Access Controller

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the installation and basic operations of the access controller (hereinafter referred to as the "Device").

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	August 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.

- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

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

Operation Requirements

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

Electrical Safety

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

Table of Contents

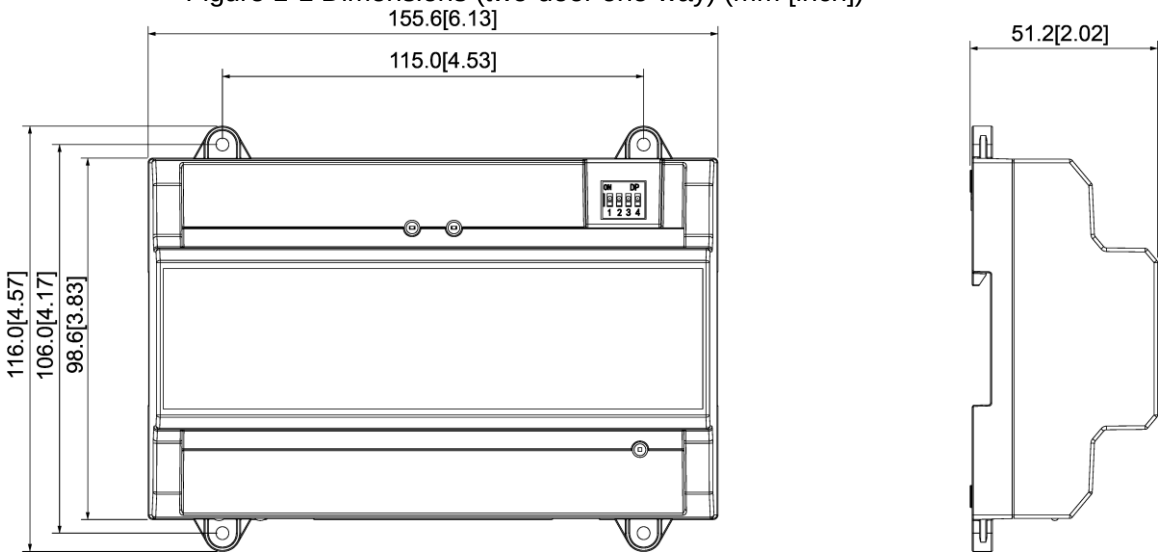
1 Overview

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 Dimensions

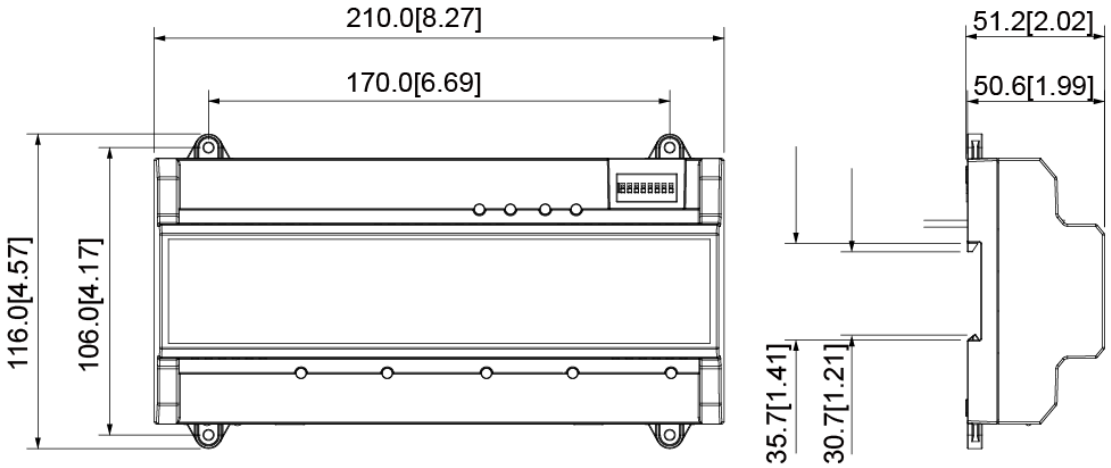
Two-door One-way Access Controller

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])



1.2 Components

Two-door One-way Access Controller

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

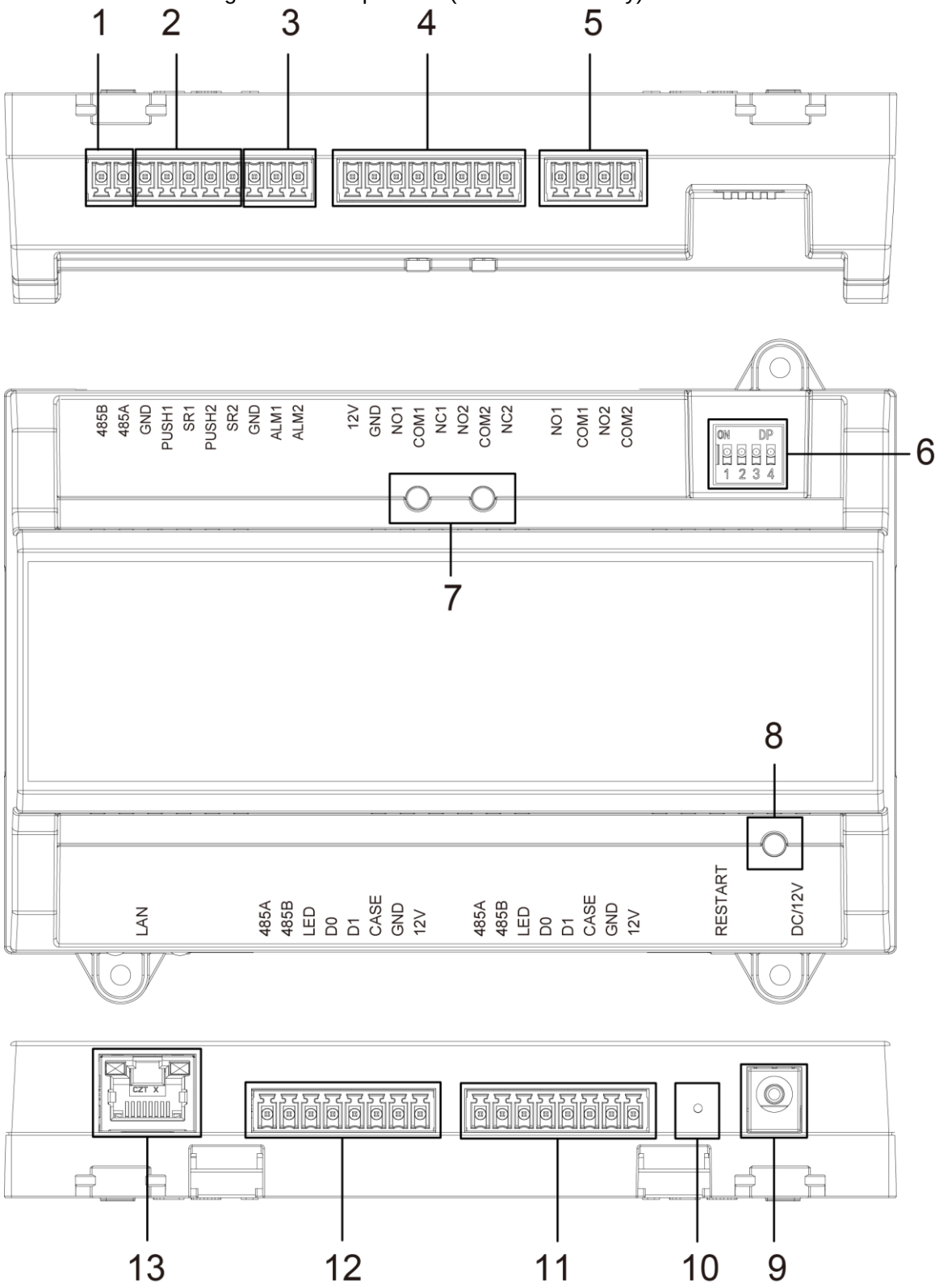


Table 1-1 Component description (two-door one-way)

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

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

Two-door Two-way Access Controller

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

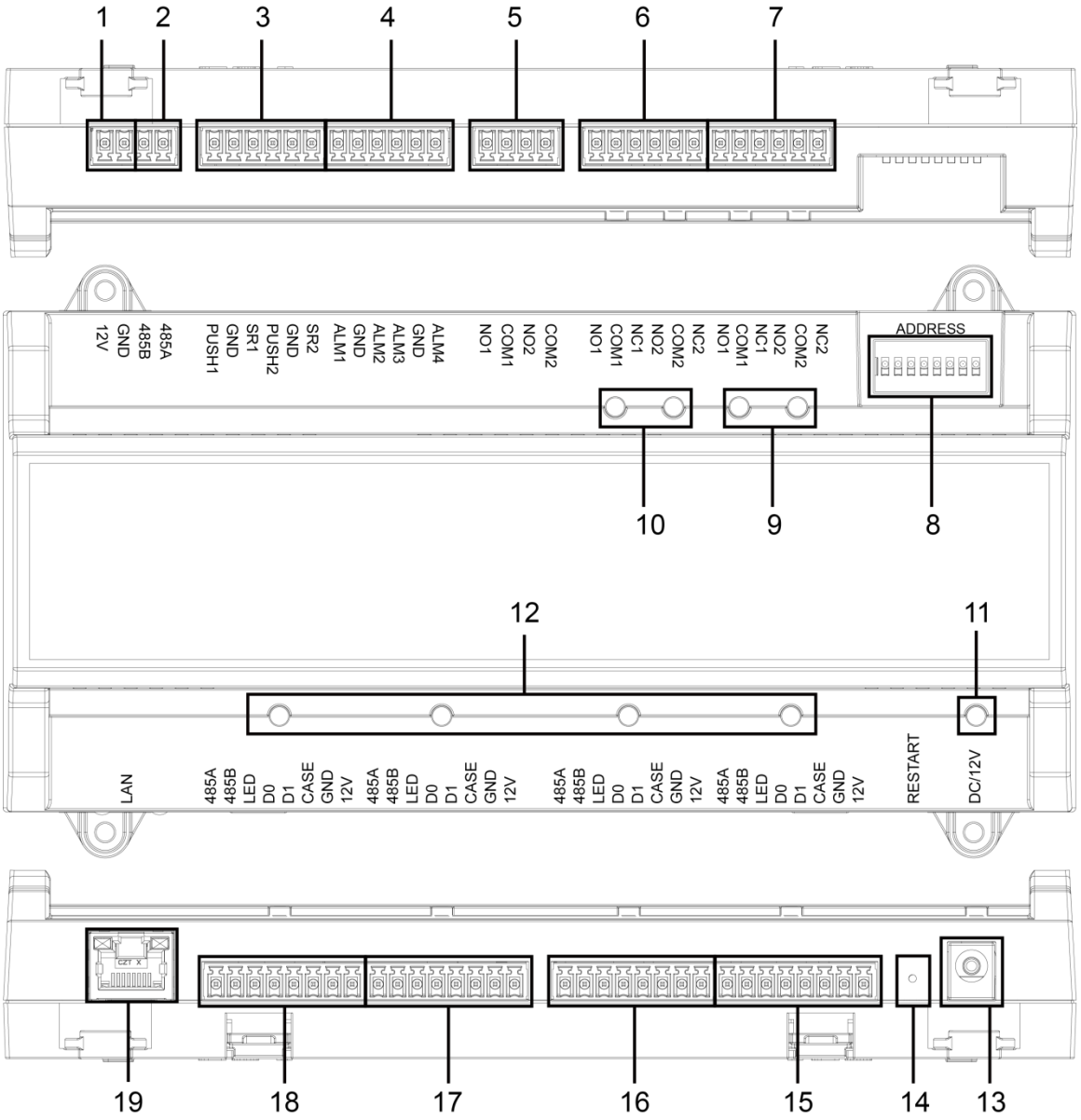


Table 1-2 Component description (two-door two-way)

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

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

Four-door One-way Access Controller

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

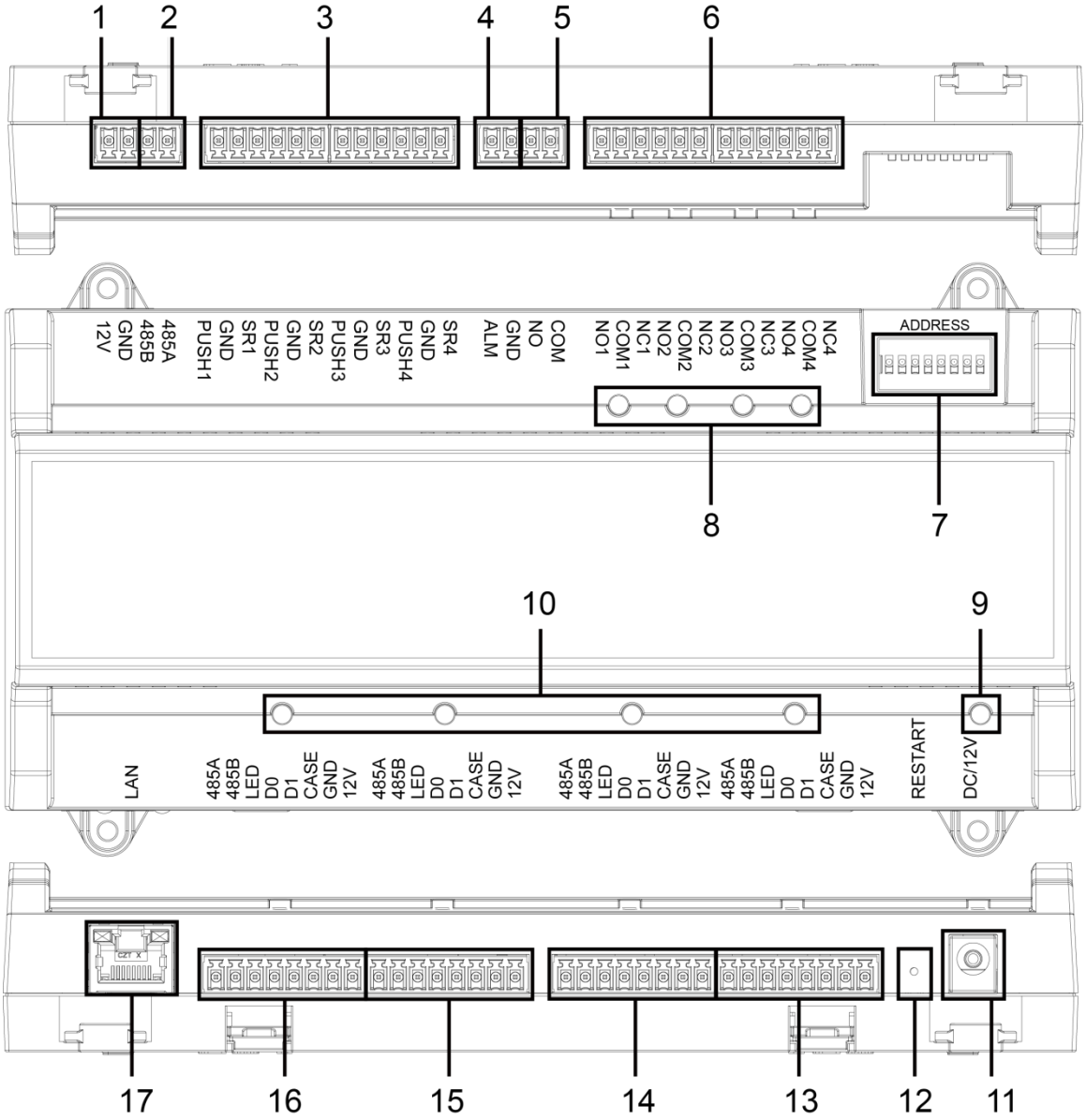


Table 1-3 Component description (four-door one-way)

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

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

Port

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

Indicator Light

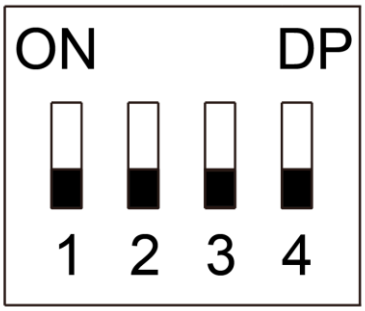
- Power indicator light
  - ◇ Green: Working normally.
  - ◇ Red: Power anomaly.
  - ◇ Blue: Upgrading.
- Alarm indicator light
  - ◇ On: Alarm is triggered.
  - ◇ Off: Alarm is not triggered.
- Door lock Indicator light
  - ◇ On: Door lock is connected.
  - ◇ Off: Door lock is not connected.
- Card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

DIP Switch

Perform corresponding operation through DIP switch.

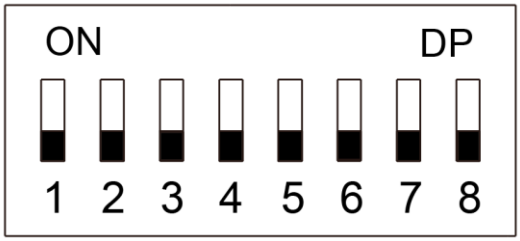
 Means 1;  means 0.

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



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

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



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

Restart

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

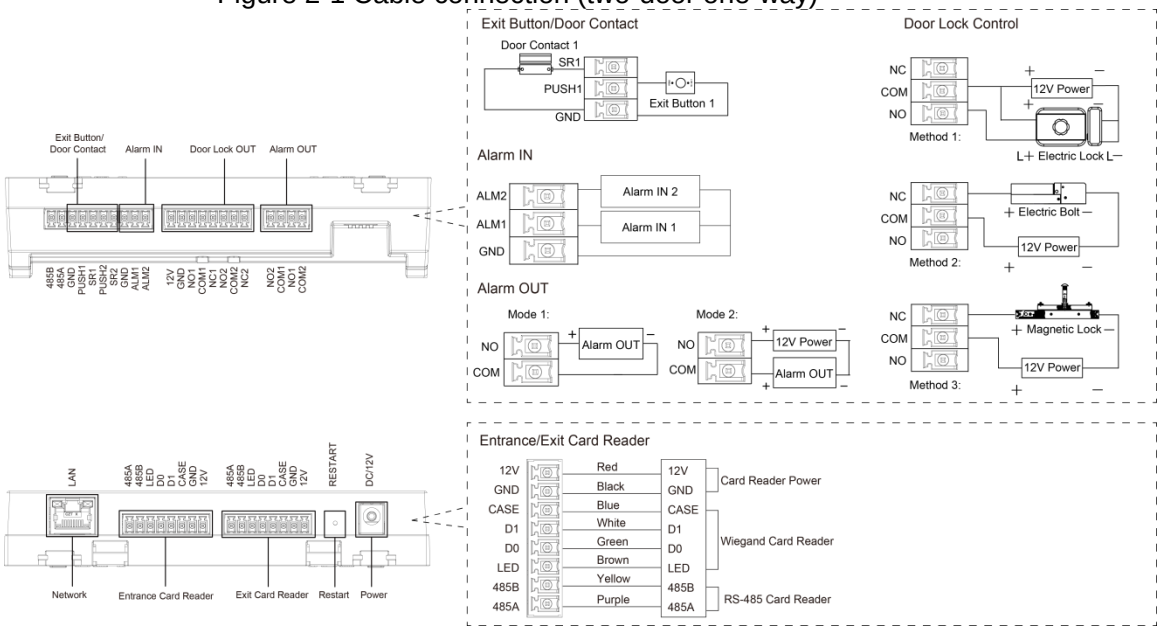
Restart button is to restart the Device, rather than modifying configuration.

2 Installation

2.1 Cable Connection

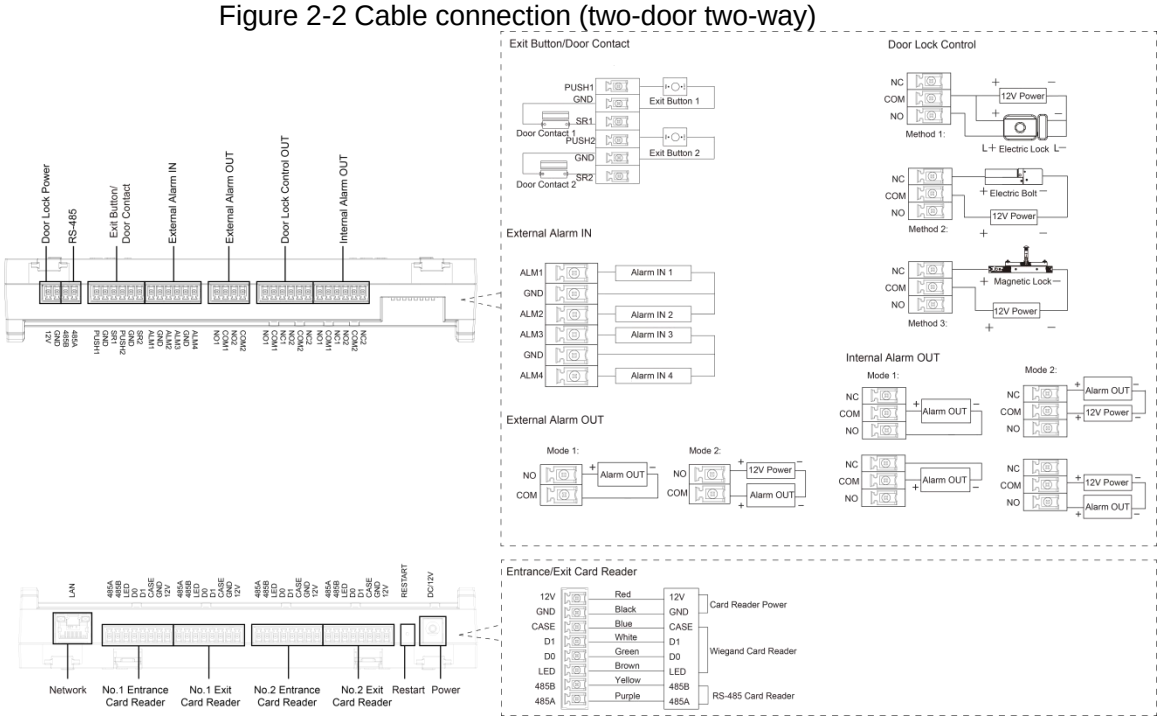
Two-door One-way Access Controller

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



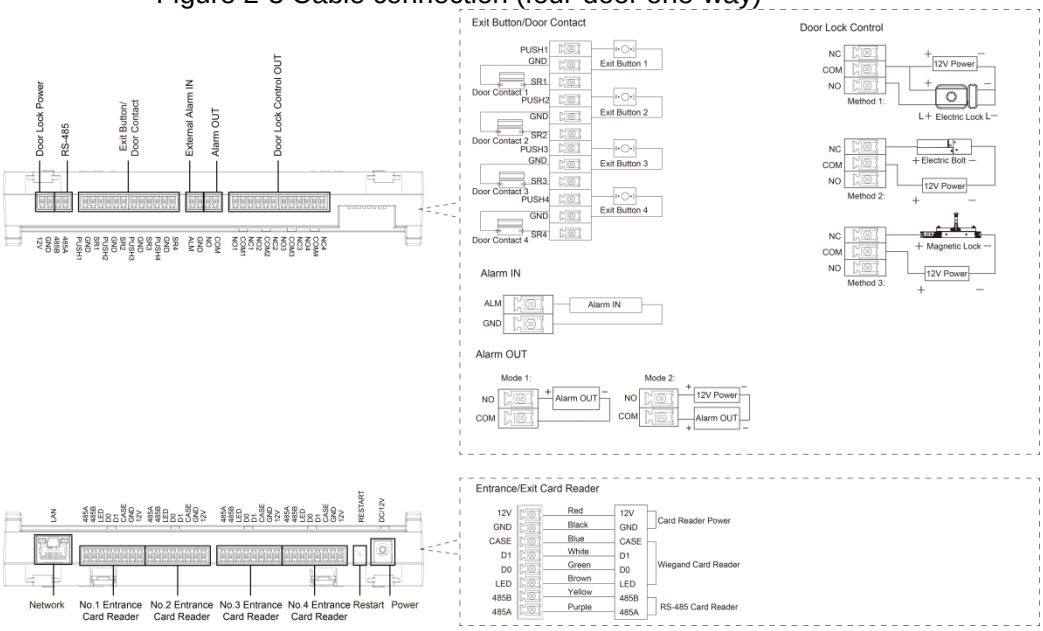
Two-door Two-way Access Controller

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



Four-door One-way Access Controller

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



2.1.1 Cable Connection of Alarm Input

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

Table 2-1 Cable connection of alarm input

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

2.1.2 Cable Connection of Alarm Output

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

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

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

Table 2-2 Cable connection of alarm output

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

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

2.1.3 Cable Connection of Card Reader

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

Table 2-3 Cable specification and length of card reader

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

2.2 Device Installation

There are two installation methods.

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

Figure 2-4 Installation (1)

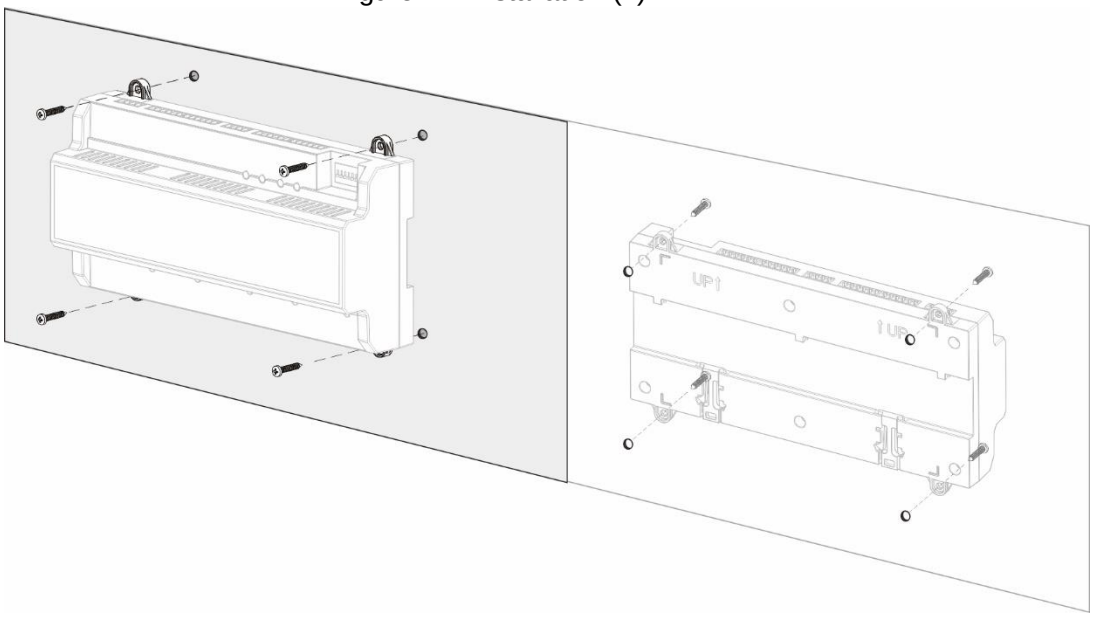
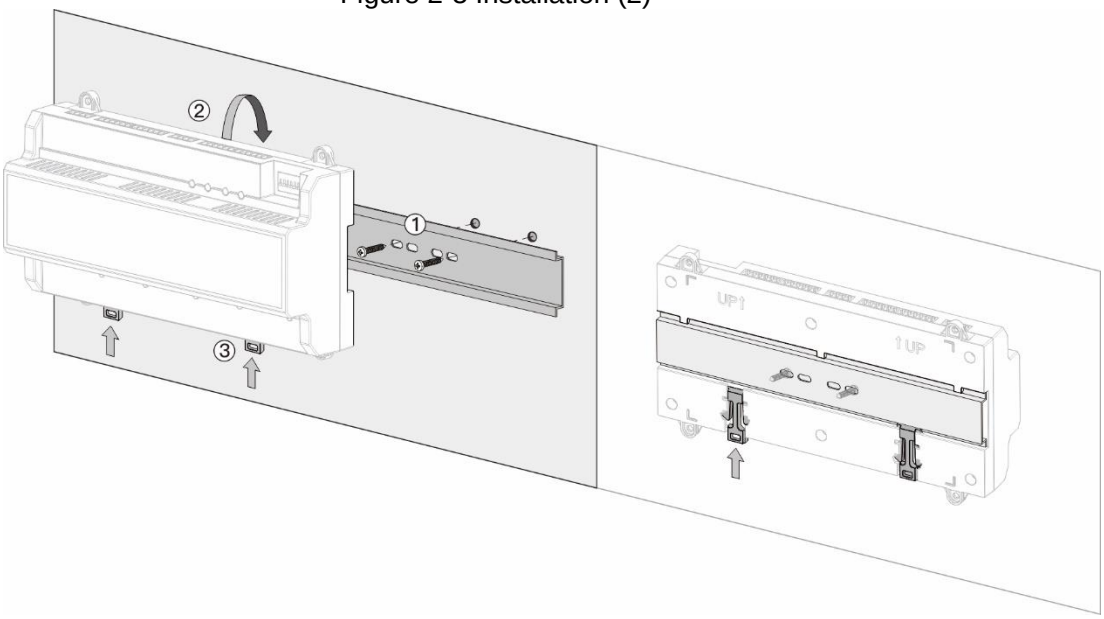


Figure 2-5 Installation (2)



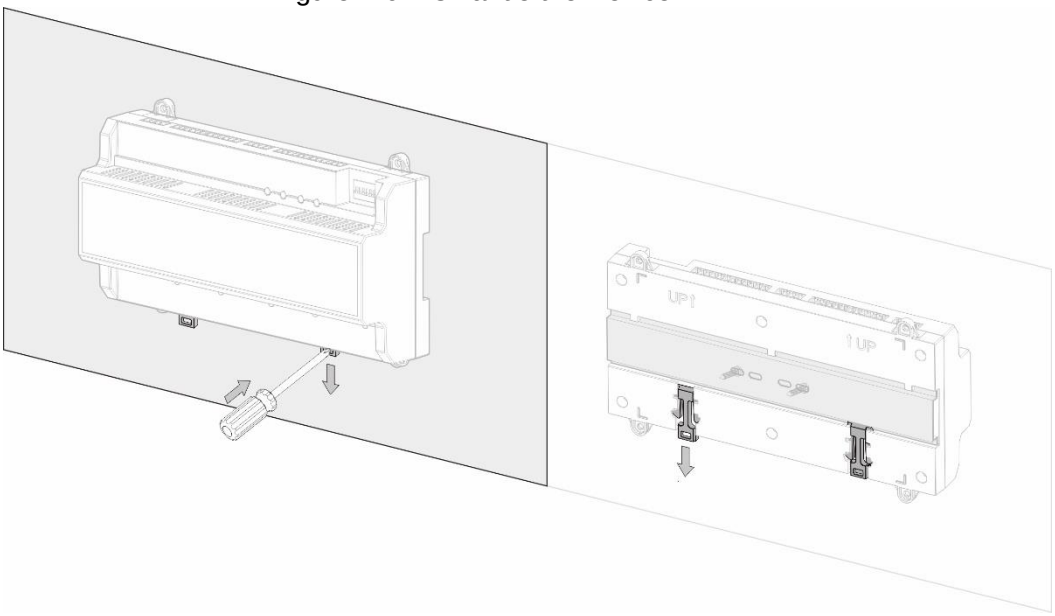
Step 1 Fix the U-shaped guide rail on wall with screws.
Step 2 Buckle the upper back part of the Device into the U-shaped guide rail.
Step 3 Push up the buckle on the lower part of the Device until hearing a click sound.

2.3 Demounting the Device

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

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

Figure 2-6 Dismantle the Device



3 SmartPSS AC Configuration

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

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

3.1 Login

Step 1 Install the SmartPSS AC.

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

3.2 Adding Devices

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

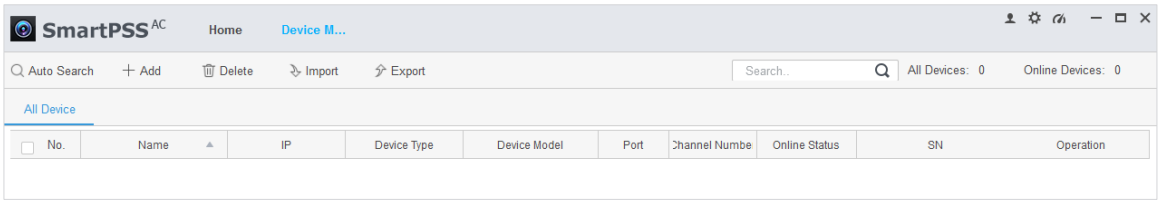
3.2.1 Auto Search

You can search and add devices at the same network segment to the SmartPSS AC.

Step 1 Log in to SmartPSS AC.

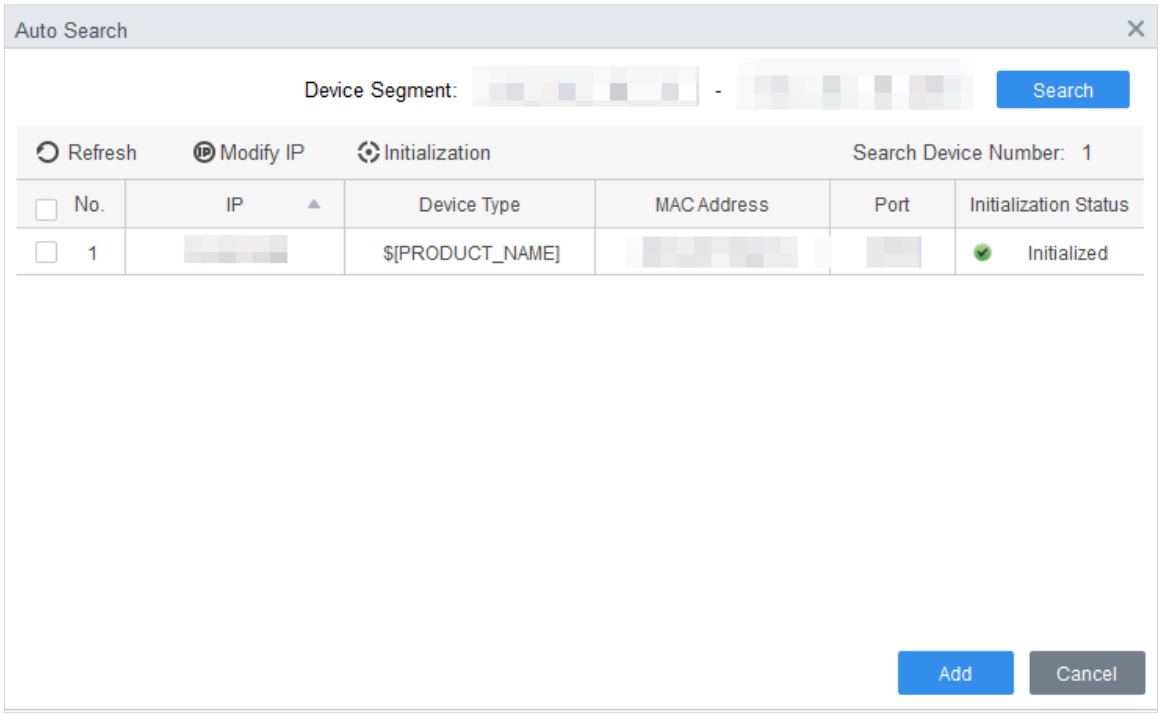
Step 2 Click **Device Manager** at the lower left corner, and the **Device Manager** interface is displayed.

Figure 3-1 Devices



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

Figure 3-2 Auto search



Step 4 Enter the network segment, and then click **Search**.
A search result list will be displayed.

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

Step 5 Select devices that you want to add to the SmartPSS AC, and then click **Add**.
The Login information dialog box will be displayed.

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

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

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

3.2.2 Manual Add

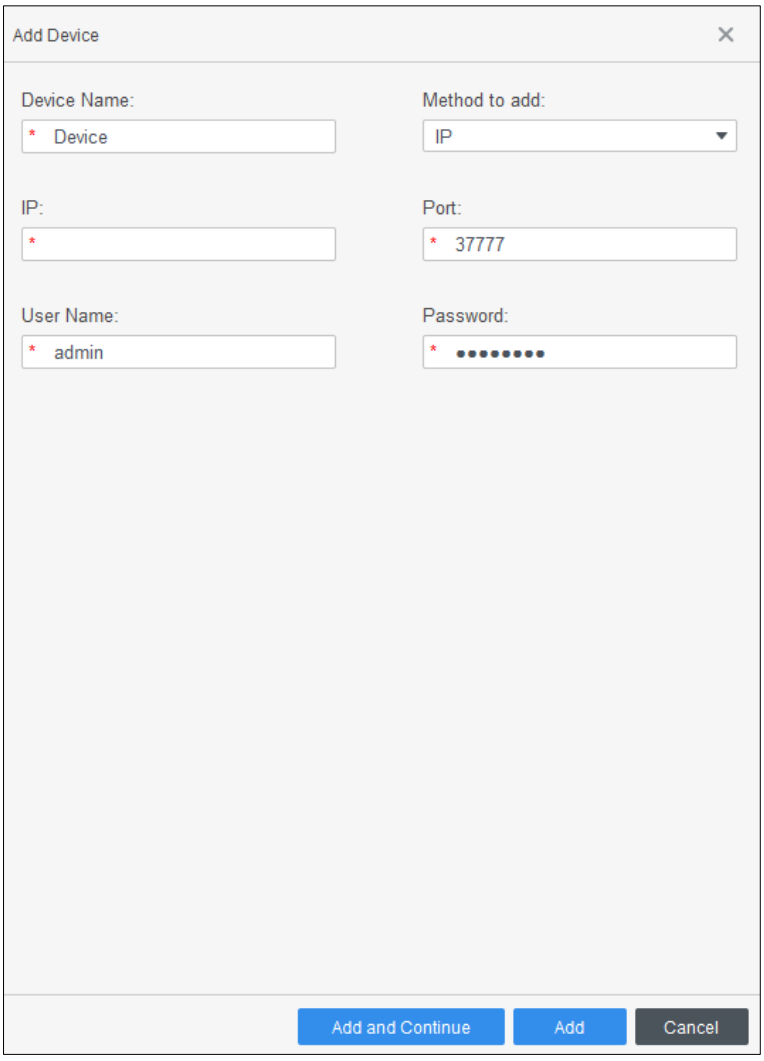
You can add devices manually. You need to know IP addresses and domain names of access controllers that you want to add.

Step 1 Log in to SmartPSS AC.

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

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

Figure 3-3 Manual add



Step 4 Enter detailed information of the Device.

Table 3-1 Parameters

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

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

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

4 ConfigTool Configuration

ConfigTool is mainly used to configure and maintain the Device.

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

4.1 Adding Devices

You can add one or multiple devices according to your actual needs. This chapter takes manually adding the Device by IP address as an example.

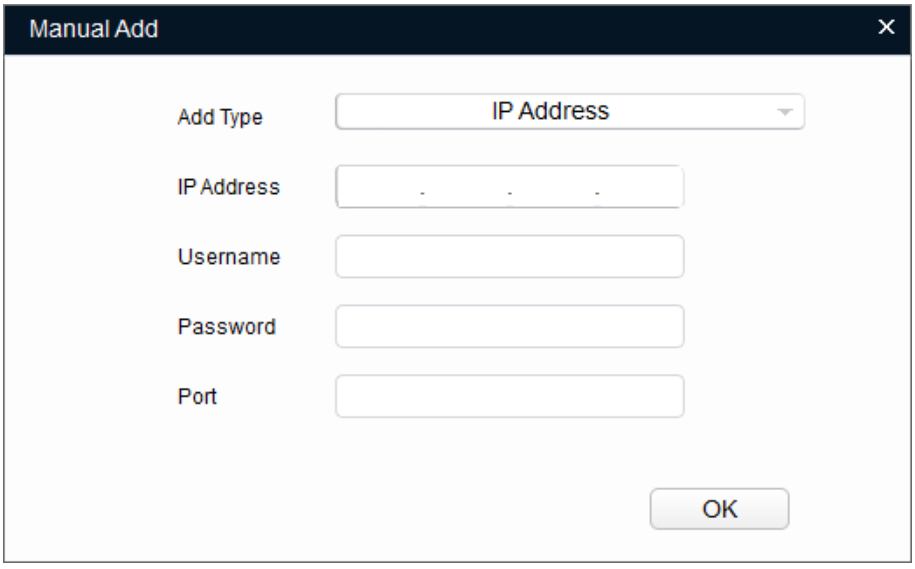
Make sure that the Device and the PC where the ConfigTool is installed are connected; otherwise the tool cannot find the Device.

Step 1 Click .

Step 2 Click Manual Add.

Step 3 Select IP Address from Add Type list.

Figure 4-1 Manual add



Step 4 Set the device parameters.

Table 4-1 Manual add parameters

Add Method	Parameter	Description
IP Address	IP Address	The IP address of the Device. It is 192.168.1.108 by default.
	Username	The username and password for login to the Device.
	Password	
	Port	The port number of the Device.

Step 5 Click **OK**.

The newly added device appears in the device list.

4.2 Configuring Access Controller

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

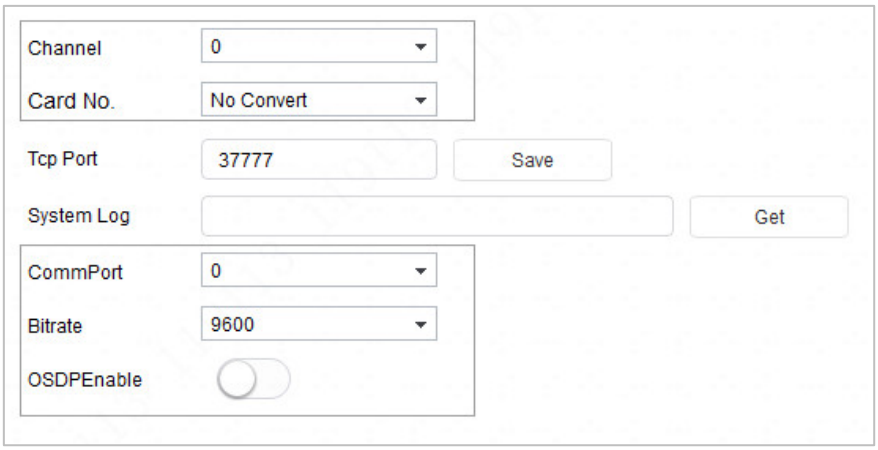
Step 1 Click  on the menu bar.

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

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

Step 4 Set access controller parameters.

Figure 4-2 Configure access controller



- Channel: Select the channel to set the parameters.

  Card No.: Set the card number processing rule of the access controller. It is **No Convert** by default. When the card reading result does not match the sent card No., select **Byte Revert** or **HIDpro Convert**.

  ◇ Byte Revert: When access controller works with third-party readers, and the card reading result does not match the sent card No. for example, the card reading result is hexadecimal 12345678 while the sent card No. is hexadecimal 78563412, you can select **Byte Revert** to match them.

  ◇ HIDpro Convert: When access controller works with HID Wiegand readers, and the card reading result does not match the sent card No., for example, the card reading result is hexadecimal 1BAB96 while the sent card No. is hexadecimal 78123456, you can select **HIDpro Revert** to match them.
- TCP Port: Modify TCP port number of the Device.
- SysLog: Click **Get** to select a storage path for system logs.
- CommPort: Select the reader to set bitrate and enable OSDP.
- Bitrate: If card reading is slow, you can increase bitrate. It is 9600 by default.

- OSDPEnable: When access controller works with third-party readers through ODSP protocol, enable ODSP.

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

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

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.