Network PTZ Camera

Installation Manual

V1.0.1

Regulatory Information

The regulatory information herein might vary according to the model you purchased. Some information is only applicable for the country or region where the product is sold.

FCC Information

⚠ CAUTION

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC conditions:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

FCC compliance:

This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication.

This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.

For class B device, these limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

SDOC Statement: https://us.dahuasecurity.com/support/notices/

Battery Replacement and Disposal

Applicable to products with battery.

⚠ CAUTION

Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

Foreword

General

This Installation Manual (hereinafter referred to as “Manual”) introduces the appearance, preparation before installation, and installation of the Network PTZ Camera (hereinafter referred to as “camera”).

Safety Instructions

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

Signal Words	Meaning
📖NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First Release.	November, 2018
V1.0.1	Optimized the language; increased the description of sticker.	June, 2019

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

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

Read the Manual carefully before using the camera, comply with them when using, and keep it well for future reference.

Requirements

- Requirements for installation personnel:
  - ◇ Have certificates related to installation and maintenance of the closed-circuit television (CCTV).
  - ◇ Have certificates related to working at height.
  - ◇ Have basic knowledge and operation technique for low-voltage wiring and low-voltage electronic circuit connection.
  - ◇ Read the Manual carefully and comprehend all the content.
- Requirements for lifting appliance
  - ◇ Select appropriate lifting appliances.
  - ◇ The lifting appliances can reach the installation height.
  - ◇ The lifting appliances shall have high safety performance.
- Requirements for installation
  - ◇ All installation and operation here should conform to your local electrical safety regulations, fire protection regulations, and relevant regulations.
  - ◇ Make sure the application scenarios of the camera conforms to the installation requirements. Contact your local retailer or customer service center if there is any problem.
  - ◇ Keep the original packing material well, you may need it to pack the camera and send it back for repair.

Warning

- Do not press hard, violently vibrate, and soak the radar when transporting, storing, and installing it.
- If smoke and abnormal odor occur, you should power off the camera, and then contact us.
  - ◇ Do not look directly at the laser light.
  - ◇ Do not disassemble or refit the camera.
- Do not put metal objects or flammable materials into the camera; otherwise fire, short-circuit, or other damage will occur.
- Power off the camera and disconnect the power supply immediately if water or liquid flows into the camera, and then contact the customer service center. Avoid the sea water or rain eroding the camera.
- Keep the camera away from devices that generate electromagnetic field like televisions, radio transmitters, electromagnetic devices, electric machine, transformers, and speakers; otherwise image quality will be influenced.
- Keep the camera away from smoke, vapor, heat, and dust.

- Install the camera at places with good condition of ventilation and cooling.
- Do not aim the lens directly at intense light like the sun, illuminators; otherwise the lens will be damaged.

Cleanning

- Use soft cloth that moistened with cleaning solution to clean the camera, and then dry the camera. Do not use gasoline, paint diluent, or other chemicals to clean the camera; otherwise deformation and paint peeling might occur.
- Read all the manuals included before you use chemical cloth. Do not let the housing of the camera be in contact with plastic or rubber materials for too long; otherwise damage to the housing or peeling paint will occur.

Table of Contents

1 Structure

After unpacking the box, check if there is obvious damage to the appearance of the camera, and make sure the components are complete against the packing list.

1.1 Appearance and Components

Appearance

📖

The camera has two types: Wi-Fi type and PoE type.

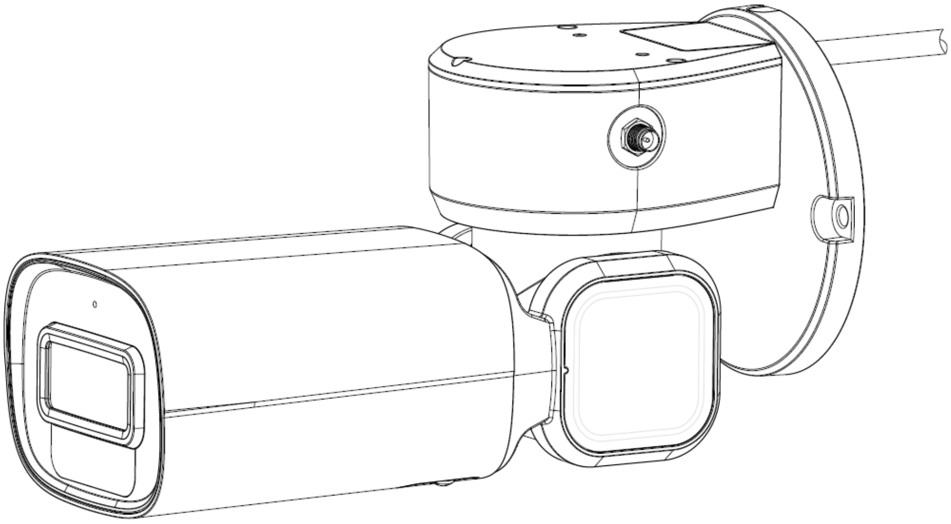
◇ Wi-Fi type: with antenna;

◇ PoE type: without antenna.

◇ Wi-Fi type camera will be taken as an example to introduce the installation.

For appearance of the camera, see Figure 1-1.

Figure 1-1 Appearance



1.2 Component

Unscrew screws at the bottom, remove the bottom cover, and then you can see the reset button and TF card.

Figure 1-2 Reset button and TF card

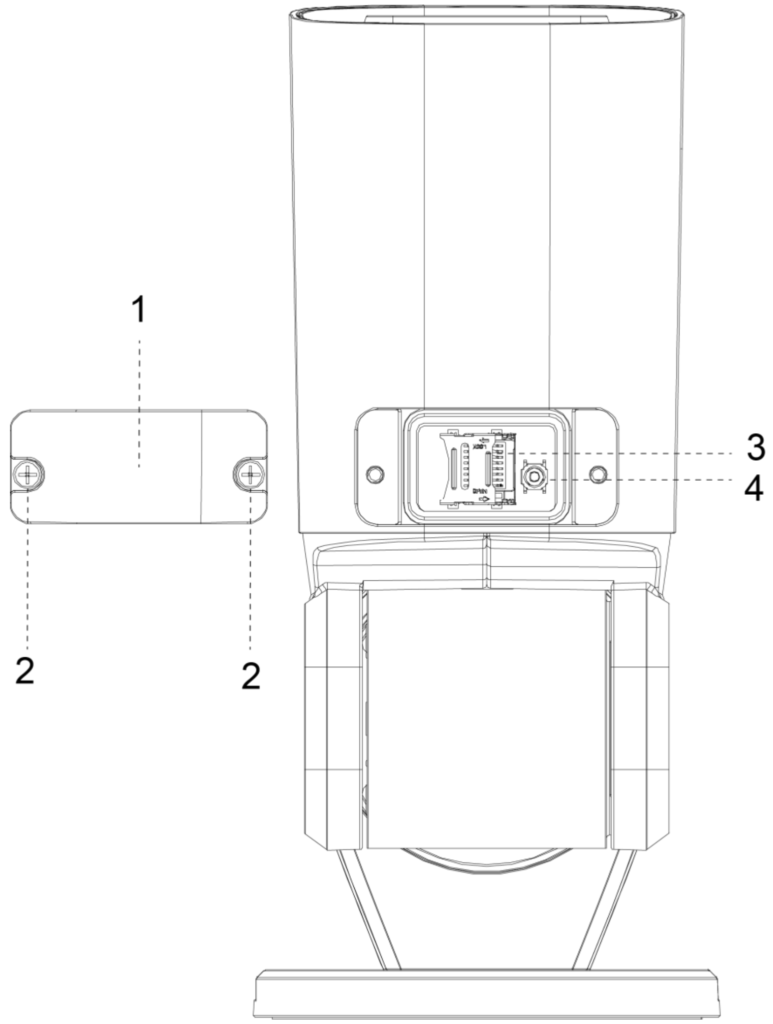


Table 1-1 Component

No.	Name
1	Cover
2	Screw
3	TF card slot
4	Reset button

Reset Button

- The reset button is used to restore the camera to the factory settings.
- After you have opened the camera rear cover, press and hold the reset button for over 10 seconds, and the camera will be restored to the factory default settings.

TF Card

The TF card is for data storage.

Make the side with metal dots face downwards, and insert the card into the card slot.

- When removing the TF card, if you push the card inside a little, and the card will be ejected automatically.
- Make sure that the TF card is removed when the camera is not communicating or transferring information; otherwise files will be corrupted and the TF card will be damaged.

1.3 Cables

1.3.1 Cable Preparation

Select video cables depending on the transmission distance.

1.3.2 Cable Requirement

- 75 ohm.
- Pure copper cored cables.
- 95% braided copper shielding.
- For RS-485 communication cable, see “Appendix 2 RS-485 Cable”.

Table 1-2 Cable model

China Model	International Model	Maximum Transmission Distance
RG59/U	RG59/U	750 ft/229 m
5C–2 V	RG6/U	1,000ft/305m
7C–2 V	RG11/U	1,500ft/457m

Cable specifications above are only applicable to network cameras.

1.3.3 Select Power Cables

For 12V AC power source devices, see “Appendix 3 Relationship between Cable Diameter (12V DC) and Transmission Distance ”.

For PoE power source devices, see Table 1-3.

Table 1-3 Cable model

PoE specification	Cable specification
AF	CAT4 and above
AT	CAT5 and above
HiPoE or BT	CAT5E and above

Cable Description

The camera is equipped with a multi-functional cable including power cord, video cable, audio cable, RS-485 control cable, alarm cable, network cable, audio cable, and optical fiber cable. For picture of the multi-functional cable, see Figure 1-3.

Camera cables can be different depending on different models, and the actual cables shall prevail.

Figure 1-3 Cables

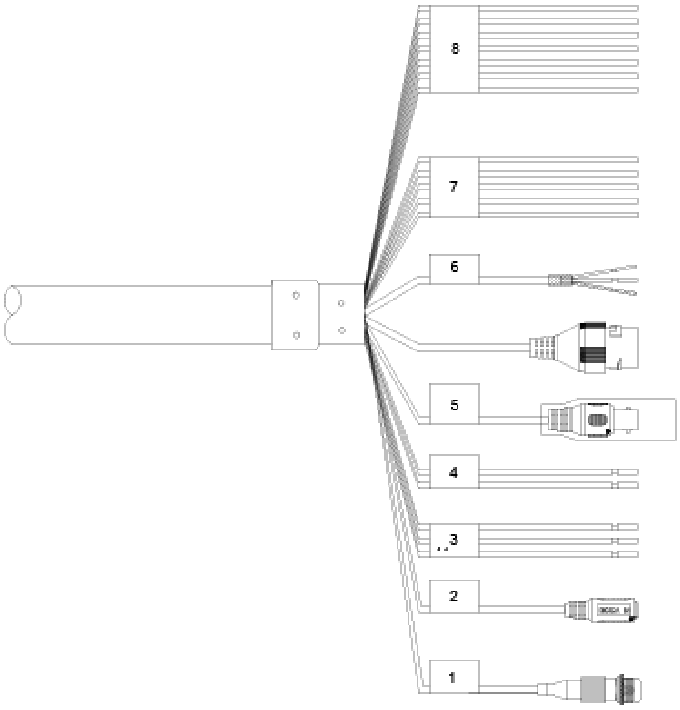


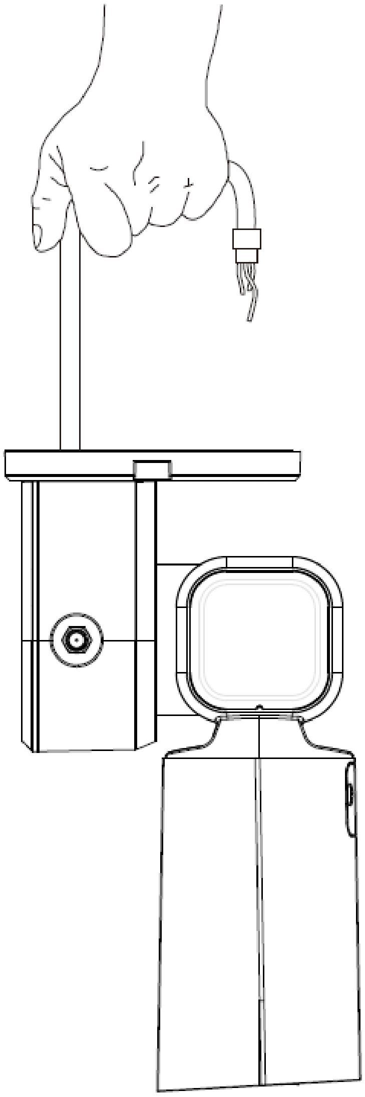
Table 1-4 Cable descriptions

No.	Description
1	FC connector
2	DC power input port
3	24V AC power input. ● Red: V+ ● Black: V– ● Yellow-green: ground cable
4	RS-485: Yellow: A+, Orange: B–
5	Video output port
6	Ethernet port: ● White: audio input ● Red: audio output ● Black: audio ground cable
7	● Blue: alarm output 1 ● Black: alarm output 2 ● Green: contact switch 1 ● Pink: contact switch 2 ● Yellow-green: ground cable
8	● Red: alarm input 1 ● Brown: alarm input 2

No.	Description
	● Grey: alarm input 3 ● Light green: alarm input 4 ● Purple: alarm input 5 ● White: alarm input 6 ● Yellow-black: alarm input 7

Do not carry the camera as displayed in Figure 1-4.

Figure 1-4 Wrong way of carrying the camera



Cable Connection

Connect the multi-functional cable of the bracket to the multi-functional cable (including power cord, video cable, audio cable, RS-485 control cable, alarm cable, network cable, high-frequency signal cable, and optical fiber cable) of the camera. Wrap the cable joints around with insulated rubber tape and do waterproof operations.

📖

The cable diameter of the RS-485 control cable can not be too large; otherwise the control performance can be influenced. For details of the RS-485 cable, see “Appendix 2 RS-485 Cable”.

There are thermal contraction tube around the video output port. After the connection is finished, heat the two ends of the tube to make the video output port moistureproof and waterproof.

Ground Cable Connection

Connect the yellow-green power cord of the multi-functional cable to the anti-thunder device, and make sure the lightning protection device is connected to the ground cable.

2 Install the Camera

2.1 Check before Installation

- 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 bracket and wall where the camera is installed have the capacity to bear eight times the weight of the speed and its accessories.
- Make sure the wall is thick enough to allow bolts to be installed.
- If the camera is laser camera, the installation height should be above 6 meters.

2.2 Sticker

There is a sticker in the package. The sticker helps you drill cable entries and srew holes at right places in the wall or ceiling.

📖

When pasting stickers, make the arrow in the sticker face downwards; otherwise the camera might be damaged.

Figure 2-1 Sticker

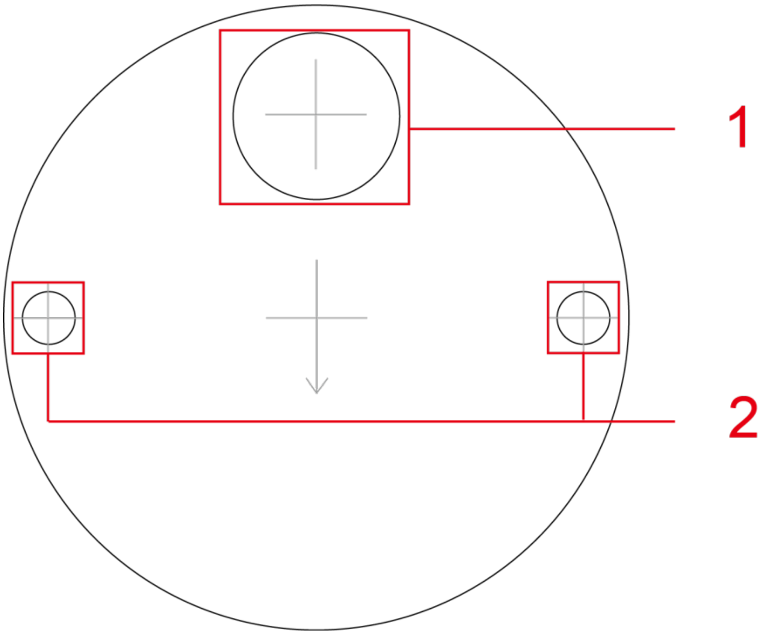


Table 2-1 Description of the sticker

No.	Description
1	Cable entry
2	Screw hole

2.3 Installation Procedure

Depending on the installation base, the camera can be installed in two manners: installed on the wall and installed on the ceiling.

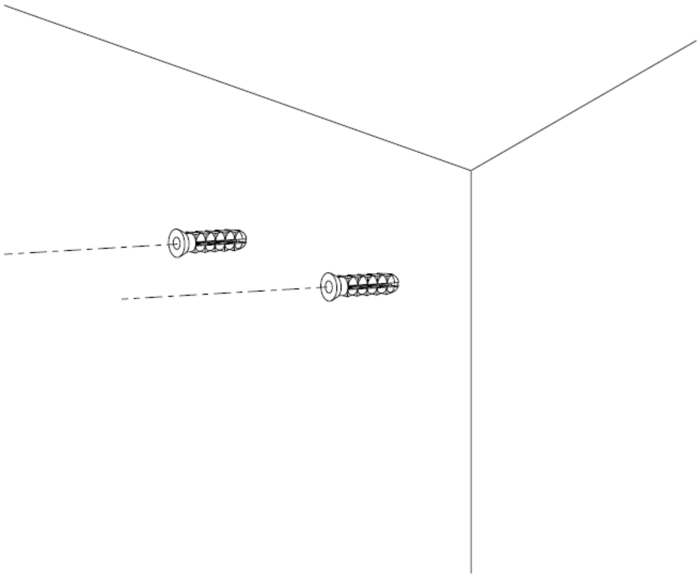
2.3.1 Installed on the Wall

Step 1 Stick stickers on the wall.

Step 2 Drill bolt holes in the wall according to holes on the sticker.

Step 3 Put expansion screws into the holes you drilled.

Figure 2-2 Put expansion screws into the holes



Step 4 Connect the camera cables to external cables, put cables into the junction box, and then do waterproof operations.

Step 5 Place the camera on the wall, and tighten the expansion screws to fix the camera on the wall.

Figure 2-3 Fix the camera on the wall

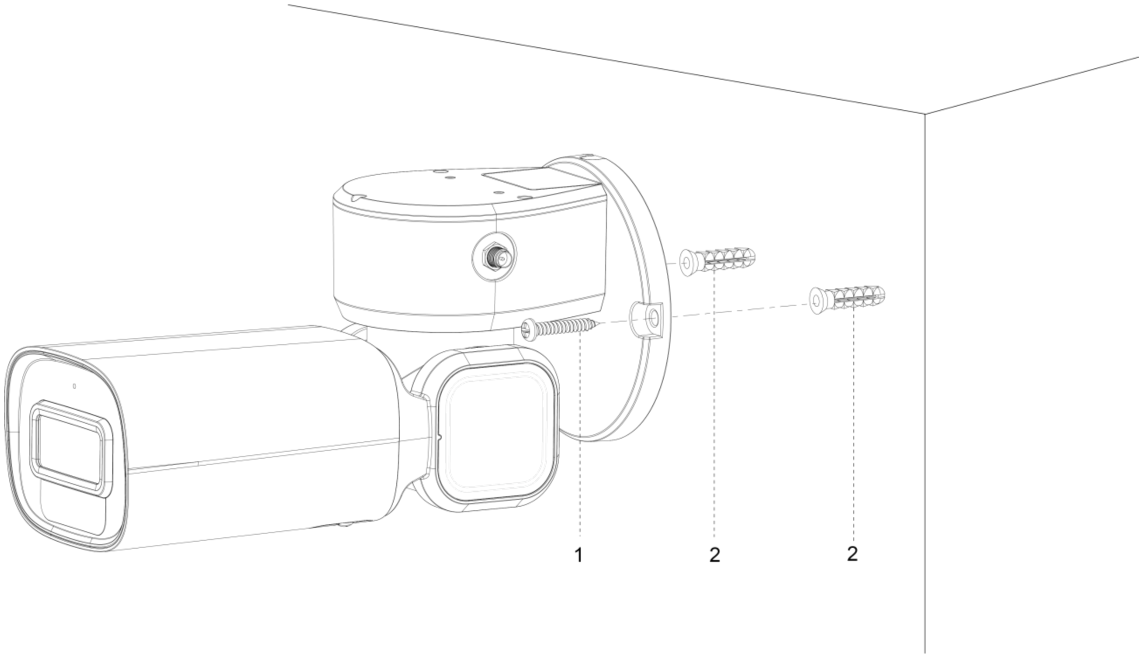


Table 2-2 Components

No.	Name
1	ST4 Screw
2	Expansion Screw

Step 6 (Optional) Choose whether to install a junction box between the camera base and the wall or not.

Figure 2-4 Install the junction box

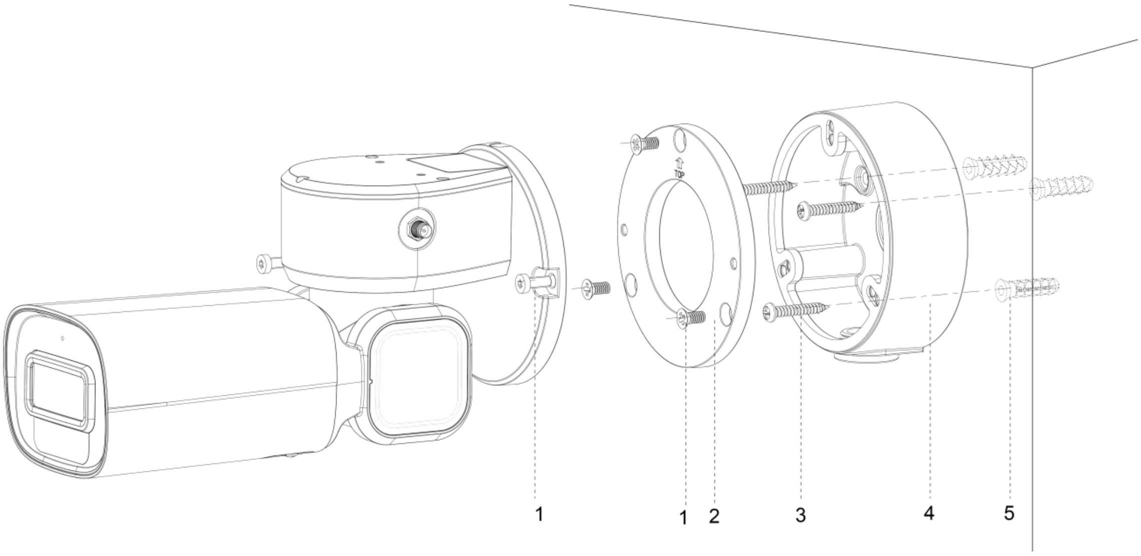
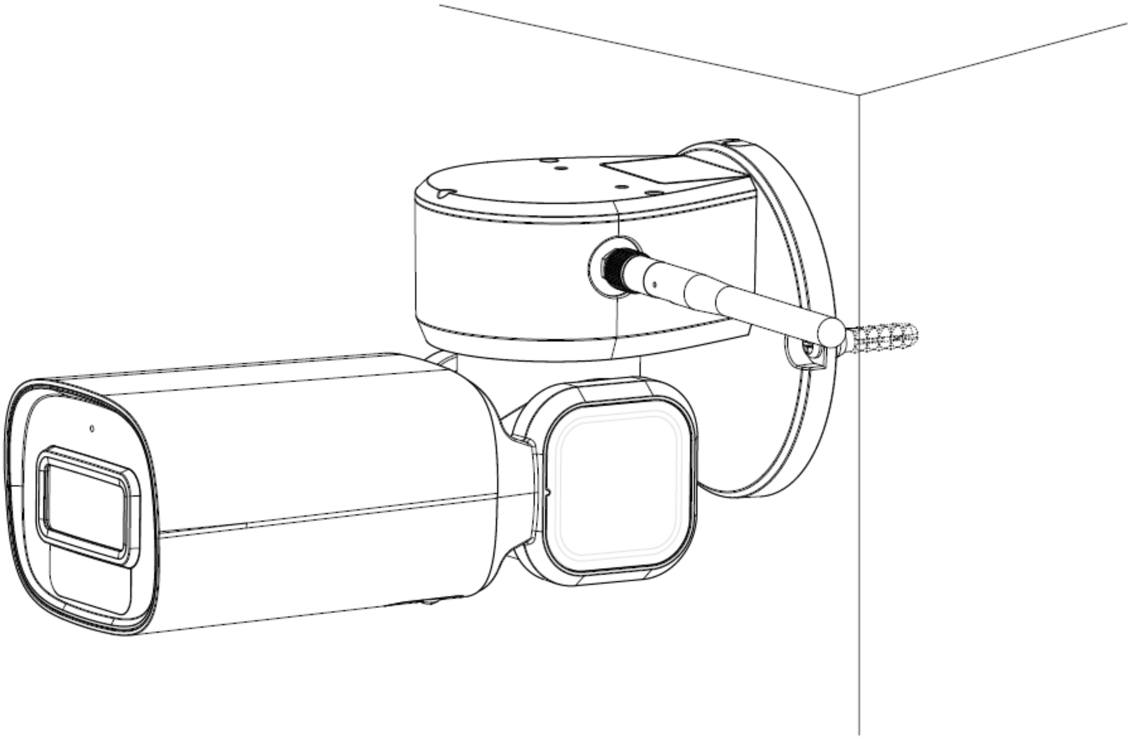


Table 2-3 Components

No.	Name
1	M4 Screw
2	Mounting plate
3	ST4 Screw
4	Junction box
5	Expansion screw

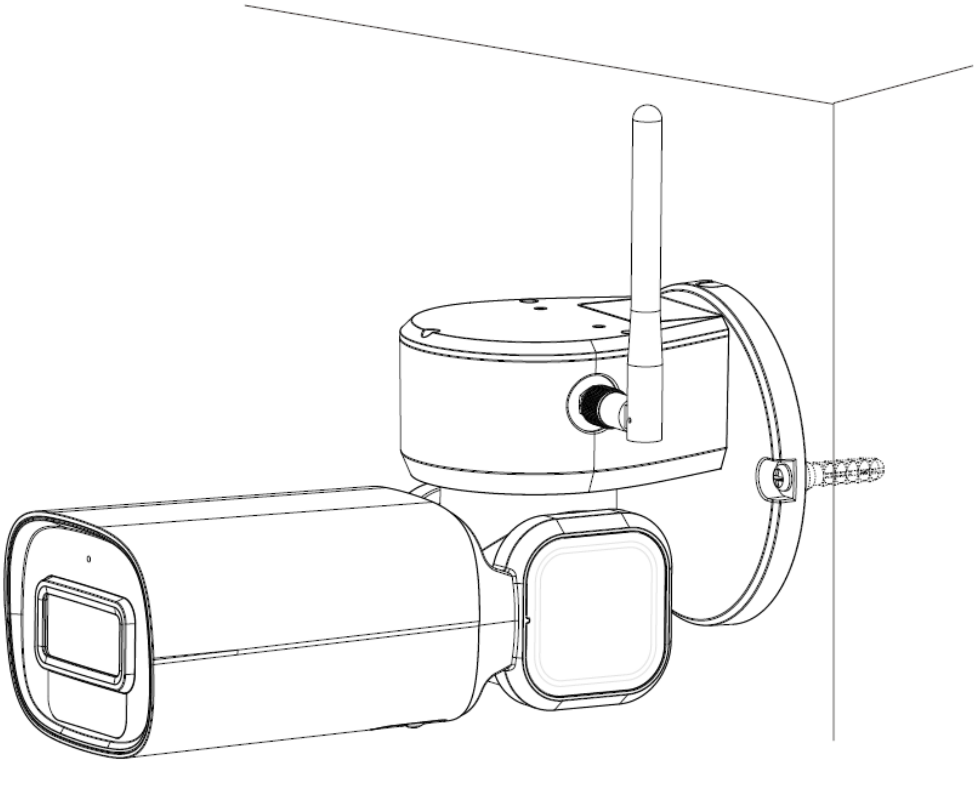
Step 7 Install the Wi-Fi antenna to the camera cover.

Figure 2-5 Install the Wi-Fi antenna



Step 8 Pull the Wi-Fi antenna up to complete the installation.

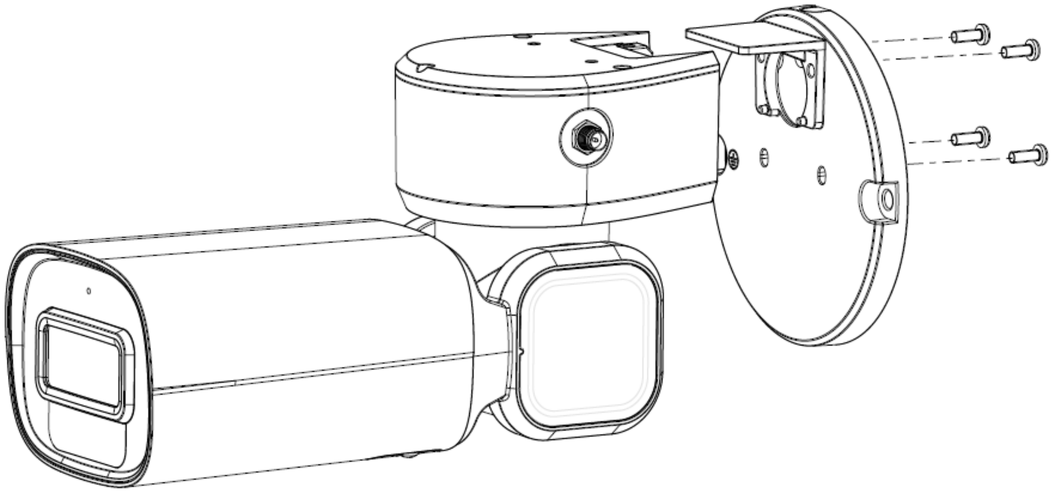
Figure 2-6 Pull the Wi-Fi antenna up



2.3.2 Installed on the Ceiling

Step 1 Detach the mounting plate from the back of the camera.

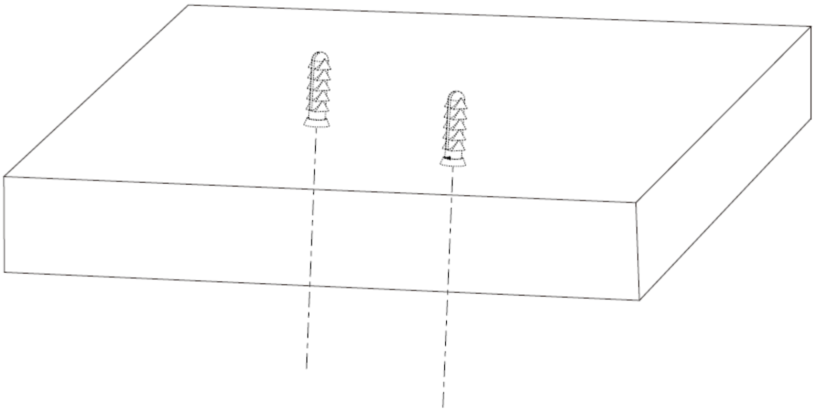
Figure 2-7 Detach the mounting plate



Step 2 Drill bolt holes in the ceiling according to holes on the sticker.

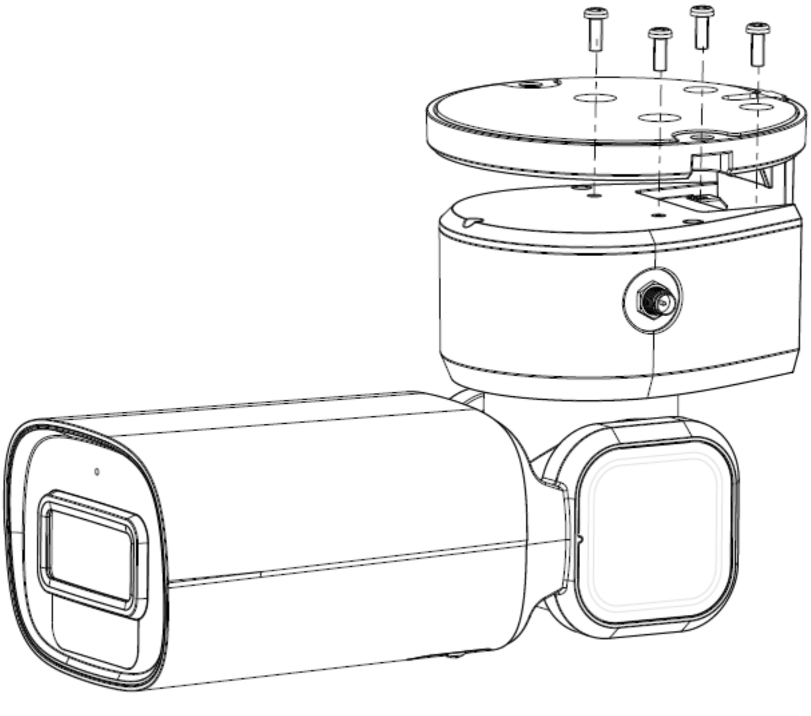
Step 3 Place expansion screws into the ceiling.

Figure 2-8 Place expansion screws into the ceiling



Step 4 Fix the mounting plate on the top of the camera.

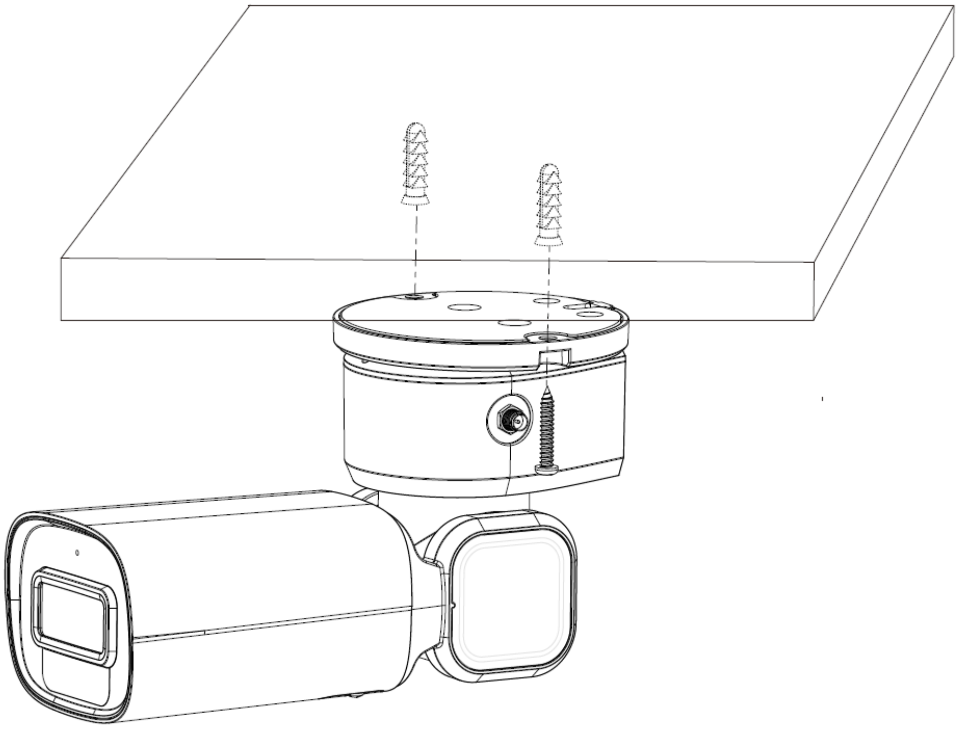
Figure 2-9 Fix the mounting plate



Step 5 Connect cables, do waterproof operations, and put cables into the junction box.

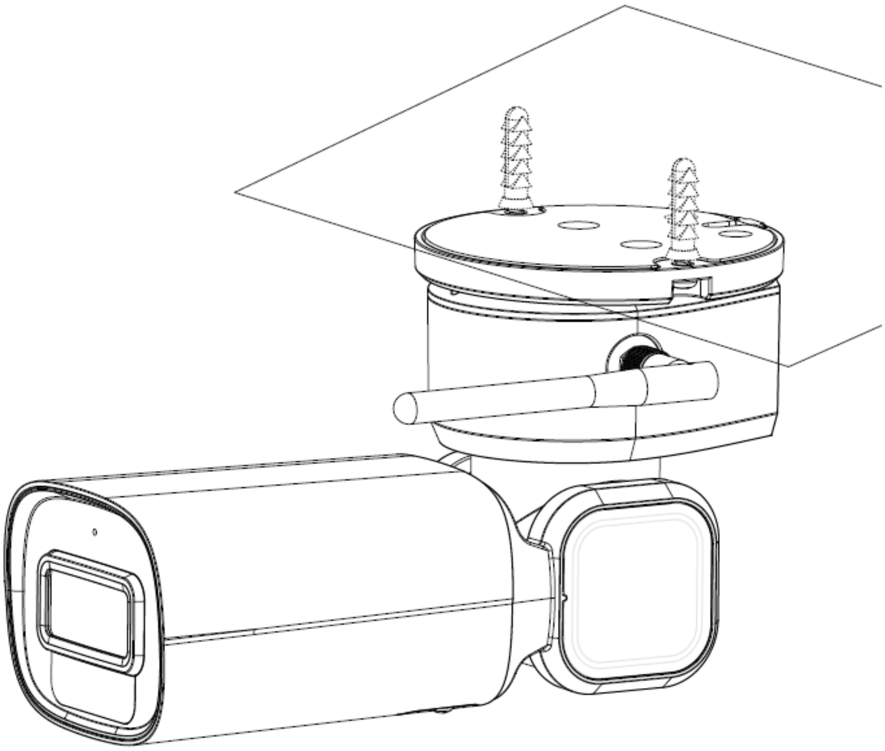
Step 6 Fix the camera on the ceiling.

Figure 2-10 Fix the Camera on the ceiling



Step 7 Install the Wi-Fi antenna and pull it up to complete the installation.

Figure 2-11 Install the Wi-Fi antenna

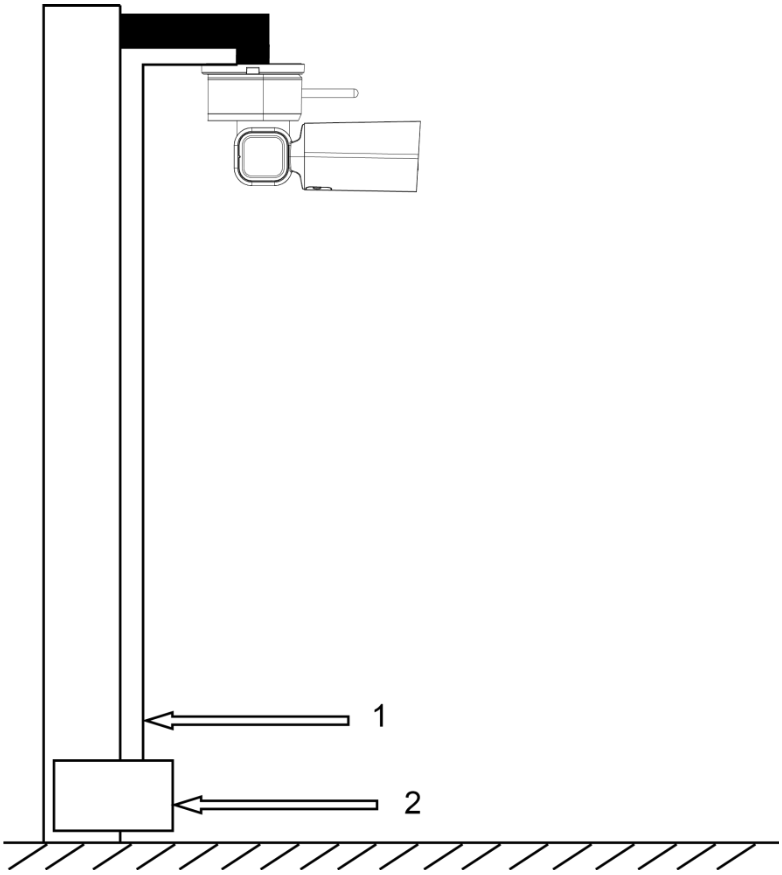


Appendix 1 Thunder-Proof and Surge Protection

Install Lightning Protection Devices Indoors

You shall use multiple copper cables whose cross-sectional area are not less than 25mm^2 to connect the yellow-green ground cable/ground screws to the indoor equipotential earthing terminals. See Appendix figure 1-1.

Appendix figure 1-1 Instal lightning protection device indoors



Appendix table 1-1 Description of lightning protection device

No.	Name
1	Yellow-green ground cable
2	Indoor equipotential earthing terminal

Appendix 2 RS-485 Cable

General

RS-485 industrial buses are half-duplex communication buses whose characteristic impedance is 120Ω. Its maximum load is 32 payloads (including drivers and receivers).

RS-485 Transmission Distance

When using 0.56 mm (24AWG) twisted pair, depending on different baud rates, the maximum theoretical transmission distances are listed. See Appendix table 2-1.

Appendix table 2-1 Theoretical maximum transmission distance

Baud rate	**Maximum transmission distance**
2400 bps	1800 m
4800 bps	1200 m
9600 bps	800 m

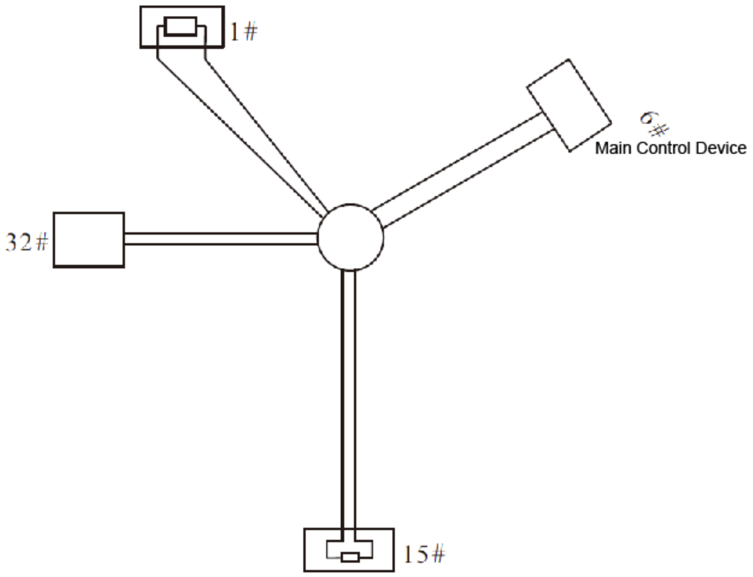
The maximum transmission distance might be reduced in the following conditions; otherwise, maximum transmission distance will be increased.

- When thinner communication cables are used;
- The camera is used in places with intense electromagnetic interference;
- Too many devices are connected to the RS-485 cable.

Frequently Occurred Problems

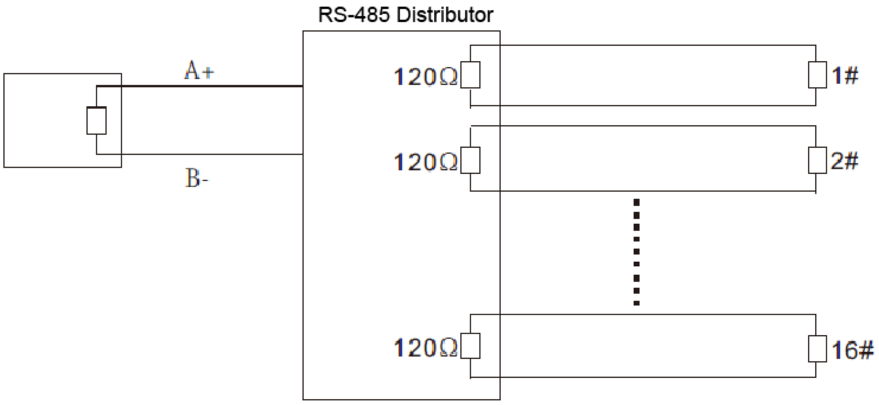
Customers tend to connect devices as the way displayed in Appendix figure 2-1. In this condition, the terminal resistance must be connected to the two devices whose cable length is the largest among all the devices (in Appendix figure 2-1, cable length between 1# and 15# is the largest). However, this connection manner dose not comply with the RS-485 industrial bus standard. As a result, problems like signal reflection and anti-interference capability reduction might occur. Due to the above mentioned problems, the camera can be out of control.

Appendix figure 2-1 The common manner of connecting devices



To solve the problems, we recommend that you use RS-485 distributors. The RS-485 distributor can avoid the common manner of connection so as to improve transmission quality. See Appendix figure 2-2.

Appendix figure 2-2 RS-485 distributor applied



FAQ

Problem	Possible reason	Solution
The camera can do self-check but it can not be controlled.	Baud rate and IP address of the host and camera are not properly configured.	Modify the baud rate/IP address of the host and camera to make them the same.
	Positive electrode and negative electrode of RS-485 cable are misconnected.	Connect cables to the positive electrode and negative electrode correctly.
	Loose connection	Connect the cables firmly.
	RS-485 cable is broken.	Replace the broken RS-485 cable with a new one.
The camera can be controlled, but the	RS-485 cable is in poor contact.	Connect the RS-485 cable firmly.
	One of the RS-485 cables is	Replace the broken RS-485 cable with a

Problem	Possible reason	Solution
control is not smooth.	broken.	new one.
	The distance between the host and camera is too long.	Install terminal resistance.
	Too many cameras are connected in parallel.	Install RS-485 distributors.

Appendix 3 Relationship between Cable Diameter (12V DC) and Transmission Distance

- The recommended transmission distances are for reference only, and the actual conditions shall prevail.
- The chart below gives the maximum transmission distance of cables with certain diameters when the 12V DC power source voltage lose rate is bellow 10%.
- For cameras powered by direct current, the maximum voltage loss rate allowed is 10%.
- Cables mentioned in the table below are copper cables (the resitivity of copper $\rho = 0.0175\Omega * \text{mm}^2/\text{m}$)

Transmission power (W)	**Cable diameter (mm)**			
	0.8000	**1.000**	**1.250**	**2.000**
	Transmission distance Feet (m)			
5	122.13 (37.23)	190.83 (58.16)	298.17 (90.88)	763.31 (232.66)
10	61.06 (18.61)	95.41 (29.08)	149.08 (45.44)	381.66 (116.33)
15	40.71 (12.41)	63.61 (19.39)	99.39 (30.29)	254.44 (77.55)
20	30.53 (9.31)	47.71 (14.54)	74.54 (22.72)	190.83 (58.16)
25	24.43 (7.45)	38.17 (11.63)	59.63 (18.18)	152.66 (46.53)
30	20.35 (6.20)	31.80 (9.69)	49.69 (15.15)	127.22 (38.78)
35	17.45 (5.32)	27.26 (8.31)	42.60 (12.98)	109.04 (33.24)
40	15.27 (4.65)	23.85 (7.27)	37.27 (11.36)	95.41 (29.08)
45	13.57 (4.14)	21.20 (6.46)	33.13 (10.10)	84.81 (28.85)
50	12.21 (3.72)	19.08 (5.82)	29.82 (9.09)	76.33 (23.27)
55	11.10 (3.38)	17.35 (5.29)	27.11 (8.26)	69.39 (21.15)
60	10.18 (3.10)	15.90 (4.85)	24.85 (7.57)	63.61 (19.39)
65	9.39 (2.86)	14.68 (4.47)	22.94 (6.99)	58.72 (17.90)
70	8.72 (2.66)	13.63 (4.15)	21.30 (6.49)	54.52 (16.62)
75	8.14 (2.48)	12.72 (3.88)	19.88 (6.06)	50.89 (15.51)
80	7.63 (2.33)	11.93 (3.64)	18.64 (5.68)	47.71 (14.54)
85	7.18 (2.19)	11.23 (3.42)	17.54 (5.35)	44.90 (13.69)
90	6.78 (2.07)	10.60 (3.23)	16.56 (5.05)	42.41 (12.93)
95	6.43 (1.96)	10.04 (3.06)	15.69 (4.78)	40.17 (12.25)
100	6.11 (1.86)	9.54 (2.91)	14.91 (4.54)	38.17 (11.63)

Appendix 4 Wire Gauge Reference Sheet

Metric bare wire diameter (mm)	AWG	SWG	Bare wire cross section area (mm^2)
0.050	43	47	0.00196
0.060	42	46	0.00283
0.070	41	45	0.00385
0.080	40	44	0.00503
0.090	39	43	0.00636
0.100	38	42	0.00785
0.110	37	41	0.00950
0.130	36	39	0.01327
0.140	35	/	0.01539
0.160	34	37	0.02011
0.180	33	/	0.02545
0.200	32	35	0.03142
0.230	31	/	0.04115
0.250	30	33	0.04909
0.290	29	31	0.06605
0.330	28	30	0.08553
0.350	27	29	0.09621
0.400	26	28	0.1257
0.450	25	/	0.1602
0.560	24	24	0.2463
0.600	23	23	0.2827
0.710	22	22	0.3958
0.750	21	/	0.4417
0.800	20	21	0.5027
0.900	19	20	0.6362
1.000	18	19	0.7854
1.250	16	18	1.2266
1.500	15	/	1.7663
2.000	12	14	3.1420
2.500	/	/	4.9080
3.000	/	/	7.0683

Appendix 5 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 Whitelist**

   We suggest you to enable whitelist 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 whitelist.

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.