Thermal Network Hybrid Bullet Camera

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the functions and operations of the thermal network hybrid bullet camera (hereinafter referred to as the "Camera").

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

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

Revision History

Revision Content	Release Time	Revision Content
V1.0.0	First release.	March 2021

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.

- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This chapter describes the contents covering proper handling of the Camera, hazard prevention, and prevention of property damage. Read these contents carefully before using the Camera, comply with them when using, and keep the manual well for future reference.

Installation and Maintenance Professionals Requirements

All the installation and maintenance professionals must have qualification certificates or experience of installing and maintaining CCTV system, and working high above the ground. Besides, they have to acquire the basic knowledge and installation skills of:

- CCTV system.
- Low voltage wiring and low voltage electronic circuit wire connection.

Power Requirement

- All installation and operation should conform to your local electrical safety code.
- Make sure the power supply is correct before operating the device.
- Strictly follow the power supply requirements of the device.
  - ◇ The specific power supply requirements such as rated voltage shall be subject to the Camera label when selecting the power adapter.
  - ◇ The power adapter provided with the Camera shall be recommended to use.
  - ◇ Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC62368-1： 2014IEC60950-1. For specific power supply requirements, refer to device labels.
- Install easy-to-use device for power off before installing cables, which is for emergent power off when necessary.
- Protect the power supply wires from treading and pressing with great force, especially wires around the holes where the plug and outlet are threaded through.

Application Environment Requirements

- Use the Camera within the allowed humidity (< 95% relative humidity) and altitude (< 3000 m).
- Do not use the Camera outside the specific operating temperature and humidity range
- Do not store or transport the Camera outside the specific temperature and humidity range.
- Do not use the Camera in corrosive environment, such as high salt spray area, sea, coastal area, environment with acid gas, and chemical plant.
- Do not use the Camera in strong vibration environment, such as in boats and vehicles.

Contact the sales staff if you need to use the Camera in the above situation. Special models or specially customized Camera that meet requirements will be provided for you. We are not responsible for any improper operation.

- Do not place the Camera in a humid, dusty, extremely hot or cold site with strong electromagnetic radiation or unstable illumination.
- Do not block the ventilation opening near the Camera to avoid heat accumulation.
- Do not install the Camera near a heat source such as radiator, heater, or stove to avoid fire.
- Do not aim the lenses at intense radiation source (such as sun, laser and molten steel) to avoid damage to thermal detector and visual lens.
- Prevent liquid from flowing into the Camera to avoid damage to the internal components. In case of the liquid entering the Camera, immediately stop using the Camera, cut off the power, disconnect all the cables, and then contact the local customer service center.
- Do not stuff foreign materials into the Camera to prevent short circuit which could cause Camera damage or injury.
- Use the factory default package or material with equal quality to pack the Camera when transporting the Camera.
- Do not press, vibrate, or soak the Camera during the whole process of transportation, storage and installation.
- Do not stain or damage optical elements, such as lens and glass.
- Avoid mechanical vibration and impact during the whole process of transportation, storage and installation.

Operation and Daily Maintenance

- Do not touch the heat dissipation component of the Camera in case you might get burnt.
- Do not dismantle he Camera; for there are no components inside that can be repaired by yourself. And it may cause water leakage or bad image for the Camera if it is dismantled unprofessionally.
- It is recommended to use the Camera together with a lightning arrester, which is to improve the effect of lightning protection. It needs to conform to the lightning protection regulation for outdoor application.
- Do not touch the photosensitive Camera with your hands. Use an air blower to clean the dust and filth on the lens. For further cleaning, pour a little alcohol into a piece of dry cloth with which you can softly wipe the dirt away.
- Clean Camera body with a piece of soft dry cloth. For any dirt hard to remove, pick up a piece of clean and soft cloth, dip it with a little neutral detergent and gently wipe the dust away. After that, wipe all the liquids on the Camera away with another dry cloth. Never use any volatile solvent such

as alcohol, benzene and thinner, or any cleaner that is strong and abrasive. Otherwise, the Camera's surface coating will be hurt and its working performance will be encumbered.

- After unpacking, if the packing bag is damaged or leaking air, and the desiccant particles are of different colors, the normal use of the Camera will not be affected.

WARNING

- Use accessories suggested by the manufacturer, and install and maintain the Camera by professional personnel.
- Contact the local dealer or the nearest service center if the Camera fails to work normally. Do not dismantle or modify the Camera on your own.

Table of Contents

1 Packing List

Check the package according to the following checklist. You need to purchase tools and accessories that are not mentioned in the checklist.

Keep accessories properly for future use.

Figure 1-1 Packing list

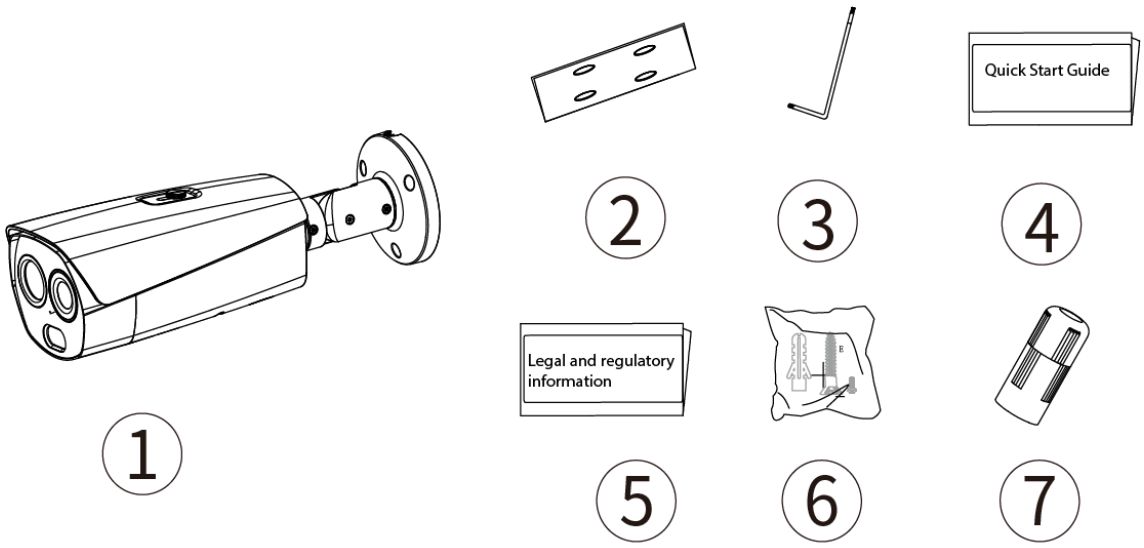


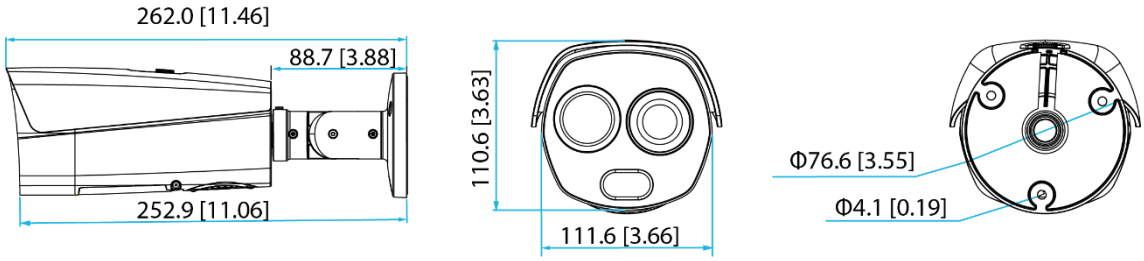
Table 1-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Thermal network hybrid bullet camera	1	5	Legal and regulatory information	1
2	Positioning map	1	6	Screw package	1
3	Wrench	1	7	Power adapter	1
4	Quick start guide	1	—	—	—

2 Design

2.1 Dimensions

Figure 2-1 Dimensions (mm [inch])



2.2 Cables

Figure 2-2 Cables

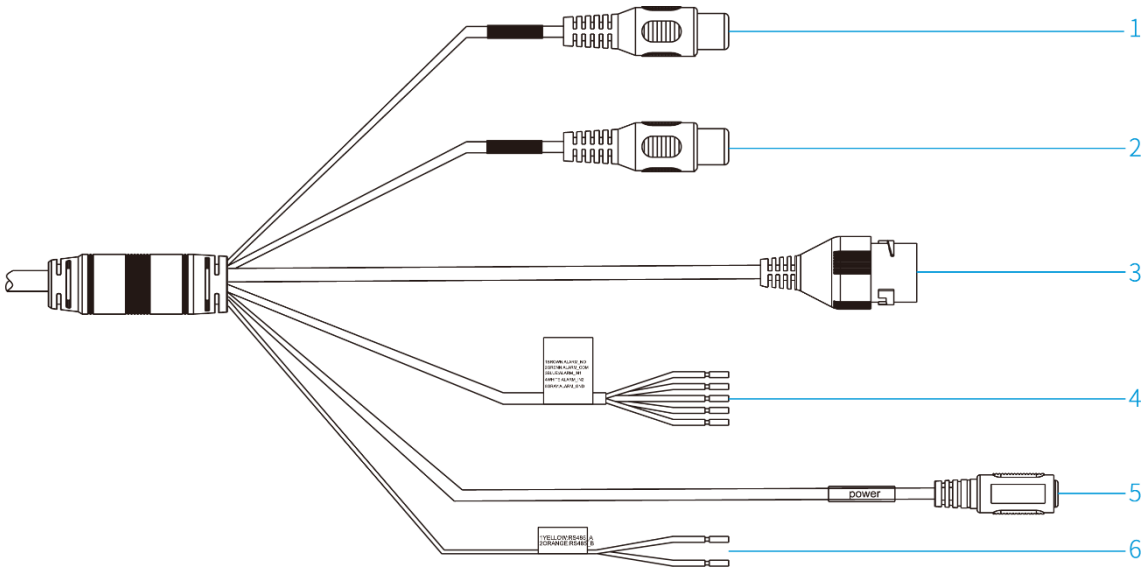


Table 2-1 Ports description

No.	Port	Port Name	Connector	Description
1	AUDIO OUT	Audio input and output	RCA	Outputs audio signal to such external devices as speaker.
2	AUDIO IN			Inputs analog audio signal from such devices as pick-up.
3	LAN	Network	Ethernet port	Connects to standard Ethernet cable.
4	ALARM-NO	Alarm output	Alarm devices, such as smoke	Outputs alarm signals to alarm devices.
	ALARM_COM			
	ALARM_IN1	Alarm input		

	ALARM_IN2		detector, and alarm siren.	Receives the on-off signal of external alarm source.
	ALARM_GND	Alarm ground		Ground port.
5	POWER	Power input	—	Inputs 12V DC voltage.  Refer to the labels attached to the Camera; otherwise the Camera might be damaged.
6	RS-485	RS-485 port	—	Connects to external RS-485 device.

3 Basic Configuration

- Configure network before installation or insert SIM card during installation to access 4G network.
- The figures in the manual are for reference only, and might differ from the actual interface. For more details, see *Thermal Hybrid Camera_Web Operation Manual*.

3.1 Initializing Camera

Initialize the Camera through ConfigTool or by logging in to the web interface with default IP after connecting the Camera to PC.

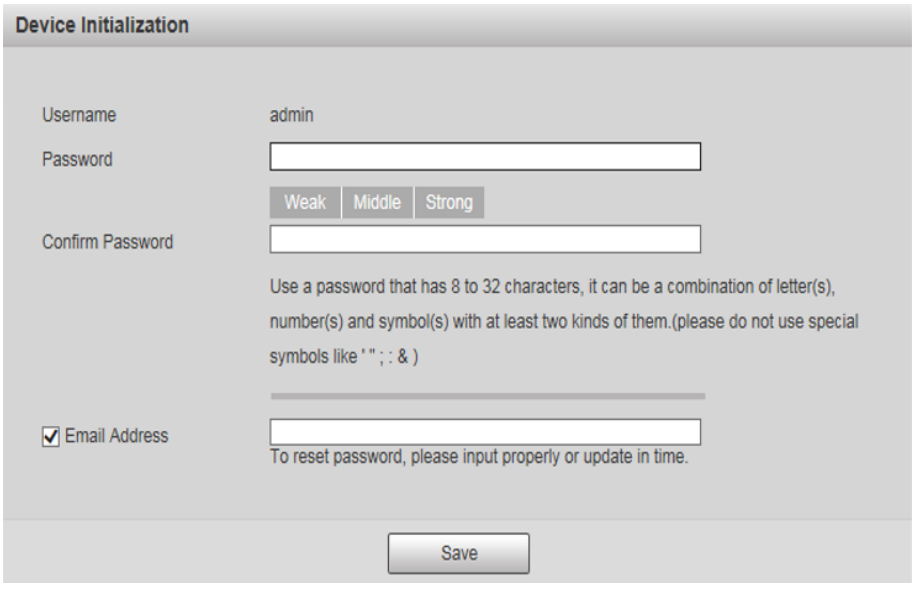
- Use ConfigTool when you want to initialize cameras in batches.
- Use web interface to initialize a single camera.

This section takes single camera initialization on the web as an example.

- Initialize the Camera for first-time use or after factory resetting.
- To secure the Camera data, keep admin password well after initialization and modify it regularly.
- Make sure the Camera IP address (192.168.1.108 by default) and PC IP address are in the same network segment.

Step 1 Open browser, enter Camera default IP address in the address bar, and then press the Enter key.

Figure 3-1 Initializing camera



Step 2 Configure the information.

- Set a password for the admin account and link your email address.

- Enter an email address to reset password when needed. This option is selected by default. After you scan the QR code for password reset, a security code will be sent to the entered email address to reset the admin password.

Step 3 Click **Save**.

3.2 Modifying IP Address

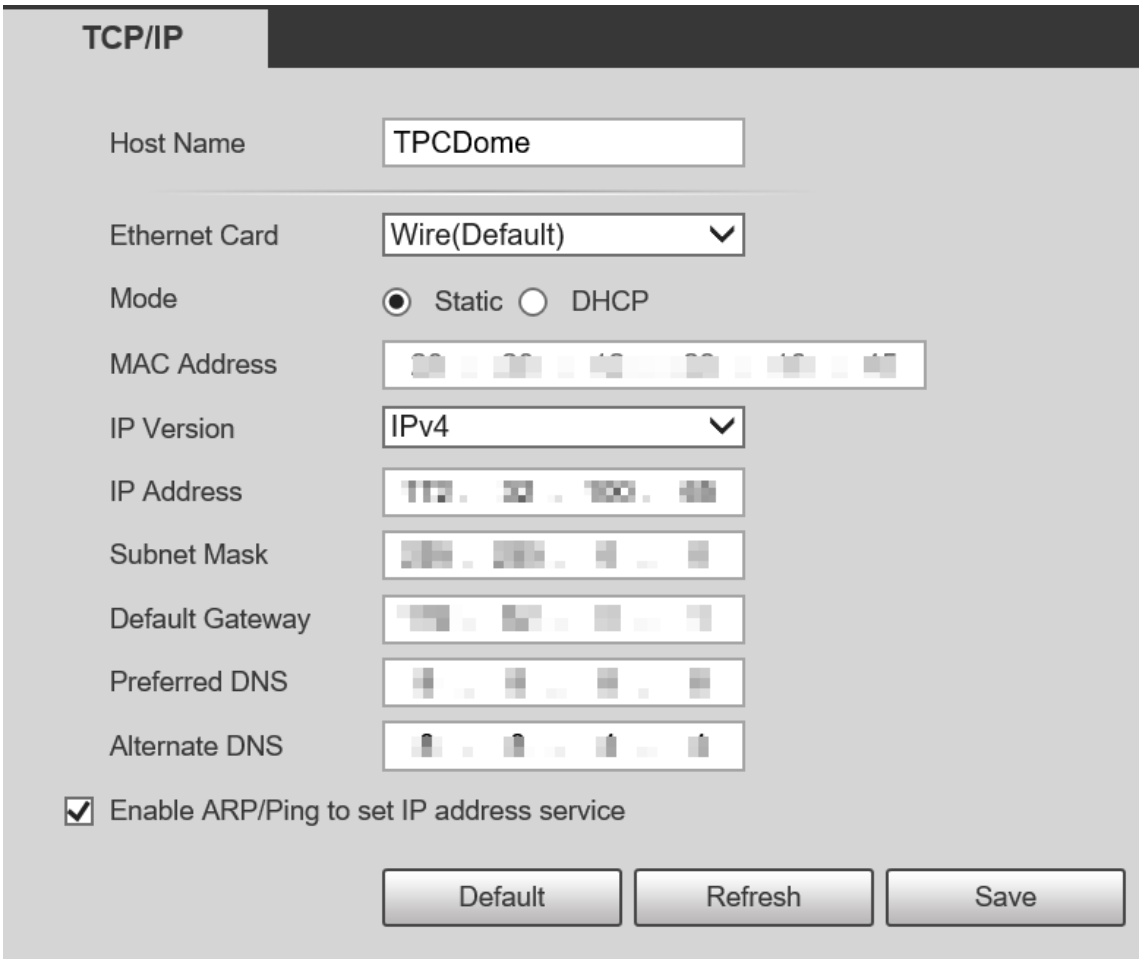
Set an IP address fitted to the actual network segment to make the Camera access network.

Step 1 Log in to Camera web interface.

Step 2 Select **Setting** > **Network** > **TCP/IP**.

Step 3 Configure IP related parameters.

Figure 3-2 TCP/IP



Step 4 Click **Save**.

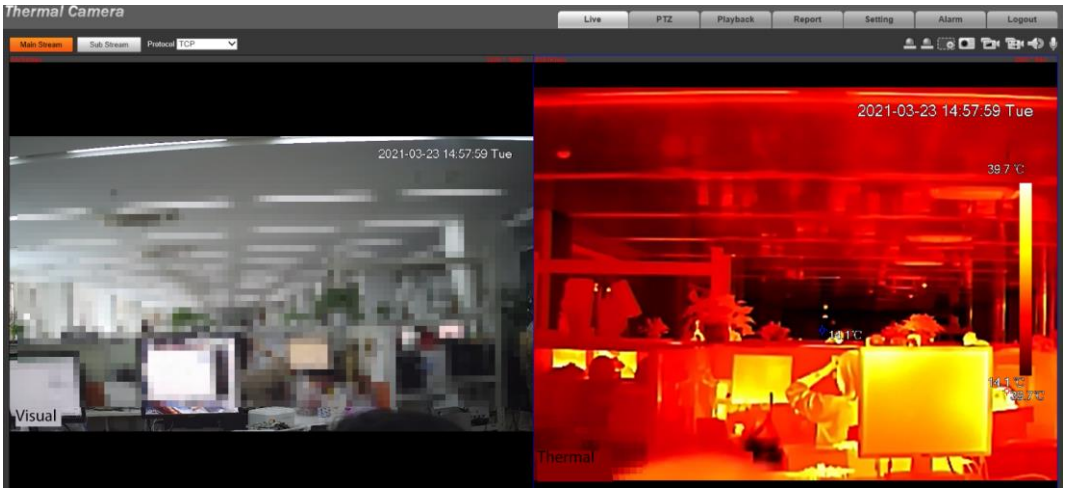
3.3 Viewing Live Image

Ensure the Camera can be accessed and live image can be viewed normally after configuring network.

Log in to the Camera web interface with the configured IP address.

When logging in for the first time, you will be prompted to install a plug-in. Save and install it. After that, the interface will be automatically refreshed. Then, live image will show up.

Figure 3-3 Web main interface



4 Installation

4.1 Preparation

4.1.1 Selecting Installation Place

- Make sure the place where the Camera is installed has enough space to hold the Camera and its mounting accessories.
- Make sure the wall and column can bear at least 8 times the total weight of the Camera and its mounting accessories.

4.1.2 Selecting Cable

Power cord

To extend the power cord you have received, evaluate the distance you want to extend and select the appropriate cord diameter.

Make sure the voltage is 12V DC and transmission power is 10 W.

Table 4-1 Power cords

Diameter (mm)	Maximum Transmission Distance [ft (m)]
0.800	61.06 (18.61)
1.000	95.41 (29.08)
1.250	149.08 (45.44)
2.000	381.66 (116.33)

Signal Cable

To extend signal cable you have received (such as alarm input/output cable and RS-485 cable), use 0.56 mm (24AWG) and above.

4.2 Camera Installation

WARNING

During installation, avoid objects such as the Camera, components and tools falling off; otherwise people, animals, other objects or the Camera might be injured.

4.2.1 (Optional) Installing Micro SD Card

Install SD card to save recordings to local storage.

- Cut off power before Micro SD card installation.
- Do not press the reset button during installation. Press and hold the reset button for 4–5 seconds and the Camera will be restored to factory default settings. Think twice before enabling the function.
- Before closing and fastening the protective cover, make sure waterproof ring is well placed; Otherwise, it will affect waterproof performance of the Camera.

Figure 4-1 Micro SD card and reset button

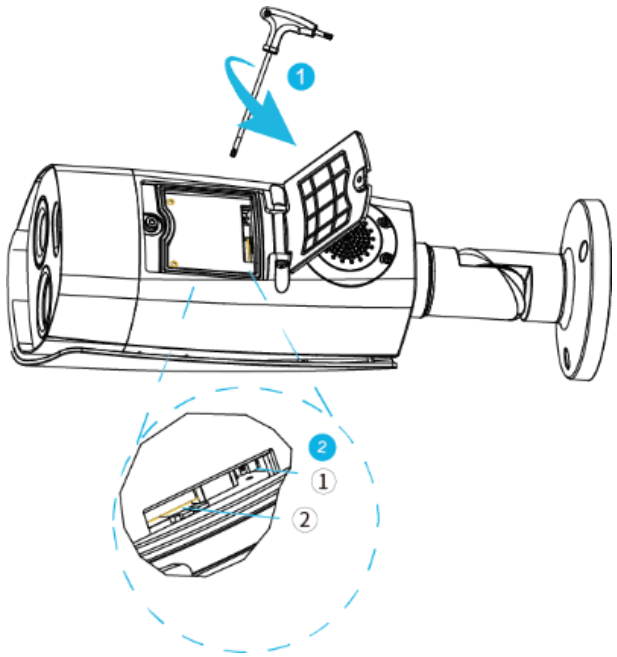
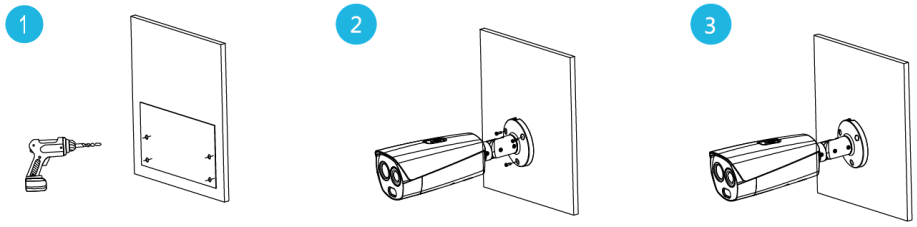


Table 4-2 Micro SD card and reset button

No.	Item Name	No.	Item Name
1	Reset button	2	Micro SD card slot

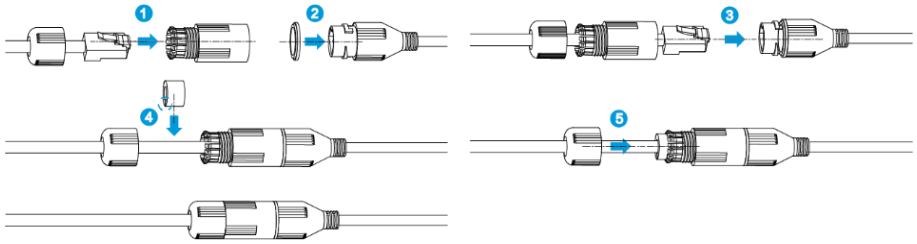
4.2.2 Fixing Camera

Figure 4-2 Fix camera



4.2.3 (Optional) Installing Waterproof Connector for Network Cable

Figure 4-3 Install waterproof connector for network cable

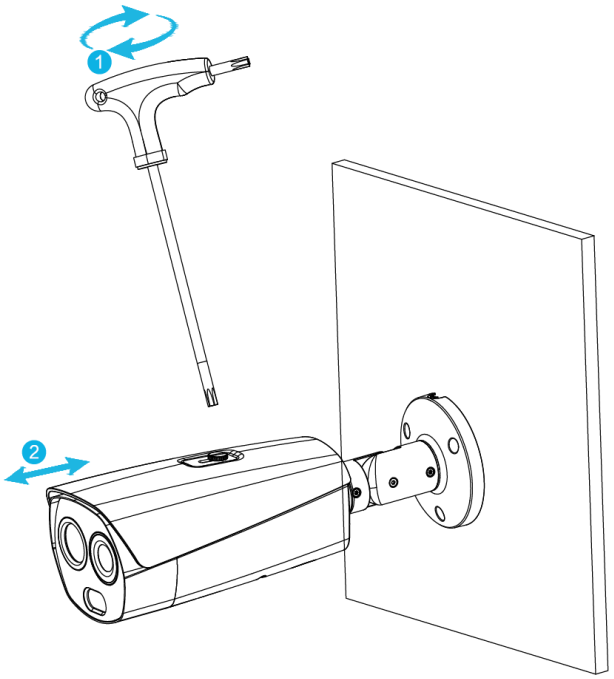


4.2.4 Connecting Cables

Connect cables, such as power, RS-485, and alarm I/O port, and then wrap the connectors of cables with waterproof insulating tape. For more details, see "2.2 Cables".

4.2.5 Adjusting Sunshield

Figure 4-4 Adjust sunshield



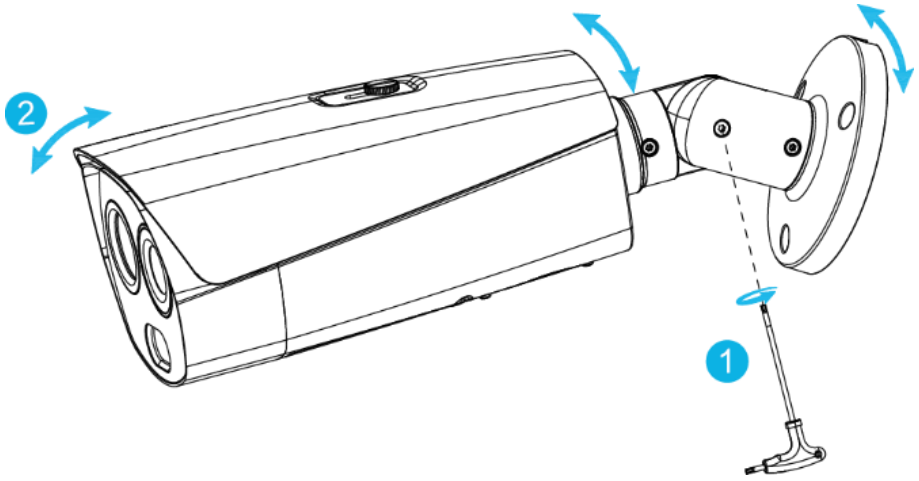
4.2.6 Adjusting Camera

⚠

Make sure loosen the screws before adjusting the angles of the camera, and then tighten them.

Avoid rotating the Camera 360° when the Camera and the pedestal are in a 90° angle with the screws tightened.

Figure 4-5 Adjust camera



5 Alarm Configuration

5.1 Alarm Input and Output Connection

Cut off power before connecting cables.

Step 1 Connect alarm input device to alarm input port of I/O cable.

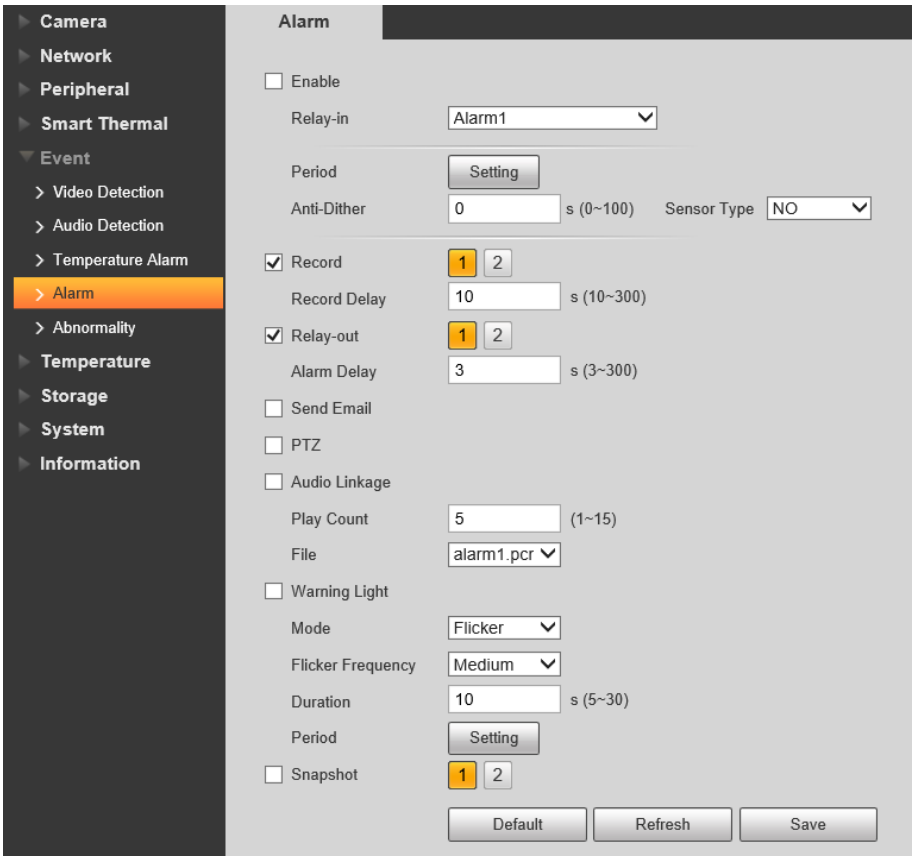
Step 2 Connect alarm output device to alarm output port of I/O cable.

Alarm output port is relay switch output, and the alarm output port can only be connected to normally open (NO) alarm sending device.

Step 3 Log in to the web interface and then select **Setting** > **Event** > **Alarm**.

Step 4 On the **Alarm** interface, configure settings for alarm input and output, and then click **Save**.

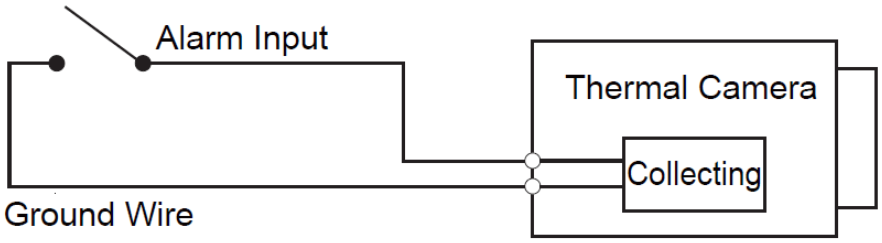
Figure 5-1 The alarm interface



- In the **Relay-in** list, select the alarm input port of I/O cable. Set the sensor type as NO if alarm input device generates high electrical level when alarm occurs, and NC if it generates low electrical level.
- In the **Relay-out** list, select the alarm output port of I/O cable.

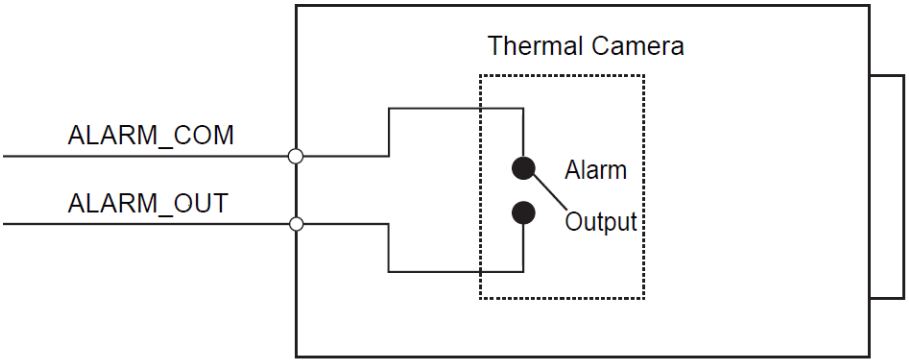
5.2 Working Theory

Figure 5-2 Alarm input



Alarm input: When input signal is 3.3 V or idle, the Camera collects logic "1"; when input signal is grounded, the Camera collects logic "0."

Figure 5-3 Alarm output



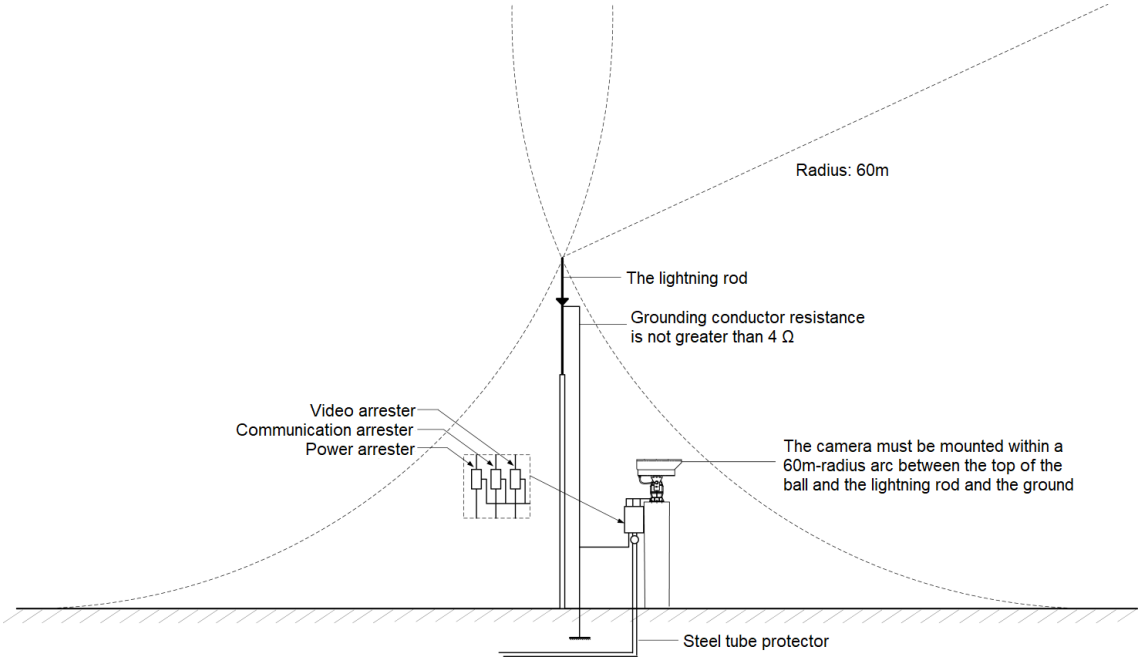
Alarm output: Port ALARM_OUT and ALARM_COM form a switch to provide alarm output. Normally the switch is on; the switch will be off when there is alarm output.

Appendix 1 Lightning and Surge Protection

The Camera adopts TVS lightning protection technology. It can effectively prevent damage from various pulse signals below 6000 V, such as a sudden lighting and surge. However, you still need to take necessary precaution measures in accordance with your local electrical safety code when installing the Camera in outdoor environment.

- The distance between the signal transmission cable and high-voltage device (or high-voltage cable) shall be at least 50 m.
- Outdoor cable layout shall go under the penthouse if possible.
- For vast land, use sealing steel tube under the land to implement cable layout and make sure that both ends of the tube are equipotentially grounded. Open floor cable layout is forbidden.
- For vast land, install a 10 KA lightning rod near the Camera's power input port and Ethernet port. For Camera with AC to DC power adapter, install a 10 KA lightning rod near the output port of the adapter.
- For Camera installed on iron tower, if there is a high-performance grounding bar on the tower, connect the Camera grounding wire to the bar. If there is no grounding bar, use multiple copper cable whose cross-sectional area are not less than 16 mm^2 to connect the Camera grounding wire to the ground.
- Make sure that the Camera is over 3 m away from the top point of tower lightning rod and within protection area against direct lighting.
- In area of strong thunderstorm or near high induced voltage (such as near high-voltage transformer substation), install additional high-power thunder protection device or lightning rod.
- The thunder protection and earth grounding of the outdoor devices and cables shall be considered based on the whole thunder protection of the building and conform to your local or industry standards.
- The system shall adopt equal-potential wiring. The grounding devices shall meet anti-jamming requirements and at the same time conforms to your local electrical safety code.
- The grounding devices shall not be connected to N (neutral) line of high voltage power grid or mixed with other wires. When you connect the system to the ground alone, the grounding resistance shall not be more than 4Ω and the cross-sectional area of grounding cable shall be no less than 25 mm^2.

Appendix Table 1-1 Install lightning protection



Appendix 2 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

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

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.