

Smart Video Parking Detector

User's Manual



Foreword

General






This manual introduces the installation, functions and operations of the smart video parking detector (hereinafter referred to as "the Camera"). Read carefully before using the Camera, and keep the manual safe for future reference.

Models

| Models | Power Supply | Pixel | Sensor |
|---------------------|--|-------|---------------|
| ITC214-PH5B-F3-POE | PoE | 2 MP | Single sensor |
| ITC414-PH5B-F2-POE | | 4 MP | |
| ITC414-PH5B-TF2-POE | | | Dual-sensor |
| ITC214-PH5B-F3 | Cascading with network cables to provide 48 V power supply | 2 MP | Single sensor |
| ITC414-PH5B-F2 | | 4 MP | |
| ITC414-PH5B-TF2 | | | Dual-sensor |

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

| Version | Revision Content | Release Time |
|---------|------------------|--------------|
| V1.0.0 | First release. | January 2022 |

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 Camera, hazard prevention, and prevention of property damage. Read carefully before using the Camera, and comply with the guidelines when using it.

Transportation Requirements



Transport the Camera under allowed humidity and temperature conditions.

Storage Requirements



Store the Camera under allowed humidity and temperature conditions.

Installation Requirements



- Do not connect the power adapter to the Camera 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 Camera.
- Do not connect the Camera to two or more kinds of power supplies, to avoid damage to the Camera.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Camera in a place exposed to sunlight or near heat sources.
- Keep the Camera away from dampness, dust, and soot.
- Put the Camera 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 Camera label.
- the Camera is a class I electrical appliance. Make sure that the power supply of the Camera 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 Camera 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 Camera while the adapter is powered on.
- Operate the Camera within the rated range of power input and output.
- Use the Camera under allowed humidity and temperature conditions.

- Do not drop or splash liquid onto the Camera, and make sure that there is no object filled with liquid on the Camera to prevent liquid from flowing into it.
- Do not disassemble the Camera.
- Do not aim the Camera at strong light sources (such as lamplight, and sunlight) when focusing it.
- Do not vibrate, squeeze or immerse the Camera in liquid during transportation, storage or installation.
- Do not block the ventilation near the Camera.
- We recommend you use the Camera 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 Camera (grounding cable or lightning surge protector) to improve its reliability. the Camera is a class I electrical appliance. Make sure that the power supply of the Camera is connected to a power socket with protective earthing.
- the Camera must be used with the protective cover for outdoor scenarios to avoid the risk of water damage to the Camera.
- 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 Camera.
- Modify the default password of the Camera after first-time login to prevent the Camera from being stolen.

Maintenance Requirements

- Pack the Camera 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 Camera 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

| | |
|--|-----------|
| Foreword | I |
| Important Safeguards and Warnings..... | III |
| 1 Introduction | 1 |
| 1.1 Overview | 1 |
| 1.2 Features..... | 1 |
| 2 Structure | 3 |
| 2.1 Appearance..... | 3 |
| 2.2 Dimensions | 3 |
| 2.3.1 PoE Cable Connection | 4 |
| 2.3.2 Cascading Power Supply..... | 4 |
| 3 Installation..... | 6 |
| 3.1 Cable Wiring..... | 6 |
| 3.2 Installing the Camera..... | 6 |
| 4 Camera Configurations..... | 8 |
| 4.1 Initialization | 8 |
| 4.2 Changing IP Address..... | 9 |
| 5 Web Configuration | 10 |
| 5.1 Web Login..... | 10 |
| 5.1.1 Recommended System Requirements | 10 |
| 5.1.2 Login | 10 |
| 5.1.3 Resetting Password | 11 |
| 5.1.4 Web Functions..... | 12 |
| 5.2 Live..... | 13 |
| 5.2.1 Video Stream..... | 14 |
| 5.2.2 Live View | 14 |
| 5.2.3 Real Plate Information | 15 |
| 5.2.4 Functions of the Live Page | 15 |
| 5.2.5 Live View Snapshot..... | 16 |
| 5.2.6 Event List..... | 16 |
| 5.3 Query | 16 |
| 5.3.1 Image Search..... | 16 |
| 5.3.2 Recording Search | 17 |
| 5.3.2.1 Recording..... | 17 |
| 5.3.2.2 Watermark..... | 17 |
| 5.3.3 Parking Record Search | 18 |

| | |
|---|----|
| 5.4 Setting | 18 |
| 5.4.1 ITC | 19 |
| 5.4.1.1 Configuring Parking Spaces | 19 |
| 5.4.1.2 Allowlist | 20 |
| 5.4.1.3 OSD Configuration | 21 |
| 5.4.1.3.1 Video OSD | 21 |
| 5.4.1.3.2 Snapshot OSD | 22 |
| 5.4.1.4 Light Control | 23 |
| 5.4.1.5 RS-485 | 26 |
| 5.4.1.6 Voice Broadcast | 27 |
| 5.4.1.6.1 Broadcast Content | 27 |
| 5.4.1.6.2 Volume/Encoding | 28 |
| 5.4.1.7 Device Test | 28 |
| 5.4.2 Camera | 29 |
| 5.4.2.1 Camera Attribute | 29 |
| 5.4.2.1.1 General | 29 |
| 5.4.2.1.2 Advanced Attributes | 30 |
| 5.4.2.2 Video | 31 |
| 5.4.2.2.1 Video | 31 |
| 5.4.2.2.2 Snapshot | 32 |
| 5.4.2.2.3 Region of Interest | 33 |
| 5.4.3 Network | 34 |
| 5.4.3.1 TCP/IP | 34 |
| 5.4.3.2 Port | 35 |
| 5.4.3.3 Auto Register | 36 |
| 5.4.3.4 Platform | 36 |
| 5.4.3.4.1 ONVIF | 36 |
| 5.4.3.4.2 Info Push Platform | 36 |
| 5.4.4 Event | 37 |
| 5.4.5 Storage | 38 |
| 5.4.6 System | 38 |
| 5.4.6.1 General | 38 |
| 5.4.6.1.1 General Setup | 38 |
| 5.4.6.1.2 Date & Time | 38 |
| 5.4.6.2 Account | 39 |
| 5.4.6.2.1 Account | 39 |
| 5.4.6.2.2 ONVIF User | 40 |
| 5.4.6.3 Safety | 41 |

| | |
|---|----|
| 5.4.6.3.1 System Service..... | 41 |
| 5.4.6.3.2 HTTPS..... | 42 |
| 5.4.6.3.3 Firewall..... | 45 |
| 5.4.6.4 Default Settings..... | 45 |
| 5.4.6.5 Import/Export..... | 46 |
| 5.4.6.6 Automatic Maintenance..... | 46 |
| 5.4.6.7 Update..... | 46 |
| 5.4.7 Information..... | 47 |
| 5.4.7.1 Version..... | 47 |
| 5.4.7.2 Log..... | 48 |
| 5.4.7.2.1 System Log..... | 48 |
| 5.4.7.2.2 Remote log..... | 48 |
| 5.4.7.3 Online User..... | 48 |
| 5.4.7.4 Legal Information..... | 48 |
| 5.5 Alarm..... | 49 |
| 5.6 Logout..... | 49 |
| Appendix 1 Cybersecurity Recommendations..... | 50 |

1 Introduction

1.1 Overview

This Camera is an intelligent parking space detector that can be used in the intelligent parking lot management system for parking guidance and reverse vehicle search in indoor parking lots.

- It detects and captures vehicles, recognizes license plates, detects parking space status (empty or occupied), and controls the indicator light of parking spaces.
- When connected to the parking management system, LED display, and reverse vehicle search device, it provides parking guidance for drivers and facilitates reverse vehicle search for an improved parking experience.

1.2 Features

Intelligent Recognition

- Supports drawing detection area to detect the status of parking spaces (empty or occupied), and automatically captures pictures.
- Recognizes license plates.
- Supports detecting vehicles without license plates, and the detection threshold can be set.
- OSD overlay on videos and snapshots.

Attractive Design

Attractive dome design, parking space indicator light, and ceiling installation allow the Camera to meet the needs of indoor parking lots.

Wide Dynamic Range (WDR)

WDR is available on select models, making these models work well in both dark and bright scenes.

Integration

- It has a dome design, parking space indicator light, and uses a ceiling mount, allowing it to meet the needs of the parking lots.
- Some models support wide dynamic mode, which can automatically adapt to brightly lit and poorly lit scenes.

Multi-color Indicator Light

- 7 colors are available for the indicator light, and the indicator light status can be adjusted as needed.
- The Camera detects vehicles by video detection and recognizes license plates. The indicator light displays the status of the parking space (empty or occupied) according to the detection results.
- Supports configuring the indicator color according to the network port status.

Multiple Parking Space Detection

- ITC214-PH5B-F series support detecting 2 parking spaces at the same time.
- ITC414-PH5B-F series support detecting 3 parking spaces at the same time.
- ITC414-PH5B-TF series support detecting 6 parking spaces at the same time.

Power Supply

Standard 48 VDC power supply. It can also adapt to 12–48 VDC voltage.

2 Structure

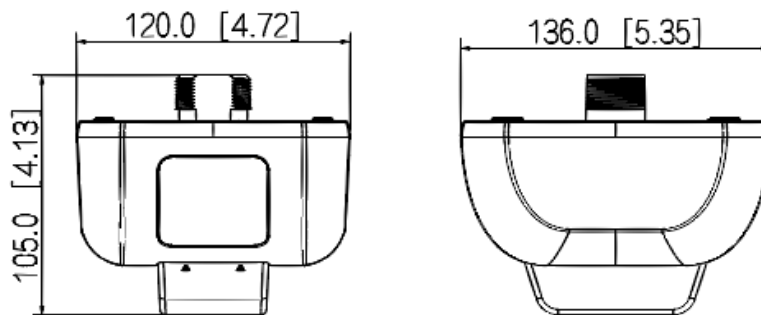
2.1 Appearance

Figure 2-1 Appearance



2.2 Dimensions

Figure 2-2 Dimensions (mm [inch])



2.3 Cable Connection

2.3.1 PoE Cable Connection

Figure 2-3 PoE

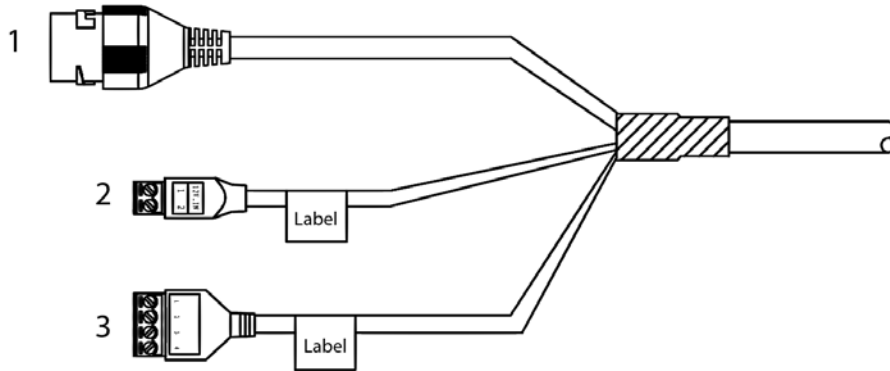


Table 2-1 PoE cable description

| No. | Name | Description |
|-----|----------------|--|
| 1 | Network port | Connect to standard Ethernet cable. PoE is supported. |
| 2 | Power | <ul style="list-style-type: none"> • 1: 12 VDC_IN. • 2: GND_IN. |
| 3 | External light | <ul style="list-style-type: none"> • 1: 12V_OUT. • 2: GND_OUT. • 3: RS-485_A. • 4: RS-485_B. |

2.3.2 Cascading Power Supply

Figure 2-4 Network cable

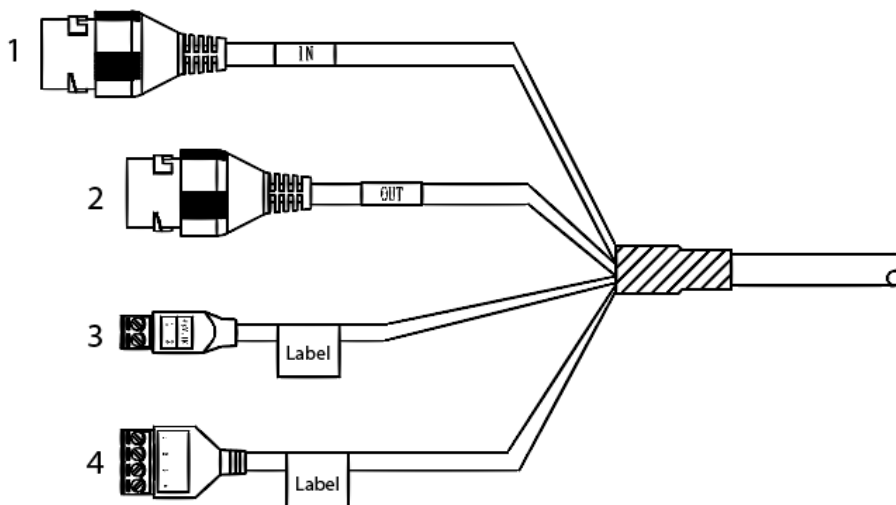


Table 2-2 Network cable description

| No. | Name | Description |
|-----|--------------------|--|
| 1 | Network port (IN) | Network power input port. |
| 2 | Network port (OUT) | Network power output port. |
| 3 | Power | <ul style="list-style-type: none"> ● 1: 48V_IN. ● 2: GND_IN. |
| 4 | External light | <ul style="list-style-type: none"> ● 1: 12V_OUT. ● 2: GND_OUT. ● 3: RS-485_A. ● 4: RS-485_B. |

3 Installation

3.1 Power Supply

- ITC214-PH5B-F3-POE, ITC414-PH5B-F2-POE and ITC414-PH5B-TF2-POE series devices are supplied with PoE.
- ITC214-PH5B-F3, ITC414-PH5B-F2 and ITC414-PH5B-TF2 series devices supports cascading with network cables to provide 48 V power supply. 4 dual-sensor cameras or 8 single-sensor cameras can be supplied at the same time.

3.2 Installing the Camera



Mount the Camera to the ceiling mounting tray, and the installation surface must be able to bear at least 3 times the weight of the Camera.



- The stud diameter is 33 mm.
- The installation uses ITC214-PH5B-F3-POE as an example. The installation diagram is for reference only, and might differ from the actual device.

Step 1 Use a hole saw to drill a hole with a diameter of 35 mm at the device mounting position.

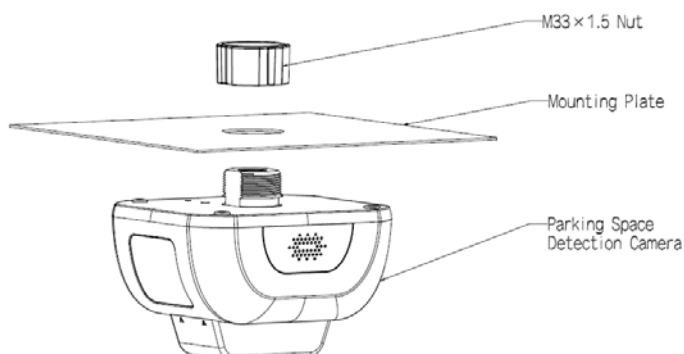
Figure 3-1 Hole saw



Step 2 Feed the cables of the Camera through the hole on the mounting plate.

Step 3 Loosen the nut, feed the cable through the nut, and then fix the nut to the mounting plate.

Figure 3-2 Installation



Step 4 Refer to "2.3 Cable Connection" to connect the cables.

Step 5 Remove the cover, and adjust the monitoring view according to the position of the Camera.

Step 6 Tighten the cover.

4 Camera Configurations

4.1 Initialization

Prerequisites

- The Camera is delivered uninitialized by default. You need to initialize it and change its password before further operations.
- Before initialization, make sure the IP of the computer and the Camera are on the same network segment, otherwise the initialization might fail.

Procedure

- Step 1 Set IP address, subnet mask, and gateway of the computer and the Camera respectively.
- If there is no router in the network, distribute IP address of the same segment.
 - If there is router in the network, configure the corresponding gateway and subnet mask.
- Step 2 Use ping `***.***.***.***` (device IP address) command to check whether network is connected.
- Step 3 Open browser, enter the IP address of the Camera in the address bar, and then press the Enter key.

Figure 4-1 Device Initialization

The screenshot shows a web form titled "Device Initialization". It contains the following elements:

- Username:** A text input field with "admin" entered.
- Password:** A text input field. Below it, a red error message reads: "The minimum pass phrase length is 8 characters".
- Confirm Password:** A text input field.
- Strength Indicators:** Three buttons labeled "Weak", "Middle", and "Strong" are positioned between the Password and Confirm Password fields.
- Instructions:** A paragraph of text below the Confirm Password field: "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:** A checkbox labeled "Email Address" is checked. Below it is a text input field.
- Footer Note:** Below the Email Address field, it says: "To reset password, please input properly or update in time."
- Confirm Button:** A button labeled "Confirm" is located at the bottom center of the form.

- Step 4 Enter and confirm the new password.




If you want to change your password again, go to **Setup > System > Account > Account**.

- Step 5 Select **Email Address**, and then enter your email address (recommended to set for resetting your password).
- Step 6 Click **Confirm**.
The **Live** page of the Camera is displayed.

4.2 Changing IP Address

You can acquire and change the IP address of devices accessed through wired network. This section uses changing IP address with ConfigTool as the example.

Step 1 Get ConfigTool from technical support and install it on your local computer.

Step 2 Double-click .

Step 3 Click **Modify IP** on the homepage.

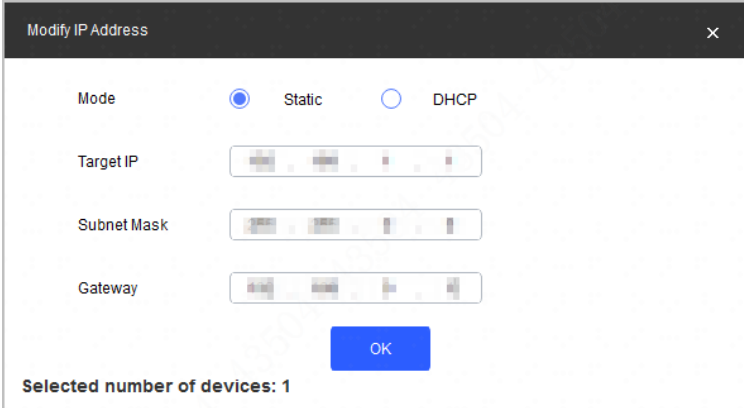
Step 4 Select the device(s) whose IP need(s) to be changed.

- Change one IP address: Click **Edit** corresponding to the device.
- Change IP addresses in batches: Select the devices, and then click **Batch Modify IP**.

Step 5 Set mode, IP, subnet mask and gateway.

Step 6 Click **OK**.

Figure 4-2 Change IP addresses in batches



Modify IP Address

Mode Static DHCP

Target IP

Subnet Mask

Gateway

OK

Selected number of devices: 1

5 Web Configuration

Log in to the Camera web client through browser on the computer, and then you can configure, operate on, and manage the Camera.



The pages and settings are for reference only, and might differ from the actual page.

5.1 Web Login

5.1.1 Recommended System Requirements

Table 5-1 Recommended system requirements

| PC Component | Recommended System Requirements |
|------------------|--|
| Operating System | Windows 7, and later |
| CPU | Intel core i3, and faster processor |
| Graphics | Intel HD Graphics, and later |
| RAM | 2 GB, and larger |
| Monitor | 1024 × 768, and higher |
| Browser | Internet Explorer 9/11, Chrome 33/41, Firefox 49 |

5.1.2 Login

For first-time login or logging in after restoring factory default settings, see "4.1 Initialization".

Step 1 Enter the IP address of the Camera in the browser address bar, and then press Enter.

Step 2 Enter your login username and password, and then click **Login**.

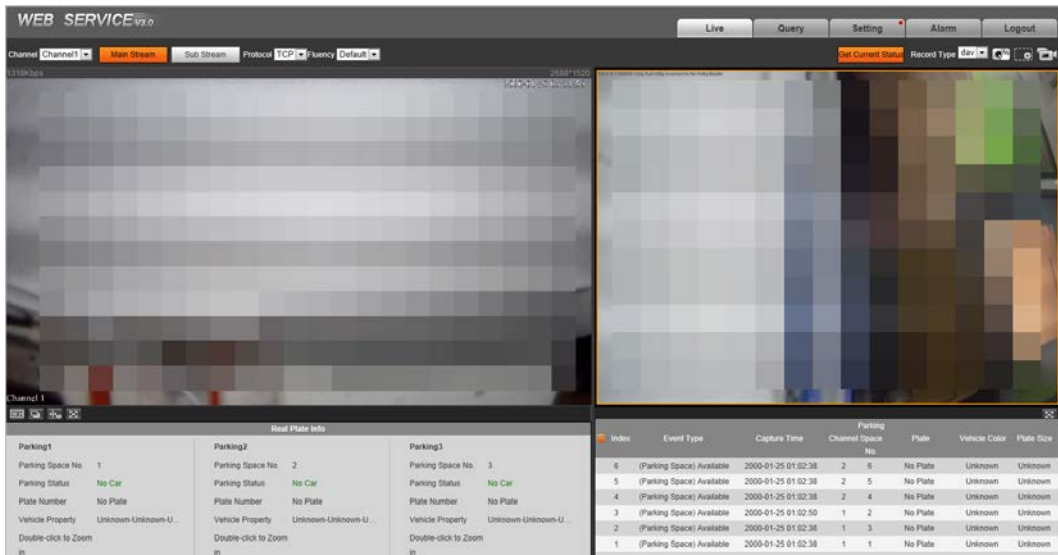
Step 3 For first-time login, click **Please click here to download and install the plug-in**, and then install the plug-in according to system prompt.



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

Step 4 After successfully installing the plug-in, the live view of the Camera is displayed.

Figure 5-1 Live



5.1.3 Resetting Password

When you forgot your password, you can configure new password through the password reset function.



- One device can generate security code up to 10 times in one day, so the Camera can be reset up to 10 times in one day.
- When scanning QR code to acquire security code, one QR code can only get two security codes at most.
- After receiving security code by email, you need to reset password within 24 hours, otherwise, the security code will be invalid.
- Email address must be filled in during device initialization; otherwise it will fail to send you the security code, and you will not be able to reset your password. Email address of admin can be modified from **Setting > System > Account > Account**.

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

Step 2 Click **Forgot password?**

Step 3 Click **OK** in the prompted window.

Step 4 Scan the QR code according to the page prompt, and send the scanning result to the designated email to acquire security code.



Scan the actual QR code. Do not scan the QR code in this manual.

Figure 5-2 Reset password (1)

Reset the password(1/2)

QR code:

Note(For admin only):
Please use an APP to scan the left QR code to get special strings. And then send the strings to support_gpwd@htmicrochip.com.

The security code will be delivered to 1***@gmail.com.

Security code:

Cancel Next

Step 5 Enter received security code in the text box of **Security code**.

Step 6 Click **Next**.

Figure 5-3 Reset password (2)

Reset the password(2/2)

Username admin

Password

Weak Middle Strong

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.

Confirm Password

No Yes

Step 7 Set **Password**, and enter your new password again in **Confirm Password**.

- The new password must consist of 8 to 32 characters, and contain at least two types from upper cases, lower cases, numbers, and special characters (excluding ' " ; : and &).
- The new password must be the same as the **Confirm Password**. Follow the password security notice to set a high security level password.

Step 8 Click **OK**.

5.1.4 Web Functions

This section mainly introduces the following 6 functions on the web page.

Figure 5-4 Tab



Table 5-2 Tab function description

| Tab | Function |
|---------|---|
| Live | View, and record live video, and image, adjust video, and image window, set client image parameter, and so on. |
| Query | Search for different types of pictures, and videos, and configure watermark verification of videos. |
| Setting | Set rules of intelligent traffic, camera basic attribute, network, event, storage, and system, and view system information. |
| Alarm | Set alarm prompt. |
| Logout | Log out web. |

The following buttons are very common on the web page.

Table 5-3 Common buttons description

| Button | Description |
|--------|---|
| | Restore all parameters to system defaults. |
| | Recover the parameters to the value last saved. |
| | Save the settings. |

5.2 Live

Click the **Live** tab.

On this page, several functions such as live video, live picture, real-time capture, record, and config (LPR) are supported.



For dual-sensor models, you can select a channel to view the corresponding live video.

Figure 5-5 Live

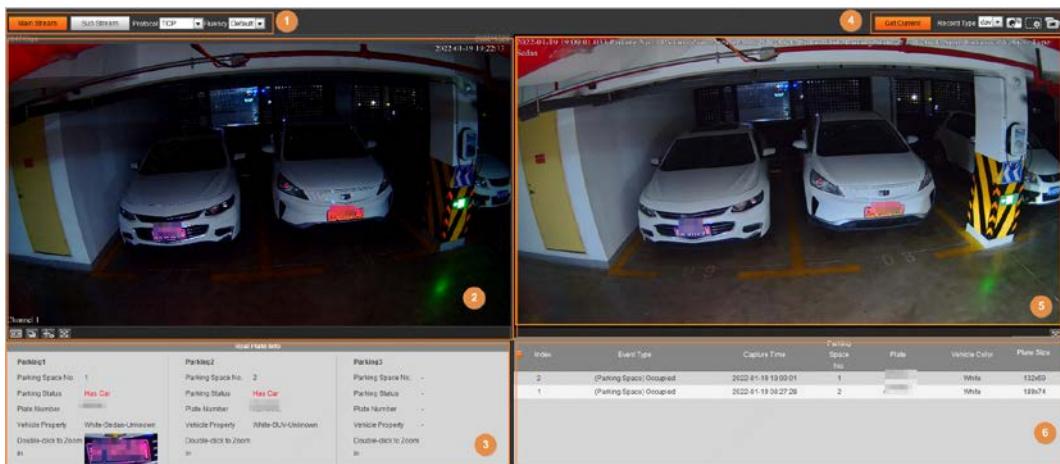


Table 5-4 Live page description

| No. | Description |
|-----|---|
| 1 | Video stream type, protocol and fluency |
| 2 | Live view |
| 3 | Information of parking spaces and parked vehicles |
| 4 | Functions of Live page |
| 5 | Live view snapshot |
| 6 | Event list |

5.2.1 Video Stream

- **Channel:** For dual-sensor models, you can select a channel and then set the corresponding stream type for the channel.
- **Main Stream:** Make sure that the Camera can record video, and carry out network surveillance when the network is normal. You can configure main stream resolution within the supported range of the Camera.
- **Sub Stream:** Replaces main stream to make network surveillance, and reduces the network bandwidth possession when network bandwidth is insufficient.
- **Protocol:** Video surveillance protocol, currently it only supports TCP.
- **Fluency:** Fluency of viewing the live video. The fluency can be set to **High**, **Middle**, **Low**, and **Default** (recommended).

5.2.2 Live View

Displays the live video captured by the Camera. You can also click the icons to change the display mode of live view.






- : Adjust the image to original size or adapt to the window.
- : Click it to switch to big window, and click  at the lower-left corner to display image adjustment window. Click it again to exit big window.

Figure 5-6 Big window



- : Click it to display the original image of the Camera.
- : Click it to enable smart track detection. plate number, vehicle bounding box, and other smart tracking information will be displayed in the video image.







- : Click it, and the window is displayed in full screen; double-click or right-click to exit full screen.

Table 5-5 Image adjustment description

| Icon | Name | Description |
|---|------------|---|
|  | Brightness | Adjust the overall image brightness. Change the value when the image is too bright or too dark. The range is from 0 to 128 (64 by default). |
|  | Contrast | Change the value when the image brightness is proper but contrast is not enough. The range is from 0 to 128 (64 by default). |
|  | Hue | Adjust the image hue. For example, change red into blue. The default value is made by the light sensor, and normally it does not have to be adjusted. The range is from 0 to 128 (64 by default). |
|  | Saturation | Adjust the color vividness, and will not influence the image overall brightness. The range is from 0 to 128 (64 by default). |
|  | — | Restore brightness, contrast, saturation, and hue to default values. |



In this image adjustment window, you can only adjust image brightness, contrast, hue, and saturation of local web. To adjust system brightness, contrast, hue, and saturation, go to **Setting > Camera > Camera Attribute > General**.

5.2.3 Real Plate Information

At the lower-left corner of the **Live** page, information of parking space and parked vehicles are displayed, including parking space number and status, plate number of the parked vehicle and vehicle property.

5.2.4 Functions of the Live Page

This section introduces operations such as image, and video capture, zoom, record, and talk.

Figure 5-7 General function option column

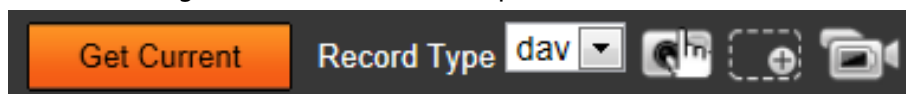










Table 5-6 General function description

| Icons | Name | Description |
|---|-----------------|--|
|  | Get Current | View the newest snapshot of parking space status change. |
|  | Record Type | Select the format of video recordings (dav by default). |
|  | Manual Snapshot | <p>Take a snapshot when a vehicle passes. The snapshot is saved to the storage path.</p> <p></p> <ul style="list-style-type: none"> • Enable ANPR Receive first. • To change the storage path of snapshots, go to Setting > Storage > Destination > Save Path. |

| Icons | Name | Description |
|---|-----------------|---|
|  | Digital Zoom | Drag to select any area in the video window, and then the area will be zoomed in. In any area of the video window, click  or right-click to exit. |
|  | Video Recording | Click it to start recording. Click  to stop recording. You can set the storage path of video recordings from Setting > Storage > Destination > Save Path . |

5.2.5 Live View Snapshot

When the status of the marked parking spaces changes, the Camera takes a snapshot and records an event. You can also manually take a snapshot.

5.2.6 Event List

Click **Get Current**, and the event information will be refreshed, including index, event type, capture time, channel, parking space number and the corresponding plate, color and plate size.



Channel information is only available when the Camera has dual sensors.

5.3 Query

Click the **Query** tab, and the system displays the query page where you can search for pictures, and video recordings.

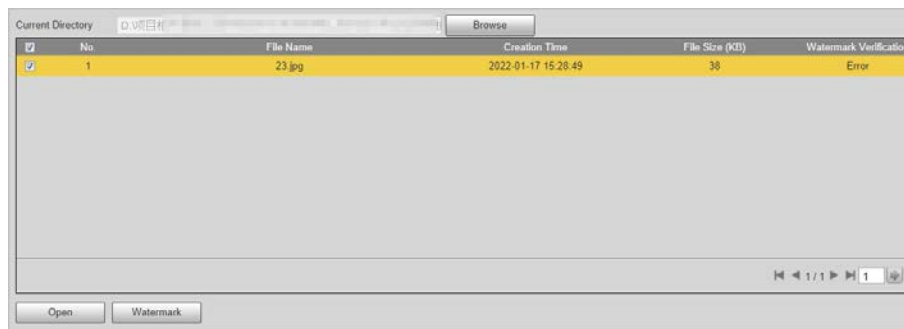
5.3.1 Image Search

With watermark verification, the Camera can check whether the captured snapshot is tampered. If the snapshot is verified with watermarks, the authenticity of the snapshot is guaranteed.

Step 1 Select **Query** > **Image Search** > **PC Picture**.

Step 2 Click **Browse**, and select the folder where the picture to be verified is located.

Figure 5-8 PC picture



Step 3 Select the picture which needs to be verified.

Step 4 Click **Watermark**, and view the result under **Watermark Verification**.

- When the result is **Error**, the picture is tampered.

- When the result is **Normal**, the picture is not tampered.



Click **Open** or double-click the picture if you need to preview the picture.

5.3.2 Recording Search

The Camera allows you to play local recordings, add watermarks to them and verify whether the video is tampered by using watermarks.

5.3.2.1 Recording

Step 1 Select **Query > Recording Search > Recording**.

Step 2 Click **Browse**, select a recording from your local storage, and then click **Open**. Functions, such as adjust image size, IVS and full screen are supported while you play the recording.

Figure 5-9 Play the recording

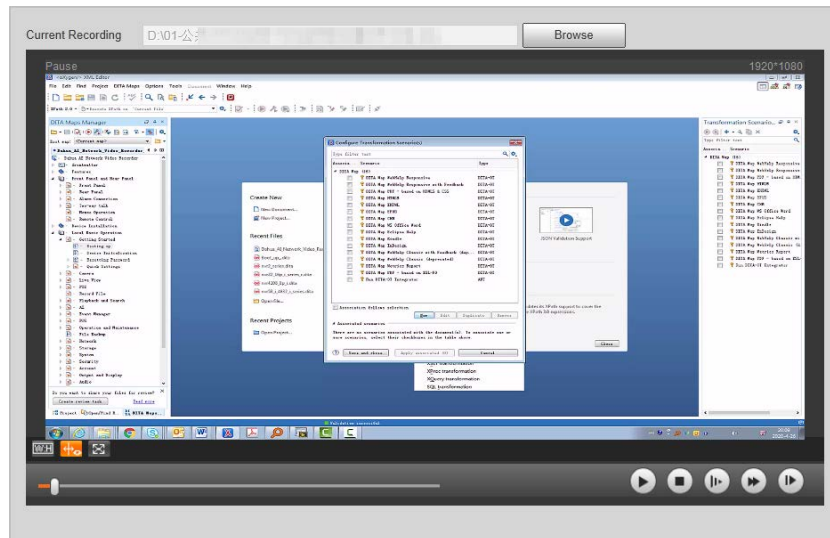


Table 5-7 Play function description

| Icon | Description |
|------|----------------------|
| | Stop playing. |
| | Slow down. |
| | Speed up. |
| | Play the next frame. |

5.3.2.2 Watermark

By verifying watermarks, you can check whether the local video recorded by the Camera is tampered.



Video watermark can be set on the web client from **Setting > Camera > Video > Video**.

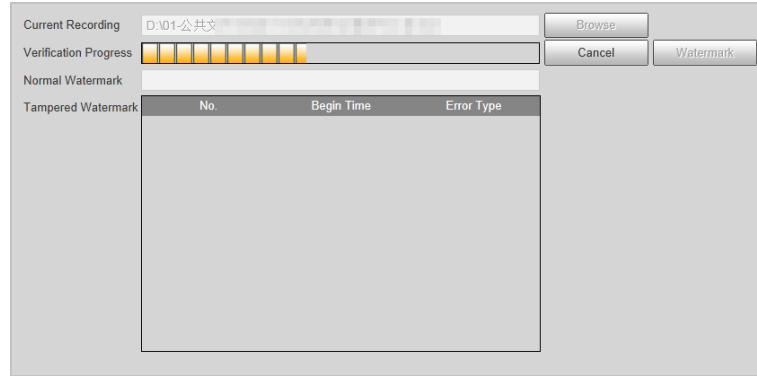
Step 1 Select **Query > Recording Search > Water Mark**.

Step 2 Click **Browse**, and select a recording that you want to verify.

Step 3 Click **Watermark**, and the Camera displays the verification progress.

- If the video is verified to be authentic, the watermark you set is displayed next to **Normal Watermark**.
- If the video is tampered, you can check the details next to **Tampered Watermark**.

Figure 5-10 Watermark



5.3.3 Parking Record Search

Search for the vehicle parking record within the defined period.

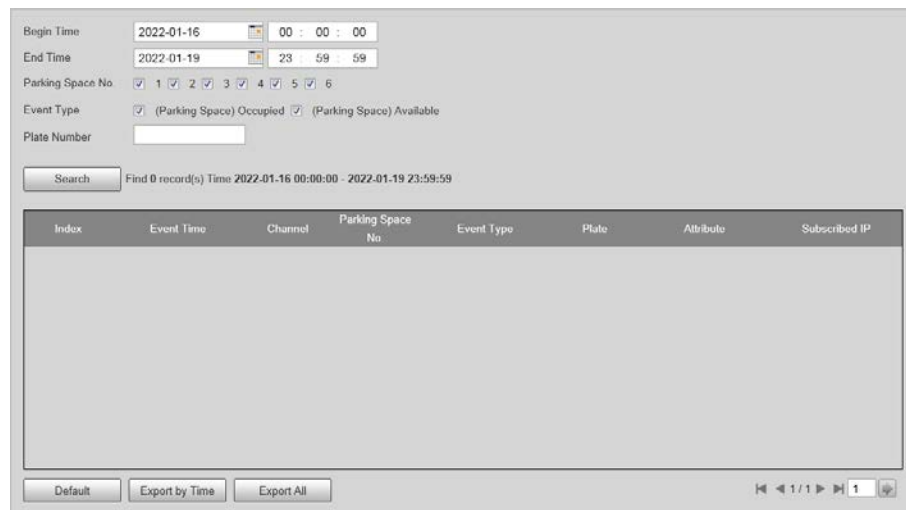
Step 1 Select **Query > Parking Record > Parking Record**.

Step 2 Set the search conditions, event type and plate number.

- **Parking Space No.:** Select parking spaces to view the corresponding records.
- **Event Type:** The status of the selected parking spaces during the set period.
- **Plate Number:** Enter plate number to search for records of the specified vehicle only.

Step 3 Click **Search**.

Figure 5-11 Parking record search



Step 4 (Optional) Click **Export by Time** or **Export All** to export parking records of the defined period or all records to local computer.

5.4 Setting

You can configure several parameters such as parking space detection mode, camera attributes,

network, event, storage, system, and system information.

5.4.1 ITC

You can set the parking space detection mode of the Camera.

5.4.1.1 Configuring Parking Spaces

Set a parking zone and parking spaces inside the zone, so the Camera can detect whether the specified parking space is occupied and recognize the vehicle.

Procedure

Step 1 Select **Setting > ITC > Park Space Config > Parking Space Management**.

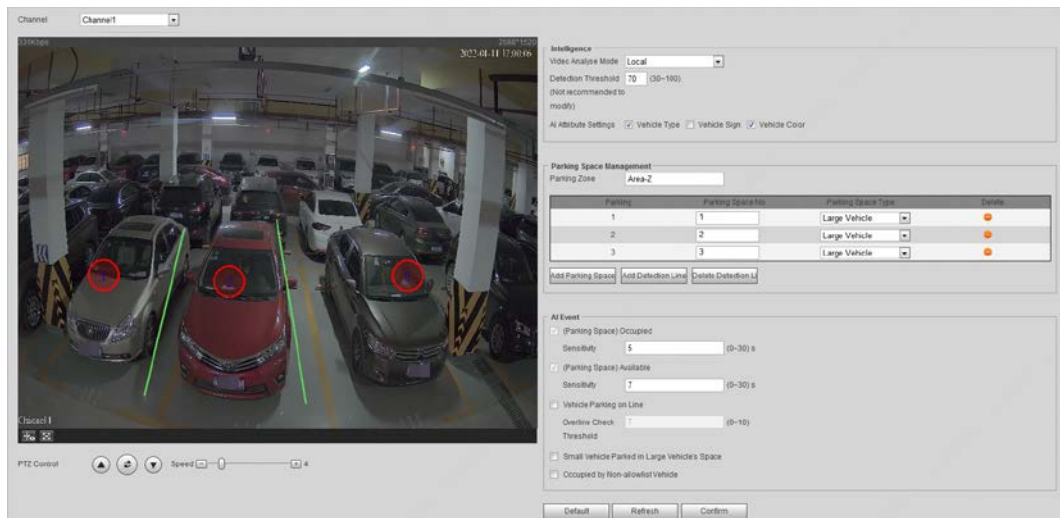
Step 2 Select **Channel** at the upper-left corner to configure parking spaces for the corresponding channel.



Only dual-sensor cameras support channel selection.

Step 3 At the lower-left corner of the page, set **Speed** and click or next to **PTZ Control** to adjust the Camera view. Make sure the target parking spaces are inside the Camera field of view and are easy to recognize.

Figure 5-12 Parking space management



Step 4 Set **Intelligence**.

1) Under **Intelligence**, select **Video Analyse Mode**.

- **Local**: Video recordings are analyzed by the Camera to get information such as parking space number, status, plate number and vehicle model, and display on the **Live** page.
- **Remote**: The Camera only sends snapshots and video recordings to terminals such as a platform for analysis.

2) Select **AI Attribute Settings**. The Camera obtains the corresponding attributes and reports them to backend terminals such as a platform for analysis.



The selected attributes can also be used as OSD information.

- Step 5** Under **Parking Space Management**, enter the **Parking Zone** name, and then click **Add Parking Space** to add parking spaces for the Camera to monitor.
- The type and number must be filled in for each parking area.
 - The number of parking spaces that can be detected varies depending on the model of the Camera.
- Step 6** Click **Add Detection Line**, draw lines between parking spaces. The Camera detects when vehicles are parking over the line and triggers alarms based on the drawn lines.
- Step 7** Under **AI Event**, select AI events and set the corresponding sensitivity as needed.
- **(Parking Space) Occupied/(Parking Space) Available**: Detects the parking space status. They are selected by default.
 - **Vehicle Parking on Line**: Detects whether the vehicle is parked on the drawn detection lines.
 - **Small Vehicle Parked in Large Vehicle's Space**: Select to enable the Camera to detect when a small vehicle is parked in a large vehicle space, and to report on these alarms to the third party platform.




To enable this function, make sure to select **Vehicle Type** when setting **AI Attribute Settings**.

- **Occupied by Non-allowlist Vehicle**: Detects and recognizes whether the specified parking space is occupied by a vehicle that is not on the allowlist.

- Step 8** Click **Confirm**.

Related Operations

- Click  to delete a parking space.
- Click **Delete Detection Li** to delete a drawn detection line.

5.4.1.2 Allowlist

You can view allowlist vehicles, add a plate number to the allowlist and set a specific parking space for the vehicle.

Procedure

- Step 1** Select **Setting > ITC > Allowlist**.



2 MP single-sensor models can manage up to 2 parking spaces; 4 MP single-sensor models can manage up to 3 parking spaces.

Figure 5-13 Allowlist

| Index | Parking | Plate | Note | Status | Begin Time | End Time | Edit | Delete |
|-------|---------|-------|------|--------|---------------------|---------------------|------|--------|
| 1 | 1 | | | Active | 2022-01-19 00:00:00 | 2023-01-19 23:59:59 | | |
| 2 | 2 | | | Active | 2022-01-19 00:00:00 | 2023-01-19 23:59:59 | | |
| 3 | 2 | | | Active | 2022-01-19 00:00:00 | 2023-01-19 23:59:59 | | |

Step 2 Select parking spaces to view the corresponding vehicles on the allowlist.

Step 3 Click **Add**, and enter a valid period, parking space and plate.

Select **Continue Adding**, and then click **Save**. The Camera saves the plate, and displays the adding window.

Figure 5-14 Add a plate

Begin Time: 2022-01-19 00 : 00 : 00
End Time: 2023-01-19 23 : 59 : 59
Parking: 1
Note:
Plate:
 Continue Adding
Buttons: Cancel, Save

Step 4 Click **Save**.

Step 5 Under **Fuzzy Matching**, select **On** and set the number to allow the Camera to misread the set number of characters on the plate.

Step 6 Click **Confirm**.

Related Operations

- Click to edit the corresponding allowlist record.
- Click to delete the corresponding allowlist record.

5.4.1.3 OSD Configuration

Set the OSD (On-screen Display) information to appear on videos and images.

5.4.1.3.1 Video OSD

Set OSD information of a video channel.

Step 1 Select **Setting > ITC > OSD > Video OSD**.

Step 2 Click **Channel Title**, and then select **On** to enable the corresponding OSD type.
The Camera supports adding information such as channel, time and customized content as OSD.



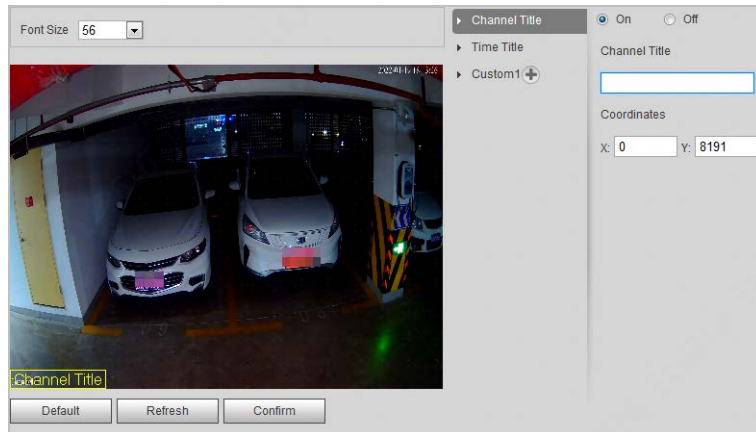
In this section, **Channel Title** is used as an example.

Step 3 Select a channel next to **Channel**.

Step 4 Set the channel title and its coordinates.

You can also drag the yellow frame to change the position of the channel title.

Figure 5-15 Video OSD



Step 5 (Optional) Click **+** next to **Custom1** to add more customized OSD information.



The system supports up to 4 customized OSD.

Step 6 Click **Confirm**.

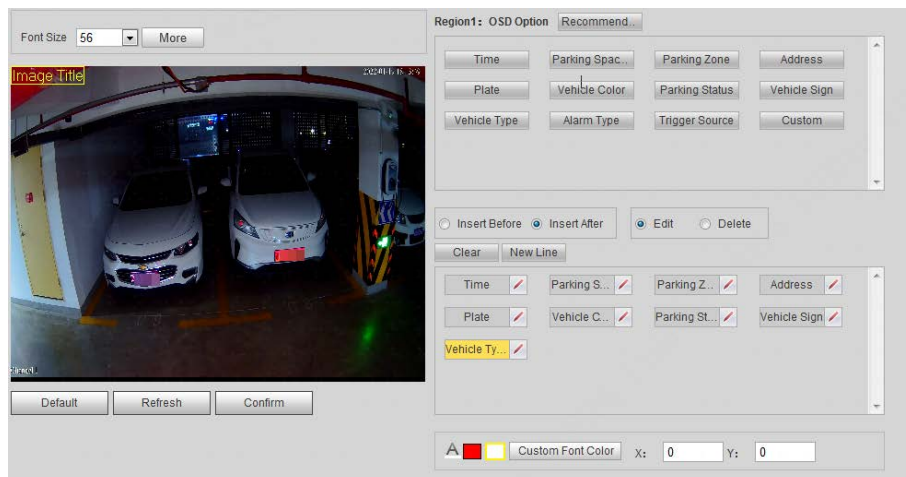
5.4.1.3.2 Snapshot OSD

You can set OSD information for pictures.

Step 1 Select **Setting > ITC > OSD > Snapshot OSD**.

Step 2 Move the title box to set its position on the snapshot, or manually enter coordinates into the X/Y box at the lower-right corner of the page.

Figure 5-16 Snapshot OSD



Step 3 Select **Black Edge Location**, and then you can set the position of the OSD black strip. You

can select from **Top**, **Bottom**, and **None**.

Step 4 Set the OSD font.

- Select a font size from the list, click **More**, and then you can set the content separator.



You can manually enter other separators when selecting **Custom** from **Osd Separator**.

Figure 5-17 New line and OSD separator



- Set the font color in . Click **Custom Font Color** to select from more colors.

Step 5 Set OSD options.

Table 5-8 Snapshot OSD description

| Parameter | Description |
|---------------|---|
| Recommended | Use the recommended configuration for snapshot OSD. |
| Insert Before | Select one OSD option, click Insert Before , and select other OSD options. The new OSD options will be displayed before the original OSD option. |
| Insert After | Select one OSD option, click Insert After , and select other OSD options. The new OSD option will be displayed after the original OSD option. |
| Edit | Click it, and all the OSD information status is displayed as except New Line . Click to modify the prefix, suffix, content, and separator of the corresponding OSD option. |
| Delete | Click it, and all the selected OSD information status is displayed as . Click to delete the corresponding OSD option. |
| Clear | Delete all the OSD information. |
| New Line | After selecting some OSD information, click New Line , and the OSD information inserted after NewLine will be displayed in a new line on the picture. |

Step 6 Click **Confirm**.

5.4.1.4 Light Control

Configure the corresponding indicator color for different statuses of parking spaces, and then the corresponding light will turn on when the parking space status changes.



- Single-sensor models support remote control of external lights connected to another camera.
- Dual-sensor models can only control the internal light and external lights that are connected to it.


Step 1 Select **Setting > ITC > Light Control**.


Step 2 Configure light control parameters.

- Dual-sensor models

Figure 5-18 Light control (1)

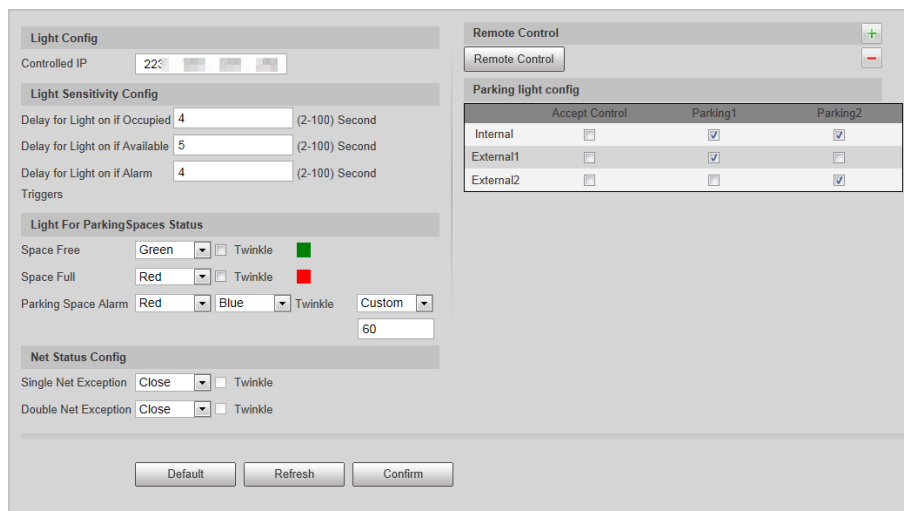
Table 5-9 Description of light control parameters

| Parameter | | Description |
|---------------------------------|--------------------------------------|--|
| Light Sensitivity Config | Delay for Light on if Occupied | Set the sensitivity that the indicator is to respond with when the status of a parking space changes between occupied, available and alarmed. The lower the value, the faster the indicator responds. |
| | Delay for Light on if Available | |
| | Delay for Light on if Alarm Triggers | |
| Light For Parking Spaces Status | Space Free | Set the indicator to indicate when a parking space is empty (Space Free), occupied (Space Full), and when an alarm is triggered (Parking Space Alarm). 1. Select a light color for each status. You can also select Close to disable the indicator light. 2. Select Twinkle for the indicator to flash. Otherwise it will remain solid on. 3. Select Light Off, Always Lighting, or Customized (twinkle duration) to set the indicator status when an alarm is triggered. |
| | Space Full | |
| | Parking Space Alarm | |
| Net Status Config | Single Net Exception | Set the indicator status when a network error is detected.  Only available for models powered by cascading network cables. Double Net Exception is for dual-sensor models. |
| | Double Net Exception | |

| Parameter | | Description |
|----------------------|----------|--|
| Parking Light Config | Internal | <p>Link the built-in indicator light of the Camera to parking spaces.</p> <p>For example, select Parking1, Parking2, and Parking3, and when the three parking spaces are occupied, the indicator shows the color defined for Space Full. When one of the three parking spaces becomes empty, the indicator shows the color defined for Space Free.</p> |
| | External | <p>Link the external indicator light of the Camera to a parking space.</p> <p>For example, link External1 to Parking1, and when parking space 1 becomes empty, the indicator shows the color defined for Space Free.</p> <p></p> <ul style="list-style-type: none"> To enable the external indicator light function, set the Protocol to DHRS from Setting > ITC > RS485. An external indicator light can be linked to multiple parking spaces. |

- Single-sensor models
 - ◇ **Controlled IP:** Enter the IP address of camera A in **Controlled IP**, and then all external lights connected to camera A can be remotely controlled by the current camera.
 - ◇ **Remote Control:** Control the indicator light of another camera.

Figure 5-19 Light control (2)



Step 3 (Optional) Configure remote control for indicator light.

- 1) Click **Remote Control**.
- 2) Select **Remote Control** in the pop-up window, and then enter the username, password and IP of another camera.
- 3) Click **Save**.



Click  to add more cameras, or click  to delete the corresponding camera.

- 4) Enter the camera IP in **Controlled IP**.

Step 4 Click **Confirm**.

5.4.1.5 RS-485

You can configure the RS-485 serial protocol of the external device. After configuration, you can set related parameters of the device on the web client.

Step 1 Select **Setting > ITC > RS-485 > Trigger Mode**.

Step 2 Configure parameters.

- DHRS

Figure 5-20 DHRS parameters

Table 5-11 DHRS parameters description

| Parameter | Description |
|-----------|---|
| Data Bit | 8 by default, and cannot be modified. |
| Stop Bit | 1 by default, and cannot be modified. |
| Baud Rate | The transmission speed of the code element. Options are 4800, 9600, 19200, 38400, and 115200. |
| Check | None by default, and cannot be modified. |

- Transparency Serial.

The third party platform can control the RS-485 output of the Camera through transparency serial, and then you can connect external devices.

Trigger capture by sending the capture command. To test the transparency serial sending and receiving conditions, select **Hexadecimal Sending**, and then click **Open** on the right side of **Receiving Area**.

Figure 5-21 Transparency serial

Step 3 Click **Confirm**.

5.4.1.6 Voice Broadcast

You can configure the voice broadcast content, volume, and encoding of the Camera.

5.4.1.6.1 Broadcast Content

Configure the broadcast content, and the Camera will broadcast the content when the corresponding event occurs.



Voice broadcast is available on select models.

Step 1 Select **Setting > ITC > Voice Broadcast > Broadcast Content**.

Step 2 Select a channel, and then select **On** to enable broadcast content configuration.

Step 3 Select broadcast event types and set the related parameters.



Make sure you have enabled the corresponding events in **Park Space Config**. For details, see "5.4.1.1 Configuring Parking Spaces".

- 1) Select **On** to enable broadcast for an event.
- 2) Select **Play Mode** from **Text** and **File**.
Select an audio file from local computer for **File**; set the audio content for **Text**.
- 3) Set the interval and duration of the audio to play.

Figure 5-22 Broadcast content

| Type | On | Play Mode | Audio Content | Interval(s) | Duration(s) |
|---|-------------------------------------|-----------|--------------------|-------------|-------------|
| Small Vehicle Parked in Large Vehicle's Space | <input checked="" type="checkbox"/> | Text | Small Occupy Large | 2 | 60 |
| Occupied by Non-allowed Vehicle | <input checked="" type="checkbox"/> | Text | Not Allow Occupy | 2 | 60 |
| Vehicle Parking on Line | <input checked="" type="checkbox"/> | Text | Over Line | 2 | 60 |
| Allowlist Vehicle | <input checked="" type="checkbox"/> | Text | Allow List In | | |
| (Parking Space) Available | <input checked="" type="checkbox"/> | Text | no car | | |
| (Parking Space) Occupied | <input checked="" type="checkbox"/> | Text | has car | | |

Notes on special characters: "[plate]" means insert the real plate number. "." means the audio will pause for 0.5 s.

Add Audio File

| Index | Name | Size (KB) | Play | Delete |
|-------|------|-----------|------|--------|
|-------|------|-----------|------|--------|

Requirement for uploading audio:
1. Size does not exceed 1024k.
2. Audio Channel: Mono; Bit Depth: 16 bit; Sample Rate: 8KHZ/16KHZ/32KHZ/48KHZ/64KHZ.
3. Audio format can only be WAV.

Refresh Confirm

Step 4 Click **Add Audio File** to add customized broadcast.

Step 5 Click **Confirm**.

5.4.1.6.2 Volume/Encoding

Configure the volume of voice broadcast.

Step 1 Select **Setting > ITC > Voice Broadcast > Volume/Encoding**.

Step 2 Set the output volume and speaking speed.

Step 3 Click **Confirm**.

5.4.1.7 Device Test

You can view and test parking event, voice broadcast, external light settings and status, and abnormal configuration. You can also export device information.

Step 1 Select **Setting > ITC > Device Test > Device Test**.

Figure 5-23 Device test

| Light Type | Color | Action | Source Ip |
|-----------------|-------|-----------------|------------|
| Internal | Green | Always Lighting | 172.16.1.1 |
| External Light1 | Green | Always Lighting | 172.16.1.2 |
| External Light2 | Green | Always Lighting | 172.16.1.3 |
| External Light3 | Green | Always Lighting | 172.16.1.4 |
| External Light4 | Green | Always Lighting | 172.16.1.5 |
| External Light5 | Green | Always Lighting | 172.16.1.6 |
| External Light6 | Green | Always Lighting | 172.16.1.7 |

Step 2 Under **Test Event**, enter a plate number and select events, and then click **(Parking Space) Occupied**. The Camera reports the corresponding event data to the third party platform. If no events are selected, only a record of parking space occupied by the set vehicle will be reported.



Click **(Parking Space) Available** to report on empty parking spaces to the platform.

Step 3 Set a text, and then click **Test** under **Voice Broadcast** to test the set text audio.

Step 4 Set the light color and status, and then click **Internal** or **External Light** under **Test Light** to

test the control of lights.

Light Status refreshes every time you test the light. **Source IP** is the IP address which sends out the test command.

Step 5 Click **Check** under **Abnormal Config** to check for abnormal configurations.

Step 6 Under **Export Device Info**, select different types of information to be exported to the local computer.

Logs can be encrypted.

5.4.2 Camera

You can configure image, video, and stream parameters.

5.4.2.1 Camera Attribute

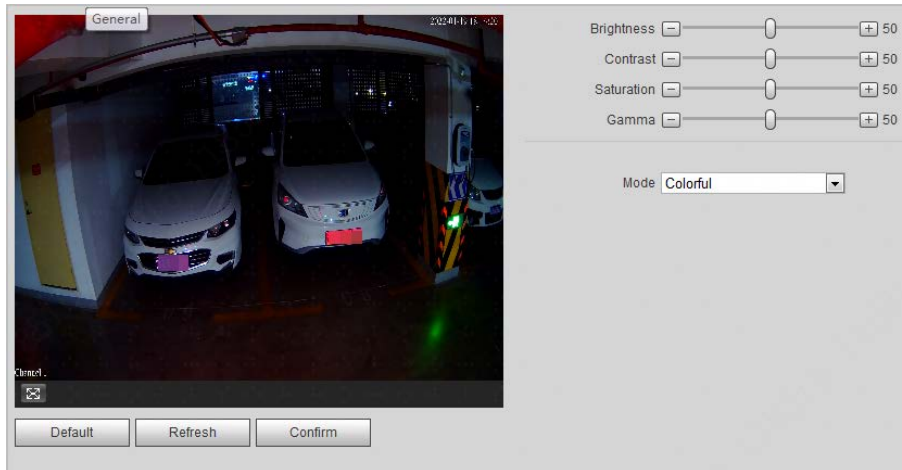
You can adjust the brightness, contrast, saturation of the video image, and set shutter parameters to get clear videos, and recordings that you want.

5.4.2.1.1 General

This section provides guidance on configuring parameters such as image brightness, contrast, saturation, and hue.

Step 1 Select **Setting** > **Camera** > **Camera Attribute** > **General**.

Figure 5-24 General settings



Step 2 Select a channel.

Step 3 Configure parameters.

Table 5-12 General parameters description

| Parameter | Description |
|------------|--|
| Brightness | <ul style="list-style-type: none">Adjust the overall image brightness. The bright and dark areas will have equal changes when adjusting the value.The image becomes blurry when the value is too big. The recommended value is from 40 to 60.The bigger the value, the brighter the image. |

| Parameter | Description |
|------------|---|
| Contrast | <p>Change the value when the image brightness is proper but contrast is not enough.</p> <ul style="list-style-type: none"> • If the value is too big, the dark area is likely to become darker, and the bright area is likely to be overexposed. • The picture might be blurry if the value is too low. The recommended value is from 40 to 60. • The higher the value, the more obvious the contrast between the bright area and dark area. |
| Saturation | <p>Adjust the color vividness, and it will not influence the image overall brightness.</p> <ul style="list-style-type: none"> • The image becomes too flamboyant if the value is too high. • The recommended value is from 40 to 60. • The higher the value, the more flamboyant the image. |
| Gamma | <p>Adjust the image brightness level. The higher the value, the brighter and more blurry the image.</p> |
| Mode | <p>Select image display mode. The image changes to colorful when the ambient brightness is higher than the preset value, and changes to black and white when lower if you select Auto Switch by Brightness.</p> |

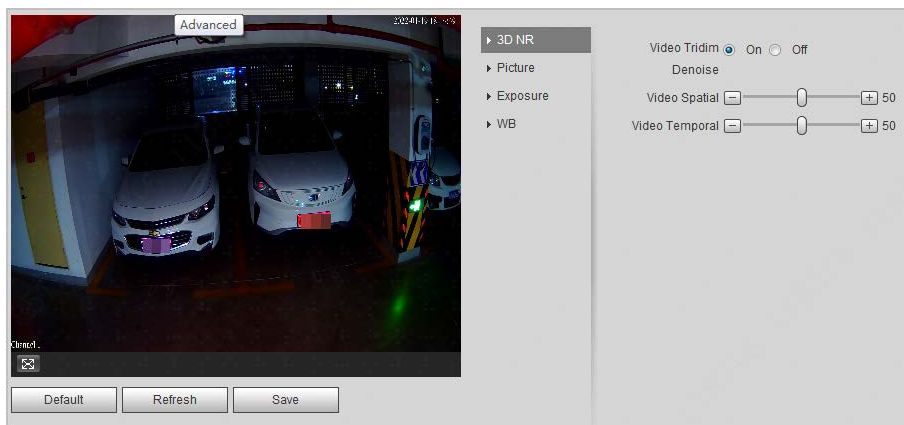
Step 4 Click **Confirm**.

5.4.2.1.2 Advanced Attributes

This section provides guidance on configuring advanced attributes, including exposure mode, shutter mode, white balance and scene mode.

Step 1 Select **Setting > Camera > Camera Attribute > Advanced**.

Figure 5-25 Advanced attributes






Step 2 Select a channel.

Step 3 Configure parameters.

Table 5-12 Advanced parameters description

| Parameter | Description | |
|-----------|----------------------|---|
| 3D NR | Video Tridim Denoise | When it is On , 3D NR is enabled to reduce noise of video. |
| | Video Spatial | Spatial video denoising. The higher the value, the fewer the noise. |

| Parameter | | Description |
|-----------|----------------|---|
| | Video Temporal | Temporal video denoising. The higher the value, the fewer the flicker noise. |
| Picture | Scene | You can change the scene, and adjust the sharpness of corresponding scene. Scenes available: Dawn/Dusk, Daytime, and Night. |
| | Sharpness | You can set the sharpness of corresponding scene. The higher the value, the clearer the image. But there will be noise if sharpness is too high. |
| | BLC Mode | Select from WDR, BLC, HLC and SSA to adjust the picture effect. |
| Exposure | Mode | Select the way of adjusting exposure mode. |
| | Shutter | Set the shutter.  Available when setting Mode to Manual or Shutter Priority . |
| | Shutter Scope | Set the time range of shutter.  Available when Mode is set to Manual or Shutter Priority and Customized Range is set as Shutter . |
| | Gain Scope | Set the value range of gain.  Available when set Mode to Manual or Gain Priority . |
| WB | Mode | Set scene mode to adjust the image to its better status. |

Step 4 Click **Save**.

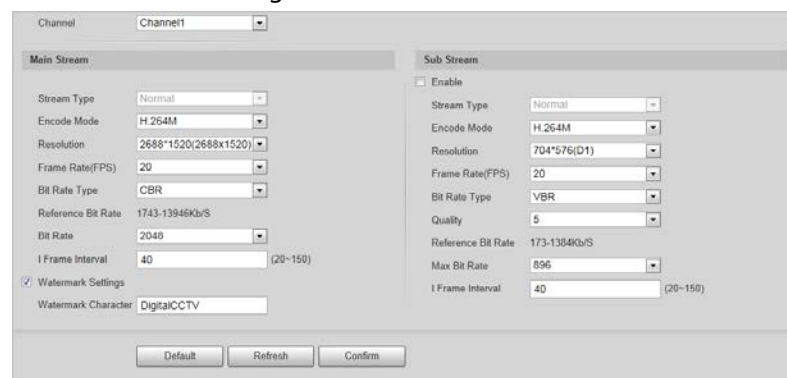
5.4.2.2 Video

5.4.2.2.1 Video

You can set the camera stream information.

Step 1 Select **Setting > Camera > Video > Video**.

Figure 5-26 Video



The screenshot shows a configuration window for video streams. At the top, there is a 'Channel' dropdown menu set to 'Channel1'. Below this, the interface is divided into two main sections: 'Main Stream' and 'Sub Stream'.

Main Stream Settings:

- Stream Type: Normal
- Encode Mode: H.264M
- Resolution: 2688*1520(2688x1520)
- Frame Rate(FPS): 20
- Bit Rate Type: CBR
- Reference Bit Rate: 1743-1394Kb/S
- Bit Rate: 2048
- I Frame Interval: 40 (range 20-150)
- Watermark Settings
- Watermark Character: DigitalCCTV

Sub Stream Settings:



- Enable
- Stream Type: Normal
- Encode Mode: H.264M
- Resolution: 704*576(D1)
- Frame Rate(FPS): 20
- Bit Rate Type: VBR
- Quality: 5
- Reference Bit Rate: 173-1384Kb/S
- Max Bit Rate: 896
- I Frame Interval: 40 (range 20-150)

At the bottom of the window, there are three buttons: 'Default', 'Refresh', and 'Confirm'.

Step 2 Select a channel.

Step 3 Configure parameters.

Table 5-14 Video parameters description

| Parameter | | Description |
|-------------|--------------------|---|
| Main Stream | Stream Type | Currently it supports normal stream. |
| | Encode Mode | Currently it supports H.264B, H.264M, H.264H, H.265, and MJPEG. |
| | Resolution | Select the resolution of the video.  The resolution of sub stream cannot be greater than main stream. |
| | Frame Rate(FPS) | Select frame rate as needed. |
| | Bit Rate Type | Includes VBR, and CBR.  Image quality can only be set in VBR mode. |
| | Reference Bit Rate | The recommended bit rate range. |
| | Bit Rate | The value is the upper limit of the stream in VBR mode while it is fixed in CBR mode. |
| | I Frame Interval | Frame or time interval between two I frames. The bigger the interval, the smaller space taken by the decompressed video. It is twice of the frame rate by default. |
| | Watermark Settings | You can view if the video is tampered through verifying watermark character. <ul style="list-style-type: none">• Select Watermark Settings, and enable the function.• Watermark Character is DigitalCCTV by default.• The watermark character can only consist of number, letter, underline, and maximum length contains 85 characters. |
| Sub Stream | Enable | Select it, and enable sub stream. |
| | Quality | Image quality can be set in VBR mode. There are 6 levels optional. The higher the level, the higher quality the video has. |
| | Max Bit Rate | The value is the upper limit of the stream in VBR mode while it is fixed in CBR mode. |

Step 4 Click **Confirm**.

5.4.2.2.2 Snapshot


You can set the picture stream, including resolution, quality or picture size.

Step 1 Select **Setting > Camera > Video > Snapshot**.

Figure 5-27 Snapshot

Step 2 Configure parameters.

Table 5-15 Snapshot parameters description

| Parameter | Description |
|--------------------------|--|
| Snapshot Type | Currently it only supports general snapshot. |
| Image Size | It is in accordance with resolution value. |
| Quality | Set the snapshot quality which includes 6 levels optional. The higher the level, the higher quality the image has. |
| Picture Coding Size (KB) | Select picture coding size from 8 options, or select Custom to define the size (50–1024).  You can only select one between picture quality and picture coding size to set the configuration. |

Step 3 Click **Confirm**.

5.4.2.2.3 Region of Interest

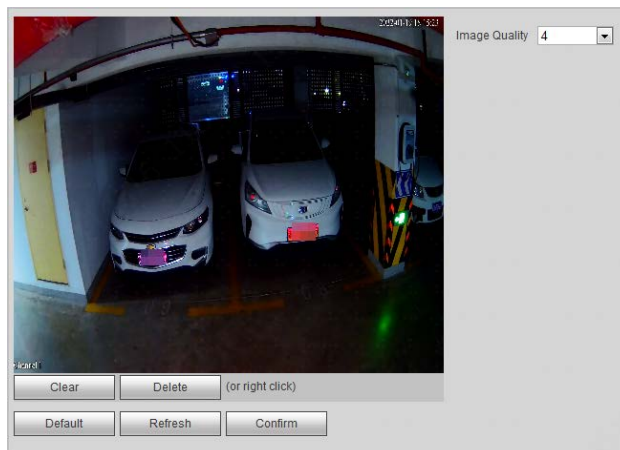
Set the region of interest in the image, and then the selected image will display with configured quality.



It supports max 3 regions at the same time.

Step 1 Select **Setting > Camera > Video > Interest Area**.

Figure 5-28 Interest area



- Step 2 Select a channel.
- Step 3 Configure parameters.

Table 5-16 Interest area parameter description

| Parameter | Description |
|---------------|--|
| Image Quality | Set snapshot quality, which includes 6 levels. |
| Clear | Delete all the configured regions. |
| Delete | Click it or right-click any position in the image to delete the latest region of interest. |

- Step 4 Click **Confirm**.

5.4.3 Network

You can set IP address, port, and other parameters.

5.4.3.1 TCP/IP

Configure the IP address of the Camera, and DNS server so that the Camera can connect with other devices in the network.



Some models support dual network ports. Do not set them on the same network segment; otherwise it might cause network error.

- Step 1 Select **Setting > Network > TCP/IP**.

Figure 5-29 TCP/IP

- Step 2 Configure parameters.

Table 5-17 TCP/IP parameter description

| Parameter | Description |
|---------------|--|
| Host Name | Enter a name (maximum 15 characters) for the host device. |
| Ethernet Card | Select the Ethernet card. The default setting is Wire . |

| Parameter | Description |
|-----------------|---|
| Mode | Network mode, including static, and DHCP. <ul style="list-style-type: none"> • Static: Manually set IP, subnet mask, and gateway. • DHCP: Automatically acquire IP. At this moment, IP, subnet mask, and gateway cannot be set. |
| MAC Address | MAC address of the host. |
| IP Version | Includes IPv4 , and IPv6 . The IP address of both versions can be accessed. |
| IP Address | Device IP Address. |
| Subnet Mask | The corresponding subnet mask of device IP address. |
| Default Gateway | Corresponding gateway of device IP address. |
| Preferred DNS | IP address of DNS server. |
| Alternate DNS | Alternative IP address of DNS server. |

Step 3 Click **Confirm**.

5.4.3.2 Port

You can set the maximum number, and value of the ports.

Step 1 Select **Setting > Network > Port**.

Figure 5-30 Port

The screenshot shows a configuration window with the following fields and values:

- Max Connection: 10 (range 1~20)
- TCP Port: 37777 (range 1025~65535)
- UDP Port: 37778 (range 1025~65534)
- HTTP Port: 80
- RTSP Port: 554
- HTTPS Port: 443

At the bottom, there are three buttons: Default, Refresh, and Confirm.

Step 2 Configure each port value of the Camera.

Table 5-18 Connection parameters description

| Parameter | Description |
|----------------|--|
| Max Connection | The maximum number of clients (such as web client, and platform client) that are allowed to access the Camera simultaneously. It is 10 by default. |
| TCP Port | Protocol communication port. It is 37777 by default. |
| UDP Port | User data packet protocol port. It is 37778 by default. |
| HTTP Port | HTTP communication port. It is 80 by default. |
| RTSP Port | Media streaming control port. It is 554 by default. |
| HTTPS Port | HTTPS communication port. It is 443 by default. |

Step 3 Click **Confirm**.

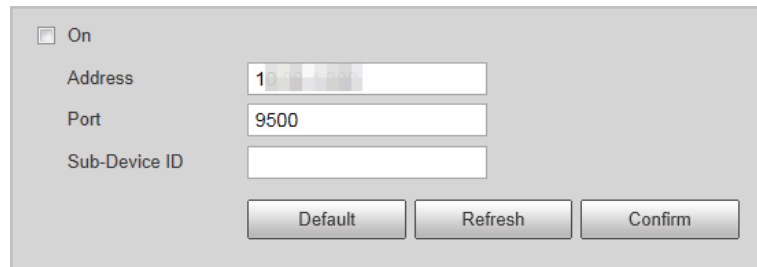
5.4.3.3 Auto Register

Through the auto registration function, when the Camera is connected with external network, its current location will be sent to the server so that the Camera can be accessed through the server.

Step 1 Select **Setting > Network > Auto Register > Auto Register**.

Step 2 Select **On** to enable the function.

Figure 5-31 Auto register



Step 3 Configure parameters.

Table 5-19 Auto register parameter description

| Parameter | Description |
|---------------|--|
| Address | The IP address of the server on which the device register. |
| Port | The port of the server for auto registration. |
| Sub-Device ID | The device ID distributed by the server for auto registration. Make sure that the ID is unique during auto registration. |

5.4.3.4 Platform

5.4.3.4.1 ONVIF

You can enable the Open Network Video Interface Forum (ONVIF) function to make network video products of different manufacturers interworking.

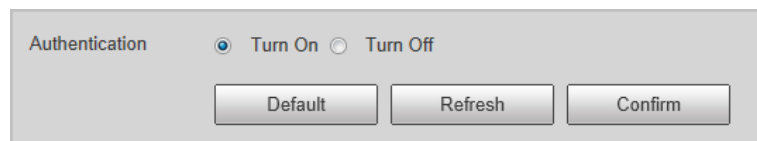


ONVIF login authentication is enabled by default.

Step 1 Select **Setting > Network > Platform > ONVIF**.

Step 2 Select **Turn on**.

Figure 5-32 ONVIF



Step 3 Click **Confirm**.

5.4.3.4.2 Info Push Platform

You can configure this parameter to push the captured vehicle violations information to the server.

Step 1 Select **Setting > Network > Platform > Info Push Platform**.

Figure 5-33 Information push configuration

Step 2 Configure parameters.

Table 5-20 ITC push parameter description

| Parameter | Description |
|------------------------|---|
| Basic configuration | |
| Client | The client from which the pushed information comes. |
| Keep Alive Circle | Time interval (0–65535) of checking whether the Camera is connected with the set client. |
| Max Keep-alive Request | Set the number of requests the Camera sends to the set client in total. When the number exceeds the defined value, the Camera stops checking. |
| Upload Type | Select the information type that you want to upload. |
| Data Acquisition | |
| Data Type | Select the types of data to be acquired from the Camera. |
| Uploading Info | Select the types of information to be uploaded. |
| Picture Config | |
| Filter Condition | Select No Plate , the Camera filters out the records without plates. |

Step 3 Click **Confirm**.

5.4.4 Event

Enable different events. When an abnormality happens, the Camera triggers an alarm.

Step 1 Select **Setting > Event > Abnormality**.

Step 2 Select events from network error, illegal access, and security exception.

Figure 5-34 Event

- Step 3 (Optional) Select event type. You only need to select this for network error.
- Step 4 Select **On** to enable detection of various abnormalities.
- Step 5 Configure parameters of each event.
- Step 6 Click **Confirm**.

5.4.5 Storage

This section provides guidance on configuring picture, record naming, and storage path.

- Step 1 Select **Setting > Storage > Destination > Save Path**.
- Step 2 Set the naming rule of pictures. Click **Help...** for more details.
- Step 3 Set the storage path for recordings and snapshots.
- Step 4 Click **Confirm**.

5.4.6 System

You can configure general information, add user, restore default settings, and configure import & export file.

5.4.6.1 General

5.4.6.1.1 General Setup

This section provides guidance on configuring device SN, language, and video standard.

- Step 1 Select **Setting > System > General Setting > General Setup**.
- Step 2 Set the information of the Camera, including camera name, code, language displayed on the web client, video standard and company details.

Figure 5-35 General

| | |
|--|--|
| Device Name | <input type="text" value="7M..."/> |
| Device Code | <input type="text"/> |
| Language | <input type="text" value="English"/> ▼ |
| Video Standard | <input type="text" value="PAL"/> ▼ |
| Machine Group | <input type="text"/> |
| Machine Address | <input type="text"/> |
| <input type="button" value="Default"/> <input type="button" value="Refresh"/> <input type="button" value="Confirm"/> | |

- Step 3 Click **Confirm**.

5.4.6.1.2 Date & Time

You can set date, and time format, system time, DST (Daylight Saving Time) or NTP server, and more.

- Step 1 Select **Setting > System > General > Date&Time**.
- Step 2 Set the format of time and date, time zone and DST information.

Figure 5-36 Date & time

The screenshot shows a configuration window for date and time. It has several sections: Date Format (YYYY-MM-DD), Time Format (24-Hour), Time Zone ((UTC+08:00) Beijing, Chongqing, Hong Kong), System Time (2022-01-18 16:48:02), DST (DST Type: Week, Begin Time: Jan 1st Mon 00:00:00, End Time: Jan 1st Tue 00:00:00), and NTP Setting (NTP Server: clock.isc.org, Port: 123, Interval: 10 minute(s)). There are buttons for Default, Refresh, and Confirm at the bottom.

Step 3 Click **Sync PC** to synchronize the Camera time with the server.

NTP Setting is necessary for the time synchronization.

Step 4 Click **Confirm**.

5.4.6.2 Account

5.4.6.2.1 Account

You can create accounts that can operate on the Camera through the web client.



- We recommend giving fewer permissions to normal users than premium users.
- You cannot delete an account when it is in login status.

Procedure

Step 1 Select **Setting > System > Account > Account**.

Step 2 Select the **Group Name** tab, and then click **Add Group**.

Step 3 Enter the name of user group, and configure group permissions.

- **Group Name** can only consist of number, letter, underline, and hyphen, and cannot exceed 15 characters.
- **Group Name** cannot be repeated.

Figure 5-37 Add group

The screenshot shows a dialog box titled "Add Group". It has three main sections: Group Name (with a red "Must" label), Memo, and Authority. The Authority section has a list of checkboxes: All, Live, System, System Info, and File Backup. There are "Cancel" and "Save" buttons at the bottom.

Step 4 Click **Save**.



Up to 8 user groups can be created, and the default user groups are **admin** and **user**.

Step 5 Select the **Username** tab, and then click **Add User**.

Step 6 Set username and password, select a user group for the account.

Step 7 Under **Operation Permission**, select the permissions that you want to assign to the account.

Step 8 Click **Restricted Login**, set login restrictions for the account.

- 1) Set the IP address to which the account has no access.
- 2) Set the period during which the account cannot access the set IP.
- 3) Set specific time periods of the restriction.

Figure 5-38 Add user

The screenshot shows the 'Add User' dialog box with the 'Restricted Login' tab selected. The 'IP Address' section has 'IPv4' selected and the IP address '1.0.0.1'. The 'Validity Period' section has 'Begin Time' set to '2022-01-18 08:00:00' and 'End Time' set to '2022-01-19 08:00:00'. The 'Period' section shows a grid for days of the week (Sun to Sat) and hours (0 to 24). The 'Setting' buttons for each day are highlighted in green. At the bottom are 'Cancel' and 'Save' buttons.

4) Click **Save**.

Related Operations

- Click to change user/group information
- Click to delete the added user/group.



Admin user/group cannot be deleted.

5.4.6.2.2 ONVIF User

You can add, delete, and modify ONVIF users.

Step 1 Select **Setting** > **System** > **Account** > **Onvif User**.

Step 2 Click **Add User**.

Figure 5-39 Add ONVIF user

Step 3 Set the name and password of the account, and then select a user group.

Step 4 Click **Save**.

5.4.6.3 Safety

5.4.6.3.1 System Service

Select to enable system services as needed.

Step 1 Select **Setting > System > Safety > System Service**.

Figure 5-40 System Service

Step 2 Select needed system services.

Table 5-21 System service parameters description

| Parameter | Description |
|----------------------------|--|
| SSH | SSH (Secure Shell) implements data encrypted transmission, and effectively avoid information leakage during remote management. |
| Multicast/Broadcast Search | <ul style="list-style-type: none"> • Multicast: It realizes point-to-multipoint network connection between sender and receiver. • Broadcast Search: Broadcast data packet in IP subnet, all the hosts in the subnet will receive these data packets. |
| Password Reset | When you forget the password of admin user, you can set new password through the password reset function. |

| Parameter | Description |
|---|--|
| CGI Service | CGI is the port between external application program and web server. |
| Onvif Service | Realizes network video framework agreement to make different network video products interconnected. |
| Audio and Video Transmission Encryption | Enable this function to encrypt streams transmitted through private protocols. |
| RTSP over TLS | Enable this function to encrypt stream transmitted through standard protocol. We recommend keeping the function on. |
| Private Protocol Authentication Mode | Keep the recommended Security Mode . |

Step 3 Click **Confirm**.

5.4.6.3.2 HTTPS

Prerequisites

- For first-time use of HTTPS or after changing device IP address, you need to create server certificate and install root certificate.
 - After creating server certificate, and installing root certificate, if you replace the computer for logging in to the web page, you need to download and install the root certificate again on the new computer or copy the downloaded root certificate on the new computer, and then install it.
- On the **HTTPS** page, you can make PC log in normally through HTTPS by creating certificate or uploading authenticated certificate. It can ensure security of communication data, and provide guarantee for user information and device safety through reliable, and stable technical approach.

Procedure

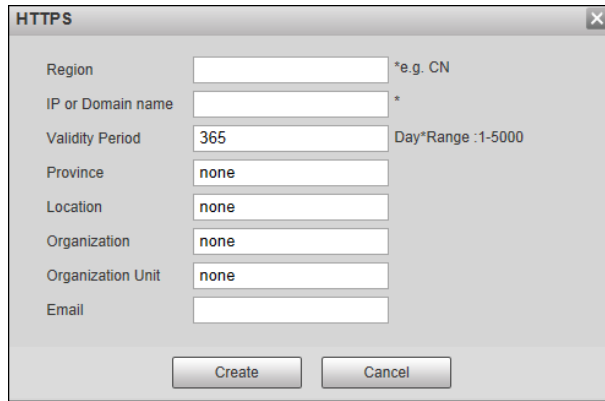
Step 1 Create certificate or upload the authenticated certificate.

- If you select **Create Certificate**, follow the steps below.
 1. Select **Setting > System > Safety > HTTPS**.

Figure 5-41 HTTPS

2. Click **Create**.

Figure 5-42 HTTPS



3. Enter the required information such as region, IP or domain name, and then click **Create**.



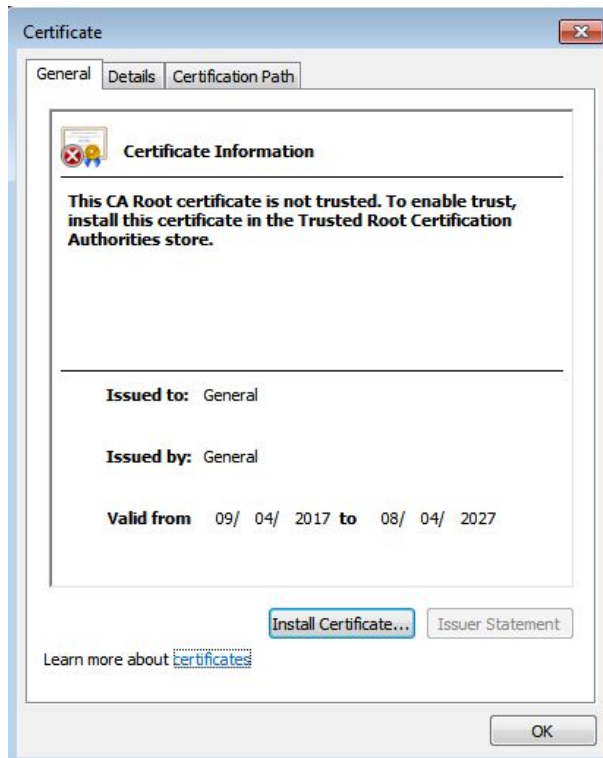
The entered **IP or Domain name** must be the same as the IP or domain name of the **Camera**.

4. Click **Install** under **Request Created**, and then click **Download** to download root certificate.

The system pops up the **Save As** dialog box, select storage path, and then click **Save**.

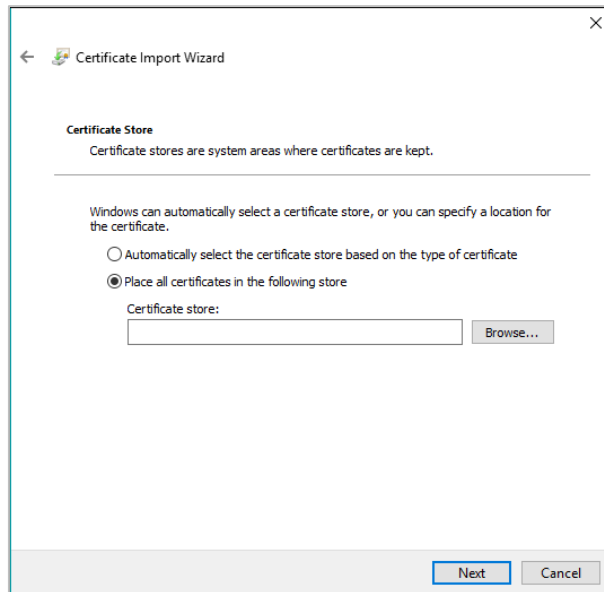
5. Double-click the RootCert.cer icon.
6. Click **Install Certificate...**

Figure 5-43 Install certificate



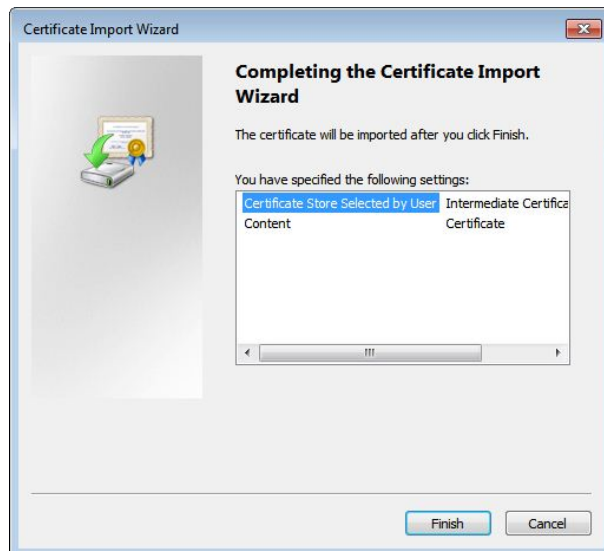
7. Click **Next**.
Select as needed.

Figure 5-44 Certificate store



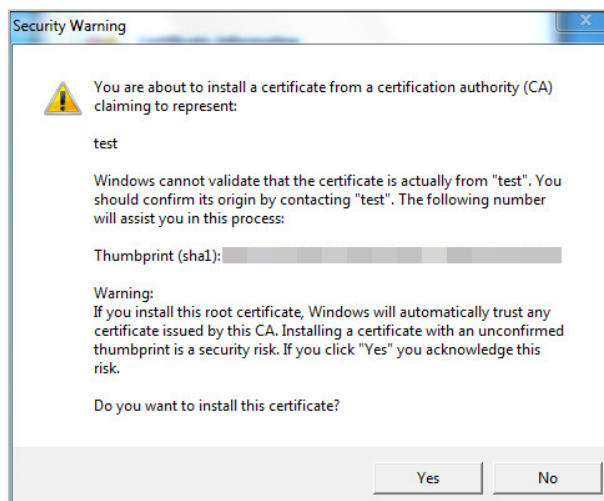
8. Click **Next**.

Figure 5-45 Completing certificate import wizard



9. Click **Finish**.

Figure 5-46 Security warning



10. Click **Yes**, and then click **OK** on the pop-up window.
- If you select **install signed certificate**, follow the steps below.
 1. Select **Setting Safety > System > Safety > HTTPS**.
 2. Select **Enable HTTPS**, and **Compatible with TLSv1.1, and earlier versions**.
 3. Click **Browse** to upload the signed certificate and certificate key, and then click **Upload**.
 4. To install the root certificate, see operation steps from 4 to 10 in **Create Certificate**.

Step 2 Select **Enable HTTPS**, and click **Confirm**.

The configuration takes effect until the Camera restarts.

Step 3 Use HTTPS to log in to the Camera.

1. Enter `https://xx.xx.xx.xx` in the browser.



`xx.xx.xx.xx` is the device IP address or domain name.

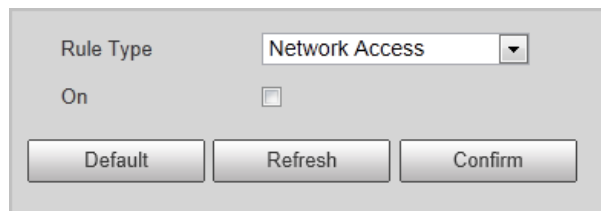
2. Enter the username and the password to log in to the Camera.

5.4.6.3.3 Firewall

Set the security rules to protect the safety of your camera system.

Step 1 Select **Setting > System > Safety > Firewall**.

Figure 5-47 Firewall



Step 2 Select **Rule Type**.



- **Network Access:** Add the IP address to allowlist or blocklist to allow or restrict it to access corresponding ports of the device.
- **PING Prohibited:** IP address of your camera is prohibited from ping. This helps prevent attempt of accessing your network system without permission.
- **Prevent Semijoin:** Prevents half-open SYN attacks.

Step 3 Select **On** to enable the selected rule type.

Step 4 Click **Confirm**.

5.4.6.4 Default Settings

You can restore the device to default settings or factory defaults.

Select **Setting > System > Default**, and then select **Default** or **Factory Default** as needed.

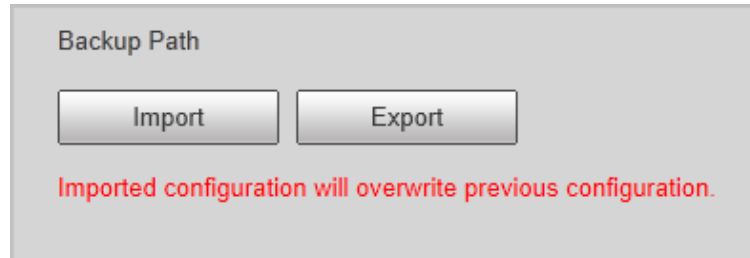
- **Default:** Restore your settings to default value. In this case, network IP address information of the Camera will not restore to default settings.
- **Factory Default:** Restore the system to factory default settings. In this case, the Camera will restart, and you need to initialize the Camera before any further operation.

5.4.6.5 Import/Export

Export the system configuration file to back up the system configuration; import system configuration file to make quick configuration or recover system configuration.

Step 1 Select **Setting > System > Import/Export**.

Figure 5-48 Import/Export



Step 2 Click **Import** or **Export**.

- **Import:** Import the local system configuration file to the system.
- **Export:** Export associated configuration to local, and save as file whose suffix is .backup.

Step 3 Select the imported file path or exported folder.

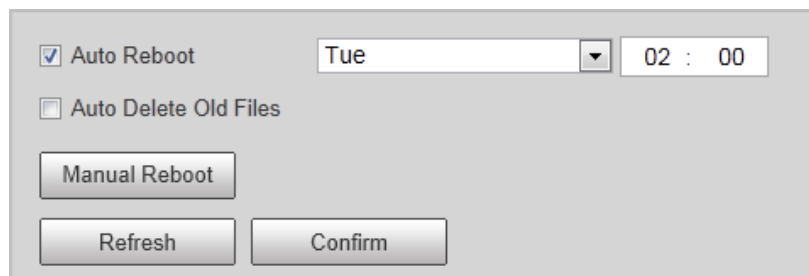
Step 4 Click **Open** or **Save**, and view import and export results on the web page.

5.4.6.6 Automatic Maintenance

You can set the time of auto restart, and automatically delete old files.

Step 1 Select **Setting > System > Auto Maintain**.

Figure 5-49 Auto maintain



Step 2 Select **Auto Reboot**, and then set the restart time.

Step 3 (Optional) Click **Manual Reboot** can restart the Camera immediately.

Step 4 Click **Confirm**.

Step 5 Select **Emergency Maintenance**, and then select **On** to enable the function.

Step 6 Click **Save**.

5.4.6.7 Update

Step 1 Select **Setting > System Upgrade > System Upgrade**.



The pages might vary depending on the device model.

Figure 5-50 Upgrade

File Upgrade

Select Firmware File

Online Upgrade

Auto-check for updates

System Version 2.62 Build Date: 2021-12-28

It is the latest version

Step 2 Click **Import** to select the update file, and then click **Upgrade** to update the system.



Do not disconnect the power or network, or restart or shut down the Camera during update. Incorrect update programs might result in malfunctions of the Camera.

5.4.7 Information

The system supports viewing version, user, and log, and more.

5.4.7.1 Version

Select **Setting** > **System Info** > **Version** to view the version information of the Camera.



- Versions might vary depending on the actual device.
- Algorithm recognition is available when algorithm is authorized (when the icon is displayed in green). If algorithm is not authorized, the Camera will not be able to recognize vehicle series, model, and logo. License plate recognition is always supported.

Figure 5-51 Version

| | |
|-------------------|--|
| Device Type | ITC... |
| Hardware Version | 1.00 |
| Algorithm Version | libits... Algorithm is authorized |
| System Version | 2.62 |
| Software Version | 2.62 |
| Soft Build Time | 2021-... |
| WEB Version | 3.1.6 |
| S/N | 7M0... |
| Security Baseline | V2.2 |
| Version | |

Copyright 2021, all rights reserved.

5.4.7.2 Log

5.4.7.2.1 System Log

You can view log information such as system, configuration, data, event, record, user management, and also clear log records.



The earliest log records will be overwritten when the number of log records reaches 1024.

Step 1 Select **Setting > System Info > Log > Log**.

Step 2 Set search conditions, and then click **Search**.

Figure 5-52 Log

| No. | Log Time | Username | Log Type |
|-----|---------------------|----------|--------------------|
| 1 | 2022-01-18 19:01:31 | admin | Set Time |
| 2 | 2022-01-18 18:35:04 | admin | Login |
| 3 | 2022-01-18 18:35:01 | admin | Login |
| 4 | 2022-01-18 18:34:48 | admin | Logout |
| 5 | 2022-01-18 18:18:06 | admin | Logout |
| 6 | 2022-01-18 18:01:31 | admin | Set Time |
| 7 | 2022-01-18 17:46:47 | admin | Logout |
| 8 | 2022-01-18 17:46:40 | admin | Login |
| 9 | 2022-01-18 17:46:35 | admin | Save Configuration |
| 10 | 2022-01-18 17:46:21 | admin | Logout |

Detailed Information

Time: 2022-01-18 18:35:01
Username: admin
Type: Login
Content: Address: 10.34.98.82
Type: Web3.0

Backup: Encrypt Log Backup Password:

Step 3 Select one log, and then you can view the details in the lower section.

Step 4 (Optional) Select **Encrypt Log Backup**, set the password and then click **Backup** to export all encrypted logs to local computer.

5.4.7.2.2 Remote log

You can save your important logs to log server. This helps provide important clues to the source of security incidents. Log server needs to be deployed in advance by a professional or system administrator.

Step 1 Select **Setting > System Info > Log > Remote Log**.

Step 2 Select **On** to enable remote log.

Step 3 Enter the IP address, port, and device number of the Camera for the server to read log data.

Step 4 Click **Confirm**.

5.4.7.3 Online User

Step 1 Select **Setting > System Info > Online User** to view the information of all the online users.

Step 2 Click **Refresh** to view the latest status.

5.4.7.4 Legal Information

Select **Setting > System Info > Legal Info** to view the **Open Source Software Notice**.

5.5 Alarm

Step 1 Click the **Alarm** tab

Step 2 Select alarm type, operation, and alarm tone.

After selecting alarm type, the Camera displays alarms that conform to the selected types on the right side.

Figure 5-53 Alarm



5.6 Logout

Click **Logout** to exit the web client.

Appendix 1 Cybersecurity Recommendations

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 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 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.