



# Access ANPR Camera

## User's Manual



# Foreword

## General






The manual introduces the structure, installation, functions and operations of the access ANPR camera (hereinafter referred to as "the Camera").

## Models

Model	Description	Focal Length	Pixel
DHI-ITC237-PW6M-LZF1050	Long Range Access ANPR Camera	10 mm–50 mm	2 MP
DHI-ITC237-PW6M-IRLZF1050			
DHI-ITC237-PW6M-IRLZF1050-B			
DHI-ITC237-PW6M-LZF1050-B			
DHI-ITC215-PW6M-IRLZF	Short Range Access ANPR Camera	3.2 mm–10.5 mm	2 MP
DHI-ITC215-PW6M-LZF			
DHI-ITC215-PW6M-IRLZF-B			
DHI-ITC215-PW6M-LZF-B			
DHI-ITC215-PW6M-IRLZF-O			
DHI-ITC215-PW6M-LZF-O			

## Safety Instructions

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

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

## Revision History

Version	Revision Content	Release Time
V1.0.1	Add more models and the SMTP function.	May 2020
V1.0.0	First release.	November 2019

## About the Manual

- The manual is for reference only. If there is inconsistency between the Manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

# Important Safeguards and Warnings

This section describes the contents covering proper handling of the Camera, hazard prevention, and prevention of property damage. Read these contents carefully before using the Camera, comply with them when using, and keep it well for future reference.

## Power Requirements

- All installation and operation should conform to your local electrical safety codes.
- The power source shall conform to the Safety Extra Low Voltage (SELV) standard. Please note that the power supply requirement is subject to the device label.
- Make sure that the power supply is correct before operating the Camera.
- A readily accessible disconnect device shall be incorporated in the building installation wiring.
- Prevent the power cable from being trampled or pressed, especially the plug, power socket and the junction extruded from the Camera.

## Environment

- Do not aim the Camera at strong light to focus, such as lamp light and sun light. Otherwise, it might cause over brightness or light marks, which are not the device malfunction, and affect the longevity of Complementary Metal-Oxide Semiconductor (CMOS).
- Do not place the Camera in a damp or dusty environment, extremely hot or cold temperatures, or the locations with strong electromagnetic radiation or unstable lighting.
- Keep the Camera away from any liquid to avoid damage to the internal components.
- Keep the indoor device away from rain or damp to avoid fire or lightning.
- Keep sound ventilation to avoid heat accumulation.
- Transport, use and store the Camera within the range of allowed humidity and temperature.
- Heavy stress, violent vibration, and water splash are not allowed during transportation, storage and installation.
- Pack the Camera with standard factory packaging or the equivalent material when transporting the Camera.
- Install the Camera in the location where only the professional staff with relevant knowledge of safety guards and warnings can access. The accidental injury might happen to the non-professionals who enter the installation area when the Camera is operating normally.

## Operation and Daily Maintenance

- Do not touch the heat dissipation component of the Camera to avoid scald.
- Carefully follow the instructions in the Guide when performing any disassembly operation about the Camera; otherwise, it might cause water leakage or poor image quality due to unprofessional disassemble. Please contact after-sale service for desiccant replacement if

there is condensed fog found on the lens after unpacking or when the desiccant turns green. (Not all models are included with the desiccant).

- It is recommended to use the Camera together with lightning arrester to improve lightning protection effect.
- It is recommended to ground the Camera to enhance reliability.
- Do not touch the image sensor directly (CMOS). Dust and dirt can be removed with air blower, or you can wipe the lens gently with soft cloth that moistened with alcohol.
- Device body can be cleaned with soft dry cloth, which can also be used to remove stubborn stains when moistened with mild detergent. To avoid possible damage on device body coating which could cause performance decrease, do not use volatile solvent such as alcohol, benzene, diluent and so on to clean the Camera body, nor can strong, abrasive detergent be used.
- Dome cover is an optical component, do not touch or wipe the cover with your hands directly during installation or operation. For removing dust, grease or fingerprints, wipe gently with moisten oil-free cotton with diethyl or moisten soft cloth. You can also air blower to remove dust.



- Please strengthen the protection of network, device data and personal information by adopting measures including but not limited to using strong password, modifying password regularly, upgrading firmware to the latest version, and isolating computer network. For some devices with old firmware versions, the ONVIF password will not be changed automatically along with the modification of the system password, and you need to upgrade the firmware or manually update the ONVIF password.
- Use standard components or accessories provided by manufacturer, and make sure that the Camera is installed and maintained by professional engineers.
- Do not expose the surface of the image sensor to laser beam radiation in an environment where a laser beam device is used.
- Do not provide two or more power supply sources for the Camera unless otherwise specified. Fail to follow this instruction might cause damage to the Camera.

# Table of Contents

<b>Foreword</b> .....	<b>I</b>
<b>Important Safeguards and Warnings</b> .....	<b>III</b>
<b>1 Introduction</b> .....	<b>1</b>
1.1 Overview .....	1
1.2 Features .....	1
<b>2 Structure</b> .....	<b>3</b>
2.1 Long Range ANPR Camera Dimensions .....	3
2.2 Short Range ANPR Camera Dimensions .....	3
2.3 Structure .....	4
2.3.1 Entire Device .....	4
2.3.2 Rear Panel .....	1
2.4 Cable Connection .....	1
<b>3 Installation</b> .....	<b>5</b>
3.1 Universal Joint Installation .....	5
3.2 Bracket Installation .....	6
3.3 Spherical Bracket Installation .....	6
<b>4 Web Configuration</b> .....	<b>9</b>
4.1 Web Login .....	9
4.1.1 Recommended Configuration .....	9
4.1.2 Device Initialization .....	9
4.1.3 Login .....	12
4.1.4 Resetting Password .....	13
4.1.5 Web Functions .....	15
4.2 Guide .....	16
4.3 Live .....	19
4.3.1 Video Stream .....	19
4.3.2 Live View .....	19
4.3.3 Logged Plate Number .....	21
4.3.4 Plate Snapshot .....	21
4.3.5 System Functions .....	21
4.3.6 Functions of the Live Interface .....	21
4.3.7 Vehicle Snapshot .....	24
4.3.8 Event List .....	24
4.4 Query .....	25
4.4.1 Picture Query .....	25
4.4.2 Record Query .....	27
4.4.3 Plate Query .....	29
4.5 Setup .....	30
4.5.1 ITC .....	30
4.5.2 Camera .....	46
4.5.3 Network .....	53
4.5.4 Event .....	58

---

4.5.5 Storage.....	63
4.5.6 System.....	67
4.5.7 Information.....	85
4.6 Alarm.....	87
4.7 Logout.....	88
<b>5 FAQ.....</b>	<b>90</b>
<b>Appendix 1 Cybersecurity Recommendations.....</b>	<b>91</b>

# 1 Introduction

## 1.1 Overview

The access ANPR camera adopts intelligent deep learning algorithm. It supports vehicle detection, license plate recognition, logo recognition, model recognition, and color recognition, and encoding mode such as H.265.

The Camera consists of protective housing, illuminator, and intelligent HD camera. The intelligent HD camera adopts progressive scanning CMOS, which owns several features such as high definition, low illuminance, high frame rate, and excellent color rendition.

The Camera is extensively applied to vehicle capture and recognition of community road, parking lot, and other entrance and exit surveillance.

## 1.2 Features



The features are available on select modes, and the actual camera shall prevail.

### Permission Management

- Each user group owns permissions. Permissions of a user cannot exceed the permissions of its group.
- 2 user levels.
- Permission of opening barrier and blacklist alarm function.
- Device configuration and permission management through Ethernet.

### Storage

- Stores corresponding video data onto the central server according to the configuration (such as alarm and timing settings).
- Users can record through web according to their requirements. The recorded video file will be stored on the computer where client is located.
- Supports local hot swapping of storage card and storage when network disconnected. It overwrites stored pictures and videos automatically when memory becomes insufficient.
- Stores 1024 log records and user permission control.
- Supports FTP storage and automatic network replenishment (ANR).

### Alarm

- It can trigger alarm upon camera operation exceptions through network, such as memory card damage.
- Some devices can connect to various alarm peripherals to respond to external alarm input in real time (within 200ms). It can correctly deal with various alarms according to the



linkage predefined by users and generate corresponding voice prompt (users are allowed to record voice in advance).

## Network Monitoring

- Transmits video data of single channel compressed by device to network terminal and make it reappear after decompression through network. Keep delay within 500ms when bandwidth is allowed.
- Supports maximum 10 users online at the same time.
- Supports system access and device management through web.
- Video data transmission adopts HTTP, TCP, UDP, MULTICAST, and RTP/RTCP.

## Capture and Recognition

- Recognition of number plate and other vehicle information, including vehicle color, logo, model, and other vehicle features.
- Supports setting OSD information, and configuring location of channel and picture.
- Supports picture capture and encoding. Supports picture watermark encryption to prevent pictures from being tampered.
- The captured pictures can automatically record vehicle time, location, license plate, vehicle color, and more.

## Peripheral Control

- Peripheral control: Supports setting various peripheral control protocols and connection interfaces.
- Connects to external devices such as vehicle detector, signal detector, and more.

## Auto Adjustment

- Auto iris: Automatically adjusts the iris opening to the changing light throughout the day.
- Auto white balance: Accurately displays the object color when light condition changes.
- Auto exposure: Automatically adjusts shutter speed according to the exposure value of the image measured by the metering system, and according to shutter and iris exposure set by factory defaults.
- Auto gain: Automatically increases camera sensitivity when illuminance is very low, enhancing image signal output so that the Camera can acquire clear and bright image.

## 2 Structure

### 2.1 Long Range ANPR Camera Dimensions

Figure 2-1 Camera dimensions (mm [inch])

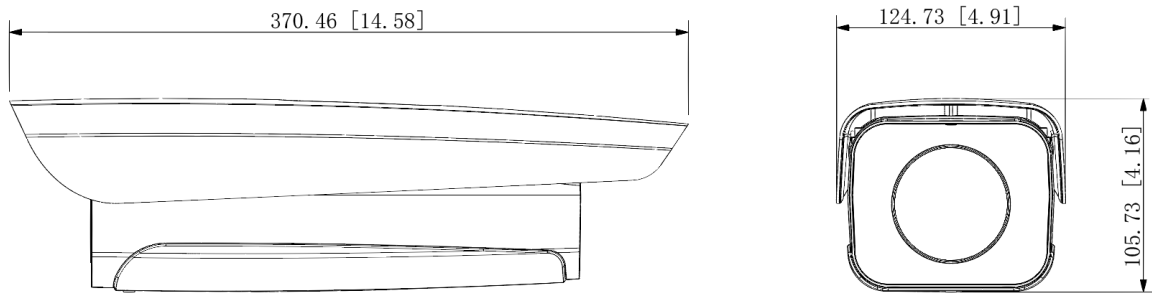
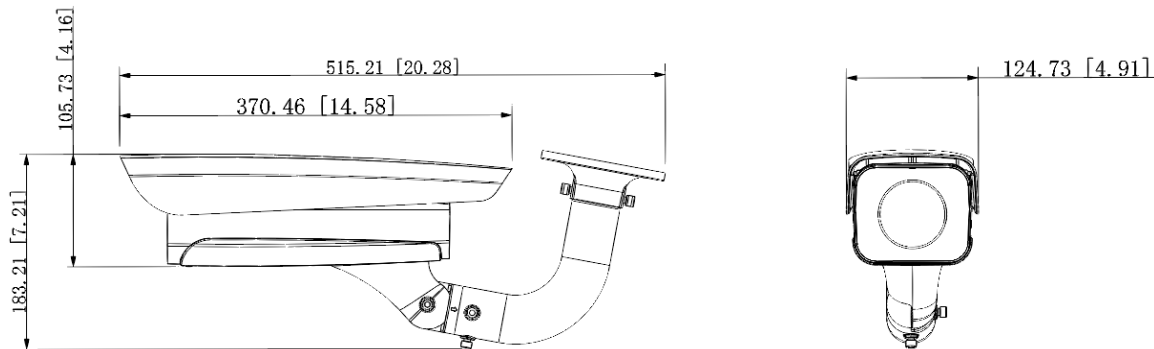


Figure 2-2 Dimensions of camera with bracket (mm[inch])



### 2.2 Short Range ANPR Camera Dimensions

Figure 2-1 General camera dimensions (mm [inch])

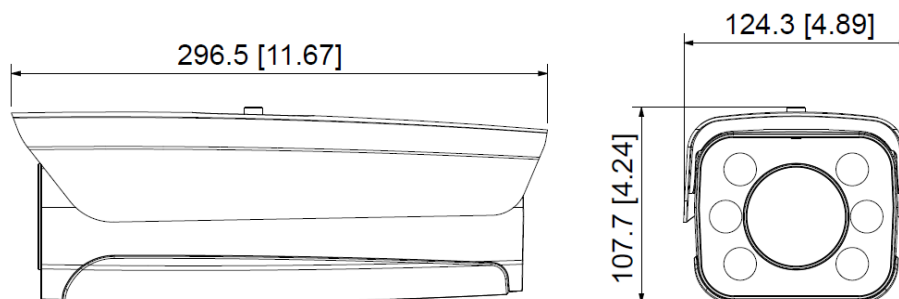


Figure 2-2 Dimensions of camera with bracket (mm [inch])

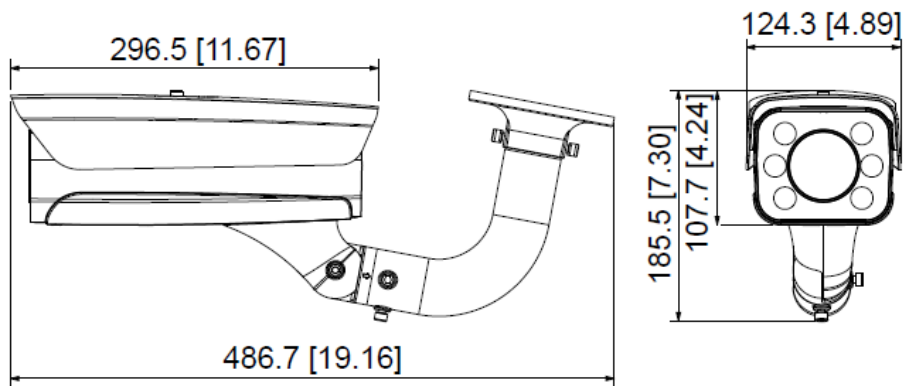
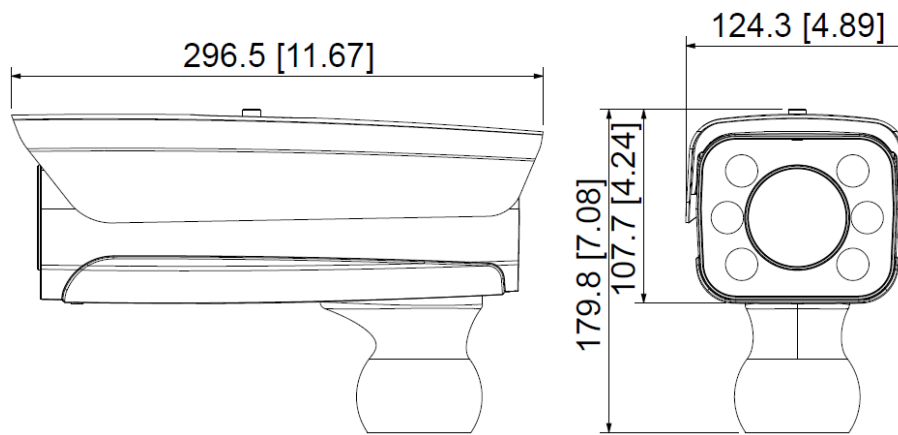


Figure 2-3 Dimensions of camera with spherical bracket (mm [inch])



## 2.3 Structure

### 2.3.1 Entire Device

Figure 2-4 Entire device structure

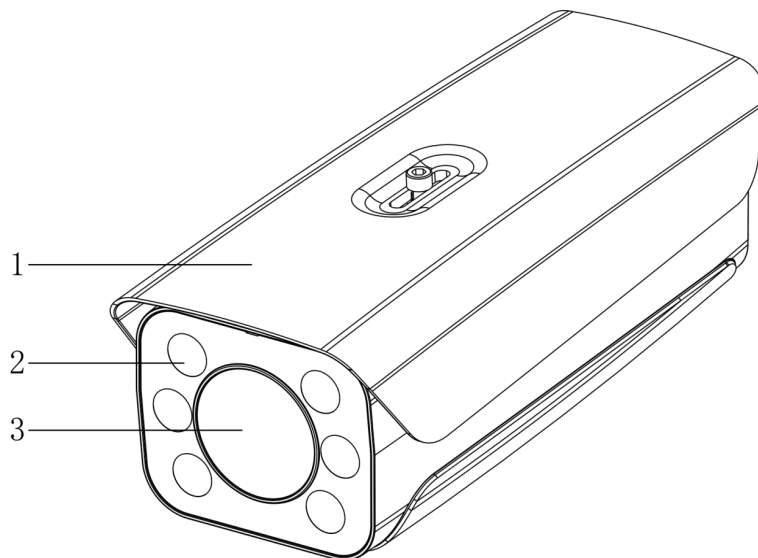


Table 2-1 Camera structure description

No.	Description	No.	Description
1	Protective cover	3	Lens
2	Illuminator	—	—

## 2.3.2 Rear Panel

Figure 2-5 Rear panel structure

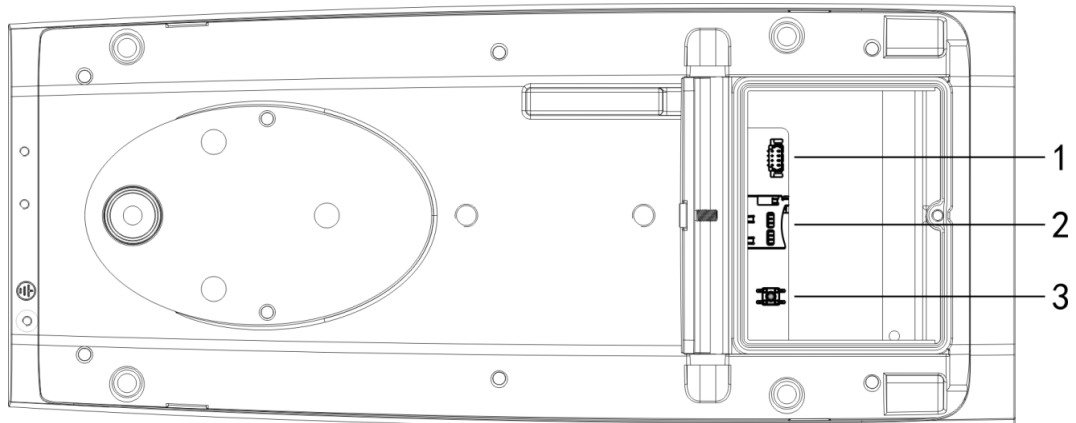


Table 2-2 Description of rear panel structure

No.	Description	No.	Description
1	Debugging port	3	Hardware reset
2	TF card	—	—

## 2.4 Cable Connection

Two cable connection methods are available, and the actual product shall prevail.

Figure 2-6 Cable connection (1)

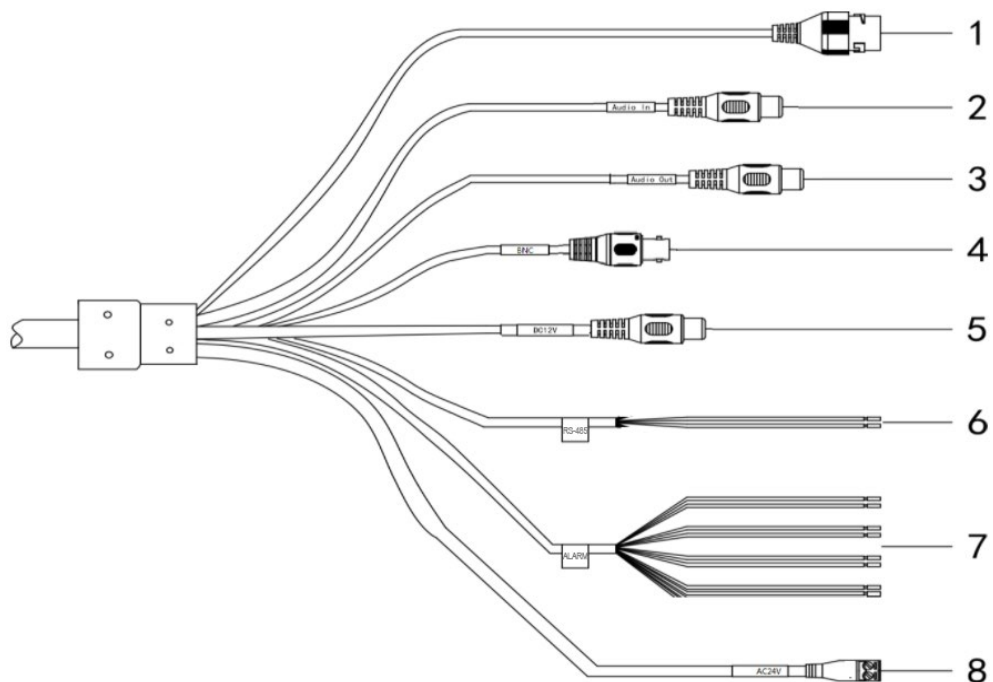


Table 2-3 Cable connection description



No.	Port	Function	Description
1	LAN	Ethernet port	Connects to standard Ethernet, supports PoE power supply.
2	AUDIO OUT	Audio output port	The Camera sends out audio signal through this port.
3	AUDIO IN	Audio input port	The Camera gets audio signal through this port.
4	BNC	Video output port	The Camera sends out video signal through this port.
5	DC 12V	Power input port	Inputs 12V DC power. Please be sure to supply power as instructed.  Device damage will occur if power is not supplied correctly.
6	RS-485	RS-485 port	Yellow: RS-485_A1 Orange: RS-485_B1
7	ALARM	Alarm port	Alarm output, connecting to barrier, and alarm output devices such as alarm light. <ul style="list-style-type: none"> <li>◇ Brown: ALARM_OUT1</li> <li>◇ Green: ALARM_OUT_GND1</li> <li>◇ Red: ALARM_OUT2</li> <li>◇ Black: ALARM_OUT_GND2</li> </ul> Alarm input, connecting to vehicle detector, IR detector, induction coil, and more. <ul style="list-style-type: none"> <li>◇ Blue: ALARM_IN1</li> <li>◇ White: ALARM_IN2</li> <li>◇ Yellow: ALARM_IN3</li> <li>◇ Gray: ALARM_IN_GND</li> </ul>
8	AC 24V	Power input port	Inputs 24V AC power. Please be sure to supply power as instructed.  Device damage will occur if power is not supplied correctly.

Figure 2-7 Cable connection

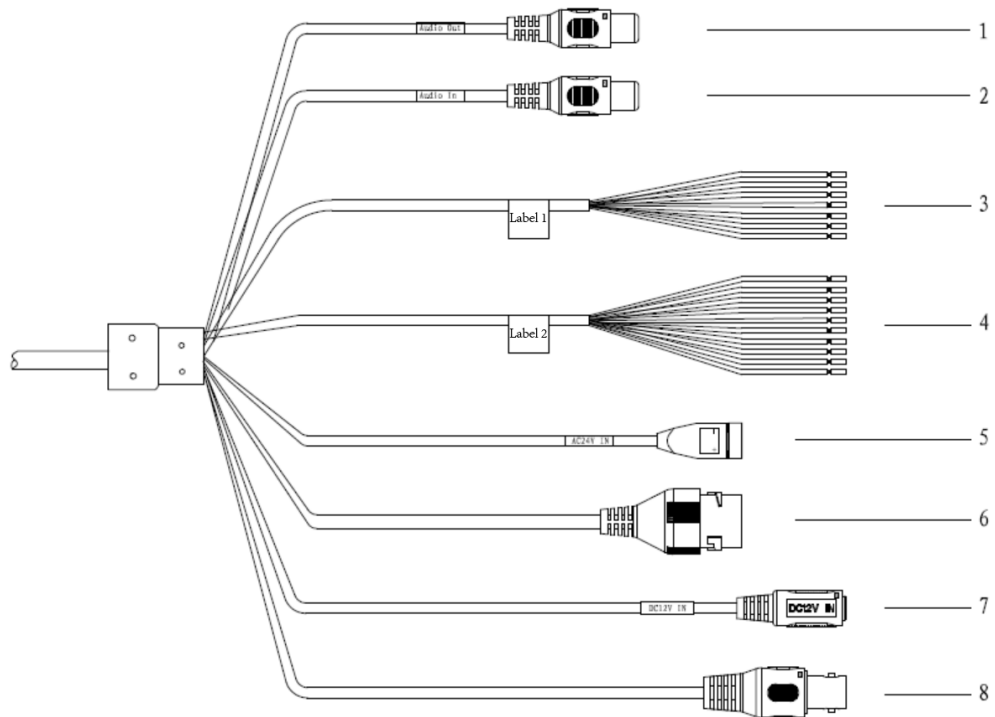




Table 2-4 Cable connection

No.	Port	Function	Description
1	AUDIO OUT	Audio output port	The Camera sends out audio signal through this port.
2	AUDIO IN	Audio input port	The Camera gets audio signal through this port.
3	RS-485/RS-232	RS-485/RS-232 port	White & Red: RS-485_A1 White & Orange: RS-485_B1 Yellow & Green: RS-485_A2 Yellow & Black: RS-485_B2 White & Yellow: RS-232_RXD White & Brown: RS-232_TXD White & Black: GND
4	ALARM	Alarm port	Alarm output, connecting to barrier, and alarm output devices such as alarm light. <ul style="list-style-type: none"> <li>◇ Brown: ALARM_NO1</li> <li>◇ Green: ALARM_COM1</li> <li>◇ White &amp; Purple: ALARM_NO2</li> <li>◇ Light Green: ALARM_COM2</li> <li>◇ Red: ALARM_NO3</li> <li>◇ Black: ALARM_COM3</li> </ul> Alarm input, connecting to vehicle detector, IR detector, induction coil, and more. <ul style="list-style-type: none"> <li>◇ Blue: ALARM_IN1</li> <li>◇ White: ALARM_IN2</li> <li>◇ Yellow: ALARM_IN3</li> <li>◇ Gray: ALARM_IN_GND</li> </ul>

No.	Port	Function	Description
5	24V AC	Power input port	Inputs 24V AC power. Be sure to supply power as instructed.  Device damage will occur if power is not supplied correctly.
6	LAN	Ethernet port	Connects to standard Ethernet. Supports PoE power supply.
7	12V DC	Power inputport	Inputs 12V DC power. Be sure to supply power as instructed.  Device damage will occur if power is not supplied correctly.
8	BNC	Video output port	The Camera sends out video signal through this port.

## 3 Installation



The following installation figures are for reference only, and the actual product shall prevail.

### 3.1 Universal Joint Installation

**Step 1** Use M6×14 screw to fix the universal joint on the bracket.

**Step 2** Use two 1/4-20×14UNC screws to fix the Camera on the universal joint. See Figure 3-1.

Figure 3-1 Universal joint installation

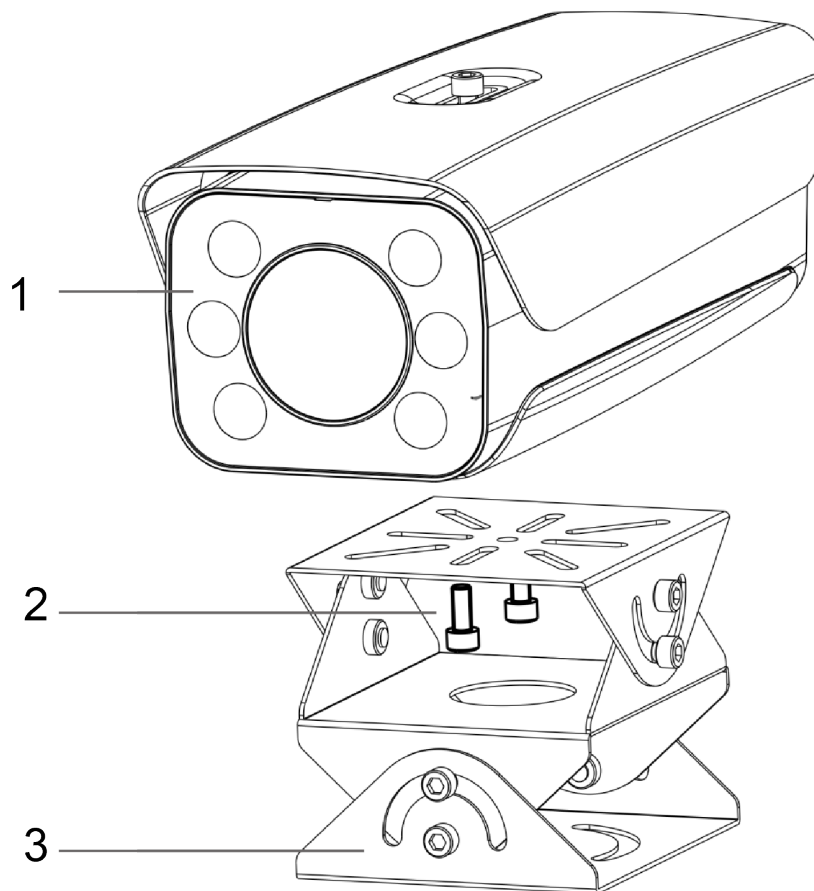


Table 3-1 Components description

No.	Description	No.	Description
1	Camera	3	Universal joint
2	1/4-20×14UNC screw	—	—

**Step 3** Adjust the universal joint and the Camera to proper position.  
Installation is completed.



## 3.2 Bracket Installation

Figure 3-2 Bracket installation

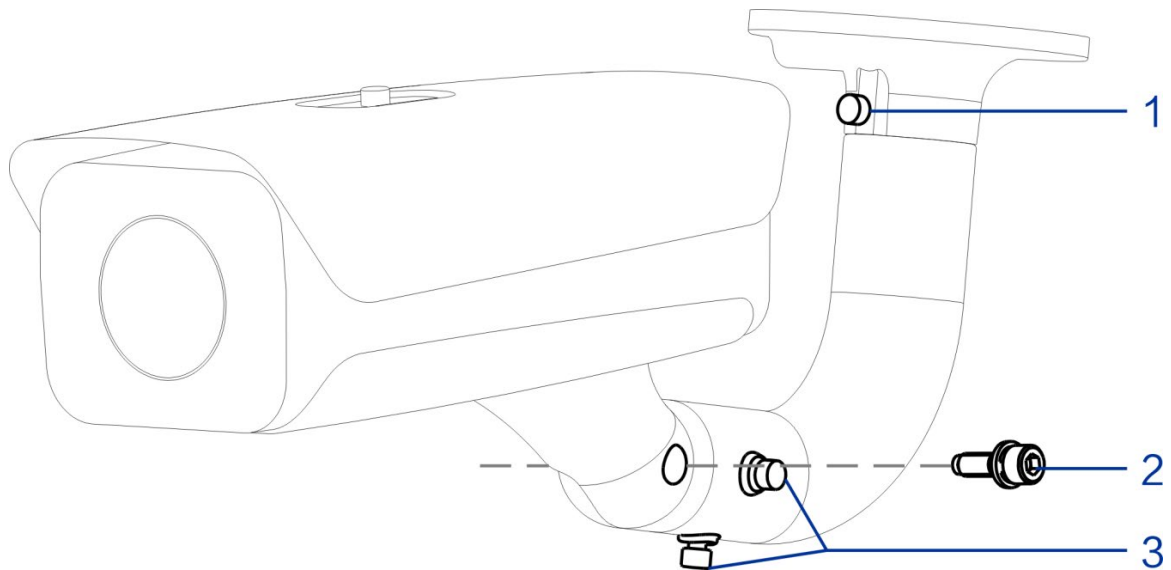


Table 3-2 Bracket installation

No.	Description
1	Adjust the Camera leftward and rightward.
2	Adjust the Camera upward and downward.
3	Adjust the Camera horizontally.

**Step 1** Loosen the No. 1 and No. 3 screws shown in Figure 3-2.

**Step 2** Insert all the camera cables into the bracket, and then pull them out from the bracket tail.

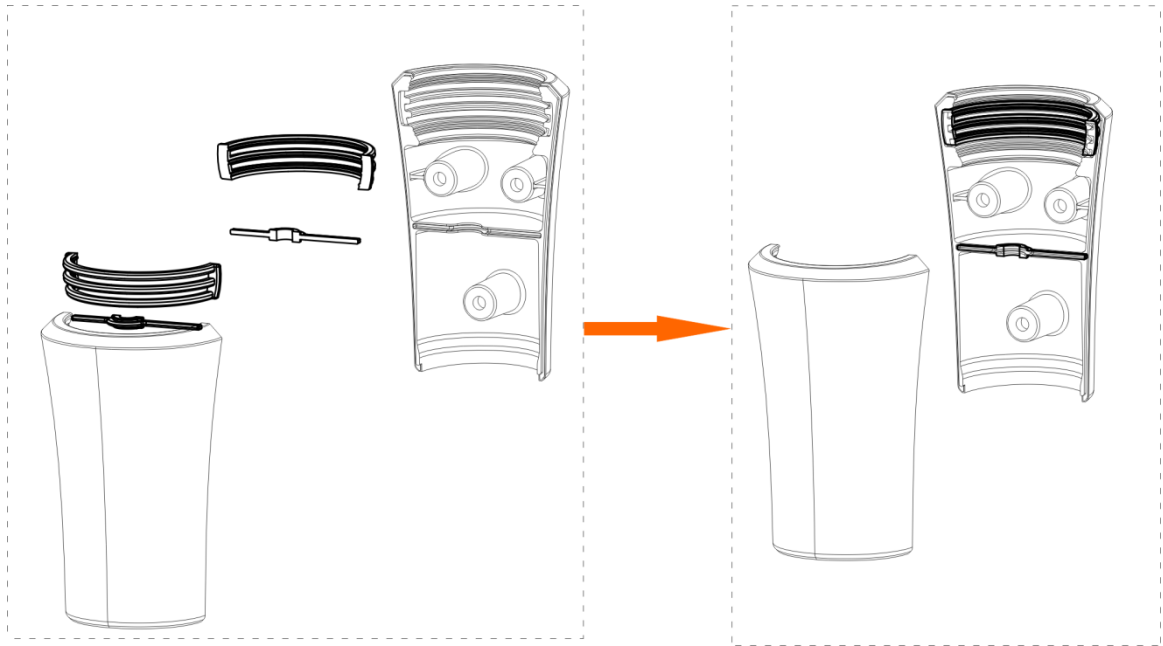
**Step 3** Use a M6×20 screw to fix the Camera and bracket. The screw can be used to adjust the Camera upward and downward.

**Step 4** Adjust the Camera to proper position, and then tighten the screws.

## 3.3 Spherical Bracket Installation

**Step 1** Insert the damping ring and waterproof ring of cable into the bracket housing.

Figure 3-3 Prepare bracket housing



**Step 2** Cover the spherical bracket with bracket housing.

**Step 3** Use three M6×20 socket head cap screws to fix the bracket housing to the Camera.  
See Figure 3-4.

For the illustration after installation, see Figure 3-5.

Figure 3-4 Fix the bracket housing

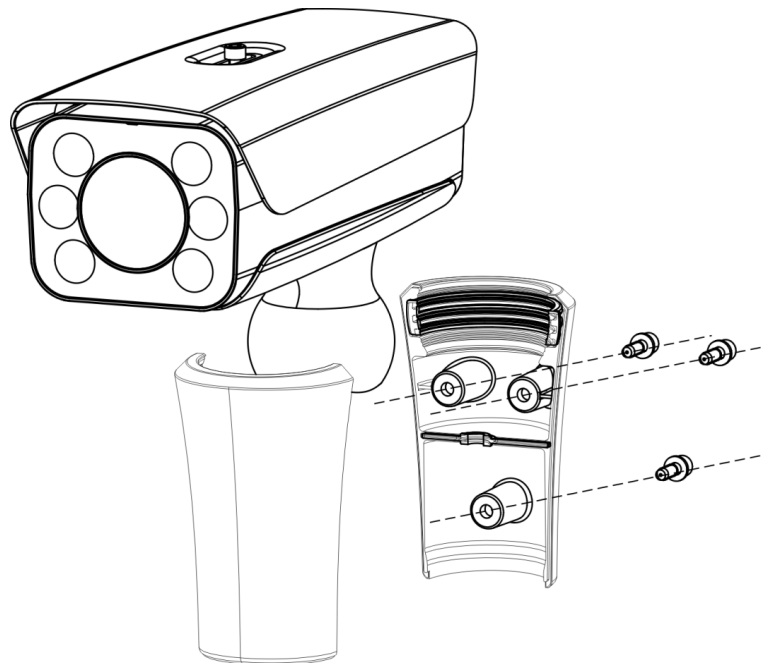
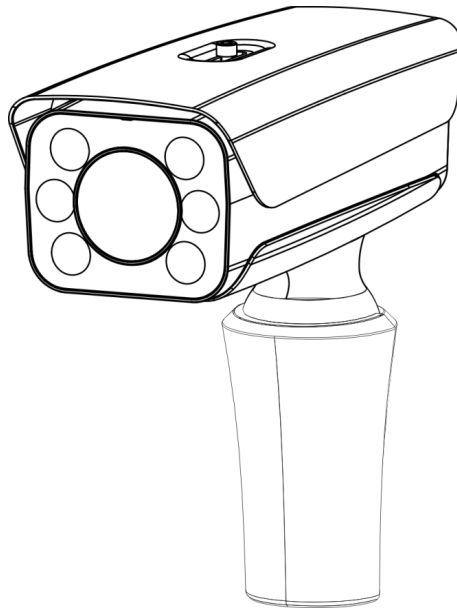


Figure 3-5 Installation completed



## 4 Web Configuration

It supports logging in to device web interface through browser on PC, and realizes device configuration, operation, and management.



The interfaces and Settings are for reference only, and the actual interface shall prevail.

### 4.1 Web Login

#### 4.1.1 Recommended Configuration

Refer to Table 4-1 for recommended PC configuration for logging in to the web interface of the Camera.

Table 4-1 Recommended PC configuration

PC Component	Recommended Configuration
Operating System	Windows 7 and newer
CPU	Intel core i3 and newer
Graphics	Intel HD Graphics and above
RAM	2GB and more
Monitor	1024×768 and higher
Browser	Internet Explorer 9/11, Chrome 33/41, Firefox 49

#### 4.1.2 Device Initialization

The Camera is delivered uninitialized by default. You need to initialize it and modify its password before further operations.

Before initialization, make sure that both PC IP and device IP are in the same network segment, otherwise it might fail to enter initialization interface.

**Step 1** Set IP address, subnet mask, and gateway of PC and device 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.

The IP address is 192.168.1.108 by default.

**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

**Device Initialization**

Username: admin

Password:

The minimum pass phrase length is 8 characters

Weak Middle Strong

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.

Confirm

**Step 4** Enter Password and Confirm Password.



- The new password must consist of 8 to 32 characters and contain at least two types from upper case, lower case, number, and special characters (excluding ' " ; : and &).
- If you want to change your password again, go to **Setup > System > Account > Account**.

**Step 5** Select the **Email Address** check box, and then enter your email address (recommended to set for resetting your password).

**Step 6** Click **Confirm**.

**Step 7** On the **Online Upgrade** interface, click **Confirm**.

Figure 4-2 Config guide

**Config Guide**

IP Address: 192 . 168 . 1 . 108

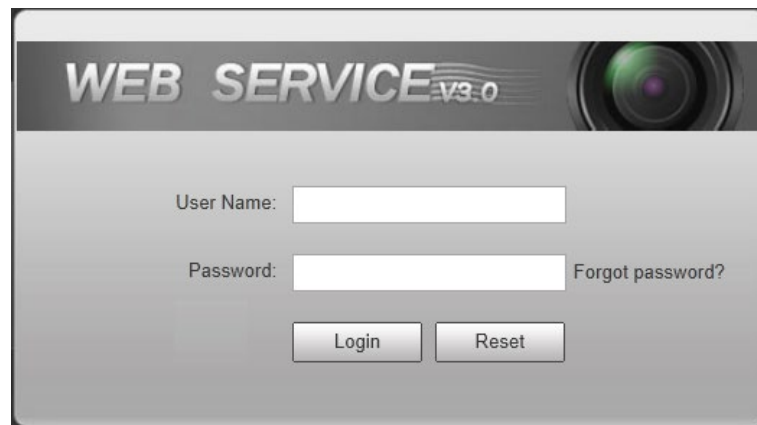
Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 1 . 1

Finish

**Step 8** Modify the default IP address, subnet mask, and default gateway, and then click **Finish**.

Figure 4-3 Login



**Step 9** Enter the username and password, and then click **Login**.

The web interface is displayed.



Prompt box will pop out when username or password is incorrect, see Figure 4-4, and it will remind you of remaining attempts. The account will be locked for 300 s if user enters incorrect username or password for 5 times consecutively. See Figure 4-5.

Figure 4-4 Login error

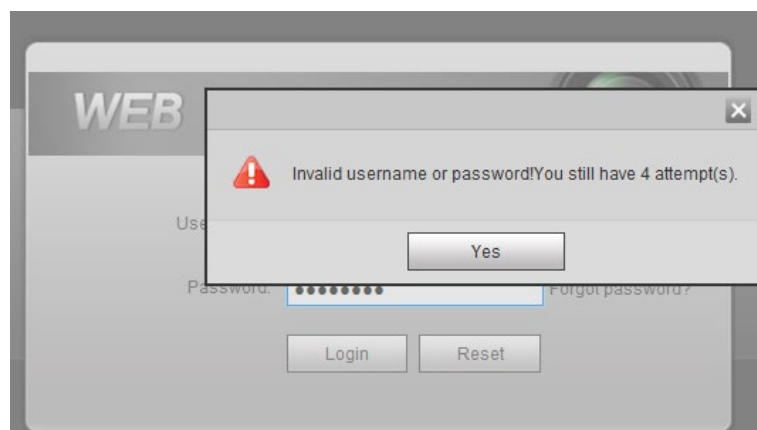
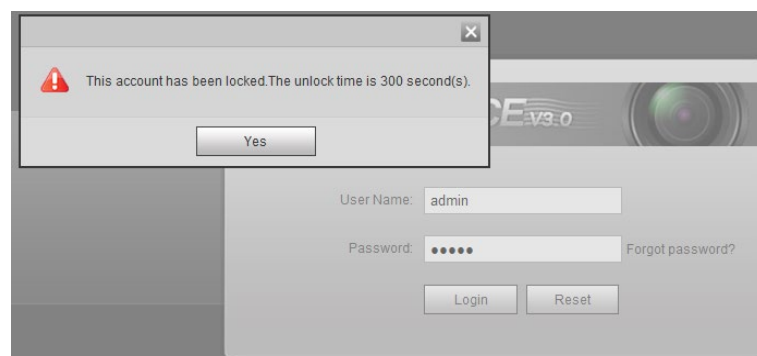


Figure 4-5 Account locked



**Step 10** Click Please click here to download and install the plug-in in the video window.

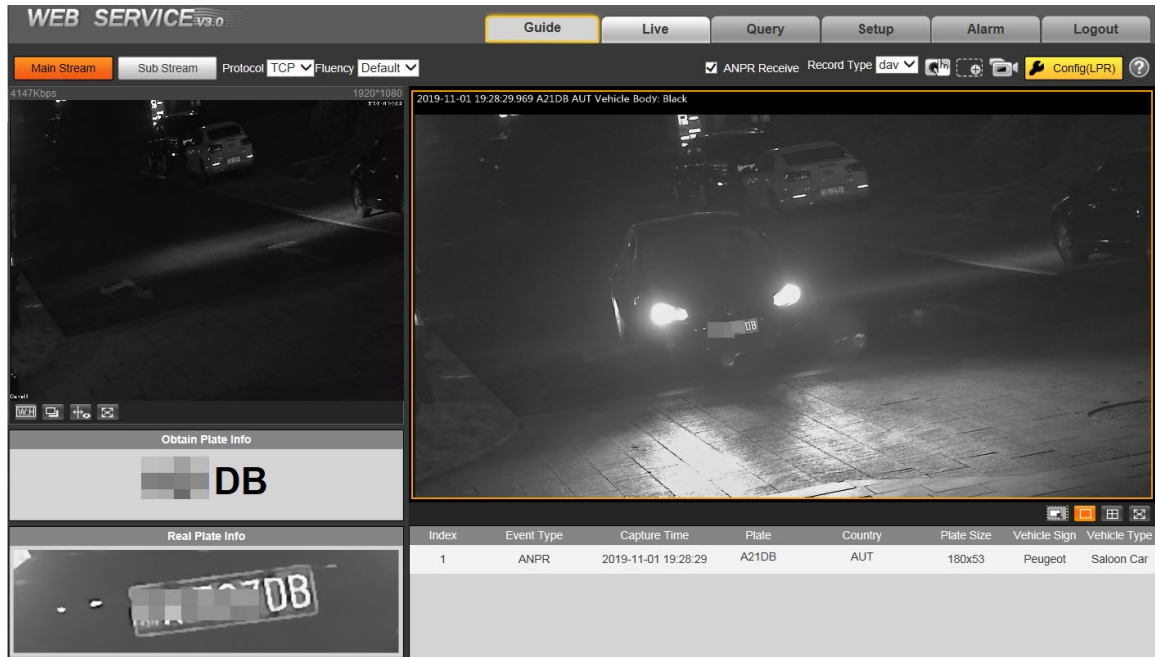
The system automatically downloads webplugin.exe and installs it according to prompt.



Before installing plug-in, make sure that the associated plug-in option of active has been modified as **Enable** or **Prompt** in **Internet Option > Security Settings**.

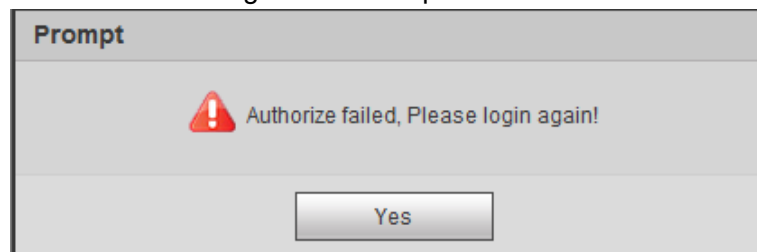
After installation is completed, the web interface is displayed. See Figure 4-6.

Figure 4-6 Web interface



It will pop out the prompt box of authorization failed when there is no operation on the web interface for a long time. In this case, you need to log in again.

Figure 4-7 Prompt



### 4.1.3 Login

You can log in to the web interface by following the steps below. For first-time login or logging in after restoring factory default Settings, see "4.1.2 Device Initialization."

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

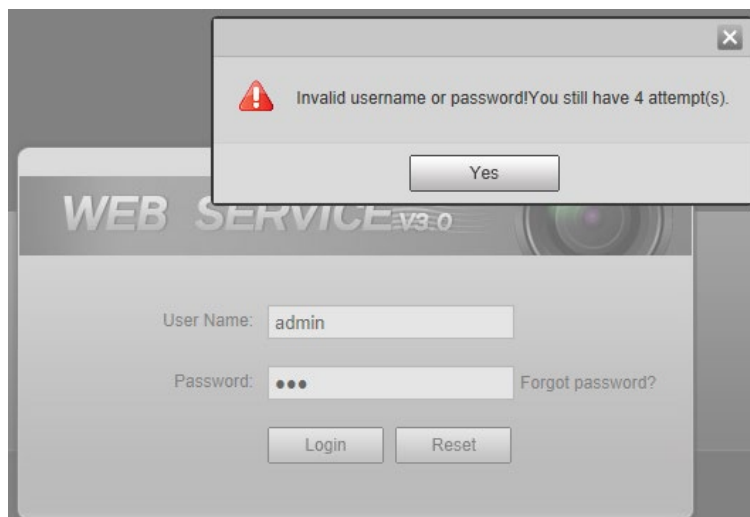
**Step 2** Enter your login username and password, and then click **Login**.

The web interface is displayed.



- A box pops up when the username or password is incorrect. See Figure 4-8.
- If you enter invalid user name or password for five times, the account will be locked for 300 s.

Figure 4-8 Invalid username or password



## 4.1.4 Resetting Password

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

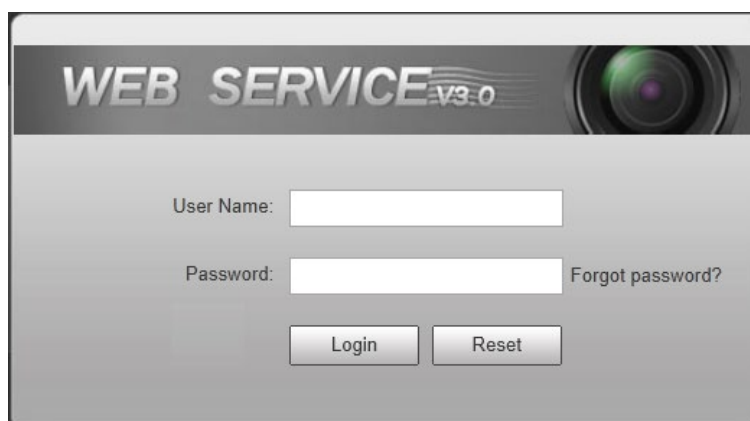


Pay attention to the following tips during password reset.

- When scanning QR code to acquire security code, one QR code supports security code acquisition up to twice.
- After receiving security code by email, you need to reset password within 24 hours, otherwise, the security code will be invalid.
- 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.
- 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 **Setup > System > Account > Account**.

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

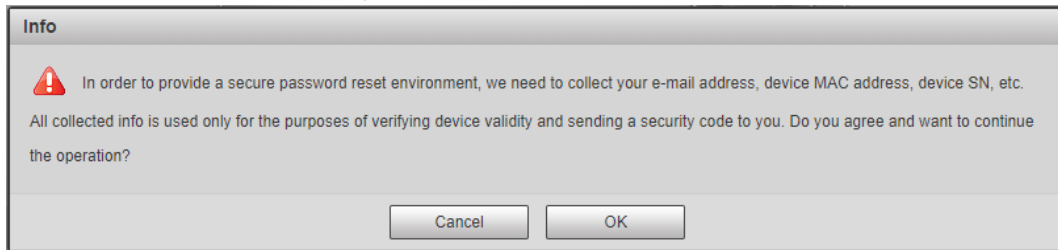
Figure 4-9 Login interface





**Step 2** Click **Forgot password?**

Figure 4-10 Information



**Step 3** Click **OK**.



If you use IE browser, the system might prompt **Stop running the script**, click **No** and continue to run the script.

Figure 4-11 Reset password (1)



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

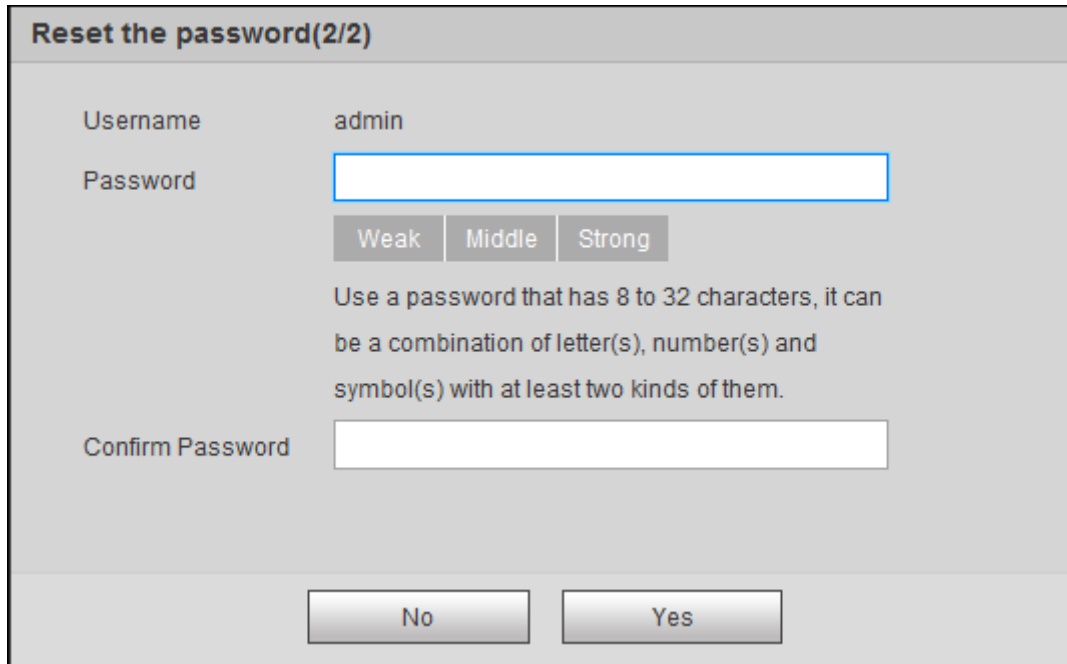


Scan the actual QR code. Do not scan the QR code in this manual.

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

**Step 6** Click **Next**.

Figure 4-12 Reset password (2)



**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** and the password is reset.

## 4.1.5 Web Functions

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

Figure 4-13 Tab

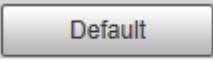
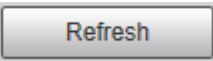



Table 4-2 Tab function description

Tab	Function
Guide	Quick configuration of plate pixel, recognition region, and more.
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.
Setup	Set rules of intelligent traffic, camera basic attribute, network, event, storage, and system, and view system information.
Alarm	Sets alarm prompt.
Logout	Log out web.

The following buttons are very common on the web interface.

Table 4-3 Common buttons description

Button	Description
	Click the button, and click <b>Confirm</b> , then all the parameters will be recovered to system defaults.
	Click the button and all the parameters will be recovered to the value which is the latest saved.
	Click the button after the parameter configuration is completed, and then it makes the current settings valid.

## 4.2 Guide

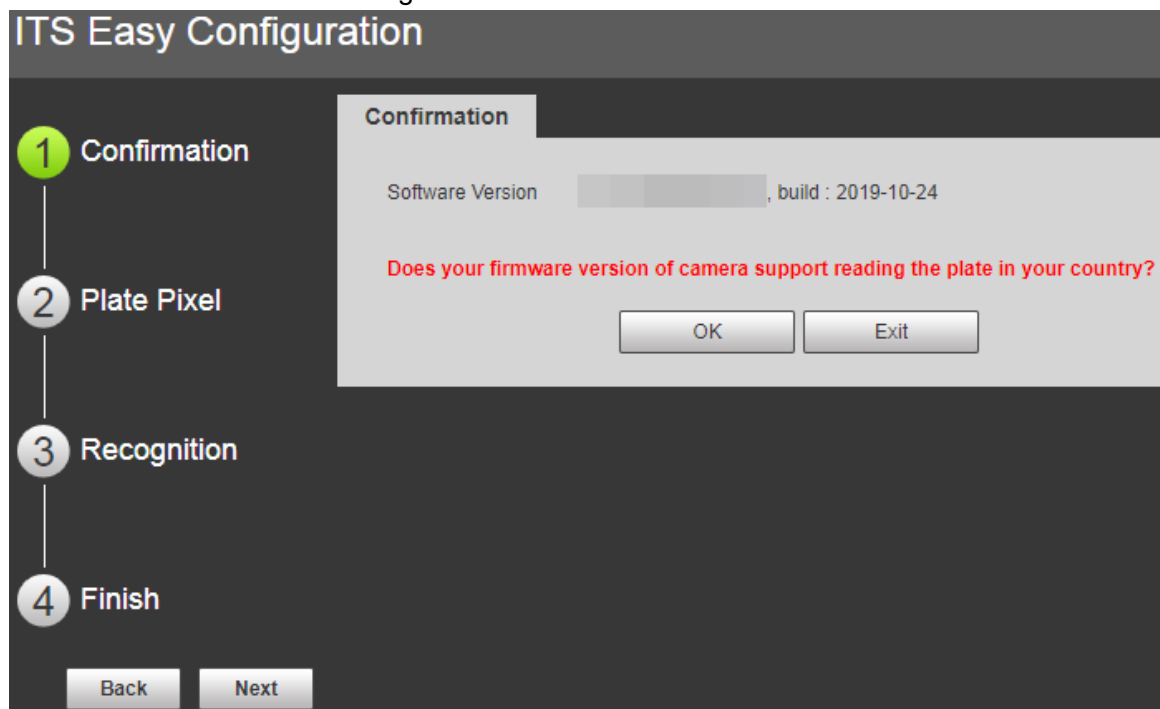
On the **Guide** interface, you can configure capture scenarios, and get assistance with setting installation scenario.



You can click  at the upper-right corner of **Guide** interface to exit.

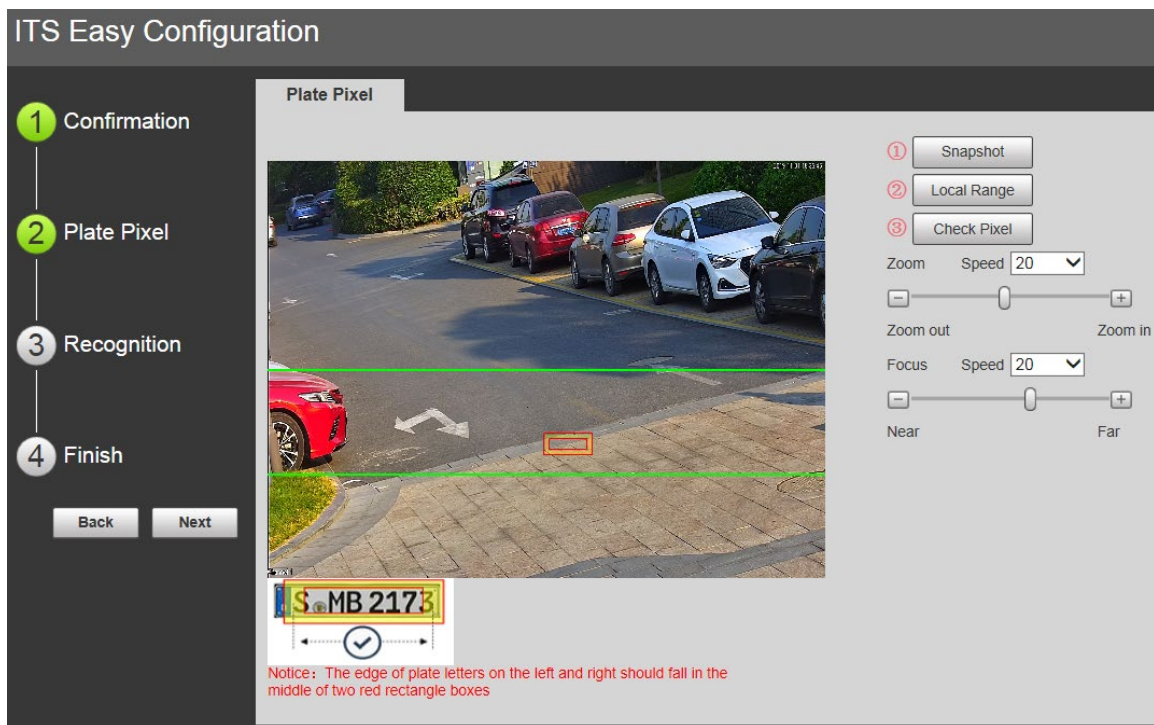
Step 1 Click the **Guide** tab.

Figure 4-14 Confirmation



Step 2 Confirm **Software Version**, and then click **Confirm**.

Figure 4-15 Plate pixel



**Step 3** You can check whether the video image is properly zoomed and focused by checking the plate pixel.

- 1) Drag zoom and focus bar to adjust the video image properly.
- 2) When the vehicle plate comes into the green line area, click **Snapshot** to take a snapshot of the plate.

**Snapshot** becomes **Resume**.

- 3) Drag the yellow plate pixel box to the position of the plate.
- 4) Click **Zoom**.  
Zoom in the picture selected by the plate pixel box. It can realize 2x or 4x zoom rate.
- 5) Adjust the position of plate pixel box and make it the optimal plate size. See Figure 4-16.



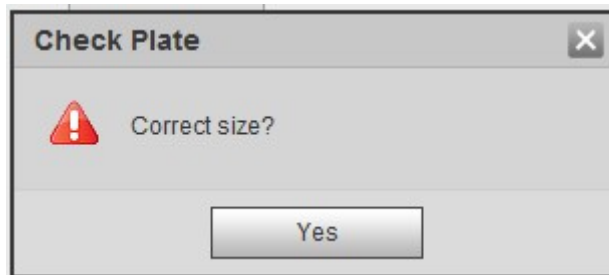
If the plate within the yellow box is larger than the optimal plate size in the example, zoom out the video image; if smaller, zoom in the video image.

Figure 4-16 Plate pixel size



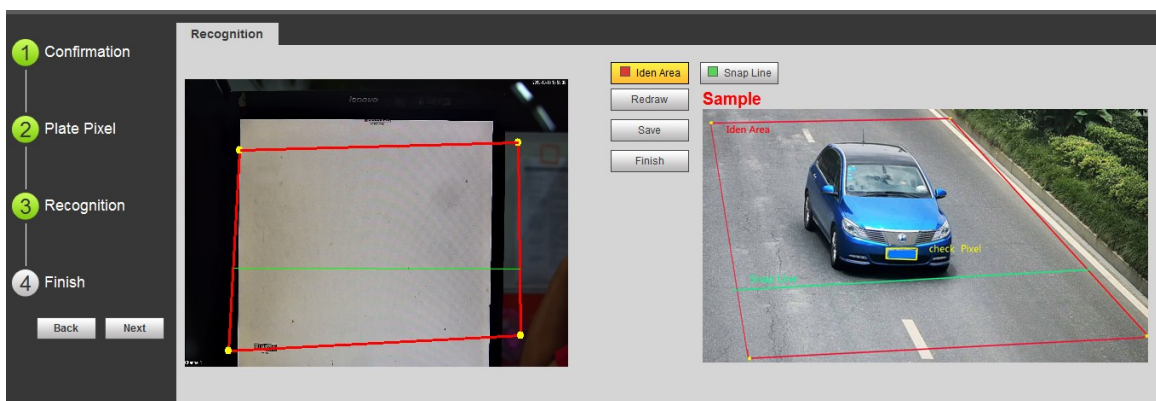
6) Click Check Pixel.

Figure 4-17 Check plate



7) Click **Yes** and plate pixel configuration is finished.

Figure 4-18 Recognition



**Step 4** Configure recognition area.

The configuration example on the right of video interface can be used as a reference.

- 1) Click **Iden Area** (identification area).  
Click and draw 4 lines on the video interface and the recognition area is formed.
- 2) Click Snap Line.  
Draw snap line by dragging mouse on the area. The snap line must cross the area.

3) Click **Save** to complete the Settings.

Step 5 Click **Finish**, exit **Guide** interface and enter **Live** interface.

### 4.3 Live

Click the **Live** tab. The **Live** interface is displayed.

On this interface, it can realize several functions such as live video, live picture, real-time capture, record and config (LPR), and more.

Figure 4-19 Live

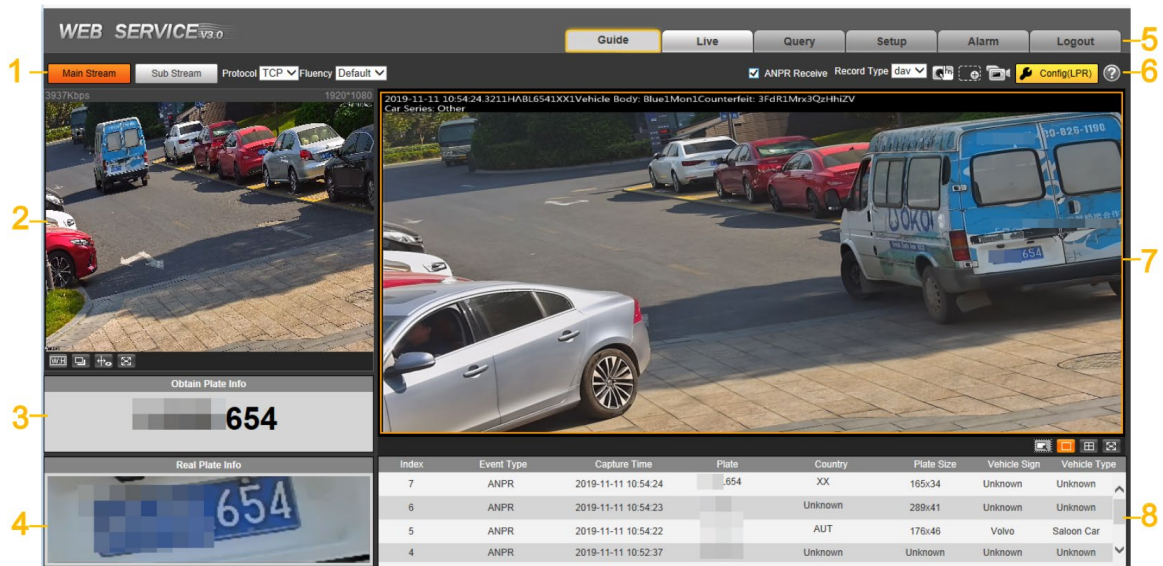


Table 4-4 Live interface bar

No.	Description	No.	Description
1	Video stream	5	System functions
2	Live view	6	Functions of Live interface
3	Logged plate number	7	Vehicle snapshot
4	Plate snapshot	8	Event list

#### 4.3.1 Video Stream

- **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 reduce 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).

#### 4.3.2 Live View

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



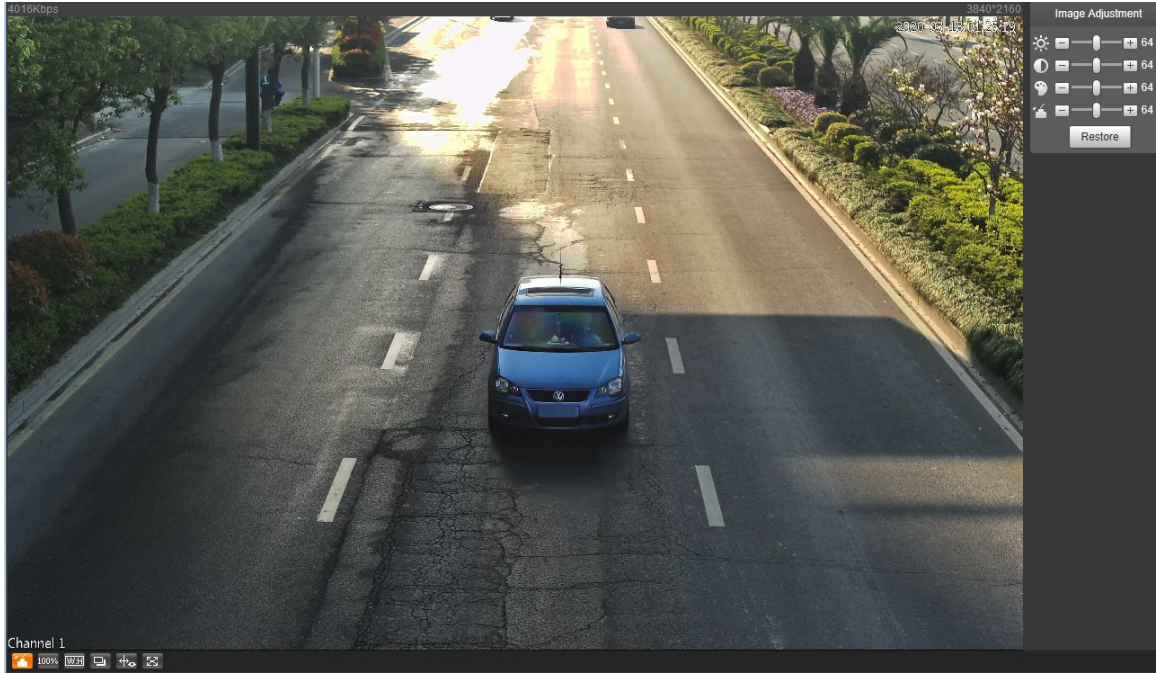
- : Adjust the image to original size or appropriate window.
- : Click it to switch to big window and display image adjustment window. Click it again to exit big window.

Figure 4-20 Big window












- ◇ : Click it to open image adjustment window on the right, meanwhile the button turns to . Click  to close image adjustment window. For image adjustment description, see □.
- ◇ : Click it and the image is 100% displayed, meanwhile the button turns to . Click  to switch back to original size.
- : Click it to enable smart track detection. Number plate, 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 4-5 Image adjustment

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).

Icon	Name	Description
	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).
	—	Click it to 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 **Setup > Camera > Attribute > General**.

### 4.3.3 Logged Plate Number

Displays the plate number recognized by the Camera in real-time when a vehicle passes.

### 4.3.4 Plate Snapshot

Displays the snapshot of license plate when a vehicle passes.

### 4.3.5 System Functions

Click the icons to set system functions, which include playback, video recording and snapshot query, intelligent rules setting, alarm event setting, and system logout. See more details in the following chapters.

### 4.3.6 Functions of the Live Interface

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

Figure 4-21 General function option column

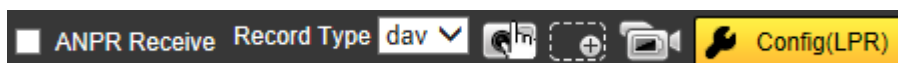


Table 4-6 General function option

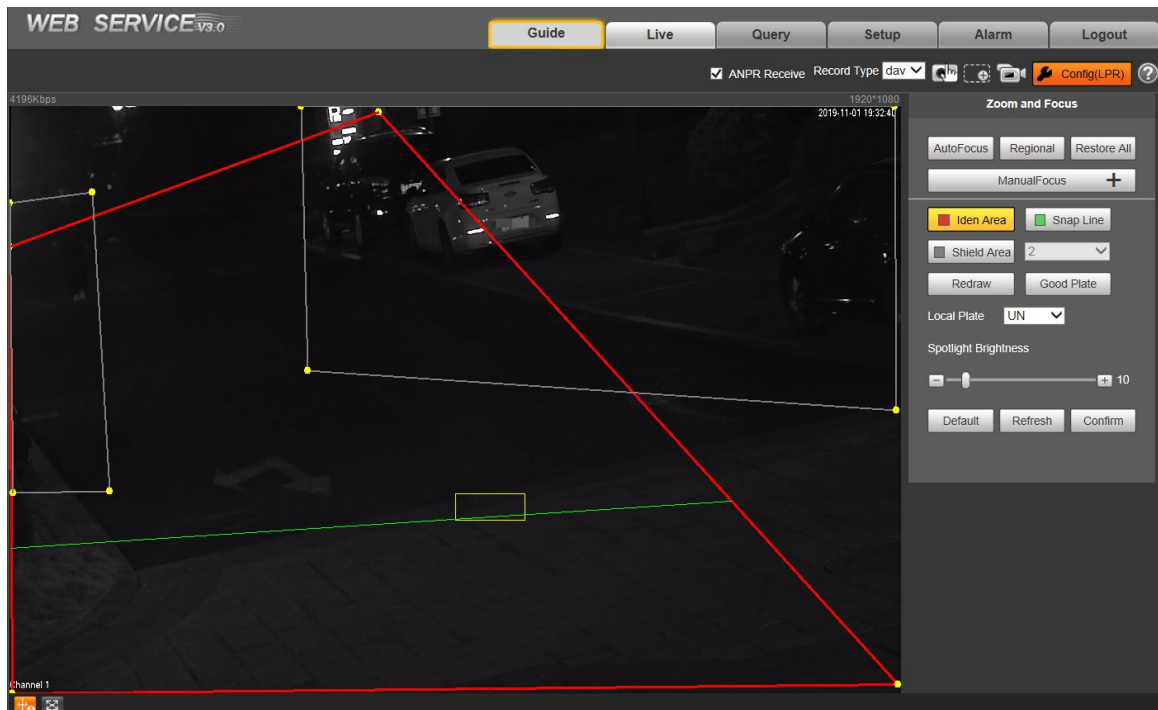
Icons	Name	Description
	ANPR Receive	Select the check box, and the Camera automatically receives vehicle snapshots and detects event information triggered by sources such as radar or video detection, and displays such snapshots and information at the lower part of the interface. The snapshots are saved in the storage path defined by <b>Setup &gt; Storage &gt; Destination &gt; Save Path</b> .



Icons	Name	Description
	Record Type	Select the format of video recordings ( <b>dav</b> by default). It is required to be <b>ps</b> for GB 28181.
	Manual Snapshot	Click it, and the Camera takes a snapshot when a vehicle passes. The snapshot is saved in the storage path. <ul style="list-style-type: none"> <li>• Enable <b>ANPR Receive</b> first.</li> <li>• To change the storage path of snapshots, go to <b>Setup &gt; Storage &gt; Destination &gt; Save Path</b>.</li> </ul>
	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  again to stop recording. You can set the storage path of video recordings from <b>Setup &gt; Storage &gt; Destination &gt; Save Path</b> .
	Config (LPR)	You can draw the area of plate detection, adjust camera's focal length, and set local character.

Click and the interface of Config (LPR) is displayed.

Figure 4-22 Config (LPR)



The steps of config (LPR) are shown as follows.

**Step 1** Set focus and zoom mode, which is used to recognize vehicle. Refer to Table 4-7 for more details.

Table 4-7 Focus parameter description

Parameter	Description
Auto Focus	Auto adjust camera lens and make the scenario clearly focused.
Regional	Click <b>Regional</b> , and then draw a box in the video image to focus the defined the region in the box.
Manual Focus	Manually set focus parameter and make the camera focus on the vehicle. Zoom: <ul style="list-style-type: none"> <li>◇ Step length: There are totally 3 levels to be selected.</li> <li>◇ Zoom in, zoom out: Click  and add a step length, click  and reduce a step length; Or directly drag adjustment bar and set zoom.</li> </ul> Focus: <ul style="list-style-type: none"> <li>◇ Step length: There are totally 3 levels to be selected.</li> <li>◇ Focal length: Click  to add a speed, click  to reduce a speed; or it can directly drag adjustment bar to set near and far focal length.</li> </ul>
Restore All	Restore all to initialized Settings.
Refresh	Check the latest status.

**Step 2** Select the config line type which needs to be drawn. Refer to Table 4-8 for more details.



The configured area line and detection line in **Guide** are displayed in the video interface.

Table 4-8 Line parameters description

Parameter	Description
Iden Area	Click it and draw the area range which needs to be detected. The recognition area line is displayed as red box.
Snap Line	Draw the detection line which triggers video capture, it is as functional as the line in traffic. It will trigger and take snapshot when the vehicle crosses the detection line. Snap line is displayed as green line.
Shield Area	Set the area range which needs to be shielded. LPR is not implemented within the shielded area. It supports setting max two shielded areas. Area line is displayed as gray box.
Good Plate	Click it, and drag the yellow plate pixel box to the range of vehicle plate on the video image.  If the plate within the yellow box is larger than the optimal plate size in the example, zoom out the video image by clicking <b>Manual Focus</b> ; if smaller, zoom in the video image.

**Step 3** Draw lines on the view interface.



Click **Redraw** to delete lines one by one.

**Step 4** Adjust the vehicle snapshot location to yellow box.

Make sure that the location and size of plate is in accordance with that of the yellow box.



Plate optimal width range is from 140 to 160. If you want to modify the range, go to **Setup > ITC > Intelligent > Video Analyse > Recognition**, and make Settings.

Step 5 Set **Local Plate**. Set local plate according to the location of the Camera.

Step 6 Set **Spotlight Brightness**. Drag the block and set brightness of flashing light according to actual requirement.

Step 7 Click **Confirm**.

### 4.3.7 Vehicle Snapshot

Select **ANPR Receive**, and then snapshots will be displayed when vehicles pass.

### 4.3.8 Event List

Select **ANPR Receive**, and the event information will be displayed, including No., event types, capture time, lanes, plates, vehicle color, speed, vehicle signs, and vehicle types.

## 4.4 Query

Click the **Query** tab and the system displays query interface where users can search for pictures and video recordings.

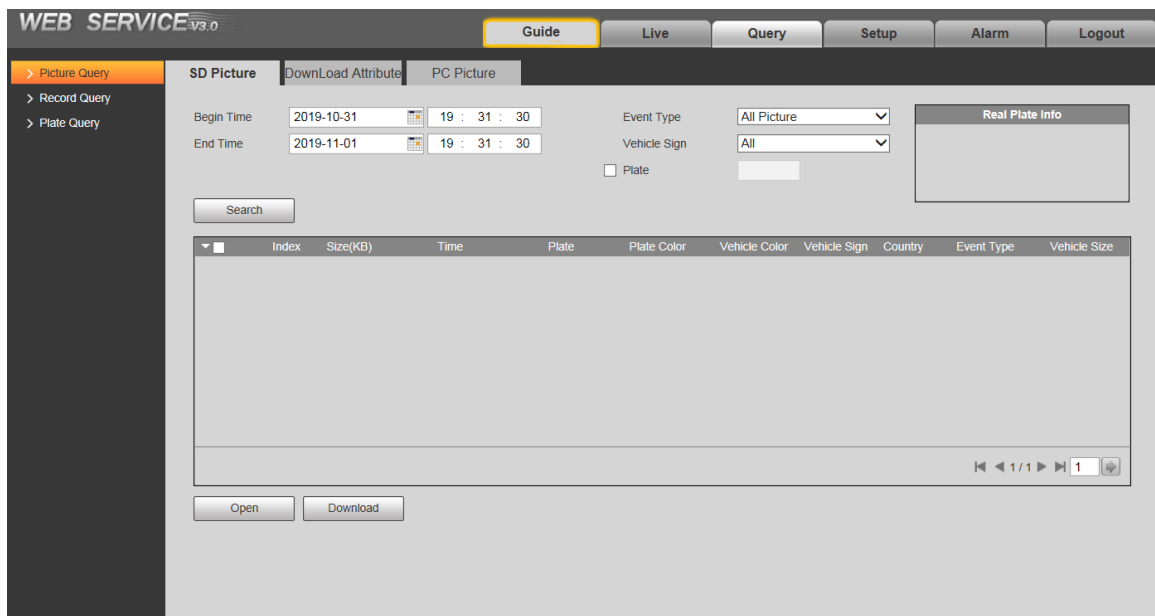
### 4.4.1 Picture Query

#### 4.4.1.1 SD Picture

Search conditions can be set in this section. You can search for event and plate information of the SD card within the period.

**Step 1** Select Query > Picture Query > SD Picture.

Figure 4-23 SD Picture



**Step 2** Configure the parameters as needed.

Table 4-9 SD picture parameter description

Parameter	Description
Begin Time	Set the start time of picture query.
End Time	Set the end time of picture query.
Event Type	Search for all pictures, or search for pictures which conform to requirements according to filtering condition based on violation type.
Vehicle Sign	Take vehicle sign as query condition, then it can select one or all.
Plate	Seelct the <b>Plate</b> check box, take plate feature as query condition and then inquire the pictures which conform to requirements. You can also set some parameters of the plate to realize fuzzy query of plate number

**Step 3** Click **Search**, and it displays all the picture file lists which conform to query condition in the file list.

Click some line in the list and the plate picture information will be displayed in **Real Plate Info**.

**Step 4** Download picture.

- Single download: Select the picture which needs to be downloaded from the file list and click **Download**.
- Check All: Click it and download all the picture files of the current page from the search list. Click **Download**.
- Download by time: Click it and download all the picture files from start time to end time. Click **Download**.

**Step 5** Set the storage path of picture in the dialog box. The system starts to download the pictures to local PC.

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



If several picture files are selected at the same time, click **Open** to open all the pictures.

### 4.4.1.2 Download Picture Attribute

In this section, you can set the picture download time and mode. Confirm picture name according to **Help**.

**Step 1** Select Query > Picture Query > Download Attribute.

Figure 4-24 Download attribute

**Step 2** Configure the download parameters.

Table 4-10 Download attribute parameters description

Parameter	Description
Download Time	Create Time: PC time when the picture is downloaded to PC. Snap Time: Device snapshot time when the picture is downloaded to PC.

Parameter	Description
Download Mode	Selected File: select the needed picture (It supports selecting single picture or several pictures at the same time, downloaded in batches), click <b>Download</b> and the system will pop out the save dialog box. Selected Time: Click <b>Download</b> and the system will automatically download all the pictures from start time and end time.
Restore	Restore the picture name to the system default name.
Help...	View the naming rule of downloaded pictures.

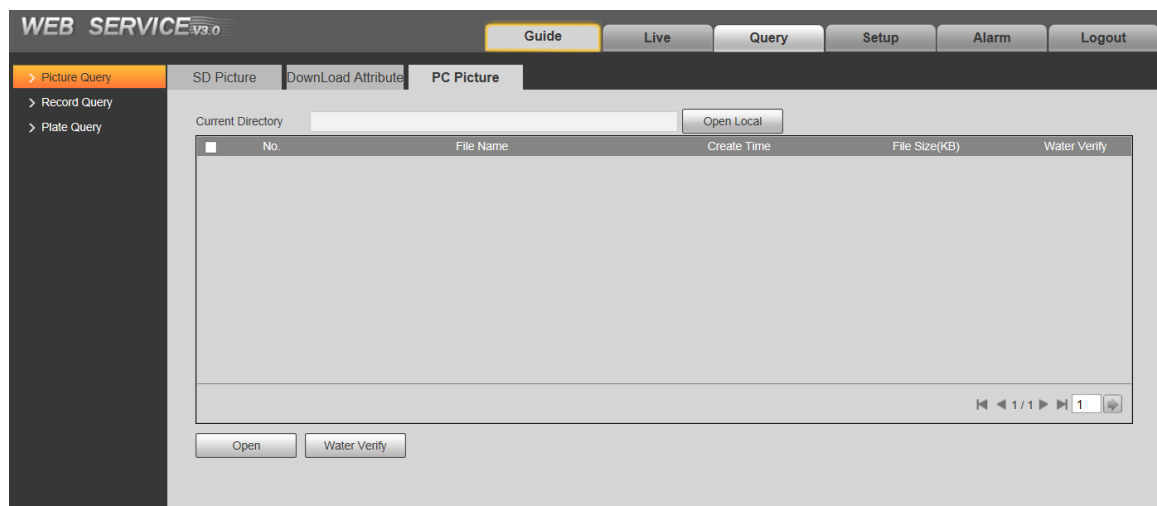
Step 3 Click **Confirm**.

### 4.4.1.3 PC Picture

The section introduces the way of checking whether the watermark of PC picture is tampered.

Step 1 Select Query > Picture Query > PC Picture.

Figure 4-25 PC picture



Step 2 Click **Open Local** and select the folder where the verified picture is located.

Step 3 Select the picture which needs to be verified.

Step 4 Click **Water Verify** and view result in the picture list.

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

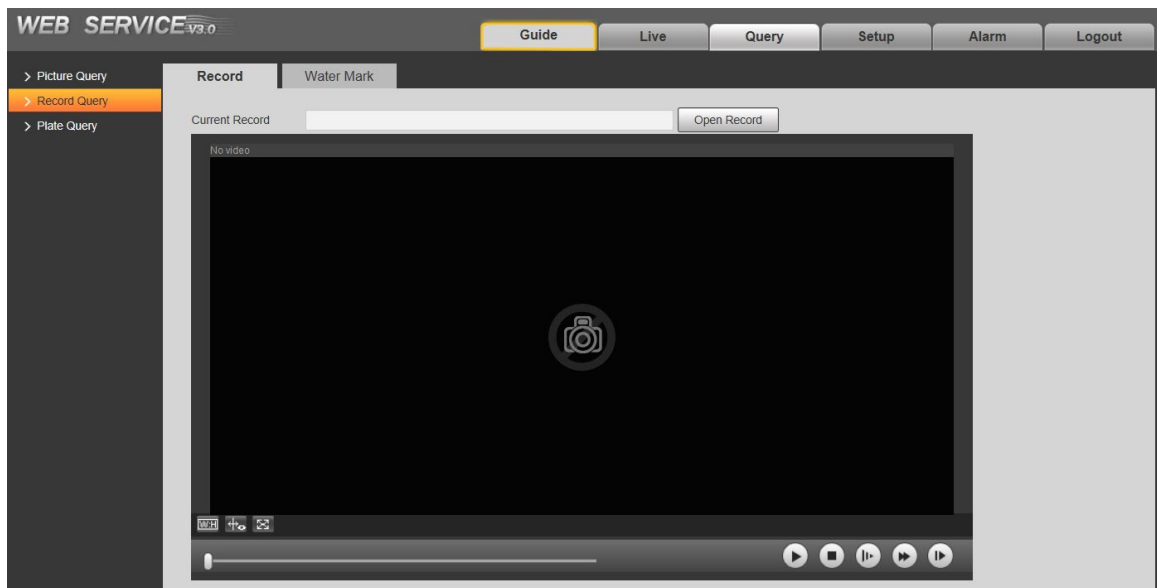
## 4.4.2 Record Query

### 4.4.2.1 Record

You can set video play of local PC on this interface.

Step 1 Select Query > Record Query > Record.

Figure 4-26 Record



**Step 2** Click **Open Record**, select record path, click **Open** and view the video.  
For the function description of video play button, see the table below.

Table 4-11 Play function

Icon	Name	Description
	Play/Pause	means pause or not playing. Click it to switch to normal play status. means playing video. Click it to pause.
	Stop	Click it to stop playing video.
	Slow-down Play	Click it to slow down video playing.
	Speed-up Play	Click it to speed up video playing.
	Play by Frame	Click it to skip to the next frame.

#### 4.4.2.2 Watermark

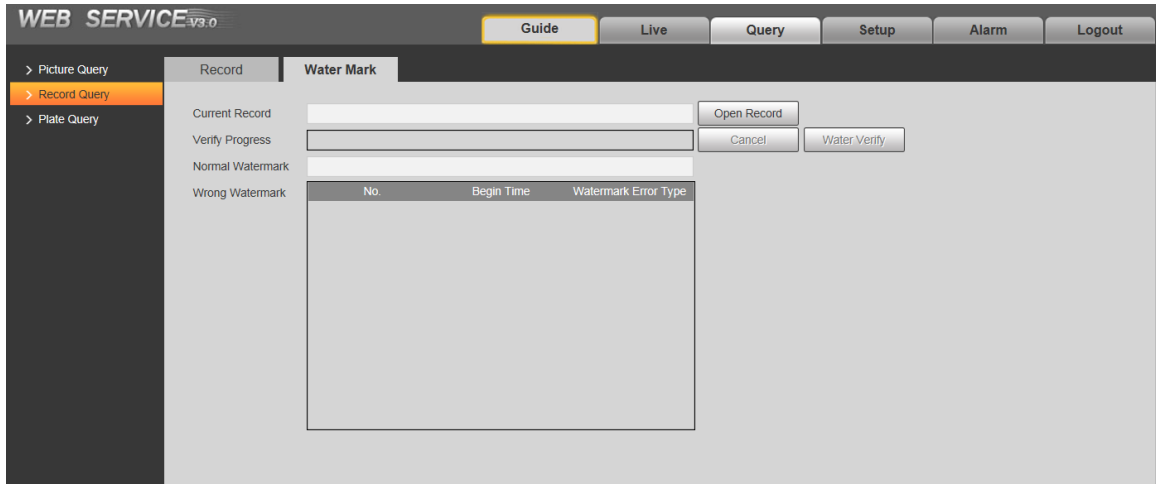
In this section, you can verify whether the watermark of local record is tampered.



Go to **Setup > Camera > Video > Video** and check **Watermark Settings** if you want to enable the function, and set corresponding **Watermark Character**. The default watermark character is **DigitalCCTV**.

**Step 1** Select Query > Record Query > Water Mark.

Figure 4-27 Watermark



**Step 2** Click **Open Record** and select a file that you want to verify.

**Step 3** Click **Water Verify** and the system displays verify progress, normal watermark and some other information.

The interface of **Watermark Verification Completed** will be displayed after verification is finished.

### 4.4.3 Plate Query

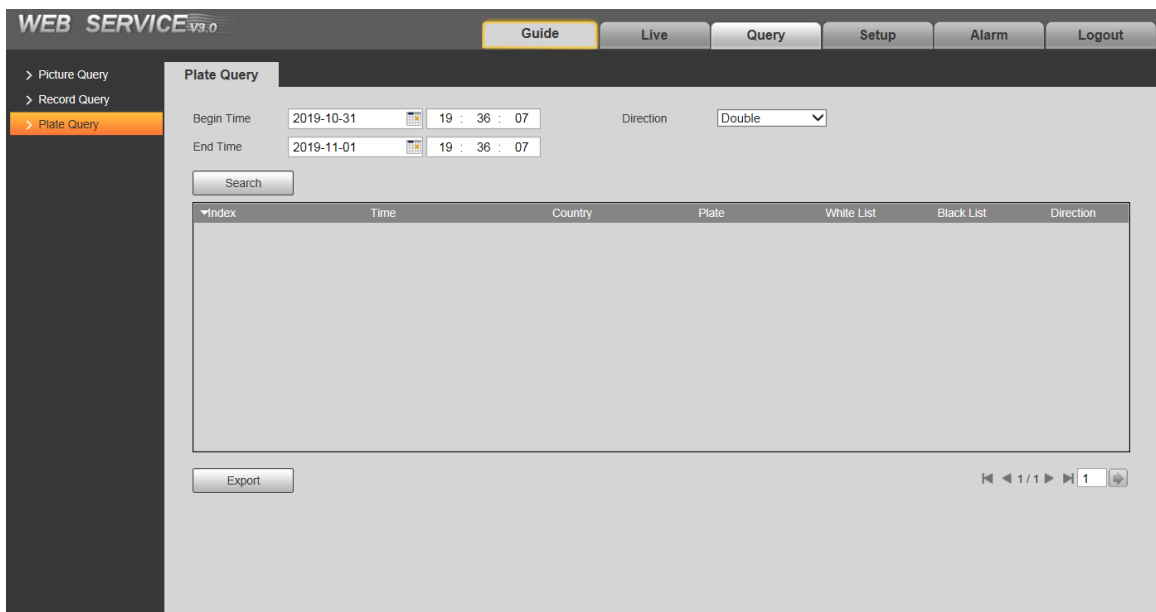
Search for the vehicle record within the defined period and according to the defined direction.



- It supports max 10,000 records or 1,024 records respectively when the camera is installed with or without TF card.
- If the passing vehicle records are unreadable in Excel after being imported, change them into UTF-8 encoding document in txt and then they can be opened normally.

**Step 1** Select Query > Plate Query.

Figure 4-28 Plate Query





- Step 2 Set **Begin Time** and **End Time**, and then set the **Direction** (vehicle movement direction, including **Double**, **Obverse**, **Reverse**, and **Unknown**).
- Step 3 Click **Search** to search for the plates that meet the search conditions.
- Step 4 Click **Export**, and then select storage path to export the results to PC.

## 4.5 Setup

You can configure several parameters such as ITC, camera, network, event, storage, system, and system information.

### 4.5.1 ITC

You can set intelligent parameters of the Camera.

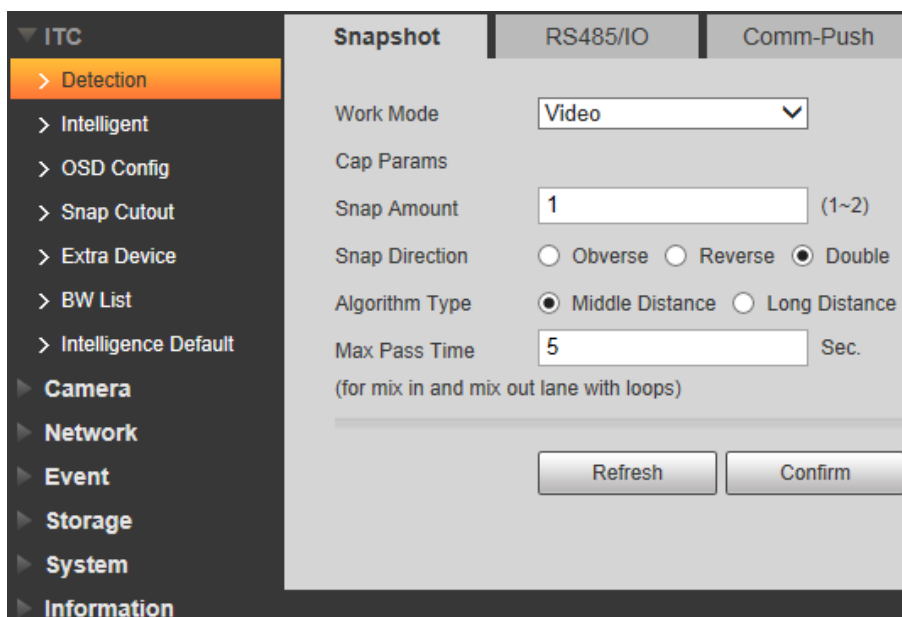
#### 4.5.1.1 Detection

##### 4.5.1.1.1 Snapshot

You can set snapshot rule of the Camera.

Step 1 Select Setup > ITC > Detection > Snapshot.


Figure 4-29 Snapshot



Step 2 Configure the parameters.

Table 4-12 Description of capture parameters

Parameter	Description
Work Mode	<p><b>Coil:</b> Use coil to take snapshots.</p> <p><b>Video:</b> Use video to take snapshots.</p> <p><b>Mixmode:</b> Use coil + video to take snapshots.</p>
Snap Amount	It can take 1–2 snapshot(s).

Parameter	Description
Snap Direction	<b>Obverse:</b> Only captures vehicles that enter. <b>Reverse:</b> Only captures vehicles that leave. <b>Double:</b> Captures vehicles that enter or leave.
Algorithm Type	Select <b>Middle Distance</b> or <b>Long Distance</b> as needed.  Algorithm type is only available for long range models.
Max Pass Time	Enter max vehicle passing time (5 s by default). For example, set max vehicle passing time as 5 s, when using mix in and mix out with loop, after the logical loop is triggered, it will trigger capture loop camera not to take snapshot within 5 s.

**Step 3** Click **Confirm**.

#### 4.5.1.1.2 RS485/IO

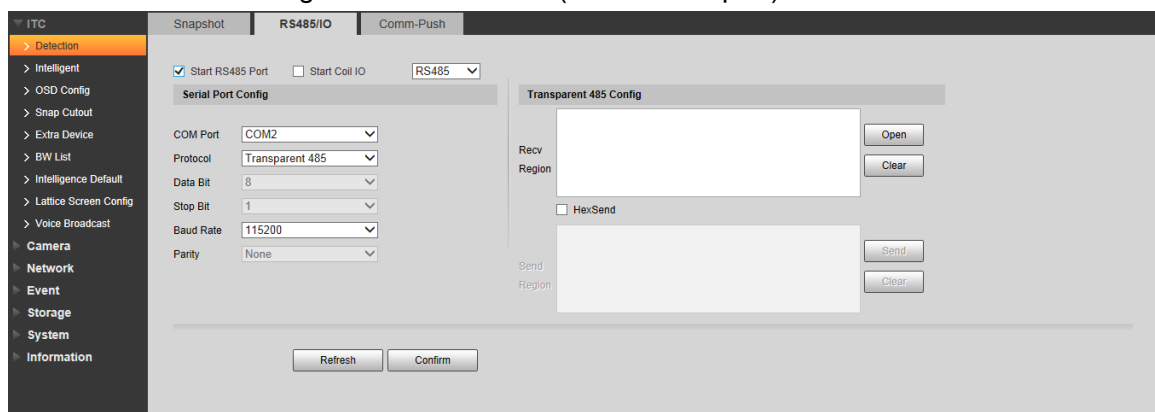
You can configure 485 interface associated configuration information and loop IO snapshot configuration.

Select **Setup > ITC > Detection > RS485/IO**, the **RS485/IO** interface is displayed.

#### Start RS-485 Port

**Step 1** Select **Start RS485 Port**, but not Start Coil IO.

Figure 4-30 RS485/IO (start RS485 port)



**Step 2** Select **Protocol**, and set protocol type according to the number of com port.

- Select **CarDetect** from **Protocol**.
  - 1) Set the baud rate of the protocol.
  - 2) Select scheme.
    - ◇ **Single\_in1-snap\_nospeed:** Lay single coil and it will take snapshot when the vehicle enters coil.
    - ◇ **Double\_in1-snap\_speed:** Lay double coil and it will take snapshot when the vehicle enters the first coil.
    - ◇ **Double\_in2-snap\_speed:** Lay double coil and it will take snapshot when the vehicle enters the second coil.
  - 3) Click **Setup** corresponding to **Coils Map** and it pops up the **Coils Map** dialog box. Select the corresponding relationship between logical coil and physical coil and click **Yes**.



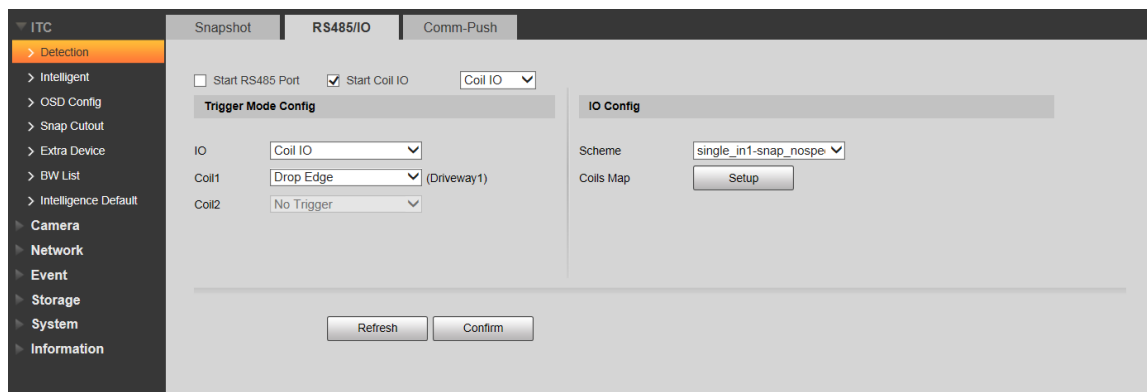
- ◇ The function needs to be configured in the mix in and mix out mode. See **Standard Construction Scheme**.
- ◇ When the scheme is **single\_in1-snap\_nospeed**, then you only need to select the corresponding physical coil of logical coil.
- Select **Transparent 485** from **Protocol**.
  - 1) Select the baud rate of the protocol.
  - 2) If it needs test, then it needs to select the **HexSend** check box. Click **Open** on the right of **Recv Region** and test the reception status of transparent 485 according to actual situation.
- Select **COM-Push** or **Wiegand** from **Protocol**: Select the baud rate of the protocol.

**Step 3** Click **Confirm**.

### Start Coil IO

**Step 1** Select **Start Coil IO** but not select Start RS485 Port.

Figure 4-31 RS485/IO (Start Coil IO)



**Step 2** Configure the parameters.

Table 4-13 Coil IO parameters description

Parameter	Description	
Trigger Mode Config	IO	Only <b>Coil IO</b> can be selected.
	Coil 1	Set the coil trigger mode.
	Coil 2	<b>No trigger</b> : No capture is triggered. <b>Rise Edge</b> : Capture is triggered when the vehicle enters coil. <b>Drop Edge</b> : Capture is triggered when the vehicle exits coil. When the scheme is <b>single_in1-snap</b> , then coil 2 can not be set.
IO Config	Scheme	Set IO snapshot scheme. <b>Single_in1-snap_nospeed</b> : Lay single coil and it will take snapshot when the vehicle enters coil. <b>Double_in1-snap_speed</b> : Lay double coil and it will take snapshot when the vehicle enters the first coil. <b>Double_in2-snap_speed</b> : Lay double coil and it will take snapshot when the vehicle enters the second coil.

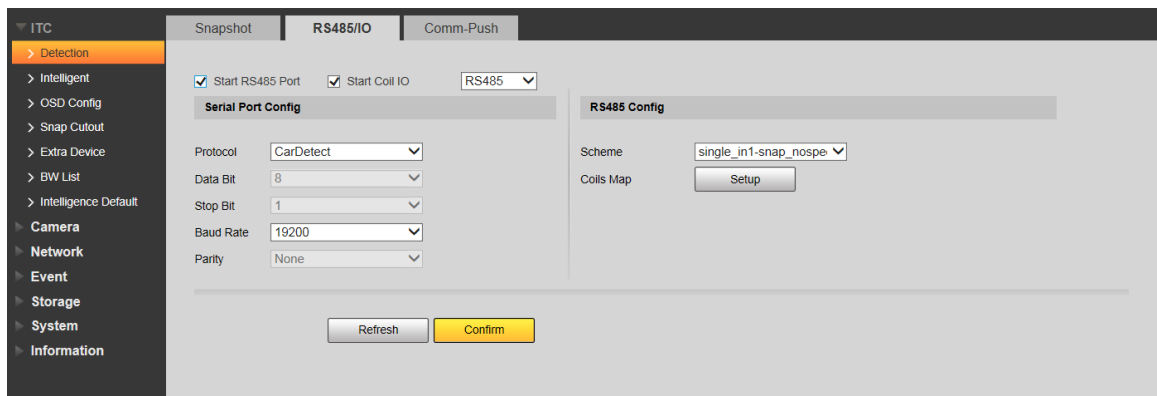
	Coils Map	Select the corresponding relationship between logical coil and physical coil.
--	-----------	-------------------------------------------------------------------------------

**Step 3** Click **Confirm**.

### Start RS485 and Coil IO

Select **Start Coil IO** and **Start RS485 Port** at the same time, and then it can realize the vehicle snapshot configuration of coil IO and RS-485 port configuration. See Figure 4-32.

Figure 4-32 RS485/IO (Start RS485 and Coil IO)



### 4.5.1.1.3 Com-Push

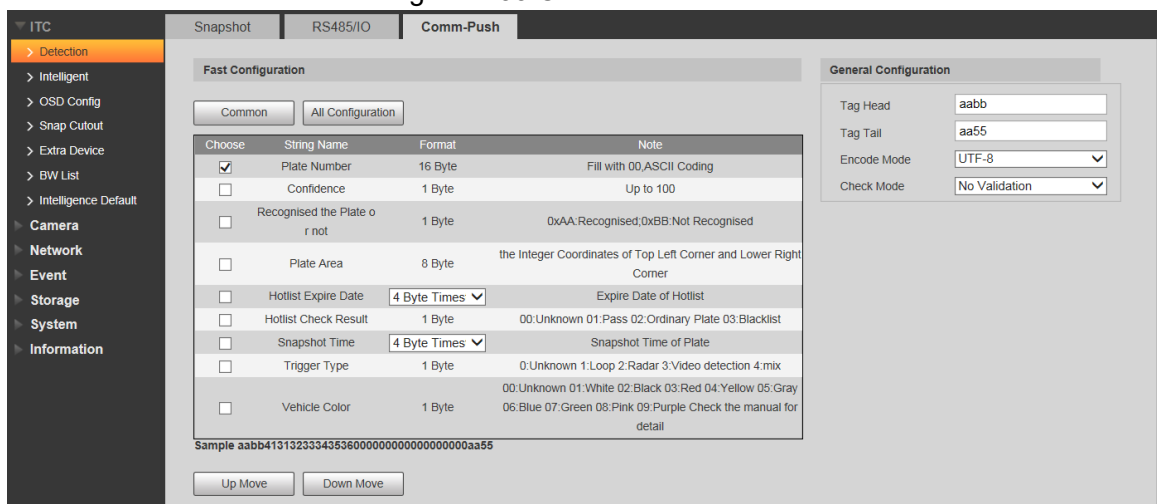
Push the snapshot and data information mode to server according to actual requirement.



Set **Comm-Push** as the **Protocol** from **RS485/IO**, and set the **Baud Rate**; otherwise, the **Comm-Push** function will not be available.

**Step 1** Select Setup > ITC > Detection > Comm-Push.

Figure 4-33 Com-Push



**Step 2** Configure the parameters.

Table 4-14 Com Push

Parameter	Description
Fast Configuration	<b>Common:</b> Click it and select the common vehicle passing option. <b>All Configuration:</b> Click it and select all the vehicle passing options in the list.
General Configuration	Configure picture data information. <b>Tag Head:</b> Com port protocol head, the standard is 4 bit; it can only input hexadecimal character. <b>Tag Tail:</b> Com port protocol tail, the standard is 4 bit; it can only input hexadecimal character. <b>Encode mode:</b> It is the encoding mode of Com port push content. <b>Check mode:</b> verification mode of com port protocol.



- Up Move: Click it, select the corresponding option, and move up.
- Down Move: Click it, select the corresponding option, and move down.

## 4.5.1.2 Intelligent

### 4.5.1.2.1 Recognition

You can set vehicle recognition parameter, recognition mode, and some other functions.


Step 1 Select Setup > ITC > Intelligent > Video Analyse > Recognition.

Figure 4-34 Recognition

The screenshot shows the 'Recognition' configuration window. On the left is a navigation menu with 'Intelligent' highlighted. The main window has two tabs: 'Recognition' (selected) and 'Advance Config'. Under 'Recognition', there are four checked checkboxes: 'CarSeries', 'Vehicle Type', 'Vehicle Color', and 'Vehicle Sign'. Below these are several input fields: 'Plate Size(Unit:Pixel)' with 'Min Width' (70) and 'Max Width' (240) fields, and 'Min Height' (15) and 'Max Height' (100) fields. There are also fields for 'Repeat Plate' (2000 Millisecond), 'CheckTime', and 'Car Detect Sensitivity' (40). At the bottom are 'Refresh' and 'Confirm' buttons.

Step 2 Configure the parameters.

Table 4-15 Recognition parameters description

Parameter	Description
Car Series	Select the target of recognition according to your requirements.
Vehicle Sign	
Vehicle Type	
Vehicle Color	
Plate Size (Unit: Pixel)	Set plate's min width, max width; min height and max height. The unit is pixel.  The setting item is combined with <b>Config(LPR)</b> or <b>Plate Pixel</b> from <b>Guide</b> interface, which is used to set the optimal location of plate and the optimal width of the location. Make sure that the location and size of plate is in accordance with that of the yellow line box.
Repeat Plate CheckTime	One plate can only trigger one ANPR event within the period.
Car Detect Sensitivity	Set the sensitivity of vehicle detection. The higher the value, the more sensitive the detection.

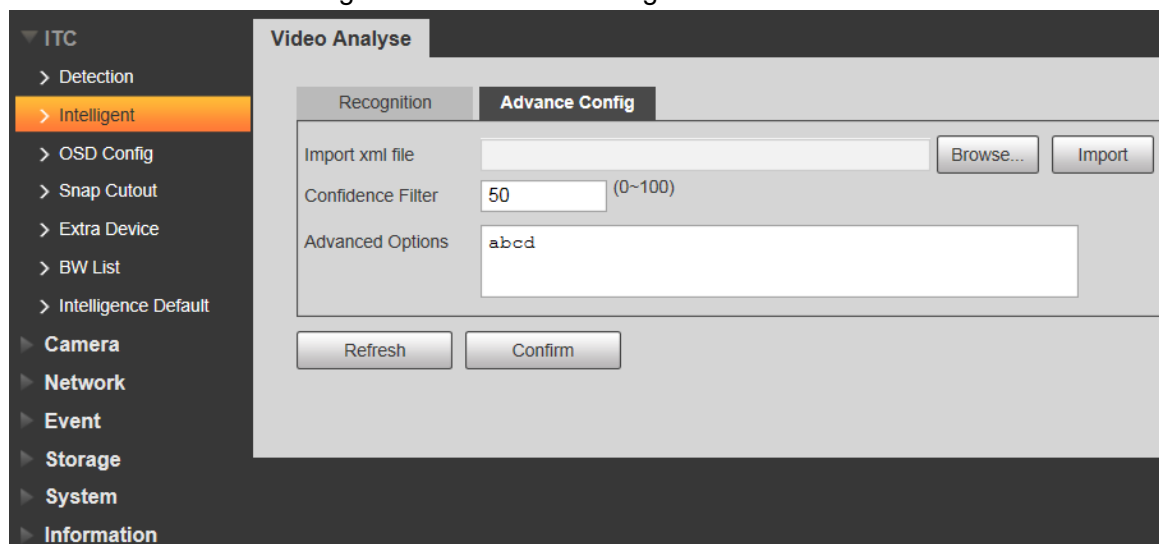
Step 3 Click **Confirm**.

#### 4.5.1.2.2 Advance Configuration

In this section, you can configure the advanced functions of plate recognition and customize special functions.

Step 1 Select Setup > ITC > Intelligent > Video Analyse > Advance Config.

Figure 4-35 Advance configuration



Step 2 Configure the parameters.

Table 4-16 Advance configuration parameters description

Parameter	Description
Import xml file	Import algorithm configuration file as needed. Click <b>Browse...</b> to select the path where the file is stored, and then click <b>Import</b> to import the file.
Confidence Filter	<p>Set the range of limiting plate recognition condition, adjustment range is from 0 to 100.</p> <p>The lower the confidence level is, the less limited conditions there will be, and correspondingly the plate is easier to be recognized and false capture rate becomes higher as well.</p> <p>The higher the confidence level is, the more limited conditions there will be, and correspondingly the plate is harder to be recognized and false capture rate becomes lower as well.</p>
Advanced Options	Enters customized algorithm expression and realize customized special function.

Step 3 Click **Confirm**.

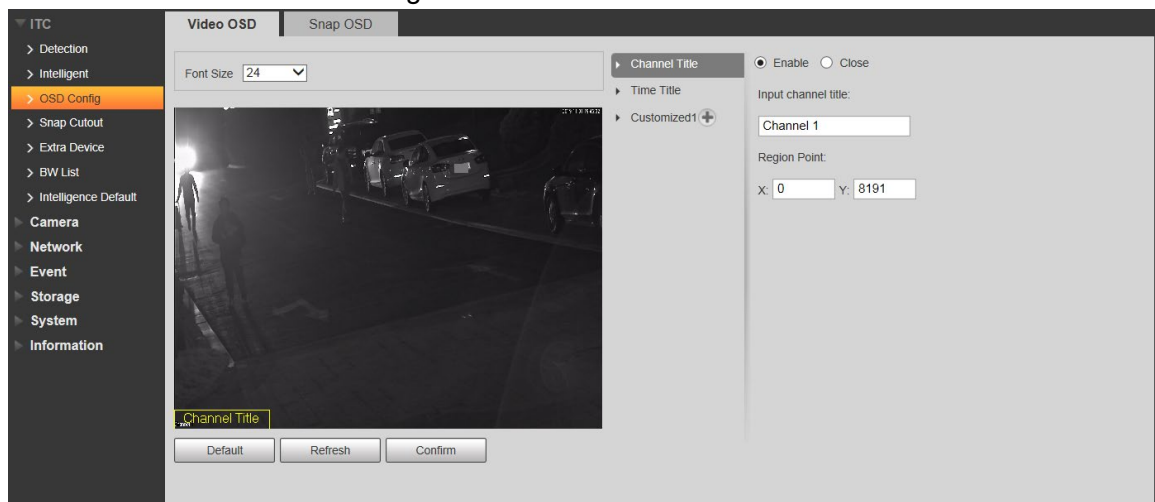
## 4.5.1.3 OSD Configuration

### 4.5.1.3.1 Video OSD

Set OSD information of video channel.

Step 1 Select Setup > ITC > OSD Config > Video OSD.

Figure 4-36 Video OSD



Step 2 Select Font Size.


Step 3 Set channel title and location.

- 1) Click Channel Title.
- 2) Select **Enable**.
- 3) Enter channel name into the **Input channel title** box.
- 4) Drag the yellow box or enter coordinate directly and then set the location of channel title.

Step 4 Set time title and location.

- 1) Click Time Title.

- 2) Select Enable and Week Display.
- 3) Drag yellow box or enter coordinate directly and then set the location of time title.

**Step 5** Click **Customized1** , add customized region, and set OSD information and its display location according to requirement.



The system supports up to 6 customized regions.

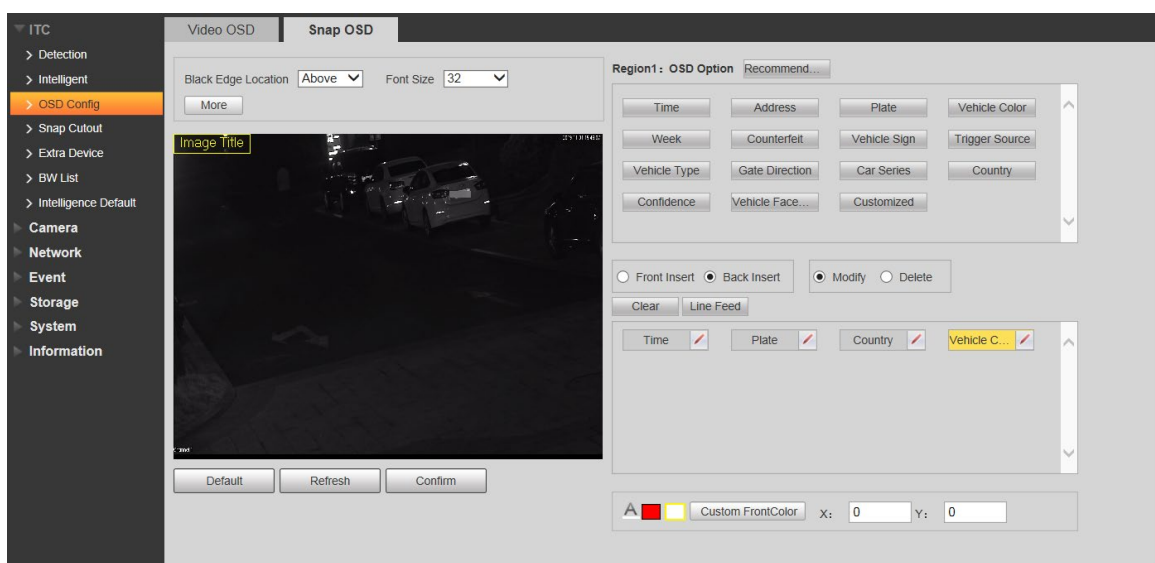
**Step 6** Click **Confirm**.

#### 4.5.1.3.2 Snap OSD

You can set OSD information of pictures.

**Step 1** Select Setup > ITC > OSD Config > Snap OSD.

Figure 4-37 Snap OSD



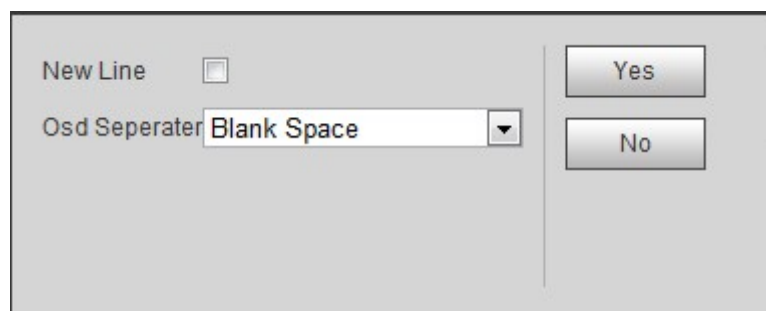
**Step 2** Move the title box to displayed location, or manually enter coordinate value into the X/Y box in the lower right corner of the interface.

**Step 3** Select **Black Edge Location**, and then you can set the position of the OSD black strip. You can select from **Above**, **Below**, and **None**.

**Step 4** Set font size of OSD information. You can set font color of picture OSD information in the right corner of the interface.

**Step 5** Click **More**.

Figure 4-38 New line and OSD separator







**Step 6** Select the **New Line** check box as need, and then set separator types of OSD information.



You can manually enter other separators when selecting **Customized** from **OSD Separator**.

Step 7 Set OSD Option.

Table 4-17 Snap OSD parameters description

Parameter	Description
Front Insert	Select one OSD option, click <b>Insert Front</b> and select other OSD options. The new OSD options will be displayed in front of original OSD option.
Back Insert	Select one OSD option, click <b>Insert Back</b> and select other OSD options. The new OSD option will be displayed behind the original OSD option.
Modify	Click it and all the OSD information status is displayed as  except line feed. Click  to modify the prefix, suffix, content and separator of corresponding OSD option.
Delete	Click it and all the selected OSD information status is displayed as  , click  to delete corresponding OSD option.
Clear	Delete all the OSD information.
Line Feed	After selecting some OSD information, click <b>Line Feed</b> , and OSD information will be displayed on the picture.

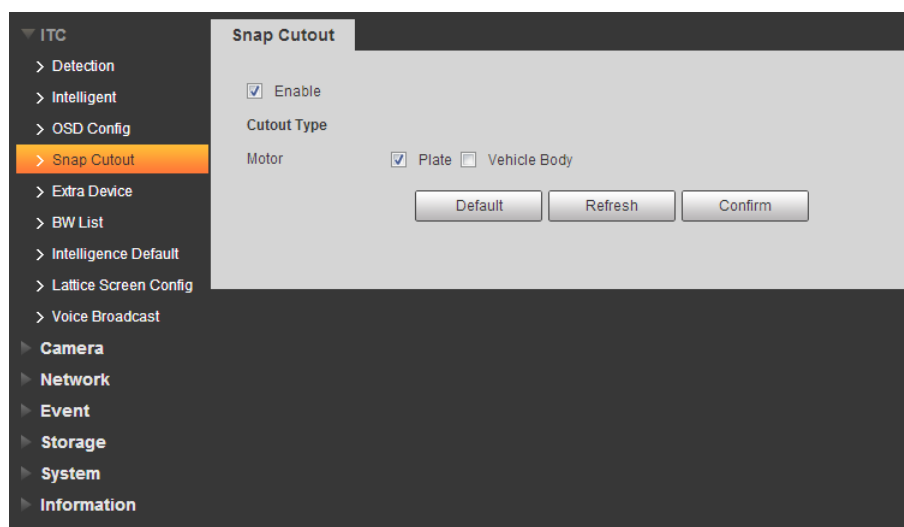
Step 8 Click **Confirm**.

#### 4.5.1.4 Snap Cutout

Enable plate cutout function, and the system will cut out the recognized plate picture and save it to the storage path.

Step 1 Select Setup > ITC > Snap Cutout.

Figure 4-39 Snap cutout



Step 2 Select **Enable** and **Plate** or **Vehicle Body**, and then the function of plate cutout or vehicle body cutout is enabled.

Step 3 Click **Confirm**.

## 4.5.1.5 Extra Device

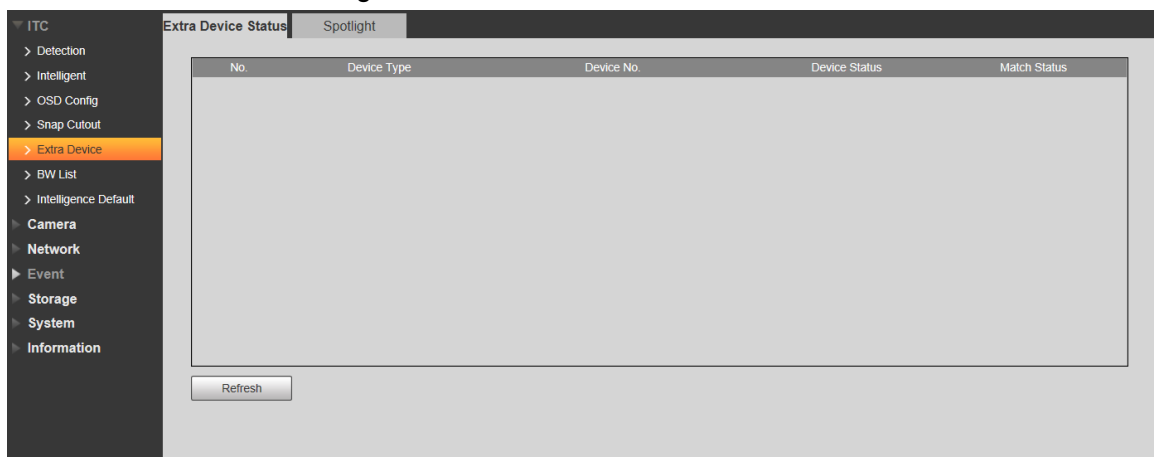
### 4.5.1.5.1 Extra Device Status

You can view the type, number, status and match status of extra device.

If it is connected to vehicle detector and **CarDetect** is selected as **Protocol** from **Setup > ITC > Detection RS485/IO**, then it can detect whether the associated information and status of vehicle detector is normal.

Select **Setup > ITC > Extra Device > Extra Device Status**. The **Extra Device Status** interface is displayed.

Figure 4-40 Extra device status



### 4.5.1.5.2 Spotlight

This section provides guidance on configuring light array and output mode of flashing light.

Step 1 Select Setup > ITC > Extra Device > Spotlight.

Figure 4-41 Spotlight (white light model)

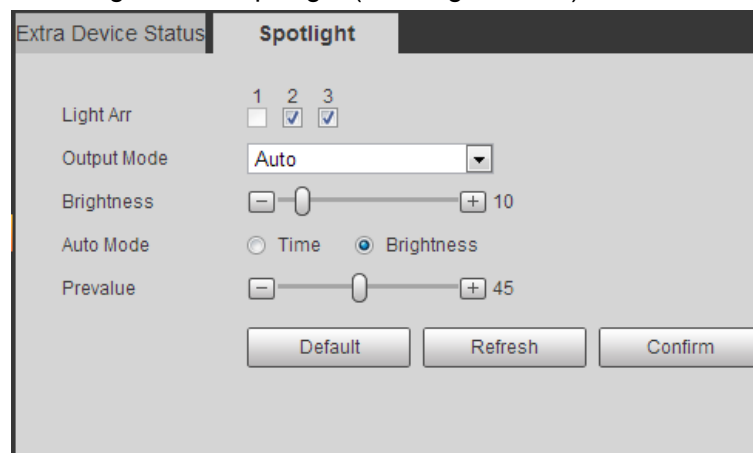
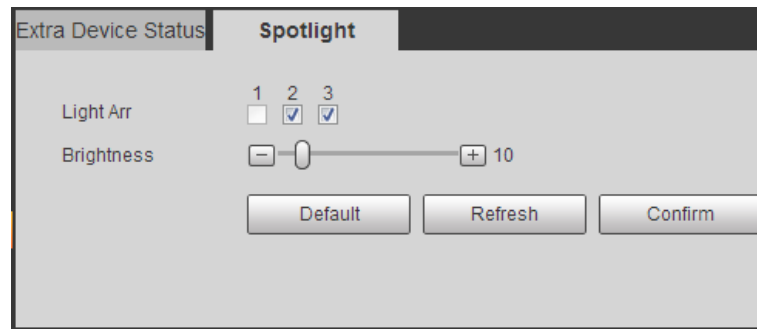




Figure 4-42 Spotlight (IR model)



**Step 2** Configure the parameters as needed.

Table 4-18 Spotlight parameters description

Parameter	Description
Light Arr	There are totally 3 groups optional.
Output Mode	Select the output mode of spotlight. <b>OFF:</b> Spotlight is always off. <b>Always:</b> Spotlight is always on. <b>Auto:</b> Automatically enable spotlight according to time or brightness.  <b>Output Mode</b> setting is only applicable to white light models.
Brightness	Set the brightness value of spotlight. It is 40 by default.
Auto Mode	When <b>Output Mode</b> is <b>Auto</b> , then you can automatically turn on or turn off spotlight according to time or brightness. <b>Time:</b> Set the period during which the spotlight is enabled. Up to 6 periods can be set for each day. <b>Brightness:</b> Set brightness default value. Spotlight is enabled when environmental brightness is lower than the default value, and the spotlight is disabled when it is higher than default value.  <b>Auto Mode</b> setting is only applicable to white light models.

**Step 3** Click **Confirm**.

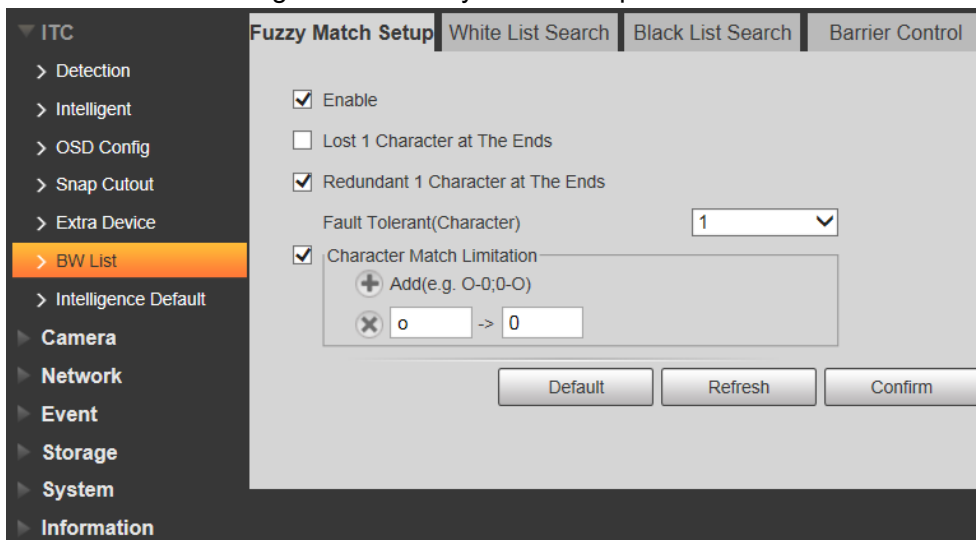
## 4.5.1.6 Block/Allow List

### 4.5.1.6.1 Fuzzy Match Setup

Enable fuzzy match, and set the fuzzy match conditions. The plates which meet the matching conditions will be considered as an allowed list vehicle, and the Camera will automatically open the barrier.


**Step 1** Select Setup > ITC > BW List > Fuzzy Match Setup.

Figure 4-43 Fuzzy match setup



**Step 2** Select the **Enable** check box to enable fuzzy match, and then configure the parameters as needed.

Table 4-19 White list parameters description

Parameter	Description
Lost 1 Character at The Ends	Plate number will be matched when the first or last character of the detected plate is missing.
Redundant 1 Character at the Ends	Plate number will be matched when one more character is detected before the first character or after the last character of the plate.
Fault Tolerant (Character)	Set the fault tolerance value ( <b>0</b> , <b>1</b> , or <b>2</b> ), and plate number will be matched successfully when 0, 1, or 2 characters different from the recorded plate number are detected.
Character Match Limitation	Click  to add the fuzzy match condition. For example, if o is detected by the Camera, the character will be automatically recognized as 0, as shown in the figure above.

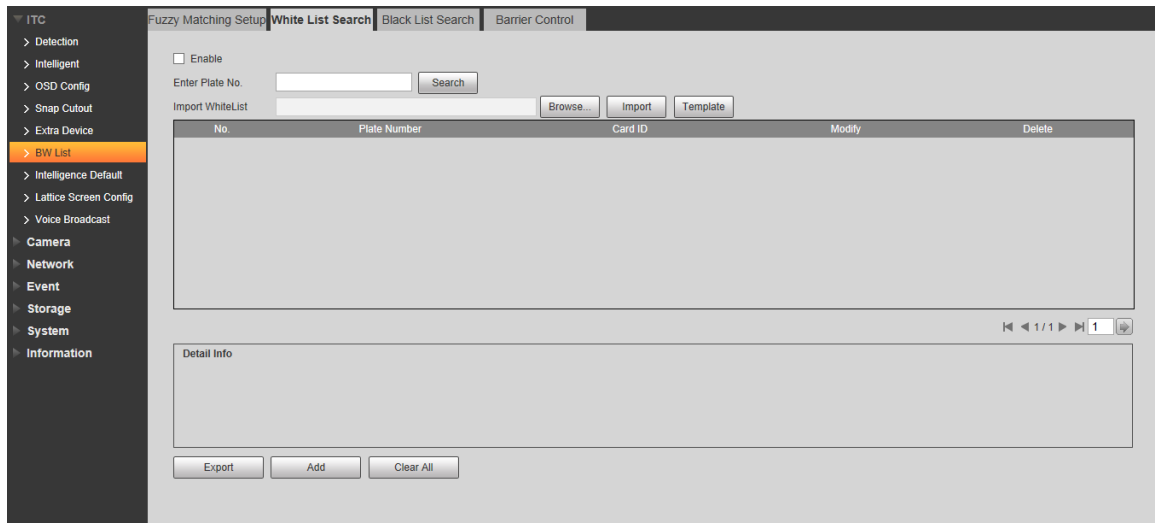
**Step 3** Click **Confirm**.

#### 4.5.1.6.2 Allow List Search

You can search and check whether a plate number is included in the white list, or you can import or export plate number in the allow list.

**Step 1** Select Setup > ITC > BW List > White List Search.

Figure 4-44 Allow List Search



### Step 2 Configure parameters.



- Search plate number: Enter the plate number (enter some characters). Click **Search** and check whether the plate number exists in the white list.
- Modify plate information: Click  of the corresponding plate number searched and modify the plate number. Click **Yes** to complete modification after modification is finished.
- Delete single plate number: Click  of the corresponding plate number searched and delete it from the allow list.
- Delete plate number in batches: click **Clear All** and click **Confirm** in the dialog box to delete all the allow list information.
- Adding vehicles to allow list one by one:
  - 1) Click **Add**.

Figure 4-45 Add

- 2) Enter complete plate number and card ID.
- 3) Set the Begin Time and End Time of the plate number which exists in the allow list.

The vehicle will be no longer considered as an allow list vehicle after it exceeds the time range.

- 4) Enter name of **Owner of Car** (vehicle owner) and select **Gate Mode** (barrier gate) from **No Authorize** (no permission of auto opening barrier) and **Authorize** (auto opening barrier) as needed.



You need to select **Enable barrier control** from **Setup > ITC > BW List > Barrier Control**.

- 5) Select **Continue Adding**, click **Save** and the system will save allow list plate number information and directly enter the adding interface of next white list plate.



You can also cancel selecting **Continue Adding**, and then click **Save** to stop adding further vehicles.

- Exporting vehicles to white list in batches:
  - 1) Click **Export** and it pops up the **Encrypt Config** dialog box.
  - 2) Check **Open** (encrypt) or **Close** (do not encrypt) as needed, and then click **Confirm**. The export file download dialog box pops up.
  - 3) Select the path of storing files. Click **Save** and export white list to local in .csv format, which can be opened in Excel.
- Importing vehicles to white list in batches:
  - 1) Click **Template** to download the template, or open the .csv file you exported, fill in the allow list data which needs to be imported according to template format, and then save the file.
  - 2) Click **Browse...** and select the path where template file exists. Click **Import** and you can import the allow list data into the system in batches.



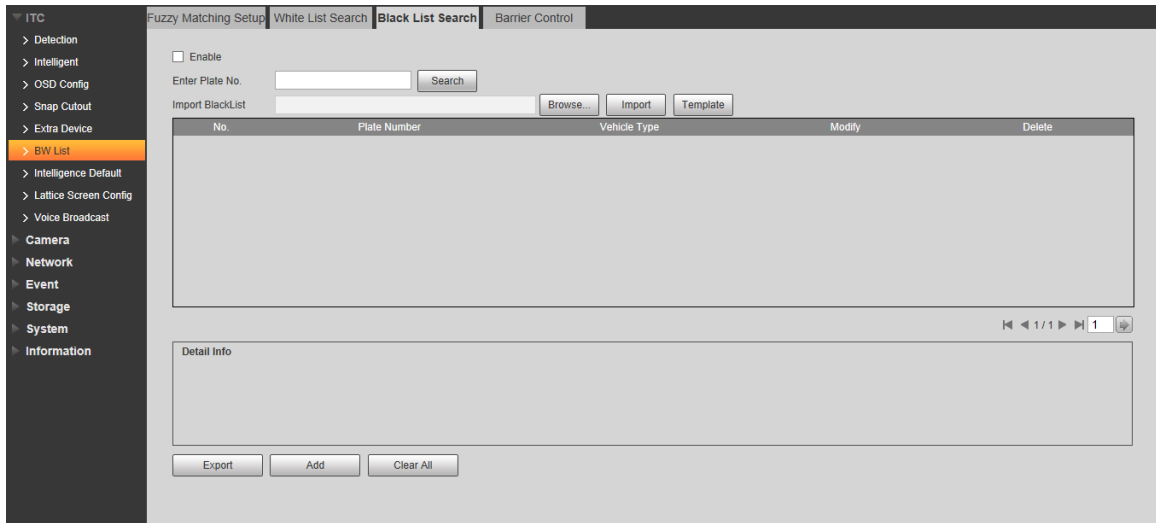
Make sure that the time format in list is in accordance with that of the Camera when importing the allow list.

#### 4.5.1.6.3 Block List Search

You can search and check whether some plate exist in the block list, import and export the block list plate number and vehicle information.

Step 1 Select Setup > ITC > BW List > Black List Search.

Figure 4-46 Block list search



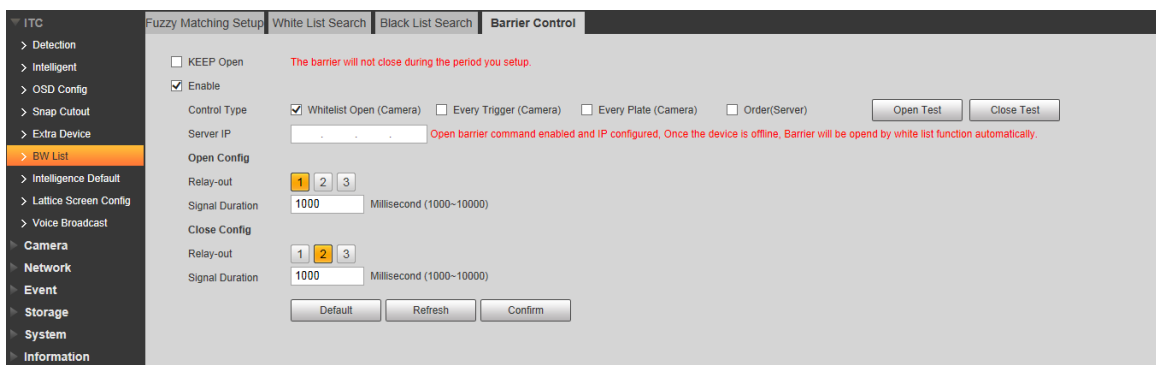
**Step 2** The query, import, and export of black list is similar to those of the allow list. See "4.5.1.6.2 White List Search" for more details.

#### 4.5.1.6.4 Barrier Control

You can set the barrier control mode, and configure information of opening and closing barrier.

**Step 1** Select Setup > ITC > BW List > Barrier Control.

Figure 4-47 Barrier control



**Step 2** Configure the parameters.

Table 4-20 Barrier control parameter description

Parameter	Description
KEEP Open	Select it and enable the function of barrier normally on. Configure the period of barrier normally on. The barrier will not close during the defined period.
Enable	Select it to enable barrier control and configuration.
Control Type	It can trigger alarm through different barrier modes. <b>Whitelist Open (Camera)</b> : Capture the vehicle which conforms to the allow list or fuzzy matching and then output open barrier signal. <b>Every Trigger (Camera)</b> : Capture any vehicle and output open barrier signal. <b>Every Plate (Camera)</b> : Capture any plated vehicle and output open barrier signal. <b>Order (Server)</b> : Platform issues command and output open barrier signal.
Server IP	After enabling open barrier command and configuring IP, if the device is offline, barrier will be opened by white list function automatically.
Open Test	Click the button and manually trigger outputting signal of opening barrier.
Close Test	Click the button and manually trigger outputting signal of closing barrier.
Open Config	<b>Relay-out</b> : Activate alarm linkage output port. You can select anyone one of the three ports.
Close Config	<b>Signal Duration</b> : It is the time for which the open barrier or close barrier signal is going to last.

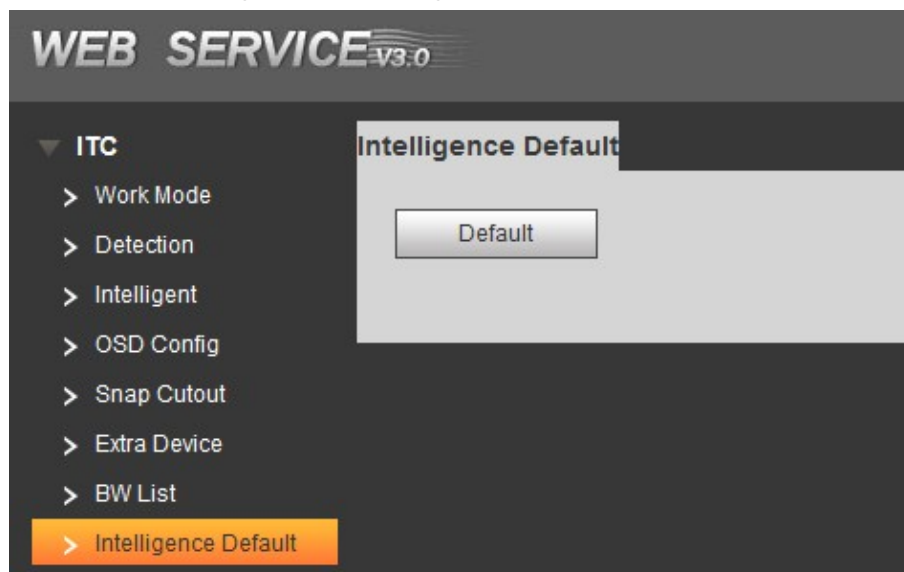
Step 3 Click **Confirm**.

### 4.5.1.7 Intelligence Default

This section provides guidance on restoring capture settings and intelligent parameters to default settings.

Step 1 Select Setup > ITC > Intelligent Default.

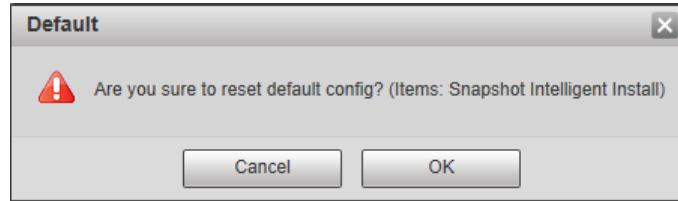
Figure 4-48 Intelligence default



Step 2 Click **Default**.



Figure 4-49 Default



**Step 3** Click **OK**.

## 4.5.2 Camera

You can configure image, video, and stream parameters.

### 4.5.2.1 Attribute

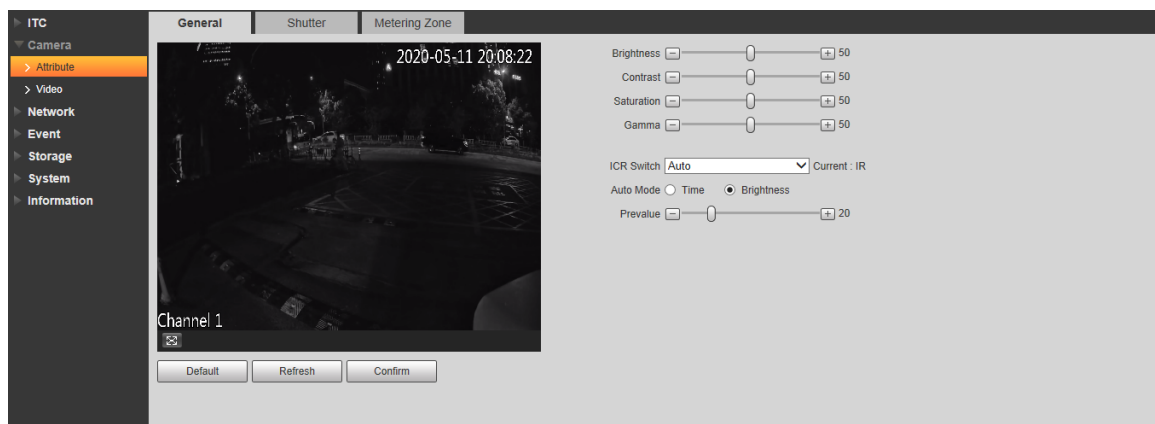
You can adjust the brightness, contrast, saturation of the video image, and set shutter parameters to get clear videos and recordings that you want.

#### 4.5.2.1.1 General

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

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


Figure 4-50 General Settings



**Step 2** Configure the parameters.

Table 4-21 General parameters description

Parameter	Description
Brightness	<p>Adjust the overall image brightness. Change the value when the image is too bright or too dark.</p> <p>The bright and dark areas will have equal changes. The image becomes blurry when the value is too big. The recommended value is from 40 to 60. The range is from 0 to 100.</p> <p>It is 50 by default. The bigger the value is, the brighter the image becomes.</p>

Parameter	Description
Contrast	<p>Change the value when the image brightness is proper but contrast is not enough.</p> <p>If the value is too big, the dark area is likely to become darker and the bright area is likely to be overexposed.</p> <p>The picture might be blurry if the value is set too small. The recommended value is from 40 to 60 and the range is from 0 to 100.</p> <p>It is 50 by default. The bigger the value is, the more obvious the contrast between the bright area and dark area will become.</p>
Saturation	<p>Adjust the color vividness and will not influence the image overall brightness. The image becomes too flamboyant if the value is too big.</p> <p>The image is not flamboyant enough if the value is too small. The recommended value is from 40 to 60 and the range is from 0 to 100.</p> <p>It is 50 by default. The bigger the value is, the more flamboyant the image becomes.</p>
Gamma	<p>Adjust the image hue. For example, change red into blue. The default value is made by the light sensor and normally it doesn't have to be adjusted. The recommended value is from 40 to 60 and the range is from 0 to 100.</p> <p>It is 50 by default. The threshold is used to adjust image hue and it will not influence image overall brightness.</p>
ICR Switch	<p><b>Auto:</b> Set time or brightness value. It will realize auto switch when it exceeds the defined time or value.</p> <p><b>IR:</b> The filter is switched to IR mode when the image is black and white.</p> <p><b>CPL:</b> The filter is switched to general mode when the image is color.</p> <p></p> <p>ICR Switch is only available for IR models.</p>
Prevalue	<p>Prevalue of brightness. You can drag the slider to adjust the value. The higher the value, the brighter the video image.</p>

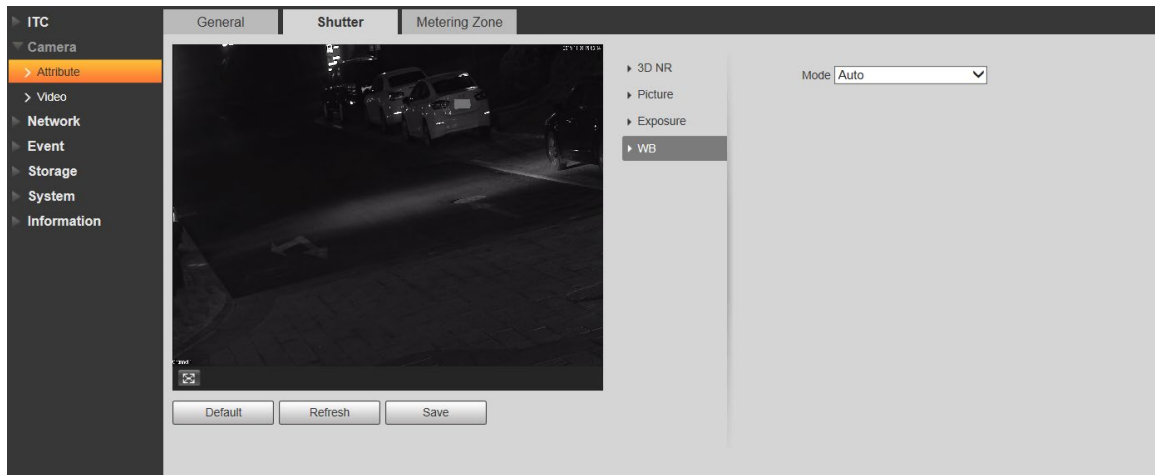
Step 3 Click **Confirm**.

#### 4.5.2.1.2 Shutter

This section provides guidance on configuring camera shutter, including shutter mode, exposure mode, gain mode, and scene mode.



Step 1 Select Setup > Camera > Attribute > Shutter.


Figure 4-51 Shutter



**Step 2** Configure parameters. See Table 4-22.

Table 4-22 Shutter parameters description

Parameter	Description
3D NR	
Video Tridim Denoise	When it is <b>On</b> , 3D NR is enabled to reduce noise of video.
Video Spatial	Spatial video denoising. The higher the value, the fewer the noise.
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.
WDR	Select <b>On</b> to enable WDR (wide dynamic range), which helps provide clear video images in bright and dark light.
Exposure	
Iris Type	Displays the detected iris type.
Iris Adjust Mode	Select the way of adjusting exposure mode. You can select from <b>Manual</b> and <b>Auto</b> .
Mode	
Shutter	 <p>You need to set shutter when <b>Manual</b> is set as <b>Mode</b>. You can select the shutter value, or select <b>Customized Range</b>, and then set the shutter range.</p>
Shutter Scope	 <p>You need to set shutter when <b>Customized Range</b> is set as <b>Shutter</b>. Set the time range of shutter.</p>

Parameter	Description
Gain Scope	 <p>You need to set gain scope when <b>Manual</b> is set as <b>Mode</b>. Set the value range of gain.</p>
WB	
Mode	Set scene mode to adjust the image to its best status.

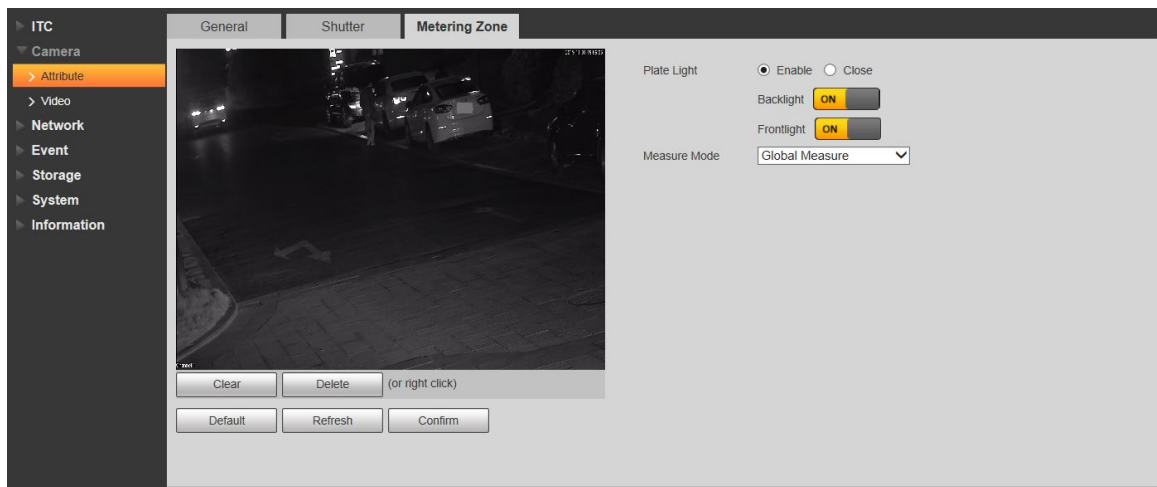
**Step 3** Click **Save**.

#### 4.5.2.1.3 Metering Zone

This section provides guidance on setting the measure mode of metering zone.

**Step 1** Select Setup > Camera > Attribute > Metering Zone.

Figure 4-52 Metering Zone



**Step 2** Configure the parameters.

Table 4-23 Metering zone parameter description

Parameter	Description
Plate Light	When selecting <b>Enable</b> , you can turn <b>ON</b> or <b>OFF</b> backlight and frontlight according to scene requirement, and then improve the backlight image brightness.
Backlight	
Frontlight	
Measure Mode	<p>Global Measure: Measure the brightness of the whole image area and intelligently adjust the overall image brightness.</p> <p>Partial Measure: Measure the brightness of sensitive area and intelligently adjust the overall image brightness. If the measured area becomes bright, then the whole area becomes dark, and vice versa.</p> <p>Drag to select the measured area and the system displays yellow box. Drag the box to proper location, and then click <b>Confirm</b> to complete configuration.</p>

**Step 3** Click **Confirm**.

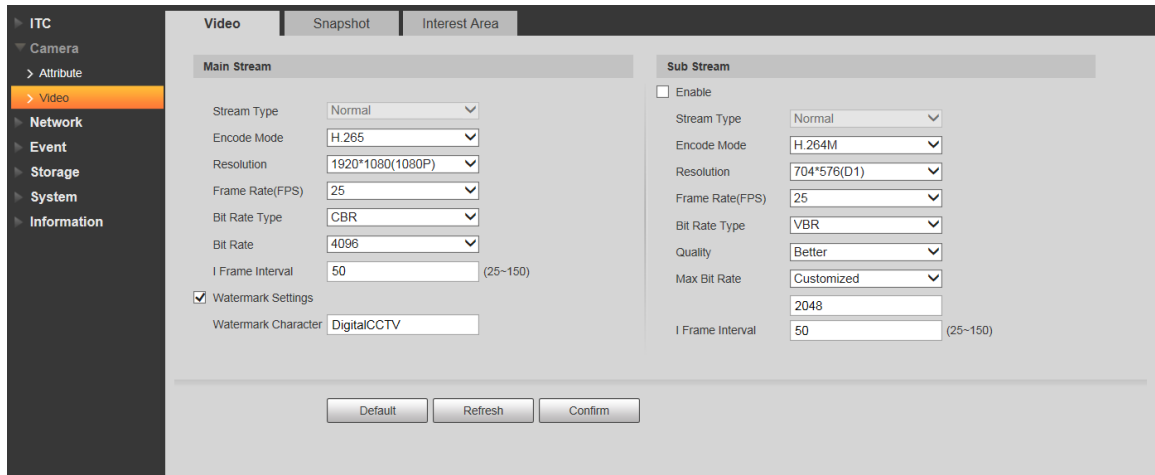
## 4.5.2.2 Video

### 4.5.2.2.1 Video

You can set the camera stream information.

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


Figure 4-53 Video



**Step 2** Configure the parameters.

Table 4-24 Video parameters description

Parameter	Description	
Main Stream	Stream Type	Currently it supports normal stream.
	Encode Mode	Currently it only supports H.264B, H.264M, H.264H, H.265 and MJPEG.
	Resolution	Select resolution according to the actual situation.
	Frame Rate(FPS)	Select frame rate according to the actual situation.
	Bit Rate Type	Include VBR and CBR. Image quality can be set only in VBR mode while it cannot be set in CBR mode.
	Bit Rate	The value is the upper limit of the stream in VBR mode while it is fixed in CBR mode.
	I Frame Interval	P frame quantity between two I frames, it is max 150. The system default is set twice as big as frame rate.
Watermark Settings	You can view if the video is tampered through verifying watermark character. Select <b>Watermark Settings</b> and enable the function. <b>Watermark Character</b> 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.
	Stream Type	Currently it only supports general stream.

Parameter	Description
Encode Mode	Currently it only supports H.264B, H.264M, H.264H, H.265 and MJPEG.
Resolution	Currently it only supports 720P, D1 and CIF.  The resolution of sub stream cannot be greater than main stream.
Frame Rate(FPS)	Select frame rate according to the actual situation.
Bit Rate Type	Include VBR and CBR. Image quality can be set only in VBR mode while it cannot be set in CBR mode.
Quality	Image quality can be set in VBR mode. There are 6 levels optional.
Max Bit Rate	The value is the upper limit of the stream in VBR mode while it is fixed in CBR mode.
I Frame Interval	P frame quantity between two I frames, it is max 150. The system default is set twice as big as frame rate.

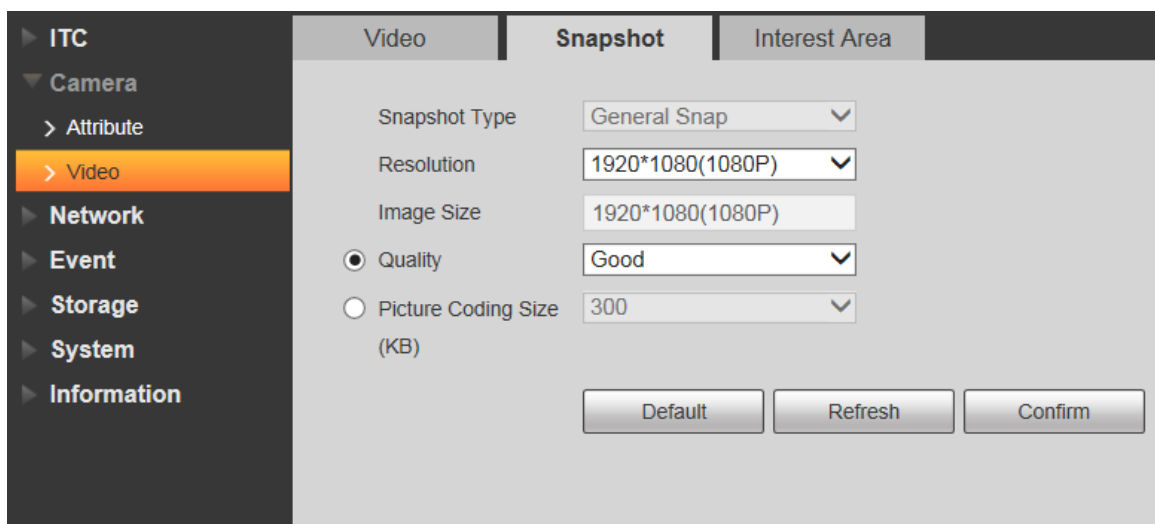
**Step 3** Click **Confirm**.

#### 4.5.2.2.2 Snapshot

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

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


Figure 4-54 Snapshot



**Step 2** Configure the parameters.

Table 4-25 Snapshot parameters description

Parameter	Description
Snapshot Type	Currently it only supports general snapshot.
Resolution	The snapshot resolution.
Image Size	It is in accordance with resolution value.
Quality	Set the snapshot quality which includes 6 levels optional.

Parameter	Description
Picture Coding Size (KB)	Set picture coding size, there are 8 levels optional; or select <b>Customized</b> , the range is from 50 to 1024.  You can select either picture quality or picture coding size to make Settings.

**Step 3** Click **Confirm**.

#### 4.5.2.2.3 Interest Area

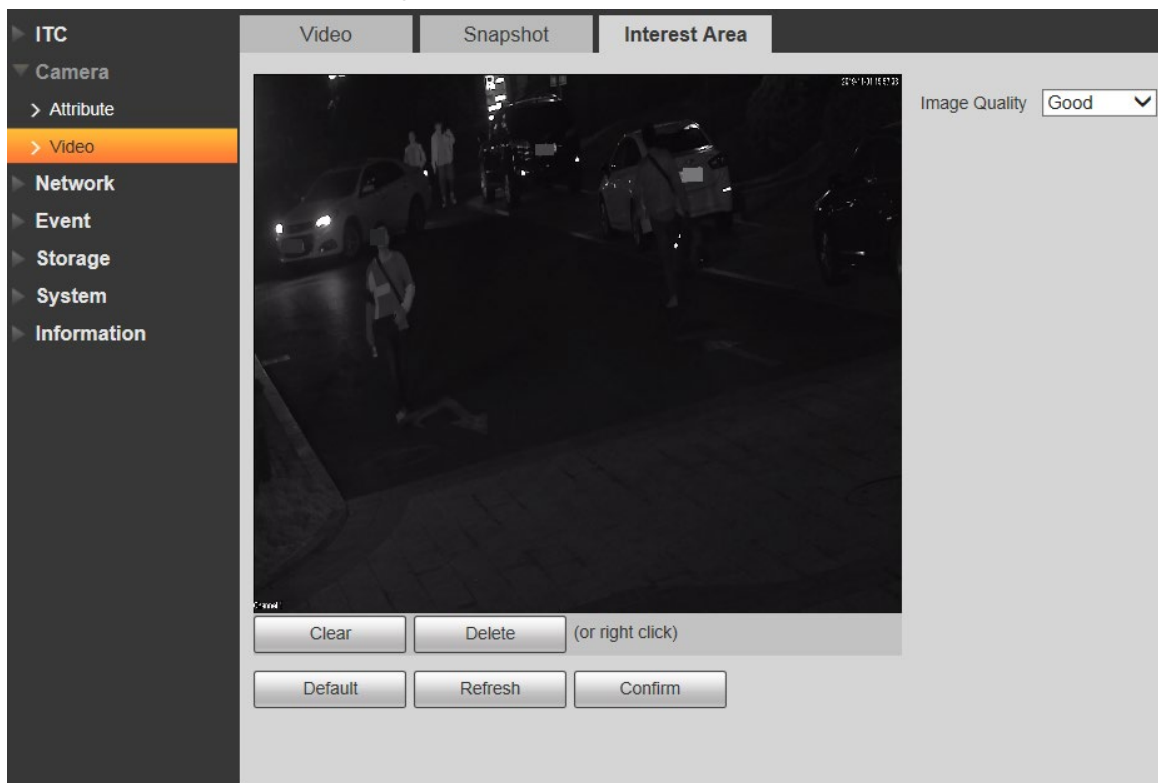
Set interest area in the image, and then the selected image would display with configured quality.



- It supports max 3 regions at the same time.
- The image quality is displayed by level: Worst, Worse, Bad, Good Better, or Best.
- Click **Remove All**, and delete all the area boxes; Select one box, and then click delete or right click to delete it.

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

Figure 4-55 Interest area



**Step 2** Configure parameters. See Table 4-26.

Table 4-26 Interest area parameter description

Parameter	Description
Image Quality	Set snapshot quality which includes 6 levels optional.
Clear	Click it and delete all the configured regions.

Delete	Click it and delete the latest ROI. It can click for several times. Right click any position in the image to realize the same effect.
--------	---------------------------------------------------------------------------------------------------------------------------------------

Step 3 Click **Confirm**.

## 4.5.3 Network

You can set IP address, port and other parameters.

### 4.5.3.1 TCP/IP

You need to configure the IP address of the Camera and DNS server. Make sure that it is connected to other devices in the network.



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

Step 1 Select Setup > Network > TCP/IP.

Figure 4-56 TCP/IP

Step 2 Configure the parameters.

Table 4-27 TCP/IP parameter description

Parameter	Description
Host Name	Enter a name for the host device. Maximum 15 characters are supported.



Parameter	Description
Ethernet Card	Select the Ethernet card. The default setting is <b>Wire</b> .
Mode	Network mode, including static and DHCP. <ul style="list-style-type: none"> <li>● Static: It needs to manually set IP, subnet mask and gateway.</li> </ul> DHCP: Automatically acquire IP, at this moment IP, subnet mask and gateway cannot be set.
MAC Address	Host MAC address.
IP Version	IP version, including <b>IPv4</b> and <b>IPv6</b> . 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	Alternate IP address of DNS server.

Step 3 Click **Confirm**.

## 4.5.3.2 Connection

### 4.5.3.2.1 Port

You can set the connected port information, it can access device through different protocols or config tool.

Step 1 Select Setup > Network > Connection > Port.

Figure 4-57 Port

Step 2 Configure each port value of the Camera. For more details, see Table 4-28.

Table 4-28 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.

Parameter	Description
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**.

#### 4.5.3.2.2 ONVIF

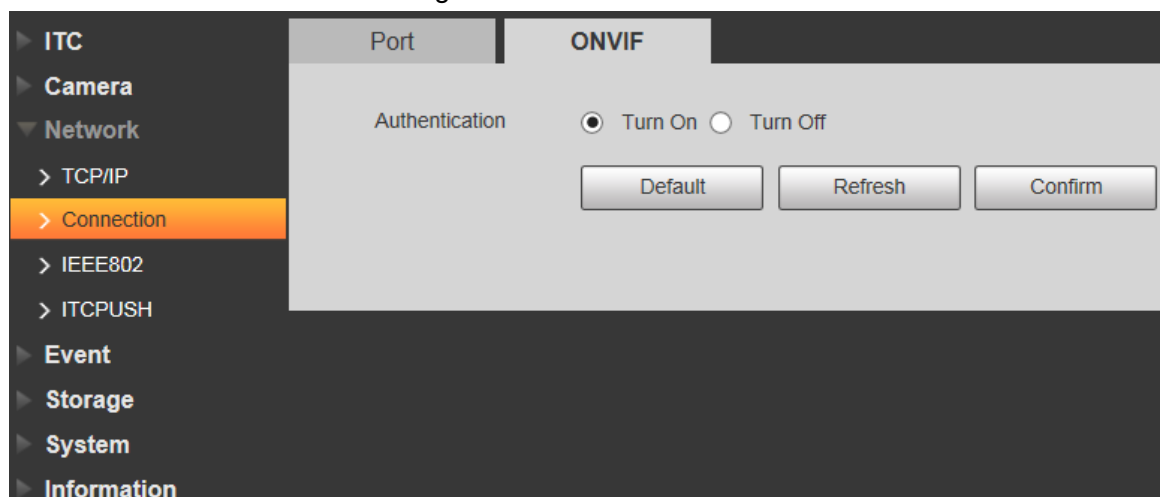
You can enable the Open Network Video Interface Forum (ONVIF) function to make network video products of different manufacturers interworking.



ONVIF login authentication is enabled by default.

**Step 1** Select Setup > Network > Connection > ONVIF.

Figure 4-58 ONVIF



**Step 2** Select the **Turn on** check box.

**Step 3** Click **Confirm**.

#### 4.5.3.3 SMTP (Email)

Configure the email, and when alarms or abnormal events are triggered, an email will be sent to the recipient server through SMTP server. The recipient can log in to the incoming mail server to receive emails.



After this function is enabled, the device data will be sent to the given server. There is data leakage risk.

**Step 1** Select Setting > Network > SMTP (Email).

Figure 4-59 SMTP (email)

**Step 2** Configure the parameters as needed.

Table 4-29 SMTP (Email) parameter description

Parameter	Description
SMTP Server	IP address of the outgoing mail server that complies with SMTP protocol.
Port	Port number of the outgoing mail server complying with SMTP protocol. It is 25 by default.
Username	Username of sender mailbox.
Password	Password of sender mailbox.
Anonymity	For servers supporting anonymous email, you can log in anonymously without entering username, password, and sender information.
Sender	Email address of the sender.
Encryption Type	Select encryption type from <b>None</b> , <b>SSL</b> and <b>TLS</b> .
Title	You can enter no more than 63 characters in English letters and numbers.
Mail Receiver	Email address of the receiver. Supports 3 addresses at most.
Attachment	Select the check box to support attachment in the email.
Interval	The interval of sending emails.
Health Mail	The system sends test mail to check whether the connection succeeds. Select the <b>Health Mail</b> check box, and configure the <b>Update Period</b> , and then the system sends test mails according to the defined period.
Test	Test whether the email function is normal. If the configuration is correct, the email address of the receiver will receive the test email. Save the email configuration before running rest.

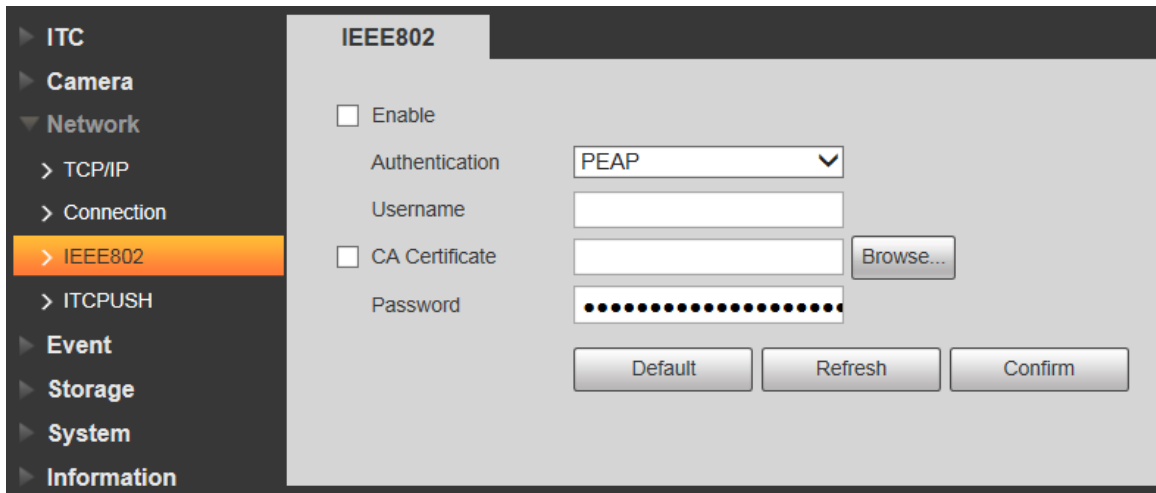
**Step 3** Click **Save**.

#### 4.5.3.4 IEEE802

The IEEE802 standard helps authenticate and secure network by providing authentication for devices trying to connect with other devices on LANs or WANs. You can configure the parameters of the standard to make it work.

**Step 1** Select Setup > Network > IEEE802.

Figure 4-60 IEEE802



**Step 2** Select the **Enable** check box to enable IEEE802, and then configure the parameters.

Table 4-30 IEEE802 parameters description

Parameter	Description
Authentication	Authentication method. <b>PEAP</b> : Ordinarily uses TLS only to authenticate the server to the client, and only the sever is required to have a public key certificate. <b>EAP-TLS</b> : Provides mutual authentication of client to server and server to client. Both the client and the server must be assigned a digital certificate signed by a CA (Certificate Authority) that they both trust.
CA Certificate	Select the <b>CA Certificate</b> check box, and then click <b>Browse</b> to import the CA Certificate to verify whether the switch is valid.
PEAP	
Username	For PEAP method, user authentication is performed by using password-based credentials (username and password).
Password	
EAP-TLS	
Client Certificate	Click <b>Browse</b> to import the client certificate and private key files for authentication.
Private Key	

**Step 3** Click **Confirm**.

### 4.5.3.5 ITC Push

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

**Step 1** Select Setup > Network > ITCPUSH.

Figure 4-61 ITC push configuration

**Step 2** Configure the parameters.

Table 4-31 ITC push

Parameter	Description
Enable	Select the <b>Enable</b> check box to push the passing vehicles information.
No Plate Upload	Select the <b>No Plate Upload</b> check box to push the unlicensed vehicle information.
Username	Username and password for logging to server.
Password	
Web URL	Http URLprefix information of uploaded picture data.
Device ID	Displays Device ID information.
Http Time Out(s)	Timeout of Http push message.
Keep Alive Time(s)	You can set Keep Alive Time.
Character Encoding	Encode mode of push content, which includes UTF8 and GB2312.
Upload List Type	Select the type of list that you want to upload.
Push Picture Config	Select the pushed picture type, and it includes <b>Original Image</b> , <b>Plate Picture</b> , and <b>Vehicle Body Picture</b> .
Upload Info Config	Select the information that you want to upload.

**Step 3** Click **Confirm**.

## 4.5.4 Event

This section provides guidance on configuring alarm and abnormality.

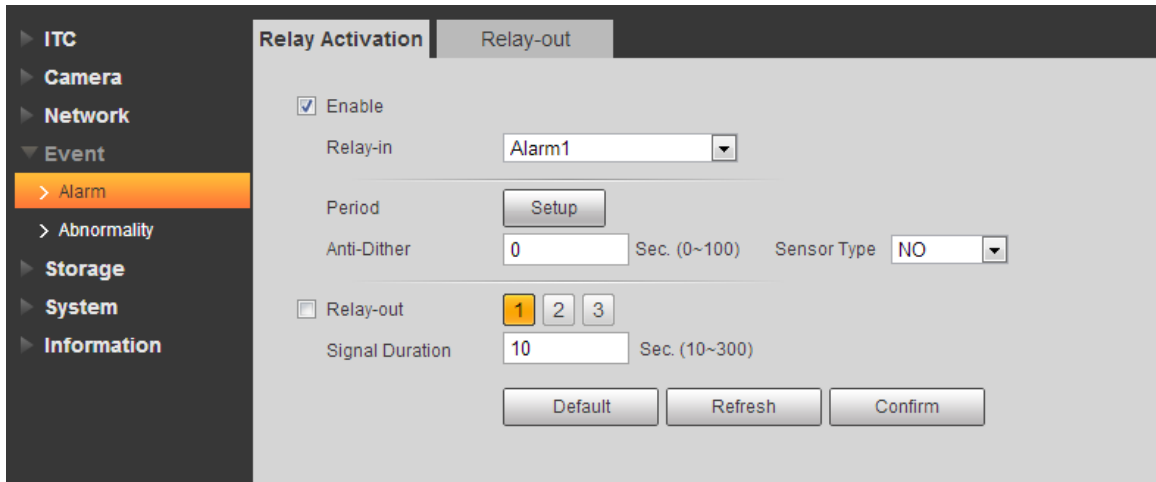
### 4.5.4.1 Alarm

#### 4.5.4.1.1 Relay Activation

You can set several parameters of relay activation such as relay-in, period, anti-dither and sensor type.

**Step 1** Select Setup > Event > Alarm > Relay Activation.

Figure 4-62 Relay activation

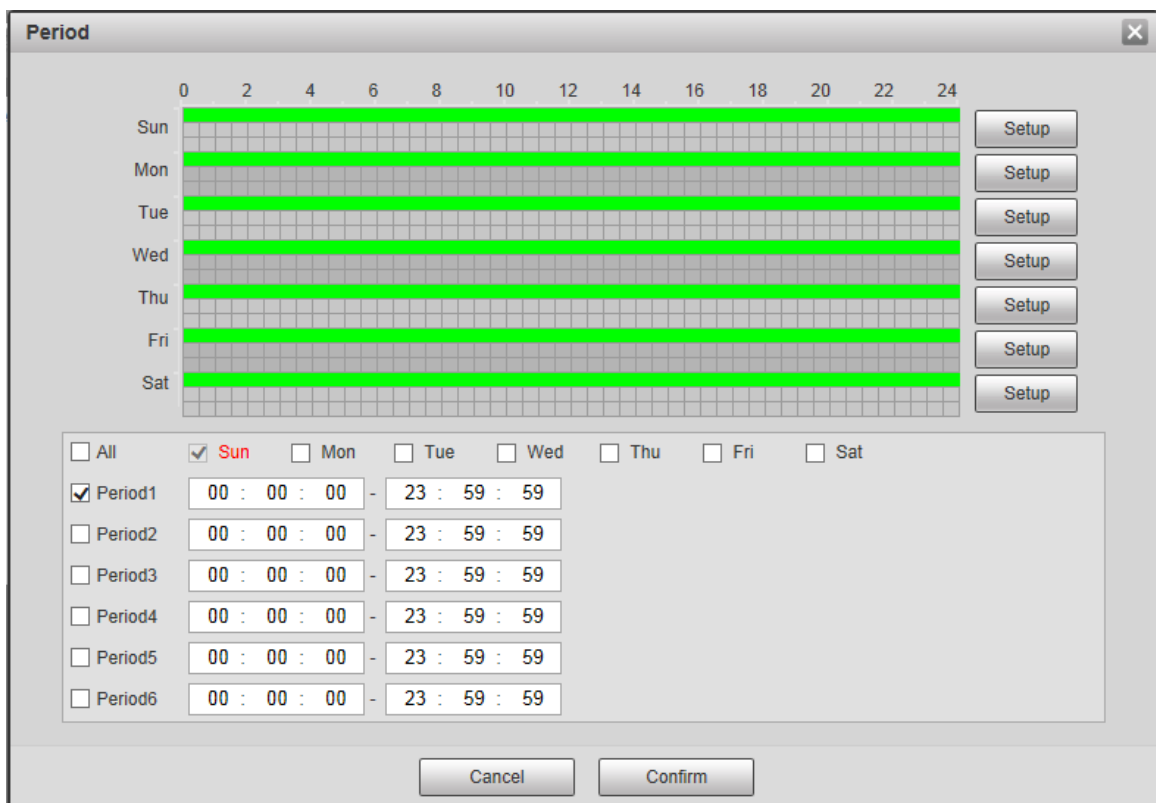


**Step 2** Select the **Enable** check box to enable alarm input for the current channel.

**Step 3** Set the period of alarm input.

- 1) Click **Setup**.

Figure 4-63 Period



- 2) Click **Setup** corresponding to the day you need to configure time period.
- 3) Select the period you need to enable and enter start time and end time of corresponding period.
- 4) If you need to apply this period setting to any other day, select the check box of the corresponding days.
- 5) Click **Confirm** to save the settings.

You can repeat these steps to apply the Settings to other days.

**Step 4** Set other parameters.

Table 4-32 Relay activation parameter

Parameter	Description
Anti-dither	Enter anti-dither time. It ranges from 0s to 100s.
Sensor Type	Select relay-in type according to the connected alarm input device. NO: Low level valid. NC: High level valid.
Relay-out	Optocoupler output, select the check box to activate corresponding alarm output device when alarm occurs.
Signal Duration	The time that delays alarm when alarm occurs.

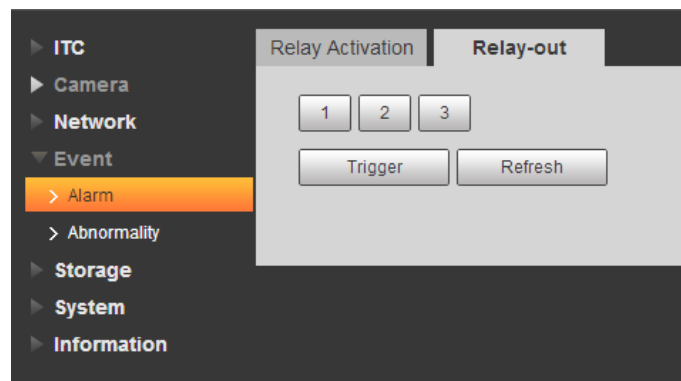
Step 5 Click **Confirm**.

#### 4.5.4.1.2 Relay-out

In this section, you can trigger one alarm output signal.

Step 1 Select Setup > Event > Alarm> Relay-out.

Figure 4-64 Relay-out



Step 2 Click **1**, **2** or **3**, and set 1 channel of alarm channel.

Step 3 Set alarm output.

- Click **Trigger** to output relay-out signal.
- Click **Refresh** to refresh alarm output status.

#### 4.5.4.2 Abnormality

This section provides guidance on setting relay-out mode of different events.

Step 1 Select Setup > Event > Abnormality.

The **Abnormality** interface is displayed. See Figure 4-65, Figure 4-66, Figure 4-67, Figure 4-68, Figure 4-69 and Figure 4-70.

Figure 4-65 No storage card

The screenshot shows the 'SD Card' configuration page with the 'No Storage' event type selected. The 'Relay-out' checkbox is checked, and the signal duration is set to 10 seconds. A red note states: '\*Please note that alarm outputs 1 and 2 are generally used to control the barrier.' Buttons for 'Default', 'Refresh', and 'Confirm' are visible at the bottom.

Figure 4-66 Storage error

The screenshot shows the 'SD Card' configuration page with the 'Storage Error' event type selected. The 'Relay-out' checkbox is checked, and the signal duration is set to 10 seconds. A red note states: '\*Please note that alarm outputs 1 and 2 are generally used to control the barrier.' Buttons for 'Default', 'Refresh', and 'Confirm' are visible at the bottom.

Figure 4-67 Not enough storage space

The screenshot shows the 'SD Card' configuration page with the 'Scarcity of Storage Sp.' event type selected. The 'Capacity Limit' is set to 10% (0-99). The 'Relay-out' checkbox is checked, and the signal duration is set to 10 seconds. A red note states: '\*Please note that alarm outputs 1 and 2 are generally used to control the barrier.' Buttons for 'Default', 'Refresh', and 'Confirm' are visible at the bottom.

Figure 4-68 Camera offline

The screenshot shows the 'Network error' configuration page with the 'Off-line Event' event type selected. The 'Relay-out' checkbox is unchecked, and the signal duration is set to 10 seconds. A red note states: '\*Please note that alarm outputs 1 and 2 are generally used to control the barrier.' Buttons for 'Default', 'Refresh', and 'Confirm' are visible at the bottom.



Figure 4-69 IP conflict

Figure 4-70 Illegal access


Figure 4-71 Security exception

Figure 4-72 Vehicle in the black list

**Step 2** Configure the parameters of each event as needed.

Table 4-33 Abnormality parameters

Parameter	Description
Enable	Check to enable corresponding abnormality event.
Relay-out	Check to enable the corresponding alarm output of abnormality event, and select the corresponding port.

Parameter	Description
Signal Duration	The alarm linkage keeps running for the defined time after alarm ends. The time range is 10s–300s.
Capacity Limit	Configure the storage available that triggers abnormality alarm.
Ethernet Card1, Ethernet Card2	Select the Ethernet card that triggers alarm output.
Max Switch Time Value	Configure the max time that traffic light remains unchanged.  This function is only available in <b>E-Police</b> mode.
Login Error	Configure the number of login error allowed. The range is 3–10 times.
Send Email	The system sends an email to the defined email address when an alarm is triggered. To set the email address, go to <b>Setup &gt; Network &gt; SMTP(Email)</b> .

Step 3 Click **Confirm**.

## 4.5.5 Storage

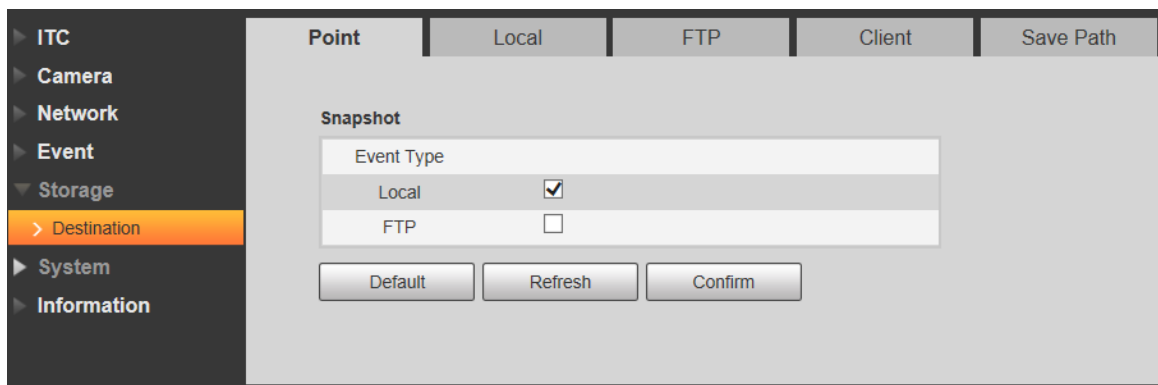
This section provides guidance on setting associated information of storage and record control.

### 4.5.5.1 Point

Set the storage path of snapshot.

Step 1 Select Setup > Storage > Destination > Point.

Figure 4-73 Point



Step 2 Select **Event Type** as needed.

- **Local**: Store into the TF card.
- **FTP**: Store into the FTP server.

Step 3 Click **Confirm**.

### 4.5.5.2 Local

Display the information of local SD card. You can set hot swap and format SD card.

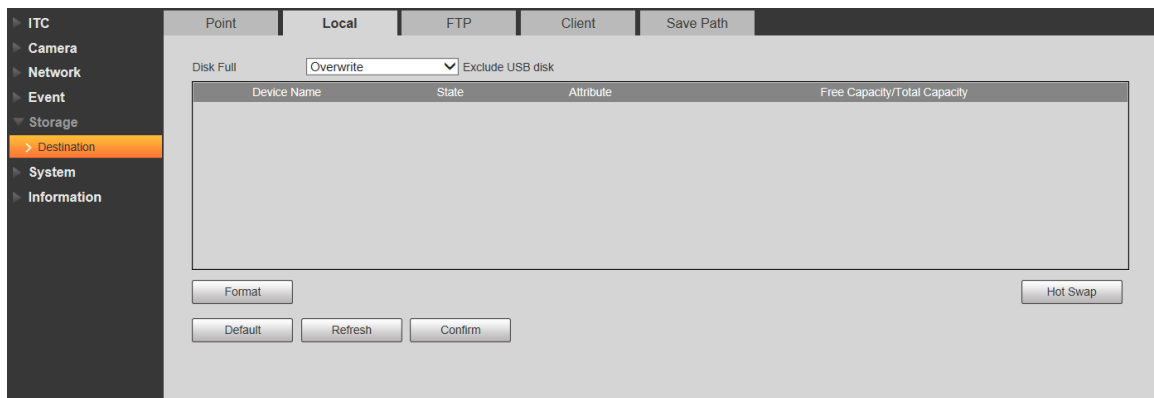


Format the SD card before use.

**Step 1** Select Setup > Storage > Destination > Local.

- Select **Overwrite** or **Stop** from **Disk Full**, meaning overwrite the records or stop storing new pictures or videos respectively when disk is full.
- View the storage information of the card.
- Click **Hot Swap**, and then you can pull out the SD card.
- Click **Format**, and then you can format the SD card.

Figure 4-74 Local



**Step 2** Click **Confirm**.

### 4.5.5.3 FTP

FTP function can be enabled only when it is selected as destination path. When the network does not work, you can save all the files to the internal SD card for emergency.



You can set picture name and storage path. Click **Help...** to view naming rule.

**Step 1** Select Setup > Storage > Destination > FTP.

Figure 4-75 FTP

**Step 2** Configure the parameters.

Table 4-34 FTP parameter

Parameter	Description
Offline Transfer	When the network disconnects or fails, snapshots will be stored in TF card. After the network is restored, the snapshots will be uploaded from the TF card to FTP or client. Make sure that TF card is inserted in the Camera; otherwise, the offline transfer function cannot be enabled.
FTP Named	Set the naming rule of snapshots to be saved in FTP server. You can click <b>Help...</b> to view the <b>Picture Naming Help</b> , or click <b>Restore</b> to restore the default naming rule.
Enable	Enable FTP server storage.
Protocol	<b>SFTP (Recommended)</b> : Secure File Transfer Protocol, a network protocol allows file access and transfer over a secure data stream. <b>FTP</b> : File Transfer Protocol, a network protocol implemented to exchange files over a TCP/IP network. Anonymous user access is also available through an FTP server.
Server IP	The IP address of FTP server.
Encode Mode	Refers to the encode mode of Chinese characters when naming pictures. Two modes are available: <b>UTF-8</b> and <b>GB2312</b> . After configuring <b>Server IP</b> and <b>Port</b> , click <b>test</b> to check whether the FTP server works.
Port	The port number of FTP server.
Username, Password	The username and password of FTP server.
Upload Type	Select event(s) and picture type(s) to be uploaded to the FTP server.

**Step 3** Click **Confirm**.

### 4.5.5.4 Client

You can set the parameters of storing to client.

**Step 1** Select Setup > Storage > Destination > Client.

Figure 4-76 Client

**Step 2** Configure parameters.

Table 4-35 Client

Parameter	Description
Offline Transfer	<p>When network is disconnected or failed, you can store the picture into local storage card and it will automatically upload to platform server after network resumes.</p> <p>When checking <b>Offline Transfer</b>, <b>Manual Upload</b> option will be displayed. Then you can configure Begin Time and End Time, and choose the server to upload.</p>
Type	<p>Select connection type with platform server.</p> <p>IP: Connect to platform server through IP address.</p> <p>MAC: Connect to platform service through MAC address.</p>
Server	<p>Select server which includes Server1 and Server2.</p>
Server IP	<p>When the type is selected as <b>IP</b>, then it has to fill in the server's IP address.</p> <p>When the type is selected as <b>MAC</b>, then it has to fill in the server's MAC address.</p>

**Step 3** Click **Confirm**.

### 4.5.5.5 Path

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

**Step 1** Select Setup > Storage > Destination > Save Path.

Figure 4-77 Storage path

**Step 2** According to your actual requirement, set the name of picture and storage path. See **Help...** for more details.

**Step 3** Set the root path of record and snapshot as needed.

**Step 4** Click **Confirm**.

## 4.5.6 System

You can configure general information, adding user, restoring default settings and configuring import & export file.

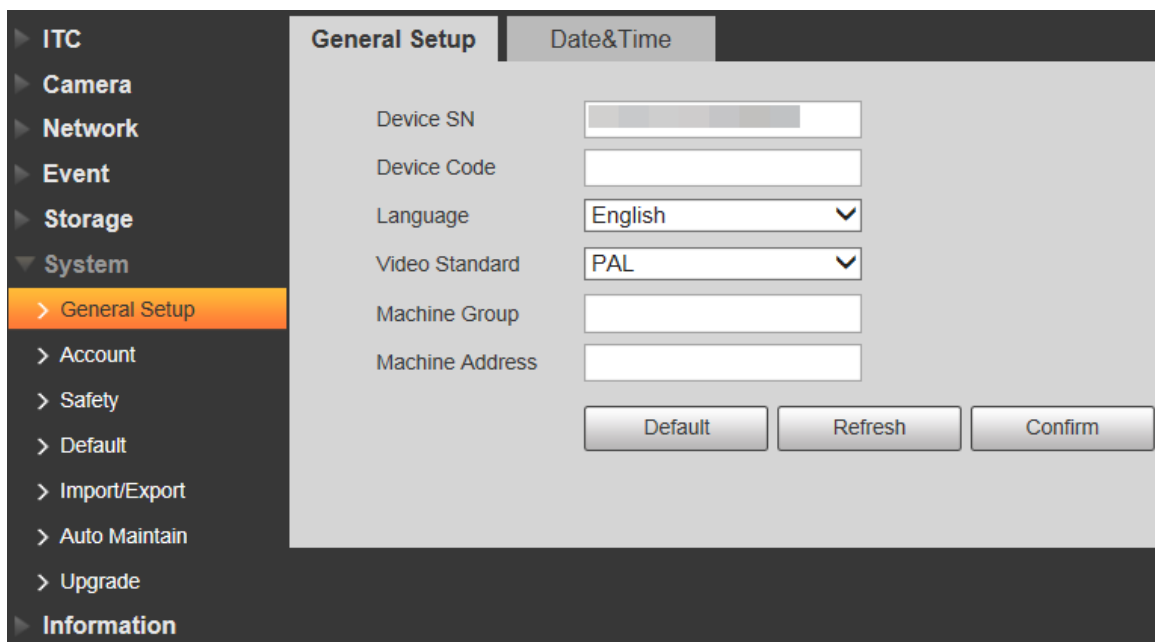
### 4.5.6.1 General

#### 4.5.6.1.1 General

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

**Step 1** Select Setup > System > General Setup > General Setup.

Figure 4-78 General



**Step 2** Configure the parameters.

Table 4-36 General parameters

Parameter	Description
Device SN	The ID number of the Camera. Supports English letters and numbers.
Device Code	Device Code Failed to support OSD information overlay.
Language	The language displayed on web. The language will be automatically switched after logging in web again. Currently it only supports English.
Video Standard	PAL: Phase Alternating Line. Currently most countries around the world (including most countries in Europe, Africa, Australia and China) adopt this standard. NTSC: National Television System Committee. The main countries which adopt this standard include America, Canada, and Japan.
Machine Group	The company group information of the Camera.
Machine Address	Set the location information of device capture.

**Step 3** Click **Confirm**.

#### 4.5.6.1.2 Date & Time

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

**Step 1** Select Setup > System > General > Date & Time.

Figure 4-79 Date &amp; time

The screenshot shows the 'Date & Time' configuration page. On the left is a navigation menu with categories like ITC, Camera, Network, Event, Storage, System, and Information. The 'System' category is expanded to show 'General Setup'. The main area contains the following settings:

- Date Format: YYYY-MM-DD
- Time Format: 24-Hour
- Current Time: 2019-11-01 20 : 12 : 11 (with a 'Sync PC' button)
- DST:  (disabled)
- DST Type:  Date,  Week
- Begin Time: Jan 1 00 : 00 : 00
- End Time: Jan 2 00 : 00 : 00
- NTP Setting:  (disabled)
- Server: clock.isc.org
- Port: 123
- Time Zone: GMT+08:00
- Interval: 10 minute(s) (1~30)

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

**Step 2** Configure the parameters.

Table 4-37 Date &amp; time parameter description

Parameter	Description
Date Format	Select date format.
Time Format	Select 24h or 12h system.
Current Time	Set current system time of the Camera. It becomes valid immediately after setting.
Sync PC	Sync the time of the Camera with the time on PC.
DST	Enable the function, and then set begin time and end time of DST. Set according to date or week.
NTP Setting	Select to enable the function of network time synchronization.
Server	Time server address.
Port	Port number of time server.
Time Zone	The time zone where the Camera is located.
Interval	The sync interval between device and time server.

**Step 3** Click **Confirm**.



## 4.5.6.2 Account

### 4.5.6.2.1 Account

The system supports configuring operation user of web. You need to configure user group before configuring user account.

#### Username



- The user with **Account** control authority can also modify the password of other users.
- It is recommended to give fewer authorities to normal users than premium users in order to make user management convenient.
- Cannot delete the user in login status.

You can add, delete or modify user.

**Step 1** Select Setup > System > Account > Account > Username.

Figure 4-80 Username

Username		Group Name				
No.	Username	Group Name	Memo	Restricted Login	Modify	Delete
1	admin	admin	admin's account	/		

Authority						
User	Live	System	System Info	File Backup	Storage	
Event	Network	Peripheral	AV Parameter	Safety	Maintenance	
Manual Control						

Add User

**Step 2** Click Add User.

Figure 4-81 Add user

**Step 3** Configure the parameters.

Table 4-38 Add user parameters description

Parameter	Description
Username	Username It can only consist of number, letter, underline and hyphen, the maximum length contains 15 characters and it cannot be the same as the existed username.
Password	User's password and confirm password. The password can be set from 8 characters to 32 nonblank characters and contains at least two categories from upper cases, lower cases, numbers and special characters (excluding “'”, “'”, “;”, “.” and “&”)
Confirm Password	Follow the password security prompt to set a high security level password. Password should be the same as Confirm Password.
Group Name	Select the group that new users belong to. Each group has different authorities.
Memo	Remarks on the user.
Operation Permission	Select the permissions that you want assign to the user.
Restricted Login	Set the IP address that is restricted to log in, and the restriction time.

**Step 4** Click **Save**.

The newly added user is displayed in the user list.



- After adding user, click to modify user password, group, memo and authorities; click to delete the added user, admin user cannot be deleted.
- Click in the admin row to modify user name and email address.

**User Group**

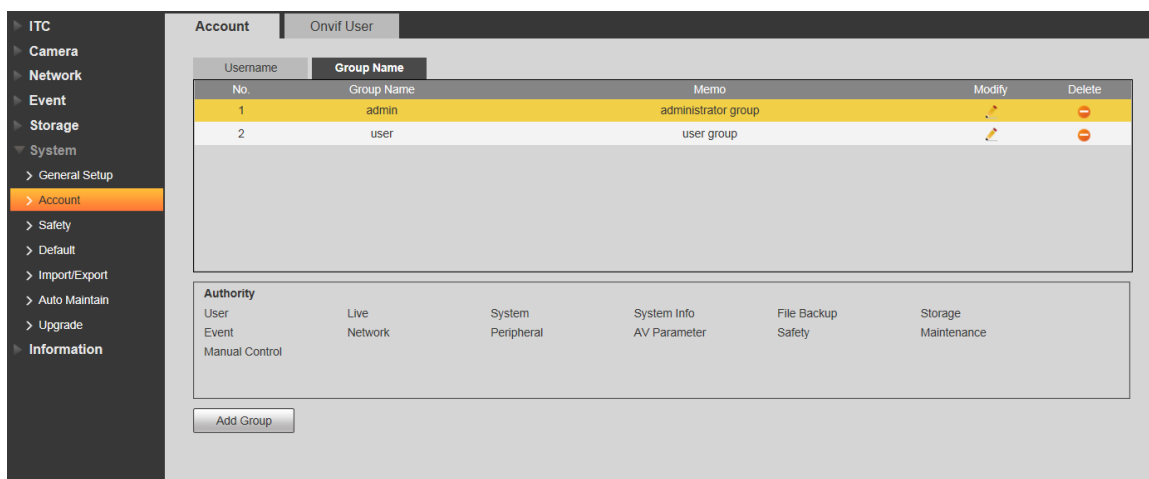
You have two groups named admin and user by default, you can add new group, delete added group or modify group authority and memo.

**Step 1** Select Setup > System > Account > Account > Group Name.



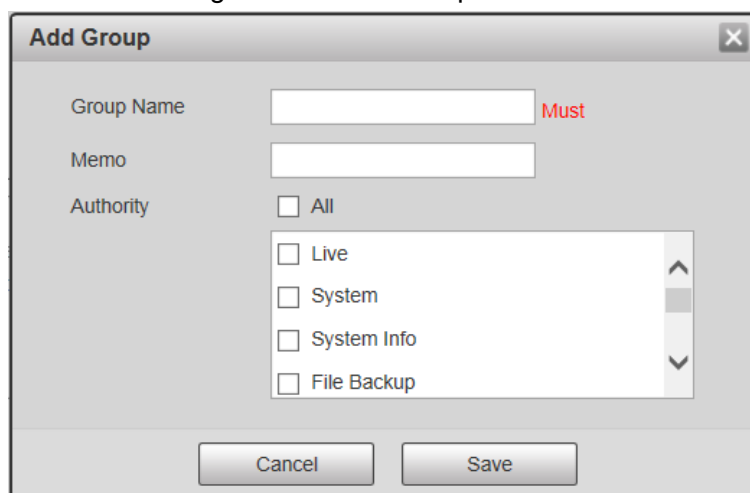
- The system supports max 8 user groups and the default initialization user groups are **admin** and **user**.
- You can modify and delete the added user group, but not the initialization user group.

Figure 4-82 User group



**Step 2** Click Add Group.

Figure 4-83 Add Group



**Step 3** Enter the name of user group and configure group authority.



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

**Step 4** Click **Save**.

The newly added group is displayed in the group list.



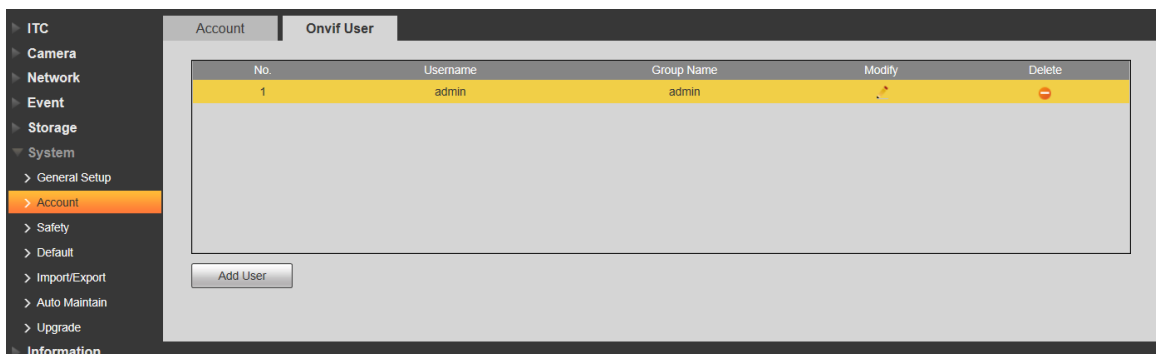
- After adding group, click to modify group memo or authorities; click to delete the added group, admin group and user group can not be deleted.
- Click in the row of admin group or user group to modify group memo.

#### 4.5.6.2.2 ONVIF User

You can add, delete, modify Onvif (Open Network Video Interface Forum) on the user management interface.

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

Figure 4-84 Onvif user



**Step 2** Click Add User.

Figure 4-85 Add user

**Step 3** Configure the parameters.




Table 4-39 User parameter description

Parameter	Description
Username	User's unique identification. You cannot use existing user name.
Password	User's password and confirm password.
Confirm Password	The password can be set from 8 characters to 32 nonblank characters and contains at least two types from upper case, lower case, number and special characters (excluding ' " ; : &) Follow the password security notice to set a high security level password. The new password should be in accordance with the confirm password.
Group Name	The group that users belong to. Each group has different authorities.

**Step 4** Click **Save**.

The newly added user is displayed in the user list.



- After adding user, click  to modify user password, group, memo and authorities; click  to delete the added user, admin user cannot be deleted.
- Click  in the admin row to modify user name and email address.

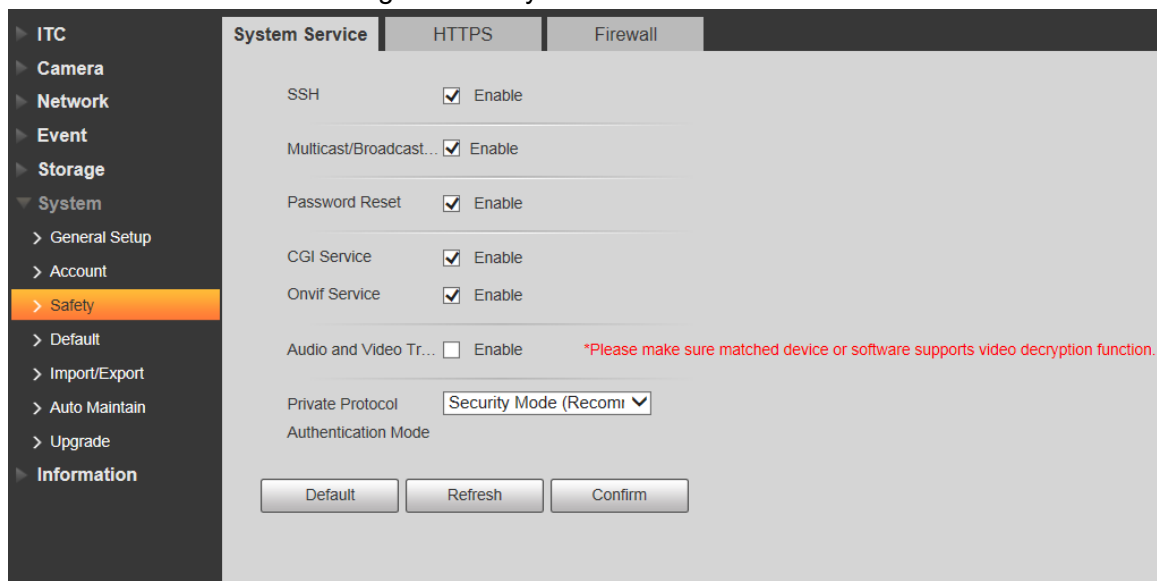
### 4.5.6.3 Safety

#### 4.5.6.3.1 System Service

Select the system service which needs to be enabled according to actual requirement.

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

Figure 4-86 System Service



**Step 2** Select needed system service.

Table 4-40 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	Multicast: It realizes point-to-multipoint network connection between sender and receiver. Broadcast: 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 password reset function.
CGI Service	CGI is the port between external application program and web server.
Onvif Service	It realizes network video framework agreement to make different network video products interconnected.
Audio and Video Transmission Encryption	It needs to be encrypted during audio and video transmission. Make sure that the device or software supports video decryption function.
Private Protocol Authentication Mode	Keep the recommended <b>Security Mode</b> .

Step 3 Click **Confirm**.

#### 4.5.6.3.2 HTTPS



- 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 it replaces the PC which logs in to the web interface, then it needs to download and install the root certificate again on the new PC or copy the downloaded root certificate on the new PC and install.

On the **HTTPS** interface, users 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.

Step 1 Create certificate or upload the authenticated certificate

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

Figure 4-87 HTTPS (1)

- 2) Select Enable HTTPS and Enable TLSv1.0, and then click Create.

Figure 4-88 HTTPS (2)

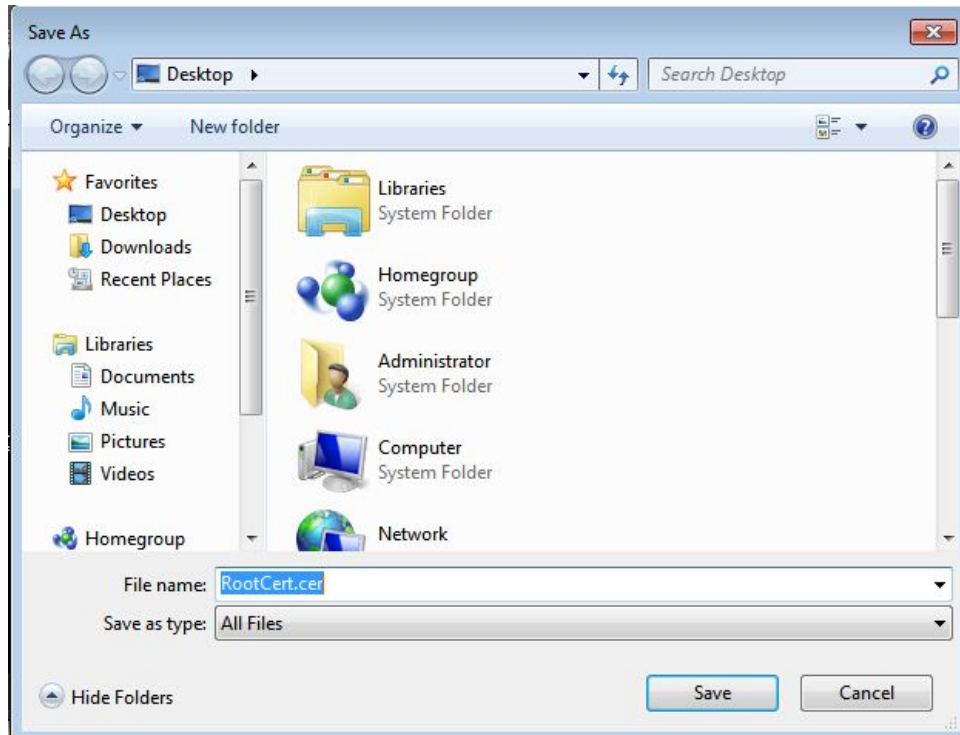
- 3) Enter the required information such as region, IP or domain name, and then click **Create**.



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

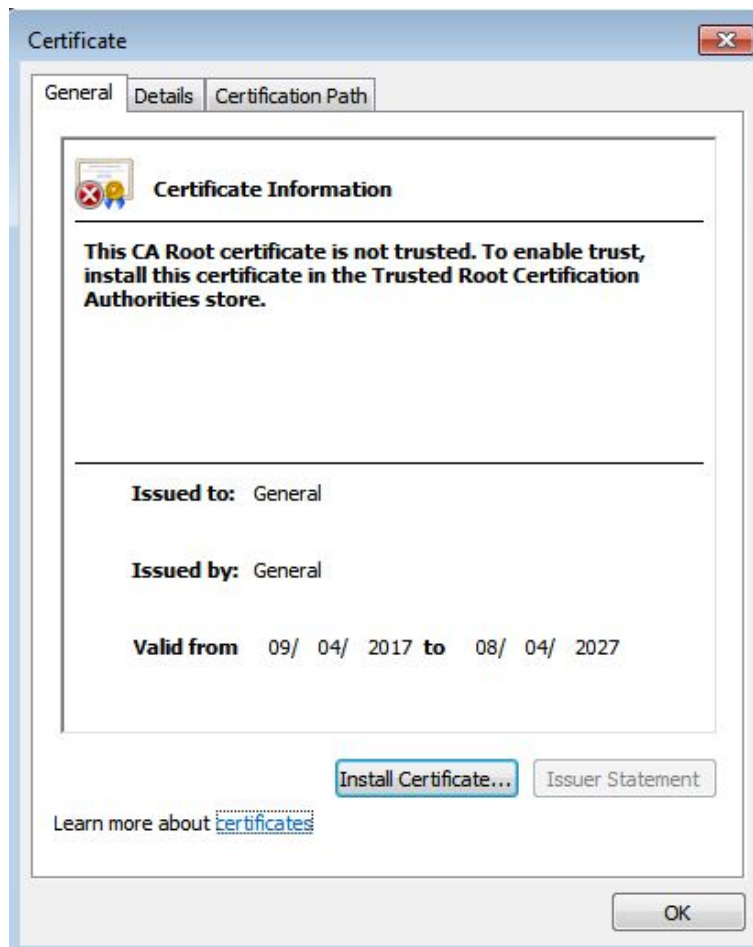
- 4) Click **Install**, and then click **Download** to download root certificate. The system pops up **Save As** dialog box, select storage path and then click **Save**.

Figure 4-89 Download root certificate



- 5) Double-click the RootCert.cer icon.

Figure 4-90 Certificate information



- 6) Click Install Certificate...



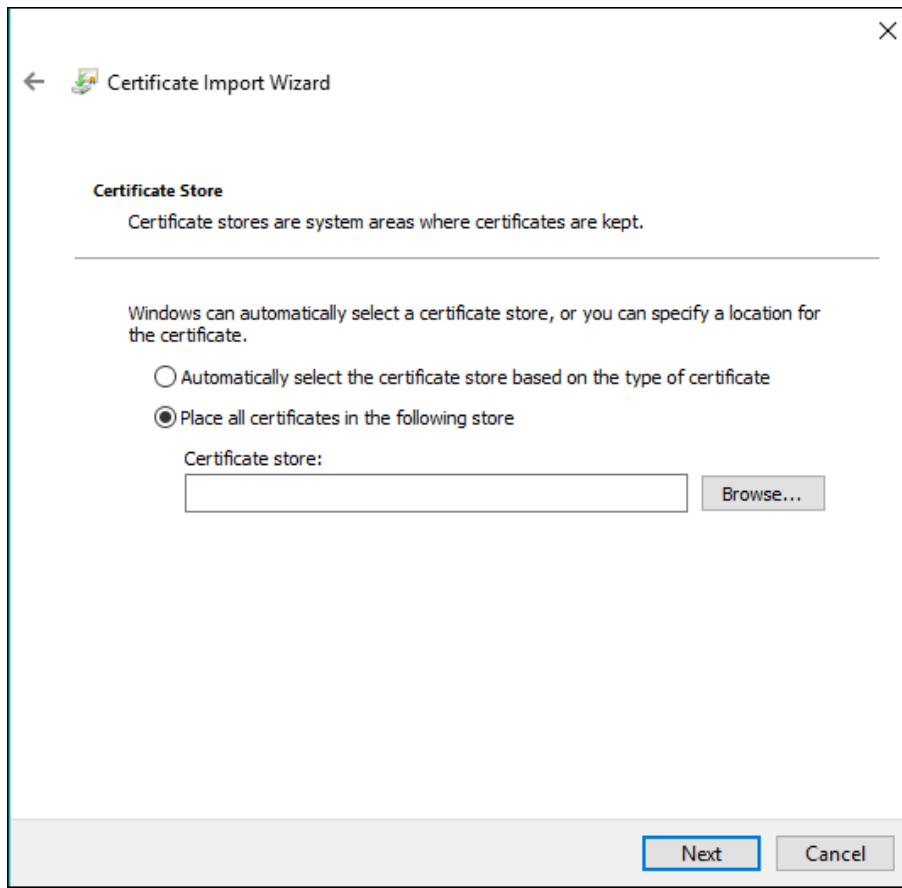
Figure 4-91 Certificate import wizard



7) Click **Next**.

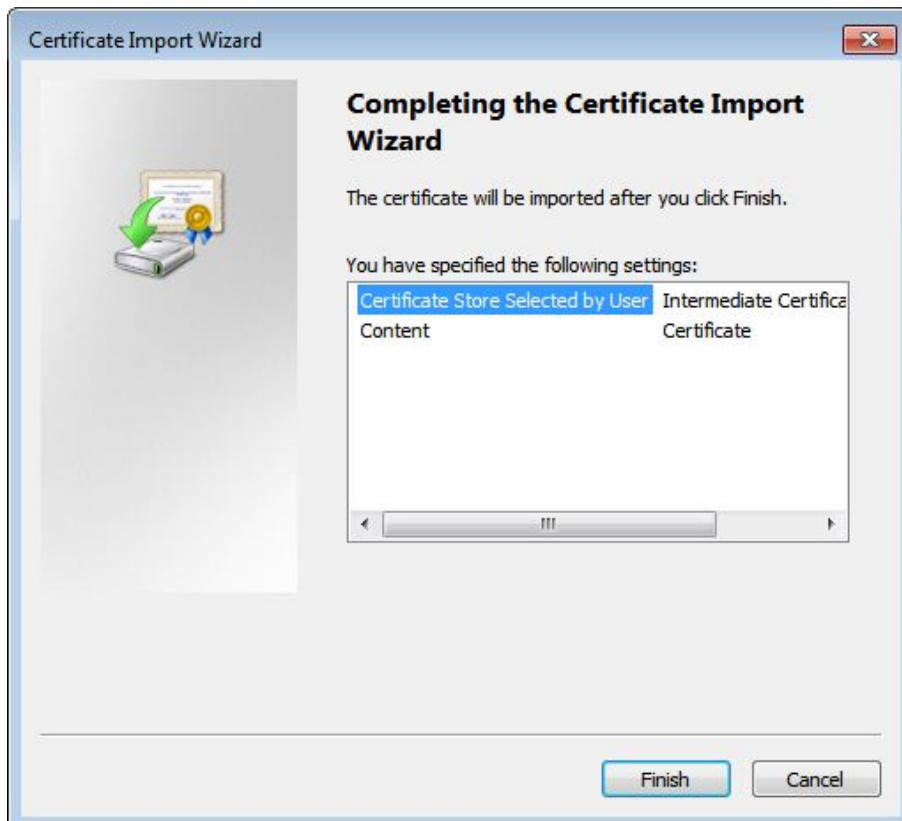
The **Certificate Store** interface is displayed. You can select automatically select the certificate store based on the type of certificate or place all certificates in custom certificate store.

Figure 4-92 Certificate store



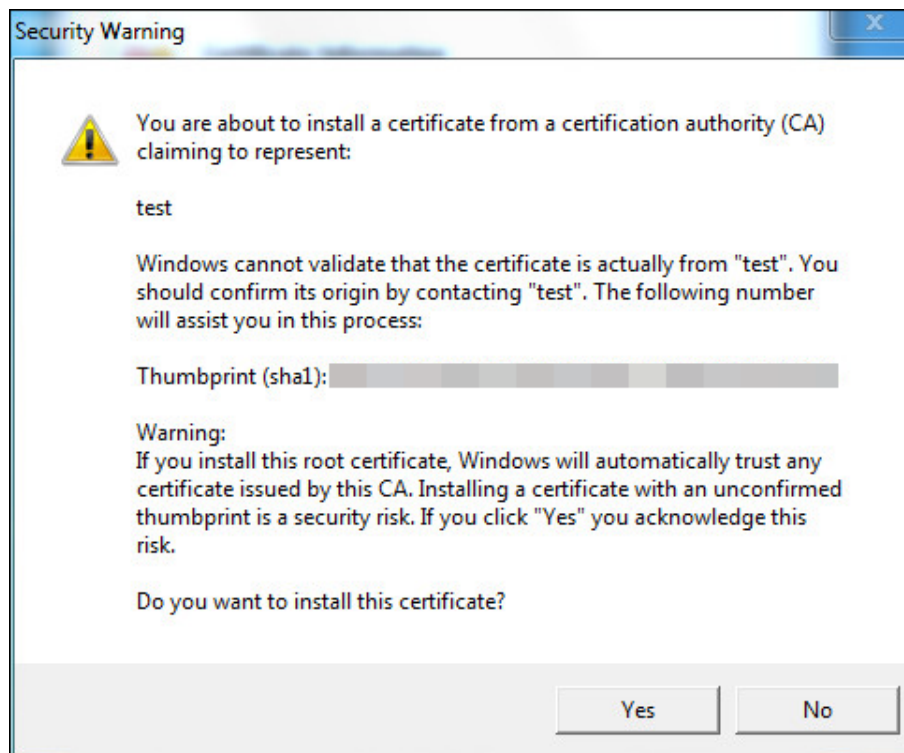
8) Click **Next**.

Figure 4-93 Completing certificate import wizard



9) Click **Finish**.

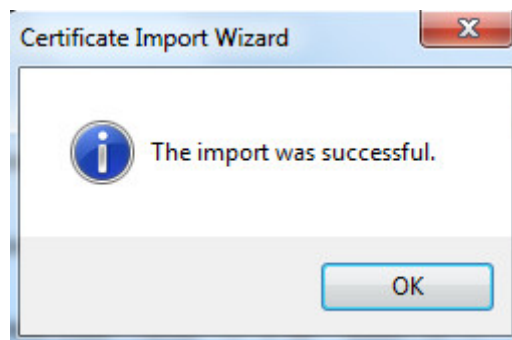
Figure 4-94 Security warning



10) Click **Yes**.

**The import was successful** dialog box is displayed, click **OK** to finish download.

Figure 4-95 Import succeeded

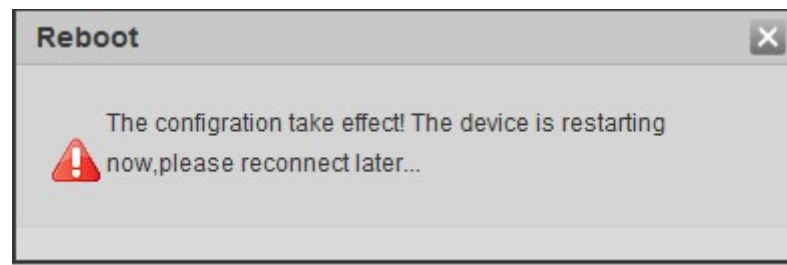


- If you select **install signed certificate**, follow the steps below.
  - 1) Select Setup > System > Safety > HTTPS.
  - 2) Select Enable HTTPS and Enable TLSv1.0.
  - 3) Click **Browse** to upload the signed certificate and certificate key, and then click **Upload**.
  - 4) To install the root certificate, see operation steps from 4) to 10) in **Create Certificate**.

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

The **Reboot** interface is displayed. Configuration takes effect. Wait until the Camera restarts.

Figure 4-96 Restart device



## Use HTTPS

Use HTTPS to log in to the Camera.

**Step 1** Enter `https://xx.xx.xx.xx` in the browser, and then the login interface is displayed.

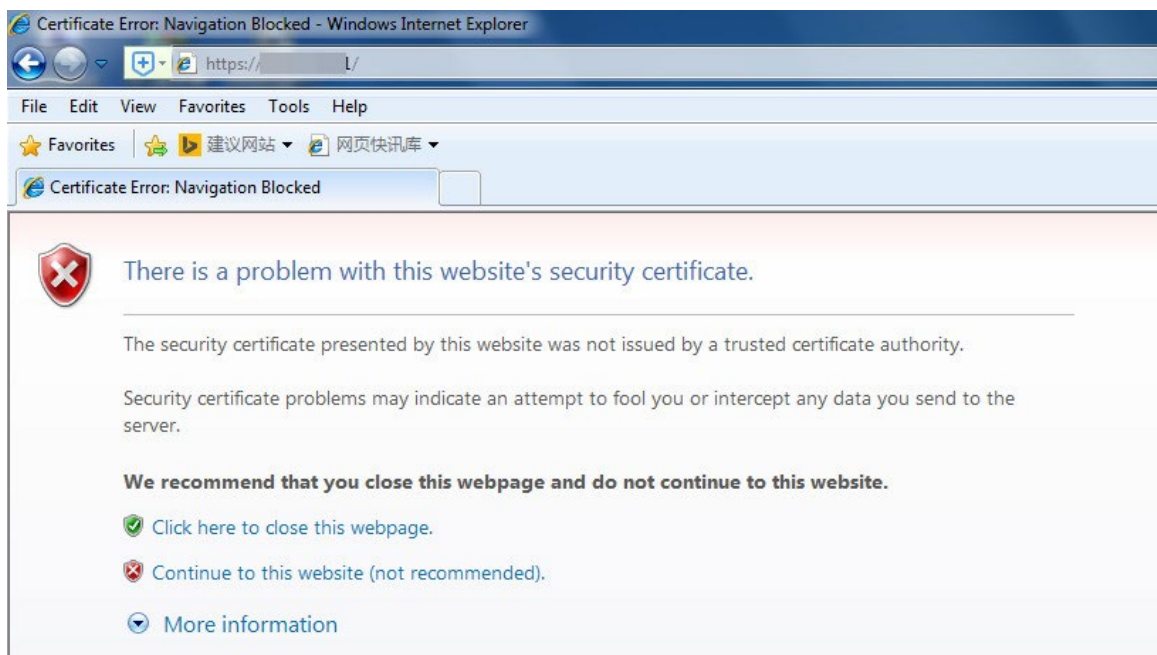


`xx.xx.xx.xx` is your device IP address or domain name.

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

The browser will prompt certificate error if certificate is not installed. See Figure 4-97.

Figure 4-97 Certificate error

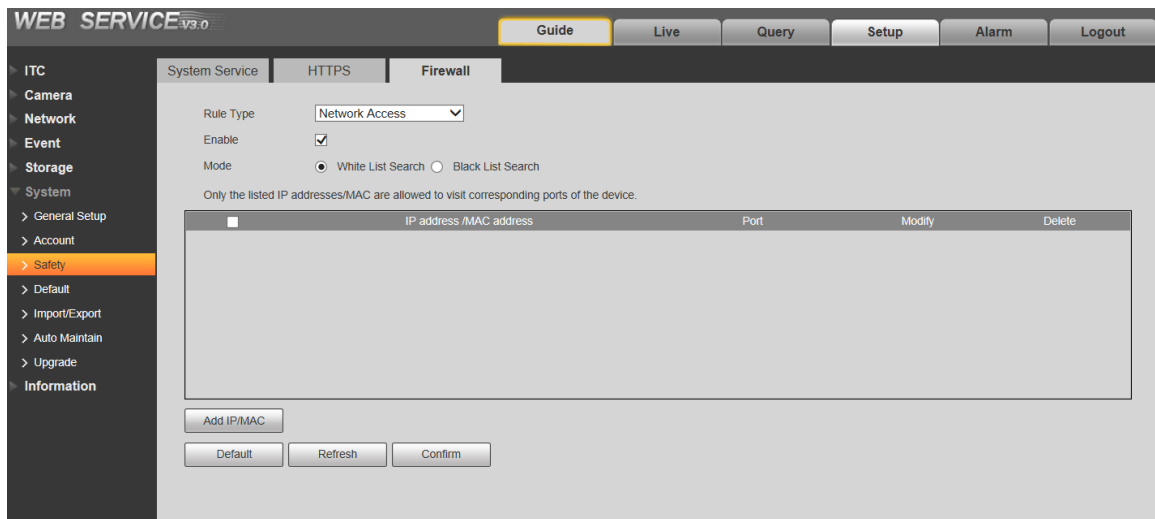


### 4.5.6.3.3 Firewall

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

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

Figure 4-98 Firewall



**Step 2** Select Rule Type.

- **Network Access:** Add the IP address to whitelist or blacklist 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 **Enable** to enable the rule type that you selected.

**Step 4** Click **Confirm**.

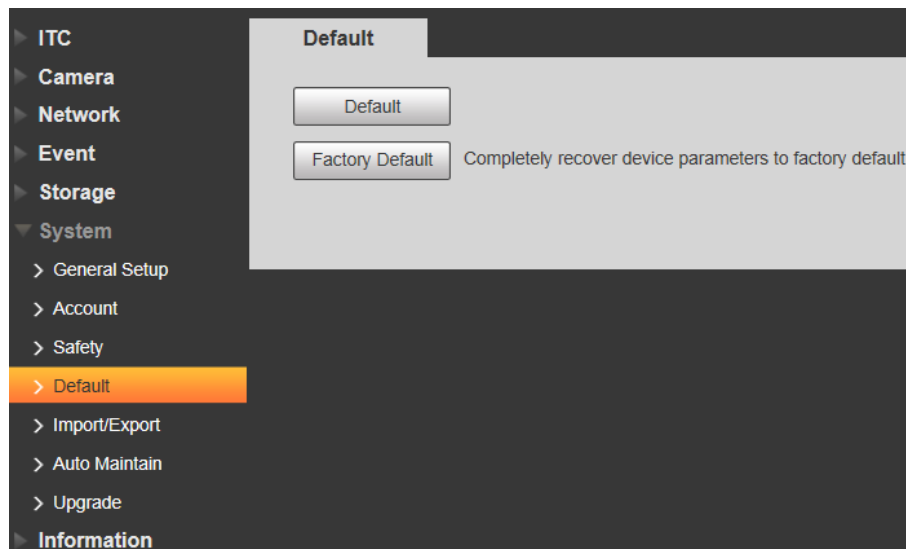
#### 4.5.6.4 Default Settings

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

- **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.

Select **Setup > System > Default**, the **Default** interface is displayed. Select **Default** or **Factory Default** as needed.

Figure 4-99 Default settings

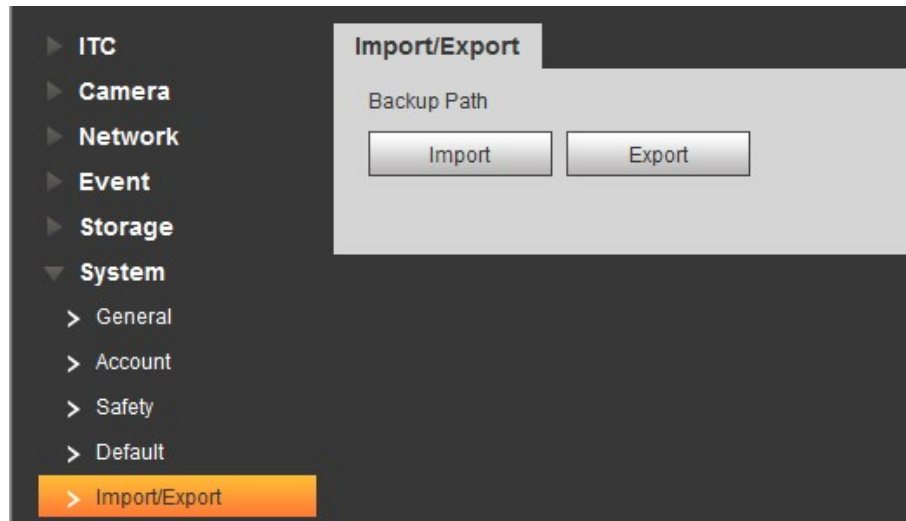


### 4.5.6.5 Import/Export

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 Setup > System > Import/Export.

Figure 4-100 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.

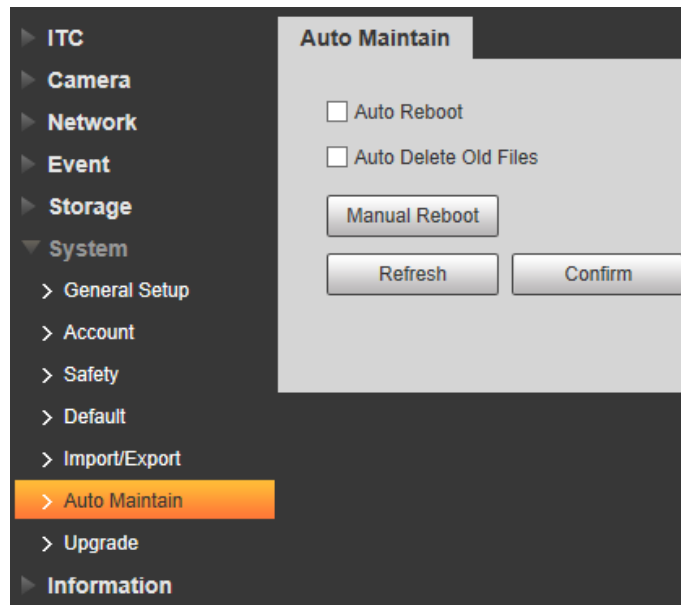
Step 4 Click **Open** or **Save** and view import and export result on the web interface.

### 4.5.6.6 Automatic Maintenance

Users can set the time of auto reboot and automatically delete old files.

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

Figure 4-101 Auto maintain



**Step 2** Configure the parameters.

Table 4-41 Auto maintain parameter description

Parameter	Description
Auto Reboot	The system will automatically restart within the defined period and time. Select and set restart period and time.
Auto Delete Old Files	Customize time and delete all the old files before the time.
Manual Reboot	Manually restart the Camera.

**Step 3** Click **Confirm**.

### 4.5.6.7 System Upgrade

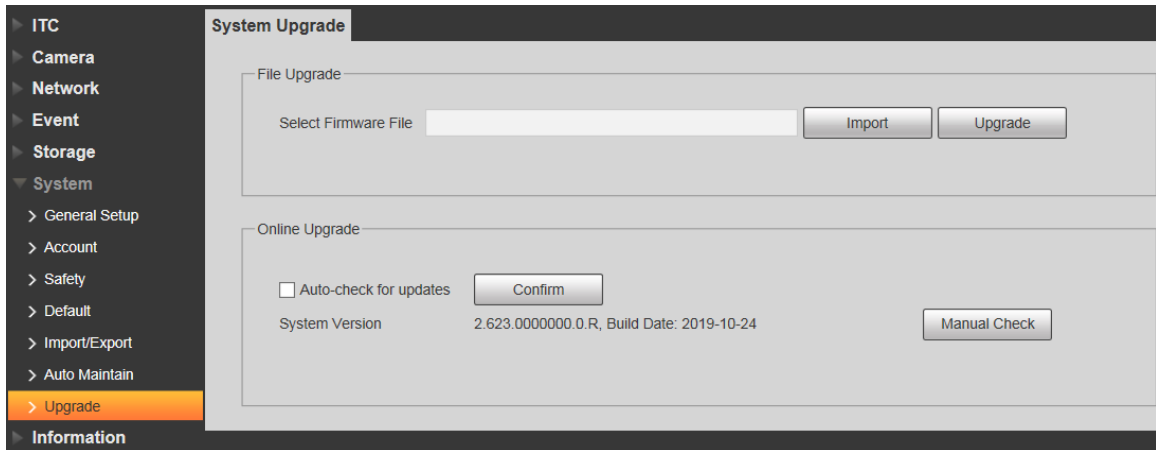
Upgrade system of the Camera to keep the camera functions always working. You can upgrade the system by using upgrade file or through online upgrade.



- Upgrading the wrong program might result in the Camera not working properly.
- During upgrading, make sure that the Camera is not disconnected from power and network, and restart or shut down the web.
- Online upgrade is not supported in the current version. Do not select **Online Upgrade** on the web interface.

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

Figure 4-102 System upgrade



**Step 2** Click **Import** and import upgrade file.

The upgrade file should be a .bin file.

**Step 3** Click **Upgrade**.

The system starts to upgrade firmware.

## 4.5.7 Information

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

### 4.5.7.1 Version

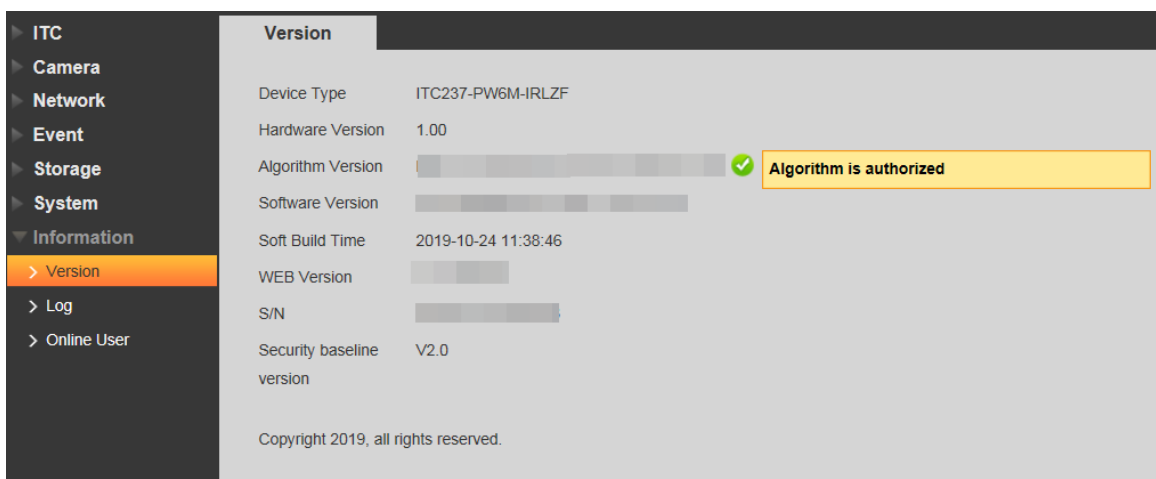
You can view the version information of the Camera.

Select **Setup > Information > Version**, and then the **Version** interface is displayed.



- Versions of different devices might vary, and the actual web interface shall prevail.
- 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 4-103 Version





## 4.5.7.2 Log

### 4.5.7.2.1 System Log

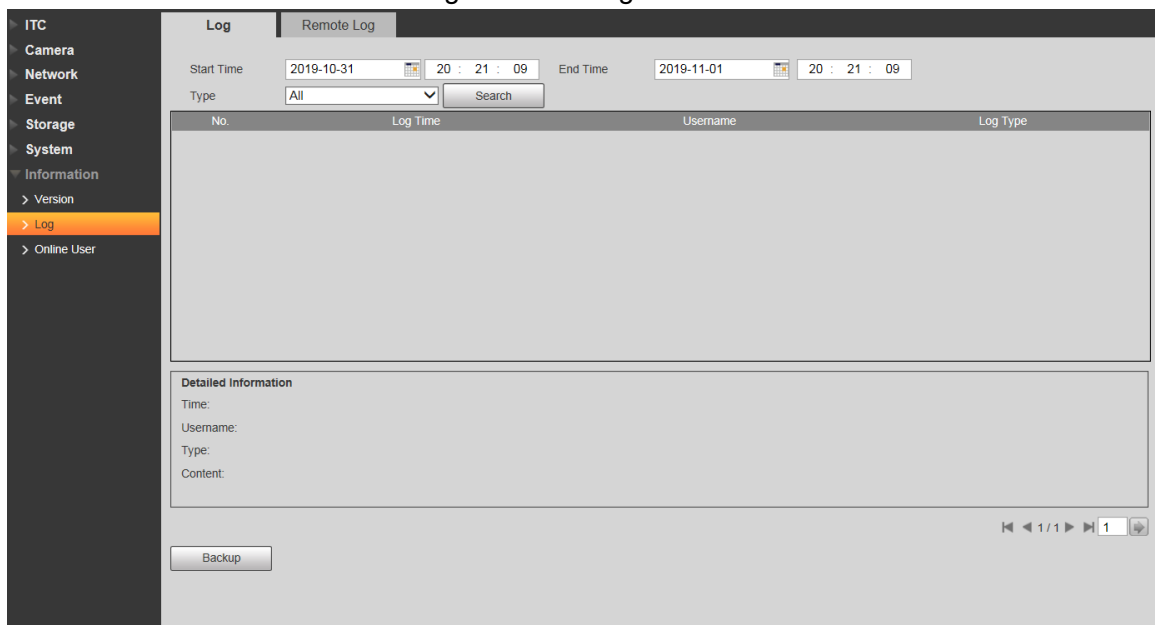
You can view log information such as system, configuration, data, event, record, user management, and also clear log records.



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

**Step 1** Select Setup > Information > Log > Log.

Figure 4-104 Log



**Step 2** Enter **Start Time** and **End Time**, and then select log type.

**Step 3** Click **Search** and it can start searching according to requirement.

**Step 4** View, back up and clear the searching results.

Backup: Backup the searched system log information to local. The backup file is in **.txt** format.

### 4.5.7.2.2 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 Setup > Information > Log > Remote Log.

Figure 4-105 Remote log

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

**Step 3** Configure the IP address, port, and device number.

**Step 4** Click **Confirm**.

Click **Refresh** to refresh the interface. Click **Default** and then **Confirm** to restore to default Settings.

### 4.5.7.3 Online User

You can view the information of all the online users on this interface.

Select **Setup > Information > Online User**, and the **Online User** interface is displayed.

Figure 4-106 Online user

No.	Username	User Local Group	Address	User Login Time	Login Type
1	admin	admin		2019-11-01 15:43:24	RPC
2	admin	admin		2019-11-01 15:43:26	RPC
3	admin	admin		2019-11-01 15:43:29	RPC
4	admin	admin		2019-11-01 19:28:12	Web3.0
5	admin	admin		2019-11-01 19:28:13	DVRIP

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

## 4.6 Alarm

Click the **Alarm** tab, and then the **Alarm** interface is displayed.

You can select alarm type, operation and tone, view the alarm time, type and channel.

Figure 4-107 Alarm

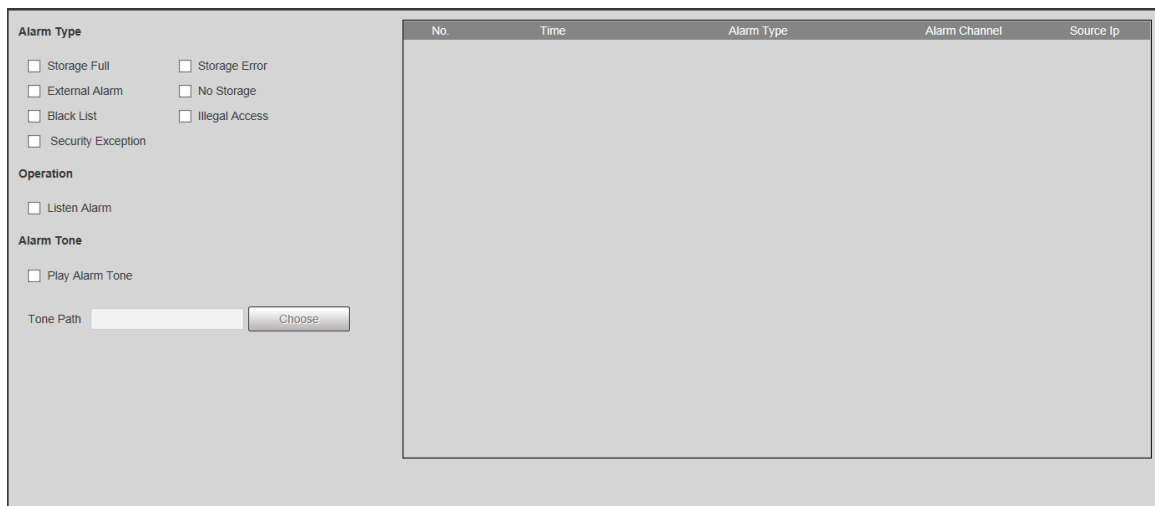


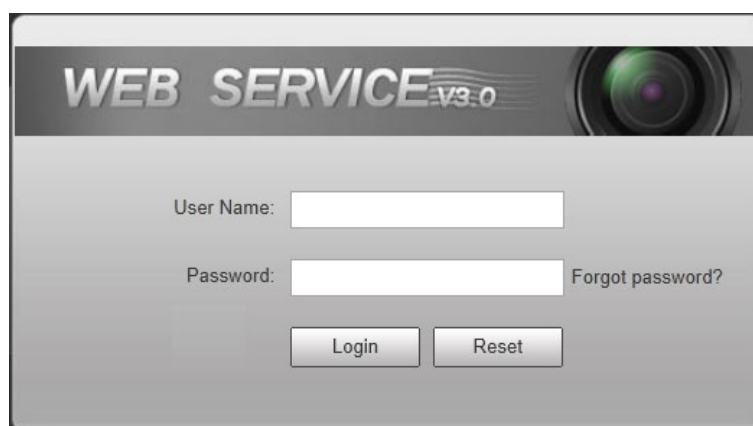
Table 4-42 Alarm parameters description

Type	Parameter	Description
Alarm Type	Storage Full	It triggers alarm when storage card is full.
	Storage Error	It triggers alarm when storage card fault occurs.
	External Alarm	It generates alarm through peripheral device when alarm is triggered.
	No Storage	It triggers alarm when there is no storage card.
	Black List	It triggers alarm when the blacklist vehicle appears.
	Illegal Access	It triggers alarm when the times of login password error reach the max value.
	Security Exception	It triggers alarm when there is security exception.
Operation	Listen Alarm	The web will prompt user when device alarm occurs.
Alarm Tone	Play Alarm Tone	It generates alarm prompt tone when alarm occurs. Alarm tone supports customized settings.
	Tone Path	The path of customized alarm tone.

## 4.7 Logout

Click **Logout** to exit the system. You need to log in again for access.

Figure 4-108 Login again



The image shows a web browser window displaying the login page for Dahua's Web Service v3.0. The page has a dark grey header with the text "WEB SERVICE v3.0" in a light grey font. To the right of the text is a circular image of a camera lens. Below the header, there are two input fields: "User Name:" followed by a white text box, and "Password:" followed by a white text box. To the right of the password field is a link that says "Forgot password?". Below the input fields are two buttons: "Login" and "Reset".

## 5 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 default 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 may damage the TF card duration.
TF card cannot be used as storage media	When the TF card hibernates or its capacity is null, format the card through web first.
Network upgrade failed	Check whether the right upgrade program (such as version, compatibility) is used.
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.
Failed to pop up the installation dialog box of web control webrec.cab	Set the security level of IE browser as <b>Low</b> , and <b>Active Plug-in and Control</b> is set as <b>Enable</b> .

# Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

## **Mandatory actions to be taken for basic equipment network security:**

### **1. Use Strong Passwords**

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

### **2. Update Firmware and Client Software in Time**

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

## **"Nice to have" recommendations to improve your equipment network security:**

### **1. Physical Protection**

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

### **2. Change Passwords Regularly**

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

### **3. Set and Update Passwords Reset Information Timely**

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

### **4. Enable Account Lock**

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

## 5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

## 6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

## 7. Enable Whitelist

We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

## 8. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

## 9. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

## 10. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

## 11. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

## 12. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

## 13. Network Log

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

## 14. Construct a Safe Network Environment

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.

- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.



ENABLING A SAFER SOCIETY AND SMARTER LIVING