Access Controller

User's Manual

V1.0.1

Foreword

General

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

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Time
V1.0.1	Added initialization process.	December 2021
V1.0.0	First release.	September 2020

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 device.
- 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 Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, comply with the guidelines when using it, and keep the manual safe for future reference.

Transportation Requirement

⚠

Transport the Device under allowed humidity and temperature conditions.

Storage Requirement

⚠

Store the Device under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the Device 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 Device.
- Do not connect the Device to two or more kinds of power supplies, to avoid damage to the Device.
- 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 Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Install the Device on a stable surface to prevent it from falling.
- Install the Device 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 Device label.
- The device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.

Operation Requirements

⚠

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the Device while the adapter is powered on.
- Operate the Device within the rated range of power input and output.
- Use the Device under allowed humidity and temperature conditions.
- 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 it.
- Do not disassemble the Device without professional instruction.

Table of Contents

1 Overview

1.1 Introduction

The Device 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.

1.2 Features

- Using PC+ABS as material, the appearance is high-end and neat.
- Supports TCP/IP network communication, communication data is encrypted for security.
- Supports OSDP protocol.
- Supports PoE function.
- 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, illegal 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, data can be stored locally after the network is disconnected, and continue to upload after the network is restored.
- Supports 128 periods, 128 holiday plans, 128 holiday periods, normally open periods, normally closed periods, remote unlock periods, first card unlock periods, and support unlock in periods.
- Supports watchdog guard mechanism to ensure the operation stability.
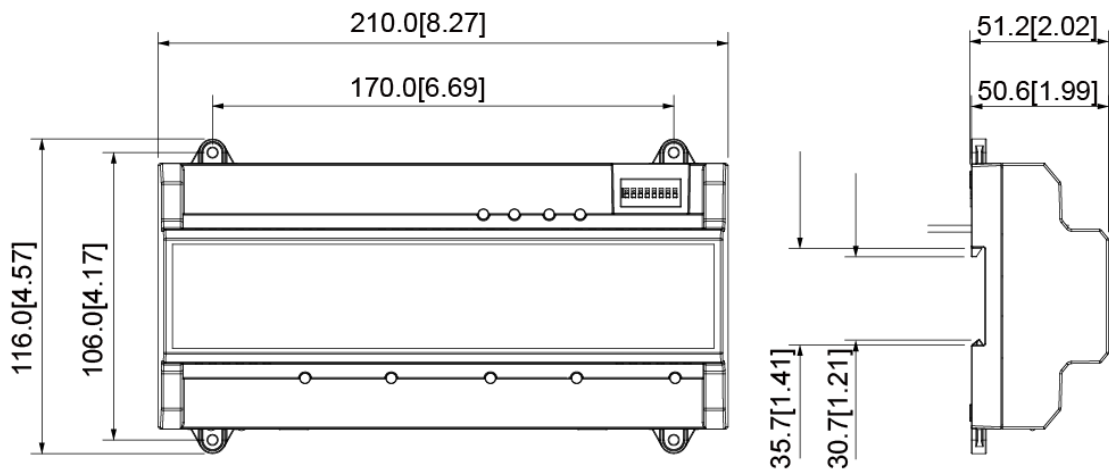
1.3 Dimensions

Two-door One-way Access Controller

Figure 1-1 Dimensions (two-door one-way) (mm [inch])
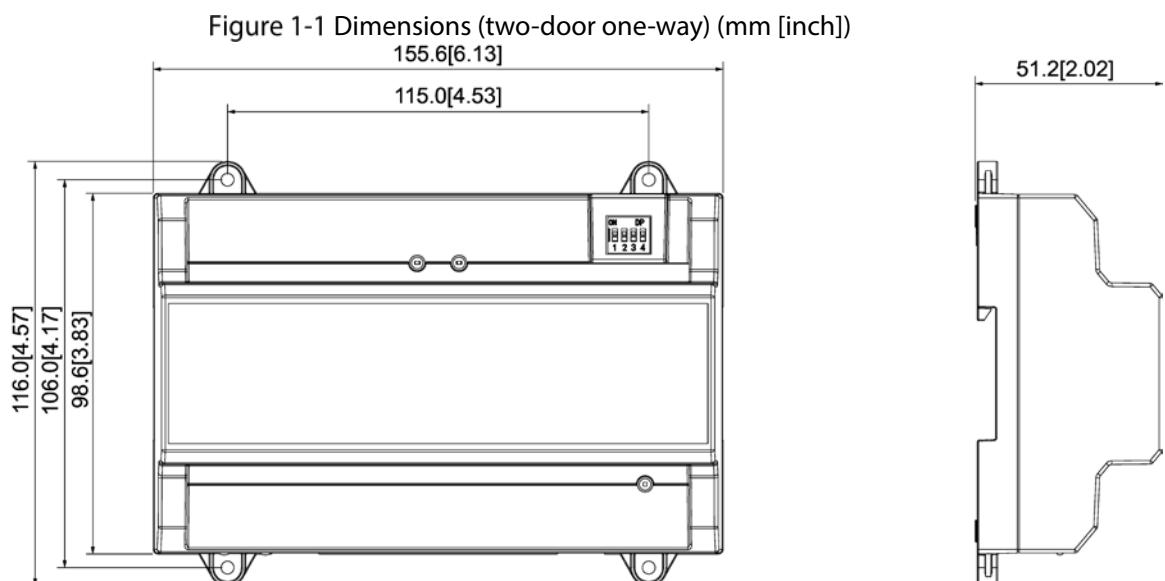
Two-door Two-way/Four-door One-way Access Controller

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

1.4 Components

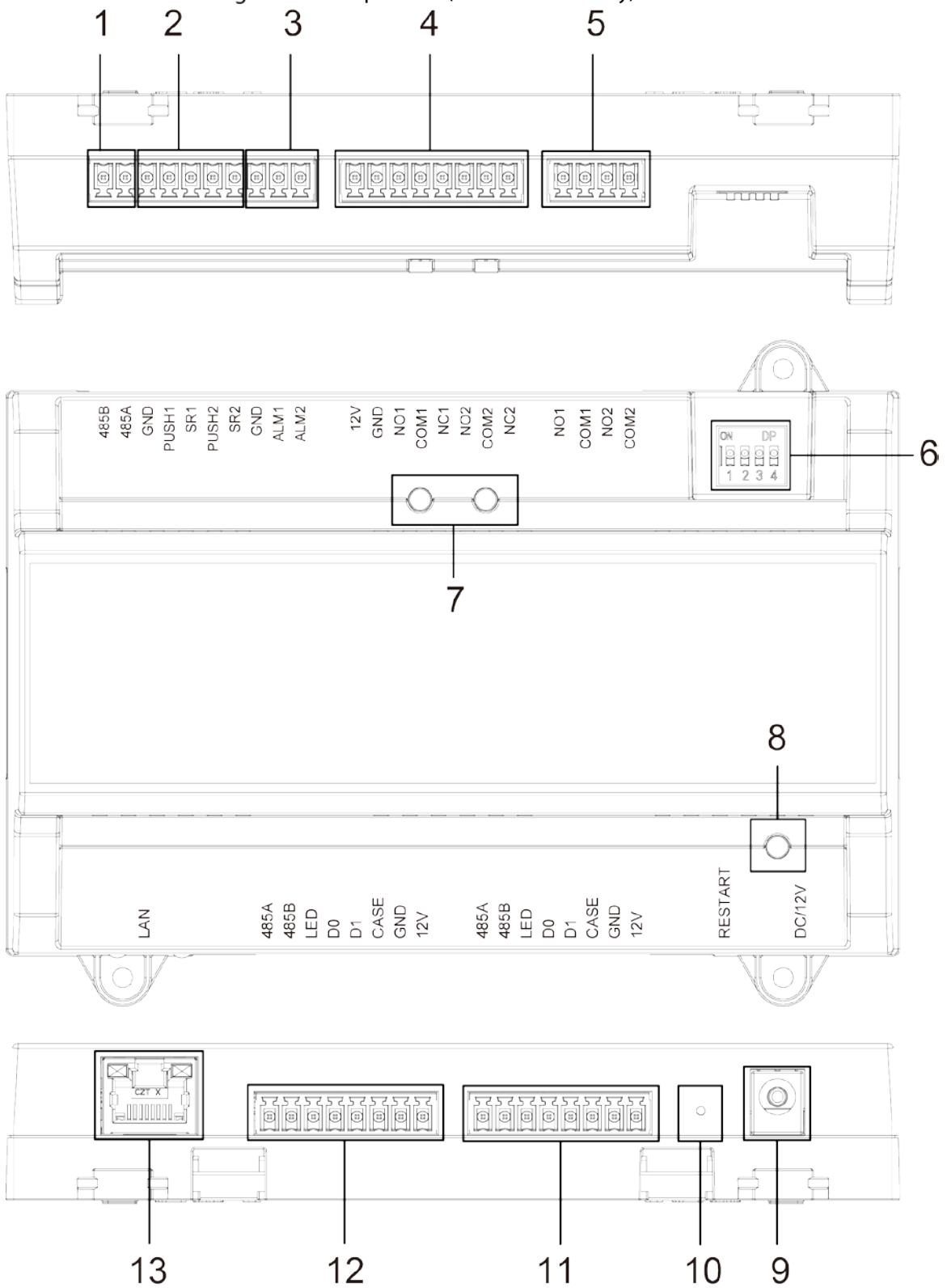Two-door One-way Access Controller

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

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

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

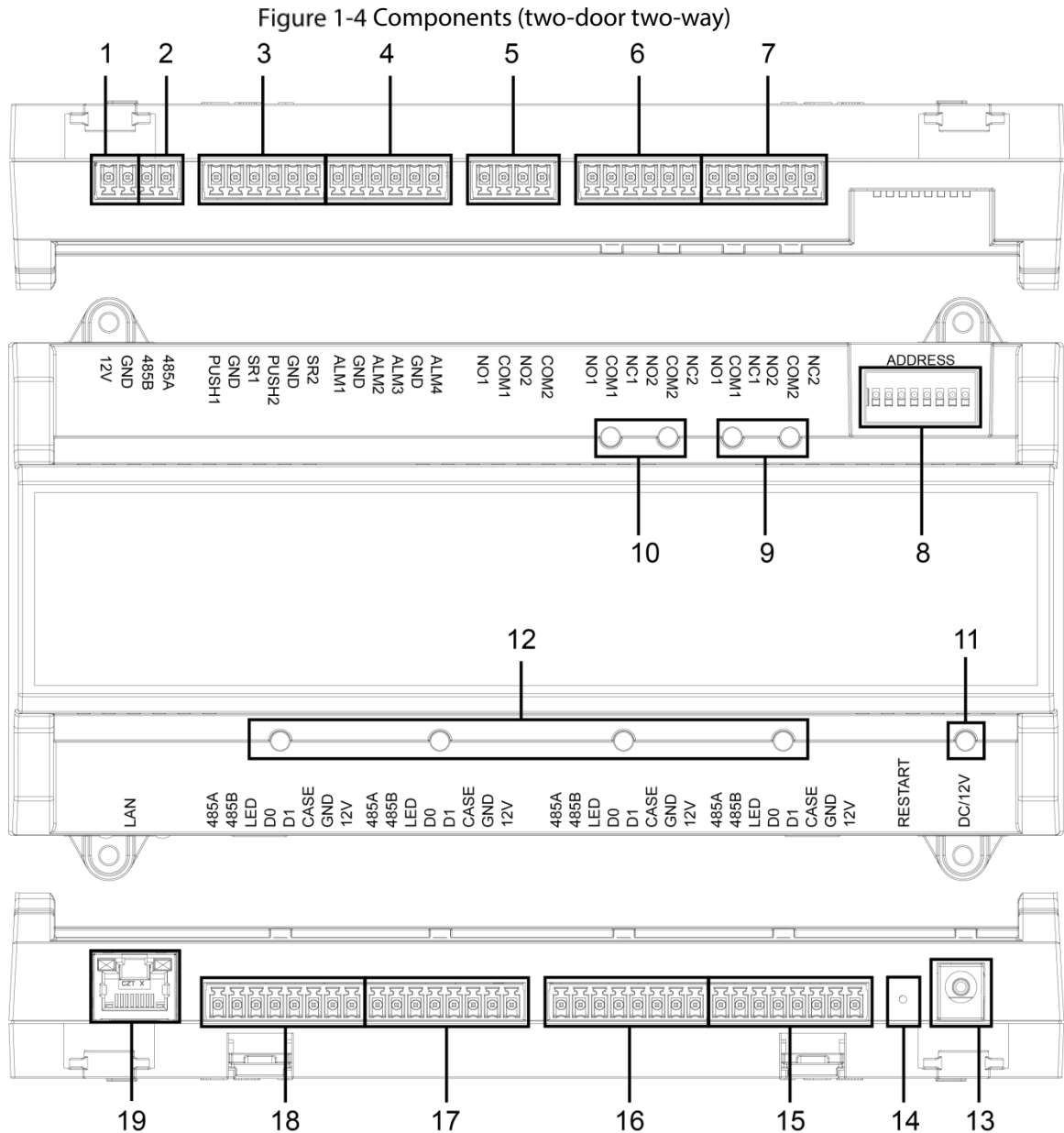| No.	Name	No.	Name
3	Alarm IN port	10	Restart button
4	Door lock OUT port	11	Entrance card reader port of No.2 door
5	Alarm OUT port	12	Entrance card reader port of No.1 door
6	DIP switch	13	Network port
7	Indicator light of door lock	14	—

Two-door Two-way Access Controller

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

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

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

No.	Name	No.	Name
6	Door lock control OUT port	16	Entrance card reader port of No.2 door
7	Internal alarm OUT	17	Exit card reader port of No.1 door
8	DIP switch	18	Entrance card reader port of No.1 door
9	Alarm indicator light	19	Network port
10	Door lock indicator light	—	—

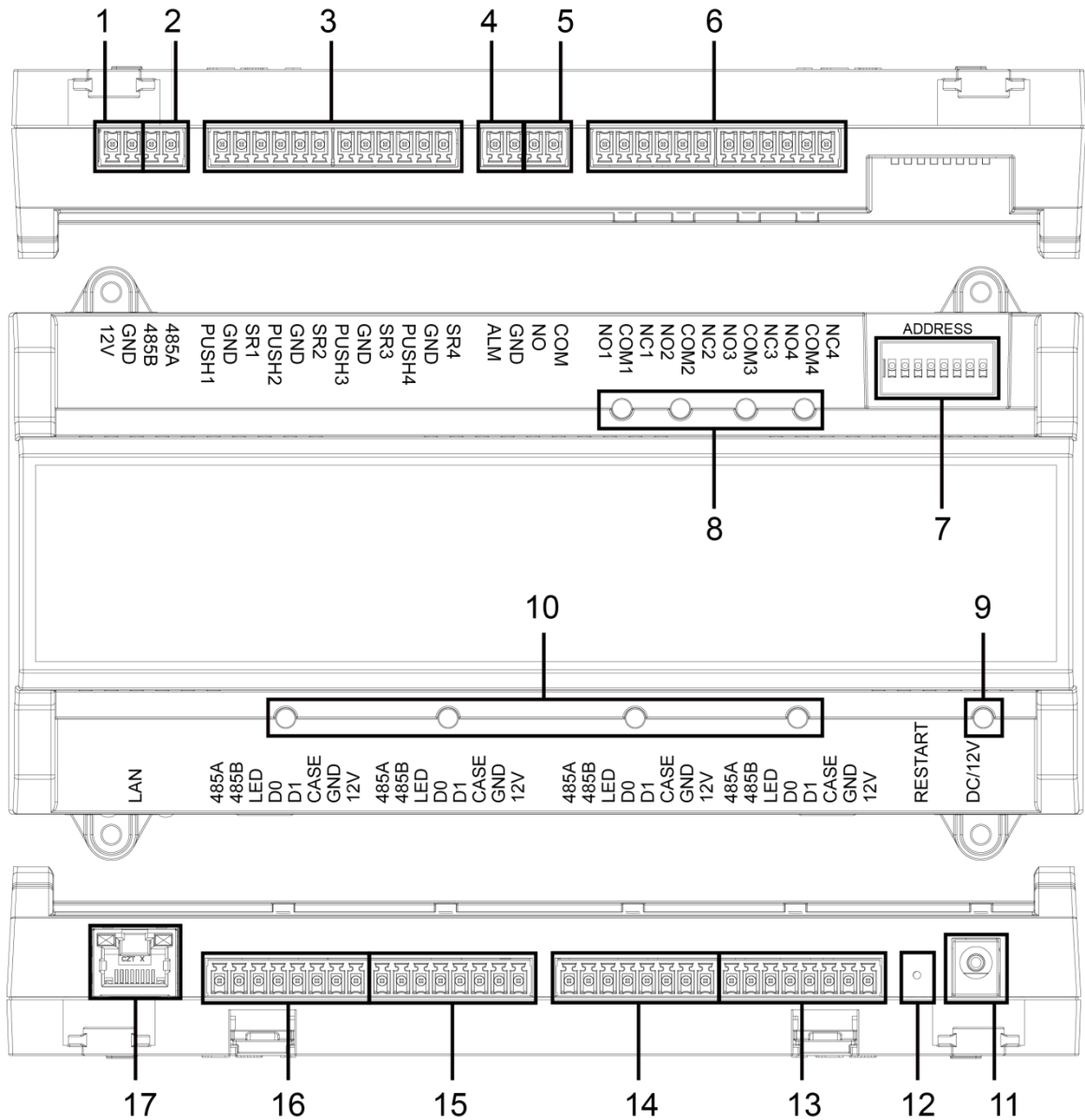## Four-door One-way Access Controller

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

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

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

No.	Name	No.	Name
5	Alarm OUT port	14	Entrance card reader port of No.3 door
6	Door lock control OUT port	15	Entrance card reader port of No.2 door
7	DIP switch	16	Entrance card reader port of No.1 door
8	Door lock indicator light	17	Network port
9	Power indicator light	—	—

Port

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

Indicator Light

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

DIP Switch

Perform corresponding operation through DIP switch.

Means 1; ■ means 0.

Figure 1-6 DIP switch (two-door one-way access controller)
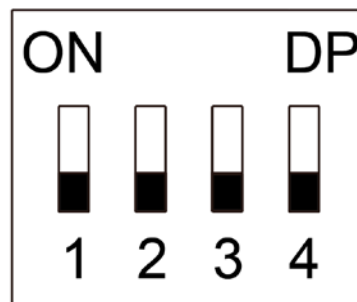
- 1–4 are all 0, the Device starts normally after power-on.
- 1–4 are all 1, the Device enters to boot mode after power-on.
- 1 and 3 are 1, 2 and 4 are 0, the Device restores to factory defaults after restart.
- 2 and 4 are 1, 1 and 3 are 0, the Device restores to factory defaults after restart. But user information will be retained.

Figure 1-7 DIP switch (two-door two-way/four-door one-way access controller)
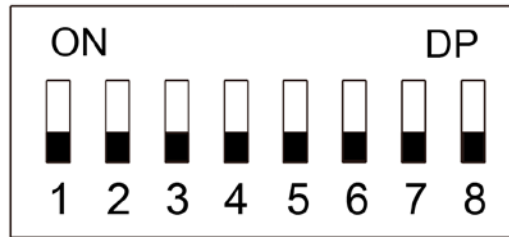
- 1–8 are all 0, the Device starts normally after power-on.
- 1–8 are all 1, the Device enters to boot mode after power-on.
- 1, 3, 5 and 7 are 1, 2, 4, 6 and 8 are 0, the Device restores to factory defaults after restart.
- 1, 2, 4, 6 and 8 are 1, 1, 3, 5 and 7 are 0, the Device restores to factory defaults after restart. But user information will be retained.

Restart

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

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

1.5 Application

Two-door One-way Access Controller

Figure 1-8 Application (two-door one-way)
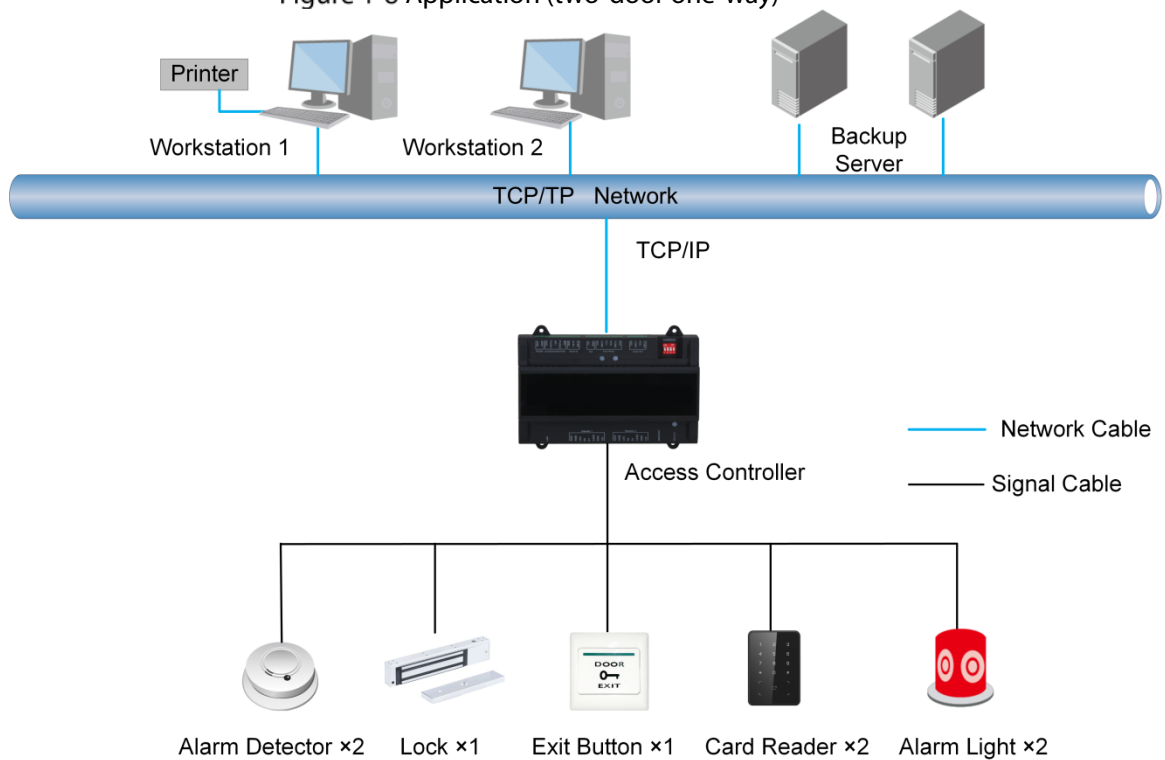
Two-door Two-way Access Controller

Figure 1-9 Application (two-door two-way)
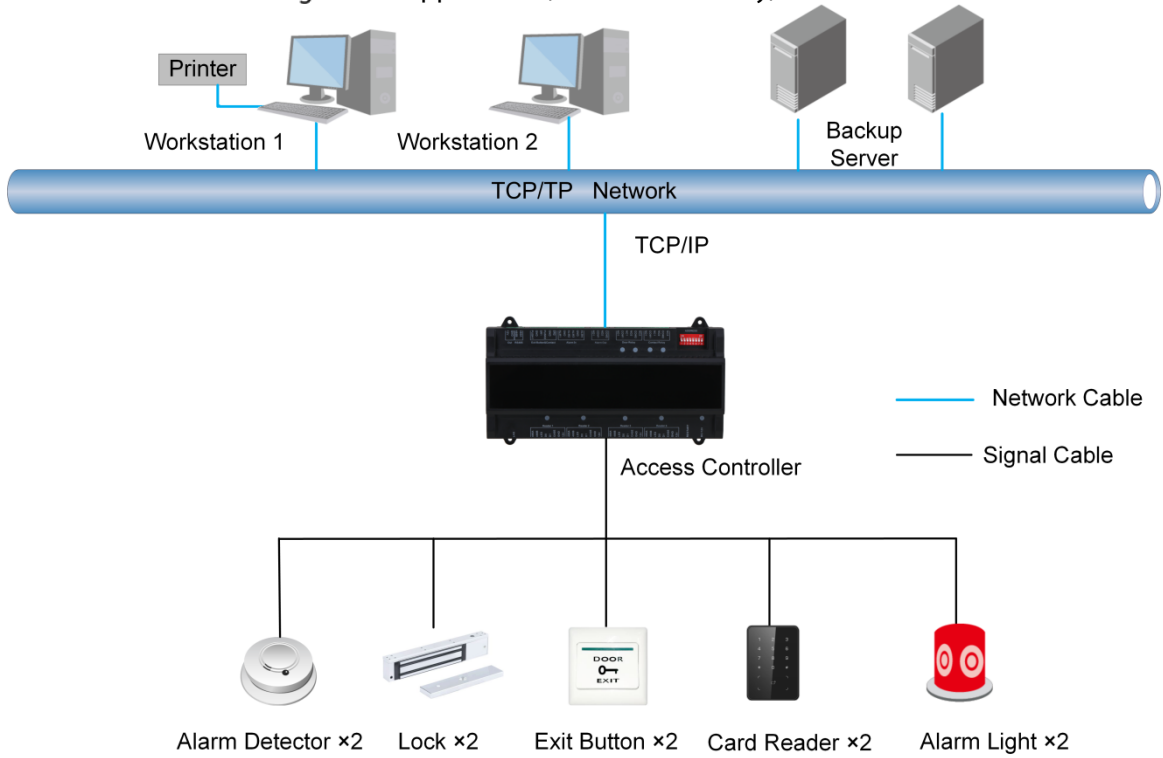
Four-door One-way Access Controller

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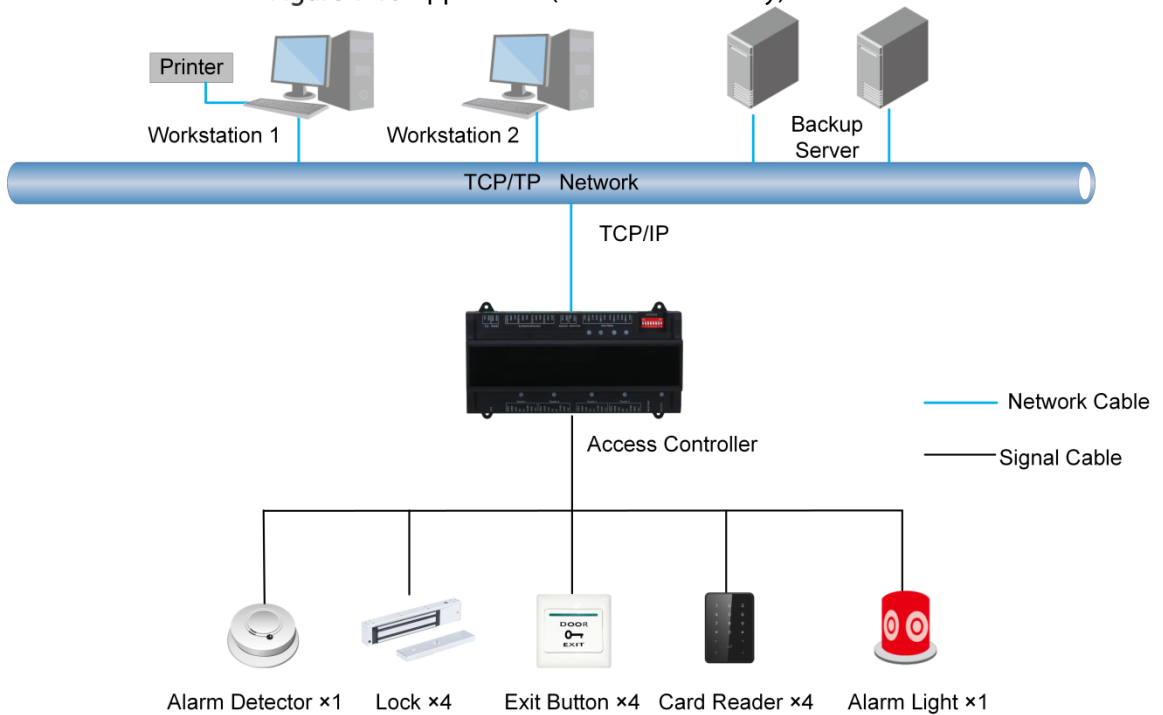
2 Installation

2.1 Cable Connection

Two-door One-way Access Controller

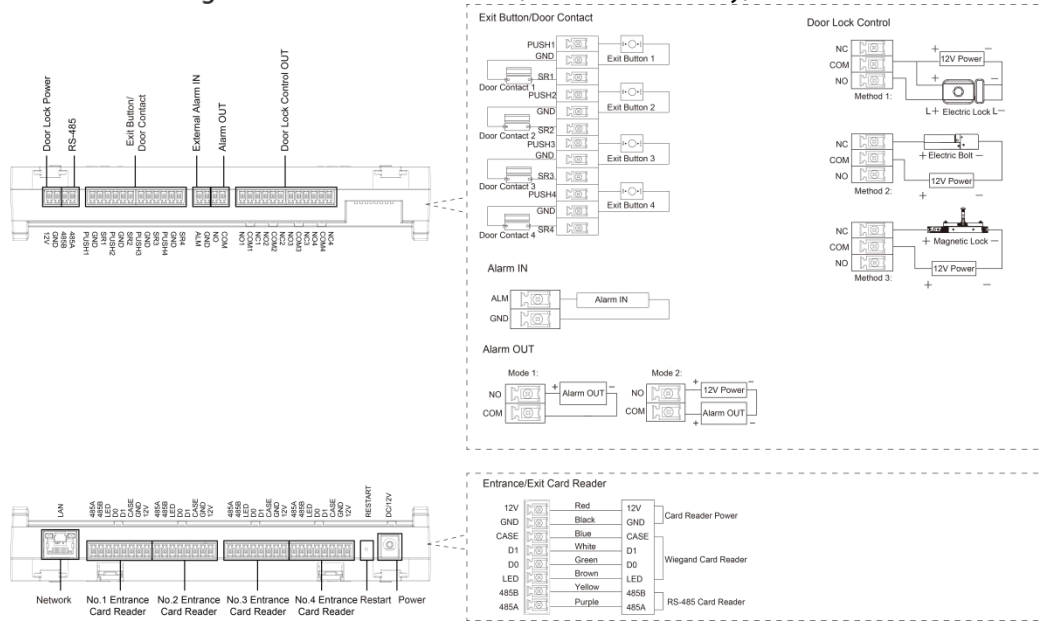Figure 2-1 Cable connection (two-door one-way)
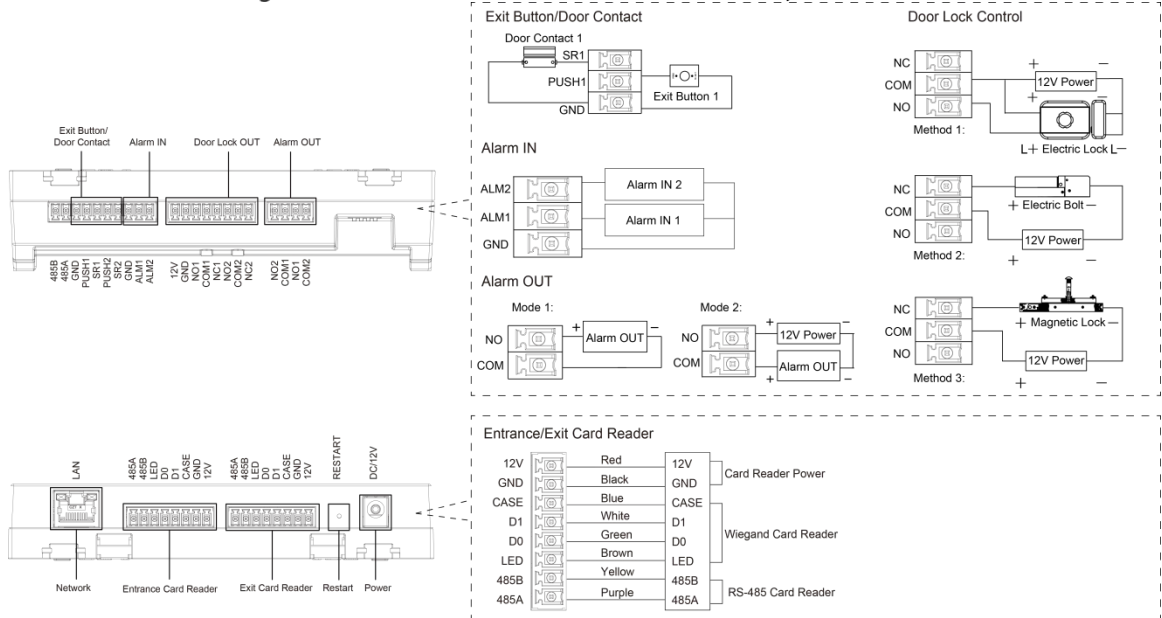
Two-door Two-way Access Controller

Figure 2-2 Cable connection (two-door two-way)
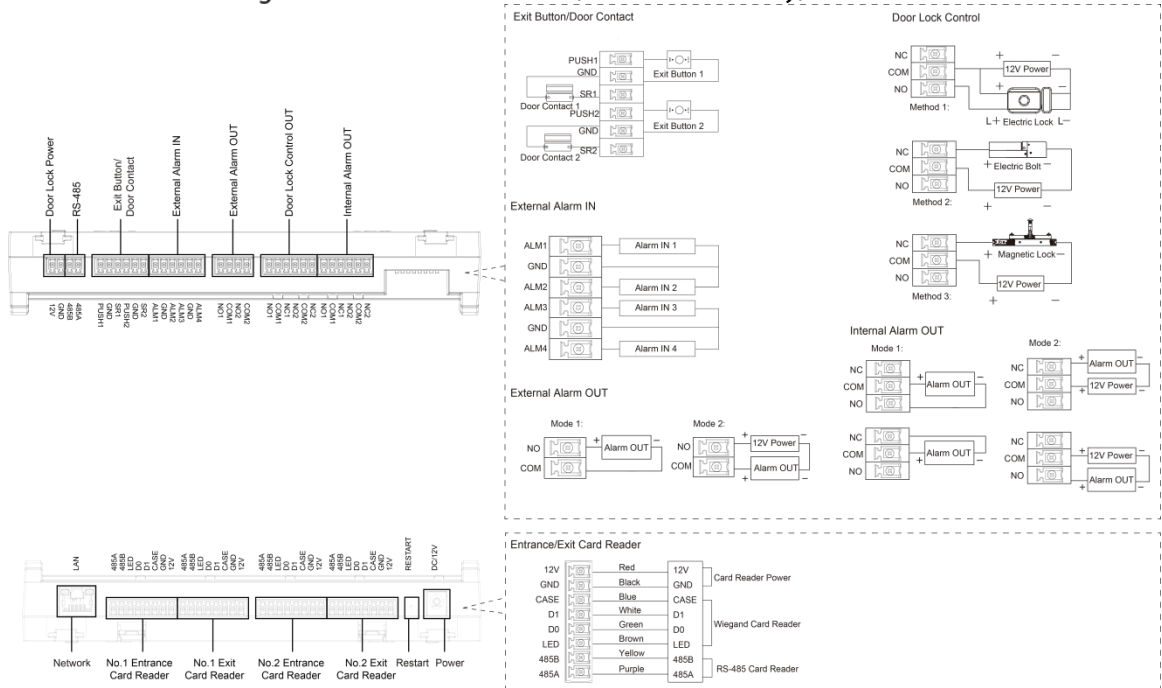
Four-door One-way Access Controller

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

2.1.1 Cable Connection of Alarm Input

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

Table 2-1 Cable connection of alarm input

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

2.1.2 Cable Connection of Alarm Output

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

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

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

Table 2-2 Cable connection of alarm output

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

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

2.1.3 Cable Connection of Card Reader

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

Table 2-3 Cable specification and length of card reader

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

2.2 Installing the Device

There are two installation methods.
- Fix the Device on wall with screws.
- Install U-shaped guide rail (not provided) on wall, and then hang the Device to the guide rail.

Figure 2-4 Installation (1)
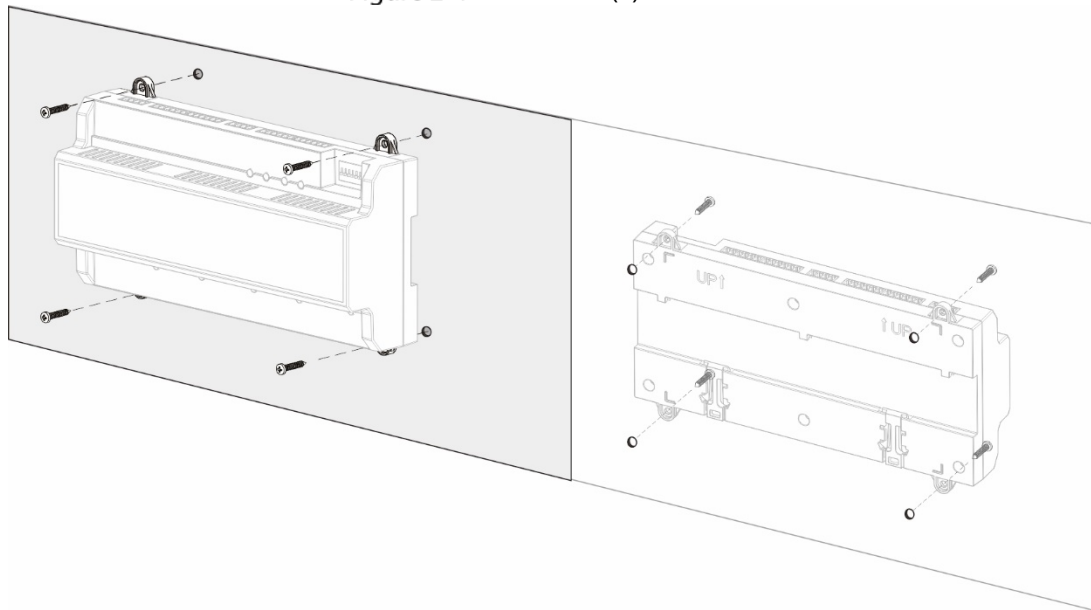
Figure 2-5 Installation (2)
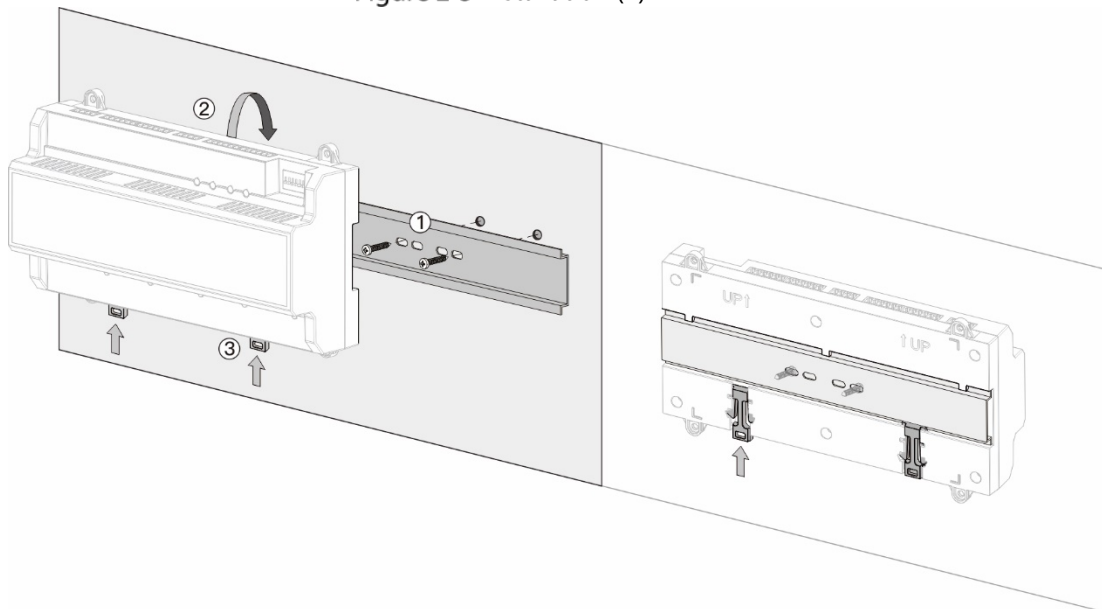
Step 1   Fix the U-shaped guide rail on wall with screws.
Step 2   Buckle the upper back part of the Device into the U-shaped guide rail.
Step 3   Push up the buckle on the lower part of the Device until you hear a click sound.

2.3 Removing the Device

If the Device is installed with the second installation method, please refer to Figure 2-6 when you want remove the Device.

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

Figure 2-6 Remove the Device
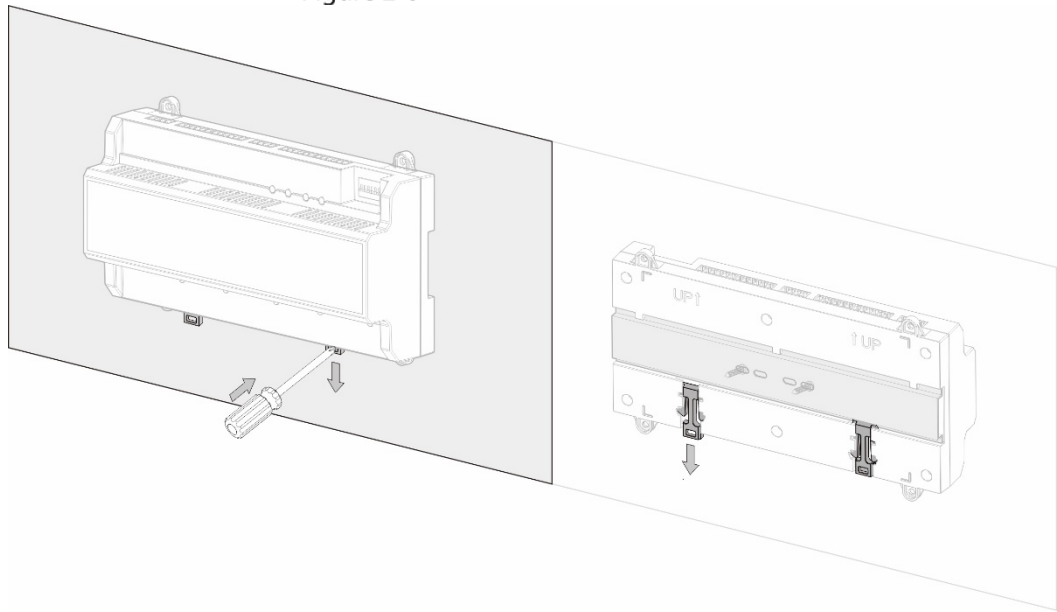
3 SmartPSS AC Configuration

You can manage the Device through SmartPSS AC. This section mainly introduces quick configuration of devices. 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 [icon], and then follow the instructions to finish the initialization and log in.

3.2 Initialization

Before initialization, make sure the device 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
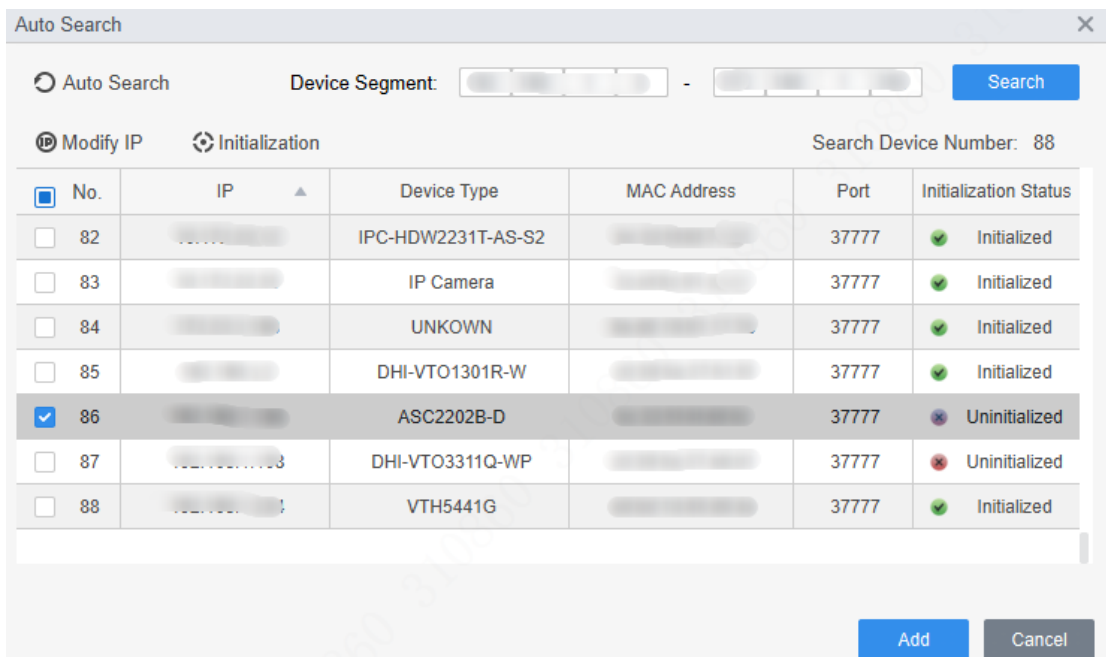
Step 2   Enter a network segment range, and then click **Search**.

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. For details, see "1.4 Components".

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 Device to SmartPSS AC. You can add devices in batches by auto search or add devices individually.

3.3.1 Auto Search

We recommend you add devices by auto search when you need to add devices in batches on the same network segment, or when you know the network segment range instead of the exact IP address.

Step 1   Log in to SmartPSS AC.

Step 2   Click **Device Manager** at the lower left corner.

Figure 3-4 Devices
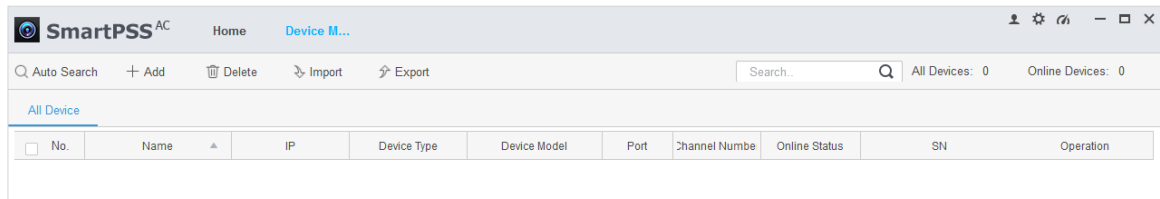
Step 3   Click **Auto Search**.

Figure 3-5 Auto search
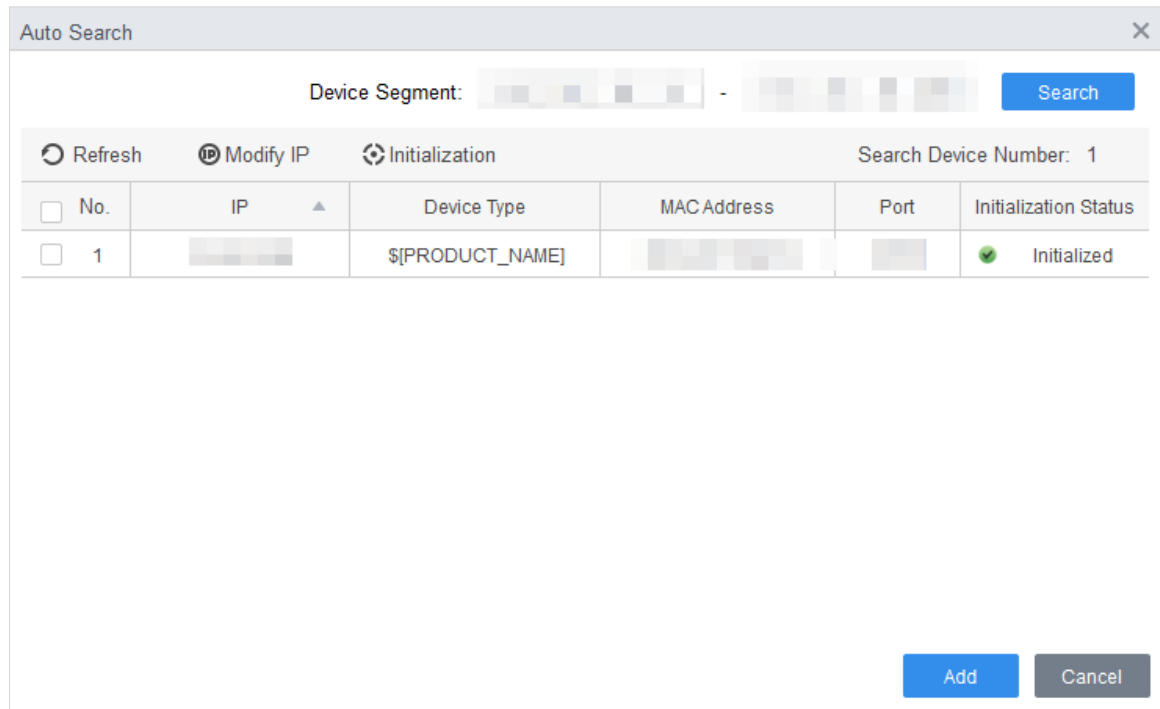
Step 4   Enter the network segment, and then click **Search**.

📖

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

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.

📖

- The username is admin and password is admin123 by default. We recommend you modify the password after login.
- After successful login, the device status displays **Online**. Otherwise, it displays **Offline**.

3.3.2 Manual Add
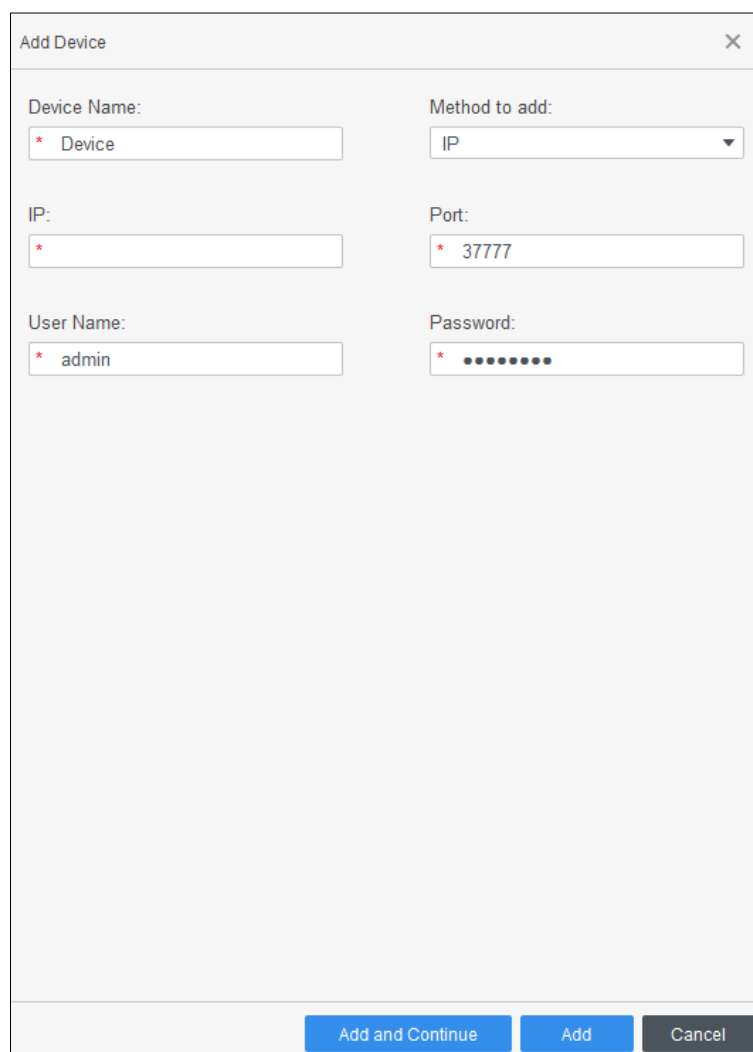
You can add devices manually. You need to know the IP addresses and domain names of the access controller that you want to add.

Step 1   Log in to SmartPSS AC.

Step 2   Click **Device Manager** at the lower left corner.

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

Figure 3-6 Manual add

Step 4 Enter the device information.

Table 3-1 Parameters

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

Step 5 Click **Add**, and then you can see the Device 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

3.4.1 Card Type Setting

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

⚠️

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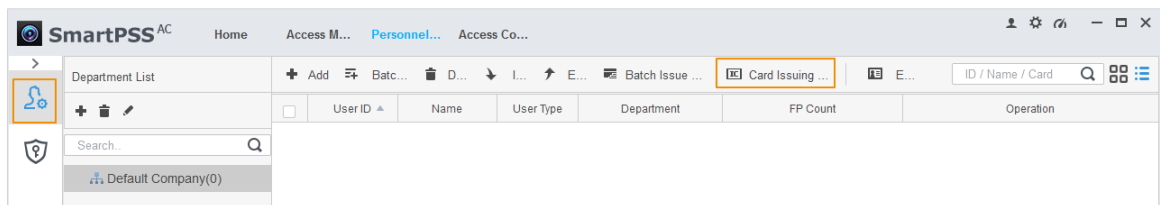
Step 3 On the **Personnel Manager** page, click 🗂️, and then click 🔲.

Step 4 On the **Setting Card Type** page, 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
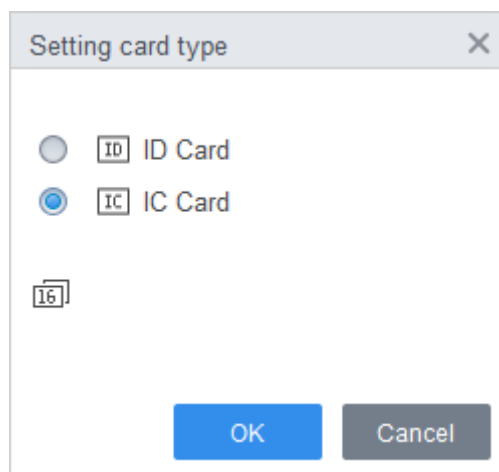
Step 6 Click **OK**.

3.4.2 Adding User

3.4.2.1 Adding Manually

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

1) Click ⚙ to select **Device** or **Card issuer** as card reader.

2) Add card. The card number must be added if the non-second generation access controller is used.

3) After adding, you can select the card as main card or duress card, or replace the card with new one, or delete the card.

● Configure fingerprint.

1) Click ⚙ to select **Device** or **Fingerprint Scanner** as fingerprint collector.

2) Add fingerprint. Click **Add Fingerprint** and press finger on the scanner three times continuously.

Figure 3-10 Configure certification

Step 5 Configure permission for the user.

For details, see "3.5 Permission Configuration".

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.

Step 4 Set the start number, card quantity, effective time and expired time of card.

Step 5 Click **Issue** to assign access cards to users.

The card number will be read automatically.

Step 6 Click **Stop** after assigning card, and then click **OK**.

Figure 3-12 Add user in batches

Step 7   In the list of user, click to modify information or add details of users.

3.5 Permission Configuration
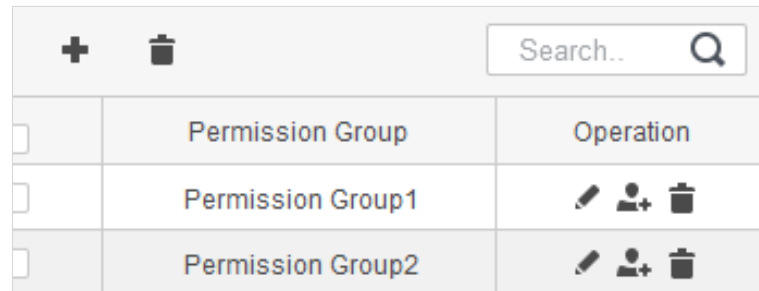
3.5.1 Adding Permission Group

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

	Permission Group	Operation
	Permission Group1	✏ 👤+ 🗑
	Permission Group2	✏ 👤+ 🗑

Step 3   Click ✚ to add a permission group.

Step 4   Set permission parameters.

    1)   Enter group name and remark.

    2)   Select a time template.

        📖

        For details, see SmartPSS AC user manual.

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

Figure 3-14 Add permission group

Step 5   Click **OK**.

On the **Permission Group List** page:

● Click ![trash icon] to delete group.

● Click ![pencil icon] to modify group info.

● Double-click permission group name to view group information.

3.5.2 Assigning Access Permissions

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.

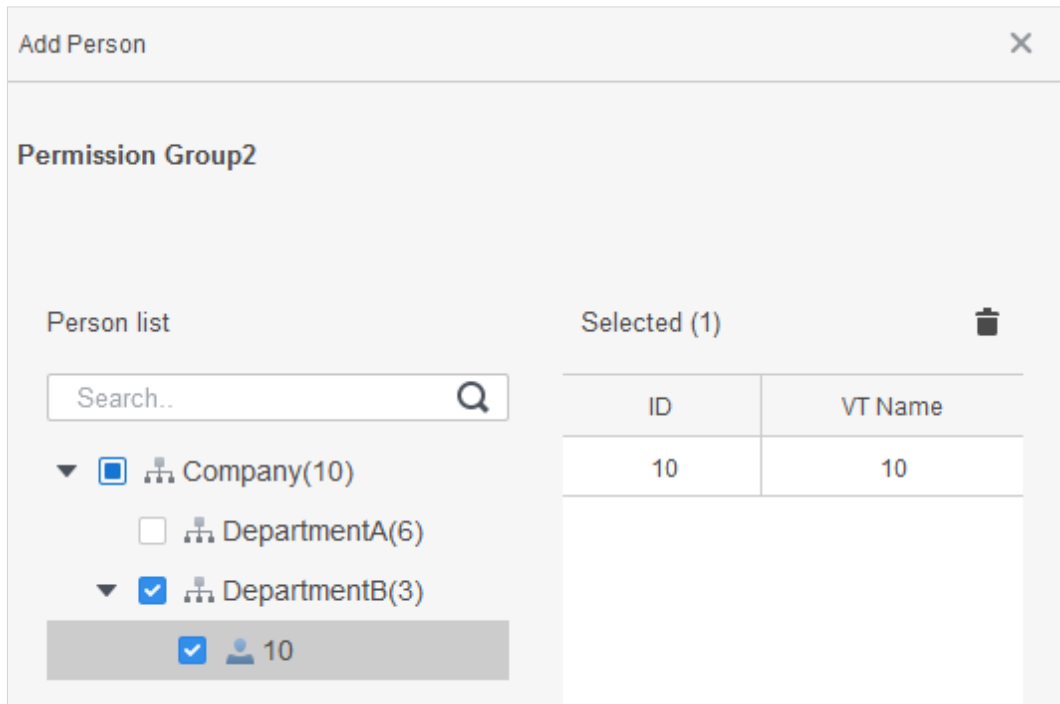Step 2   Click **Personnel Manger** > **Permission Configuration**.

Step 3   Select a permission group, and then click ![add person icon].

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 Advanced Functions Configuration

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 permission should be the **General** user type and have access to certain doors. For details, see "3.4.2 Adding User."
- For details of permission assignment, see "3.5 Permission Configuration."

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

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

Step 3   Click **Add**.

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

Figure 3-16 First card unlock configuration

Table 3-2 Parameters of first card unlock

Parameter	Description
Door	Select the door for first-card permission.

Parameter	Description
Timezone	First-card permission is only valid during the selected time template.
Status	After first card unlock is enabled, select the door status: **Normal mode** or **Always Open mode**.
User	You can select one or multiple first-card holders.

Step 5 (Optional) Click [icon]. The icon changing into [icon] 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 "3.4.2 Adding User."
- For details of permission assignment, see "3.5 Permission Configuration."
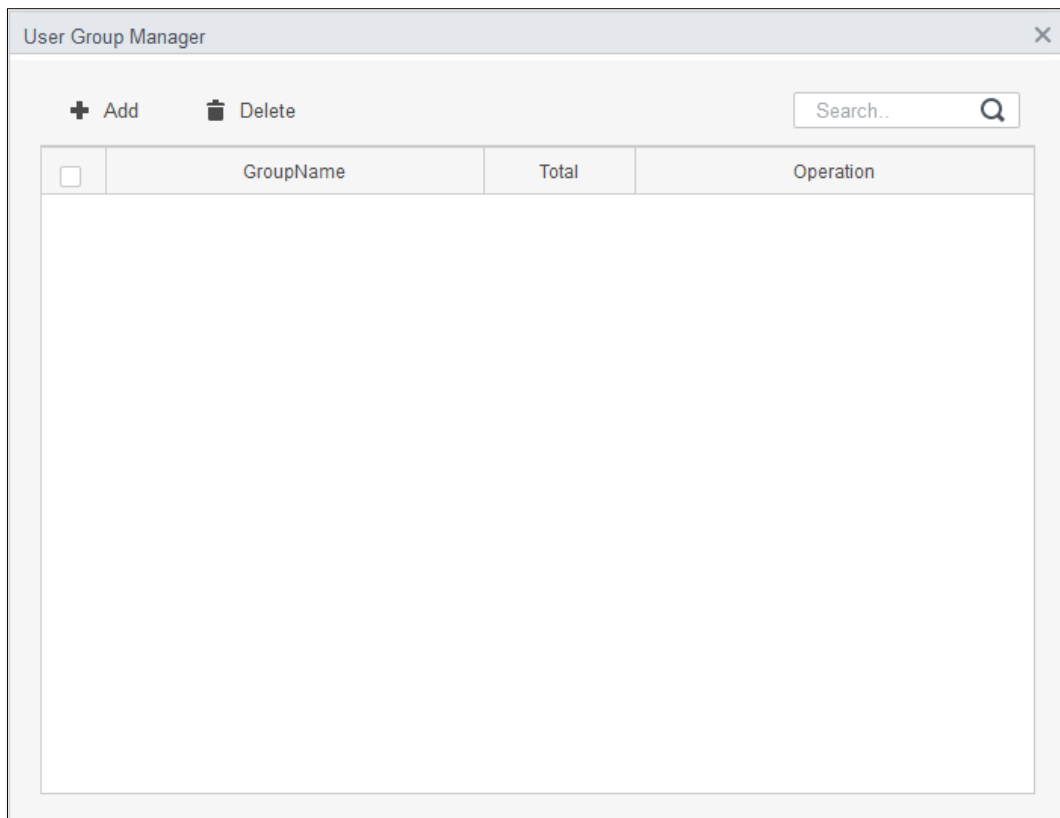
Step 1 Select **Access Configuration** > **Advanced Config**.

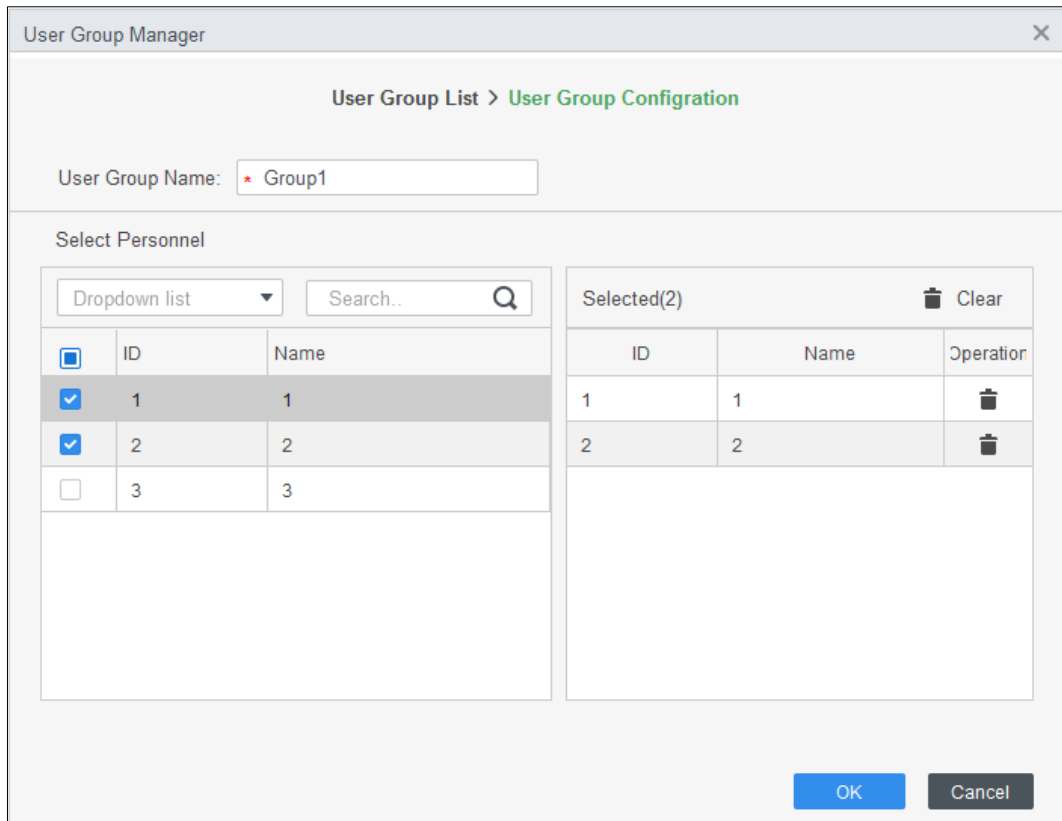Step 2 Click the **Multi Card Unlock** tab.

Step 3 Add user group.

1) Click **User Group**.

Figure 3-17 User group manager
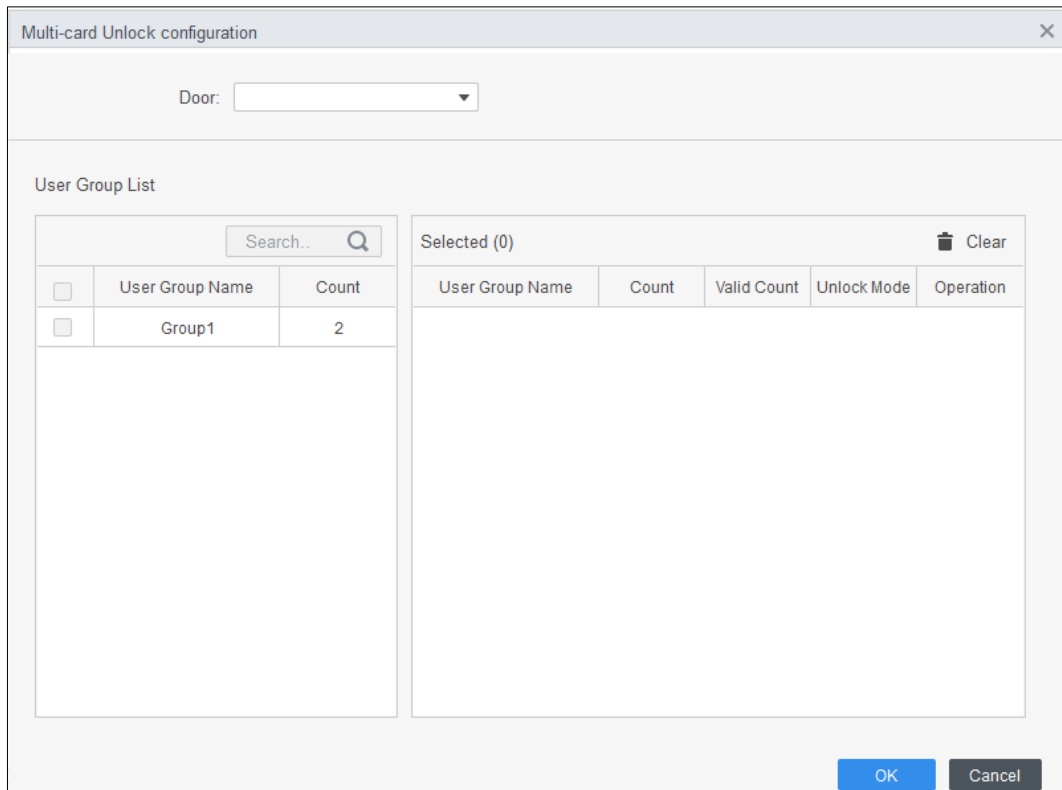

2) Click **Add**.

Figure 3-18 User group configuration

3) Enter the user group name. Select users from the user list and click **OK**. You can select up to 50 users in one group.
4) Click ☒.

Step 4 Configure parameter 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** in each group. Click 🔼 or 🔽 to adjust the group sequence to verify identity.

📖

- The valid count refers to the number of users in each group that must be present to verify their identities to unlock the door. Take Figure 3-20 as an example. The door can be unlocked only after one user in the group 1 swipe the card first and two users in group swipe their cards.
- Up to five valid users in total are allowed.

5) Click **OK**.

Step 5 (Optional) Click 🔘. The icon changing into 🔵 indicates **Multi Card Unlock** is enabled. The **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.
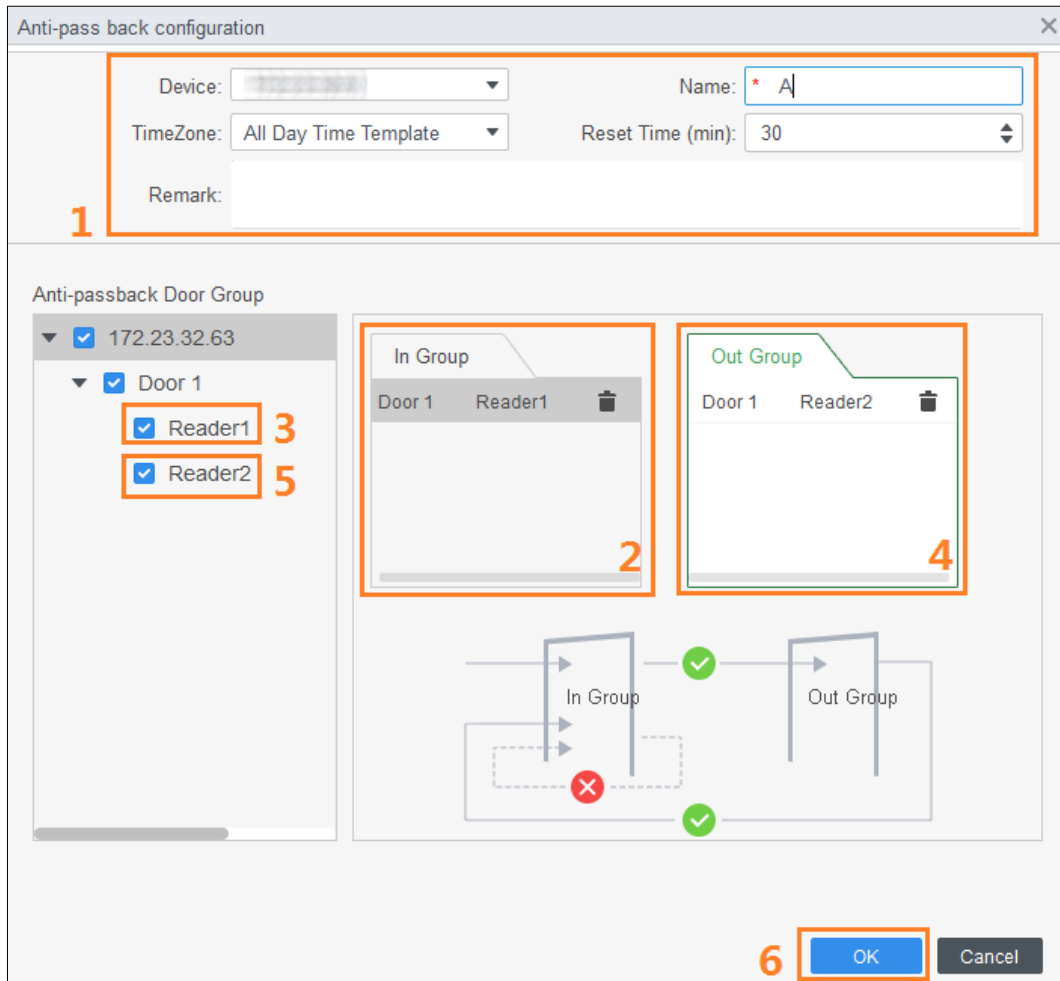
Step 1 Select **Access Configuration** > **Advanced Config**.

Step 2 Click **Add**.

Step 3 Configure parameters.

1) Select device and enter device name.
2) Select time template.
3) Set rest time.

   For example, set the reset time as 30 minutes. If a person swipes in but not swipes out, the anti-pass back alarm will be triggered when the person attempts to swipe in again within the 30 minutes. They can enter the controlled area until the defined time period has passed.
4) Click **In Group** and select the entry reader, and then click **Out Group** and select the exit reader.
5) Click **OK**.

Figure 3-21 Anti-pass back configuration

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

3.6.1.4 Door Interlock

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 a device and enter the device name.

2) Enter remark.

3) Click **Add** twice to add two door groups.

4) Add doors to door groups.

5) Click **OK**.

Figure 3-22 Inter-door lock configuration

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

3.6.2 Access Controller Configuration

You can configure access door, such as entry reader and exit reader, and door status.

<u>Step 1</u>   Select **Access Configuration** > **Access Config**.

<u>Step 2</u>   Click the door.

<u>Step 3</u>   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	Click ⇌ to set entry and exit reader.
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 and the door will remain open during the defined period.
Keep Close Timezone	Select time template and the door will remain closed during the defined period.
Alarm	Enable alarm function and set alarm type, including intrusion, overtime and duress. When alarm function is enabled, the SmartPSS-AC will receive alarm messages when the alarm is triggered.
Door Sensor	Enable door sensor so that you can know the actual door status. We recommend you enable the function.
Administrator Password	Enable and set the administrator password. You can access by entering the password.
Remote Verification	Enable the function and set the time template. The access must be granted from the SmartPSS-AC when a user attempts to unlock the door after valid identity verification.

Parameter	Description
Remote Channel	Link video channel with access channel. You can view the real-time video of the access channel.
Unlock Hold Interval	The time during which the door remains open after the door is unlocked. The door will auto close when the predefined time is over.
Close Timeout	An alarm is triggered when the door remains open beyond the defined period. For example, set the close timeout as 60 seconds. If the door remains open for more than 60 seconds, the alarm is triggered.
Unlock Mode	Select the unlock mode. **And:** Verify all the selected unlock methods to open the door. **Or**: Verify one of the selected unlock methods to open the door. **Unlock by time period**: Users can only unlock the door through predefined unlock methods and based on the time schedules.
Memory Mode	After swiping card once, more than one person can pass the turnstile. There are two modes: Off (default) and On. If several people are granted access through the turnstile, and one of them did not start to pass the turnstile in 5 seconds, or one of them did not pass the turnstile within defined duration and stay overtime between the turnstiles, the swing barriers will be locked. At this time, you need to swipe cards several times to allow several people pass the turnstile continuously. In the memory mode, if card swiping interval exceeds a single person passing duration, the memory function will not be triggered. The interval between two identity verifications must be longer than the unlock duration of the access controller or the face recognitions access controller; otherwise, only one identity verification will be counted. The recommended identity verification interval is 2 s to 5 s. In the memory mode, at most 255 people can pass the turnstile continuously.
Second Unlock	After people entered the turnstile and triggered alarms, they do not need to step backwards and can get identities verified. 📖 Only turnstiles supports memory mode and second unlock functions.

Step 4   Click **Save**.

3.6.3 Viewing History 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   Click **Access Configuration** > **History Event** on the homepage.
Step 2   Click **Access Manager**.
Step 3   Extract events from door device to the local. Click **Extract**, set the time, select the device, and
then click **Extract Now**.

☐
You can select multiple devices at the same time.

Figure 3-25 Extract events

Step 4   Set filtering conditions, and then click **Search**.

Figure 3-26 Search for events by filtering conditions

3.7 Access Management

3.7.1 Remotely Control Door Access

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 access. There are two methods.
- Method 1: Select the door, right click and select **Open**.

Figure 3-27 Remotely control (method 1)
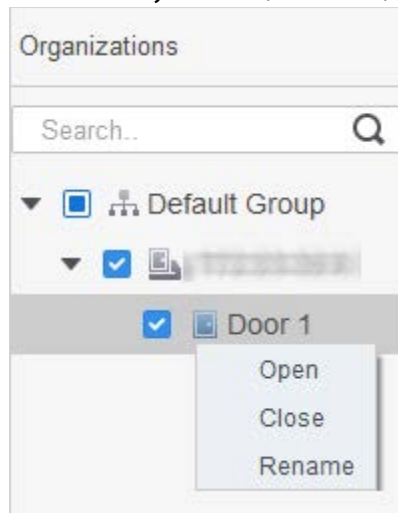
- Method 2: Click ⬛] or ⬛ to open or close the door.

Figure 3-28 Remotely control (method 2)
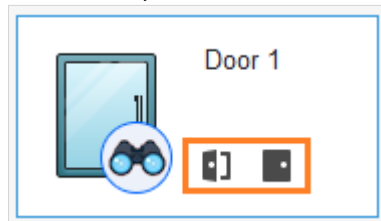
3.7.2 Setting Door Status

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
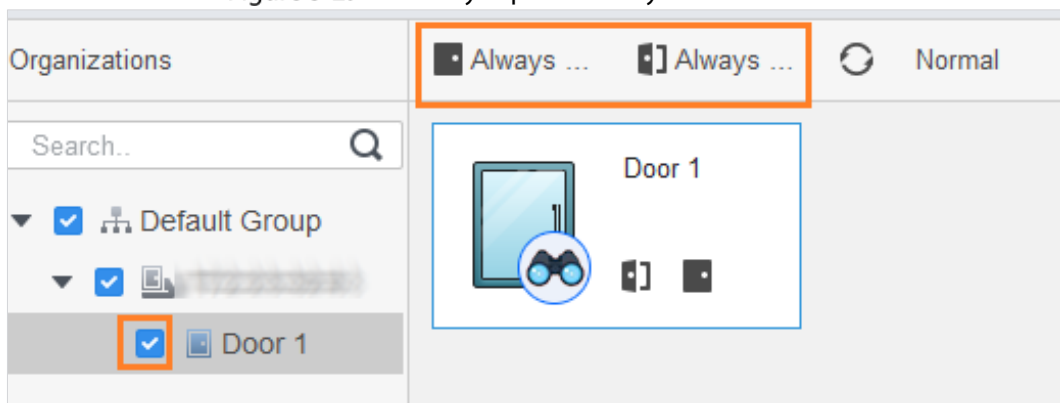
3.8 Configuring Alarm Linkage

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

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

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

Step 3 Turn on **Intrusion Event**.

Step 4 Configure intrusion alarm linkage.

- Turn on sound alarm.

    Click the **Notify** tab, and turn on **Alarm Sound**. When intrusion events occur, sound alarms are triggered.

- Send mail.

1) Turn on **Send Mail** and confirm to set SMTP.

2) Configure SMTP, 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
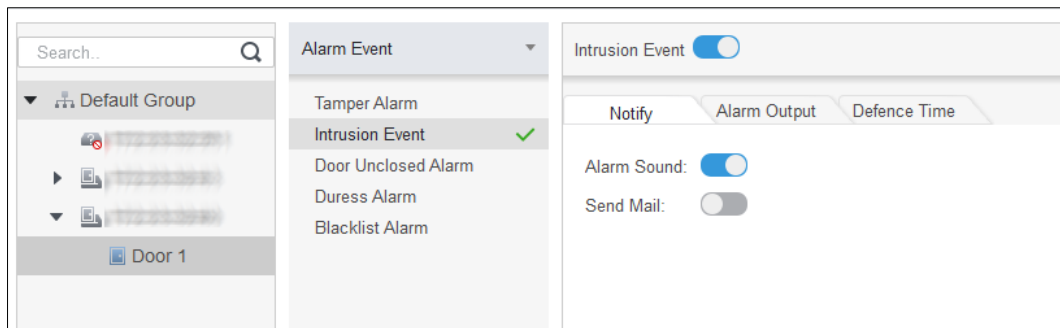
- Configure alarm output.

1) Click **Alarm Output** tab.

2) Select the device which supports alarm out, then select alarm-out port.

3) Turn on **Auto Open** for the alarm linkage.

4) Set the alarm duration.

Figure 3-31 Configure alarm linkage
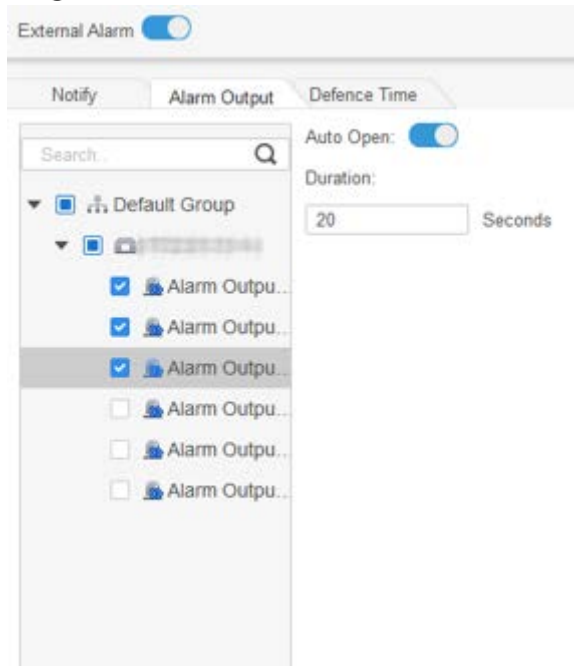
● Set arming periods. There are two methods.
  ◇ Method 1: Move the cursor to set periods. When the cursor is pencil, click to add periods; when the cursor is eraser, click to remove periods. The green area is the arming periods

Figure 3-32 Set defense time (method 1)
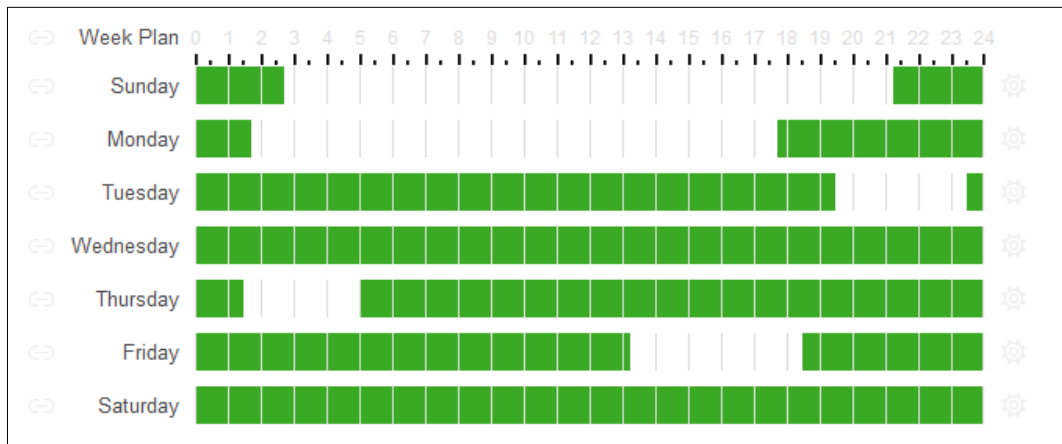
  ◇ Method 2: Click ⚙ to set arming periods, and then click **OK**.

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 Device and the computer are on the same network.

Step 1   Search for the Device 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 device, and then click **Initialize**.

Figure 4-1 Search for the device

Step 2   Select uninitialized devices, 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.

📖

Make sure that the Device and the computer where the ConfigTool is installed are connected; otherwise the ConfigTool cannot find the Device.
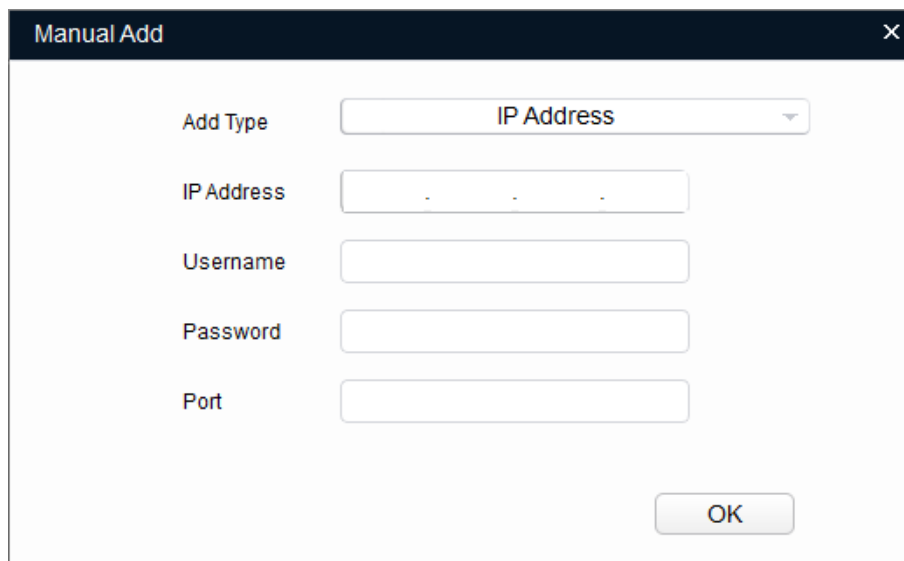
4.2.1 Adding Device Individually

Step 1   Click ⑫.

Step 2   Click **Manual Add**.

Step 3   Selec**t IP Address** or **Device SN** from **Add Type** list.

Figure 4-2 Manually add (IP address)

Figure 4-3 Manually add (Device SN)

Step 4   Set the device parameters.

Table 4-1 Manual add parameters

Add Method	Parameter	Description
IP Address	IP Address	The IP address of the device. It is 192.168.1.108 by default.

Add Method	Parameter	Description
	Username	The user name and password for device login.
	Password	
	Port	The device port number.
Device SN (Device support P2P only)	SN	The serial number of the device.
	Username	The user name and password for device login.
	Password	

Step 5   Click **OK**.

The added device displays in the device list.

4.2.2 Adding Device 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 network segment or other network segment.

📖

You can set the filtering conditions to search for devices.

Step 1   Click ⚙ Search setting .

Figure 4-4 Setting

Step 2   Select the search methods.

● Current Segment Search

Select **Current Segment Search**. Enter the username and password. The system will search for devices accordingly.

● Other Segment Search

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 search for devices.

The searched devices will display in the device list.

- Click to refresh the device list.
- The system saves the searching conditions when you exit 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 4-5 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**. **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 apply the configured parameters to, and then click **Config**.

✔ indicates application success; ⚠ indicates application failed. You can click them to view details.
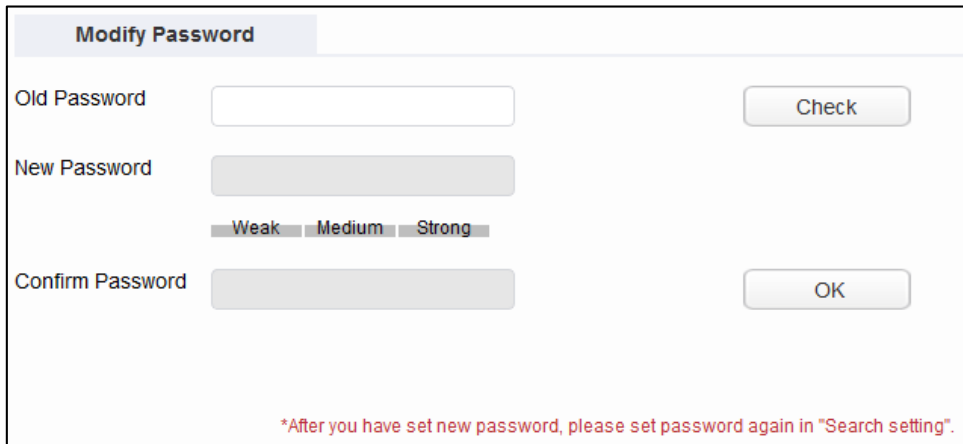
4.4 Modifying Device Password

You can modify the device login password.

Step 1   Click ⬚.

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

Figure 4-6 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 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

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

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

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

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

4. **Enable Account Lock**

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

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

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

6. **Enable HTTPS**

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

7. **MAC Address Binding**

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

the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

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

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

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

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

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

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

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

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

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