Thermal Network Mini Hybrid Eyeball Camera

Quick Start Guide

V1.0.1

Foreword

General

This manual introduces the functions and operations of the "thermal network mini hybrid eyeball 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

Version	Revision Content	Release Time
V1.0.1	Updated name: thermal network mini hybrid eyeball camera.	December 2020
V1.0.0	First release.	February 2020

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 regions. For detailed information, see 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, please refer to our 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 occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

In the manual, "thermal network mini hybrid eyeball camera" is referred to as "the Camera." 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 it well for future reference.

Installation and Maintenance Professionals Requirements

All the installation and maintenance professionals must have qualification certificates or experiences of installing and maintaining CCTV system, electric apparatus in the explosive gas environment 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.
- Electric apparatus installation and maintenance in hazardous sites.

Power Requirements

- All installation and operation should conform to your local electrical safety code.
- Check whether the power supply is correct before operating the Camera.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Note that the power supply requirement is subject to the Camera label.
- Install easy-to-use Camera for power off before installing wiring, which is for emergent power off when necessary.
- Prevent the line cord from being trampled or pressed, especially the plug, power socket and the junction from the Camera.

- Risk of explosion if the battery is replaced by an incorrect type.
- Replacement of a battery with an incorrect type that can defeat a safeguard (for example, in the case of some lithium battery types).
- Disposal of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery can result in an explosion.
- High or low extreme temperatures that a battery can be subjected to during use, storage or transportation; and low air pressure at high altitude.
    - ◇ Leaving a battery in an extremely high temperature surrounding environment that can result in an explosion or the leakage of flammable liquid or gas.
    - ◇ A battery subjected to extremely low air pressure that may result in an explosion or the leakage of flammable liquid or gas.

Application Environment Requirements

- Use the Camera within the allowed humidity (<95% relative humidity) and altitude (<3000 m).

- Do not use the Camera in the strong vibration environment such as in boats and vehicles.

If you still want to use thermal cameras in the two 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 Camera in the humid, dusty, extremely hot and cold site with strong electromagnetic radiation or unstable illumination.
- Do not block the ventilation of the Camera to avoid hear accumulation.
- Do not install the Camera near the heat source such as radiator, heater, and 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 the liquid entering the Camera, immediately stop using the Camera, cut off the power, and disconnect all the cables. 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 transportation, storage and installation.

Operation and Maintenance Requirements

- Do not touch the heat dissipation component of the Camera in case you might get burnt.
- Do not dismantle the Camera; there is no part which can be repaired by users themselves. 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 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.

WARNING

- Modify the default password after login to prevent from being stolen.
- Use the accessories regulated by the manufacturer. The Camera should be installed and maintained by professionals.
- Internal and external ground connection should be stable.
- Do not provide two or more power supply modes to the Camera, otherwise, it may cause damage to the Camera.

- A 2.5 m control cable is provided when the Camera leaves factory. It should use explosion-proof flexible tube or armor cable to protect when the control cable is connected to the explosion-proof control cabinet.
- Cut off power before Camera maintenance and overhaul. Opening the cover with power on in the explosion environment is prohibited.
- Make sure all the explosion-proof components and parts are complete without any cracks and there is no defect which might affect explosion-proof performance.
- Contact the local dealer or the nearest service center if the Camera fails to work normally. Do not dismantle or modify the Camera.

Table of Contents

1 Packing List

Check the package according to the following checklist. If you find device damage or any loss, contact the after-sales service. In the manual, "thermal network eyeball camera" is referred to as "the Camera."

Figure 1-1 Package items

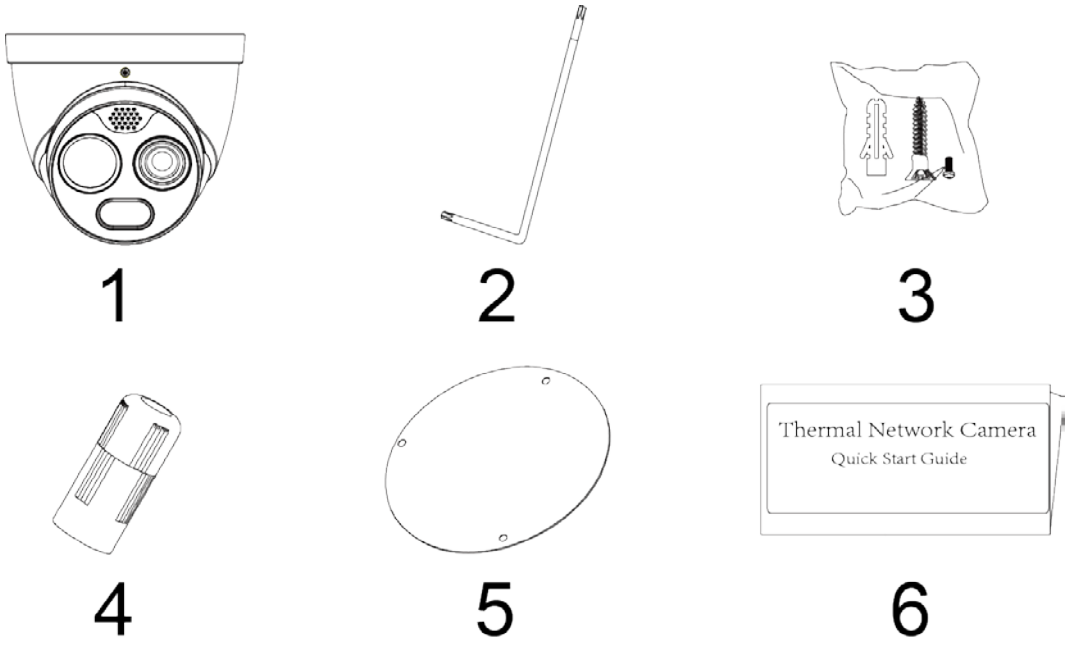


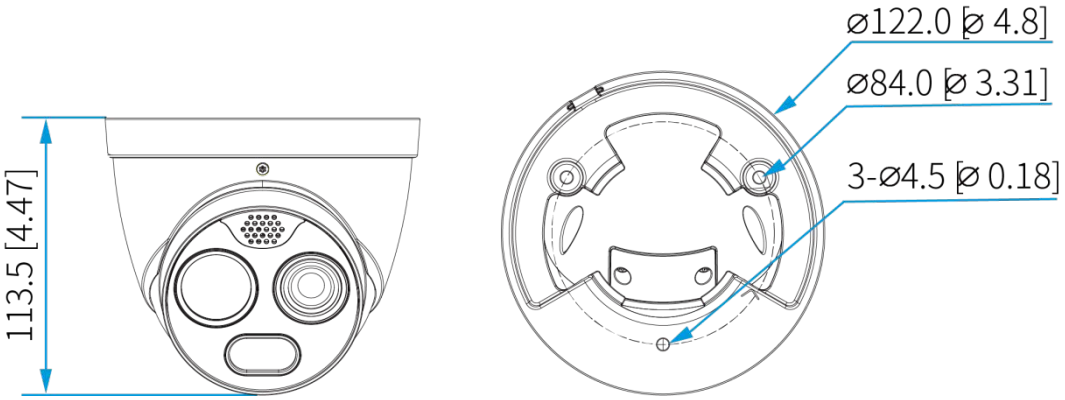
Table 1-1 Checklist

No.	Item	Quantity
1	Thermal network eyeball camera	1
2	Wrench	1
3	Screws	1
4	Water-proof connector	1
5	Positioning map	1
6	Quick start guide	1

2 Design

2.1 Dimensions

Figure 2-1 Dimensions (mm [inch])



2.2 Cables

Figure 2-2 Cables

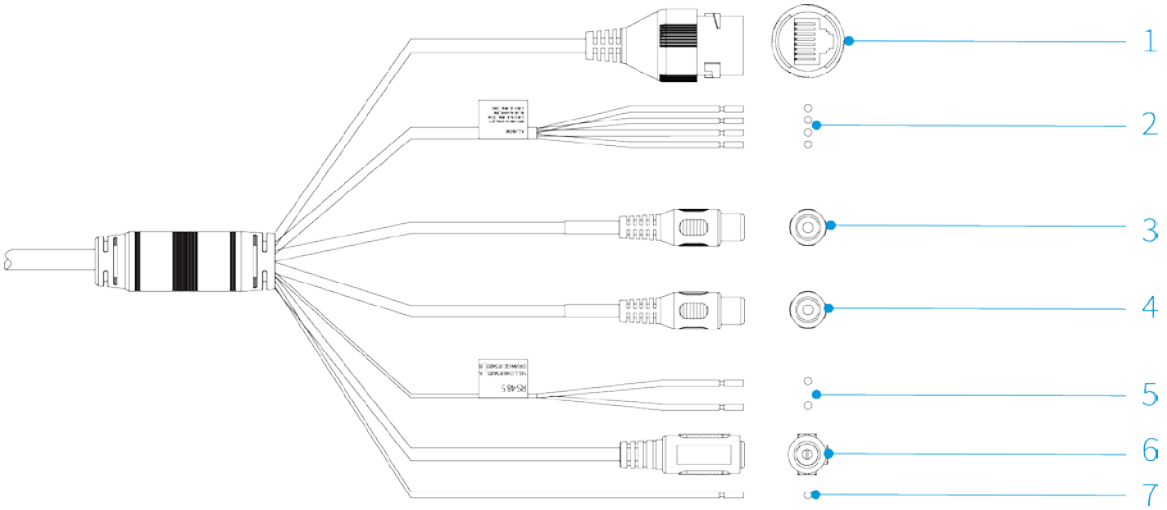


Table 2-1 Ports description

No.	Port	Description
1	LAN	Connects to Ethernet cable.
2	Alarm IN1	Inputs signals from an alarm detection device such as a smoke detector. When smoke detector is triggered, it makes sounds and meanwhile transmits alarm signals to Camera for the Camera to start the corresponding linkage such as Snapshot and Send Email (see "5 Configuring Alarm" for details).
	ALARM_NO	Connect ALARM_NO and ALARM_COM altogether to an alarm sending device to deliver an alarm (alarm voice, for example).

	ALARM_COM	
	GND	Ground terminal.
3	Audio OUT	Outputs audio information to a speaker. When the speaker is used together with the sound pick-up, on the web interface you can live chat with people near the speaker.
4	Audio IN	Inputs the analog audio signals (passengers' voice in a railway station, for example) from the sound pick-up.
5	RS-485	Use RS-485 cables and its converter to connect the Camera to a computer. Then you can use computer to get the Camera implement several tasks. Also, use RS-485 cables to connect the Camera to another PTZ camera. Then the Camera will send signals to and command another PTZ camera.
6	Power cords	**DANGER** When connecting power cords to power adapter, ensure power adapter is disconnected from the power source. Installing Camera with power on might result in serious injury. Inputs 12V DC voltage.
7	GND	Ground terminal.

3 Web Interface Configuration

For detailed camera operation on web interface, see *Thermal Hybrid Camera_Web Operation Manual*.

3.1 Initializing Camera

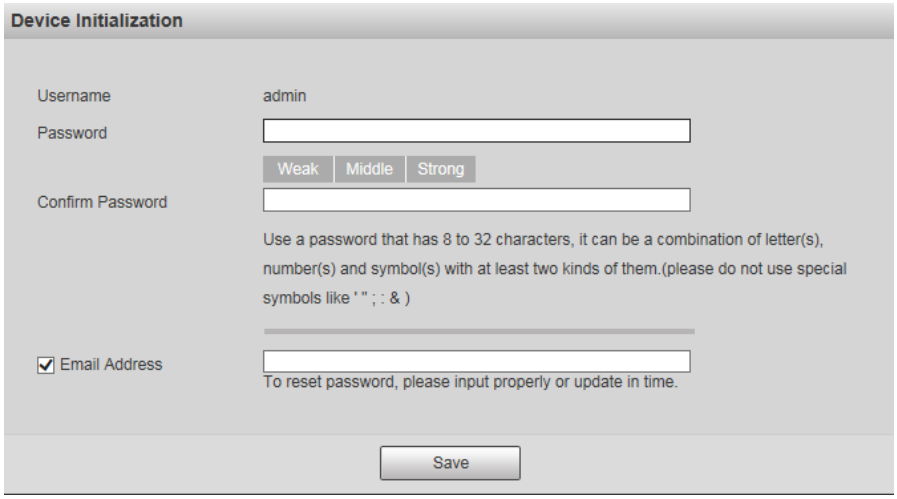
Initialize your Camera and set the user password when you are logging in for the first time or after you have restored your camera to default settings. Initialize the Camera by ConfigTool or through web. This section takes web for example.

- Ensure your Camera IP address (192.168.1.108 by default) and your PC IP address are in the same network segment.
- To secure the Camera data, keep admin password well after initialization and modify it regularly.

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

The **Device Initialization** interface is displayed. See Figure 3-1.

Figure 3-1 Initializing camera



Step 2 Set the login password for admin account. See Table 3-1.

Table 3-1 Password setting description

Parameter	Description
Password	Enter your password and enter it again to confirm it. You are recommended to use strong password. The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
Confirm Password	
Email Address	Enter an email address to reset password when you forget it.

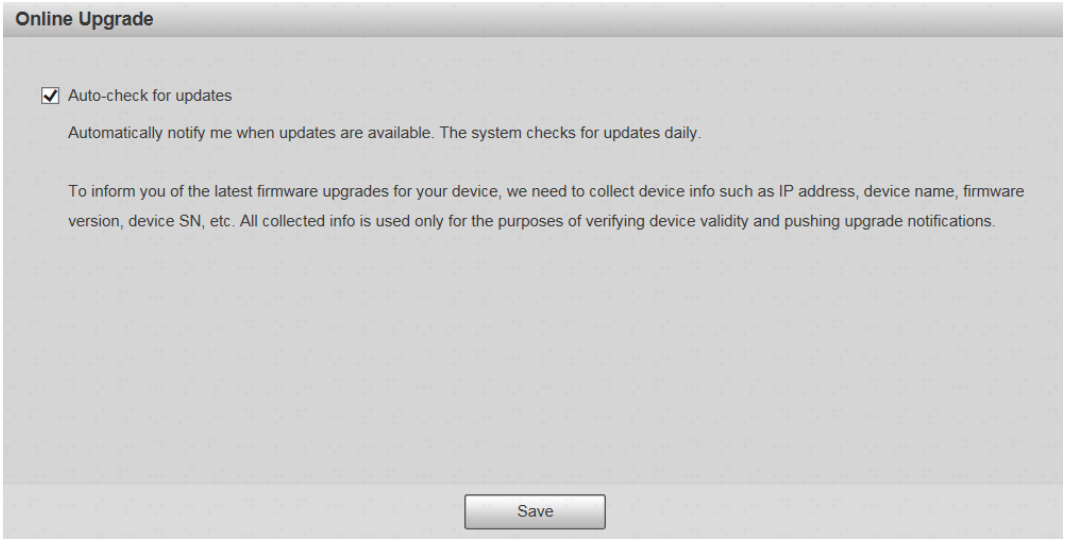
Step 3 Click **Save** and P2P interface is displayed (P2P is reserved for now).

Click **Next**.

Step 4 In the **Online Upgrade** interface, decide whether to do auto check for updates. After selecting the auto check, the newest version information will be displayed in **Setting >**

System > Upgrade and **Setting > Information > Version**. You can also enable auto check in **Setting > System > Upgrade**.

Figure 3-2 Online upgrade



Step 5 Click **Save**.

3.2 Modifying IP Address

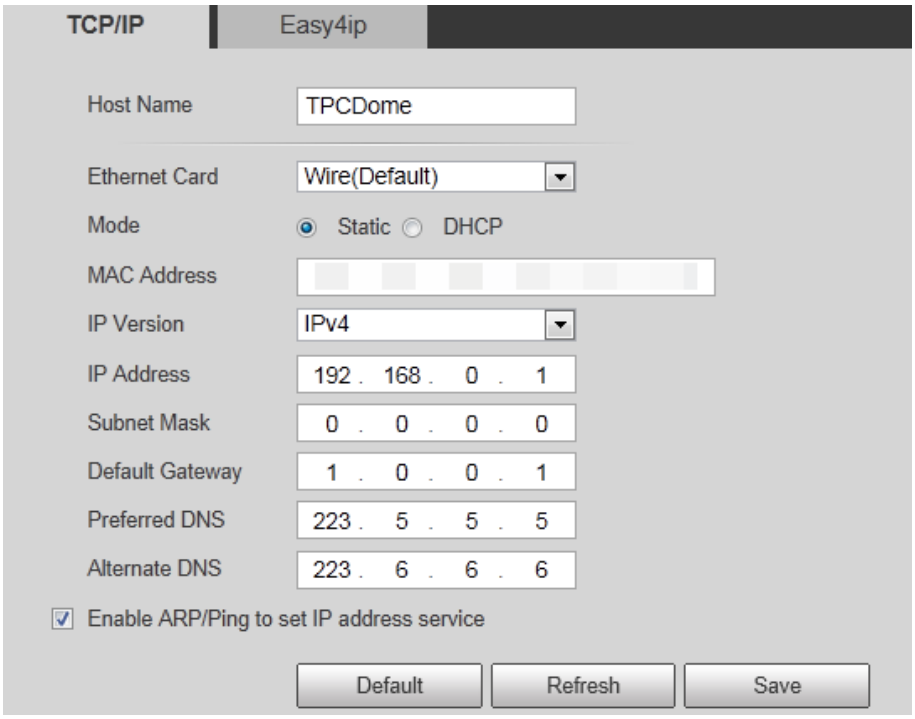
Modify Camera IP address and ensure it is fitted to the actual network segment to get the Camera access network.

Step 1 Log in to Camera web interface.

Step 2 Select Setup > Network > TCP/IP.

The **TCP/IP** interface is displayed. See Figure 3-3.

Figure 3-3 TCP/IP



Step 3 Configure TCP/IP parameters. See Table 3-2.

Table 3-2 TCP/IP parameters

Parameter	Description
Host Name	Give your Camera a name (TPCDome, for example) to help other people, (a router operator, for example), know the Camera information such as camera shape—dome thermal camera.
IP Address, Subnet Mask and Default Gateway	Enter the three item values according to the actual network segment.
Ethernet Card, Mode, MAC Address, IP Version, Preferred DNS and Alternate DNS	Leave them to the default values.

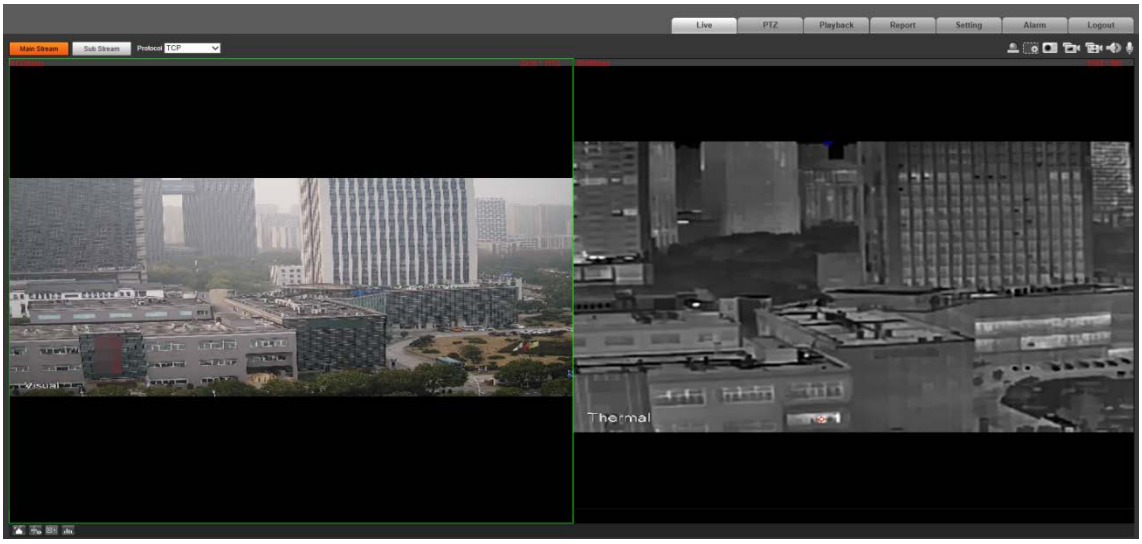
Step 4 Click **Save**.

3.3 Viewing Live Image

Use IP address you have modified to log in to web interface to ensure you can view live image. See Figure 3-4.

When logging in for the first time, you will be prompted to install a plug-in. Save and install it. After that, the web interface displays live image.

Figure 3-4 The live interface



4 Installation

DANGER

Before installation, make sure the power adapter is disconnected from the power source. Installing Camera with power on might result in serious injury. And, powering a pan & tilt camera might cause camera rotation and camera might fall over.

4.1 Selecting Cable

Power Cord

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

Table 4-1 Power cord

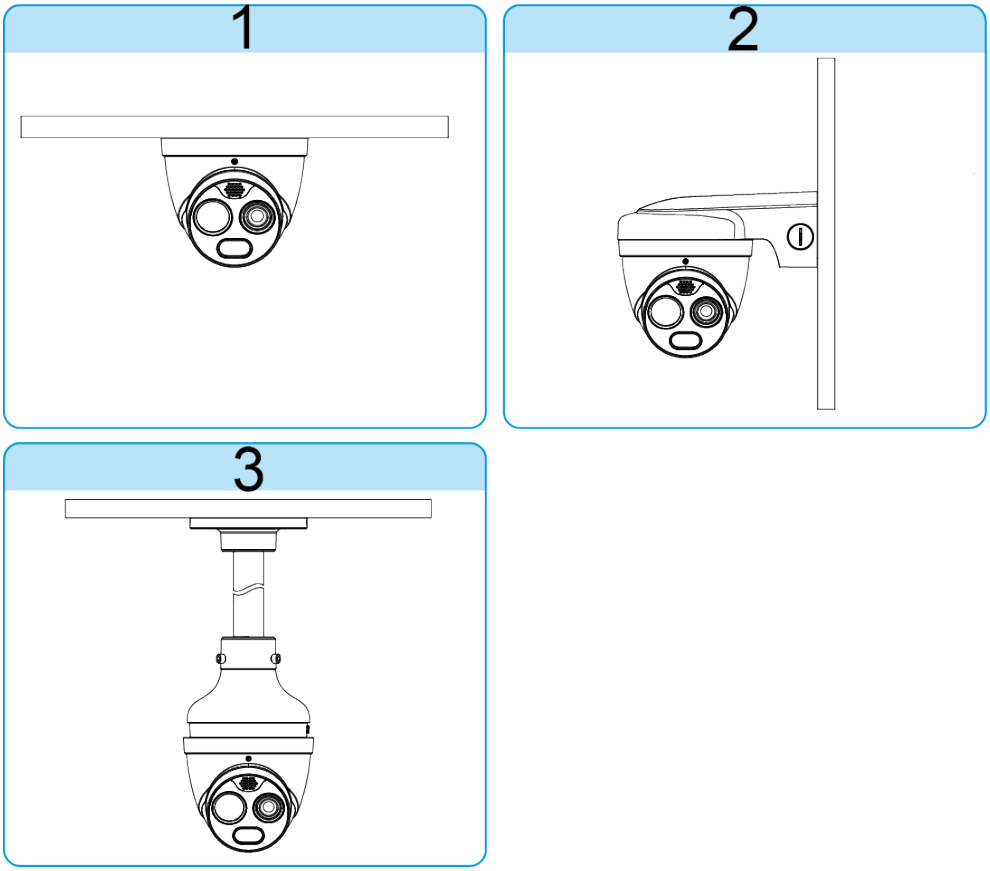
Extension Distance [m (ft.)]	Cord Diameter (mm)
10 (32.81)	0.9
15 (49.21)	1.1
20 (65.62)	1.3
25 (82.02)	1.5
30 (98.43)	1.6
35 (114.83)	1.7
40 (131.23)	1.8
50 (164.04)	1.9

Signal Cable

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

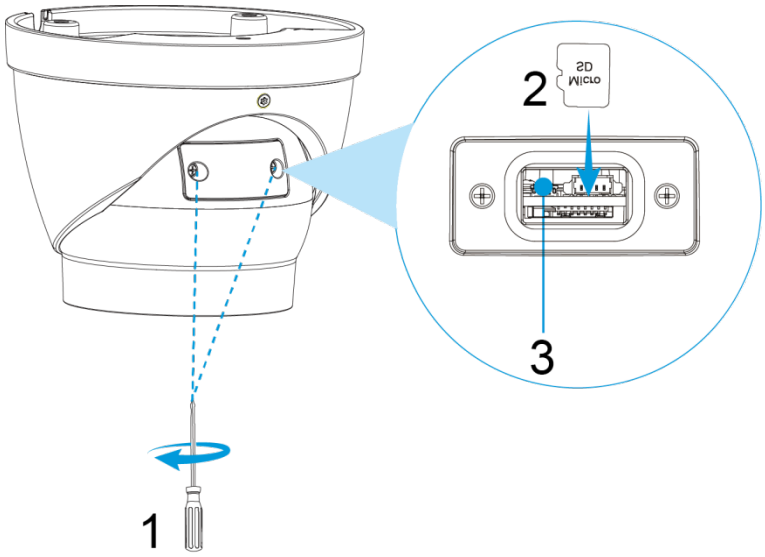
4.2 Selecting Installation Methods

Figure 4-1 Selecting installation methods



4.3 (Optional) Installing SD Card

Figure 4-2 Installing SD card



1	Cross screwdriver	2	SD card slot	3	Reset button

4.4 Fixing Camera

Figure 4-3 Cable tray (through the wall)

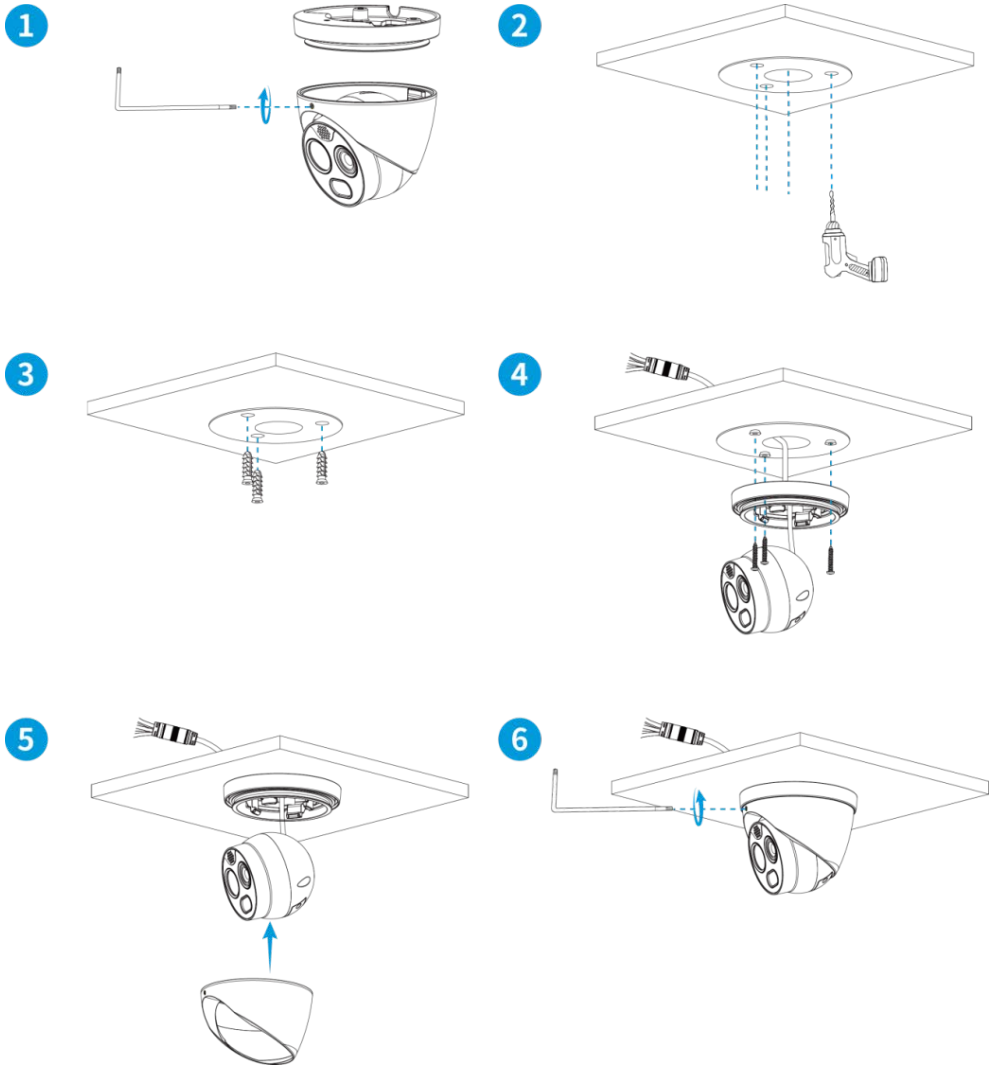
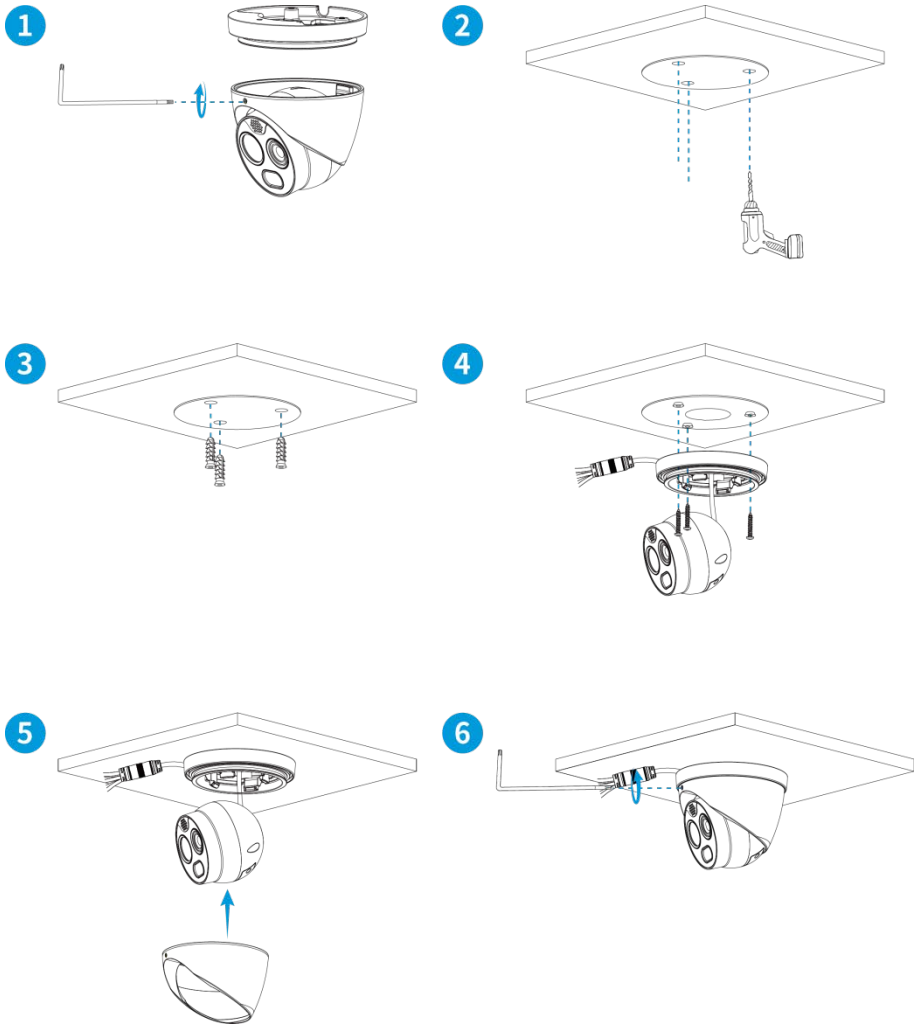
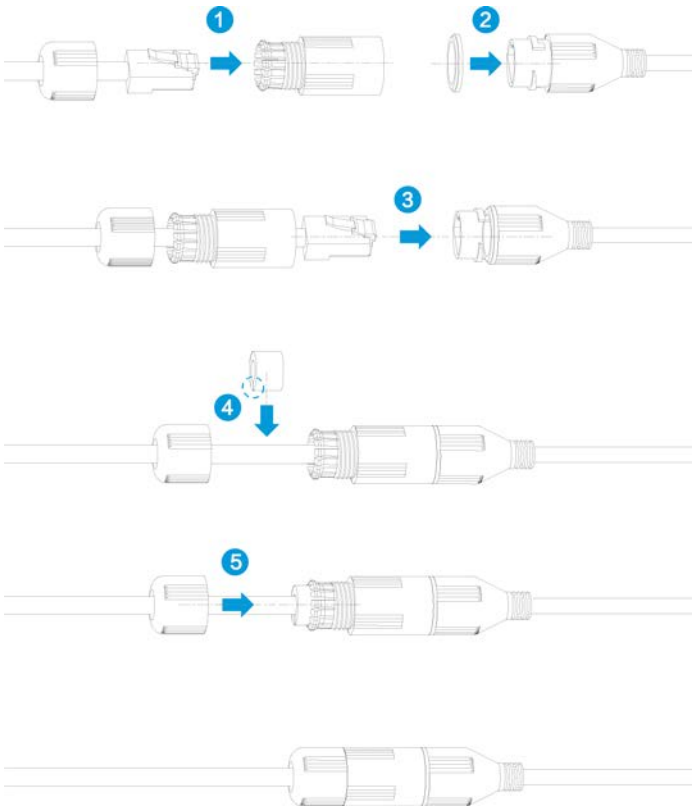


Figure 4-4 Cable tray (through the pedestal side)



4.5 Installing Waterproof Connector

Figure 4-5 Installing waterproof connector for network port

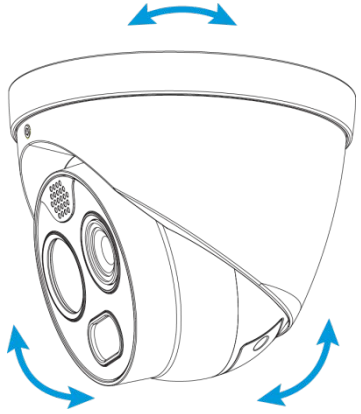


4.6 Connecting Cable Ports

Refer to "2.2 Cables." and connect each cable port to corresponding cables. Then use the insulting tape to seal each port to prevent water leakage.

4.7 Adjusting Lenses Angle

Figure 4-6 Adjusting lenses angle



5 Configuring Alarm

5.1 Configuring Alarm Input and Output

Add an alarm detection device, such as a smoke alarm device to your Camera to receive signals. For those signals, you can set camera linked measures such as Record, Send Email and Snapshot. You can also add an alarm sending device, such as a speaker to your Camera to warn suspicious people.

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

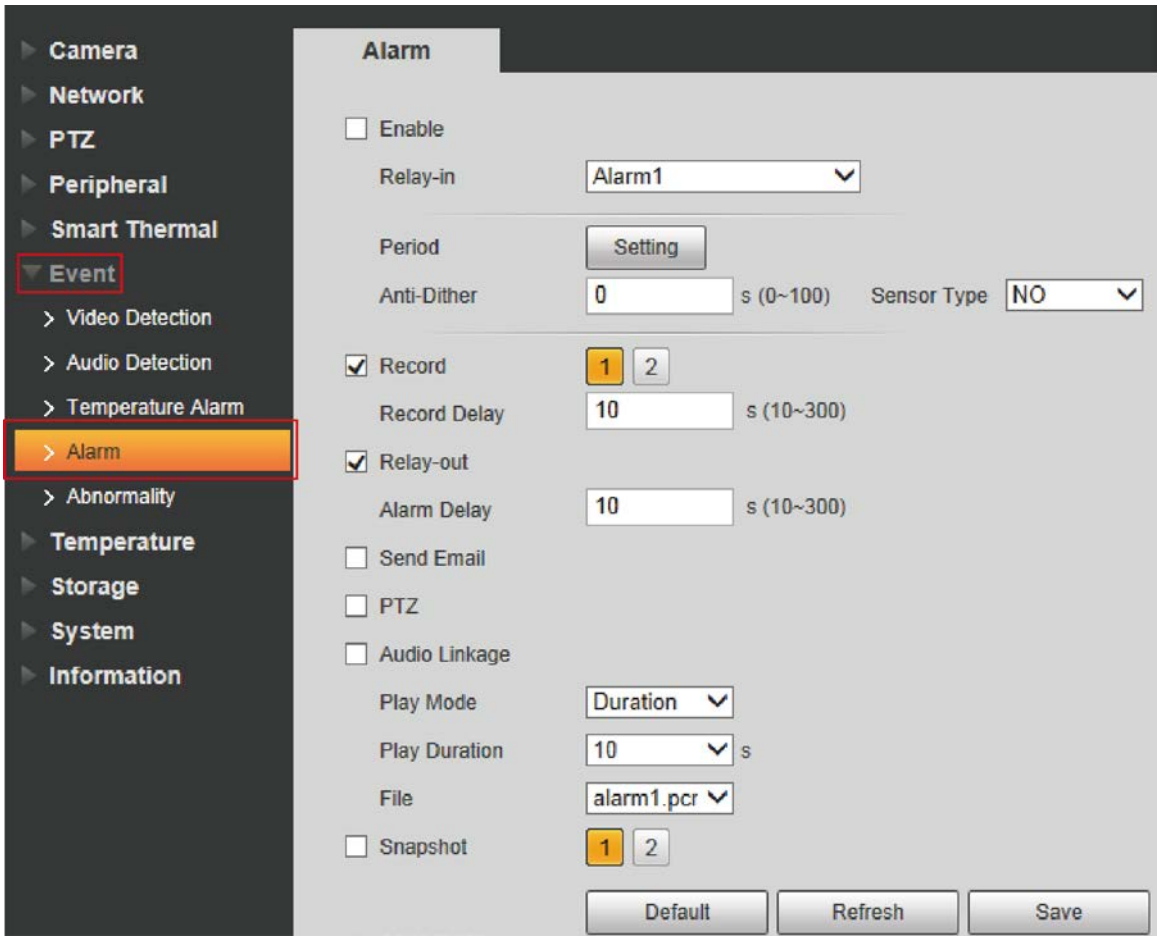
Step 2 Connect alarm sending device to alarm output port of I/O cable. Alarm output port is relay switch output, and the alarm output port can only be connected to normally open (NO) alarm sending device.

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

Step 4 Configure settings on the **Alarm** interface. See Figure 5-1.

- In the **Relay-in** list, select an alarm detection device. Next, you can configure the detection device parameters including **Period**, **Record**, **Send Email** and **Snapshot**. And select the alarm detection device **Sensor Type** in accordance with the electrical level released by the alarm detection device when there is an alarm.
- In the **Relay-out** list, select an alarm sending device from 1 2 and configure its alarm delay.

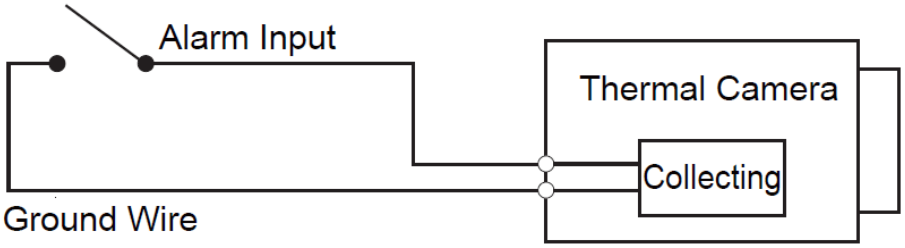
Figure 5-1 The alarm interface



5.2 Working Theory

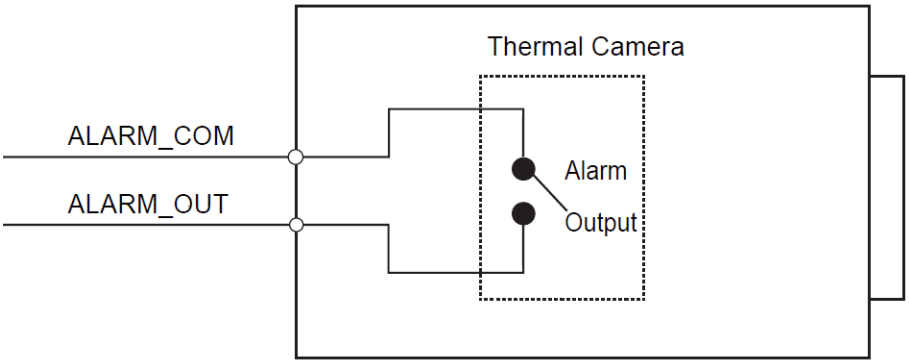
- Alarm input: When input signal is 3.3V or idle, the Camera collects logic "1"; when input signal is grounded, the Camera collects logic "0."

Figure 5-2 Alarm input



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

Figure 5-3 Alarm output

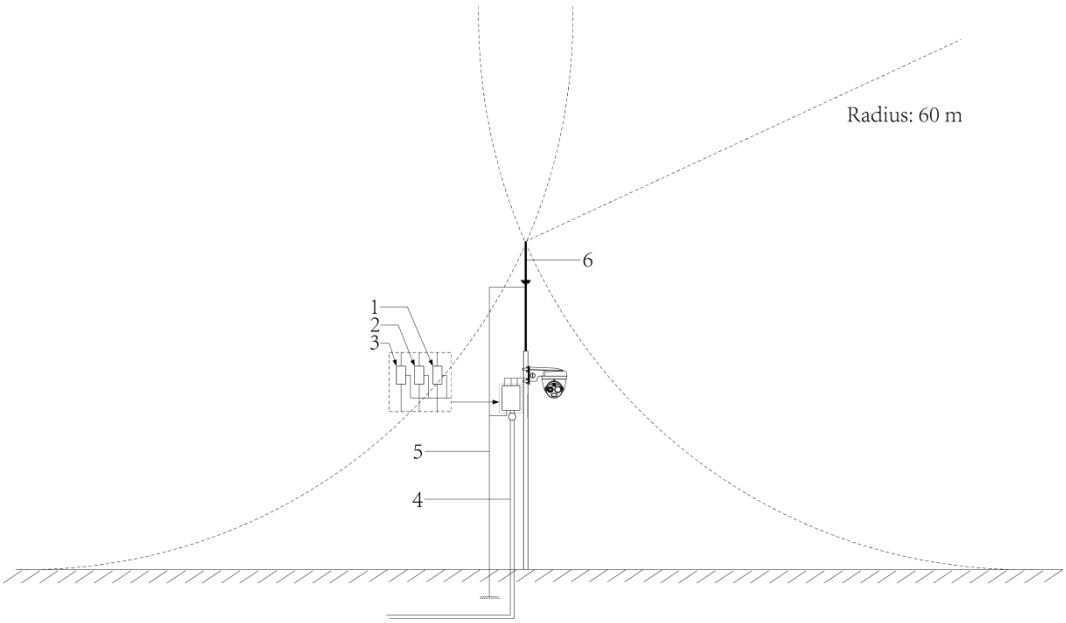


Appendix 1 Lightning and Surge Protection

This series camera adopts TVS lightning protection technology. It can effectively prevent damages from various pulse signals below 6000V, such as sudden lightning and surge. While maintaining your local electrical safety code, you still need to take necessary precaution measures when installing the Camera in the outdoor environment.

- The distance between the signal transmission cable and high-voltage device (or high-voltage cable) shall be at least 50 meters.
- 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 connects one end to the earth. Open floor cable layout is forbidden.
- If there is no ground wire on the tower, connect the Camera's ground wire into the ground. Ground wire resistance shall be less than 4Ω.
- In area of strong thunderstorm hit 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 grounding of the outdoor device and cable shall be considered and conform to your local national or industry standard.
- System shall adopt equal-potential wiring. The earth device shall meet anti-jamming and at the same time conforms to your local electrical safety code. The earth device 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 earth alone, the earth resistance shall not be more than 4Ω and earth cable cross-sectional area shall be no less than 25 mm^2. See Appendix figure 1-1.

Appendix figure 1-1 Lightning protection



Appendix table 1-1 Components for lightning protection

No.	Name	No.	Name	No.	Name
1	Video lightning rod	2	Communication lightning rod	3	Power lightning rod
4	Steel tube shield	5	Ground wire	6	Lightning rod

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 equipment 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 equipment (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 equipment 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 equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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. **Enable Allowlist**

   We suggest you to enable allowlist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the allowlist.

8. **MAC Address Binding**

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

9. **Assign Accounts and Privileges Reasonably**

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

10. **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.

11. **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.

12. **Secure Auditing**

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

13. **Network Log**

    Due to the limited storage capacity of the equipment, 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.

14. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment 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.
- It is recommended that you enable your device's firewall or blocklist and allowlist feature to reduce the risk that your device might be attacked.