All-in-one Enforcement Camera

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.3

Foreword

General

This manual introduces the structure, installation, system networking, and initial configurations of the all-in-one enforcement camera (hereinafter referred to as the "Camera").

Models

All-in-one Enforcement Camera	HD Intelligent Enforcement Camera	Pixel
ITC952-AU3F-L (ZF1640)	ITC952-AF3F	11 MP
ITC952-AU3F-IRL7 (ZF1640)	ITC952-AF3F-IR7	
ITC952-AU3F-IRL8 (ZF1640)		
ITC952-RU2D-IRL7 (ZF1640)	ITC952-RF2D-IR7	9 MP
ITC952-RU2D-IRL8 (ZF1640)	ITC952-RF2D-IR8	
ITC952-RU2F-L (ZF1640)	ITC952-RF2F	
DHI-ITC952-RU2F-L (ZF1640)		
DHI-ITC952-RU2F-BD (ZF1640)		
ITC952-RU2F-BD (ZF1640)		
ITC352-AU3F-L (ZF1640)	ITC352-AF3F	3 MP
ITC352-AU3F-IRL7 (ZF1640)	ITC352-AF3F-IR7	
ITC352-AU3F-IRL8 (ZF1640)	ITC352-AF3F-IR8	

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
⚠ DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.3	Updated manual format and cybersecurity contents.	November 2021
V1.0.2	Updated manual format.	February 2021
V1.0.1	Added camera models and updated manual font.	January 2021
V1.0.0	First release.	April 2020

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user’s manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, comply with the guidelines when using it, and keep the manual safe for future reference.

Transportation Requirements

⚠

Transport the device under allowed humidity and temperature conditions.

Storage Requirements

⚠

Store the device under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.

⚠

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- 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.
- 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.
- An emergency disconnect device must be installed during installation and wiring at a readily accessible location for emergency power cut-off.
- Disconnect the device when installing and connecting the lens.

Operation Requirements

⚠

- Make sure that the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.

- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device.
- Do not aim the device at strong light sources (such as lamplight, and sunlight) when focusing it.
- Do not vibrate, squeeze or immerse the device in liquid during transportation, storage or installation.
- Do not block the ventilation near the device.
- 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 function earthing portion of the device (grounding cable or lightning surge protector) to improve its reliability. 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 device must be used with the protective cover for outdoor scenarios to avoid the risk of water damage to the device.
- 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.
- Modify the default password of the device after first-time login to prevent the device from being stolen.

Maintenance Requirements

- Pack the device with packaging provided by its manufacturer or packaging of the same quality before sending it back for repair.
- Please do not touch the photosensitive device with your hands. Use an air blower to clean off the dust and filth on the lens.
- Clean the surface of the device with a soft dry cloth or a clean soft cloth dipped in neutral detergent.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.

Table of Contents

1 Overview

1.1 Introduction

Designed with industry-specific GS-CMOS image sensor and high-performance AI processor, and integrated with deep learning algorithms, the Camera enjoys 4K high definition and ultra-high video fluency. It collects real-time data of traffic conditions, and captures clear images of vehicles at day and night. In addition, it analyzes the recorded or captured vehicle information and other road conditions, and transmits the image and record data to control center or storage device for management. The Camera is ideal for a wide range of businesses such as smart traffic.

1.2 Features

Structured Design

- Embedded component-based design.
- Integrated structure that realizes low power consumption.

High Integration Level

The Camera is integrated with high-definition camera, fill light, terminal, etc., significantly saving on-site installation time.

Excellent Performance

- High-performance multi-core process.
- High-performance CCD and CMOS image sensors featured by high color reproduction and speed.
- High-performance image signal processor (ISP).

Abundant Interfaces

- Diverse signal, data and communication interfaces.
- Precise input and output control of synchronizing signal.

Extensive Applications

The Camera is extensively applied to surveillance systems of city roads, highways, and residence communities.

1.3 Functions

Picture Composition

Composites several pictures of violations into one picture, and the composition way can be flexibly configured.

Picture Cutout

With sufficient light supplement of flashing light, when capturing one vehicle, the Camera can also cut out the plate number part of the snapshot. Camera in ANPR mode can even cut out the face picture of people in the front.

Intelligent Recognition

- Supports recognizing license plate, logo, color, model, and more.
- Supports detecting violations such as overspeed, running a red light, crossing solid white line, illegal lane change, wrong-way driving, and more.

Drawing Detection Lines Automatically

Provides ease of drawing detection lines by clicking **AutoDrawLine** from **Setup** > **ITC** > **Intelligent** > **Video Analyse**.

User Management

- Supports configuring multiple user groups and users, and each user groups and user can be configured with different authorities.
- Supports querying information of online users.

Log Management

- Stores up to 1,792 log records.
- User permission control.

Storage

- Stores the record data on central server according to the storage policy configured by user.
- After recording according to user needs and by web recording mode, video files are stored on the client computer.
- Supports TF card local storage, hot swapping, and ANR. When storage space is insufficient, it automatically overlays the stored files.

Alarm

- Supports sending alarm through network of camera abnormity, such as storage damage.
- Supports connecting to external alarm devices through alarm inputs, and real-time response to external alarm inputs within 200ms. Supports processing alarm information and sending voice prompt according to predefined alarm settings by user.

Network Surveillance

- Through network, single-channel record data compressed by the Camera is transmitted to the network terminal for decompression and reconstruction. Delays 400 ms at most if bandwidth allows.
- Max supports 10 connections.
- Adopts the following A/V transmission protocol: HTTP, TCP, UDP, MULTICAST, RTP/RTCP, and more.
- Supports web access, widely used in WAN.

Traffic Flow Statistics

Traffic flow statistics of lane is realized through connection to traffic signal controller or camera. Supports uploading statistics data to corresponding platform server.

Snapshot

- Supports snapshot and coding of picture.
- Supports watermark encryption to prevent tampering.
- You can configure the speed limit and interval of snapshot.
- The captured picture displays the time, place, speed, speed limit, and lane of vehicle, as well as picture number, violation type, and more.
- Supports snapshot of traffic violations.

Record Linkage

Supports recording the violations of vehicles, and linking snapshots to the record.

OSD Settings

You can configure the OSD information and location of video channel, picture, and composite picture.

Network Management

- Supports configuration and permission management through Ethernet.
- Supports managing the Camera by web.

Extra Device Control

- Supports peripheral device management. The control protocol and port of peripheral device can be configured freely.
- Supporting connection to peripheral devices such as flashlight, strobe light, vehicle detector, signal detector, radar, and more.

Power Supply

AC synchronization, and 12 VDC power supply.

White Balance

- Automatic white balance: Accurately reflecting the color balance when the illumination source changes.
- Partial white balance: Adjusting the color balance according to the surrounding environment.

Automatic Exposure

Automatically determines the correct exposure for captured pictures, and the shutter speed based on the factory settings of aperture and shutter speed.

Automatic Gain

Automatically increases the sensitivity of camera when the illumination is weak, and enhances image signal output for clear, bright images.

Auxiliary Functions

- Watermark encryption of video image coding to prevent tampering.
- Real-time display of system resource information and running status. Support log function.
- Signal control and output of strobe, flashing light, and continuous light.
- GPS positioning.

2 Device Structure

2.1 Structure

Protective cover of the Camera includes power supply, terminal, and HD camera.

The structure is taken as an example. Different devices might have different components.

Figure 2-1 Structure

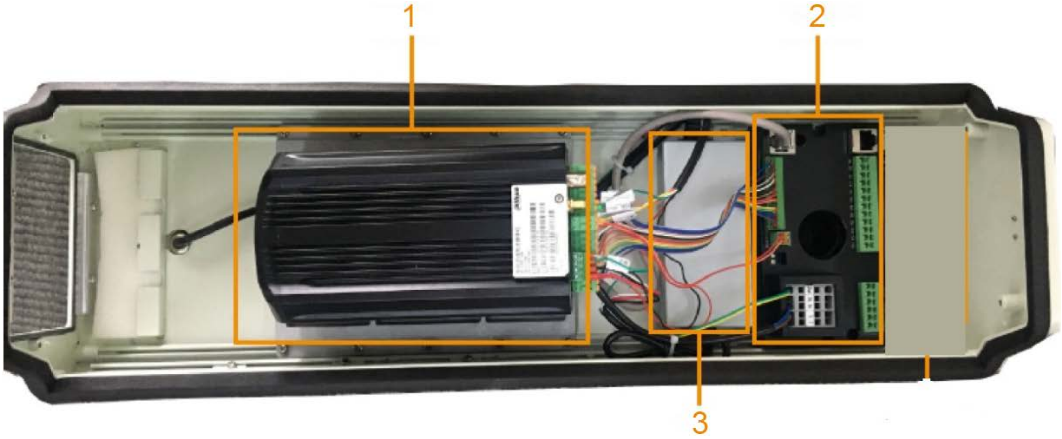


Figure 2-2 Structure (2)

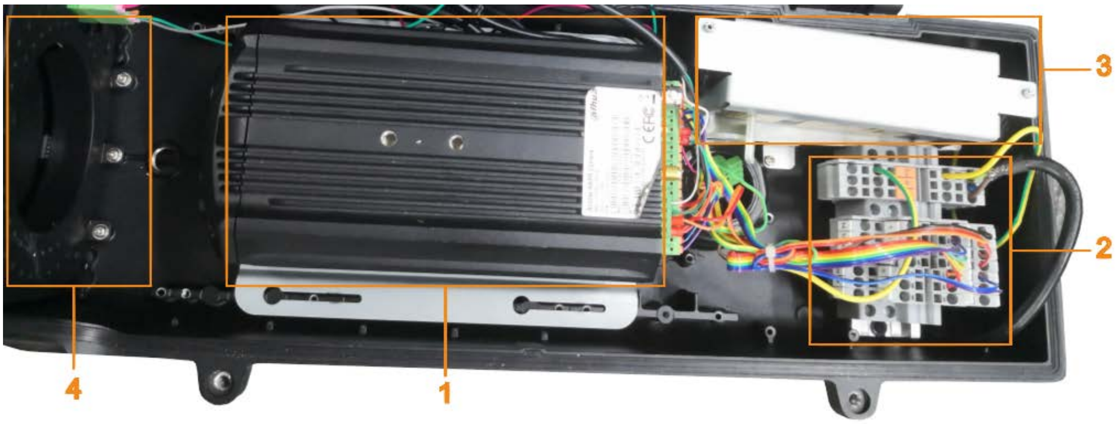


Figure 2-3 Structure (3)

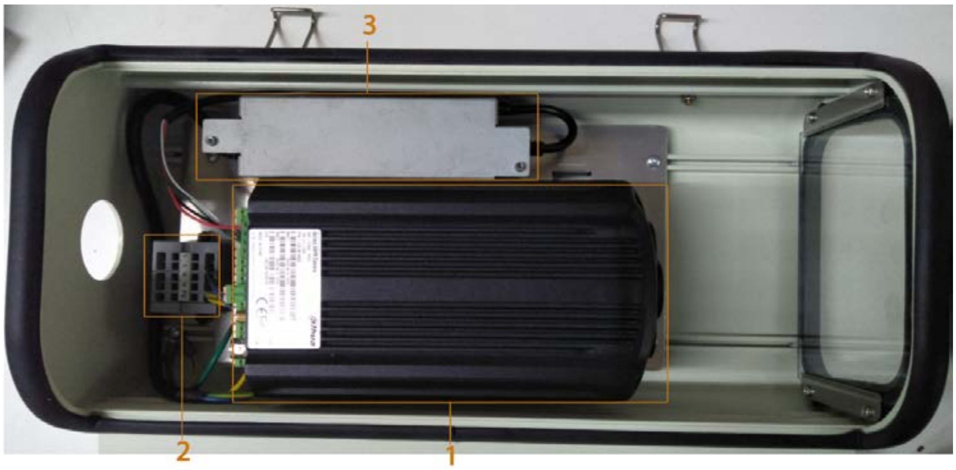


Table 2-1 Protective cover

No.	Description	No.	Description
1	Camera	3	Power
2	Terminal	4	Built-in LED illuminator

2.2 Terminal

The two typical kinds of terminals are shown in the following two figures.

Different devices might have different types of terminals.

Figure 2-4 Terminal (1)

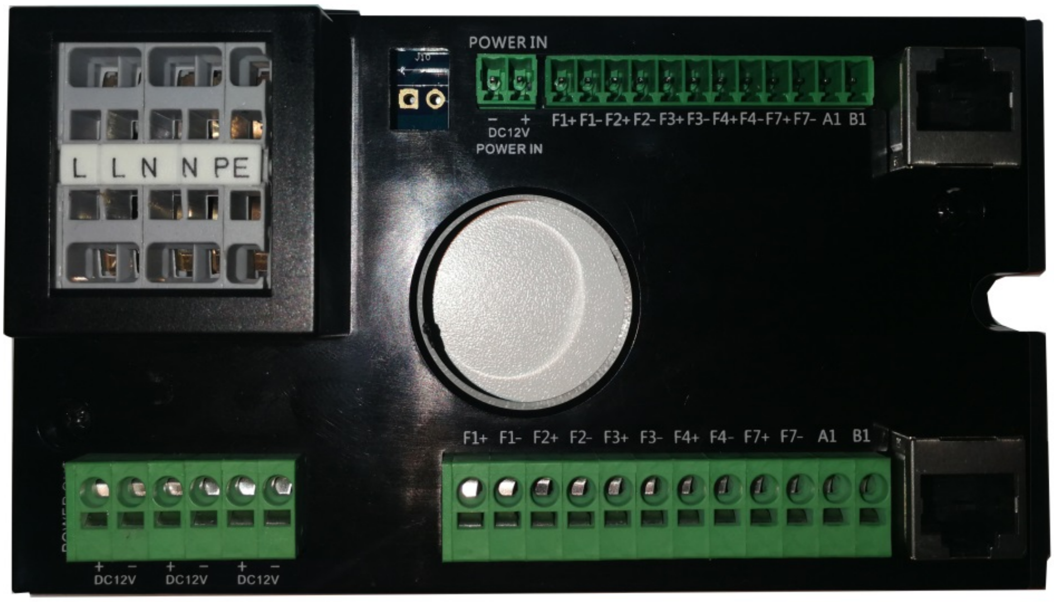

POWER IN
J10
− +
DC12V
POWER IN
F1+ F1- F2+ F2- F3+ F3- F4+ F4- F7+ F7- A1 B1
L L N N PE
F1+ F1- F2+ F2- F3+ F3- F4+ F4- F7+ F7- A1 B1
+ − DC12V
+ − DC12V
+ − DC12V

Table 2-2 Description of terminal (1)

Name	Description
F1+	Flashing light 1 triggers output F1+
F1-	Flashing light 1 triggers output F1-
F2+	Flashing light 2 triggers output F2+
F2-	Flashing light 2 triggers output F2-
F3+	Flashing light 3 triggers output F3+
F3-	Flashing light 3 triggers output F3-
F4+	Flashing light 4 triggers output F4+
F4-	Flashing light 4 triggers output F4-
F7+	Strobe synchronous output F7+
F7-	Strobe synchronous output F7-
A1	RS–485_A1

Name	Description
B1	RS–485_B1
L	AC 220V live wire
N	AC 220V neutral wire
PE	AC 220V earth wire

Figure 2-5 Terminal (2)

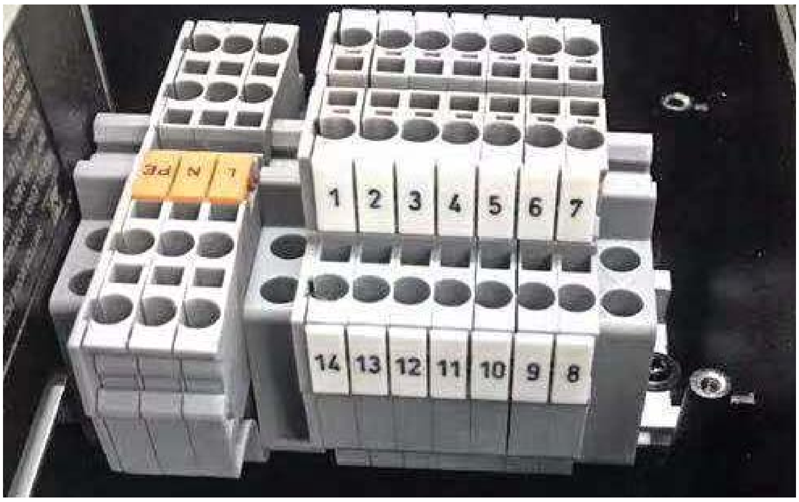


Figure 2-6 Terminal (3)

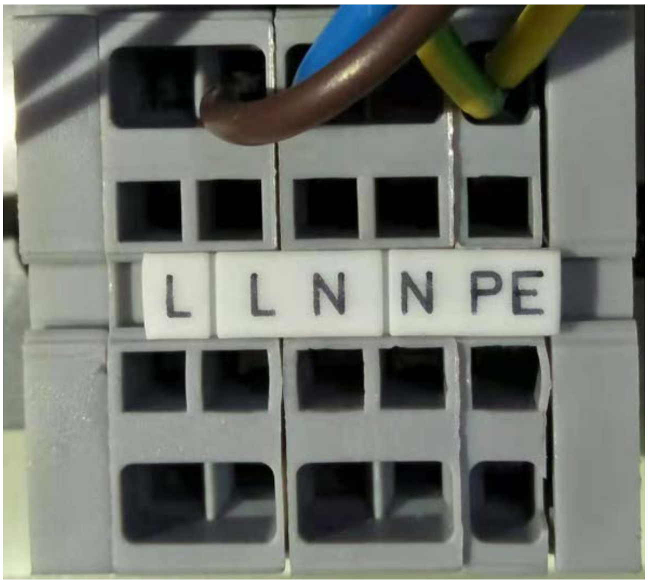


Table 2-3 Description of terminal (2)

Name	Description
1	Flashing light 1 triggers output F1+
2	Flashing light 1 triggers output F1-
3	Flashing light 2 triggers output F2+
4	Flashing light 2 triggers output F2-
5	Flashing light 3 triggers output F3+
6	Flashing light 3 triggers output F3-

Name	Description
7	Flashing light 7 triggers output F7+
8	Flashing light 7 triggers output F7-
9	RS485-A1
10	RS485-B1
11	12+ DC
12	
13	12- DC
14	
L	220 VAC live wire
N	220 VAC neutral wire
PE	220 VAC earth wire

2.3 Camera

2.3.1 Rear Panel

Figure 2-7 Rear panel

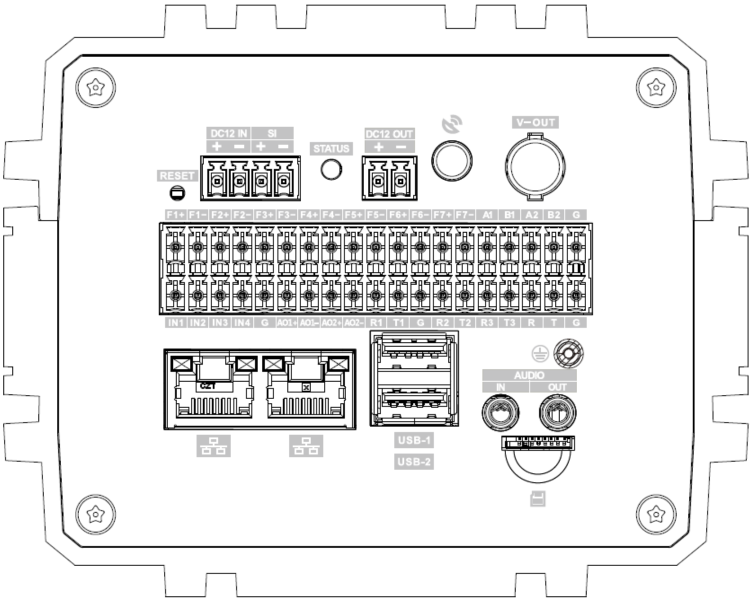


Table 2-4 Rear panel ports

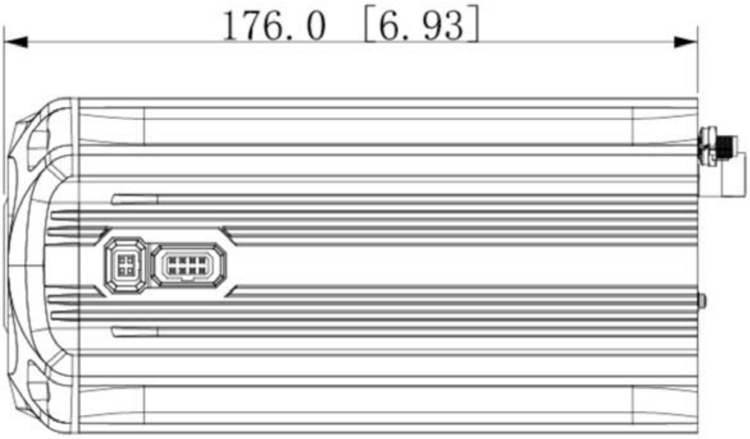
Port		Function
DC 12 IN	Power input port	12 VDC input.
SI+, SI-	Synchronous input port of external frequency source	The camera synchronizes with external signal source.

Port		Function
RESET	Reset button	Restore to factory settings. When the Camera runs normally (the power indicator light is blue), press and hold the RESET button for at least 5 seconds, and the Camera restores to factory defaults.
STATUS	Indicator light	Displays the activity status of the Camera. ● The blue light keeps on: The Camera is running normally. ● The red light flashes: The Camera is upgrading. ● The red light keeps on: The Camera is in safety mode.
DC12 OUT	Power output port	12 VDC output.
📡	Positioning	GPS/BeiDou positioning.
F1+, F1-, F2+, F2-, F3+, F3-, F4+, F4-, F5+, F5-, F6+, F6-, F7+, F7-	Ports for connecting external light	Connect to flashing light and strobe. 📖 The configuration must be consistent with the light actually connected, otherwise the light might burn out.
A1, B1	RS–485 ports	2 ports, connecting to signal detector, vehicle detector, radar, flashing light, strobe, and other illuminators.
A2, B2		2 ports, connecting to flashing light, strobe, and other illuminators.
G	GND	Ground terminal.
IN1, IN2, IN3, IN4	IO input	4 IO snapshot ports or 4 alarm input ports.
AO1, AO2	2-channel alarm output	Can be configured respectively as alarm output port and wiper output port.
R1, T1, G R2, T2, G R3, T3, G	3-channel radar port	Supports connecting 3 radars at the same time.
R	RS–232 port	RS–232_RX, RS-232 port receiving terminal.
T		RS–232_TX, RS-232 port transmitting terminal.
🖧	2 network ports	Two 100/1000M RJ-45 Ethernet ports with different MAC addresses.
USB-1/USB-2	2 USB ports	Two USB3.0 ports, reserved for expansion of 4G and Wi-Fi modules.
⏚	GND	Ground this port to improve reliability of the Camera, otherwise the Camera might be exposed to lightning strikes.
AUDIO IN/OUT	Audio input/output	Audio input/output port.

Port		Function
▤	TF card port	Connects TF card. 📖 Before hot swapping the TF card, go to **Setup** > **Storage** > **Destination** > **Local** on the web page of the Camera, and click **Hot Swap**.

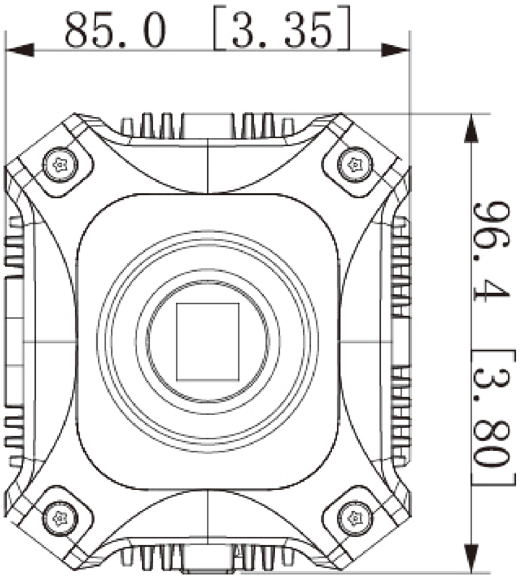
2.3.2 Side Panel

Figure 2-8 Side panel dimensions (mm (inch))



2.3.3 Front Panel

Figure 2-9 Front panel dimensions (mm (inch))



2.4 LED Illuminator

Different models are designed with different types and numbers of LED illuminators to meet your various needs. Models with IR illuminators bring less light pollution, and it is more suitable to use during the night.

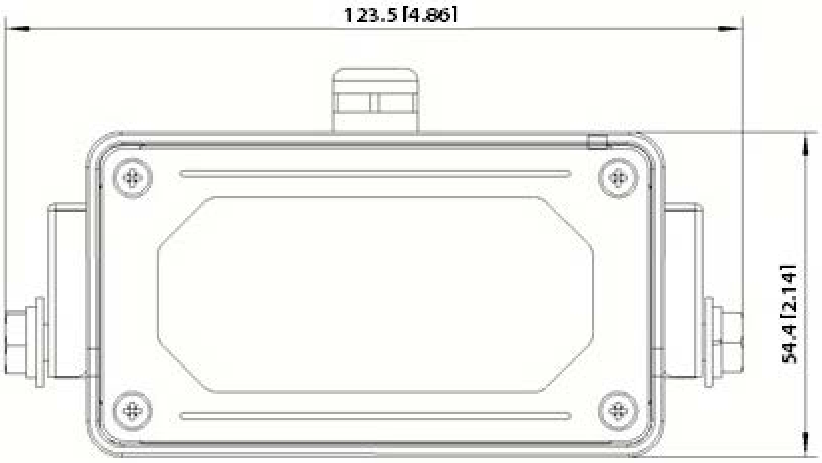
⚠

- Do not use the illuminator in water.
- Do not hit the illuminator and pull its cable.

DHI-ITC952-AU3F-L, DHI-ITC352-AU3F-L

These two models are designed with 3 white light LED illuminators.

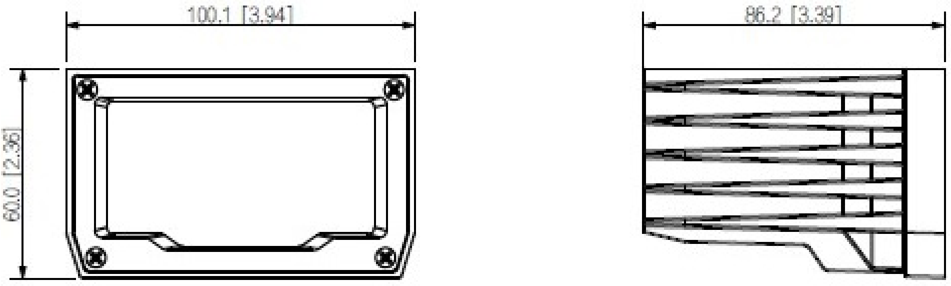
Figure 2-10 Dimensions (mm [inch])



DHI-ITC952-AU3F-IRL7, DHI-ITC952-AU3F-IRL8, DHI-ITC352-AU3F-IRL7, DHI-ITC352-AU3F-IRL8

These models are designed with 8 IR illuminators.

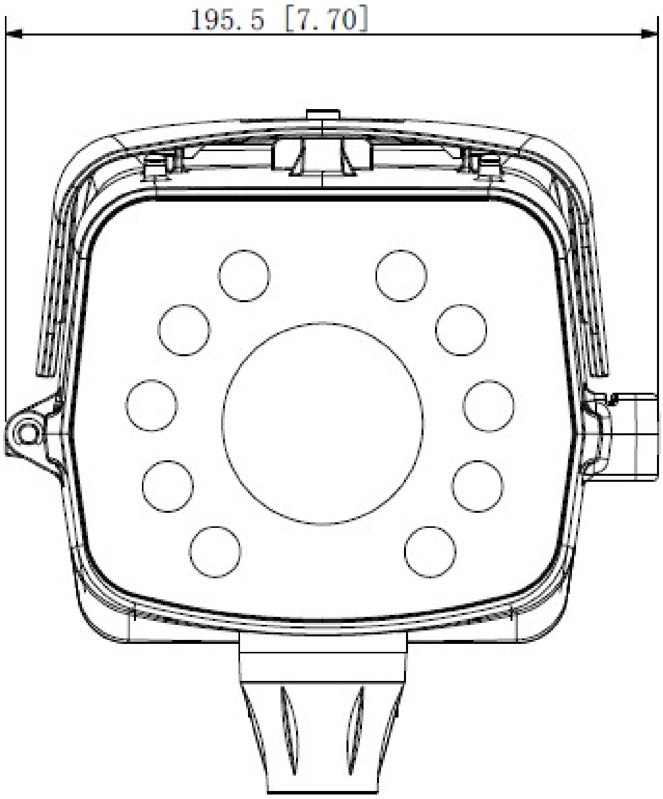
Figure 2-11 Dimensions (mm [inch])



DHI-ITC952-RU2D-IRL7, DHI-ITC952-RU2D-IRL8

These two models are designed with 10 built-in IR LED illuminators.

Figure 2-12 Dimensions (mm [inch])



DHI-ITC952-RU2F-BD

No illuminators.

3 Installation

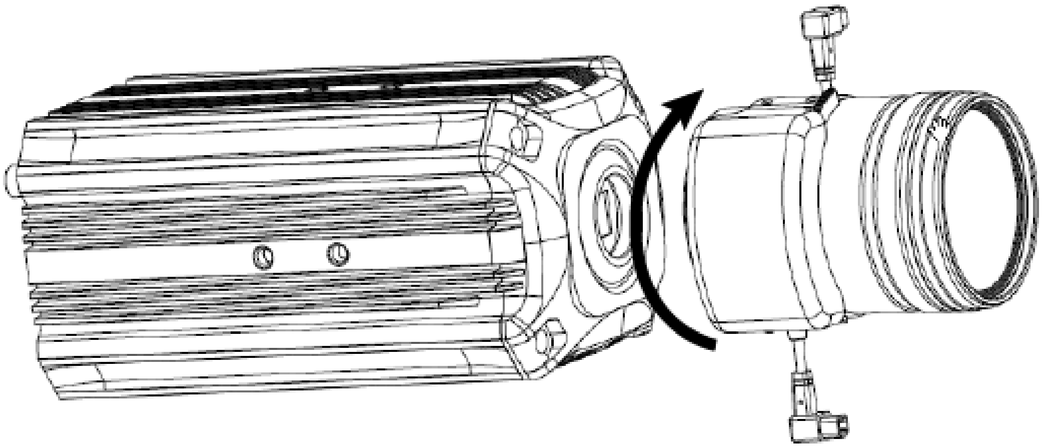
When you open the package, check the Camera and accessories against the checklist. After confirming the package, install the Camera by following the instructions in the manual.

You need to manually install the accessories such as lens, TF card, cables, and corrugated pipe. For other accessories and connections, install according to the actual condition.

3.1 Installing Lens

Power off the Camera before installing the lens. Otherwise, the lens might be damaged.

Figure 3-1 Install the lens



3.1.1 Installing the Lens

Step 1 Remove the protective covers of sensor and lens. Insert the spacer in between the lens and the camera.

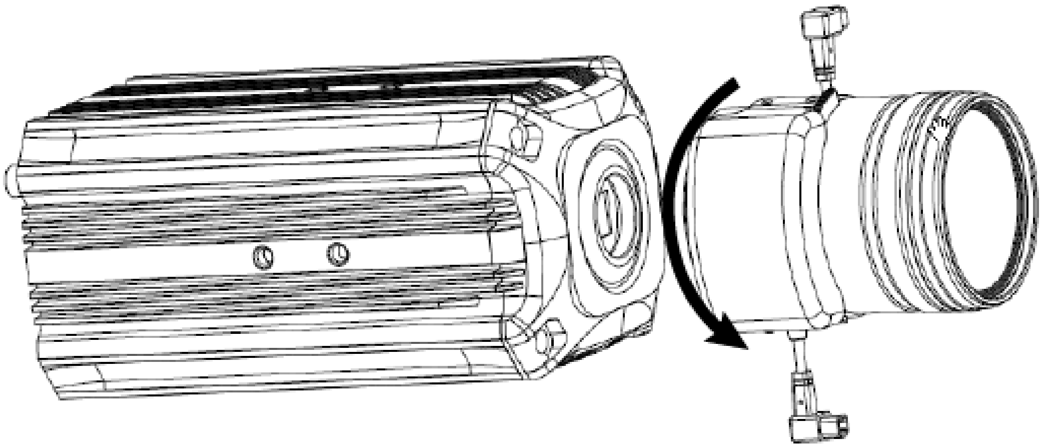
Step 2 Align the lens to the lens mount position on the camera, and turn the lens clockwise until it is securely mounted.

Step 3 Insert the cable plug of lens into the auto iris lens connector on the side panel of camera.

Step 4 Correct the focus to make the images clear.

3.1.2 Removing the Lens

Figure 3-2 Removing lens



Step 1 Unplug the cable from the lens mount.

Step 2 Turn the lens to counter-clockwise until the lens is removed.

Step 3 Install the protective covers of sensor and lens to prevent them from being spotted.

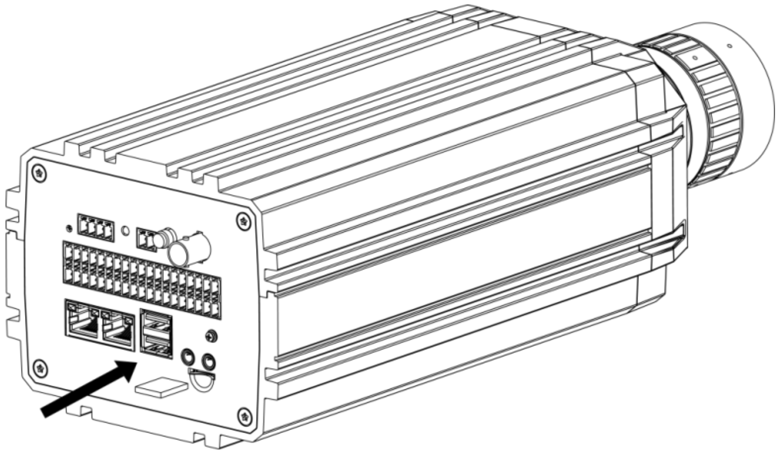
3.2 Installing TF Card

This section takes some models as the example, and might differ from the actual model.

3.2.1 Installing the TF Card

Orient the TF card to make the teeny triangle on the card points toward the open slot, and then gently shove the card all the way into the slot.

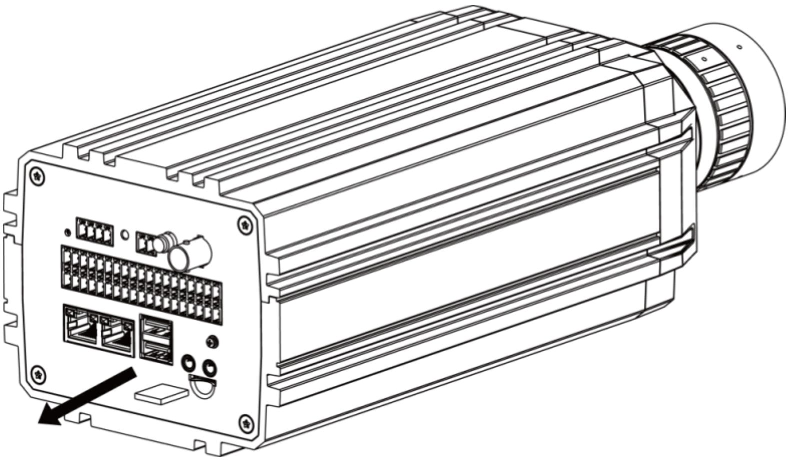
Figure 3-3 Installing TF card



3.2.2 Removing the TF Card

Remove the TF card according to the direction shown by the arrow.

Figure 3-4 Removing TF card



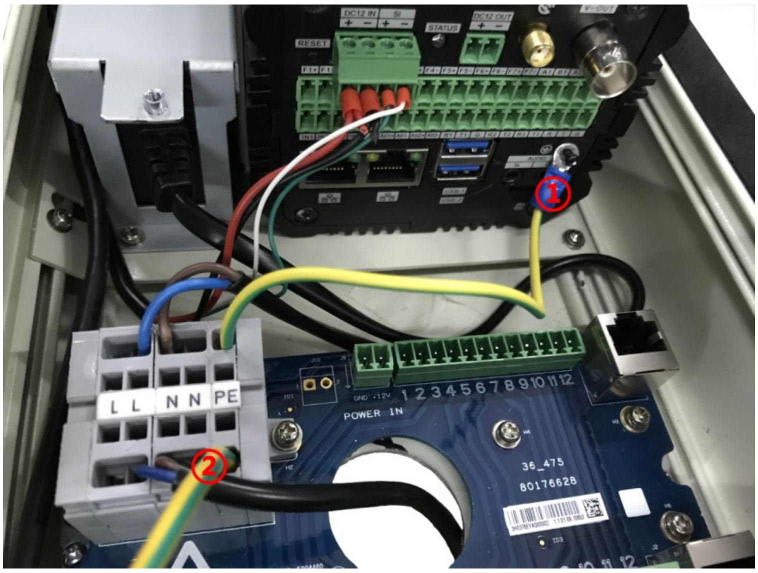
3.3 Connecting Cable

You need to use a 2.0 mm screwdriver to connect cables.

⚠

- Avoid copper wire exposure when connecting the power cord. With 220 V power supply, copper wire exposure might cause electric leakage, and thus bringing personal injury.
- When removing the cable, turn off the power of the Camera first to avoid leakage. This helps prevent personal injury.
- To ensure the Camera is properly grounded and improve device reliability, make sure that: ① The device port ⏚ is connected to the PE (earth wire) of the protective cover. ② The PE is connected to the ground.
- The picture is for reference only, and might differ from the actual device cable.

Figure 3-5 Cable connection example (1)



3.3.1 Installing the Cable

Step 1 Insert the screwdriver into the square slot corresponding to the connecting cable. Press the screwdriver vertically to loosen and expose the metal sheet of the circular slot.

Step 2 Insert the cable into the circular slot.

Step 3 Remove the screwdriver, and the cable installation is finished.

3.3.2 Removing the Cable

Step 1 Insert the screwdriver into the square slot corresponding to the connecting cable. Press the screwdriver vertically to loosen and expose the metal sheet of the circular slot.

Step 2 Pull the cable out of the circular slot.

Step 3 Remove the screwdriver, and the cable is disassembled.

3.4 Installing Sun Shade

Figure 3-6 Cable connection example (2)

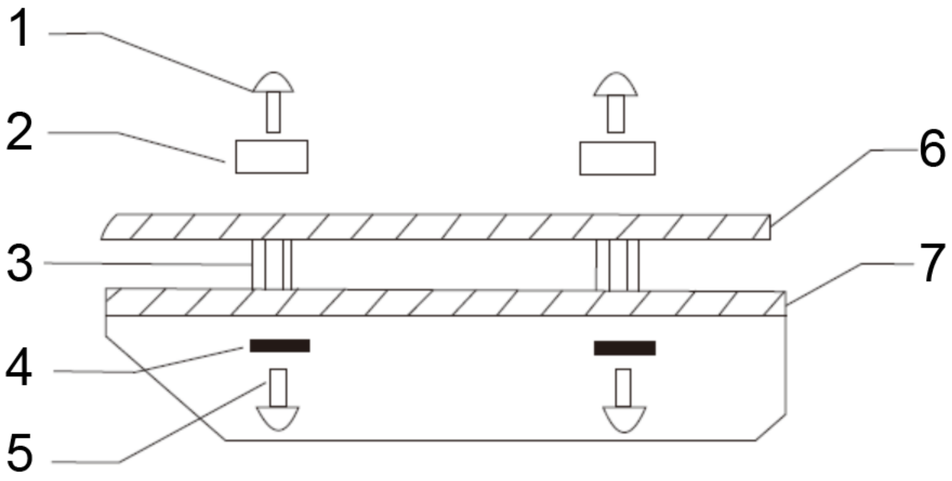


Table 3-1 Sunshade connection description

No.	Description	No.	Description
1, 5	Screw	4	Washer
2	PTFE gasket	6	Sunshade
3	Pillar	7	Camera protective cover

Step 1 Remove the screws on the top of the camera protective cover.

Step 2 Fix the pillar to the top of the camera protective cover.

Step 3 Align the sunshade with the center hole of the pillar, and securely fix the sunshade with screws.

3.5 Installing Corrugated Pipe

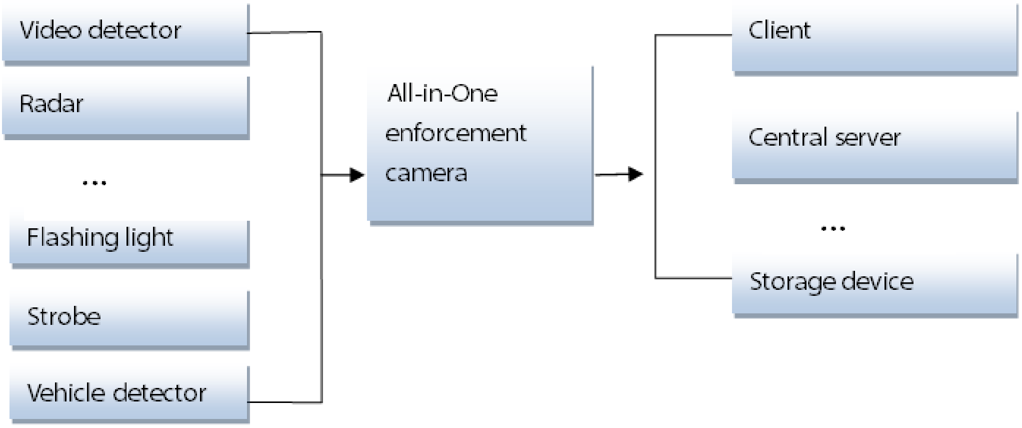
The corrugated pipe helps protect the cable.

Pull the cable into the corrugated pipe, and then pass the cable through the hole at the bottom of the Camera. After the cable is properly placed, insert the corrugated pipe into the hole until it is securely clamped.

4 System Network

As the center of traffic surveillance system, the Camera can record videos of different surveillance scenes, and transmit video data to controller, central server or storage device through network.

Figure 4-1 System network



5 Configuration

After mounting the Camera, power on the Camera, connect it to the network and make initial settings, then you can successfully log in to the web page of the Camera.
For more configurations, see the web operation manual of the HD intelligent enforcement camera.

5.1 Initialization

The Camera is delivered in uninitialized status. You need to initialize the Camera and modify its default password before it can be used.
You can initialize the cameras one by one on camera web page or in batches by using ConfigTool.

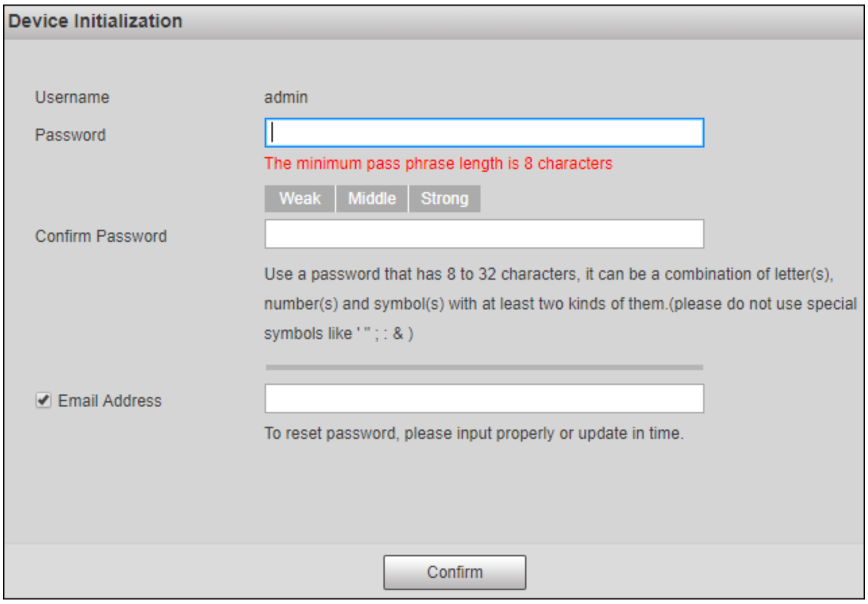
5.1.1 Initializing Single Camera on Web Page

Step 1 Connect the Camera to network.

1) Connect the Camera to PC over the Ethernet cable.
2) Keep the IP address of the PC and the camera on the same network segment. The network segment can be set to *192.168.1.X*, but cannot be the same with the factory default IP of the Camera (192.168.1.108).
3) Execute ping *x.x.x.x* (device IP) command on PC to check network connection.

Step 2 Enter the IP address of the Camera (192.168.1.108) in the browser address bar, and press the Enter key to log in to the web page of the Camera.

Figure 5-1 Device initialization



Device Initialization

Username admin

Password

The minimum pass phrase length is 8 characters

Confirm Password

Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them.(please do not use special symbols like ' " ; : &)

☑ Email Address

To reset password, please input properly or update in time.

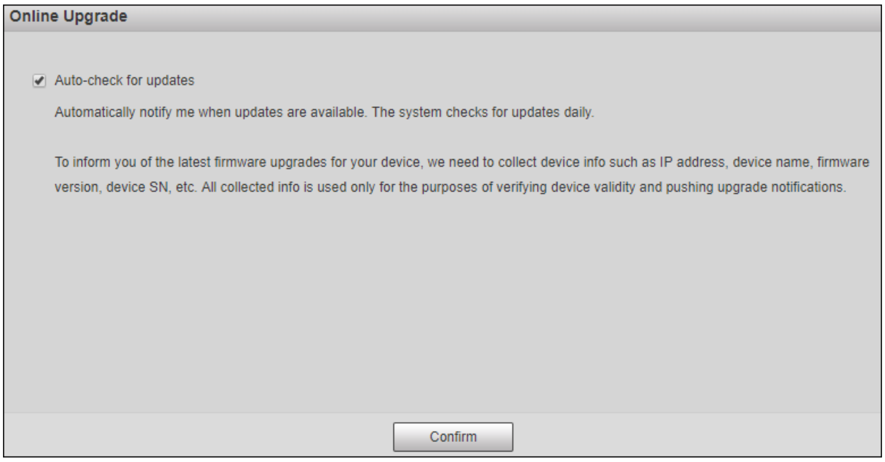
Step 3 On the **Device Initialization** page, enter your new password.

Step 4 Select the **Email Address** checkbox, and then enter your email address. This helps you reset your password when your password is lost or forgotten.

Step 5 Click **Confirm**.

Step 6 On the **Online Upgrade** page, you can cancel selecting **Auto-check for updates** (selected by default).

Figure 5-2 Login



Online Upgrade

☑ Auto-check for updates

Automatically notify me when updates are available. The system checks for updates daily.

To inform you of the latest firmware upgrades for your device, we need to collect device info such as IP address, device name, firmware version, device SN, etc. All collected info is used only for the purposes of verifying device validity and pushing upgrade notifications.

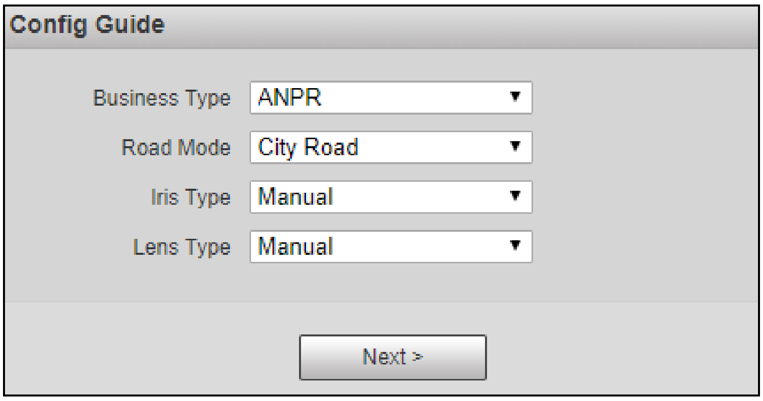
Step 7 Click **Confirm**.

Step 8 On the login page, enter the username (admin) and the password that you set.

Step 9 On the **Config Guide** page, set the business type and road mode.

- **Business Type**: You can select from **ANPR**, **E-Police** and **Yield to Pedestrians**.
- **Road Mode**: Select **City Road** or **High Road** (expressway) according to the actual installation position of the Camera.
- **Iris Type**/**Lens Type**: Only **Manual** is available.

Figure 5-3 Config guide (1)



Config Guide

Business Type: ANPR

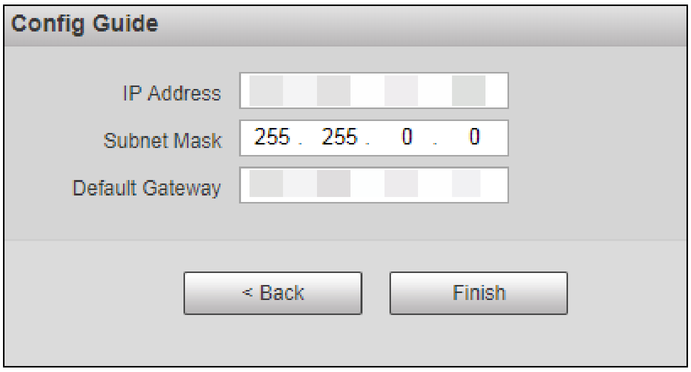
Road Mode: City Road

Iris Type: Manual

Lens Type: Manual

Step 10 Click **Next**, and you can start modifying the default IP address of the Camera.

Figure 5-4 Config guide (2)



Config Guide

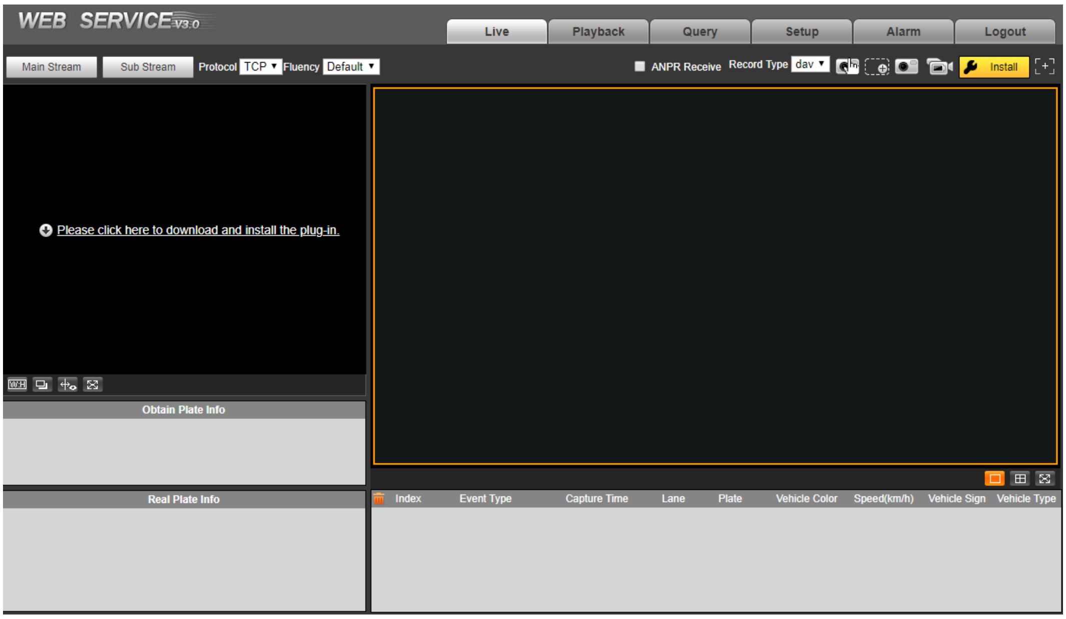
IP Address:

Subnet Mask: 255 . 255 . 0 . 0

Default Gateway:

Step 11 After configuration, click **Finish**.

Figure 5-5 Live page

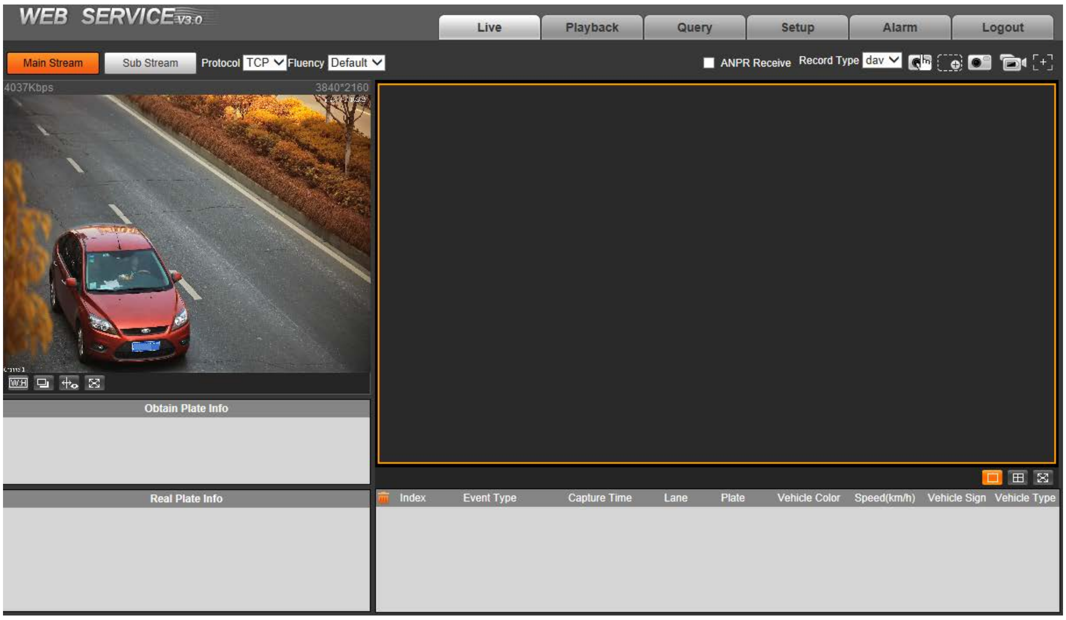


Step 12 For first-time login, click **Please click here to download and install the plug-in**, and then install the plug-in according to system prompt.

Before installing the plug-in, make sure that **ActiveX controls** (in Internet Explorer) from **Tools** > **Internet Options** > **Security** > **Custom Level** is enabled.

Step 13 After successfully installing the plug-in, the live view of the Camera is displayed.

Figure 5-6 Web page



5.1.2 Initializing Cameras in Batches with ConfigTool

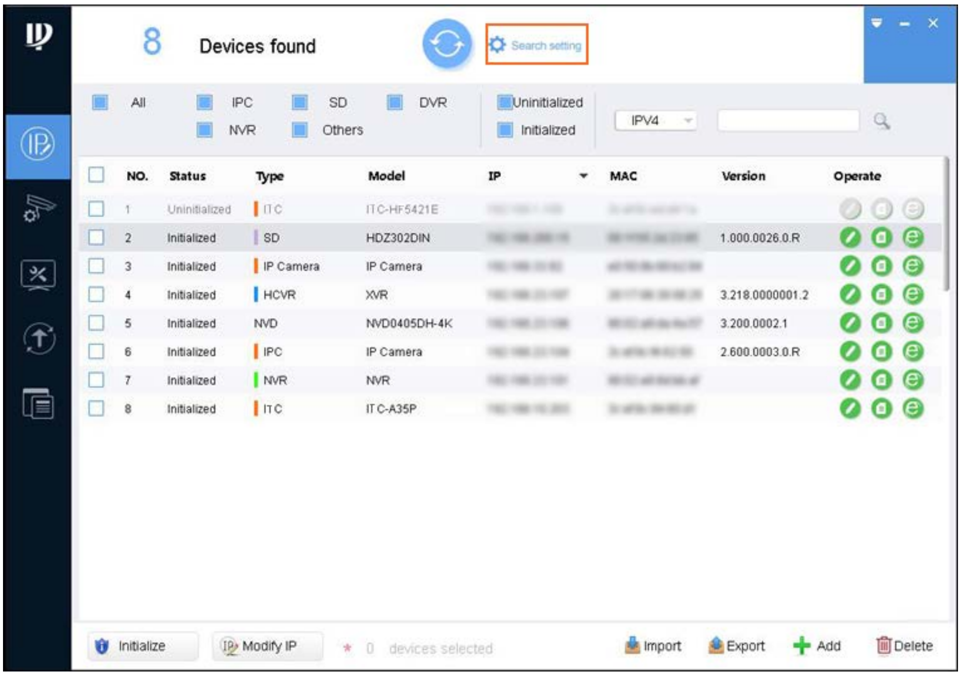
It is ideal to initialize cameras in batches and modify their default IP addresses by using ConfigTool.To acquire ConfigTool, go to Dahua official website, and then select **Support** > **Download Center** > **Tools** > **Maintenance Tools**. Find **ConfigTool**, and download and install it according to onscreen instructions.

This section takes ConfigTool 4.07.0 as the example. Different versions might have different pages.

Step 1 After installing ConfigTool, open the tool.

Step 2 Click , and then click **Search setting**.

Figure 5-7 Modify IP



NO.	Status	Type	Model	IP	MAC	Version	Operate
1	Uninitialized	ITC	ITC-HF5421E	[redacted]	[redacted]		
2	Initialized	SD	HDZ302DIN	[redacted]	[redacted]	1.000.0026.0.R	
3	Initialized	IP Camera	IP Camera	[redacted]	[redacted]		
4	Initialized	HCVR	XVR	[redacted]	[redacted]	3.218.0000001.2	
5	Initialized	NVD	NVD0405DH-4K	[redacted]	[redacted]	3.200.0002.1	
6	Initialized	IPC	IP Camera	[redacted]	[redacted]	2.600.0003.0.R	
7	Initialized	NVR	NVR	[redacted]	[redacted]		
8	Initialized	ITC	ITC-A35P	[redacted]	[redacted]		

Step 3 Enter the start IP address and end IP address of the network segment in which you want to search devices, and then click **OK** (default IP address of the Camera: 192.168.1.108).

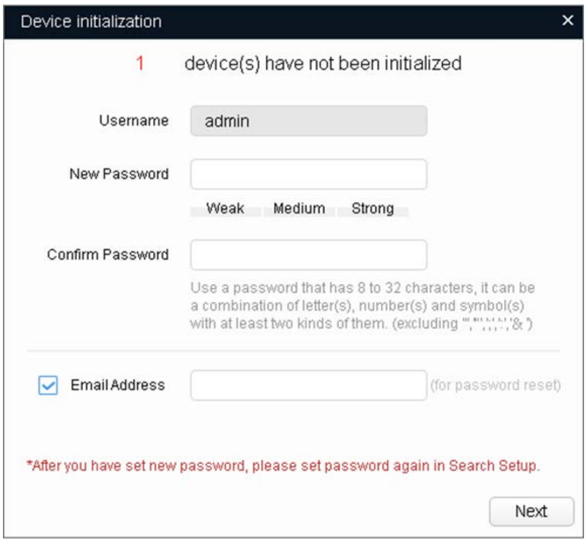
Step 4 All the devices found in the network segment are listed.

Step 5 Select cameras with **Status** showing **Uninitialized**, and then click **Initialize**.

Step 6 On the **Device initialization** page, select the devices that need initialization, and then click **Initialize**.

Step 7 Set and confirm the password of the devices, then enter a valid email address to help you reset the password when you forgot it, and then click **Next**.

Figure 5-8 Password setting



1 device(s) have not been initialized

Username: admin

New Password:

Confirm Password:

Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them. (excluding ''', '''', ';', ':', '&')

☑ Email Address: (for password reset)

*After you have set new password, please set password again in Search Setup.

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

Step 9 The **Initialization** page is displayed after initialization is completed. Click the success icon (✓) or the failure icon (⚠) for the details.

Step 10 Click **Finish**.

Step 11 The device status on the **Modify IP** page turns to **Initialized**.

5.1.3 Modifying IP Addresses in Batches with ConfigTool

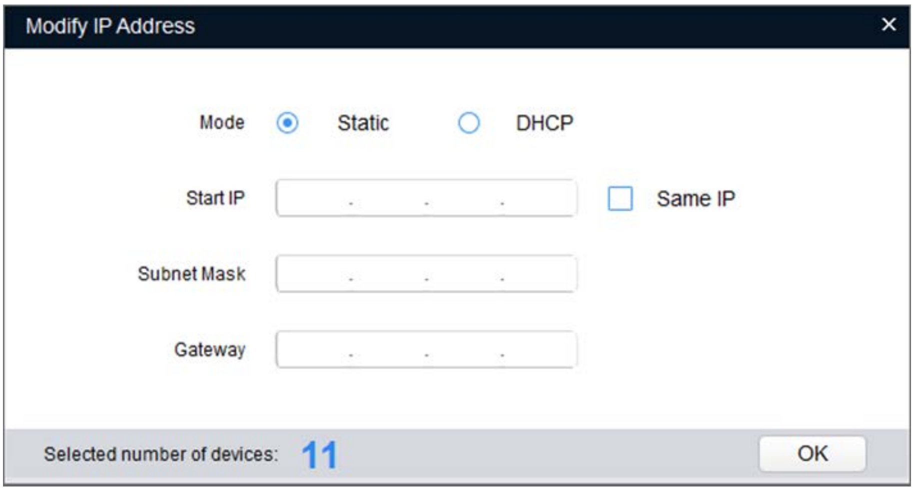
You can modify IP address of one or multiple cameras at one time. This section is based on modifying IP addresses in batches. Modifying IP addresses in batches is available only when the corresponding devices have the same login password.

Step 1 Do "Step 1" to "Step 3" in "5.1.2 Initializing Cameras in Batches with ConfigTool" to search for cameras in your network segment.

After clicking **Search setting**, enter the username and password, and make sure that they are the same as what you set during initialization; otherwise there will be **Wrong Password** notice.

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

Figure 5-9 Modify IP Address



Modify IP Address ×

Mode ● Static ○ DHCP

Start IP . . . □ Same IP

Subnet Mask . . .

Gateway . . .

Selected number of devices: 11 OK

Step 3 On the **Modify IP Address** page, select **Static** mode, and then enter start IP, subnet mask, and gateway. All the IP addresses will be modified sequentially from the start IP.

If DHCP server is available in the network, when you select **DHCP**, devices will automatically obtain IP addresses from DHCP server.

Step 4 Click **OK**.

5.2 Login

Step 1 You can log in to the web by using web browser. For first-time login, see "5.1 Initialization."

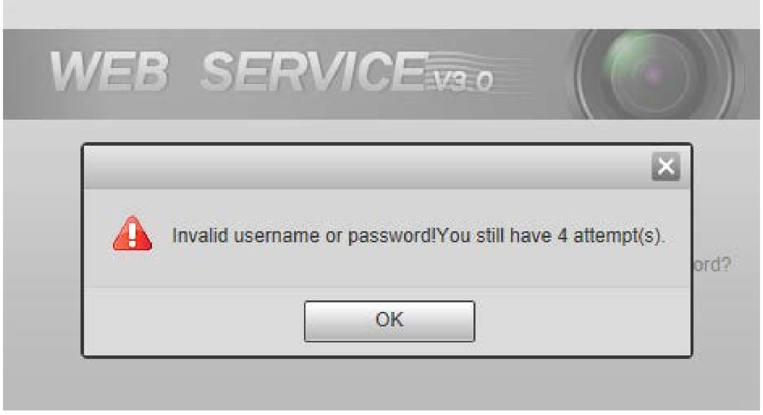
After initializing cameras in batches, you can easily go to the camera login page by clicking ⓔ on the ConfigTool page. See Figure 5-11. In this case, you do not need to enter the IP address of each camera when login.

Step 2 Enter the IP address of the Camera in the browser address bar, and press the Enter key.

Step 3 Enter username and password on the displayed page, and then click **Login**.

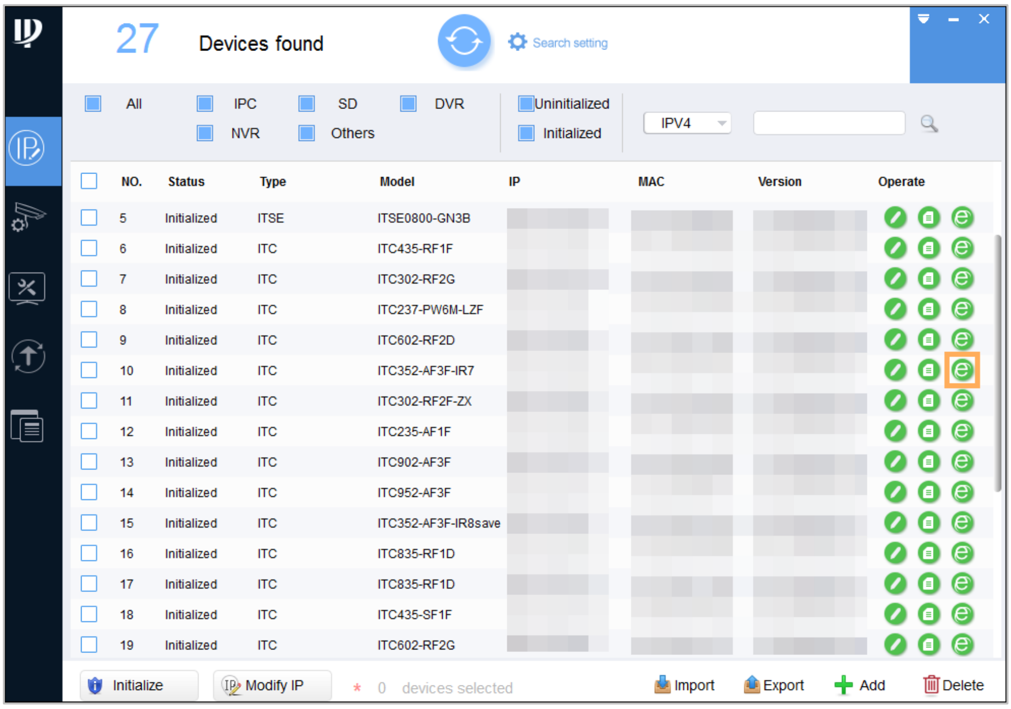
- A box pops up when the username or password is incorrect. See Figure 5-10.
- If you enter invalid username or password for five times, the account will be locked for five minutes.

Figure 5-10 Invalid username or password



Invalid username or password!You still have 4 attempt(s).

Figure 5-11 Devices found page



* 0 devices selected

NO.	Status	Type	Model	IP	MAC	Version	Operate
5	Initialized	ITSE	ITSE0800-GN3B	[redacted]	[redacted]	[redacted]	
6	Initialized	ITC	ITC435-RF1F	[redacted]	[redacted]	[redacted]	
7	Initialized	ITC	ITC302-RF2G	[redacted]	[redacted]	[redacted]	
8	Initialized	ITC	ITC237-PW6M-LZF	[redacted]	[redacted]	[redacted]	
9	Initialized	ITC	ITC602-RF2D	[redacted]	[redacted]	[redacted]	
10	Initialized	ITC	ITC352-AF3F-IR7	[redacted]	[redacted]	[redacted]	
11	Initialized	ITC	ITC302-RF2F-ZX	[redacted]	[redacted]	[redacted]	
12	Initialized	ITC	ITC235-AF1F	[redacted]	[redacted]	[redacted]	
13	Initialized	ITC	ITC902-AF3F	[redacted]	[redacted]	[redacted]	
14	Initialized	ITC	ITC952-AF3F	[redacted]	[redacted]	[redacted]	
15	Initialized	ITC	ITC352-AF3F-IR8save	[redacted]	[redacted]	[redacted]	
16	Initialized	ITC	ITC835-RF1D	[redacted]	[redacted]	[redacted]	
17	Initialized	ITC	ITC835-RF1D	[redacted]	[redacted]	[redacted]	
18	Initialized	ITC	ITC435-SF1F	[redacted]	[redacted]	[redacted]	
19	Initialized	ITC	ITC602-RF2G	[redacted]	[redacted]	[redacted]	

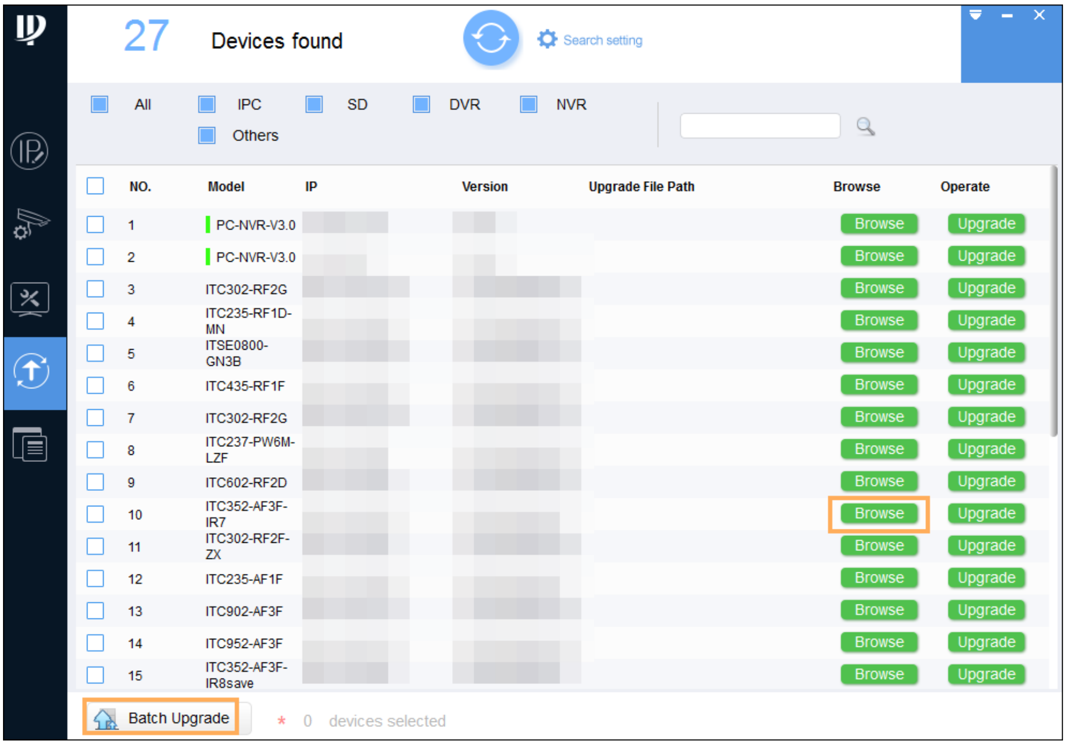
5.3 Updating the Camera with ConfigTool

The ConfigTool supports updating the cameras one by one or in batches.

Step 1 Open ConfigTool.

Step 2 Click ⬆.

Figure 5-12 Upgrade



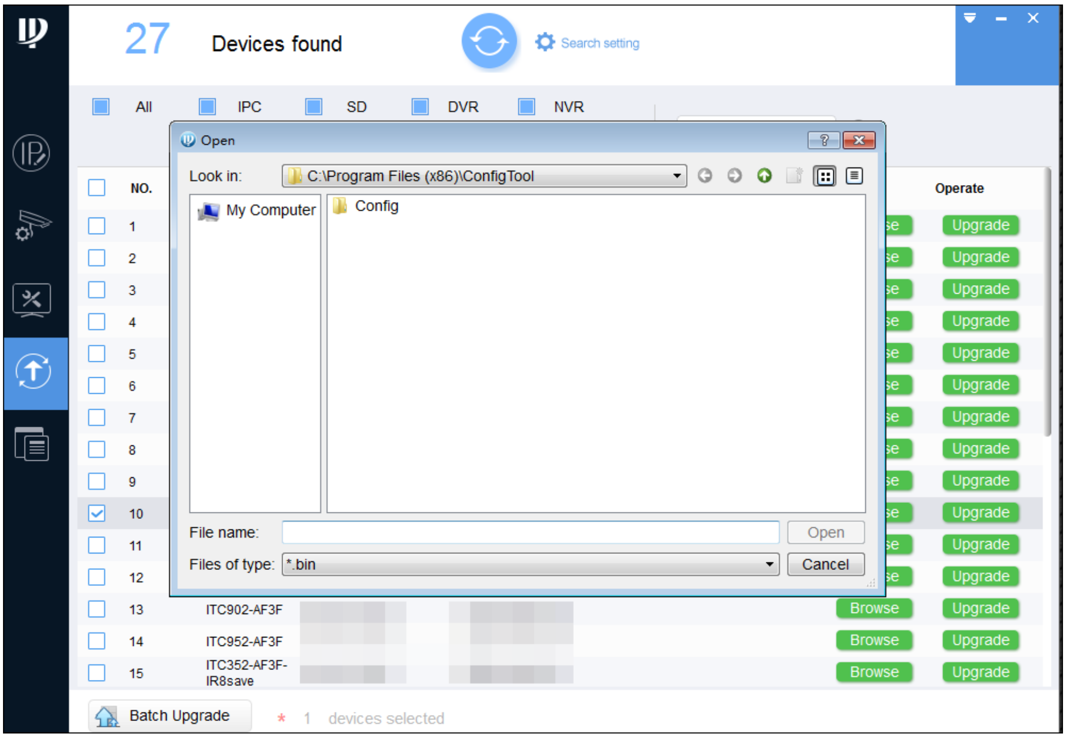
☐	NO.	Model	IP	Version	Upgrade File Path	Browse	Operate
☐	1	PC-NVR-V3.0	[redacted]	[redacted]		Browse	Upgrade
☐	2	PC-NVR-V3.0	[redacted]	[redacted]		Browse	Upgrade
☐	3	ITC302-RF2G	[redacted]	[redacted]		Browse	Upgrade
☐	4	ITC235-RF1D-MN	[redacted]	[redacted]		Browse	Upgrade
☐	5	ITSE0800-GN3B	[redacted]	[redacted]		Browse	Upgrade
☐	6	ITC435-RF1F	[redacted]	[redacted]		Browse	Upgrade
☐	7	ITC302-RF2G	[redacted]	[redacted]		Browse	Upgrade
☐	8	ITC237-PW6M-LZF	[redacted]	[redacted]		Browse	Upgrade
☐	9	ITC602-RF2D	[redacted]	[redacted]		Browse	Upgrade
☐	10	ITC352-AF3F-IR7	[redacted]	[redacted]		Browse	Upgrade
☐	11	ITC302-RF2F-ZX	[redacted]	[redacted]		Browse	Upgrade
☐	12	ITC235-AF1F	[redacted]	[redacted]		Browse	Upgrade
☐	13	ITC902-AF3F	[redacted]	[redacted]		Browse	Upgrade
☐	14	ITC952-AF3F	[redacted]	[redacted]		Browse	Upgrade
☐	15	ITC352-AF3F-IR8save	[redacted]	[redacted]		Browse	Upgrade

Step 3 Select the ITCs (cameras) that you want to update.

- Update one ITC: Click **Browse** corresponding to the ITC to be updated.
- Update ITCs in batches: Select the ITCs to be updated, and then click **Batch Upgrade**.

Step 4 Select the update file.

Figure 5-13 Select the upgrade file



Open

Look in: C:\Program Files (x86)\ConfigTool

My Computer

Config

File name:

Files of type: *.bin

Open

Cancel

☐	NO.	Model
☐	1	
☐	2	
☐	3	
☐	4	
☐	5	
☐	6	
☐	7	
☐	8	
☐	9	
☑	10	
☐	11	
☐	12	
☐	13	ITC902-AF3F
☐	14	ITC952-AF3F
☐	15	ITC352-AF3F-IR8save

Step 5 Update the cameras.

- Update one ITC: Click **Upgrade**, and the system starts updating. You can view the update progress.
- Update ITCs in batches: Click **OK**, and the system starts updating.

If the camera is disconnected during updating, as long as the ConfigTool stays on the update page, the update will resume when the connection is restored.

6 FAQ

Question	Solution
Device error, unable to start or operate normally	Press and hold Reset button for 5 seconds to restore the Camera to factory settings.
TF card hot swapping	Stop recording and image capturing, and then wait for at least 15 seconds before removing the TF card. This helps ensure data integrity and avoid losing all the data of the card.
TF card read/write limit	Do not set the TF card as the storage media of pre-set recording. It might damage the TF card duration.
TF card cannot be used as storage media	When the TF card hibernates or its capacity is full, format the card through web first.
Recommended TF card	It is recommended to use TF card of 16 GB or above. This helps avoid data loss arising from insufficient capacity. You can use card of 16 GB, 32 GB, 64 GB, and 128 GB.

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 from Dahua 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. **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.

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 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.

12. **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.

13. **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.

- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883