Wireless Alarm System

User Manual

Legal Information

About this Manual

The Manual includes descriptions 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (https://www.hikvision.com/).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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 MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
Note	Provides additional information to emphasize or supplement important points of the main text.
Caution	Indicates a potentially hazardous situation, which if not avoided, could result in device damage, data loss, performance degradation, or unexpected results.
Danger	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Descriptions

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- Correctly install and maintain the product. Although the product can help save lives by providing an early warning of a fire, they are not a substitute for an insurance policy. Home owners should have adequate insurance to protect their lives and property.
- Please be sure to disconnect the power supply of the product during wiring, installation and other operations, and do not operate with power on.
- Please strictly follow the installation method in this guide to install the equipment.
- To prevent injury, the device must be securely fastened to the wall as specified in the instructions.
- The gateway is a class A product, which may cause radio interference in a living environment. In this case, the user may be required to take practical measures against the interference.
- Photoelectric smoke alarm can send out audible and visual alarm signals in the event of fire, but cannot extinguish fire. To ensure the normal detection of the alarm, do not use hair spray, insecticide, diluent and other substances that can produce colloidal suspension near the alarm.
- This device is not suitable for use in areas where children may be present.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.

- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- Dispose of used batteries according to the instructions.
- When carrying or using the device, keep the body vertically downward.
- The plug or socket of the gateway is a device for disconnecting the power supply, so please do not cover it for easy plugging and unplugging.
- To prevent fire hazard or electric shock, the product shall be kept from rain or moisture.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- Avoid placing the device in direct sunlight, poorly ventilated locations, near heat sources such as heaters or radiators (ignoring this may result in a fire hazard).
- Please do not use the device in high temperature, low temperature or high humidity environment.
- Do not drop the proudct or subject it to physical shock, and do not expose it to high electromagnetic radiation. Avoid mounting the product in places subject to vibration or shock.
- When the device is connected to the Internet, it may cause network security problems. Please strengthen the protection of personal information and data security. When you find network security risks, please contact us in time.
- Keep the packing so that in case of any problem, pack the product in its original packing and send it to the agent or return it to the factory for disposal.
- If the product does not work properly, contact the dealer or the nearest service center. Never attempt to disassemble the alarm yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

Table of Contents

Chapter 1 Product Introduction

1.1 Introduction

The wireless automatic fire alarm system is suitable for fire detection and security alarm. The system can be combined with smoke/heat detector, audible strobe light, call point, gateway and other wireless peripherals together to form a protection system so as to improve firefighting efficiency. This product can be widely used in dormitories, public rental housing, nursing homes, Taoist temples, temples, markets, buildings, factories and other small and medium-sized situations with concentrated protective areas.

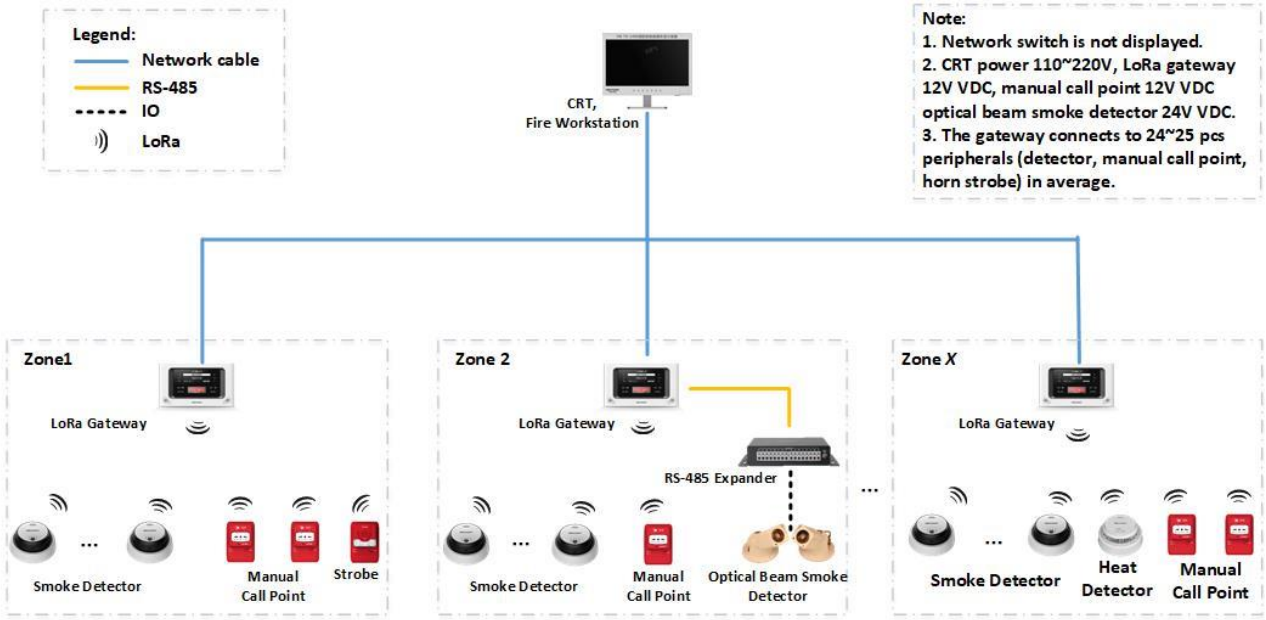


Figure 1-1 System Chart

1.2 Features

1.2.1 Fire Alarm Gateway

- Up to 128 wireless peripherals can be added
- Access to 4 reporting centers
- Supports sending voice or SMS to 6 mobile phone numbers
- Communicates with wireless peripherals through LoRa wireless communication

1.2.2 Smoke/Heat Detector

- Supports smoke/temperature real-time detection and alarm, and supports alarm information upload
- Powered by high-performance lithium battery, it can be used for 3 to 5 years

- Supports self-test function to check whether the components can work properly
- Supports fault alarm function: low voltage alarm, TAMPER alarm, pollution alarm and sensor fault alarm

1.2.3 Audible Strobe Light/Call Point

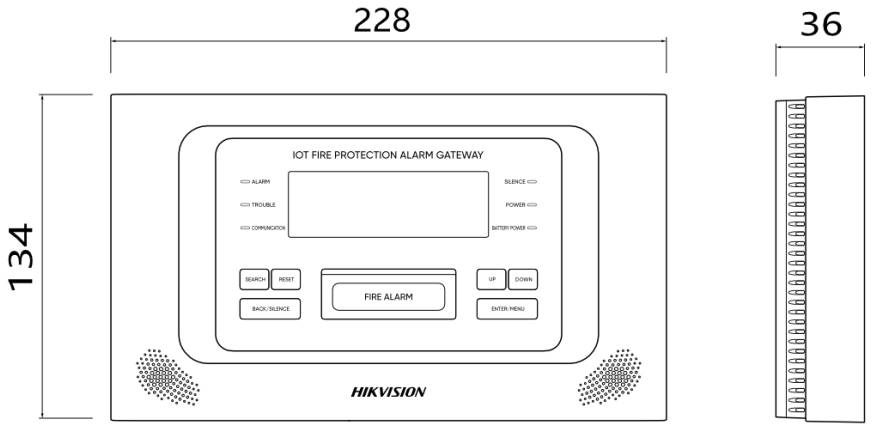
- Supports alarm audible strobe light linkage; call point supports manual alarm and recovery by key
- Supports low battery alarm, TAMPER alarm, and abnormal communication detection
- Supports signal strength query, easy to deploy and install
- Lithium battery power supply, long life, and the theoretical design life of the battery is more than 5 years

Chapter 2 Appearance

Note

The product pictures in this manual are schematic diagrams. Please refer to the actual device.

2.1 Gateway Appearance



Unit: mm

Figure 2-1 Dimension Figure of Gateway

Table 2-1 Button Description

Button	Description
RESET	When an alarm is triggered, press it to return to the standby state.
SEARCH	Quickly search alarm, faults and other information.
SILENCE	When an alarm is triggered, press it to mute.
FIRE ALARM	Manually trigger an alarm.

Table 2-2 Prompt Description

Prompt	**Description**
The buzzer	Key tone, alarm or system fault.
Voice prompt	Voice broadcast.

Table 2-3 Indicator Decription

Indicator	**State**	**Description**
ALARM	On	There is a fire alarm or in a fire alarm state.
	Off	No fire alarm.
TROUBLE	On	Device fault.
	Off	No fault.
COMMUNICATION	On	The device is communicating.
	Off	Communication is not connected.
SILENCE	On	The device is muted.
	Off	Device is not muted.
POWER	On	The device is powered by the main power.
	Off	The main power is not connected or not supplied.
BATTERY POWER	On	The device is powered by backup power.
	Off	Backup power is not connected or does not supply power.

2.2 Smoke/Heat Detector Appearence

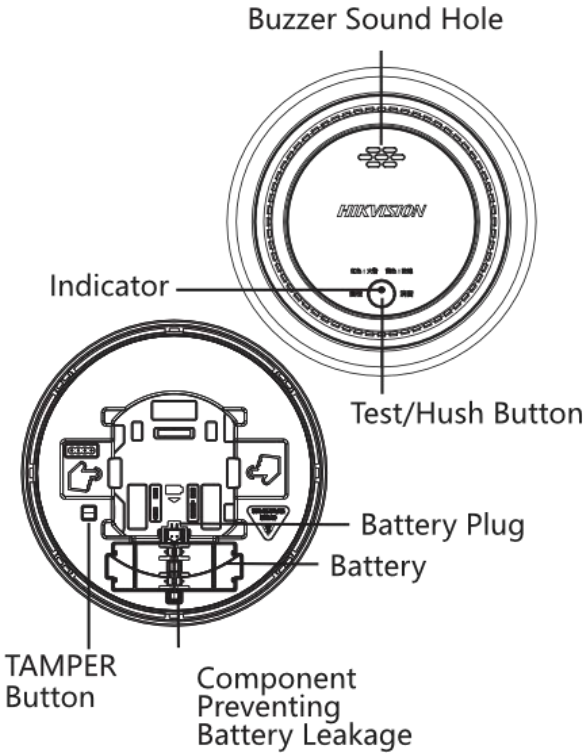


Figure 2-2 Smoke/Heat Detector Appearance

Table 2-4 Status Description

Status Description	Indicator	Buzzer
Standby Mode	The green light flashes every 90 seconds.	Off
Smoke/Heat detector	The red light is on.	Rapid beeps
Low voltage state	The yellow light flashes every 40 seconds.	Beep every 40 seconds
TAMPER Alarm	The green light flashes for 3 times.	Off
Labyrinth Pollution	Every 100 seconds, according to the "red light - green light" flashes once.	Off
Temperature sensor failure	Every 100 seconds, according to the "red light - green light" flashes once.	Off
Communication Failure	The red light flashes every 100 seconds.	Off

Note

The battery leakage prevention part is used to confirm that the battery is installed correctly. If the battery is not fully inserted, this part will prevent the device from being properly secured to the base.

2.3 Audible Strobe Light/Call Point Appearance

Call point appearance is as follows:

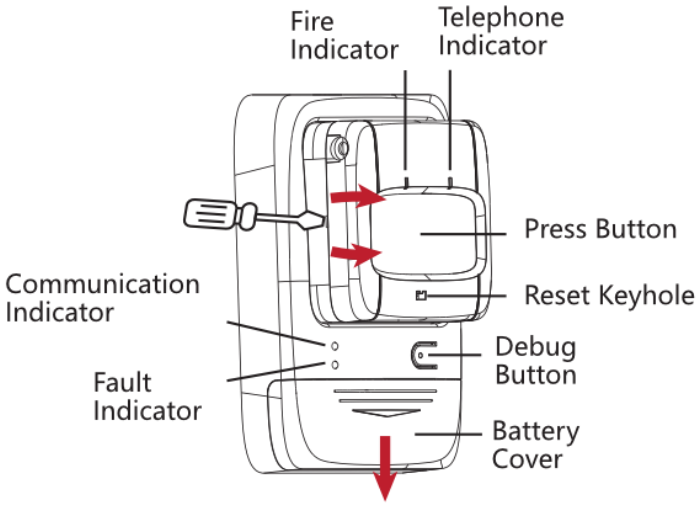


Figure 2-3 Call Point Appearance

Table 2-5 Indicator Description

Indicator	State	Description
Fire Alarm	The Red light is on.	Trigger an alarm.
Telephone	The red light is on.	On the phone.
Communication	The green light flashes every 120 seconds.	Device communication normal.
Fault	The yellow light flashes every 120 seconds	Device communication fault.
	The green light flashes every 40 seconds.	Low battery
	The yellow light flashes for 3 times.	TAMPER alarm

Audible strobe light appearance is as follows:

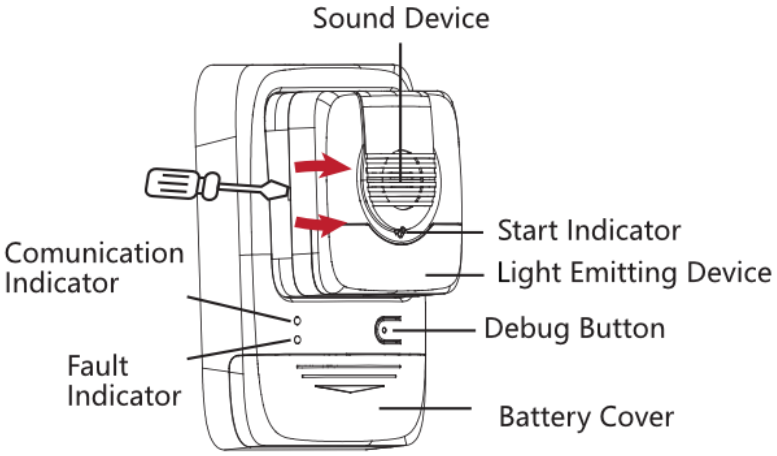


Figure 2-4 Audible Strobe Light Appearance

Table 2-6 Indicator Description

Indicator	State	Description
Start	The red light is on.	Started successfully.
Communication	The green light flashes every 120 seconds.	Device communication is normal.
Fault	The yellow light flashes every 100 seconds.	Device communication fault.
	The yellow light flashes every 40 seconds.	Low battery.
	The yellow light flashes for 3 times.	TAMPER alarm/ Main power supply not connected /Battery Power not Connected

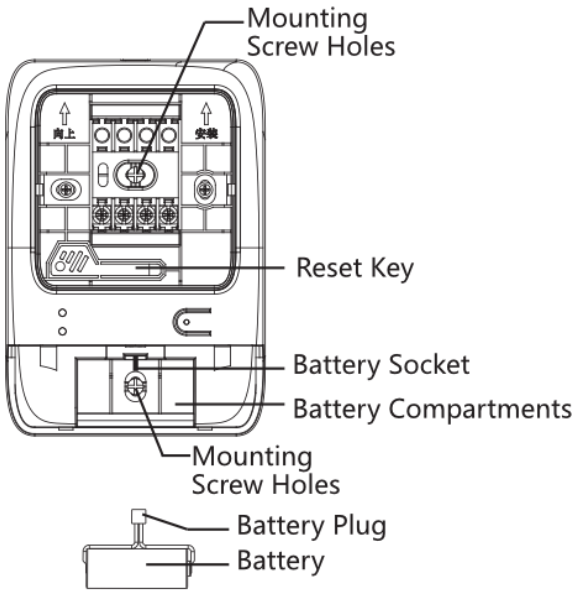


Figure 2-5 Base Of Audible Strobe Light

Note

The picture above shows the base of the audible strobe light device and call point. The structure is similar, please refer to the actual product.

Chapter 3 Wiring

3.1 Gateway Wiring

At the back of the device, slide down the mounting plate from top to bottom, and connect cables according to the descriptions below.

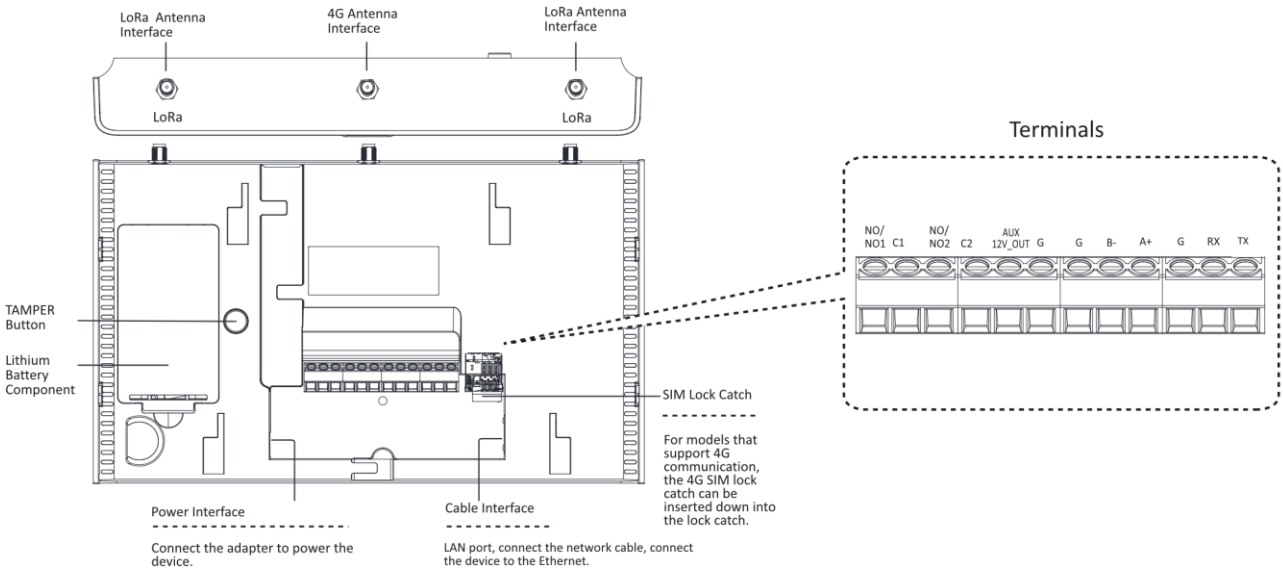


Figure 3-1 Wiring Diagram of Gateway

Table 3-1 Terminal Description

Terminals	Description
NO1	Alarm output 1, normally open.
C1	
NO2	Alarm output 2, normally open.
C2	
AUX 12V_OUT	Auxiliary power output
G	Auxiliary power negative pole
G	RS-485 Signal to Ground Wire.
B-	RS-485-
A+	RS-485+
G	RS-232 signal to ground wire.
RX	RS-232 receiver
TX	RS-232 sender

Note

The gateway is delivered with a power adapter. To ensure the normal operation and safety of the gateway, do not replace the power adapter at will.

3.2 Audible Strobe Light/Call Point

The wiring descriptions for the wiring terminals on the rear of the gateway are as follows:

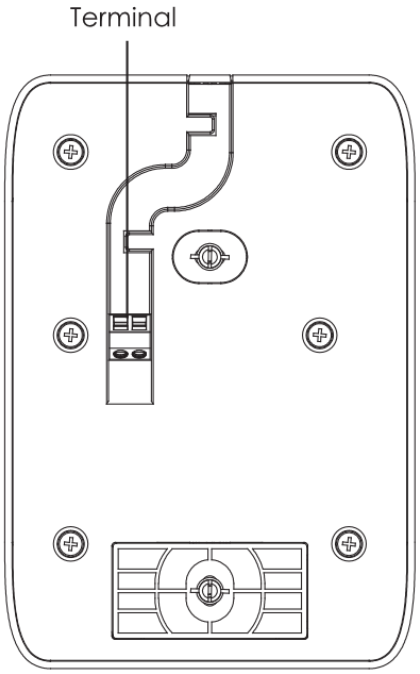


Figure 3-2 Terminals

Table 3-2 Terminals of Audible Strobe Light

Terminals	Wiring Description	Note
12V	Positive power input.	Connect to DC 12V/1A power supply. The allowable power input range is DC 10 ~15 V/1 A.
GND	Negative power input.	

Table 3-3 Terminals of Call Point

Terminals	Descriptions
K+	Access to one DC 24 V/1 A relay output, allow access to the maximum DC 30 V/2 A or AC 125 V/0.5 A relay output(Does not distinguish between positive and negative).
K-	

Chapter 4 Installation Introduction

4.1 Installation Cautions

Please strictly follow the installation method in this guide to install the device.

- To prevent injury, make sure the product is securely fastened when installing on a wall or ceiling.
- Install the device on a flat wall.
- Make sure that the installation wall can bear at least four times the weight of the device.
- Pay attention to the following when installing the alarm.
  - If the installation location (eg ceiling) length is longer than 10 meters, multiple alarms need to be installed.
  - Please install the alarm after finishing the interior decoration to prevent the alarm from being polluted.
  - The installation location should be at least 30 cm away from the path of strong wires, so as to avoid the accumulation of small insects under the influence of phototaxis, resulting in smoke maze pollution and alarm.
  - When installed on a flat roof, the edge of the alarm should be at least 500 mm from any wall.
  - When installed on a sloped or diamond-shaped roof, the alarm should keep a certain distance from the roof. When the slope is less than 30°, the appropriate distance is 500 mm.
  - Avoid installing alarms in the following locations:
    - Spaces with high humidity such as kitchens, water heaters, bathrooms, etc.
    - Air conditioners, fans, heating air outlets, and strong convection at wind speed.
    - Dusty, dirty or insect-infested places.
    - Places with high temperature and easy pollution such as stoves.
    - Where objects are occluded.
    - Places within 1.5 meters from the lamps.
    - The upper part of the spire house, the corner of the room and other closed spaces.

4.2 Gateway Installation Method

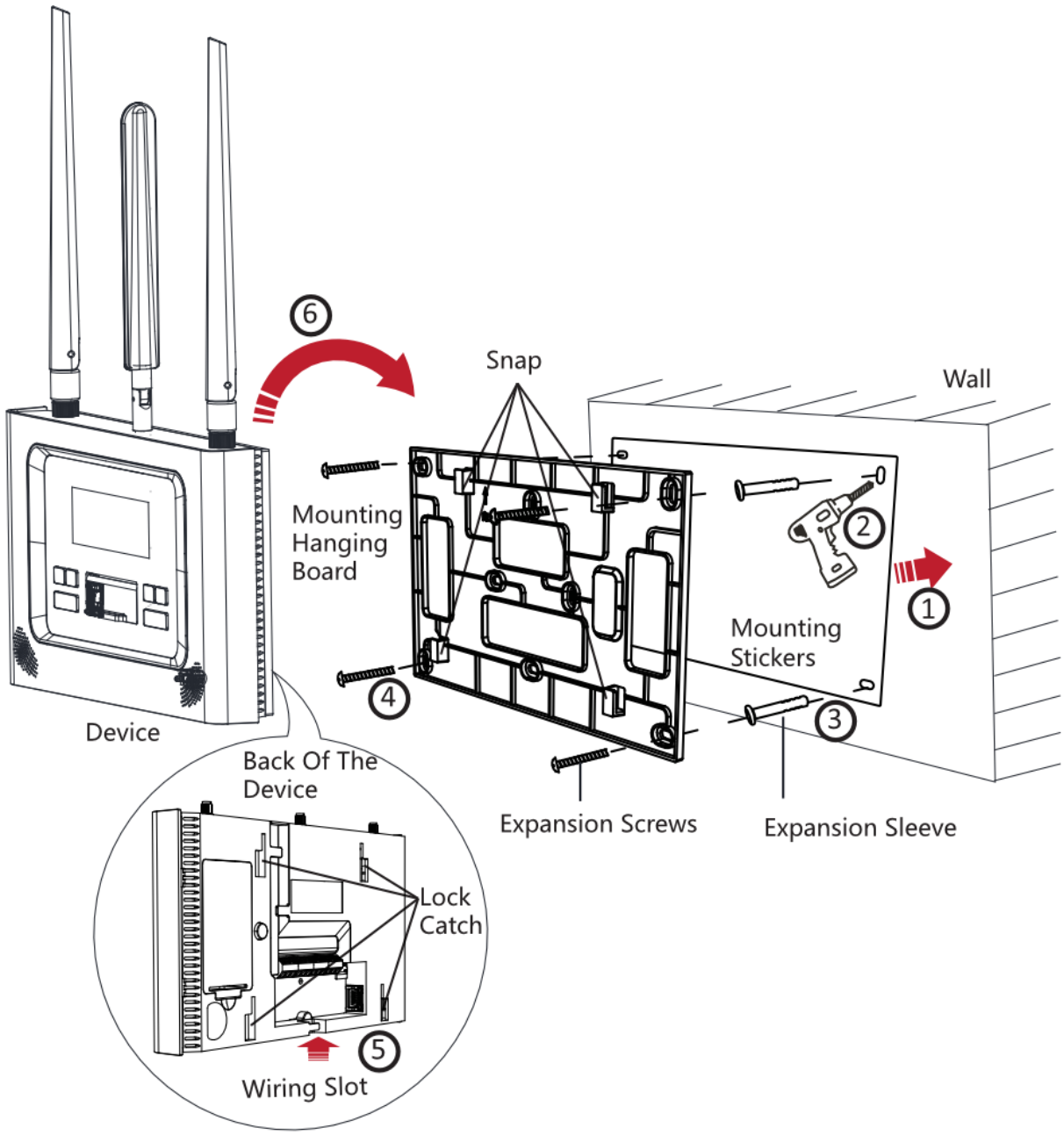


Figure 4-1 Fire Alarm Gateway

Steps:

Step 1 Fix the installation sticker to the wall installation location.

Step 2 Drill holes on the wall according to the positions of the screw holes for the installation stickers.

Step 3 Install the expansion sleeve.

Step 4 Fix the device mounting hanging board to the wall with screws.

Step 5 Trim the device wiring and route the cables through the bottom cable channel.

Step 6 Align the lock catch on the back of the device with the snaps on the mounting hanging board, and fix the device on the mounting board from top to bottom.

4.3 Smoke/Heat Detector Installation

4.3.1 Preparation before Installation

Steps:

Step 1 Install the battery.

1) At the position indicated by the gesture on the back of the alarm, squeeze the buckle inward with two fingers at the same time to take out the back cover.
2) Insert the connector (battery) into the connector (device), put the battery into the battery base in the direction shown in the figure and insert it as far as it will go, and then install the back cover to its original position.

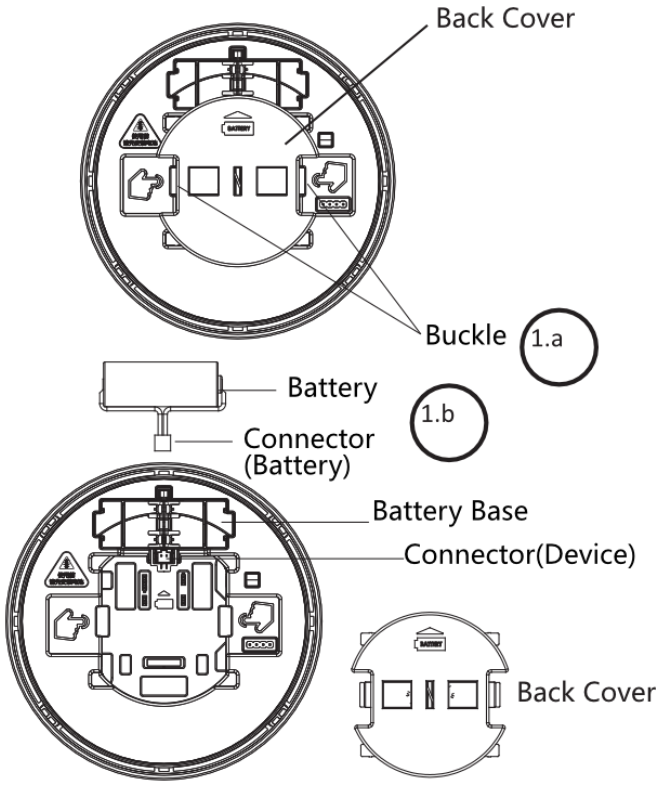


Figure 4-2 Smoke/Heat Detector Mounting Preparation

Step 2 Check alarm status. Press the ***Test/Hush*** button. When the buzzer beeps for 5 times and the red light is steady on, it indicates that the buzzer and indicator are working normally and can be installed.

Step 3 Determine the installation location according to the signal strength of the alarm.

1) Enroll the alarm in the gateway and snap the base to the detector. For the enrollment method, refer to 6 Quick Configuration Introduction.
2) On the gateway side, enter ***Main Menu-Device List-Smoke Detector***, and turn to the corresponding alarm in the list.
3) Press and hold the ***Test/Hush*** button of the alarm for more than 3 seconds, and enter the signal inquiry mode after one beep.

Note

- Strong signal: the indicator light of the alarm flashes green 3 times rapidly, which means the position is suitable for installation.
- Weak signal: the red light of the alarm indicator flashes 3 times rapidly, which means this location is not suitable for installation.

4.3.2 Installation Method

Steps

Step 1 Locate the holes on the ceiling according to the mounting template.

Step 2 Insert the plastic expansion sleeve into the punched position, align the U-shaped hole corresponding to the mounting base with the plastic expansion sleeve, and then use the self-tapping screw to fix the mounting base.

Step 3 Rotate the alarm in the direction shown and fasten the alarm to the mounting base to complete the installation.

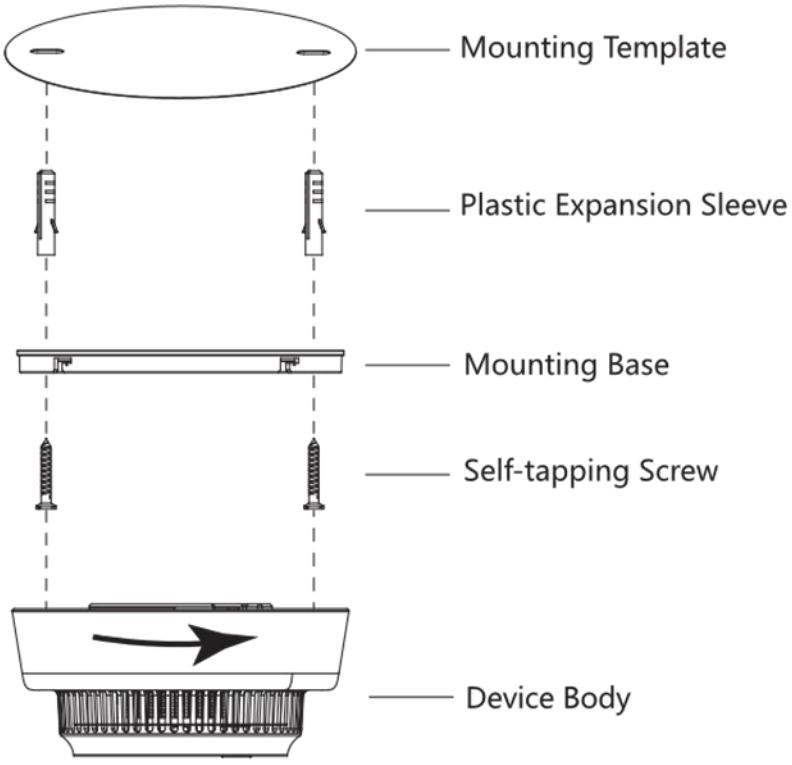


Figure 4-3 Smoke/Heat Detector Mounting

4.4 Audible Strobe Light/Call Point Installation

The installation methods of call point and audible strobe light are similar, and the installation of audible strobe light device is taken as an example to introduce.

4.4.1 Preparation before Installation

Steps

Step 1 Install the battery. Insert the battery plug into the battery socket on the audible strobe light/ device and close the call point battery cover.

Step 2 Pair the audible strobe light/call point with the gateway. For the enrollment method, see 5 Quick Configuration Overview.

Step 3 Move the audible strobe light/call point to the selected installation position, and double-click the ***Debug*** button to confirm the signal strength of the device.

Note

- Strong signal: the communication indicator light flashes for 3 times, which means the position is suitable for installation.
- Weak signal: the fault indicator flashes for 3 times, which means this location is not suitable for installation.

4.4.2 Installation Method

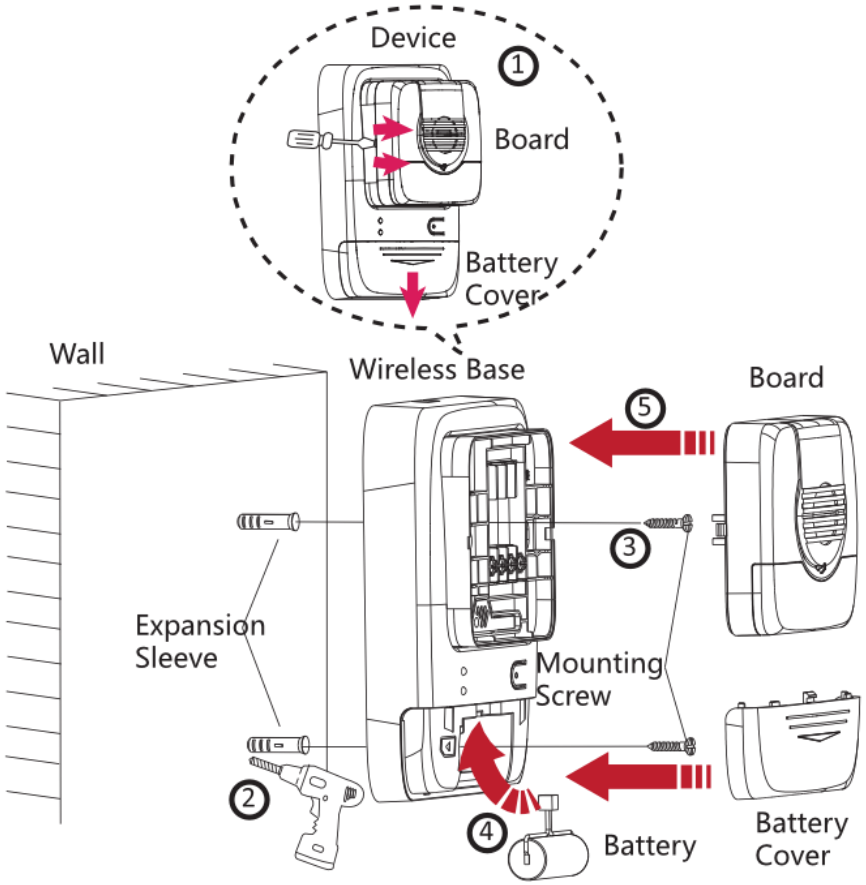


Figure 4-4 Audible Strobe Light Mounting

Step 1 Remove the board and battery cover.

Step 2 In the selected installation location of audible strobe light/call point, attach the wireless base to the wall to draw the drill position, and use the drilling machine to drill holes.

Step 3 Knock the expansion sleeve into the hole and screw the mounting screw to the head to leave a distance of about 2 mm. Then align the mounting holes on the wireless base with the heads of the mounting screws and hang them to ensure a firm installation.

Step 4 Insert the connector(battery) firmly into the device's battery socket to complete the battery installation.

Caution

Snap the board and battery cover to complete the installation.

Chapter 5 Quick Enrollment

5.1 Gateway Preparation

Step 1 Power on the gateway.

When powered on for the first time, set a 6-digit installer password to ensure the security of the product, please set a high complexity password and keep it properly.

Step 2 Press the ***Enter/Menu*** button, enter the user password, and press ***Enter/Menu*** again to enter the gateway main menu.

5.2 Smoke/Heat Detector Enrollment

Before you start

Prepare the alarm and gateway.

Steps:

Step 1 Optional: If the alarm has been paired, please choose one of the following clear enrollment methods to clear the enrollment.

- Enter the Main Menu → Peripheral Management → Device deletion on the gateway side, then move the alarm close to the gateway (<2 m), and press and hold the ***Test/Hush*** and the ***TAMPER*** button for more than 2 seconds, until the buzzer beeps for 3 times and the green indicator flashes for 3 times quickly, indicating that the enrollment is successful.
- Press and hold the ***Test/Hush*** button and the TAMPER button at the same time, power on the alarm until the buzzer beeps for 3 times and the green indicator flashes for 3 times quickly, indicating that the device is cleared successfully. Then enter the gateway, enter the ***Main Menu*** → ***Device List***, locate the device to be deleted, press the ***OK*** button, move the cursor to Node Delete and press ***OK***, switch the option to confirm and press the ***OK*** button, and follow the interface prompts to confirm whether the deletion is successful.

Note

- Clear enrollment successfully: the buzzer beeps for 3 times and the green indicator flashes for 3 times quickly.
- Clear enrollment failure: the buzzer is silent and the green indicator is off.

Step 2 Complete the enrollment between the alarm and the gateway.

1) On the gateway side, enter ***Main Menu*** → ***Peripheral Management*** → ***Device Add***.
2) Move the alarm close to the gateway (<2 m), and press and hold the ***TAMPER*** button for more than 3 seconds until the green indicator flashes and then release.

If the enrollment is successful, the buzzer will beep twice and the green indicator off.

5.3 Call Point/Audible Strobe Light Enrollment

Enroll the call point/audible strobe light in the gateway to manage the call point/audible strobe light alarm through the gateway.

Before you start

Prepare the call point/audible strobe light and the gateway to be enrolled.

Step 1 (Optional)If the call point/audible strobe light have been paired, please choose one of the following clear enrollment methods to clear the enrollment.

- On the gateway side, enter the ***Main Menu*** → ***Peripheral Management*** → ***Device Deletion***, then move the call point/audible strobe light close to the gateway (<2 m), and press and hold the [Debug] button on the call point/audible strobe light side until the green indicator of the communication indicator stops flashing and turned off, release it, and the yellow fault indicator rapidly flashes for 3 times, indicating that the enrollment is cleared successfully.
- Press and hold ***Debug*** until the yellow light of the fault indicator is always on and release it. The yellow light of the fault indicator rapidly flashes for three times, indicating that the device is cleared successfully. Then enter the gateway, enter the ***Main Menu*** → ***Device List***, locate the device to be deleted, press the ***OK*** button, move the cursor to the Node Delete and press ***OK***, switch the option to confirm and press the ***OK*** button, and follow the interface prompts to confirm whether the deletion is successful.

Note

- Clear enrollment successfully: yellow light of the fault indicator flashes rapidly for 3 times and then goes off.
- Clear enrollment failure: the green light of communication indicator keeps on for 1.5 seconds and then turns off.

Step 2 Complete the enrollment between the call point/audible strobe light and the gateway.

1) On the gateway side, enter Main Menu → Peripheral Management → Device Add.
2) Move the call point/audible strobe light close to the gateway (<2 m), press and hold the Debug button on the call point/audible strobe light end, and then release the button when the green light of the communication indicator flashes.

   If the enrollment is successful, the communication indicator flashes for three times; if the enrollment fails, the communication indicator is always on.

Note

If the enrollment fails, solve it according to the following conditions:

- Enrolled in another gateway already: perform clear enrollment operation.
- Not been paired with any gateway: press the [Debug] button, the yellow light of the fault indicator flashes once, and it will automatically re-enroll.

5.4 Input Expander Enrollment

Enrollment

Connect the input expander to gateway according to the following wiring method:

Table 5-1 Input Expander Wiring

Terminal (input expander)	Terminal (gateway)
D+	A+
D-	B-

After the connecting， input expander will be automatically enrolled to gateway. Enter the ***Main Menu*** → ***Device List*** → ***Channel***, you can see the enrolled input expander, indicating that the enrollment is successful.

Note

Disconnect the expander and the gateway to delete the peripheral.

Chapter 6 Gateway Configuration and Operation

6.1 Gateway Local Configuration

The gateway can be configured through the local menu of the gateway (hereinafter referred to as "device"), including peripheral management, linkage function configuration, network configuration, communication configuration, system configuration, status and information query, etc.

Note

When the gateway is powered on for the first time, a 6-digit installer password and device time need to be set. In order to ensure the security of the product, please set a password with high complexity and keep it properly.

Basic Operation Description

The basic operations of the gateway local configuration are as follows:

- Enter the menu: press the ***OK/Menu*** button, enter the user password, and press the ***OK/Menu*** button again to enter the menu.
- Input password: The default password number is 555555. Press ***Up/Down*** to adjust the size of the number; press ***Enter/Men***u to confirm the current setting number and move to the next digit.

Peripherals Management

Adding a device

Add peripherals to the gateway to pair the peripherals with the gateway. For the enrollment method, please refer to *Smoke/Heat Detector Enrollment* and *Call Point/Audible Strobe Light Enrollment*.

Deleting a device

Clear the enrollment between the peripheral and the gateway. For details about how to clear the enrollment, please refer to *Smoke/Heat Detector Enrollment* and *Call Point/Audible Strobe Light Enrollment*.

Deleting all

Remove all added peripherals. After deletion, perform a clear enrollment operation on all deleted peripherals so that the peripherals can be paired with other gateways again. For the operation method of clearing enrollment on the peripheral side, please refer to *Smoke/Heat Detector Enrollment* and *Call Point/Audible Strobe Light Enrollment*.

Device List

View the peripherals connected to the gateway, such as smoke/heat detector (alarms), call point /audible strobe light device, household combustible gas detectors, etc.

Log Search

Query alarm, fault and operation logs.

After entering the alarm/fault/Operation log interface, you can view the alarm/fault/operation time, device, serial number, specific type and event type. Press ***UP/DOWN*** to view more log records.

Functional Configuration

Interconnection

Enable or disable alarm linkage between gateways.

Alarm linkage

Relay linkage configuration, including alarm linkage output, fault linkage output, configuration linkage mode and linkage time.

Note

The default linkage mode is on and the linkage time is one minute.

Fault broadcast

Configure whether to broadcast through the gateway speaker when the corresponding fault events (such as main power, backup power, wired, wireless, TAMPER, Hik-Connect, and node failure) occur.

Anti-false alarm

When the gateway receives only one fire alarm, it does not link the audible strobe light nodes under it; when the gateway receives two or more fire alarms, it links the audible strobe light nodes under it.

Simulate alarm

Simulates the state and alarm output action when the gateway receives an alarm signal.

SF configuration

Spreading factor(SF) in LoRa communication, aiming to improve the signal strength of transmitted data.

Network Configuration

Dynamic IP

Enable or disable the automatic IP matching function.

Static IP

Manually set parameters such as gateway IP address, gateway, subnet mask and DNS server.

Communication configuration

SMS/Phone Configuration

Number and status configuration for receiving SMS/phone voice alarm prompts, up to 6 mobile numbers can be configured.

Wired/Wireless Network Center

Configure the monitoring center platform IP and port.

Network reporting policy

Configure whether to use wired/wireless network center.

Heartbeat reporting period

Configure the period for reporting data to the central platform.

System status

Query device power status, TAMPER status, bus status, wired network status, 4G network status, relay status, Hik-Connect status.

System message

Device Information

View gateway information, including gateway name, serial, model, and program version.

Password configuration

Set local installer, administrator and operator passwords. For user permission descriptions, see *Manage Device Local Users* .

Manual timing

Set the gateway local time.

Factory data reset

Enter the installer password to restore the gateway to its factory configuration (inactive state).

RS-232 configuration

According to the RS-232 connection status, configure the RS-232 baud rate for the gateway to be consistent with the RS-232 baud rate of the connected device.

Caution

The debugging function of the RS-232 configuration interface is only used for debugging, and users are prohibited from using it.

RS-485 configuration

According to the RS-485 connection status, configure the RS-485 baud rate for the gateway to keep it consistent with the RS-485 baud rate connected to the gateway.

Device restart

Gateway restarts.

Device self-check

Check whether the gateway buzzer, speaker and indicator work normally.

6.2 Descriptions before Use

6.2.1 Internet Connection

Caution

If you connect your products to the Internet, you are at your own risk, including but not limited to network attacks, hacker attacks, virus infection, etc., and the company will not be responsible for abnormal work of the products, information leakage and other problems caused by this, but the company will provide you with technical support related to the products in a timely manner.

Connect the device to the Ethernet with a network cable. After connecting to the network, you can enter the device web page through a browser to configure device function and parameter settings.

6.2.2 Activate the device

The device supports activation through SADP software and through the web terminal. You can choose one method to activate according to the actual situation.

Note

Gateway factory IP address: 192.0.0.64.

Device Activation Via SADP Software

Download the SADP software and run it, the SADP software will automatically search for inactive devices or all online devices under the same network segment, and the list will display the device type, IP address, security status, device serial number and other information. Inactive devices can be activated through the SADP software.

Before you start

The device is powered on and connected to the network.

Step 1 Download the SADP software from the official website and run it.

Step 2 Select the device to be activated, and the related information of the device will be displayed on the right side of the list.

Step 3 Set the device password in the Activate Device field and confirm the password.

Caution

- In order to protect your personal privacy and corporate data, and avoid network security problems of device products, it is recommended that you set a strong password that complies with security specifications.
- In order to improve the security of product network use, the length of the set password must reach 8-16 digits, and it must be composed of at least two or more types of numbers, lowercase letters, uppercase letters and special characters.

After the device is successfully activated, the activation status in the list is updated to ***Activated***.

Step 4 (Optional) Modify the device IP address.

1) Check the activated device in the device list.
2) Input the IP address, subnet mask, gateway and other information in the ***Modify Network Parameters*** on the right.
3) After modification, input the password set when activating the device, and click ***Modify***.

Note

Modify the IP address according to actual needs. For example, when you need to log in to the device web page to configure the device, please set the IP address of the device and the IP address of the computer that needs to log in to the device web page in the same network segment.

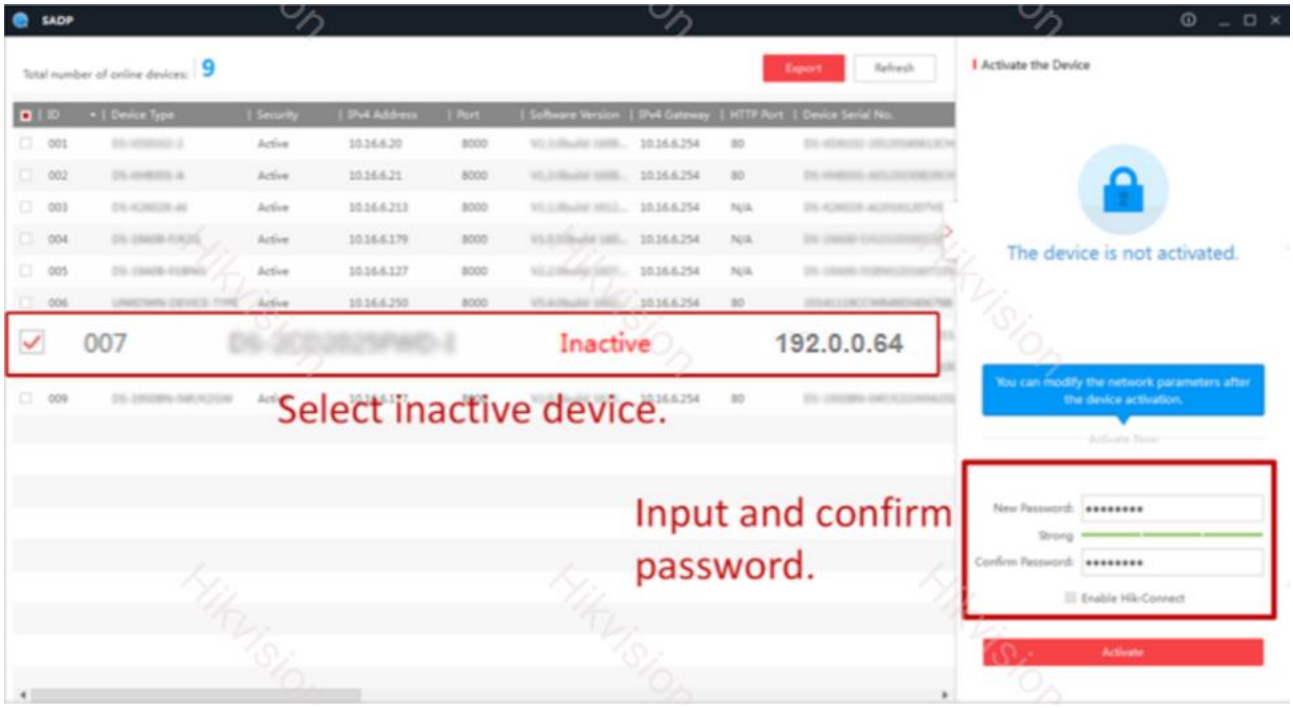


Figure 6-1 Modify device IP address

Activate via web

Access the device through the web terminal and activate the device.

Step 1 Directly connect the device to the computer with a network cable.

Step 2 Modify the computer IP address and the device IP address to be in the same network segment.

Note

The gateway factory IP address: 192.0.0.64, the computer IP address can be set to any IP address from 192.0.0.2 to 192.0.0.254 (except 192.0.0.64), for example: set the computer IP address to 192.0.0.100.

Step 3 Input the device IP address in the browser to display the activation interface.

Step 4 Set the device activation password.

Caution

- In order to protect your personal privacy and corporate data, and avoid network security problems of device products, it is recommended that you set a strong password that complies with security specifications.
- In order to improve the security of product network use, the length of the set password must reach 8-16 digits, and it must be composed of at least two or more types of numbers, lowercase letters, uppercase letters and special characters.

Step 5 Click ***OK*** to activate the device.

6.2.3 Access the Device

Introduce the method of accessing the device through the web terminal and Hik-Connect.

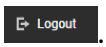
Access The Device Through The Web

Log in system

You can log in to the web page of the device, and configure and operate the device through the web page. Power on the device and connect to the network, input the IP address of the device in the address bar of the browser to log in.

Exit system

If you have completed the setup or operation of the device, you need to safely log out of the device system when you no longer perform any operations.

Safely exit the device system by clicking 

.

Access devices through Hik-Connect

On devices that support Hik-Connect access, through the video service of Hik-Connect, you can view video images, historical recordings and other functions in real time. And through the alarm service of Hik-Connect, you can instantly receive abnormal information of the places you care about to take safety precautions immediately.

Open Hik-Connect Through The Webpage

The Hik-Connect function can be enabled and set through the web page to realize the Hik-Connect access to the device.

Steps

Step 1 On the device web page, enter *Configuration* → *Network Parameters* → *Hik-Connect Configuration*.

Step 2 Click the slider to enable the Hik-Connect function.

Step 3 Set the Hik-Connect access parameters.

Escalation Policy

You can choose wired or wireless network according to the actual use of the network.

Hik-Connect opcode

For the security of device access, you need to input an operation code (verification code) when adding a device to your Hik-Connect account.

Note

If the device has been added to Hik-Connect, the opcode will not be displayed; if the device has been deleted from the platform, you can click ***Mandatory Access*** to obtain a new opcode.

Step 4 Click ***Save***.

Add Device To Hik-Connect Video Mobile Client

Through the Hik-Connect video mobile client, the device can be connected to the Hik-Connect, and the device can be accessed through the mobile client.

Before you start

According to the actual environment and the communication methods that the device can support, choose one of the following methods to connect the device to the network.

- The device is connected to the router through a wired network. Please ensure that the router is normally connected to the WAN.
- The device is connected wirelessly, and ensure that the wireless network signal is normal and the SIM card traffic is sufficient.

Step 1 Install Hik-Connect client and register a user account for iOS and Android.

1) Search Hik-Connect in App Store or Google Play™ to downdoad and install the client.

2) Lounch the App and follow the on-screen instructions to register a user account.

Step 2 Start the Hik-Connect client, and login the client.

Step 3 Click + in the upper left corner of the client software to add a device.

- Scan the QR code on the device body to add the device.
- Click in the upper right corner of the software and manually input the serial number on the device label to add the device.

Note

The adding and configuration operations should be completed within 3 minutes after the camera is powered on, otherwise, the device needs to be restarted and the operation will be repeated.

6.3 Configure the Gateway through the Web Terminal

Enter the gateway IP address in the browser to enter the login interface, input the admin user password and click ***Login*** to enter the gateway web page.

The gateway supports configuring device parameters through the web page, including configuring network parameters, managing users, configuring alarm parameters, modifying device information, setting time, and system maintenance, etc.

Note

Before logging in to the web terminal, you need to complete gateway activation.

6.3.1 Basic Configuration

Network Settings

When the device is connected to the network through a network cable, if you need to modify the IP address for network access, you can configure network parameters through this page.

Step 1 On the device web page, click ***Configuration*** → ***Network Parameters***.

Step 2 Select the network parameter configuration mode.

- - Automatically obtain network address

  Check DHCP to automatically assign network addresses to devices without manual settings.

- - Manually configure the network address

  Uncheck ***DHCP*** and manually set network parameters for the device, including IP address, subnet mask address and gateway address.

Note

After modifying and saving the local network parameters, the device will restart automatically.

Step 3 (Optional) When the device is accessed through a domain name, a correct and available DNS server address needs to be configured.

Step 4 Click ***Save***.

User Management

Manage local users and web-side admin users.

Modify Web User Password

The web terminal admin user is the user who logs in to the web terminal of the device and has all the configuration and operation rights. Change the password for the admin user on the web page according to actual needs.

Step 1 On the device webpage, click ***Configuration*** → ***User Management*** .

Step 2 Click ***Modify***, input the old password, create a new password, and confirm.

Caution

- In order to protect your personal privacy and corporate data, and avoid network security problems of the device product, it is recommended that you set a strong password that conforms to security specifications.
- In order to improve the security of product network use, the length of the set password must reach 8-16 digits, and it must be composed of at least two or more types of numbers, lowercase letters, uppercase letters and special characters.

Step 3 Click ***OK*** to complete the password modification.

Manage Device Local Users

Manage device local users, including local installer users, administrator users, and operator users.

Local user permissions are as follows:

Table 6-1 User Permission Description

Local User Type	Permission description
Installer	With the highest authority for local operations and can perform all local configurations and operations.
Administrator	With all local configuration and operation rights except factory reset operation
Operator	Only with the permission to view local parameters, but not to configure it.

Steps

Step 1 On the device web page, click ***Configuration*** → ***User Management*** to edit device local users in the ***User Management*** module.

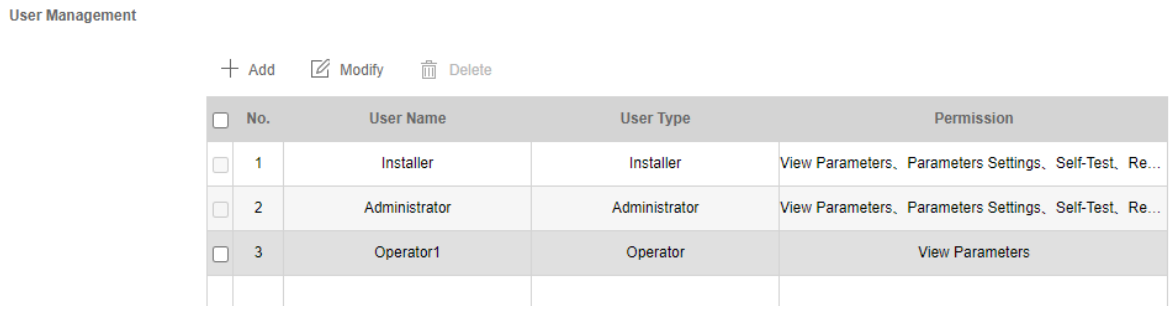


Figure 6-2 Manage local users of device

Optional: Perform the following user management operations according to actual requirements.

Edit Local User In the user list, click the the user to be edited, and click ***Modify*** to edit the user name and set a new password. Click ***OK*** to save the settings.

Add Local User Click ***Add***, set the user name and password, and click ***OK*** to save the settings.

Note

- Before adding an operator user, you need to add an administrator user.
- Supports adding up to 1 administrator user and 8 operator users. After the device is powered on for the first time, an initial password needs to be set. After the setting is completed, one installer user will be generated by default.

Delete operator Select the operator user to be deleted, click ***Delete***, and click ***OK*** in the displayed prompt box to delete the selected user.

Note

Installer and Admin users are not allowed to be delete.

6.3.2 Alarm configuration

Network Function Configuration

Configure the functions related to automatic networking of the gateway, such as platform synchronization peripheral information, channel frequency band, peripheral search, etc.

Step 1 On the device web page, click ***Alarm Settings*** → ***Network Function.***

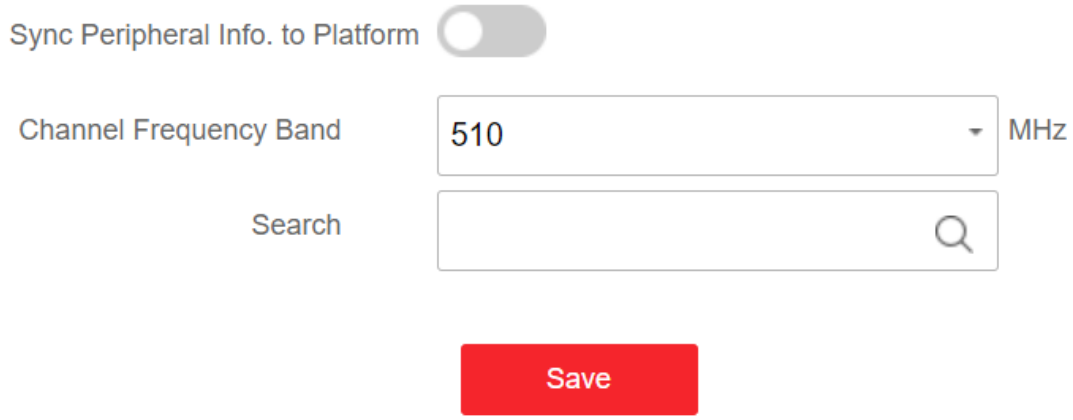


Figure 6-3 Network Function Configuration Page

Step 2 Configure related functions according to actual needs.

Platform Sync Peripheral Information

After this function is turned on, the peripheral configuration issued by the platform shall prevail; after this function is turned off, the local configuration of the peripheral shall prevail.

Channel Frequency Band

When there is a channel conflict between the device and other gateways, the channel frequency band can be modified to prevent data from interfering with each other.

Search

The peripheral search function can find the gateway where the peripheral is located through the communication between the gateways, so as to help the scene to find the corresponding peripheral in time and perform related operations.

When using, please input the peripheral serial number (located on the peripheral label), click to automatically search and prompt the search result.

Step 3 Click ***Save.***

Alarm Linkage Configuration

Configure the relay output parameters for event linkage. When the corresponding event occurs, the device will link the relay output according to the configured parameters.

Steps:

Step 1 On the device webpage, click **Alarm Settings → Alarm Linkage**

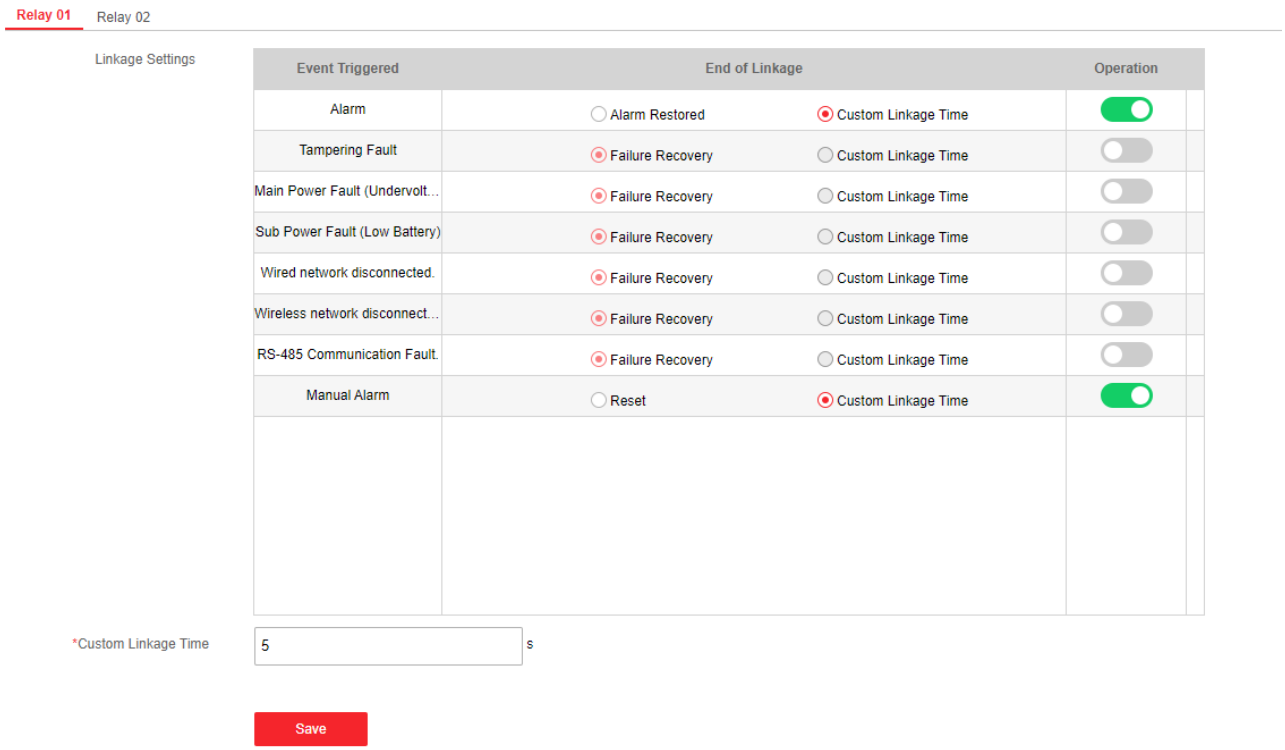


Figure 6-4 Alarm Linkage

Step 2 Select the relay that needs to be configured.

Step 3 Select the linkage event, and click the slider to enable the event linkage configuration.

Step 4 Select the linked end action for the relay.

Options	Descriptions
Recovery/Reset	When the corresponding alarm or fault event is recovered, or when manually reset, the linkage output is automatically turned off.
Custom Linkage Time	After the linkage output is turned on, it will automatically turn off after the custom linkage time expires. When selecting this option, you need to set a custom linkage time, which is 30 seconds by default.

Alarm Reporting Center Configuration

The device supports reporting information to the monitoring center platform. You need to select a reporting strategy for the device and configure reporting center parameters. After the device is added to the platform and the reporting center is configured in this section, the device can be monitored through the central platform.

Step 1 On the device web page, click Alarm Settings → Upload Center

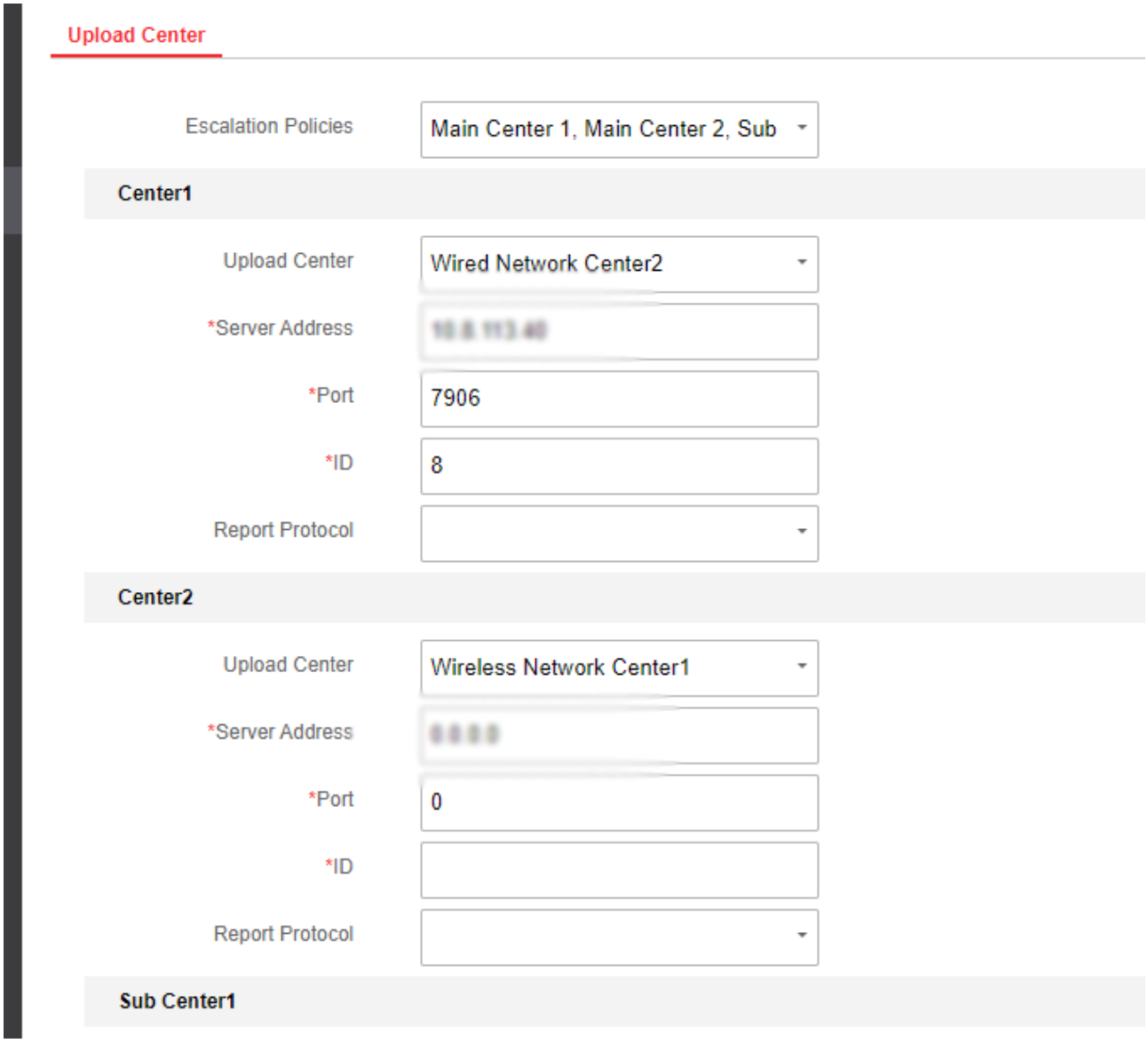


Figure 6-5 Alarm Upoad Center Configuration

Step 2 Select an escalation policy.

Note

When the main line fails, it can be switched to the backup line, and when the fault is removed, it can be restored to the main line.

Step 3 According to the selected reporting policy, configure reporting center parameters.

Upload center

Select the reporting center to be configured.

Server address

Central platform server IP address.

Port

Central platform server port.

ID

The ID number is the unique identification of the device during communication and is used for data transmission.

Step 4 (Optional) Repeat step 3 to configure parameters for all hubs.

Step 5 Click ***Save.***

6.3.3 System Configuration

Device Information

Viewing basic device information, including gateway model, serial number, version, and web version. You can also customize the gateway name (the length should not exceed 16 English characters or 8 Chinese characters). It is recommended that you type the gateway address in the gateway name, so that you can quickly obtain the location of the alarm gateway when prompted by voice/SMS.

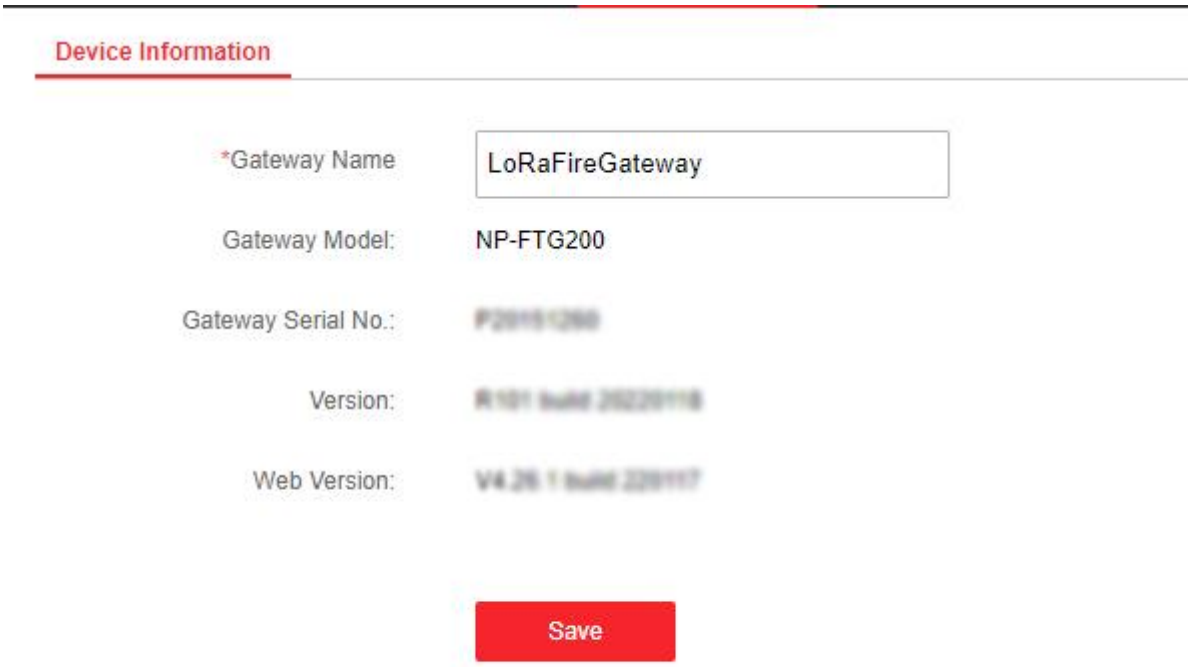


Figure 6-6 View device information

Time Settings

You can configure the time of the device, including automatic timing or manual timing.

Caution

If the device is powered off, the device time will be restored to the default value. It is recommended to use the NTP time calibration method.

On the device webpage, click ***Configuration*** → ***Time Settings***.

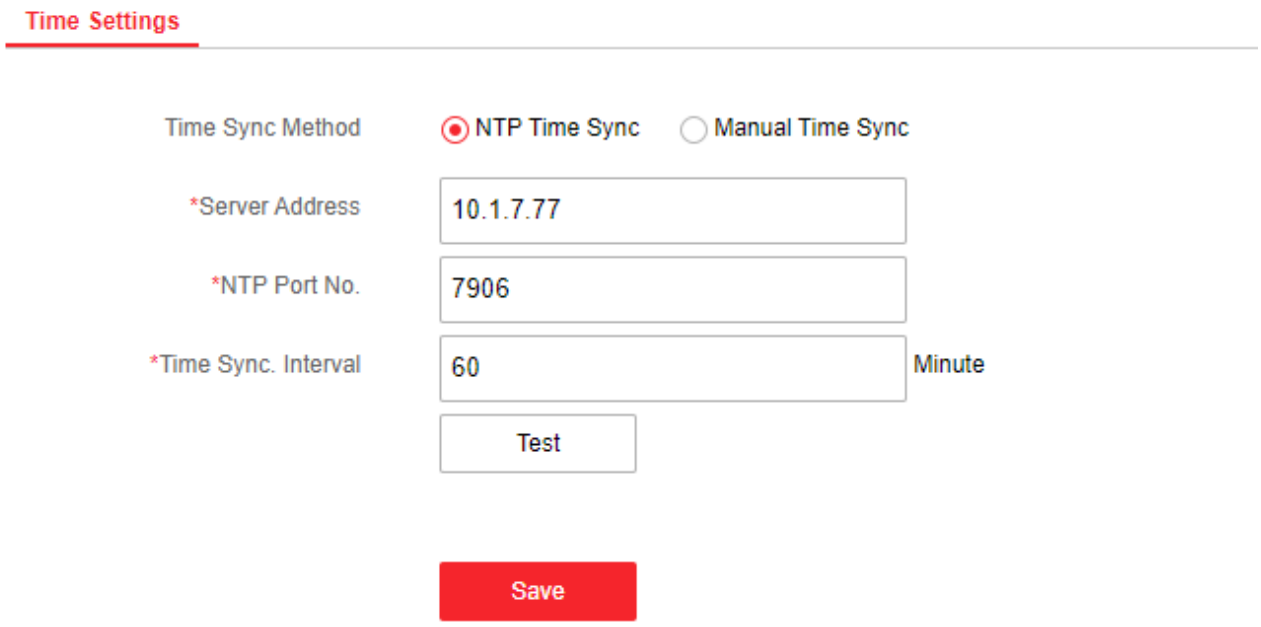


Figure 6-7 Configuring Device Time

NTP Time Sync

Select ***Time Sync Method***. You can select ***NTP Time Sync*** or ***Manual Time Sync***.

Note

- Click ***Test*** to test whether the set NTP server is correct.
- The recommended network timing server address is time.ys7.com, and the port is 123.

After the setting is complete, the device will periodically synchronize time with the NTP server based on the time interval.

Manual timing

You can set the device time directly or check ***Sync. with computer time***.

Heartbeat Settings

Configure the heartbeat interval. The heartbeat interval refers to the time period during which the device reports the running status to the platform.

Steps:

Step 1 On the device web page, click ***Configuration*** → ***Heartbeat Settings***.

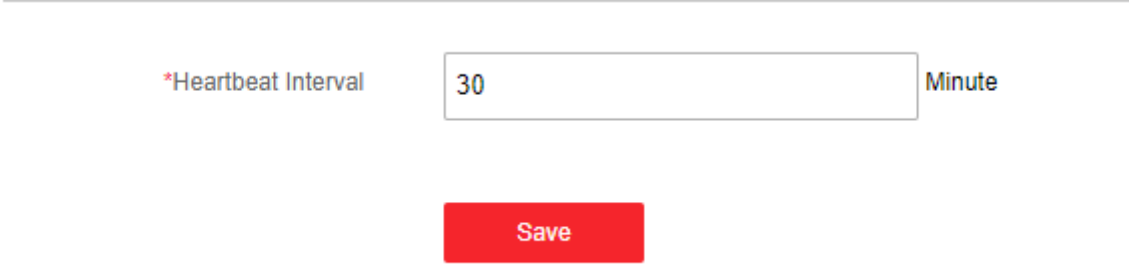


Figure 6-8 Heartbeat settings

Step 2 Input the heartbeat interval (1~65535 minutes).

Step 3 Click ***Save***.

Port No. Settings

When using RS-485 and RS-232 communication, set the baud rate of RS-485 and RS-232 according to the actual situation.

Steps

Step 1 On the device web page, click ***Configuration*** → ***Port No. Settings***.

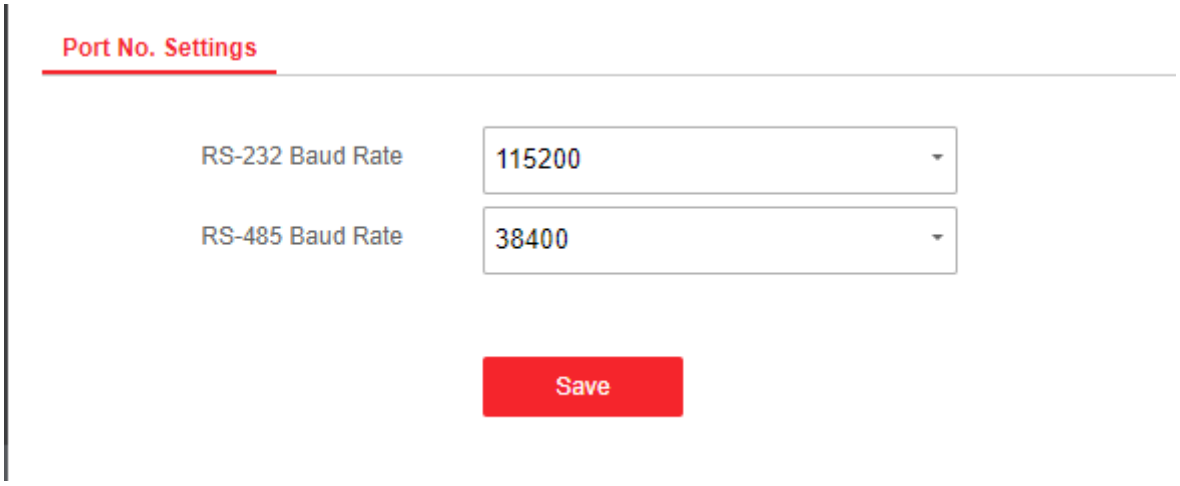


Figure 6-9 Serial port configuration

Step 2 According to the connection of RS-232 and RS-485, set the baud rate of RS-232 and RS-485 to make it consistent with the baud rate of the connected device.

Step 3 Click ***Save***.

Maintenance

This section describes operations such as device restart, device recovery, maintenance and upgrade.

On the device web page, click ***Configuration*** → ***Maintenance***.

Upgrade

Click ***Browse***, select the upgrade file, and click ***Upgrade*** to remotely upgrade the device program version.

Caution

Please do not turn off the power during the upgrade process, it will restart automatically after the upgrade is completed.

Note

After the upgrade is complete, please clear the browser cache and re-open the browser to log in to the device webpage to obtain the upgraded device program.

Restore

Restore

Click ***Restore Default Settings***. All other parameters are restored to the factory settings except for the user password, network parameters, time configuration, wireless peripheral configuration, alarm configuration and channel band configuration.

Default

Click ***Restore All.*** All parameters are restored to factory settings. The device is restored to inactive state, and needs to be reactivated.

Reboot

Click ***Reboot*** to restart the device.

Parameter Import

The device parameter is used to import the device parameter file, which is convenient for users to configure the same parameters for the device.

Step 4 Click ***Browse***, select the storage path of the device parameter file, and click ***Open***.

Step 5 Click ***Parameter Import.*** A prompt message will be displayed.

Step 6 Click ***OK***, input the encryption password, and import the device parameter file after confirming.

Parameter Export

It is used to export configuration files, which can facilitate the editing and reuse of parameter configurations.

6.4 Web Page Operation

Input the device IP address in the browser, log in to the device web page, to view the device information, log information and local information.

6.4.1 View device status

View alarm gateway device status, alarm input device status, relay output status, and basic status such as alarm, fault, and communication.

Gateway Status

View the basic information of the gateway (including IP address/serial number/version/model), as well as the current fire alarm and fault status.

Basic Status

Check the basic status of the gateway, including mains status, backup power status, TAMPER status, RS-485/RS-232 status, wired network, status, 4G status.

Gateway Output

Check the relay output status of the gateway.

Device Type

View the relevant status of peripherals (wireless smoke detector/manual call point/audible strobe light/heat detector/gas detector), including device type, serial number, alarm status, TAMPER status, power status, and signal strength. And can set the installation location for the peripherals (not more than 12 English characters) to facilitate the positioning of the detector.

In the device type section, peripherals can be added and paired with the gateway; and peripheral deletion operations are supported.

- Add peripheral: select the type of peripheral (Smoke Detector/Call Point/Audible Strobe Light/Heat Detector/Gas Detector), click ***Register***, in the pop-up prompt, click ***OK*** in the interface to trigger the peripheral enrollment. Once paired correctly, the list shows the peripherals registered to the gateway.
- Delete peripherals: Select the type of peripherals (Smoke Detector/Call Point/Audible Strobe Light/Heat Detector/Gas Detector), then select the peripherals to be deleted in the list, click ***Delete***, and click ***OK*** in the pop-up prompt interface to delete the selected peripheral.
- Edit peripherals: Select the type of peripherals (Smoke Detector/Call Point/Audible Strobe Light/Heat Detector/Gas Detector/ Wired I&O Expander), then click the text under the installation location list to edit the content and click ***Save*** to keep the edition.

Note

- For the method of triggering a peripheral to enter the enrollment state, please refer to the Quick Start Guide or the User Manual ***Peripheral Local Configuration and Operation Introduction*** section.
- After deleting the peripheral, please clear the enrollment operation on the peripheral side to cancel the enrollment with the gateway.

6.4.2 Log Search

On the device web page, click ***Log Search***, select the main type and sub-type to be searched, set the start time and end time, and click ***Log Search*** to search.

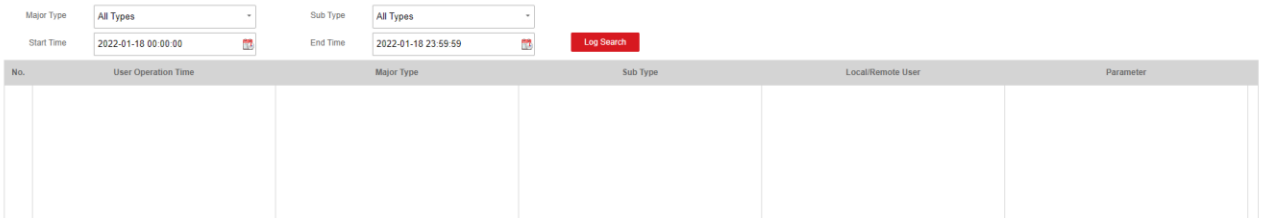


Figure 6-10 Log Search

Chapter 7 Peripheral Local Configuration and Operation Introduction

7.1 Alarm Local Operation

7.1.1 Test

Confirm whether the buzzer and indicator light work properly.

In the standby state of the alarm, short press the [self-test/silence] button, the alarm will enter the self-test state; after the self-test is completed, it will automatically resume to standby state.

Self-checking status: the buzzer beeps 5 times as "beep, beep, beep..."; the indicator light is always on red.

After the test is completed, the device will automatically exit the self-test state.

7.1.2 Smoke/Temperature Alarm

In the standby state of the alarm, when the smoke concentration or temperature reaches the response threshold, the alarm will generate an alarm signal.

Alarm status: the buzzer beeps rapidly, the indicator light is always on red.

7.1.3 Hush

During the alarming process of the alarm, short press the ***Test/Hush*** button to silence the alarm (silence period is 60 seconds).

Mute state: the buzzer will stop beeping; the indicator light is always on red.

Silencing period: After the alarm is silenced, when the smoke concentration or temperature is higher than the response threshold, the alarm will remain silent for 60 seconds and then an audible alarm signal will sound again.

Note

The silencing functions of the smoke alarm and temperature alarm are independent of each other. For example, after the smoke alarm is silenced, if a temperature alarm occurs within the silence period, the alarm will send out an audible alarm signal again.

7.1.4 Reset

When the alarm is in the mute state (that is, the red light is always on and the buzzer does not sound), short press the ***Test/Hush*** button again, and the alarm can return to the standby state.

In the alarm state, if the smoke concentration or temperature is lower than the response threshold, the alarm will automatically return to the standby state.

7.2 Local operation of Audible Strobe Light/Call Point

7.2.1 Audible Strobe Light Alarm/Alarm Recovery

Alarm

When the audible strobe light receive the alarm signal from the gateway or the monitoring center platform, it will send out the audible strobe light alarm signal.

Alarm recovery

When the gateway performs the reset operation, it will stop emitting audible strobe light alarm signals, and restore the alarm state to the standby state.

7.2.2 Call Point/Alarm Recovery

Alarm

When a fire occurs, manually press the starting part to trigger the fire alarm signal.

Note

If the switch output has been connected to the terminal on the back of the call point, the output will be linked after the alarm.

Alarm recovery

When it is confirmed that there is no alarm, if you need to restore the alarm state to the standby state, please insert the reset key into the reset key hole on the front panel of the call point, and push it inward until the call point makes a crisp sound and the starter parts bounce up and fire alarm light goes out, the manual reset is completed, and the manual is restored to the standby state.


See Far, Go Further