Access Controller

Quick Start Guide

V1.0.1

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
V1.0.1	Added initialization process.	December 2021
V1.0.0	First release.	August 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

- 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

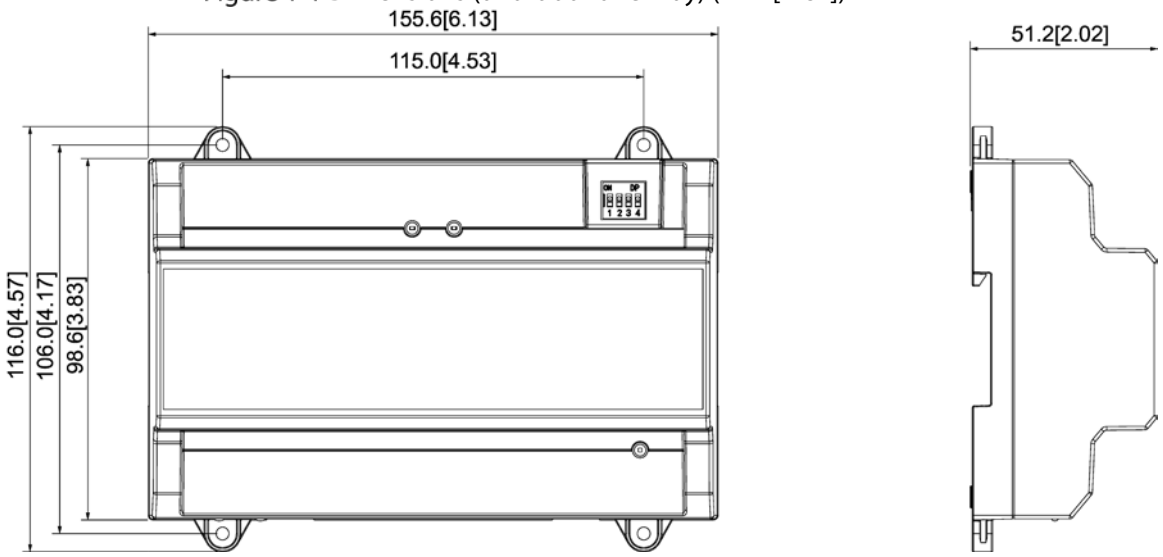
1 Overview

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.

1.1 Dimensions

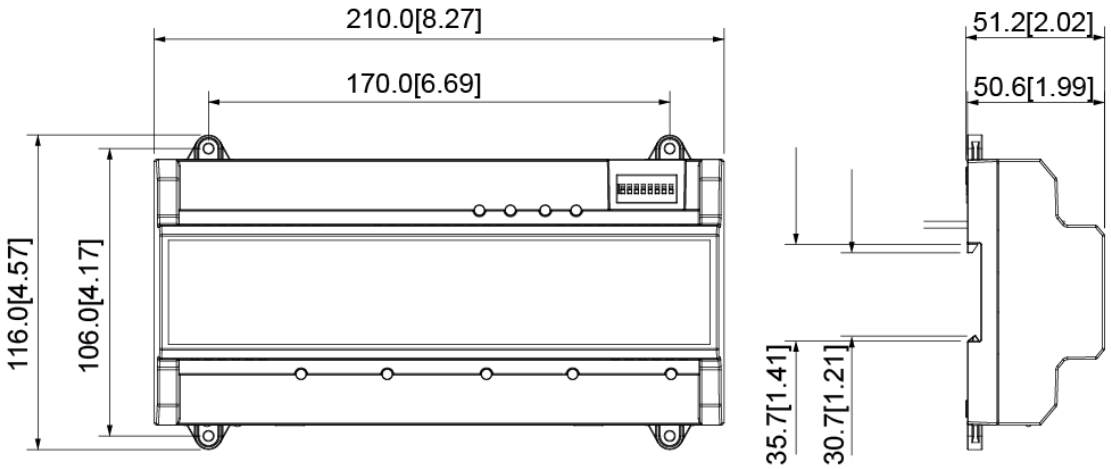
Two-door One-way Access Controller

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)

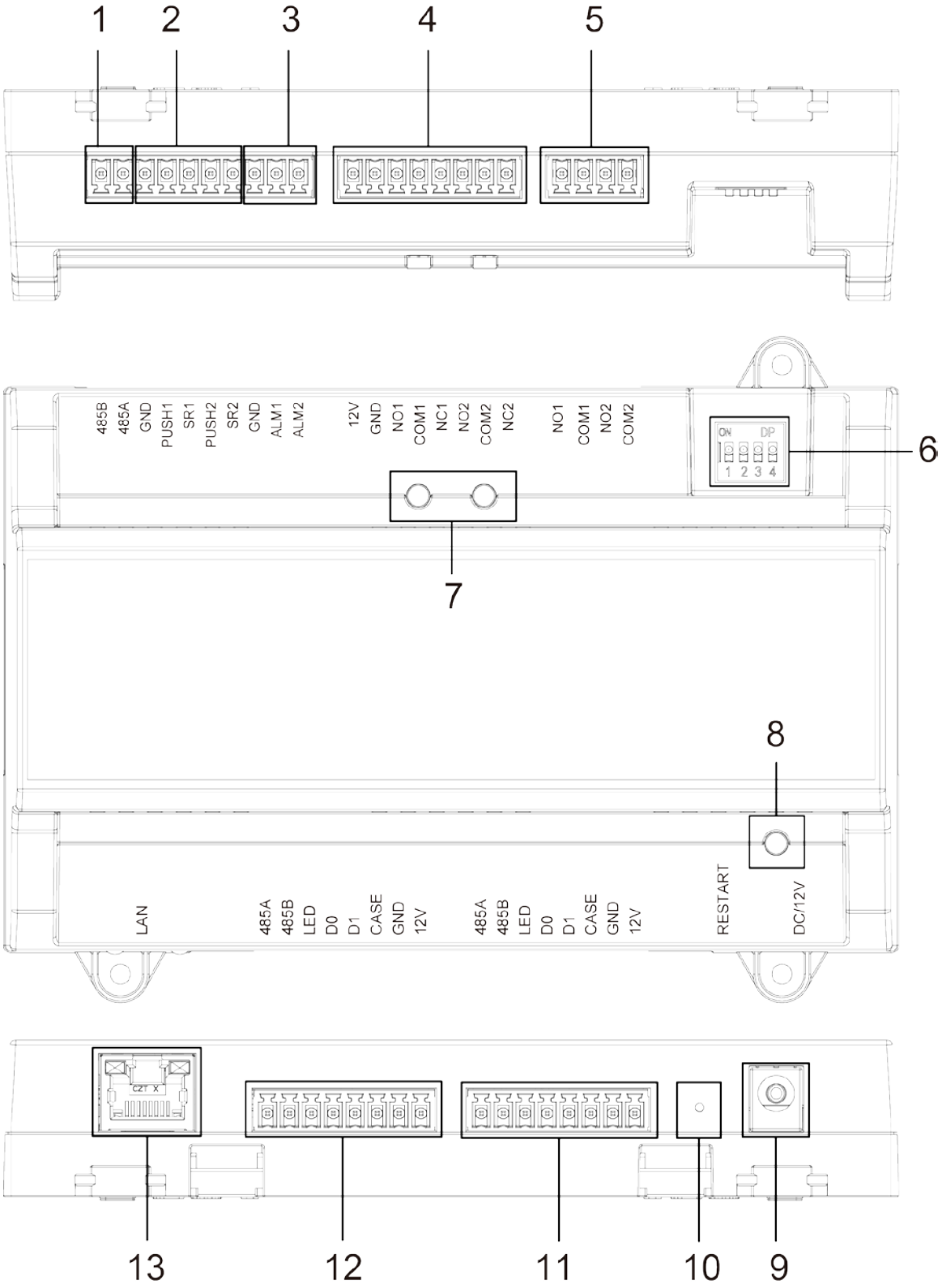


Table 1-1 Component description (two-door one-way)

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)

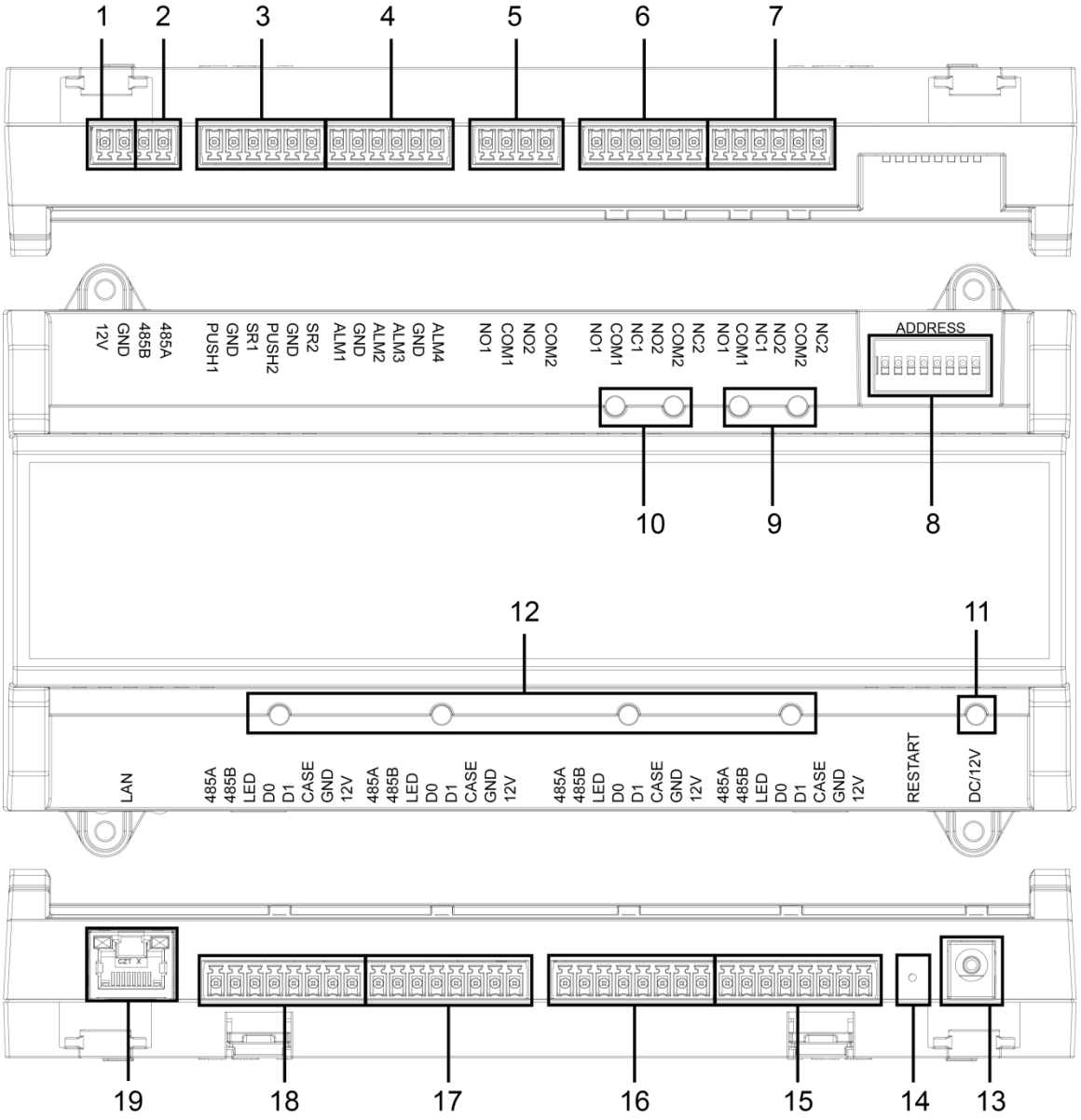


Table 1-2 Component description (two-door two-way)

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)

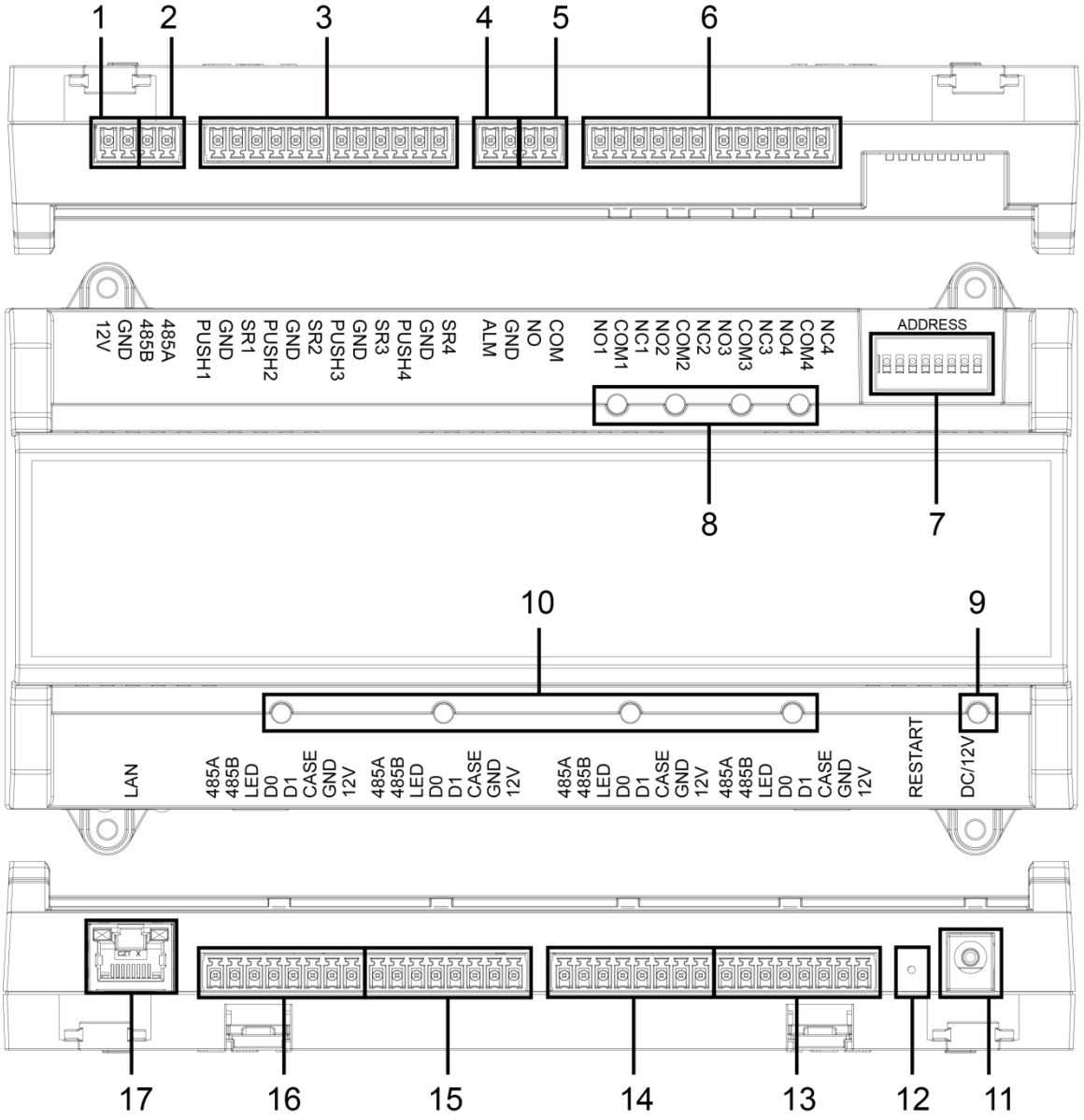


Table 1-3 Component description (four-door one-way)

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

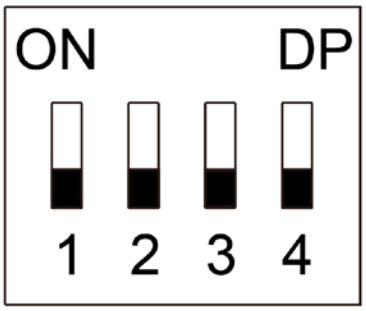
- Power indicator light
  - ◇ Green: Working normally.
  - ◇ Red: Power anomaly.
  - ◇ Blue: Upgrading.
- Alarm indicator light
  - ◇ On: Alarm is triggered.
  - ◇ Off: Alarm is not triggered.
- Door lock Indicator light
  - ◇ On: Door lock is connected.
  - ◇ Off: Door lock is not connected.
- Card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

DIP Switch

Perform corresponding operation through DIP switch.

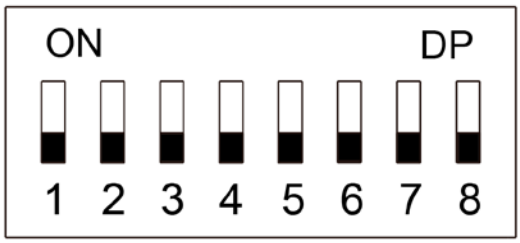
 Means 1;  means 0.

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.

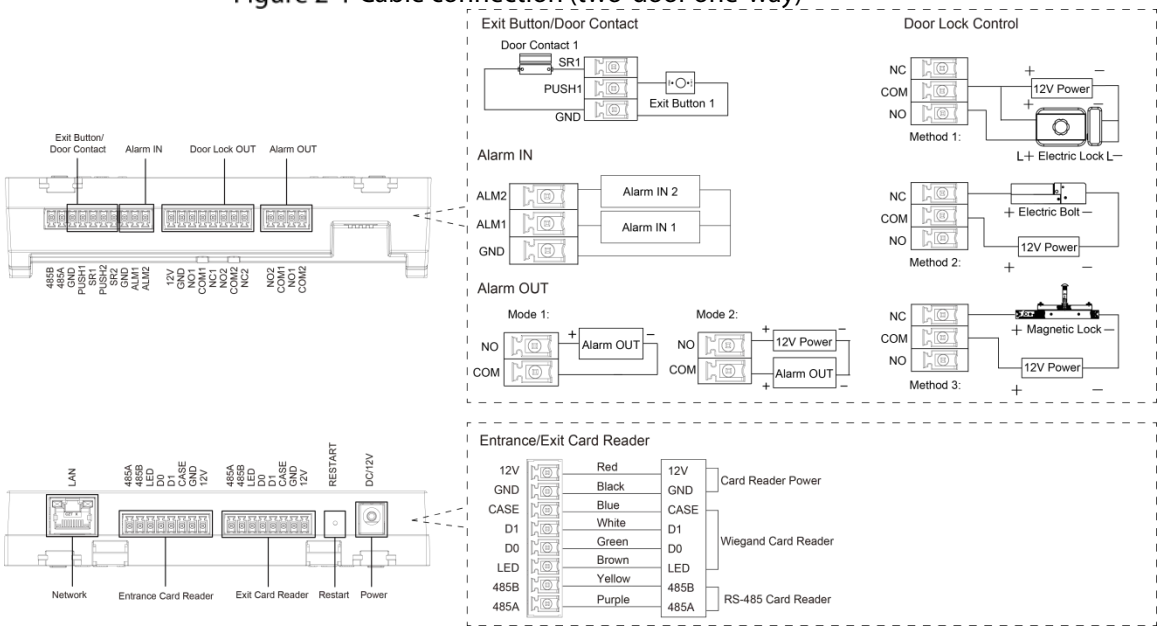
Restart button is to restart the Device, rather than modifying configuration.

2 Installation

2.1 Cable Connection

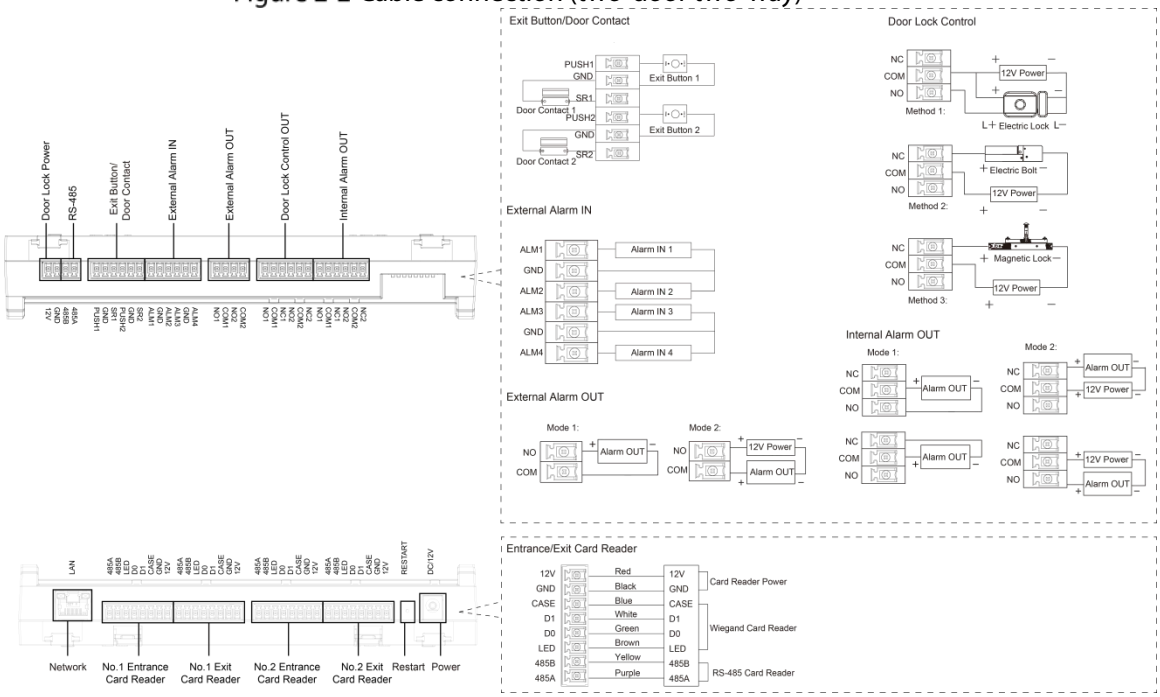
Two-door One-way Access Controller

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



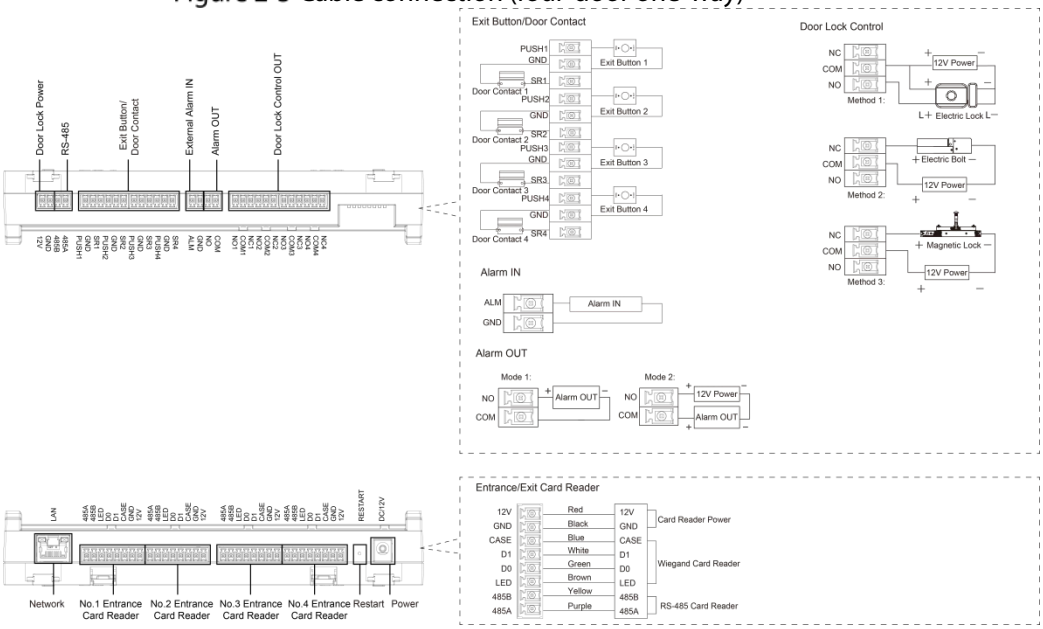
Two-door Two-way Access Controller

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
	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. ● 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 Installing the Device

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)

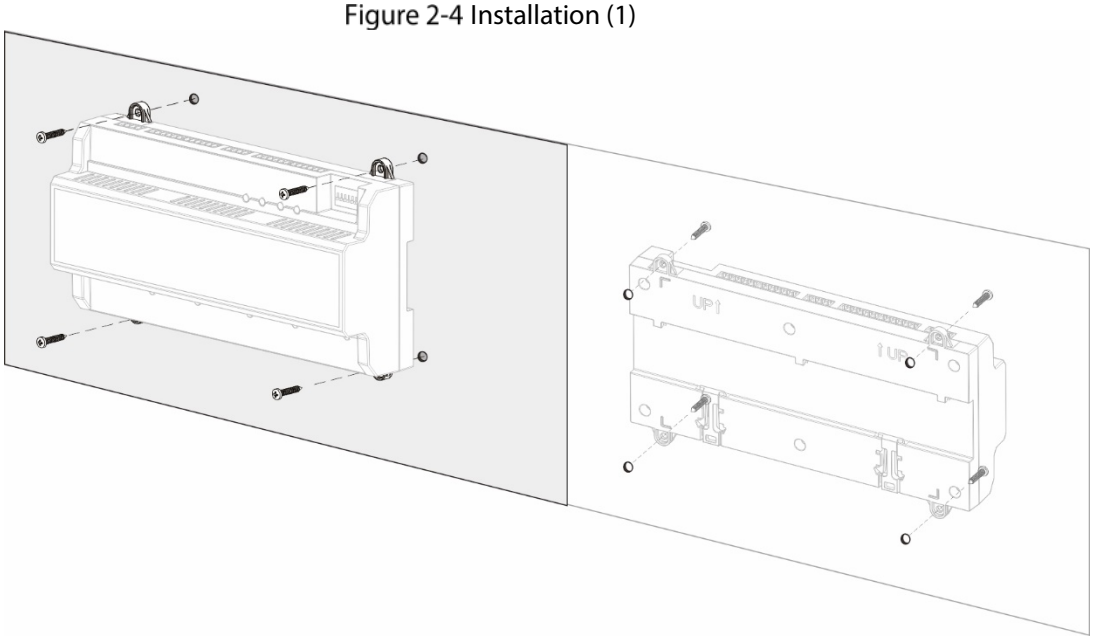
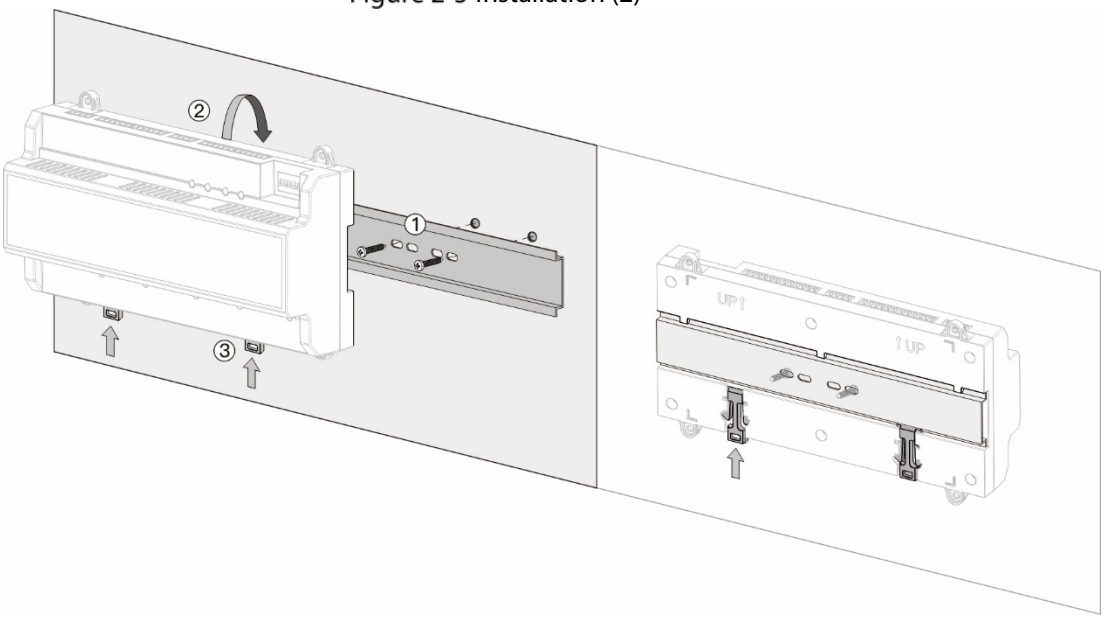


Figure 2-5 Installation (2)



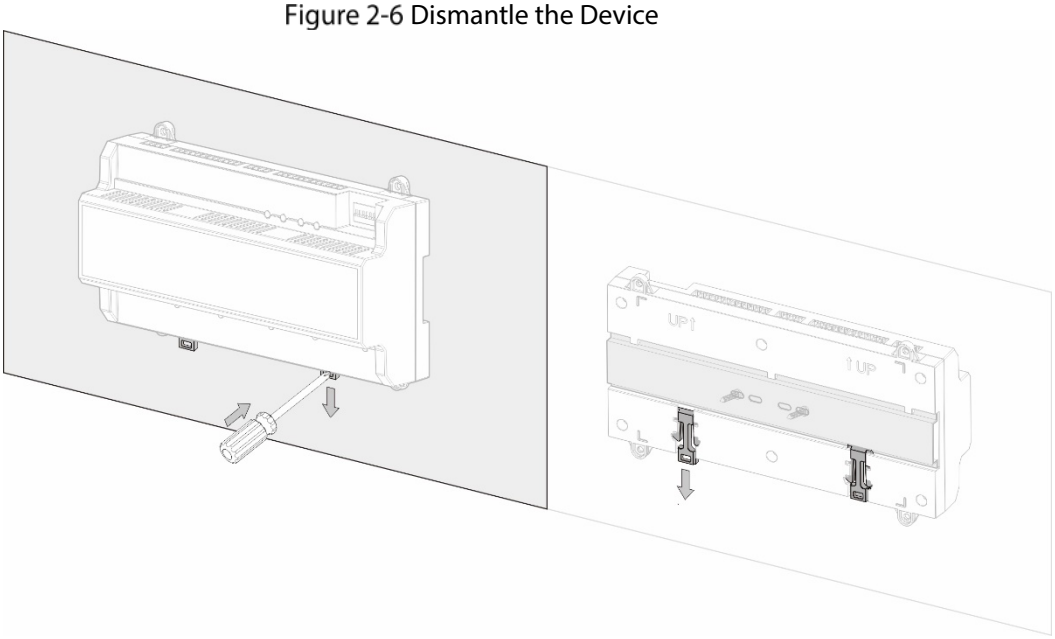
Step 1 Fix the U-shaped guide rail on wall with screws.
Step 2 Buckle the upper back part of the Device into the U-shaped guide rail.
Step 3 Push up the buckle on the lower part of the Device until you hear a click sound.

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 Dismantle 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.

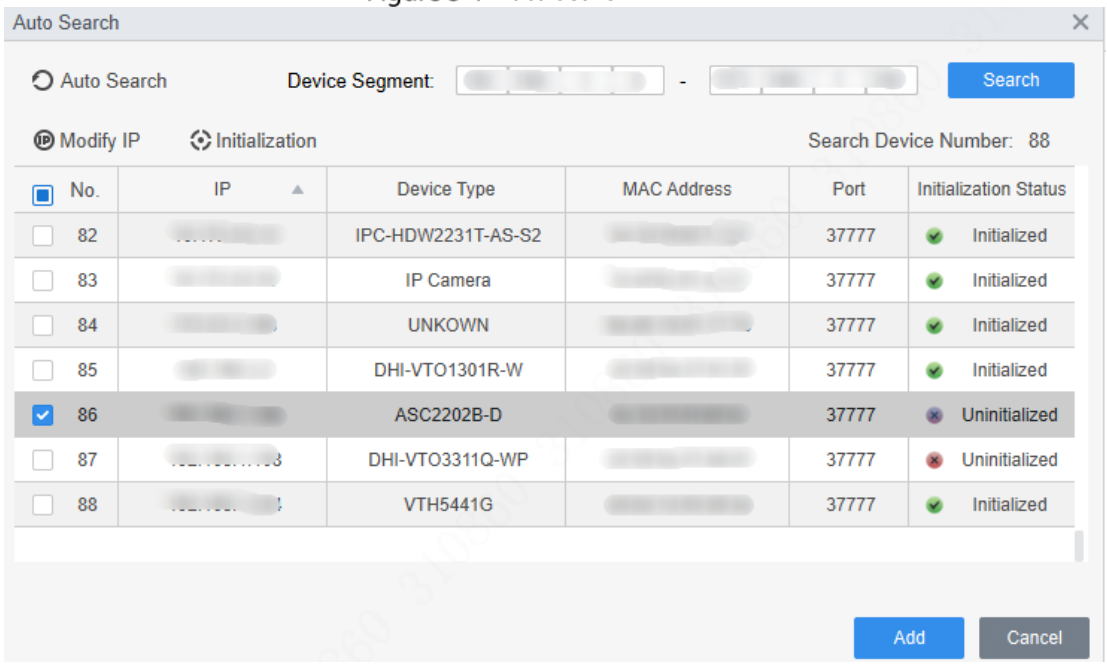
Step 2 Double-click , and then follow the instructions to finish the initialization and log in.

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



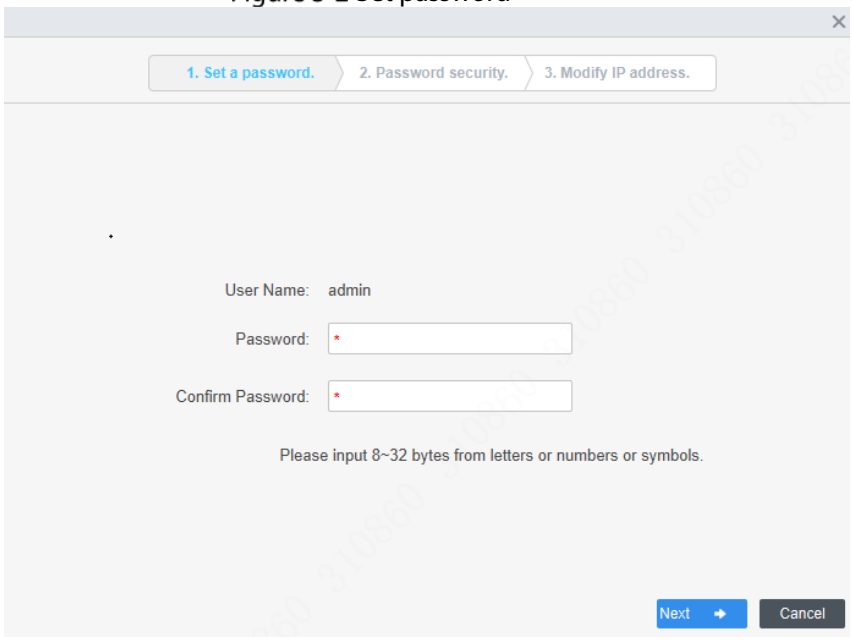
Step 2 Enter a network segment range, and then click **Search**.

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.

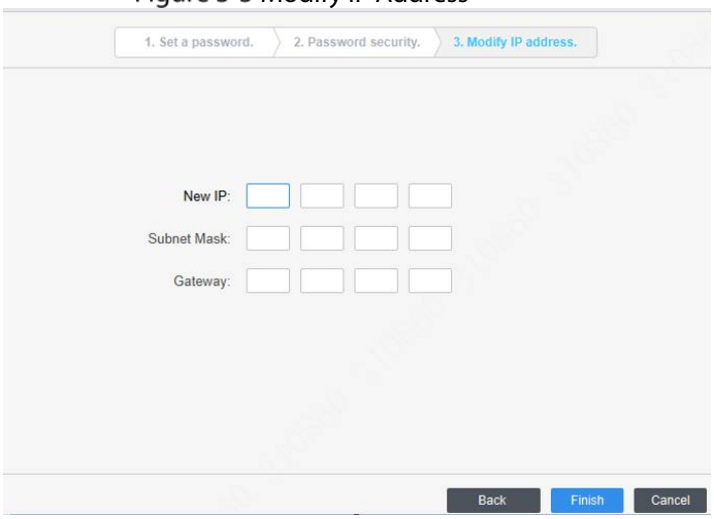
Figure 3-2 Set password



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.

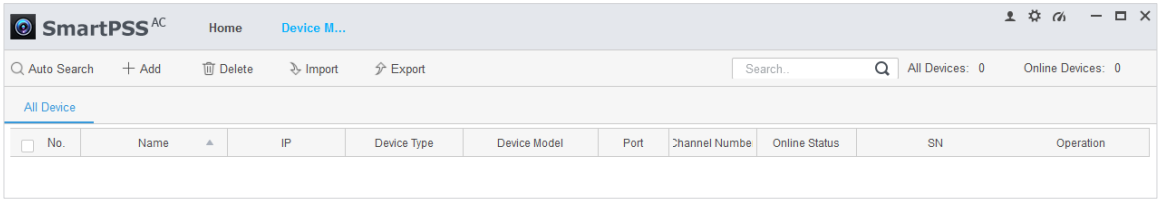
3.3.1 Auto Search

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.

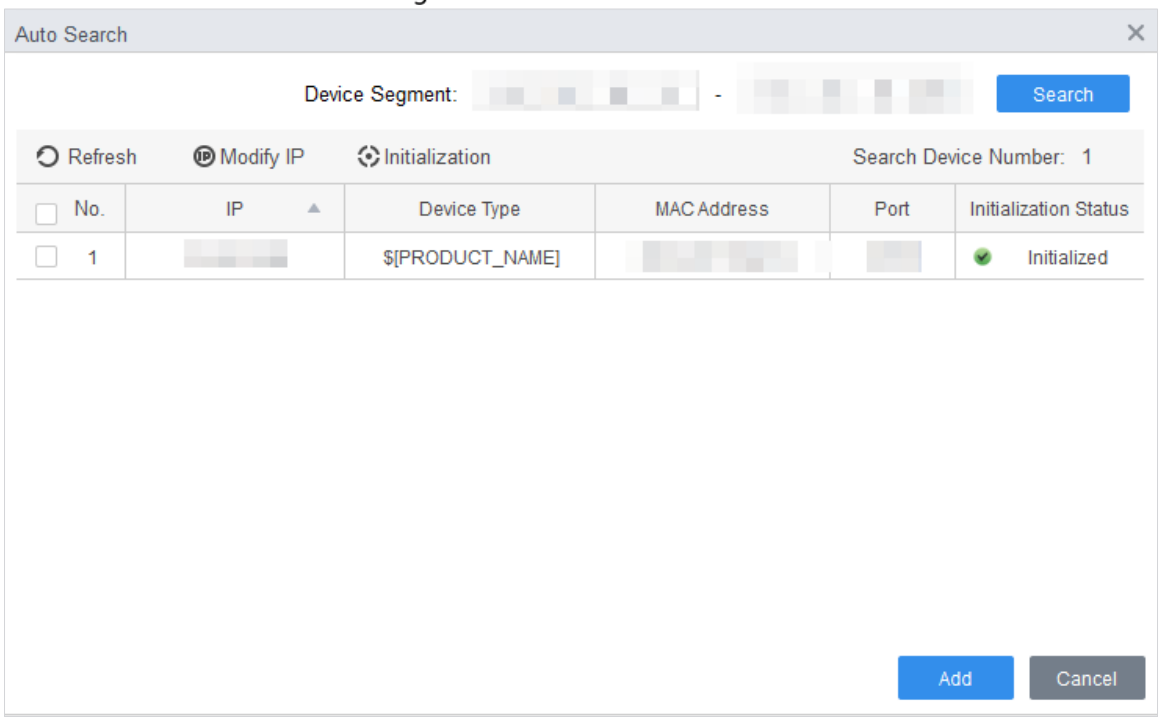
Step 2 Click **Device Manager** at the lower left corner.

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 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.

- 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

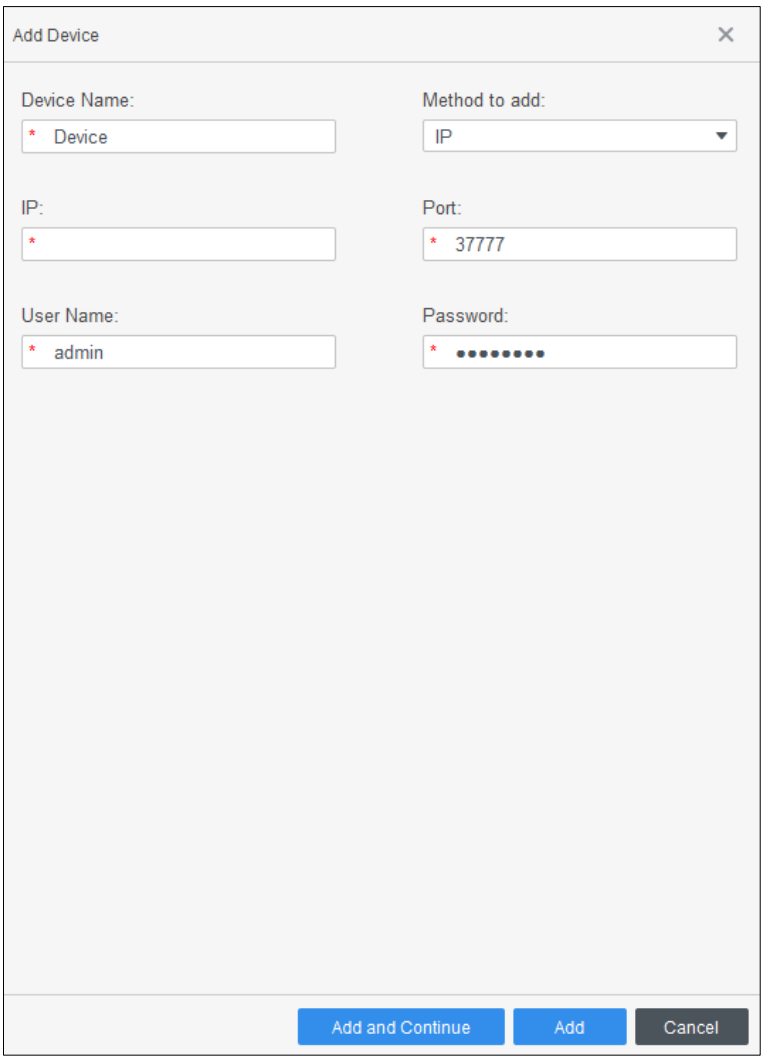
You can add devices manually. You need to know the IP addresses and domain names of the access controller that you want to add.

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 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** page.

After adding, SmartPSS AC logs in to the Device automatically. After successful login, the 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 results when you searching for devices.

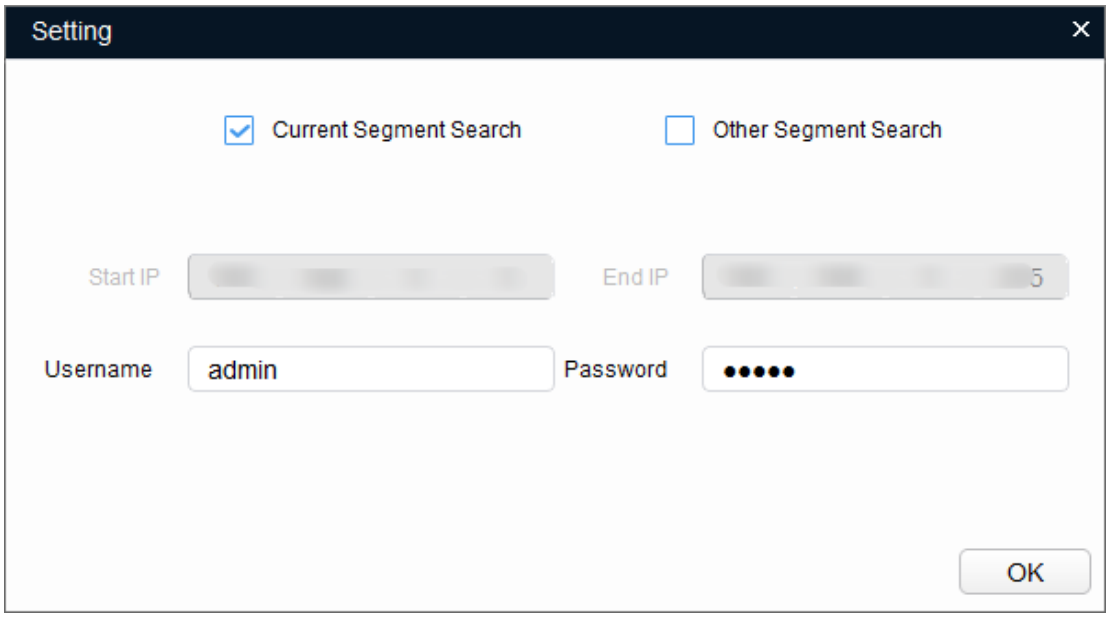
4.1 Initialization

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

Step 6 Search for the Device through the ConfigTool.

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

Figure 4-1 Search for the device



Step 7 Select uninitialized devices, and then click **Initialize.**

Step 8 Click **OK**.

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

Step 9 Click **Finish**.

4.2 Adding Devices

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

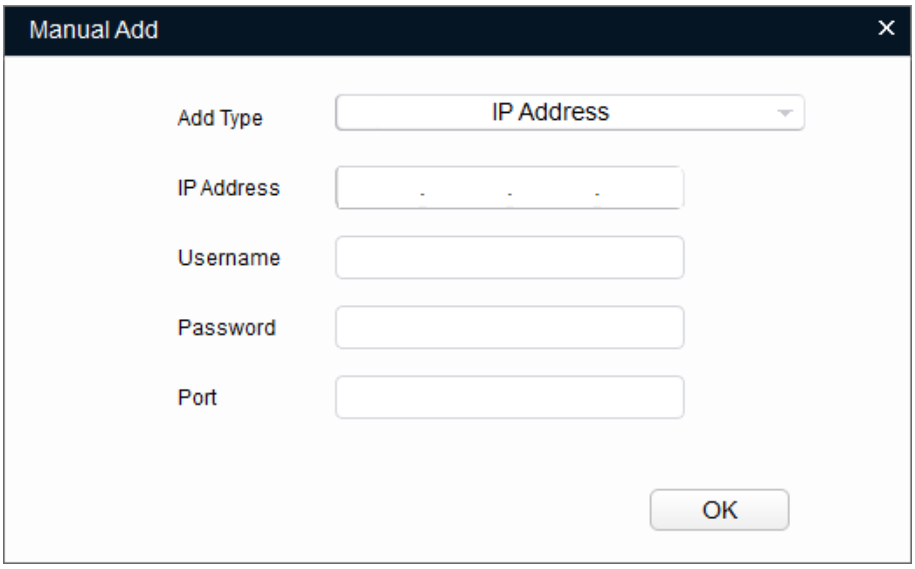
Make sure that the Device and the PC where the ConfigTool is installed are connected; otherwise the tool cannot find the Device.

Step 1 Click  .

Step 2 Click Manual Add.

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

Figure 4-2 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 displays 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 4-3 Configure access controller

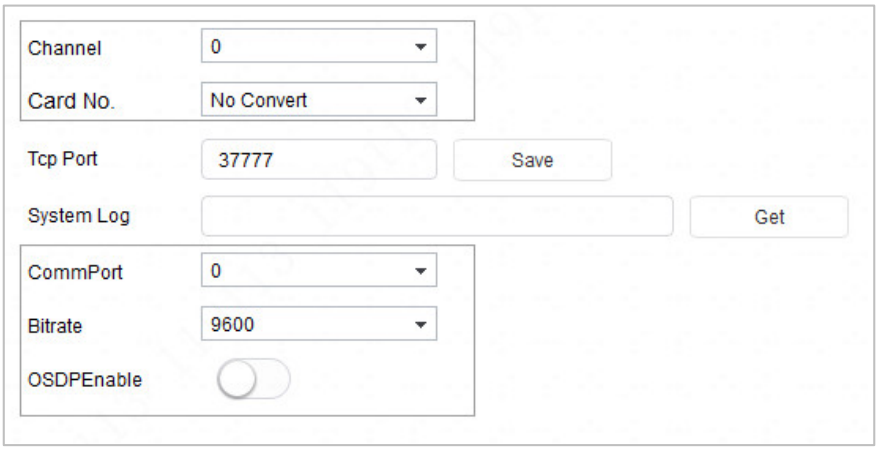


Table 4-2 Access controller parameters

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.

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.