Embedded Stereo Vision Passenger Flow Camera

Quick Start Guide

V1.0.0

Foreword

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Date
V1.0.0	First release.	2023.03

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

- Transport the device under allowed humidity and temperature conditions.
- Pack the device with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during transportation.

Storage Requirements

- 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 unstable illumination.
- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during storage.

Installation Requirements

 **WARNING**

- Strictly comply with the local electrical safety code and standards, and check whether the power supply is correct before operating the device.
- Please follow the electrical requirements to power the device.
  - ◇ When selecting the power adapter, 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.
  - ◇ We recommend using the power adapter provided with the device.
- Do not connect the device to two or more kinds of power supplies, unless otherwise specified, to avoid damage to the device.
- The device must be installed in a location that only professionals can access, to avoid the risk of non-professionals becoming injured from accessing the area while the device is working. Professionals must have full knowledge of the safeguards and warnings of using the device.

- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during installation.
- An emergency disconnect device must be installed during installation and wiring at a readily accessible location for emergency power cut-off.
- 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.

- Ground the earthing portion ⏚ of the device to improve its reliability.
- Ground the function earthing portion ⏚ of the device to improve its reliability (certain models are not equipped with earthing holes). The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- The lens is an optical component. Do not directly touch or wipe the lens surface during installation.

Operation Requirements

WARNING

- The cover must not be opened while the device is powered on.
- Do not touch the heat dissipation component of the device to avoid the risk of getting burnt.

- Use the device under allowed humidity and temperature conditions.
- Do not aim the device at strong light sources (such as lamplight, and sunlight) when focusing it, to avoid reducing the lifespan of the CMOS sensor, and causing overbrightness and flickering.
- When using a laser beam device, avoid exposing the device surface to laser beam radiation.
- Prevent liquid from flowing into the device to avoid damage to its internal components.
- Protect indoor devices from rain and dampness to avoid electric shocks and fires breaking out.
- Do not block the ventilation opening near the device to avoid heat accumulation.
- Protect the line 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 directly touch the photosensitive CMOS. Use an air blower to clean the dust or dirt on the lens.

● Strengthen the protection of the network, device data and personal information. All necessary safety measures to ensure the network security of the device must be taken, such as using strong passwords, regularly changing your password, updating firmware to the latest version, and isolating computer networks. For the IPC firmware of some previous versions, the ONVIF password will not be automatically synchronized after the main password of the system has been changed. You need to update the firmware or change the password manually.

Maintenance Requirements

- Strictly follow the instructions to disassemble the device. Non-professionals dismantling the device can result in it leaking water or producing poor quality images. For a device that is required to be disassembled before use, make sure the seal ring is flat and in the seal groove when putting the cover back on. When you find condensed water forming on the lens or the desiccant becomes green after you disassembled the device, contact after-sales service to replace the desiccant. Desiccants might not be provided depending on the actual model.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.
- Do not directly touch the photosensitive CMOS. Use an air blower to clean the dust or dirt on the lens. When it is necessary to clean the device, slightly wet a soft cloth with alcohol, and gently wipe away the dirt.

- 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.
- The lens is an optical component. When it is contaminated with dust, grease, or fingerprints, use degreasing cotton moistened with a little ether or a clean soft cloth dipped in water to gently wipe it clean. An air gun is useful for blowing dust away.
- It is normal for a camera made of stainless steel to develop rust on its surface after being used in a strong corrosive environment (such as the seaside, and chemical plants). Use an abrasive soft cloth moistened with a little acid solution (vinegar is recommended) to gently wipe it away. Afterwards, wipe it dry.

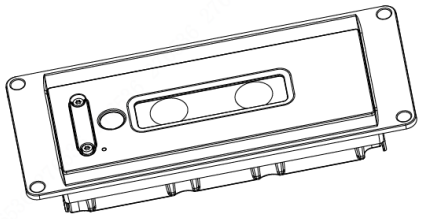
Contents

1 Structure

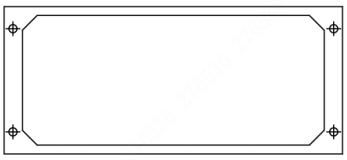
1.1 Unpack and Check

- The following figures are for reference only, and the actual product shall prevail.
- For tools or accessories not mentioned in the box, please purchase them as needed.

Figure 1-1 Unpack and Check

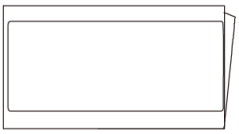


IP Camera×1



Installation Sticker×1

Accessory bag×1



Quick Start Guide×1

1.2 Appearance

Figure 1-2 Appearance

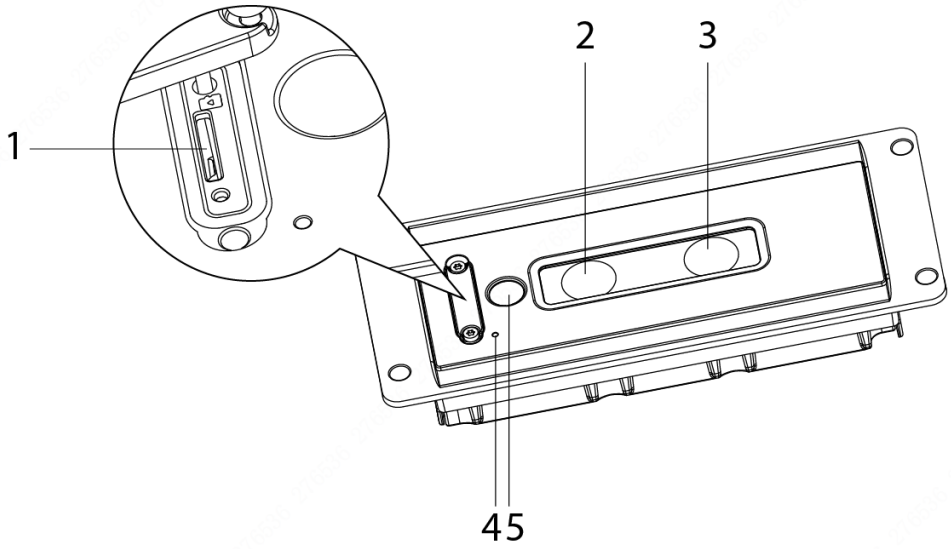


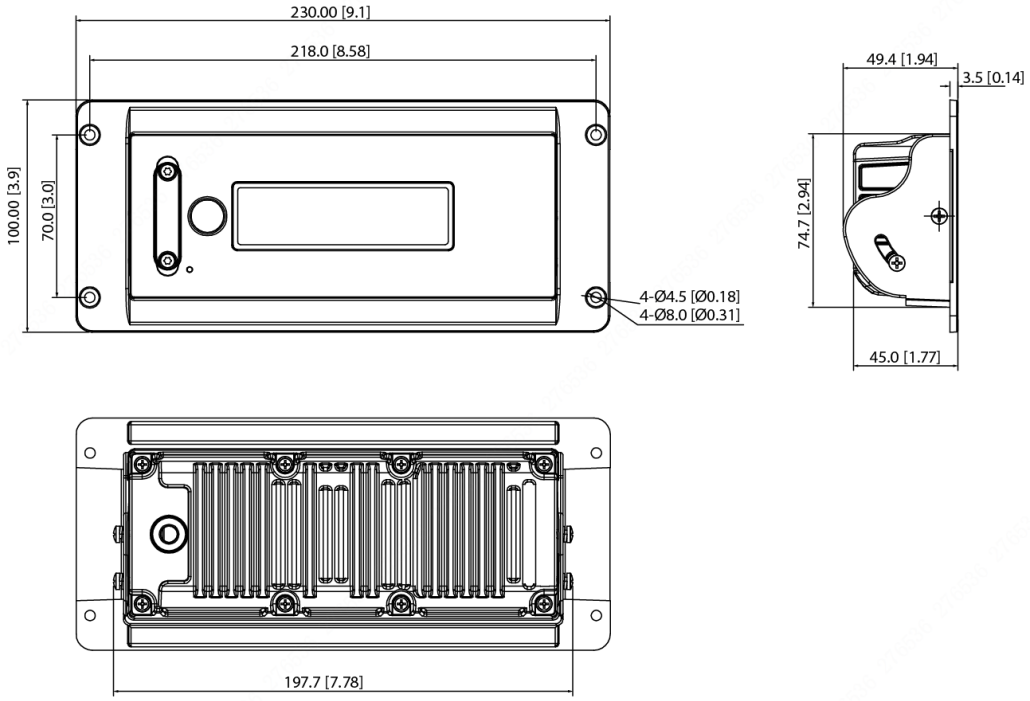
Table 1-1 Appearance description

No.	Name
1	TF card slot

No.	Name
2	Lens
3	
4	MIC
5	Fill light

1.3 Dimension

Figure 1-3 Dimension(mm[inch])



1.4 Port Definition

When connecting cables, it is recommended to use insulating tape and waterproof tape to avoid short circuit and water leakage.

Figure 1-4 Ports

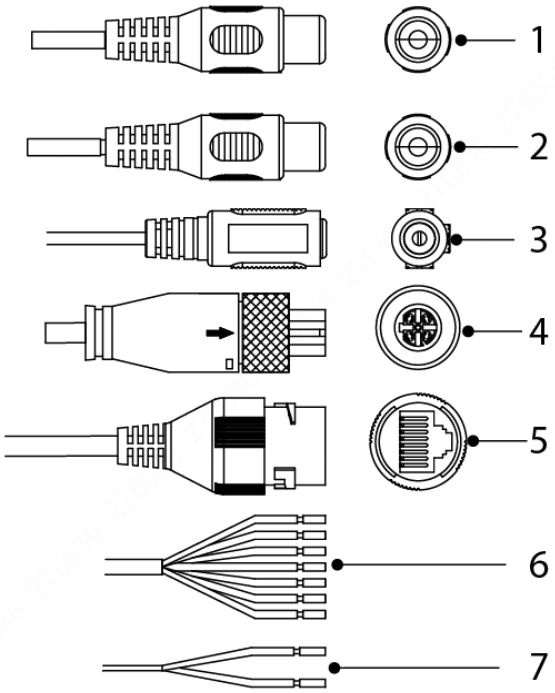


Table 1-2 Functions

No.	Cable	Name	Description
1	AUDIO IN	Audio input port	RCA interface for inputting audio signals, e.g. Simulation receiving audio signals from pickup and other equipment.
2	AUDIO OUT	Audio output port	RCA port, used to output audio signals to such external devices as speaker.
3	POWER	Power input port	Inputs 9-36V DC power.
4	Aviation port	Ethernet and power supply port	Used for connecting to mobile video recorder.
5	LAN	Ethernet port	Connect to standard Ethernet cable.
6	I/O	I/O port	Including alarm input and output. Different devices have different i/o ports. For actual use, see instructions on the device label.
7	RS-485	RS-485 port	Control the PTZ

Table 1-3 I/O port description

Port	Name	Description
I/O port	ALARM_OUT	Alarm output port, used to output alarm signal to alarm device.
	ALARM_OUT_GND	When the alarm output device is connected, ALARM_ Out can be used together with ALARM_ OUT_ GND. For details, see labels of cables.
	ALARM_IN	Alarm input port, used to receives the on-off signal of external

Port	Name	Description
	ALARM_IN_GND	alarm source. Different alarm input devices are connected to the same ground terminal, the ALARM_ IN_ GND. For details, see labels of cables.

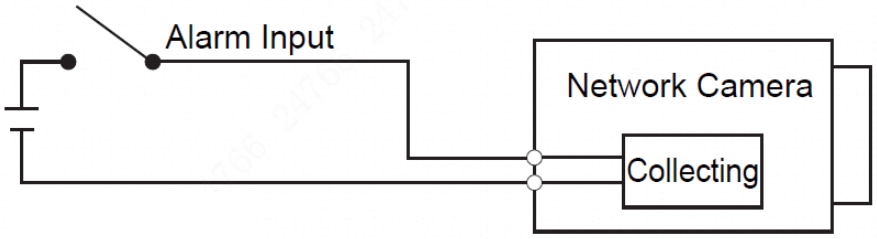
1.5 Alarm Configuration

Step 1 Connect the camera to alarm input device, see Figure 1-5.

Device collects different states of alarm input port when the input signal is idling and being grounded.

- Device collects logic "1" when input signal is connecting to +4.5 V to +36 V.
- Device collects logic "0" when input signal being connected to the ground or idling.

Figure 1-5 Alarm input

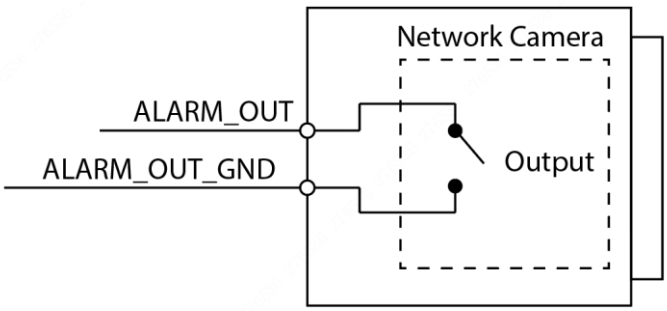


Step 2 Connect to alarm output device, see Figure 1-6.

The alarm output is switch output, which can only connect to NO alarm devices.

Port ALARM_OUT and ALARM_OUT_GND form a switch, which can be used to provide alarm output. Normally the switch is on; the switch will be off when there is alarm output.

Figure 1-6 Alarm input



Step 3 Log in to the WEB client, and configure the alarm input and output in Alarm Settings.

- Alarm input on the WEB client is corresponding to the alarm input end of I/O port. Please set the input mode to "NO" (default) if the alarm input signal is logic "0" and to "NC" if the alarm input signal is logic "1".
- The alarm output on the WEB client is corresponding to the alarm output end of I/O port.

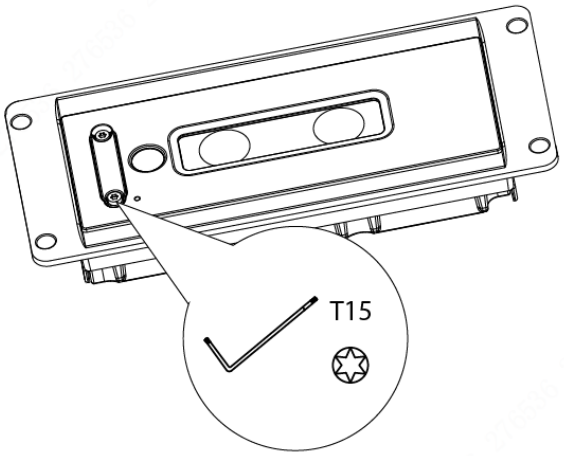
2 Installation

2.1 (Optional) TF Card Installation

The device has a TF card slot. Please install the TF card to store videos. Cut off the power supply before installing TF card.

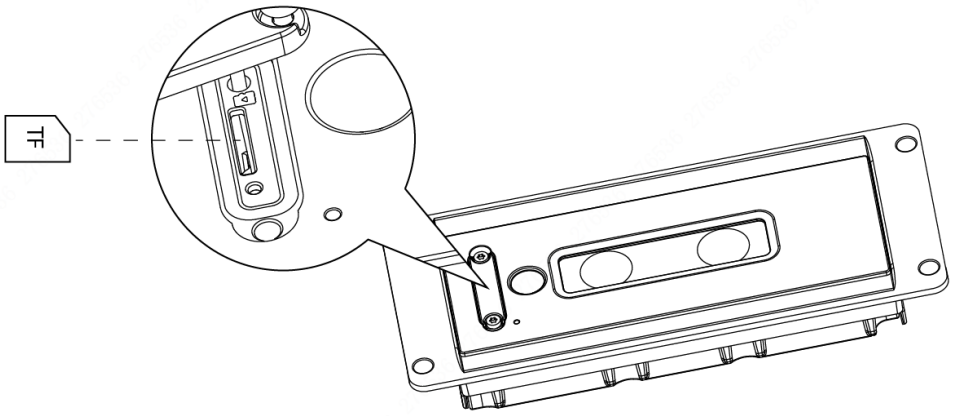
Step 1 Use a T15 wrench to loosen the two screws on the TF card cover.

Figure 2-1 Open the card cover.



Step 2 Insert the TF card into the card slot with the metal side facing towards the lens. After inserting the card, you will hear a "click" sound.

Figure 2-2 TD card installation



2.2 Fixing Device

The installation method is embedded installation.

⚠

- Make sure the installation surface can withstand at least three times the combined weight of the bracket and the device to be installed.
- To ensure the monitoring effect, it is recommended that the installation height of the device should be between 1.9m and 5m.

Cut installation hole

Step 1 Select a flat mounting surface and stick the installation sticker on the mounting surface.

Step 2 Cut a mounting hole on the mounting surface along the reference line of the installation sticker.

Figure 2-3 Installation sticker

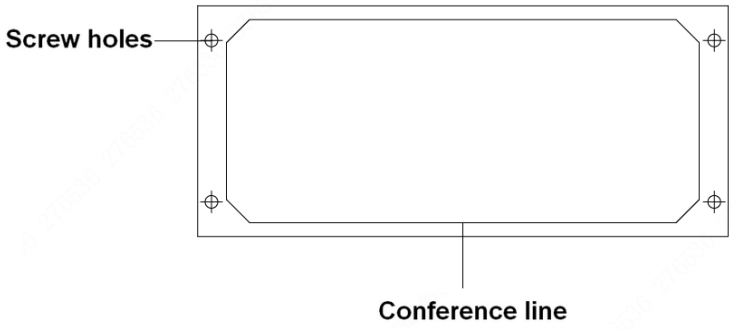
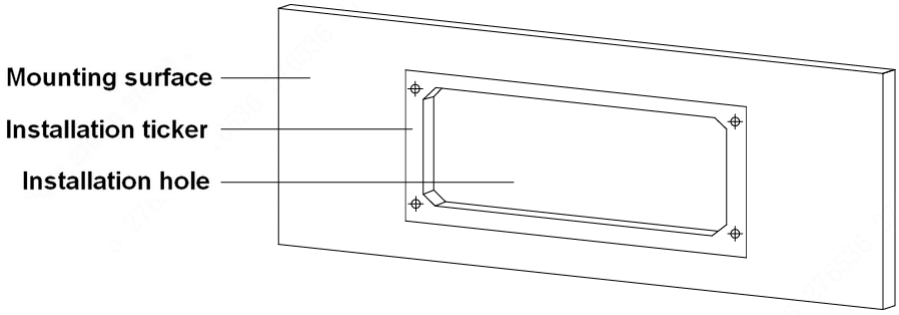
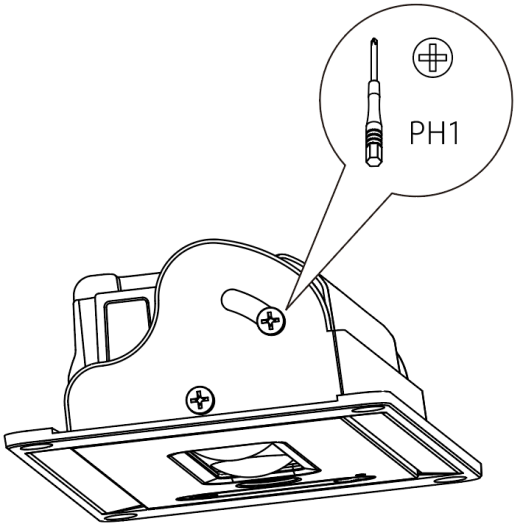


Figure 2-4 Cut installation hole



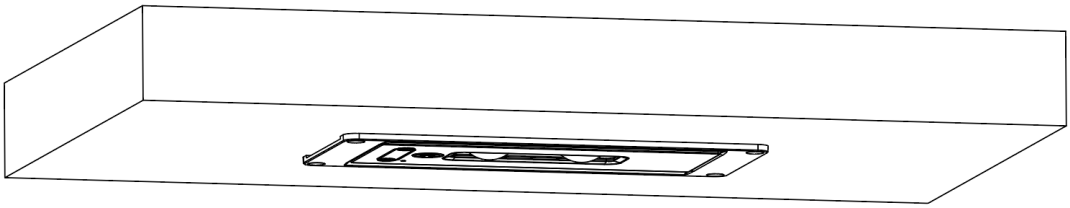
Adjusting angle

Step 1 Use a cross screwdriver to loosen four adjusting screws on both sides of the camera until the camera can rotate.



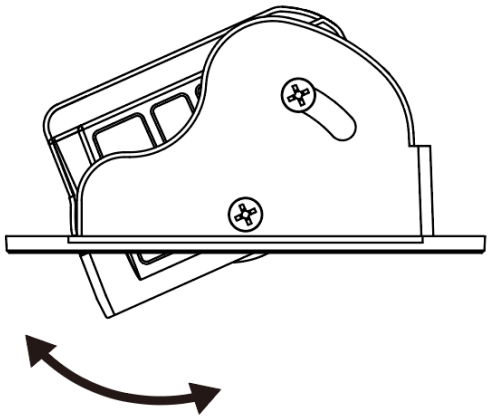
Step 2 Embed the camera into the mounting hole.

Figure 2-5 Embed the camera



Step 3 Connecting device and mobile video recorder, log in to the WEB interface of the device, preview the video image in real time, and adjust the lens angle of the camera according to the image to align it with the required monitoring position. See "3.3Logging in to WEB Interface" for logging in to the WEB interface.

Figure 2-6 Adjusting angle



Step 4 Adjust the lens to a proper angle, and tighten four adjusting screws on both sides of the camera.

Fixing device

Screw in 4 ST4× 25 self-tapping screws according to the screw hole position on the sticker to fix the equipment on the mounting surface.

Figure 2-7 Fixing device (1)

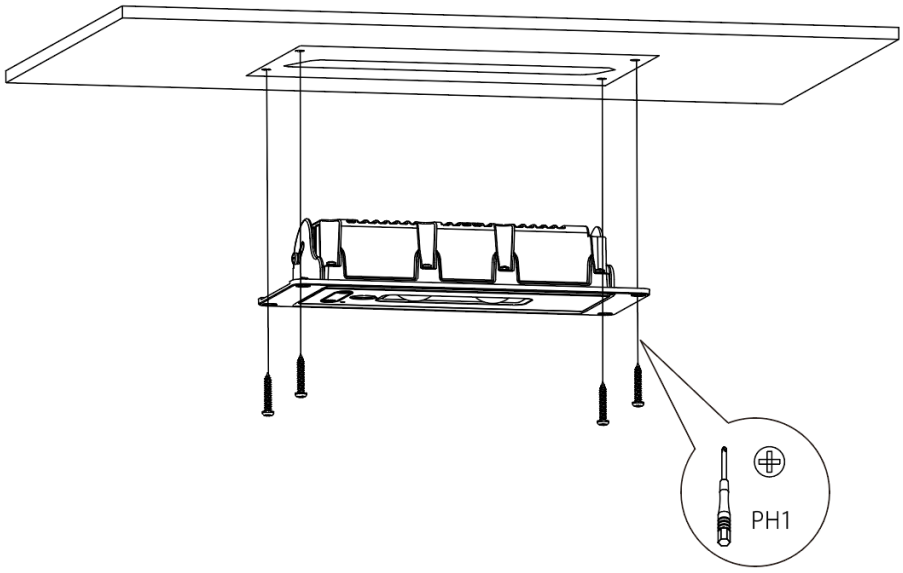
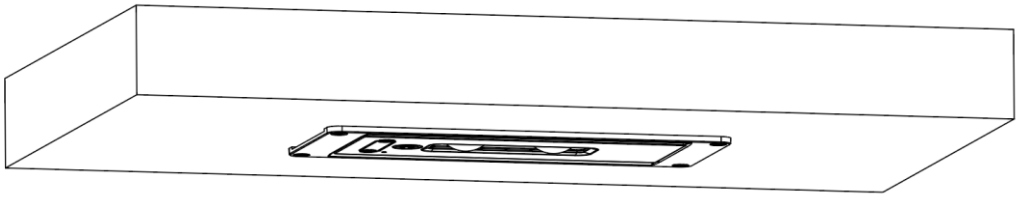


Figure 2-8 Fixing device (2)



2.3 Connection

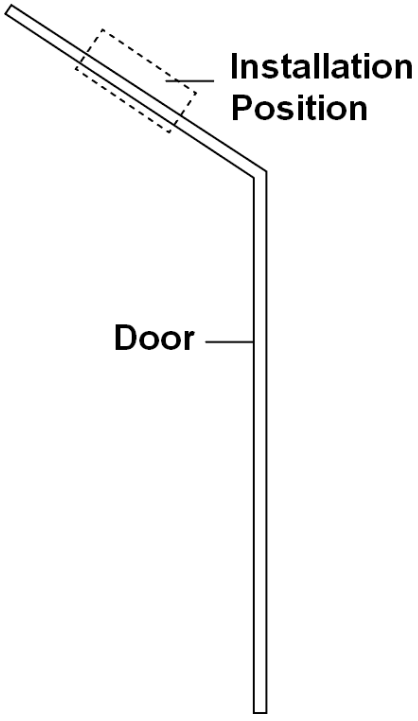
2.3.1 Cable Connection

Connect the camera to the mobile video recorder to realize real-time monitoring. For details, see"1.4Port Definition".

- The mobile video recorders of various manufacturers are different. Please refer to the actual equipment for details.
- Camera with PoE port needs to be connected with extension cable, and the specification of extension cable is D-type/RJ45/6-pin aviation connector. The extension cable is not equipped by default. Purchase it as needed.

2.3.2 Installation Position

The installation position of camera is above the door of the vehicle (installed inside the vehicle), and the video screen should cover the area where passengers get on and off.



2.3.3 Cable Layout

There are two main installation positions of the mobile video recorder: the top of the door (the position of the air conditioning box) and the back of the driver's seat (the device box). There are two ways to lay the cable.

Use the extension cable to connect the camera and the mobile video recorder, and lay the cable as shown in the figure. (Here we take the rear door installation as an example, and the installation on the front door is the same.)

Figure 2-9 Top of the door

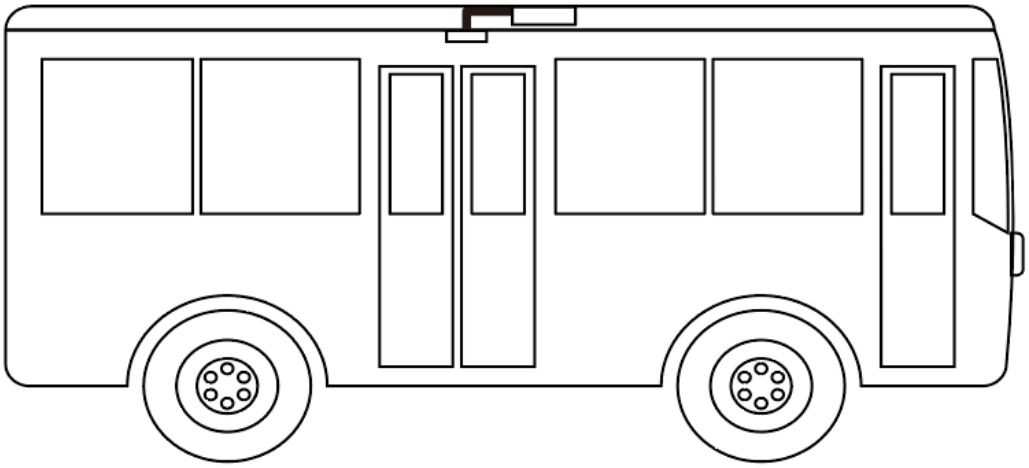
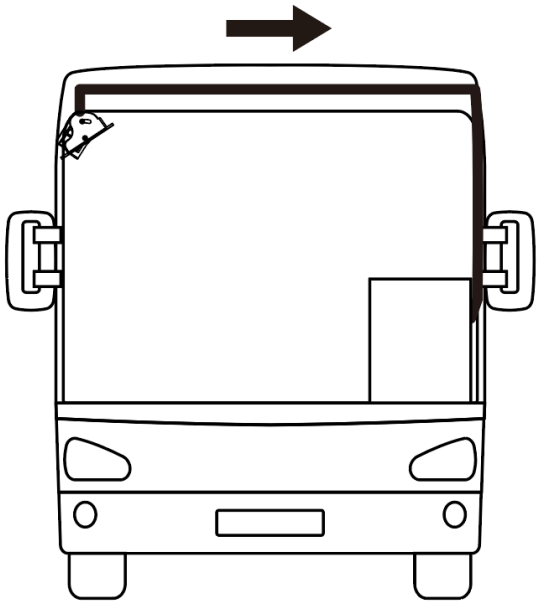


Figure 2-10 Back of the driver's seat



3 Network configuration

Device initialization and IP setting can be finished with the "ConfigTool" or in WEB interface. For more information, see the *WEB operation manual*.

- Device initialization is available on select models, and it is required at first use and after device is being reset.
- Device initialization is available only when the IP addresses of the device (192.168.1.108 by default) and the PC stays in the same network segment.
- Planning useable network segment properly to connect the device to the network.
- The following figures and interfaces are for reference only, and the actual product shall prevail.

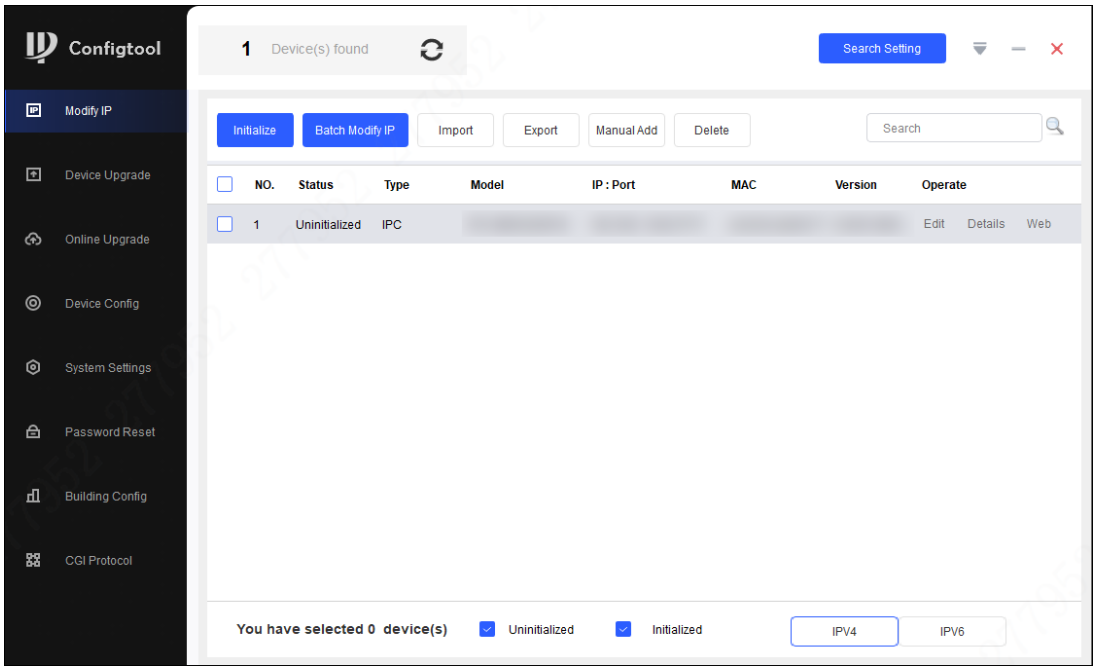
3.1 Initializing Device

Step 1 Double-click "ConfigTool.exe" to open the tool.

Step 2 Click Modify IP.

The **Modify IP** interface is displayed. See Figure 3-1.

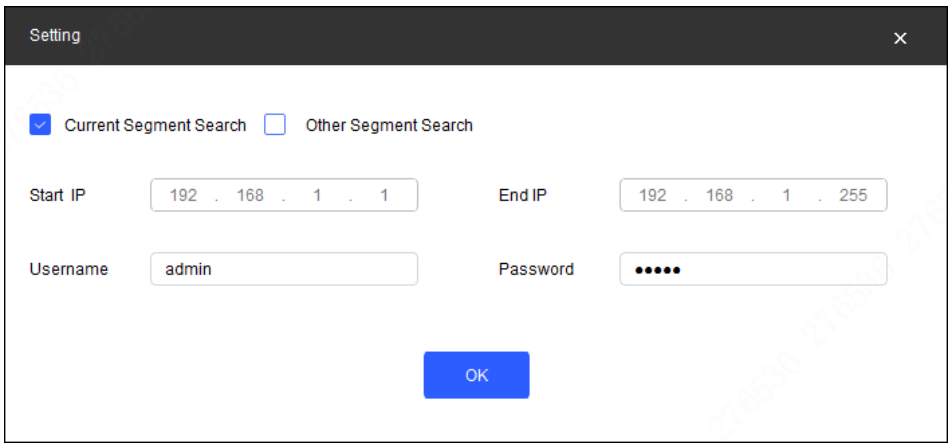
Figure 3-1 Modify IP interface



Step 3 Click Search Setting.

The **Setting** interface is displayed.

Figure 3-2 Setting



Step 4 Enter the **Start IP** and **End IP** of the network segment in which you want to search devices, and then click **OK**.

All the devices found in the network segment are listed.

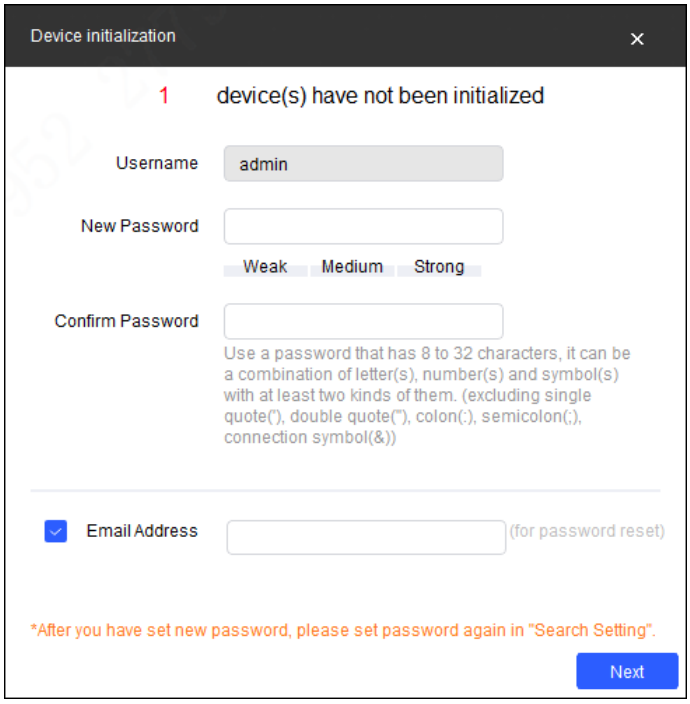
Step 5 Select one or several devices whose **Status** is **Uninitialized**, and then click **Initialize**.

The **Device initialization** interface is displayed.

Step 6 Select the devices that need initialization, and then click **Initialize**.

The password setting interface is displayed. See Figure 3-3.

Figure 3-3 Password setting interface



Step 7 Set and confirm the password of the devices, and then enter a valid email address. Click **Next**.

The final setting interface is displayed.

Email Address is used to reset password. Please set **Email Address** as needed.

Step 8 Select the options according to your needs and then click **OK**.

The **Initialization** interface is displayed after initializing is completed. Click the success icon ( ) or the failure icon ( ) for the details.

Step 9 Click **Finish**.

The device status in the **Modify IP** interface (Figure 3-1) turns to **Initialized**.

3.2 Modifying Device IP Address

- You can modify IP address of one or multiple devices in one time. This section is based on modifying IP addresses in batch.
- Modifying IP addresses in batch is available only when the corresponding devices have the same login password.

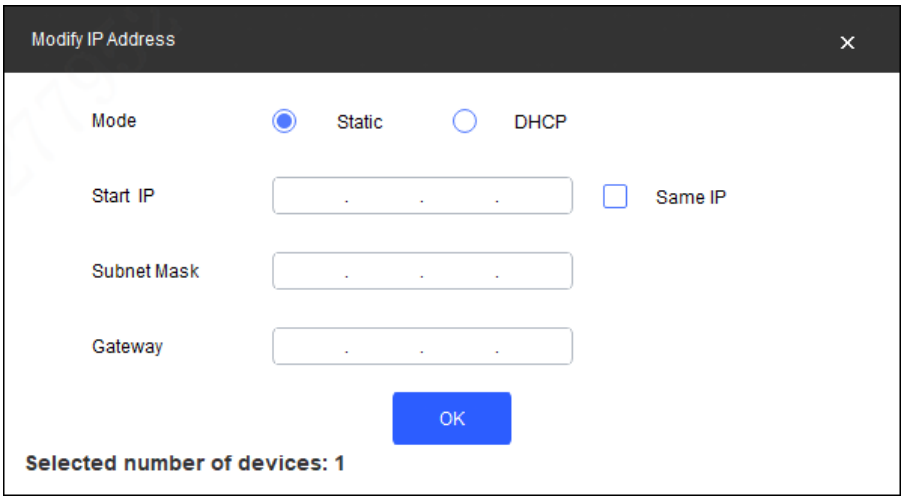
Step 1 Follow Step 1 to Step 4 in 3.1 to search devices in your network segment.

After clicking **Search setting**, please make sure the **username** and **password** are the same as what you set during initialization, otherwise there will be "wrong password" notice.

Step 2 Select the devices which IP addresses need to be modified, and then click **Modify IP**.

The **Modify IP Address** interface is displayed. See Figure 3-4.

Figure 3-4 Modify IP Address interface



Step 3 Select **Static** mode and enter start IP, subnet mask and gateway.

- IP addresses of multiple devices will be set to the same if you select **Same IP**.
- If DHCP server is available in the network, devices will automatically obtain IP addresses from DHCP server when you select **DHCP**.

Step 4 Click **OK**.

3.3 Logging in to WEB Interface

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

- If the setup wizard is displayed, follow the instructions to finish the settings.

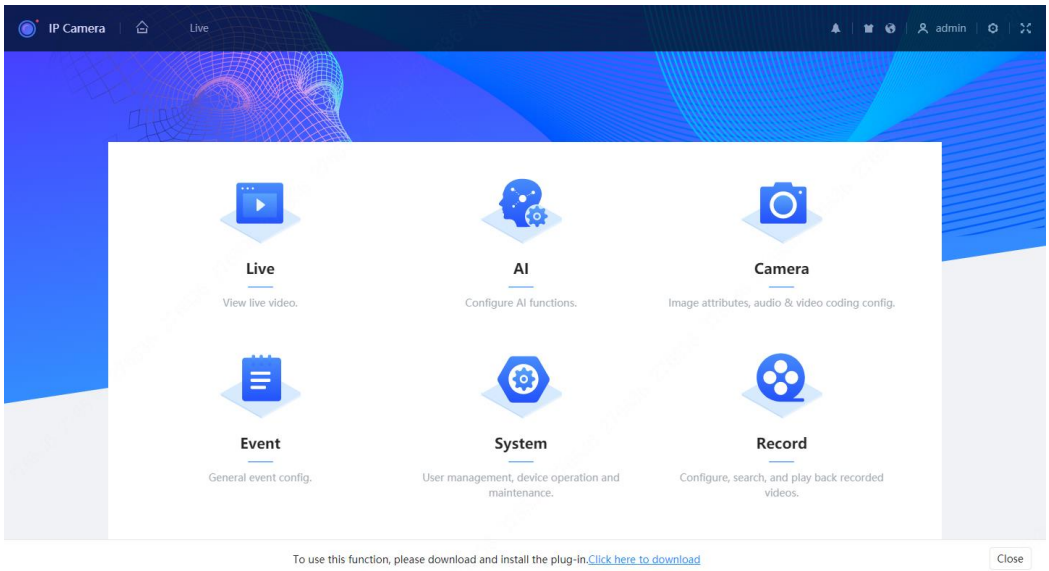
- If you forget your password, click **Forgot password?** to reset it.

Figure 3-5 Login

Step 2 Enter user name and password in the log in box, and then click **Login**.

For first time login, click **Click here to download** and install the plugin as instructed.

Figure 3-6 WEB interface



Appendix 1 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 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.