

Thermal Network Mini Hybrid Eyeball Camera Quick Start Guide








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
V1.0.0	First release.	March 2024

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

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: -40 °C to +70 °C (-40 °F to 158 °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 Packing List	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 Selecting Cable	9
4.2 Selecting Installation Methods	10
4.3 (Optional) Installing SD Card	10
4.4 Fixing Camera	11
4.5 Installing Waterproof Connector	13
4.6 Connecting Cable Ports	13
4.7 Adjusting Lenses Angle	13
5 Alarm Configuration	14
Appendix 1 Lightning and Surge Protection	16
Appendix 2 Cybersecurity Recommendations	17

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

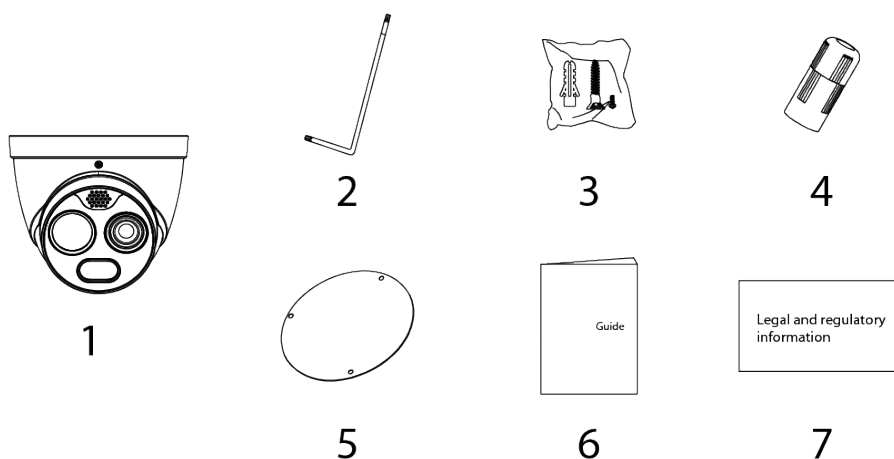


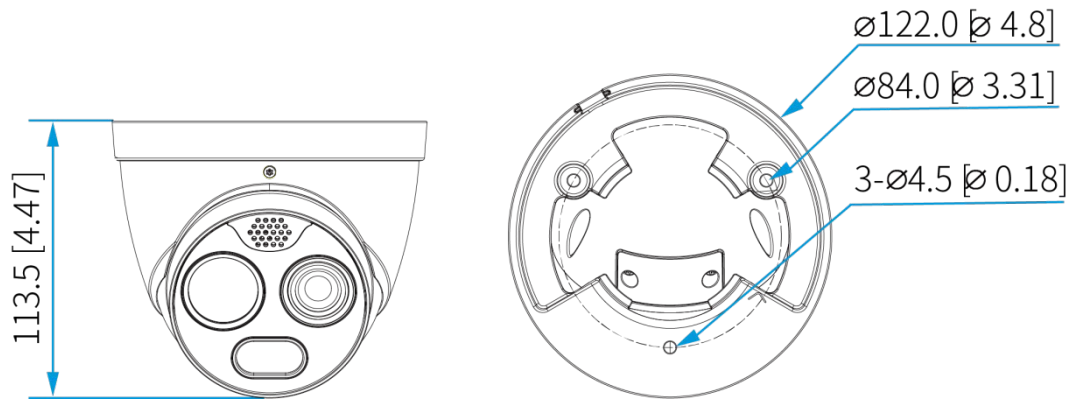
Table 1-1 Checklist

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/Installation guide	1
7	Legal and regulatory information	1

2 Design

2.1 Dimensions

Figure 2-1 Dimensions (mm [inch])



2.2 Cables

Figure 2-2 Cables

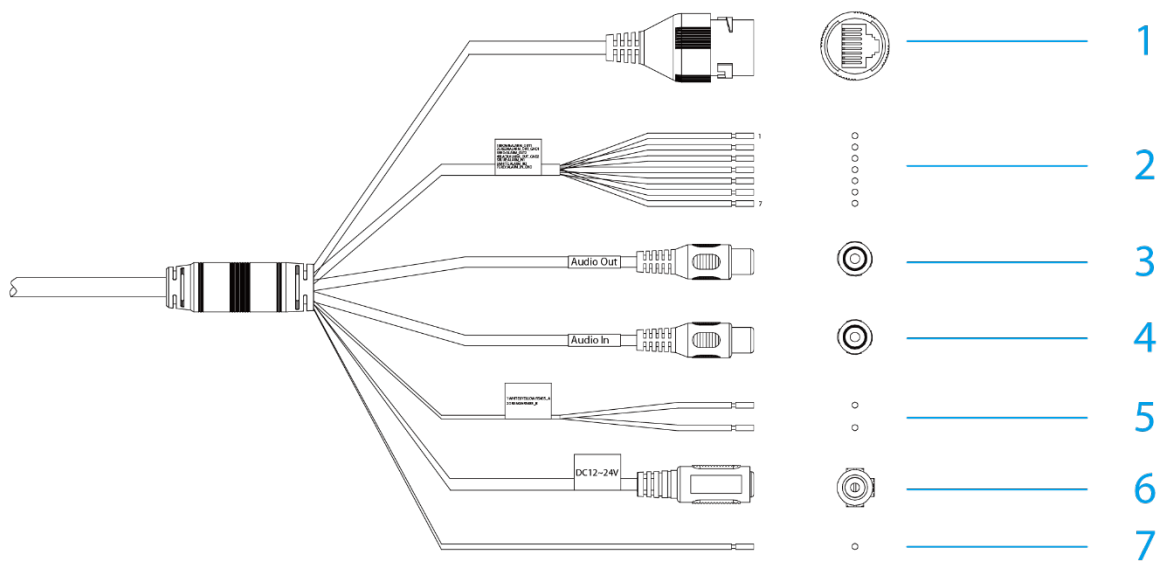



Table 2-1 Ports description

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

	ALARM_OUT2	used together.
	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	<p>Inputs 12 VDC voltage.</p>  DANGER <p>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.</p>
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

The screenshot shows the 'Device Initialization' web interface. At the top, there is a dark blue header with the text 'Device Initialization'. Below the header, there is a light blue navigation bar with four tabs: 'Region Setting' (selected with a blue icon), 'Time Zone Setting' (with a clock icon), 'Password Setting' (with a key icon), and 'P2P' (with a cloud icon). The main content area is white and contains three dropdown menus: 'Area' (with a grey background and a downward arrow), 'Language' (with 'English' selected and a downward arrow), and 'Video Standard' (with 'NTSC' selected and a downward arrow). At the bottom center of the main content area, there is a blue button labeled 'Next'.

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

Figure 3-2 Time zone setting

The screenshot shows the 'Time Zone Setting' step in the 'Device Initialization' wizard. The progress bar at the top indicates that 'Region Setting' is completed, 'Time Zone Setting' is the current step, and 'Password Setting' is pending. The main content area includes a 'Date Format' dropdown set to 'YYYY-MM-DD', a 'Time Zone' dropdown set to '(UTC-08:00)Pacific Time (US & Canada)', and a 'System Time' section showing '2020-08-13' and '17:12:46' with a 'Sync PC' button. Below this, it states 'Will be modified as 2020-08-13 01:12:46'. A blue 'Next' button is at the bottom.

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

Figure 3-3 Password setting

The screenshot shows the 'Password Setting' step in the 'Device Initialization' wizard. The progress bar at the top indicates that 'Region Setting' and 'Time Zone Setting' are completed, and 'Password Setting' is the current step. The main content area includes a 'Username' field with 'admin', a 'New Password' field with a strength indicator, a 'Confirm Password' field with a green checkmark, and a 'Reserved Email' checkbox with a text field containing '.com'. Below the email field, it says 'For password reset. Recommended or improved in time.' A blue 'Next' button is at the bottom.

Step 4 Set the password for admin account.

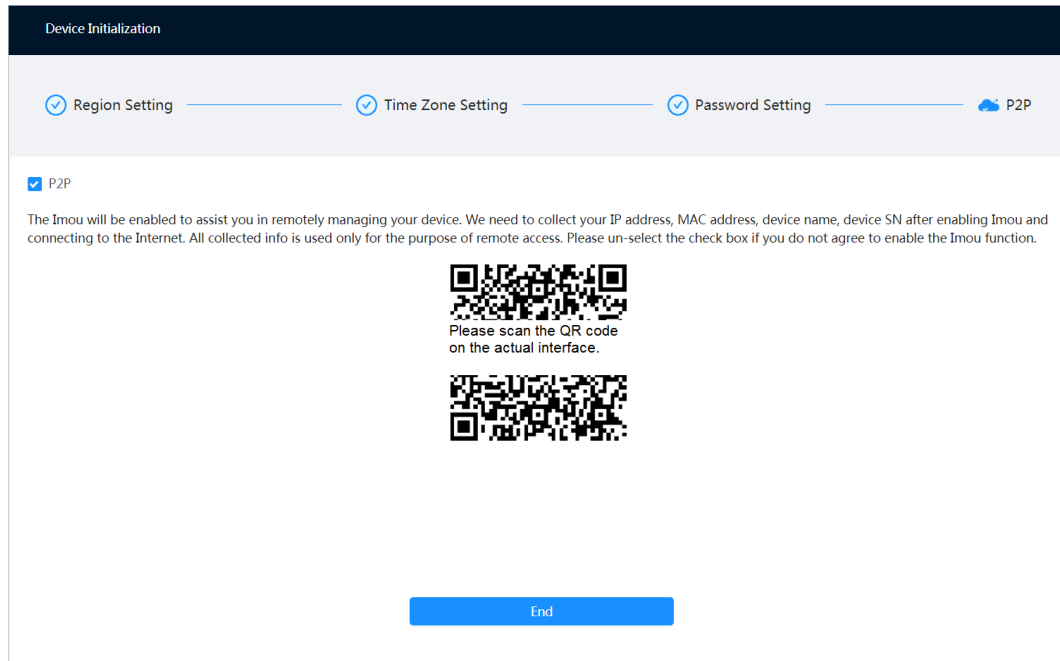
Table 3-1 Description of password configuration

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



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: ☒

NIC: Wired(Default)

Mode: ☒ Static ☐ DHCP

MAC Address: [Hex digits]

IP Version: IPv4

IP Address: [Hex digits]

Subnet Mask: [Hex digits]

Default Gateway: [Hex digits]

Preferred DNS: [Hex digits]

Alternate DNS: [Hex digits]

Buttons: Apply, Refresh, Default

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.



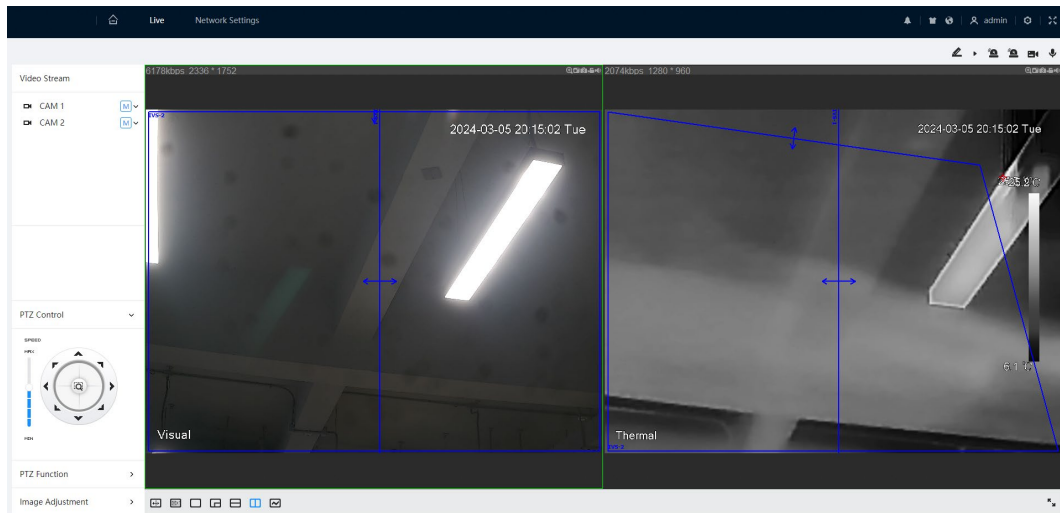
The default username is admin, and the password is the one that was set during initialization.

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



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

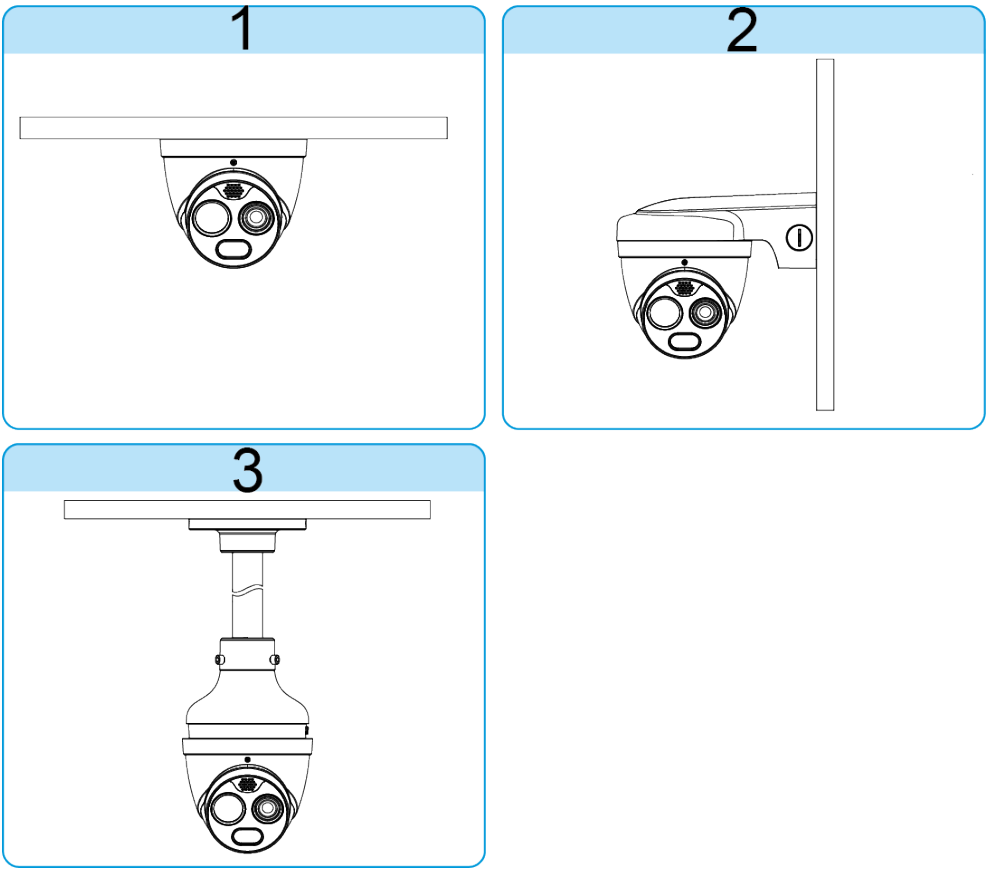
Extension Distance [m (ft.)]	Cord Diameter (mm)
10 (32.81)	0.9
15 (49.21)	1.1
20 (65.62)	1.3
25 (82.02)	1.5
30 (98.43)	1.6
35 (114.83)	1.7
40 (131.23)	1.8
50 (164.04)	1.9

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 (24 AWG) and above.

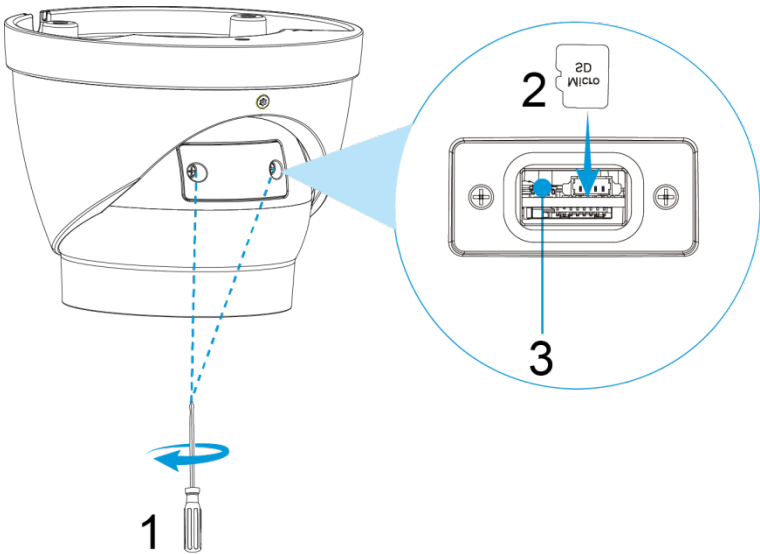
4.2 Selecting Installation Methods

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)

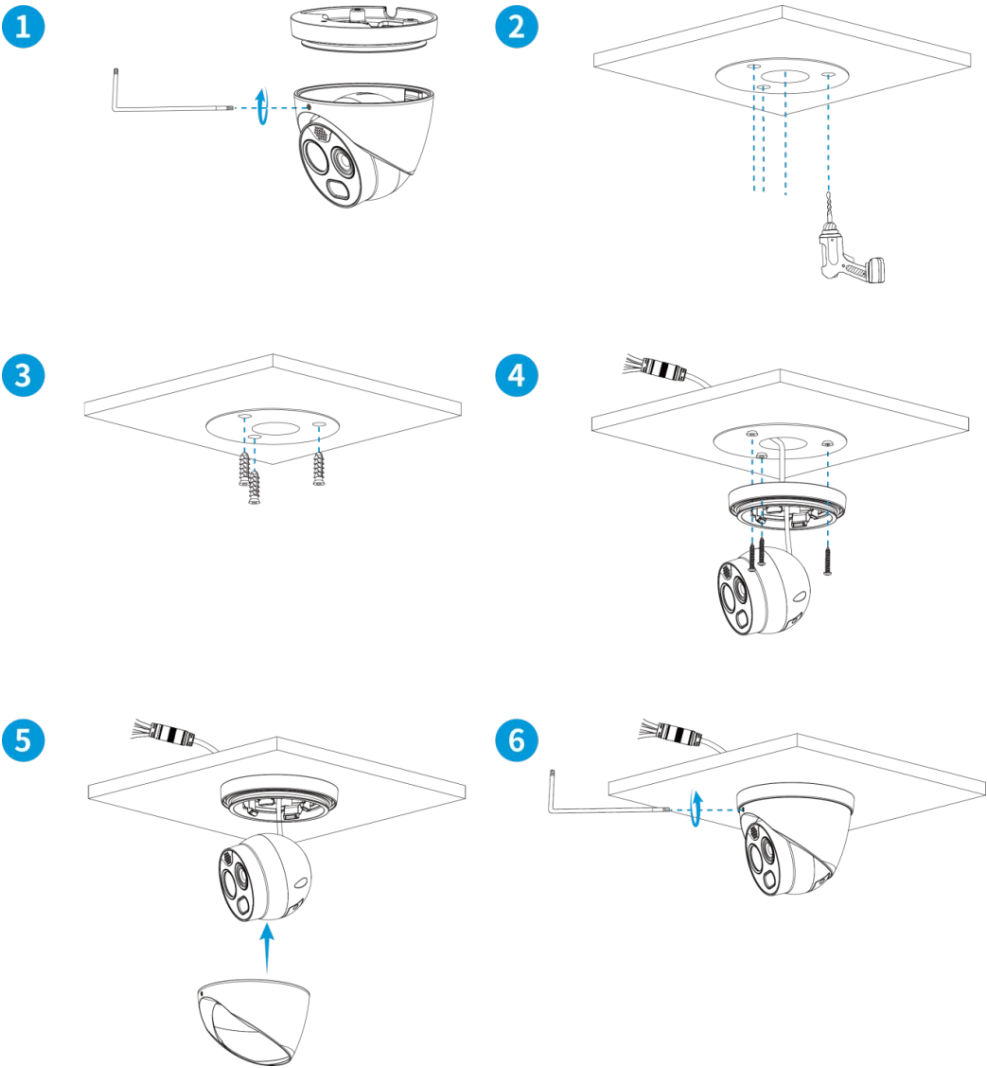
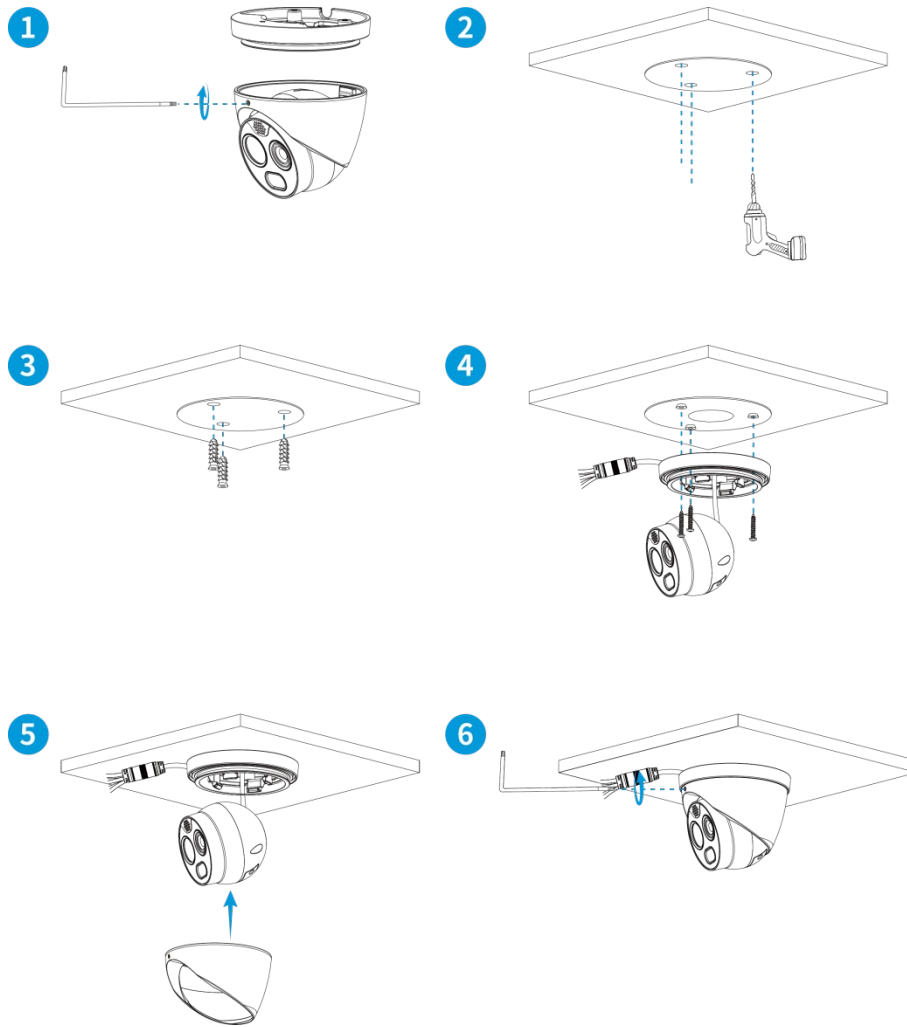
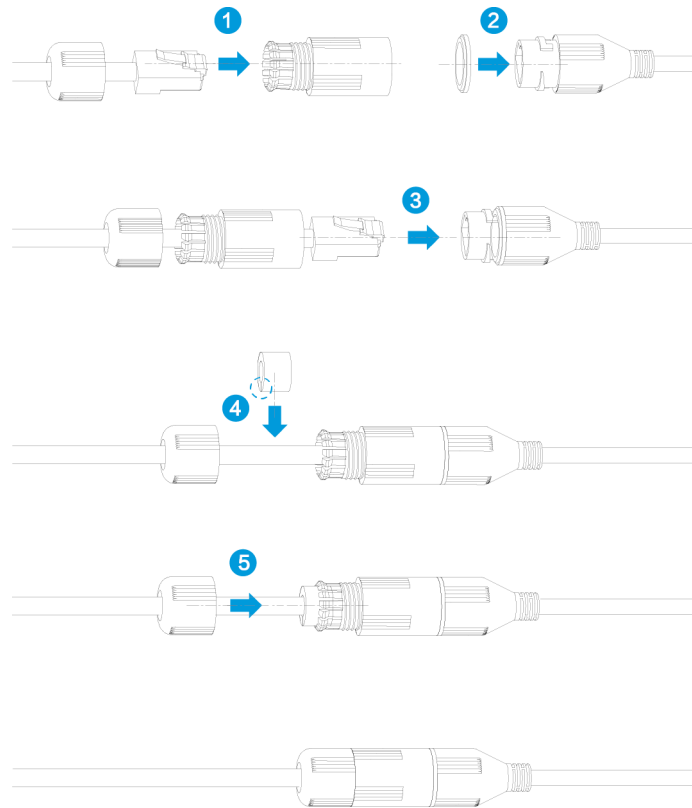


Figure 4-4 Cable tray (through the pedestal side)



4.5 Installing Waterproof Connector

Figure 4-5 Installing waterproof connector for network port

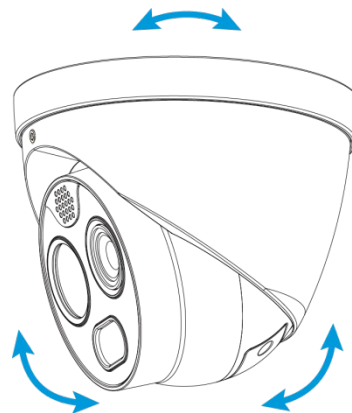


4.6 Connecting Cable Ports

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

4.7 Adjusting Lenses Angle

Figure 4-6 Adjusting lenses angle



5 Alarm Configuration



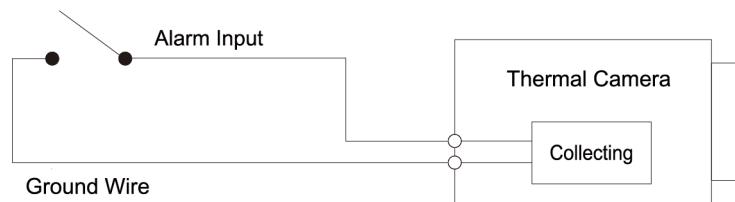
Cut off power before connecting cables.

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



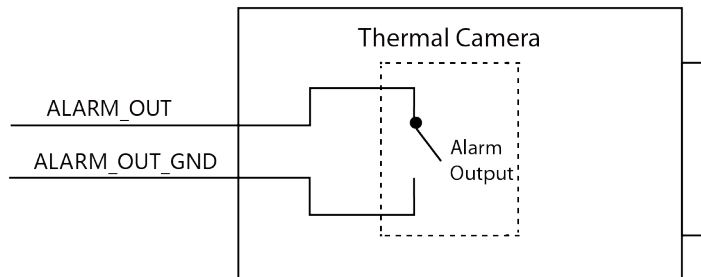
Step 2 Connect alarm output device to alarm output port of I/O cable. Alarm output is a relay switch output. The alarm output port can only be connected to NO alarm device.


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 4 Click  next to **Enable** to enable alarm linkage.

Step 5 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

Alarm-in Port

Alarm1

Mode

Alarm

Schedule

Full Time

Add Schedule

Anti-dither

0

sec (0-100)

Sensor Type

NO

+Event Linkage

Record

Enabled

Channel

1

2

Post-Record

10

sec (10-300)

Alarm-out Port

Enabled

Alarm Channel

1

2

Post-alarm

3

sec (3-300)

Apply

Refresh

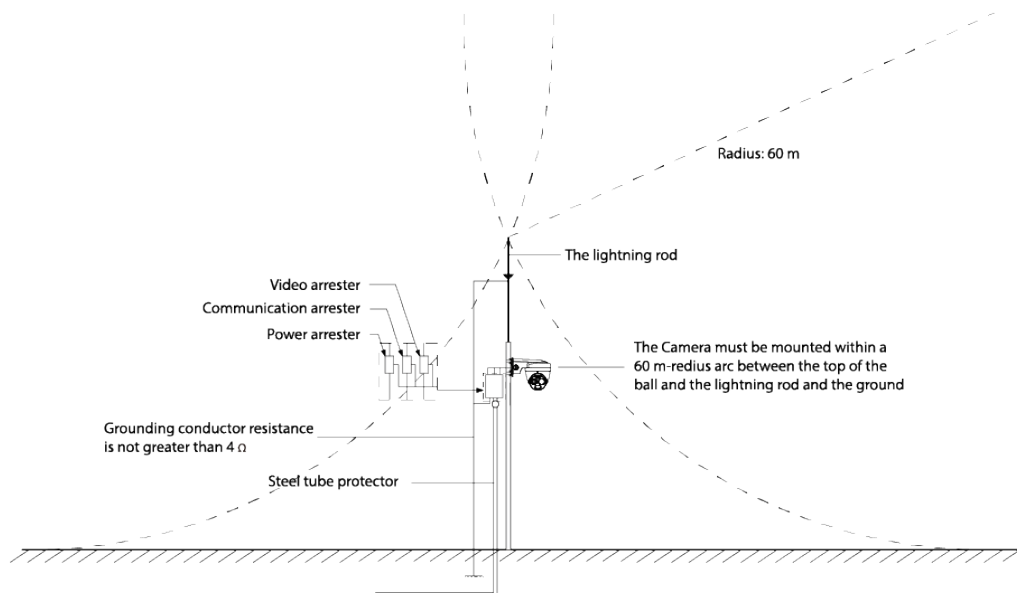
Default

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 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.