

Access Controller (C)

User's Manual



Foreword

General






This manual introduces the structure, functions and operations of the access controller (hereinafter referred to as "the device").

Models

Two-door one-way;
Two-door two-way;
Four-door one-way;
Four-door two-way;
Eight-door one-way.

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	March 2021

About the Manual

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

jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.

- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This chapter describes the contents covering proper handling of the access controller, hazard prevention, and prevention of property damage. Read the manual carefully before using the access controller, comply with the manual when using, and keep it 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 disassemble 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.
- Use power supply that meets ES1 but does not exceed PS2 limits defined in IEC 62368-1. For specific power supply requirements, refer to device labels.
- Connect the device (type-I 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

Foreword	I
Important Safeguards and Warnings	III
1 Overview	1
1.1 Introduction.....	1
1.1 Features.....	1
1.2 Dimensions.....	1
1.3 Application.....	2
1.3.1 Two-door One-way.....	2
1.3.2 Two-door Two-way.....	3
1.3.3 Four-door One-way.....	3
1.3.4 Four-door Two-way.....	4
1.3.5 Eight-door one-way.....	4
2 Structure	5
2.1 Wiring.....	5
2.1.1 Two-door One-way.....	6
2.1.2 Two-door Two-way.....	7
2.1.3 Four-door One-way.....	8
2.1.4 Four-door Two-way.....	9
2.1.5 Eight-door One-way.....	10
2.1.6 Lock.....	10
2.1.7 Alarm Input.....	11
2.1.8 Alarm Output.....	11
2.1.9 Card Reader.....	13
2.2 Power Indicator.....	13
2.3 DIP Switch.....	14
2.4 Power Supply.....	14
2.4.1 Door Lock Power Port.....	14
2.4.2 Card Reader Power Port.....	14
3 SmartPSS AC Configuration	15
3.1 Login.....	15
3.2 Adding Devices.....	15
3.2.1 Auto Search.....	15
3.2.2 Manual Add.....	16
3.3 User Management.....	18
3.3.1 Setting Card Type.....	18
3.3.2 Adding User.....	19
3.4 Configuring Permission.....	22
3.4.1 Adding Permission Group.....	22
3.4.2 Assigning Permission.....	24
3.5 Access Controller Configuration.....	25
3.5.1 Configuring Advanced Functions.....	25
3.5.2 Configuring Access Controller.....	31
3.5.3 Viewing Historical Event.....	34
3.6 Access Management.....	36

3.6.1 Remotely Opening and Closing Door	36
3.6.2 Setting Always Open and Always Close	37
3.6.3 Resetting Door Status	37
3.7 Event Configuration	38
4 ConfigTool Configuration	41
4.1 Adding Devices.....	41
4.1.1 Adding One Device	41
4.1.2 Adding Multiple Devices.....	42
4.2 Configuring Access Controller	43
4.3 Changing Device Password.....	44
Appendix 1 Cybersecurity Recommendations	46

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.

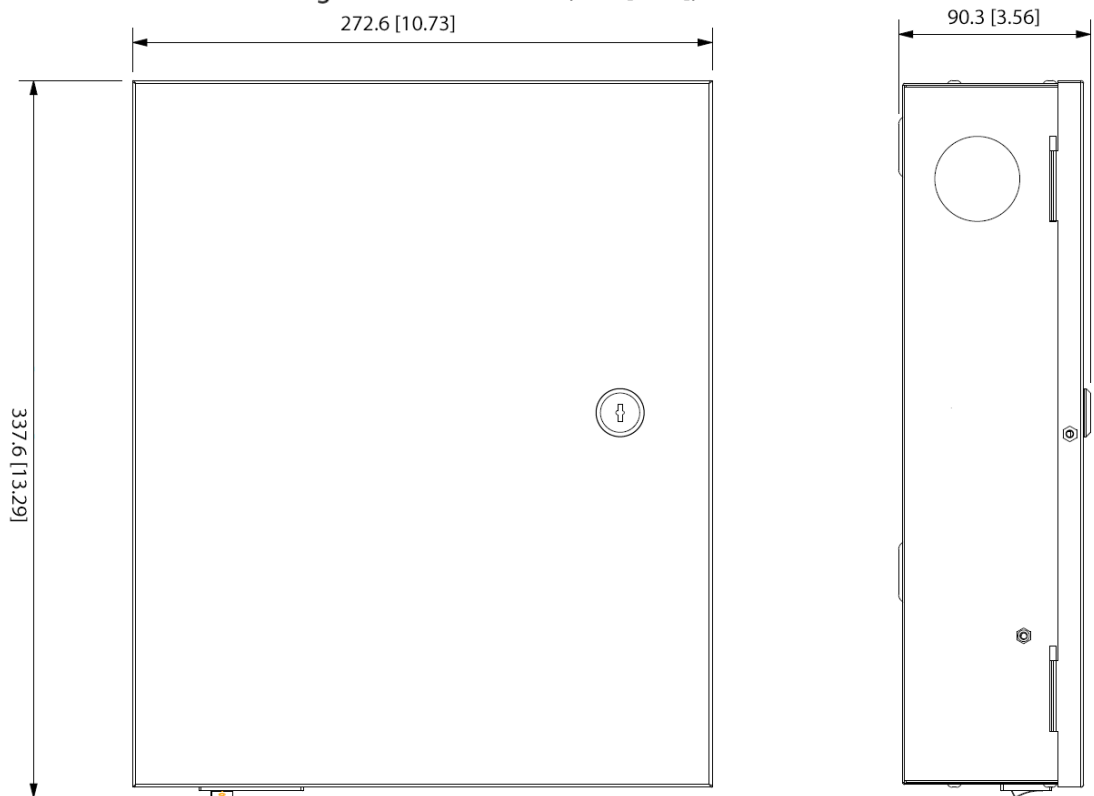
1.1 Features

- 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.

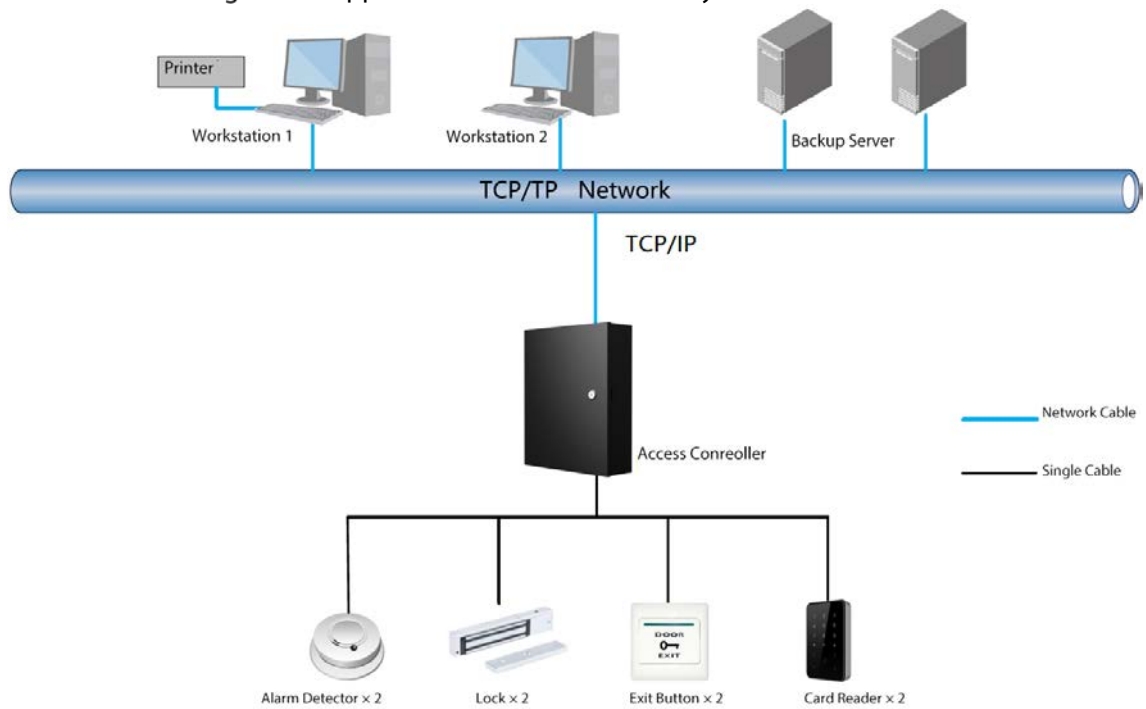
Figure 1-1 Dimensions (mm [inch])



1.3 Application

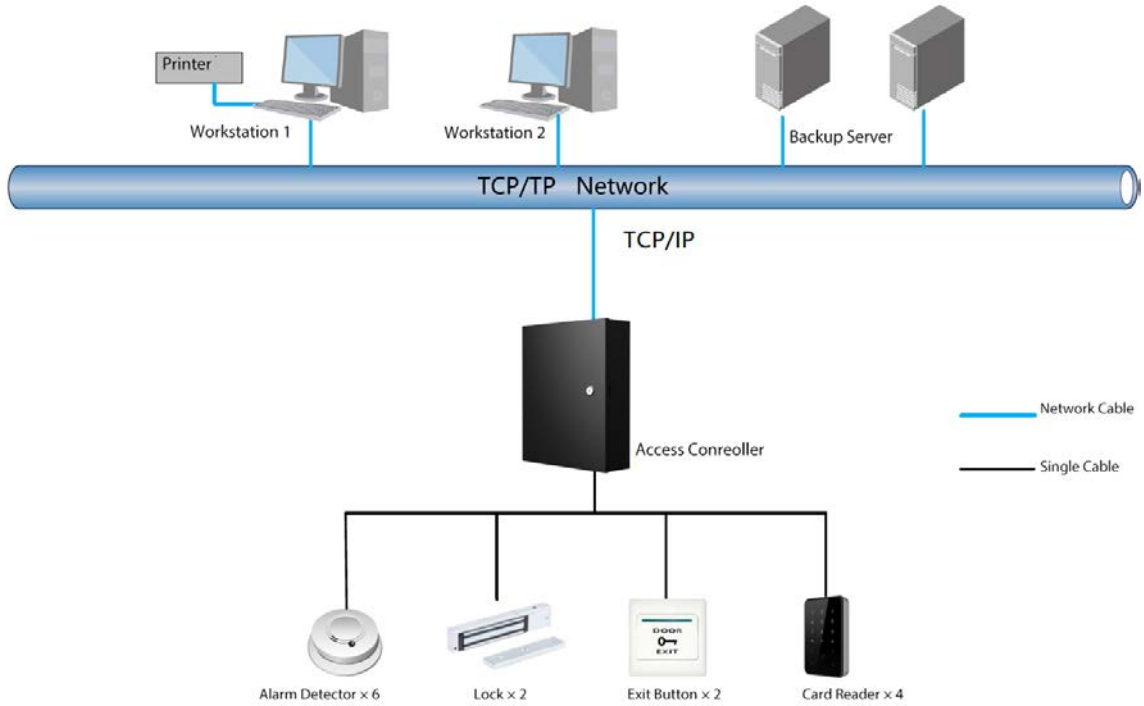
1.3.1 Two-door One-way

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



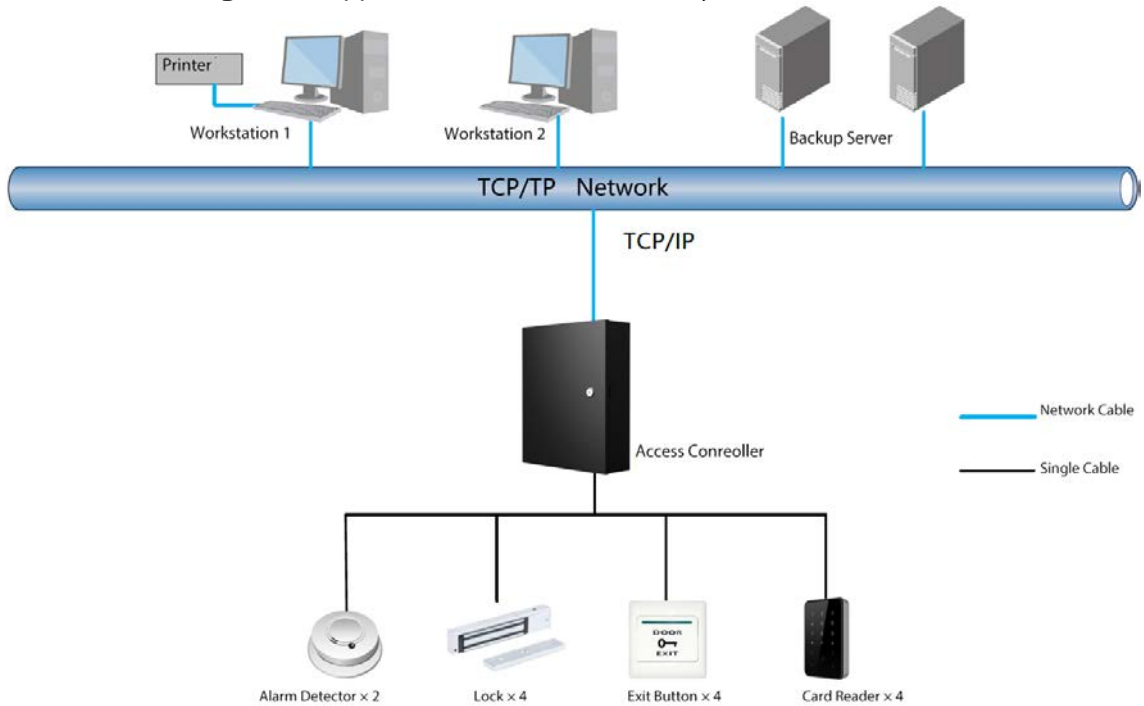
1.3.2 Two-door Two-way

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



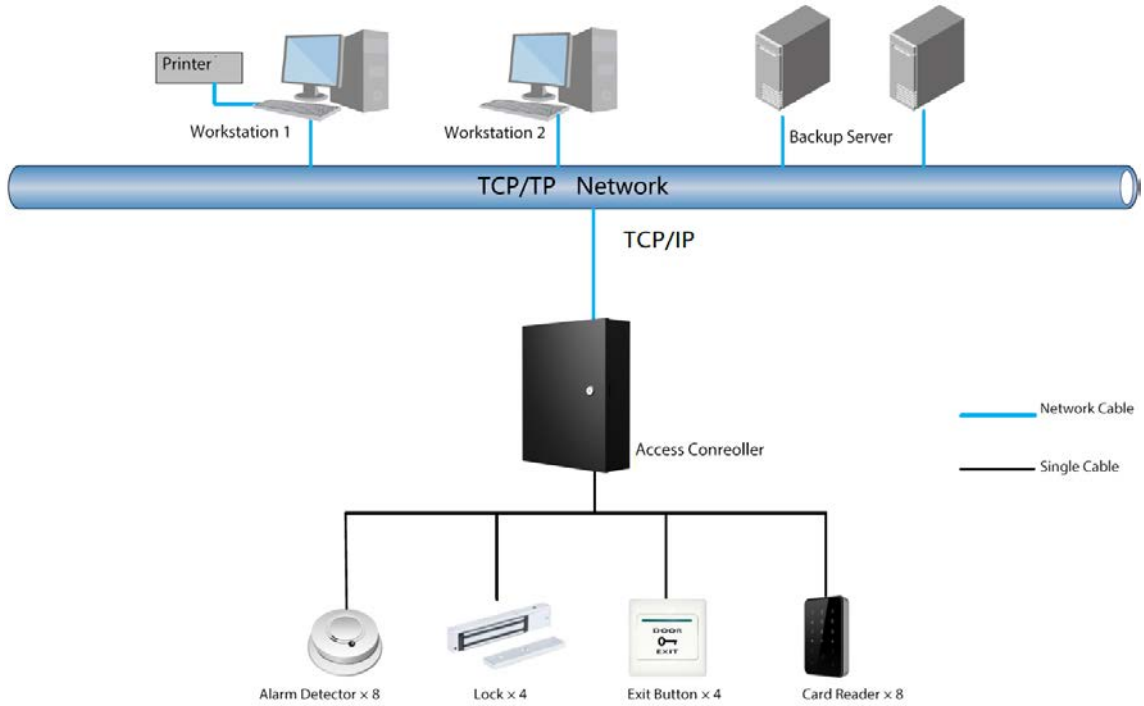
1.3.3 Four-door One-way

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



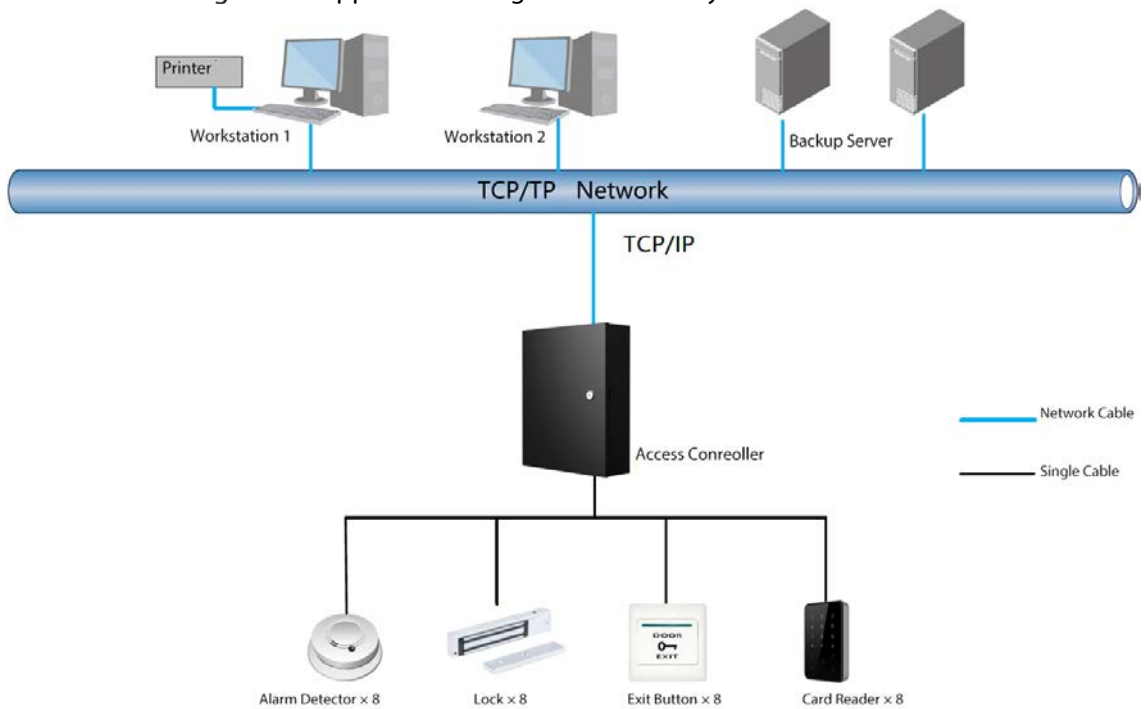
1.3.4 Four-door Two-way

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



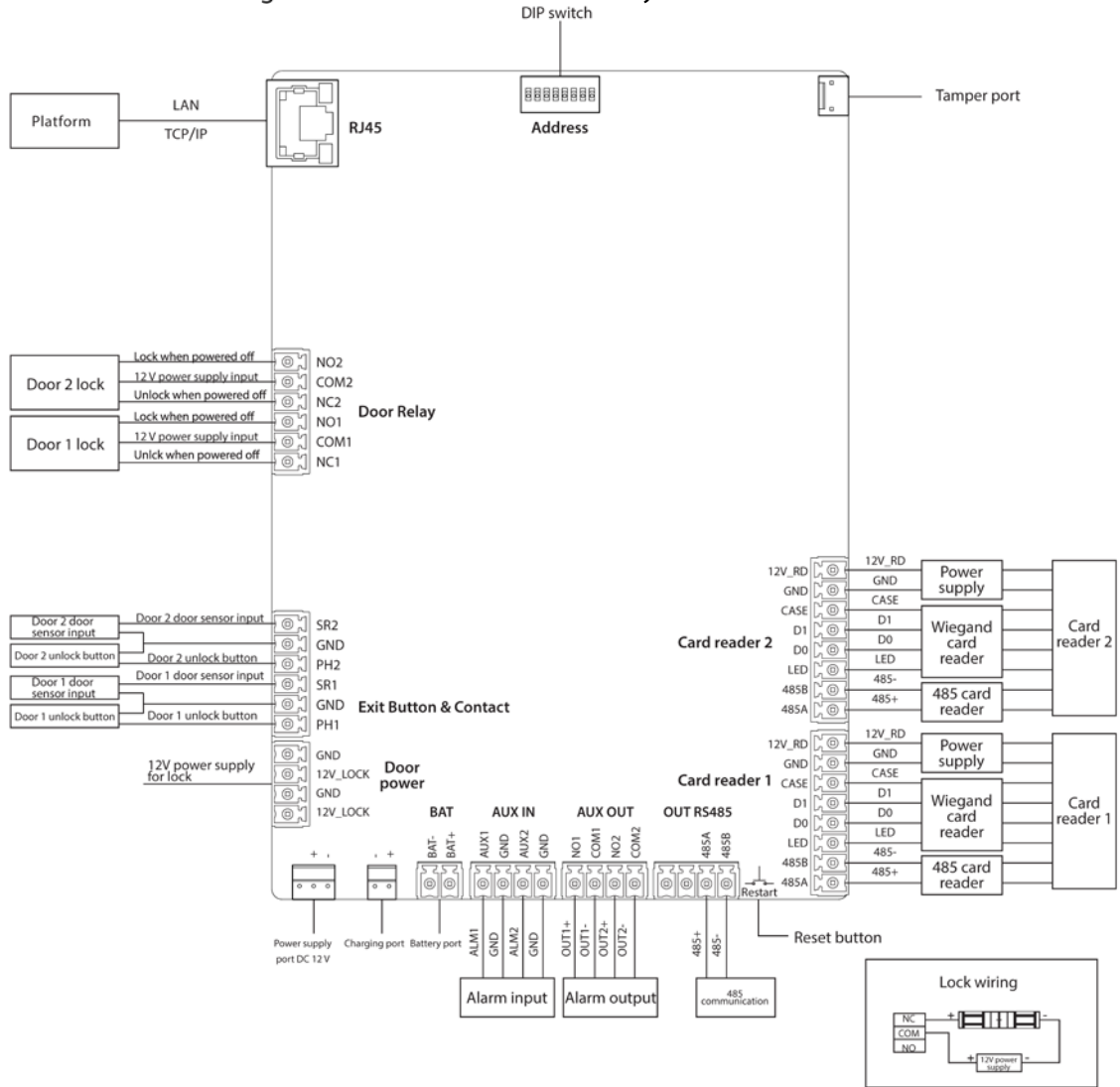
- Connect the wires only when powered off.
- Make sure that the plug of the power supply is grounded.
- 12 V: Maximum current for an extension module is 100 mA.
- 12 V_RD: Maximum current for a card reader is 2.5 A.
- 12 V_LOCK: Maximum current for a lock is 2 A.

Table 2-1 Wire specification

Device	Cable	Cross-sectional Area of Each Core	Remarks
Card reader	Cat5 8-core shielded twisted pair	$\geq 0.22 \text{ mm}^2$	Suggested $\leq 100 \text{ m}$
Ethernet cable	Cat5 8-core shielded twisted pair	$\geq 0.22 \text{ mm}^2$	Suggested $\leq 100 \text{ m}$
Button	2-core	$\geq 0.22 \text{ mm}^2$	-
Door contact	2-core	$\geq 0.22 \text{ mm}^2$	-

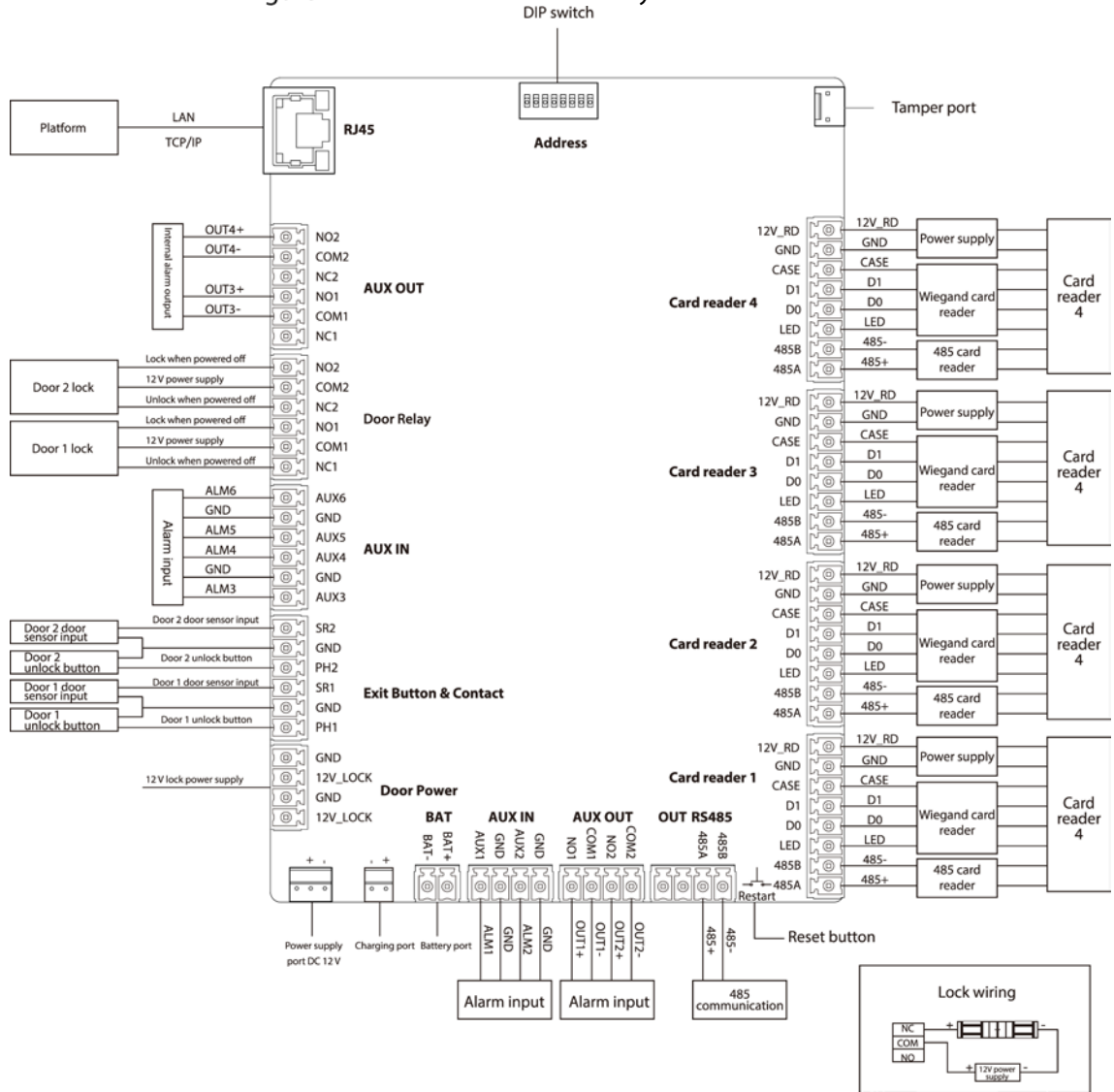
2.1.1 Two-door One-way

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



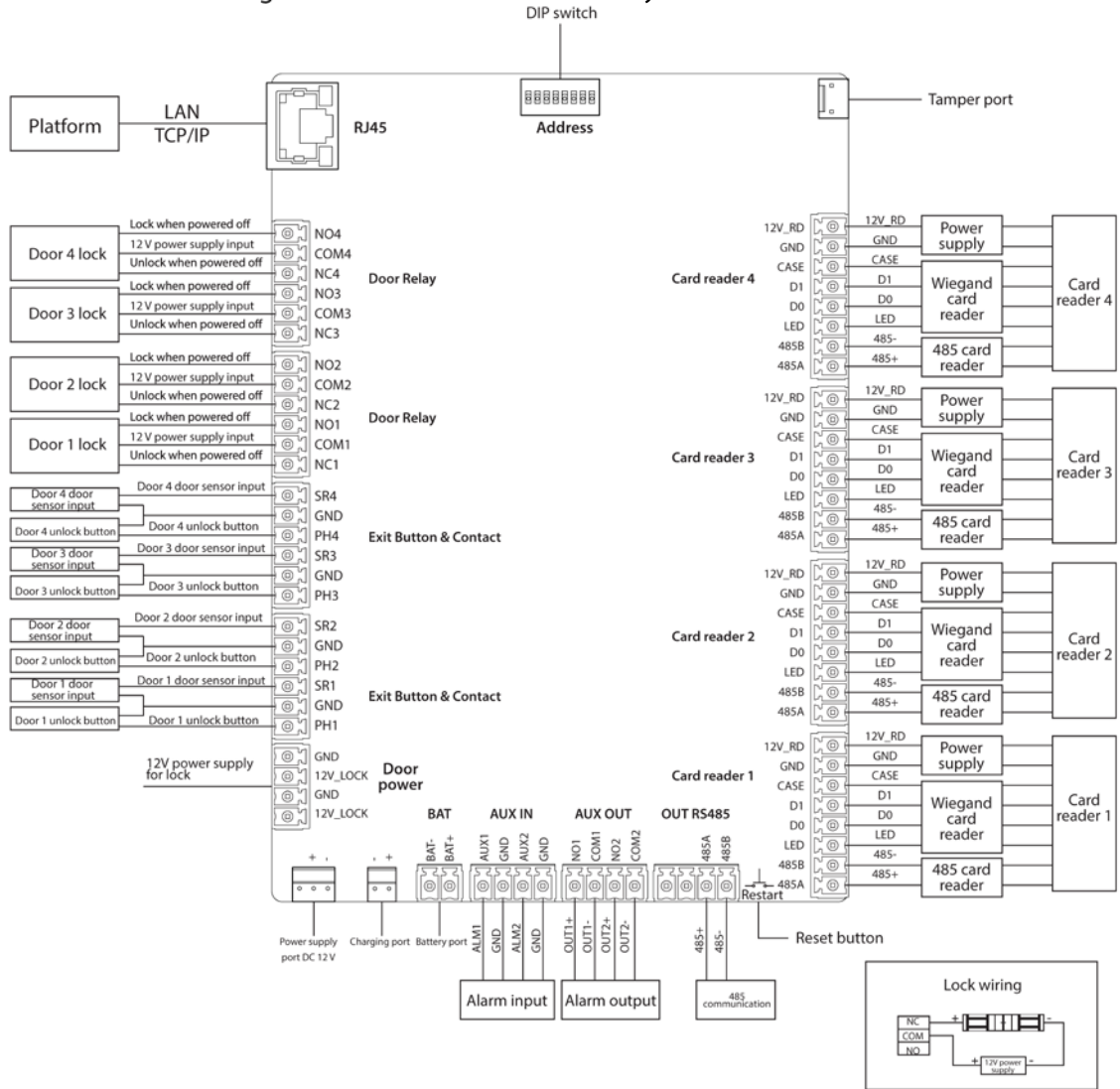
2.1.2 Two-door Two-way

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



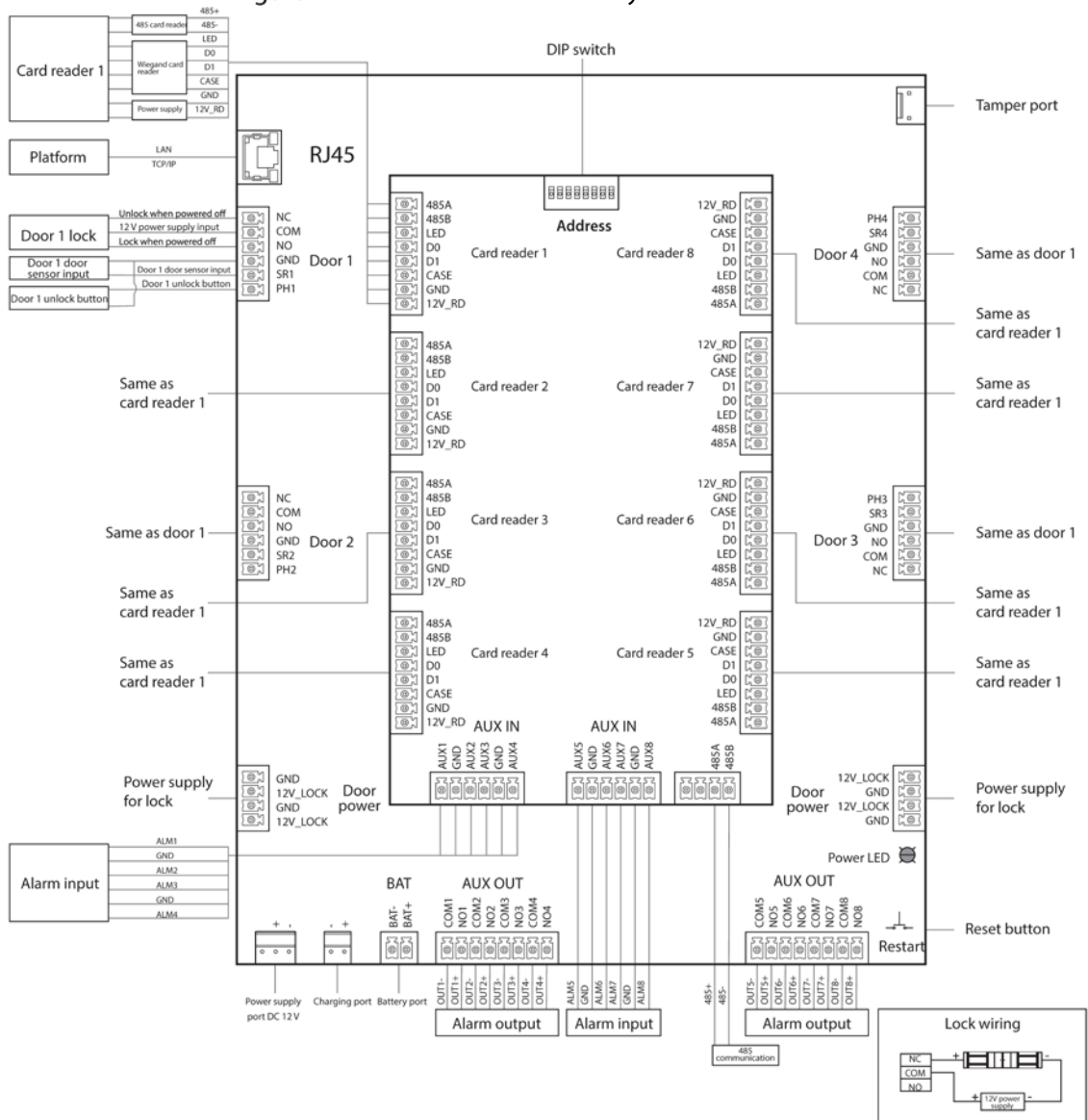
2.1.3 Four-door One-way

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



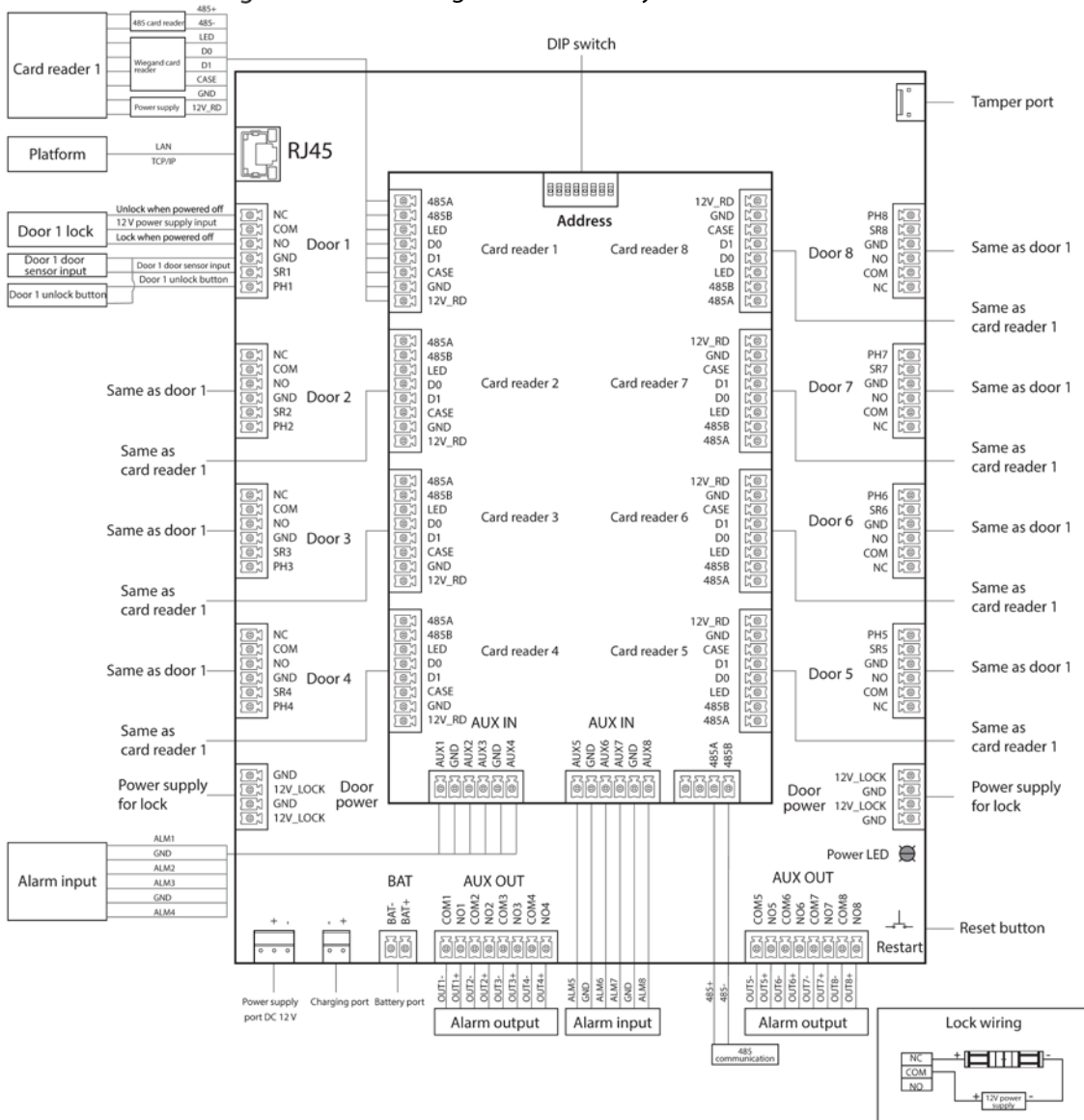
2.1.4 Four-door Two-way

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

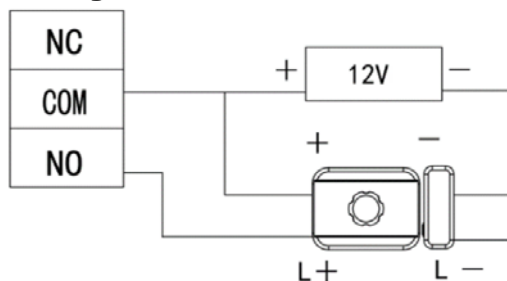


Figure 2-7 Magnetic lock

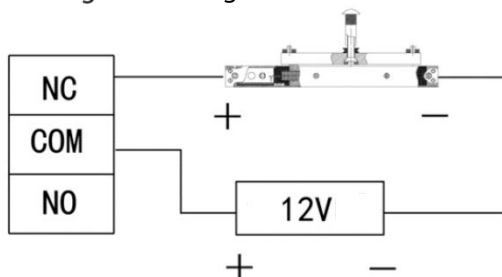
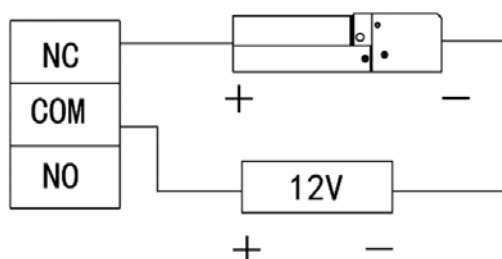


Figure 2-8 Electric bolt



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: <ul style="list-style-type: none"> ● 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: <ul style="list-style-type: none"> ● AUX1–AUX2 external alarm links Normally Open for all doors. ● AUX3–AUX4 external alarm links Normally Closed for all doors.
Four-door One way	2	Linkable door status: <ul style="list-style-type: none"> ● 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: <ul style="list-style-type: none"> ● AUX1–AUX2 external alarm links Normally Open for all doors. ● AUX3–AUX4 external alarm links Normally Closed for all doors.
Eight-door One-way	8	Linkable door status: <ul style="list-style-type: none"> ● AUX1–AUX2 external alarm links Normally Open for all doors. ● AUX3–AUX4 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	2	NO1 <ul style="list-style-type: none"> ● AUX1 triggers alarm output.

Type	Number of Alarm Output Channels	Description	
One-way		COM1	<ul style="list-style-type: none"> Door timeout and intrusion alarm output for door 1. Card Reader 1 tamper alarm output.
		NO2	<ul style="list-style-type: none"> AUX2 triggers alarm output.
		COM2	<ul style="list-style-type: none"> Door timeout and intrusion alarm output for door 2. Card Reader 2 tamper alarm output.
Two-door Two-way	2	NO1	AUX1/AUX2 triggers alarm output.
		COM1	
		NO2	AUX3/AUX4 triggers alarm output.
	COM2		
	2	NC1	<ul style="list-style-type: none"> Card Reader 1/2 tamper alarm output. Door 1 timeout and intrusion alarm output.
		COM1	
NO1		<ul style="list-style-type: none"> Card Reader 3/4 tamper alarm output. Door 2 timeout and intrusion alarm output. 	
COM2			
NO2			
Four-door One way	2	NO1	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> AUX1 triggers alarm output. Card Reader 1/2 tamper alarm output. Door 1 timeout and intrusion alarm output. Device tamper alarm output.
		COM1	
		NO2	
		COM2	<ul style="list-style-type: none"> AUX2 triggers alarm output. Card Reader 1/2 tamper alarm output. Door 2 timeout and intrusion alarm output.
		NO3	
		COM3	<ul style="list-style-type: none"> AUX3 triggers alarm output. Card Reader 5/6 tamper alarm output. Door 3 timeout and intrusion alarm output.
		NO4	
		COM4	<ul style="list-style-type: none"> AUX4 triggers alarm output. Card Reader 7/8 tamper alarm output. Door 4 timeout and intrusion alarm output.
		NO5	
		COM5	AUX5 triggers alarm output.
		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	<ul style="list-style-type: none"> ● AUX1 triggers alarm output. ● Card Reader 1 tamper alarm output. ● Door 1 timeout and intrusion alarm output. ● Device tamper alarm output.
		COM1	
		NO2	<ul style="list-style-type: none"> ● AUX2 triggers alarm output. ● Card Reader 2 tamper alarm output. ● Door 2 timeout and intrusion alarm output.
		COM2	
		NO3	<ul style="list-style-type: none"> ● AUX3 triggers alarm output. ● Card Reader 3 tamper alarm output. ● Door 3 timeout and intrusion alarm output.
		COM3	
		NO4	<ul style="list-style-type: none"> ● AUX4 triggers alarm output. ● Card Reader 4 tamper alarm output. ● Door 4 timeout and intrusion alarm output.
		COM4	
		NO5	<ul style="list-style-type: none"> ● AUX5 triggers alarm output. ● Card Reader 5 tamper alarm output. ● Door 5 timeout and intrusion alarm output.
		COM5	
		NO6	<ul style="list-style-type: none"> ● AUX6 triggers alarm output. ● Card Reader 6 tamper alarm output. ● Door 6 timeout and intrusion alarm output.
		COM6	
		NO7	<ul style="list-style-type: none"> ● AUX7 triggers alarm output. ● Card Reader 7 tamper alarm output. ● Door 7 timeout and intrusion alarm output.
		COM7	
		NO8	<ul style="list-style-type: none"> ● 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

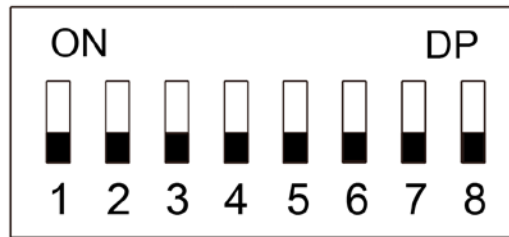
2.2 Power Indicator

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

2.3 DIP Switch



Figure 2-9 DIP switch



- When 1–8 are all switched to 0, the device starts normally after power-on.
- When 1–8 are all switched to 1, the device enters the BOOT mode after it starts.
- When 1, 3, 5 and 7 are switched to 1 and the others are 0, the device restores to factory defaults after it restarts.
- When 2, 4, 6 and 8 are switched to 1 and the others are 0, the device 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 remotely manage the device through SmartPSS AC. This chapter mainly introduces quick configuration. For detailed operations, refer to SmartPSS AC user manual.




Smart PSS AC client offers different interfaces for different versions.

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.

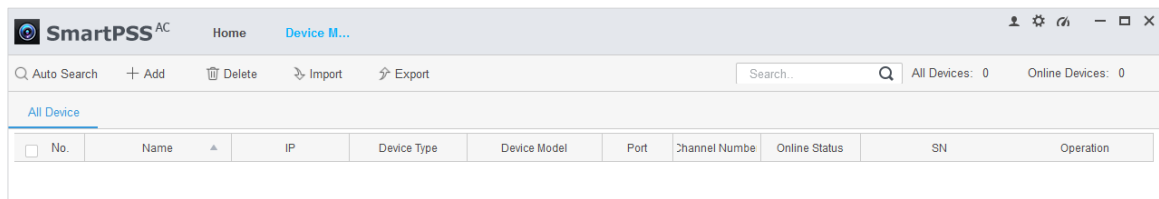
3.2.1 Auto Search

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.

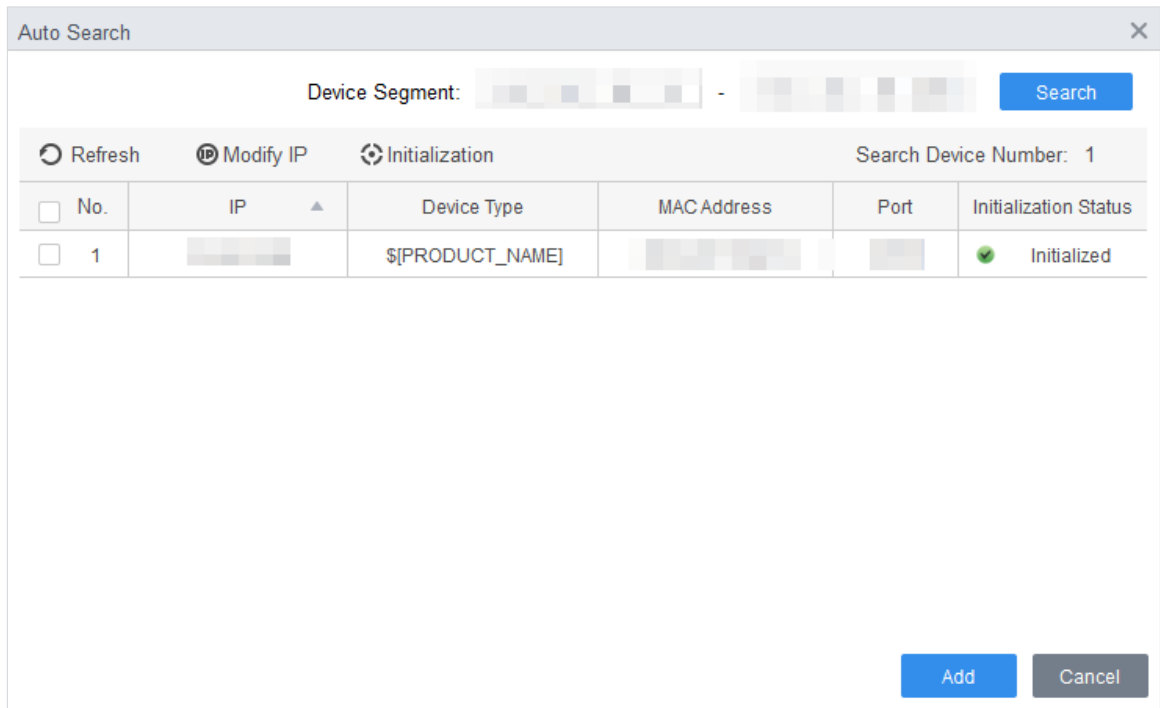
Step 2 Click **Device Manager** on the lower-left corner.

Figure 3-1 Devices



Step 3 Click **Auto Search**.

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**.

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. We recommend changing 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

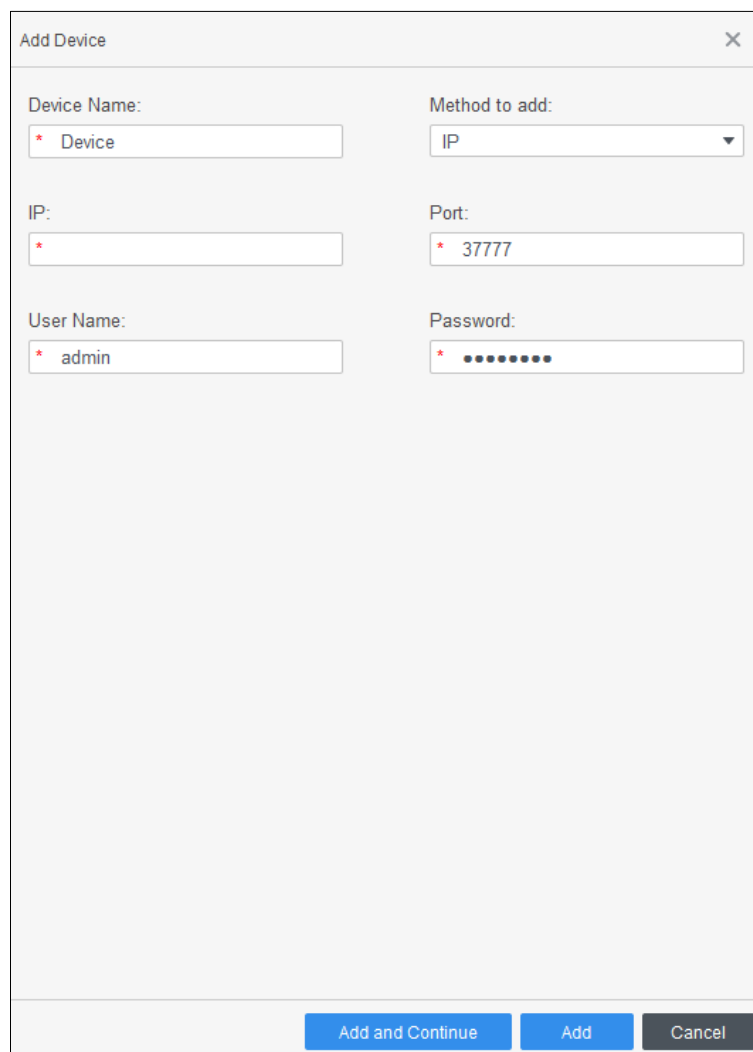
You can add devices manually. You need to know IP addresses and domain names of access controllers that you want to add.

Step 1 Log in to SmartPSS AC.

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


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

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. We recommend naming 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. The port number is 37777 by default.
User Name, Password	Enter the username and password of the added device.  The username is admin and password is admin123 by default. We recommend changing 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

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

3.3.1 Setting Card Type

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

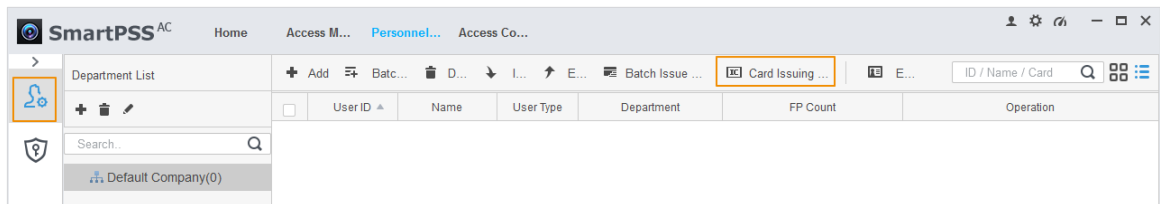


Card types must be the same as card issuer types; otherwise, card numbers cannot be read.

Step 1 Log in to SmartPSS AC.

Step 2 Click **Personnel Manager**.

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.


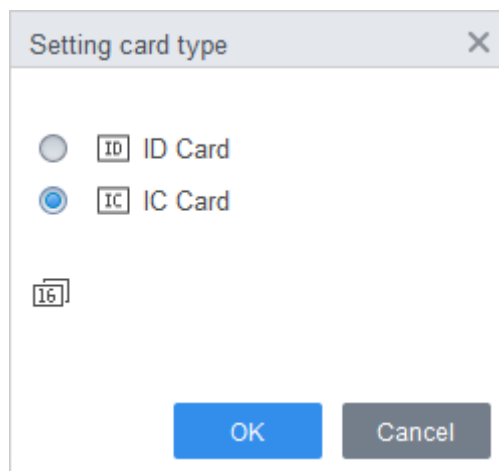
Step 5 Click  to select display method of card number in decimal or in hex.

Figure 3-5 Setting card type



Step 6 Click **OK**.

3.3.2 Adding User

3.3.2.1 Manual Add

You can add users 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

The screenshot shows the 'Add User' dialog box with the 'Basic Info' tab selected. The form contains the following fields and values:

- User ID: 2
- Name: test
- Department: Default Company
- User Type: General
- Valid Time: 2020/6/5 0:00:00 to 2030/6/5 23:59:59 (3653 Days)
- Gender: Male (selected)
- Title: Mr
- DOB: 1985-3-15
- Tel: (empty)
- Email: (empty)
- Mailing Address: (empty)
- Administrator: (toggle off)
- Remark: (empty text area)
- ID Type: ID
- ID No.: (empty)
- Company: (empty)
- Occupation: (empty)
- Entry Time: 2020/6/4 14:37:59
- Resign Time: 2030/6/5 14:37:59

A camera capture frame on the right shows a silhouette of a person with an 'Upload Picture' button highlighted in orange. Below the frame, it says 'Image Size: 0 ~ 120KB'. At the bottom of the dialog, there are 'Continue', 'Finish', and 'Cancel' buttons.

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.


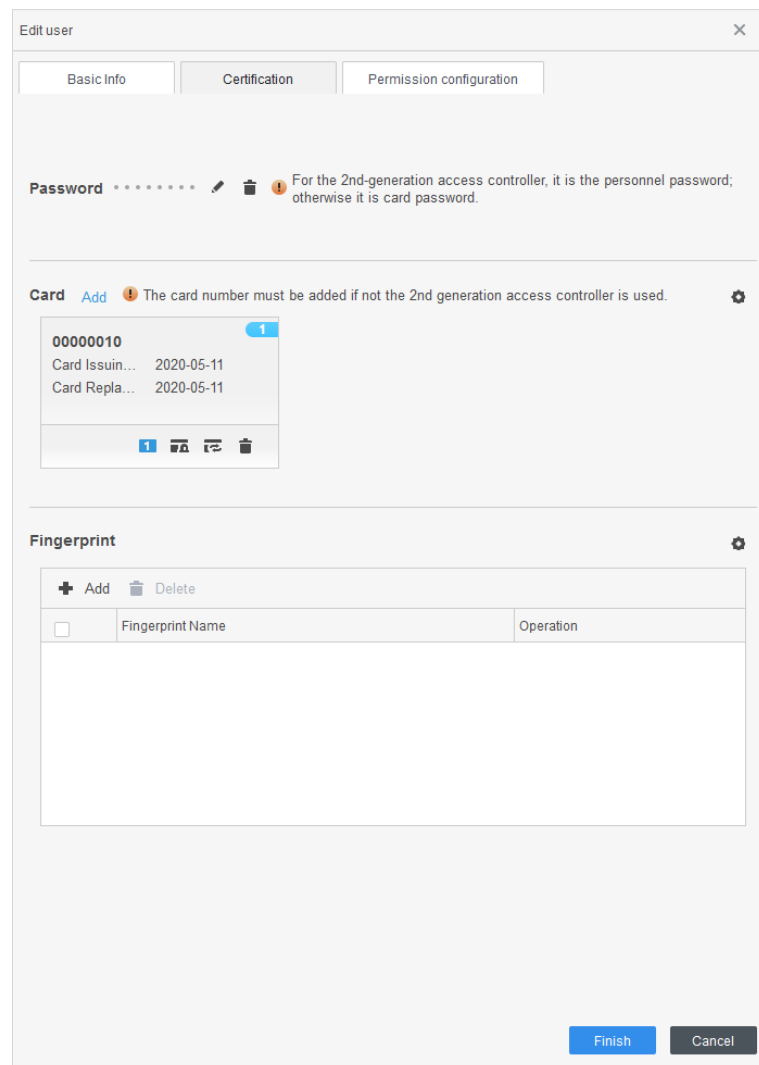
- 1) Click  to set **Device** or **Fingerprint Scanner** to fingerprint collector.
- 2) Click **Add Fingerprint** and press your finger on the scanner three times continuously.

Figure 3-7 Configure certification



The screenshot shows the 'Edit user' dialog box with the 'Certification' tab selected. It contains the following sections:

- Password:** A text field with a masked password and a gear icon. A note states: "For the 2nd-generation access controller, it is the personnel password; otherwise it is card password."
- Card:** A section with an 'Add' button and a note: "The card number must be added if not the 2nd generation access controller is used." Below this is a card preview showing:
 - Card Number: 00000010
 - Card Issuance Date: 2020-05-11
 - Card Replacement Date: 2020-05-11
- Fingerprint:** A section with an 'Add' button and a 'Delete' button. Below is a table with columns for 'Fingerprint Name' and 'Operation'. The table is currently empty.

At the bottom right, there are 'Finish' and 'Cancel' buttons.

Step 5 Configure permissions for the user.

For details, see "3.4 Configuring Permission".

Figure 3-8 Permission configuration

Basic Info Certification **Permission configuration**

Permission group is a combination of various devices including attendance check and access control. After selecting the permission group, the personnel info will be sent to corresponding device and used for related functions of access control and attendance check.

Add Group

<input type="checkbox"/>	Permission Group	Memo
<input type="checkbox"/>	Permission Group1	
<input type="checkbox"/>	Permission Group2	

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 users in batches

Batch Add ✕

Device
Card issuer Issue


Start No.: * 5 Quantity: * 10

Department:
Company\DepartmentB

Effective Time: 2020/4/30 0:00:00 📅 Expired Time: 2030/4/30 23:59:59 📅

Issue Card

ID	Card No.
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	

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

3.4 Configuring Permission







3.4.1 Adding Permission Group


Add permission group, and then you can add users to the group to assign them various access permissions.

Step 1 Log in to SmartPSS AC.

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

Figure 3-10 Permission group list

	Permission Group	Operation
<input type="checkbox"/>	Permission Group1	  
<input type="checkbox"/>	Permission Group2	  

Step 3 Click  to add a permission group.

Step 4 Set permission parameters.

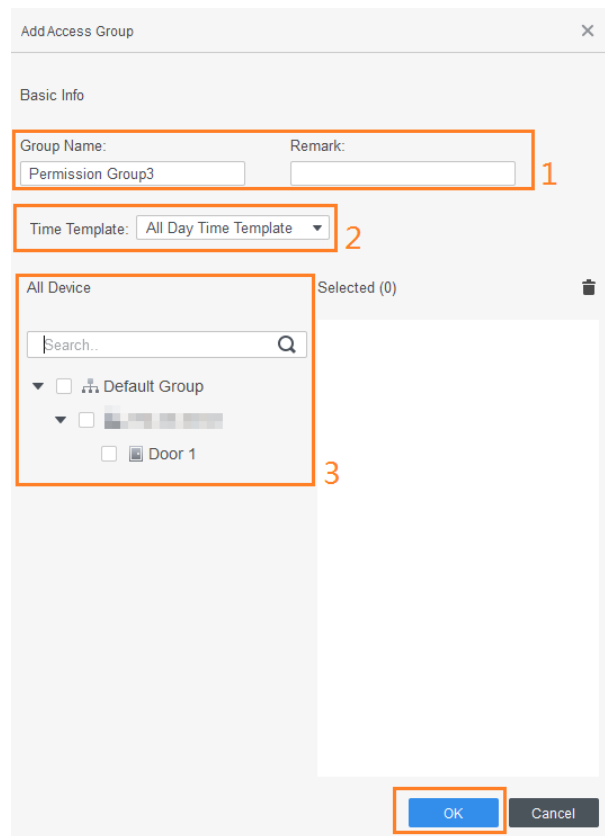
- 1) Enter group name and remark.
- 2) Select the needed time template.



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

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

Figure 3-11 Add permission group




The 'Add Access Group' dialog box is shown with three numbered callouts. Callout 1 points to the 'Group Name' and 'Remark' input fields, which contain 'Permission Group3' and are empty respectively. Callout 2 points to the 'Time Template' dropdown menu, which is set to 'All Day Time Template'. Callout 3 points to the 'All Device' section, which includes a search bar and a list of devices: 'Default Group', 'Door 1', and an unselected device. The 'OK' button is highlighted with a red box.

Step 5 Click **OK**.



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

- Click  to delete group.

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

3.4.2 Assigning Permission

Assign permissions to users, and then they can unlock doors.

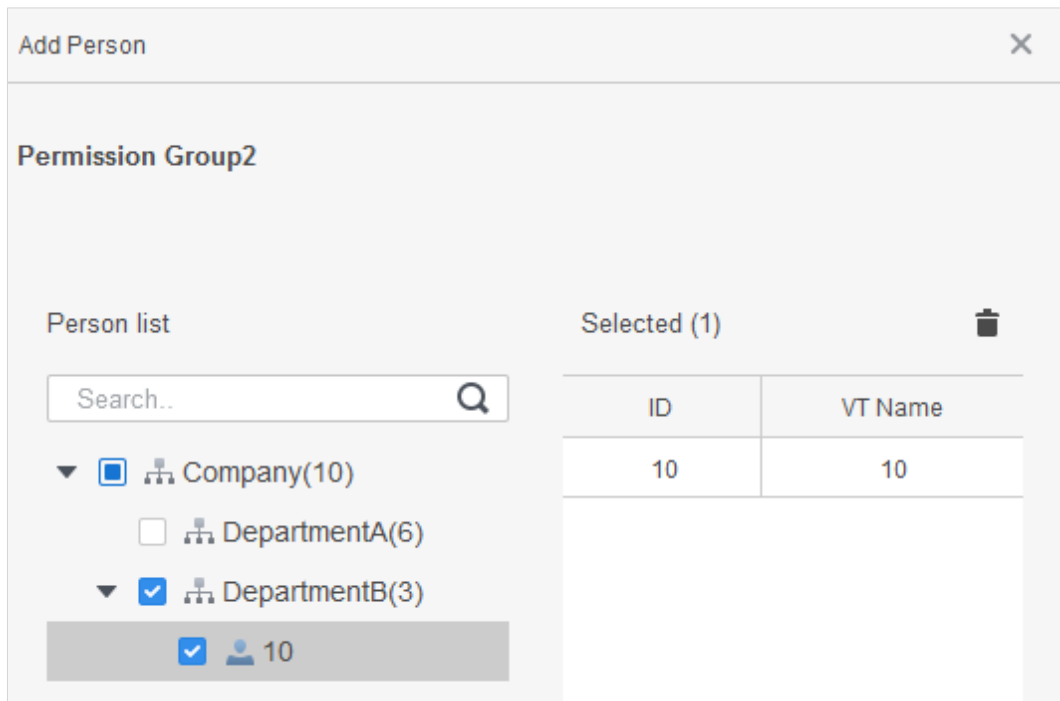
The method to configure permissions for department and for users is similar. This section takes users as an example.

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 that needs to be configured permissions.

Step 5 Click **OK**.

3.5 Access Controller Configuration

3.5.1 Configuring Advanced Functions

3.5.1.1 First Card Unlock

You can set multiple first cards. Only after any first-card user swipes the card can other users unlock the door with their cards.



- 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 "3.4 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 3-13 First card unlock configuration

First Card Unlock configuration

Door: Door 1 Timezone: All Day Time Template
Status: Normal

Select Personnel

Dropdown list Search..

ID	Name
<input checked="" type="checkbox"/>	1
<input checked="" type="checkbox"/>	2
<input type="checkbox"/>	3



Selected(2) Clear

ID	Name	Operation
1	1	
2	2	

Save Cancel

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.

3.5.1.2 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 Configuring Permission".

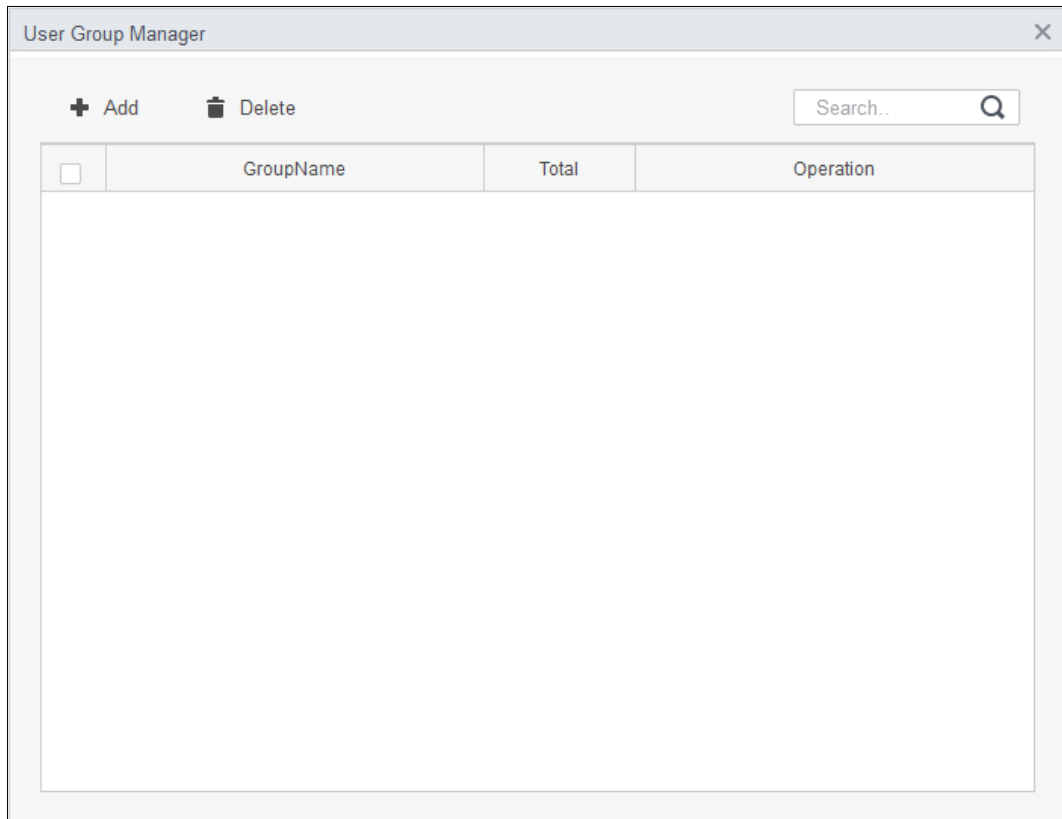
Step 1 Select **Access Configuration > Advanced Config**.

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

Step 3 Add user group.

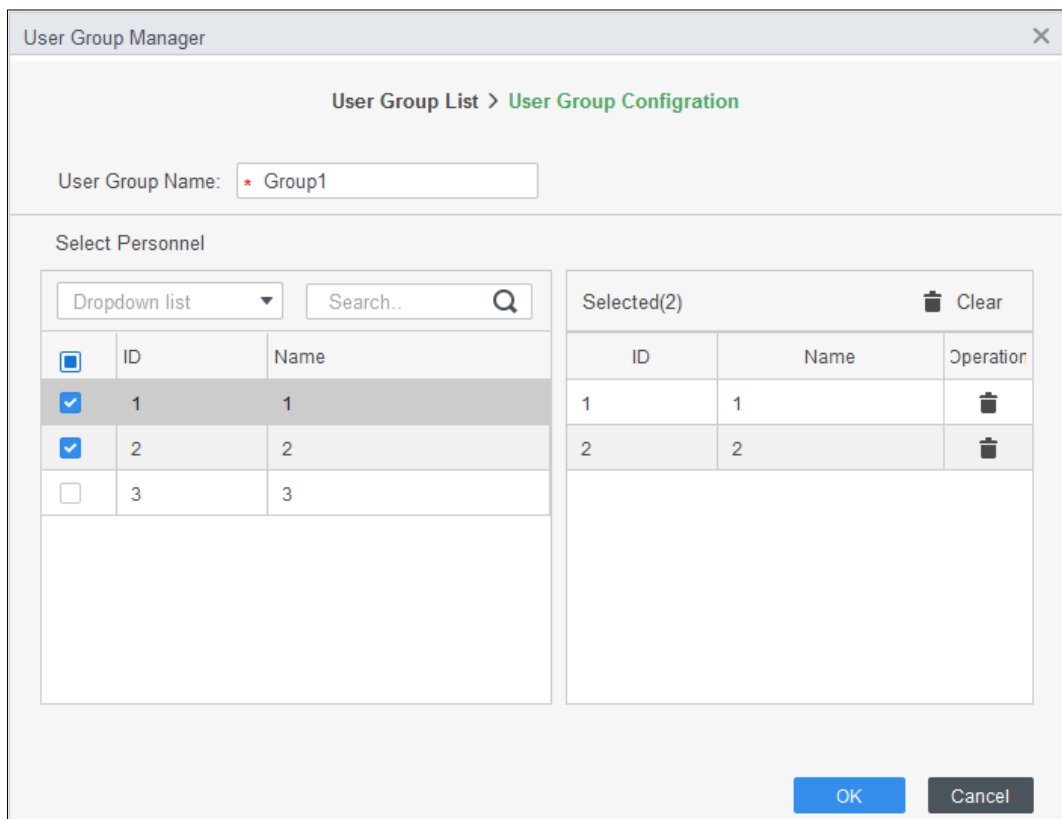
- 1) Click **User Group**.


Figure 3-14 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 parameters of multi-card unlock.

- 1) Click **Add**.

Figure 3-16 Multi-card unlock configuration (1)

Multi-card Unlock configuration

Door:

User Group List

Search..		Q
<input type="checkbox"/>	User Group Name	Count
<input type="checkbox"/>	Group1	2

Selected (0) Clear

User Group Name	Count	Valid Count	Unlock Mode	Operation
-----------------	-------	-------------	-------------	-----------

OK Cancel

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

Figure 3-17 Multi-card unlock configuration (2)

Multi-card Unlock configuration

Door:

User Group List



Search..		Q
<input checked="" type="checkbox"/>	User Group Name	Count
<input checked="" type="checkbox"/>	Group1	2
<input checked="" type="checkbox"/>	Group2	2

Selected (2) Clear

User Group Name	Count	Valid Count	Unlock Mode	Operation
Group1	2	1	Card	↑ ↓ 🗑
Group2	2	2	Card	↑ ↓ 🗑

OK Cancel

- 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.

3.5.1.3 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.

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

Step 2 Click **Add**.

Step 3 Configure parameters.

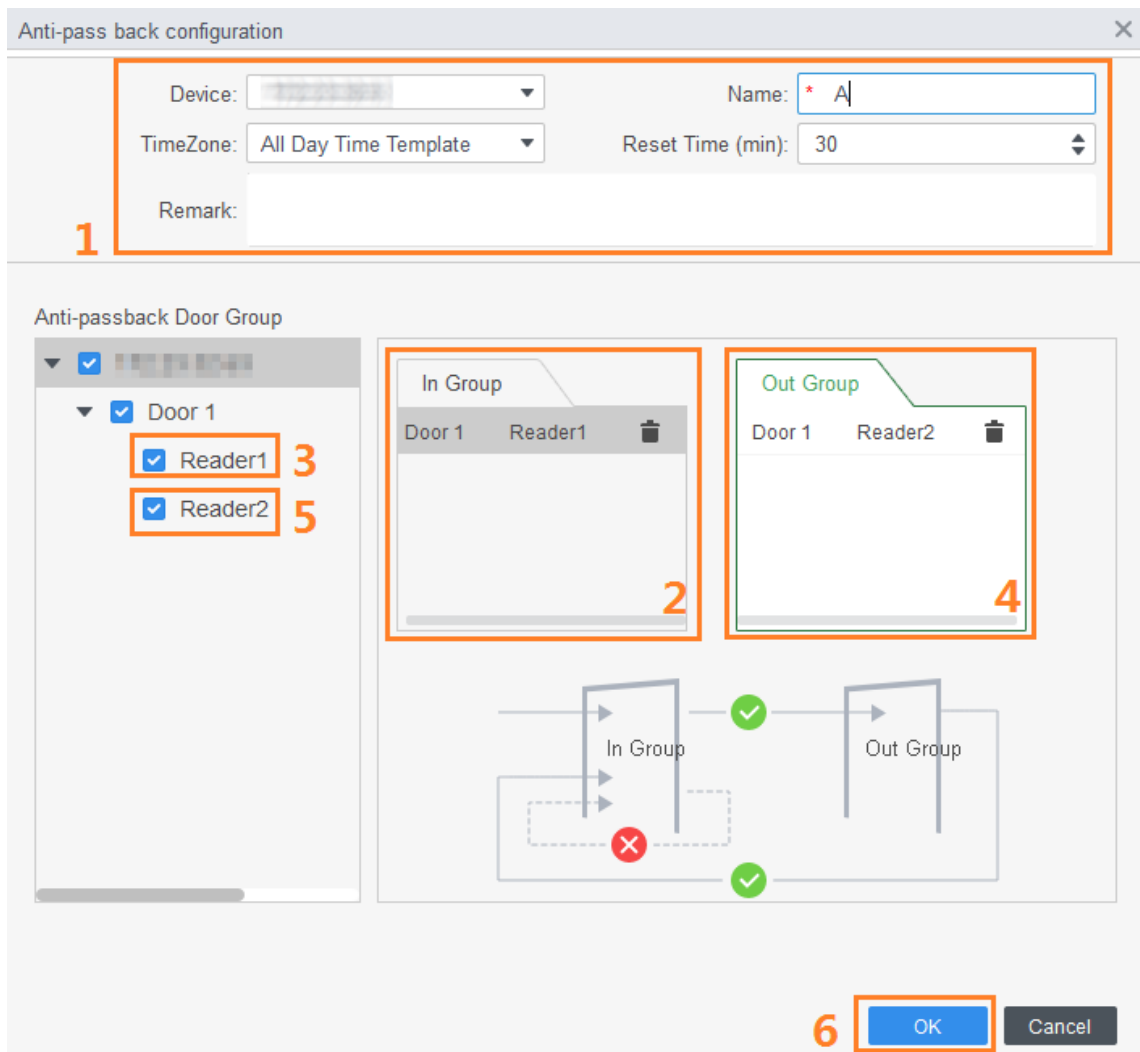
- 1) Select device and enter device name.
- 2) Select time template.
- 3) Set rest time and the unit is minute.

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 3-18 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.

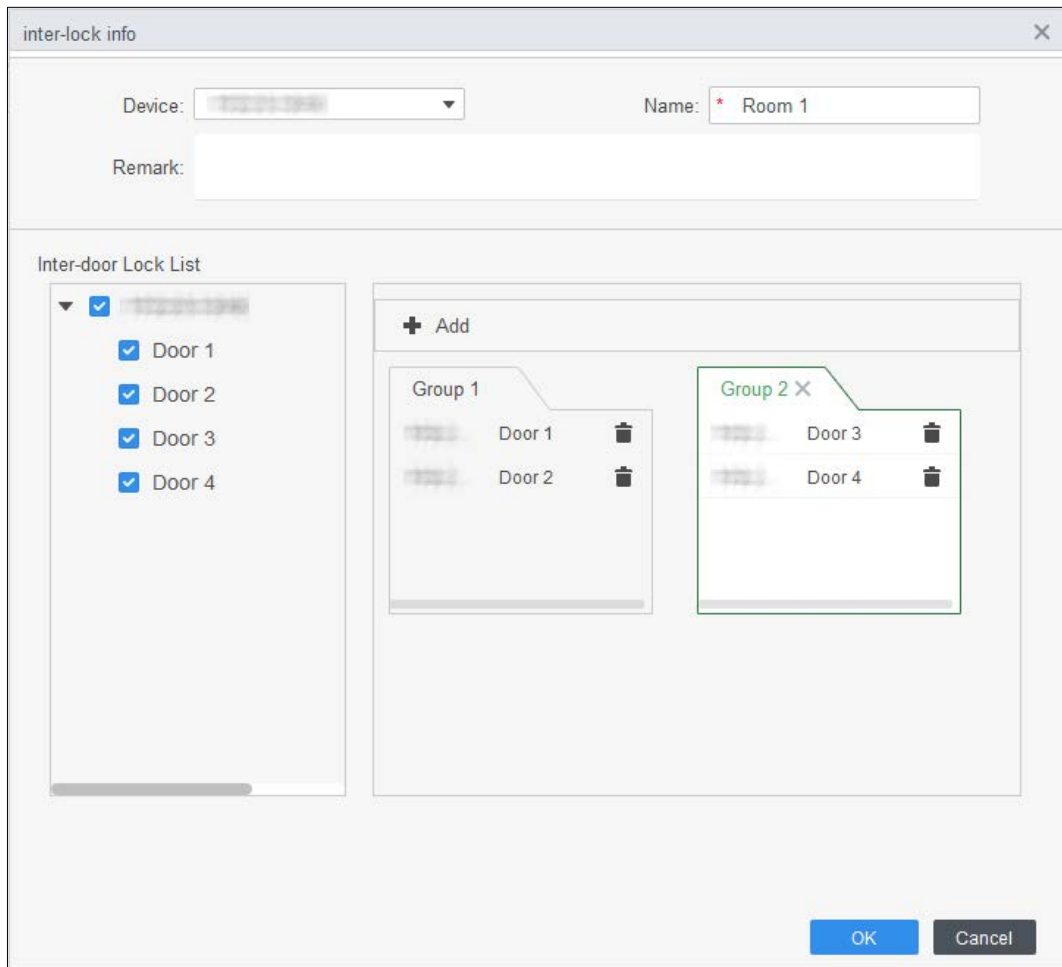
Step 3 Click **Add**.



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 , which indicates **Inter-door Lock** is enabled.

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

3.5.2 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 3-20 Configure access door

Access Door Config

Door: * Door 1

Reader Direction Config: IN Reader1 ⇌ OUT

Status: Normal Always Open Always Close

Keep OpenTimezone: Unopened

Keep Close Timezone: Unopened

Alarm: Intrusion Overtime Duress

Door Sensor:

Administrator Password: *

Remote Verification:

Unlock Hold Interval: 3 Second

Close Timeout: 15 Second

Unlock Mode: or

Card Fingerprint Face Password

Save Cancel

Figure 3-21 Unlock by time period

Timezone set

Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Timezone 1 00:00 — 06:00 Unlock Mode Card / Fingerprint / Face / Password

Timezone 2 06:00 — 10:00 Unlock Mode Card + Fingerprint



Timezone 3 10:00 — 12:00 Unlock Mode Password

Timezone 4 12:00 — 23:00 Unlock Mode Fingerprint

All

OK Cancel

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. <ul style="list-style-type: none"> ● 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** 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.

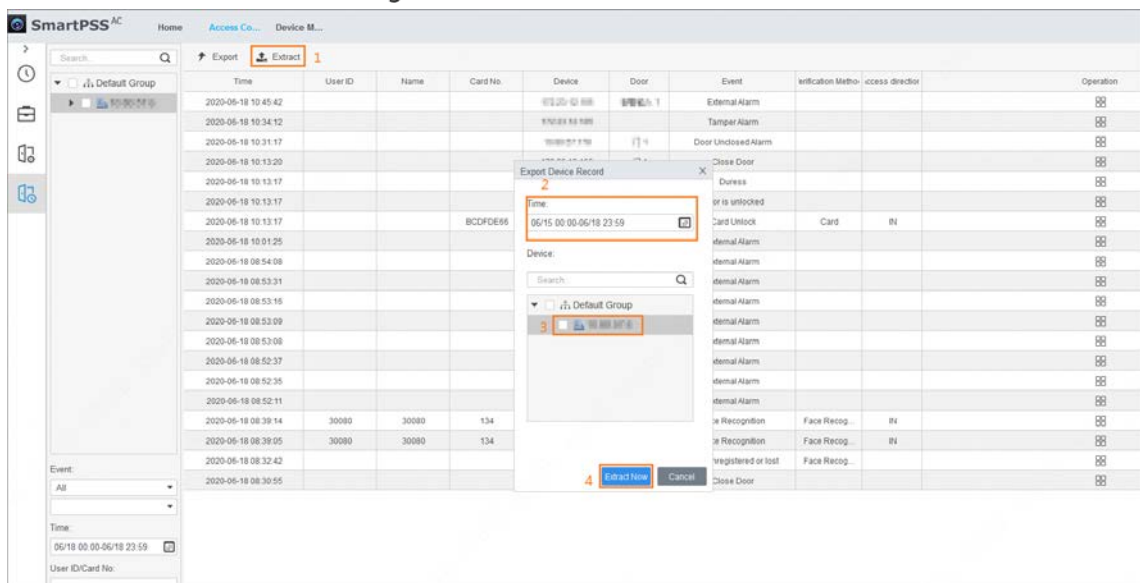
Step 3 Click on the **Access Manager** interface.

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

The screenshot shows a search interface with the following elements:


- A search bar at the top with the placeholder text "Search.." and a magnifying glass icon.
- A tree view showing a hierarchy: "Default Group" (expanded) > "Door 1" (selected and highlighted).
- Filter sections:
 - Event:** A dropdown menu with "Abnormal" selected.
 - Time:** A date range selector showing "05/07 00:00-05/07 23:59" with a calendar icon.
 - User ID/C...:** A text input field containing "1".
 - Name:** A text input field containing "1".
 - Departme...:** A dropdown menu with "Company\DepartmentA" selected.
- A blue "Search" button at the bottom.

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

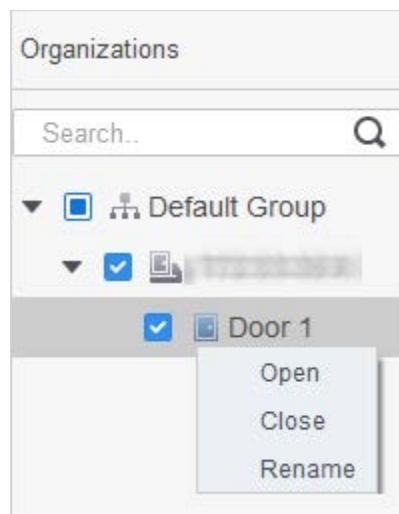
After access configuration, you can remotely control door through SmartPSS AC.

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

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

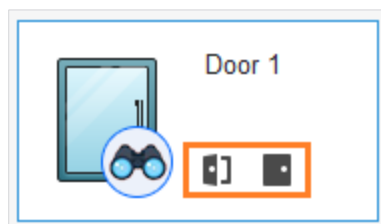
- Method 1: Select the door, right click and select **Open**.

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  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.

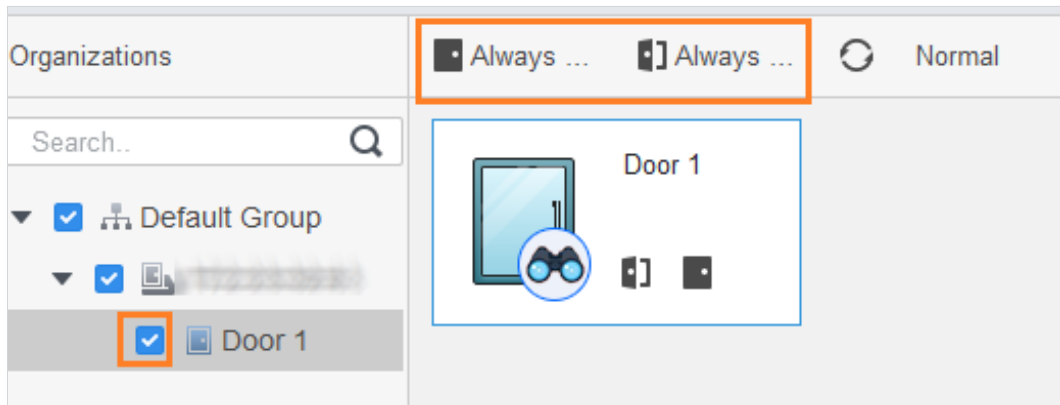
3.6.2 Setting Always Open and Always Close

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



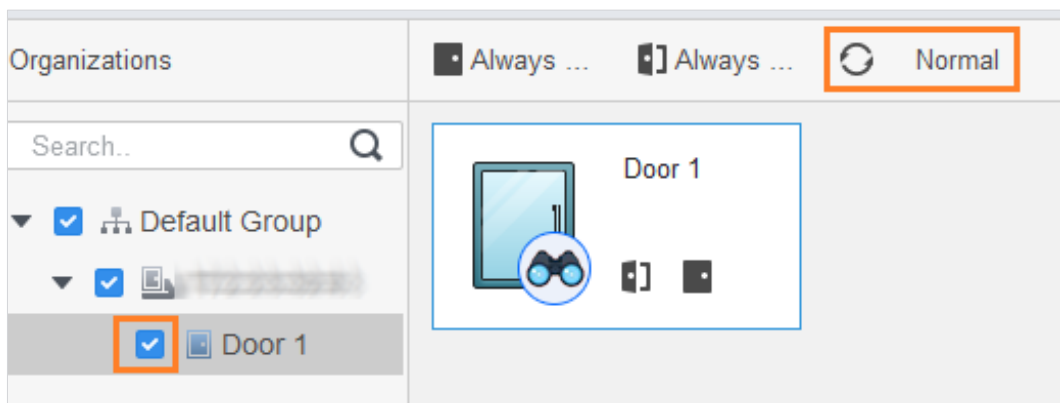
3.6.3 Resetting Door Status

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**. 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 Configuring Advanced Functions."

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

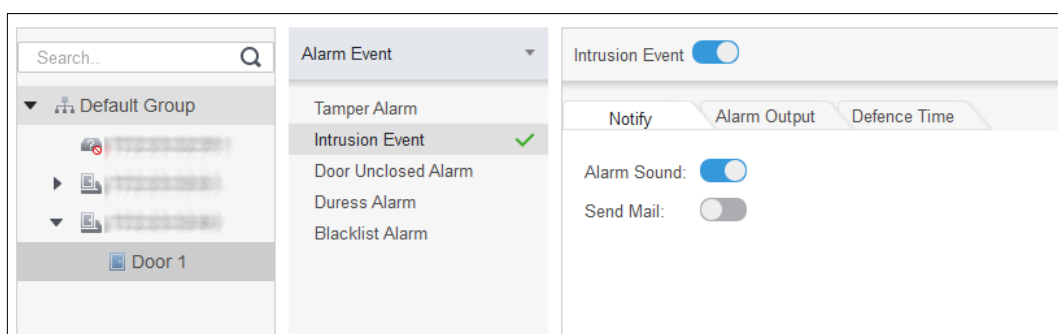
Step 2 Select the needed door and select **Alarm Event > Intrusion Event**.

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

Step 4 Configure intrusion alarm linkage actions as needed.

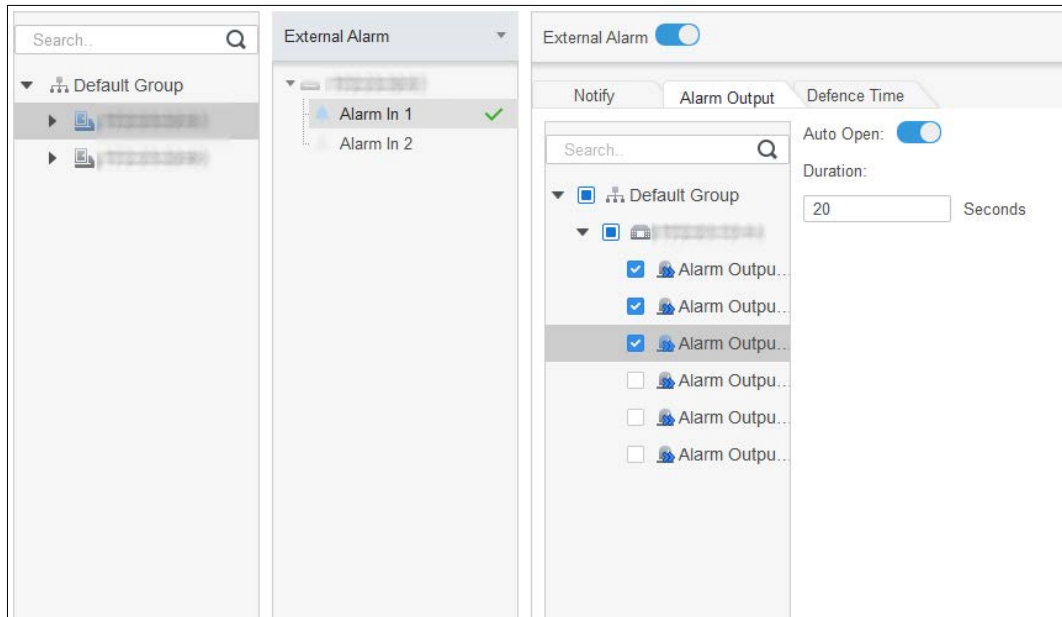
- Enable alarm sound.
Click the **Notify** tab, and click next to **Alarm Sound**. When intrusion event happens, the access controller warns with alarm sound.
- Send alarm mail.
 - 1) Enable **Send Mail** and confirm to set SMTP. The **System Settings** interface is displayed.
 - 2) Configure SMTP parameters, 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



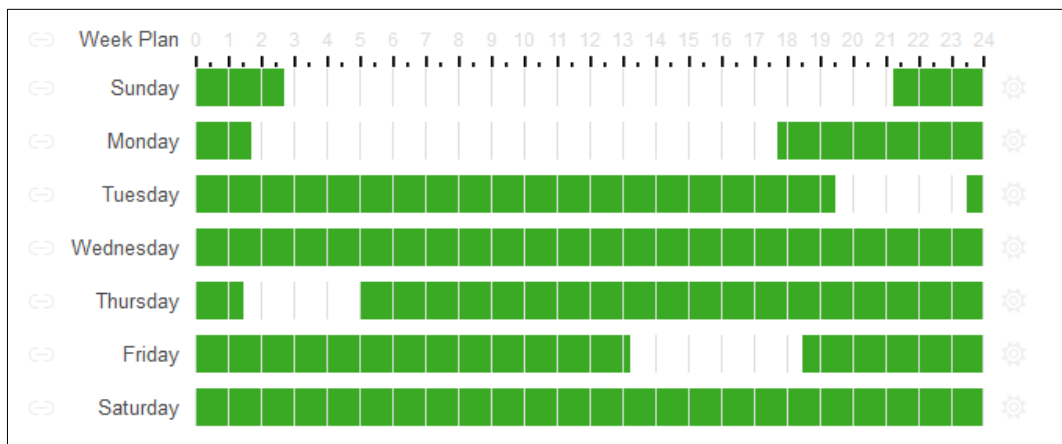
- Configure alarm I/O.
 - 1) Click the **Alarm Output** tab.
 - 2) Select the device which supports alarm in, select alarm-in interface, and then enable **External Alarm**.
 - 3) Select the device which supports alarm out, then select alarm-out interface.
 - 4) Enable **Auto Open** for the alarm linkage.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

Figure 3-29 Configure alarm linkage



- Set defense 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 defense.

Figure 3-30 Set defense time (method 1)




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

Figure 3-31 Set defence time (method 2)

The screenshot shows a dialog box titled "Time Editor" with a close button (X) in the top right corner. It contains six rows, each representing a "Timezone" (Timezone 1 through Timezone 6). Each row has two time input fields separated by a hyphen. The first field in each row has a small up/down arrow icon, and the second field also has a small up/down arrow icon. The values are: Timezone 1 (0:00:00 - 2:45:00), Timezone 2 (11:30:00 - 14:15:00), Timezone 3 (21:15:00 - 23:59:59), Timezone 4 (0:00:00 - 0:00:00), Timezone 5 (0:00:00 - 0:00:00), and Timezone 6 (0:00:00 - 0:00:00). Below the timezones is a "Check All" checkbox, which is checked. Underneath is a horizontal line, followed by seven day selection options: Sun (checked), Mon, Tue, Wed, Thu, Fri, and Sat, each with an unchecked checkbox. At the bottom right are two buttons: "OK" (blue) and "Cancel" (grey).

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 might 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.

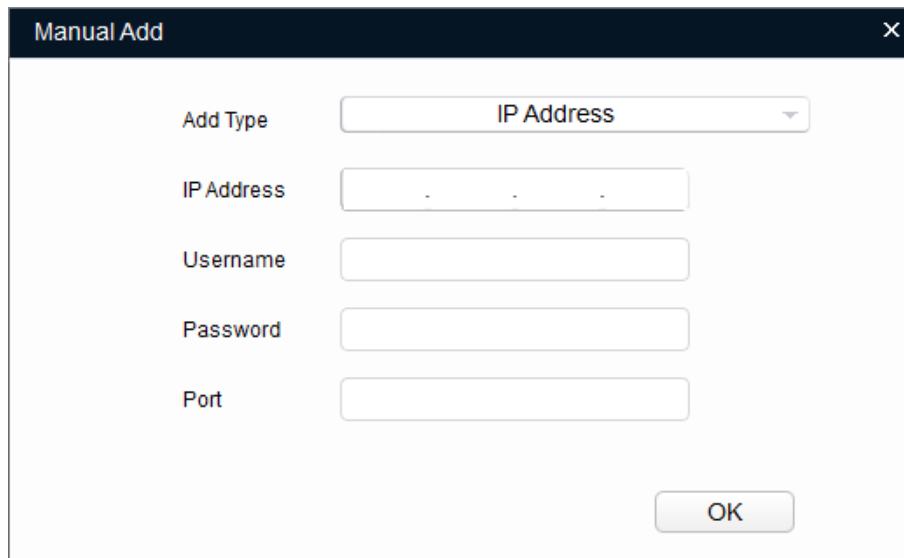
4.1.1 Adding One Device

Step 1 Click .

Step 2 Click **Manual Add**.

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

Figure 4-1 Manual add (IP address)



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.

Add Method	Parameter	Description
	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.

4.1.2 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 4-2 Setting

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

- Search current segment

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.

- Search other segment

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 the **Current Segment Search** and the **Other Segment Search** checkboxes together, the system searches devices under both conditions.
- The username and the password are the ones used to log in when you want to change 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 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 interfaces and parameters in this manual are for reference only, and might differ from the actual ones.

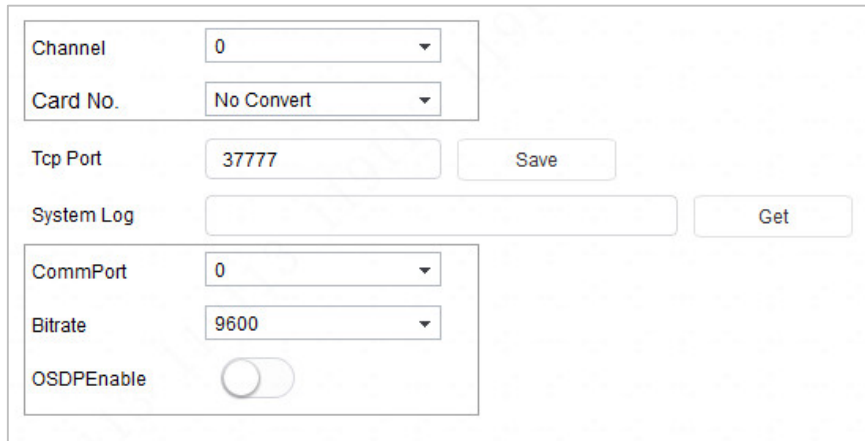
Step 1 Click  on the menu bar.

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 4-3 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 number. 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 9,600 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.


4.3 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 4-4 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.