DS-K3GL606WX Series Sliding Gate Opener

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.

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 A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
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

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

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.

COMPLIANCE NOTICE

The thermal series products might be subject to export controls in various countries or regions, including without limitation, the United States, European Union, United Kingdom and/or other member countries of the Wassenaar Arrangement. Please consult your professional legal or compliance expert or local government authorities for any necessary export license requirements if you intend to transfer, export, re-export the thermal series products between different countries.

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:

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- The equipment must be connected to an earthed mains socket-outlet.
- Shock hazard! Disconnect all power sources before maintenance.
- ⚡ indicates hazardous live and the external wiring connected to the terminals requires installation by an instructed person.
- This equipment is not suitable for use in locations where children are likely to be present.
- 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.

  If the top caps should be open and the device should be powered on for maintenance, make sure:

  1. Power off the fan to prevent the operator from getting injured accidentally.
  2. Do not touch bare high-voltage components.
  3. Make sure the switch’s wiring sequence is correct after maintenance.
- 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:

- Fit the warning signs visibly.
- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the equipment.
- Ensure correct wiring of the terminals for connection to an AC mains supply.
- The equipment has been designed, when required, modified for connection to an IT power distribution system.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current. + identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains, etc. The openings shall never be blocked by placing the equipment on a bed, sofa, rug or other similar surface.
- Stainless steel may be corroded in some circumstances. You need to clean and care the device by using the stainless steel cleaner. It is suggested to clean the device every month.
- 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.
- 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.
- Keep all wrappers away from children to prevent potential hazards.
- 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.
- Dispose of packaging materials, batteries, and other waste in accordance with local regulations.
- Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.
- SUITABLE FOR MOUNTING ON CONCRETE OR OTHER NON-COMBUSTIBLE SURFACE ONLY.
- The instructions shall require connection of the equipment protective earthing conductor to the installation protective earthing conductor.
- Activate the device only when visible and its path is confirmed clear of people, pets, or obstructions.
- Don't cross or allow people/objects near a moving device or its travel path.
- Secure controls in order to prevent unauthorised use of the device.
- The device shall execute a self-test routine upon reboot initialization.
- For emergency power supply, connect the battery directly from the power supply board to the control board for power transmission.
- Do not lift the device by holding the main control board.

Contents

Chapter 1 Main Features

- Support built-in Wi-Fi and LAN interfaces, easy for remote management system.
- Battery-driven, Max. open speed at 36 m/Min (2 x 12V 7AH batteries are essential for normal operation).
- Support mobile web configuration with AP mode by a simple touch on NFC tags.
- Support component status self-diagnostics
- Support built-in access system, could achieve the functions of opening doors via PIN, card, and QR code with external AC card reader.
- The system supports linkage function, enabling integrated applications with intercom, alarm, and access control systems.
- The product supports low-power mode, which allows for excellent power consumption management after a power outage, achieving longer standby times and more door opening and closing cycles.

Chapter 2 Installation and Wiring

2.1 Installation and Wiring Guide Video

Scan the QR Code to view the installation guide video.

2.2 General Considerations

The preparation before installation and general wiring.

Note

- Install extra safety edges and beams to prevent entrapment and mechanical risks.
- Check no pipes or cables are in the installation area.
- Ensure sufficient space for the gate opener, especially for the release handle.
- Inspect soil for looseness or sandiness when installing a foundation; a larger one may be needed.
- Do not install the gate opener on the gate's outer side accessible to the public.
- If the width of the gate is less than 1.5 m, the speed cannot reach 36 m/min.
- Install the device strictly according to the recommended location and method to avoid potential malfunctions.

2.3 Foundation Plate Installation

2.3.1 Position Determination

Note

When installing the door operator, refer to this chapter to determine the installation position and height of the foundation plate.

Initial Reference Point

Establish a reference point by manually opening and closing the gate past a stationary point (e.g., a vertical spike). Identify the furthest protruding gate component (including wheels) toward the gate opener installation area. Once the point which protrudes the furthest has been found, this will be the reference point to be used when finding the optimum position for the gate opener.

Minimum Clearances

Determine the minimum clearances according to examples illustrating below.

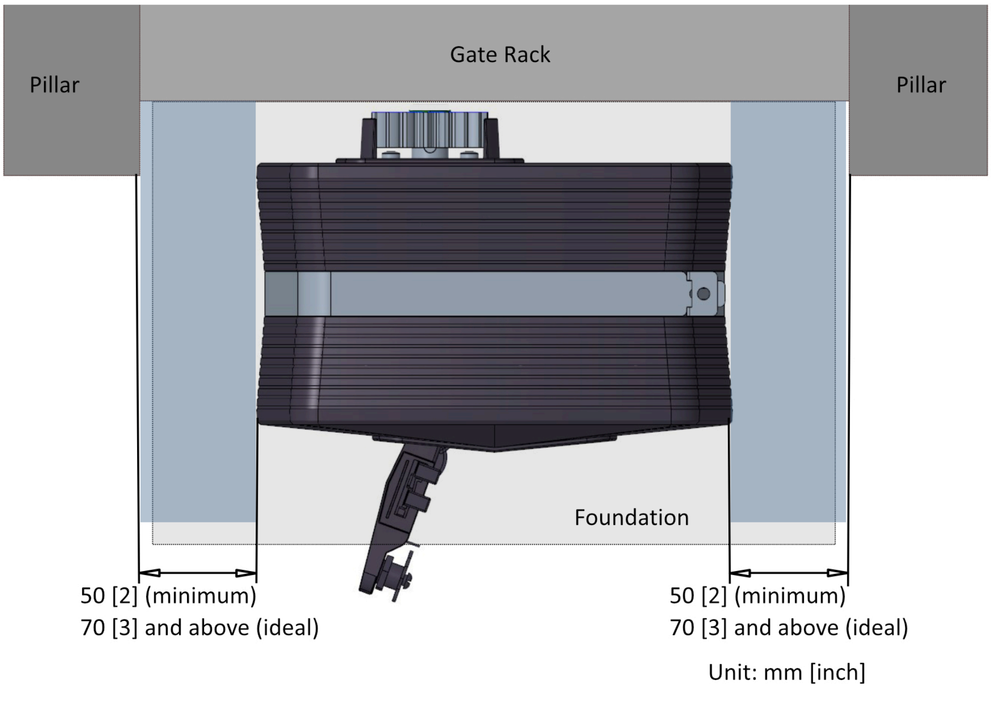


Figure 2-1 Minimum Clearance - Sides

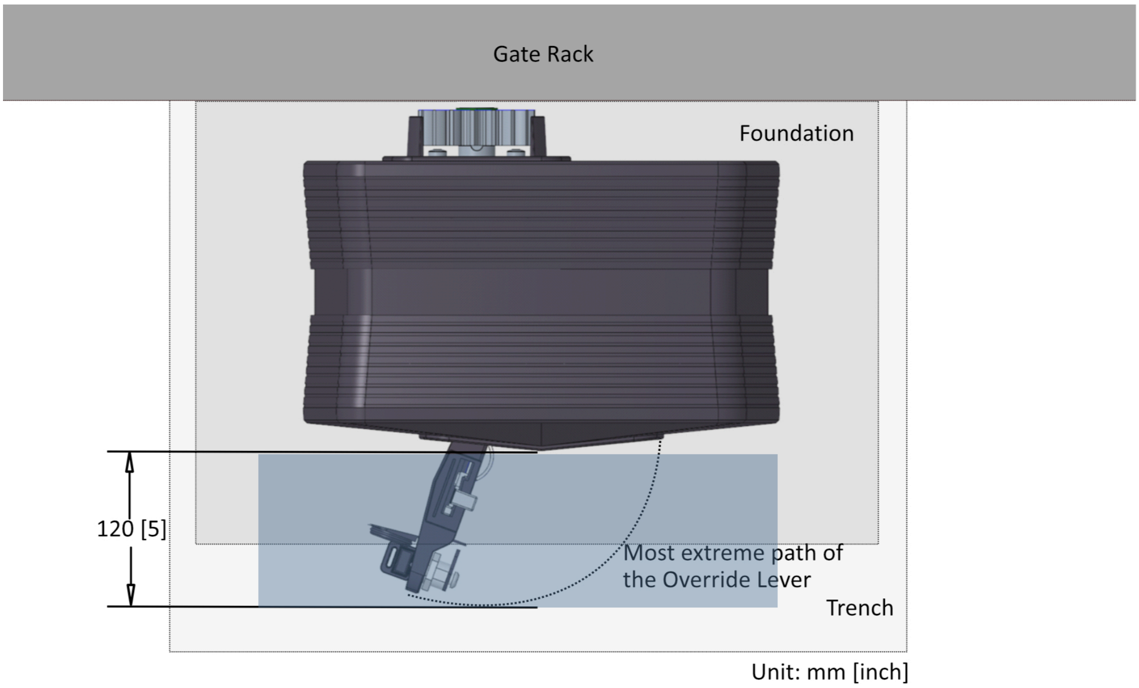
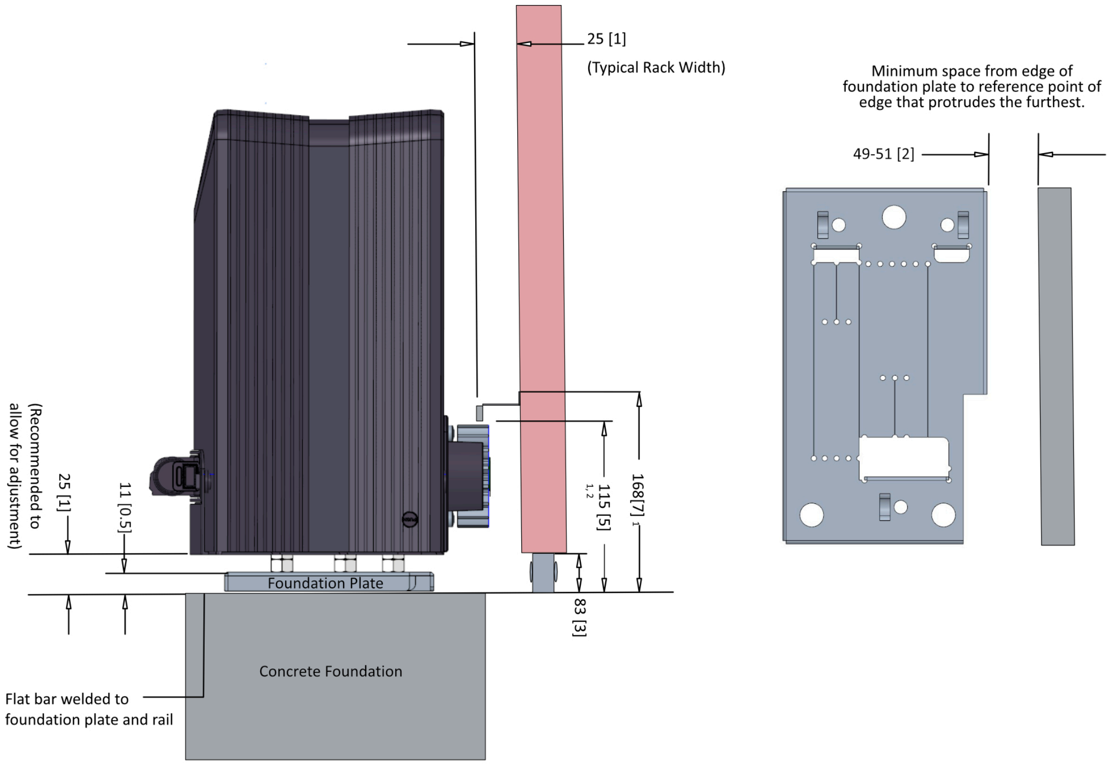


Figure 2-2 Minimum Clearance - Front

Operator's Position

Install the base plate flush with the driveway entrance to prevent operator protrusion. Mount the rack above the pinion or underneath according to examples illustrating below.


25 [1]
(Typical Rack Width)
Minimum space from edge of foundation plate to reference point of edge that protrudes the furthest.
49-51 [2]
(Recommended to allow for adjustment)
25 [1]
11 [0.5]
115 [5]
168[7]
83 [3]
Foundation Plate
Concrete Foundation
Flat bar welded to foundation plate and rail

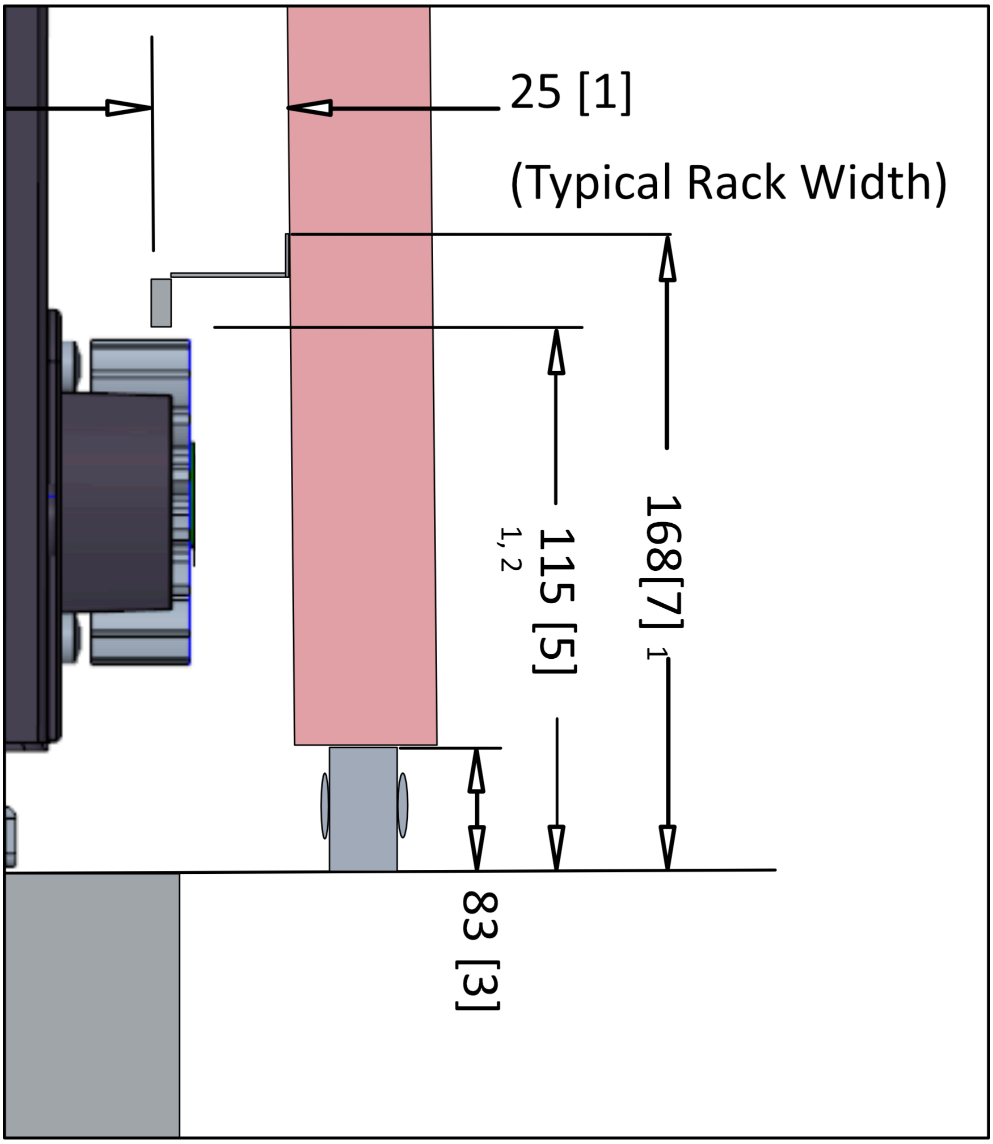
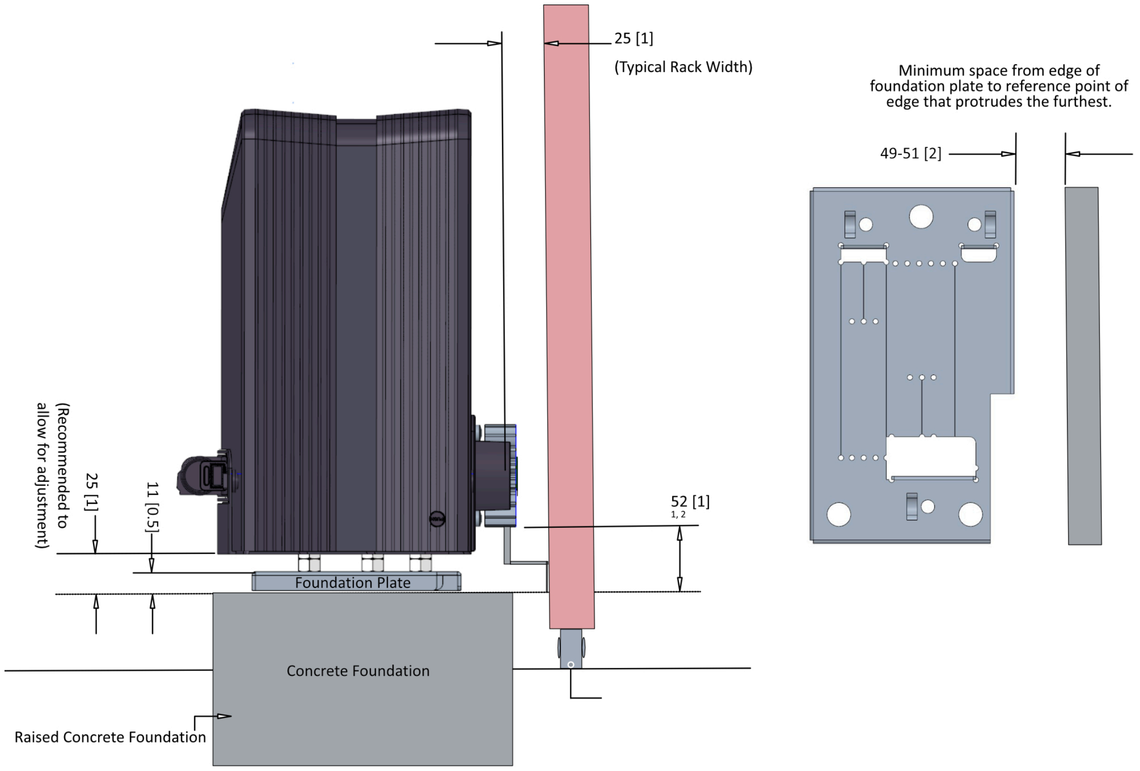


Figure 2-3 Rack Above Pinion


25 [1]
(Typical Rack Width)
Minimum space from edge of foundation plate to reference point of edge that protrudes the furthest.
49-51 [2]
52 [1]
1, 2
(Recommended to allow for adjustment)
25 [1]
11 [0.5]
Foundation Plate
Concrete Foundation
Raised Concrete Foundation

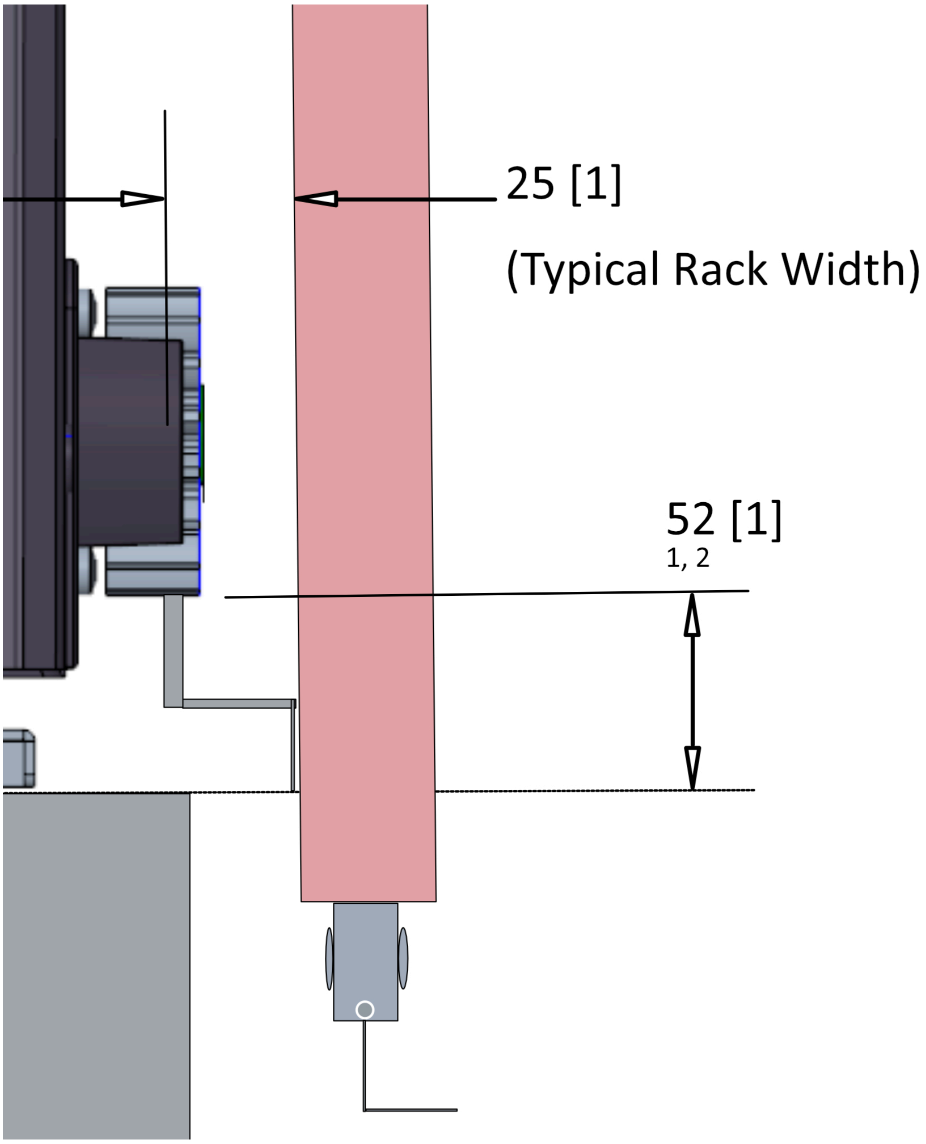


Figure 2-4 Rack Below Pinion

Note

- 1 stands 3mm clearance required between rack and pinion is included.
- 2 stands distance between bottom of the Foundation Plate and bottom edge of the Rack Tooth.

2.3.2 Mount Foundation Plate

You can mount the foundation plate either by setting it into a new concrete foundation or by bolting it down onto an existing concrete plinth.

Before You Start

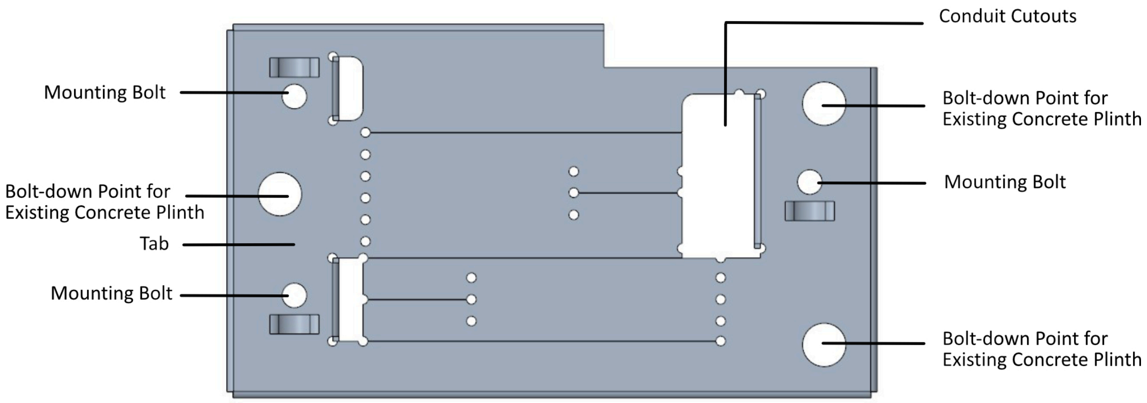

Conduit Cutouts
Mounting Bolt
Bolt-down Point for Existing Concrete Plinth
Bolt-down Point for Existing Concrete Plinth
Mounting Bolt
Tab
Mounting Bolt
Bolt-down Point for Existing Concrete Plinth

Figure 2-5 Foundation Plate Components

New Concrete Foundation

Before You Start

Note

- Do not deform the foundation plate while bending the tabs.
- For concrete foundation installation, it's suggested to attach the foundation plate to the gate's track using a flat bar. This method enables you to complete the mechanical and electrical setup while the concrete is still wet. After finishing the setup, cast the concrete and leave the operator in manual mode until it cures. Do not activate the motor until the concrete has completely cured.

Steps

1. Tighten the M10 half-nuts to 20Nm on the mounting bolts. Gently bend the two tabs on the foundation plate to a 90° angle using a pair of pliers.

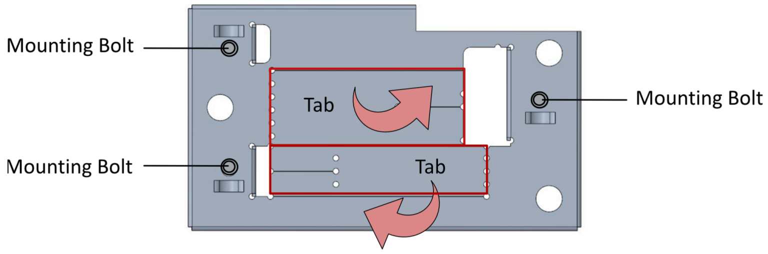
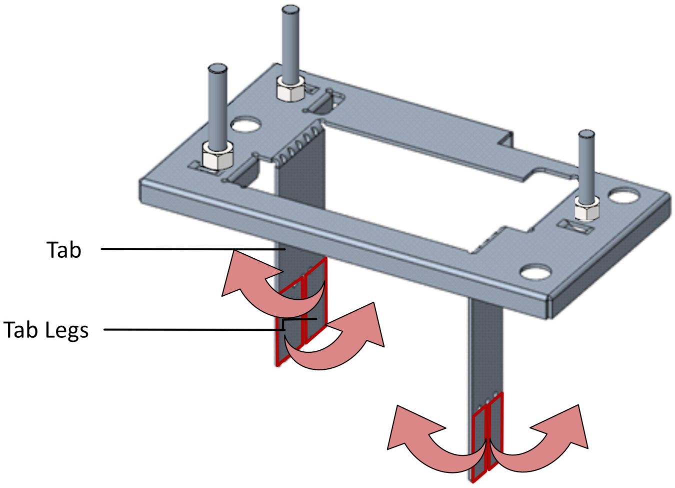


Figure 2-6 Bent Tabs Down

2. Gently bend the tab legs on each tab to an angle of 90° in opposite directions using a pair of pliers.



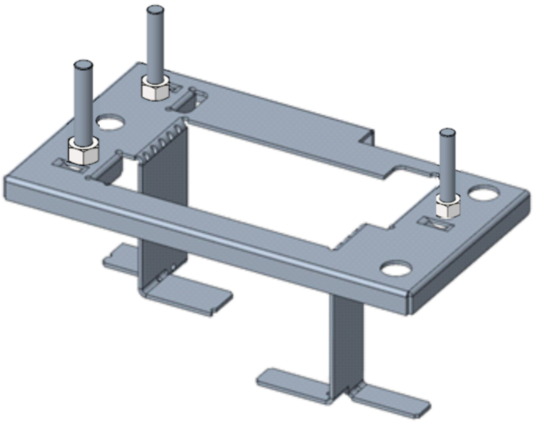


Figure 2-7 Bend Tab Legs Down

3. Place the cabling conduit so it directs the cables to the back of the foundation plate, making sure that 30mm of the conduit sticks out above the concrete.

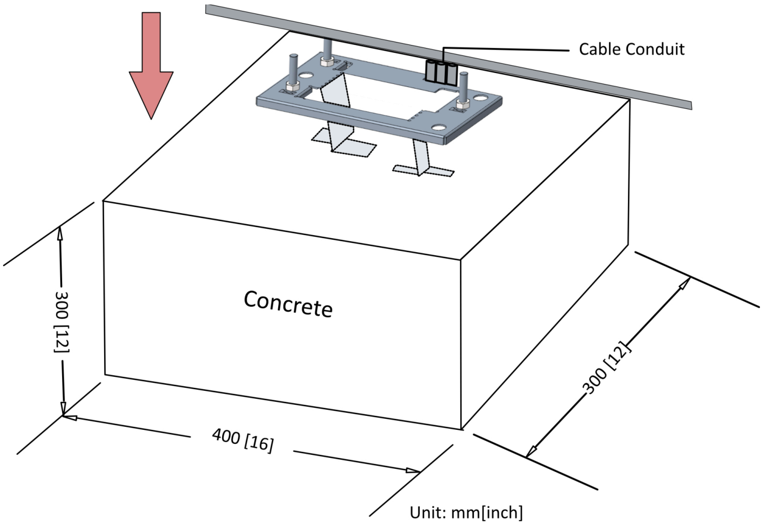


Figure 2-8 Place Cabling

4. Use medium-strength concrete (25MPa) to cast the plinth according to the dimensions.

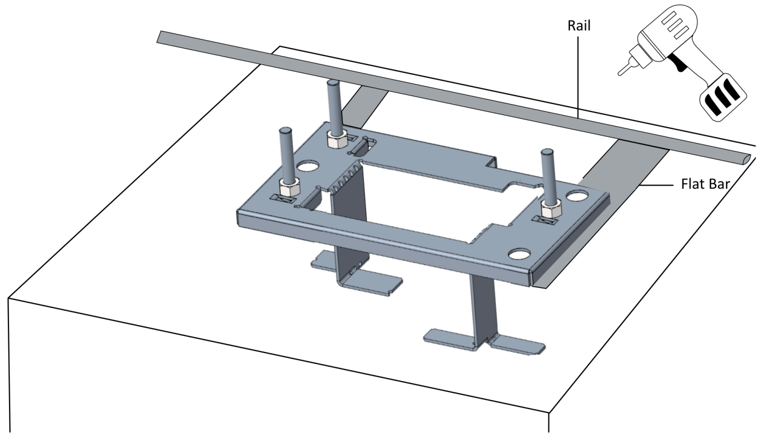


Figure 2-9 Cast Plinth

Exist Concrete Plinth

Before You Start

Before bolting the gate opener to an existing concrete plinth, position the foundation plate accurately and use it to mark the locations for the rawl bolt holes.

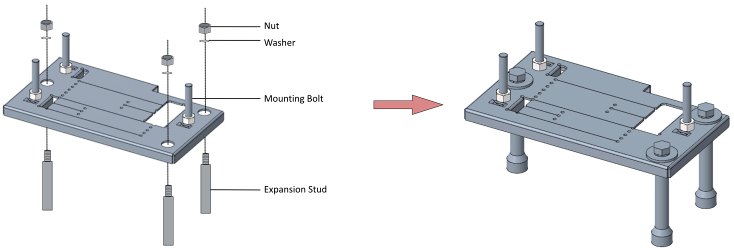


Figure 2-10 Exist Concrete Plinth

Note

- Tightening the M10 half-nuts to 20Nm on the mounting bolts is necessary.
- Rerouting of existing cables may be necessary.

Route Cable

Cast the conduits and route the cables. Ensure that all conduits protrude above the concrete foundation. The mains cables should protrude 360mm above the concrete foundation, while all signal cables should extend 550mm above it.

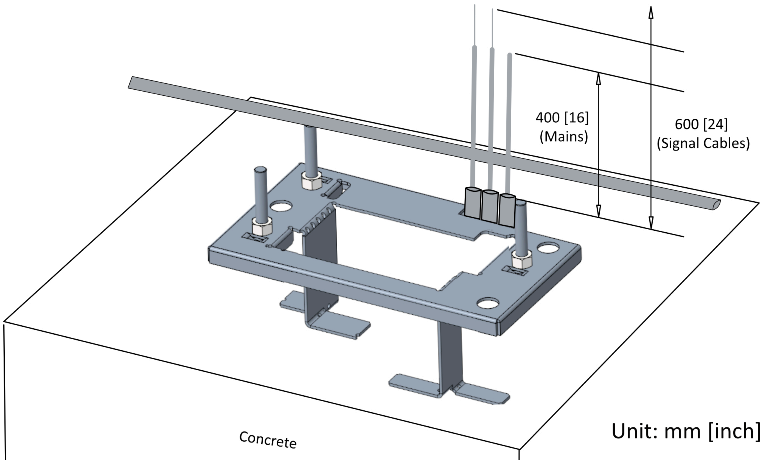


Figure 2-11 Route Cable

2.4 Remove Components

2.4.1 Remove Cover

Before You Start

Note

There is no need to open the release handle to remove the cover.

Steps

1. Insert the operator key into the camlock to unlock the product cover.

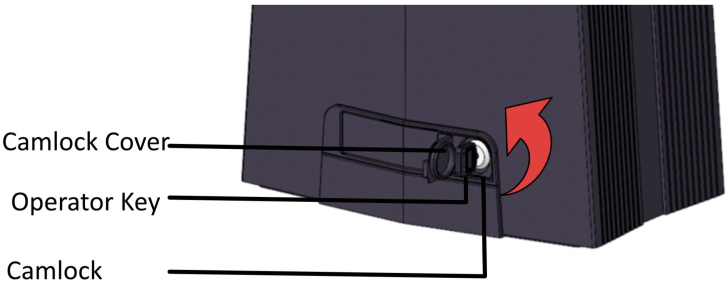


Figure 2-12 Open Camlock

2. Push the side button and at the same time open the camlock cover.

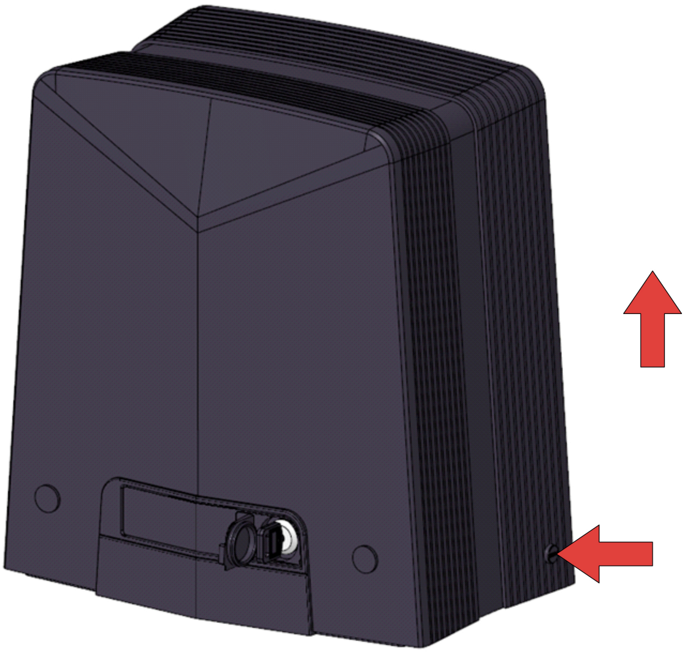
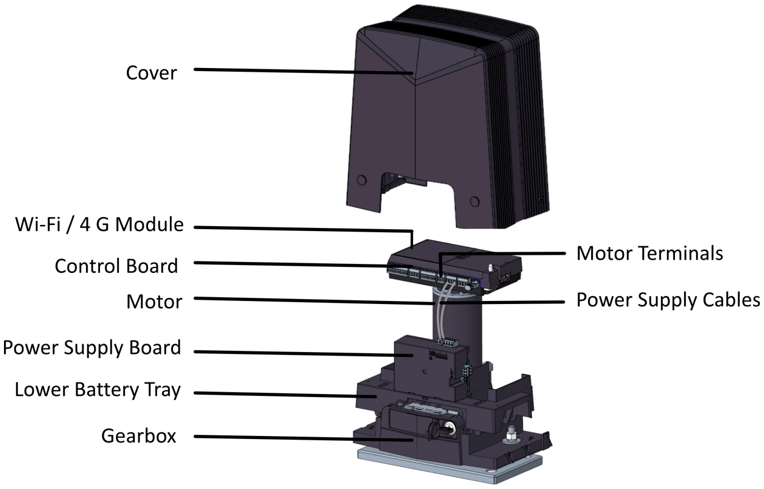


Figure 2-13 Remove Cover

3. Remove the cover of the gate opener to expose the internal components, and place it one side in a safe location.



Note

- By default, the device contains Wi-Fi module. You should remove the Wi-Fi module to replace the 4 G module.
- The device requires 2 batteries to operate; without it, it will not function. You should purchase the batteries separately.

2.4.2 Unplug Battery Cables

Unplug the motor power cables, encoder cables, and power supply cables., and store them in a safe place.

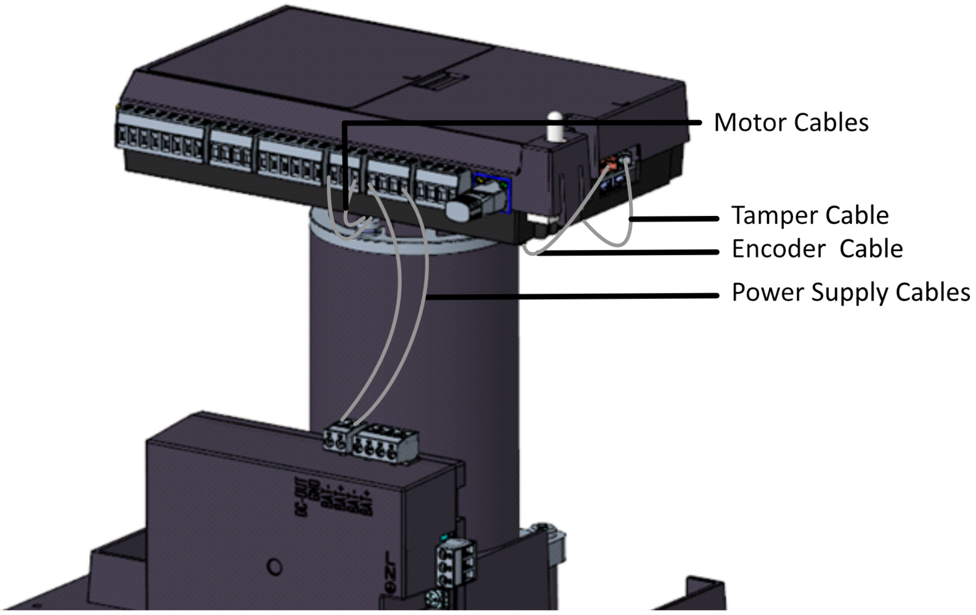


Figure 2-14 Unplug Cables

2.4.3 Remove Control Board

Press down the front side of the board, then pull forward gently to remove the control board; store the control board in a safe place.

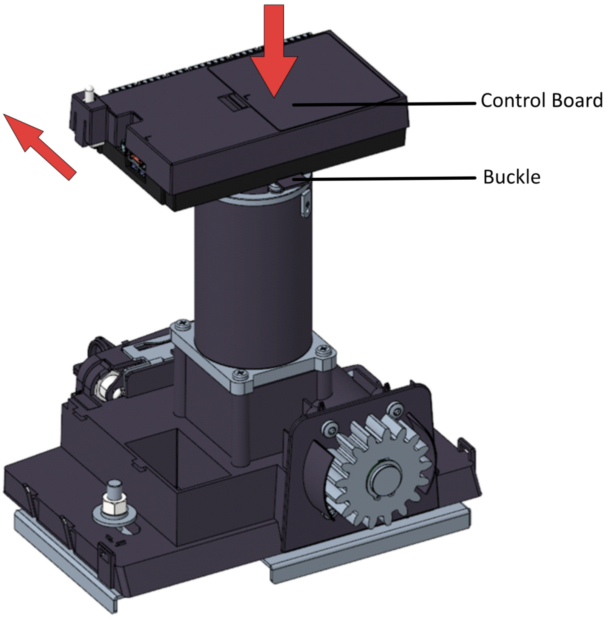


Figure 2-15 Remove Control Board

Note

By tapping the NFC-enabled area, users can automatically connect to the device's Wi-Fi hotspot and access its mobile web interface.

2.4.4 Remove Power Supply Board

Take out the power supply board from the lower battery tray by gently pressing it down as you pull it forward.

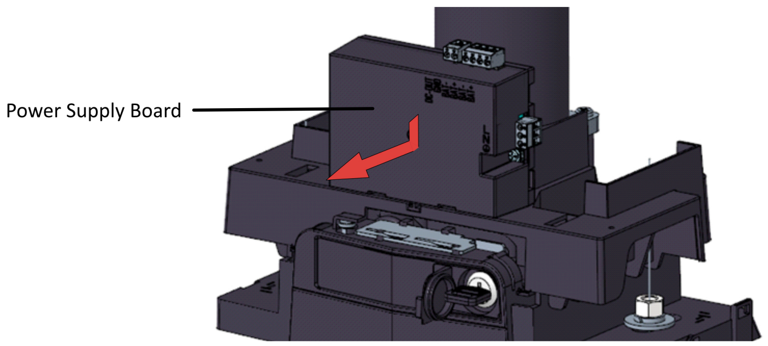


Figure 2-16 Remove Power Supply Board

2.4.5 Remove the Lower Battery Tray

Before You Start

To remove the lower battery tray, make sure the camlock is unlocked. Then, open the release handle until the camlock cam is visible.

Gently press down on the tabs, then pull the lower battery tray forward to remove.

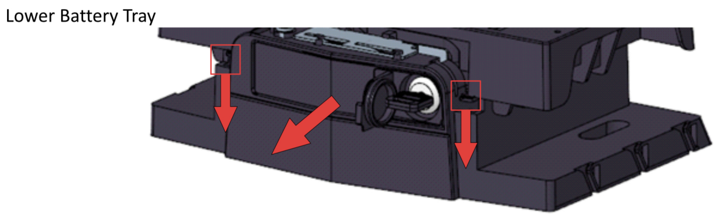


Figure 2-17 Remove the Lower Battery Tray

What to do next

The gate opener is now ready to be mounted onto the foundation plate.

2.5 Manual Override

Steps

1. Turn the key counterclockwise to unlock the camlock; pull the handle fully to the left. The motor will enter a temporary disengaged state.
2. Slide the override cam (located inside the handle) toward the gearbox until a click confirms proper engagement.
3. Return the handle to the closed/locked position to enable manual gate operation while maintaining secure cover lockage.

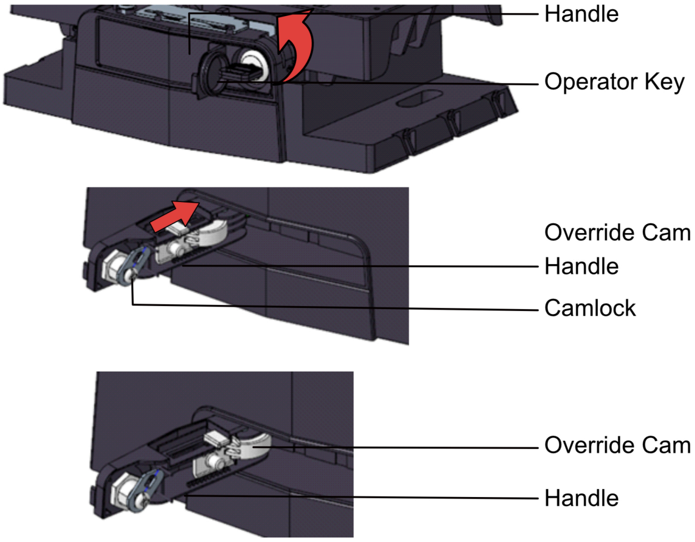


Figure 2-18 Return Handle

What to do next

Note

You can push the override cam to the left ro restore normal operation.

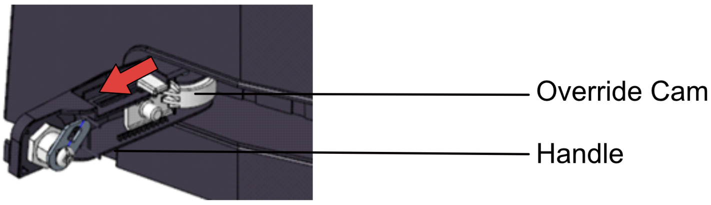


Figure 2-19 Restore Handle

2.6 Mount Gearbox

Note

- Adjust the half-nuts to be 12 mm clear from the foundation plate.
- After securing the foundation plate, it is required to fasten another nut and flat washer on the three studs; otherwise, the cover may crack.

Place the gate opener into position over the three mounting bolts, aligning them with the three slots at the bottom of the gearbox.

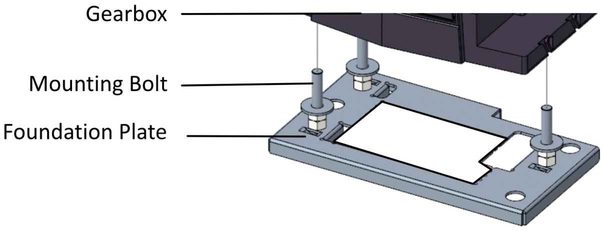


Figure 2-20 Mount Gearbox

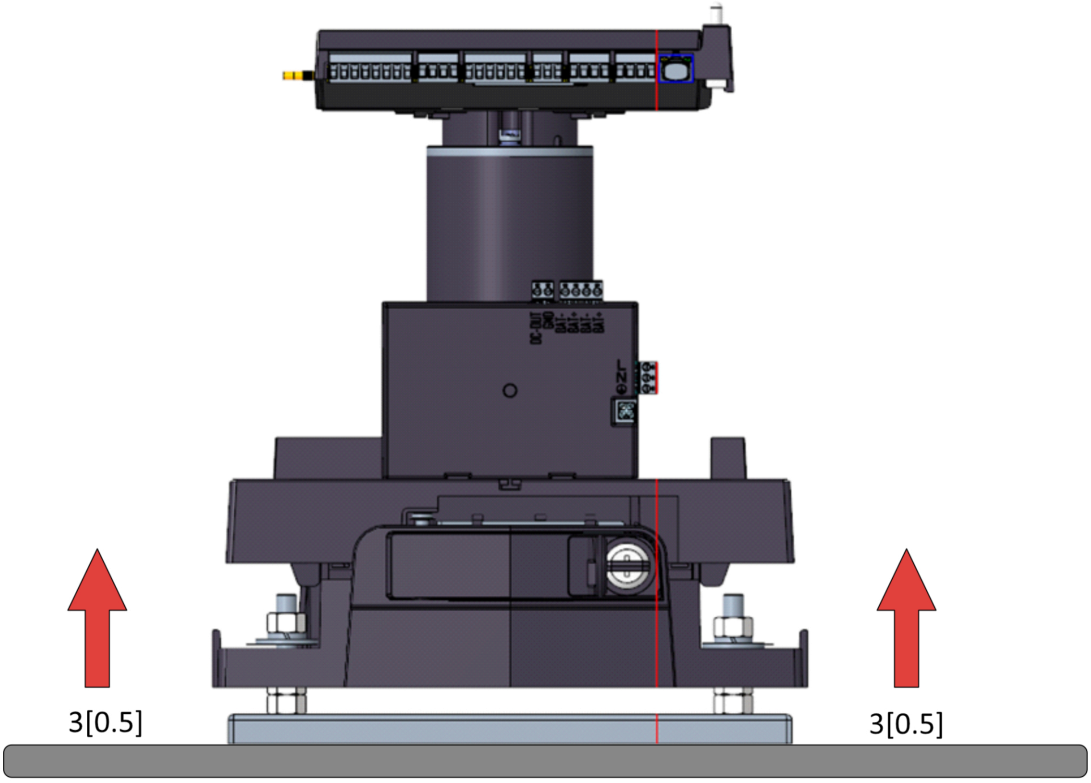
2.7 Adjust Height

Adjust the gate operator height when gate track deviation, abnormal friction, or operational parameter optimization is required.

2.8 Mount Rack

Steps

1. Reserve 3 mm between gate opener and rack to reserve gear clearance space. Verify the gearbox is set to manual override.



Unit: mm[inch]

Figure 2-21 Reserve Gear Clearance Space

2. Position the gate at mid-span of the first rail section, level the free end ensuring rack-pinion contact without downward force; repeat until all sections are secured.
3. Test gate movement along each unfixed rack section to confirm natural rack-pinion engagement and zero compressive loading.

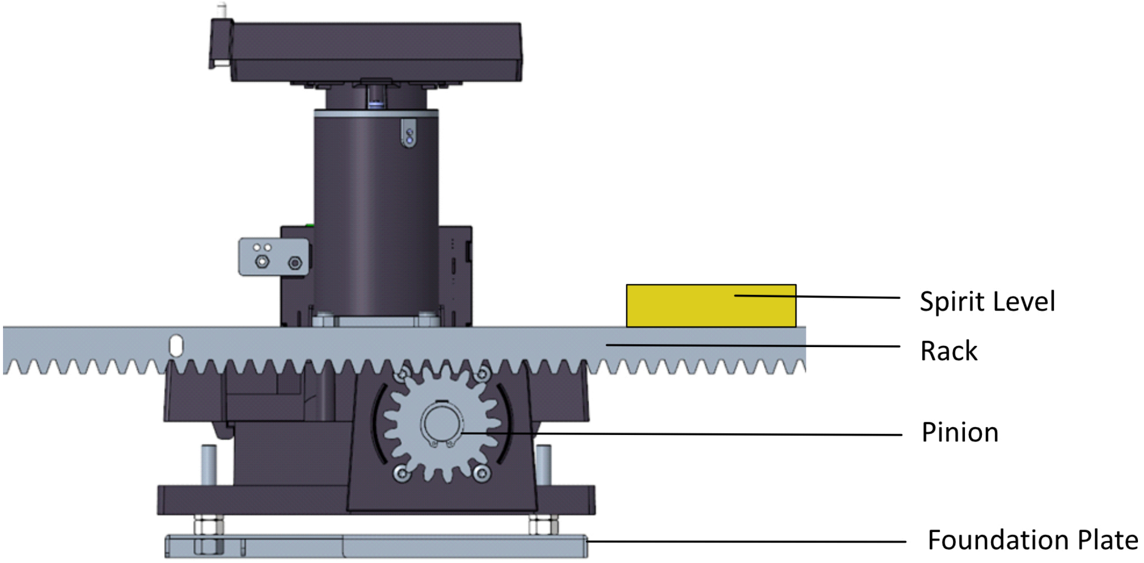


Figure 2-22 Test Gate Movement

4. Lower operator 3 mm to attain 3 mm gear clearance.

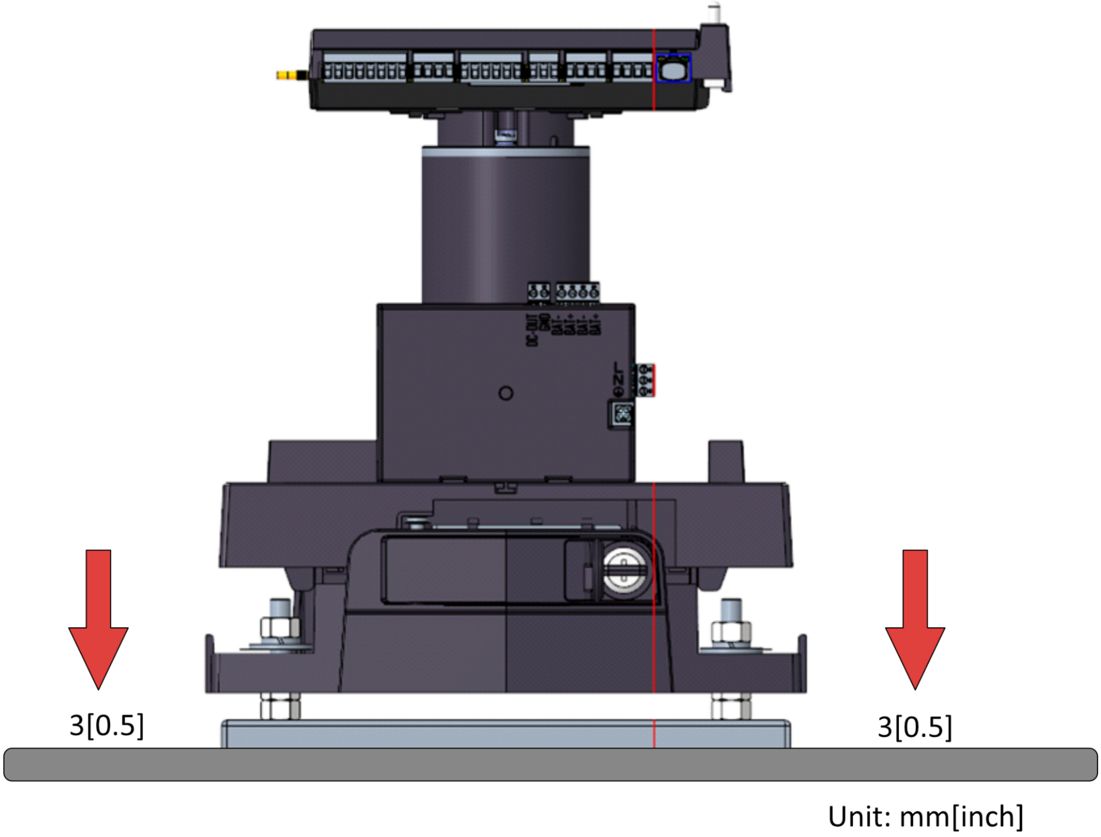


Figure 2-23 Attain 3 mm Gear Clearance

2.9 Restore Components

2.9.1 Restore Control Board

Align the control board with the motor's top interface and slide firmly until an "click" confirms proper engagement.

2.9.2 Restore Power Supply Board

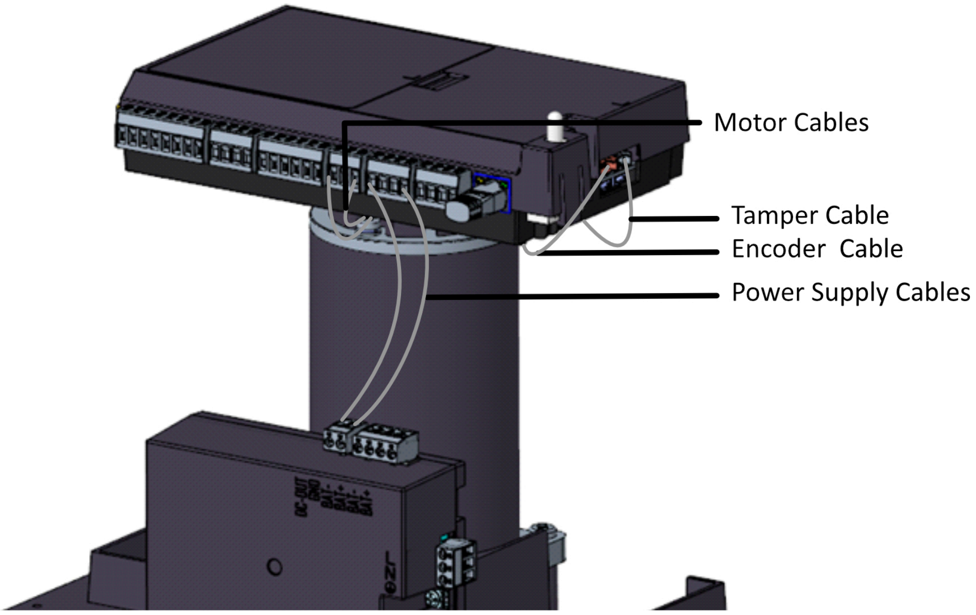
Position the power supply board with the alignment grooves on the lower battery tray, applying even pressure until the retention mechanism snaps into place.

2.9.3 Restore Lower Battery Tray

Align the lower battery tray's alignment grooves horizontally with the motor then gently push until an "click" confirms secure engagement.

2.9.4 Re-Plug Battery Cables

Connect the motor wires and power supply cables to power supply board and control board.



2.10 Fix Gearbox

Before You Start

After the rack has been installed and the operator height is correct, add the spring washers and lock nuts.

Install a spring washer followed by a lock nut on each mounting bolt. Torque all lock nuts with a 17mm socket.

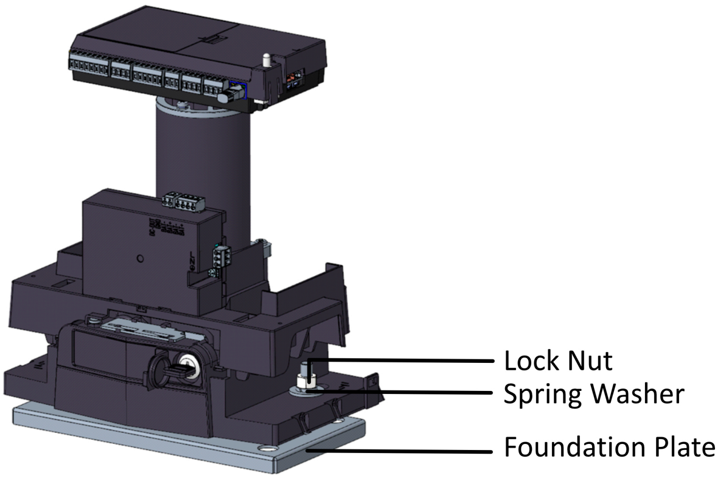
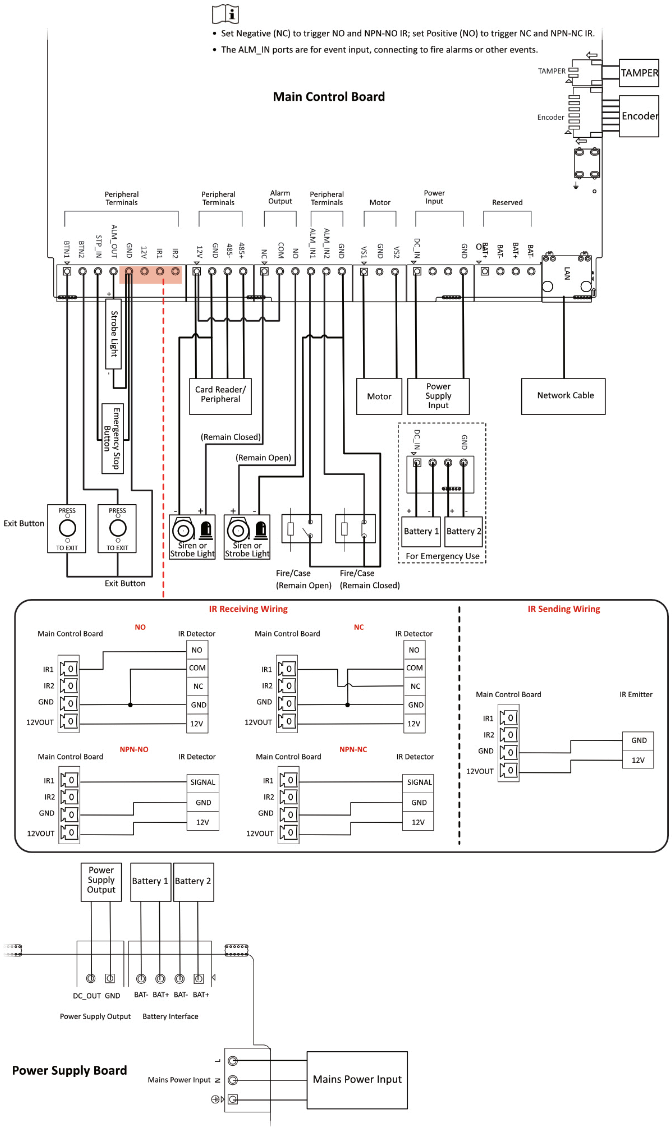


Figure 2-24 Fix Gearbox

2.11 General Wiring

Note

Peripheral wiring must implement reinforced insulation meeting.



- Set Negative (NC) to trigger NO and NPN-NO IR; set Positive (NO) to trigger NC and NPN-NC IR.
- The ALM_IN ports are for event input, connecting to fire alarms or other events.

Figure 2-25 Wiring

2.12 Connect Protective Ground Wire

Grounding via Power Outlet

If there is a power outlet near the installation environment and the grounding pin inside the outlet is properly grounded, grounding can be achieved directly through the PE (Protective Earth) wire of the power cable. Note that the power cable used for the device must be a three-core cable with a protective grounding wire.

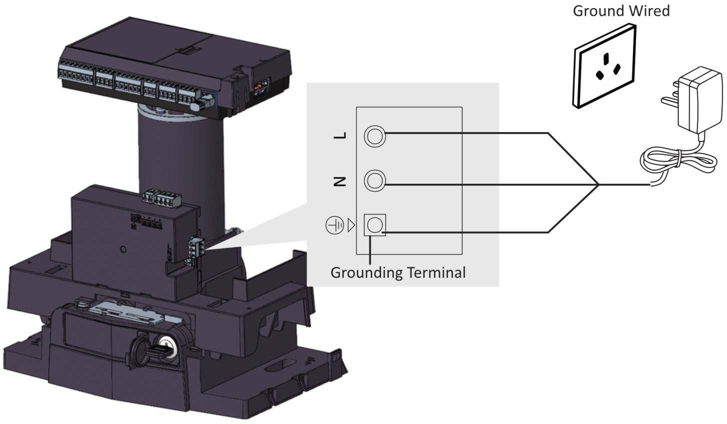


Figure 2-26 Power Cable Grounding Method

Grounding via Buried Grounding Electrode

If there is soil near the installation environment and it is permissible to bury a grounding electrode, follow these steps for grounding installation:

Drive an angle iron (or steel pipe) with a length of no less than 0.5 meters into the ground.

Weld one end of the grounding wire to the angle steel (or steel pipe) and apply anti-corrosion treatment (e.g., electroplating or coating) to the welded area.

Connect the other end of the grounding wire to the protective grounding terminal inside the gate chassis marked with a full-circle protective grounding symbol, and tighten the fixing screw.

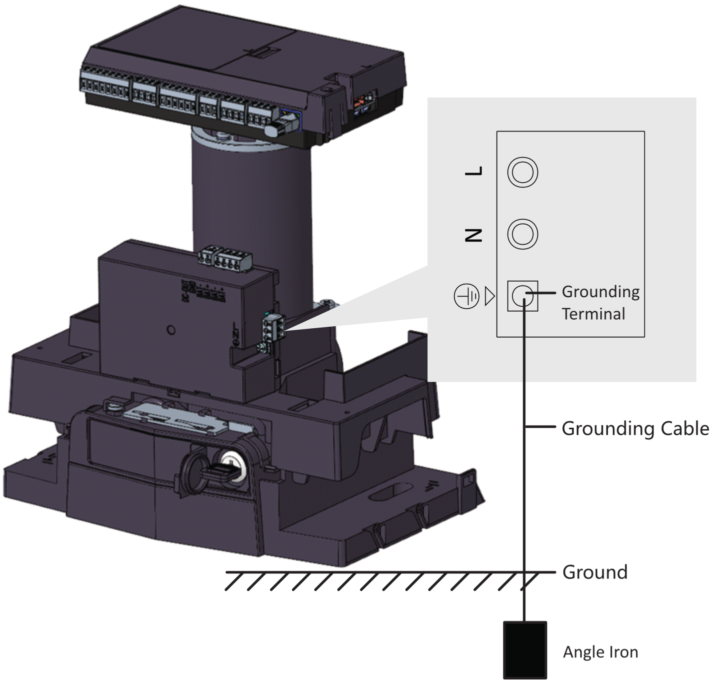


Figure 2-27 Simplified Diagram of Grounding Installation When Buried Grounding Electrode is Permitted Near the Equipment Room

Grounding via Grounding Bar

If there is a grounding bar near the installation environment, connect one end of the grounding wire to the terminal of the engineering grounding bar and the other end to the protective grounding terminal inside the gate chassis marked with a full-circle protective grounding symbol, then tighten the fixing screw.

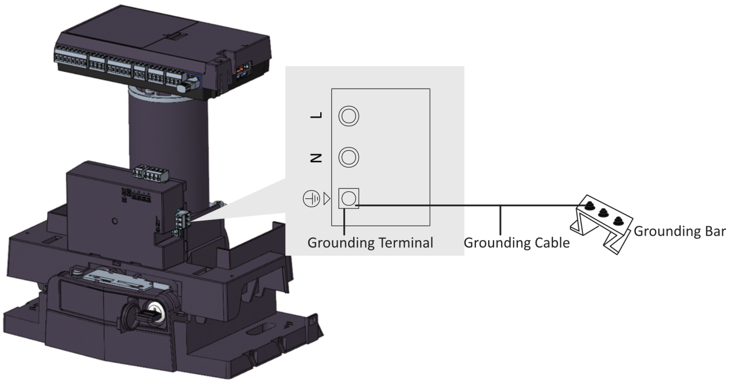


Figure 2-28 Simplified Diagram of Grounding Installation When Grounding Bar is Available in the Equipment Room

Note

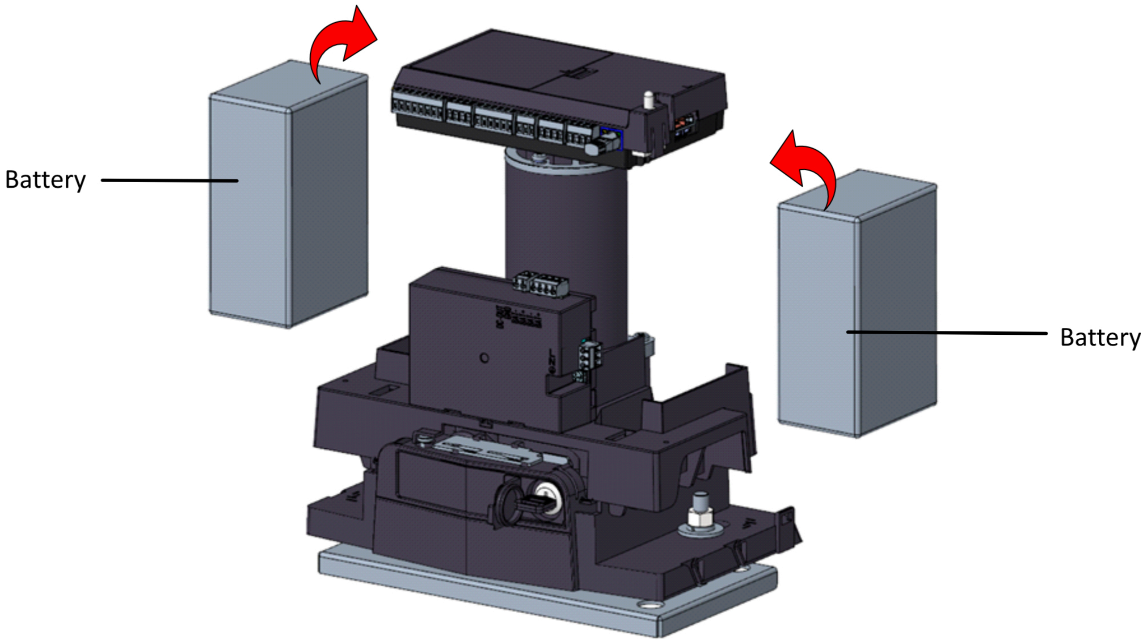
- For all the above grounding methods, the grounding device connected to the product must comply with national standards, and the grounding resistance should not exceed 4Ω.
- The grounding wire and PE wire must use a yellow-green grounding wire of at least 18 AWG.

2.13 Install Battery (Purchased Separately)

Insert battery into slot.

Note

- The device requires 2 batteries to operate; without it, it will not function.
- This battery is inside the device and is charged by the device's power supply. You should purchase 2 batteries (lead-acid battery) that meet the working voltage of 12 V, 7 AH, working temperature of 75°C, and dimension within 66 mm × 49.5 mm × 177.5 mm.



2.14 Install Cover

Steps

1. Place the cover down, aligning it gently onto the motor.
2. Push the override cam to the outside ro restore normal operation. Insert the key into the camlock, lock it by turning the key clockwise, then close the camlock cover.

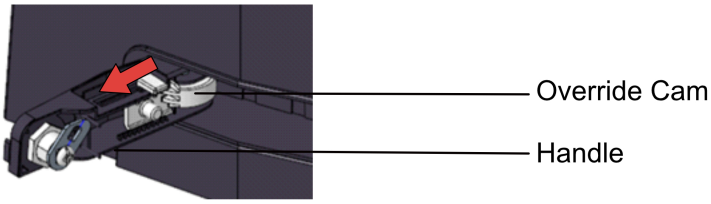


Figure 2-29 Install Cover

Chapter 3 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 IPV4 address: 192.0.0.64
- The default port No.: 80
- The default user name: admin

3.1 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.

3.2 Activate via Mobile Web

You can activate the device via mobile web.

Steps

1. If device hotspot is disabled: Make sure your mobile phone and the device are connected to the same network. Place your phone to the NFC area or scan the device QR code to connect to the hotspotand the device IP address will pop up, tap the address to go to the login page.
2. If device hotspot is enabled:
   - Android System: Place your phone to the NFC area or scan the device QR code to connect to the hotspot and the name and password of the device hotspot will be obtained automatically. Confirm to connect, you will go to the login page.
   - iOS Ssystem: Enable the phone's Wi-Fi function, and connect to the current device's hotspot. After hotspot is connected, you will go to the login page.

   Note

   - Hotspot Name: AP_Serial No.
   - Hotspot Password: Device's Serial No.

   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.
3. Create a 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**.

5. You can configure the turnsile basic parameters, keyfob settings, light settings, network settings, access control settings, etc.

3.3 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.

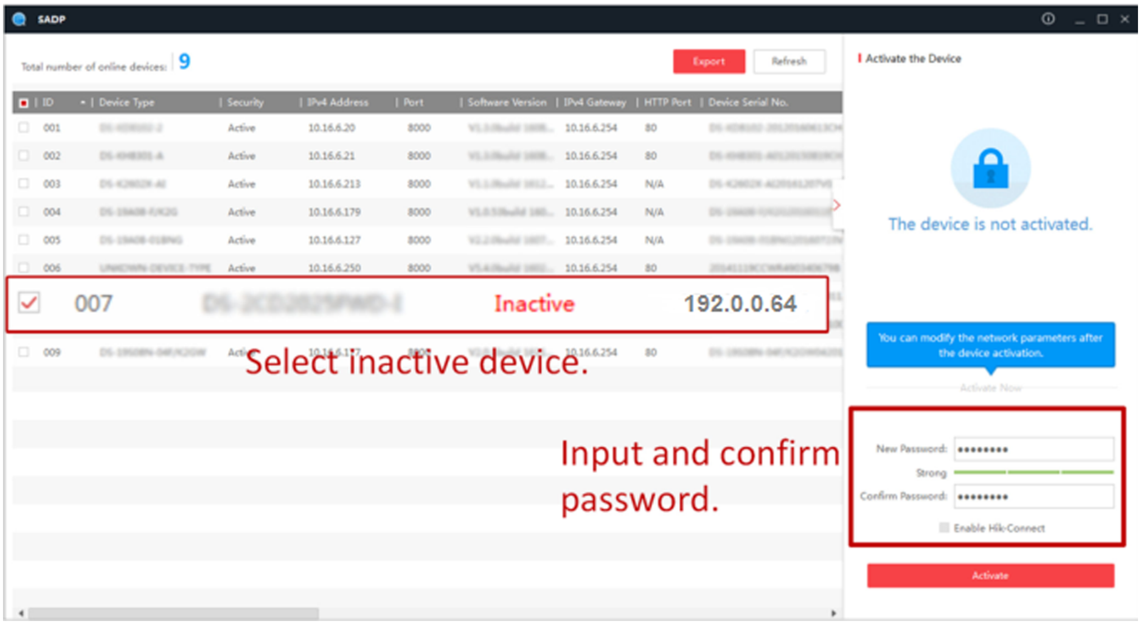
Steps

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.

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



SADP

Total number of online devices: 9

Export | Refresh

■	ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
□	001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
□	002	[illegible]	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
□	003	[illegible]	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
□	004	[illegible]	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
□	005	[illegible]	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
□	006	UNKOWN-DEVICE-TYPE	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑	007	[illegible]	Inactive	192.0.0.64					
□	009	[illegible]	Acti	10.16.6.1[illegible]	80[illegible]	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

Input and confirm password.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

New Password: ••••••••

Strong

Confirm Password: ••••••••

□ Enable Hik-Connect

Activate

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 4 Configure Device via Mobile Web

4.1 Login

You can login via mobile browser.

Note

Make sure the device is activated.

Login via NFC / QR Code

Make sure the device cover is removed (tamper is triggered). In this situation, the device hotspot function is enabled.

-Android System: Switch your phone to **Airplane Mode** and place your phone to the NFC area on the access control board. The login page will pop up.

-iOS System: Switch your phone to **Airplane Mode** and use the browser app to scan the QR code on the access control board. The login page will pop up.

Note

If the browser is not go to the login page directly, you can enter ***http://acsvis.com*** to enter the login page.

Enter the admin password (activation password) to login.

Login via Wi-Fi IP Address

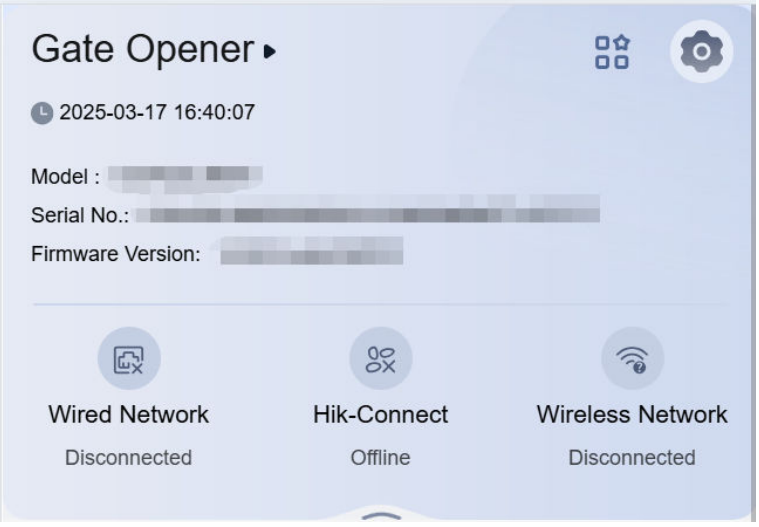
Make sure the device Wi-Fi function is enabled and is linked to a Wi-Fi. Remember the device IP address.

On the phone's browser, enter the IP address to enter the login page.

Enter the admin password (activation password) to login.

4.2 Overview

You can view the device status, conduct remote control, etc.



Gate Opener ▸

2025-03-17 16:40:07

Model : [redacted]

Serial No.: [redacted]

Firmware Version: [redacted]

Figure 4-1 Network Status and Basic Information

You can view network status, model, serial No. and firmware version, and you can tap to fast enter the basic information page.

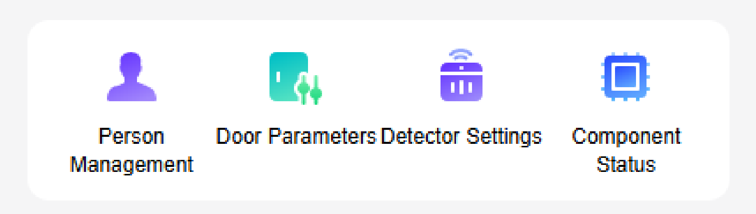


Figure 4-2 Qucik Settings

You can tap to fast enter the basic settings page, person page, and keyfob settings page.

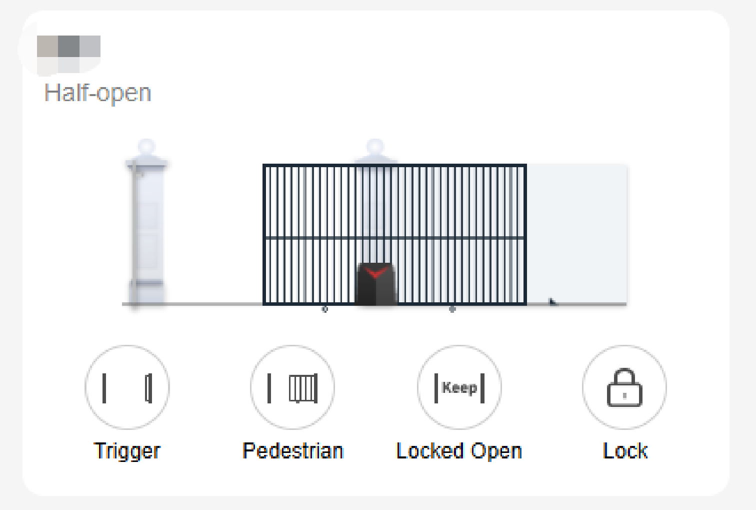
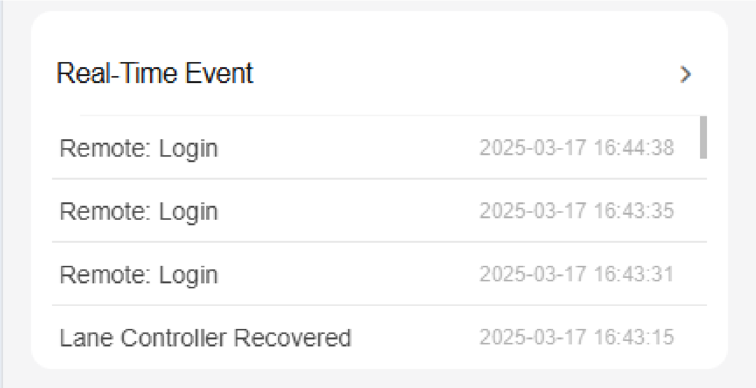


Figure 4-3 Remote Control

You can remotely control gate opener by tap the icons.


Real-Time Event

```
Remote: Login                 2025-03-17 16:44:38
Remote: Login                 2025-03-17 16:43:35
Remote: Login                 2025-03-17 16:43:31
Lane Controller Recovered     2025-03-17 16:43:15
```

Figure 4-4 Real-Time Event

You can tap to view real-time events.

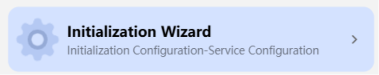
4.3 Configuration

4.3.1 Initialization Wizard

Gate Opening/ Closing Learning

Before You Start

Tap ⚙ → **Initialization Wizard**



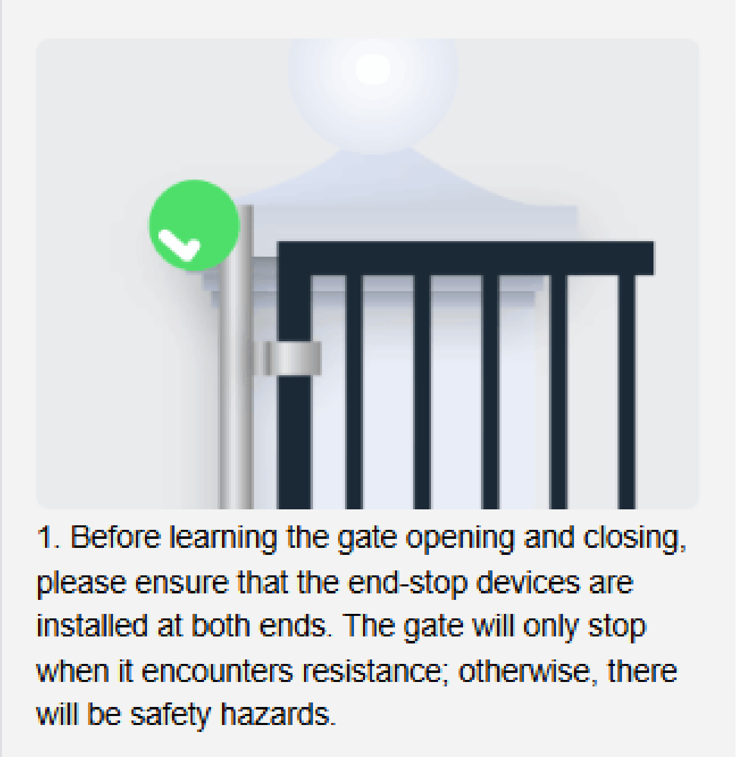
Initialization Wizard

Initialization Configuration-Service Configuration

Figure 4-5 Installation Wizard

Steps

1. Ensure the end-stop devices are installed at both ends. During learning period, the safety configurations such as the linked detectors are unavailable.

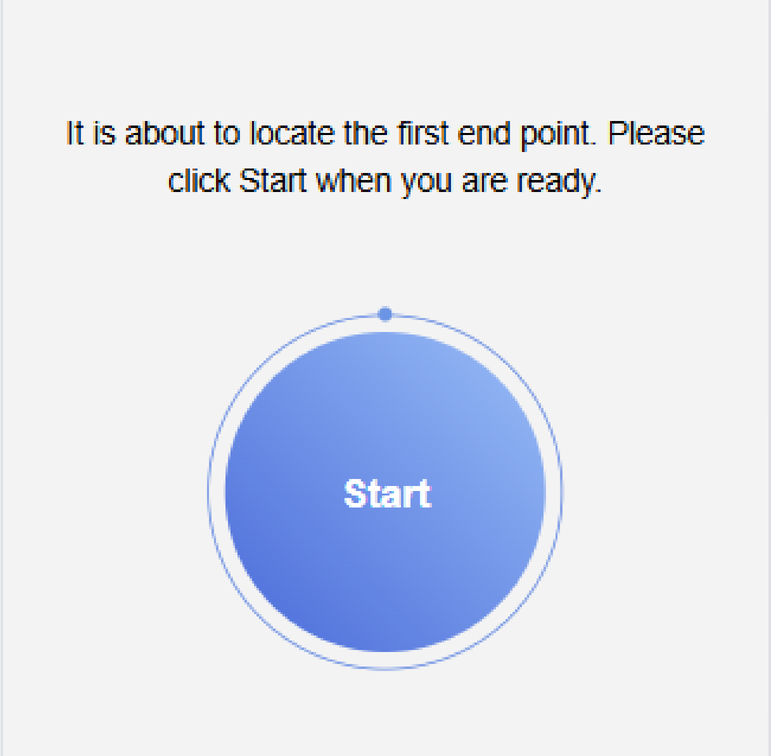


1. Before learning the gate opening and closing, please ensure that the end-stop devices are installed at both ends. The gate will only stop when it encounters resistance; otherwise, there will be safety hazards.

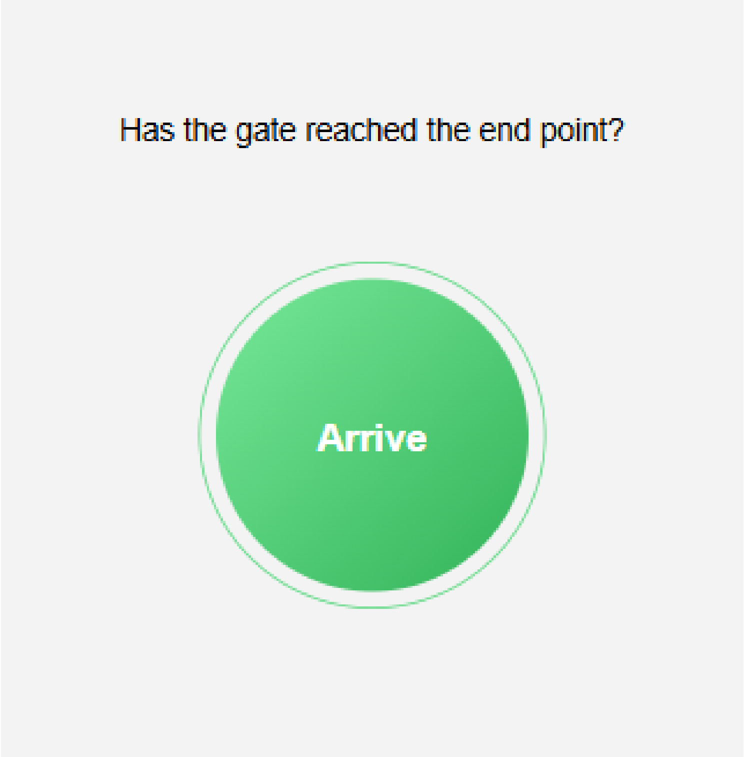
2. During gate opening/closing learning period, the safety configurations such as the linked detectors are unavailable.

Figure 4-6 Safety Confirmation

2. Tap **Start** to locate the first end point. Tap **Arrive** when the gate reaches the end point or tap **Not Reached** to relocate the first end point.



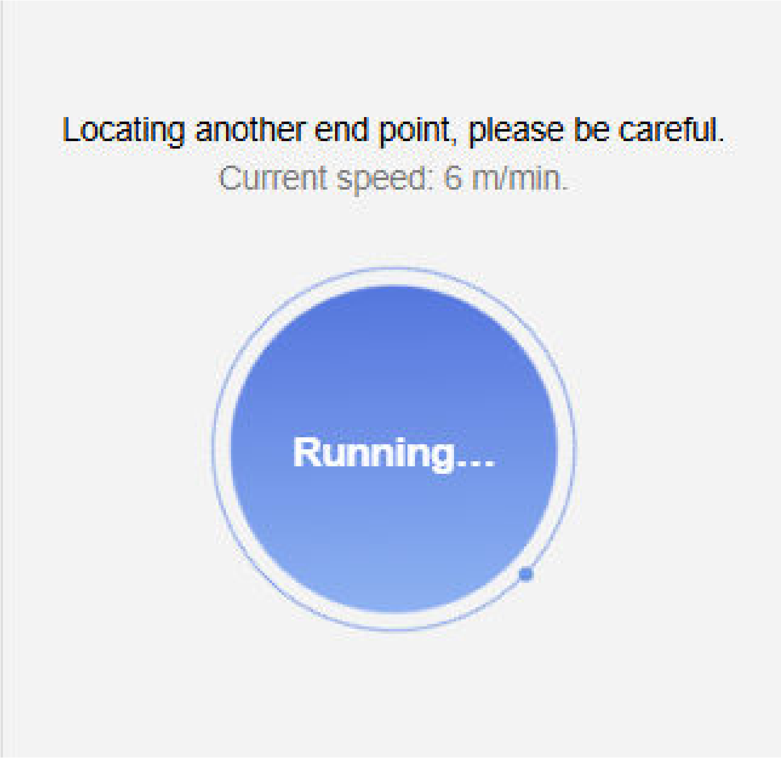
It is about to locate the first end point. Please click Start when you are ready.



Has the gate reached the end point?

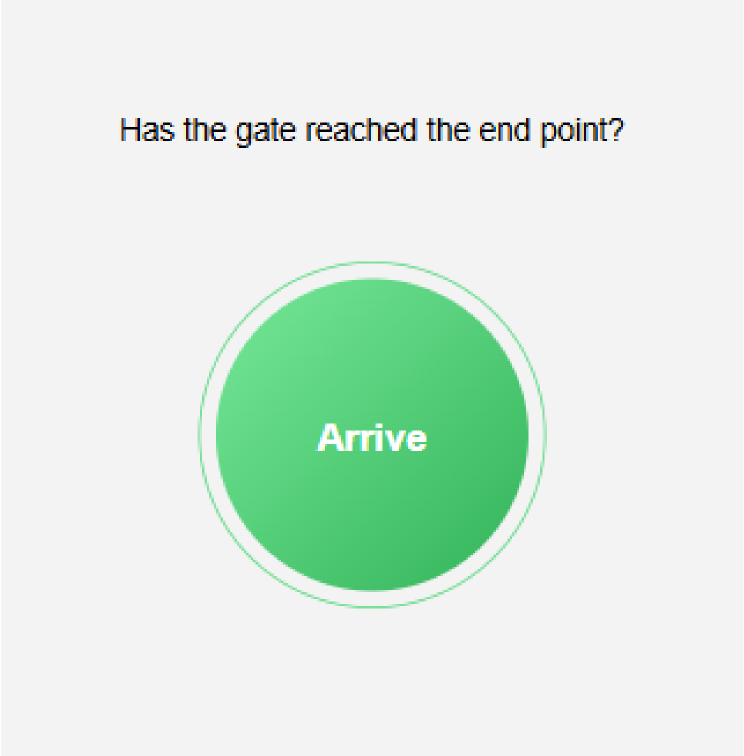
Figure 4-7 Locate the First End Point

3. Locate another end point. Tap **Arrive** when the gate reaches the end point or tap **Not Reached** to relocate the end point.



Locating another end point, please be careful.

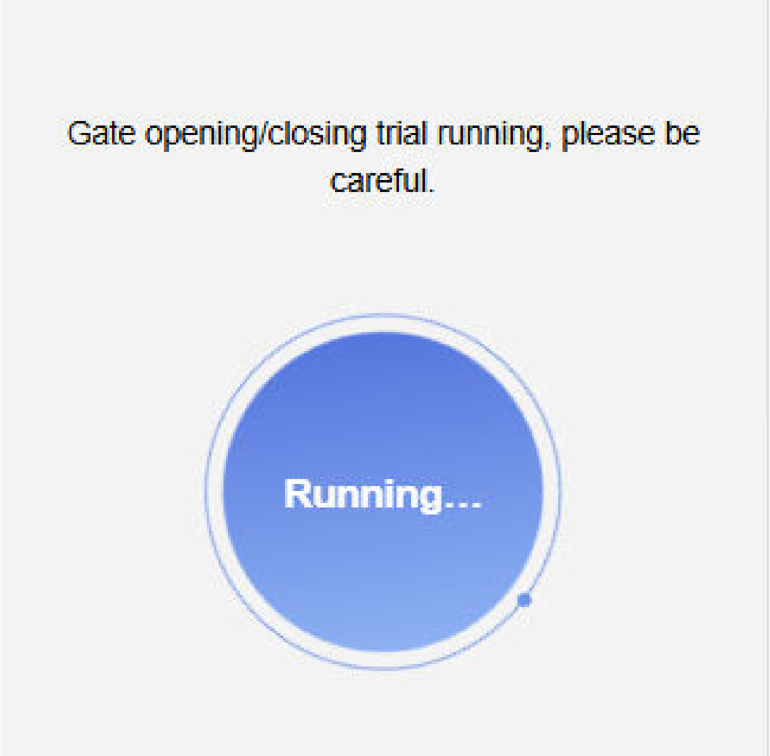
Current speed: 6 m/min.



Has the gate reached the end point?

Figure 4-8 Locate Another End Point

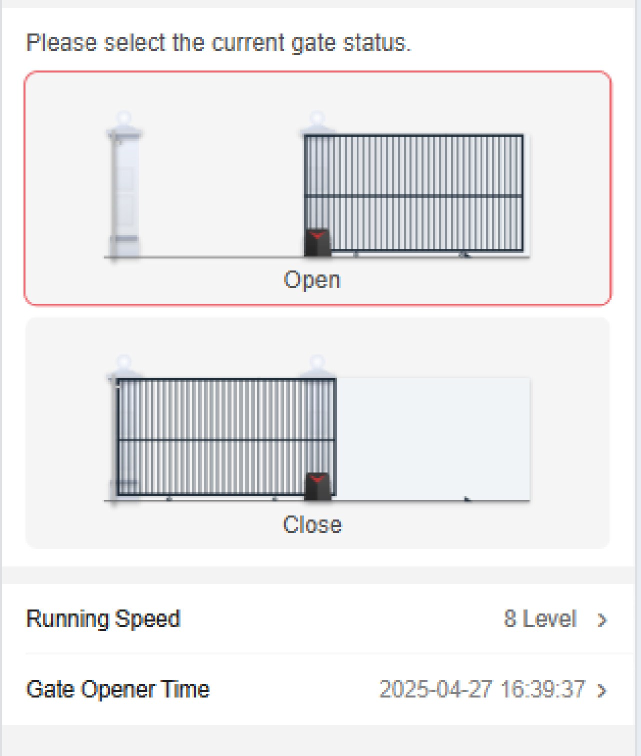
4. Trial run.
]



Gate opening/closing trial running, please be careful.

Figure 4-9 Trial Run

5. Set run configurations such as gate status, running speed, and device time.



Please select the current gate status.

Open

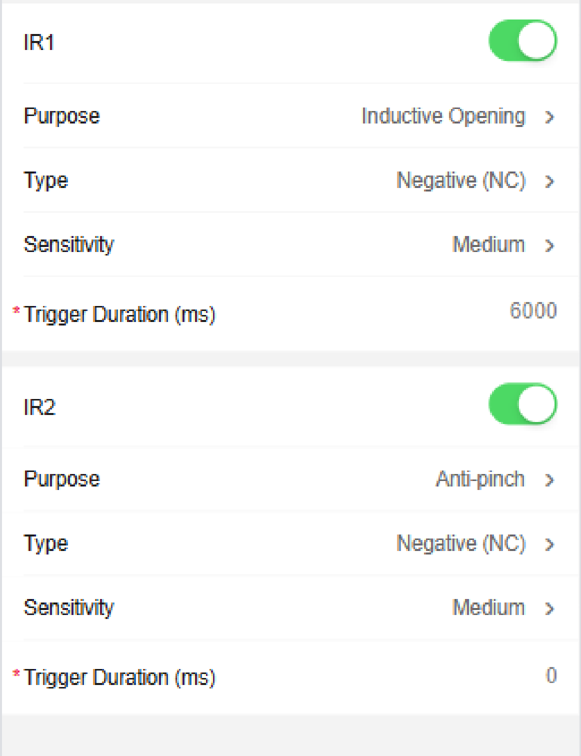
Close

Running Speed 8 Level >

Gate Opener Time 2025-04-27 16:39:37 >

Figure 4-10 Run Configuration

6. Set detector configurations.



IR1

Purpose: Inductive Opening >

Type: Negative (NC) >

Sensitivity: Medium >

*Trigger Duration (ms): 6000

IR2

Purpose: Anti-pinch >

Type: Negative (NC) >

Sensitivity: Medium >

*Trigger Duration (ms): 0

Figure 4-11 Detector Configuration

7. Tap **Next** to save the settings and go to the next parameter. Or tap **Skip** to skip settings.

4.3.2 Gate Opener System Settings

You can view the basic information and set time zone of the device.

View Device Basic Information

You can view the device name, language, model, serial No., version, and Mac address, etc.

Tap ⚙ **→ System Settings → Basic Information** .

You can change the device name.

You can view the device language, model, serial No., version, local RS-485 number, number of alarm input, number of alarm output, Mac address and factory information, etc.

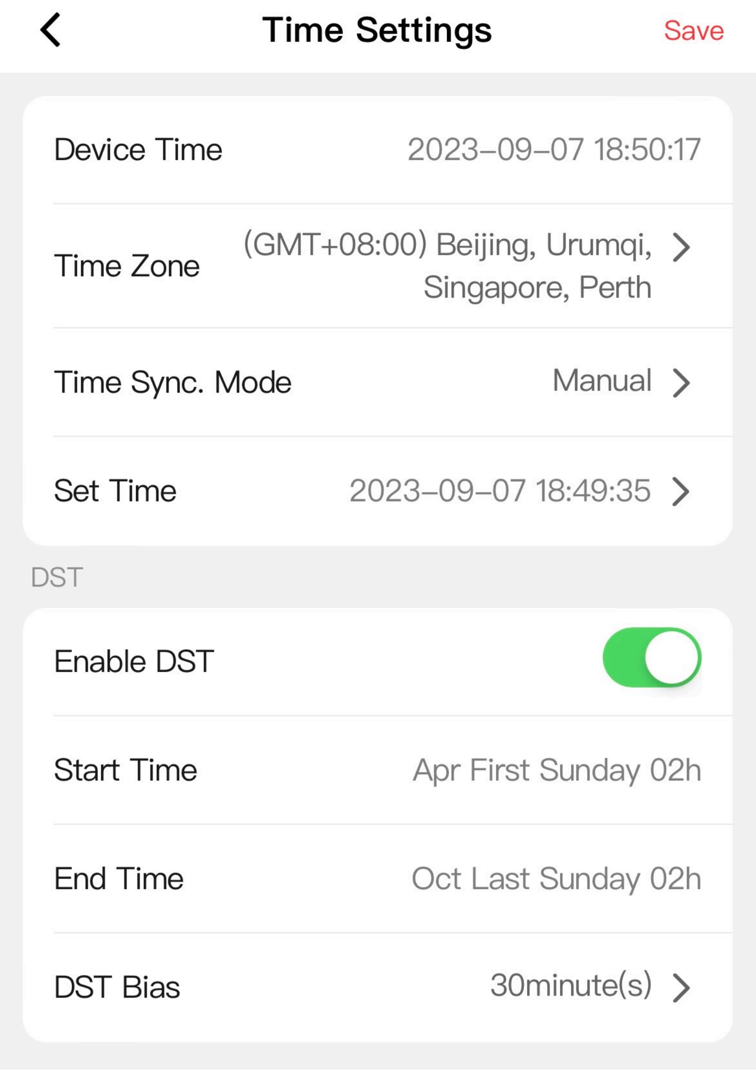
Tap **Device Capacity** to view the quantity and capacity of person, face, card and event.

Tap **Save**.

Time Settings

View current time and set the time zone.

Tap ⚙ → **System Settings** → **Time Settings** .



Time Settings

Save

Device Time 2023–09–07 18:50:17

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth >

Time Sync. Mode Manual >

Set Time 2023–09–07 18:49:35 >

DST

Enable DST

Start Time Apr First Sunday 02h

End Time Oct Last Sunday 02h

DST Bias 30minute(s) >

Figure 4-12 Time Settings

Device Time

You can view current time.

Time Zone

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

Time Sync. Mode

Manual

By default, the device time should be synchronized manually. You can set the device time manually.

NTP

Set the NTP server's IP address, port No., and interval.

DST

Slide to enable DST, and set the start time, end time and DST bias.

Tap **Save**.

4.3.3 User Management

You can change user password.

Tap ⚙ → **User Management** on the home page.

Tap the **Administrator**, enter the old password and create a new password, and confirm the password.

Tap **Save**.

4.3.4 Account Security Settings

Change the reserved phone No. and when you forgot the password, you can use the phone No. to change the login password.

Steps

Note

Only the device and the phone are in the same LAN, can you see the settings.

1. Tap ⚙ → **User Management** → ··· → **Account Security Settings** .
2. Change the reserved phone No. When you forget your login password, you can answer the security questions to change password.
3. Tap **Save**.

4.3.5 Network

You can configure the wired network, Wi-Fi and hotspot parameters of the device.

Wired Network

Set wired network.

Tap ⚙ → **Network Settings → TCP/IP** to enter the configuration page.

NIC Type

Select a NIC type from the drop-down list.

DHCP

If you disable 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.

If you enable the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway automatically.

MAC Address and MTU

You can view the default MAC address and MTU.

IPv6 Mode

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.

Note

Route advertisement mode requires the support from the router that the device is connected to.

Manual

Enter **IPv6 Address**, **IPv6 Subnet Mask**, and **IPv6 Default Gateway**. Consult the network administrator for required information.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

DNS Server

Note

Only when DHCP is enabled can DNS server be set.

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

Set Wi-Fi Settings

Set the Wi-Fi parameters of the device.

Steps

1. On the home page, tap ⚙ → **Networks Settings → Wi-Fi** .
2. Enable **Wi-Fi**.
3. Select a Wi-Fi in the list and enter the password to connect.
4. **Optional:** Add a Wi-Fi.
   1) Slide the page to the end and tap **Add Network**.

2) Enter **Wi-Fi Name**, and select the Wi-Fi’s **Encryption Type**.
3) Tap **OK**.

5. **Optional:** Set WLAN.
   1) Set the connected Wi-Fi’s name, and view the network details.
   2) Tap **WLAN Settings**.
   3) Set the WLAN parameters.

      Enable DHCP

      Enable **DHCP** to **Auto DNS**, the device will allocate the IP and DNS automatically.

      Disable DHCP

      Manually set the IP and DNS server.
   4) Tap **Save**.

Result

After Wi-Fi and WLAN settings, you can enter the WLAN IP address in the mobile browser to login the device.

Set Device Hotspot

After enabling the device hotspot, you can use the mobile phone to connect the hotspot and set.

On the home page, tap ⚙ → **Network Settings → Device Hotspot** .

Slide to **Enable Device Hotspot**, set hotspot’s **Name**, enter password and confirm it. Tap **Save**.

Set Cellular Data Network

Set the mobile data parameters for the device.

Note

If the wi-fi function is enabled, the 3G/4G function cannot be used.

Tap ⚙ → **Networks Settings → Cellular Data Network** .

Enable 3G/4G

If the device supports 3G/4G communication function, you can enable it.

Dialing Mode/Dialing No.

Select the dialing mode as **Manual**. And set the dialing No.

User Name/Password/APN/PIN

If you need, you can set the user name, password, APN, and PIN for mobile number.

Set Port Parameters

You can set the HTTP, HTTPS according to actual needs when accessing the device via network.

Tap ⚙ → **Network Service → HTTP(S)** to enter the setting page.

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.

Set WebSocket(s)

You can set the WebSocket, WebSockets according to actual needs when accessing the device via network.

Tap ⚙ → **Network Service → WebSocket(s)** to enter the setting page.

WebSocket

View the WebSocket for accessing the browser.

WebSockets

View the WebSockets for accessing the browser.

Platform Access

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

Steps

1. Tap ⚙ → **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. Slide to enable the function.
3. You can enable **Custom** to enter the server address.

   Note

   - 6 to 12 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.

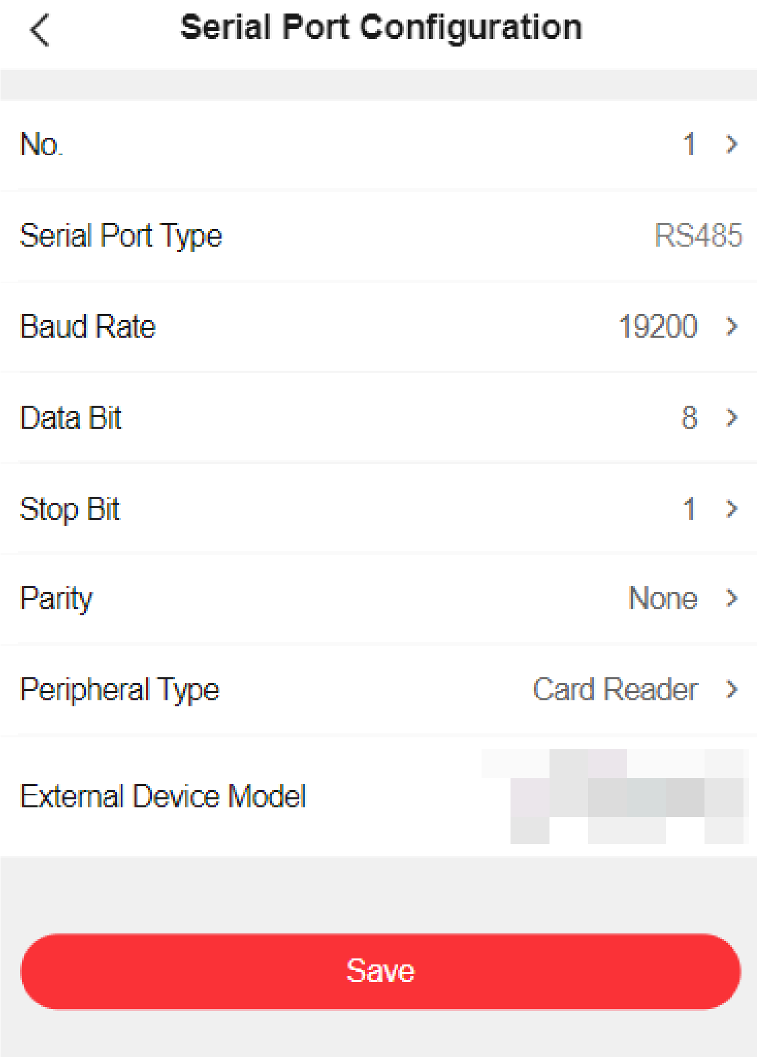
4. You can view **Register Status** and **Binding Status**.
5. You can tap **Bind An Account → View QR Code** , scan the QR code to bind an acount.
6. Tap **Save** to enable the settings.

4.3.6 Serial Port Settings

Set serial port parameters.

Steps

1. Tap ⚙ → **Access Configuration** → **Serial Port Configuration** to enter the setting page.



Serial Port Configuration

No. 1

Serial Port Type RS485

Baud Rate 19200

Data Bit 8

Stop Bit 1

Parity None

Peripheral Type Card Reader

External Device Model

Figure 4-13 Serial Port Configuration

2. Set the serial port position as **Entrance** or **Exit**.
3. Select a serial port No., and the corresponding serial port type will display automatically.
4. Set the serial port parameters.

   Baud Rate

   Configure data transfer rate.

   Data Bit

Configure the number of bits to send data.

Stop Bit

Select the end point for one frame of data.

Parity

Select the serial communication error detection principle. You can choose to detect that the number of 1 of the data bits and check digits is odd or even, or that there is no check digit.

5. Set the **Peripheral Type** the port connected.
6. You can view the external device model.
7. Tap **Save**.

4.3.7 Person Management

You can add the person's information, including the basic information, credentials, authentication and settings.

Add Basic Information

Tap **Person Management** of the shortcut entry or tap ⚙ → **Person Management → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, and person type.
If you select **Visitor** as the person type, you can set the visit times.
Tap **Save** to save the settings.

Manage Keyfob

Tap **Person Management** of the shortcut entry or tap ⚙ → **Person Management → Add** to enter the Add Person page.
Tap **+** and you can add new keyfob. Tap **Delete** to delete the keyfob.

Add Manually

You can enter the keyfob's **Name** and **Serial Number**. Tap **Save**.

Device Pairing

Stand close to the current device, press and hole the button on the bottom left of the keyfob to pair. After pairing completed, the keyfob's serial No. will be added to the device. Tap **Complete**.

Tap added keyfobs to set keyfob names, serial No., and buttons.

Note

Press boutton once to open/close the gate, press twice to pause, press three times to reverse open the gate.

Trigger

The gate is open fully.

Pedestrian

The gate is half-open for pedestrian access.

Locked Open

The gate remains locked and all operations are disabled, requiring remote unlocking to regain control.

Lock

The gate is locked and all operations are disabled, requiring remote unlocking to regain control.

Manage Card

Tap **Person Management** of the shortcut entry or tap ⚙ → **Person Management** → **Add** to enter the Add Person page.
Tap **Card**, enter the **Card No.** and select the **Property**, and tap **Save** to add the card.
Tap **Save** to save the settings.

Set PIN

Tap **Person Management** of the shortcut entry or tap ⚙ → **Person Management** → **Add** to enter the Add Person page.
Set or auto-generate a password of **Configured PIN**.
Click **Save** to save the settings.

Set Permission Time

Tap **Person Management** of the shortcut entry or tap ⚙ → **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.
Tap **Save** to save the settings.

4.3.8 Access Control Settings

Set Door Parameters

You can set door name, open duration, closing mode, etc.

Tap ⚙ → **Access Control** → **Door Parameters** .

Tap **Save** to save the settings.

Door Name

You can create a name for the gate opener.

Barrier Opening/Closing Speed

Set gate opening/closing speed.

Half-open Distance

If you want the half-open the gate, you can set the distance.

Positive Open/Close

If you enable the function, the gate will be heavily open/closed.

Keyfob Receiving Distance

Set the Max. distance that the keyfob can control the gate opener.

Normal

In a spacious environment, keep the keyfob right at the door about 0 to 15 meters.

Long

In a spacious environment, keep the keyfob right at the door about 15 to 200 meters.

Closing Mode

Set the closing mode as **Auto** or **Manual**

Auto

The gate will be closed after the configured **Auto-Close Time**.

Note

In the automatic closing mode, the schedule of opening and closing barrier will not take effect.

Manual

You should use the keyfob or card to manual control the gate.

Authentication Gate Opening Mode

When a person is authenticated by a credential, the gate will be open according to the configured item.

Mechanical Anti-Pinch

Select the appropriate sensitivity level of the anti-pinch function based on the actual scenario.

Exceed Height Limit

Triggered when the height limit is exceeded.

High Profile

High sensitivity, suitable for complex scenarios.

Medium

Medium sensitivity, suitable for general scenarios.

Low

Low sensitivity, suitable for stable environments.

Enable Exit Button 1/2

If the gate opener has connected with exit buttons, you can set the exit button's parameters.

Exit Button Status

You can set the gate's status after press the exit button.

Exit Button Mode

You can set the gate's opening mode when you press the exit button.

Default

Execute the actions of open → pause → close → pause sequentially.

Only Gate Opening Mode

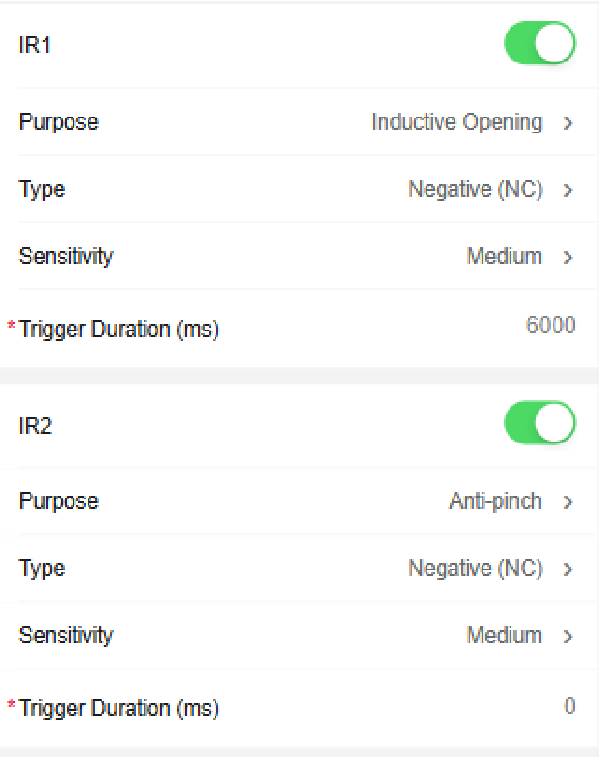
Execute the open action only.

IR Detector Settings

Set the IR detector parameters.

Steps

1. Tap ⚙ → **Access Control** → **Detector Configuration** to enter the configuration page.



IR1 ●

Purpose: Inductive Opening >

Type: Negative (NC) >

Sensitivity: Medium >

*Trigger Duration (ms): 6000

IR2 ●

Purpose: Anti-pinch >

Type: Negative (NC) >

Sensitivity: Medium >

*Trigger Duration (ms): 0

Figure 4-14 Detector Configuration

2. Set the parameters.

Enable Detector

Enable the function and the anti-pinch function or inductive opening function can be used.

Purpose

Anti-Pinch

If you select **Anti-Pinch**, the detector will be used to prevent obstacles or personnel from being pinched.

Inductive Opening

If you select **Inductive Opening**, the detector will be used to open/close the gate.

Anti-Pinch Type

If the **Anti-Pinch** is selected, you should set the anti-pinch type when person is detected to be pinched by the gate.

Barrier Stopped

If the person is pinched by the gate, the gate will be stopped.

Barrier Fully Open

If the person is pinched by the gate, the gate will be fully open.

Type

Set the type of the detector according to the wiring.

Negative (NC)

Normally Closed, triggered when there is no signal.

Positive (NO)

Normally Open, triggered when there is a signal.

Sensitivity

Select the appropriate sensitivity level based on the actual scenario. Low sensitivity means it is not responsive and requires a lot of force to trigger the mechanical anti-pinch mechanism, while high sensitivity corresponds to being very responsive, requiring only a small force to trigger the mechanical anti-pinch mechanism.

Trigger Duration

Set the trigger duration and the anti-pinch or inductive opening function will be triggered within the configured value.

Note

Unit: milliseconds. Value range: 0 to 65535 ms.

3. Tap **Save**.

Set Privacy Parameters via Mobile Web

Set picture uploading and storage parameters.

Tap ⚙ → **Access Control → Privacy Settings** .

Overwriting

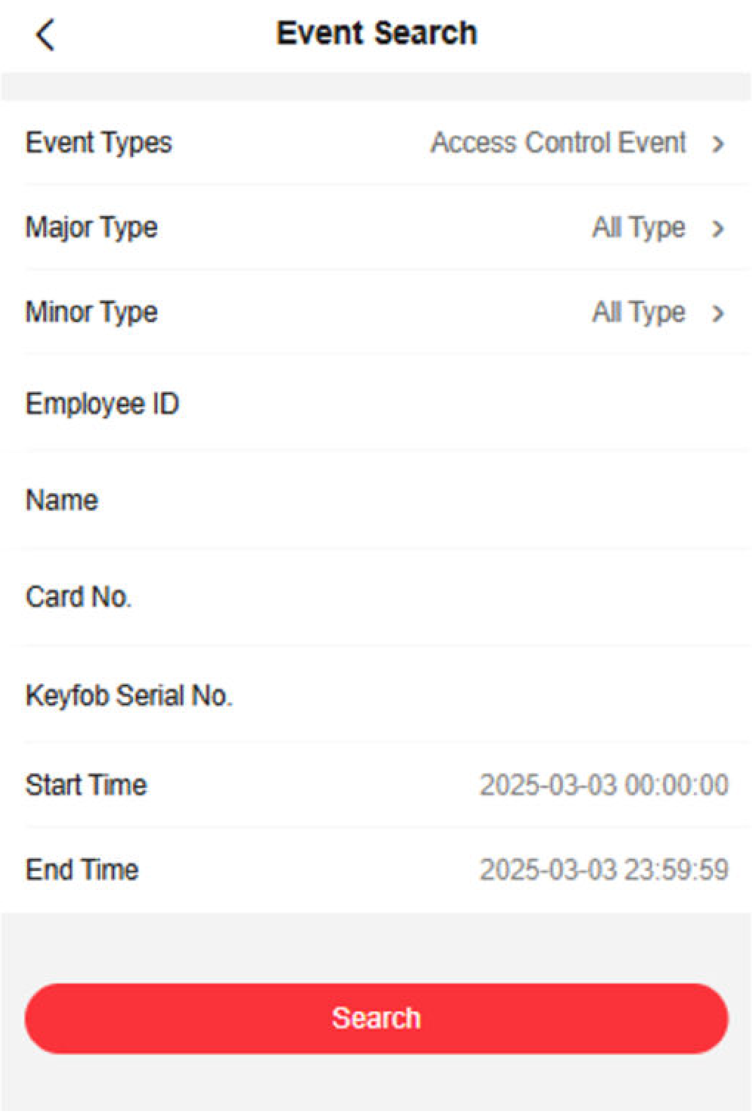
The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

PIN Mode

Set **PIN Mode** as **Device-Set Personal PIN** or **Platform-Applied Personal PIN**.

4.3.9 Event Search

Tap ⚙ → **Event Search** .



Event Search

Event Types: Access Control Event >

Major Type: All Type >

Minor Type: All Type >

Employee ID

Name

Card No.

Keyfob Serial No.

Start Time: 2025-03-03 00:00:00

End Time: 2025-03-03 23:59:59

Search

Figure 4-15 Event Search

Enter the search conditions, including the employee ID, the name, the card No., the Keyfob Serial No., the start time, and the end time, and tap **Search**.

Note

Support searching for names within 32 digits.

The result will display in the list.

4.3.10 Upgrade and Maintenance

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

Restart Device

Tap ⚙ → **Maintenance** → **Restart** .
Tap **Restart** to restart the device.

Upgrade

Tap ⚙ → **Maintenance** → **Upgrade** .
Tap **Upgrade** to upgrade the device.

Note

Do not power off during the upgrading.

Restore Parameters

Tap ⚙ → **Maintenance** → **Default** .

Restore to Default Settings

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

Restore to Factory Settings

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

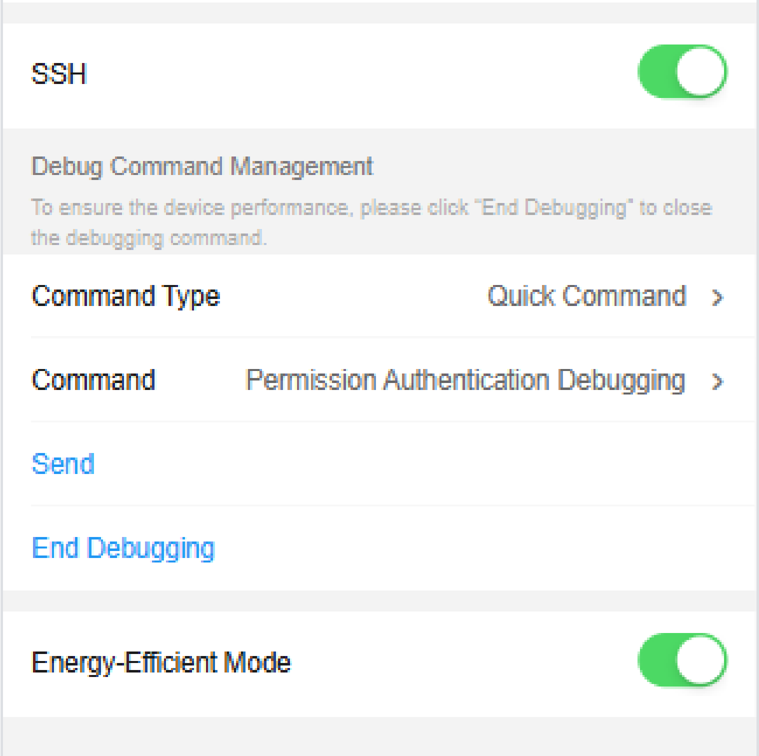
Log Search

Tap ⚙ → **Maintenance** → **Log** .
Set the searching condition, and tap **Search**.

4.3.11 Device Debugging

You can finish studying and self-test, and mange the debugging.

Tap ⚙ → **Maintenance** → **Device Debugging** .



SSH

Debug Command Management

To ensure the device performance, please click "End Debugging" to close the debugging command.

Command Type: Quick Command

Command: Permission Authentication Debugging

Send

End Debugging

Energy-Efficient Mode

Figure 4-16 Device Debugging

Tap **Enable** to enable SSH.

SSH

SSH is used for remote debugging. When you don't need to use this service, it's recommended to disable SSH to improve security.

Debugging Command Management

Select a command type and select the command or tap the command manually. Tap **Send**. The command will send to the device.

When the command is complete, you can see the result in the page.

Tap **End Debugging** to finish the debugging.

Note

If you do not tap End Debugging, the device will end the debugging mode within 7×24 hours automatically.

Energy-Efficient Mode

When enabled, the system directly enters Energy-Efficient Mode when the mains power is off. In Energy-Efficient Mode, unnecessary program will be closed.

4.3.12 Log Export

Tap ⚙ → **Maintenance** → **Device Debugging** → **Log Export** to enter the page.

Select a log type and tap **Export**.

4.3.13 View User Document

View the user document.

Note

Only when you enter the mobile web by IP address, can you view the user document. Login by hot spot does not support the function.

Tap ⚙ to enter the page.

Tap **View Online Document** to view the user manual.

4.3.14 Log Out

Log out the configuration page.

Tap ⚙ → **Logout** , tap **OK**.

If you need to enter the configuration page, you need to enter the user name and password again.

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. Set the security questions before configuration.

Click ◅ in the top right of the web page to enter the **Change Password** page. You can click **Skip** to skip the step. Or select three questions to answer and click **Next**.

5.2 Gate Opening/Closing Learning

Go to learn the gate opening and closing position before using the device.

Read the note on the page and click **Start**.

Follow the step instruction to prepare and click **Start** to start learning.

Note

- Before learning the gate opening and closing, please ensure that the end-stop devices are installed at both ends. The gate will only stop when it encounters resistance; otherwise, there will be safety hazards.
- Before learning the gate opening/closing, ensure that the handle clutch is disengaged and the handle is closed.
- During the gate opening/closing learning period, the linkage detector and other security configurations will not run.

5.3 Detector Settings

Set the 2 detector's parameters to set anti-pinch or inductive opening functions.

Enable Detector

Enable the function and the anti-pinch function or inductive opening function can be used.

Purpose

Anti-Pinch

If you select **Anti-Pinch**, the detector will be used to prevent obstacles or personnel from being pinched.

Inductive Opening

If you select **Inductive Opening**, the detector will be used to open/close the gate.

Anti-Pinch Type

If the **Anti-Pinch** is selected, you should set the anti-pinch type when person is detected to be pinched by the gate.

Barrier Stopped

If the person is pinched by the gate, the gate will be stopped.

Barrier Fully Open

If the person is pinched by the gate, the gate will be fully open.

Type

Set the type of the detector according to the wiring.

Negative (NC)

Normally Closed, triggered when there is no signal.

Positive (NO)

Normally Open, triggered when there is a signal.

Sensitivity

Select the appropriate sensitivity level based on the actual scenario. Low sensitivity means it is not responsive and requires a lot of force to trigger the mechanical anti-pinch mechanism, while high sensitivity corresponds to being very responsive, requiring only a small force to trigger the mechanical anti-pinch mechanism.

Trigger Duration

Set the trigger duration and the anti-pinch or inductive opening function will be triggered within the configured value.

Note

Unit: milliseconds. Value range: 0 to 65535 ms.

Chapter 6 Operation via PC Web

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.

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 Help

6.3.1 Open Source Software Licenses

You can view open source software licenses.

Click ⓘ → **Open Source Software Statement** on the upper-right corner to view the licenses.

6.3.2 View Online Help Document

You can view the help document for Web configuration.

Click ⓘ → **Online Document** on the upper right of the Web page to view the document.

6.3.3 Logout

Log out the account.

Click **admin → Logout → OK** to logout.

6.4 Person Management

You can add the person's information, including the basic information and credentials.

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, gender, and person type.
If you select **Visitor** as the person type, you can set the visit times.

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.

Add Card

Click **Person Management → Add** to enter the Add Person page.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **Save** to add the card.

6.5 Turnstile

6.5.1 Overview

You can view the device component status, real-time event, person information, network status, basic information, and device capacity. You can also control the barrier remotely.

Function Descriptions:

Device Component Status

You can check if the device is working properly. Click **View More** to view the detailed component status.

Remote Control

| | / |▥ / |Keep| / 🔒

The door is fully opened/ half-opened/ locked open/ locked.

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.

Person Information

You can view the added and not added information of person, face, and card.

Network Status

You can view the network connection status.

Basic Information

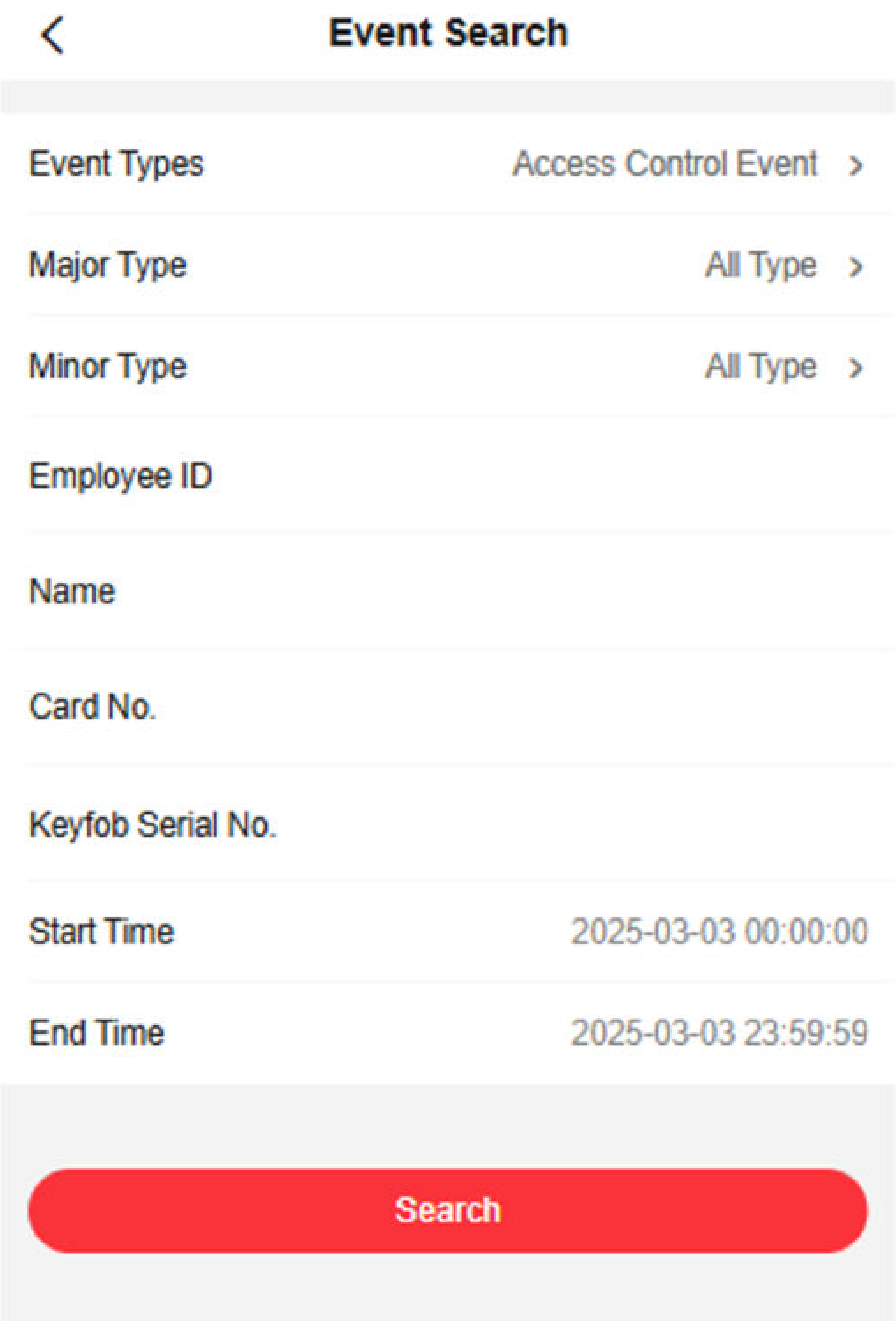
You can view the model, serial No. and firmware version.

Device Capacity

You can view the person, face, card, event capacity.

6.5.2 Search Event

Click **Sliding Gate Opener → Event Search** to enter the page.



Event Search

Event Types	Access Control Event
Major Type	All Type
Minor Type	All Type
Employee ID	
Name	
Card No.	
Keyfob Serial No.	
Start Time	2025-03-03 00:00:00
End Time	2025-03-03 23:59:59

Figure 6-1 Search Event

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

The results will be displayed on the right panel.

6.5.3 Access Control Settings

Set Door Parameters

Click **Sliding Gate Opener → Access Control Parameter → Door Parameters** .

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

Door Name

You can create a name for the gate opener.

Barrier Opening/Closing Speed

Set gate opening/closing speed.

Half-open Distance

If you want the half-open the gate, you can set the distance.

Positive Open/Close

If you enable the function, the gate will be heavily open/closed.

Keyfob Receiving Distance

Set the Max. distance that the keyfob can control the gate opener.

Normal

In a spacious environment, keep the keyfob right at the door about 0 to 15 meters.

Long

In a spacious environment, keep the keyfob right at the door about 15 to 200 meters.

Closing Mode

Set the closing mode as **Auto** or **Manual**

Auto

The gate will be closed after the configured **Auto-Close Time**.

Note

In the automatic closing mode, the schedule of opening and closing barrier will not take effect.

Manual

You should use the keyfob or card to manual control the gate.

Authentication Gate Opening Mode

When a person is authenticated by a credential, the gate will be open according to the configured item.

Mechanical Anti-Pinch

Select the appropriate sensitivity level of the anti-pinch function based on the actual scenario. Low sensitivity means it is not responsive and requires a lot of force to trigger the mechanical anti-pinch mechanism, while high sensitivity corresponds to being very responsive, requiring only a small force to trigger the mechanical anti-pinch mechanism.

Enable Exit Button 1/2

If the gate opener has connected with exit buttons, you can set the exit button's parameters.

Exit Button Status

You can set the gate's status after press the exit button.

Exit Button Mode

You can set the gate's opening mode when you press the exit button.

Default

Execute the actions of open → pause → close → pause sequentially.

Only Gate Opening Mode

Execute the open action only.

Weekly Schedule

You can set the weekly gate opening schedule by drawing time duration on the time table.

Note

If you enable the weekly schedule, the configuration of exit button and keyfob will not take effect.

Holiday Schedule

You can set the holiday gate opening schedule and during the added holiday time duration.

Note

After enabling the holiday schedule, configurations such as the weekly schedule, exit button, and keyfob will not take effect.

Click **Add** and set the holiday name, start date and end date. Select an opening type and draw on the time table.

Set Detector Parameters

Set the 2 detector's parameters to set anti-pinch or inductive opening functions.

Click **Sliding Gate Opener → Access Control Parameters → Detector Configuration** .

Set the parameters and click **Save**.

Enable Detector

Enable the function and the anti-pinch function or inductive opening function can be used.

Purpose

Anti-Pinch

If you select **Anti-Pinch**, the detector will be used to prevent obstacles or personnel from being pinched.

Inductive Opening

If you select **Inductive Opening**, the detector will be used to open/close the gate.

Anti-Pinch Type

If the **Anti-Pinch** is selected, you should set the anti-pinch type when person is detected to be pinched by the gate.

Barrier Stopped

If the person is pinched by the gate, the gate will be stopped.

Barrier Fully Open

If the person is pinched by the gate, the gate will be fully open.

Type

Set the type of the detector according to the wiring.

Negative (NC)

Normally Closed, triggered when there is no signal.

Positive (NO)

Normally Open, triggered when there is a signal.

Sensitivity

Select the appropriate sensitivity level based on the actual scenario.

Exceed Height Limit

Triggered when the height limit is exceeded.

High Profile

High sensitivity, suitable for complex scenarios.

Medium

Medium sensitivity, suitable for general scenarios.

Low

Low sensitivity, suitable for stable environments.

Trigger Duration

Set the trigger duration and the anti-pinch or inductive opening function will be triggered within the configured value.

Note

Unit: milliseconds. Value range: 0 to 65535 ms.

Set Privacy Parameters

Set the event storage type and PIN mode.

Click **Sliding Gate Opener → Access Control Parameters → Privacy Settings** .

Event Storage Settings

Select a method to delete the event. The device supports **Overwriting**.

Overwriting

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

PIN Mode

Set **PIN Mode** as **Device-Set Personal PIN** or **Platform-Applied Personal PIN**.

6.6 System and Maintenance

You can view the system information and the capacity. You can also upgrade the device, restore to factory settings, restore to default settings, and reboot the device.

6.6.1 View Device Information

View the device name, language, model, serial No., version, number of channels, IO input, IO output, 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 view the language, model, serial No., version, IO input, IO output, Local RS-485, alarm input and alarm output number.

You can change **Device Name** and click **Save**.

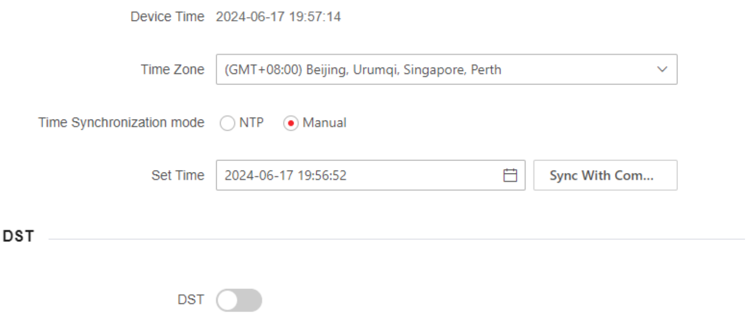
Click **Upgrade** to upgrade the firmware version.

You can view the device capacity, including person, face, card, event, and palm print.

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** .



Device Time 2024-06-17 19:57:14

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Synchronization mode ○ NTP ● Manual

Set Time 2024-06-17 19:56:52

Figure 6-2 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 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.

DST

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

6.6.3 Change Administrator's Password

Steps

1. Enter the password change page.
   - Click **System and Maintenance → System Configuration → System → User Management → User Management** and click ✎ .
   - Click **admin → Modify Password** at the upper right corner of the page.
2. Enter the old password and create a new password.
3. Confirm the new password.
4. 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.

6.6.4 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 according your actual needs.
3. Enter the device password and click **OK** to confirm changing.

6.6.5 Online Users

The information of users logging into the device is shown.

Go to **System and Maintenance → System Configuration → System → User Management → Online User** to view the list of online users.

6.6.6 View Device Arming/Disarming Information via PC Web

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.

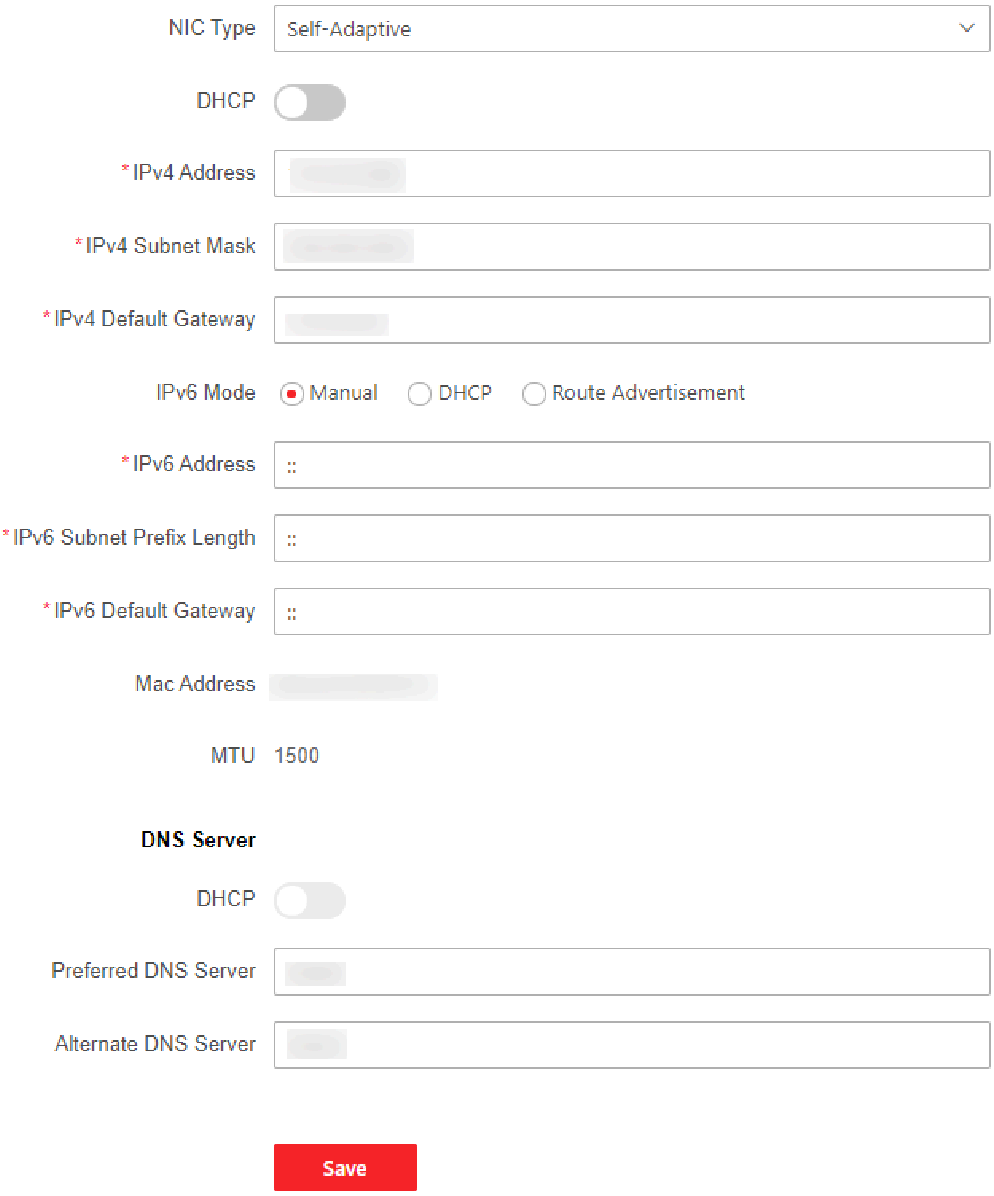
6.6.7 Network Settings

Set Basic Network Parameters

Click **System and Maintenance → System Configuration → System → Network → Network Settings → TCP/IP** .

You can view the mac address and MTU.

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



NIC Type: Self-Adaptive

DHCP

*IPv4 Address: [redacted]

*IPv4 Subnet Mask: [redacted]

*IPv4 Default Gateway: [redacted]

IPv6 Mode: ● Manual ○ DHCP ○ Route Advertisement

*IPv6 Address: ::

*IPv6 Subnet Prefix Length: ::

*IPv6 Default Gateway: ::

Mac Address: [redacted]

MTU: 1500

DNS Server

DHCP

Preferred DNS Server: [redacted]

Alternate DNS Server: [redacted]

Figure 6-3 Set TCP/IP

NIC Type

Select a NIC type from the drop-down list. By default, it is **Auto**.

DHCP

If uncheck the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 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 automatically.

IPv6 Mode

Manual

Set the IPv6 address, IPv6 subnet prefix length and IPv6 default gateway manually.

DHCP

The system will allocate the IPv6 address, IPv6 subnet prefix length and IPv6 default gateway automatically.

Route Advertisement

A mechanism for automatic address configuration in the IPv6 protocol stack. The device can complete IPv6 address configuration as long as there are routers in the environment that can provide routing notification messages.

Click **View Route Advertisement** to view the IPv6 address list.

DNS Server

Note

Only when DHCP is enabled can DNS server be set.

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

Set Wi-Fi Parameters

Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

1. Click **System and Maintenance → System Configuration → Network → Network Settings → Wi-Fi** .
2. Check **Wi-Fi**.
3. Select a Wi-Fi
   - Click 🔗 of a Wi-Fi in the list and enter the Wi-Fi password.
   - Click **Add** and enter a Wi-Fi's name, password, and encryption type. Click **Connect**. When the Wi-Fi is connected, click **OK**.
4. **Optional:** Set the WLAN parameters.
   1) Set the IP address, subnet mask, and default gateway. Or enable **DHCP** and the system will allocate the IP address, subnet mask, and default gateway automatically.
5. Click **Save**.

Set Cellular Data Network

Set the mobile data parameters for the device.

Note

If the wi-fi function is enabled, the 3G/4G function cannot be used.

Click **System and Maintenance → Network → Network Settings → Cellular Data Network** .

Enable 3G/4G

If the device supports 3G/4G communication function, you can enable it.

Dialing Mode/Dialing No.

Select the dialing mode as **Manual**. And set the dialing No.

User Name/Password/APN/PIN

If you need, you can set the user name, password, APN, and PIN for mobile number.

Device Hotspot

Set the device hotspot.

Click **System and Maintenance → System Configuration → Network → Network Settings → Device Hotspot** .

Click to **Enable Device Hotspot**. Set hotspot **Name** and **Password**.

Click **Save**. You can use your phone to connect the hotspot and set parameters on the mobile web.

Set Port via PC Web

Click **System and Maintenance → System Configuration → Network → Network Service** .

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)** .

Platform Access via PC Web

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 the checkbox of **Custom**, and you can set the server address by yourself.
4. Enter the verification code.
5. **Optional:** Check **Enable** to enable video encryption, set an encryption password and confirm it.
6. Click **More** to view the network type and access priority. Drag the operation icon upward or downward to adjust the network priority.
7. Click **View** to view device QR code. Scan the QR code to bind the account.

   Note

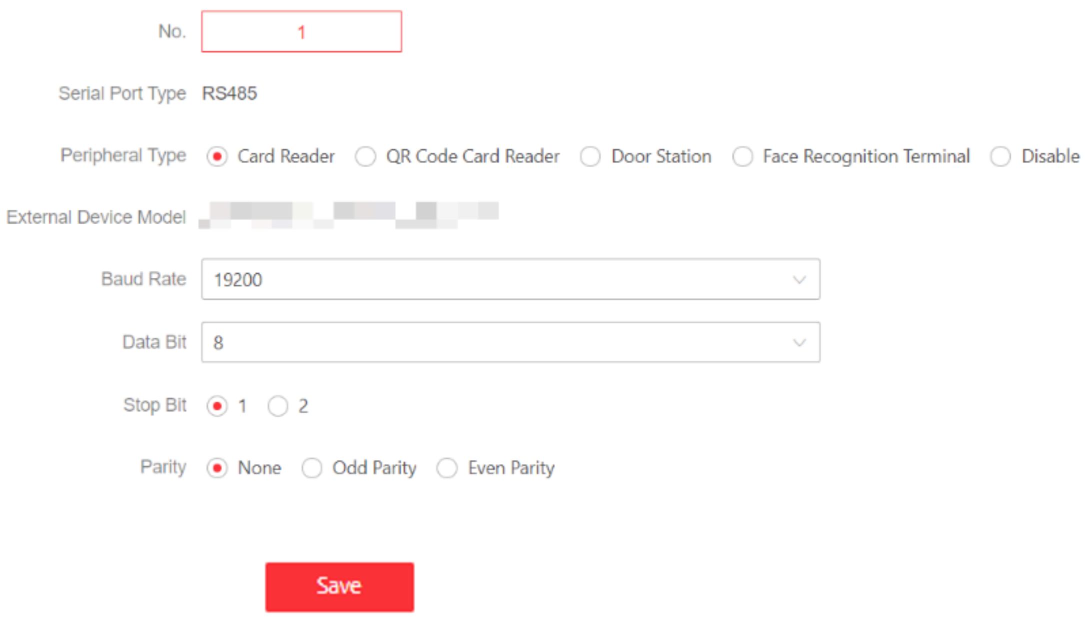
   8 to 32 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.
8. Click **Save** to enable the settings.

6.6.8 Serial Port Settings

Set serial port parameters.

Steps

1. Click **System and Maintenance → System Configuration → Access Configuration → Serial Port Configuration** .



No. 1

Serial Port Type RS485

Peripheral Type ● Card Reader ○ QR Code Card Reader ○ Door Station ○ Face Recognition Terminal ○ Disable

External Device Model [redacted]

Baud Rate 19200

Data Bit 8

Stop Bit ● 1 ○ 2

Parity ● None ○ Odd Parity ○ Even Parity

Figure 6-4 Serial Port Configuration

2. Select a serial port No., and the corresponding serial port type will display automatically.
3. Set the serial port parameters.

   Baud Rate

   Configure data transfer rate.

   Data Bit

   Configure the number of bits to send data.

   Stop Bit

   Select the end point for one frame of data.

   Parity

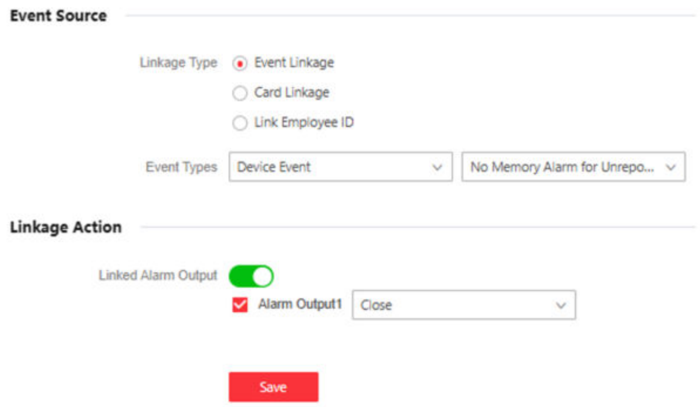
   Select the serial communication error detection principle. You can choose to detect that the number of 1 of the data bits and check digits is odd or even, or that there is no check digit.
4. Set the **Peripheral Type** the port connected.
5. You can view the external device model.
6. Click **Save**.

6.6.9 Event Linkage

Set linked actions for events.

Steps

1. Click **System and Maintenance → System Configuration → Event → Linkage Configuration** to enter the settings page.



Event Source

Linkage Type ● Event Linkage
○ Card Linkage
○ Link Employee ID

Event Types Device Event | No Memory Alarm for Unrepo...

Linkage Action

Linked Alarm Output (on)
☑ Alarm Output1 Close

Figure 6-5 Event Linkage

2. Click **+** to 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 **Employee ID Linkage**, you need to enter the employee ID and select the card reader.
3. Set linkage action.

   Linked Alarm Output

   Enable **Linked Alarm Output**, set the alarm output status for the target event.

6.6.10 Upgrade and Maintenance

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

Reboot Device

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

Upgrade

Click **System and Maintenance → Maintenance → Upgrade** .

Local 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.

Online Upgrade

Check for upgrades.

Note

Do not power off during the upgrading.

Restore Parameters

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

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 network parameters and the user information.

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.

6.6.11 Log Debugging

You can set device debugging parameters.

Steps

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

   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 Capture** to capture.

   Debug Command Management

   Select the command type **Quick Command** or enter the content of **Custom Command**.

Select the board type from the drop-down list, click **Send** to send the debug command, you can view the received command information of the device in **Execution Result**.

Click **End Debugging**, the device restores to normal operation status.

Note

- To ensure the device performance, please click **End Debugging** to close the Debugging command
- If you do not tap **End Debugging**, the device will end the debugging mode within 7×24 hours automatically.

Energy-Efficient Mode

When enabled, the system directly enters Energy-Efficient Mode when the mains power is off. In Energy-Efficient Mode, unnecessary program will be closed.

6.6.12 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**.

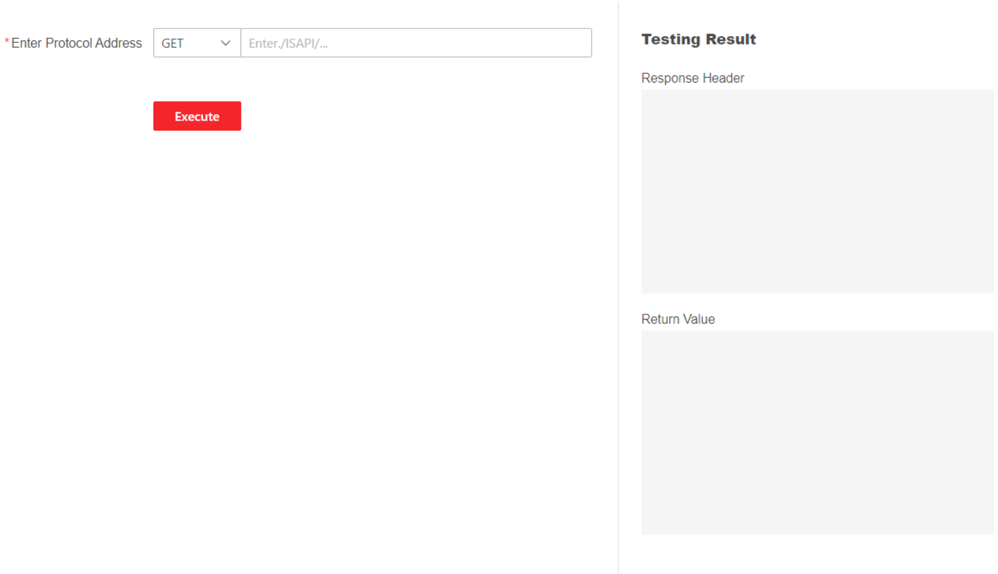


Figure 6-6 Protocol Testing

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

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

6.6.13 Component Status

You can view the status of different components.

You can view main power status, battery status, alarm output status, tamper input status, emergency stop status, keyfob receiving module status, 4G module status, RS-485 card reader status, lane control board status, motor encoder working status, motor encoder online status, detector status, pedestal temperature.

6.6.14 View Log via PC Web

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.

6.6.15 Certificate Management

It helps to manage the HTTPS certificates and SYSLOG certificate.

Note

The function is only supported by certain device models.

Create and Import HTTPS Certificate

Steps

1. Go to **System and Maintenance → Safe → 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 **System and Maintenance → Safe → 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 **System and Maintenance → Safe → 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 iVMS-4200 Client Software or HikCentral Access Control. For details, see the platforms' user manual.

iVMS-4200 Client Software

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

http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247

HikCentral Access Control (HCAC)

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

http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42

See Far, Go Further