Thermal Mini Hybrid Network Bullet Camera

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of Thermal Security Bullet Camera (hereinafter referred to as "the Camera"). Read carefully before using the device, and keep the manual safe for future reference.

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 time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	March 2024

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, and comply with the guidelines when using it.

Transportation Requirements

⚠

- Do not place heavy stress on the device, allow it to fall, violently vibrate or immerse it in liquid during transportation. Handle the device with care to avoid damaging the internal precision parts.
- The complete package is necessary for transportation and storage. It is strictly forbidden to transport the device without full packaging. Whether it is delivered by the contractor or returned to the factory for repair, we will assume no responsibility for any damage or problems caused during transportation due to the incomplete package being sent.

Storage Requirements

⚠ WARNING

- Store the device under allowed humidity and temperature conditions.
- Do not place the device in a humid, dusty, extremely hot or cold site that has strong electromagnetic radiation or poor ventilation.
- Do not place heavy stress on the device, allow it to fall or collide with other objects, violently vibrate or immerse it in liquid during storage.

Installation Requirements

⚠ DANGER

- All service personnel must have required certification or qualified training for performing installations and maintenance of electric apparatuses in environments that have explosive gas. They must also be trained and certified to work at heights, and must have knowledge and skills in the following areas:
  - ◇ Basic knowledge and skills in installing CCTV system and components.
  - ◇ Basic knowledge and skills in low-voltage wiring and in connecting low-voltage electronic circuits.
- All installation and operations must conform to the local electrical safety code and standards.
- Strictly comply with the local electrical safety code and standards, and check whether the power supply is correct before operating the device.
  - ◇ When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.
  - ◇ We recommend using the power adapter provided with the device.
  - ◇ The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- Make sure that the power is off when you connect the cables, install or disassemble the device.

- An emergency disconnect device must be installed during installation and wiring at a readily accessible location for emergency power cut-off.
- Protect the power cord and wires from being walked on or squeezed particularly at plugs, power sockets, and the point where they exit from the device.
- Do not expose the device to heat sources such as a radiator, heater, stove or other types of heating equipment. This is to avoid the risk of fire.
- Do not connect multiple devices to the same power adapter to avoid the risk of overheating or fire if the rated load is exceeded. Please use the power adapter provided by the manufacturer.

⚠ **WARNING**

- A high joule surge protector must be installed when using the device in environments with strong thunder storms or high induced voltage, such as in high voltage transformer substations.
- We recommend you use the device with a lightning protection device for stronger protection against lightning. For outdoor scenarios, strictly comply with the lightning protection regulations. The device must be installed by a certified lightning protection contractor.
- The lightning protection standards of buildings must be taken into consideration when designing the lightning protection and grounding for outdoor circuits. They must conform to the related national and industrial standards. The grounding device must meet the dual requirements of system anti-interference and electrical safety, and must not be short-circuited or mixed with the neutral line of the strong power grid.

⚠

- Appropriate brackets must be installed when the device cannot be used alone.
- Do not pull on the cable to avoid damaging the device.
- Do not place heavy stress on the device, allow it to collide with other objects, and do not violently vibrate or immerse it in liquid during installation.
- Do not connect the device to two or more kinds of power supplies, to avoid safety risks and damage to the device.
- Do not expose the device to environments with strong magnetic fields to avoid damage to the device.
- Do not install the device in an environment that has strong vibrations, such as in a vehicle or ship.
- Remove the electrostatic film from the visible window and the thermal imaging lens cover after installation is complete.
- Do not block the ventilation opening near the device to avoid the device being damaged from heat accumulation.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.
- Make sure a durable and reliable waterproof treatment has been applied to the connectors of the network and power cables, to avoid damaging the device.
- Protect the accessories that come with the device for future maintenance and debugging.
- Make sure that the device is installed horizontally (the bubble inside the spirit level stays in the middle), and on a stable surface that is resistant to deformation.
- Power on the device for inspection of basic functions before installing it in a high location. This is to avoid reinstalling it if it behaves abnormally.
- Do not place the device in environments with smoke, vapor, heavy dust, or that have high temperatures to avoid damage to the device.
- If a circular connector comes with the device, make sure it is securely screwed in place.

Otherwise, the device might behave abnormally due to erosions or oxidation of the connector or the pins.

- Make sure the wire diameter of the cables meets the requirements of the corresponding distance to avoid equipment damage caused by undervoltage and overcurrent.
- Do not aim the lens at intense radiation sources (such as the sun, lasers and molten steel) to avoid damage to the thermal detector and the visible lens.

📖

After unpacking, even if the packing bag is damaged or leaking air, the normal use of the device will not be affected.

Operation Requirements

⚠ DANGER

Do not insert foreign matter into the device to avoid the risk of short circuits, damaging the device and injuring people.

⚠ WARNING

Do not touch the heat dissipation component of the Camera or you might get burnt.

⚠

- Operating temperature: –30 °C to +60 °C (–22 °F to 140°F).
- Do not use a temperature measuring device to measure temperatures that extend beyond its measuring range.
- Do not stain or damage optical components such as the lens and glass.
- Prevent liquid from flowing into the device to avoid damage to its internal components.
- Do not place the device in a highly humid, extremely hot or cold site.
- Use the device within the allowed humidity (less than 95% RH) and altitude (less than 3000 m) conditions.
- The operating temperature of the device must meet the requirements. Refer to the device specifications for information on the allowed temperature and humidity conditions.
- Do not expose the device to corrosive environments such as coastal areas, sea areas with thick salt fog, environments with acid gas, chemical plants and the seaside.

📖

- There is a limit to the life cycle of the quick-wear parts. Make sure to use them correctly, and follow the manufacturer's recommendations and guidance. Log in to the official website for instructions on using the quick-wear parts.
- Devices suitable for low temperature environments automatically preheat before they start to work when placed in a low temperature environment. The preheat time depends on the ambient temperature. When it heats to a suitable temperature, the device starts to work normally.

Maintenance and Repair Requirements

⚠ DANGER

- The maintenance personnel of the camera must have required certification or qualified training for installing closed-circuit television (CCTV) systems. They must also be trained and certified to work at heights, and must have knowledge and skills in the following areas:
  - ◇ Basic knowledge and skills in installing CCTV systems and components.

- ◇ Basic knowledge and skills in low-voltage wiring and in connecting low-voltage electronic circuits.
- Do not allow liquid to get into the device to avoid damage to the internal components. If any liquid flows into the device, immediately disconnect the power supply, unplug all the cables connected to the device, and contact after-sales service.
- Cut off the power before cleaning the device to avoid the risk of electrocution.

⚠

- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals
- If the device produces smoke, an odd odor, noise, or behaves faulty, cut the power immediately, and contact the local dealer or service center at your earliest convenience. Do not disassemble the device. We assume no responsibility for issues caused by uninstructed maintenance.
- Clean the device body with a soft dry cloth. If there are any stubborn stains, clean them away with a soft cloth dipped in a neutral detergent, and then wipe the surface dry. Do not use volatile solvents such as ethyl alcohol, benzene, diluent, or abrasive detergents on the device to avoid damaging the coating and degrading the performance of the device.
- Use a clean cloth or lens wipe to gently wipe off the dust on the visible window. Dried stains can be washed with clean water or ordinary diluted detergent. Do not use alkaline detergents to clean the device, and do not vigorously wipe the device with a damp cloth to avoid permanently damaging the glass.

Laser Protection

⚠ **LASER RADIATION**

If the device is equipped with a laser beam, pay extra attention to the following:

- The laser can cause permanent damage to human eyes and skin within safe distance. Keep the device a safe distance away from humans while installing or operating the device.
- Do not use the distance measurer to measure the distance of targets that are within 50 m of the laser. The laser can permanently damage the device.
- Laser radiation can ignite flammables. Do not directly expose objects (excluding scattered or absorber) to the laser beam, and do not place volatile flammables (such as alcohol) in the working area of laser radiation products, to avoid producing laser beams or fire caused by sparks from high voltage discharge.
- Clear all the reflective objects from the working area of laser radiation products. The reflected or scattered beam of a laser can cause severe damage to eyes. Take necessary precautions when reflective objects are required for use, to minimize its reflecting and scattering range.
- Before dismantling or moving the device to another location, wait 5 minutes after the laser distance measurer finishes operating, so that the accumulated electrons inside the device can be fully discharged. This is to avoid the risk of electrocution.
- Do not touch the circuit of the distance measurer while the device is in a working state, especially the power supply of the laser, which possesses thousands of volts of voltage.
- Install the device with laser function within 3 m of distance, and make sure there are no objects obstructing it to avoid the risk of laser burn and fire.
- When using a laser beam device, avoid exposing the device surface to laser beam radiation.

Table of Contents

Foreword I

Important Safeguards and Warnings III

1 Checklist 1

2 Design 2

2.1 Dimensions 2

2.2 Cables 2

3 Basic Configuration 4

3.1 Initializing Camera 4

3.2 Modifying IP Address 6

3.3 Live View 7

4 Installation 9

4.1 Preparations 9

4.1.1 Checking Installation Space and Intensity 9

4.1.2 Cable Preparation 9

4.2 Installing Camera 10

4.2.1 Installation Methods 10

4.2.2 (Optional) Installing SD Card 11

4.2.3 Fixing Camera 12

4.2.4 (Optional) Installing Waterproof Connector 13

4.2.5 Connecting Cables 14

4.2.6 Adjusting Camera 14

4.3 Installation Requirements on Perimeter Protection 14

4.3.1 Site Selection 14

4.3.2 Typical Scenes 15

4.3.3 Scene Confirmation 16

5 Alarm Configuration 18

Appendix 1 Lightning and Surge Protection 20

Appendix 2 Cybersecurity Recommendations 21

1 Checklist

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

Keep accessories safe for future use.

Figure 1-1 Checklist

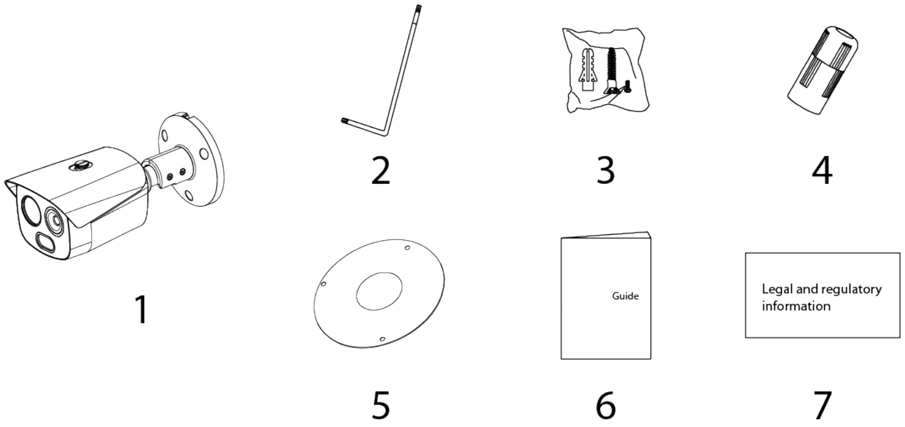


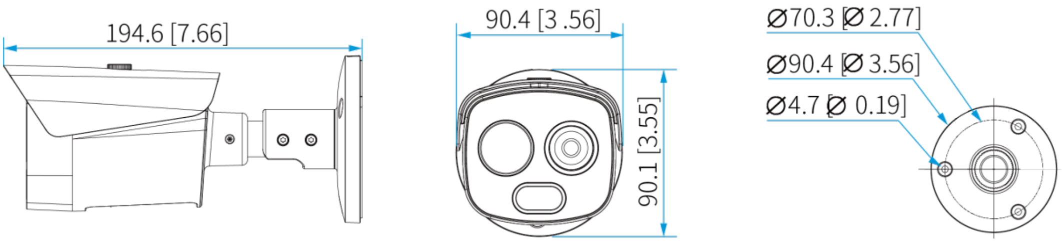
Table 1-1 Checklist

No.	Item	Quantity
1	Thermal network mini hybrid bullet camera	1
2	Wrench	1
3	Screw bag	1
4	Water-proof connector	1
5	Positioning map	1
6	Quick start guide/Installation guide	1
7	Legal and regulatory information	1

2 Design

2.1 Dimensions

Figure 2-1 Dimensions (mm [inch])



2.2 Cables

Cable type might vary with different cameras, and the actual product shall prevail.

Figure 2-2 Cable ports

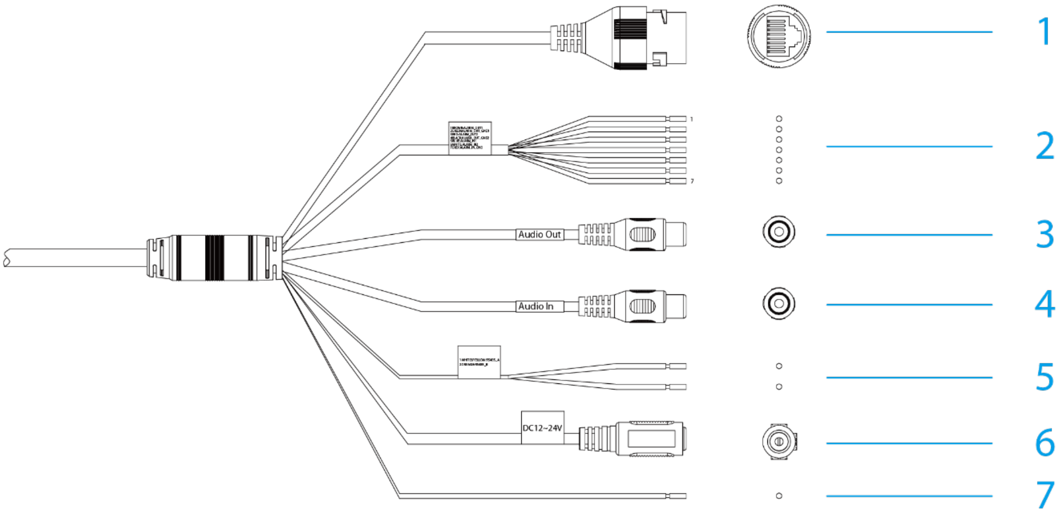


Table 2-1 Ports description

No.	Port	Description
1	LAN	Connects to Ethernet cable.
2	ALARM_OUT1	Outputs alarm signal to alarm device. When connecting to alarm device, only the ALARM_OUT port and ALARM_OUT_GND port with the same number can be used together.
	ALARM_OUT_GND1	
	ALARM_OUT2	

	ALARM_OUT_GND2	
	ALARM_IN1	Alarm input port, receives on-off signal from the external alarm devices.
	ALARM_IN2	
	ALARM_IN_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	Inputs 12 VDC voltage. ⚠ 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.
7	GND	Ground terminal.

3 Basic Configuration

For first-time login, set a password for the admin account (admin by default).

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

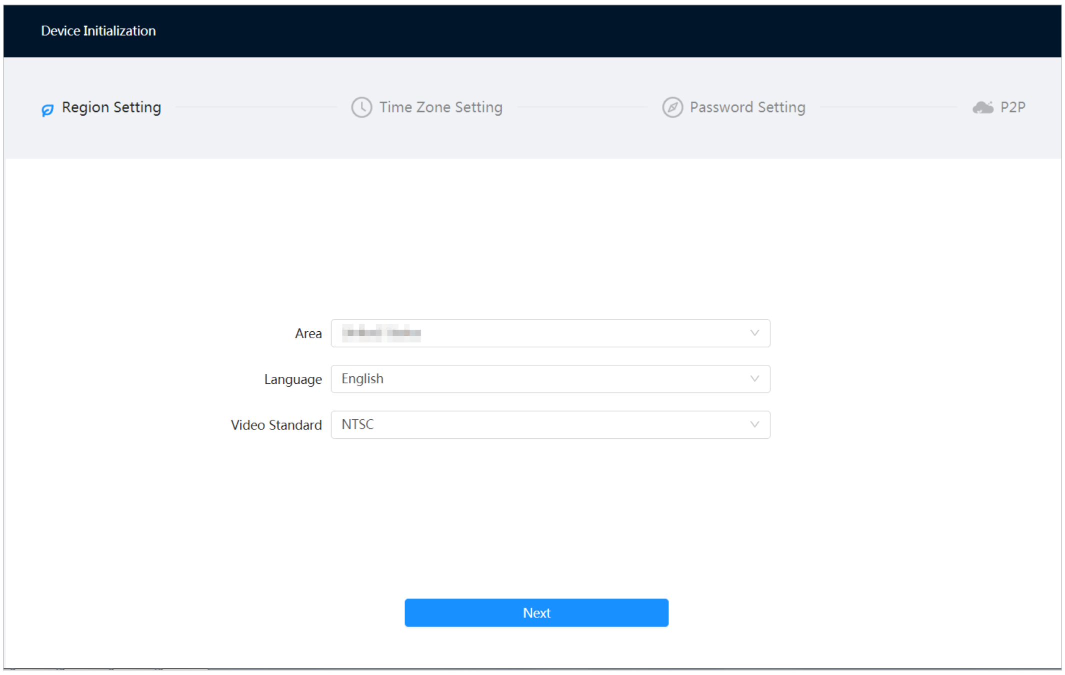
Device initialization is required for the first-time use. This manual is based on the operation on the web interface. You can also initialize device through ConfigTool, NVR, or platform devices.

- To ensure the device safety, keep the password properly after initialization and change the password regularly.
- When initializing device, keep the PC IP and device IP in the same network.

Step 1 Open IE browser, enter the IP address of the device in the address bar, and then press the Enter key.

The IP is 192.168.1.108 by default.

Figure 3-1 Region Setting



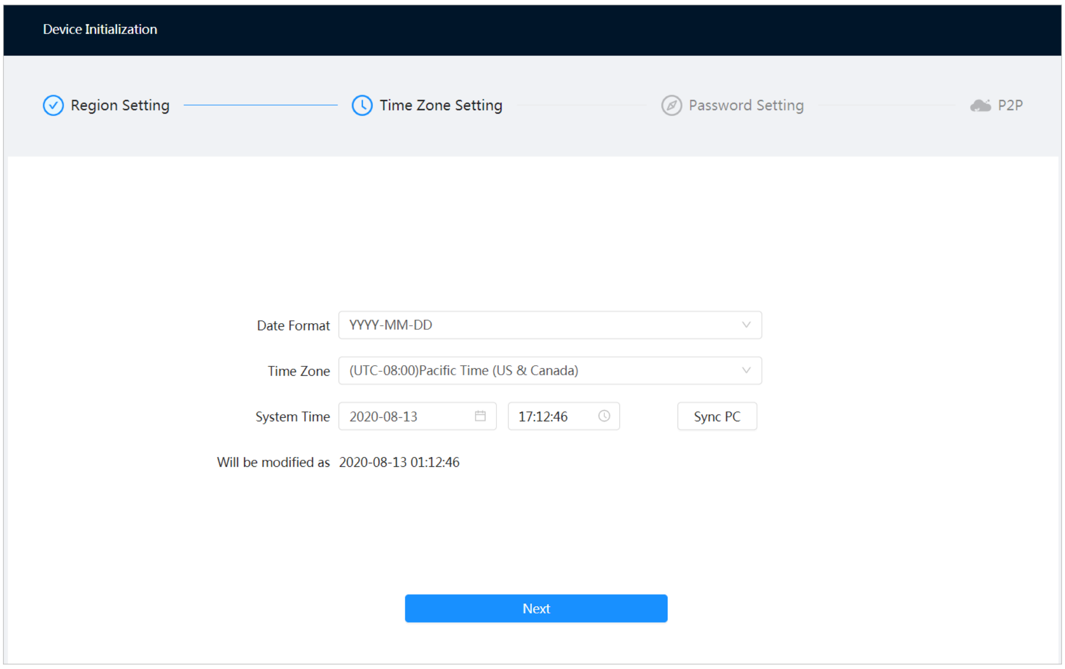
Area

Language: English

Video Standard: NTSC

Step 2 Select the area, language, and video standard according to the actual situation, and then click **Next**.

Figure 3-2 Time zone setting



Date Format YYYY-MM-DD

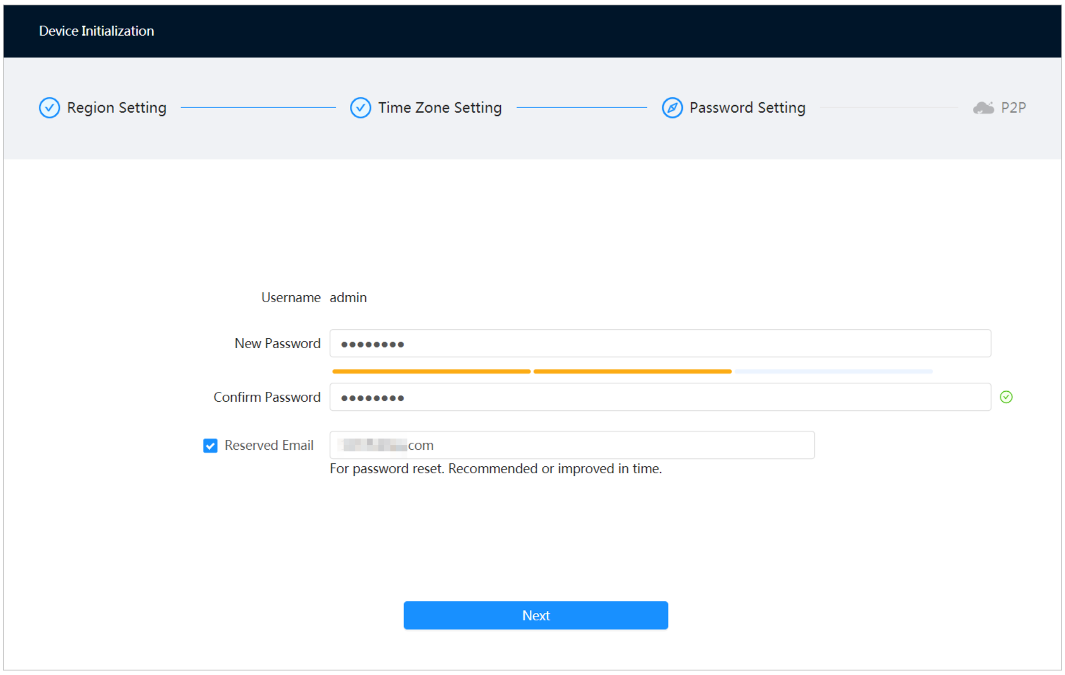
Time Zone (UTC-08:00)Pacific Time (US & Canada)

System Time 2020-08-13 17:12:46

Will be modified as 2020-08-13 01:12:46

Step 3 Configure the time parameters, and then click **Next**.

Figure 3-3 Password setting



Username admin

New Password ••••••••

Confirm Password ••••••••

☑ Reserved Email [redacted]com

For password reset. Recommended or improved in time.

Step 4 Set the password for admin account.

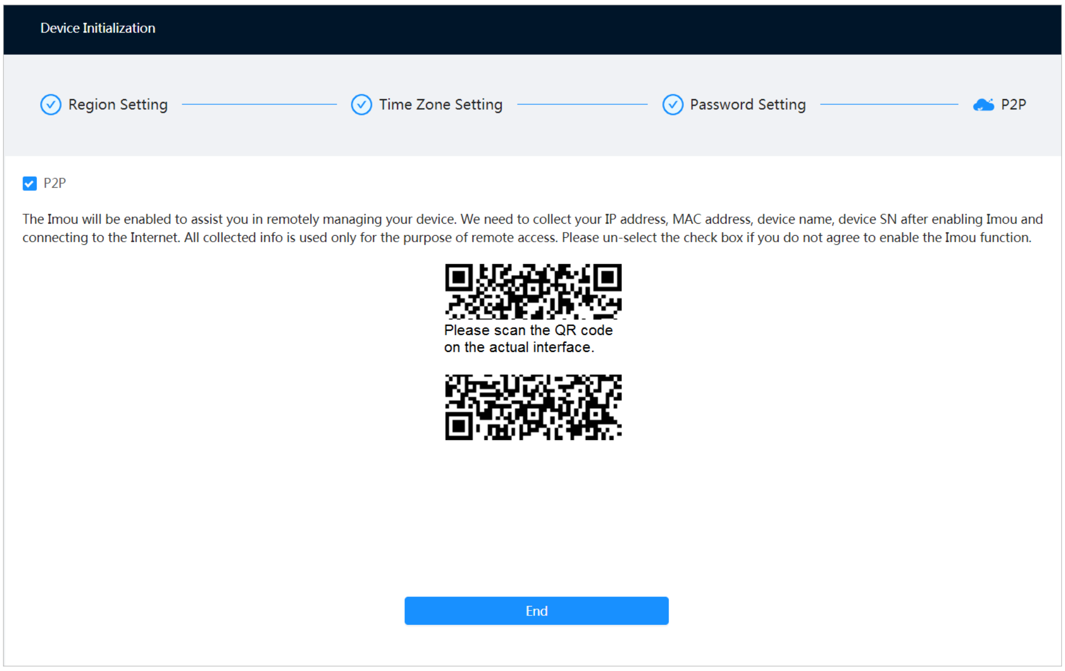
Table 3-1 Description of password configuration

Parameter	**Description**
Username	The default username is admin.
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 ' " ; : &). Set a high security level password according to the password security notice.
Confirm password	

Parameter	Description
Reserved email	Enter an email address for password resetting, and it is selected by default. When you need to reset the password of the admin account, a security code for password resetting will be sent to the reserved email address.

Step 5 Click **Next**, and then **P2P** interface is displayed.

Figure 3-4 P2P



Device Initialization

☑ P2P

The Imou will be enabled to assist you in remotely managing your device. We need to collect your IP address, MAC address, device name, device SN after enabling Imou and connecting to the Internet. All collected info is used only for the purpose of remote access. Please un-select the check box if you do not agree to enable the Imou function.

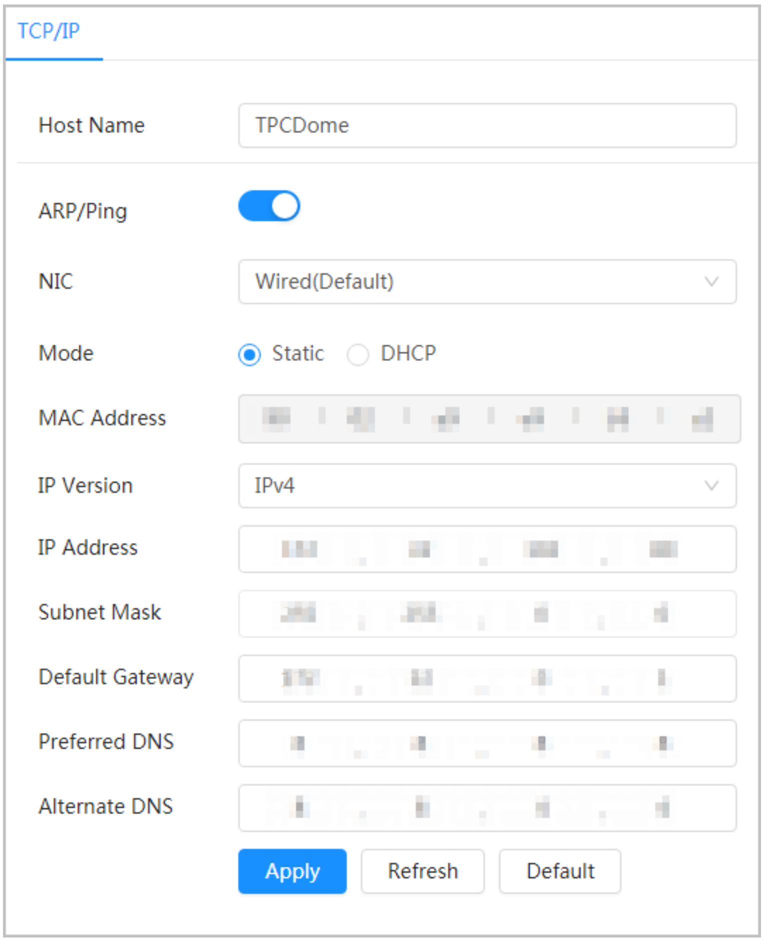
Please scan the QR code on the actual interface.

3.2 Modifying IP Address

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

Step 1 Select ⚙ > **Network** > **TCP/IP**.

Figure 3-5 TCP/IP



TCP/IP

Host Name	TPCDome
ARP/Ping	● (on)
NIC	Wired(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]

Step 2 Configure TCP/IP parameters.

Step 3 Click **Apply**.

3.3 Live View

Make sure that the Camera can access the network and check the video after configuring the network.

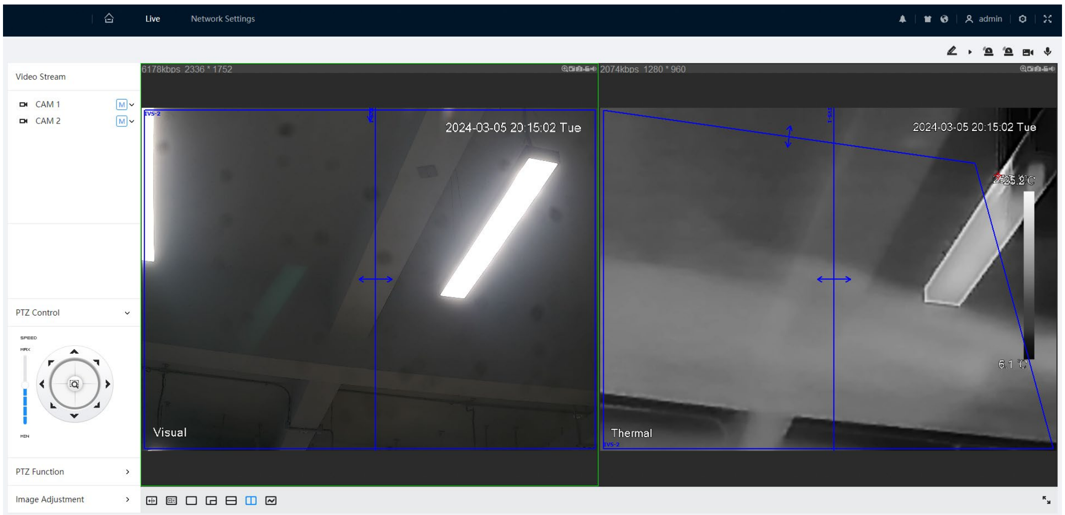
Step 1 Log in to the web page of the Camera.

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 web main page.

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

Figure 3-6 Live view



4 Installation

4.1 Preparations

4.1.1 Checking Installation Space and Intensity

- Make sure that the place where the Camera is installed has enough space to hold the Camera and its mounting accessories.
- Make sure that the mounting surface 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 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 Cables

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

4.2 Installing Camera

4.2.1 Installation Methods

Figure 4-1 Model A

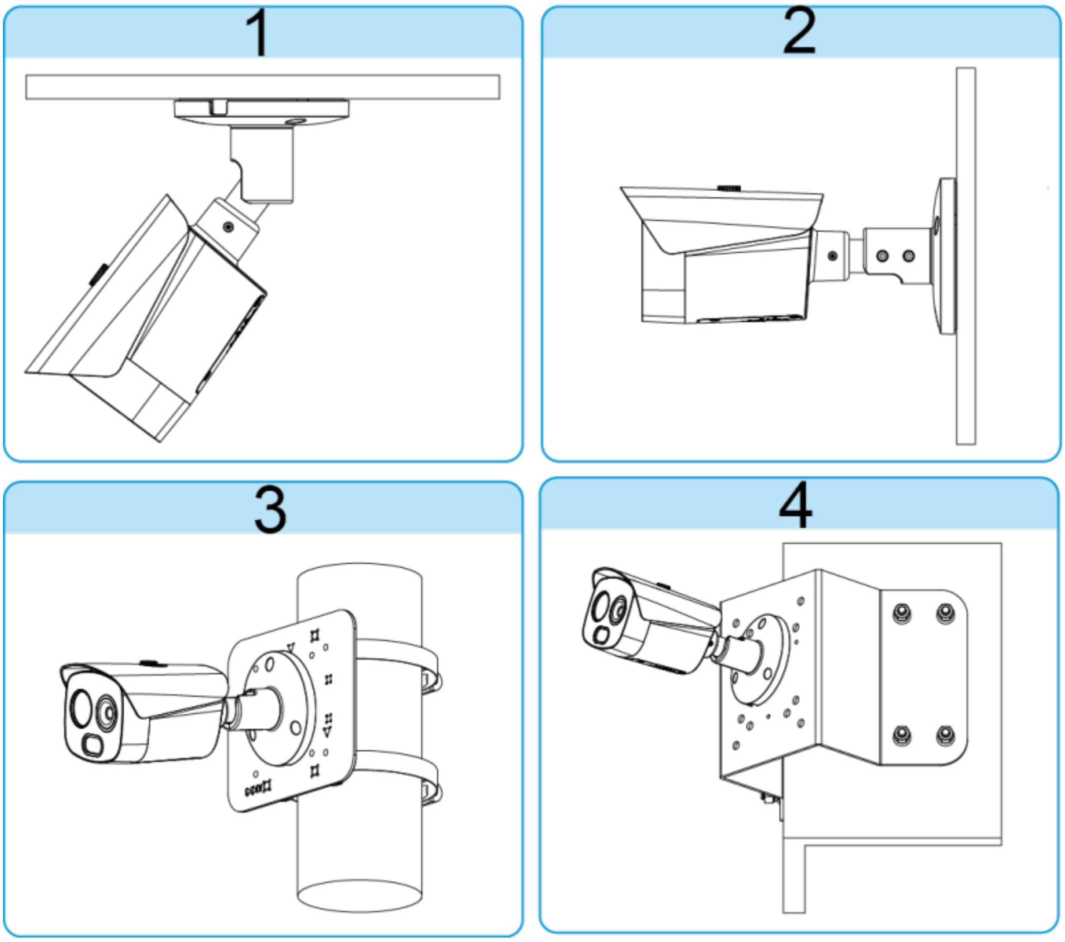


Table 4-2 Description

No.	Description	No.	Description
1	Ceiling mount	2	Wall mount
3	Pole mount	4	Corner mount

Figure 4-2 Model B

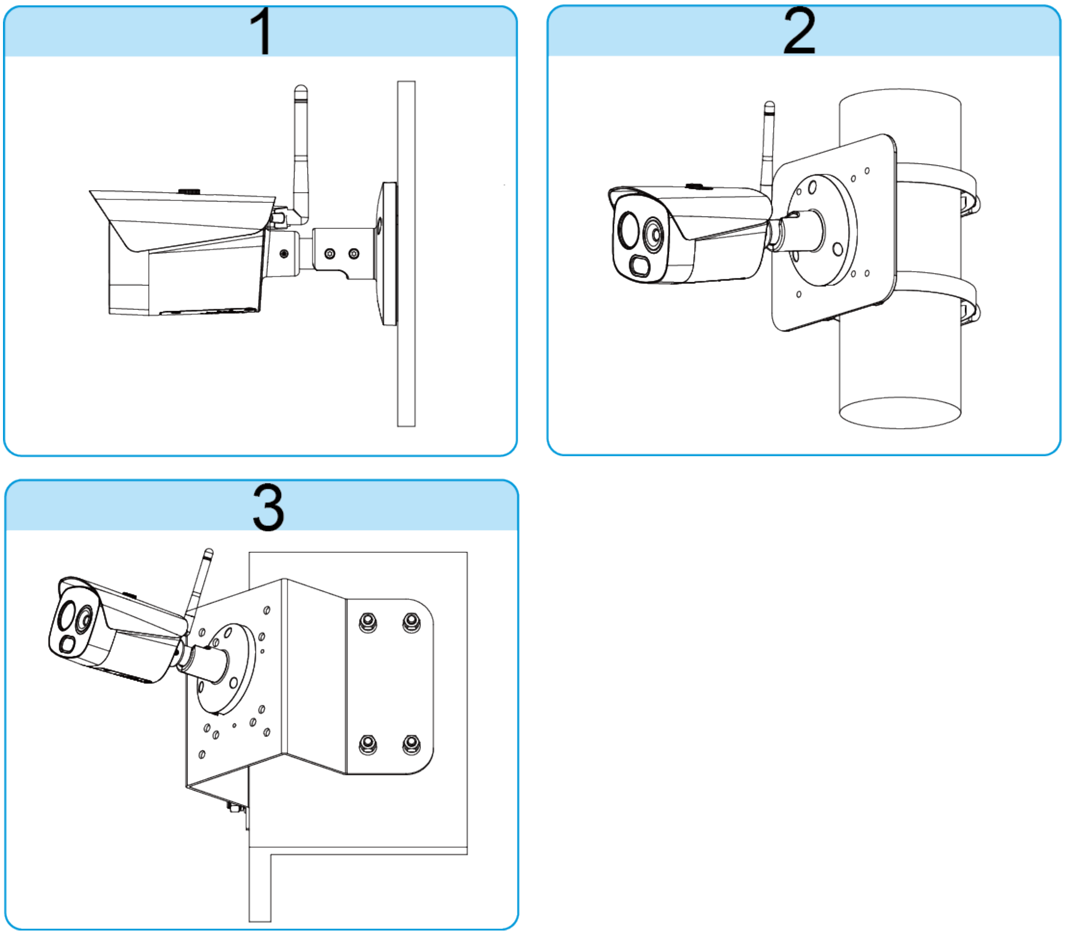


Table 4-3 Description

No.	Description	No.	Description
1	Wall mount	2	Pole mount
3	Corner mount	—	—

For model B, the space between its antenna and the wall (or ceiling) should be no less than 3 cm.

4.2.2 (Optional) Installing SD Card

Install Micro SD card to save recordings to local storage.

- Cut off power before installation.
- Do not press the reset button during installation. Press and hold the reset button for 10 seconds and the Camera will be restored to factory settings.
- Before closing and fastening the protective cover, make sure the waterproof ring is well placed; Otherwise, it will affect waterproof performance of the Camera.

Figure 4-3 Installing SD card

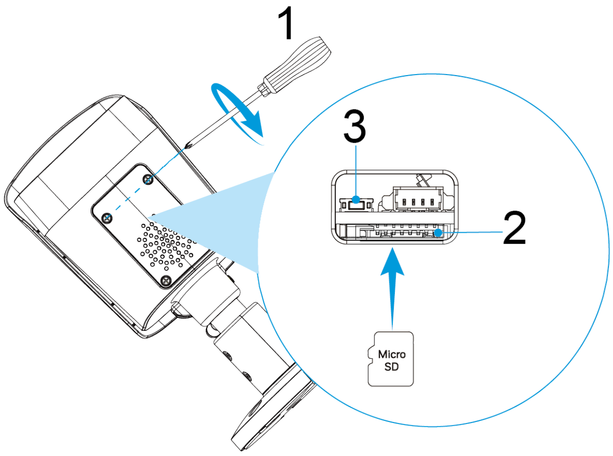


Table 4-4 Tool and components

No.	Description	No.	Description	No.	Description
1	Cross screwdriver	2	SD card slot	3	Reset button

4.2.3 Fixing Camera

Figure 4-4 Cable tray (through the wall)

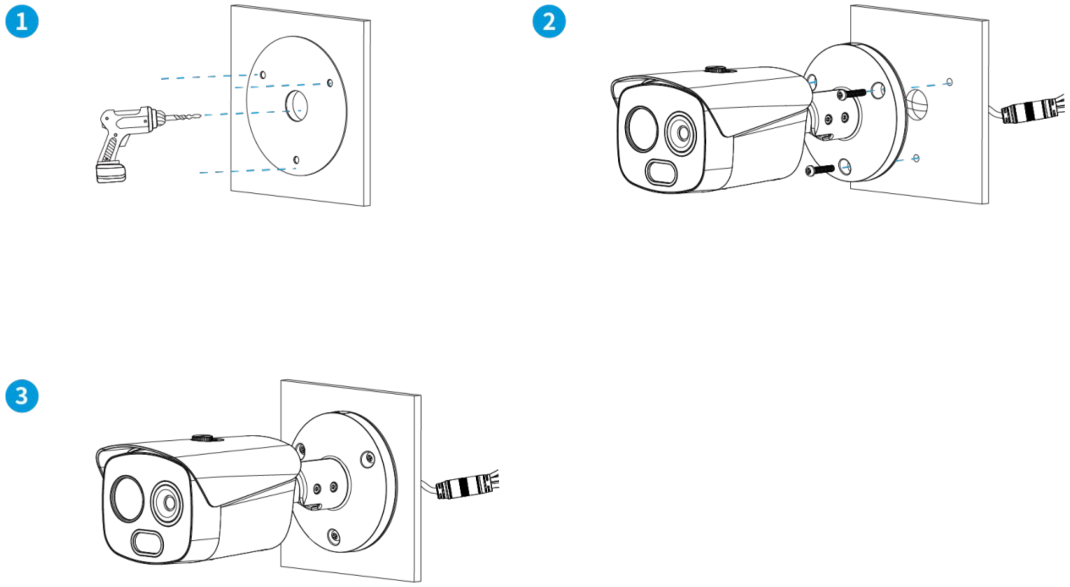
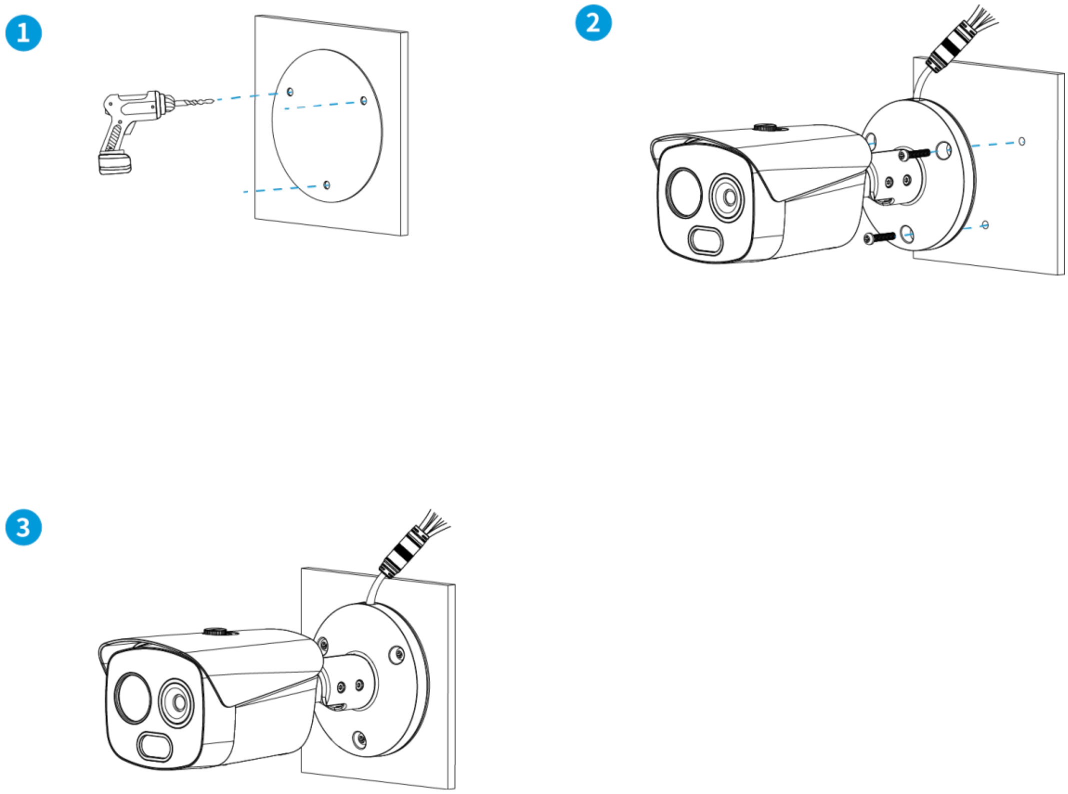
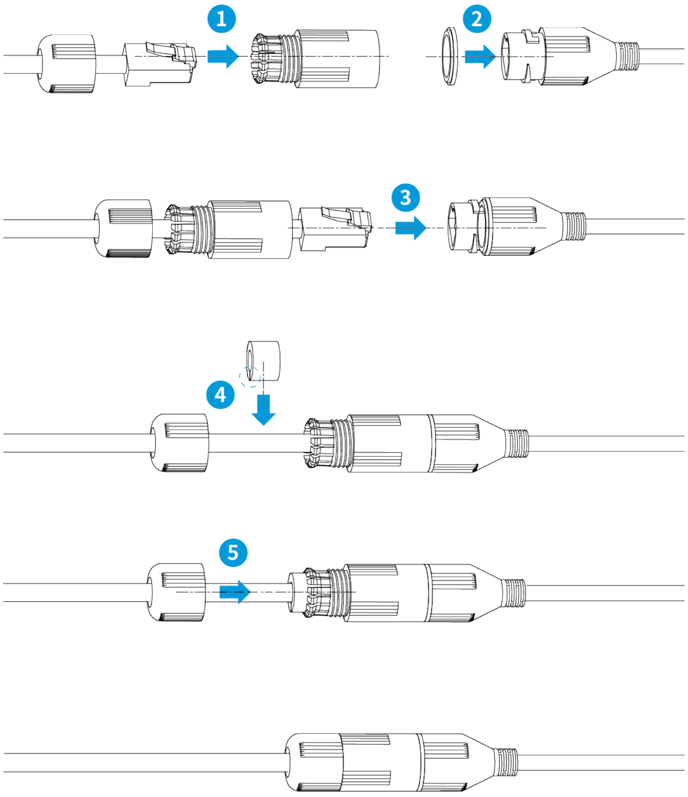


Figure 4-5 Cable tray (through the pedestal side)



4.2.4 (Optional) Installing Waterproof Connector

Figure 4-6 Installing waterproof connector for network port



4.2.5 Connecting Cables

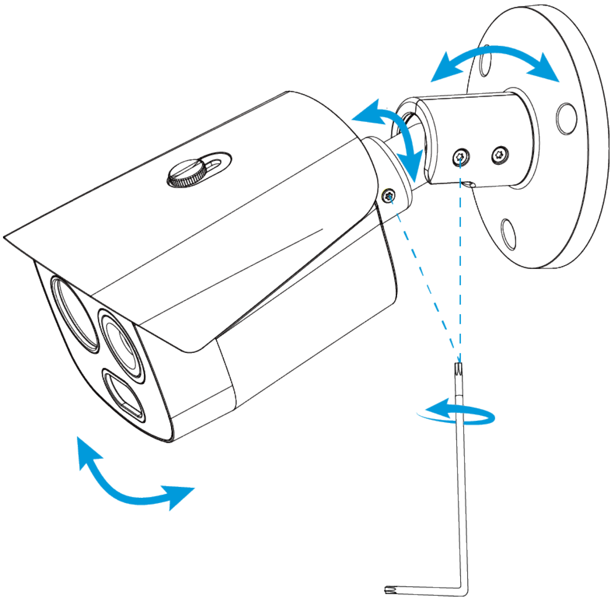
Refer to "2.2 Cables" and connect each cable port to corresponding cables. Then use the insulting tape to seal each port to prevent water leakage.

4.2.6 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 4-7 Adjusting camera



4.3 Installation Requirements on Perimeter Protection

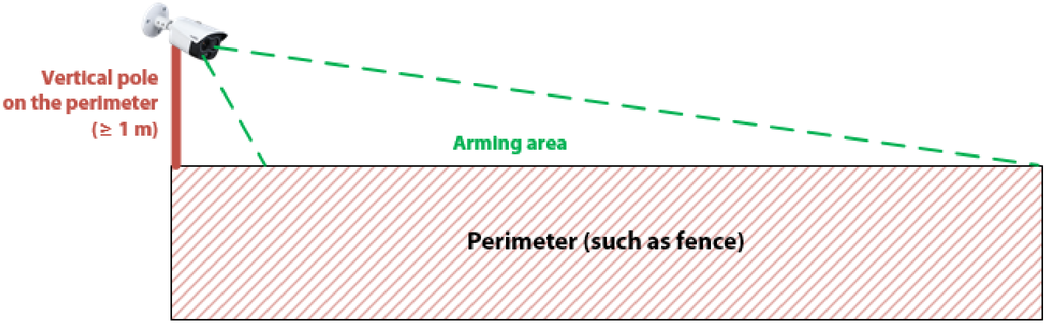
4.3.1 Site Selection

- When installing the camera, keep a depression angle (10°–40°) to avoid obstruction or overlap between the targets caused by parallel view, which can reduce the false alarms and missed alarms.
- The recommended installation height is 3 m–5 m. (In the detection area, we recommended high-point installation rather than low-point installation).
- Install the camera horizontally and firmly to guarantee the analysis result.
- To get a clearer movement of the target, make the monitoring direction vertical to the moving direction. Make sure that the target is continuously present in the image, and has crossing action. Make sure that there is no obstruction in the detection area, and leave some space at both sides of the rule line, otherwise the target might rush out of the image because of the fast speed.

4.3.2 Typical Scenes

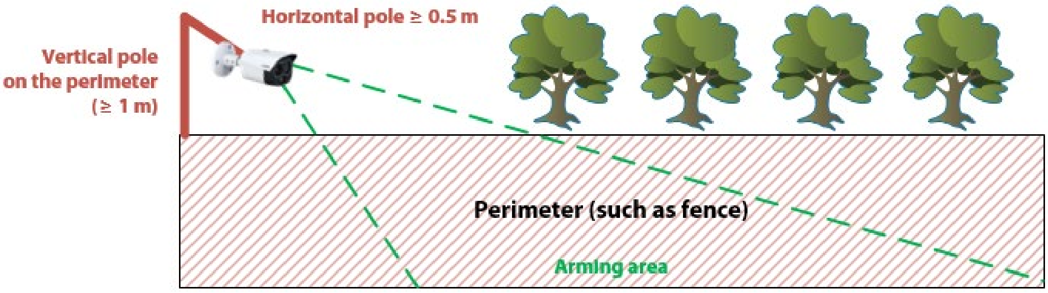
- When there is no obstruction around the perimeter, install a vertical pole (≥ 1 m) on the perimeter, and then install the camera on the vertical pole.

Figure 4-8 Typical scene (1)



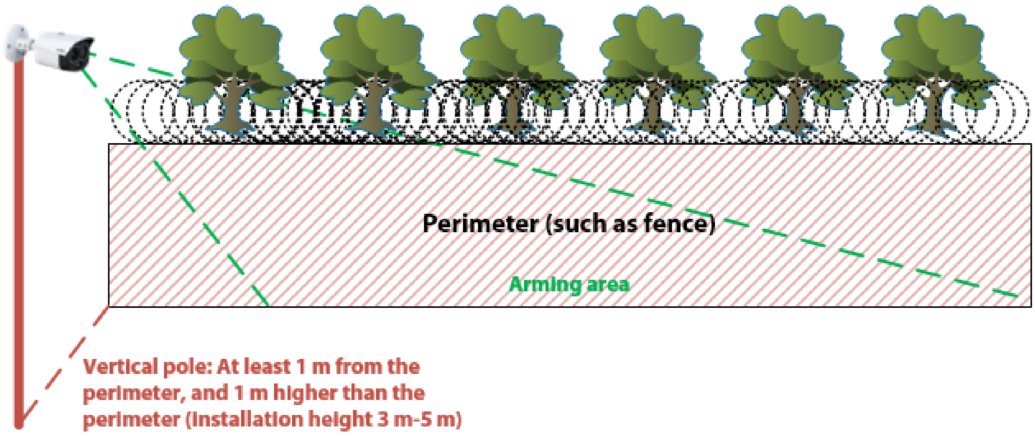
- When there are obstructions (such as trees and vegetation) around the perimeter, install an L pole (horizontal pole ≥ 0.5 m) on the perimeter, and then install the camera on the L pole.

Figure 4-9 Typical scene (2)



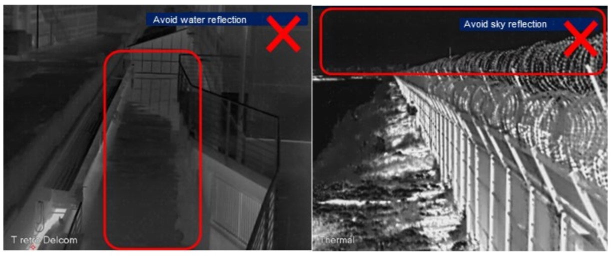
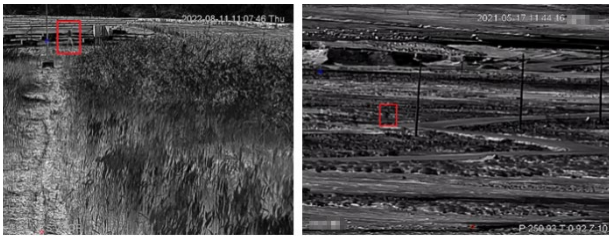
- When there are obstructions (such as trees and vegetation) around the perimeter, and wire netting on the perimeter, install a vertical pole separately. Keep the pole 1 m from the perimeter, and 1 m higher than the perimeter (installation height 3 m-5 m).

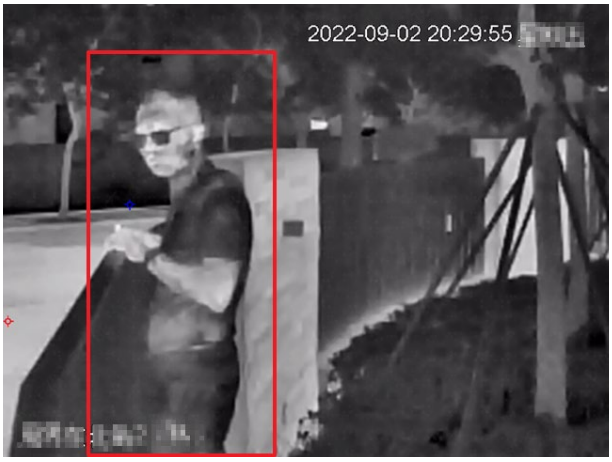
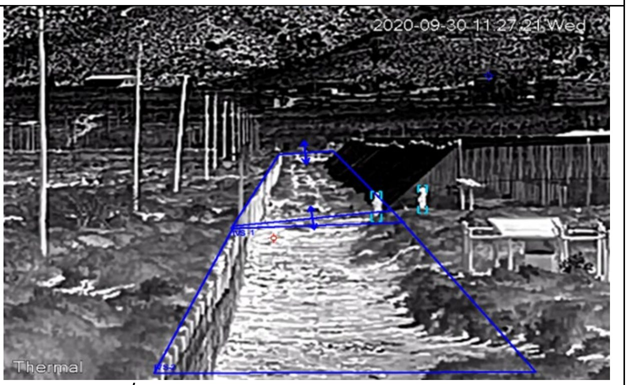
Figure 4-10 Typical scene (3)


Perimeter (such as fence)
Arming area
Vertical pole: At least 1 m from the
perimeter, and 1 m higher than the
perimeter (installation height 3 m-5 m)

4.3.3 Scene Confirmation

Table 4-5 Scene Confirmation

Item	Standard	Example
Burning warning	● To avoid damaging the thermal detector, do not aim the lens at intense radiation sources (such as the sun, molten iron and heat sources) during the storage, installation or operation, and avoid direct sunlight and reflection for outdoor use. ● Avoid sky and water reflection.	 Not suitable. The camera lens might be burnt. (×)
Wide view and no obstructions	● The monitoring scene should be with a wide view. ● No obstructions, such as trees, vegetation, and wire netting in the detection area.	No obstructions No obstructions Set the rule in the middle of the road Not suitable. The target is blocked. (×)
Background complexity	● In scenes with complex background, the target is hard to be identified, and the detection distance will be shorter. ● The larger the temperature difference between the target and the background, the better the detection result will be.	 Not suitable. False alarm and missed alarm might be caused, and the detection distance will be shorter. (×)

Item	Standard	Example
Target size	The maximum width and height of the target should be no more than 2/3 that of the image.	 Not suitable. False alarm and missed alarm might be caused. (×)
Suitable scene	● No sky in the image. ● The detection area should be with a wide view and no obstructions. ● The background is simple. ● Drawing multiple rule boxes from far to near.	 Suitable. (√)

5 Alarm Configuration

⚠

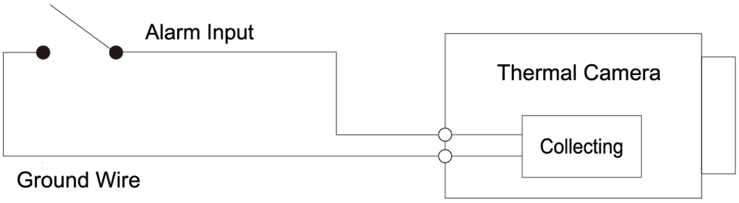
Cut off power before connecting cables.

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

Alarm input: input signal is idle or grounded and the device can collect different states of alarm input port.

- 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 5-1 Alarm input

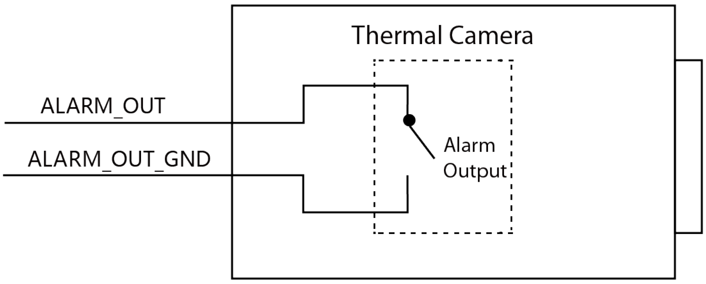


Step 2 Connect alarm output device to alarm output port of I/O cable. Alarm output is a relay switch output. The alarm output port can only be connected to NO alarm device.

Alarm output: Port ALARM_OUT and ALARM_OUT_GND form a switch to provide alarm output. Normally the switch is on. The switch will be turned off when there is an alarm output.

ALARM_OUT1 can only be used together with ALARM_OUT_GND1 while ALARM_ OUT2 can only be used together with ALARM_OUT_GND2 when connecting to alarm devices.

Figure 5-2 Alarm output



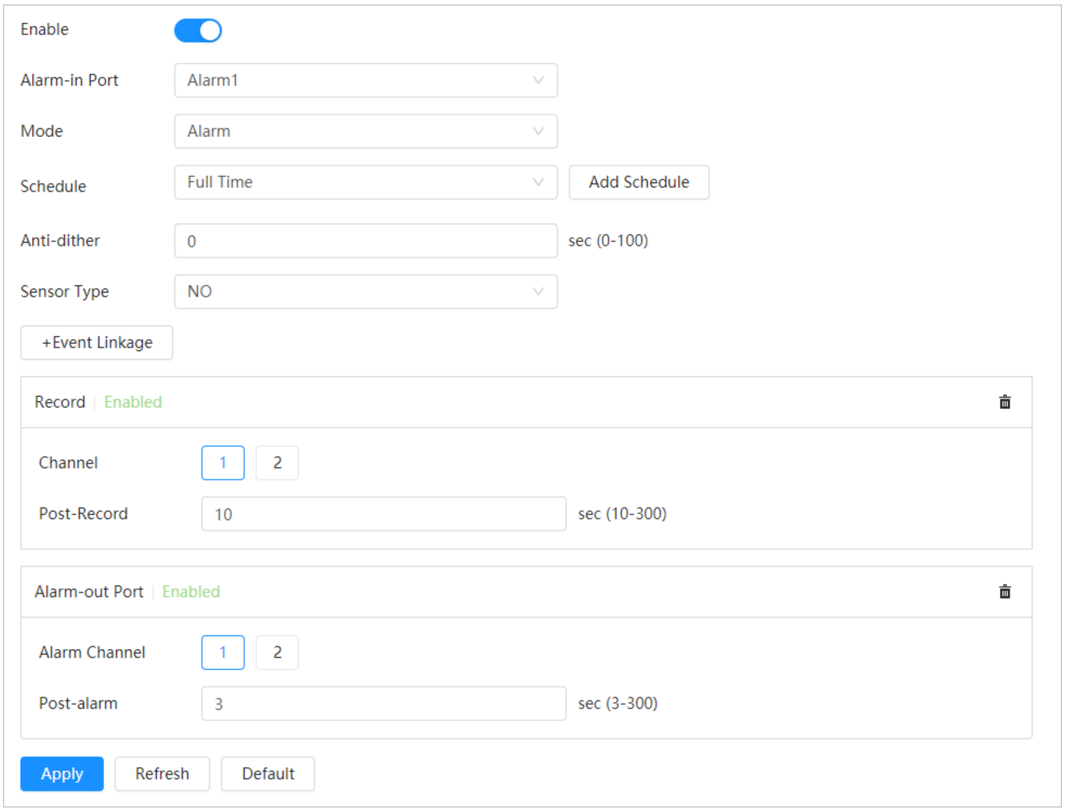
Step 3 Log in to the web page, and select ⚙ > **Event** > **Alarm**.

Step 3 Click ○ next to **Enable** to enable alarm linkage.

Step 4 Configure the settings for alarm input and output in the alarm setup page, and then click **Apply**.

- Alarm input is corresponding to the alarm input port of device I/O cable. It is to set corresponding NO and NC according to the high and low level signal generated by alarm input devices when an alarm is triggered.
- The alarm output corresponds to the alarm output port of device I/O cable.

Figure 5-3 Alarm settings



Enable: on

Alarm-in Port: Alarm1

Mode: Alarm

Schedule: Full Time

Anti-dither: 0 sec (0-100)

Sensor Type: NO

Record | Enabled

Channel: 1

Post-Record: 10 sec (10-300)

Alarm-out Port | Enabled

Alarm Channel: 1

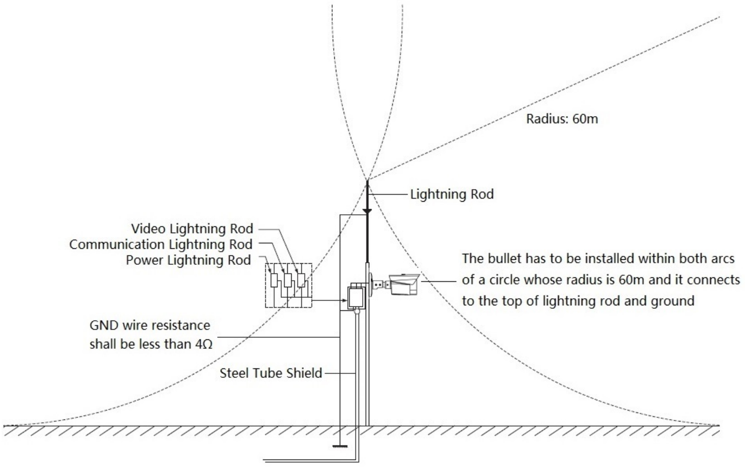
Post-alarm: 3 sec (3-300)

Appendix 1 Lightning and Surge Protection

This series bullet 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 point to the earth. Open floor cable layout is forbidden.
- For vast land, install a 10KA lightning rod near the Camera's power input port and Ethernet port. For Camera with AC to DC power adapter, install a 10KA lightning rod near the adapter's input port.
- For Camera installed on the iron tower, if there is a wire connected properly into the ground, connect the Camera's ground wire to the tower's ground wire. And:
  - ◇ Make sure that the Camera is over 3 m away from the tower lightning rod's top point.
  - ◇ Use several strands of copper wire whose total diameter is up to 16 mm2.
  - ◇ Make sure the Camera is installed within both arcs of circles whose radius is 60m. See Appendix Figure 1-1.
- If there is no ground wire on the tower, connect the Camera's ground wire into the ground.
- In area of strong thunderstorm hit or near high sensitive voltage (such as near high-voltage transformer substation), you need to install additional high-power thunder protection device or lightning rod.
- The thunder protection and earth of the outdoor device and cable shall be considered in the building whole thunder protection 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 short circuit 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


Radius: 60m
Lightning Rod
Video Lightning Rod
Communication Lightning Rod
Power Lightning Rod
The bullet has to be installed within both arcs of a circle whose radius is 60m and it connects to the top of lightning rod and ground
GND wire resistance shall be less than 4Ω
Steel Tube Shield

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 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.