EC20 Elevator Controller

User Manual

V1.0

Table of Contents

Foreword

Introduction

This manual introduces the installation, functions and operations of the elevator controller (hereinafter referred to as "the Controller"). Please read carefully before using the Controller, and keep the manual for future reference.

Symbol Conventions

The symbols that might be found in this guide are defined as follows.

Symbol	Description
⚠ DANGER	Indicates a hazardous situation that, 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 potentially hazardous situation which, if not avoided, could result in property damage, data loss, performance degradation, or unexpected results.
TIP	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Changes	Release Date
V1.0	First release.	January 2026

About the Manual

- The Manual is for reference only. Slight differences might be found between the manual and the Controller.
- We are not liable for losses incurred due to operating the Controller in ways that are not in compliance with the manual.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Safety Instructions

To ensure safe and reliable operation of the Controller, please strictly observe the following precautions during installation, commissioning, operation, and maintenance:

- Installation and commissioning must be performed by qualified technicians only. Before installation, verify that the on-site power supply, elevator control method, and interface types meet the product requirements. Perform all wiring according to the wiring diagram and confirm correct power polarity and communication wiring to prevent damage or malfunction.
- Use shielded twisted-pair cables for communication and route them away from high-voltage lines, motors, and elevator main power supply to reduce interference. Do not connect or disconnect power or signal cables while the system is powered on. Securely mount the device inside the elevator control cabinet or low-voltage enclosure to prevent loosening caused by vibration.
- The Controller is supplied with a power supply. Do not replace the power supply or apply voltage outside the rated range. Ensure proper grounding to protect the equipment from static electricity, lightning, and surge currents.
- Confirm that all hardware connections are correct before first power-on. Configure system parameters (such as number of floors, access rules, and communication addresses) according to the actual condition. Do not put the Controller into service until commissioning and testing are completed. After modifying key parameters, re-test all access authorization and elevator call functions.
- The Controller controls permissions only and must not replace the elevator's safety protection systems. In case of abnormal operation, ensure elevator safety first and switch to non-elevator-control mode if required. Do not disassemble, modify, or tamper with the Controller.
- Regularly inspect the terminals for looseness and check for dust or moisture. Power off the Controller before cleaning, and never use corrosive liquids.
- The Controller is an auxiliary control device and must be compatible with the elevator manufacturer before use. The manufacturer is not responsible for damage or safety incidents caused by improper use in violation of this manual.
- For information not covered in this manual, refer to the latest technical documentation or technical support provided by the manufacturer.

Chapter 1 Product Introduction

1.1 Overview

The EC20 Elevator Controller is an intelligent device designed for managing floor access in elevators. By integrating with elevator, access control system, and management platform, it provides precise assignment of floor permissions to residents and visitors to improves access safety and management efficiency, making it suitable for residential communities, commercial buildings, and office buildings.

1.2 Components

The Controller consists of the elevator master controller (EC20-1), elevator sub-controller (EC20-2), protocol conversion panel (EC20-3), power supply, and other modules.

Table 1-1 Description of product components

Component	Description
EC20-1	The core of the Controller, responsible for command distribution and data exchange. It sends floor authorization signals to the sub-controller when receiving access information from access control devices or authentication terminals.
EC20-2	Expands floor outputs or provides permission control for multiple elevators. By communicating with the EC20-1, it controls elevator buttons to enable multi-floor and multi-elevator operation to meet complex project deployments.
EC20-3	Facilitates communication between elevator mainboards with different protocols and allows management of the EC20-1.

NOTE

- This manual serves as a reference guide for the better comprehension and operation of the Controller.
- The manual may not reflect the latest software version. For assistance, you can refer to the device's built-in help interface or download the latest user manual from the Fanvil official website.

1.3 Specification

Table 1-2 Product specification

Category	Parameter	Description
Communication	Upstream	TCP/IP
	Downstream	RS-485, Wiegand 26/34
Environment	Operating Temperature	−30 °C to +70 °C (−22 °F to +158 °F)
	Storage Temperature	−40 °C to +70 °C (−40 °F to +158 °F)
	Operating Humidity	10% to 90% (RH), non-condensing
Performance	Power Input	110 V / 220 V AC ± 10%, 60/50 Hz (Built-in 12 VDC, 3 A)
	Number of Floors	16, expandable to 128
Data Storage	User Capacity	50,000
Interfaces	Sub-controller Interface	The master controller provides a single output port, to which all sub-controllers are connected in a serial daisy-chain.
	RS-485	4 channels: 1 set of protocol conversion panel, 1 card reader, and 1 reserved channel
	Wiegand 26/34	1 channel
	Fire Alarm	1 fire alarm input
	Network	1 RJ45 10/100 Mbps self-adaptive Ethernet port
Dimension	Product Dimension	370.0 mm × 260.0 mm × 65.0 mm (14.57" × 10.24" × 2.56") (L × W × H)
Installation	Installation Method	Wall mounting or installed on top of the elevator car

Chapter 2 Installation

2.1 Packing List

Table 2-1 Packing list

No.	Items	Description
1	EC20-1	Elevator master controller, installed inside the product.
2	EC20-2	1 sub-controller installed inside the product, controlling up to 16 floors. Purchased separately for floor expansion.
3	EC20-3	Protocol conversion panel, installed inside the product.
4	Switch Mode Power Supply (SMPS)	12 VDC, 5 A; installed inside the product.
5	Switch	Switch of the EC20-1.
6	Power Cable	1 meter in length for SMPS.
7	QIG	Quick Installation Guide.
8	Ribbon Cable	Purchased separately for floor expansion.

2.2 Installing the Controller

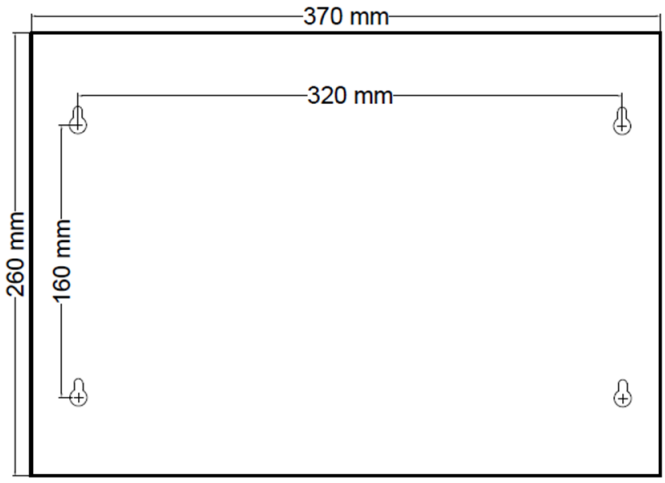
The Controller supports wall mounting, but we recommend installing it on the top of the elevator car.

> ⚠ **WARNING**
>
> Ensure that the device enclosure is properly grounded during the installation.

Procedure

1. Drill holes according to the box's mounting positions, and then insert expansion anchors into the holes.
2. Align the box to hole positions, and then secure it with expansion bolts.

Figure 2-1 Product dimensions

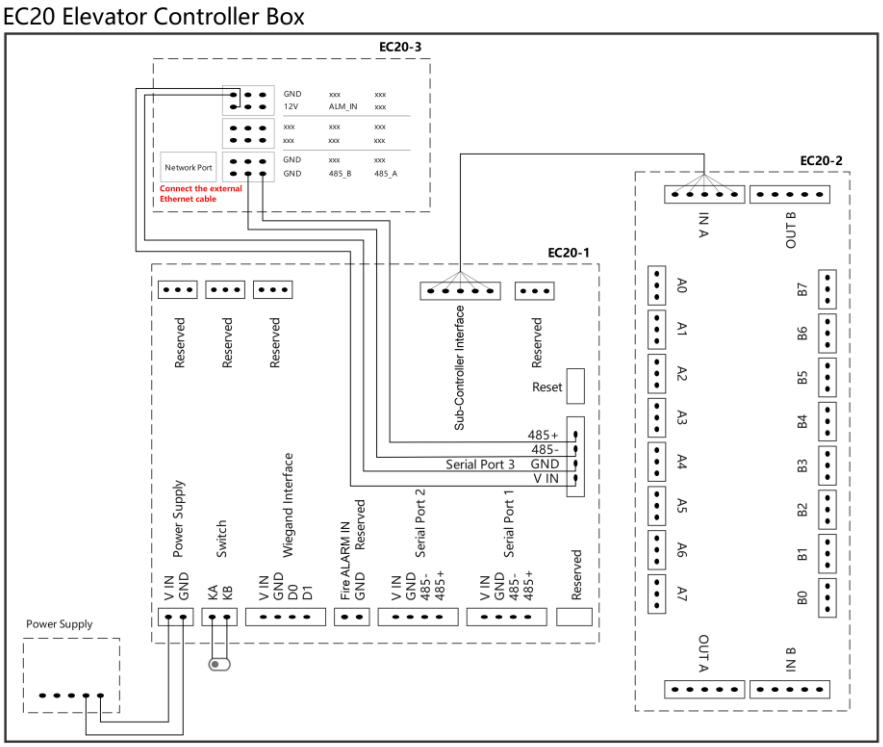


2.3 Wiring

2.3.1 Internal Wiring of the Device

The internal wiring of the Controller is completed at the factory. After receiving the device, you only need to verify that the internal connections are correct and secure. Disassembly or rewiring is not recommended.

Figure 2-2 Internal wiring diagram

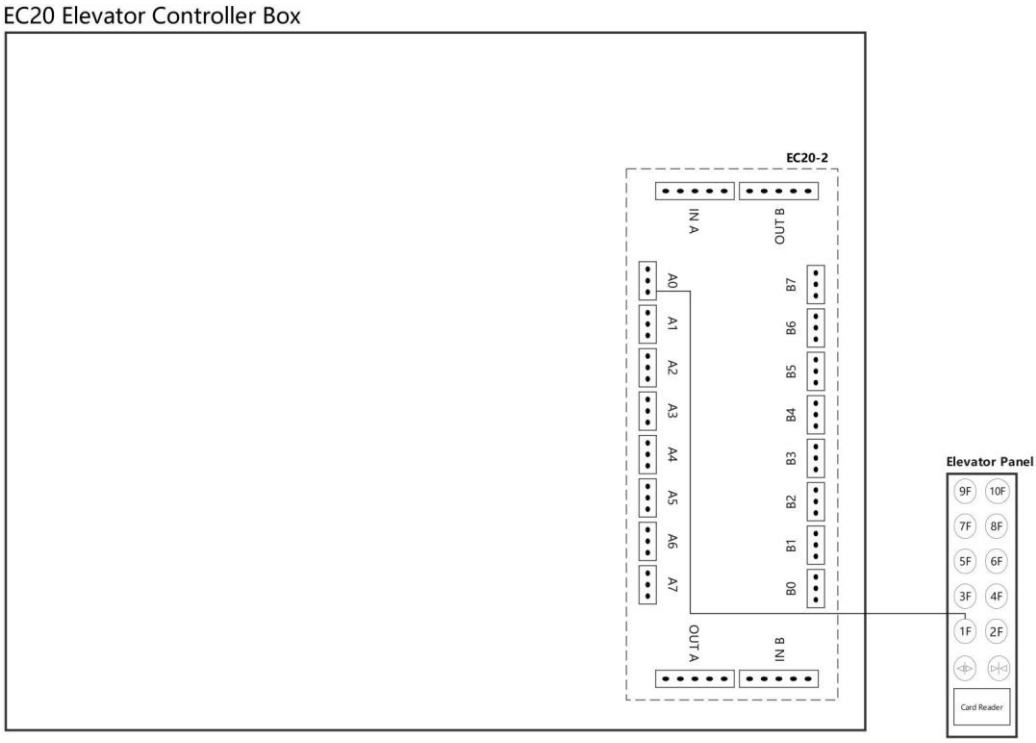


2.4 External Wiring of the Device

Includes the wiring for the elevator panel, sub-controllers, floor buttons, card reader, and fire alarm.

2.4.1 Wiring for the Elevator Panel

Figure 2-3 Wiring for the elevator panel



2.4.2 Wiring for Multiple Sub-Controllers

The EC20-2 sub-controller adopts a serial daisy-chain topology.

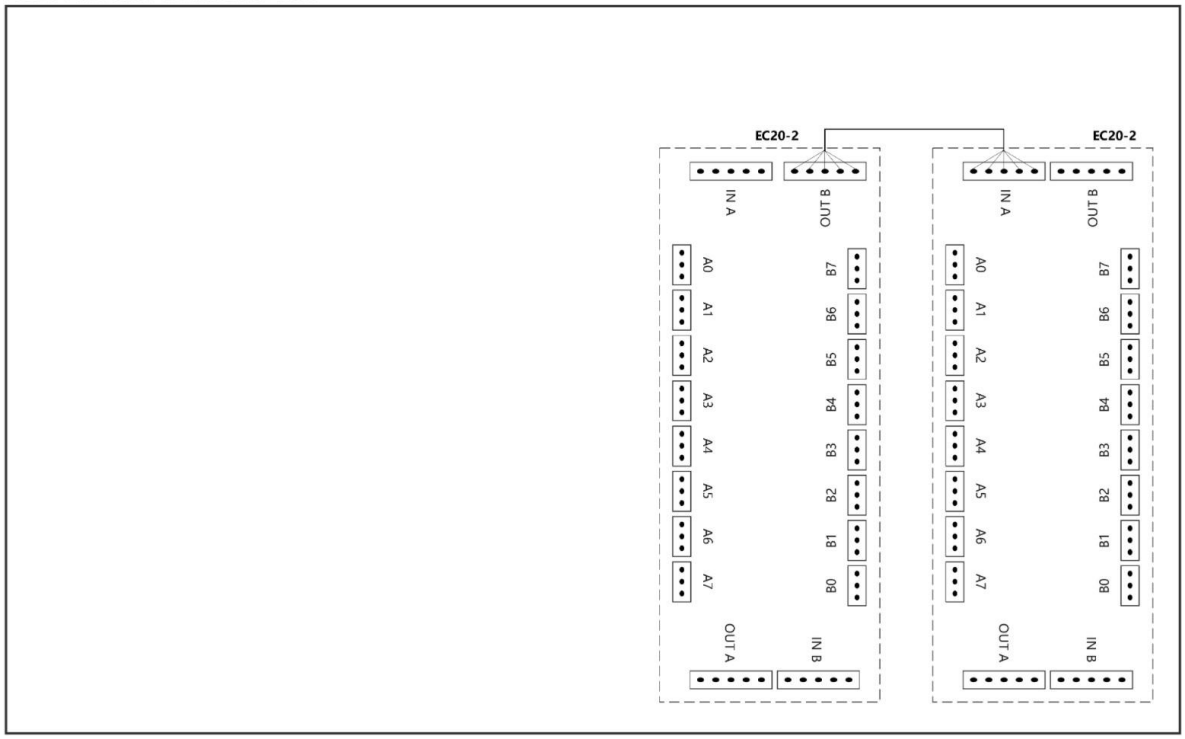
- Each sub-controller supports control of 16 floors.
- The device supports up to eight sub-controllers for control of up to 128 floors.
- Each sub-controller is equipped with a 5-pin ribbon cable.

Procedure

1. Connect the **IN A** port of the first sub-controller to the **Sub-Controller Interface** of the master controller.
2. Connect the **IN A** port of the second sub-controller to the **OUT B** port of the first sub-controller, and so on.

Figure 2-4 Wiring for multiple sub-controllers

EC20 Elevator Controller Box



2.4.3 Wiring for Floor Buttons

The elevator buttons are connected to the sub-controllers. Each port on a sub-controller uses two relays to control one floor.

- The lowest floor (Floor 1 by default) connects to the port **A0** on the first sub-controller.
- Floor 9 connects to the port **B0** on the first sub-controller.
- Floor 17 connects to the port **A0** on the second sub-controller (if required).

Figure 2-5 Relay wiring diagram

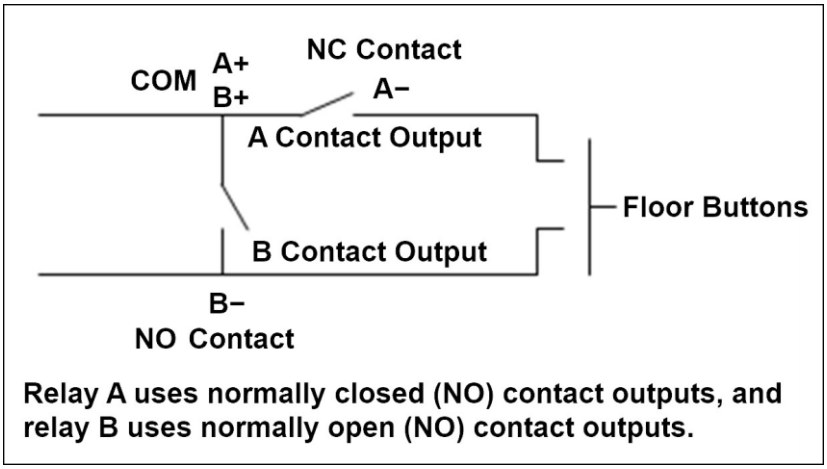
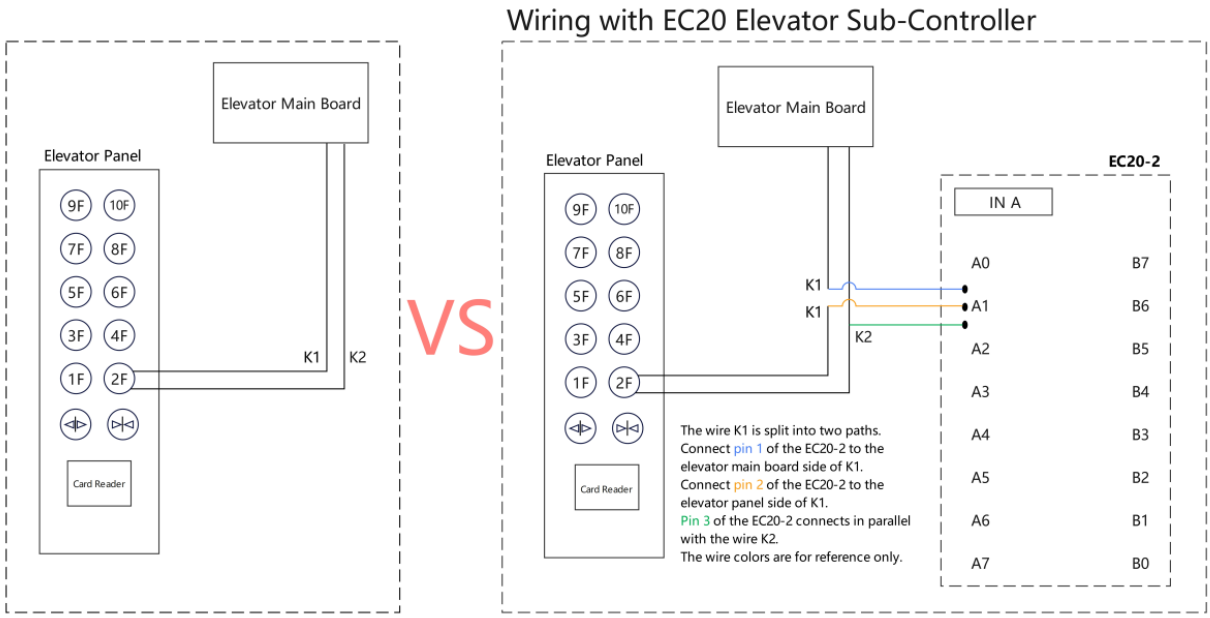


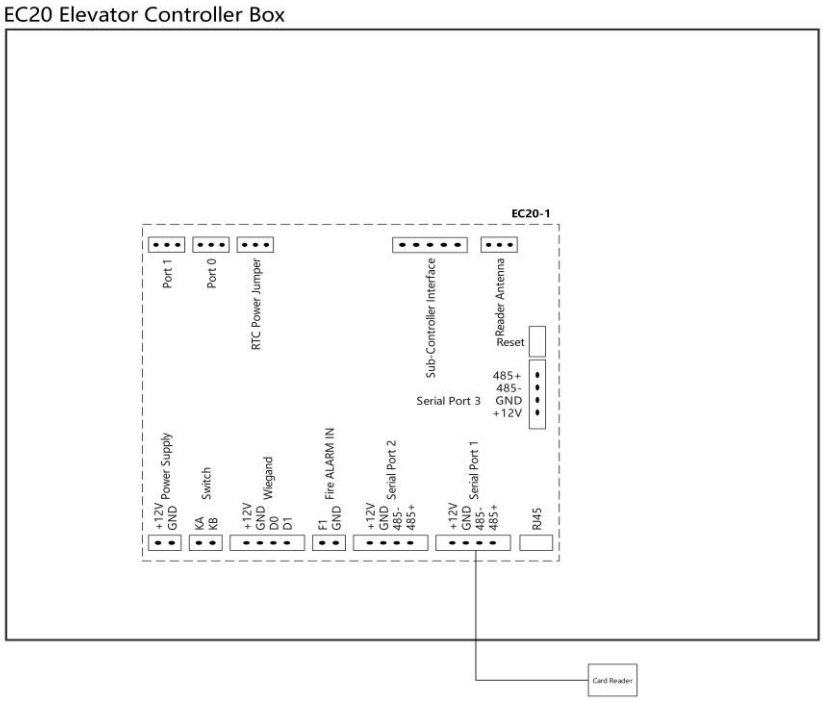
Figure 2-6 Wiring comparison diagram



2.4.4 Wiring for Card Reader

The WR01 card reader is an RS-485 type reader. By default, it can be connected to serial port 3. The required cable is supplied with the card reader. If a Wiegand reader is required, it can be connected to the Wiegand interface on the EC20- 1.

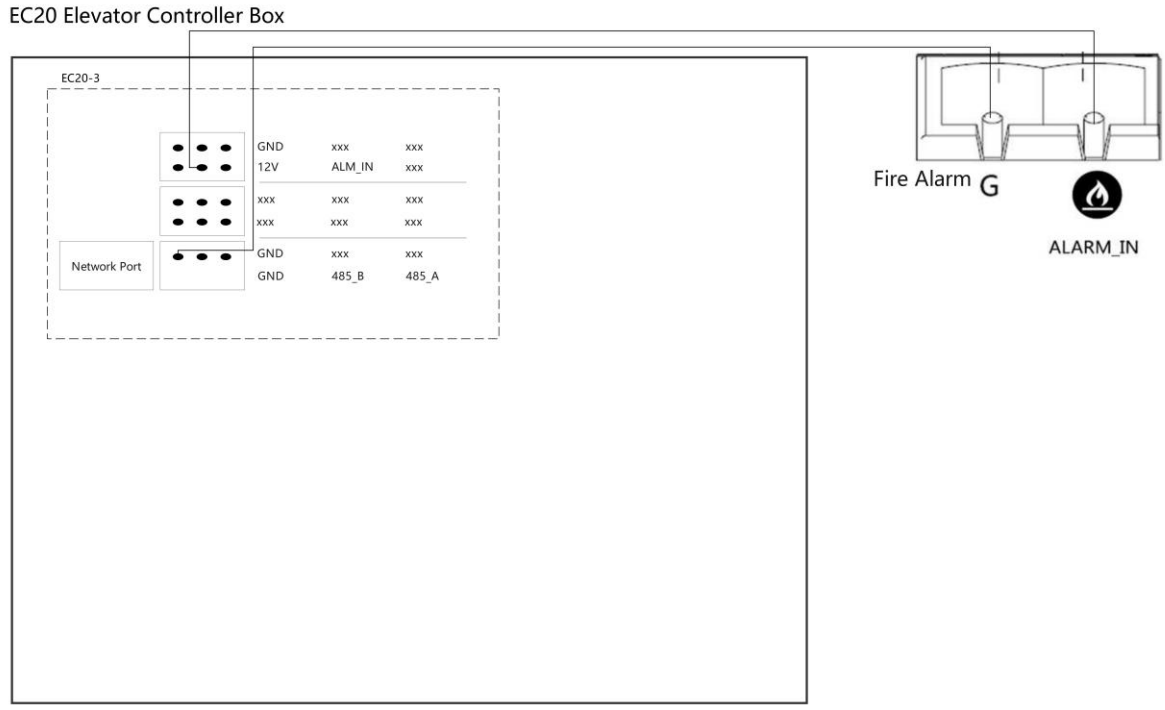
Figure 2-7 Wiring for card reader



2.4.5 Wiring for Fire Alarm

For fire alarm connection, wire to the **Fire ALARM IN** and **GND** ports on the **EC20-3 protocol conversion board**.

Figure 2-8 Wiring for fire alarm



Chapter 3 Getting Started

3.1 Web Login

3.1.1 Obtaining IP Address

You can find the Controller's IP address by using an IP scanner tool **(Device Manager**) on the computer.

Procedure

1. Go to our official website *https://fanvil.com*, and then select **Support** > **Download Center** > **Tools** > **IP Scanner**.
2. Click to download the latest version of the tool.
3. Open the tool, and then click **Rescan** to view the Controller's IP address.

3.1.2 Logging in to the Webpage

Prerequisites

You have obtained the IP address of the Controller. We recommend setting a static IP address for the Controller.

Procedure

1. Open a web browser on your computer (such as Chrome, Edge, Safari).
2. Enter the device's IP address in the browser's address bar, and then press the Enter key.

NOTE

- Ensure that the computer and the Controller are on the same network segment.
- The default username and password are both **admin**.

3. Enter the username and password, and then click **Login**.
4. On the home page of web interface, select the language from the drop-down list in the upper-right corner.

   After a factory reset, the language will be reset to English.

NOTE

A valid username and password are required to log in to the device's webpage. After three consecutive failed attempts, the login will be locked for 5 minutes. The lockout rules are as follows:

- If the same IP address attempts to log in with different usernames more than the specified number of times, the login will be locked.
- If the same username attempts to log in from different IP addresses more than the specified number of times, the login will be locked.

3.2 Elevator Control Settings

3.2.1 Configuring Elevator Control Parameters

You can set the number of floors, manage public floors, and configure other elevator parameters on the webpage of the Controller.

Procedure

1. On the Controller's home page, select **Elevator control** > **Elevator Control Settings**.
2. Configure the parameters.
3. Click **Apply**.

Table 3-1 Parameter description of elevator control

Parameter	Description
Number of Floors	Enter the actual number of floors. The Controller supports up to 128 floors.
Floor Management	Map floors to the ports of the elevator sub-controller. Floors set as public are accessible to all users.
Elevator Control Operation Mode	The Controller offers three operating modes. • **Controlled Mode**: The elevator is controlled according to the configured rules. • **Forced Freedom Mode**: The elevator can be used at any time. • **Mandatory Prohibition Mode**: The elevator cannot be used at any time. **NOTE** The operating modes do not affect the public floors.

Enable the Time Period inside the Elevator Box	Set the effective time periods when card authentication is required for the card reader inside the elevator car.
Enable the Time Period outside the Elevator Box	Set the effective time periods applicable to devices outside the elevator car and the remote devices that call the elevator.
Effective Duration of Remote Floor Opening	Sets the effective duration of floor access when the door is unlocked or when the indoor station calls the elevator. This duration can be adjusted based on the estimated time for the elevator to arrive at the user's floor and for the user to reach the elevator lobby.
Swipe Card to Automatically Select Layers	Applicable to card reader inside the elevator car. • For users with access to only one floor, the corresponding floor button lights automatically. • For users with multiple floor permissions, no button lights, but all authorized floors are unlocked for manual selection.

3.2.2 Personnel Management

On the Controller's webpage, you can add users to the system and authorize them by assigning an access card and setting a valid time schedule. Once authorized, users can call the elevator by swiping their cards at the reader.

Table 3-2 Parameter description of personnel management

Parameter	Description
Name	Enter the user name.
Card Number Type	• **User Card**: Used by ordinary users to call the elevator. • **Administrator Card**: Typically assigned to property managers and elevator maintenance personnel for system management purposes.
Card Number	The first 10 digits of the card (e.g., 0004111806).
Password	Call the elevator by entering a PIN on the card reader. PIN-enabled readers are currently unavailable.

Floor	Select the floor permission. Multiple selections are allowed.
Mode	• **Enabled**: Once enabled, this mode is effective for the next 24 hours. • **Disabled**: Cards, passwords, or facial recognition cannot unlock the door. • **Period**: Effective only within the set time period.
Times	Number of times the user can unlock the door. When this value reaches the limit, the mode will switch to **Disabled**. If left blank, there is no limit.
Sources	Indicates the sources of the user data. • **Local**: manually added • **Server**: provisioned by the server

3.2.2.1 Adding Users

Procedure

1. On the Controller's home page, select **Elevator control** > **Personnel Management**.
2. Click **Add**, and then configure the name, card type, card number, password, and other parameters.
3. Select floor permission, mode, and times.
4. Click **Apply**.

3.2.2.2 Editing Users

Procedure

1. On the Controller's home page, select **Elevator control** > **Personnel Management**.
2. Select a user, click **Edit**, and then edit the information.
3. Click **Apply**.

3.2.2.3 Deleting Users

Procedure

1. On the Controller's home page, select **Elevator control** > **Personnel Management**.
2. Select one or more users, and then click **Delete**.

   Click **Delete All** to delete all users.

3.2.2.4 Importing and Exporting Users

You can import or export users in batches via the web interface.

Procedure

1. On the Controller's home page, select **Elevator control** > **Personnel Management**.
2. Click **Import** or **Export** to import or export users in batches.

3.2.3 Time Schedule

Time schedule allows you to create and manage schedules, which can be set to repeat **daily, weekly, or monthly**. They are applied to restrict user access, allowing the designated authentication mode to operate only within the specified time periods.

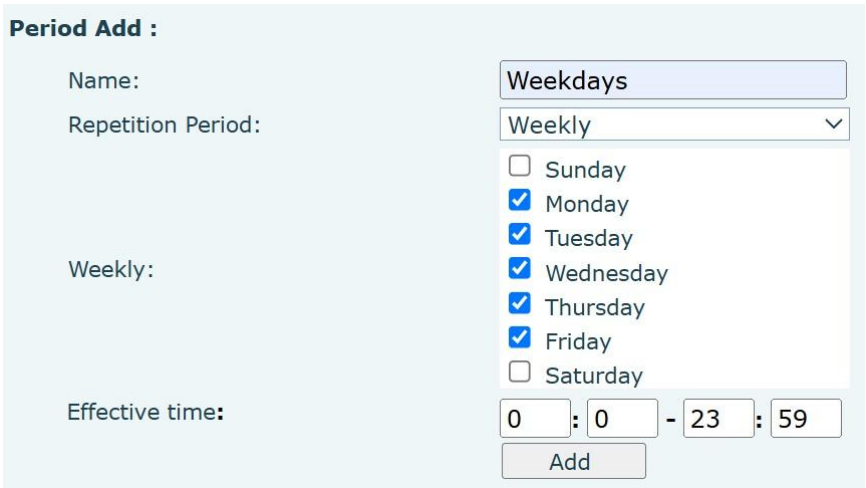
Procedure

1. On the Controller's home page, select **Elevator control** > **Time Profile**.
2. Set the name for the schedule, such as "Weekdays" and "Weekends".
3. Select **Repetition Period**.
   - **Daily:** Repeats every day.
   - **No Repeat:** The schedule is valid only on the selected single date.
   - **Weekly:** Repeats weekly on selected days (Monday through Sunday).
   - **Monthly:** Repeats monthly on selected dates (e.g., 1st, 15th, 30th of each month).
4. Set the effective time, which ranges from 00:00 to 23:59.
5. Click **Add**.

Example

1. Create a time schedule named "Weekdays".
2. Configure the parameters as follows:
   - **Repetition Period:** Weekly
   - **Selected Days:** Monday through Friday
   - **Active Time:** 00:00 to 23:59

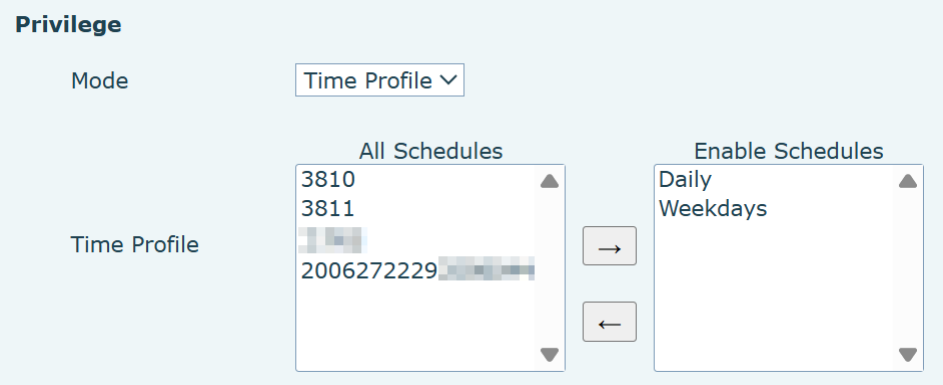
Figure 3-1 Time schedule



3. Click **Add**.

   You can select this schedule when you add or edit users in **Personnel Management**.

Figure 3-2 Time schedule selection



3.2.4 Test Instructions

You can perform testing for the sub-controllers and specified ports via the web interface.

Procedure

1. On the Controller's home page, select **System** > **Tools** > **Slave Controller Test**.
2. Click **Test Auto-Illumination** or **Test Manual Illumination**.
   - Test on the sub-controller

     The number zero is set for the first sub-controller, the number one is set for the second sub-controller, and so on.

     - Auto-illumination: The port indicators from **A0** to **B7** will light up in **green** sequentially, then return to their normal **blue** state.
     - Manual illumination: The port indicators from **A0** to **B7** will turn off sequentially, then return to their controlled **blue** state.
   - Test on the port number
     - Auto-illumination: The corresponding port indicator turns **green**.
     - Manual illumination: The corresponding port indicator turns off.

Chapter 4 Device Configuration

4.1 System Settings

You can view system information, change web login password, configure system settings, upgrade firmware, and perform other operations on the **System** page.

4.1.1 System Information

You can view system information form **System** > **Information**, such as device model, software version, hardware version, network information, and more.

4.1.2 User Configuration

You can change the web login password from **System** > **Account**. Administrators can add, edit, and delete users, and set permissions and passwords for new users.

4.1.3 System Configuration

Administrators can view, import, and export device configurations, and restore the Controller to factory settings from **System** > **Configurations**.

Table 4-1 Parameter description of system configuration

Operation	Description
Export configuration	Click to export the configuration file in .txt format.
Import configuration	Upload a previously saved configuration file to apply its settings to the Controller.
Clear configuration	Clears all configurations and data.

4.1.4 Upgrade

4.1.4.1 Upgrading Software Version

Procedure

1. On the Controller's home page, select **System** > **Upgrade** > **Software Upgrade**.
2. Click **Select,** and then select a software version file.
3. Click **Upgrade**.

4.1.4.2 Upgrading Server

The Controller sends an HTTP request to the server. If a version description file is returned, the device parses it and prompts the user to upgrade if a new version is available; otherwise, a 404 error or timeout is reported.

Procedure

1. On the Controller's home page, select **System** > **Upgrade** > **Upgrade Server** or **Firmware Information**.
2. Configure the parameters.
3. Click **Apply**.

Table 4-2 Parameter description of server upgrade

Parameter	Description
Upgrade Server	
Upgrade Server Address1	The URL of the main HTTP upgrade server.
Upgrade Server Address2	The URL of a backup HTTP upgrade server when the main server is unavailable.
Firmware Information	
Current Software Version	Displays the currently installed software version.
Server Firmware Version	Displays the currently installed firmware version available on the server.
Upgrade	Becomes active when a newer version is detected. Click to upgrade to the new version.
New Firmware Information	Displays update information from the server's version file when available.

4. Place a corresponding version information file on your HTTP server.
    - The version file must be named in this format: vendor_model_hwv1_0.txt, where the number following **hw** indicates the hardware version. Replace any spaces in the file name with underscores.

- The device sends the request to `http://<server_address>/`. Both the new firmware and the requested file must be placed in the download directory of the HTTP server.
- The .txt file must be UTF-8 encoded and contain the following information.

```
Version=1.6.3
Firmware=xxx/xxx.z   #xxx.z or http://ip:port/directory/xxx.z
BuildTime=2024.08.11 20:00
Info=TXT|XML

Xxxxx
Xxxxx
Xxxxx
Xxxxx
```

4.1.5 Auto-Provisioning

The Controller supports four methods to obtain auto-provisioning parameters: SIP plug-and-play (PnP), DHCP, Static provisioning and TR-069.

Supported protocols: FTP, TFTP, HTTP, and HTTPS.

Procedure

1. On the Controller's home page, select **System** > **Auto Provision**.
2. Configure the Parameters.
3. Click **Apply**.

Table 4-3 Parameter description of auto-provisioning

Parameter	Description
Basic Settings	
CPE Serial Number	Displays the serial number of the Controller.
Authentication Name	The username for the FTP server. Not required for TFTP protocol. If using FTP and this field is left blank, the default is set to **anonymous**.
Authentication Password	Password for the FTP user.

Configuration File Encryption Key	If the configuration file to be upgraded is encrypted, enter its decryption key here.
General Configuration File Encryption Key	If the common configuration file to be upgraded is encrypted, enter its decryption key here.
Download Fail Check Times	The number of times the Controller retries after a failed download. Default: 1.
Save Auto Provision Information	Select ☐ to save the auto-provisioning information.
Download CommonConfig enabled	Select ☐ to download the common configuration file during automatic upgrading.
Enable Server Digest	If the Controller uses Digest authentication to match configuration content, enabling this will trigger an update download whenever the configuration on the server is modified, or if the local configuration differs from the server's.
List Update Mode	Set the update mode.
DHCP Option	
Option Value	DHCP option used to obtain auto-provisioning parameters, supporting **Custom Option**, **Option 66**, and **Option 43**. **Disabled** is set by default.
Custom Option Value	The valid range for a custom option is 128 to 254. The custom option type must match the definition on the DHCP server.
Protocol Type	FTP, TFTP, HTTP, HTTPS.
Enable DHCP Option 120	Enables setting the SIP server address via DHCP Option 120.
DHCPv6 Option	

Option Value	DHCP option used to obtain auto-provisioning parameters, supporting **Custom Option**, **Option 66**, and **Option 43**. **Option 66** is set by default.
Custom Option Value	The valid range for a custom option is 128 to 254. The custom option type must match the definition on the DHCP server.
Static Server	
Server Address	The address of the FTP/TFTP/HTTP server. It can be an IP address (e.g., 192.168.1.1) or a domain name (e.g., ftp.domain.com). The system also supports specifying a subdirectory path (e.g., 192.168.1.1/ftp/Config/ or ftp.domain.com/ftp/config), indicating that it will access the server at the given address or domain, with the file storage path under the specified subdirectory. A trailing slash is optional.
Configuration File Name	The name of the configuration file to download. For typical auto-provisioning, leave this field empty. The Controller will then use its own MAC address as the filename to retrieve the file from the server.
Protocol Type	The server type: **FTP**, **TFTP**, or **HTTP**.
Update Interval	The interval (in hours) for checking updates.
Update Mode	The auto-update type. • **Disabled**: No update. • **Update After Reboot**: Update after the device reboots. • **Update at Time Interval**: Updates at the specified interval.
Autoprovisioning Now	Click to start auto-provisioning.
TR069	
Enable TR069	Select ☐ to enable TR069.
ACS Server Type	Select the ACS server type. Supports **China Telecom**, **Common**, **China Unicom**, and **eSight**.
ACS Server URL	The URL of the ACS server.

ACS User	The username for ACS server authentication.
ACS Password	The password for ACS server authentication.
Enable TR069 Warning Tone	Select ☐ to enable TR069 prompt tone.
TLS Version	If "Auto Login" is selected, the Controller will use the previously entered credentials to connect to the ACS server upon reboot without prompting for username and password.
INFORM Sending Period	The interval at which the Controller periodically sends an INFORM message to the ACS server.
STUN Server Address	The address of the STUN server.
STUN Enable	Select ☐ to enable STUN.

4.1.6 FCMS

You can check the connection status of the Fanvil Cloud Management System (FCMS) platform from **System** > **FCMS**. If the Controller is being bound to FCMS for the first time, or is offline on the platform, click **Connect** on this page to connect the device to FCMS.

4.1.7 Tools

If the Controller is not functioning properly, you can try the following methods from **System** > **Tools** to restore normal operation or collect log information for technical support.

- Syslog: If a system log server address is configured, the device will record log information to the server. In case of issues, the logs can be provided to the device manufacturer's technical support for analysis.
- Sub-controller test: Perform tests on the elevator sub-controller to verify whether it is operating normally. For details, see *3.2.4 Test Instructions*.

4.1.8 Restarting the Device

Click **Reboot** from **System** > **Reboot Device** to restart the Controller.

4.2 Network Settings

4.2.1 Basic Network Settings

Set the network type and network mode.

Procedure

1. On the Controller's home page, select **Network** > **Basic**.
2. Configure the parameters.
3. Click **Apply**.

Table 4-4 Parameter description of basic network settings

Parameters	Description
Network Mode	Supports **IPv4 Only**, **IPv6 Only**, and **IPv4 & IPv6**.
IPv4 Network Status	
IP	Displays the IP address of the Controller.
Subnet Mask	Displays the subnet mask of the Controller.
Default Gateway	Displays the IP address of the gateway.
MAC	Displays the MAC address of the Controller.
IPv4 Settings	
Static IP	• You can select this mode if your internet service provider (ISP) provides a fixed IP address. • If this mode is selected, you must configure the static information: IP address, subnet mask, gateway, DNS, etc. • If you do not know these values, contact your ISP or network administrator.
Primary DNS Server	Enter the IP address of the primary DNS server.
Secondary DNS Server	Enter the IP address of the secondary DNS server.
DNS Domain	Enter the DNS domain name.

DHCP	In this mode, the network information will be automatically obtained from the DHCP server. Manual entry is not required.
Enable Vendor Identifier	When enabled, the configured vendor identifier will display in DHCP Option 60.
Vendor Identifier	Customizable. When enabled, it will be included in DHCP Option 60.
DNS Server Configured By	Select a configuration method for the DNS server.
PPPoE	In this mode, you must enter your asymmetric digital subscriber line (ADSL) account and password for connection.

NOTE

- If the IP address is changed, the web interface will no longer respond. You must enter the new IP address in the browser's address bar to reconnect to the Controller.
- We recommend configuring a static IP address after the Controller has been deployed.
- The Controller supports three network modes: Static IP, DHCP, and PPPoE. Refer to your actual network environment to select the appropriate mode for device connectivity.

4.2.2 Web Server

Configure the web login protocol, protocol port, and RTP port settings.

Procedure

1. On the Controller's home page, select **Network** > **Service Port**.
2. Configure the parameters.
3. Click **Apply**.

Table 4-5 Parameter description of service port

Parameter	Description
Web Server Type	Select **HTTP** or **HTTPS**. A restart is required for changes to take effect.
Web Login Timeout	The period of inactivity before the web interface is logged out. The default value is 15 minutes.
Web auto login	If enabled, the browser automatically logs in to the web interface after a timeout. You do not need to enter the username and password again.
HTTP Port	The TCP port for HTTP access. The default value is 80. Format: `http://device-ip:port`. For security, the port value can be customizable.
HTTPS Port	The TCP port for HTTPS access. The default value is 443. Format: `http://device-ip:port`. For security, the port value can be customizable.

4.2.3 VPN

- Virtual private network (VPN) creates a secure tunnel to a private network over the public Internet.
- The Controller supports connecting to a VPN via L2TP and OpenVPN, and you can configure them via the web interface.

NOTE

Both L2TP and OpenVPN connections automatically reconnect after the device restarts, unless manually disabled.

Procedure

- Configuring L2TP
  1. On the Controller's home page, select **Network** > **VPN**.
  2. Select ☐ to enable VPN function, and then select to enable **L2TP**.
  3. Configure **L2TP Server Address**, **Authentication Name**, and **Authentication Password**.
  4. Click **Apply**.

     The device attempts to connect. Once connected, the assigned VPN IP address will display in **Virtual Private Network (VPN) Status**.

NOTE

L2TP on the device only supports basic unencrypted authentication and data transmission. If data encryption is required, use the OpenVPN.

- Configuring OpenVPN

  1. Obtain the following files from your OpenVPN service provider:
     - OpenVPN configuration File: client.ovpn
     - CA Root Certification: ca.crt
     - Client Certification: client.crt
     - Client Key: client.key
  2. On the Controller's home page, select **Network** > **VPN**.
  3. Select ☐ to enable VPN function, and then select ◯ to enable **OpenVPN**.
  4. Click **Select** to select a VPN file, and then click **Upload**.

4.3 Advanced Network Settings

Advanced network settings are typically configured by IT administrators to optimize the device's service quality.

Procedure

1. On the Controller's home page, select **Network** > **Advanced**.
2. Configure the parameters.
3. Click **Apply**.

Table 4-6 Parameter description of service port

Parameter	Description
Link Layer Discovery Protocol (LLDP) Settings	
Enable LLDP	Select ☐ to enable LLDP.
Packet Interval (1–3600 seconds)	LLDP sending or monitoring interval. Valid value: 1–3600 seconds.
Enable Learning Function	Select ☐ to enable LLDP automatic VLAN learning.

Cisco Discovery Protocol (CDP) Settings	
Enable CDP	Select ☐ to enable CDP.
Packet Interval:(1~3600)	CDP sending or monitoring interval. Valid value: 1–3600 seconds.
DHCP VLAN Settings	
Option Value	1. **Custom** 2. **Disabled**
Option Value Data Type	1. **Auto** 2. **Decimal** 3. **Octal** 4. **Hexadecimal** 5. **ASCII Code**
DHCP Option Vlan (128-254)	Set a value (128–254) to obtain VLAN via DHCP.
ARP Cache Life	Set the ARP aging time. Do not change this value if the system is functioning normally. Valid value: 0–99.
WAN VLAN Settings	
Enable VLAN	Select ☐ to enable VLAN. The system will handle VLAN tagging automatically for direct VLAN network access.
WAN VLAN ID	The VLAN ID configured on the WAN port. Valid value: 0–4095.
802.1p Signal Priority	Priority for SIP messages. Valid value: 0 (lowest) to 7 (highest)
802.1p Media Priority	Priority for media traffic. Valid value: 0–7.
802.1X Settings	
802.1x Mode	The mode of 802.1X authentication, including **Off EAP-MD5**, **EAP-TLS**, and **PEAP-MSCHAPV2**.

Identity	The username, supporting alphanumeric and symbol characters, up to 50 characters.
Password	The password, supporting alphanumeric and symbol characters, up to 50 characters.
CA Certificate	Certificate file. Supports browsing, uploading, and deleting.
Device Certificate	Device certificate. Supports browsing, uploading, and deleting.
Certification File	
HTTPS Certification File	Custom uploaded HTTPS certificate.

4.4 Device Settings

4.4.1 Configuring Date and Time

Procedure

1. On the Controller's home page, select **Device Settings** > **Time/Date**.
2. Configure the parameters.
3. Click **Apply**.

Table 4-7 Parameter description of date and time

Parameter	Description
Network Time Server Settings	
Time Synchronized via SNTP	Enable time synchronization using the SNTP protocol.
Time Synchronized via DHCP	Enable time synchronization using the DHCP protocol.
Time Synchronized via DHCPv6	Enable time synchronization using the DHCPv6 protocol.

Primary Time Server	The address of the primary network time protocol (NTP) server.
Secondary Time Server	The address of the backup NTP server. The device will attempt to synchronize with this server if the primary is unavailable.
Time zone	Select your local time zone.
Resync Period	The interval at which the device re-synchronizes with the time server.
Time/Date Format	
12-hour clock	When enabled, displays time in a 12-hour format (AM/PM).
Time/Date Format	Set the display format for the date.
Daylight Saving Time Settings	
Location	Select your geographic location for automatic daylight saving time (DST) rules.
DST Set Type	• **Disabled**: DST adjustments are not applied. • **Manual**: Configure DST start and end times manually. • **Automatical**: DST rules are automatically applied based on the selected Location. When set to **Automatical**, the start and end parameters become read-only.
Fixed Type	Defines how the DST start/end dates are specified. • **By Date**: Set an exact calendar date (e.g., March 31). • **By Week**: Set a relative day (e.g., Second Sunday of March).
Offset	The amount of time to adjust the clock at the start and end of DST (e.g., +1 hour at the start, −1 hour at the end).
Start and End	• **By Date**: Configure **Month**, **Day**, and **Hour**. • **By Week**: Configure **Month**, **Week**, **Weekday**, and **Hour**.
Manual Time Settings	Manually set the current date and time.

4.4.2 Time Plan

Time plan enables scheduling of automated actions at a precise time or across a defined time range, allowing tasks like reboots or upgrades to be performed automatically.

> **NOTE**
>
> If the device is on a call within the scheduled time period, restarting and upgrading will be skipped.

Procedure

1. On the Controller's home page, select **Device Settings** > **Time Plan**.
2. Configure the parameters.
3. Click **Apply**.

Table 4-8 Parameter description of time plan

Parameter	Description
Name	Set a custom name for the action rule.
Type	The action to perform. • Upgrade • Reboot • Call forwarding
Repetition Period	Sets the recurrence pattern. • **No Repetition**: Executes once within the set time range. • **Daily**: Executes at the same time every day. • **Weekly**: Executes on the same weekday(s) every week. • **Monthly**: Executes on the same date every month.
Start Date	The date when the rule becomes active.
End Date	The date when the rule expires.
Effective Time	The effective time period for action execution.

4.5 Security

4.5.1 Filtering Web Access

You can create an allowlist of IP address ranges permitted to access the web interface.

Procedure

1. On the Controller's home page, select **Security** > **Web Filter**.
2. Enter the starting IP address and the ending IP address in **Start IP Address** and **End IP Address** fields.
3. Select ☐ to enable the function.
4. Click **Apply**.

Related Operations

Click **Delete** to delete the current IP address range.

> **NOTE**
>
> If your computer is on the same network as the Controller, ensure its IP address falls within an allowed range. Otherwise, you cannot log in to the web interface after saving the configuration.

4.5.2 Network Firewall

Configure inbound and outbound firewall rules to control network access, prevent malicious traffic, and enhance system security. Each rule is assigned a unique sequence number, with up to 10 rules allowed for each rule type.

Procedure

1. On the Controller's home page, select **Security** > **Firewall**.
2. Configure the parameters.
3. Click **Add**.

Table 4-9 Parameter description of network firewall

Parameter	Description
Enable Input Rules	Select ☐ to enable **Input Rules**.
Enable Output Rules	Select ☐ to enable **Output Rules**.
Input/Output	• **Input**: The traffic to the device. • **Output**: The traffic from the device.
Deny/Permit	Select **Permit** to enable the rule.
Src Port Range	The source port range.
Dst Port Range	The destination port range.
Src Address	The source IP address. It can be a host address, network address, or **0.0.0.0** (all addresses).
Dst Address	The destination IP address. It can be a host address, network address, or **0.0.0.0** (all addresses).
Src Mask	The source subnet mask. When it is set to **255.255.255.255**, it indicates a specific host. When it is set to a subnet mask such as **255.255.255.0**, it indicates that a network segment is being filtered.
Dst Mask	The destination subnet mask. When it is set to **255.255.255.255**, it indicates a specific host. When it is set to a subnet mask such as **255.255.255.0**, it indicates that a network segment is being filtered.

4.6 Device Logs

When an exception occurs, you can capture device logs from the **Device Log** page and send them to technical support email for troubleshooting.

4.7 Arming Settings

The Controller provides dry contact input ports for connecting external security sensors such as door magnetic contacts, infrared detectors, or vibration sensors. When a sensor is triggered, the device can send an alert message to a remote server, call a configured number, and play a local alarm tone to help administrators respond promptly.

You can configure alarm input parameters via the web interface.

Procedure

1. On the Controller's home page, select **Security Settings** > **Alert**.
2. Configure the parameters.
3. Click **Apply**.

Table 4-10 Parameter description of arming settings

Parameter	Description
Status	Indicates whether the device is currently in an alarm state.
Information	The content of the alert message sent to the server. `$` can be replaced with real-time values. The supported parameters are as follows: • `$model`: The device's model. • `$mac`: The device's MAC address. • `$ip`: The device's IP address. • `$triggerName`: Name of the triggering port.
Alarm Name	The alarm name reported to the server.
Triggered By	Defines the electrical state that represents an alarm: • **Low Level Trigger (Close Trigger)**: Alarm triggers when the input circuit is closed. • **High Level Trigger (Disconnect Trigger)**: Alarm triggers when the input circuit is opened.
Name	Name of the connected alarm device.
Input Duration	The minimum time the trigger state must be held before an alarm is registered. The default value is **0** seconds.

Cancel Alarm Mode	Includes **Manually Cancel Alarm** and **Automatically Cancel Alarm**. • **Manually Cancel Alarm**: The alarm must be cleared manually on the web interface, or it will be automatically cleared when the alarm input stops. • **Automatically Cancel Alarm**: Set a duration for the alarm. The alarm will be cleared automatically after the set duration.
Alarm Message Push	Enable or disable sending alarm messages from the input port to the server.
Alarm Server Location	Enter the alarm server address.

4.8 Action URL

Action URL allows you to configure HTTP URLs for valid and invalid card events. The card number is sent to the specified HTTP server in the format `$card_sn`.

Example

```
http://192.168.1.200/validcard=$card_sn
http://192.168.1.200/invalidcard=$card_sn
```

Chapter 5 Troubleshooting

When the Controller malfunctions or operates abnormally, you can try the following methods to restore normal operation, or collect relevant information and send a problem report directly to the technical support email.

5.1 Viewing System Status

You can view the Controller's current status, network, and account information from **System** > **Information**.

5.2 Restarting the Device

You can restart the Controller via the web interface or a power cycle.

Procedure

- Via the web interface
  1. On the Controller's home page, select **System** > **Reboot Device**.
  2. Click **Reboot**.
  3. Click **OK**.
- Power cycle

  Physically disconnect and then reconnect the device's power source.

5.3 Restoring Factory Settings

Procedure

1. On the Controller's home page, select **System** > **Configurations** > **Reset Device**.
2. Click **Reset**.
3. Click **OK**.

5.4 Capturing Network Packets

Packet capture allows you to record network traffic to analyze call setup, registration failures, or other network-related issues.

Procedure

1. On the Controller's home page, select **System** > **Tools** > **LAN Packet Capture**.
2. Click **Start**.

The web browser will open a download dialog, prompting you to save the packet capture file locally.

3. Click **Save** to save the offered capture file.
4. Reproduce the issue.

   For example: Make a call or register SIP account.

5. Return to the webpage and click **Stop**.

   The saved file contains all network packets during that period.

5.5 Exporting Logs

The Controller supports exporting system logs for exception analysis.

Procedure

1. On the Controller's home page, select **System** > **Tools** > **Syslog**.
2. Select ☐ to enable **Syslog**, and then select **Debug** from the **App Log Level** drop-down list.
3. Select ☐ to enable **Export Log**, and then click **Apply**.
4. Reproduce the issue, and then click **Export Log**.

5.6 Common Issues

Table 5-1 Parameter description of common issues

No.	Symptom	Possible Cause	Solution
1	The device fails to power on and the indicator is off.	Power not connected or abnormal voltage; power polarity reversed.	Check the power wiring and voltage specifications, and ensure correct polarity.
2	The device does not respond after power-on.	Insufficient power supply; loose internal wiring.	Replace with a compliant power supply, and check if internal wiring is secure.
3	Communication failure between master controller and sub-controller.	A/B communication lines reversed; address conflict; communication interference.	Verify A/B polarity and address settings, and check wiring and shielding.

4	Sub-controller malfunction.	Sub-controller not powered; communication interrupted.	Check sub-controller power and communication cable connections.
5	The elevator cannot reach authorized floor after access permission is granted.	Incorrect floor wiring; incorrect permission configuration.	Verify floor output wiring and parameter configuration.
6	Some floors cannot be controlled.	Incorrect number of floors configured; sub-controller exceeds supported floor count.	Check floor parameter settings and ensure no more than 16 floors per sub-controller.
7	The card reader shows no response when card is swiped.	Wiring issue.	Check the reader output type and system parameter configuration.
8	The elevator is not restricted by the access control system.	Elevator control circuit not connected; linkage point not enabled.	Check elevator interface wiring and linkage parameters.
9	The device restarts frequently.	Unstable power supply; wiring short circuit.	Replace with a regulated power supply and check external wiring.
10	Intermittent communication.	Excessive cable length or severe interference.	Use shielded cables and add terminal resistors.