DS-K2220 Series Elevator Controller

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

- To protect data, the development of Hikvision Products incorporates privacy by design principles. For example, for Products with facial recognition features, biometrics data is stored in your Products with encryption method; for fingerprint Products, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
- As a data controller/processor, you may process personal data, including collection, storage, use, processing, disclosure, deletion, etc. You are advised to pay attention to and comply with applicable laws and regulations related to the protection of personal data, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and the assessments of the effectiveness of your security controls.

Available Model

Product Name	Model
Elevator Controller	DS-K2220LX(P) Series Elevator Controller
	DS-K2220X(P) Series Elevator Controller
	DS-K2220X Series Elevator Controller

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.
FCC Conditions
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

CE

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed

under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU,the RoHS Directive 2011/65/EU

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. this device may not cause interference, and
2. this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.
Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into Dangers and Cautions:

Dangers: Neglecting any of the warnings may cause serious injury or death.

Cautions: Neglecting any of the cautions may cause injury or equipment damage.

⚠	⚠
Dangers: Follow these safeguards to prevent serious injury or death.	**Cautions:** Follow these precautions to prevent potential injury or material damage.

⚠ Danger:

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Do not ingest battery, Chemical Burn Hazard.
  This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
  Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ Cautions:

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

Contents

Chapter 1 Appearance

1.1 Appearance and Interfaces

The appearance and interfaces are as follows.

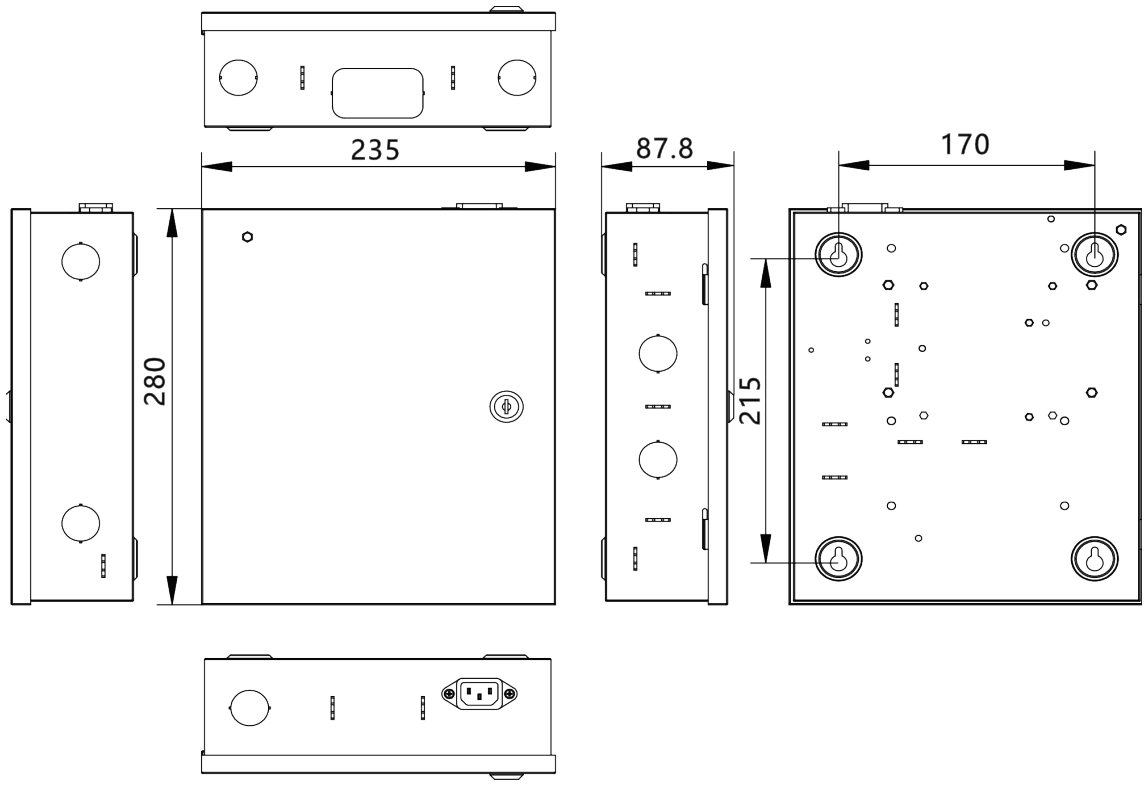


Figure 1-1 Appearance(With Chassis)

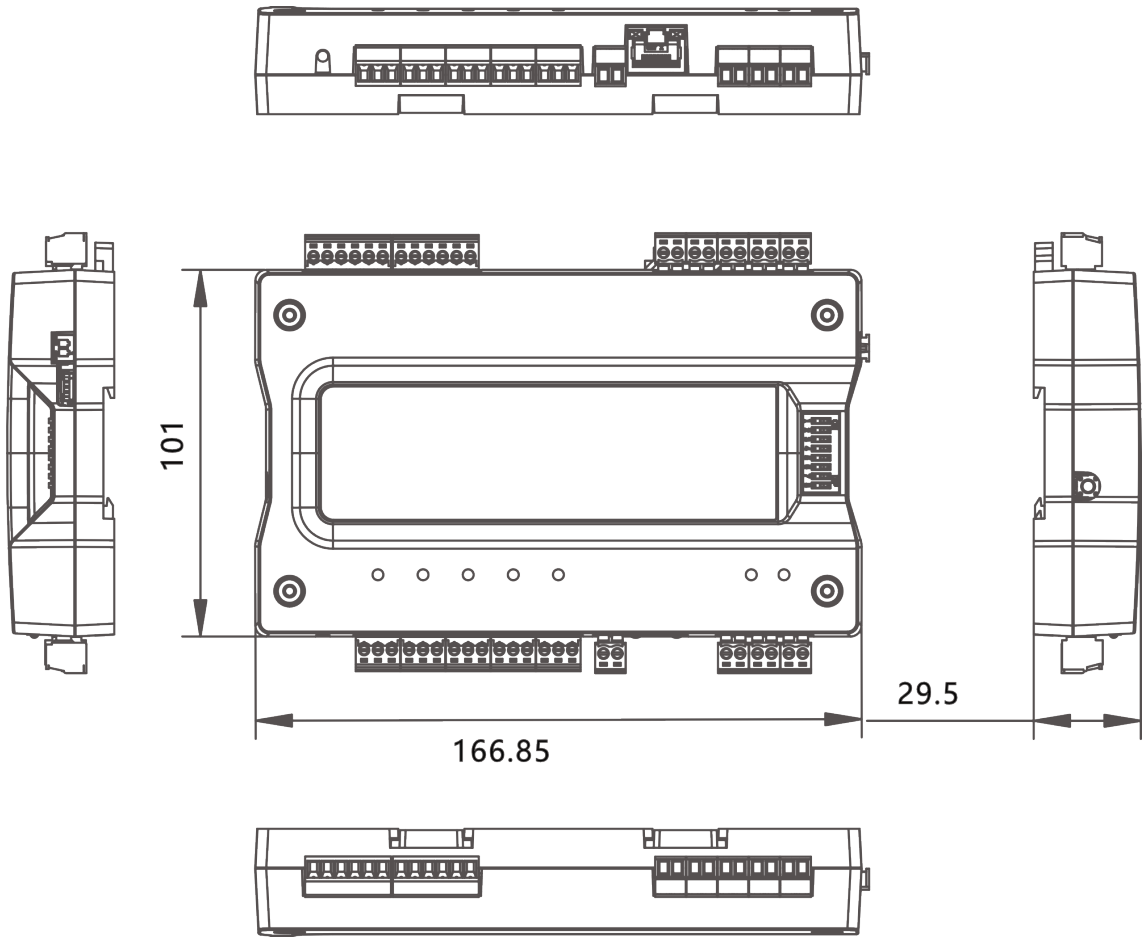


Figure 1-2 Appearance(Without Chassis)

Unit: mm.

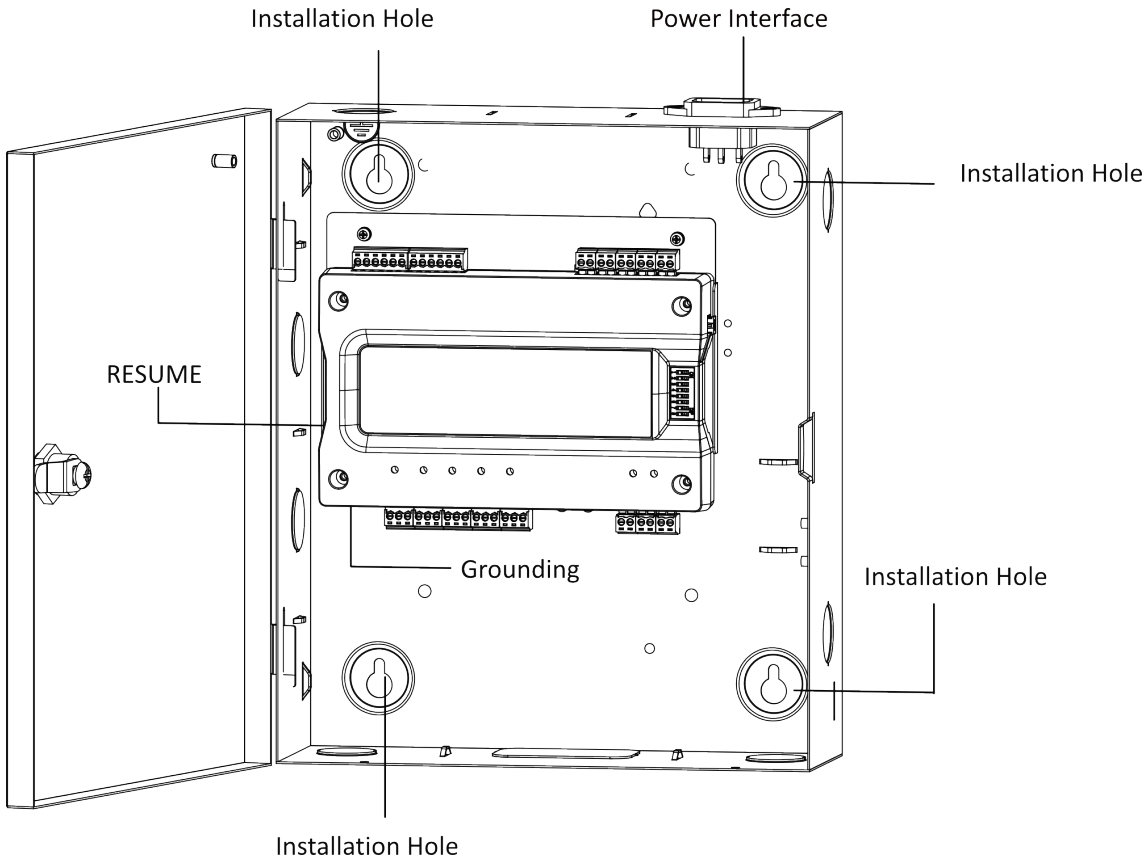


Figure 1-3 Interface (Without Chassis)

Chapter 2 Terminal Wiring

Terminal Wiring Description of the Elevator Controller.

2.1 Wiring Description

The wiring are as follows.

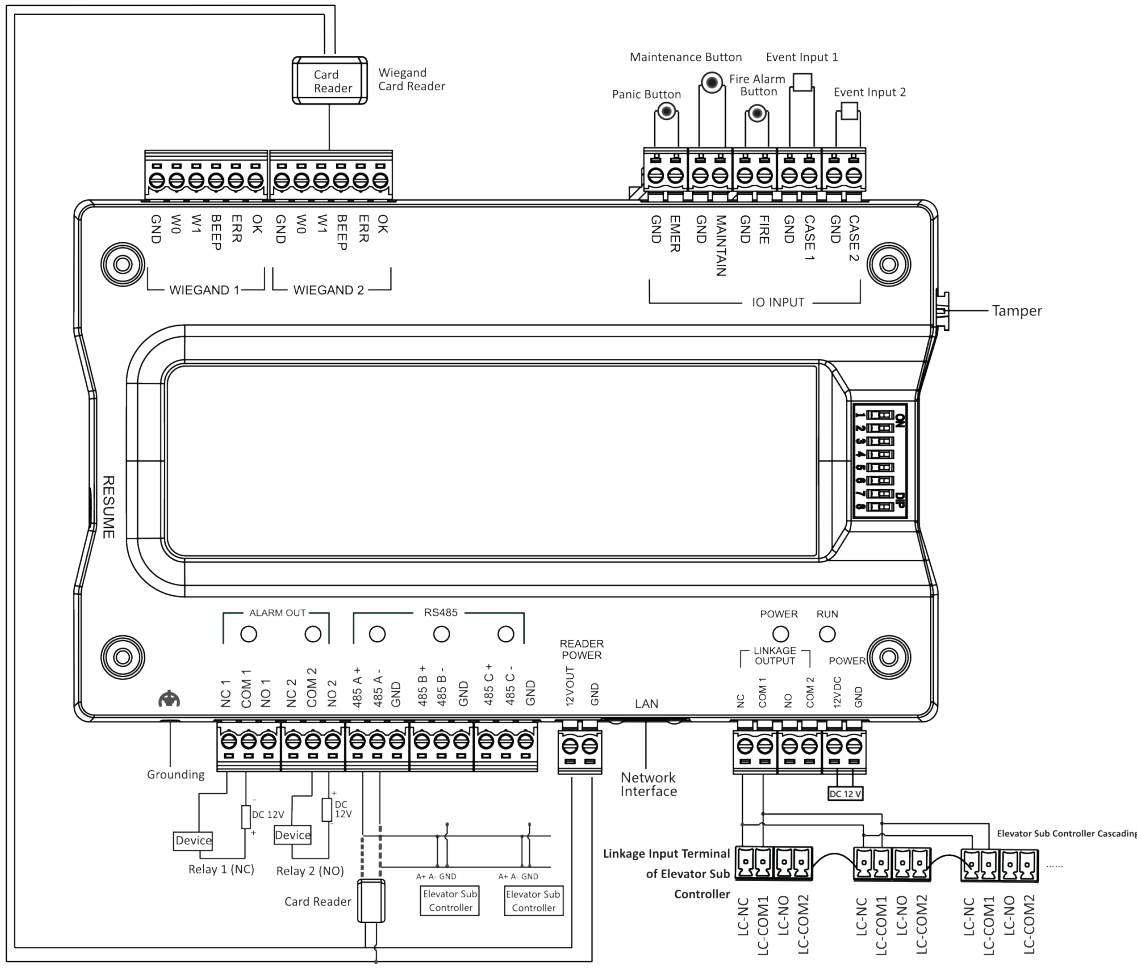


Figure 2-1 The Wiring of Elevator Controller

Note

- Disconnect any AC power before reconditioning.
- Make sure the GND end is reliably grounded. Although the control panel is designed with multiple lightning protection function, it relies on the prerequisite of reliable grounding.

Otherwise, these measures will not play a protective role. The GND resistance cannot be more than 8 Ω.

- The total load current connected to the reader power supply cannot be more than 0.6A.
- Recommended specifications of cable: Access Controller: AWG16; Card reader power supply: AWG16; Other cables: AWG20 to AWG16.
- It is not recommended to connect both the Wiegand and RS-485 readers.

Chapter 3 Installation

3.1 Install Elevator Controller

Steps

Note

The minimum bearing weight of the wall or other places should be 3 times heavier than the device weight.

1. Drill holes on the wall or other places according to the holes on the guide rail.

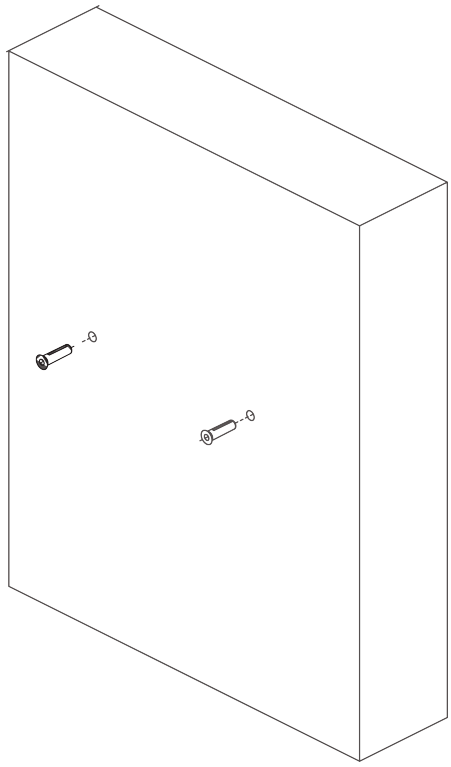


Figure 3-1 Drill Hole

2. Insert the screw sockets of the set screws (supplied) in the drilled holes.

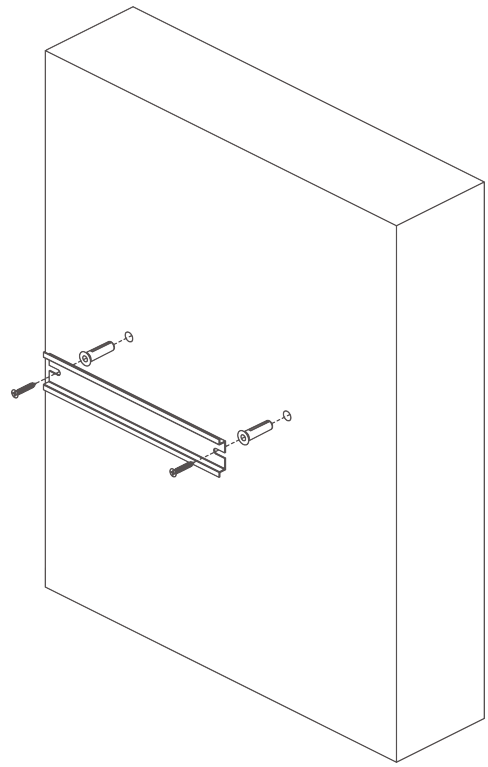


Figure 3-2 Insert Sockets

3. Push the device to the guide rail and complete the installation.

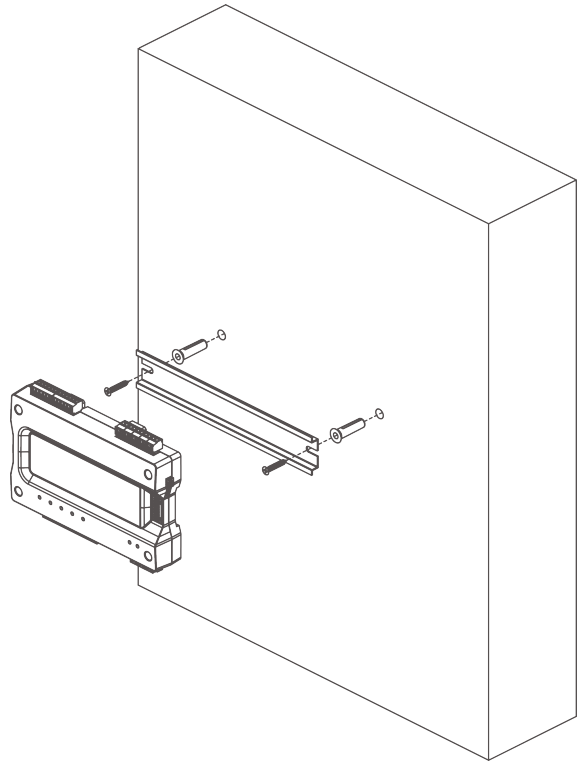


Figure 3-3 Fix Device

3.2 Install Elevator Controller(With Chassis)

Steps

Note

The minimum bearing weight of the wall or other places should be 3 times heavier than the device weight.

1. Make holes in the wall according to the screw holes of the chassis, and insert the sleeve of the expansion screws included in the package into the screw holes.
2. Use the expansion screws included in the package to align the sleeve position, fix the chassis on the mounting position, and complete the installation.

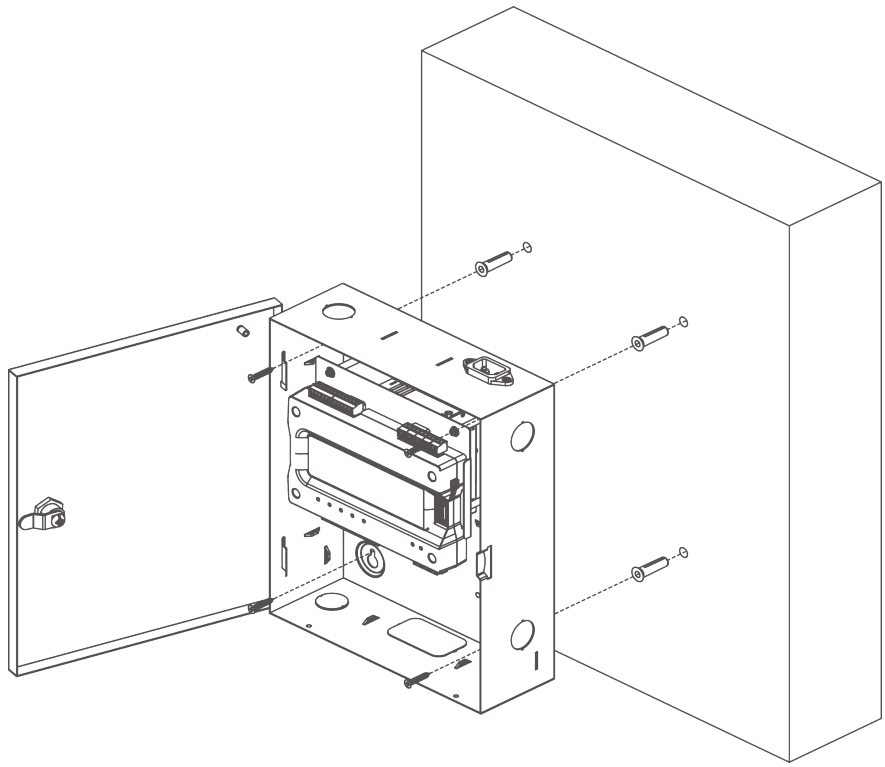


Figure 3-4 Install Device

Chapter 4 Activation

You should activate the device before the first login. After powering on the device, the system will switch to Device Activation page.

Activation via the device, SADP tool and the client software are supported.

The default values of the device are as follows:

- The default IP address: 192.0.0.64
- The default port No.: 8000
- The default user name: admin

4.1 Activate via Web Browser

You can activate the device via the web browser.

Steps

1. Enter the device default IP address (192.0.0.64) in the address bar of the web browser, and press **Enter**.

   Note

   Make sure the device IP address and the computer's should be in the same IP segment.

2. Create a new password (admin password) and confirm the password.

   Caution

   - The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
   - Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
   - Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
   - Password cannot contain words such as hik, hkws, and hikvision (case insensitive).

3. Click **Activate**.
4. Edit the device IP address. You can edit the IP address via the SADP tool, the device, and the client software.

4.2 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/en/*** , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

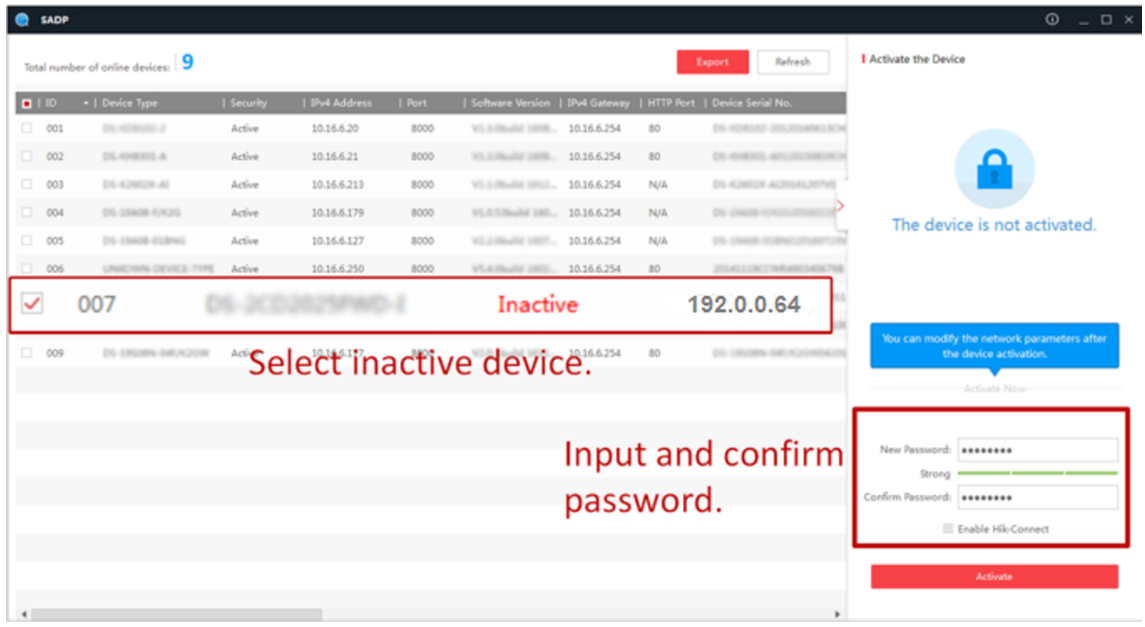
Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Note

Characters containing admin and nimda are not supported to be set as activation password.

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.

1) Select the device.

2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.

3) Input the admin password and click **Modify** to activate your IP address modification.

Chapter 5 Quick Operation via Web Browser

5.1 Set Security Question

If you forget the device activation password, you can change the password via security questions and E-mail. Set the security questions before configuration.

Click in the top right of the web page to enter the **Change Password** page.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

click **Next**. Or you can click **Skip** to skip the step.

5.2 Time Settings

Click in the top right of the web page to enter the wizard page.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address/NTP Port/Interval

You can set the server address, NTP port, and interval.

DST

You can view the DST start time, end time and bias time.

5.3 Floor Settings

You can set Floor No., lowest floor name, and relay linked button type.

1. Enter Floor No. and lowest floor name.

Note

Negative floors (i.e., basement floors) are allowed. When the total and lowest floors are entered, the order and name of the floors in the list of relay associated buttons are automatically generated (except for non-stop floors).

2. Set **Relay Linked Button Type**.

Button

Linked with floor button, used to authenticate elevator pressing button.

Auto Button

Linked with floor button, replaced to pressing button.

Call Elevator Upwards

When Calling Elevator Upwards is enabled, the function of Upwards button out of elevator cab will be linked and replaced.

Call Elevator Downwards

When Calling Elevator Downwards is enabled, the function of Downwards button out of elevator cab will be linked and replaced.

3. Click **Next**.

5.4 Relay Settings

You can set relay corresponding parameters.

You can set the Floor Name and Floor No. as **Non-stop Floor** and set relay linked rules. That is, the output port of the IO module associated with each type of relay for each gate. For example, 3-1 represents the NO1/NC1 and COM1 relay terminals on the RS-485 address 3 sub-controller, and 8-16 represents the NO16/NC16 and COM16 terminals on the RS-485 address 8 sub controller.

You can click **Import** or **Export** to import or export relay linked table.

Click **Complete**.

Chapter 6 Operation via Web Browser

6.1 Login

You can login via the web browser or the remote configuration of the client software.

Note

- Make sure the device is activated. For detailed information about activation, see Activation Chapter.
- It is recommended to log in through the Chrome browser.

Login via Web Browser

Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.
Enter the device user name and the password. Click **Login**.

Login via Remote Configuration of Client Software

Download and open the client software. After adding the device, click to enter the Configuration page.

6.2 Forget Password

If you forget the password when logging in, you can change the password by email address or security questions.

On the login page, click **Forget Password**.

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

Click **Next**, create a new password and confirm it.

6.3 Elevator Control Management

6.3.1 Overview

You can view the elevator working status, view the device status, view the event, view the alarm data, view the person information, network status, basic information, and device capacity. You can also enter the page from quick start part.

Login the web browser and click .

Elevator Working Status

You can view elevator working status.

Quick Start

Click **Add Person**, **Elevator Control Permission**, **Relay Settings**, or **Maintenance** on the upper-right of the page to quick enter the page to configure parameters.

Recent Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation.

You can also click **View More** to enter the search conditions, including the event type, employee ID, the name, the card No., the start time, and the end time, and click **Search**. The results will be displayed on the right panel.

Exception Alarm Data

You can view the alarm data.

Device Status

View the other linked devices' status.

Person Information

View the person number, card number, fingerprint No.

Network Status

You can view the connected and registered status of wired network, ISUP and cloud service.

Basic Information

You can view the model, serial No. and firmware version.

Device Capacity

You can view the person, card, fingerprint, and event capacity.

6.3.2 Search Event

Click **Access Control → Event Search** to enter the Search page.

Enter the search conditions, including the event type, major type, sub type, the employee ID, the name, the card No., the start time, and the end time, and click **Search**.

Note

The searched name should be up to 32 bits.

The results will be displayed on the right panel.

6.3.3 Permission Management

You can set elevator control permission schedule template, holiday schedule template, and set elevator control permission.

Configure Schedule Template

Add Access Schedule Template

Schedule template is used to set the allowed passing time for people to entry and exit. The system disk provides 3 default access schedule templates: All-Day Template, Workday Template and Weekday Template. The user can also add customized template according to needs.

Steps

1. Click **Elevator Control → Elevator Control Permission → Permission Management → Access Plan Management → +Add** .
2. Set basic information.

   Name

   Set basic information.

   Copy from

   The user can select an existing template. After selected, the chosen one will be duplicate to your current template. The user can make adjustments based on this template.
3. On Weekly Schedule, click **Access Time Period**, then you can drag your cursor on the time bar to set access time. You can enable authentication times, and set the authentication times.

   Note

   A maximum of 8 period is allowed per day.
4. **Optional:** Click **Clear**, then drag your cursor. The overlapping part can be erased. You can also click a certain time period then adjust it manually.
5. **Optional:** Select Holiday Schedule.

   Note

   If the chosen Holiday schedule has conflict with Weekly Schedule, the Weekly Schedule will be prioritized.

   1) Click **Select Holiday**.

2) Select existing holiday schedule or click **Add**. Enter Holiday Name, Date and Access Time Period.

Note

A maximum of 8 period is allowed per day.

3) Click **OK**.

4) The user can then check the allowed access time period during the holiday.

6. Click **Save**.

Holiday Schedule Template

Set official holidays or specified dates as holidays. The access level of set holidays is higher than the other basic access level.

Steps

1. Click **Elevator Control → Elevator Control Permission → Permission Management → Holiday Schedule Management → +Add** .
2. Enter holiday name in the right column.
3. **Optional:** Enable **Repeat Annually** according to actual demand. Once enabled, the template will take effect every year. No need to set again. Applicable to set official holidays.
4. Set Start Date and End Date.
5. Drag cursor on corresponding time bar to map valid access period. People can access during valid access period. You can enable authentication times, and set the authentication times.
6. **Optional:** Click **Clear** to adjust chosen time period. You can also click a certain time period then adjust it manually.
7. Click **Save**.

Elevator Control Permission Management

Elevator control permission can be customized or classified based on access point.

Steps

1. Click **Elevator Control → Elevator Control Permission → Permission Management → Elevator Control Permission Management → +Add** .
2. Enter **Access Permission Name**.
3. Select **Access Schedule** Template. Click **View Details** on the right side to check the access time period of different templates.
4. Click **+Add**. Select access floor.
5. Click **Next**, enter or check the organization name or person.
6. Click **Complete**.
7. **Optional:** You can click **Batch Add Passing Persons**, select permission for person to add, organization and person.

View Permission

Steps

1. Click **Access Control → View Permission** .
2. Select organization or enter employee ID or name, you can view corresponding permission.

6.3.4 Elevator Control Application

Elevator Control for First Person

Set the first person on each floor to be allowed to access.

Steps

1. Click **Elevator Control → Elevator Control Configuration → Elevator Control for First Person → +Add** .
2. Click **+Add**.Select floor.
3. Set parameters for Elevator Control for First Person.

   Elevator Control Rule

   Free Access

   The mode is applicable for the passing of groups of persons, such as visitors entering the scenic spots. After the set person passes through, the elevator will open for a set time and other persons can pass through without authentication.

   Controlled Arrival

   This floor needs verification to access.

   Consecutive Authentication Times

   Numbers of successful authentication during consecutive authentication.

   Interval of Consecutive Authentication

   The permitted length of interval of consecutive authentication for a same person. Repeated authentication for the same person during the interval is not valid.

   First Person Authentication Time

   Set **Rules Takes Effect at** and **Authentication Period**.
4. Add First Person Click **+Add** to choose person.
   1) Click **+Add**.
   2) Select a person.
   3) Click **OK**.
5. Click **OK**.
6. **Optional:** Select persons you want to delete from the list. Click **Delete**.

Elevator Arrival Settings

Set elevator free access duration and access forbidden duration by week.

Steps

1. Click **Elevator Control → Elevator Control Configuration → Elevator Arrival Schedule → Set** .
2. Enter schedule name.
3. Click **+ Add**, select floor.
4. Set **Weekly Schedule Template**. You can choose the type of arrival, click and drag on the corresponding time bar, and draw the valid scheduled period. You can also click **Quick Operation** to directly select a plan template.
5. Click **Save**.

Double-sided Elevator Configuration

When the user takes the double-sided elevator, after the elevator reaches the floor, the door with permission will be opened, and the other door will not. Or the user can enter the elevator from one door. After the elevator reaches the floor, the user can exit from the other door.

Steps

1. Click **Elevator Control → Elevator Control Configuration → Double-sided Elevator Configuration** .
2. Enable the elevator as **Double-sided Elevator** as you need.
3. Enter **Elevator Door Name** and **Name of Other Side Door of Elevator**.
4. Click **Save**.
5. **Optional:** You can click **Relay Settings**, and quickly operate.

6.3.5 Parameters Settings

Floor Settings

You can set floor parameters.

Steps

1. Click **Elevator Control → Parameter Settings** .
2. Select floor, and set **Floor Name** and **Door Name**.

   Note

   The number of relays will affect the number of floors.
3. Set **Remote Calling Elevator Button Duration**, **Relay Action Time** and **Extended Open Duration**.

   Extended Open Duration

After configuring this parameters, the door contact restoring time can be appropriately delayed.

4. Click **+ Add** in Linkage Room No.
5. Set **Duress Code**, **Super Password** and **Dismiss Code**.

Duress Code

The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.

Super Password

The specific person can open the door by inputting the super password.

Dismiss Code

When the alarm is triggered, you can enter the dismiss code to dismiss the alarm.

Note

The duress code and the super password should be different.

Set Authentication Parameters

Click **Elevator Control → Parameter Settings → Authentication Parameters** .

Click **Save** to save the settings after the configuration. Click **Copy to** to copy the card reader's parameters to other card readers.

Note

The functions vary according to different models. Refers to the actual device for details.

Card Reader Parameter Configuration

Terminal/Terminal Name

Create a name for the card reader.

Enable Authentication Device

Enable the authentication function.

Authentication Interval

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed.

Alarm of Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Max. Authentication Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Communication with Controller Every

When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

Max. Interval When Entering Password

When you entering the password on the card reader, if the interval between pressing two digits is longer than the set value, the digits you pressed before will be cleared automatically.

OK LED Polarity/Error LED Polarity/Buzzer Polarity

Set OK LED Polarity/Error LED Polarity/Buzzer Polarity of the access control device according to the card reader parameters. Generally, adopts the default settings.

Tampering Detection

Enable the anti-tamper detection for the card reader.

QR Code

Enable the function and the card reader can recognize the QR code for authentication.

Note

The function should be supported by the card reader.

Bluetooth Parameter Configuration

Enable Bluetooth

Enable the bluetooth function and the you can use the bluetooth function (e.g. opening door) on the card reader.

Device Name/Transmitting Power

Edit the card reader's name and its transmitting power.

Open Door via Bluetooth

Enable the function and you can open the door via bluetooth through App. You should add the device to the App before use the function.

Authentication Plan Configuration

Set the authentication schedule for the card reader.

Select an authentication type and drag the time duration on the time schedule table to draw the authentication duration.

Click **Clear** and drag a time duration to delete, or click ··· → **Clear All** to delete all time durations.

Set Smart Parameters

Click **Elevator Control → Parameter Settings → Smart** .

Note

- The functions vary according to different models. Refers to the actual device for details.
- After configuring the general parameters, all card readers will take effect.

Click **Save** to save the settings after the configuration.

Fingerprint Security Level

Select the fingerprint security level.

The higher is the security level, the lower is the false acceptance rate (FAR).

Card Settings

Set Card Security

Click **Elevator Control → Parameter Settings → Card Settings** to enter the settings page.

Set the parameters and click **Save**.

Enable NFC Card

In order to prevent the mobile phone from getting the data of the access control, you can enable NFC card to increase the security level of the data.

Enable M1 Card

Enable M1 card and authenticating by presenting M1 card is available.

M1 Card Encryption
Sector

M1 card encryption can improve the security level of authentication.

Enable the function and set the encryption sector. By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

Enable EM Card

Enable EM card and authenticating by presenting EM card is available.

Note

If the peripheral card reader supports presenting EM card, the function is also supported to enable/disable the EM card function.

Enable DESFire Card

The device can read the data from DESFire card when enabling the DESFire card function.

DESFire Card Read Content

The device can read the DESFire card content.

Enable FeliCa Card

The device can read the data from FeliCa card when enabling the FeliCa card function.

Set Card No. Authentication Parameters

Set the card reading content when authenticate via card on the device.

Go to **Elevator Control → Parameter Settings → Card Settings** .

Select a card authentication mode and set the reversed card No. and click **Save**.

Enable Reversed Card No.

The read card No. will be in reverse sequence after enabling the function.

Set Privacy Parameters

Set the event storage type.

Go to **Elevator Control → Parameter Settings → Privacy Settings**

Select a method to delete the event. You can select from **Delete Old Events Periodically**, **Delete Old Events by Specified Time**, or **Overwriting**. Click **Save** after configuration.

Delete Old Events Periodically

Drag the block or enter number to set the period for event deleting. All events will be deleted according to the configured time duration.

Delete Old Events by Specified Time

Set a time and all events will be deleted on the configured time.

Overwriting

The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

Set Password Mode

Before configuring passwords, it is necessary to clarify whether the password is a device-set personal PIN or a platform-applied personal PIN. If it is a device-set personal PIN, it can be created or edited on the device or on the web, and cannot be set on other platforms; If it is a platform-applied personal PIN, it can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.

Steps

1. Click **Elevator Control → Parameter Settings → Privacy Settings**

Device-Set Personal PIN

It can be created or edited on the device or on the web, and cannot be set on other platforms.

Platform-Applied Personal PIN

It can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.

2. Click **Save**.

6.4 Person Management

6.4.1 Add Organization

After you add an organization, you can add people to the corresponding organization.

Steps

1. Click **Person Management** to enter the settings page.
2. Click **+** on the left side of the page and select the parent organization.
3. Create the organization name.
4. Click **Save**.

   The added organization will be listed in the selected parent organization.
5. **Optional:** Edit / Delete
   - Click an organization, and then click to edit the organization information.

     Select people and click **Delete** to delete the information in batch.

     Click **Clear All**, and all person information will be deleted.
   - Click an organization and click to delete that organization information.

6.4.2 Add Person

Add the person's information, including the basic information, certificate, authentication and settings.

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, organization, gender, and person type.
This person can be set as a **Property Manager**, who has access to all floors 24 hours a day.

Note

- If you select **Visitor** as the person type, you can set the visit times.
- Letters are allowed in the employee ID. Up to 32 bits are allowed.
- Up to 128 bits are allowed in the name.

Click **Add** to save the settings.
Click **Save and Continue** to save the settings and continue to add next person.

Set Permission Time

Click **Person Management → Add** to enter the Add Person page.
Enable **Long-Term Effective User**, or set **Start Time** and **End Time** and the person can only has the permission within the configured time period according to your actual needs.
Click **Add** to save the settings.
Click **Save and Continue** to save the settings and continue to add next person.

Add Card

Click **Person Management → Add** to enter the Add Person page.
Click **Configuration**. If select the Collection Device as **Card Enrollment Station**, you should select the device model, card type, set buzzing, M1 card encryption, and sector. Click **OK** to save.

Note

If select the Collection Device as **Card Enrollment Station**, click **Download** to download the plug-in to view the device status. During the installation, you should close the web page.

If select the Collection Device as **Card Reader**, you should select the card reader from the drop-down list. Click **OK** to save.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.
Click **Add** to save the settings.
Click **Save and Continue** to save the settings and continue to add next person.

Add Fingerprint

Note

Only devices supporting the fingerprint function can add the fingerprint.

Click **Person Management → Add** to enter the Add Person page.
Click **Configuration**. If you select**USB Fingerprint Recorder**, you can click **Download**to download the plug-in and view the status. Or select **Fingerprint and Card Reader** and select a card reader from the drop-down list. Click **OK** to save.

Note

During the installation, you should close the web page.

Click **Add Fingerprint**, and press your finger on the fingerprint module of the device to add your fingerprint.
Click **Add** to save the settings.
Click **Save and Continue** to save the settings and continue to add next person.

Note

The plugin for adding card or fingerprint via USB is only available in Windows.

Add PIN

Before configuring PIN, it is necessary to clarify whether the PIN is a device-set personal PIN or a platform-applied personal PIN. If it is a device-set personal PIN, it can be created or edited on the device or on the web, and cannot be set on other platforms; If it is a platform-applied personal PIN, it can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.
Make sure you have already set the PIN mode as **Device-Set Personal PIN** in ***Set Password Mode*** .
Click **PIN Mode** on the page to go to configure.
Click **Person Management → Add** to enter the Add Person page.
Set the PIN. Or click **Auto Generate** to generate a PIN automatically.
Click **Add** to save the settings.
Click **Save and Continue** to save the settings and continue to add next person.

Authentication Settings

Click **Person Management → Add** to enter the Add Person page.
Set the authentication type.
Click **Add** to save the settings.
Click **Save and Continue** to save the settings and continue to add next person.

Set Device No.

Click **Add** in **Room No. Settings** to add corresponding room.

Edit/Delete/Search Person

Click **Person Management** to enter the page.
Select a person and click to edit the person's information.
Select a person and click to delete the person information.
Select multiple person, click **Delete** can delete person in batch.
Click **Import** or **Export**.
Click **Clear All** to delete all person information.
Click or to switch the viewing method.
Enter the person's employee ID and select the credential status and click **Filter** to search. Click **Reset** to reset all conditions.
Check **Show Sub Organization**, all persons in the sub organizations will be displayed.

6.5 Device Management

6.5.1 Module Management

The system can automatically search for modules that have been connected to the controller.

Click **Device Management → Module Management** . The searched modules will be displayed in the list of the page.

6.5.2 Relay Settings

You can view relay status and set relay parameters.

Steps

1. Click **Device Management → Elevator Control Relay → Relay Status** , view each gate relay status..
2. Click **Device Management → Elevator Control Relay → Relay Settings**
3. You can set the Floor No. as **Non-stop Floor** and set relay linked rules. That is, the output port of the IO module associated with each type of relay for each gate. For example, 3-1 represents the NO1/NC1 and COM1 relay terminals on the RS-485 address 3 sub-controller, and 8-16 represents the NO16/NC16 and COM16 terminals on the RS-485 address 8 sub controller.
4. Click **Save**.
5. You can click **Elevator Control Test** to test elevator control here.

6.6 System and Maintenance

6.6.1 View Device Information

View the device name, language, model, serial No., version, IO input, IO output, RS-485, alarm input, alarm output, and device capacity, etc.

Click **System and Maintenance → System Configuration → System → System Settings → Basic Information** to enter the configuration page.

You can the device name, language, model, serial No., version, RS-485, alarm input, alarm output, and device capacity, etc.

6.6.2 Set Time

Set the device's time zone, synchronization mode, server address, NTP port, and interval.

Click **System and Maintenance → System Configuration → System → System Settings → Time Settings** .

Click **Save** to save the settings after the configuration.

Time Zone

Select the device located time zone from the drop-down list.

Time Synchronization Mode

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server IP Address/NTP Port/Interval

You can set the server IP address, NTP port, and interval.

6.6.3 Set DST

Steps

1. Click **System and Maintenance → System Configuration → System → System Settings → Time Settings** .
2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

6.6.4 Change Administrator's Password

Steps

1. Click **System and Maintenance → System Configuration → System → User Management** .
2. Click .
3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **Save**.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

6.6.5 Account Security Settings

You can change the security questions and answers, or the email address for the device. After change the settings, once you forgot the device password, you should answer the new questions or use the new email address to reset the device password.

Steps

1. Click **System and Maintenance → System Configuration → System → User Management → Account Security Settings** .
2. Change the security questions or email address according your actual needs.
3. Enter the device password and click **OK** to confirm changing.

6.6.6 View Online User

You can view online users.

Click **System and Maintenance → System Configuration → System → User Management → Online Users** .

You can view online users' information including name, type, IP Address and operation time. Click **Refresh** to refresh the page.

6.6.7 View Open Source Software License on PC Web

On the main page of the device PC Web, click → **Open Source Software Statement** , to view the device license.

6.6.8 View Device Arming/Disarming Information

View device arming type and arming IP address.

Go to **System and Maintenance → System Configuration → System → User Management → Arming/Disarming Information** .

You can view the device arming/disarming information. Click **Refresh** to refresh the page.

6.6.9 Network Settings

Set Basic Network Parameters

Click **Configuration → Network → Network Settings → TCP/IP** .

Set the parameters and click **Save** to save the settings.

NIC Type

Select a NIC type from the drop-down list.

DHCP

If uncheck the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, IPv6 mode, IPv6 address, IPv6 subnet prefix length, IPv6 default gateway, Mac address, and MTU.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway, IPv6 mode, IPv6 address, IPv6 subnet prefix length, and IPv6 default gateway automatically.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Set Port Parameters

Set the HTTP, HTTPS, HTTP Listening, RTSP and Server port parameters.

Click **System and Maintenance → System Configuration → Network → Network Service → HTTP(S)** .

HTTP

It refers to the port through which the browser accesses the device. For example, when the HTTP Port is modified to 81, you need to enter ***http://192.0.0.65:81*** in the browser for login.

HTTPS

Set the HTTPS for accessing the browser. Certificate is required when accessing.

HTTP Listening

The device can send alarm information to the event alarm IP address or domain name via HTTP protocol/HTTPS protocol. Edit the event alarm IP address or domain name, URL, port, and protocol.

Note

The event alarm IP address or domain name should support the HTTP protocol/HTTPS protocol to receive the alarm information.

Click **System and Maintenance → System Configuration → Network → Network Service → WebSocket(s)** .

View WebSocket and WebSockets port.

Set ISUP Parameters

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

1. Click **System and Maintenance → System Configuration → Network → Device Access → ISUP** .
2. Check **Enable**.

3. View the ISUP version, set server IP address, port, device ID, encryption key and view the ISUP status.
4. Set the ISUP listening parameters, including ISUP alarm center IP address/domain name, ISUP alarm center URL, and ISUP alarm center port.
5. Click **Save**.

Platform Access

Platform access provides you an option to manage the devices via platform.

Steps

1. Click **System and Maintenance → System Configuration → Network → Device Access → Hik-Connect** to enter the settings page.

   Note

   Hik-Connect is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.

2. Check **Enable** to enable the function.
3. **Optional:** Check **Custom**, and you can set the server address by yourself.
4. Enter the verification code.
5. **Optional:** View the register status. Click **Refresh** to refresh the status.
6. Click **View** to view device QR code. Scan the QR code to bind the account.

   Note

   8 to 32 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

7. Click **Save** to enable the settings.
8. **Optional:** Click **Refresh** to refresh the binding status.
9. Click **Save**.

6.6.10 Access Configuration

You can set RS-485, Wiegand and host parameters.

Set RS-485 Parameters

You can set the RS-485 parameters including the peripheral, address, baud rate, etc.

Click **System and Maintenance → System Configuration → Access Configuration → RS-485** .

Click **Save** to save the settings after the configuration.

RS-485 Communication Backup

When enabled, there will be a backup line when the reader communicates via RS-485.

RS-485 Protocol

Select the RS-485 protocol from the drop-down list.

No.

Select the RS-485 No.

Baud Rate

The baud rate when the devices are communicating via the RS-485 protocol.

Serial Port Name

View the serial port name.

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

Note

Some device models do not support this function. Refer to the actual products when configuration.

1. Click **System and Maintenance → System Configuration → Access Configuration → Wiegand Settings** .
2. Select a access point from the list on the left.
3. Set Wiegand parameters.

   No.

   Select Wiegand No. for parameters settings.

   Wiegand

   select to enable the card reader's Wiegand function.

   Wiegand Direction

   By default, the direction is **Input**.

   Wiegand Mode

   Select the Wiegand mode and the card reader can communicate with the controller.

   Click **Auto Recognize**, enter card No. to recognize the Wiegand mode. Enter the Card No., and click **Start to Recognize**. Present the card on the related card reader. The system will show the Wiegand mode. Click **OK**.

   If select **Custom**, you should set custom Wiegand parameters. Click **Custom Wiegand Settings**, and set the name, parity type, total length and Wiegand rule. Click **OK**.
4. Click **Save** to save the settings.

Note

If you change the peripheral, and after you save the device parameters, the device will reboot automatically.

6.6.11 Event Settings

Set the event linkage and the alarm output paramters.

Alarm Output Settings

Set the device's alarm output parameters.

Click **System and Maintenance → System Configuration → Event → Alarm Settings → Alarm Output** .

Select an access point from the list on the left. Select a alarm output device No. Create a name for the alarm output device and set the alarm duration. Click **Save**. You can click **Copy To** the copy the parameters.

Continuous Alarm

The alarm output device will continuously in the alarm status.

Custom Alarm Duration

You should set the custom duration. The alarm output device will be in the alarm status for the configured time duration.

Note

Range: from 1 to 5999s.

Event Linkage

Set linked actions for events.

Steps

1. Click **System and Maintenance → System Configuration → Event → Linkage Configuration** to enter the page.
2. Click +
3. Set event source.
   - If you choose **Linkage Type** as **Event Linkage**, you need to select event types from the drop-down list.
   - If you choose **Linkage Type** as **Card Linkage**, you need to enter the card No. and select the card reader.
   - If you choose **Linkage Type** as **Link Employee ID**, you need to enter the employee ID and select the card reader.

4. Set linked action.

Linked Access Controller Buzzing

Enable **Linked Access Controller Buzzing** and select **Start Buzzing** or **Stop Buzzing** for the target event.

Card Reader Linkage

Enable **Card Reader Linkage** and click **Add** can check the card reader that will buzz. Click **Save**.

Set the card reader's buzzing action.

Click to delete single card reader. Check the card readers and click **Delete** to delete in batch. Click **Batch Configure** to configure all card readers in the list.

Linked Button

Enable **Linked Button** and click **Add**.

Select linked button and action. Click **Save**.

Linked Alarm Output

If the Linkage Type in the Event Source is **Card Linkage**, when enable **Linked Alarm Output**, you can set **Triggering Times Configuration**, **Triggering Times (Enable)**, and **Triggering Times (Disable)**.

If set **Triggering Times (Enable)** as 3, and **Triggering Times (Disable)** as 3, you can present the card that configured in the Event Source for 3 time to stop alarm when the following alarm output in the list is in open status. If the alarm output is in the disabled status, you can present the card for 3 times to trigger alarm.

Set the alarm output. Click **Add** and check the alarm outputs in the list and click **Save**.

5. You can enable **Linkage Triggering Time Configuration**, and set **Triggering Times** and **Interval**.
6. Click **Save**.

6.6.12 Maintenance and Security

Set Network Diagnosis

Enter the device IP address or domain name, you can perform PING settings. Debug the network according to the PING result.

Go to **Maintenance and Security → Maintenance → Network Diagnosis** .

Enter the device IP for PING operation, select the network connection mode, PING duration, and Ping data package size (default parameter is recommended.) Click **Diagnose**. The result will displayed in **PING Result**.

Upgrade and Maintenance

Reboot device, restore device parameters, and upgrade device version.

Reboot Device

Click **System and Maintenance → Maintenance → Host** .
Click **Restart** to reboot the device.

Reboot Sub Device

Click **System and Maintenance → Maintenance → Sub-Device** .
Set the device, and click **Restart**.

Upgrade

Click **System and Maintenance → Maintenance → Upgrade** .
Select an upgrade type from the drop-down list. Click and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.
If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can click **Upgrade** after Online Update to upgrade the device system.

Note

Do not power off during the upgrading.

Sub Device Upgrade

Click **System and Maintenance → Maintenance → Upgrade** .
Select an upgrade type from the drop-down list. Click and select the upgrade file from your local PC and click **Next**. Click **Upgrade** to start upgrading.

Restore Parameters

Click **System and Maintenance → Maintenance → Backup and Reset → Host** .

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Restore

The device will restore to the default settings, except for the device IP address and the user information.

Restore Sub-Device Parameters

Click **System and Maintenance → Maintenance → Backup and Reset → Sub-Device** .
Select the device, and click **Restore to Factory Settings**.

Import and Export Parameters

Click **System and Maintenance → Maintenance → Backup and Reset** .

Export

Click **Export** to export the device parameters.

Note

You can import the exported device parameters to another device.

Import

Click and select the file to import. Click **Import** to start import configuration file.

Device Debugging

You can set device debugging parameters.

Steps

1. Click **System and Maintenance → Maintenance → Device Debugging** .
2. You can set the following parameters.

Enable SSH

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals. You can click **Debug** to debug SSH.

Print Log

You can click **Export** to export log.

Capture Network Packet

You can set the **Capture Packet Duration**, **Capture Packet Size**, and click **Start** to capture.

Log Query

You can search and view the device logs.

Go to **System and Maintenance → Maintenance → Log** .

Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

Test Protocol via PC Web

Select a protocol address, and enter the protocol to test. You can debug the device according to the response header and returned value.

Go to **System and Maintenance → Maintenance → Device Debugging → Protocol Testing**.

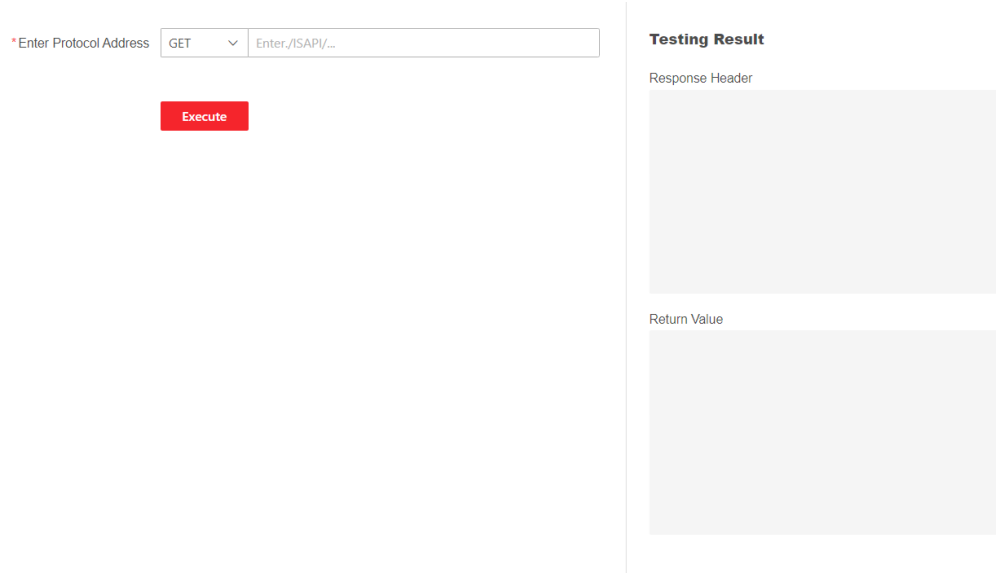


Figure 6-1 Protocol Testing

Select a protocol address, and enter the protocol. Click **Execute**.

Debug the device according to the response header and returned value.

Elevator Control Test

To test the configuration and wiring of the elevator control relay, whether the relay is functioning normally, and whether the elevator operates normally after button actions.

Steps

Note

Please ensure that the IO Module No. and IO Module Output Port No.linked with the auto button have been set in **Device Management → Elevator Control Relay → Relay Settings** .

1. Click **System and Maintenance → Maintenance → Elevator Control Test → Enter Test Mode** .
2. Click **Test** according to you needs, to test the configuration and wiring of the elevator control relay, whether the relay is functioning normally, and whether the elevator operates normally after button actions.

6.6.13 Certificate Management

It helps to manage the server/client certificates and CA certificate.

Note

The function is only supported by certain device models.

Create and Import HTTPS Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **HTTPS Certificate** area, click **Create Certificate Request**.
3. Input certificate information and click **Save**.
   - Click **View** and the created certificate will be displayed.
   - The certificate will be saved automatically.
4. Download the certificate and save it to an asking file in the local computer.
5. Send the asking file to a certification authority for signature.
6. Import the signed certificate.
   1) In the **Import Key** area, select a certificate from the local, and click **Import**.
   2) In the **Import Communication Certificate** area, select a certificate from the local, and click **Import**.

Create and Import SYSLOG Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **SYSLOG Certificate** area, click **Create Certificate Request**.
3. Input certificate information and click **Save**.
   - Click **View** and the created certificate will be displayed.
   - The certificate will be saved automatically.
4. Download the certificate and save it to an asking file in the local computer.
5. Send the asking file to a certification authority for signature.
6. Import the signed certificate.
   1) In the **Import Key** area, select a certificate from the local, and click **Import**.
   2) In the **Import Communication Certificate** area, select a certificate from the local, and click **Import**.

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Create an ID in the **CA Certificate ID** area.

Note

The input certificate ID cannot be the same as the existing ones.

3. Upload a certificate file from the local.
4. Click **Import**.

Chapter 7 Other Platforms to Configure

You can also configure the device via HikCentral Professional Mobile Client. For details, see the platforms' user manual.

HikCentral Professional Mobile Client (HCP)

Click/tap the link to view the HCP's user manual.

http://enpinfodata.hikvision.com/analysisQR/showQR/24cb4850

Appendix A. Dimension

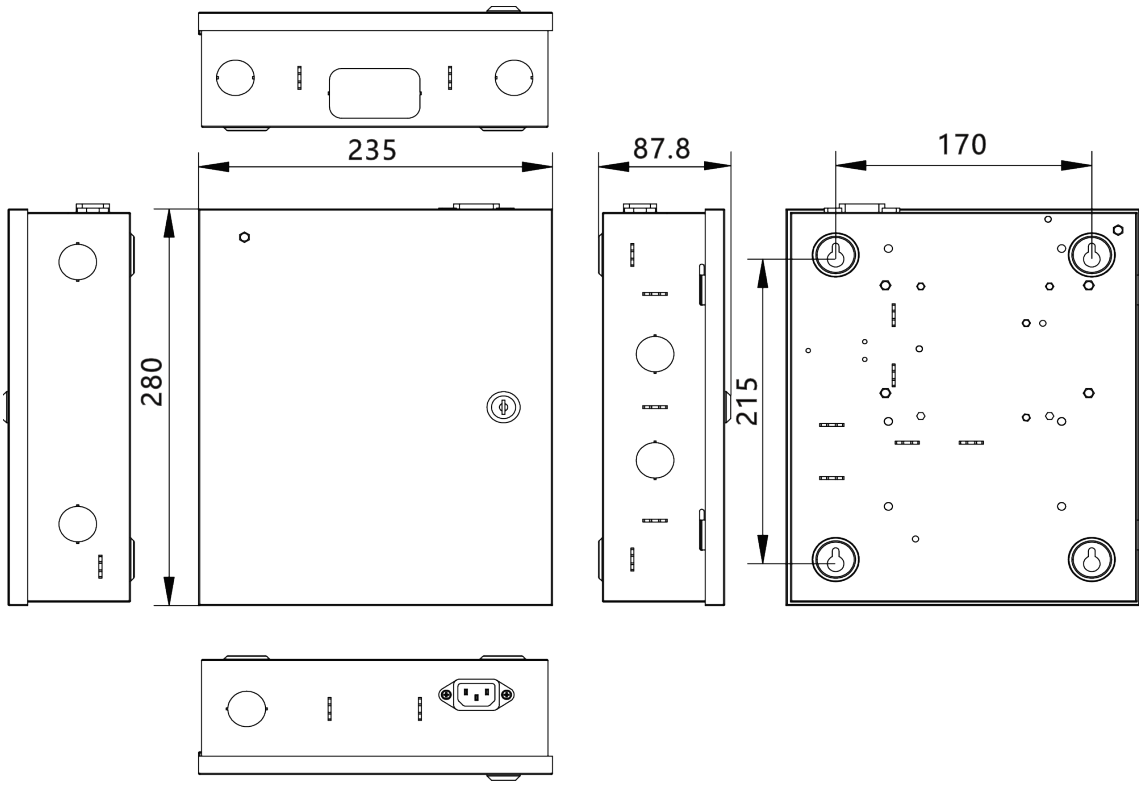


Figure A-1 Dimension (With Chassis)

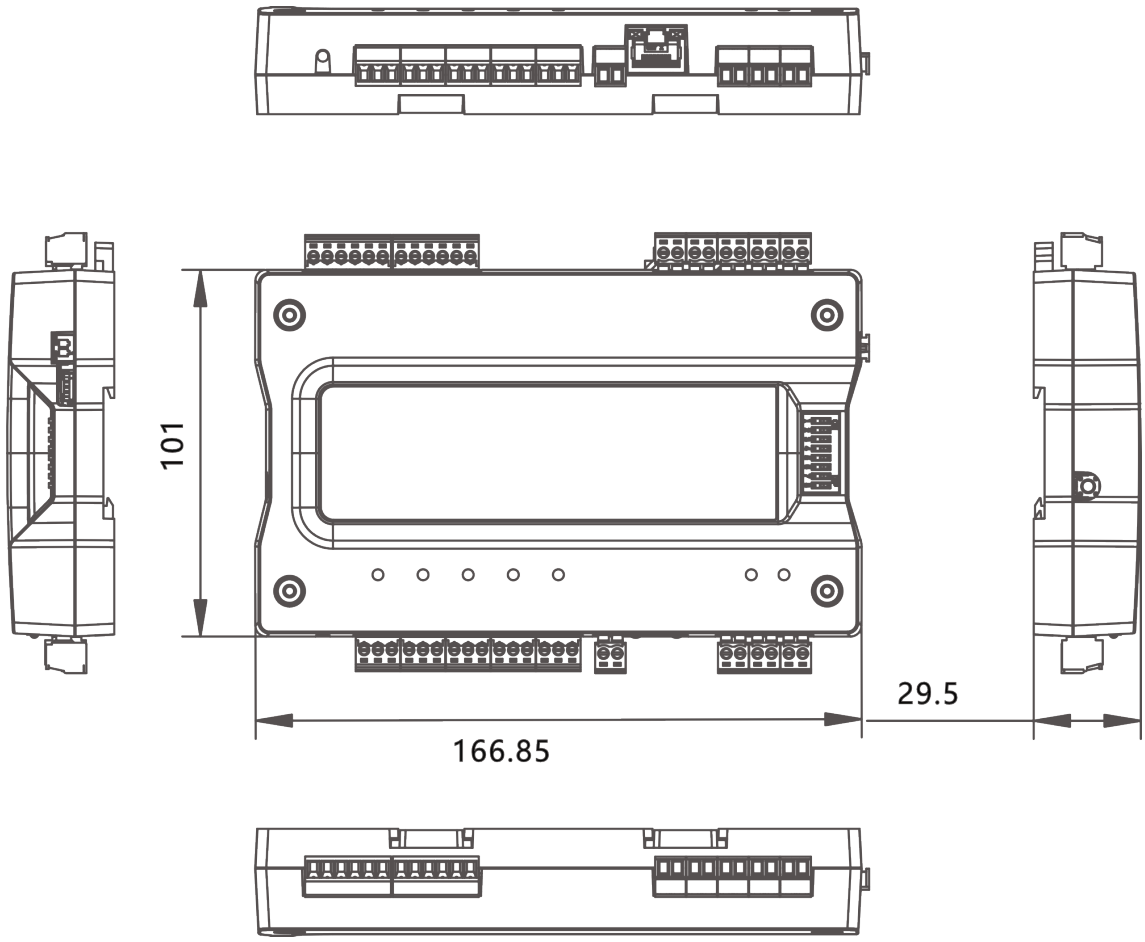


Figure A-2 Dimension (Without Chassis)

Unit: mm.


See Far, Go Further