Thermal Network Hybrid Thermography Cube Camera

Quick Start Guide

V1.0.0

Foreword

General

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

Safety Instructions

The following signal words 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, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	October 2021

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations

and technical data. 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, comply with the guidelines when using it, and keep the manual safe for future reference.

Installation and Maintenance Professionals Requirements

- All maintenance professionals must have qualification certificates or experience installing and maintaining CCTV systems, electric apparatus in explosive gas environments and working at heights. They must also have to acquire basic knowledge and installation skills in:
  - CCTV systems.
  - Low voltage wiring and low voltage electronic circuit wire connection.
  - Electric apparatus installation and maintenance in hazardous sites.

Power Requirements

- All installation and operation should conform to your local electrical safety code.
- Make sure that the power supply is correct before operating the Camera.
  - Note that the power supply requirements are subject to the device label.
  - Use the power adapter or case power supply provided by the device manufacturer.
  - The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2.
- Install an easy-to-use device for power off before installing wiring, which is for emergency power off when necessary.
- Prevent the line cord from being trampled on or squeezed, especially the plug, power socket and the junction from the Camera.

Application Environment Requirements

- Please use the device within the allowed humidity (< 95% RH) and altitude (< 3000 m).
- Store and transport the Camera within the allowed humidity and temperature conditions.
- Do not use the device in the corrosive environment such as high salt fog area (sea, beach and coastal area), acid gas environment and chemical plants.
- Do not use the device in the strong vibration environment such as in boats and vehicles.

⚠

If you still want to use thermal cameras in the conditions mentioned above, please contact our sales staff to buy cameras of special model or cameras that are customized. If you use cameras in improper environments, we shall not take the costs of camera damage.

- Do not place the device in a humid, dusty or extremely hot or cold site that has strong electromagnetic radiation or unstable illumination.
- Do not block the ventilation of the Camera to avoid heat accumulation.
- Do not install the Camera near a heat source such as a radiator, heater, or stove to avoid fire.
- Do not aim the lenses at intense radiation sources (such as the sun, a laser or molten steel) to avoid damage to the thermal detector and visual lens.
- Prevent liquid from flowing into the Camera to avoid damage to the internal components. In case the liquid enters the Camera, immediately stop using the Camera, cut off the power, and

disconnect all the cables, and then contact your local customer service center.

- Do not stuff foreign materials into the Camera to prevent a short circuit which could result in the Camera being damaged or people becoming injured.
- Use the factory default package or material of equal quality to pack the Camera when transporting it.
- Do not squeeze, violently vibrate or immerse the device in liquid.

Operation and Maintenance Requirements

- Do not touch the heat dissipation component of the Camera or you might get burnt.
- Do not dismantle the Camera. The internal components can only be repaired by a qualified professional. Dismantling it without professional assistance might cause water seeping in or might result in the Camera producing poor quality images.
- Do not touch the photosensitive Camera with your hands. Use an air blower to clean the dust on the lens. For deeper cleaning, pour a little alcohol on to a piece of dry cloth and then softly wipe the dirt away.
- Clean the Camera body with a piece of soft dry cloth. For any dirt that is hard to remove, pick up a piece of clean and soft cloth, dip it into a little neutral detergent and gently wipe the dust away. After that, wipe away all the remaining liquid on the Camera with another dry cloth. Never use volatile solvents such as alcohol, benzene and thinner, or cleaners that are strong and abrasive. Otherwise, the Camera’s surface coating will be damaged and its working performance will be encumbered.
- After unpacking, the problems that the packaging bag is damaged, leaking, or the desiccant particles in the packaging bag are of different colors will not affect the normal use of the Camera.

⚠ **WARNING**

- Use the accessories regulated by the manufacturer. The Camera should be installed and maintained by qualified professionals.
- Make sure that the surface of the Camera is not irradiated from laser when using laser product.
- Do not provide two or more power supply modes to the Camera, otherwise the Camera might sustain damage.
- If the Camera malfunctions, contact your local customer service center. Do not dismantle the Camera.

Table of Contents

1 Checklist

Check the package according to the following checklist. If you find something has been damaged or is missing, contact customer service.

The bracket and drill required for the installation process do not come with the delivery. Please buy them if they are needed.

Keep accessories safe for future use.

Figure 1-1 Checklist

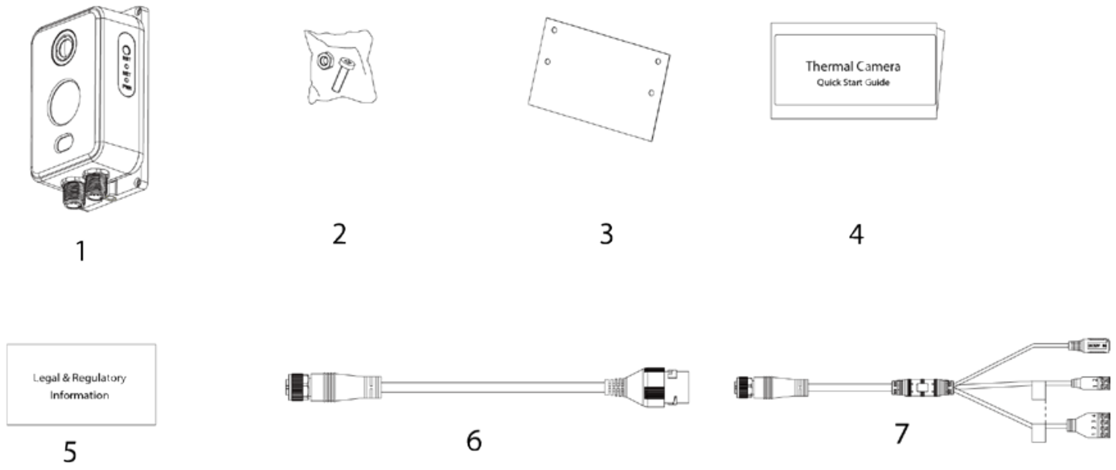


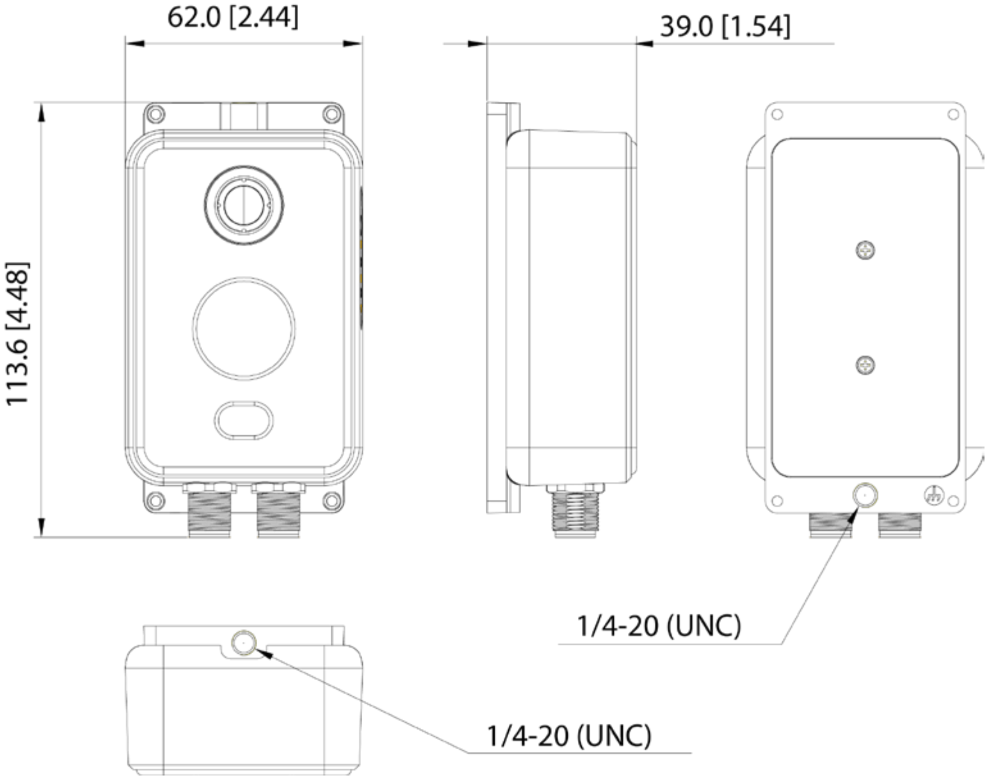
Table 1-1 Checklist

No.	Name	Quantity	No.	Name	Quantity
1	Thermal network hybrid thermography cube camera	1	5	Legal and regulatory information	1
2	Accessory bag	1	6	Network cable	1
3	Positioning map	1	7	Other cable	1
4	Quick start guide	1	—	—	—

2 Design

2.1 Dimensions

Figure 2-1 Component dimensions (mm [inch])



2.2 Cables

The following figure of the cable is for reference only, and might differ from the actual product.

Figure 2-2 External cable (1)

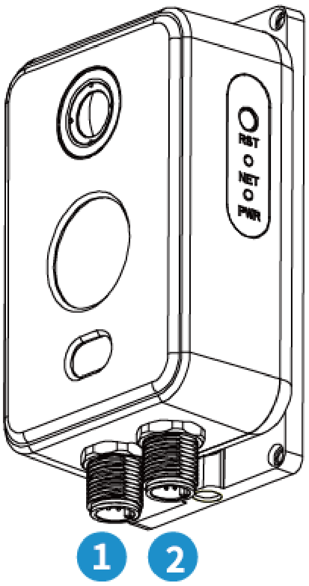


Figure 2-3 External cable (2)

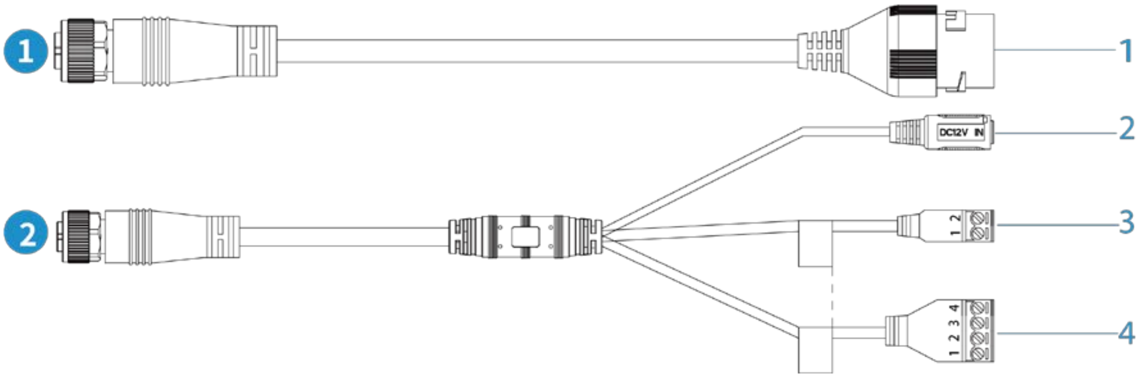


Table 2-1 Ports description

No.	Port	Port Name	Connector	Description
1	LAN	Network port	Ethernet port	Connects to standard Ethernet cable.
2	POWER	Power input port	—	Inputs 12 VDC. ⚠ Supply power to the device according to the label to avoid damages to the Camera.
3	RS-485	RS-485 port	—	Connects to external RS-485 devices.
4	ALARM_OUT	Alarm output port	Alarm devices, such as smoke detectors and sirens.	Alarm output port. Outputs alarm signals to alarm devices.
	ALARM_IN	Alarm input port		Alarm input port. Receives on-off signals from external alarm devices.
	GND	Alarm ground		Connects to the ground.

3 Basic Configuration

- We recommend you install the Camera before configuring the network.
- The figures in this 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

You can initialize the Camera through the ConfigTool, or by connecting the computer to the Camera, and logging in to the web interface with the default IP address.

- To initialize multiple devices at the same time in batches, use the ConfigTool.
- To initialize one device at a time, log in to the web interface.

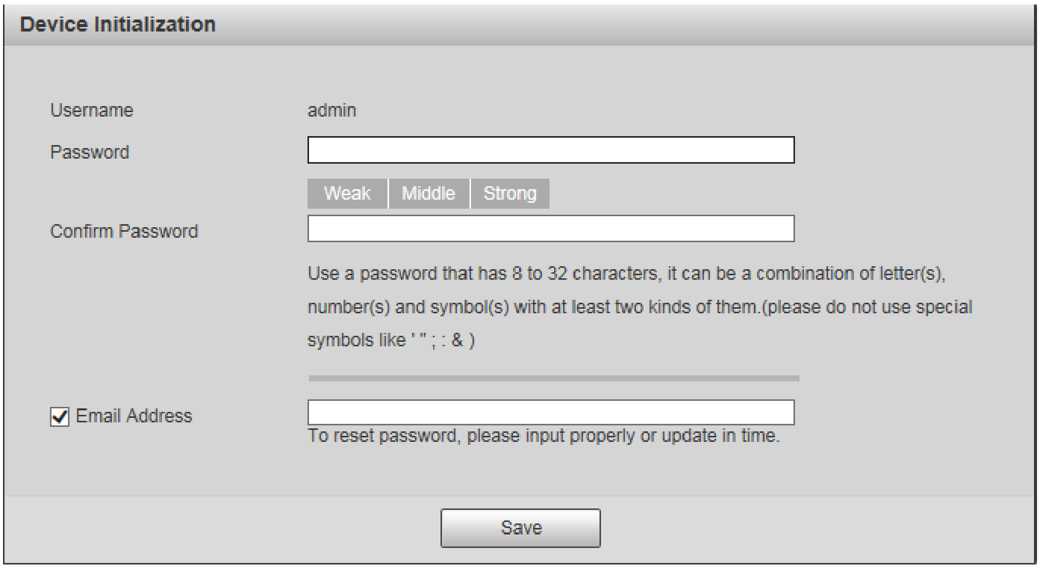
- Initialize the device for first-time use after performing a factory reset.
- To keep the data on the Camera secure, keep the admin password safe after initialization and regularly change it.
- Make sure the Camera IP address (192.168.1.108 by default) and the IP address of the computer are on the same network segment.

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

Step 2 Set the login password of admin and the email address.

- The email address is for password reset.
- We recommend entering your email address in case you forget the password and need to reset the password.

Figure 3-1 Device initialization



Device Initialization

Username admin

Password

Confirm Password

Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them.(please do not use special symbols like ' " ; : &)

☑ Email Address

To reset password, please input properly or update in time.

Step 3 Click **Save** to complete initialization.

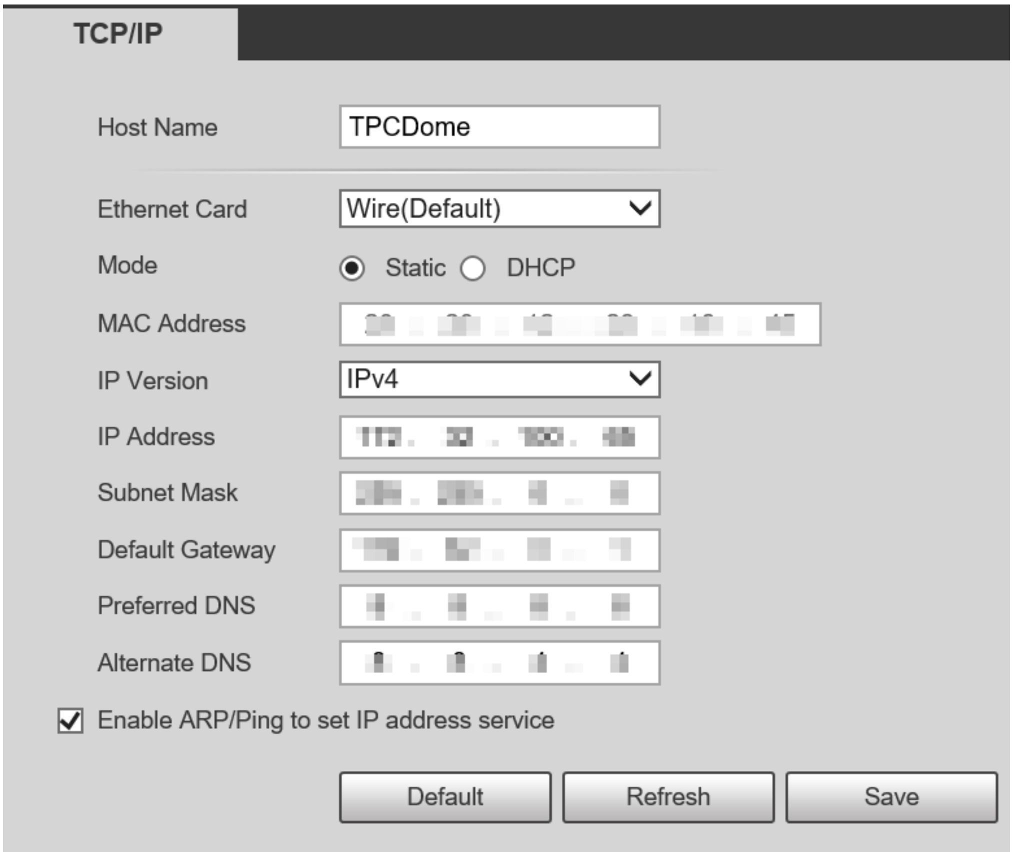
3.2 Modifying IP Address

Set the IP address for the network segment to allow the Camera to access the network.

Step 1 Log in to the Camera web interface.

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

Figure 3-2 TCP/IP



TCP/IP

Host Name	TPCDome
Ethernet Card	Wire(Default)
Mode	● Static ○ DHCP
MAC Address	[redacted]
IP Version	IPv4
IP Address	[redacted]
Subnet Mask	[redacted]
Default Gateway	[redacted]
Preferred DNS	[redacted]
Alternate DNS	[redacted]

☑ Enable ARP/Ping to set IP address service

Step 3 Configure IP related parameters.

Step 4 Click **Save**.

3.3 Live Video

The web interface might differ depending on the device. Figures in this guide are for reference only.

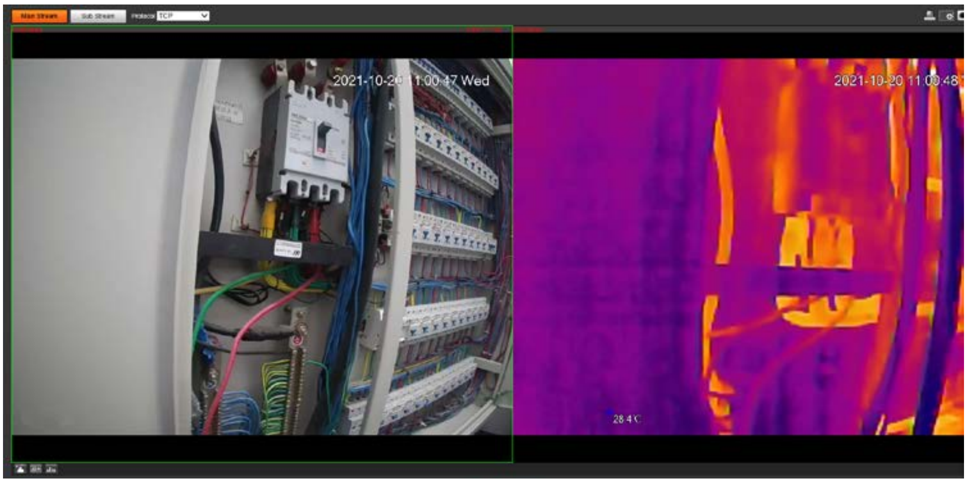
Step 1 Log in to the web interface of the Camera.

The default username is admin, and the password is the one that was set during initialization.

Step 2 Click **Login,** and then the system will display the home page.

You will be prompted to install a plug-in for first-time system login. Please download and install the plug-in. The web interface will refresh automatically after the plug-in is installed, and then the live video will be displayed.

Figure 3-3 Live video



4 Installation

4.1 Preparations

4.1.1 Checking Installation Space and Intensity

- Make sure the place where the Camera is installed has enough space to hold the Camera and its mounting accessories.
- Make sure the mounting platform can sustain at least 8 times the weight of the Camera and its mounting structural components.

4.1.2 Cable Preparation

Power Cord

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

Table 4-1 Power cord description

Distance [ft (m)]	Wire Diameter [inch (mm)	Area [in^2 (mm^2)]	Material
32.81 (10)	0.035 (0.9)	0.001 (0.63)	Hard copper wire
49.21 (15)	0.043 (1.1)	0.0015(0.95)	
65.62 (20)	0.051 (1.3)	0.0021 (1.32)	

Other Signal Cable

For all other signal cables (such as alarm input and output, RS-485), we recommend you use wires that have a diameter of 0.56 mm (24 AWG) and above for the signal cable.

4.2 Installing Camera

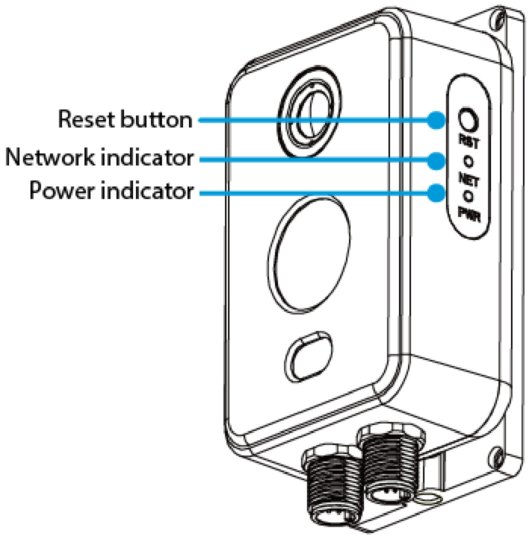
WARNING

Avoid dropping objects such as parts and tools of the Camera from high altitudes during installation to avoid people getting hurt and the Camera being damaged.

4.2.1 Restoring to Default Settings

Press the reset button for more than 10 s to reset the Camera to factory settings.

Figure 4-1 Component



Network indicator: It flashes orange when the network is connected.

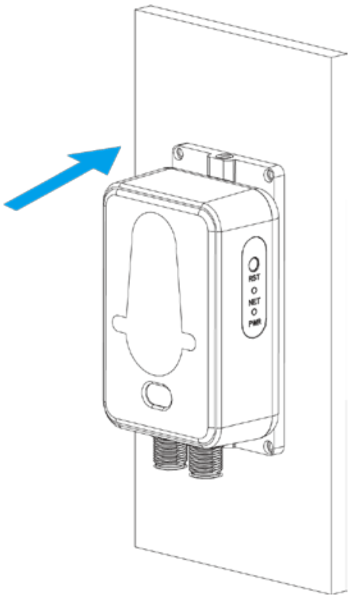
Power indicator: Before the Camera starts, it is red when powering up. After the Camera starts, it turns to green.

4.2.2 Installation procedure

4.2.2.1 Magnetic Installation

The Camera is equipped with a magnet on the rear panel. The Camera can be installed and attached to ferromagnetic objects.

Figure 4-2 Magnetic installation



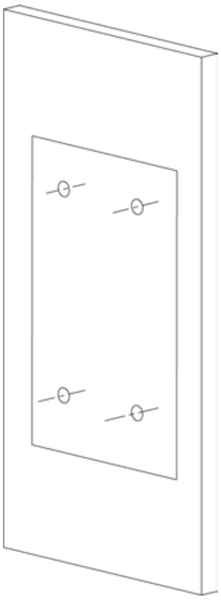
4.2.2.2 Surface installation

You can install the Camera with screws and nuts that come with the Camera.

Step 1 Paste the positioning map.

Choose a suitable mounting surface, and then paste the positioning map to the surface. Drill the holes according to the label signs.

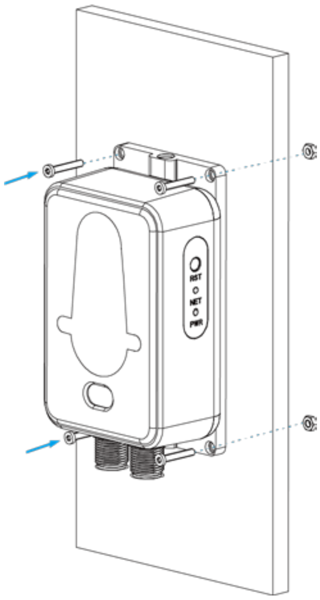
Figure 4-3 Paste the positioning map



Step 2 Secure the Camera.

Align the holes on both the rear panel and the mounting surface, and then secure the Camera with M2.5 × 10 screws and M2.5 nuts.

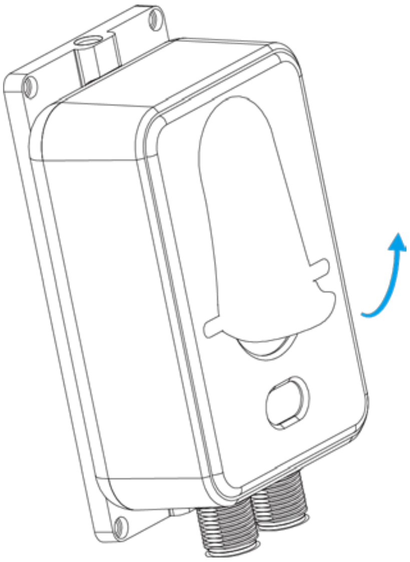
Figure 4-4 Secure the Camera



Step 3 Remove the label.

After attaching the Camera to the mounting surface, remove the label from the lens.

Figure 4-5 Remove the label



5 Alarm Configuration

The Camera can link to alarm output devices to report alarms when alarms are triggered from external alarm input devices.

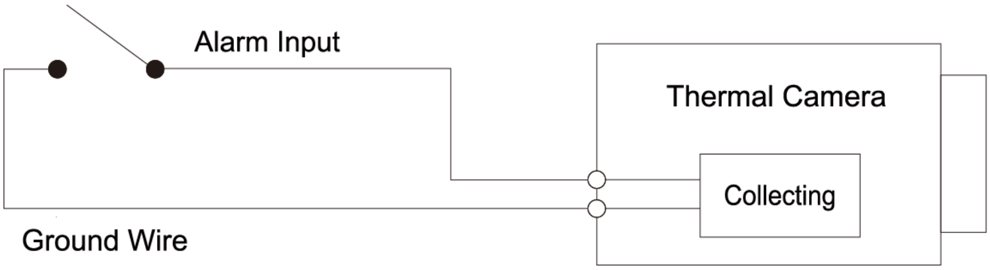
Cut off the power before connecting the cables.

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

Alarm input: Receives on-off signals from external alarm devices, and supports NO and NC alarm input. The input signal is idle or grounded, and the Camera can collect different states of the alarm input port.

- When the input signal is 3.3 V or idle, the Camera collects logic "1".
- When the input signal is grounded, the Camera collects logic "0".

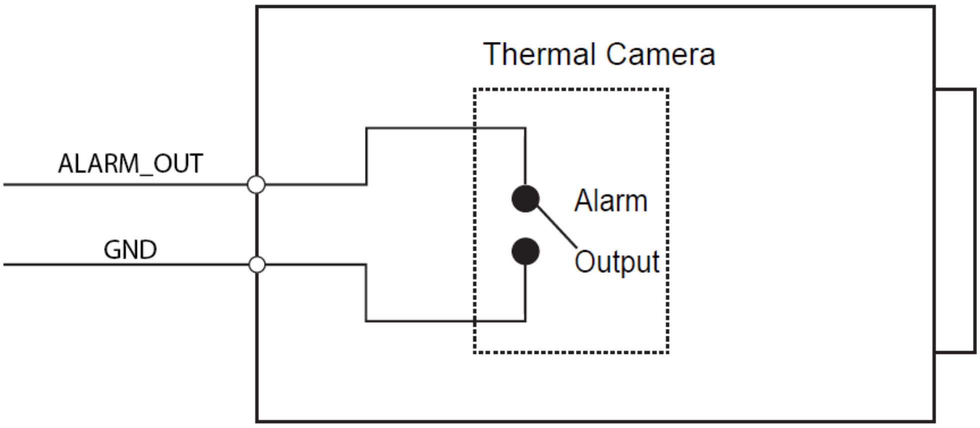
Figure 5-1 Alarm input



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

Alarm output: Port ALARM_OUT and GND form a switch to provide alarm output. The switch is normally on and has a high resistance. ALARM_OUT is connected to ground when there is an alarm output.

Figure 5-2 Alarm output

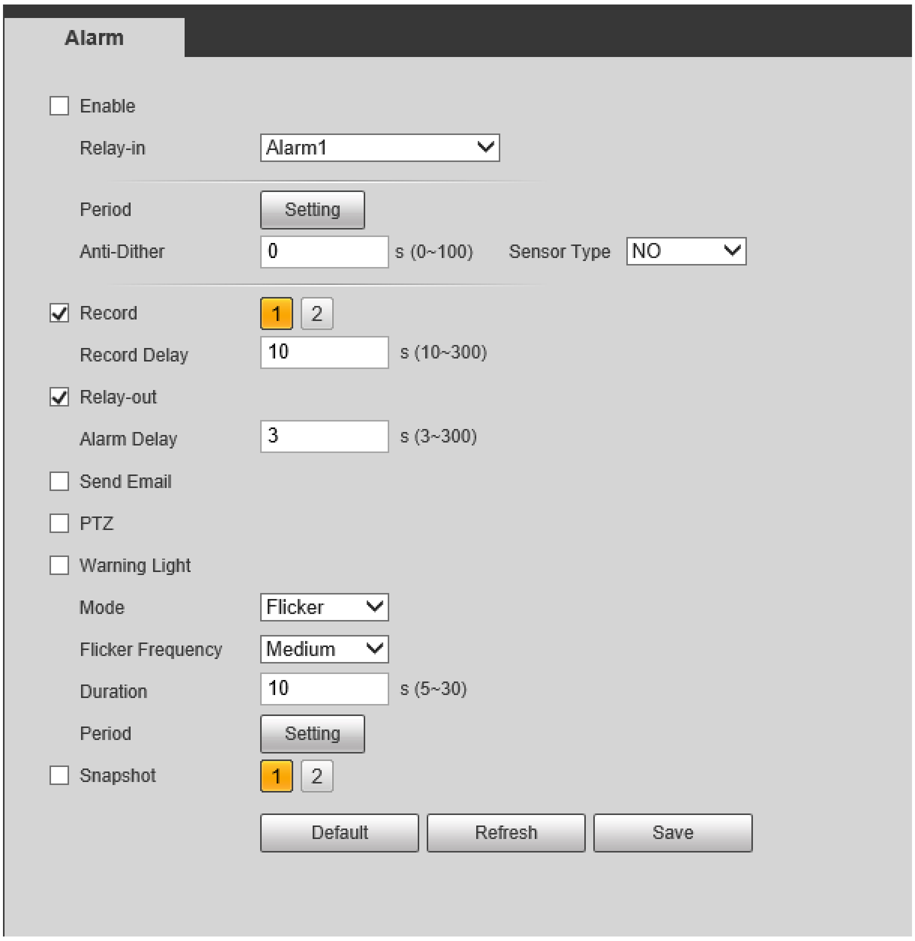


Step 3 Log in to the web interface, and then select **Setting** > **Event** > **Alarm**.

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

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

Figure 5-3 Alarm setting



Alarm

□ Enable

Relay-in: Alarm1

Period: Setting

Anti-Dither: 0 s (0~100) Sensor Type: NO

☑ Record: 1 2

Record Delay: 10 s (10~300)

☑ Relay-out

Alarm Delay: 3 s (3~300)

□ Send Email

□ PTZ

□ Warning Light

Mode: Flicker

Flicker Frequency: Medium

Duration: 10 s (5~30)

Period: Setting

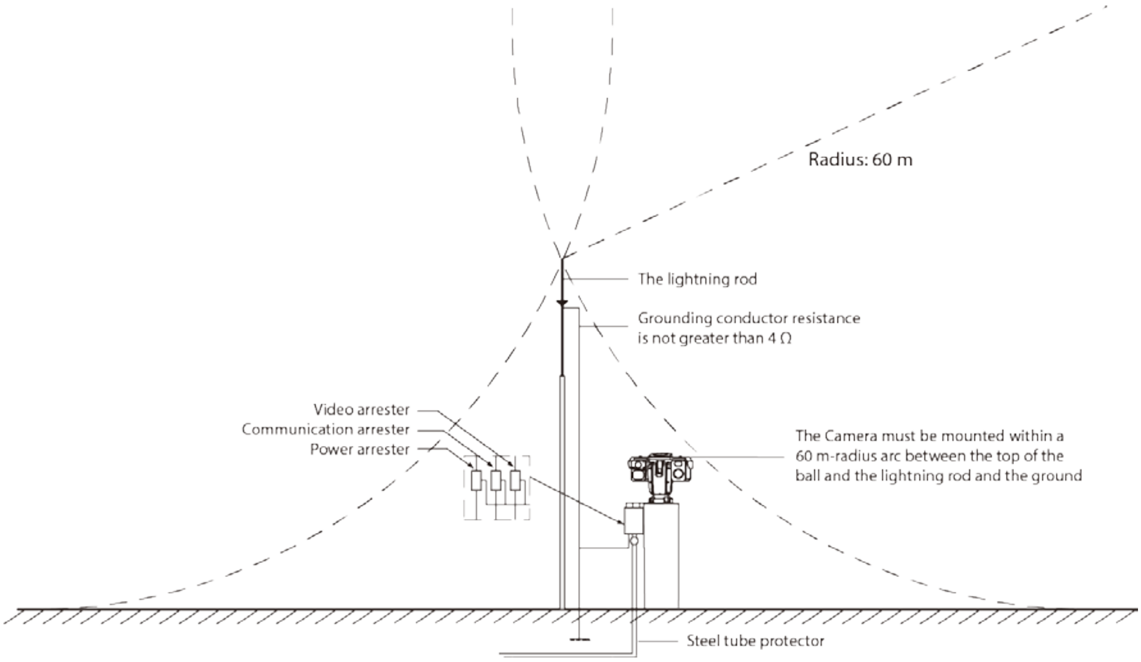
□ Snapshot: 1 2

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 lightning 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 into 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 lightning.
- In area of strong thunderstorm or near high sensitive 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.

Figure 1-1 Lightening protection


Radius: 60 m
The lightning rod
Grounding conductor resistance
is not greater than 4 Ω
Video arrester
Communication arrester
Power arrester
The Camera must be mounted within a
60 m-radius arc between the top of the
ball and the lightning rod and the ground
Steel tube protector

Appendix 2 Cybersecurity Recommendations

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 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.