Elevator Controller

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the wiring, installation and basic operations of the Elevator Controller. Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	August 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, 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 Elevator Controller, hazard prevention, and prevention of property damage. Read carefully before using the Elevator Controller, and comply with the guidelines when using it.

Transportation Requirement

Transport, use and store the Elevator Controller under allowed humidity and temperature conditions.

Storage Requirement

Store the Elevator Controller under allowed humidity and temperature conditions.

Installation Requirements

- Do not connect the power adapter to the Elevator Controller while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Elevator Controller.
- Do not connect the Elevator Controller to two or more kinds of power supplies, to avoid damage to the Elevator Controller.
- Improper use of the battery might result in a fire or explosion.
- Please follow the electrical requirements to power the Elevator Controller.
  - Following are the requirements for selecting a power adapter.
    - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
  - We recommend using the power adapter provided with the Elevator Controller.
  - When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the Elevator Controller label.

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Elevator Controller in a place exposed to sunlight or near heat sources.
- Keep the Elevator Controller away from dampness, dust, and soot.
- Install the Elevator Controller on a stable surface to prevent it from falling.

- Install the Elevator Controller in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The Elevator Controller is a class I electrical appliance. Make sure that the power supply of the Elevator Controller is connected to a power socket with protective earthing.

Operation Requirements

- Check whether the power supply is correct before use.
- Ground the device to protective ground before you power it on.
- Do not unplug the power cord on the side of the Elevator Controller while the adapter is powered on.
- Operate the Elevator Controller within the rated range of power input and output.
- Use the Elevator Controller under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Elevator Controller, and make sure that there is no object filled with liquid on the Elevator Controller to prevent liquid from flowing into it.
- Do not disassemble the Elevator Controller without professional instruction.
- This product is professional equipment.
- The Elevator Controller is not suitable for use in locations where children are likely to be present.

Table of Contents

1 Dimensions and Appearance

Figure 1-1 Dimensions (mm [inch])

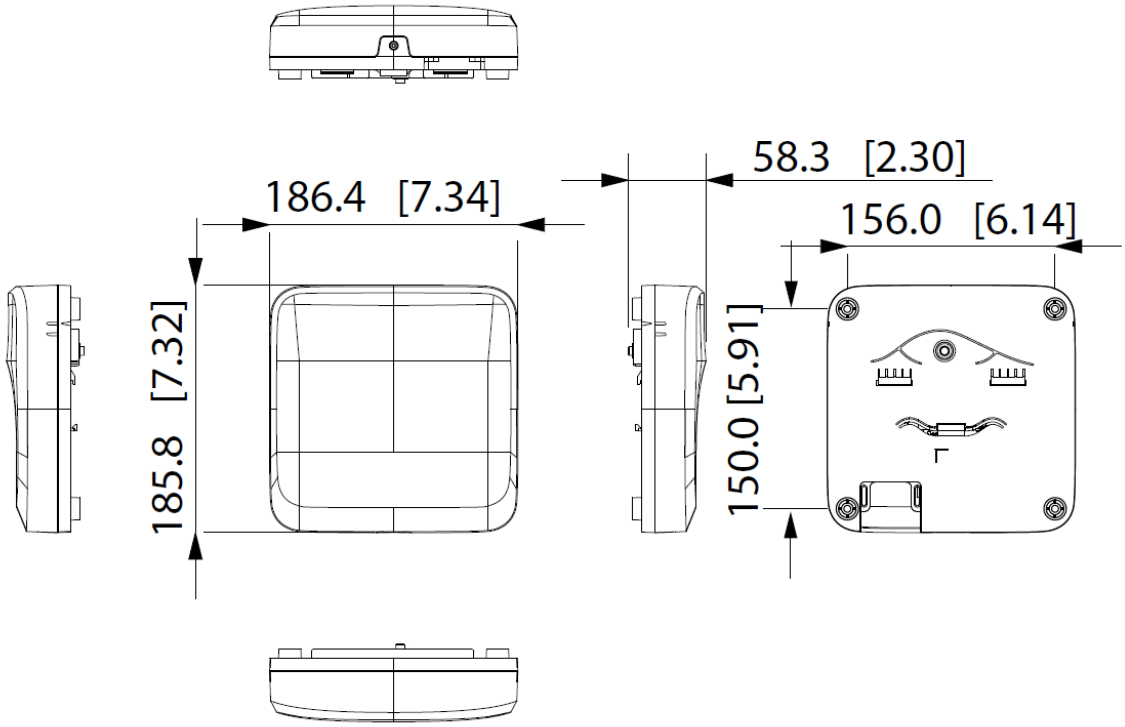


Figure 1-2 Front view

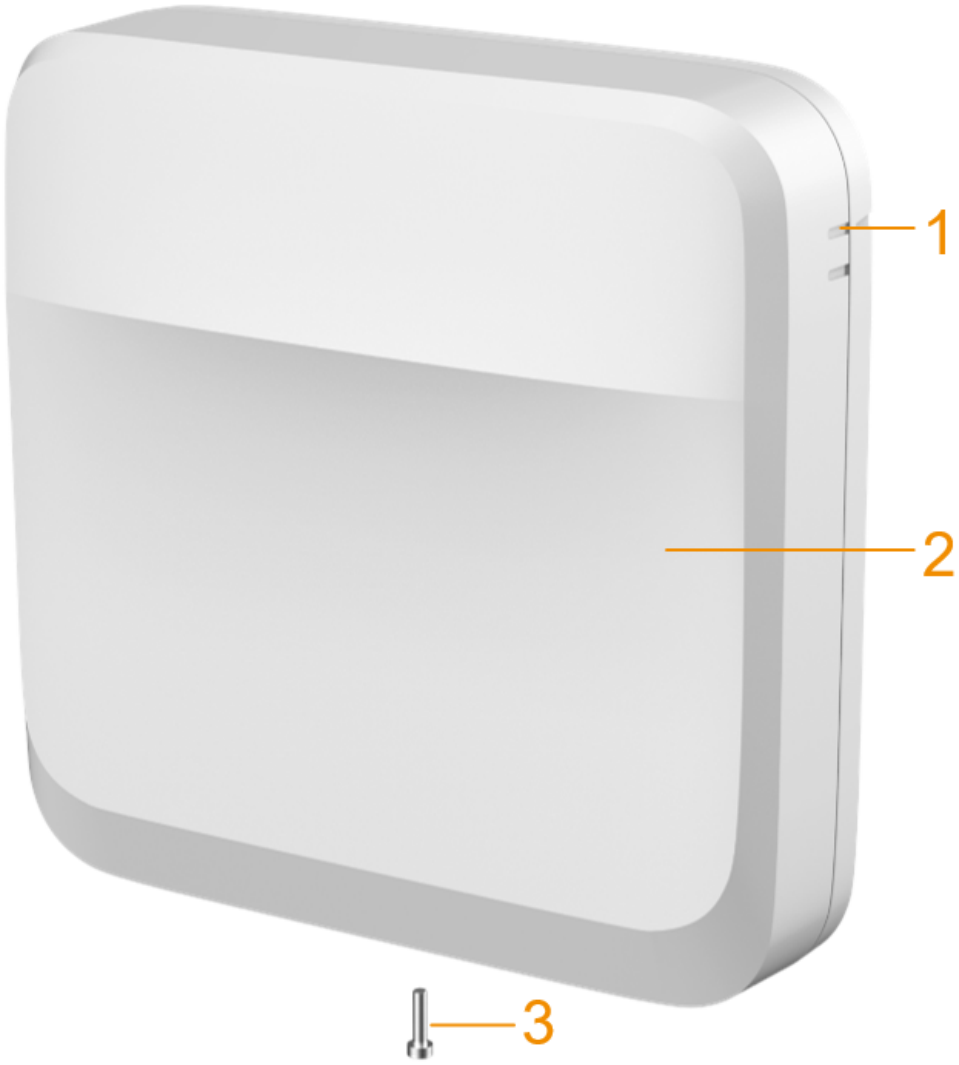


Table 1-1 Components description

No.	Description
1	Guiding mark
2	Front panel
3	Screw

Figure 1-3 Back cover

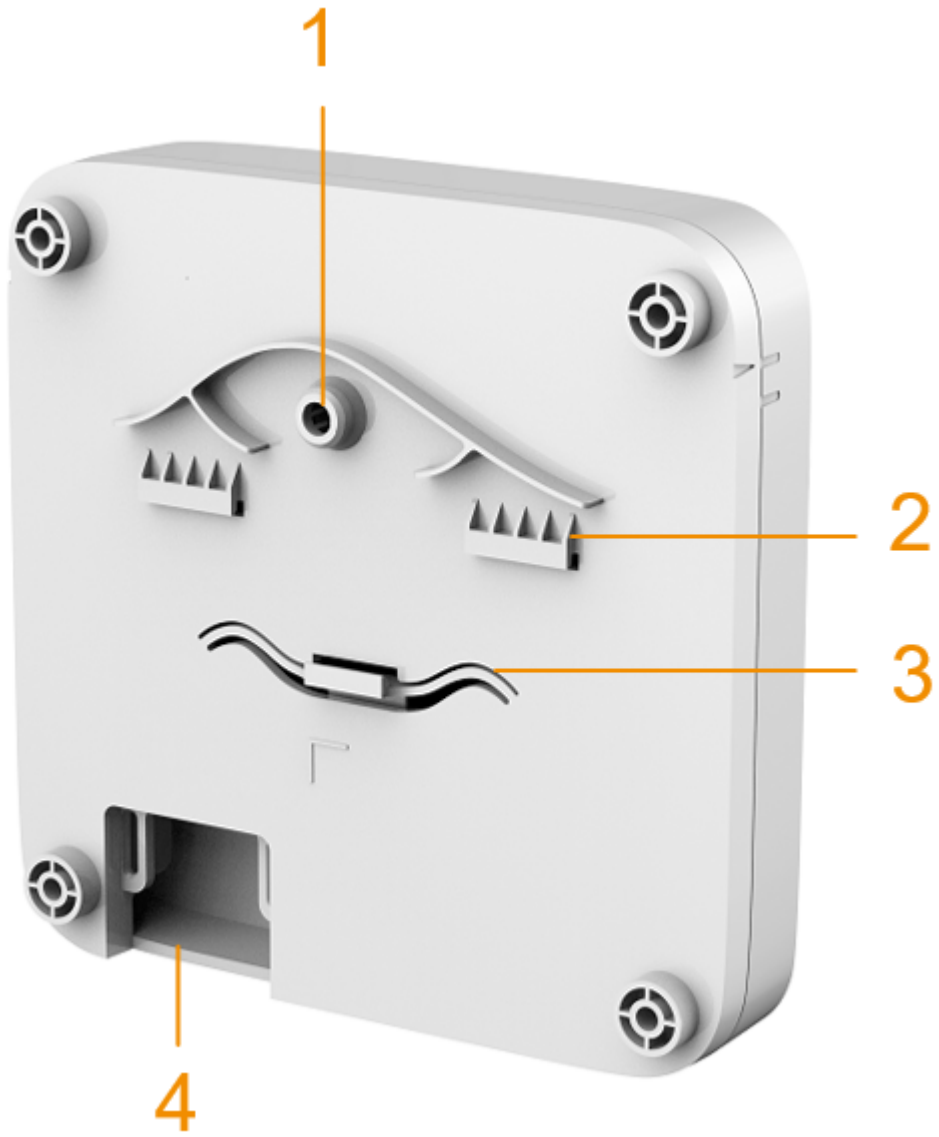


Table 1-2 Back cover description

No.	Description
1	Tamper alarm switch
2	Upper DIN clip
3	Lower DIN clip
4	Wiring outlet

2 Ports Overview

Figure 2-1 Ports

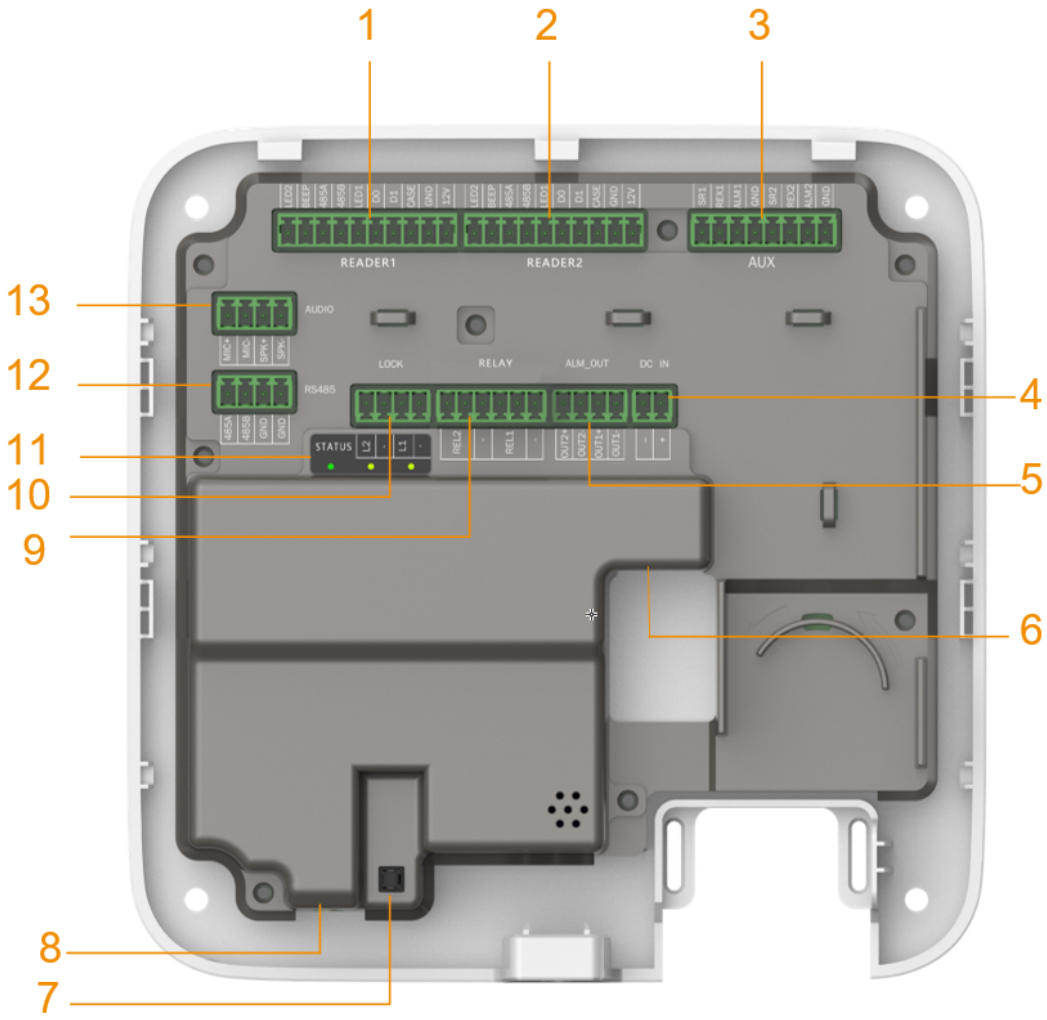


Table 2-1 Ports description

No.	Name	Description
1	READER1	Reader connector
2	READER2	Reader connector
3	AUX	Auxiliary connector This function is not available currently.
4	DC IN	Power connector
5	ALM_OUT	Alarm output connector
6	RJ45	Network connector PoE(802.3at)

No.	Name	Description
7	—	Tampering alarm switch
8	—	Reset button
9	RELAY	Relay connector This function is not available currently.
10	LOCK	Power lock connector This function is not available currently.
11	STATUS	LED indicator
12	RS485	RS485 connector (reserved port)
13	AUDIO	Audio connector (reserved port)

Figure 2-2 Reader connector

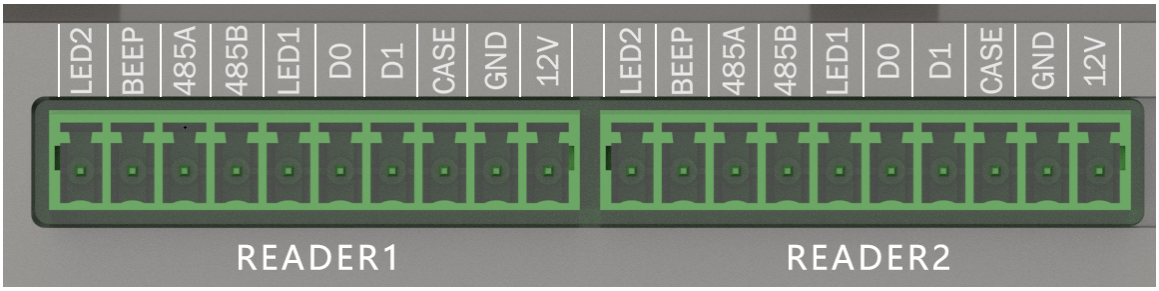


Table 2-2 Reader connector description

Port	Description
12 V	Supplies 12 VDC power for the reader.
GND	Connects the grounding wire.
CASE	Connects the reader tampering alarm.
D1	Connects a Wiegand reader.
D0	
LED1	Signal response. Connects to the signal wire of the Wiegand reader.
RS485B	Connects a RS-485 reader.
RS485A	
BEEP	Reserved port
LED2	Reserved port

Figure 2-3 Auxiliary I/O ports

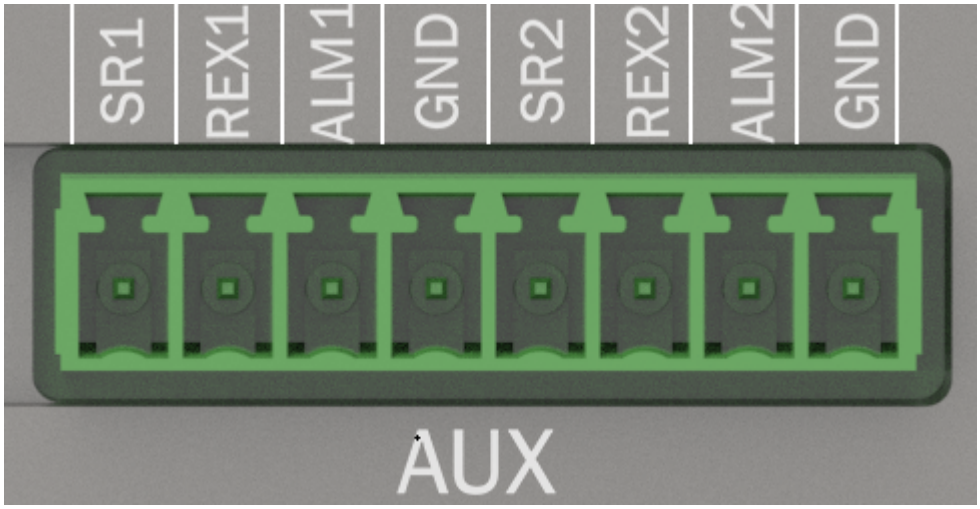


Table 2-3 Description of auxiliary I/O ports

Ports	Description
SR1	Reserved port
REX1	Reserved port
ALM1	Alarm input 1
GND	Grounding wire
SR2	Reserved port
REX2	Reserved port
ALM2	Alarm input 2
GND	Grounding wire

Figure 2-4 Power ports

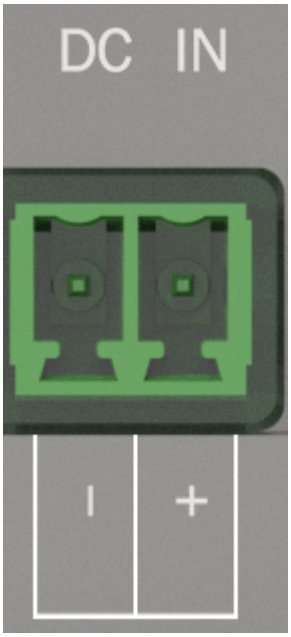


Table 2-4 Description of power ports

Ports	Description
–	Grounding wire
+	12 VDC. For powering the Elevator Controller when not using Power over Ethernet.

Figure 2-5 Alarm output ports

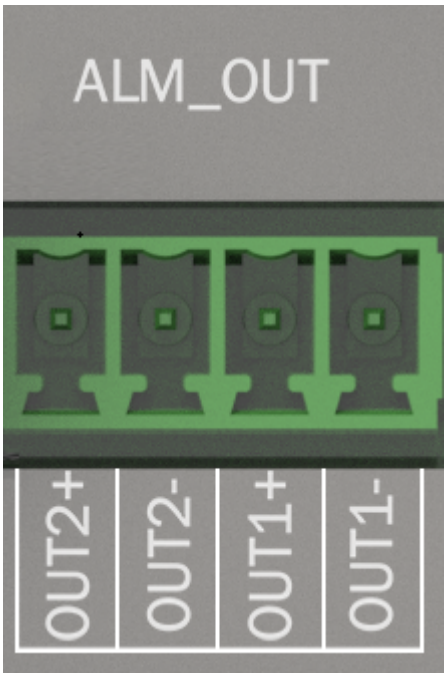


Table 2-5 Description of alarm output ports

Ports	Description
OUT2+	Alarm output 2
OUT2-	
OUT1+	Alarm output 1
OUT1-	

Figure 2-6 Relay ports

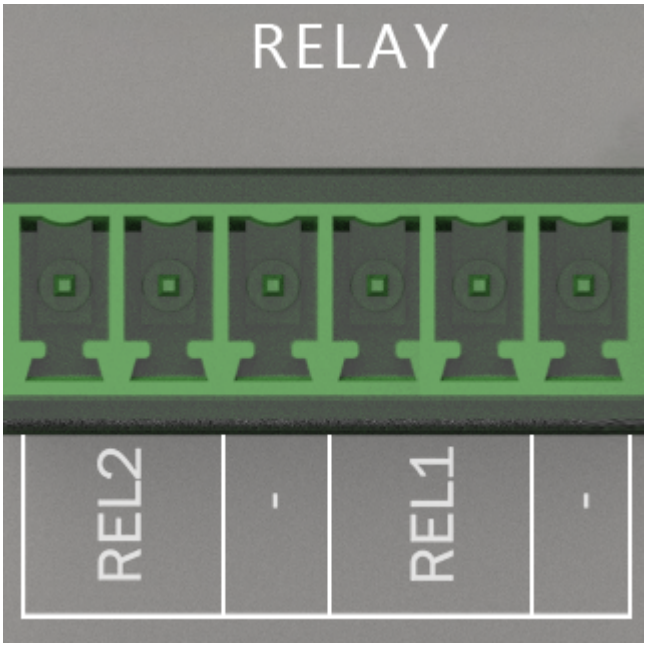


Table 2-6 Description of relay ports

Ports	Description
REL1	Reserved port
REL2	
–	Grounding wire

Figure 2-7 LED indicator

Table 2-7 Description of LED indicator ports

Port	Port Name	Indicator color	Status
STATUS	Power indicator	Solid green	Working normally.
		Solid red	The system starts.
		Blue light flashes	System is updating.
L2	Elevator 2 indicator	Solid yellow and green	The authentication succeeds.
		Solid red	The authentication fails.
L1	Elevator 1 indicator	Solid yellow and green	The authentication succeeds.

Port	Port Name	Indicator color	Status
		Solid red	The authentication fails.

Figure 2-8 RS-485 ports

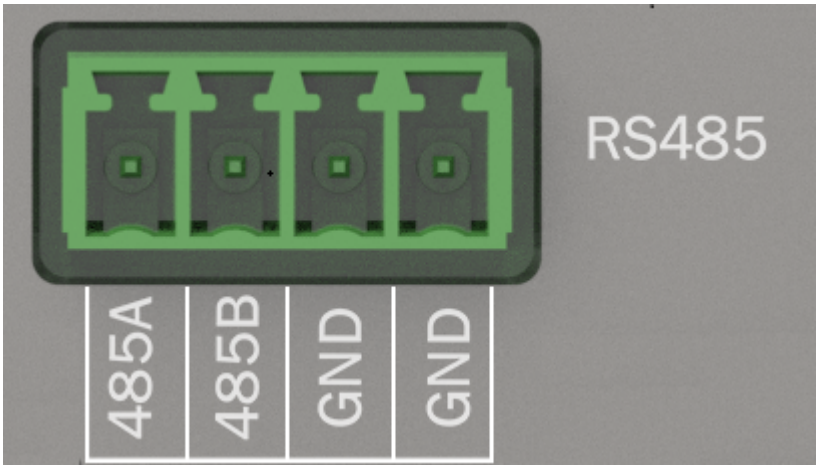


Table 2-8 Description of RS-485

Ports	Description
485A/485B	Reserved port
GND	Grounding wire

Figure 2-9 Audio ports

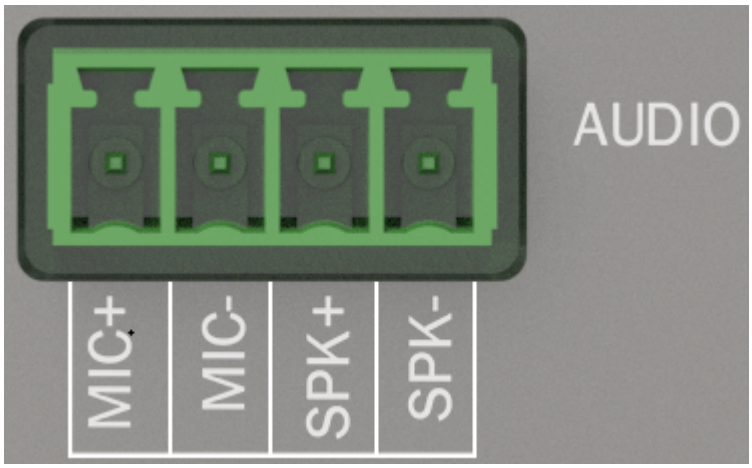


Table 2-9 Description of audio ports

Ports	Description
MIC+	Reserved port
MIC-	Grounding wire
SPK+	Reserved port
SPK-	Grounding wire

3 Installation

3.1 Wall Mount

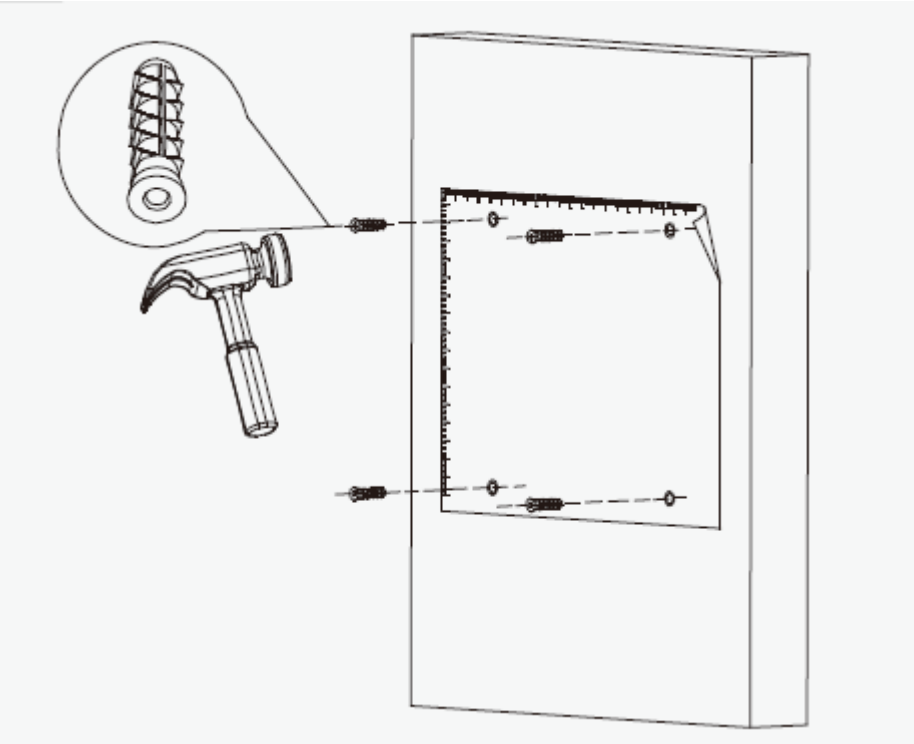
Procedure

Step 1 Paste the positioning map to the wall at an appropriate position.

Step 2 Drill holes through the marks on the map.

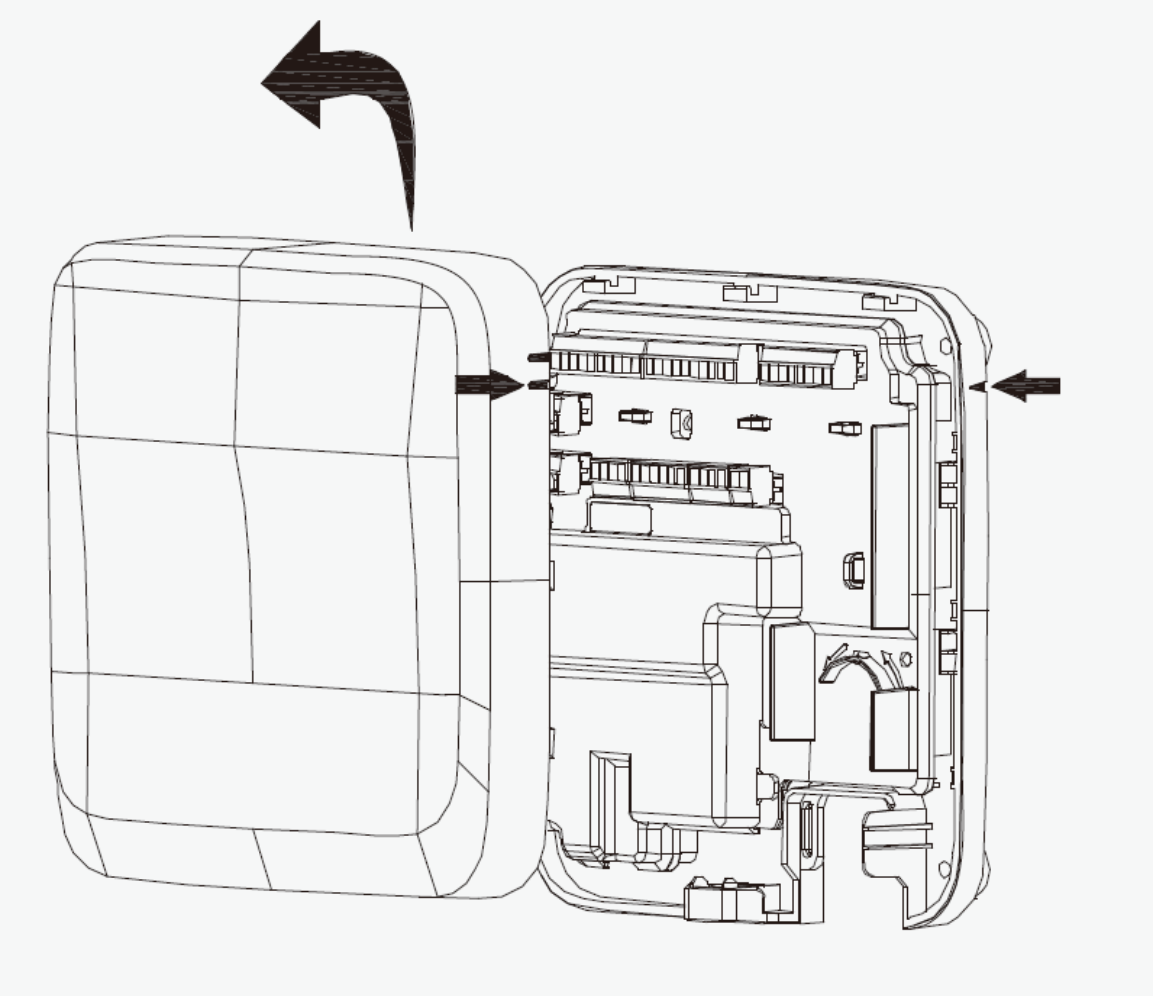
Step 3 Hammer in the expansion tubes, and then remove the map.

Figure 3-1 Hammer in the expansion tubes



Step 4 Slide up the front panel of the Elevator Controller and remove the panel.

Figure 3-2 Remove the front panel



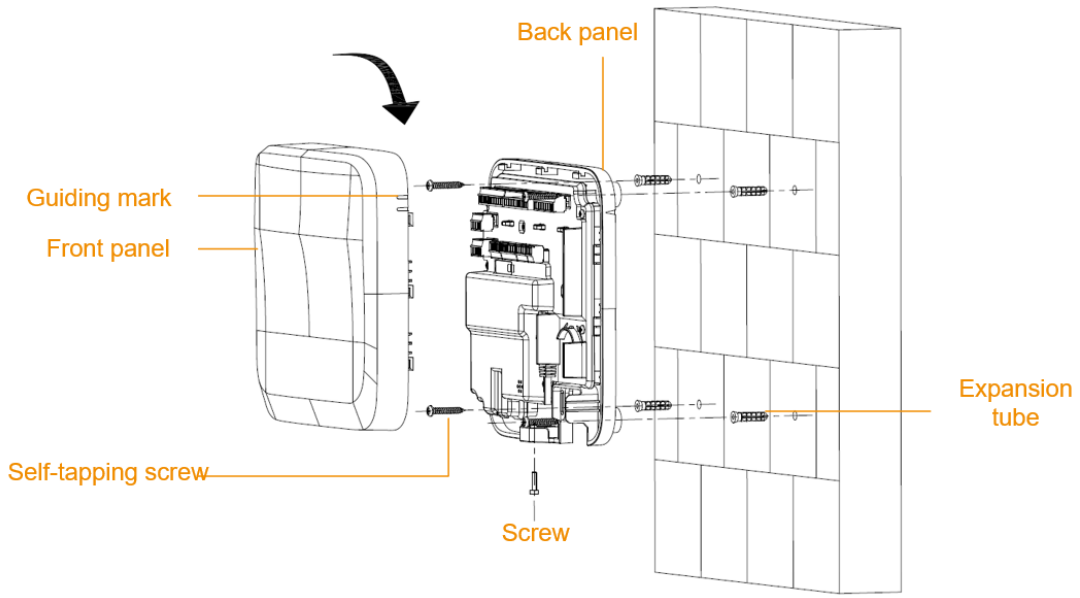
Step 5 Attach the back panel of the Elevator Controller to the wall with self-tapping screws.

Step 6 Wire the Elevator Controller, bind the wires with nylon cable ties, and then cut off the excess part of the ties.

Step 7 Align the marks on the front panel with the marks on the back panel, and then slide down the front panel to cover the Elevator Controller.

Step 8 Screw a screw into the bottom of the Elevator Controller to secure it.

Figure 3-3 Mount the Elevator Controller to the wall



Step 9 Remove the protection film.

3.2 DIN Rail Mount

Procedure

Step 1 Attach the DIN rail to the wall with screws.

The DIN rail does not come with the Elevator Controller.

Step 2 Hook the lower DIN clip of the back panel onto the bottom of the DIN rail, slightly push upwards the back panel, and then push the back panel backwards to hook the upper DIN clip onto the top of the DIN rail.

Make sure the clips "grip" the rail on both the top and bottom of the rail.

If you want to remove the Elevator Controller from the rail, simply push upwards on the DIN clip, remove the upper clip off the rail, and then lower the back panel to remove the lower clip off the rail. No screwdrivers or special tools are required.

Figure 3-4 DIN clips

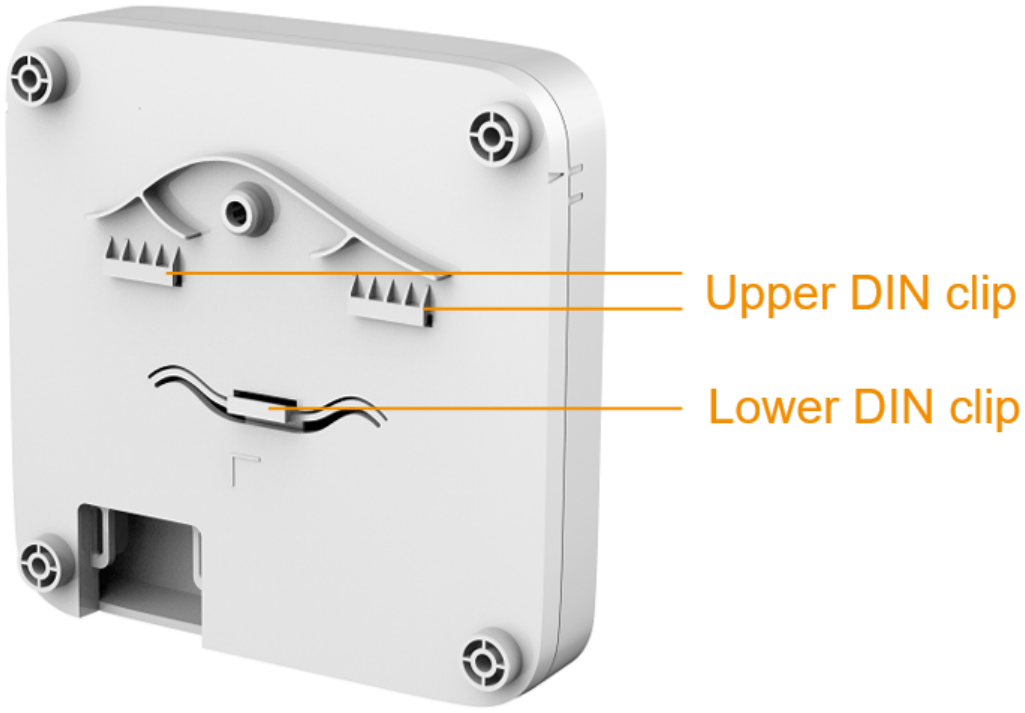
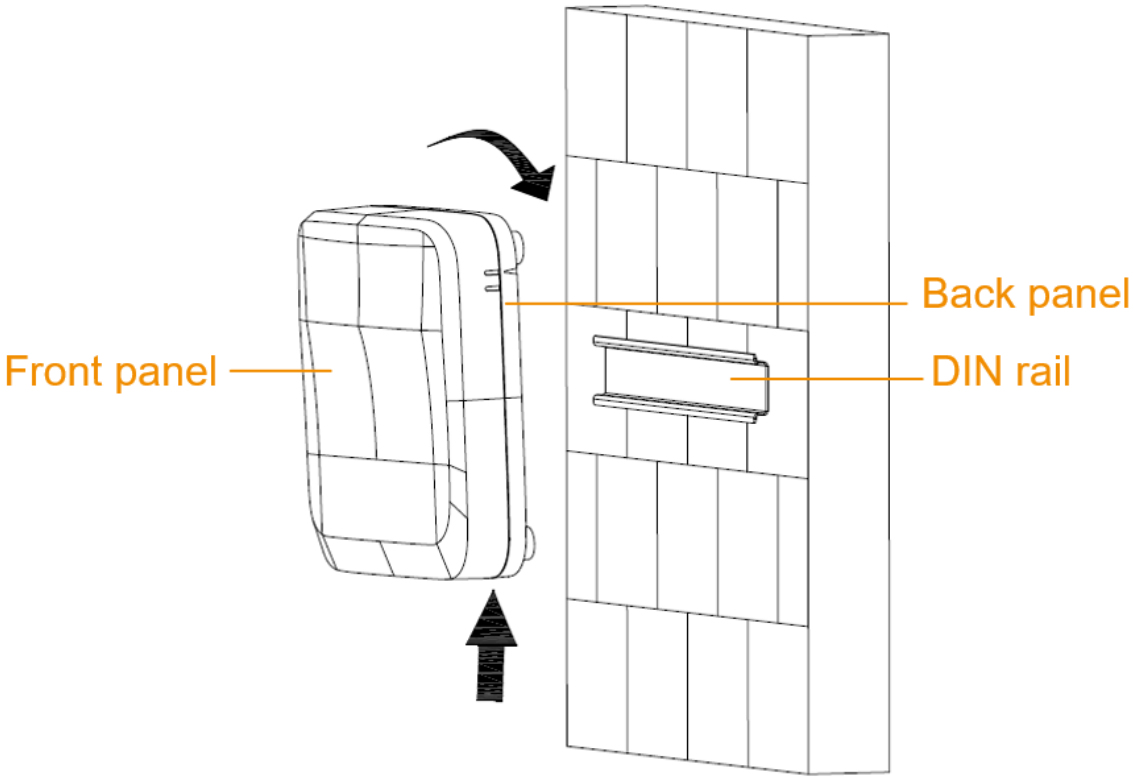


Figure 3-5 Hook DIN clips to the rail

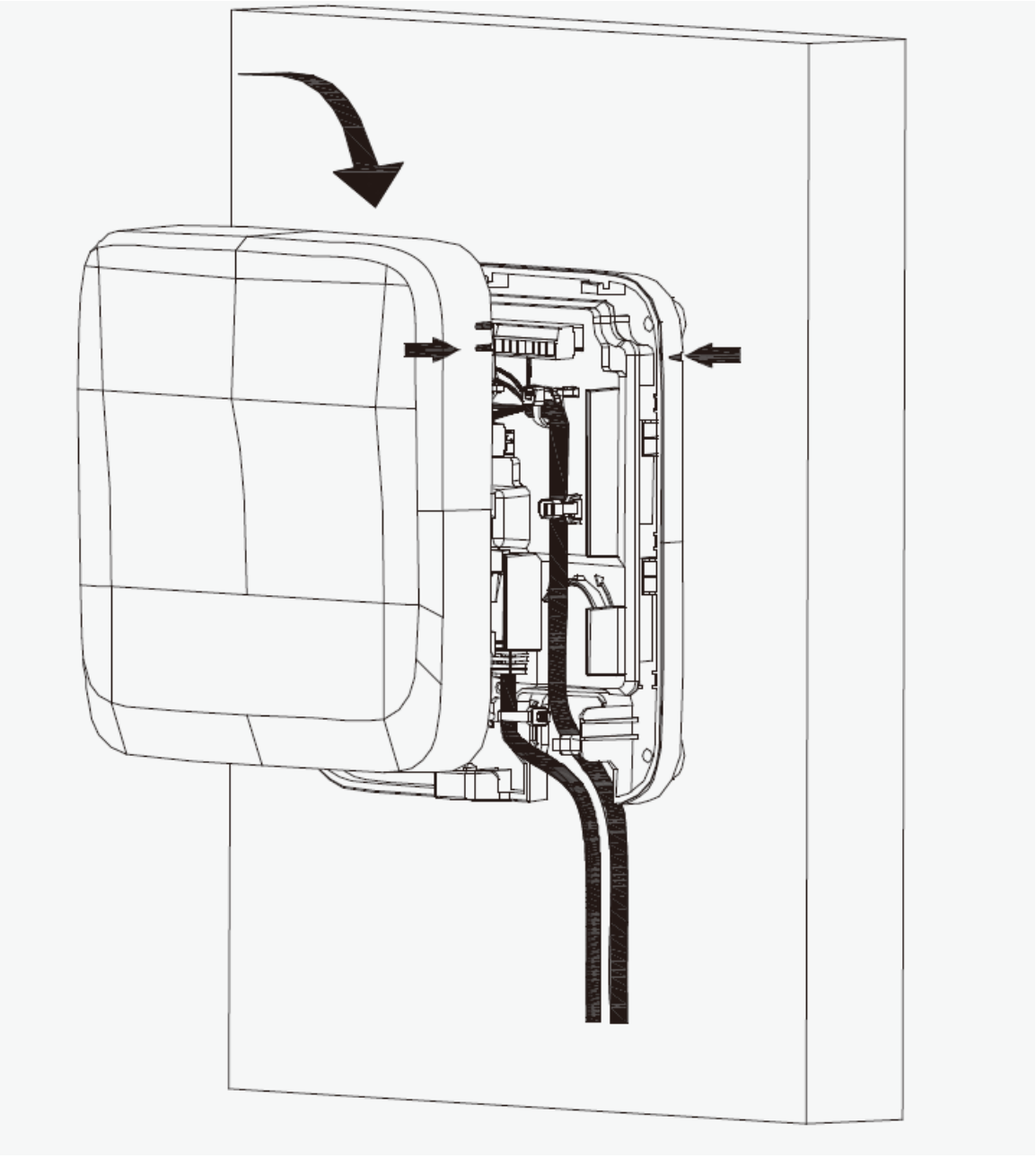


Step 3 Slide up the front panel of the Elevator Controller to remove the cover.

Step 4 Wire the Elevator Controller, bind the wires with nylon cable ties, and then cut off the excessive part of the ties.

Step 5 Align the marks on the front panel with the marks on the back panel, and then slide down the front cover to attach it.

Figure 3-6 Slide down the front cover



Step 6 Screw a screw into the bottom of the Elevator Controller to secure it.

Step 7 Remove the protection film.

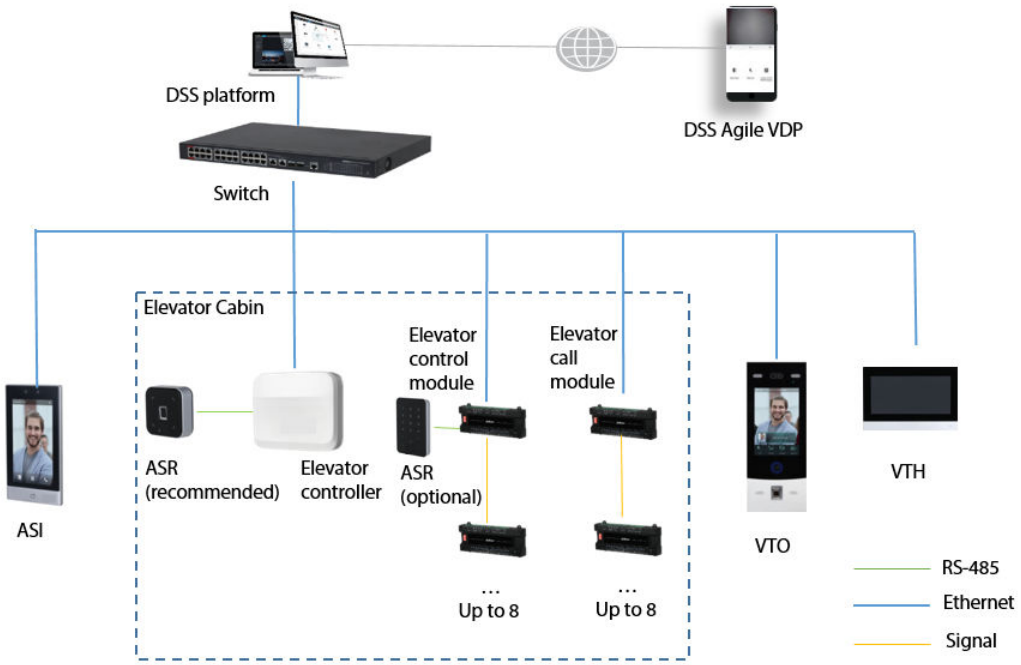
4 Elevator Control Configurations

4.1 Networking Diagram

The Elevator Controller supports the platform mode and the standalone mode.

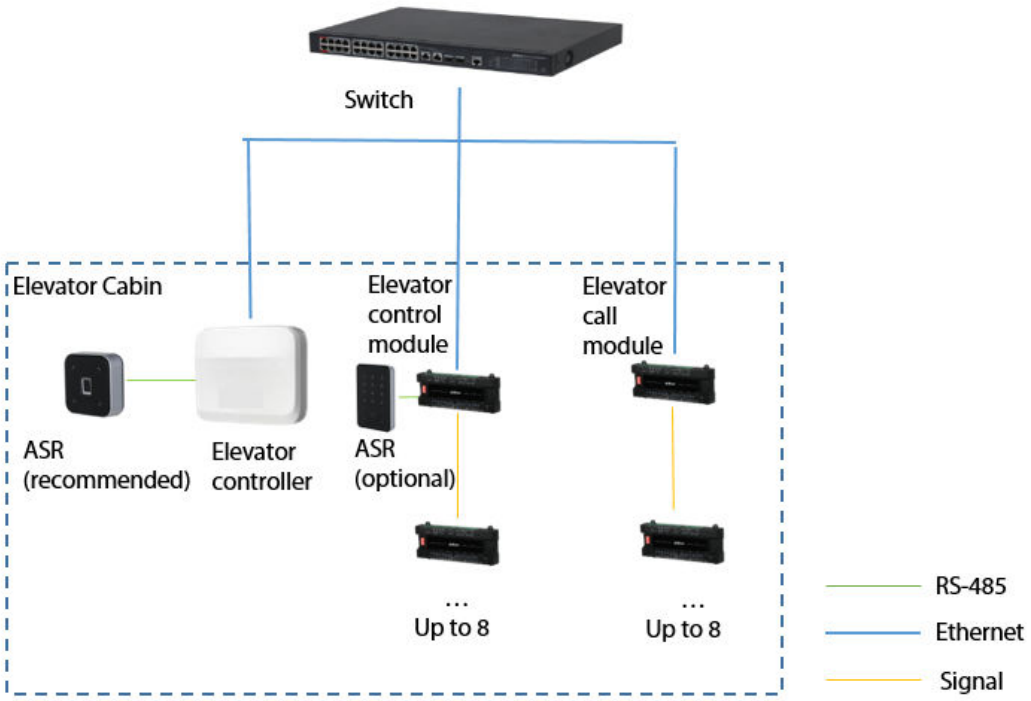
- The platform mode:
  - ◇ Add the Elevator Controller, face recognition access controller, and VTO to the DSS platform.
  - ◇ Add the Elevator Controller to the face recognition access controller and the VTO.
  - ◇ The elevator control module is connected to the Elevator Controller.
  - ◇ The card reader is connected to the Elevator Controller. The card, fingerprint, password and QR code on the card reader are supported when connected through RS-485. Only the card is supported when connected through Wiegand.
  - ◇ The card reader is connected to the elevator control module. The card and password on the card reader are supported when connected through RS-485. Only the card is supported when connected through Wiegand.

Figure 4-1 The platform mode



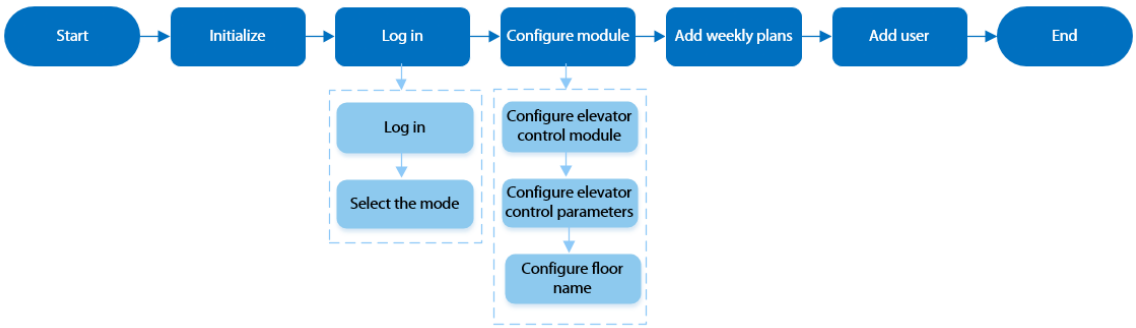
- The standalone mode:
  - ◇ Manage the people on the Elevator Controller.
  - ◇ The elevator control module is connected to the elevator controller.
  - ◇ Connect the sub elevator control module to the main elevator control module through the signal cable.
  - ◇ The card reader is connected to the Elevator Controller. The card, fingerprint, password and QR code on the card reader are supported when connected through RS-485. Only the card is supported when connected through Wiegand.
  - ◇ The card reader is connected to the elevator control module. The card and password on the card reader are supported when connected through RS-485. Only the card is supported when connected through Wiegand.

Figure 4-2 The standalone mode



4.2 Configuration Flowchart

Figure 4-3 Configuration flowchart



4.3 Initialization

Initialize the Elevator Controller when you log in to the webpage for the first time or after it is restored to its factory defaults.

Prerequisites

Make sure that the computer used to log in to the webpage is on the same LAN as the elevator controller.

Procedure

Step 1 Open a browser, go to the IP address (the IP address is 192.168.1.108 by default) of the elevator controller.

We recommend you use the latest version of Chrome or Firefox.

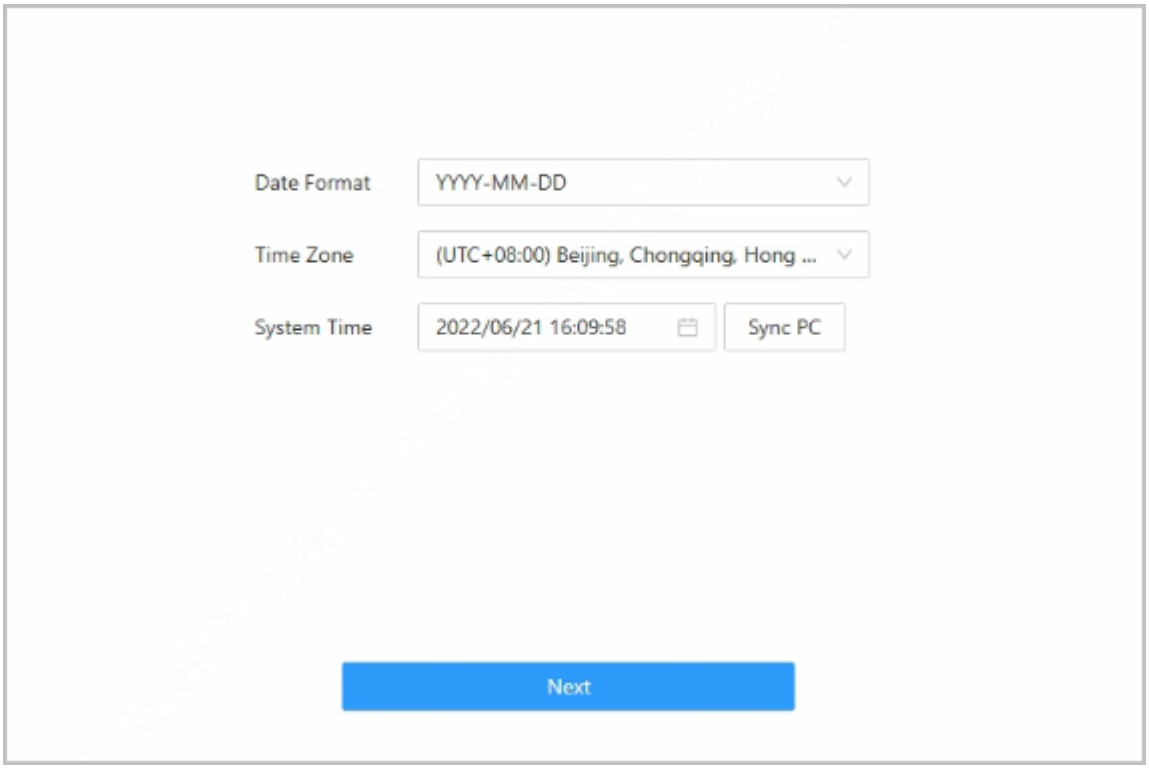
Step 2 Select a language, and then click **Next**.

Step 3 If there are the software license agreement and privacy policy, read them carefully, select **I have read and agree to the terms of the Software License Agreement and Privacy Policy.** , and then click **Next**.

The software license agreement and privacy policy are available on select models.

Step 4 Configure the system time, and then click **Next**.

Figure 4-4 Configure the time



Step 5 Set the password and email address.

- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case and lower case letters, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.
- Keep the password safe after initialization and change the password regularly to improve security.

Step 6 (Optional) Select **Auto Check for Updates** , and then click **Completed**.

The system automatically checks that if there is any higher version available, and informs the user to update the system.

Step 7 Click **Completed**.

The system automatically goes to the login page after initialization is successful.

4.4 Logging in

For first-time login after the initialization, you need to configure the mode. The elevator controller supports the platform mode and the standalone mode.

Procedure

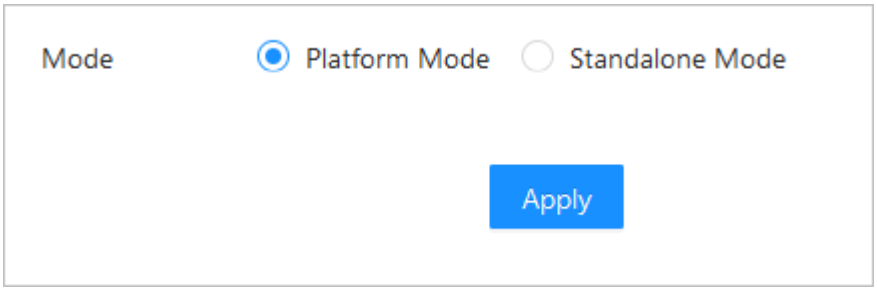
Step 1 On the login page, enter the username and password.

- The default administrator name is admin, and the password is the one you set during initialization. We recommend you change the administrator password regularly to increase the security of the platform.
- If you forget the administrator login password, you can click **Forgot password?**.

Step 2 Select the mode, and then click **Apply**.

- Platform mode: The platform sends the people information, the time template and the floor permissions.
- Standalone mode: Manage the people information, configure the time template and the floor on the Elevator Controller.

Figure 4-5 Select the mode



4.5 Configuring Module

We recommend you use one elevator controller for one elevator.

4.5.1 Configuring Elevator Control Module

You can add the elevator control module to the elevator controller.

Prerequisites

Before adding the module, make sure that the elevator controller and the elevator control module are in the same network and can be connected through the network.

Procedure

Step 1 On the home page, select **Elevator Control Module** > **Elevator Control Module**.

Step 2 Click , and then configure the module.

Figure 4-6 Elevator control module

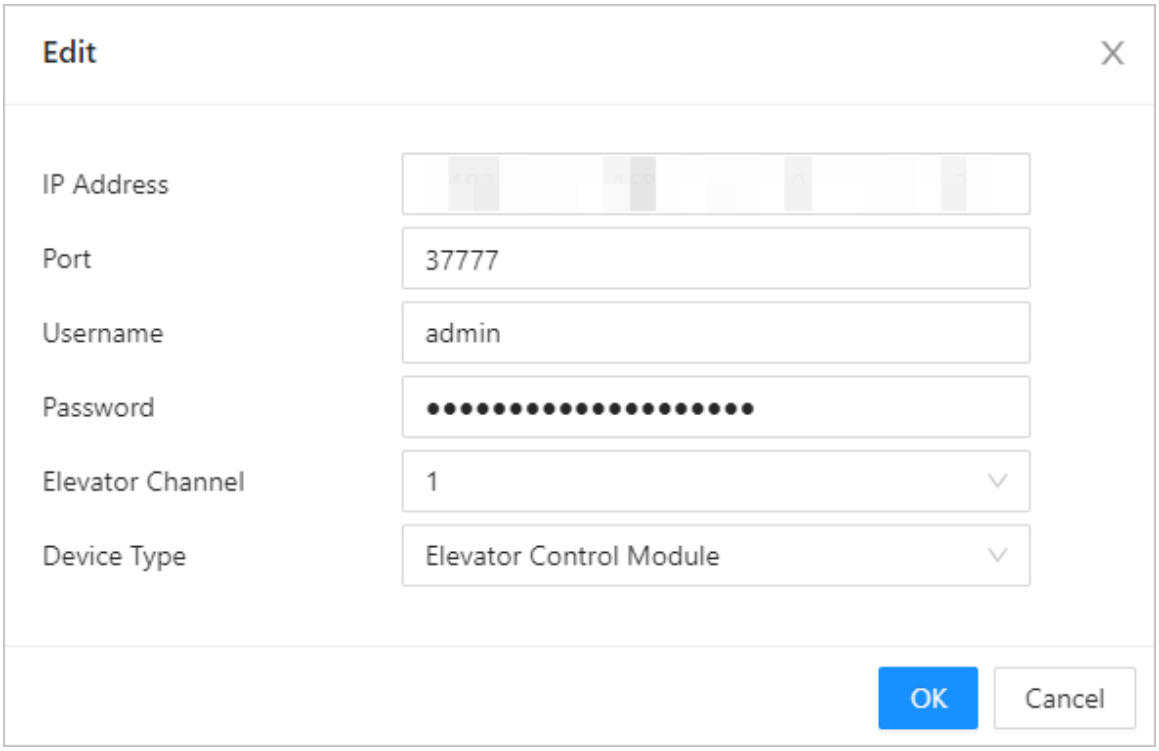


Table 4-1 Device parameters description

Parameter	Description
IP Address	Enter the IP address of the elevator control module.
Port	The port number is 37777 by default.
Username/Password	Enter the username and password of the elevator control module.
Elevator Channel	Select from **1** and **2**.
Device Type	Select from **Elevator Control Module** and **Elevator Call Module**.

Step 3 Click **OK**.

4.5.2 Configuring Elevator Control Parameters

Configure basic parameters for the elevator channel 1 and channel 2.

On the home page, select **Elevator Control Module** > **Elevator Control Config**. Configure the parameters, and then click **Apply**.

Figure 4-7 Elevator control configuration

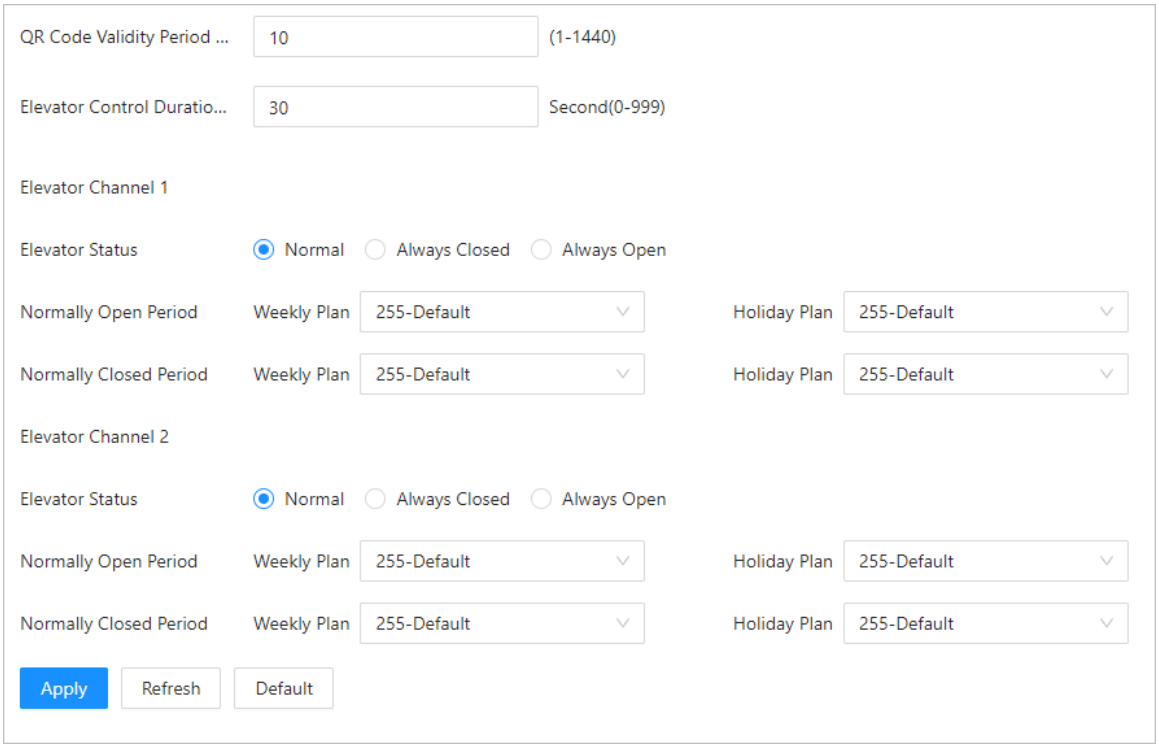


Table 4-2 Description of elevator control parameters

Parameter		Description
QR Code Validity Period (min)		Configure the validity period for the QR code that is generated for the host. Hosts can access to the elevator using the QR code within the configured period.
Elevator Control Duration		Configure the elevator control duration. It is 10 seconds by default. The value ranges from 0 second to 999 seconds.
Elevator Channel 1/Elevator Channel 2	Elevator Status	Configure the elevator status for the elevator channel 1 or elevator channel 2. ● Normal: Authentication mode. After configuring weekly plan and holiday plan, the elevator can be accessed within the configured period. The holiday plan has the priority over the weekly plan. ● Always closed: The elevator is not running. ● Always open: You can access to the elevator without verification.

Parameter		Description
	Normally Open Period	If you select **Normal** as the elevator status, configure the normally open period for weekly pan and holiday plan. The elevator can be accessed within the configured period. The holiday plan has the priority over the weekly plan. Normally open period has priority over the normally closed period. For example, if you select the same weekly plan for normally open period and the normally closed period, during the period, the elevator normally opens.
	Normally Closed Period	If you select **Normal** as the elevator status, configure the normally closed period for weekly plan and holiday plan. The elevator cannot be accessed within the configured period. The holiday plan has the priority over the weekly plan.

4.5.3 Configuring Floor Name

Procedure

Step 1 On the home page, select **Elevator Control Module** > **Floor Config**.

Step 2 Add the floor.

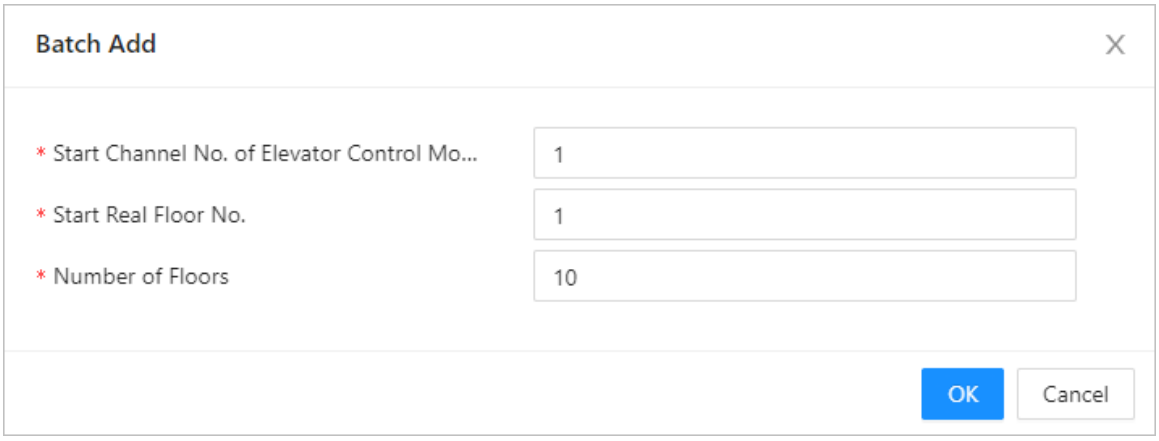
You can add up to 128 elevator control module channels.

- Click **Add**, and then enter the elevator control module channel number and the real floor name.

Figure 4-8 Add the floor

- Click **Batch Add**, and then enter the start channel number of the elevator control module, the start real floor number and the number of floors.

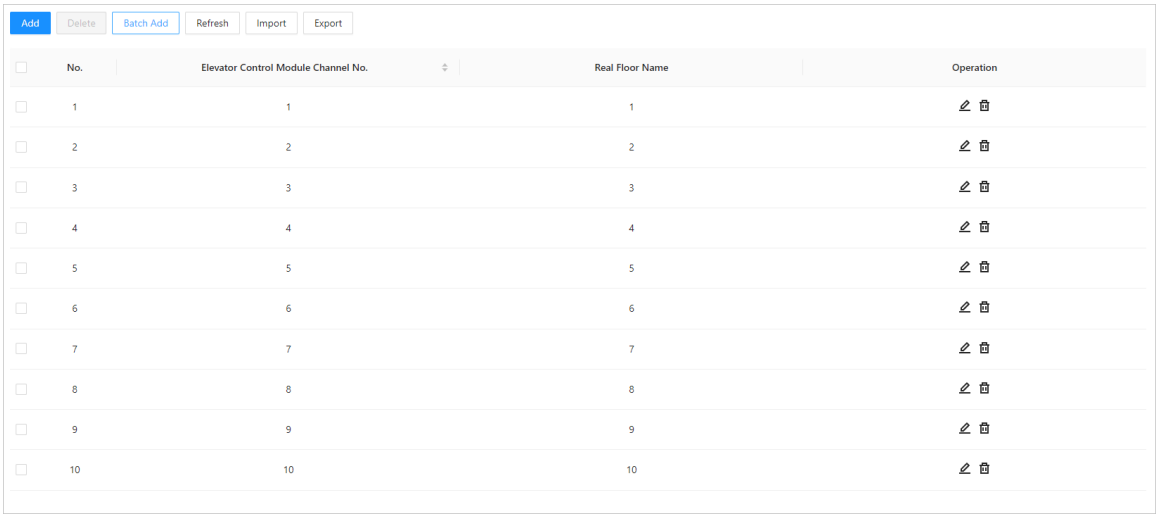
Figure 4-9 Add the floor in batches



Step 3 Click **OK**.

View the floor number and the real floor name in the list. Click the channel number of the elevator control module to sort in ascending or descending order.

Figure 4-10 Floor list



4.6 Adding Weekly Plans

The weekly plan is used to set the elevator control schedule for the week. You can also create your own templates.

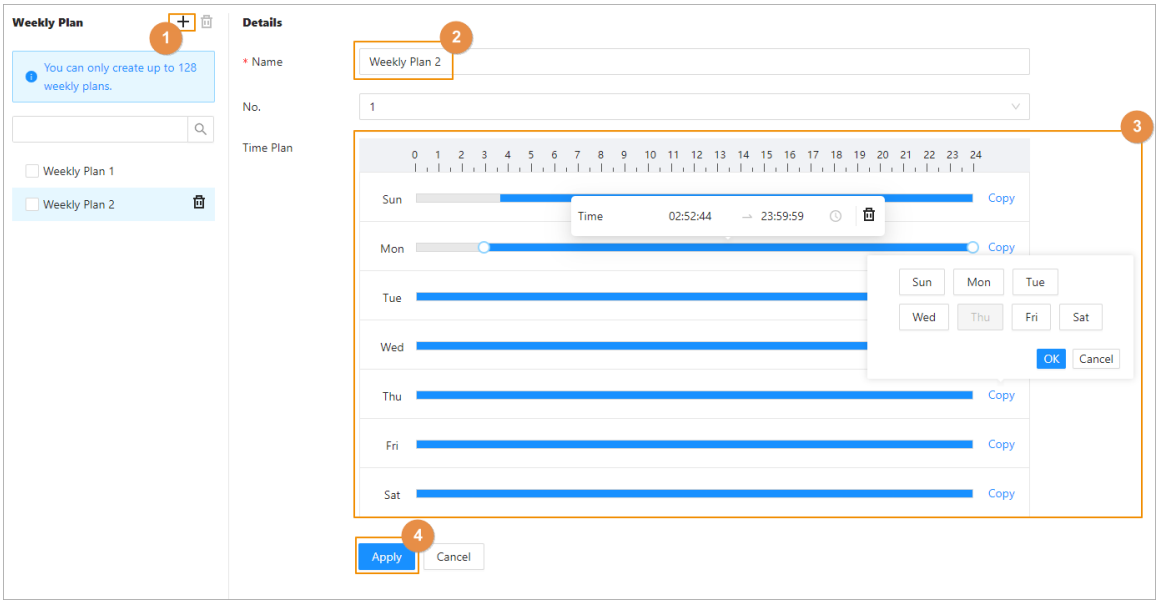
Procedure

Step 1 On the home page, select **Weekly Plan**, and then click + .

You can create up to 128 weekly plans.

Step 2 Enter the name of the time template.

Figure 4-11 Create the weekly plan



Step 3 Drag the slider to adjust the time period for each day.

You can also click **Copy** to apply the configured time period to other days.

You can only configure up to 4 time sections for each day.

Step 4 Click **Apply**.

4.7 Adding Users

Procedure

Step 1 On the home page, select **Person Management**.

Step 2 Add users.

- Add users one by one.
  1. Click **Add**, and then enter the basic information on the user.

Figure 4-12 Basic information on the user

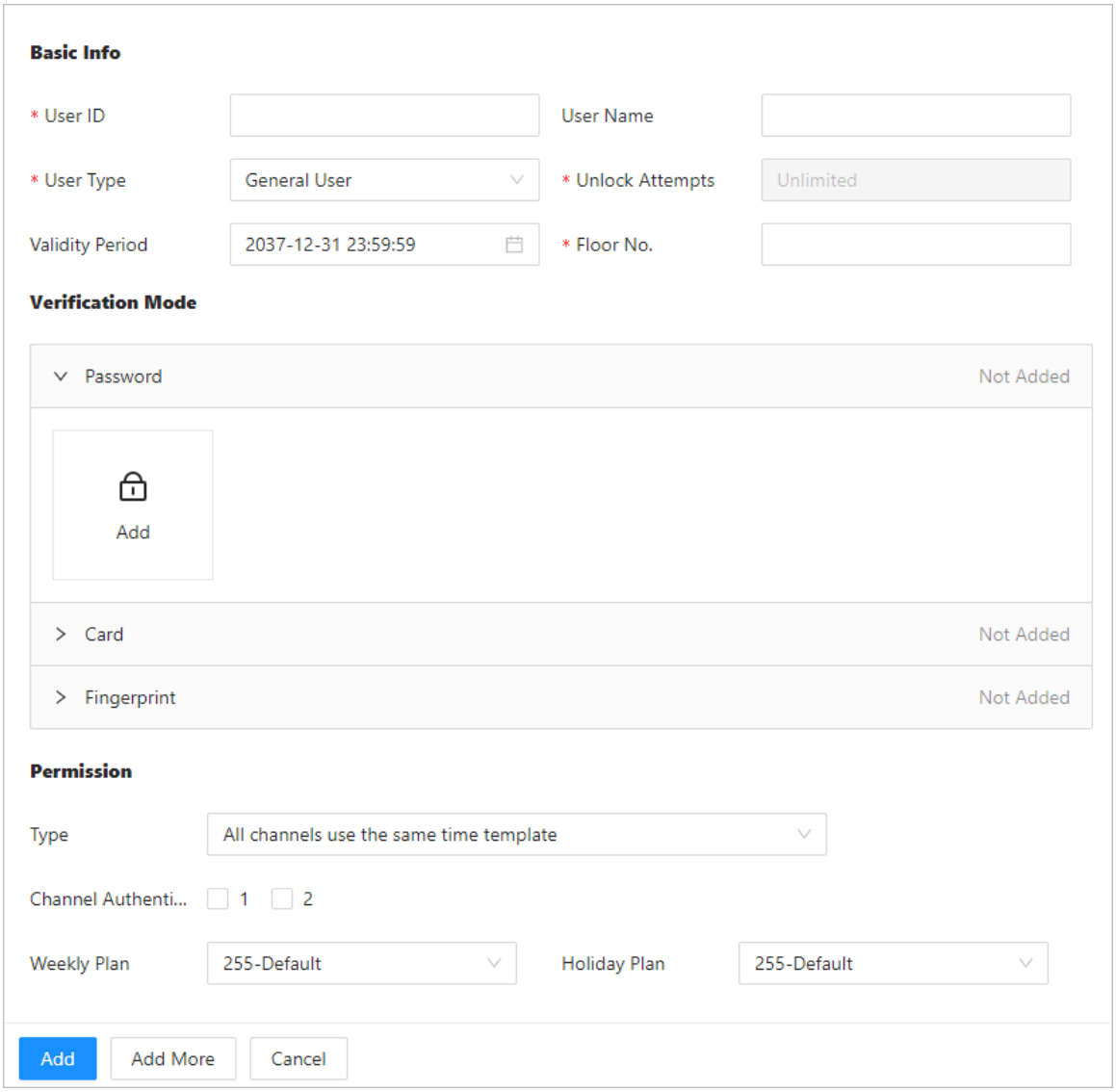


Table 4-3 Parameters description

Parameter	Description
User ID	The ID of the user.
User Name	Enter the name of the user.
User Type	◇ **General User** , **VIP User**, **Patrol User**, **Other User**, and **Custom User 1/Custom User 2**: Can access floors that they were granted permission for within the configured validity period. ◇ **Guest User** : Can access floors within a defined period or for a set number of times. After the period expires or they reach the limit for the number of accessing to the elevator, they cannot access the floor anymore. ◇ **Blocklist User** : The users in the blocklist cannot access floors.

Parameter	Description
Unlock Attempts	The number of times a guest user can access floors. This parameter can be configured when the user type is **Guest User**.
Validity Period	Set a date on which the access permissions of the person will become effective.
Floor No.	Select the floors, and the person has access to the selected floors. If there is no floor to be selected, please configure the floors first.

2. Configure the verification method for the user.

   Add password, cards, or fingerprints to users, so that users can access floors through authentication. Each user can have up to 1 password, 5 IC/ID cards and 3 fingerprints.

Figure 4-13 Add the password (example)

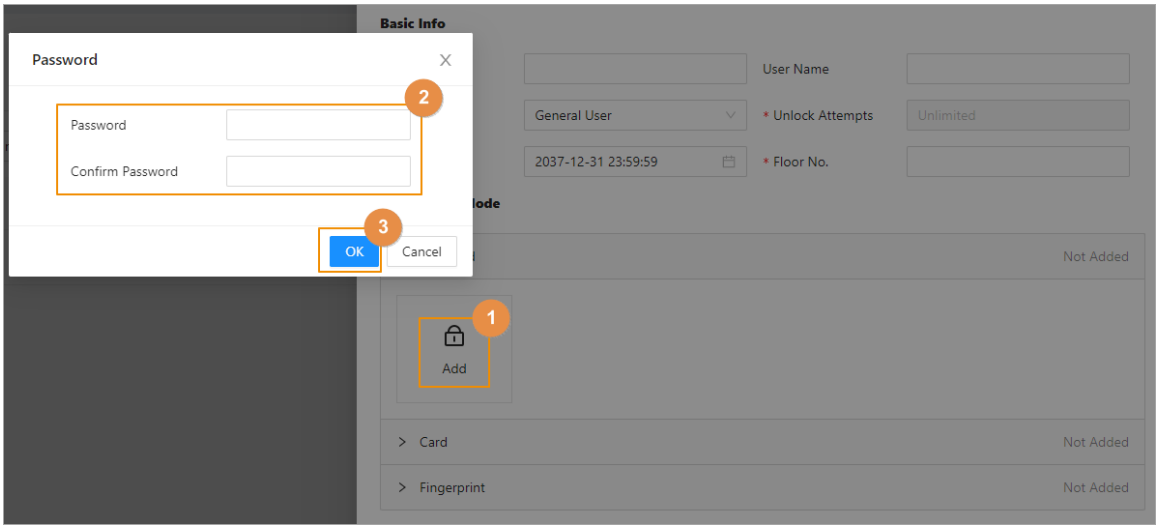


Table 4-4 Parameters description

Parameter	Description
Password	a. Click **Add**. b. Enter and confirm the password. The password must include 6 numbers. The length of user ID and password should not exceed 18. c. Click **OK**. People can access floors by entering ***user ID#Password#*** on face recognition access controller, door station or card reader. For example, the user ID is 2, and the password is 123456. You can enter 2#123456# to be recognized and access floors in the elevator.
Card	a. Click **Add**. b. Swipe the card or enter the card number to add the card. ◇ Click **Modify** to select the card reader device that connecter to the Elevator Controller or the USB scanner that connected to the computer, and then swipe the card on the corresponding device. The card number will be displayed on the platform. ◇ Enter the card number. c. Click **Add**. ◇ : Change the number of the card. ◇ : Set the card to duress card. An alarm is triggered when people use the duress card to unlock the door. ◇ : Delete the card.
Fingerprint	a. Click **Add**. b. Follow the on-screen instructions to register the fingerprint. Click **Modify** to select the card reader device that is connected to the elevator controller or the USB scanner that connected to the computer, and then register the fingerprint on the corresponding device according to the instructions. c. Click **Add**.

3. Configure the permission for the user.

   Select the type that whether all the channels use the same template, select channel authentication, and then select the weekly plan and the holiday plan.
4. Click **Add**.

   You can click **Add More** to add more users.

- Add users through importing the template.
  1. Click **Import** > **Download Template** to download the user template.
  2. Enter user information in the template, and then save it.

3. Click **Import**, and upload the template to the Elevator Controller.

   The users are added to the Elevator Controller automatically.

Appendix 1 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

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

2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. **Set and update password reset information in a timely manner**

   The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access web services through secure channels.

2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

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

4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**

   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

   By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.
3. **Configure network log**

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

Software Security

1. **Update firmware in time**

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

   It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).