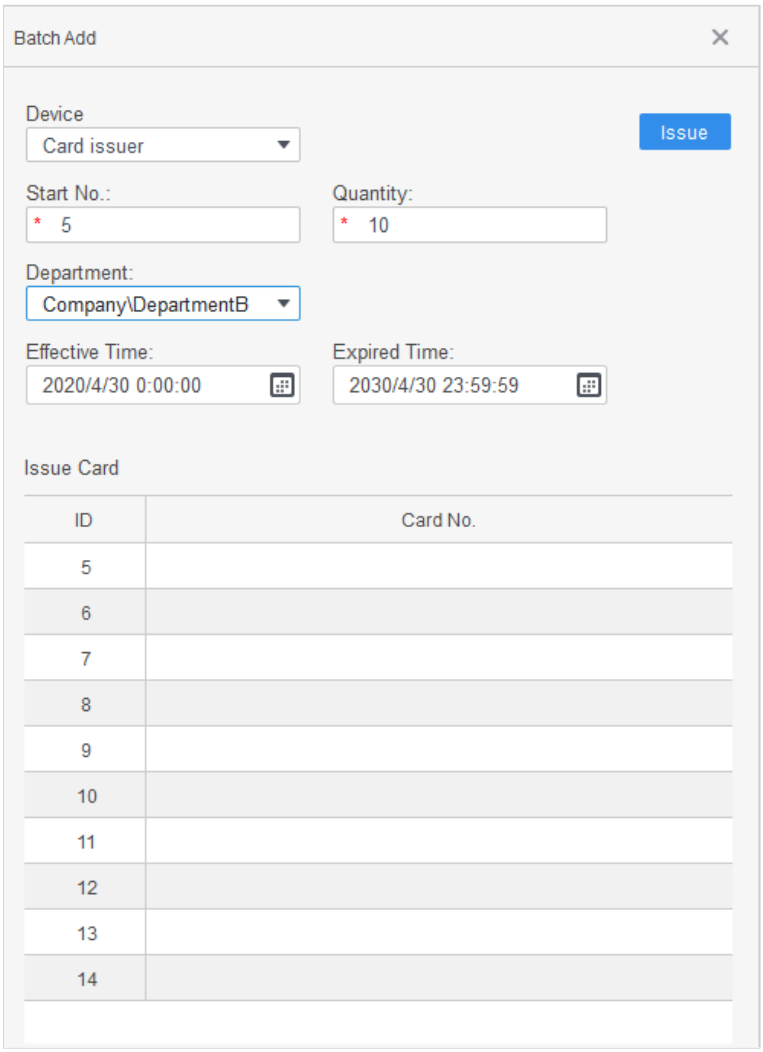
Step 3 Select card reader and the department of user. Set the start number, card quantity, effective time and expired time of card.

Step 4 Click **Issue** to assigning cards.

The card number will be read automatically.

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

Figure 3-12 Add users in batches



3.5 Configuring Permission

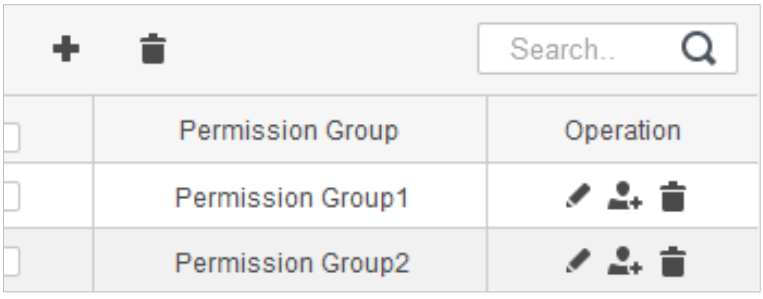
3.5.1 Adding Permission Group

Create a permission group that is a collection of door access permissions.

Step 1 Log in to SmartPSS AC.

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

Figure 3-13 Permission group list



Step 3 Click ✚ to add a permission group.

Step 4 Set permission parameters.

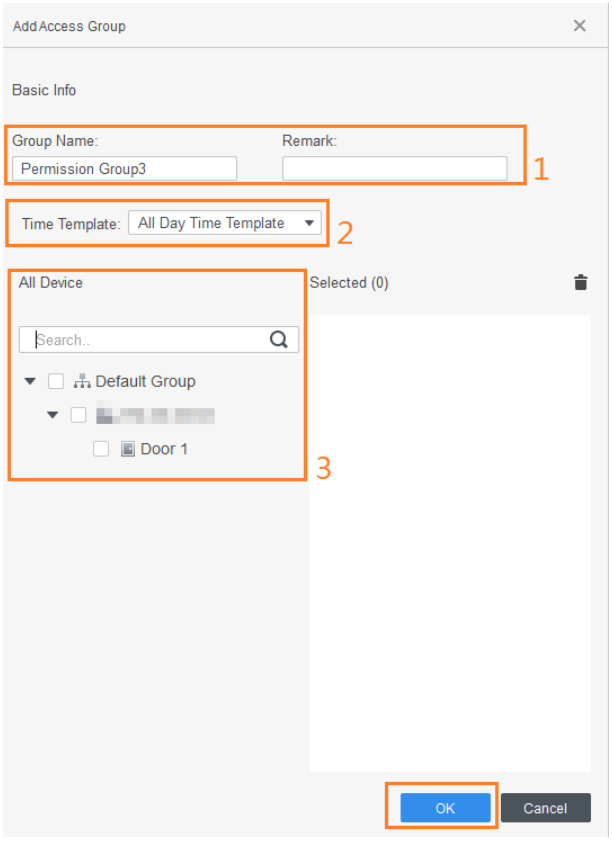
1) Enter group name and remark.

2) Select the time template.

For details of time template setting, see SmartPSS AC user's manual.

3) Select the corresponding device, such as door 1.

Figure 3-14 Add permission group



Step 5 Click **OK**.

Related Operation

On the **Permission Group List** page, you can:

- Click 🗑 to delete group.
- Click ✎ to modify group information.
- Double-click permission group name to view group information.

3.5.2 Assigning Access Permission

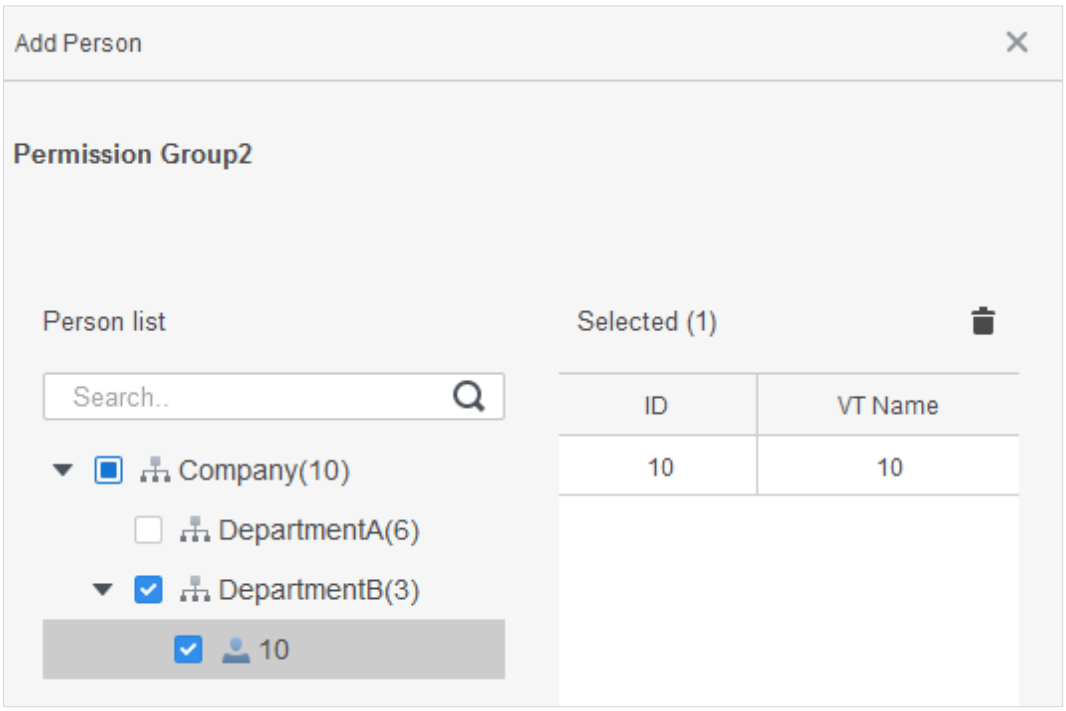
Associate users with desired permission groups, and then the users will be assigned access permissions to defined doors.

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 3-15 Configure permission



Step 4 Select users to associate them with the selected group.

Step 5 Click **OK**.

3.6 Access Controller Configuration

3.6.1 Configuring Advanced Functions

3.6.1.1 First Card Unlock

Other users can swipe to unlock the door only after the specified first card holder swipes the card. You can set multiple first-cards. Other users without first-cards can unlock the door only after one of the first-card holders swipe the first card.

- The person to be granted with the first card unlock permission should be of the **General** user type and have permissions of the certain doors. Set the type when adding users. For details, see "3.3.2 Adding User".
- For details of assigning permissions, see "3.5 Configuring Permission".

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 then click **Save**.

Figure 3-16 First card unlock configuration

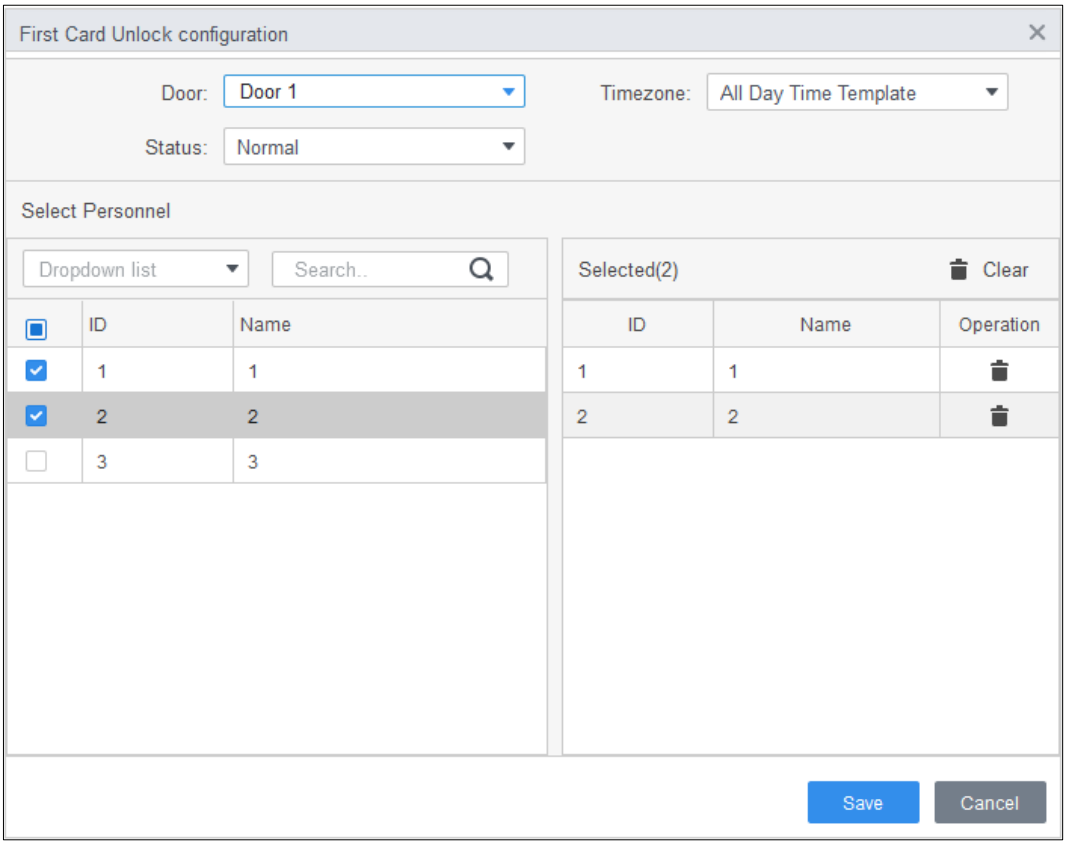


Table 3-2 Parameters of first-card unlock

Parameter	Description
Door	Select the target access control channel to configure the first card unlock.
Timezone	**First Card Unlock** is valid in the 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.

3.6.1.2 Multi-card Unlock

Users can only unlock the door after defined users or user groups grant access in sequence.

- One group can have up to 50 users, and one person can belong to multiple groups.
- You can add up to four user groups with multi-card unlock permission for a door, with up to 200 users in total and up to 5 valid users.

- First card unlock takes priority over the multi-card unlock, which means if the two rules are both enabled, the first card unlock comes first. We recommend you not assign multi-card unlock permission to first card holders.
- 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 Configuring Permission".

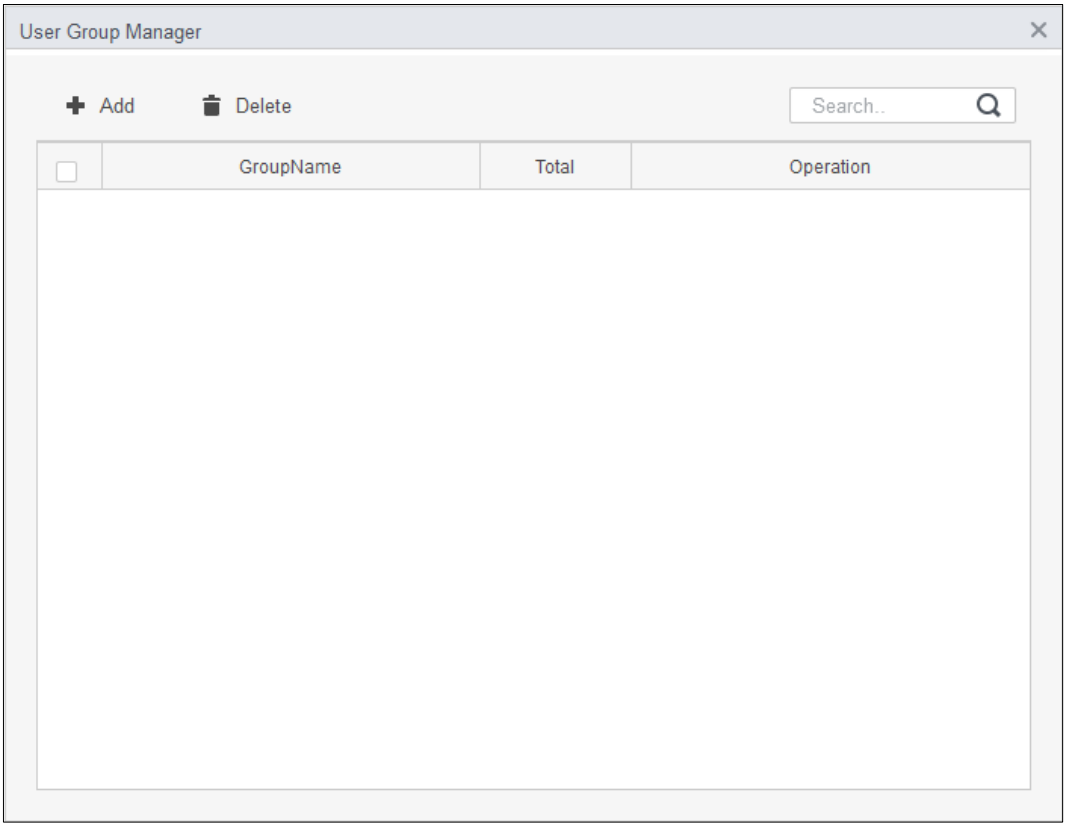
Step 1 Select **Access Configuration** > **Advanced Config**.

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

Step 3 Add user group.

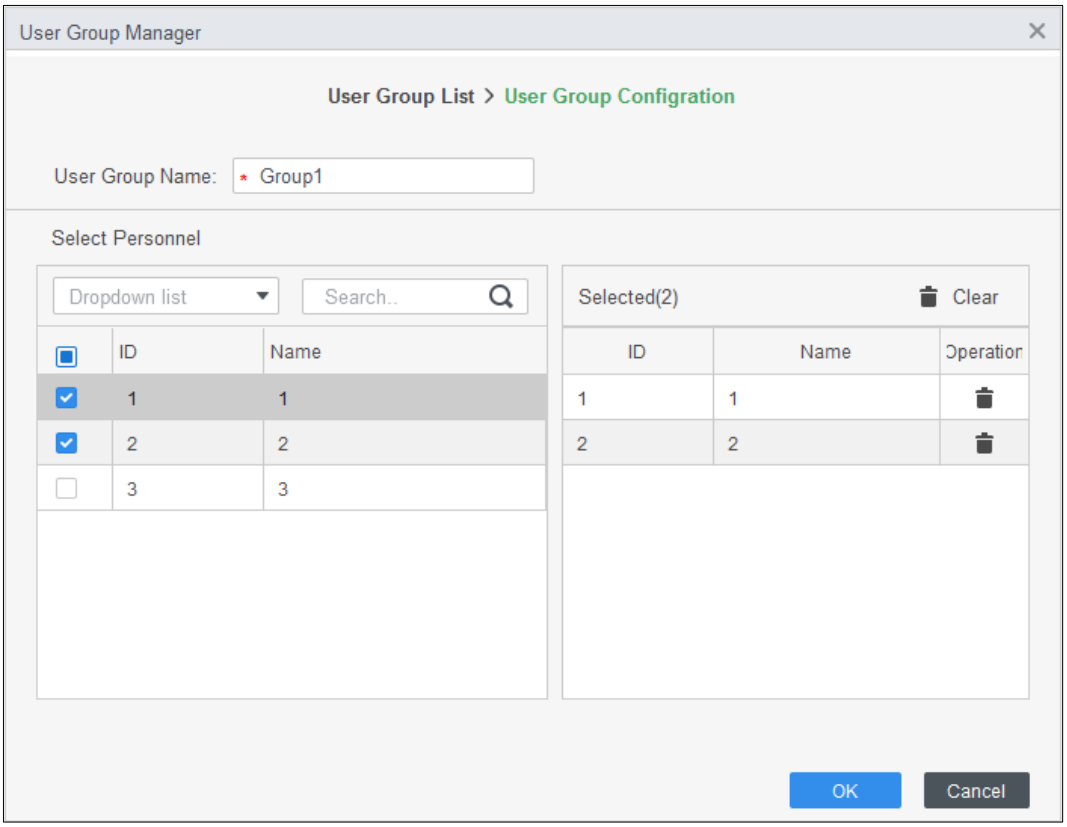
1) Click **User Group**.

Figure 3-17 User group manager



2) Click **Add**.

Figure 3-18 User group configuration



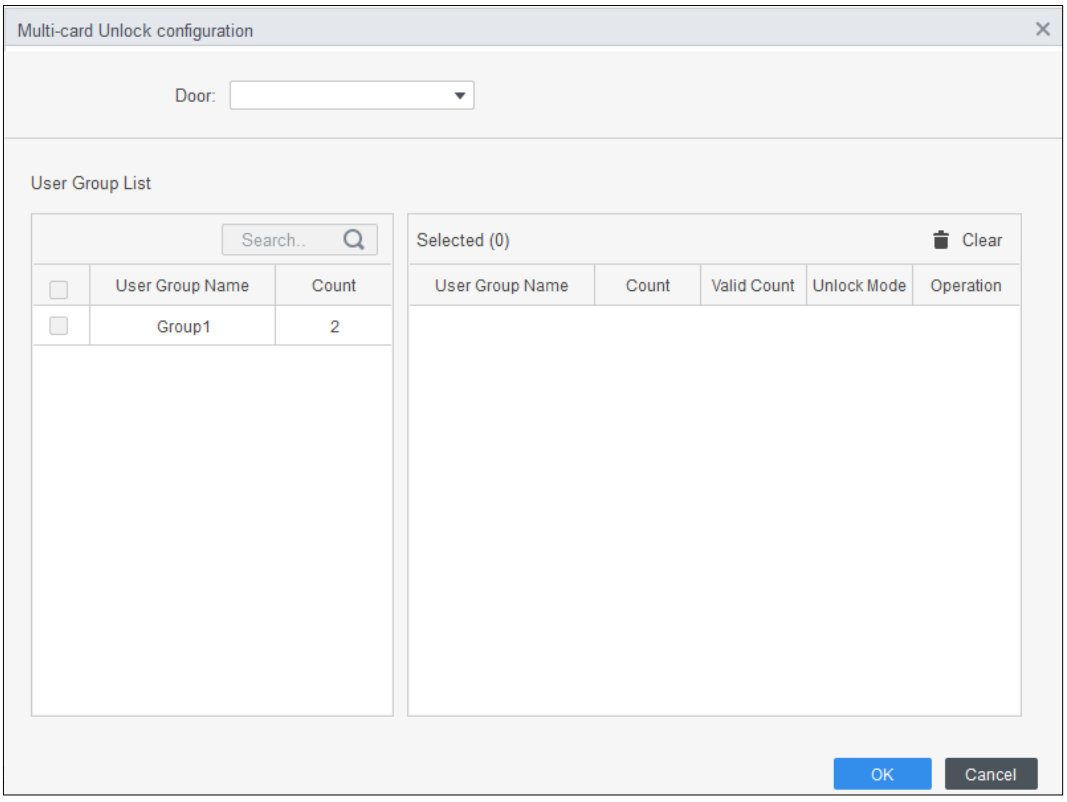
3) Set up **User Group Name**. Select users from **User List** and click **OK**. You can select up to 50 users.

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

Step 4 Configure parameters of multi-card unlock.

1) Click **Add**.

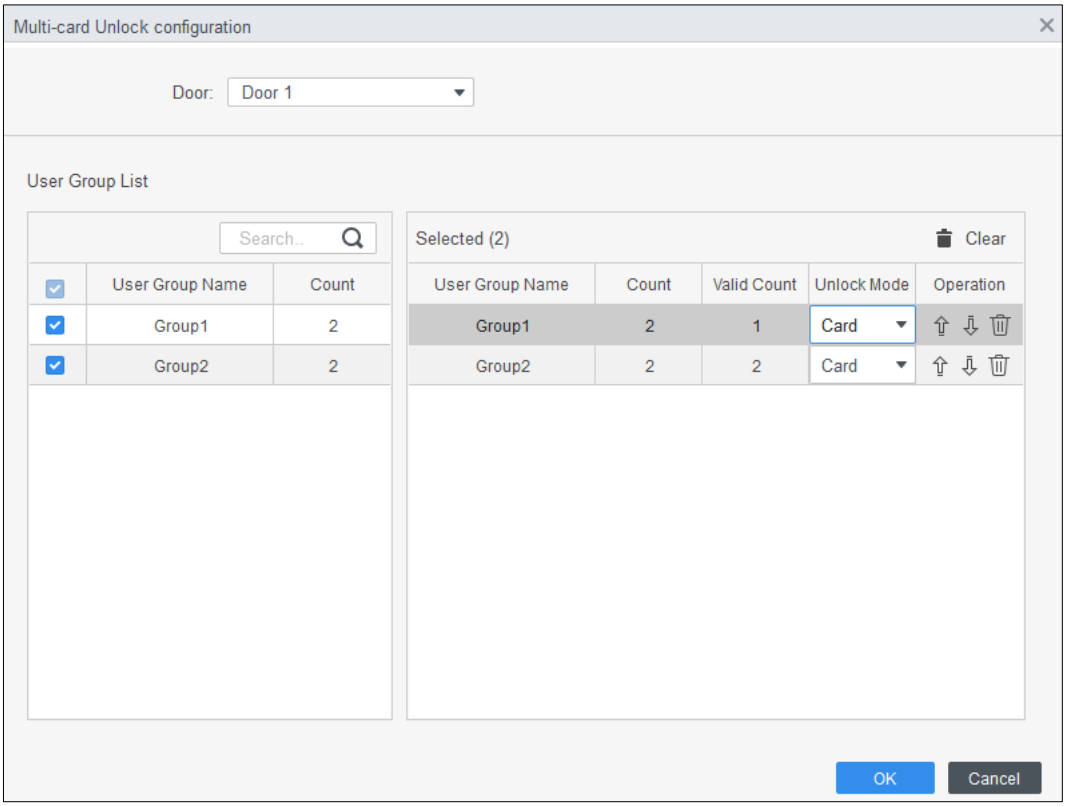
Figure 3-19 Multi-card unlock configuration (1)



2) Select the door.

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

Figure 3-20 Multi-card unlock configuration (2)



4) Enter the **Valid Count** for each group to be on site, and then select 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 after one person of group 1 and 2 people of group 2 have swiped their cards.
- 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.

3.6.1.3 Anti-passback

Users must verify their identities both for entry and exit; otherwise an alarm will be triggered. If a person enters with valid identity verification and exits without verification, an alarm will be triggered when they attempt to enter again, and access is denied at the same time. If a person enters without identity verification and exits with verification, exit is denied when the they attempt to exit.

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

Step 2 Click **Add**.

Step 3 Configure parameters.

1) Select device and enter device name.

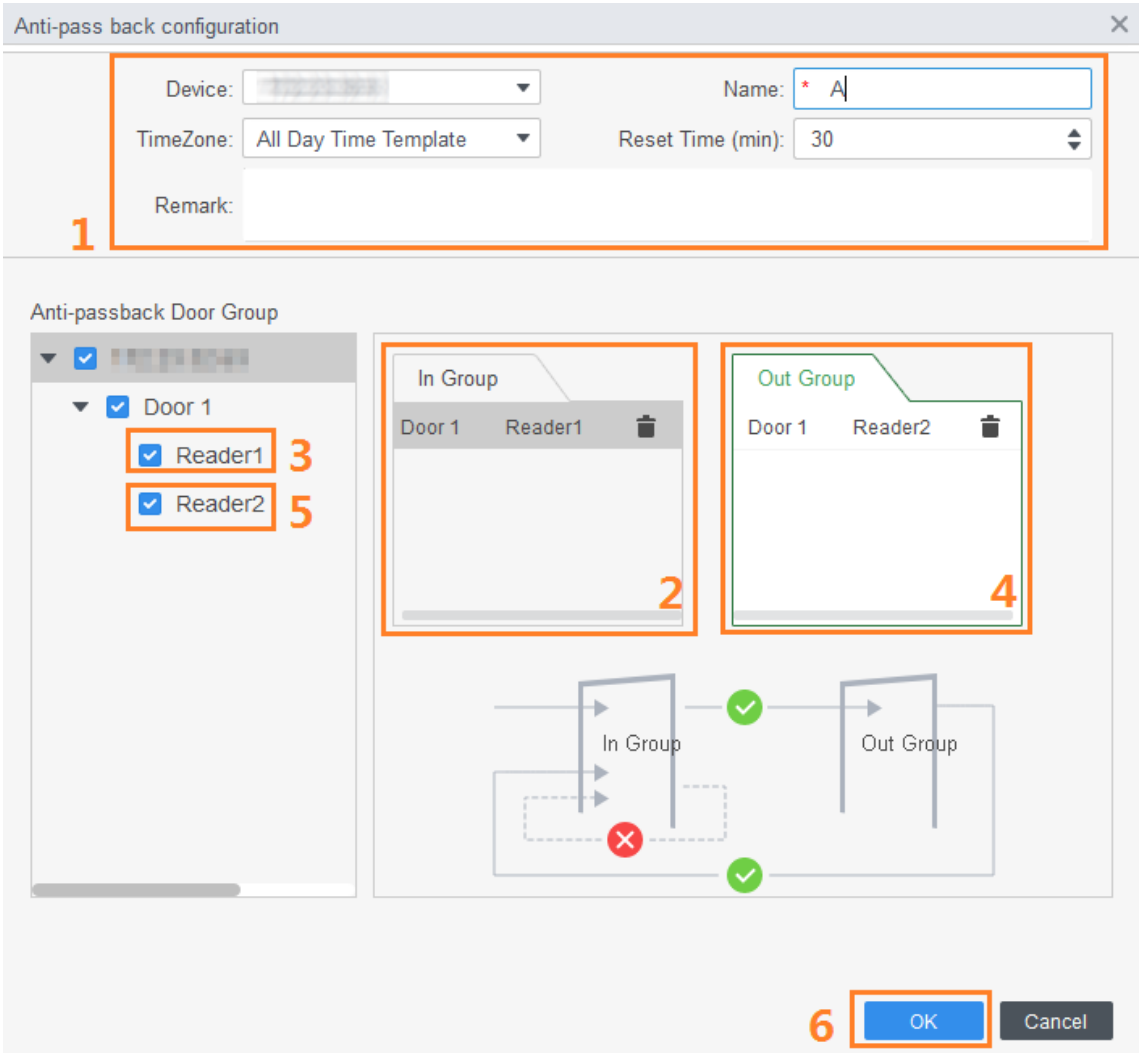
2) Select time template.

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**.
The configuration will issue to device and take effect.

Figure 3-21 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.

3.6.1.4 Inter-door Lock

The access through one or more doors depends on the status of another door (or doors). For example, when two doors are interlocked, you can access through one door only when the other door is closed. One device supports two groups of doors with up to 4 doors in each group.

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

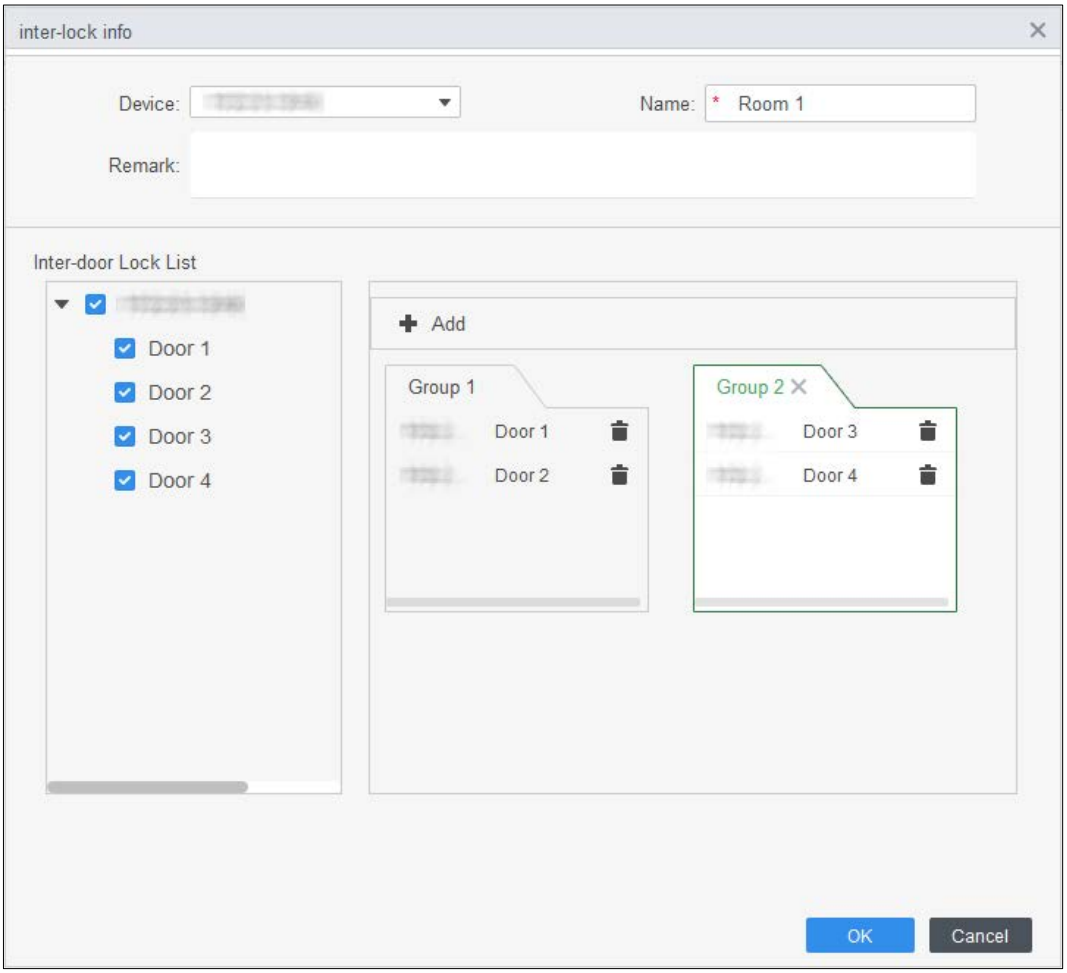
Step 2 Click the **Inter-Lock** tab.

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 3-22 Inter-door lock configuration



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

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

3.6.2 Configuring Access Controller

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 that needs to be configured.

Step 3 Configure parameters.

Figure 3-23 Configure access door

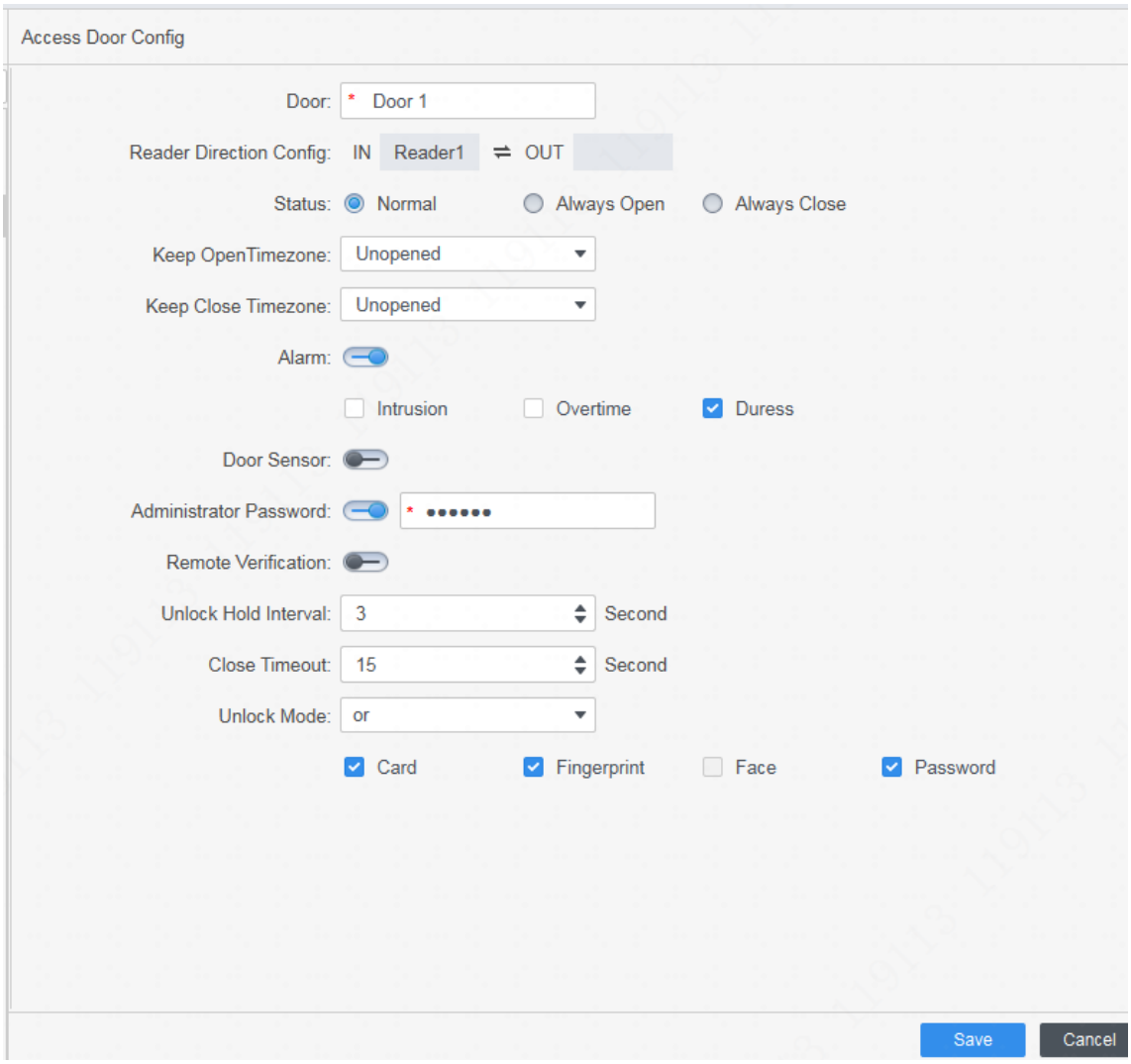


Figure 3-24 Unlock by time period

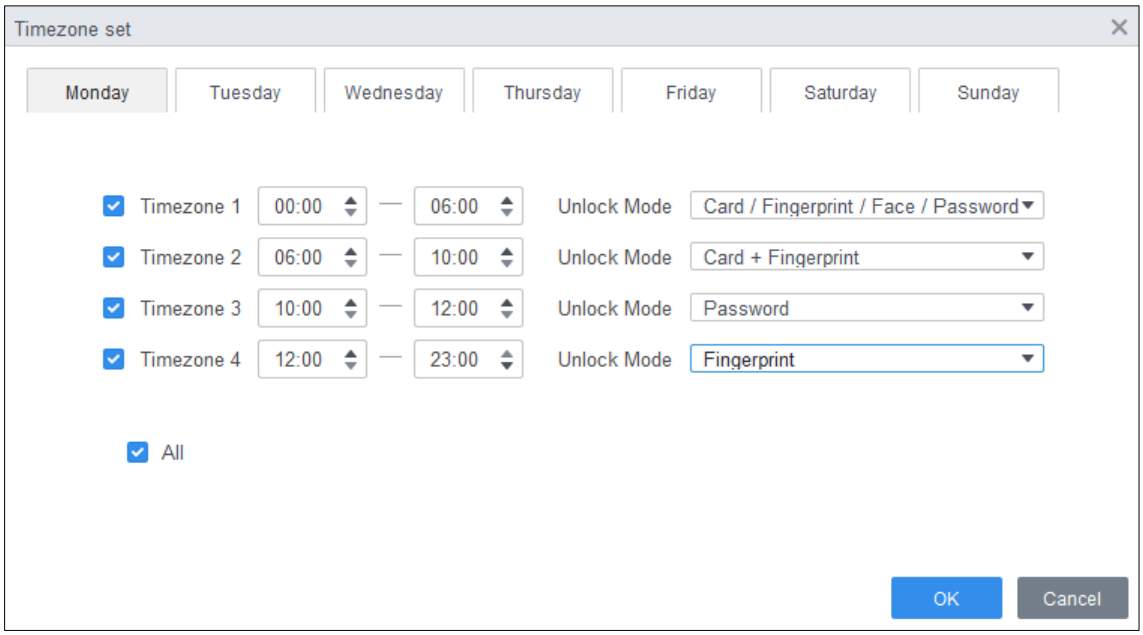


Table 3-3 Parameters of access door

Parameter	Description
Door	Enter door name.
Reader Direction Config	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 open.
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. We recommend enabling 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 person has to be verified remotely through the SmartPSS-AC during the template periods.
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 can open the door by combining the selected unlock methods. ● Select **Or** and select unlock methods. You can open the door in one of the way that you configured. ● Select **Unlock by time period** and select unlock mode for each time period. The door can only be opened by the selected method(s) within the defined period.

Step 4 Click **Save**.

3.6.3 Viewing Historical Event

History door events include events both on SmartPSS-AC and devices. Extract history events from devices to make sure all event logs are available to be searched for.

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

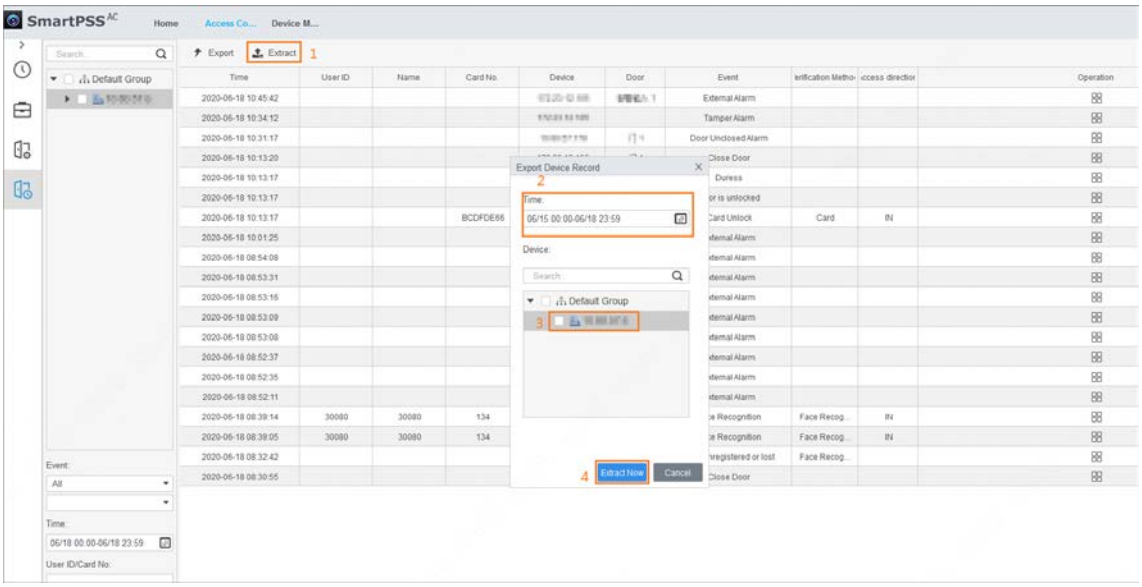
Step 2 Click **Access Configuration** > **History Event** on the homepage.

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

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

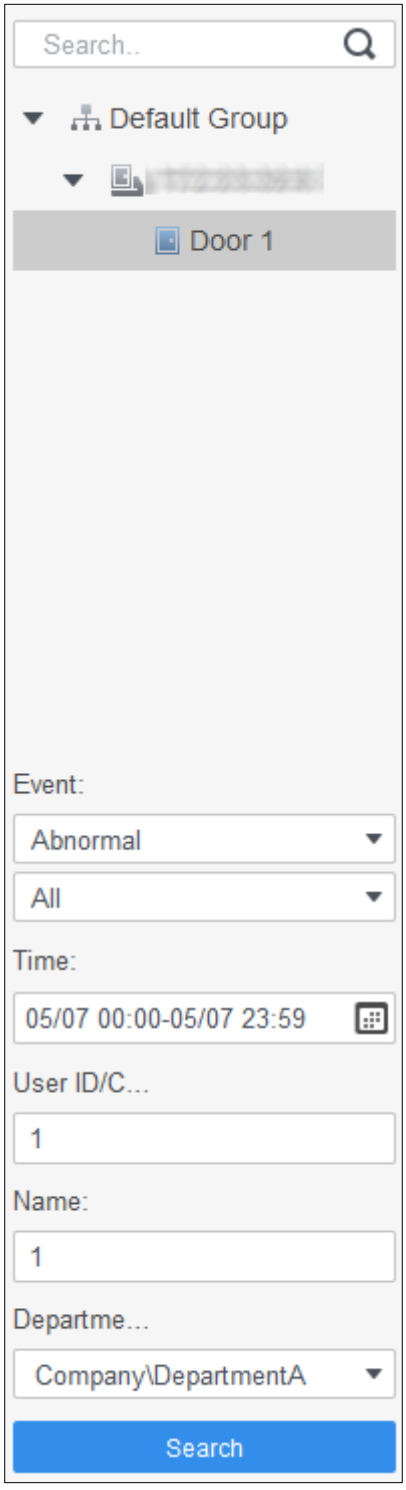
You can select multiple devices at one time to extract events.

Figure 3-25 Extract events



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

Figure 3-26 Search for events by filtering conditions



3.7 Access Management

3.7.1 Remotely Opening and Closing Door

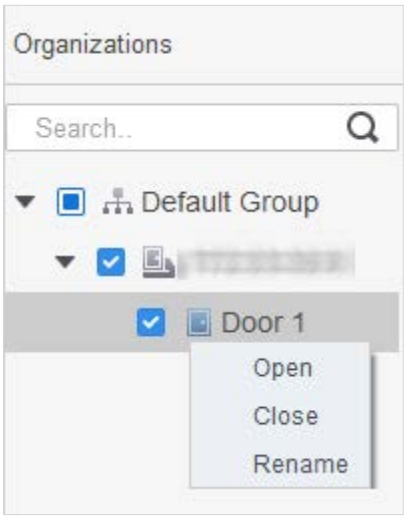
You can remotely control door through SmartPSS AC.

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 3-27 Remotely control (method 1)



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

Figure 3-28 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 next to **Event Info** to lock or unlock the event list, and then the real-time events cannot be viewed.
- Event deleting: Click next to **Event Info** to clear all events in the event list.

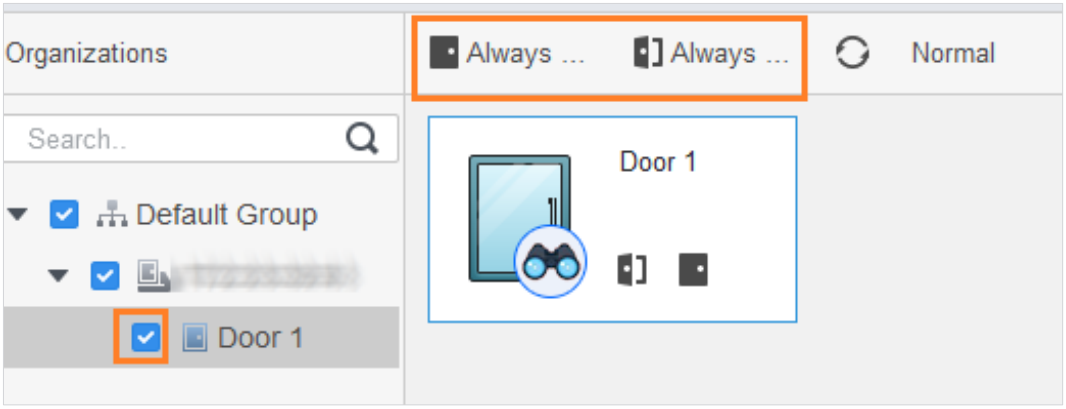
3.7.2 Setting Door Status

After setting always open status or always close status, the door remains open or closed all the time. You can click **Normal** to restore the door status to normal so that users can unlock the door after identity verification.

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

Step 2 Select the door, and then click **Always Open** or **Always Close**.

Figure 3-29 Set always open or always close



3.7.3 Configuring Alarm Linkage

After you configure alarm linkage, alarms will be triggered. For details, refer to the user manual of SmartPss AC. This section uses intrusion alarm as an example.

- 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 Configuring Advanced Functions".

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

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

Step 3 Click next to **Intrusion Alarm** to enable the function.

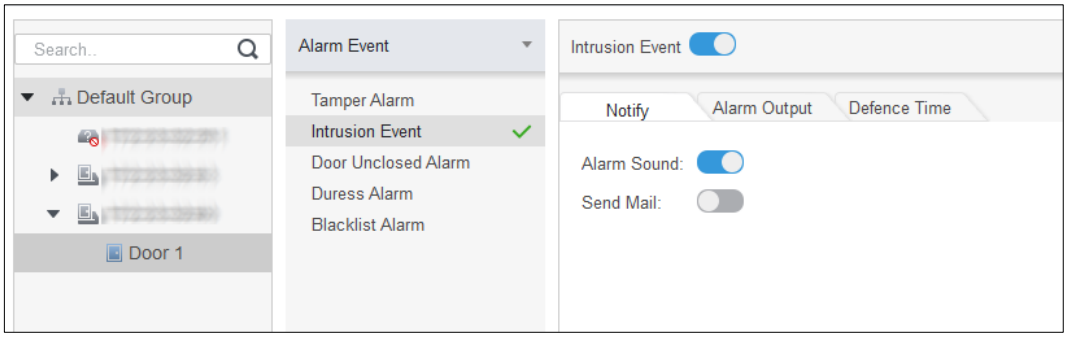
Step 4 Configure intrusion alarm linkage actions as needed.

- Enable alarm sound.

  Click the **Notify** tab, and click next to **Alarm Sound**. When intrusion event happens, the access controller warns with alarm sound.
- Send alarm mail.

1) Enable **Send Mail** and confirm to set SMTP. The **System Settings** page is displayed.
2) Configure SMTP parameters, such as server address, port number, and encrypt mode. When intrusion events occur, the system sends alarm notifications through mails to the specified receiver.

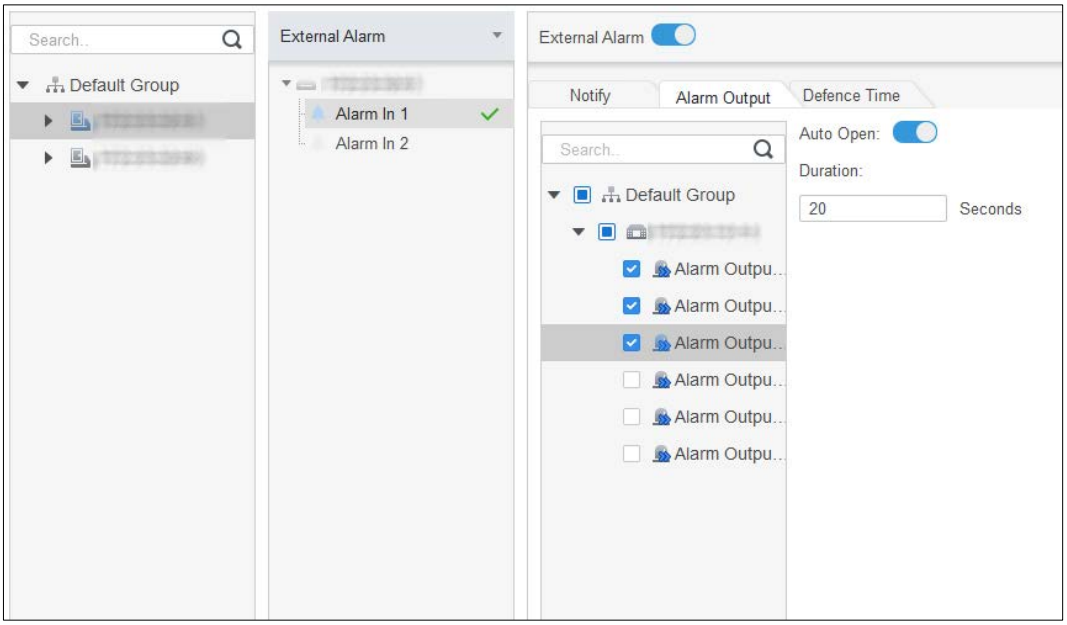
Figure 3-30 Configure intrusion alarm



- Configure alarm I/O.

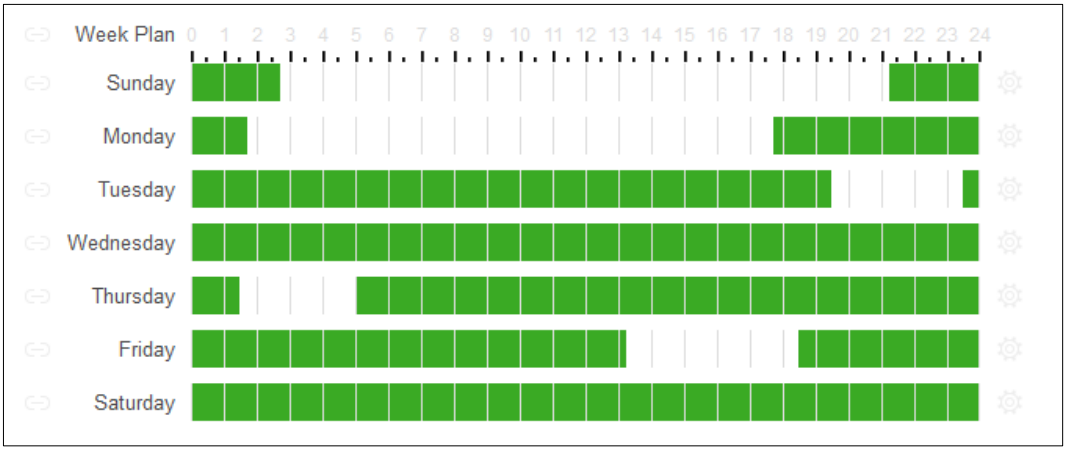
1) Click the **Alarm Output** tab.
2) Select the device which supports alarm in, select alarm-in interface, and then enable **External Alarm**.
3) Select the device which supports alarm out, then select alarm-out interface.
4) Enable **Auto Open** for the alarm linkage.
5) Set the duration.

Figure 3-31 Configure alarm linkage



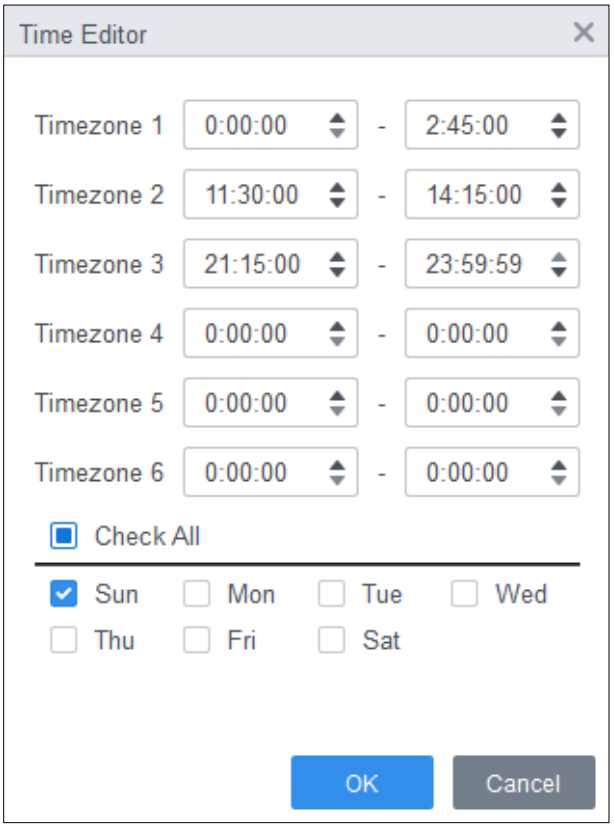
- Set arming time. There are two methods.
  - ◇ Method 1: Move the cursor to set periods. When the cursor is pencil, click to add periods; when the cursor is eraser, click to remove periods. The green area is the arming periods.

Figure 3-32 Set arming time (method 1)



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

Figure 3-33 Set arming time (method 2)



Step 5 (Optional) If you want to set the same arming periods for other access controller, click **Copy To**, select the access controller, 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 results when you searching for devices.

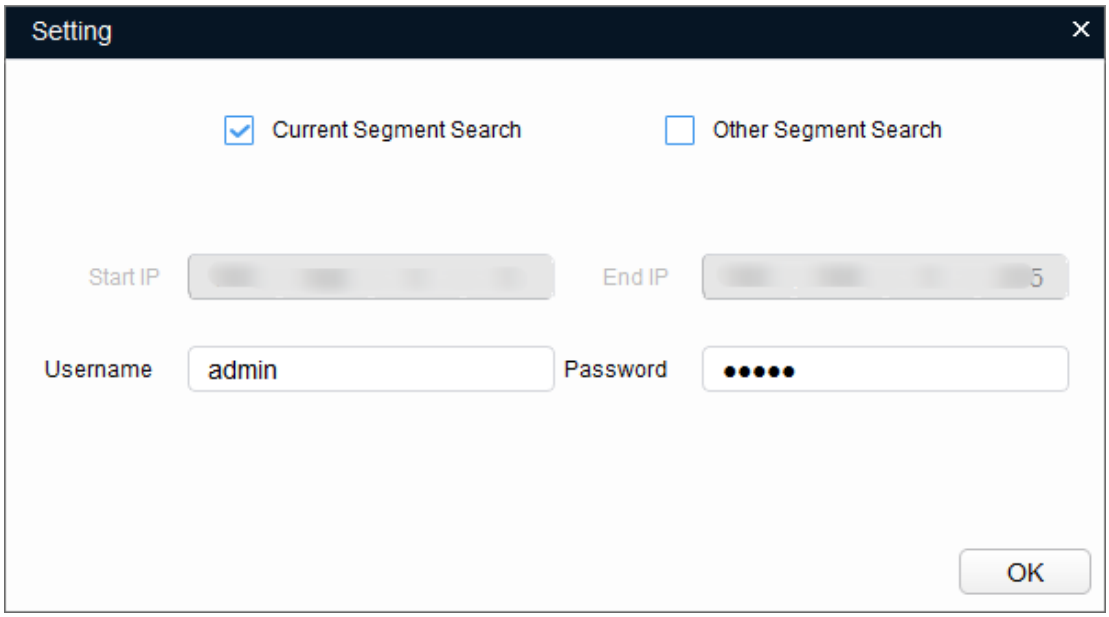
4.1 Initialization

Before initialization, make sure the Controller and the computer are on the same network.

Step 1 Search for the Controller through the ConfigTool.

1) Double-click ConfigTool to open it.
2) Click **Search setting**, enter the network segment range, and then click OK.
3) Select the uninitialized Controller, and then click Initialize.

Figure 4-1 Search for the device



Step 2 Select the uninitialized Controller, and then click **Initialize.**

Step 3 Click **OK**.

The system starts initialization. indicates initialization success, indicates initialization failed.

Step 4 Click **Finish**.

4.2 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.

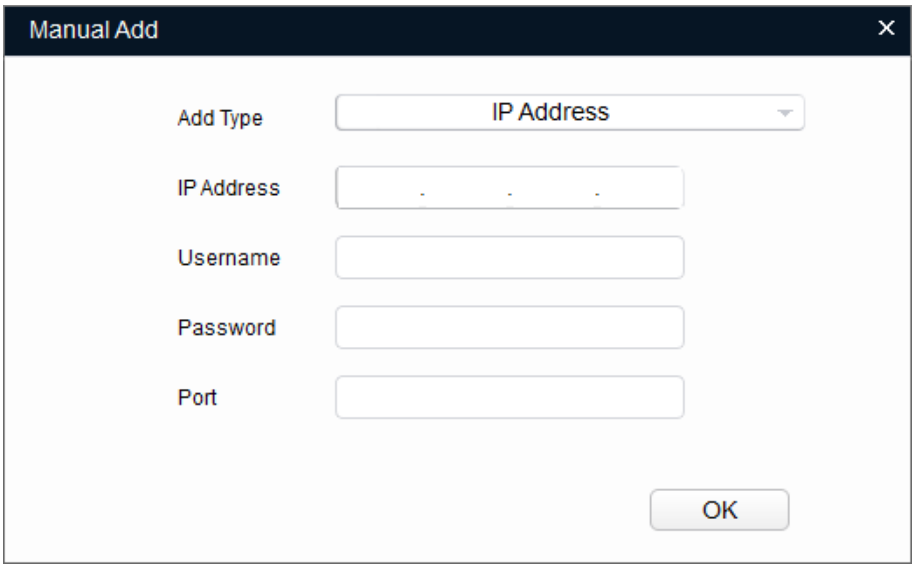
4.2.1 Adding Device Individually

Step 1 Click .

Step 2 Click **Manual Add**.

Step 3 Select **IP Address** from **Add Type**.

Figure 4-2 Manual add (IP address)



Step 4 Set the Controller 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 username and password for device login.
	Password	
	Port	The device port number.

Step 5 Click **OK**.

The newly added device is displayed in the device list.

4.2.2 Adding Devices in Batches

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

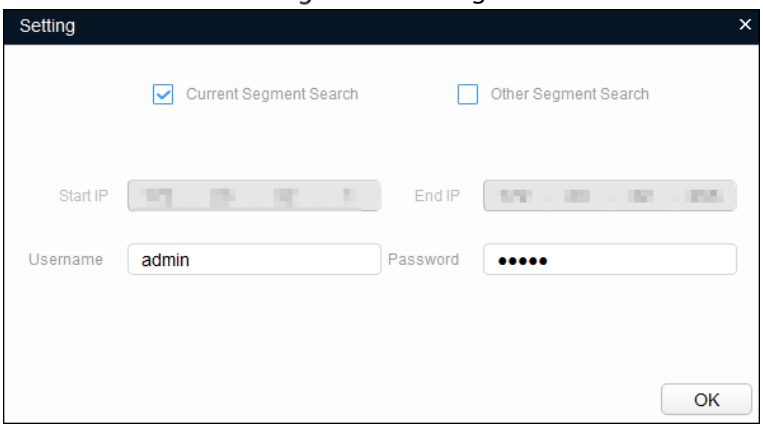
4.2.2.1 Adding by Searching

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

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.

- Search current segment
  Select **Current Segment Search**. Enter the username and password. The system will search for devices accordingly.
- Search other segment
  Select **Other Segment Search**. Enter the start IP address and end IP address. Enter the username and the password. The system will search for devices accordingly.

- If you select both **Current Segment Search** and **Other Segment Search**, the system searches for devices on the both segments.
- 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 be displayed in the device list.

- 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.

4.2.2.2 Adding by Importing Device Template

You can add the devices by importing an Excel template. You can import up to1000 devices.

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

Step 1 Click , select one device, and then click **Export** to export a device template.

Step 2 Follow the on-screen instructions to save the template file locally.

Step 3 Open the template file, change the existing device information to the information of devices you want to add.

Step 4 Import the template. Click **Import**, select the template and click **Open**.
The system starts importing the devices.

Step 5 Click **OK**.
The newly imported devices display in the device list.

4.3 Configuring Access Controller

The screenshots and parameters might be different depending on the device types and models.

Step 1 Click on the main menu.

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 page shows, enter the username and password, and then click **OK**.

Step 4 Set access controller parameters.

Figure 4-4 Configure access controller

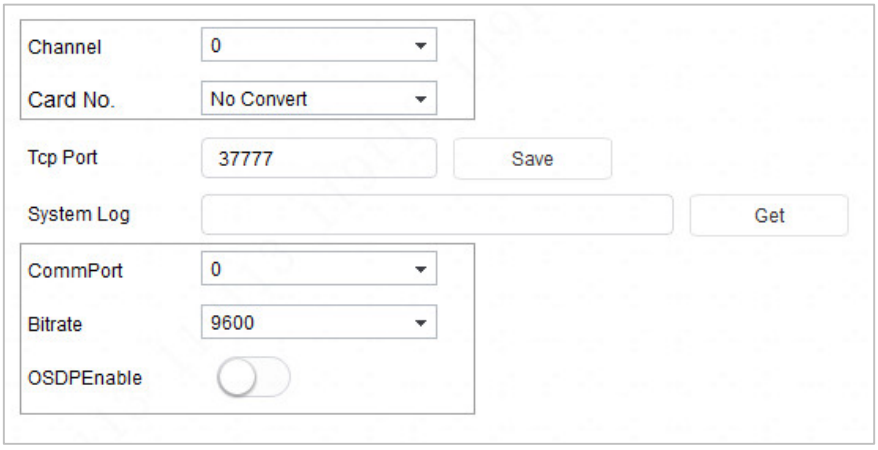


Table 4-2 Access controller parameters

Parameter	Description
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 actual card No., select **Byte Revert** or **HIDpro Convert**. ● **Byte Revert**: When access controller works with third-party readers, and the card number read by the card reader is in the reverse order from the actual card number. For example, the card number read by the card reader is hexadecimal 12345678 while the actual card number is hexadecimal 78563412, and you can select **Byte Revert**.

Parameter	Description
	• **HIDpro Convert**: When access controller works with HID Wiegand readers, and the card number read by the card reader does match the actual card number, you can select HIDpro Revert to match them. For example, the card number read by the card reader is hexadecimal 1BAB96 while the actual card number is hexadecimal 78123456,
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 succeeded, ✓ is displayed on the right side of the device; if failed, ⚠ is displayed. You can click the icon to view detailed information.

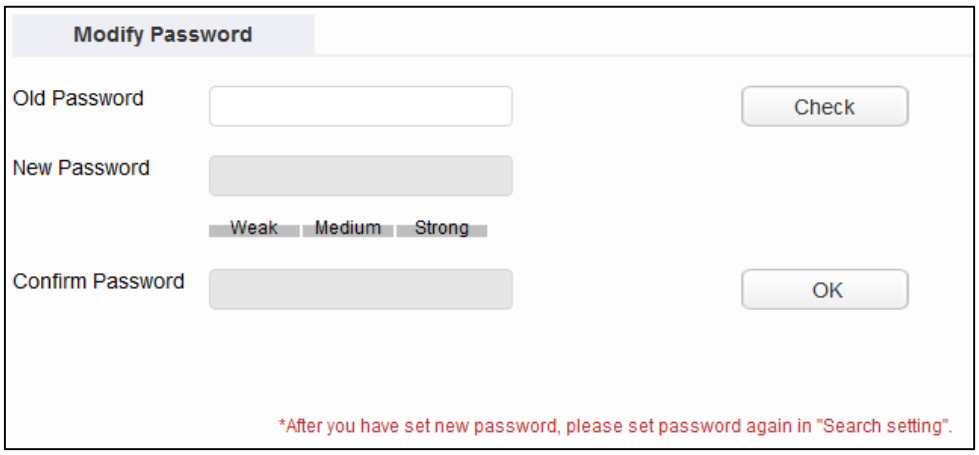
4.4 Changing Device Password

You can modify the device login password.

Step 1 Click  on the menu bar.

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 4-3 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 Security Recommendation

Account Management

1. **Use complex 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: 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 repeating characters, such as 111, aaa, etc.
2. **Change passwords periodically**
   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.
3. **Allocate accounts and permissions appropriately**
   Appropriately add users based on service and management requirements and assign minimum permission sets to users.
4. **Enable account lockout function**
   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.
5. **Set and update password reset information in a timely manner**
   The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**
   It is recommended that you enable HTTPS to access web services through secure channels.
2. **Encrypted transmission of audio and video**
   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**
   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.
   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:
   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**
   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**
   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.
2. **MAC address binding**
   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**
   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:
   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**
   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**
   By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.
3. **Configure network log**
   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**
   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.
2. **Update client software in time**
   It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).