VSIPNP-2BIRM-I

User's Manual

V1.0.0

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

● Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.

● These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system’s credentials. You will need to either update the camera’s firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

● Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.

● You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

● UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.

● If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

General

This user's manual (hereinafter referred to be "the Manual") introduces the functions and operations of the deep learning access ANPR camera (hereinafter referred to be "the Device").

Models

VSIPNP-2BIRM-I

Safety Instructions

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

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

Revision History

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release.	November 27, 2018

Privacy Protection Notice

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

About the Manual

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

Important Safeguards and Warnings

This Chapter describes the contents covering proper handling of the Device, hazard prevention, and prevention of property damage.Read these contents carefully before using the Device, 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 the power supply is correct before operating the device.
- 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 device.

Environment

- Do not aim the device 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 device in a damp or dusty environment, extremely hot or cold temperatures, or the locations with strong electromagnetic radiation or unstable lighting.
- Keep the device 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 device within the range of allowed humidity and temperature.
- Heavy stress, violent vibration or water splash are not allowed during transportation, storage and installation.
- Pack the device with standard factory packaging or the equivalent material when transporting the device.
- Install the device 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 device is operating normally.

Operation and Daily Maintenance

- Do not touch the heat dissipation component of the device to avoid scald.
- Carefully follow the instructions in the Guide when performing any disassembly operation about the device; 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 device together with lightning arrester to improve lightning protection effect.
- It is recommended to ground the device to enhance reliability.
- Do not touch the image sensor directly (CMOS). Dust and dirt could 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 device 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.

WARNING

- Please strengthen the protection of network, device data and personal information by adopting measures which include but not limited to using strong password, modifying password regularly, upgrading firmware to the latest version, and isolating computer network. For some device with old firmware versions, the ONVIF password will not be modified 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 the device is installed and maintained by professional engineers.
- The surface of the image sensor should not be exposed 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 device unless otherwise specified. A failure to follow this instruction might cause damage to the device.

FCC Information

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

FCC conditions:

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

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

FCC compliance:

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

- For class A device, these limits are designed to provide reasonable protection against harmful interference in a commercial environment. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
- For class B device, these limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
    - Reorient or relocate the receiving antenna.
    - Increase the separation between the equipment and receiver.
    - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
    - Consult the dealer or an experienced radio/TV technician for help.

Table of Contents

1 Introduction

1.1 Overview

Deep learning access ANPR camera adopts deep learning smart algorithm. It supports vehicle detection, license plate recognition, logo recognition, model recognition, vehicle brand and color recognition and H.265 encoding.

The device consists of protection housing, flash light and HD smart camera. Built-in camera adopts HD progressive scanning CMOS, which owns several features such as high definition, low illuminance, high frame rate and excellent color rendition etc. Meanwhile, it supports simultaneous processing of two channels' video for both master and slave cameras. It will automatically select one channel video with better recognition result to report.

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

1.2 Features

Some product functions are listed below, which is for reference only. Product functions might not be completely same according to different models. The actual product shall prevail.

Authority Management

- Each user group owns a permission set, which can be freely modified. It is a subset of the total permission set, and user permission within the group cannot exceed the set of group permission
- Supports 2 user levels.
- Sets if the vehicle owns the permission of opening barrier and supports blacklist alarm function.
- Realizes device config management and control permission management via Ethernet.

Storage

- Stores corresponding video data onto the central server according to users' config and strategy (such as alarm and timing setting)
- Users can record via 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 implements circulated coverage of picture storage automatically when memory becomes insufficient.
- Supports log function. It can store 1024 log records and support user permission control.
- Supports FTP storage and ANR.

Alarm

- It can trigger alarm upon camera operation exceptions via network, such as memory card damage and so on.
- Some devices support alarm output terminal connecting to various alarm peripherals, responding to external alarm input (within 200ms) in real time. It can correctly deal with various alarms according to the linkage setting defined by users in advance (such as informing user via email) and generate corresponding voice prompt (users are allowed to record voice in advance).

Network Monitoring

- Transmit video data of single channel compressed by device to network terminal and make it reappear after decompression via network. Keep delay within 500ms when bandwidth is allowed.
- The device supports max. 10 users on line at the same time.
- Supports system access via WEB, applied to WAN.
- Supportsdevice management via WEB mode.
- Video data transmission adopts HTTP, TCP, UDP, MULTICAST and RTP/RTCP etc.
- Supports system access via WEB, applied to WAN.

Capture and Recognition

- Supports vehicle recognition.
- Supports license plate recognition.
- Supports setting OSD info and location of channel, picture.
- Supports picture capture and encoding. Supports picture watermark encryption, prevent pictures from being tampered.
- The captured pictures can automatically record vehicle time, location, license plate, vehicle color and bayonet direction etc.
- Supports vehicle color, logo, vehicle model and other vehicle feature recognition.

Peripheral Control

- Supports peripheral control function, it can freely set various peripheral control protocol and connection interface.
- It can externally connect to vehicle detector, signal detector and other devices.

Auto Adjustment

- AWB: It can still accurately display the object color when light condition changes
- Auto exposure: It can automatically set shutter speed according to the exposure value of the image measured by metering system, according to shutter and iris exposure set by factory default.
- Auto gain: It can automatically increase camera sensitivity when illuminance is very low, enhance image signal output so that it can acquire clear and bright image

Panoramic Camera

It can receive HDCVI image signal input of panoramic camera. Video stream of panoramic camera can be accessed in real time via WEB.

2 Device Structure

Deep learning access ANPR camera is an integrated device. The camera is installed in the housing, the interface board of the camera is concealed and the camera port is connected via cable.

2.1 Dimension

Figure 2-1 General product dimension diagram (Unit: mm)

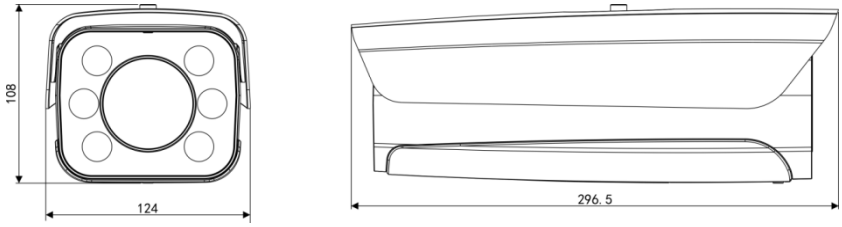
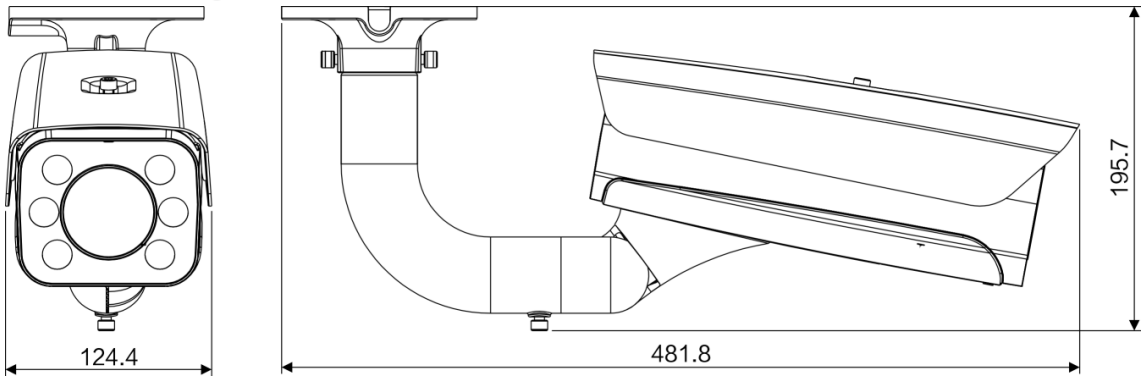


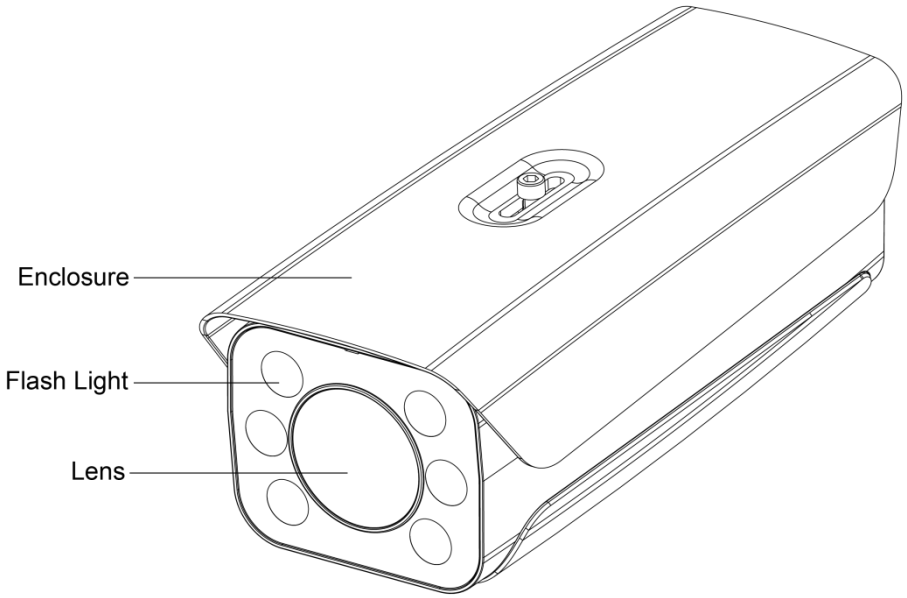
Figure 2-2 Product with bracket dimension diagram (Unit: mm)



2.2 Structure

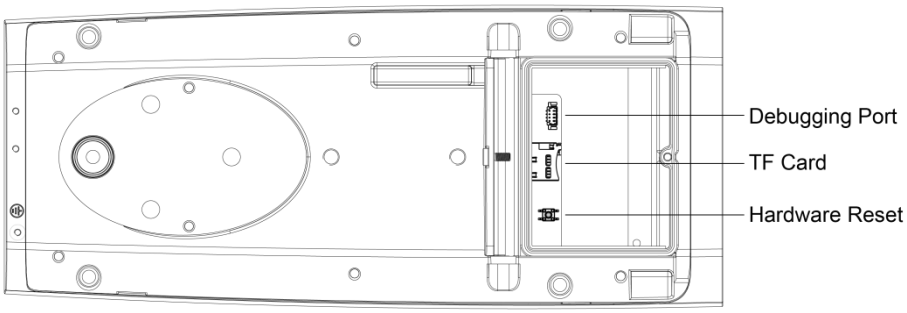
2.2.1 Unit Device

Figure 2-3 Product structure diagram



2.2.2 Rear Panel

Figure 2-4 Rear panel structure diagram



2.3 Device External Cable

Figure 2-5 Port diagram

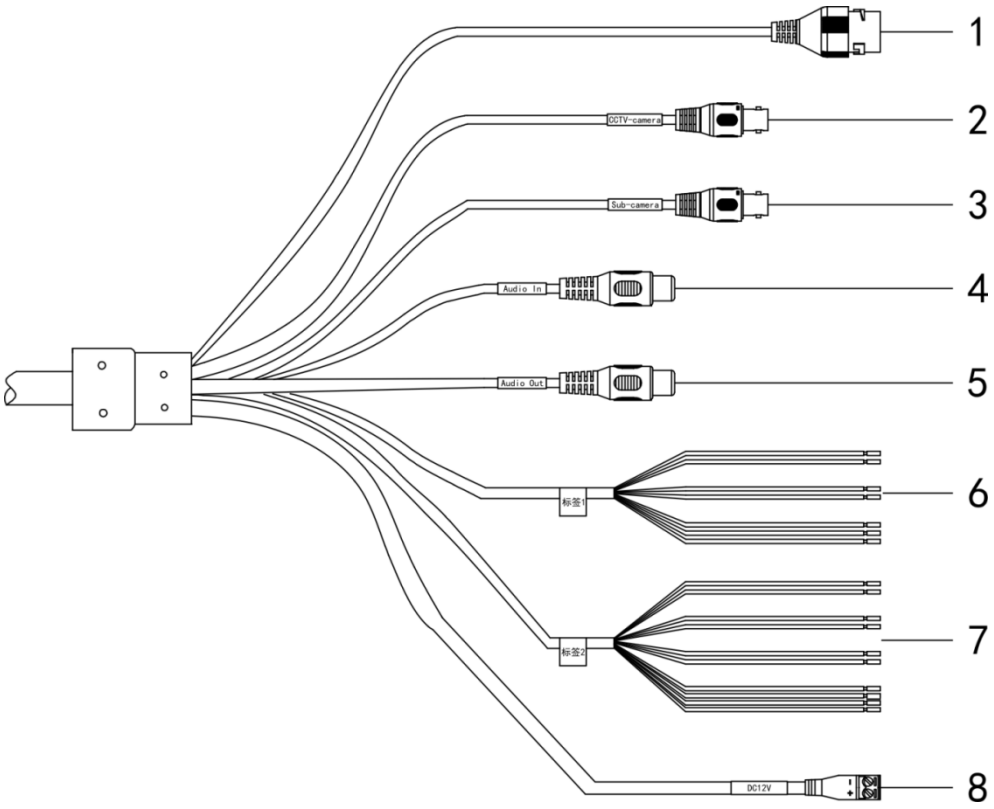


Table 2-1 External cablefunction introduction

No.	Port	Function	Description
1	LAN	Network port	Connects to standard Ethernet, supports PoE power supply.
2	CCTV-camera	Panoramic camera input port	Connects to panoramic camera, receives image input by panoramic camera.
3	Sub-camera	Sub camera input port	Function reserved.
4	AUDIO OUT	Audio output port.	Audio output port.
5	AUDIO IN	Audio input port.	Audio input port.
6	RS485	RS-485 port	● RS-485 ◇ Light blue: RS-485_A1 ◇ Yellow black: RS-485_B1 ◇ Yellow green: RS-485_A2 ◇ White orange: RS-485_B2 ● RS-485/232 ◇ Blue white: RS-485_A/RS-232_R ◇ Green white: RS-485_B/RS-232_T ◇ Gray: GND

No.	Port	Function	Description
7	ALARM	Alarm port	● Alarm output ◇ Brown: ALARM_NO1 ◇ Green: ALARM_NC1 ◇ Blue: ALARM_NO2 ◇ White: ALARM_NC2 ◇ Yellow: ALARM_NO3 ◇ Orange: ALARM_NC3 ● Alarm input ◇ Purple: IO_IN1 ◇ Pink: IO_IN2 ◇ Red: ALARM_IN1 ◇ Black: GND
8	Power	Power input port	Inputs DC 12V power. Please be sure to supply power as instructed in the Guide.  Device abnormity or damage could occur if power is not supplied correctly.

3 Device Installation

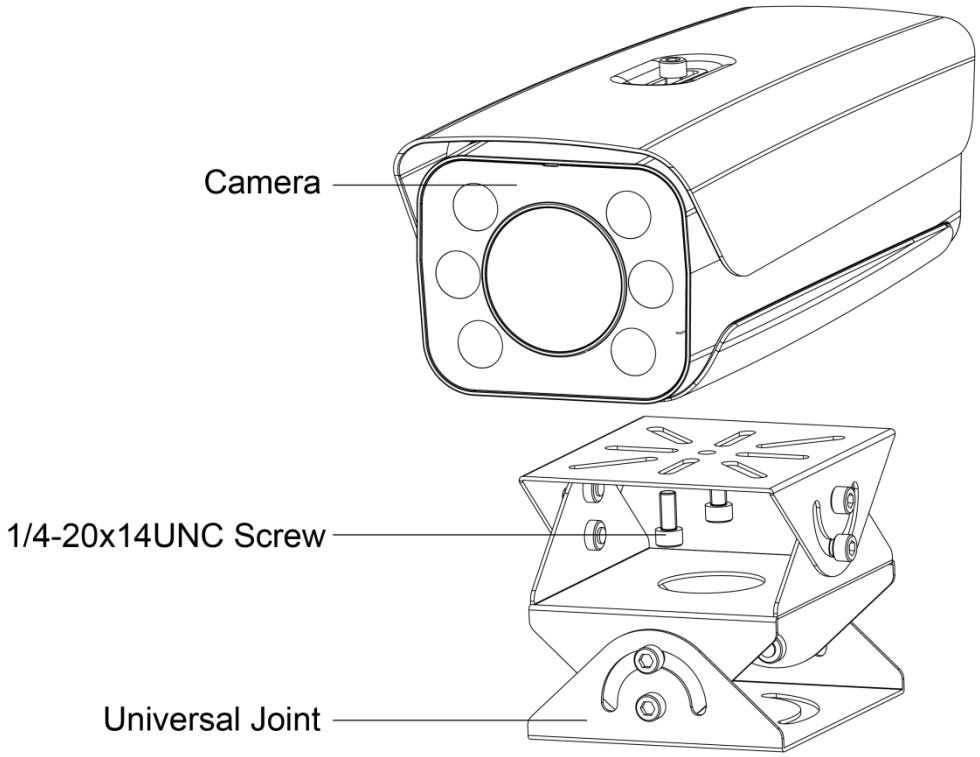
The actual product shall prevail. The following installation figures are for reference only.

3.1 Universal Joint Installation

Step 1 UseM6× 14 screw to fix the universal joint on the bracket.

Step 1 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

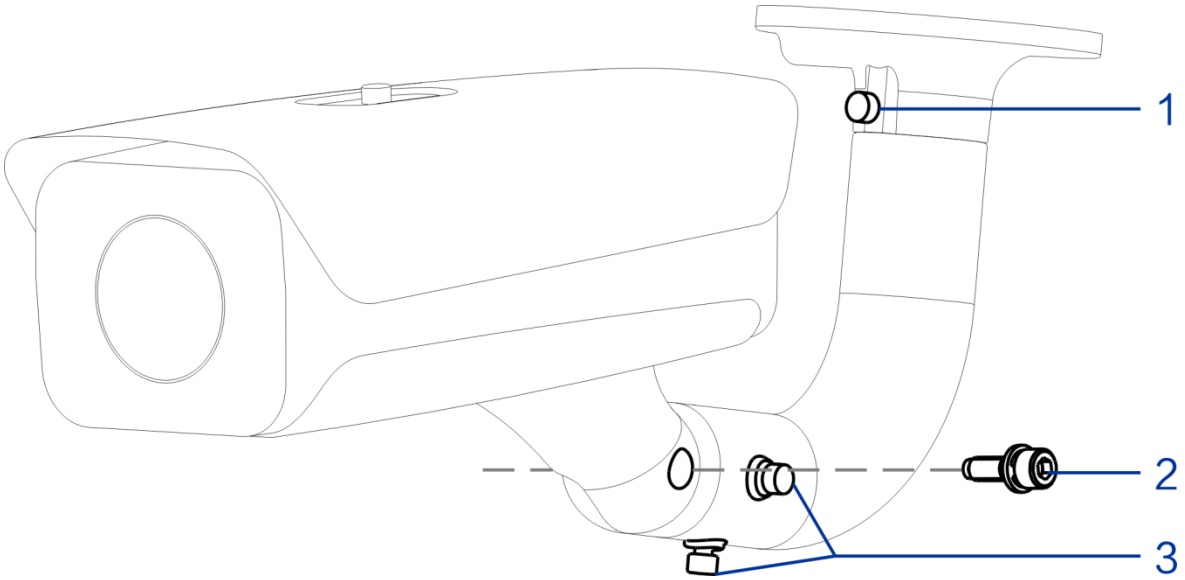


Step 2 Adjust the universal joint UDLR and adjust the camera location.

So far, device installation is completed.

3.2 Bracket Installation

Figure 3-2 Bracket installation



Bracket installation description

No.	Note
1	Adjust the screw leftward and rightward, and then it can adjust the camera leftward and rightward.
2	Adjust the screw upward and downward, and then it can adjust the camera upward and downward.
3	Adjust the screw horizontally, and then it can adjust the camera horizontally.

Step 1 Loosen the adjusting screw of the camera UDLR.

Step 2 Insert all the camera cable into the bracket and then pull it 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 location via all possible directions, and then tighten all the adjusting screws.

4 Basic Configuration

4.1 Quick Config Tool

- In this chapter, it only introduces the general operations of quick config tool. Please refer to *Quick Config Tool User's Manual*
- The figures shown in this chapter are for reference only. The actual interface shall prevail.

The default IP of the device is 192.168.1.108. Please modify device IP address according to network plan when you use it for the first time or network is adjusted.

You can modify device IP address individually or in batches via ConfigTool or you can log in WEB client and modify device IP address as well.

- It can modify device IP address individually when there are fewer devices or device login password does not match.
- When there are more devicesand device login password matches, you can modify IP addresses in batches.

Preparation

- It has acquired ConfigTool setup package, if not, please contact technical support.
- The PC which is installed with ConfigTool is interconnected with device via network.

4.1.1 Initializing Tool

It supports initializing device in the same LAN individually or in batches.

Associated operations cannot be implemented for uninitialized device, which will display gray in the device list. Besides, it fails to display associated information in other interfaces.

Step 1 Double click the shortcut key on the desktop 

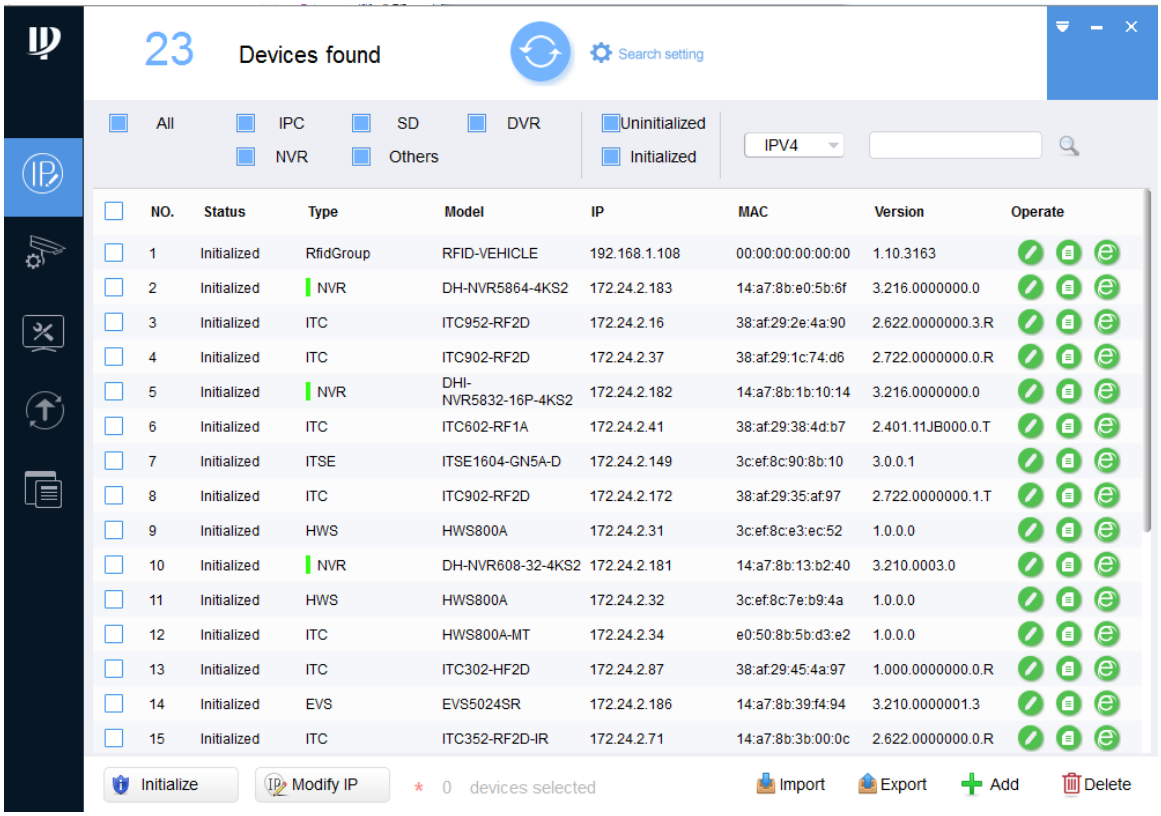
.

The system displays the main interface.

Step 2 Click  .

The **Modify IP** interface is displayed. See Figure 4-1.

Figure 4-1 Modify IP



Step 3 Select the uninitialized device. Click. Initialize

The **Device Initialization** interface is displayed.See Figure 4-2.

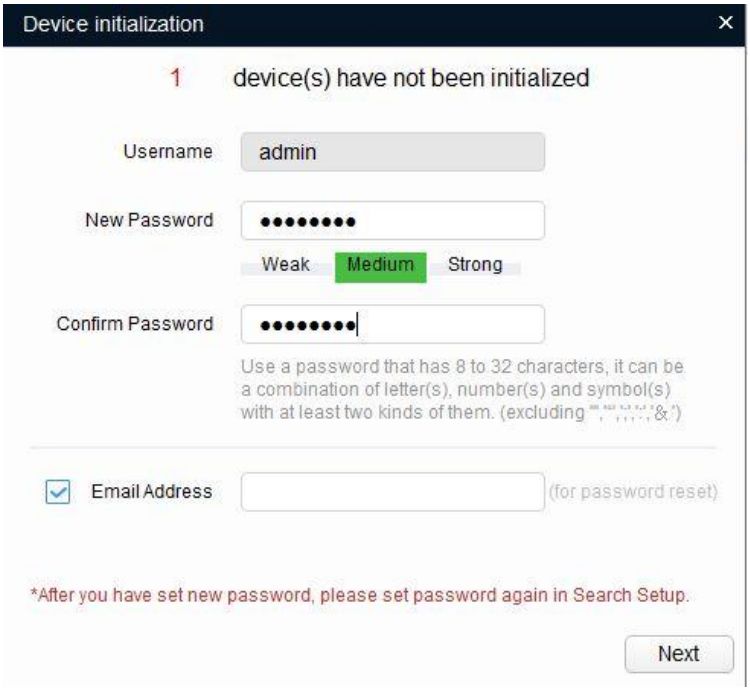
Figure 4-2 Device Initialization (1)

Step 4 Select the device which needs to be initialized. Click **Initialize**.

The **Device Initialization** interface is displayed.See Figure 4-3.

- The interface might be different depending on the model you purchased. The actual product shall prevail.
- The initialization interface of the first selected device will be displayed during initialization in batches.

Figure 4-3 Device initialization (2)



Step 5 Sets parameters of device initialization. Please refer to 0 for more details.

Device parameters description

Parameter	Note
Username	The username is admin by default.
New Password	• The new password can be set from 8 characters to 32 characters and contains at least two types from capital letter, small letter, number and special characters (excluding “'”, “"”, “;”, “:” and “&”) • Follow the password security notice to set a high security level password. • The new password should be in accordance with the confirm password.
Confirm Password	
Reserved Phone Number	It is selected by default; the input mobile phone number will be used for password retrieval and reset.

Step 6 Click **Initialize** and the system begins to initialize device.

After initialization is completed, see 错误!未找到引用源。 for the interface displayed by the system. If initialization succeeded, it will display✓; if initialization failed, it will display⚠. Click the icon to check more details.

Step 7 Click **Complete**, and then operation of device initialization is over.

After initialization is completed, the device status becomes initialized on the main interface. The device information will be displayed on other interfaces.

4.1.2 Modifying IP Address

4.1.2.1 Single

Please refer to **5.4.3 Network** for details of logging in WEB client and modifying IP address.

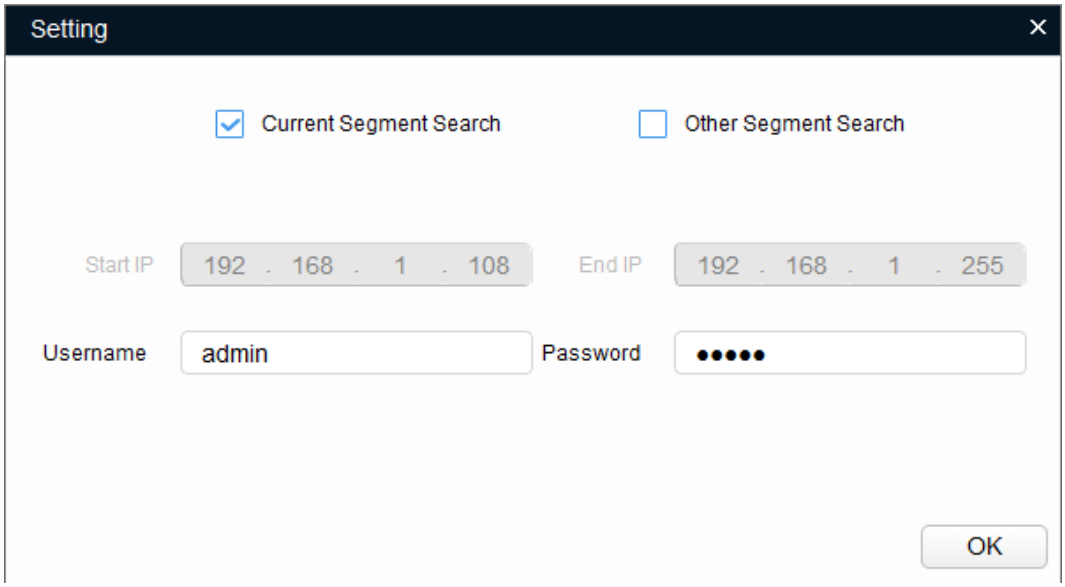
Step 1 Click  .

The **Modify IP** interface is displayed.

Step 2 Click Search Setup.

The **Setting** dialog box is displayed. See Figure 4-4.

Figure 4-4 Setting



Step 3 Set device segment, enter login username and password. Click **OK**.

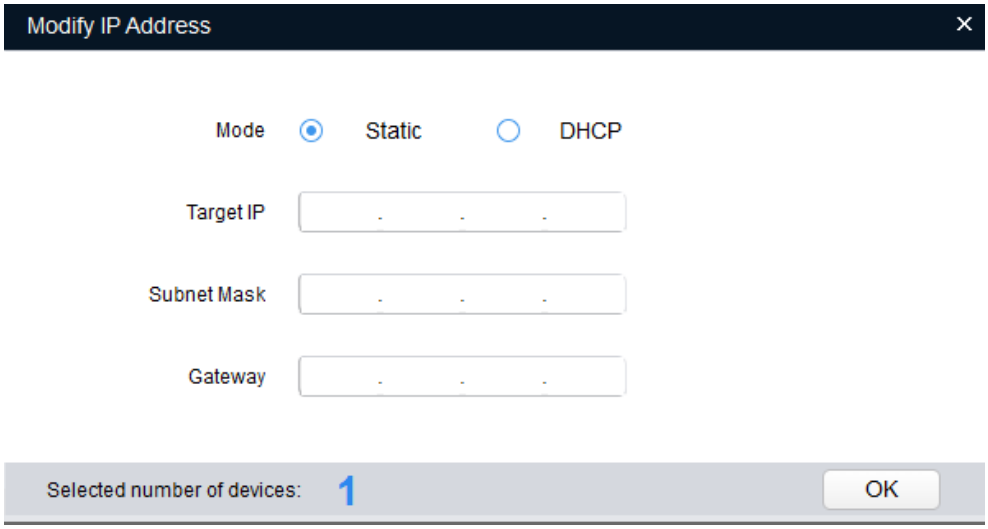
The searched devices will be displayed after searching is completed.

As for the devices which need to be initialized, they can be used after initialization.

Step 4 Click the corresponding of the device whose IP needs to be modified.

The **Modify IP** interface is displayed. See Figure 4-5.

Figure 4-5 Modify IP



Step 5 Select the mode of setting IP address according to the actual situation.

- DHCP (Dynamic Host Configuration Protocol) mode: When there is DHCP server in the network, set **Mode** as **DHCP**, and then the device can automatically acquire IP address from DHCP server.

- Manual mode: Set **Mode** as **Static**, and fill in **Target IP**, **Subnet Mask** and **Gateway**, and then the device can automatically acquire IP address from DHCP server.

Step 6 Click **OK** to complete modification.

4.1.2.2 Batch

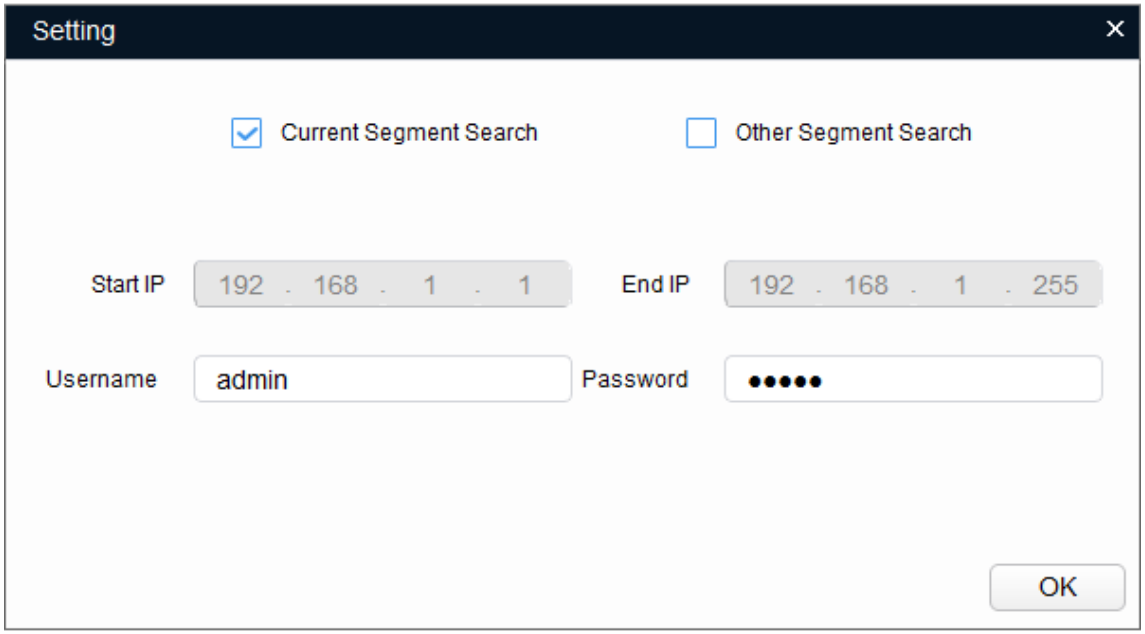
Step 1 Click  .

The **Modify IP** interface is displayed.

Step 2 Click Search Setup.

The **Setting** dialog box is displayed. See Figure 4-6.

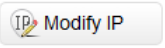
Figure 4-6 Setting



Step 3 Set device segment, enter username and password. Click **OK**.

The searched devices will be displayed after searching is completed.

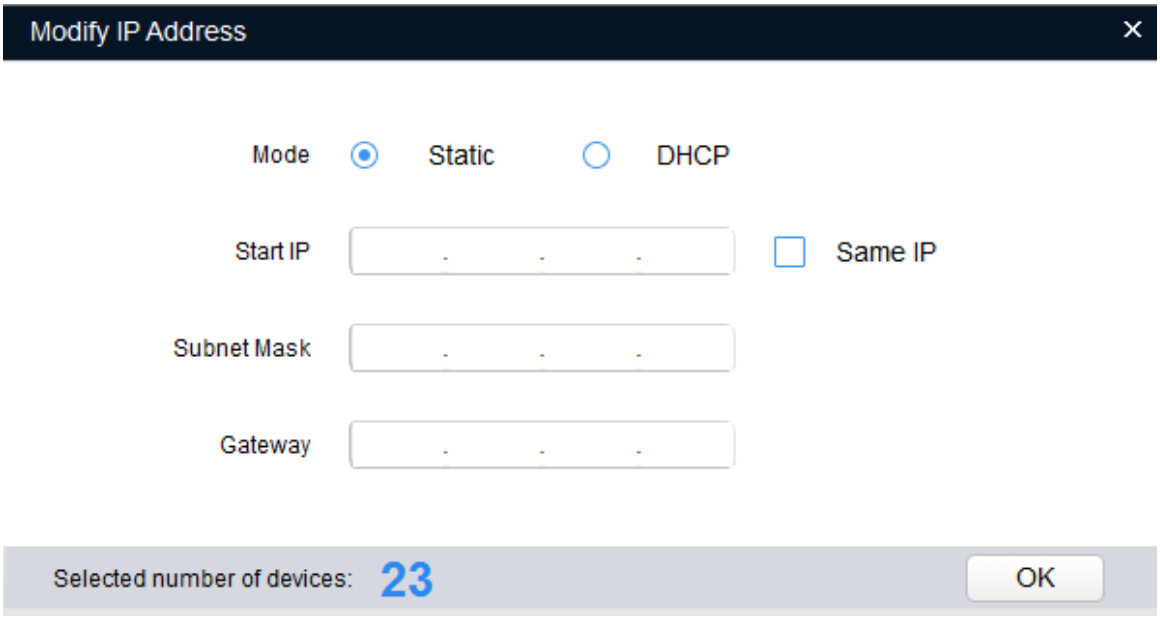
As for the devices which need to be initialized, they can be used after initialization.

Step 4 Select the device w**hose IP n**eeds to be modified, click 

.

The **Modify IP** interface is displayed. See Figure 4-7.

Figure 4-7 Modify IP



Step 5 Select the mode of setting IP address according to the actual situation.

- DHCP (Dynamic Host Configuration Protocol) mode: When there is DHCP server in the network, set **Mode** as **DHCP**, and then the device can automatically acquire IP address from DHCP server.
- Manual mode: Set **Mode** as **Static**, and fill in **Start IP**, **Subnet Mask** and **Gateway,** and then the device IP addresses will be modified successively from start IP.

Select **Same IP** and the selected device will be set as the same IP address.

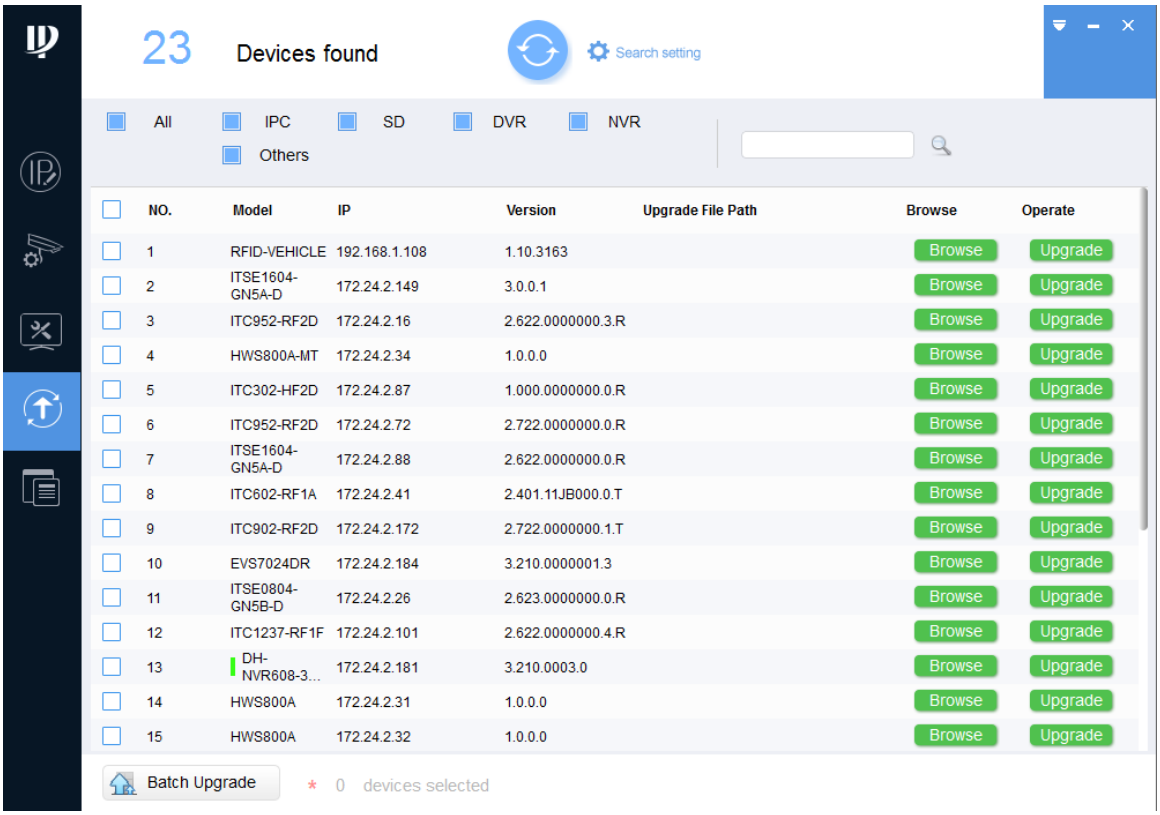
Step 6 Click **OK** to complete modification.

4.1.3 Device Upgrade

Device upgrade supports single and batch.

Step 7 Click  and the upgrade interface is displayed. See Figure 4-8.

Figure 4-8 Upgrade

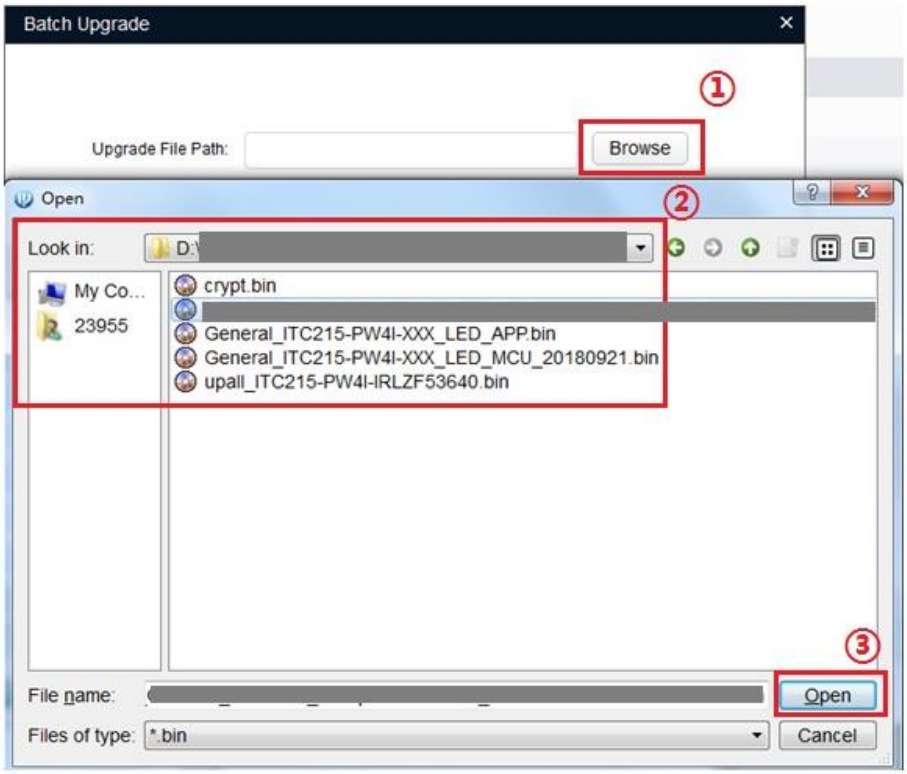


Step 8 Select the device which needs to be upgraded.

- Single: Click the corresponding **Open** of the device which needs to be upgraded.
- Batch: Select the devices which need to be upgraded, and click **Batch Upgrade**.

Step 9 Select upgrade file. See Figure 4-9

Figure 4-9 Select upgrade file



Step 10 Upgrade device.

- Single: Click **Upgrade** and the system begin to upgrade and display progress.

- Batch: Click **OK** and the system begins to upgrade.

If the device is disconnected during upgrade process, it will continue to upgrade when the device is connected to network again as long as ConfigTool continues to stay at the upgrade interface.

4.2 Web Login

It supports logging in device WEB interface via browser on PC, and realizes device operation, configuration and maintenance.

The interface and setting are for reference only. The actual interface shall prevail.

4.2.1 Recommended Config

Please refer to 0 for recommended config of PC which logs in device WEB interface.

PC recommended config

PC Component	Recommended Config
Operating System	Windows 7 and higher
CPU	Intel core i3 and higher
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

4.2.2 Device Initialization

- It needs to implement initialization when it is the first time to log in or it logs in after restoring factory default setting.
- Please confirm that both PC IP and device IP are in the same network segment, otherwise it fails to enter initialization interface.

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

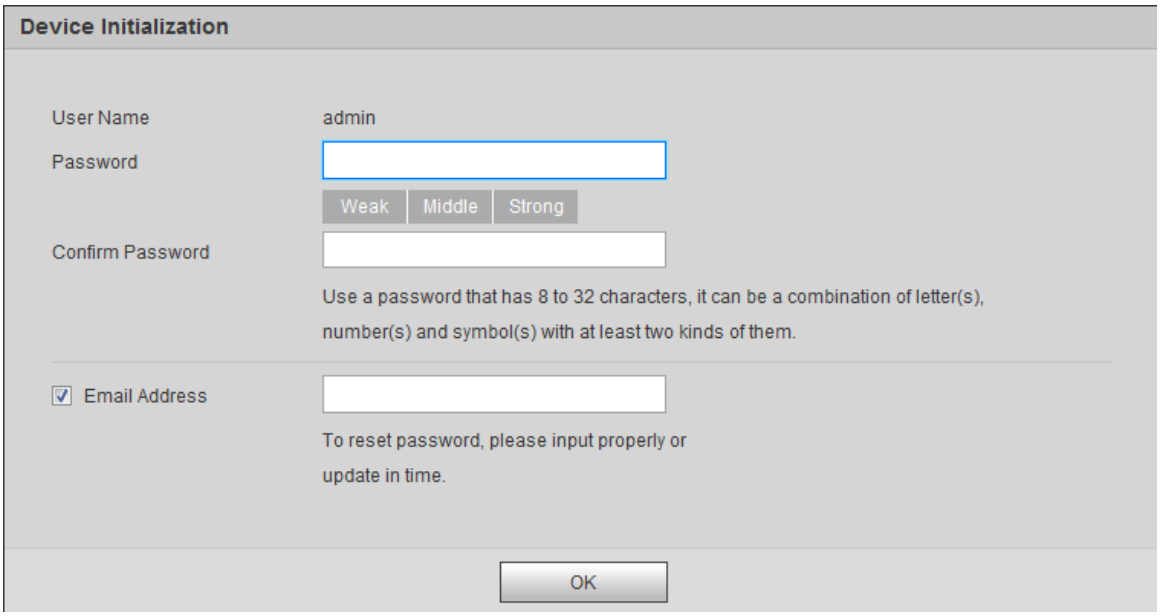
- Distribute IP address of the same segment if there is no router in the network.
- It needs to set corresponding gateway and subnet mask if there is router in the network.

The default IP is 192.168.1.108.

Step 2 Use ping ***.***. ***. *** (device IP address) command and check if network is connected.

Step 3 Open browser, input the IP address of the device in the address bar and press **Enter**. After it is successfully connected, the **Device Initialization** interface is displayed. See Figure 4-10.

Figure 4-10 Device Initialization



Step 4 Enter Password and Confirm Password.

- The new password can be set from 8 characters to 32 characters and contains at least two types from capital letter, small letter, number and special characters (excluding “‘”, “"”, “;”, “:” and “&”)
- If it needs to update password again, go to **Setting** > **System** > **User** > **User** and modify.
- Prompt box will pop out when username or password is incorrect, see Figure 4-11, and it will remind you of remaining attempts The account will be locked if user enters incorrect username or password for 5 times consecutively, the lock time is 300s.See Figure 4-12

Figure 4-11 Login error

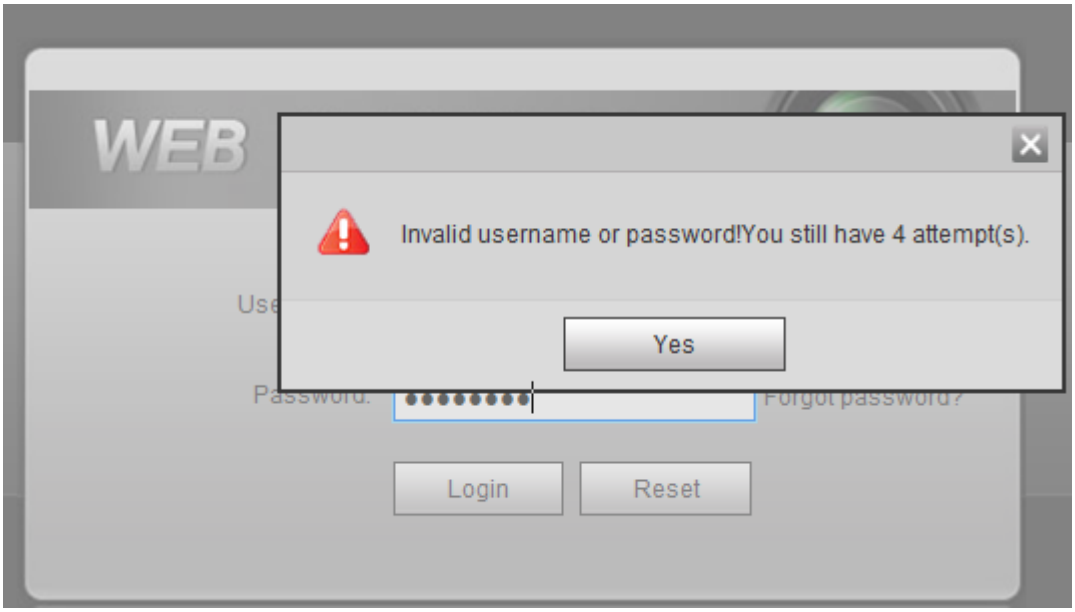


Figure 4-12 Account locked

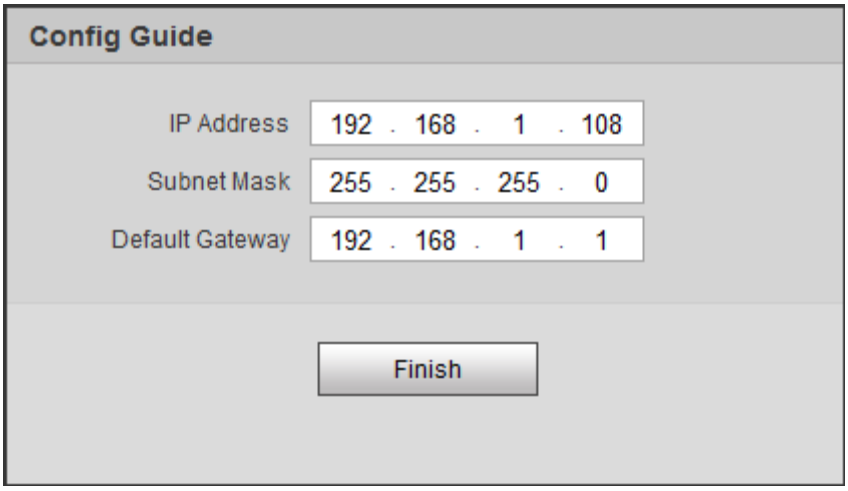
Step 5 Select **Reserved Mobile** and then enter mobile phone number.

The mobile phone number is used for password reset, it is recommended to set.

Step 6 Click **OK**.

The **Config Guide** interface is displayed. See Figure 4-13.

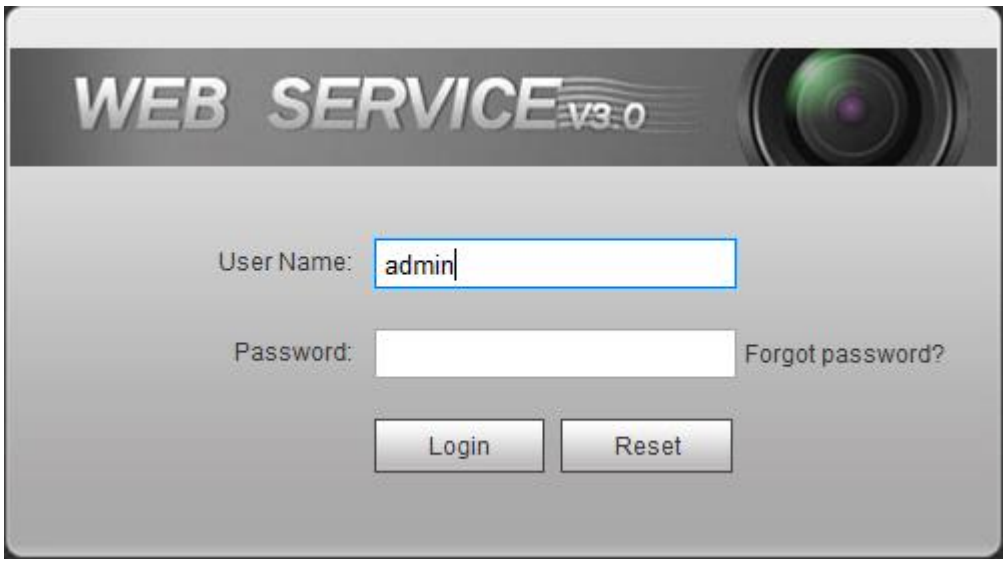
Figure 4-13 Config Guide



Step 7 Click **Finish**.

The login interface is displayed. See Figure 4-14.

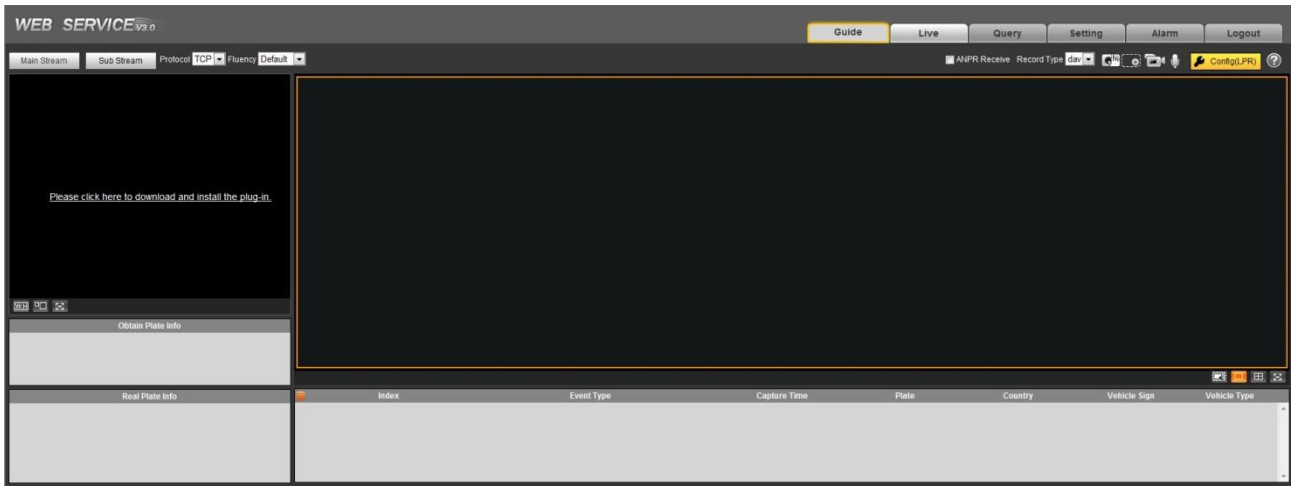
Figure 4-14 Login interface



Step 8 Enter the **Password**, and then click **Login**.

The WEB interface (1) is displayed. See Figure 4-15.

Figure 4-15 WEB interface (1)



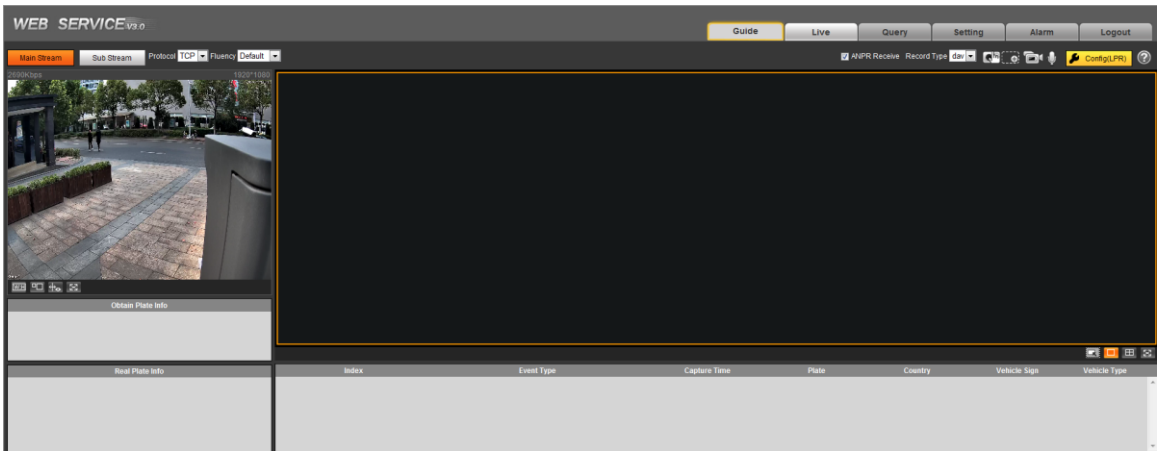
Step 9 Click Please click here to download and install the plug-in in the video window.

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

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

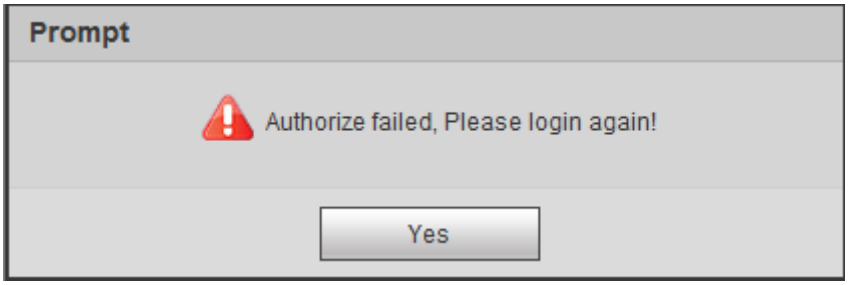
After installation is completed, the WEB interface (2) is displayed. See Figure 4-16.

Figure 4-16 WEB Interface (2)



It will pop out the prompt box of authorization failed when the WEB interface hasn't been operated for a long time, and then it needs to log in again.

Figure 4-17 Prompt



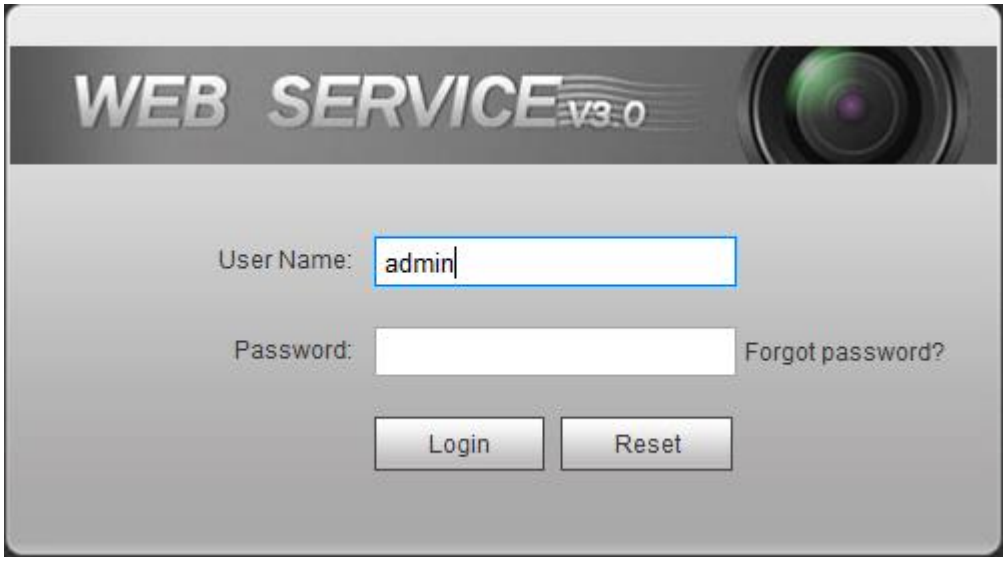
4.2.3 Direct Login

You can directly log in WEB interface if device initialization is completed.

Step 1 Open the browser, enter the device IP address, and then press **Enter**.

After it is successfully connected, the login interface is displayed. See Figure 4-18.

Figure 4-18 Login interface



Step 2 Enter **Username** and **Password**, and then click **Login**.

Step 3 Click Please click here to download and install the plug-in in the picture/ video window.

The interface of **File Download - Security Warning** is displayed. See Figure 4-19

Figure 4-19 File download-security warning

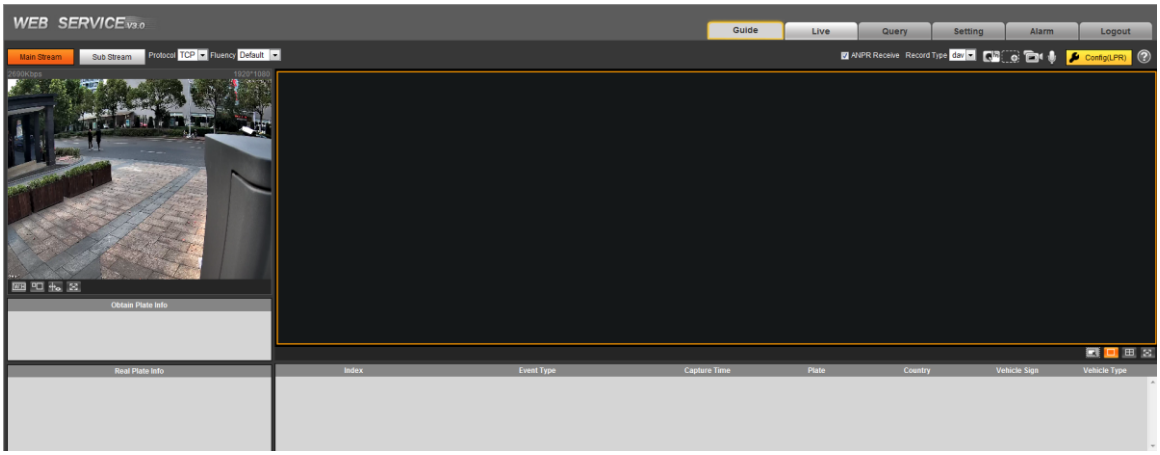
Step 4 Click **Run**.

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

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

After installation is completed, the WEB main interface is displayed. See Figure 4-20.

Figure 4-20 WEB main interface (2)



4.2.4 Password Reset

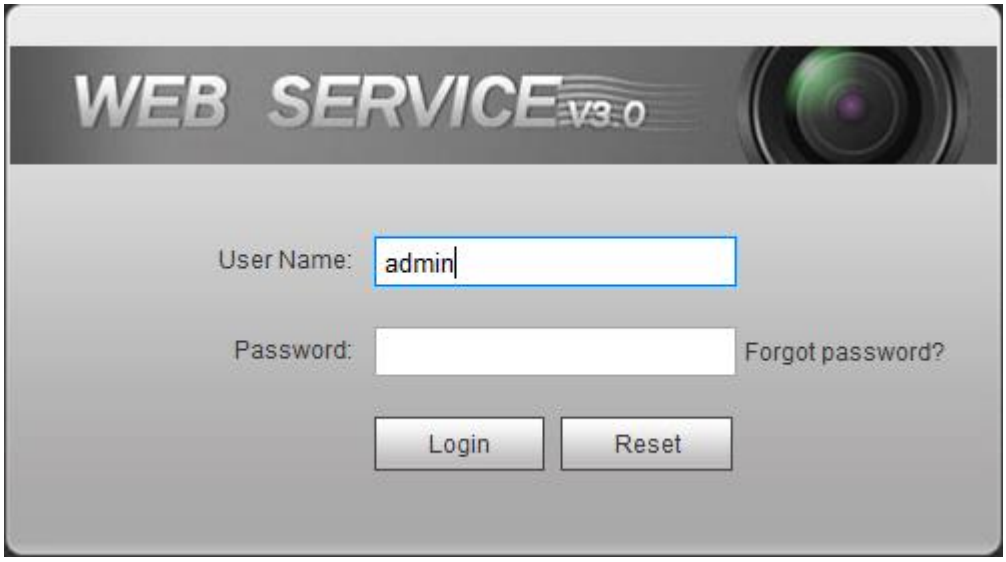
When you forget the password of admin user, you can set new password via password reset function.

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 is allowed to generate security code up to 10 times in one day, so the device is allowed to be reset up to 10 times.
- User email must be filled in during device initialization, which is used to receive security code; otherwise it fails to implement password reset. Reserved email of admin can be modified from **Setting** > **System** > **User** > **User**.

Step 1 Open the browser, enter the device IP address, and then press **Enter**.
The login interface is displayed. See Figure 4-21.

Figure 4-21 Login interface



Step 2 Click Forgot password.
The **Reset the password** interface is displayed. See Figure 4-22

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

Figure 4-22 Reset password (1)

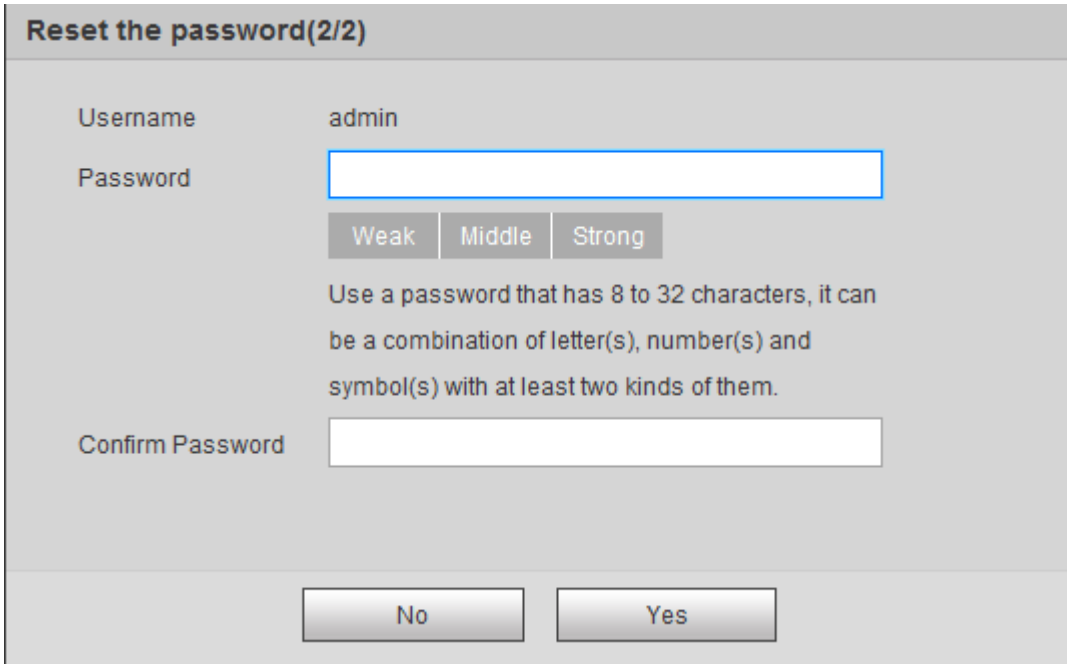
Step 3 Scan the QR code according to the interface prompt, and send the scanning result to designated email and acquire security code.

Step 4 Input received security code in the text box of **Security code**.

Step 5 Click **Next**.

The **Reset the password** is displayed.See Figure 4-23.

Figure 4-23 Reset password (2)



Step 6 Set Password and Confirm Password.

The new password can be set from 8 characters to 32 characters and contains at least two types from capital letter, small letter, number and special characters (excluding “'”, “"”, “;”, “:” and “&”) The new password should be in accordance with the confirm password. Follow the password security notice to set a high security level password.

Step 7 Click **OK** and password reset is completed.

4.2.5 Interface Layout

The chapter mainly introduces the operation of following 6 functions on the WEB interface. SeeFigure 4-24. Please refer to0for more details.

Figure 4-24 Tab

Tab function description

Tab	Function
Guide	It configures basic functions of the camera, including
Preview	Adjust video and image window, record video and image, set client image parameter and so on.
Query	Inquires different types of picture and video, watermark verification of video as well.
Setting	Sets business rules of intelligent traffic, camera basic attribute, network, event, storage, system and view system information.
Alarm	Sets alarm prompt.
Logout	Logs out WEB client.

The following buttons are very common in the WEB interface. Please refer to0 for respective definition.

Common buttons description

Button	Note
Default	Click the button, and click **OK**, then all the parameters will be recovered to system default.
Refresh	Click the button and all the parameters will be recovered to the value which is the latest saved.
OK	Click the button after the parameter config is completed, and then it makes the current setting valid.

The interface and its setting are for reference only, the actual interface shall prevail.

5.1 Guide

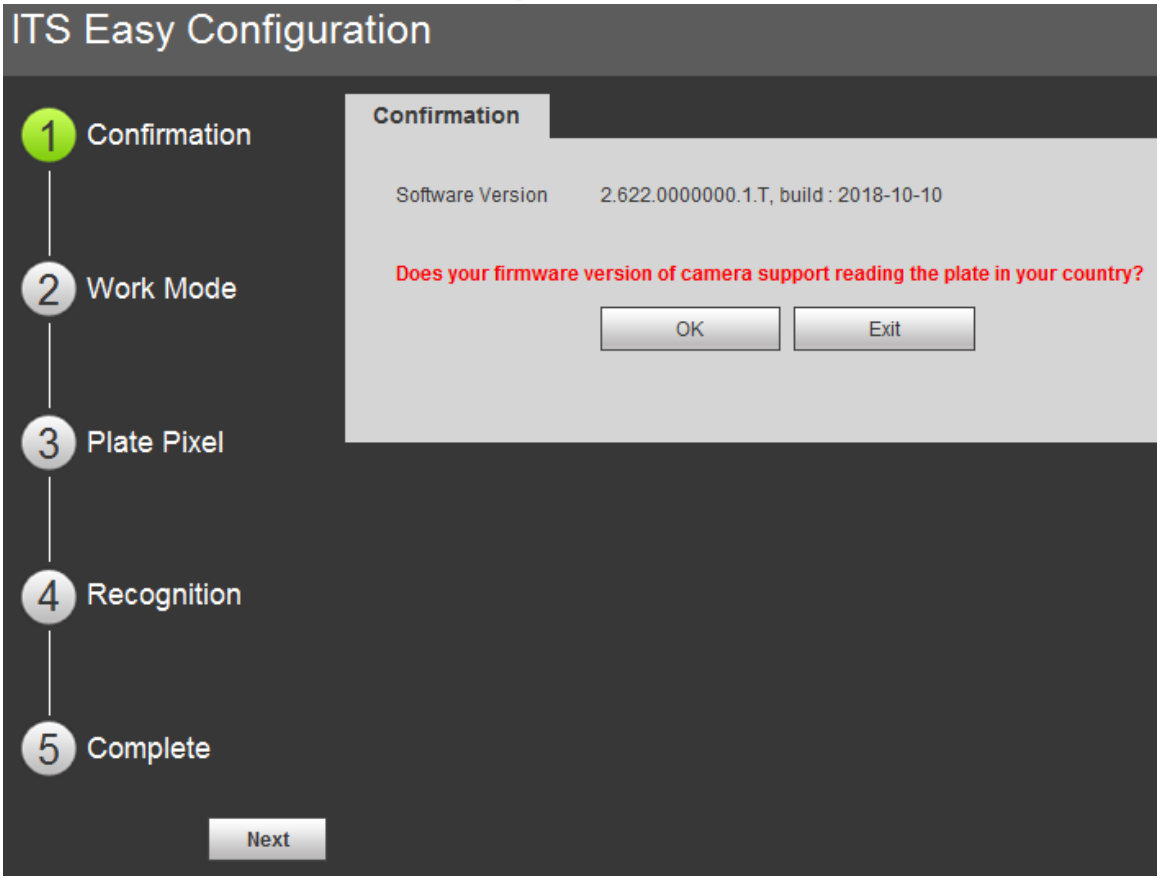
Click the on the upper right corner of guide interface to exit.

It can configure capture scenario and assist user with installation scenario on the guide interface.

Step 1 Click **Guide** tab.

The **Confirmation** interface is displayed. See Figure 5-1.

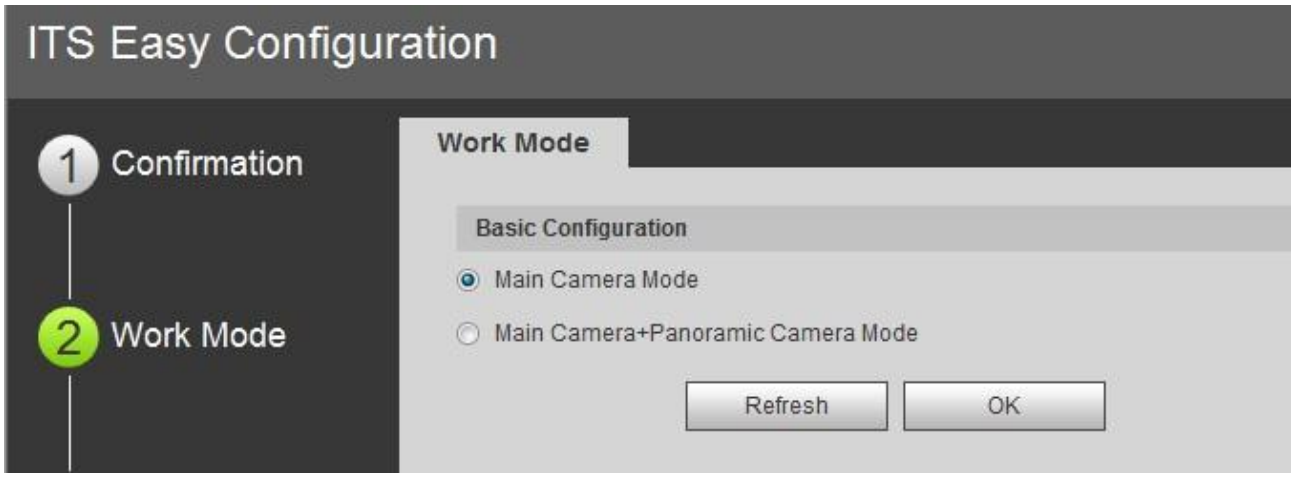
Figure 5-1 Confirmation



Step 2 Confirm **Software Version**, click **OK**.

Work Mode interface is displayed. See Figure 5-2.

Figure 5-2 Work Mode



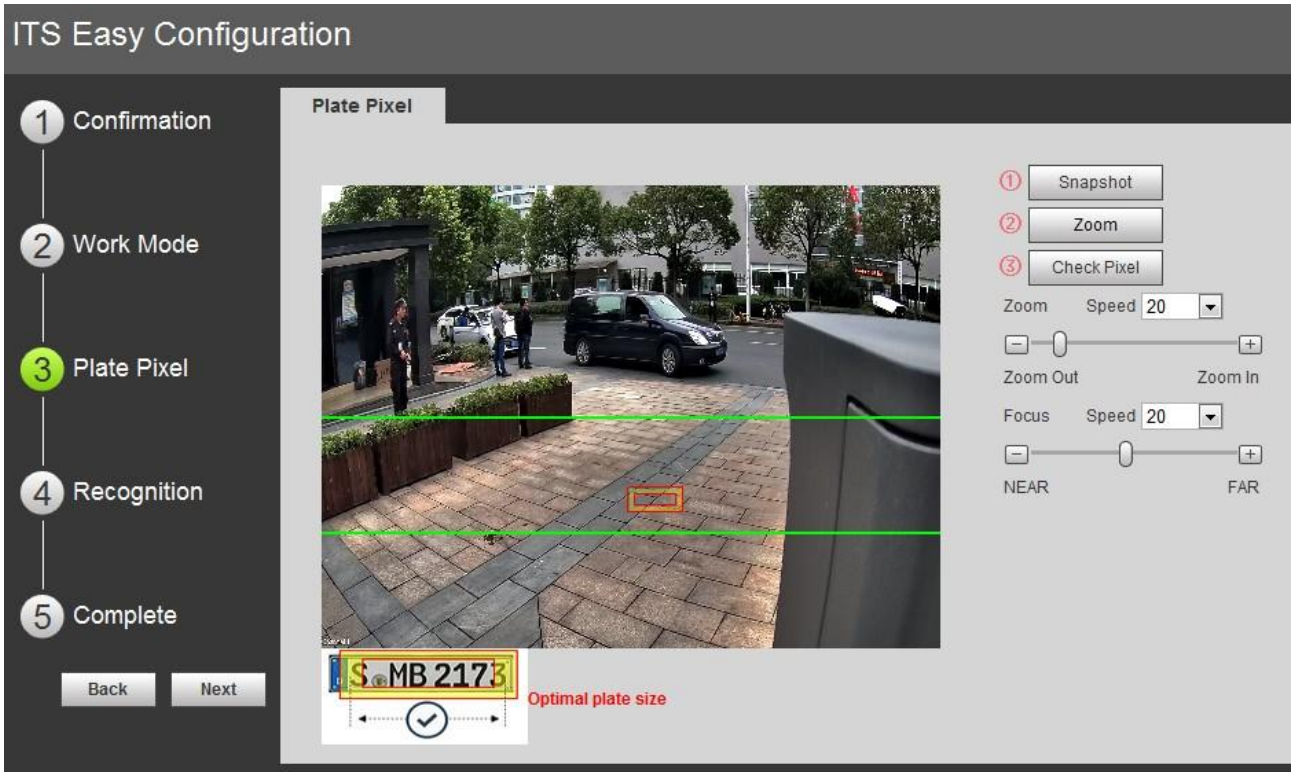
Step 3 Select work mode according to actual requirement.

- Main Camera Mode: Applied to doorways where the vehicle front bumper is straight to the camera for snapshot. Refer to **Standard Construction Scheme** for more details.
- Main Camera + Panoramic Camera Mode: Applied to the doorways where the vehicle front bumper is straight to the camera for both snapshot and surveillance. Refer to **Standard Construction Scheme** for more details.

Step 4 Click **OK**.

The **Plate Pixel** interface is displayed, see Figure 5-3.

Figure 5-3 Plate pixel

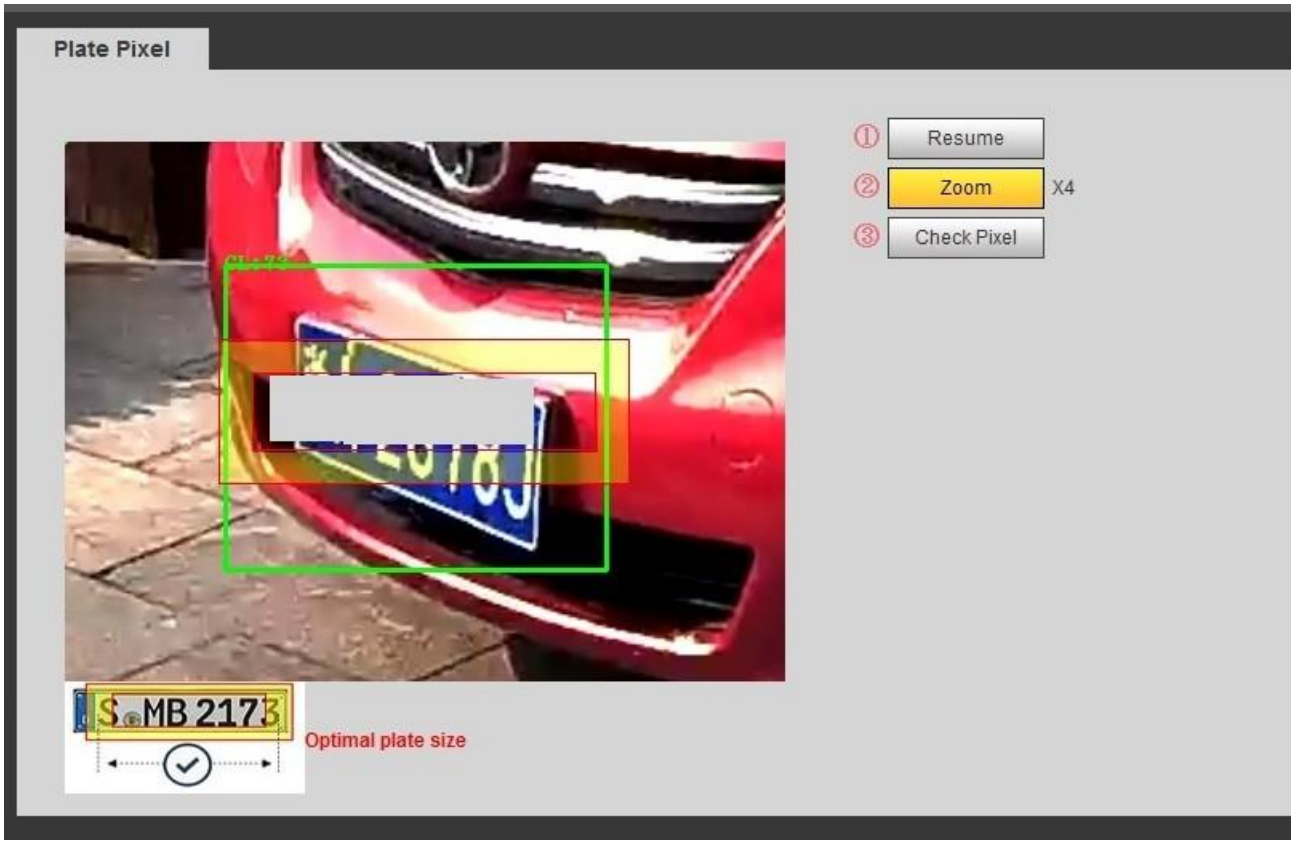


Step 5 Configure plate pixel box and make it the optimal plate size.

1) Drag zoom and focus bar.
   Adjust visual field to the best.
2) Click **Snapshot**.
   Snapshot becomes **Resume**.

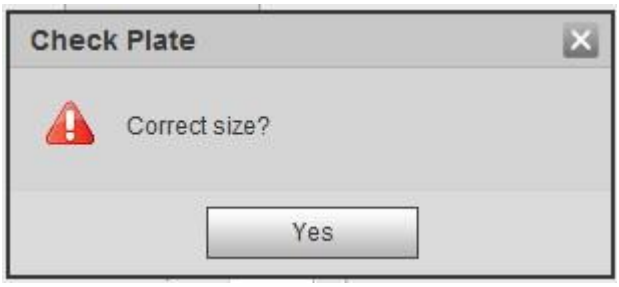
3) Drag the yellow plate pixel box to the plate location.
4) Click **Zoom**.
   Zoom in the picture selected by the plate pixel box. It can realize 2x or 4x zoom rate.
5) Adjust the location of plate pixel box and make it the optimal plate size. See Figure 5-4.

Figure 5-4 Plate pixel size



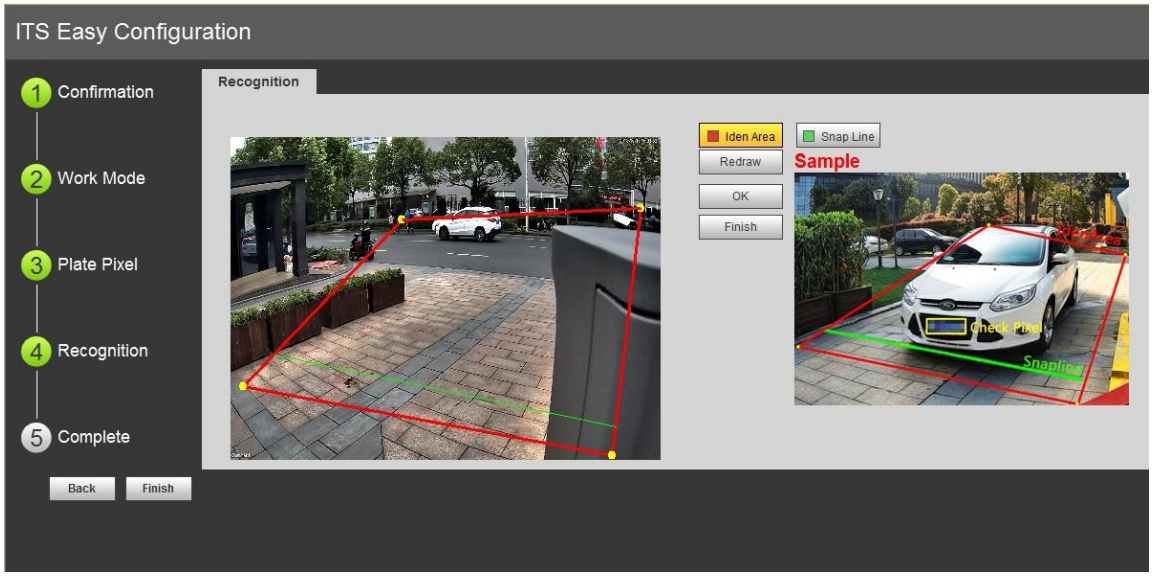
6) Click **Check Plate.**
   The **Check Plate** interface is displayed, see Figure 5-5.

Figure 5-5 Check plate



7) Click **Yes** and plate pixel config is finished.
   The Recognition interface is displayed, see Figure 5-6.

Figure 5-6 Recognition



Step 6 Configure recognition area.

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

1) Click **Iden Area**.

   Click and draw 4 lines on the video interface and the recognition area is formed.

2) Click **Snap Line**.

   Draw snap line via dragging mouse on the area. The snap line must cross the area.

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

Step 7 Click **Finish,** exit guide interface and enter **Live** interface.

5.2 Live

Click **Live** tab. The system will display live interface. On this interface it can realize several functions such as live video, live picture, realtime capture, record and config (LPR) etc.

Figure 5-7 Live

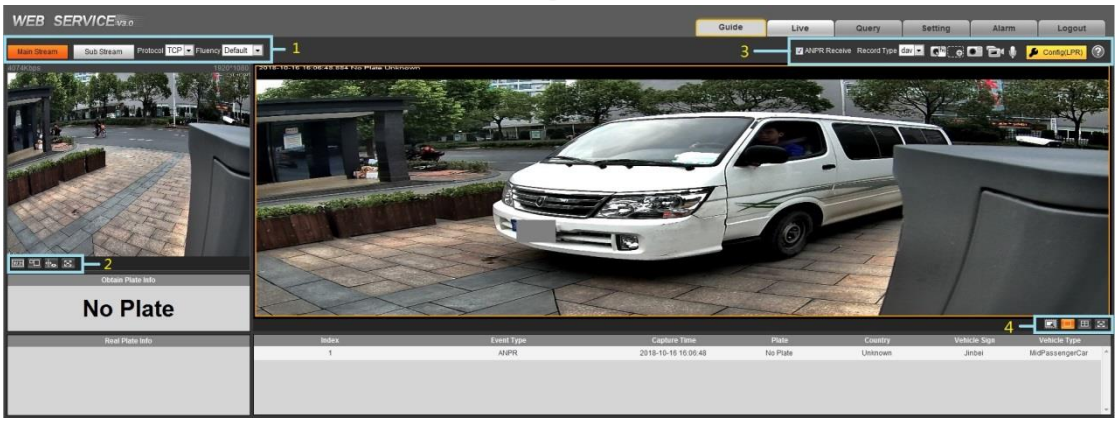


Table 5-1 Live interface bar

No.	Column name
1	Video stream
2	Video window
3	General functions
4	Window picture adjustment

5.2.1 Stream

Set the stream, protocol, fluency and other parameters on the live interface.

Figure 5-8 Stream

Video stream option

Parameter	Note
Main Stream	The device implements video recording and network surveillance in the environment with normal network bandwidth.
Sub Stream	It is used to replace main stream to make network surveillance and reduce the network bandwidth possession when network bandwidth is insufficient.
Protocol	Select video surveillance protocol, currently it only supports TCP.
Fluency	Selects image preview fluency. The fluency can be set as high, medium, low and default.

5.2.2 Video Window Setting Bar

Select the display mode of current live interface.

Figure 5-9 Video Window Setting Column

Table 5-2 Video window setting

Icons	Name	Note
	Width and height ratio	Adjust the image to original size or appropriate window.
	Window switch	Switch to big window and display image adjustment window.
	Smart track frame	Click to enable smart track detection. License plate, vehicle detection box and other smart tracks will be displayed on the video.
	Full screen display	Click it and the window is displayed with full screen; double click or ring-click to exit full screen.

Click  to switch to big window.

Figure 5-10 Big window

Table 5-3 Video window setting in big window

Icons	Name	Note
	Image adjustment	Image adjustment button. Click it and open image adjustment window on the right, meanwhile the button becomes orange. Click  to close image adjustment window.
	Original size	Image size adjustment button Click it and the image is 100% displayed, meanwhile the button becomes orange. Click  to switch back to original size.

Click  and display image adjustment window on the right.

Figure 5-11 Image adjustment window

- The function can only adjust image brightness, contrast, hue and saturation of local WEB.
- As for the adjustment of system brightness, contrast, hue and saturation, it needs to go to **Setting** > **Camera** > **Image** and make settings.

Table 5-4 Image adjustment

Icons	Name	Note
	Brightness	Adjust monitoring image brightness. The range is from 0 to 128. It is 64 by default.

	Contrast	Adjust monitoring image contrast. The range is from 0 to 128. It is 64 by default.
	Hue	Adjust monitoring image hue. The range is from 0 to 128. It is 64 by default.
	Saturation	Adjust monitoring image saturation. The range is from 0 to 128. It is 64 by default.
Reset	—	Click the icon to restore brightness, contrast, saturation and hue to default value.

5.2.3 General Function Option Column

In this chapter, it is to implement operations such as image and video capture, zoom, record and talk etc.

Figure 5-12 General Function Option Column

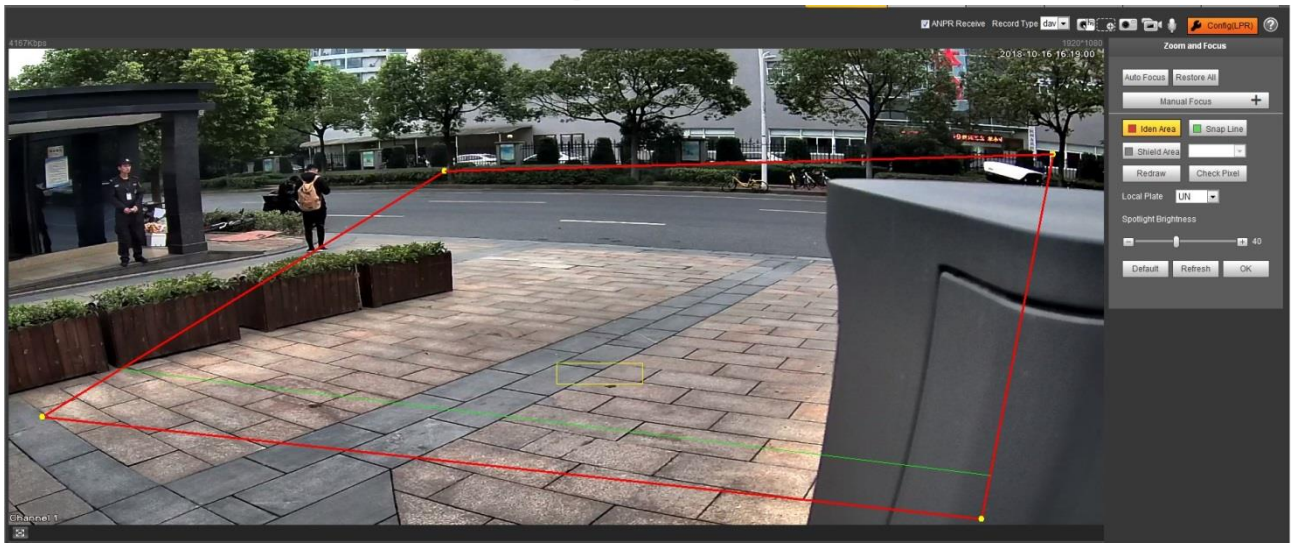
Table 5-5 General function option

Icons	Name	Note
	ANPR Receive	Check it and the system will automatically receive triggered pictures, record plate, logo and associated info, which will be displayed on the bottom of the page.
	Record Type	Select the format of record file, it is dav by default. It is required to be ps for GB 28181.
	Manual Snapshot	Click the button and the device takes a snapshot and it is saved in the storage path. It needs to select **ANPR Receive** first, and then the captured picture and vehicle info will be displayed on the live interface.
	Regional Zoom	Drag left mouse button and select any area within the video window, and then the area will be zoomed in. In any area of the video window, click right mouse button, or left mouse button to click and exit.
	Record	Click to start recording. Click again to stop recording.
	Talk	Click to enable talk. Click again to end talk.
	Config (LPR)	It is able to draw the area of plate detection, adjust camera's focal length and set local character etc.

Click 

, enter the interface of Config (LPR).

Figure 5-13 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 5-6for more details.

Table 5-6 Focus parameter description

Parameter	Note
Auto Focus	Auto adjust camera lens and make the scenario clearly focused.
Manual Focus	Manually set focus parameter and make the camera focus on the vehicle. ● Zoom: ◇ Step length: There are totally 3 levels to be selected. ◇ Zoom in, zoom out: Click + and add a step length, click − and reduce a step length; Or directly drag adjustment bar and set zoom. ● Focus: ◇ Step length: There are totally 3 levels to be selected. ◇ Focal length: Click + and add a speed, click − and reduce a speed; or it can directly drag adjustment bar to set near and far focal length.
Restore All	All is restored to initialization settings.
Refresh	Check the latest status.

Step 2 Select the config line type which needs to be drawn. Refer to Table 5-7 for more details.

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

Table 5-7 Config line parameters description

Parameter	Note
Recognition	Click it and draw the area range which needs to be detected. The recognition area line is displayed as red box.

Parameter	Note
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.
Shielded 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.
Optimal Plate	Click it and drag the yellow plate pixel box to proper location on the video interface.

Step 3 Draw lines on the view interface.

Click **Redraw** to delete config line one by one.

Step 4 Adjust the vehicle snapshot location to yellow box.

Try to make sure the location and size of plate is in accordance with that of the yellow line box.

Plate optimal width rangevalue is from 140 to 160, If it needs to be modified, go to Setting > Smart Traffic > Smart Parameter >Smart Analysis > Recognition Config and make setting.

Step 5 Set **Local Character**. Set local character according to the device location.

Step 6 Set **Built-in NO Brightness**. Drag the block and set brightness of NO light according to actual requirement.

Step 7 Click **OK** to finish configuration.

5.2.4 Window Picture Adjustment Bar

Select the picture display mode of the live interface.

Figure 5-14 Window Picture Adjustment Column

Table 5-8 Window picture adjustment

Icons	Name	Note
	Selected window	View the pixel of selected area and it can be used to check plate width.
	Single window	Display the picture with one window.
	Four window	Display the picture with four windows.
	Full screen window	Display the picture with full screen.

5.3 Query

Click **Query** tab and the system displays query interface where users can inquire picture and record info.

5.3.1 Picture Query

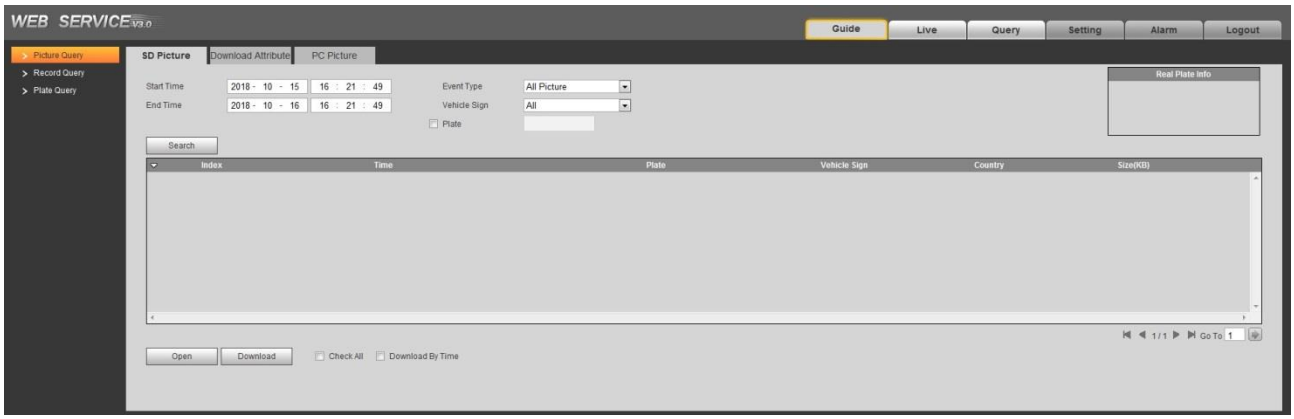
5.3.1.1 SD Picture

Query condition can be set in this section. It inquires the event info and plate info of the SD card within the period.

Step 1 Select Query > Picture Query > SD Picture.

The **SD Picture** interface is displayed. See Figure 5-15.

Figure 5-15 SD Picture



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-9 for more details.

Table 5-9 SD picture parameter description

Parameter	Note
Start Time	Set the start time of picture query.
End Time	Set the end time of picture query.
Event Type	Inquire all pictures, or it can inquire the pictures which conform to requirements according to filtering condition based on violation type.
Vehicle Logo	Take vehicle logo as query condition, then it can select one or all.
Plate	Select **Plate**, take plate feature as query condition and then inquire the pictures which conform to requirements. It can also set some parameters of the plate and realize fuzzy query of plate no.

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

Click some line in the list and the plate picture info will be displayed in the **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 and 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.

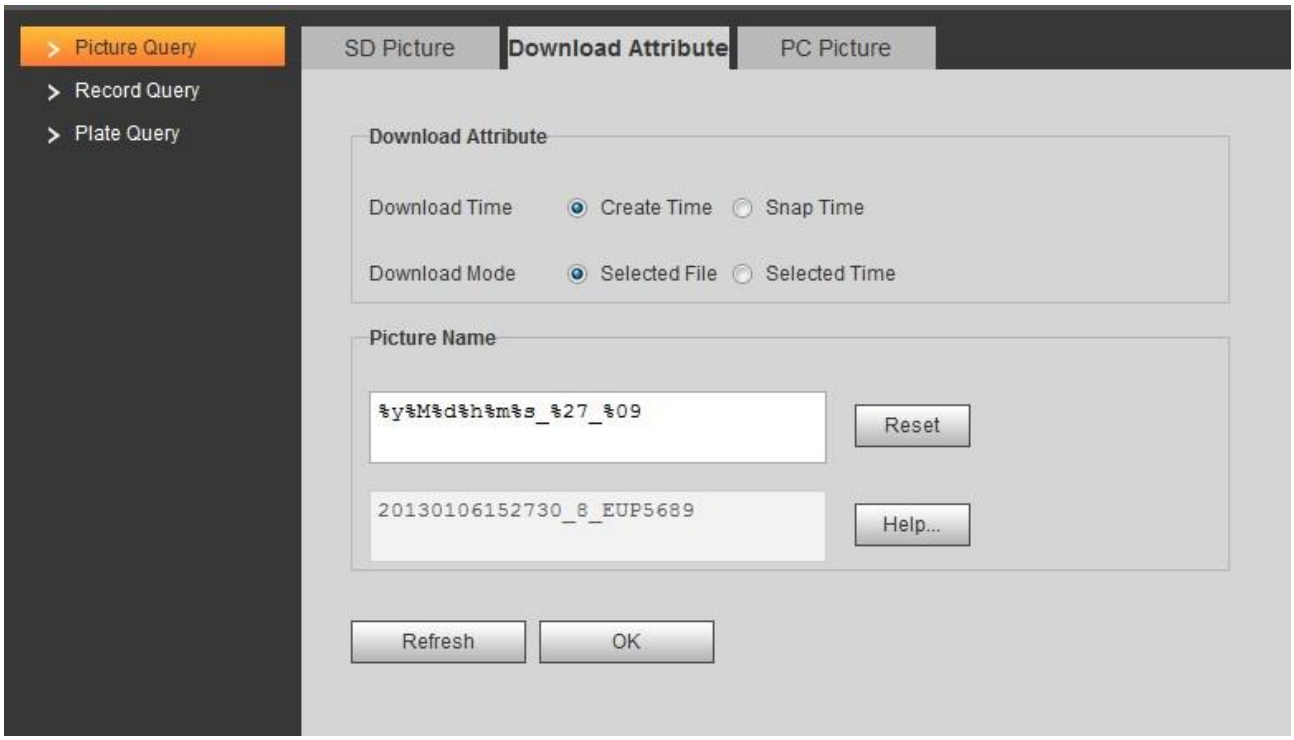
5.3.1.2 Download Picture Attribute

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.

The **Download Attribute** interface is displayed. See Figure 5-16.

Figure 5-16 Download attribute



Step 2 Configure the parameters. Please refer to Table 5-10 for more details.

Table 5-10 Download attribute parameters description

Parameter	Note
Download Time	● Create time: It uses PC time when the picture is downloaded to PC. ● Snap time: It uses device snapshot time when the picture is downloaded to PC.
Download Mode	● Selected file: Select the needed picture (It supports selecting single picture or several pictures at the same time, which is download in batches), click Download and the system will pop out the save dialog box. ● Selected time: Click **Download** and the system will automatically download all the pictures from start time and end time.
Reset	Restore the picture name to the system default name.
Help	View the naming rule of downloaded pictures.

Step 3 Click **OK** to finish configuration.

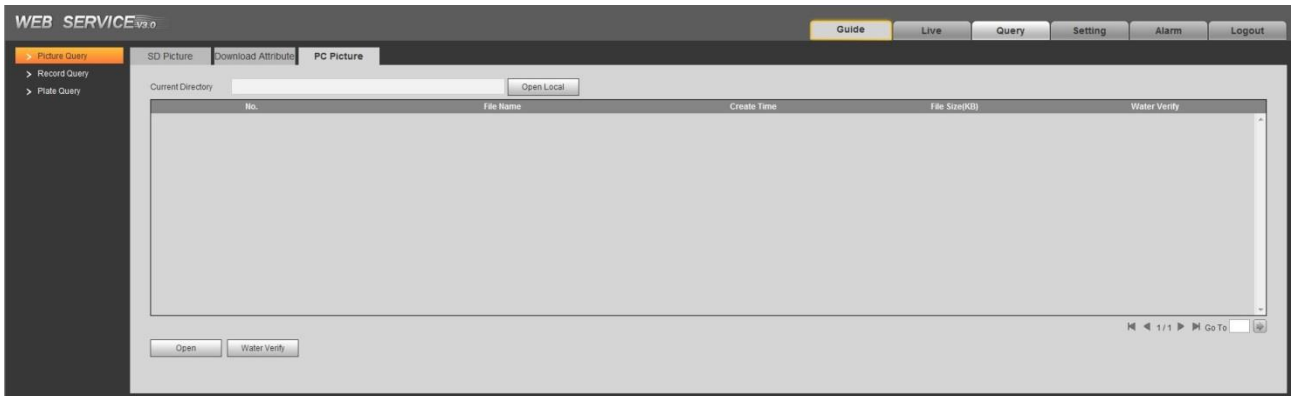
5.3.1.3 PC Picture

In this section, it is to check if the watermark of PC picture is tampered.

Step 1 Select Query > Picture Query > PC Picture.

The **PC Picture** interface is displayed. See Figure 5-17.

Figure 5-17 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 **Watermark Verify** and view result in the picture list.

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

5.3.2 Record Query

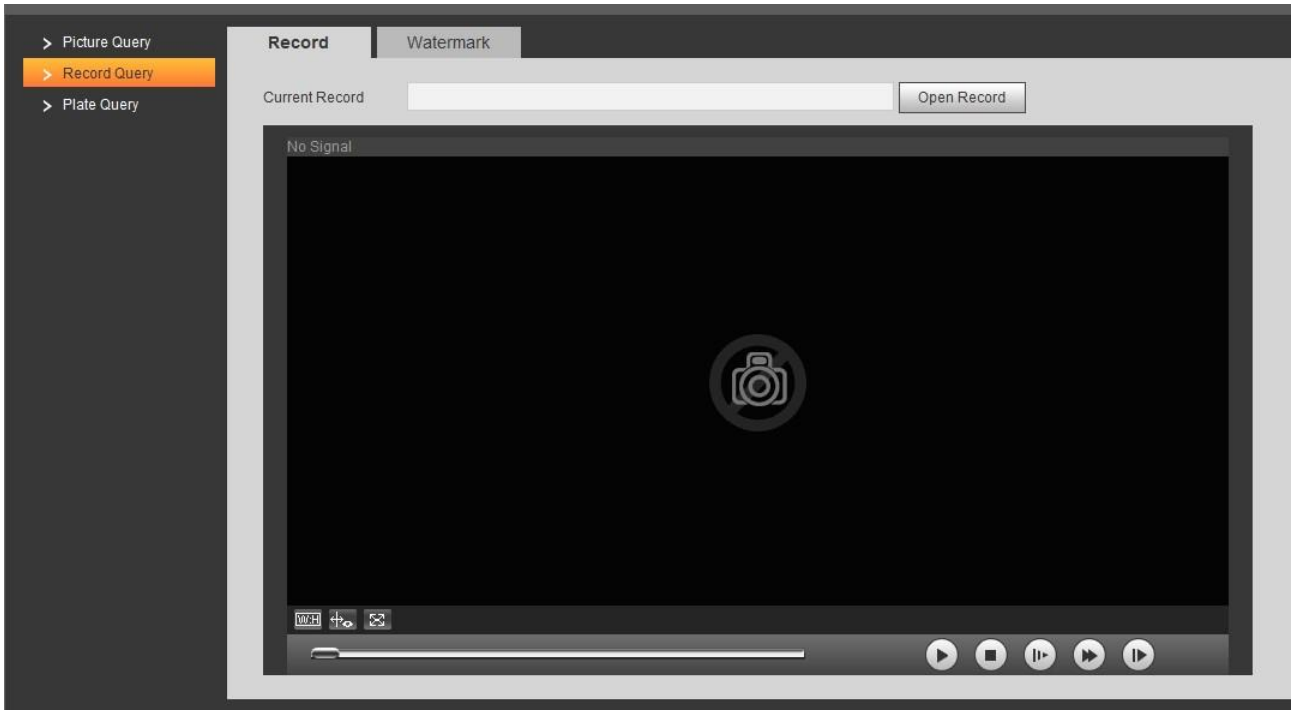
5.3.2.1 Record

It can realize playing video of local PC on this interface.

Step 1 SelectQuery > Record Query > Record.

The **Record** interface is displayed, see Figure 5-18.

Figure 5-18 Record



Step 2 Click **Open Record**, select record path, click **Open** and view the video.
For the function description of video play button, see Table 5-11.

Table 5-11 Play function description

Icons	Name	Note
	Play/Pause	● When it displays  , then it means pause or not played. Click it to switch to normal play status. ● When it displays  , then it means playing video. Click it to pause.
	Stop	Click the icon to stop playing video.
	Play by Frame	Click the icon to skip to the next frame.
	Slow-down Play	Click this icon to slow down video playing.
	Speed-up Play	Click this icon to speed up video playing.

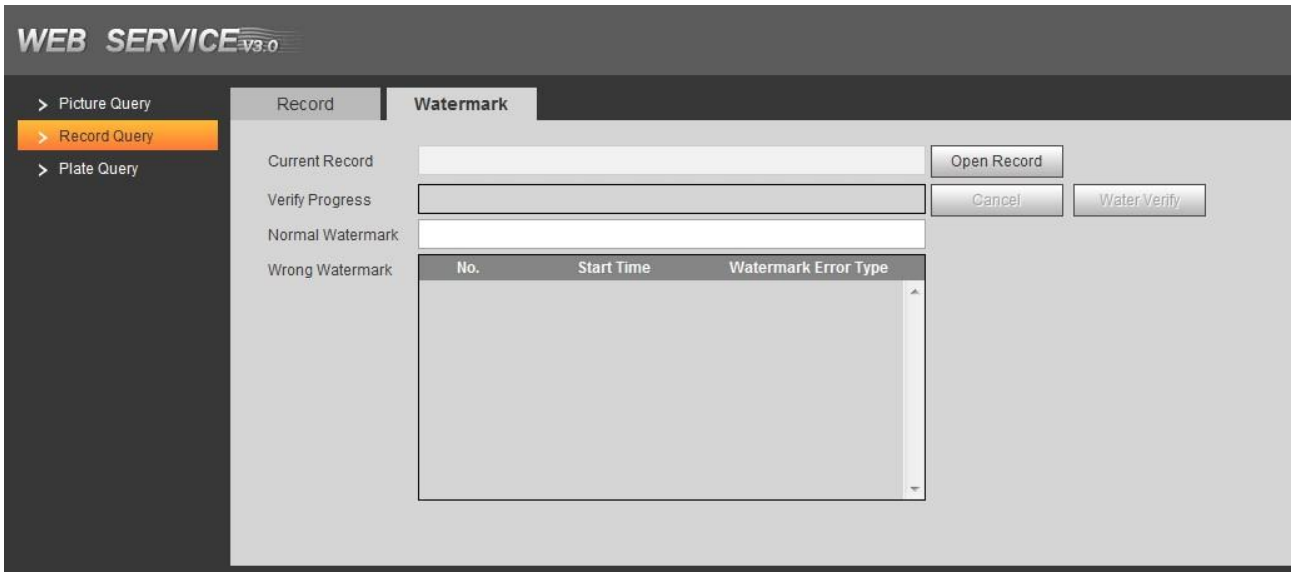
5.3.2.2 Watermark

It needs to go to **Setting** > **Camera** > **Stream** > **Video Stream** and select watermark setting if you want to enable the function, and set corresponding watermark character. The default watermark character is DigitalCCTV.

In this section, it is able to verify if the watermark of local record is tampered.

Step 1 Select Query > Record Query > Watermark.
The **Watermark** interface is displayed. See Figure 5-19.

Figure 5-19 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 info.

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

5.3.3 Plate Query

- It supports max 10,000 records and 1024 records respectively when the camera is installed with SD card or not.
- If the passing vehicle records are unreadable in excel after being imported, change them into UTF-8 encoding in txt and then they can be opened normally.

Set start time and end time, inquire the vehicle record within the period.

Step 1 Select Query > Plate Query > Plate Query.

The **Plate Query** interface is displayed. See Figure 5-20.

Figure 5-20 Plate Query

Step 2 Set **Start Time** and **End Time** for query.

Step 3 Click **Query**, select storage path and export the result to PC.

Step 4 Click **Export**, select storage path and export the result to PC.

5.4 Setting

In this interface, you can configure several parameters such as ITC, camera, network, event, storage, system and system info etc.

5.4.1 ITC

In this section, you can set business rules of ITC.

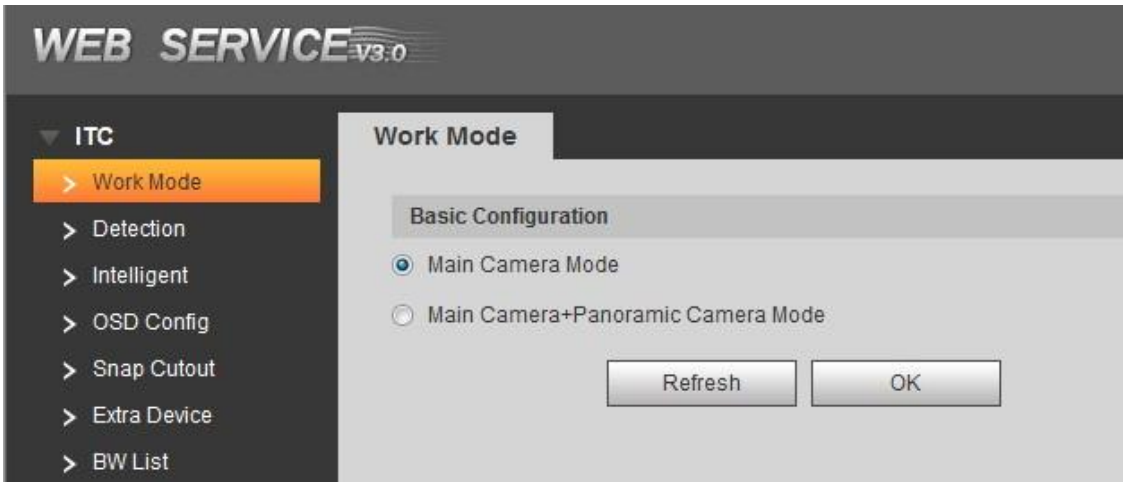
5.4.1.1 Work Mode

Select proper work mode according to actual scenario.

Step 1 Select Setting > ITC > Work Mode.

Work Mode interface is displayed. See Figure 5-21.

Figure 5-21 Work Mode



Step 2 Select work mode.

- Main Camera Mode: Applied to doorways where the vehicle front bumper is straight to the camera for snapshot. Refer to *Standard Construction Scheme* for more details.
- Main Camera + Panoramic Camera Mode: Applied to the doorways where the vehicle front bumper is straight to the camera for both snapshot and surveillance. Refer to *Standard Construction Scheme* for more details.

Step 3 Click **OK** to finish configuration.

When work mode is selected as **Main Camera Mode + Panoramic Camera Mode**, then **Panoramic Camera** will be displayed in the video stream bar on the upper left corner of the **Live** interface.

5.4.1.2 Detection

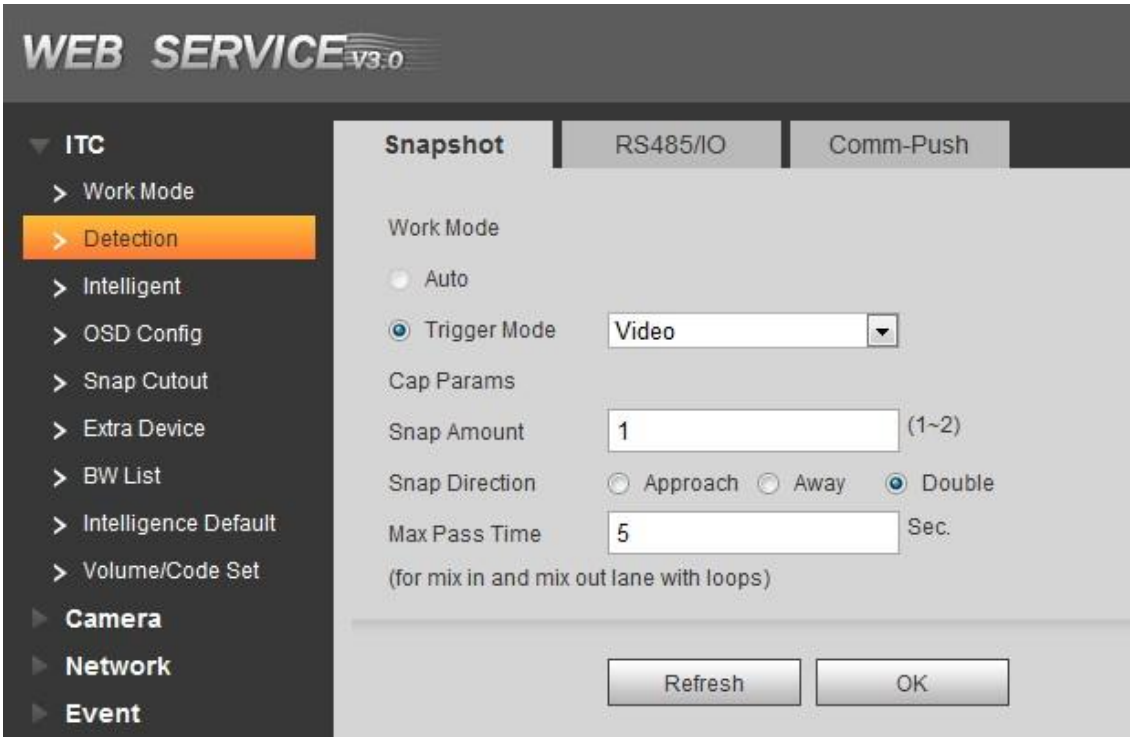
5.4.1.2.1 Snapshot

In this section, you can set snapshot rule of the device.

Step 1 Select Setting > ITC > Detection > Snapshot.

The **Snapshot** interface is displayed, see Figure 5-22.

Figure 5-22 Snapshot



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-12 for more details.

Table 5-12 Snapshot setting parameters description

Parameter		Note
Work Mode	Auto	Automatically select work mode according to actual scenario.
	Manual	● Loop: Forced to use loop for snapshot. ● Video: Forced to use video for snapshot. ● Mix: Forced to use coil + video mixed mode to take snapshot.
ANPR Parameters	Snapshot Amount	It can take 1 to 2 snapshots.
	Snapshot Direction	● Approach: Capture the entered vehicles. ● Away: Capture the exited vehicles. ● Double: Both entered and exited vehicles are captured.
	Max pass time	Input max vehicle passing time, the unit is s, it is 5s by default. For example, set max vehicle passing time as 5s, 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 5s.

Step 3 Click **OK** to finish configuration.

5.4.1.2.2 I/O

In this section, it will configure 485 interface associated config info and loop IO snapshot config.

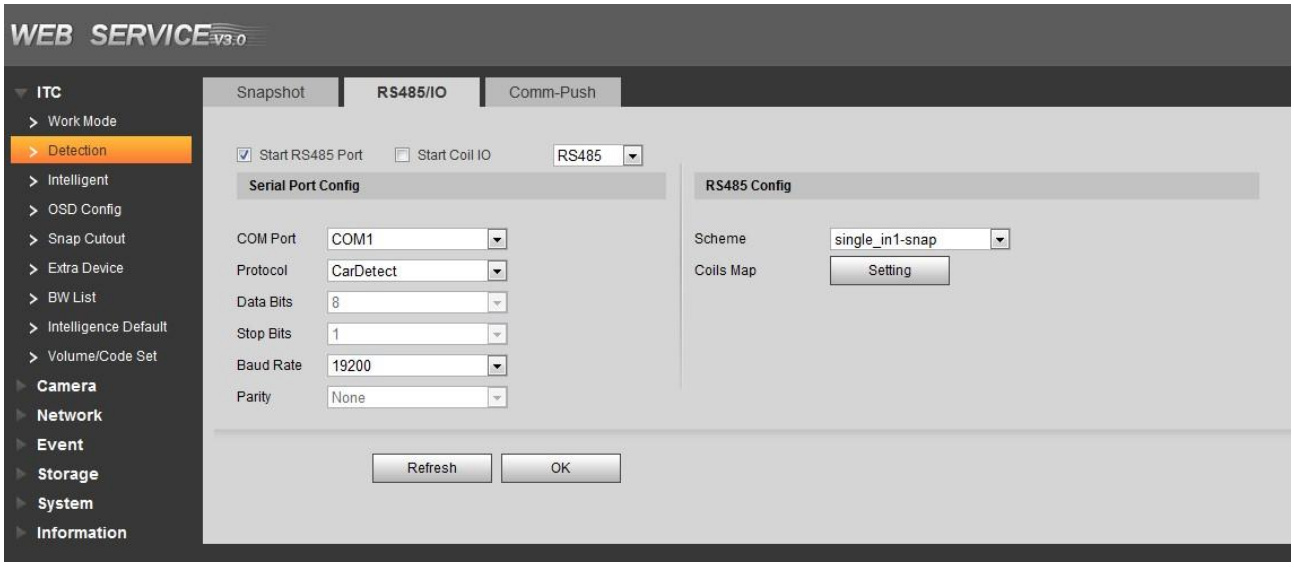
Select **Setting** > **ITC** > **Detection** > **I/O**, the **I/O** interface is displayed.

Start RS-485 port

Step 1 Select Start RS-485 Port, but not Start Coil IO

The **Setting** interface is displayed. See Figure 5-23.

Figure 5-23 RS485/IO（Start RS485）



Step 2 Select **COM Port**, and then you can select COM 1, COM 2 and COM3.

- Select COM1 and support vehicle detector, transparent 485 and com port push protocol.
- Select COM2, support transparent 485 and com port push protocol.
- Select COM3, support transparent 485, transparent 232 and com port push protocol.

Step 3 Select **Protocol**, and set protocol type according to the number of com port.

- Select **Car Detect** from **Protocol**. The setting steps are shown as follows.

1) Set the baud rate of the protocol.
2) Select scheme.
   - ◇ Single_in 1 snapshot: Lay single coil and it will take snapshot when the vehicle enters coil.
   - ◇ Vehicle_double_in 1 snapshot: Lay double coil and it will take snapshot when the vehicle enters the first coil.
   - ◇ Vehicle_double_in 2 snapshot: Lay double coil and it will take snapshot when the vehicle enters the second coil.
3) Click **Setting** and it pops up the dialog box of **Coil Map**. Select the corresponding relationship between logical coil and physical coil and click **OK**.

- The function needs to be configured in the mix in and mix out mode. Please refer to *Standard Construction Scheme* for more details.
- When the scheme is **Single_in_1 snapshot**, then it only needs to select the corresponding physical coil of logical coil.
- For **Protocol**, it selects **Transparent 485** or **Transparent 232**. The steps are shown as follows.

1) Select the baud rate of the protocol and complete setting.
2) If it needs test, then it needs to select **Hexadecimal Push**. Click **Open** on the right of reception area and test the reception status of transparent 485 according to actual situation.

- For **Protocol**, it selects **COM Push**. The setting steps are shown as follows.

Select the baud rate of the protocol and complete setting.

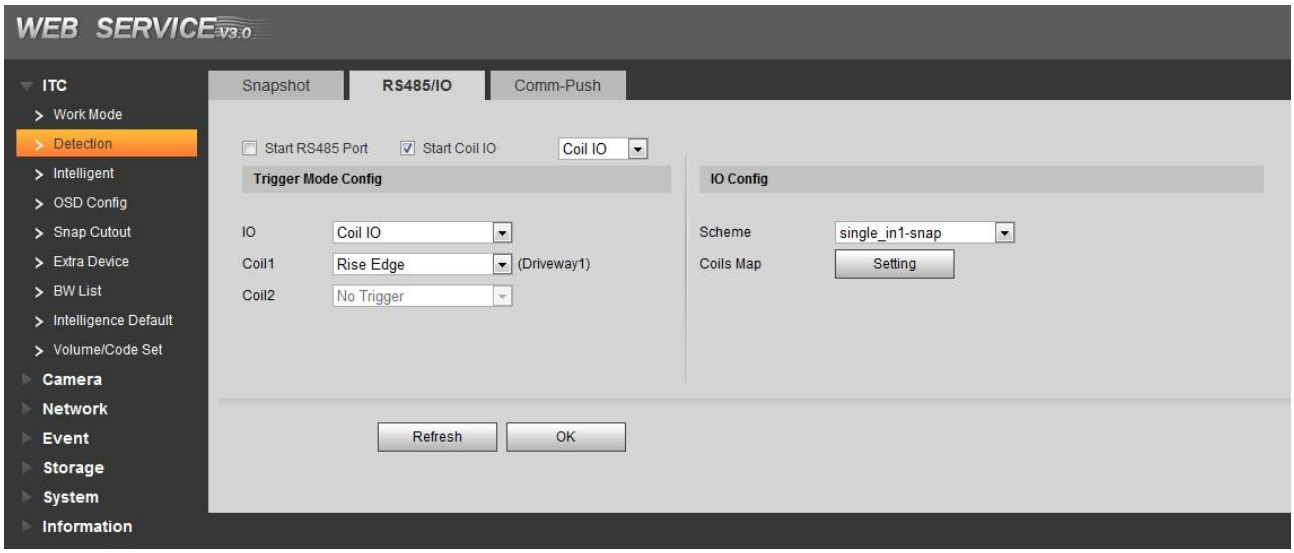
Step 4 Click **OK** to finish configuration.

Start Coil IO

Step 1 Select Start Coil IO butnot select Start RS485 Port.

The **Setting** interface is displayed. See Figure 5-24.

Figure 5-24 I/O (Start Coil IO)



Step 2 Configure the parameters. Please refer to Table 5-13 for more details.

Table 5-13 Coil IO parameters description

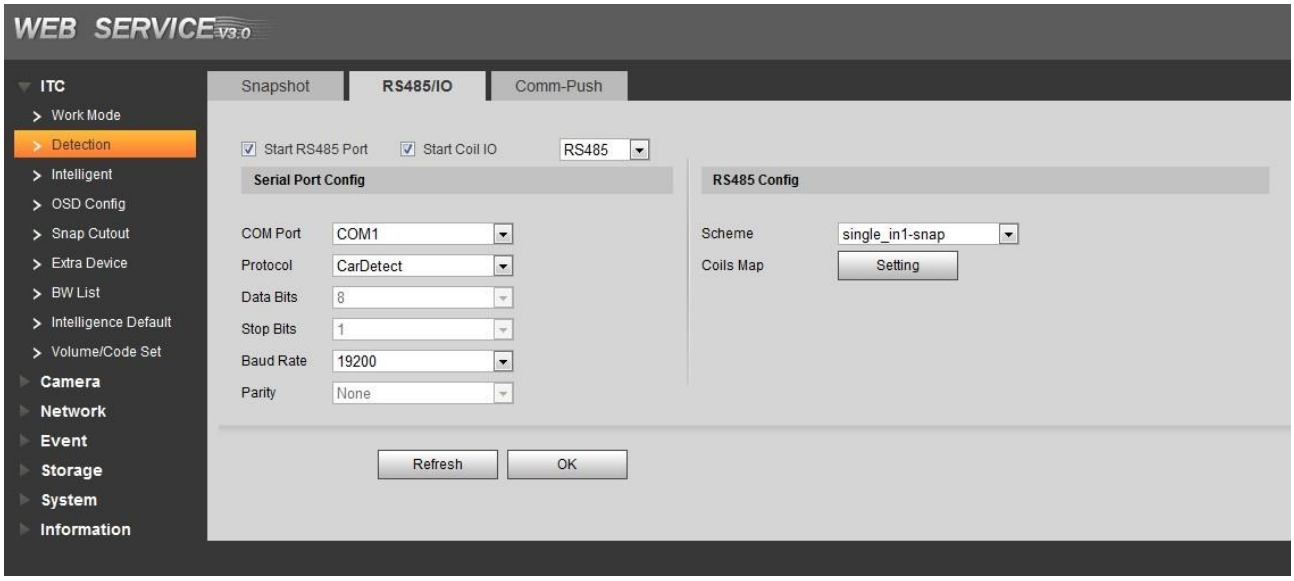
Parameter		Note
Trigger Mode Config	IO	Select IO, and only **Coil IO** can be selected here.
	Coil 1	Set the coil trigger mode. ● No trigger: No snapshot is triggered. ● Rise Edge: Snapshot is triggered when the vehicle enters coil. ● Fall Edge: Snapshot is triggered when the vehicle exits coil. When the scheme is **Single_in_1 snapshot**, then coil 2 can not be set.
	Coil 2	
IO Config	Scheme	Set IO snapshot scheme. ● Single_in 1 snapshot: Lay single coil and it will take snapshot when the vehicle enters coil. ● Vehicle_double_in 1 snapshot: Lay double coil and it will take snapshot when the vehicle enters the first coil. ● Vehicle_double_in 2 snapshot: Lay double coil and it will take snapshot when the vehicle enters the second coil.
	Coil Map	Select the corresponding relationship between logical coil and physical coil.

Step 3 Click **OK** to finish configuration.

Start RS485 and coil IO at the same time

Select Start Coil IO and Start RS-485 Port at the same time, and then it can realize the vehicle snapshot config of coil IO and RS-485 port config. See Figure 5-25.

Figure 5-25 I/O (Start RS-485 and Coil IO)



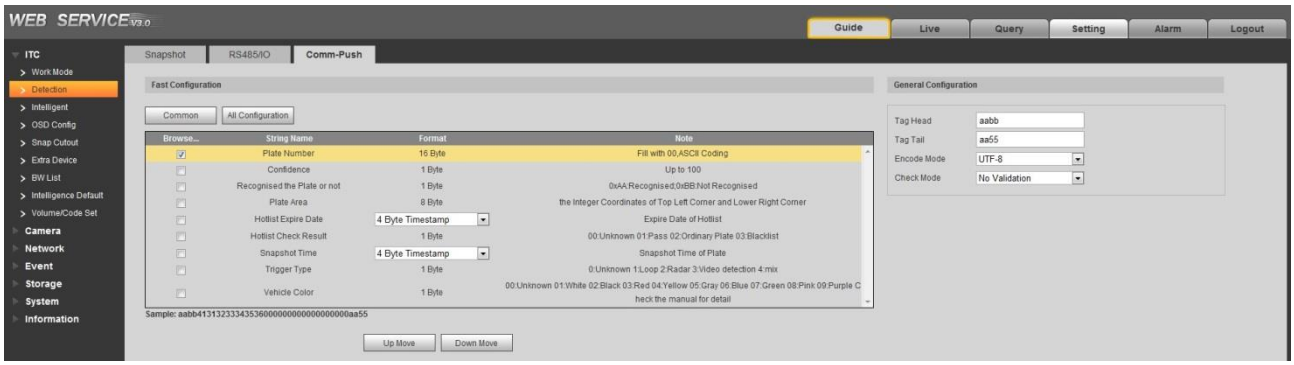
5.4.1.2.3 Com Push

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

Step 1 Select Setting > ITC > Detection > Com Port.

The **Com Push** interface is displayed. See Figure 5-26.

Figure 5-26 Com Push



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-14 for more details.

Table 5-14 Com Push

Parameter	Note
Fast Configuration	Select fast configuration mode, which includes common config and all config. ● Common config: Click it and select the common vehicle passing option. ● All config: Click it and select all the vehicle passing options in the list.
General Configuration	Configure picture data information. ● Tag Head: Com port protocol head, the standard is 4 bit, it can only input hexadecimal character. ● Tag Tail: Com port protocol tail, the standard is 4 bit, it can only input hexadecimal character. ● Encode mode: It is the encoding mode of Com port push content. ● Check mode: verification mode of com port protocol.

● Up Move: Click it and select the corresponding option and move up.

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

5.4.1.3 Intelligent

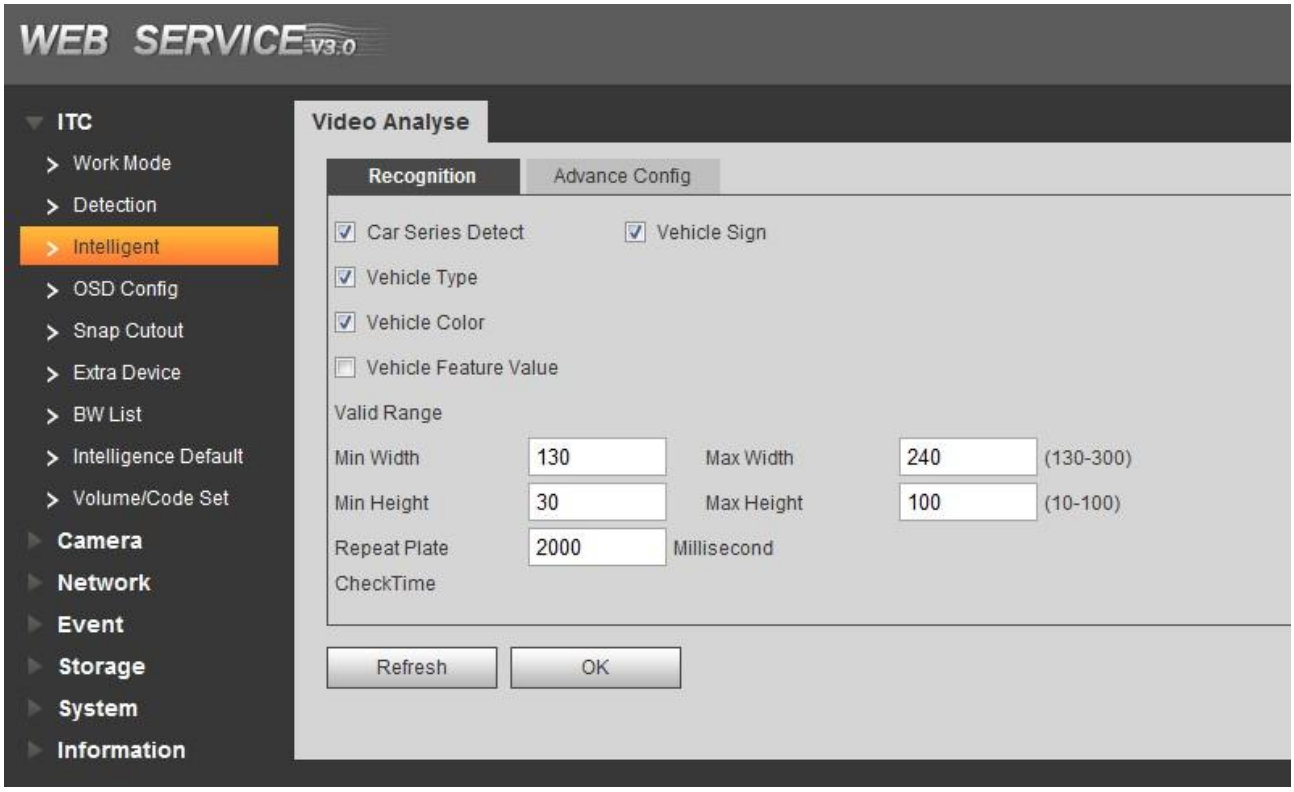
5.4.1.3.1 Recognition

In this section, you can set vehicle recognition parameter, recognition mode and some other functions.

Step 1 Select Setting > ITC > Intelligent > Video Analysis > Recognition.

The **Recognition** interface is displayed. See Figure 5-27.

Figure 5-27 Recognition



Step 2 Configure the parameters. Please refer to Table 5-15 for more details.

Table 5-15 Recognition parameters description

Parameter	Note
Car Series Detect	Select parameters of car series recognition according to requirement.
Vehicle Logo	
Vehicle Type	
Vehicle Color	
Non-Structured Data	
Plate Size	Set plate's min width, max width; min height and max height. The unit is pixel. The setting item is combined with config (LPR) or guide plate pixel on the live interface, which is used to set the optimal location of plate and the optimal width of the location. Try to make sure the location and size of plate is in accordance with that of the yellow line box.

Parameter	Note
Repeat plate detection time	One plate can only trigger one ANPR event within the period.

Step 3 Click **OK** to finish configuration.

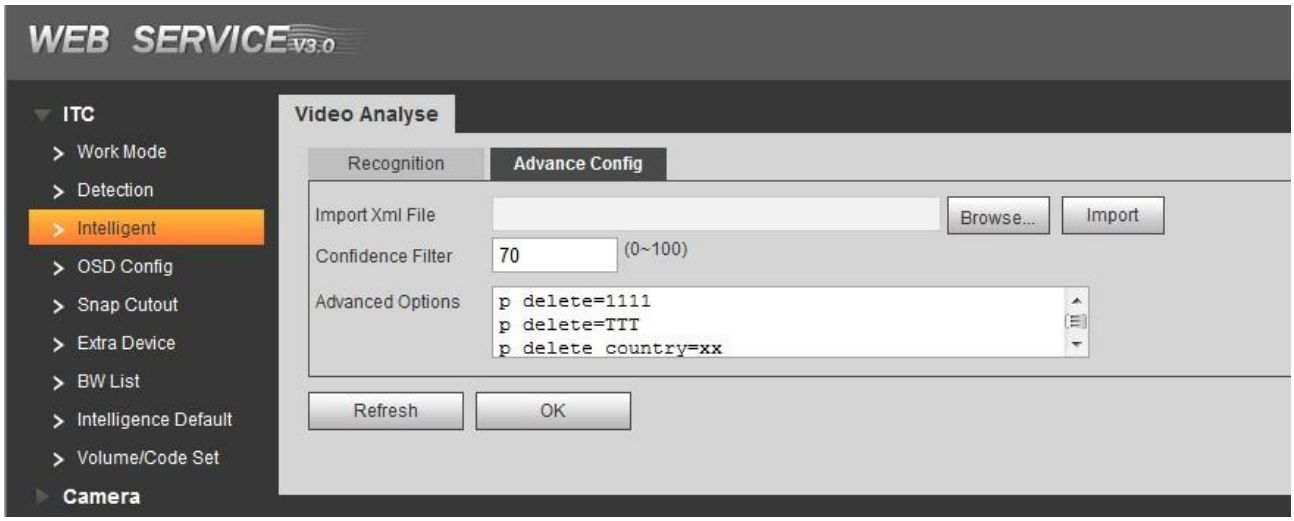
5.4.1.3.2 Advance Config

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

Step 1 Select Setting > ITC > Intelligent > Video Analysis > Advance Config.

The Advance Config interface is displayed. See Figure 5-28.

Figure 5-28 Advance Config



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-16 for more details.

Table 5-16 Advance config parameters description

Parameter	Note
Plate confidence filtering	Confidence level, used to set the range of limiting plate recognition condition, adjustment range is from 0 to 100. ● 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. ● 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.
Algorithm Customized Expression	Inputs customized algorithm expression and realize customized special function.

Step 3 Click **OK** to finish configuration.

5.4.1.4 OSD Config

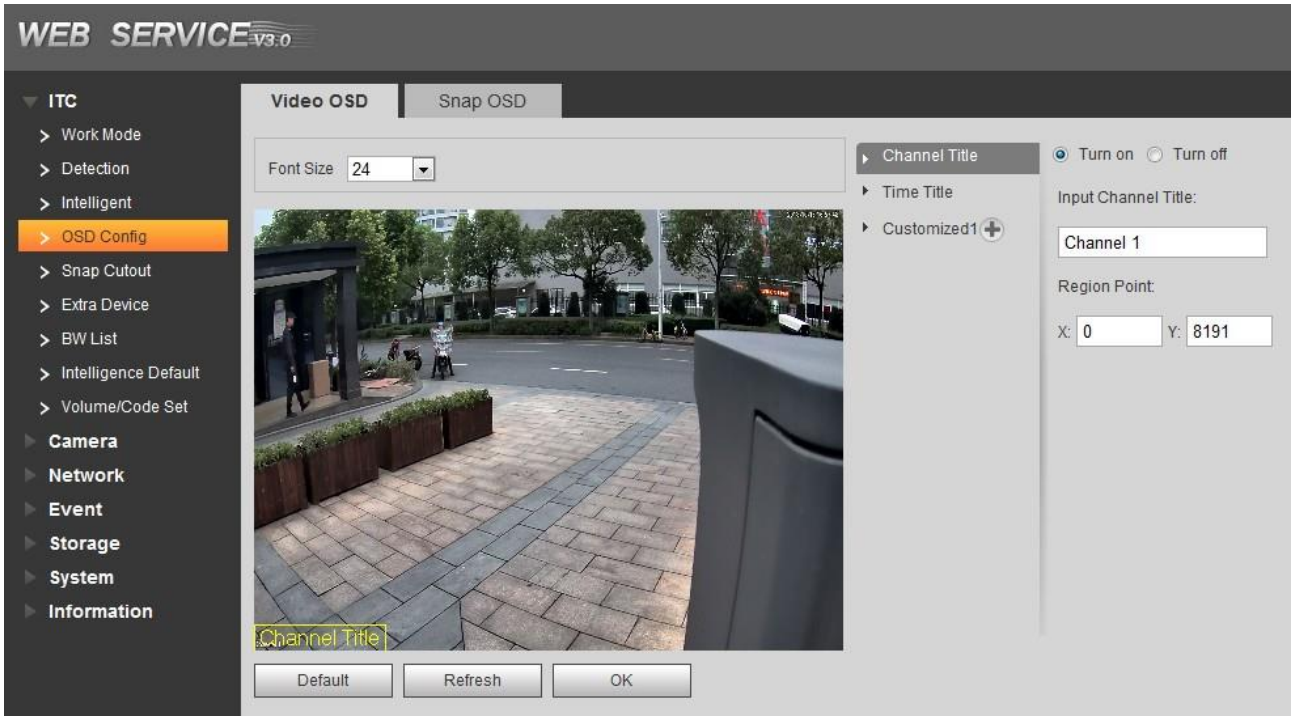
5.4.1.4.1 Video OSD

In this section, you can set OSD info of video channel.

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

The **Video OSD** interface is displayed, see Figure 5-29.

Figure 5-29 Video OSD



Step 2 Select Font Size scheme.

Step 3 Set channel title and location.

1. Click **Channel Title**.
2. Select **Enable**.
3. Input channel name into the **Input Channel Title**.
4. Use left mouse button to drag yellow box or input coordinate directly and then set the location of channel title.

Step 4 Set time title and location.

1. Click **Time Title**.
2. Select **Enable**.
3. Select **Display Week**.
4. Use left mouse button to drag yellow box or input coordinate directly and then set the location of time title.

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

The system supports max 3 customized regions.

Step 6 Click **OK** to finish configuration.

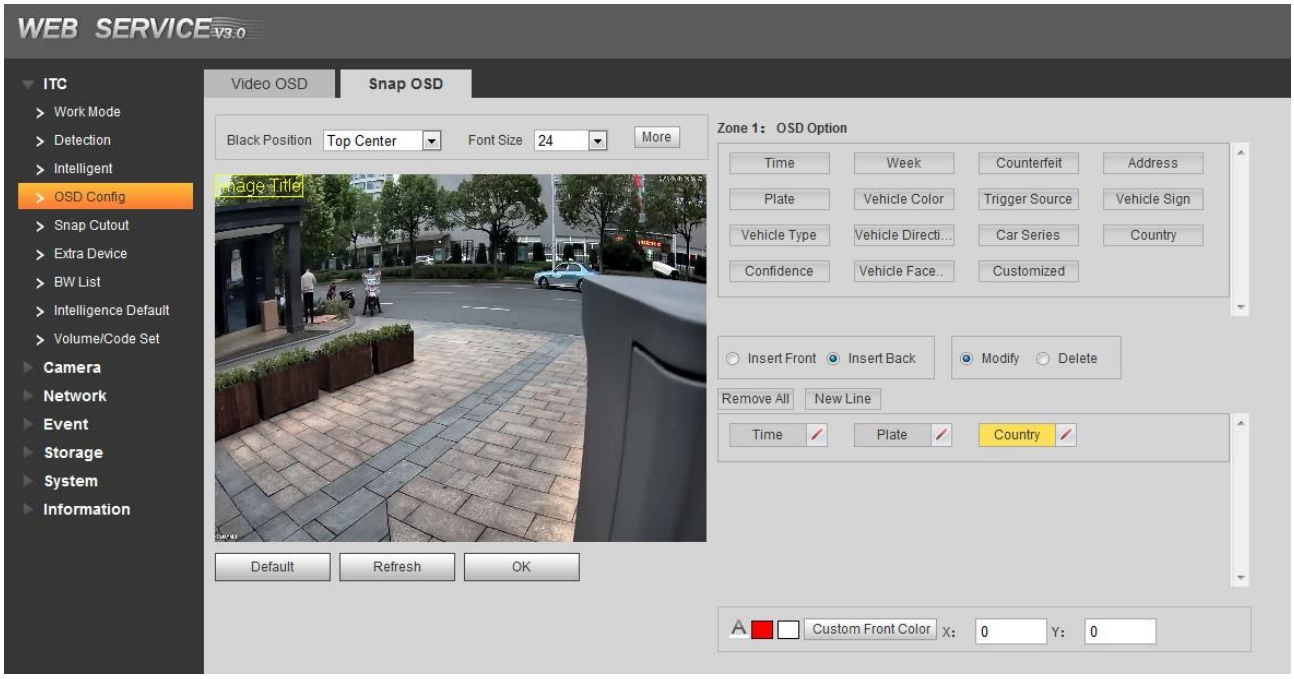
5.4.1.4.2 Picture OSD

In this section, you can set OSD info of Picture.

Step 1 Select Setting > ITC > OSD Config > Picture OSD.

The **Picture OSD** interface is displayed, see Figure 5-30.

Figure 5-30 Picture OSD



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

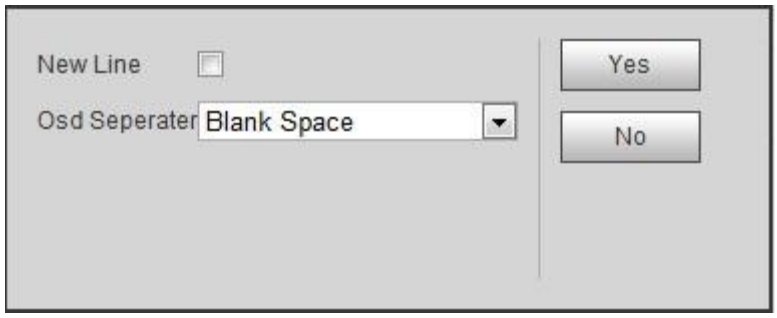
Step 3 Select **Black Position**, which includes top, bottom or none.

Step 4 Set font size and scheme of OSD info. You can set font color of picture OSD info in the lower right corner of the interface.

Step 5 Click **More**.

Line feed and separator are displayed. See Figure 5-31.

Figure 5-31 Line and separator



Step 6 Select New Line according to actual requirement and set separator types of OSD info. You can manually input other separators when selecting **Customize** from **OSD Separator**.

Step 7 Set OSD option.

Click **Recommended Overlay** and quickly set general overlay formats.

Table 5-17 Picture OSD parameters description

Parameter	Note
Insert Front:	Select one OSD option, click **Insert Front** and select other OSD options. The new OSD options will be displayed in front of original OSD option.
Insert Back	Select one OSD option, click **Insert Back** and select other OSD options. The new OSD option will be displayed behind the original OSD option.

Parameter	Note
Modify	Click it and all the OSD info 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 info status is displayed as  , click  to delete corresponding OSD option.
Clear	Delete all the OSD info.
Line Feed	After selecting some OSD info, click **New Line** and next OSD info will be displayed on the picture.

Step 8 Click **OK** to finish configuration.

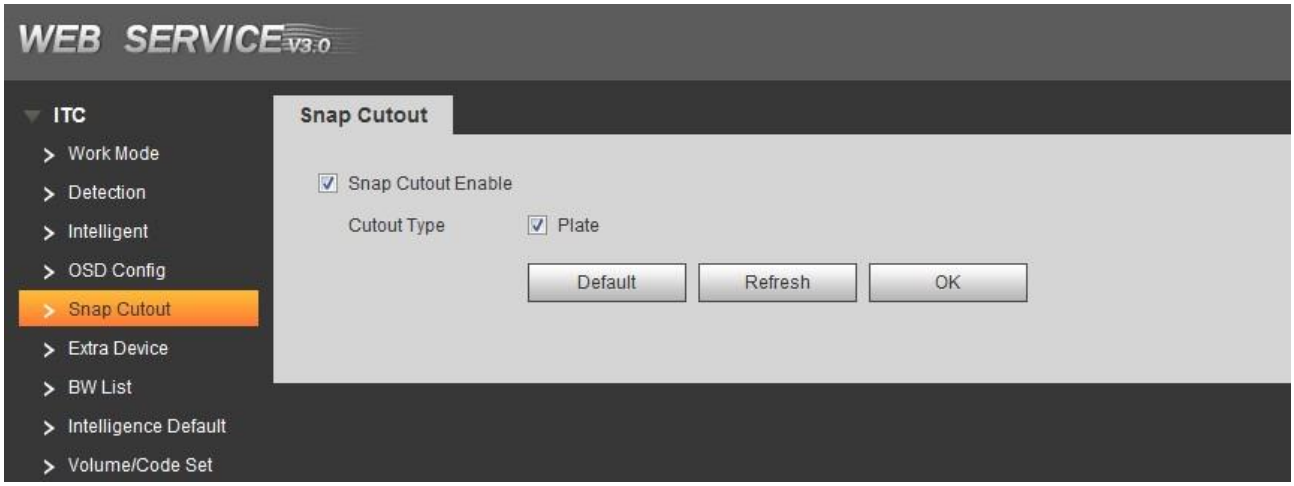
5.4.1.5 Snap Cutout

In this section, plate cutout function will be enabled. The system will cut out the recognized plate picture and save it under the storage path.

Step 1 Select Setting > ITC > Snap Cutout.

The **Snap Cutout** interface is displayed. See Figure 5-32.

Figure 5-32 Snap Cutout



Step 2 Select **Snap Cutout** and **Plate**, and then plate cutout function is enabled.

Step 3 Click **OK** to finish configuration.

5.4.1.6 Extra Device

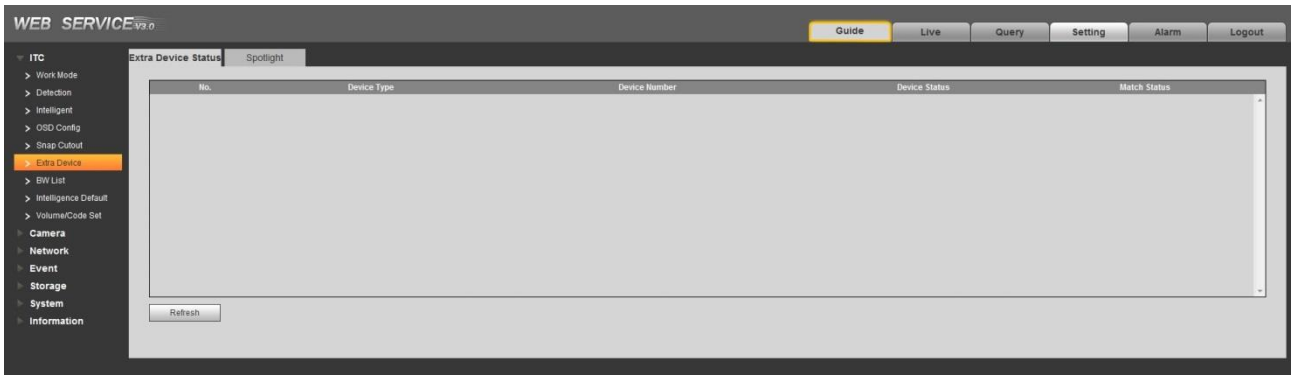
5.4.1.6.1 Extra Device Status

In this interface, it can view the type, number, status and match status of extra device.

If it is connected to vehicle detector of our company and the com protocol selects vehicle detector, then it can detect if the associated info and status of vehicle detector is normal.

Select **Setting** > **ITC** > **Extra Device** > **Extra Device Status** and the interface of **Extra Device Status** is displayed. See Figure 5-33.

Figure 5-33 Extra Device Status



5.4.1.6.2 Spotlight

In this section, you can configure light array and output mode of spotlight.

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

The **Spotlight** interface is displayed, see Figure 5-34.

Figure 5-34 Spotlight

Step 2 Select Configure parameters according to actual requirement. Please refer to Table 5-18 for more details.

Table 5-18 Spotlight parameters description

Parameter	Note
Light Array	There are totally 3 groups optional.
Output Mode	Select the output mode of spotlight. ● Off: Spotlight is always off. ● Always: Spotlight is always on. ● Auto: Automatically enable spotlight according to time or brightness.
Brightness	Set the brightness value of spotlight. It is 40 by default.

Parameter	Note
Auto Mode	When **Work Mode** is **Auto**, then you can automatically turn on or turn off spotlight according to time or brightness. ● Time: Set the period during which the spotlight is enabled. Independent config 7 days a week, each day supports 6 periods. ● Brightness: 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.

Step 3 Click **OK** to finish configuration.

5.4.1.7 BW List

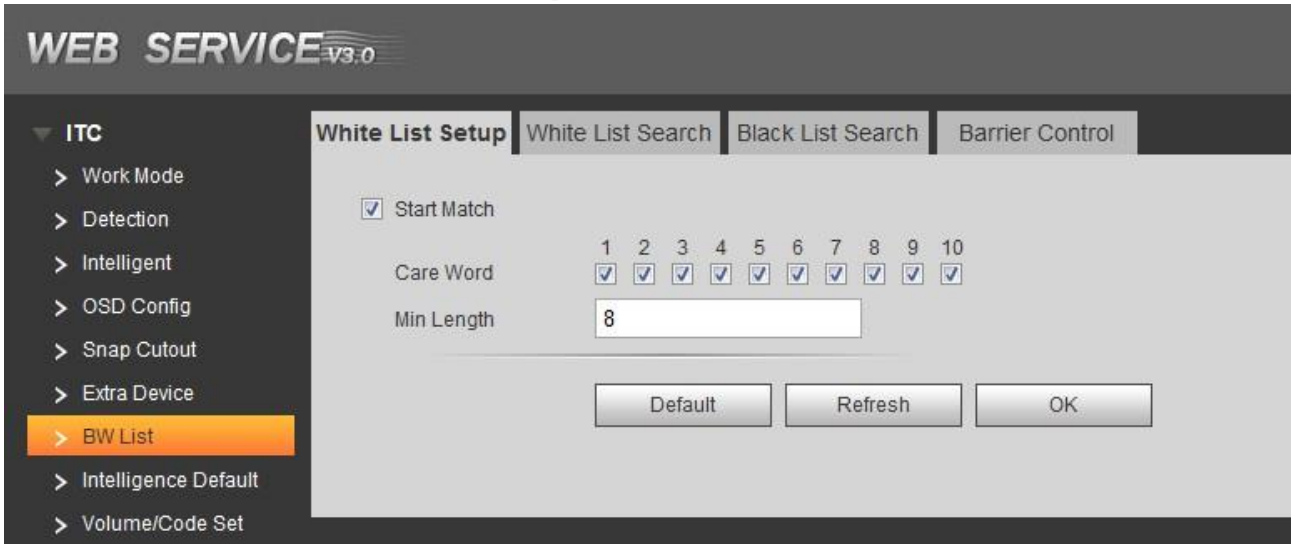
5.4.1.7.1 White List Setup

Enable white list. When the system detects the vehicles in the white list, then it will enable open-barrier mode and set white list matching function.

Step 1 Select Setting > ITC > BW List > White List Setup.

The **White List Setup** interface is displayed. See Figure 5-35.

Figure 5-35 White List Setup



Step 2 Configure parameters according to actual requirement. Please refer to 0 for more details.

White list setup parameters description

Parameter	Note
Start Match	After it is selected, you can set matching character and min length. The plates which meet the matching condition will be considered as white list vehicle. It is unnecessary for each character to totally match the plate number which exists in white list data.
Card Word	Match the selected character bit and the unselected characters will not be analyzed.
Min Length	When the number of matched characters meets the value, then it will be considered as white list vehicle regardless of whether other characters match.

Step 3 Click **OK** to finish configuration.

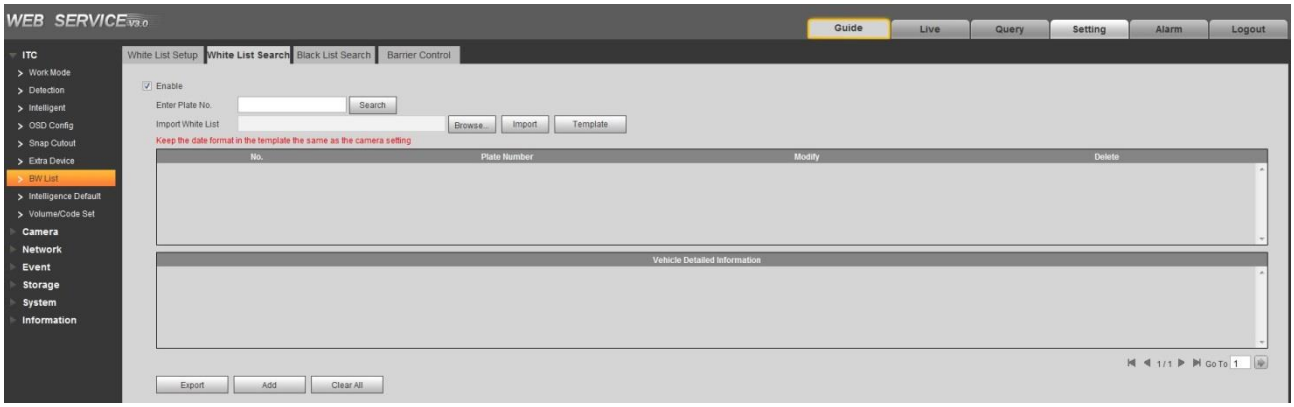
5.4.1.7.2 White List Search

In this section, you can inquire if some plate exists in the white list, import and export white list vehicle info.

Step 1 Select Setting > ITC > BW List >White List Setup.

The **White List Search** interface is displayed. See Figure 5-36.

Figure 5-36 White List Search



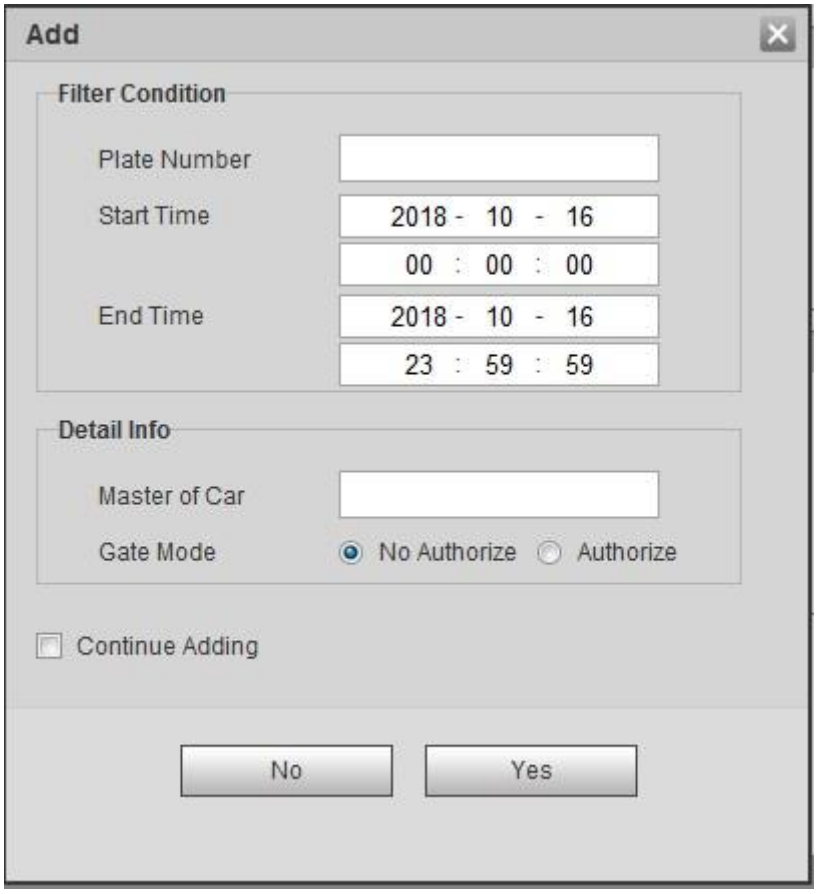
Step 2 Configure parameters according to actual requirement.

- Search plate No.: Input the plate No. (Input some characters). Click Search and inquire if the plate No. exists in the white list.
- Modify plate info: Click Modify of the plate No. line and modify and detail of the plate number. Click **OK** to complete modification after modification is finished.
- Delete single plate No.: Click **Delete** of the plate No. line and delete it from the white list.
- Delete plate No. in batch: click **Delete** All and click **OK** in the dialog box to delete all the white list info.
- The steps of importing into white list one by one are shown as follows.

3) Click **Add**.

The **Add** interface is displayed. See Figure 5-37

Figure 5-37 Add



4) Input complete plate No.
5) Set the start time and end time of the plate number which exists in white list.
   The vehicle will be no longer considered as white list vehicle after it exceeds the time range.
6) Input name of vehicle owner and select if barrier authority is given.
7) Select Continue Adding, click OK and the system will save white list plate number info and directly enter the adding interface of next white list plate.
   Not select **Continue Adding**. Click **OK** and complete adding.

- The steps of importing white list in batch are shown as follows.

1) Click **Template** and download the template to local PC.
2) Open the template and fill in the white list data which needs to be imported according to template format and save file.
3) Click **Browse** and select the path where template file exists. Click **Import** and you can import the white list data of template file into the system in batch.

- Export white list in batch. Click Export and it will pop up the dialog box of file download. Click Save and select the path of storing files. Click Save and export white list to local in form of table.

Please make sure the time format in list is in accordance with that of the camera when importing white list.

Step 3 Click **OK** to finish configuration.

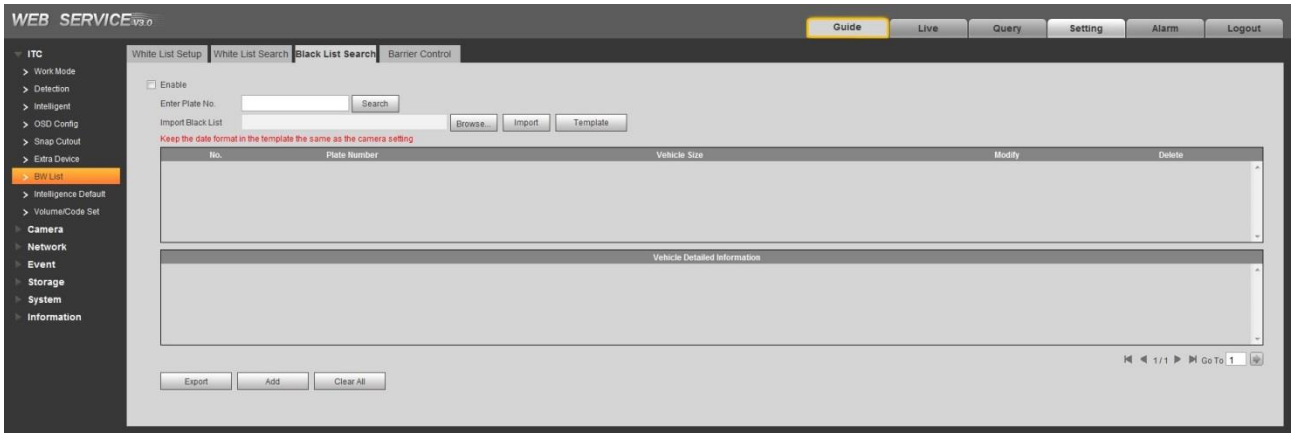
5.4.1.7.3 Black List Search

In this section, you can inquire if some plate exists in black list, import and export black list plate number and vehicle info.

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

The **Black List Search** interface is displayed. See Figure 5-38.

Figure 5-38 Black List Search



Step 2 The query, import and export function of black list is similar to those of white list. Please refer to 5.4.1.7.2White List Search for more details.

Step 3 Click **OK** to finish configuration.

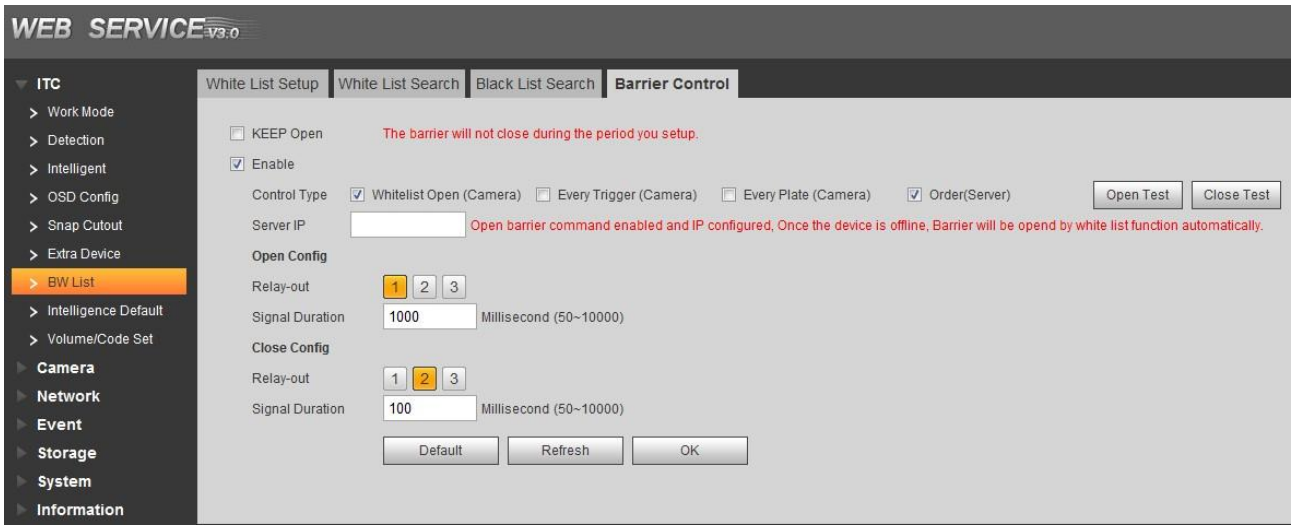
5.4.1.7.4 Barrier Control

In this section, you can set the barrier control mode; configure info of opening barrier and closing barrier.

Step 1 Select Setting > ITC > BW List >Barrier Control.

The Barrier Control interface is displayed, see Figure 5-39.

Figure 5-39 Barrier control ,



Step 2 Configure the parameters. Please refer to Table 5-19 for more details.

Table 5-19 Barrier control parameter description

Parameter	Note
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 period you set.
Enable	Select it to enable barrier control and config.

Parameter	Note
Barrier Control Type	It can trigger alarm via different barrier mode. ● White List Open: Capture the vehicle which conforms to white list or fuzzy matching and then output open barrier signal. ● Every Trigger (Camera): Capture any vehicle and output open barrier signal. ● Every Plate (Camera): Capture any plated vehicle and output open barrier signal. ● Order (Server): Platform issues command and output open barrier signal.
Manual Open	Click the button and manually trigger outputting signal of opening barrier.
Manual Close	Click the button and manually trigger outputting signal of closing barrier.
Open Config Close Config	● Relay-out: Activate alarm linkage output port. You can select anyone out of 3 ports. ● Signal Duration: It is the time for which the open barrier or close barrier signal is going to last.

Step 3 Click **OK** to finish configuration.

5.4.1.8 Intelligence Default

In this section, you can restore capture setting and intelligent parameter to default setting.

Step 1 Select Setting > ITC > Intelligent Default.

The **Intelligence Default** interface is displayed. See Figure 5-40.

Figure 5-40 Intelligence Default

Step 2 Click **Default**.

The **DEFAULT** interface is displayed. See Figure 5-41.

Figure 5-41 Default

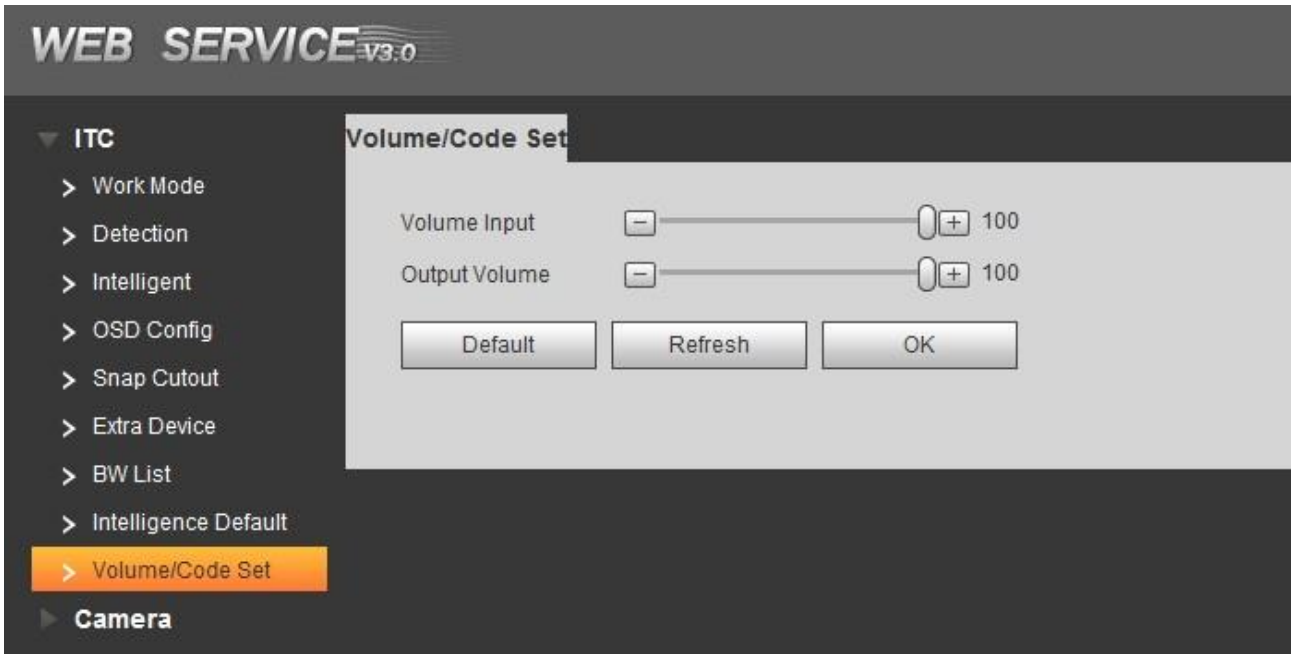
Step 3 Click **OK** to finish configuration.

5.4.1.9 Volume/Code Set

In this section, you can adjust the input, output volume and speed of external voice device.

Select **Setting** > **ITC** > **Volume/Code Set** and the interface of **Volume/Code Set** is displayed. See Figure 5-42.

Figure 5-42 Volume/Code Set



5.4.2 Camera

In this section, you can set image parameter, video and stream parameters.

5.4.2.1 Attributes

5.4.2.1.1 General

In this section, you can set parameters such as image brightness, contrast, hue, saturation and ICR switch etc.

Step 1 Select Setting > Camera > Attributes > General.

The **GENERAL** interface is displayed. See Figure 5-43.

Figure 5-43 General system settings

Step 2 Configure parameters according to actual requirement. Please refer to Table 5-20 for more details.

Table 5-20 General parameters description

Parameter	Note
Brightness	It is used to adjust the overall image brightness, change the value when the image is too bright or too dark. 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. The default value is 50. The bigger the value is, the brighter the image becomes.
Contrast	Change the value when the image brightness is proper but contrast is not enough. ● If the value is too big, the dark area is likely to become darker and the bright area is likely to be overexposed. ● The picture might be blurry if the value is set too small. The recommended value is from 40 to 60 and the range is from 0 to 100. The default value is 50. The bigger the value is, the more obvious the contrast between the bright area and dark area will become.
Hue	It is used to 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. The default value is 50. The threshold is used to adjust image hue and ot will not influence image overall brightness.

Parameter	Note
Saturation	It is used to adjust the color vividness and will not influence the image overall brightness. ● The image becomes too flamboyant if the value is too big. ● 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. The default value is 50. The bigger the value is, the more flamboyant the image becomes.
ICR Switch	● Auto: Set brightness default value, it will realize auto switch when it exceeds the default value. ● IR: The filter is switched to IR mode when the image is black and white. ● General: The filter is switched to general mode when the image is color.

Step 3 Click **OK** to finish configuration.

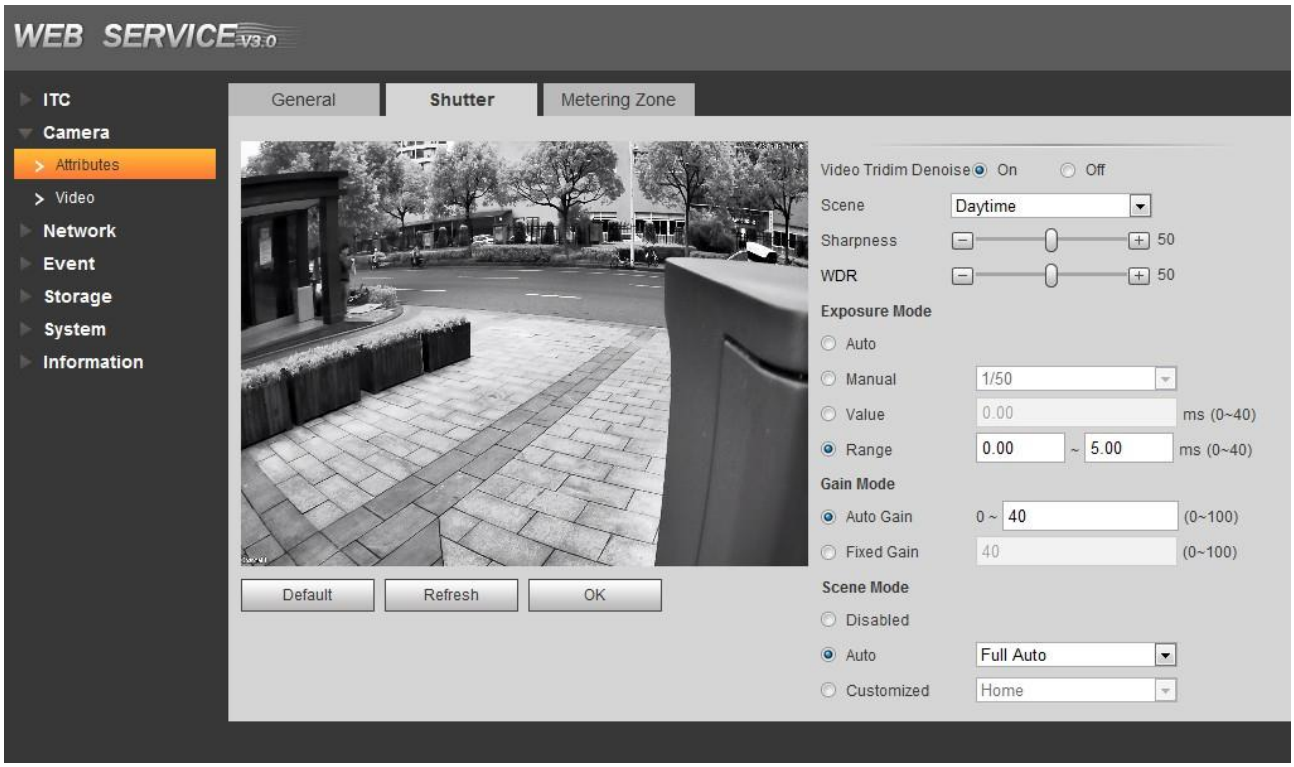
5.4.2.1.2 Shutter

In this section, you can set camera shutter config, including shutter mode, exposure mode, gain mode and scene mode etc.

Step 1 Select Setting > Camera > Attributes > Shutter.

The **Shutter** interface is displayed. See Figure 5-44.

Figure 5-44 Shutter



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-21 for more details.

Table 5-21 Shutter parameters description

Parameter	Note
Shutter Mode	Both video recording and image capture adopt the same exposure mode.
Video 3D NR	Select **On** to enable 3D NR function and lower video noise.
Scene	Switch to different scene for config.

Parameter	Note
Sharpness	Set the image sharpness under the scene. The bigger the value is, the higher the detail contrast becomes, the clearer the image becomes. The image tends to generate noise when the value is set too big.
WDR	The system dims bright areas and compensates dark areas to ensure the clarity of both areas. The bigger the value is, the higher the WDR level becomes.
Exposure Mode	Select lens exposure mode, which includes auto and manual. ● Auto: Auto exposure. ● Manual: Fixed exposure value. It needs to set the time of manual exposure, including 8 options between 1/50 and 1/10000. ● Users can customize value and range.
Gain Mode	● Auto Gain: Set the range of auto gain. ● Fixed Gain: Set the fixed gain value.
Scene Mode	Select the device environment and set scene mode. Adjust the device monitoring image to its best status.

Step 3 Click **OK** to finish configuration.

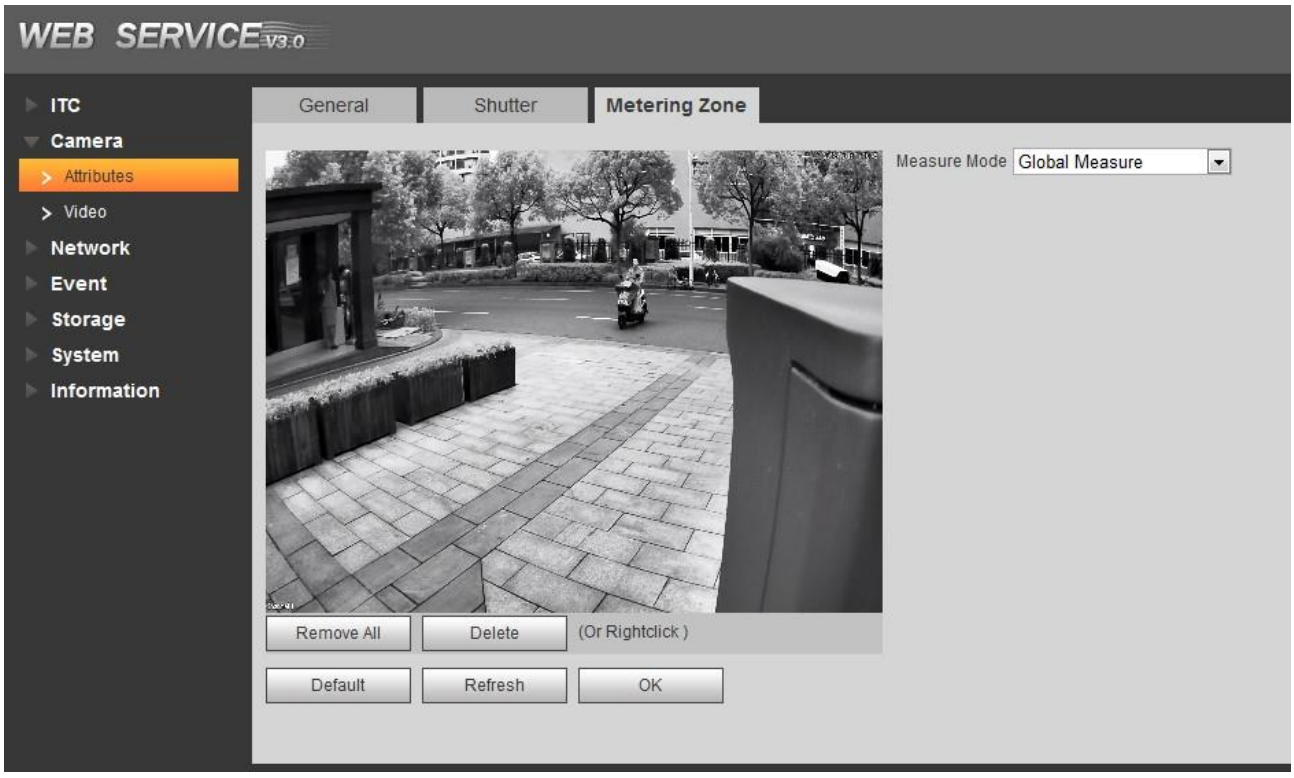
5.4.2.1.3 Metering Zone

In this section, you can set the measure mode of metering zone.

Step 1 Select Setting > Camera > Attributes > Metering Zone.

The Metering Zone interface is displayed, see Figure 5-45.

Figure 5-45 Metering Zone



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-22 for more details.

Table 5-22 Metering zone parameter description

Parameter	Note
Measure Mode	Select measure mode: It includes spot measure, global measure ans partial measure. ● Spot measure: Measure the brightness of moving vehicle and intelligently adjust the overall image brightness. ● Global measure: Measure the brightness of the whole image area and intelligently adjust the overall image brightness. ● 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. Drag the mouse to select the measured area and the system displays yellow box; Drag the box to proper location, click **OK** and complete config.
Backlight	When selecting Spot Measure, you can select backlight and frontlight according to scene requirement, and then improve the backlight image brightness.
Frontlight	
Plate Meter Enable	When selecting Partial Measure, you can select if it is to enable plate exposure mode according to actual requirement. If there is vehicle plate in the selected partial area, it will adjust the image according to plate info and display plate info more clearly.

Step 3 Click **OK** to finish configuration.

5.4.2.2 Video

5.4.2.2.1 Video

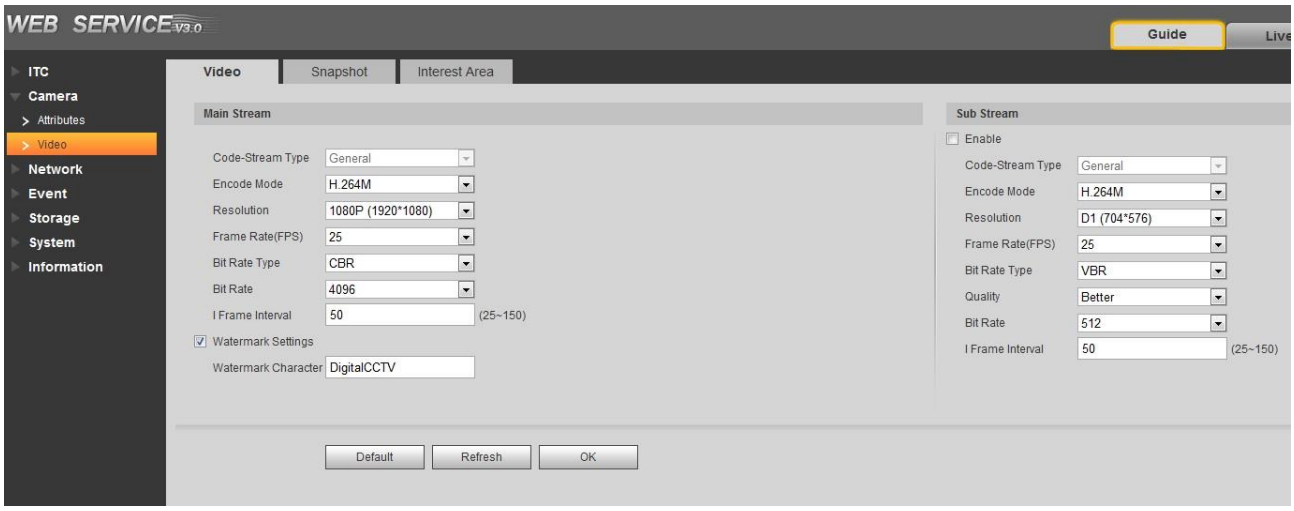
- When selecting the work mode of two cameras from **Setting** > **ITC** > **Work Mode**, the main camera needs to configure main stream and sub stream, besides, the panoramic camera needs to configure main stream as well.
- In this chapter, it is to select the work mode as **Main Camera** + **Panoramic Camera** and introduce the stream config.

In this section, you can set the camera stream information.

Step 1 Select Setting > Camera > Video > Video.

The Video interface is displayed, see Figure 5-46.

Figure 5-46 Video



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-23 for more details.

Table 5-23 Video parameters description

Parameter		Note
Main Stream	Stream Type	Currently it supports general 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.
	Image Quality	Image quality can be set in VBR mode. There are 6 levels optional.
	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 via verifying watermark character. ● Select **Watermark Settings** and enable the function. ● Default Watermark character is: DigitalCCTV. ● 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.
	Encode Mode	Currently it only supports H.264B, H.264M, H.264H, H.265 and MJPEG.

Parameter		Note
	Resolution	Currently it only supports 720P and D1. 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.
	Image Quality	Image quality can be set in VBR mode. There are 6 levels optional.
	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 **OK** to finish configuration.

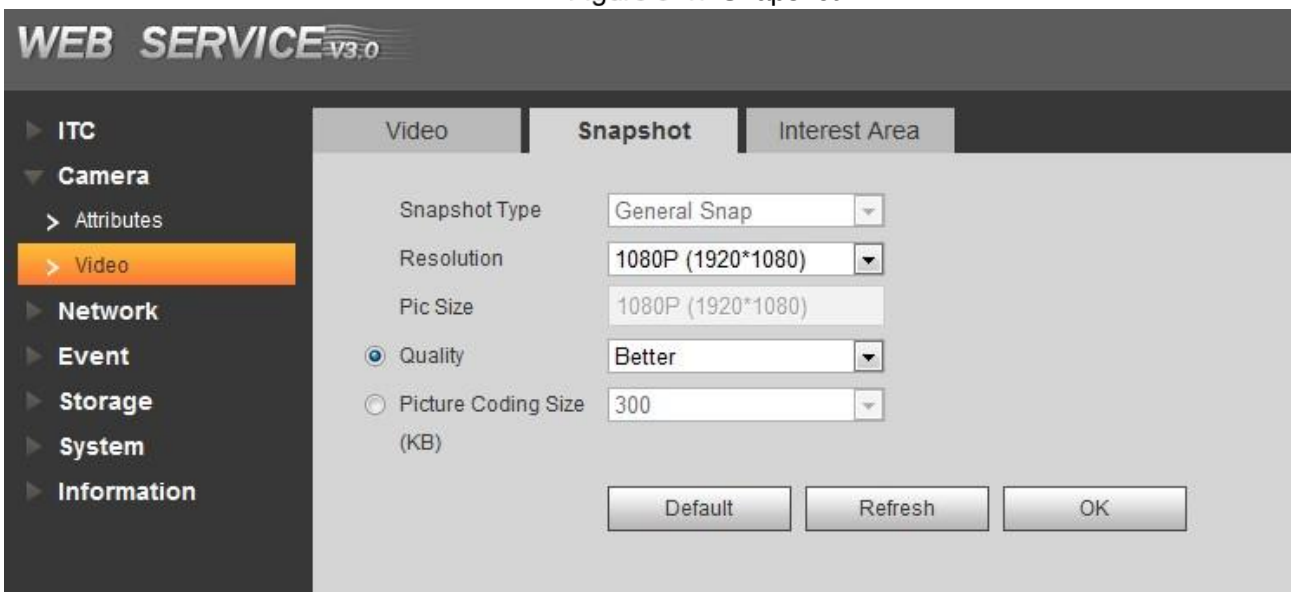
5.4.2.2.2 Snapshot

In this section, you can set the picture stream, including resolution, quality or picture size.

Step 1 Select Setting > Camera > Video > Snapshot.

The **Snapshot** interface is displayed, see Figure 5-47.

Figure 5-47 Snapshot



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-24 for more details.

Table 5-24 Snapshot parameters description

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

Parameter	Note
Picture Coding Size	Set picture coding size, there are 8 levels optional; Or select **Customized**, the range is from 50 to 1024. You can select either picture quality or picture coding size to make setting.

Step 3 Click **OK** to finish configuration.

5.4.2.2.3 ROI

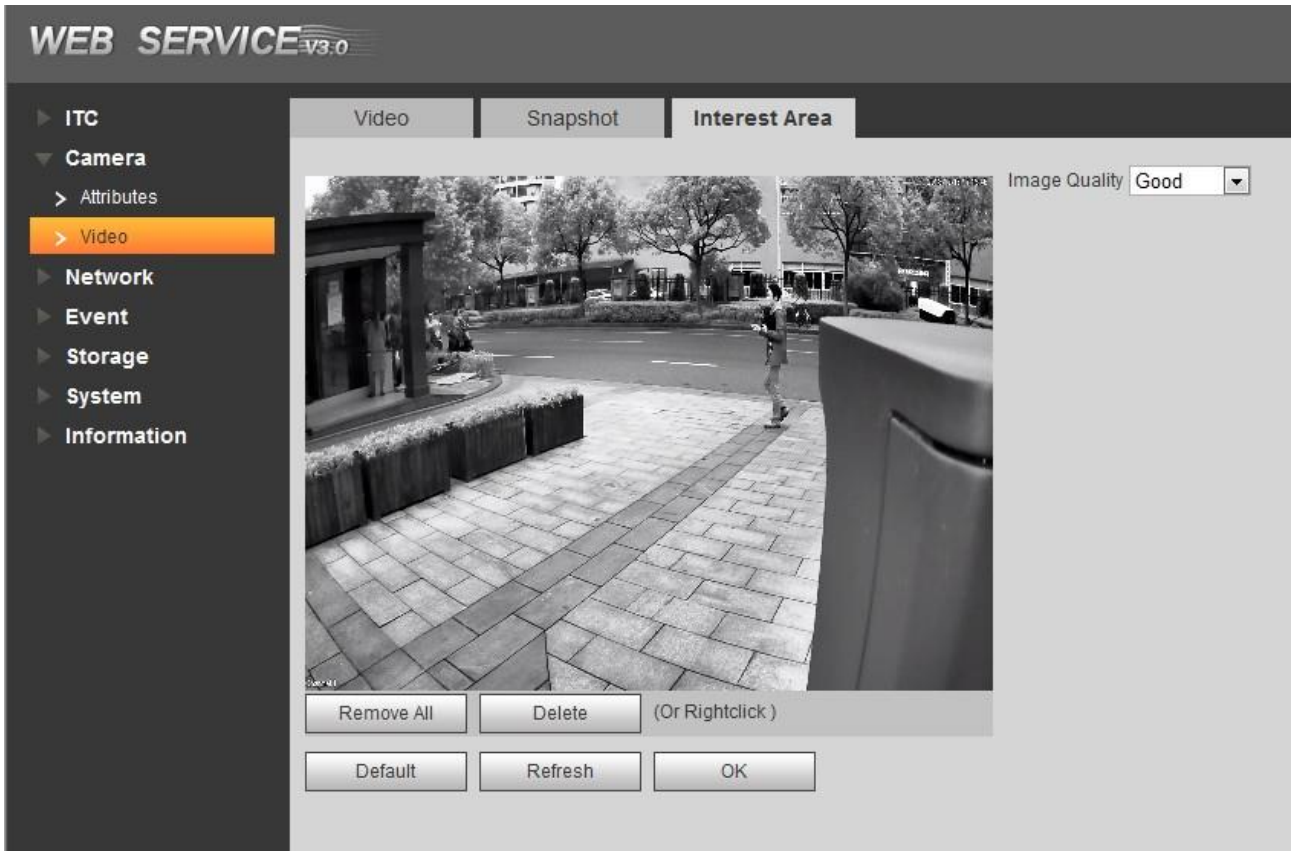
- It supports max 3 regions at the same time.
- The bigger the image quality value is, the better the quality will be.
- Click **Remove All**, and delete all the area boxes; Select one box, and then click delete or right click to delete it.

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

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

The ROI interface is displayed, see Figure 5-48.

Figure 5-48 ROI



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-25 for more details.

Table 5-25 ROI parameter description

Parameter	Note
Image Quality	Set snapshot quality which includes 6 levels optional.
Remove All	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 **OK** to finish configuration.

5.4.3 Network

In this section, you can set IP address, port and other parameters.

5.4.3.1 TCP/IP

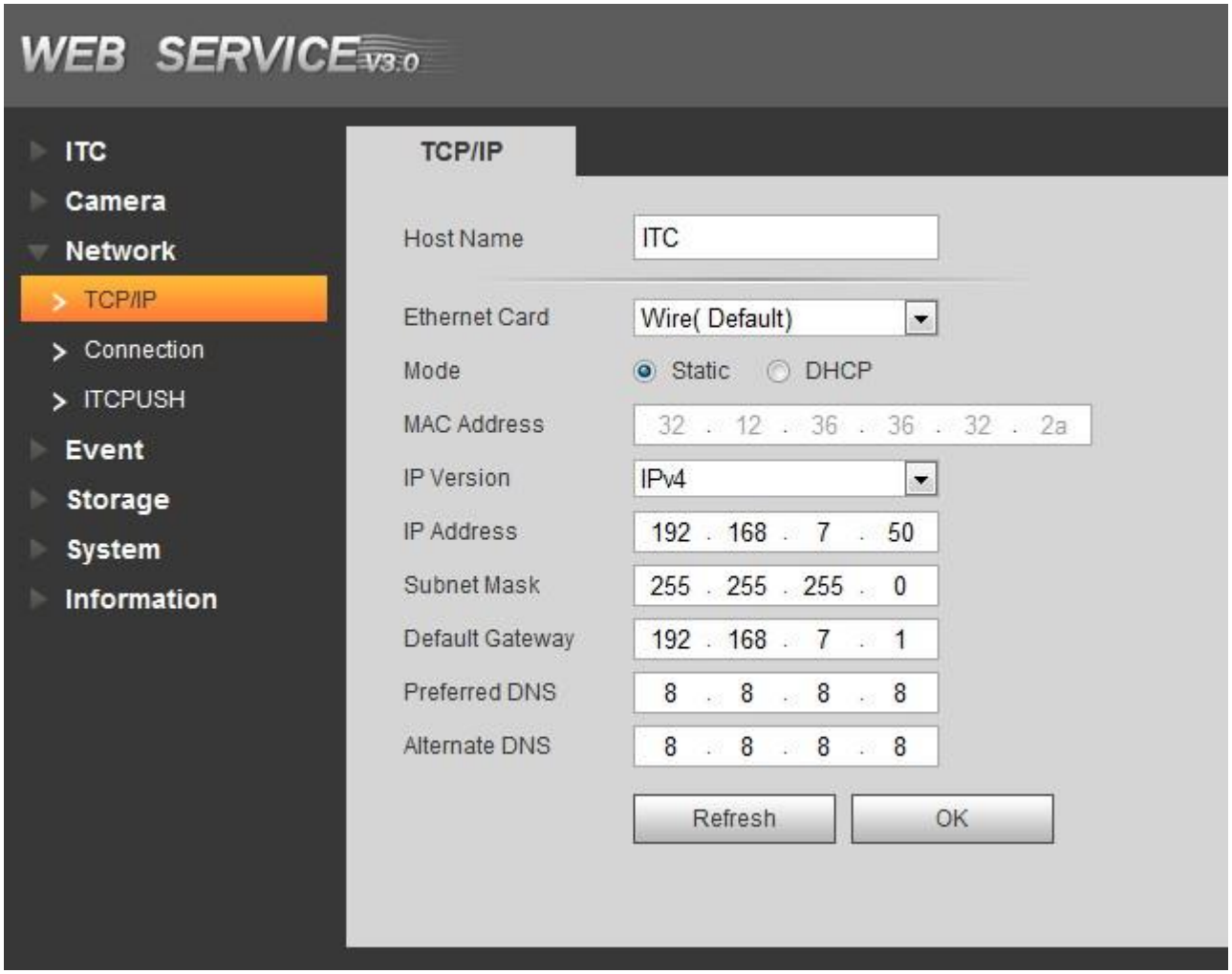
Some models support dual network port. Please do not set them in the same network segment; otherwise it may cause network error.

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

Step 1 Select Setting > Network > TCP/IP.

The **TCP/IP** interface is displayed. See Figure 5-49.

Figure 5-49 TCP/IP



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-26 for more details.

Table 5-26 TCP/IP parameter description

Parameter	Note
Host Name	The name of host device Supports max 15 characters.
Ethernet Card	Select the Ethernet Card you need to configure, the default one is Wire.
Mode	Network mode, including static and DHCP. ● DHCP Mode: Automatically acquire IP, at this moment IP, subnet mask and gateway cannot be set. ● Static Mode: It needs to manually set IP, subnet mask and gateway.
MAC Address	Host MAC Address
IP Version	IP version, including IPv4 and IPv6. The IP address of both versions can be accessed.
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 **OK** to finish configuration.

5.4.3.2 Connection

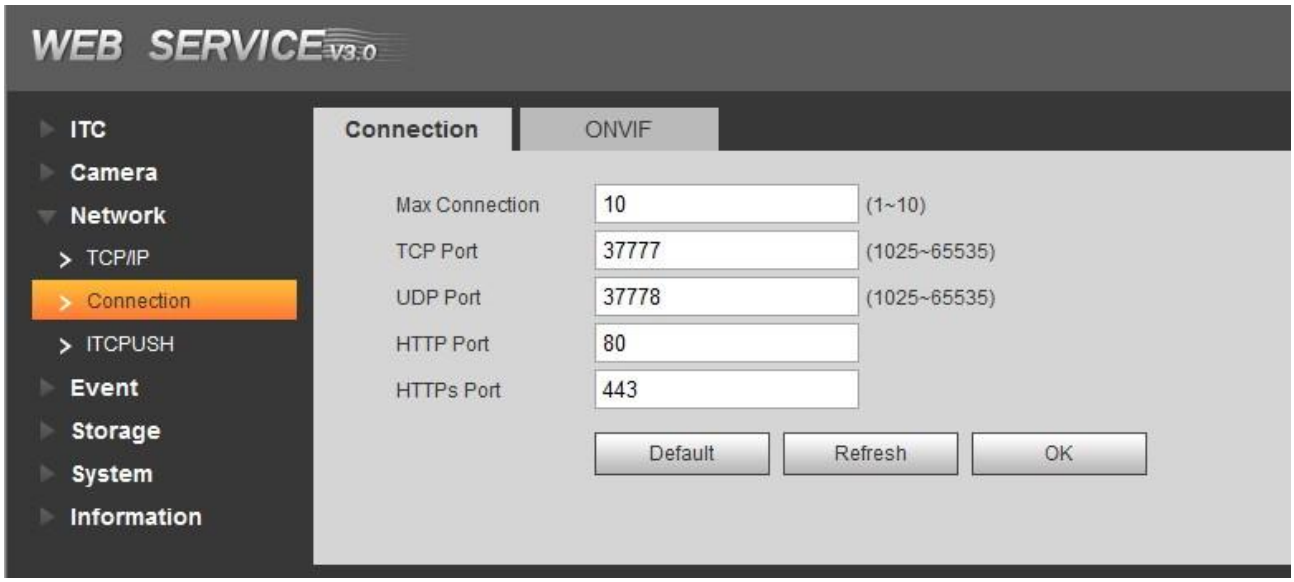
5.4.3.2.1 Connection

In this interface, it can set the connected port info, it can access device via different protocols or config tool.

Step 1 Select Setting > Network > Connection > Connection.

The **Connection** interface is displayed, see Figure 5-50.

Figure 5-50 Connection



Step 2 Configure each port value of the device. Please refer to Table 5-27 for more details.

Table 5-27 Connection parameters description

Parameter	Note

Parameter	Note
Max Connection	The max number of clients (web client, platform client and so on) that can connect to the device simultaneously; the value is 20 by default.
TCP Port	TCP protocol communication provides service. The default is 37777.
UDP Port	User data packet protocol port. The default is 37778.
HTTP Port	HTTP communication port, the value is 80 by default.
HTTPS Port	HTTPS communication port. The default is 443.

Step 3 Click **OK** to finish configuration.

5.4.3.2.2 ONVIF

ONVIF (Open Network Video Interface Forum) enables network video framework agreement. Enable ONVIF, and realize network video framework agreement to make different network video products interconnected.

ONVIF login authentication is enabled by default.

Step 1 Select Setting > Network > Connection > ONVIF.

The ONVIF interface is displayed, see Figure 5-51.

Figure 5-51 ONVIF

Step 2 Set Authentication as On.

Step 3 Click **OK** to finish configuration.

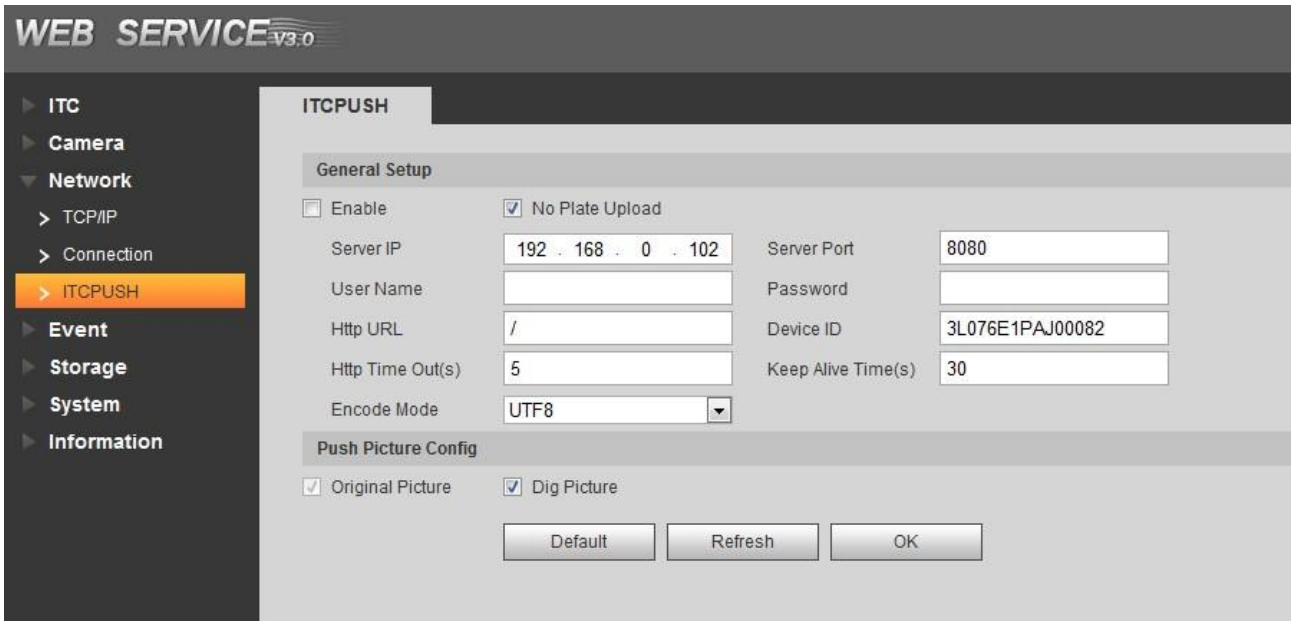
5.4.3.3 ITC Push

Push the captured vehicle violation info to server.

Step 1 Select Setting> Network > ITC Push.

The ITC Push interface is displayed. See Figure 5-52.

Figure 5-52 ITC push config



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-28 for more details.

Table 5-28 ITC Push

Parameter	Note
Enable	Select it and enable the push function of passing vehicle info.
No Plate Upload	Select it and enable the unlicensed push function.
Server IP	It is the IP of server which receives passing vehicle info.
Server Port	The port of server which receives passing vehicle info.
Username	Username and password used to log in server.
Password	
Http URL	Http URLprefix info of uploaded picture data.
Device ID	Device ID
Http Timeout	Timeout of Http push message.
Keep Alive Time	It can set keep alive time.
Encode Mode	Encode mode of push content, which includes UTF8 and GB2312.
Push Picture Config	Select the pushed picture type, which includes original picture and dig picture.

Step 3 Click **OK** to finish configuration.

5.4.4 Event

In this section, you can set alarm and abnormality.

5.4.4.1 Alarm

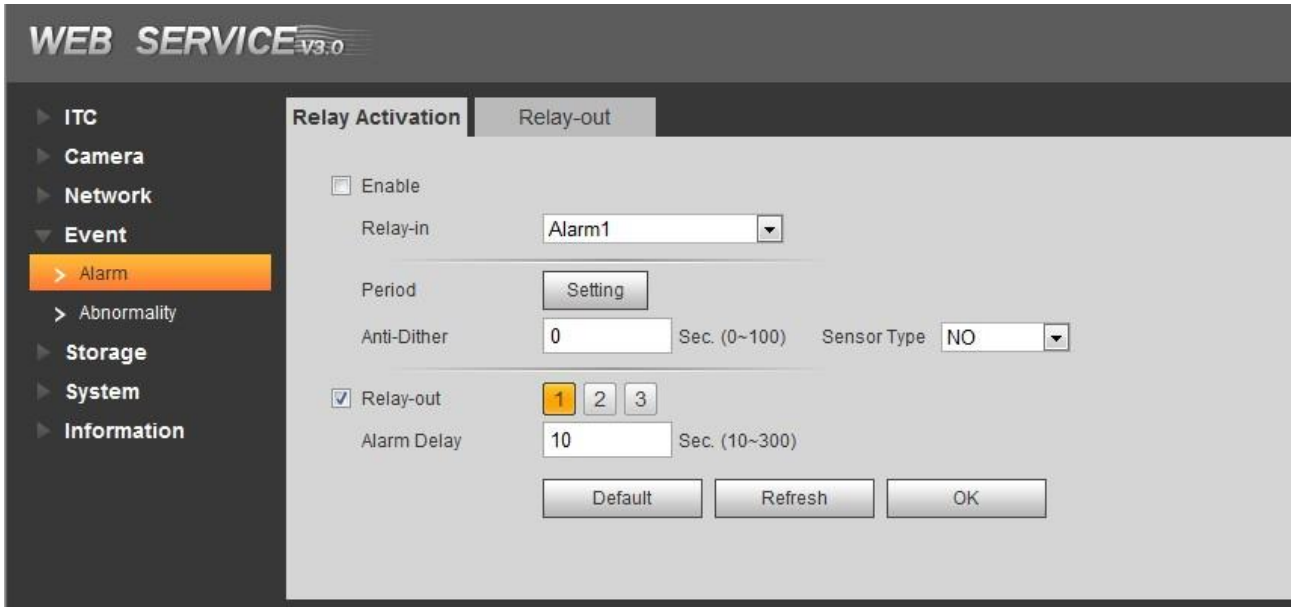
5.4.4.1.1 Relay Activation

In this interface, you can set several parameters of relay activation such as relay-in, period, anti-dither and sensor type etc.

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

The **Relay Activation** interface is displayed, see Figure 5-53.

Figure 5-53 Relay Activation



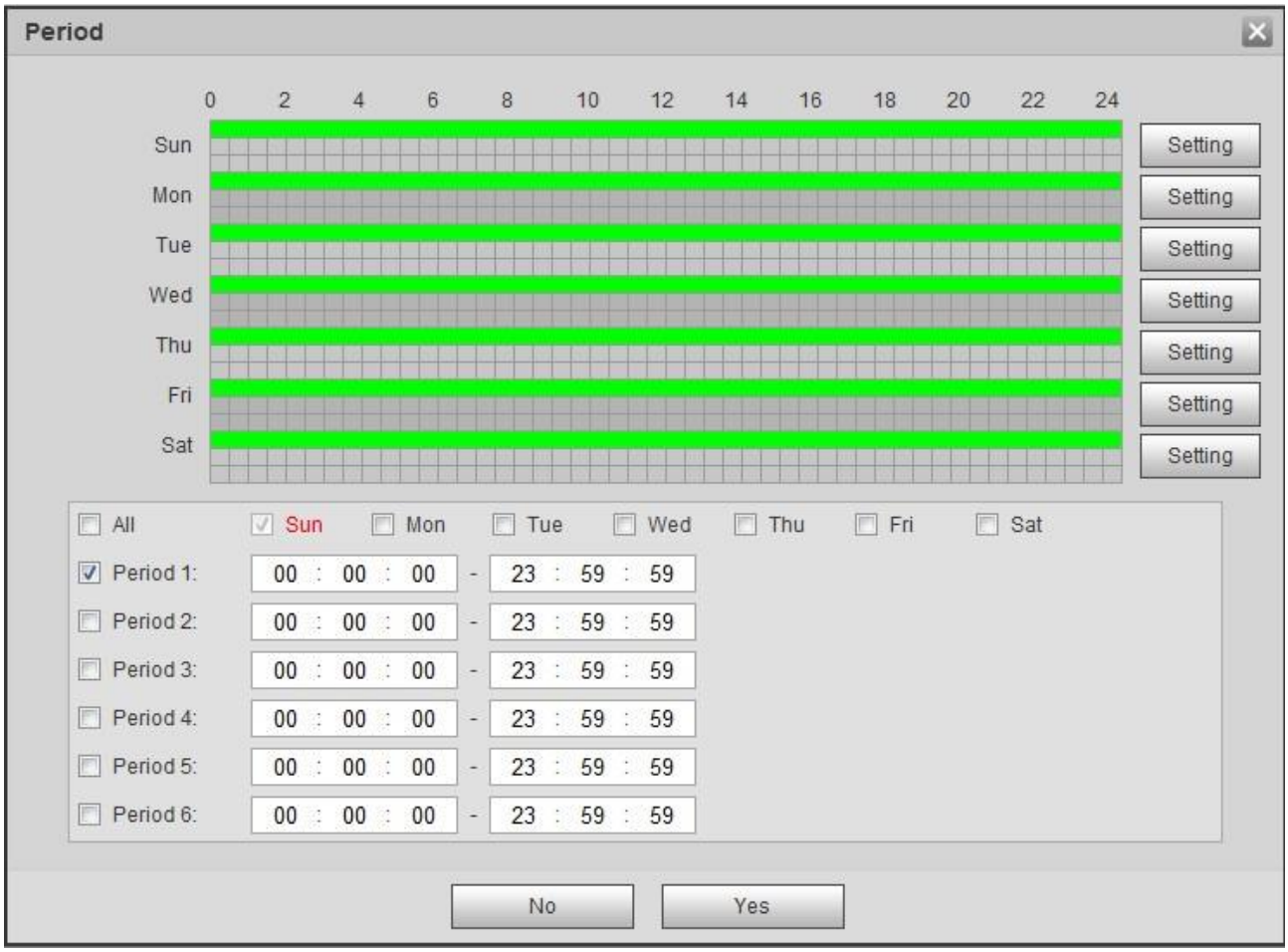
Step 2 Select **Enable** and current channel input is enabled.

Step 3 Set arm and unarm time of relay-in.

1) Click **Setup**.

The **Arm and Unarm Period** interface is displayed. See Figure 5-54.

Figure 5-54 Period



2) Click the **Setting** behind the day you need to configure time period.

3) Select the period you need to enable and input 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 **OK** and make the period of the day valid.
Repeat the steps above and make settings upon any other day.

Step 4 Make setting upon other parameters. Please refer to Table 5-29 for more details.

Table 5-29 Relay activation parameter description

Parameter	Note
Anti-dither	Input 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 check box and it will activate corresponding alarm output device when alarm occurs.
Alarm Delay	The time that delays alarm when alarm occurs.

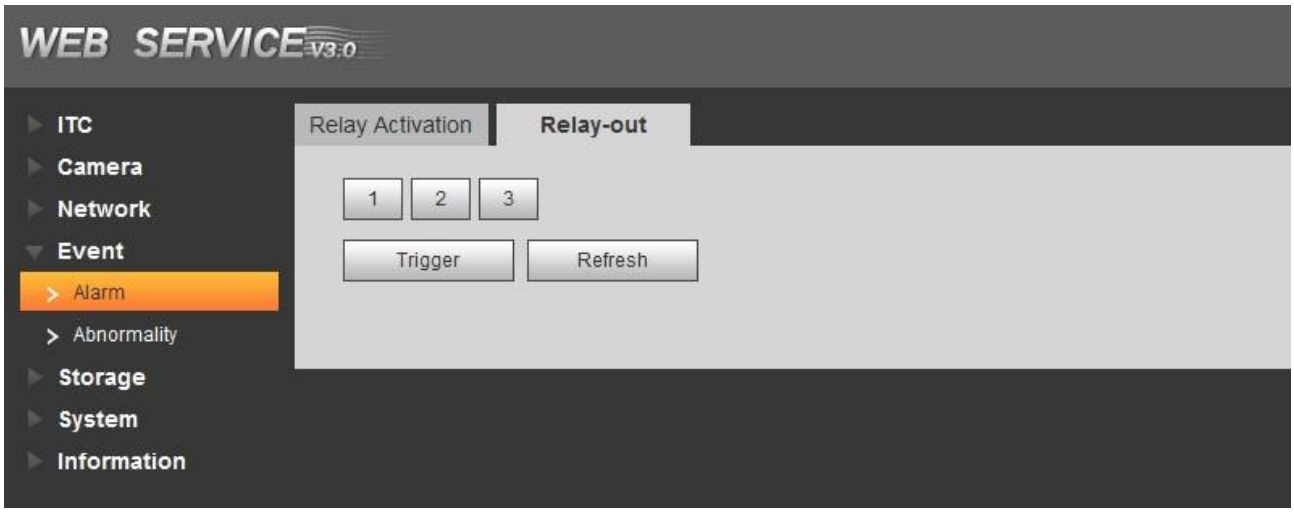
Step 5 Click **OK** to finish configuration. ，

5.4.4.1.2 Relay-out

In this section, it can analog trigger one alarm output signal.

Step 1 Select Setting > Event > Alarm> Relay-out.
The **Relay-out** interface is displayed. See Figure 5-55.

Figure 5-55 Relay-out



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

Step 3 Set alarm output

- Click Trigger and output relay-out signal
- Click **Refresh** and inquire relay-out status.

5.4.4.2 Abnormality

In this section, you can set relay-out mode of different events.

Step 1 Select Setting > Event > Abnormality.

The **Abnormality** interface is displayed. See Figure 5-56, Figure 5-57, Figure 5-58, Figure 5-59, Figure 5-60 and Figure 5-61.

Figure 5-56 No Storage Card

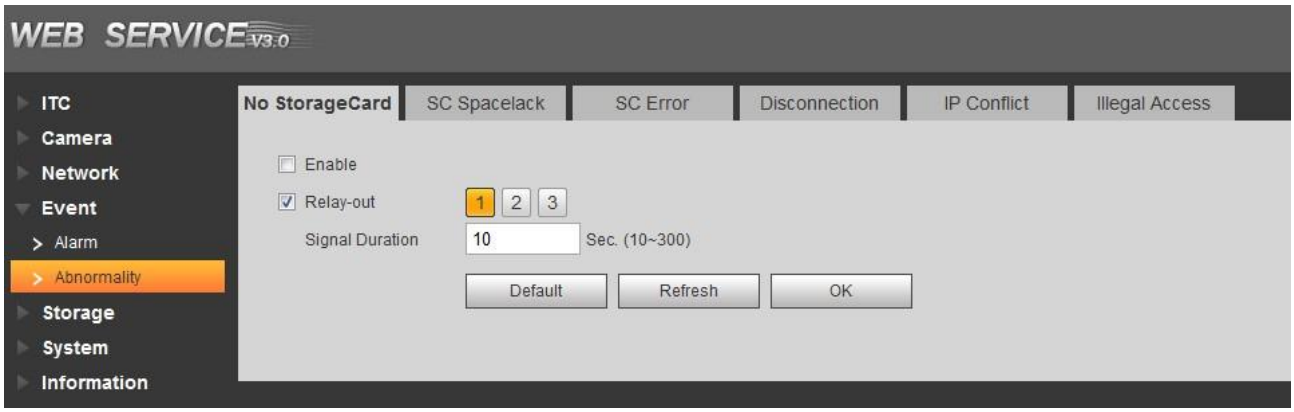


Figure 5-57 SC Space Lack

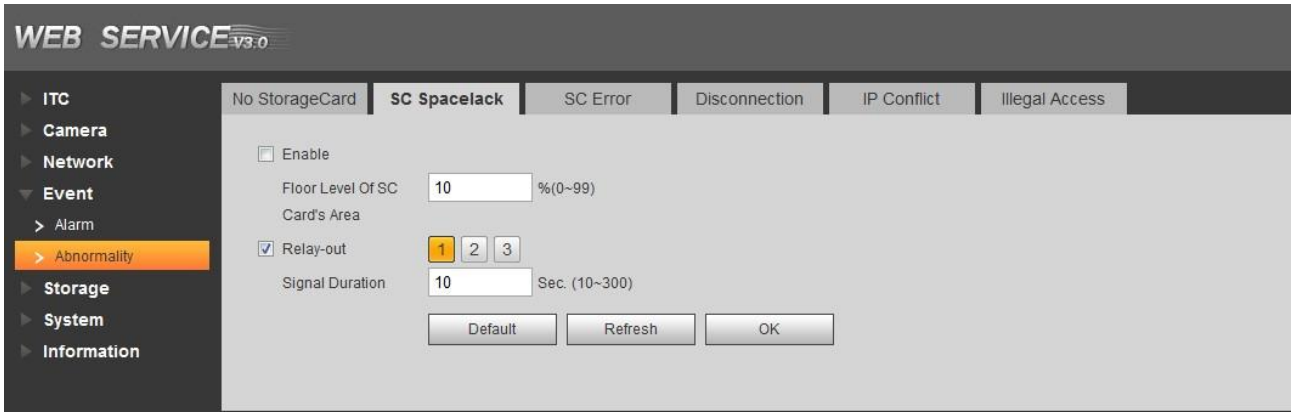


Figure 5-58 SC Error

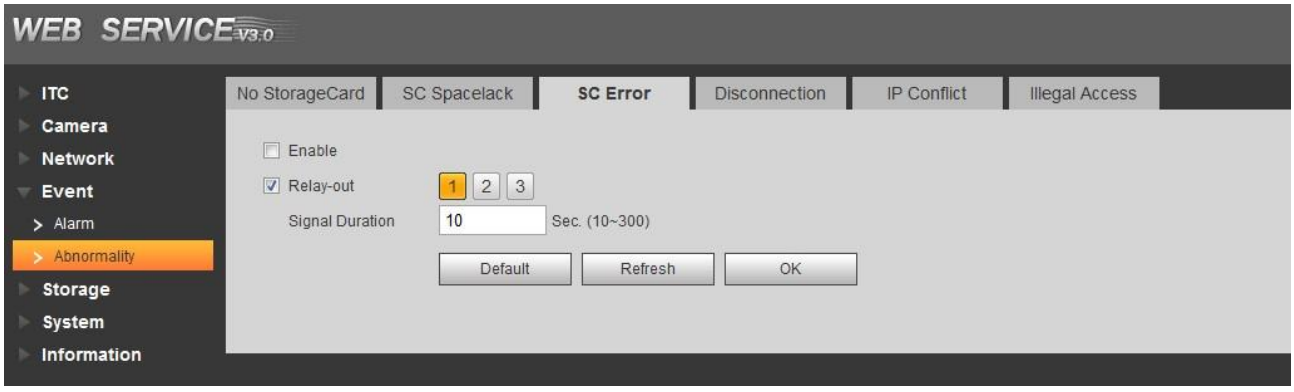


Figure 5-59 Disconnection

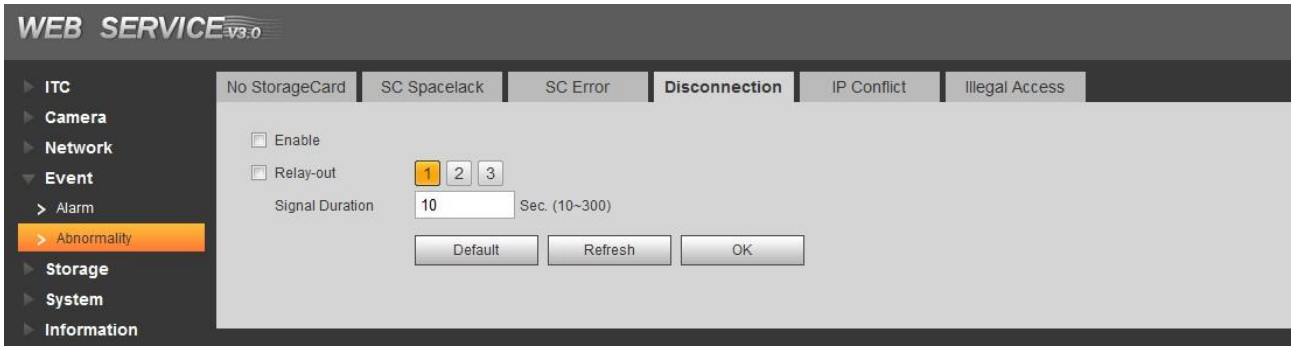


Figure 5-60 IP Conflict

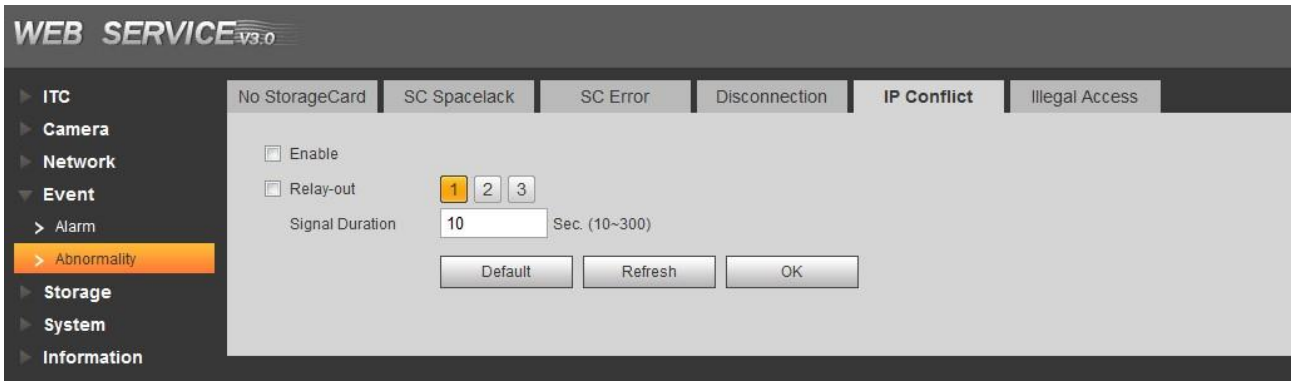
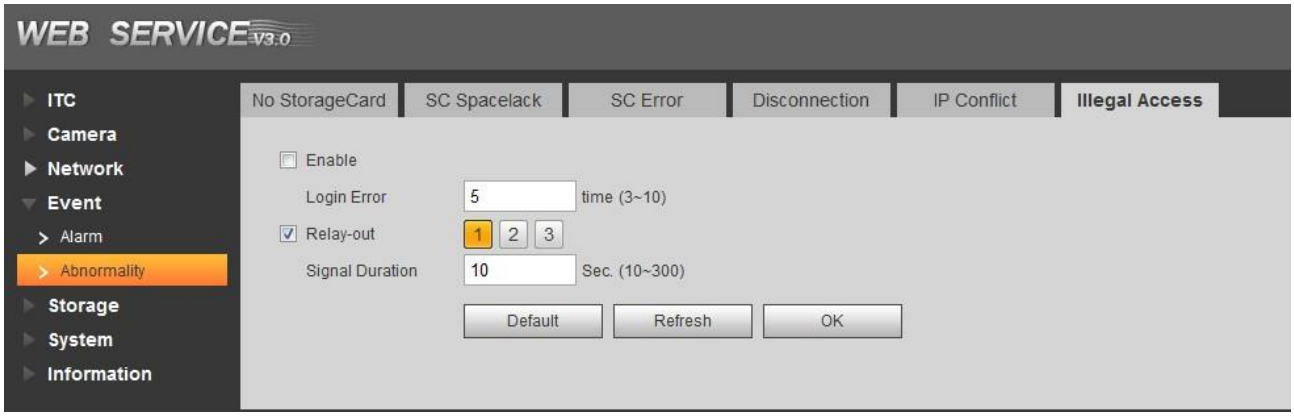


Figure 5-61 Illegal access



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-30 for more details.

Table 5-30 Abnormality parameters description

Parameter	Note
Enable	Select it and enable corresponding functions of processing abnormality.
Floor Level of SC	Set the remaining max space which triggers abnormality.
Relay-out	Select it and enable corresponding relay-out function, select the port number of relay-out.
Signal Duration	Relay-out lasts a period of time and stops after alarm is over. The time unit is second and it ranges from10s to 300s.
Login Error	Set the max times of login error, it ranges from 3 to 10

Step 3 Click **OK** to finish configuration.

5.4.5 Storage

In this section, you can set associated info of storage and record control.

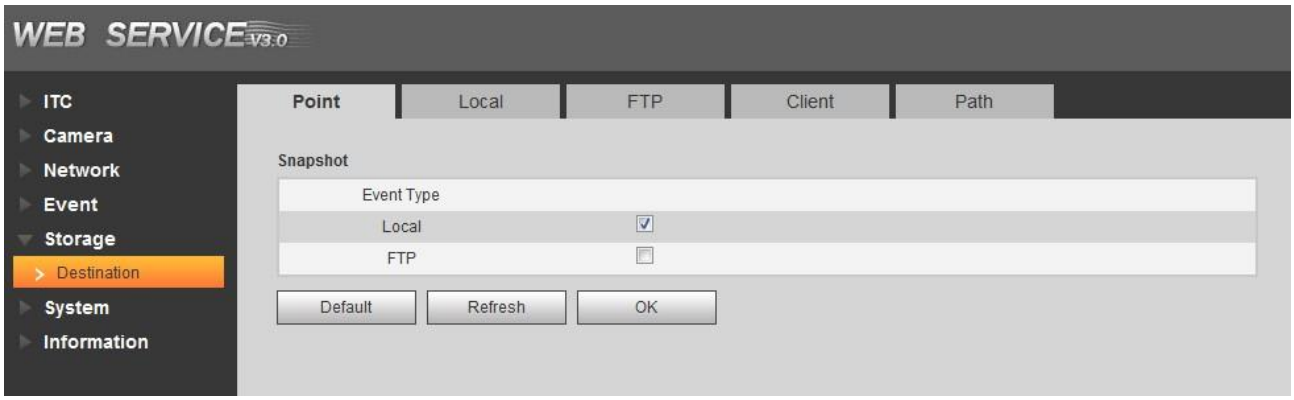
5.4.5.1 Point

Set the storage path of snapshot.

Step 1 Select Setting > Storage > Destination > Path.

The **Point** interface is displayed, see Figure 5-62.

Figure 5-62 Point



Step 2 Select **Event Type** according to actual requirement.

- Local: Store into the SD card.
- FTP: Store into the FTP server.

Step 3 Click **OK** to finish configuration.

5.4.5.2 Local

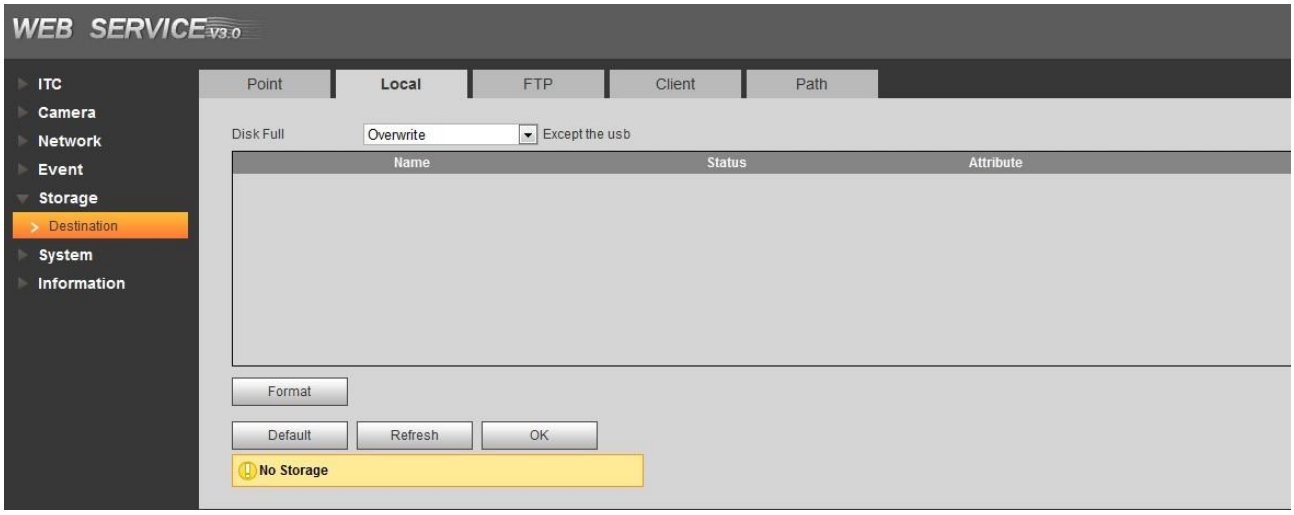
Please format the SD card before use.

Display the info of local SD card; you can set hot swap and formatting SD card.

Select **Setting** > **Storage** > **Destination** > **Local**, and the **Local** interface is displayed, see Figure 5-63.

- Select **Disk Full** and it includes overwrite and stop.
- View the storage info of the card.
- Click **Hot Swap**, you can then pull out the SD card.
- Click **Format**, you can then format the SD card.

Figure 5-63 Local



Click **OK** to finish configuration.

5.4.5.3 FTP

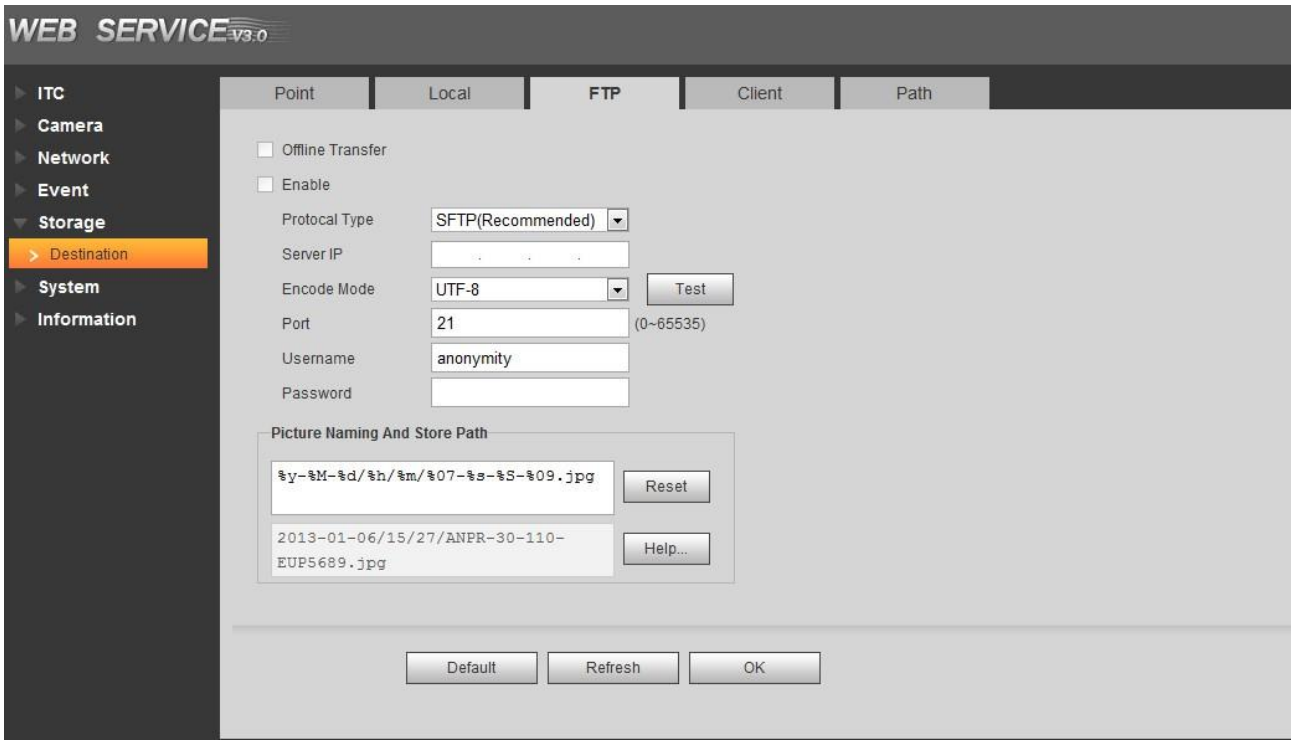
It can set picture name and storage path, click **Help** to view naming rule.

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

Step 1 Select Setting > Storage > Destination > FTP.

The FTP interface is displayed, see Figure 5-64.

Figure 5-64 FTP



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-31 for more details.

Table 5-31 FTP parameter description

Parameter	Note
Protocol Type	Select FTP storage protocol, which includes SFTP and FTP.
Offline Transfer	Select it and enable offline transfer. When network is disconnected or failed, you can store the picture into local storage card and it will automatically upload to FTP server or platform after network resumes.
Enable	Enable the storage path of FTP server.
Server IP	IP address of FTP server.
Encode Mode	Encode mode of Chinese character when naming picture, which includes UTF8 and GB2312. Click Test and it create two files adopting UTF-8 and GB2312 on the FTP server, which can be used to confirm server's encoding mode.
Port	The port number of FTP server.
Username	Username and password of FTP server.

Parameter	Note
Password	
FTP Naming	Set the naming mode of picture and storage path. Please refer to **Help** for more details.

Step 3 Click **OK** to finish configuration.

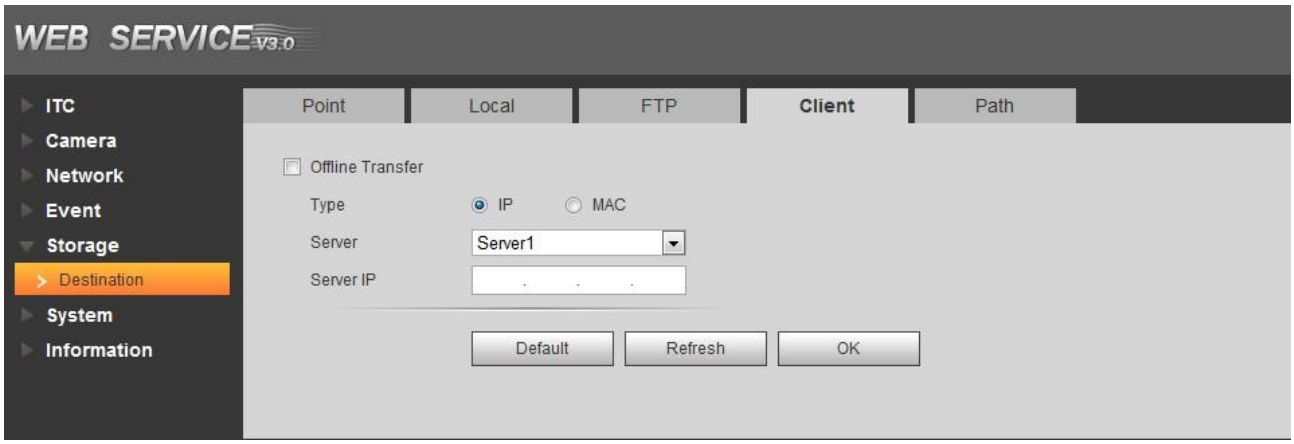
5.4.5.4 Client

In this section, you can set the parameters of offline transfer.

Step 1 Select Setting > Storage > Destination > Client.

The **Client** interface is displayed. See Figure 5-65.

Figure 5-65 Client



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-32 for more details.

Table 5-32 Client

Parameter	Note
Offline Transfer	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.
Type	Select connection type with platform server. ● IP: Connect to platform server via IP address. ● MAC: Connect to platform service via MAC address.
Server	Select server which includes server 1 and server 2.
Server IP	● When the type is selected as **IP**, then it has to fill in the server's IP address. ● When the type is selected as MAC, then it has to fill in the server's MAC address.

Step 3 Click **OK** to finish configuration.

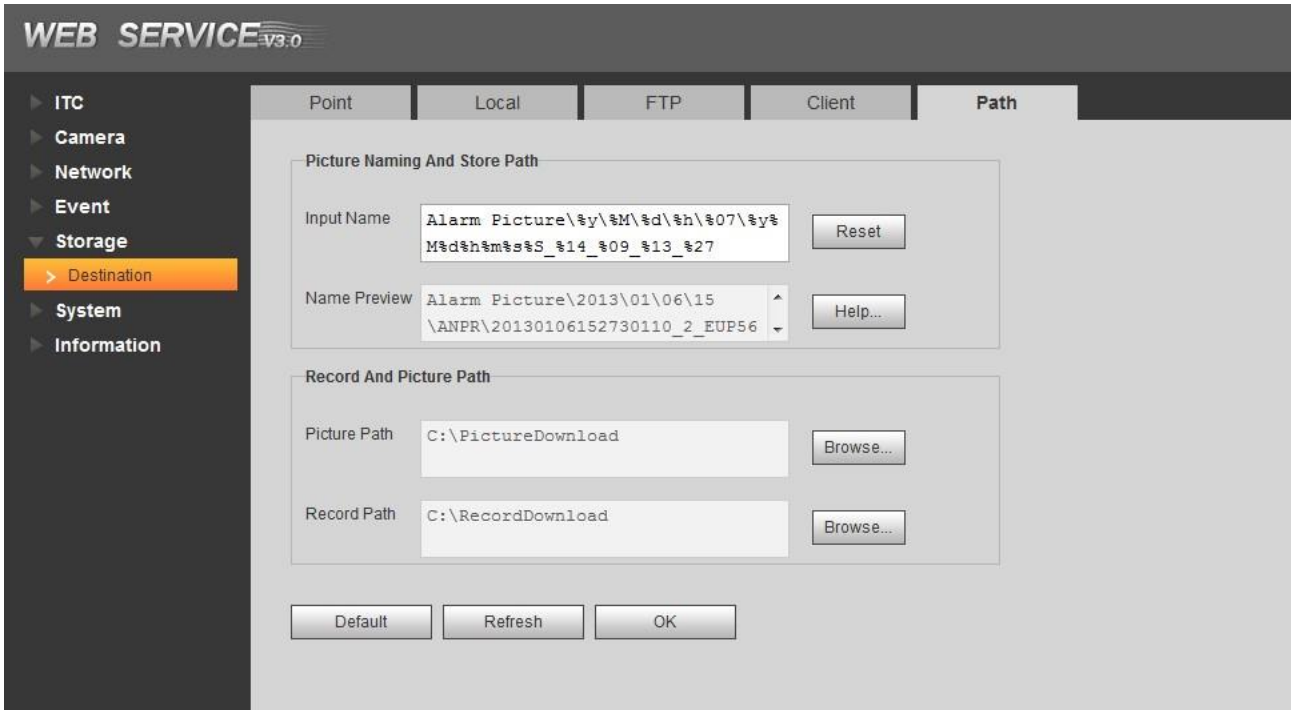
5.4.5.5 Path

In this section, you can set picture, record naming and path.

Step 1 Select Setting > Storage > Destination > Path.

The **Path** interface is displayed. See Figure 5-66.

Figure 5-66 Storage path



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

Step 3 Set the root path of record and snapshot according to actual requirement.

Step 4 Click **OK** to finish configuration.

5.4.6 System

The system supports configuring general info, adding user, restoring default setting and configuring import & export file etc.

5.4.6.1 General

5.4.6.1.1 General

In this section, you can set device SN, language and video standard etc.

Step 1 Select Setting > System > General > General.

The **General** interface is displayed. See Figure 5-67.

Figure 5-67 General

Step 2 Configure the parameters. Please refer to Table 5-33 for more details.

Table 5-33 General parameters description

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

Step 3 Click **OK** to finish configuration.

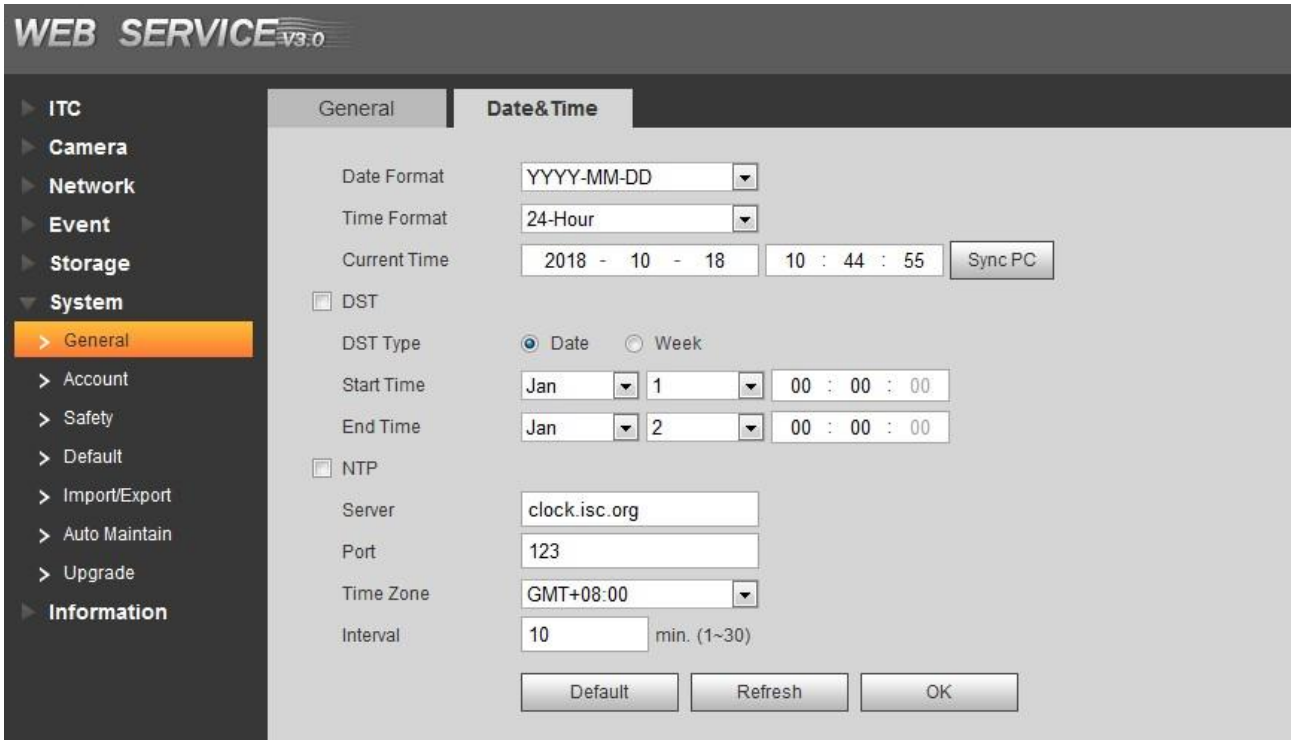
5.4.6.1.2 Date & Time

In this interface, you can set date and time format, system time, DST (Daylight Saving Time) or NTP server and so on.

Step 1 Select Setting > System > General > Date & Time.

The **Date & Time** interface is displayed. See Figure 5-68.

Figure 5-68 Date & Time



Step 2 Configure the parameters. Please refer to Table 5-34 for more details.

Table 5-34 Date & Time parameter description

Parameter	Note
Date Format	Select date format.
Time Format	Select 24h or 12h system.
System Time	Set current system time of the device. It becomes valid immediately after setting.
Sync PC	Modify the device system time to the PC system time.
DST	Enable the function and then set start time and end time of DST. Set according to data or week.
NTP	Select to enable the function of network time sync.
NTP Server.	Time server address.
Port	Port number of time server.
Time Zone	The time zone where the device is located.
Interval	The sync interval between device and time server.

Step 3 Click **OK** to finish configuration.

5.4.6.2 Account

5.4.6.2.1 Account

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

Username

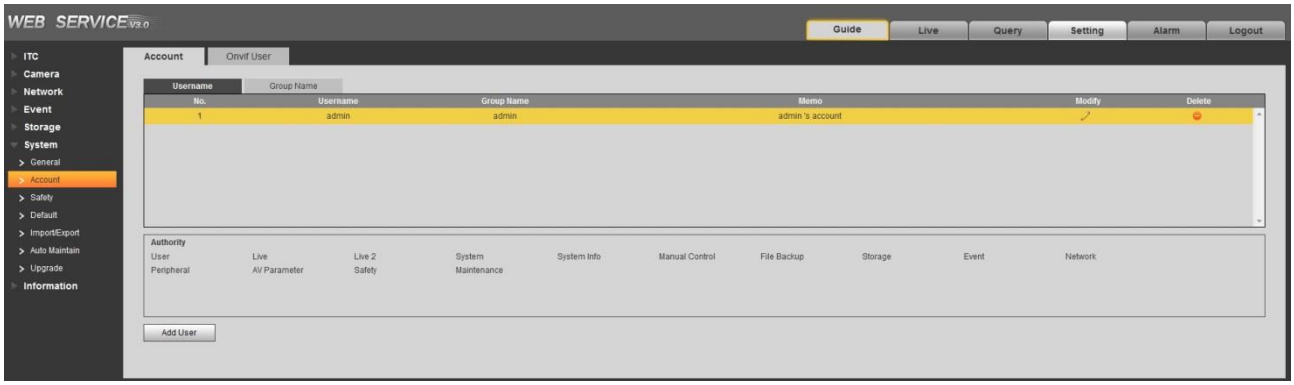
- The user with **Account** control authority can also modify the password of other users.
- It is recommended to give fewer authorities to normal users than premium users in order to make user management convenient.
- Cannot delete the user in the login status.

In this interface, it can add, delete or modify user.

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

The **User** interface is displayed. See Figure 5-69.

Figure 5-69 Username



Step 2 Click Add User.

The **Add User** interface is displayed. See Figure 5-70

Figure 5-70 Add user

Step 3 Configure the parameters of dialog box. Please refer to Table 5-35 for more details.

Table 5-35 Add user parameters description

Parameter	Note

Parameter	Note
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 types from capital letter, small letter, number and special characters (excluding "'", """, ";", ":" and "&") ● Follow the password security notice to set a high security level password. ● The new password should be in accordance with the confirm password.
Confirm Password	
User Group	Select the group that new users belong to. Each group has different authorities.
Authority	Select the authorities which belong to the user.

Step 4 Click **Save** to finish configuration.

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

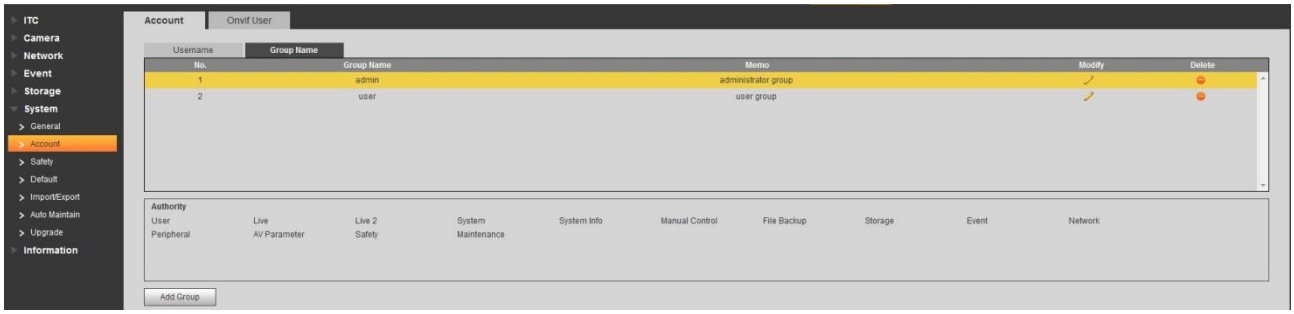
You have two groups named admin and user by default, you can add new group, delete added group or modify group authority and memo.

Step 1 Select Setting > System > Account > Account > Group Name.

The **Group Name** interface is displayed, see Figure 5-71.

- 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.

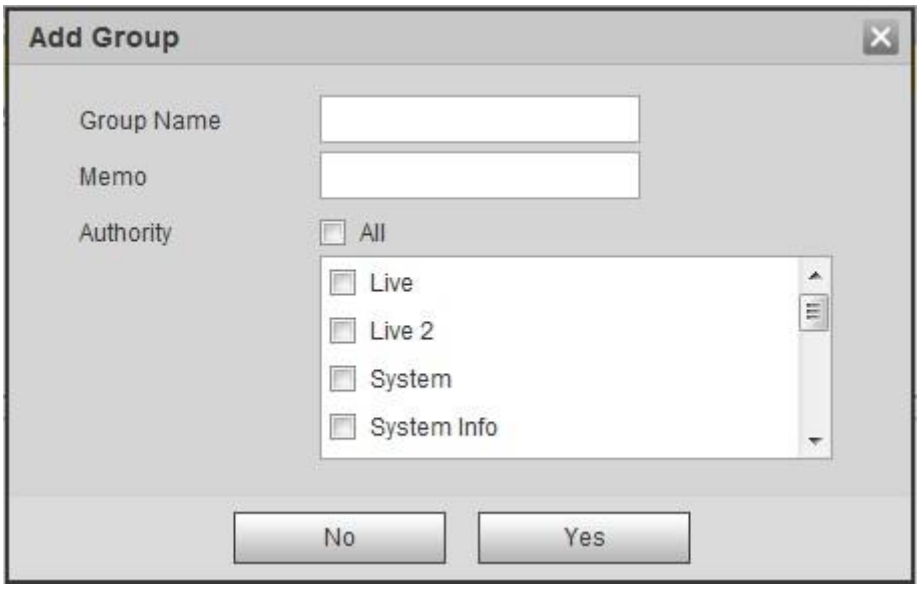
Figure 5-71 User Group



Step 2 Click Add Group.

The **Add Group** interface is displayed. See Figure 5-72.

Figure 5-72 Add Group



Step 3 Fill in the name of user group and configure 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** to finish configuration.

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.

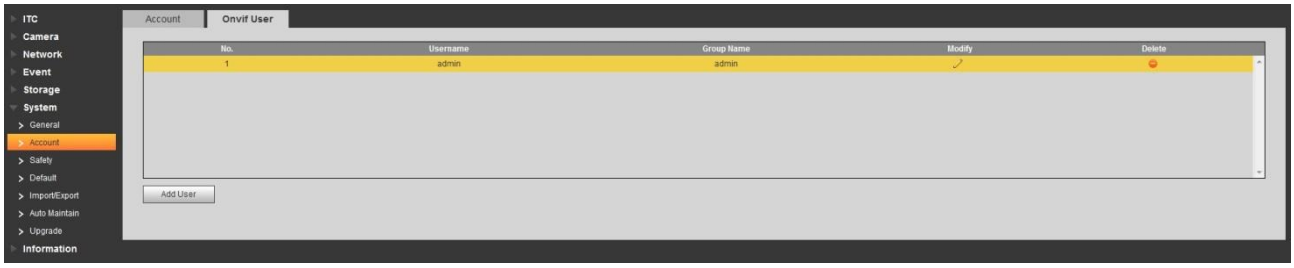
5.4.6.2.2 ONVIF User

Onvif (Open Network Video Interface Forum), it can add, delete, modify Onvif in the user management interface

Step 1 Select “Setting > System > Account > ONVIF user”.

The ONVIF user interface is displayed, see Figure 5-73.

Figure 5-73 Configuring Onvif Users



Step 2 Click Add User.

The **Add User** interface is displayed. See Figure 5-74

Figure 5-74 Add user

Step 3 Configure user parameters. For the detailed description, see Table 5-36.

Table 5-36 User parameter description

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

Step 4 Click **Save** to finish configuration.

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.

5.4.6.3 Safety

5.4.6.3.1 IP Filter

In order to strengthen network security and protect device data, you can set the user who has access to the device via IP filter.

- Set trusted list mode: It only allows the user whose IP address exists in trusted list to log in device.

- Set banned list mode: The user whose IP address exists in banned list is forbidden to log in device.

It fails to support enabling trusted list and banned list at the same time.

Step 1 Select Setting > System > Safety > IP filter.

The **IP Filter** interface is displayed, see Figure 5-75.

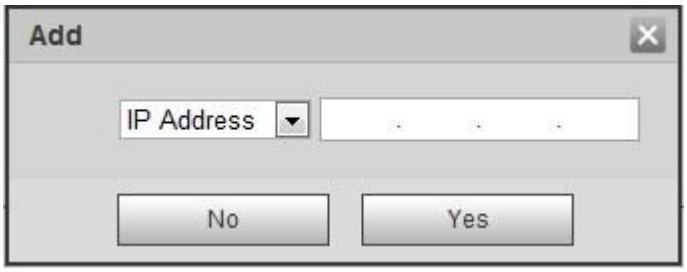
Figure 5-75 IP Filter

Step 2 Take the example of adding IP address user in trusted list.

1) Click **Add**.

The **Add** interface is displayed. See Figure 5-76

Figure 5-76 Add



2) Configure address information. Please refer to Table 5-37 for more details.

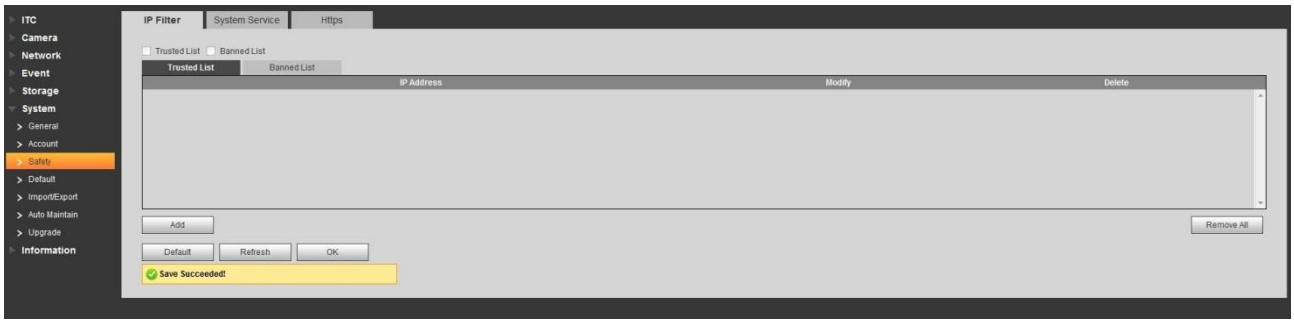
Table 5-37 Address parameter description

Parameter	Note
IP Address	Input the host IP address which needs to be added. The system supports up to 64 IP addresses.
IP Segment	Input the start IP and end IP of the target IP segment.
MAC Address	Enter the MAC address of the target host.
IPv6	Enter the IP v6 address of the target host.

3) Click **OK**.

The system will prompt **Operation succeeded. Click OK to take effect.** . See Figure 5-77

Figure 5-77 Trusted List



Step 3 Select **Trusted List** and select some line in the list.

Step 4 Click **OK** on the bottom of **Trusted List** tab. The system will prompt **Successfully saved**.

You can also implement following operations in the **Trusted List** tab.

- Click  and modify the added IP address or IP segment.
- Click  and delete the added IP address or IP segment.
- Click  and remove all the IP address or IP segment.

The setting method of banned list is similar to trusted list. Please make settings by referring to the setting method of trusted list.

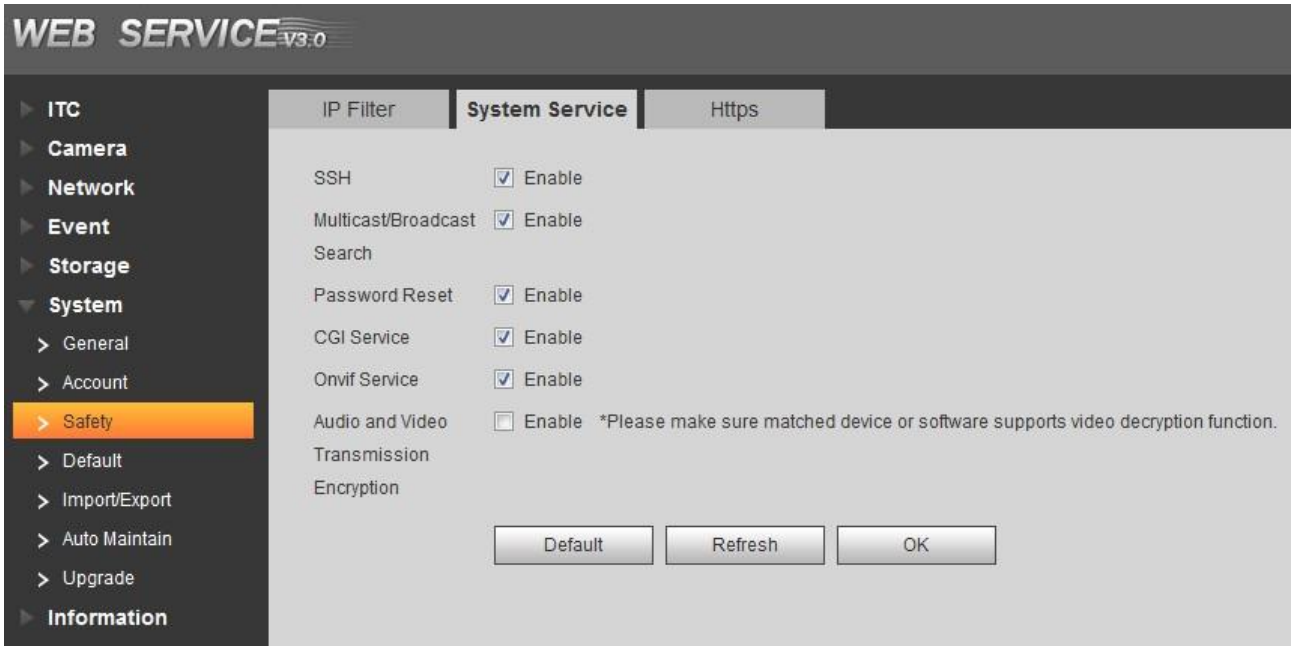
5.4.6.3.2 System Service

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

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

The **System Service** interface is displayed. See Figure 5-78.

Figure 5-78 System Service



Step 2 Select needed system service. Please refer to Table 5-38 for more details.

Table 5-38 System service parameters description

Parameter	Note
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 via password reset function.

Parameter	Note
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.

Step 3 Click **OK** to finish configuration.

5.4.6.3.3 Https

- You need to create server certificate and install root certificate if it is the first time to use HTTPS or after changing device IP address.
- After creating server certificate and installing root certificate, if it replaces the PC which logs in WEB, then it needs to redownload and install root certificate on the new PC or copy the downloaded root certificate on the new PC and install.

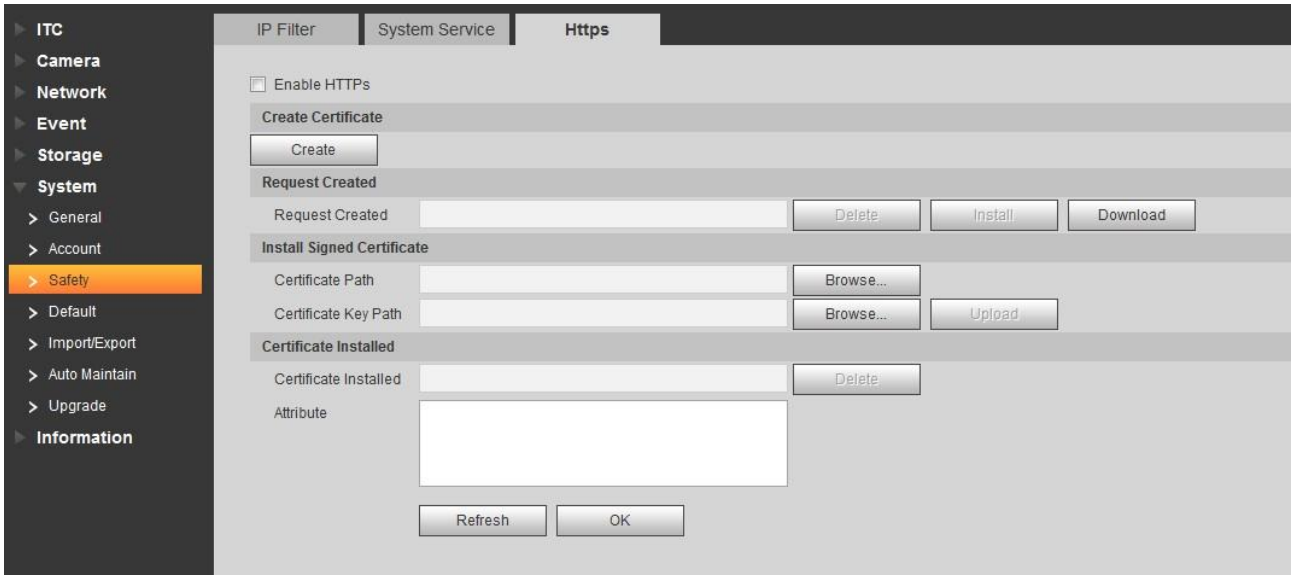
In the HTTPS setting interface, users can make PC log in normally via HTTPs by creating certificate or uploading authenticated certificate. It can ensure security of communication data and provide guarantee for user information and device safety via reliable and stable technical approach.

Step 1 Create certificate or upload the authenticated certificate

- If you select **Create Certificate**, follow the steps below.

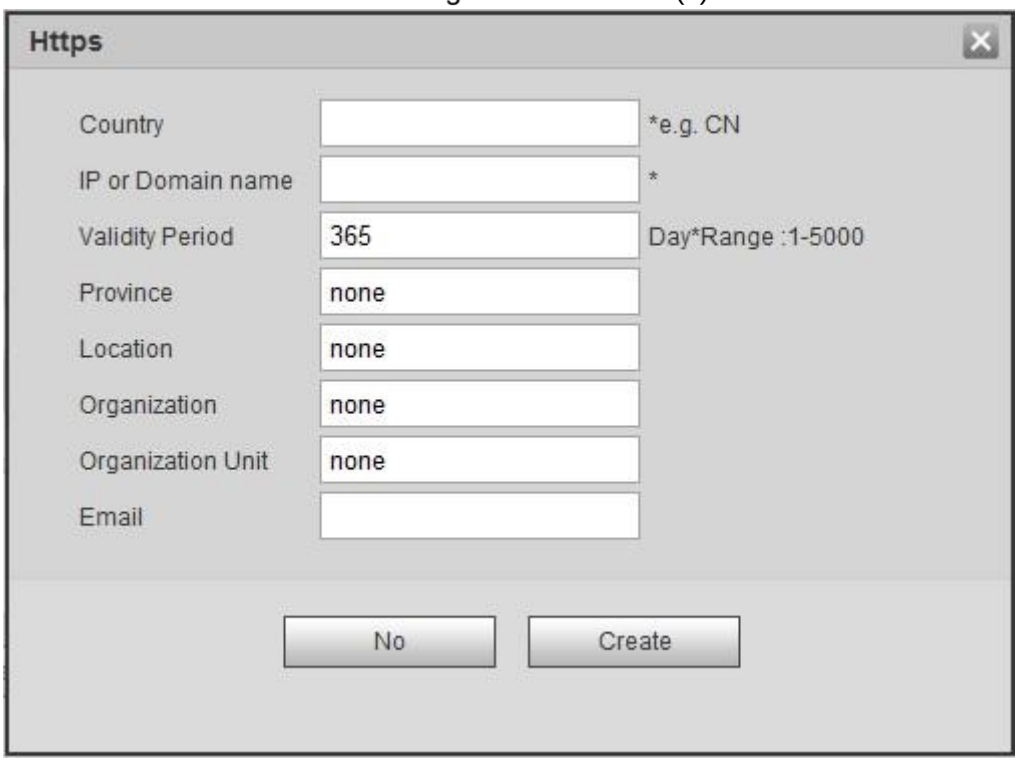
1) Select **Setting** > **Network** > **Https**.
The **HTTPs** interface is displayed. See Figure 5-79

Figure 5-79 HTTPS (1)



2) Click **Create**.
The **HTTPs** dialog box is displayed. See Figure 5-80.

Figure 5-80 HTTPS (2)

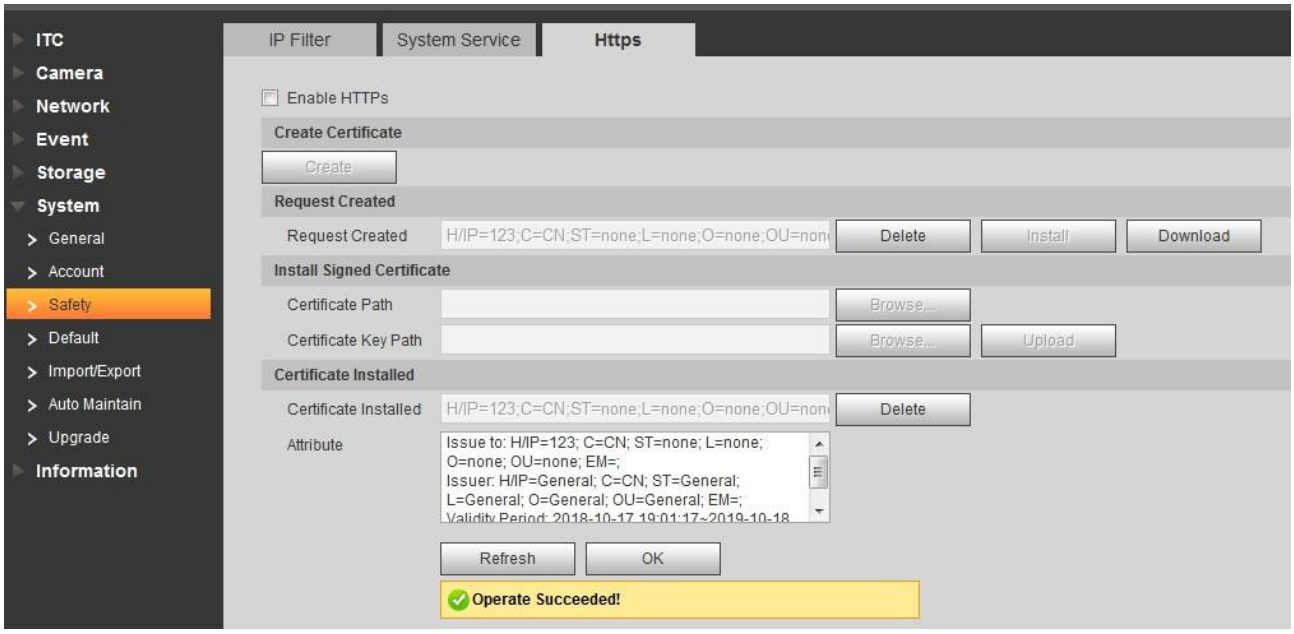


3) Enter the required information such as Country and IP/Domain Name etc. and then click **Create**.
   If the operation is correct, then the **Create successful** prompt is displayed.

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

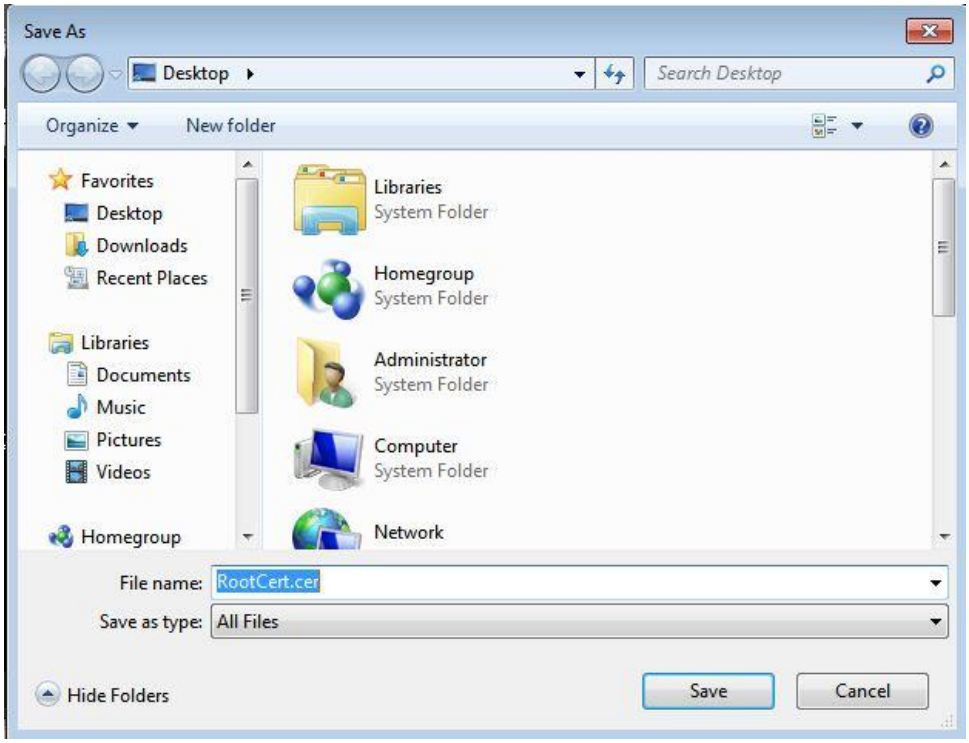
4) Click **Install**, see Figure 5-81.

Figure 5-81 Certificate Installation



5) Click **Download** to download root certificate.
   The system pops up **Save** as dialog box, select storage path and then click **Save**.

Figure 5-82 Download Root Certificate



6) Double-click the “RootCert.cer” icon.
The **Certificate** interface is displayed, see Figure 5-83.

Figure 5-83 Certificate information

7) Click **Install Certificate**.
The **Certificate Import Wizard** interface is displayed, see Figure 5-84.

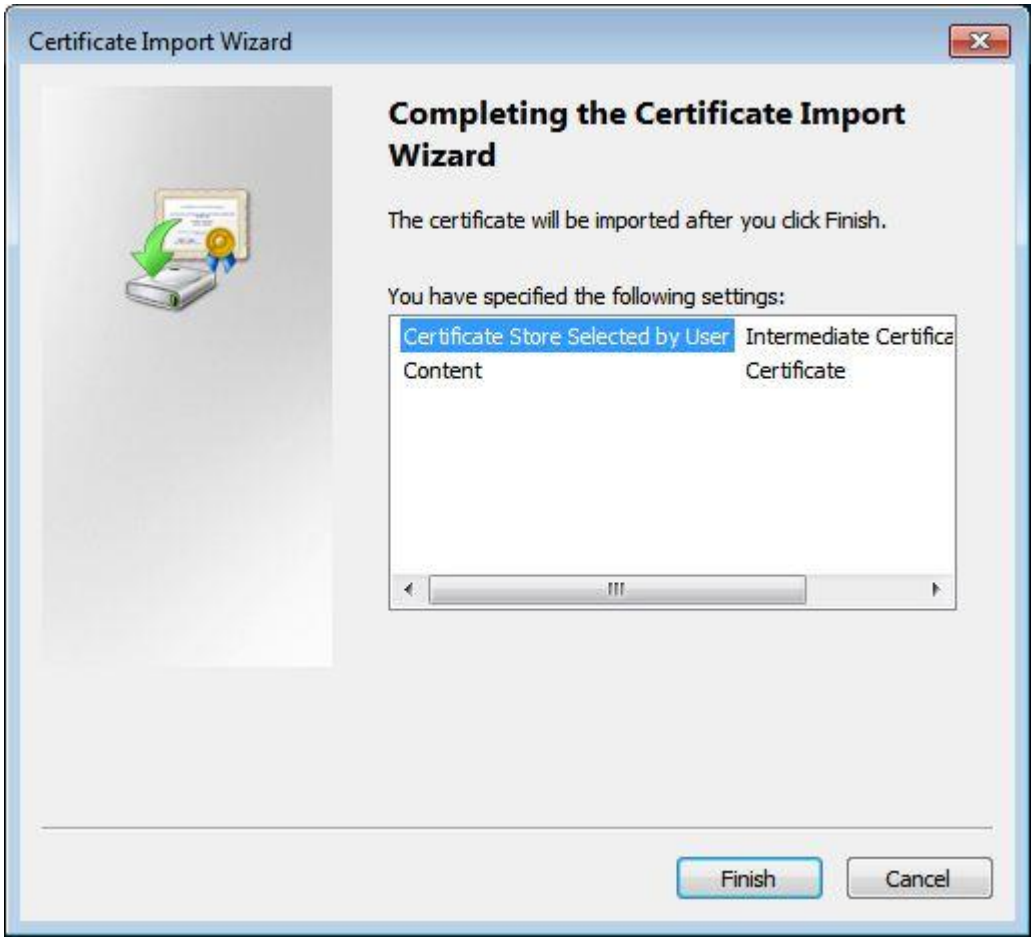
Figure 5-84 Certificate import wizard

8) Click **Next**.
Select **Trusted Root Certification Authorities**, see Figure 5-85.

Figure 5-85 Certificate Store

9) Click **Next**.
The **Completing the Certificate Import Wizard** interface is displayed, see Figure 5-86.

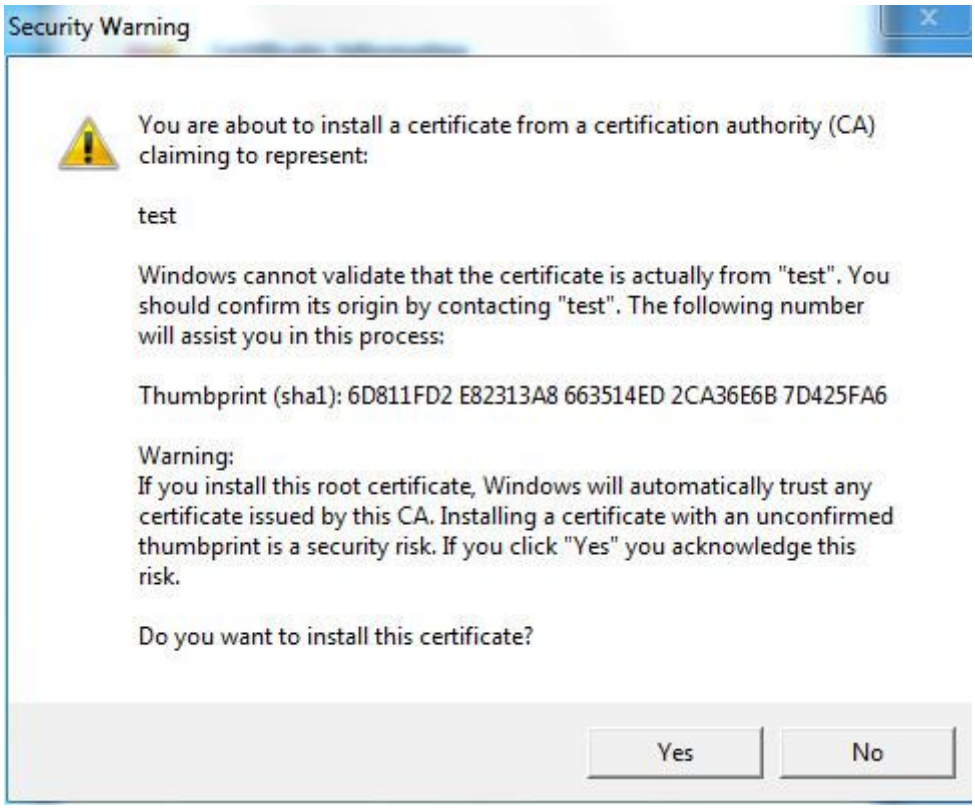
Figure 5-86 Completing certificate import wizard



10) Click **Finish**.

The **Security Warning** dialog box is displayed, see Figure 5-87.

Figure 5-87 Security warning



11) Click **Yes**.

The **Import was successful** dialog box is displayed, click **OK** to finish download, see Figure 5-88.

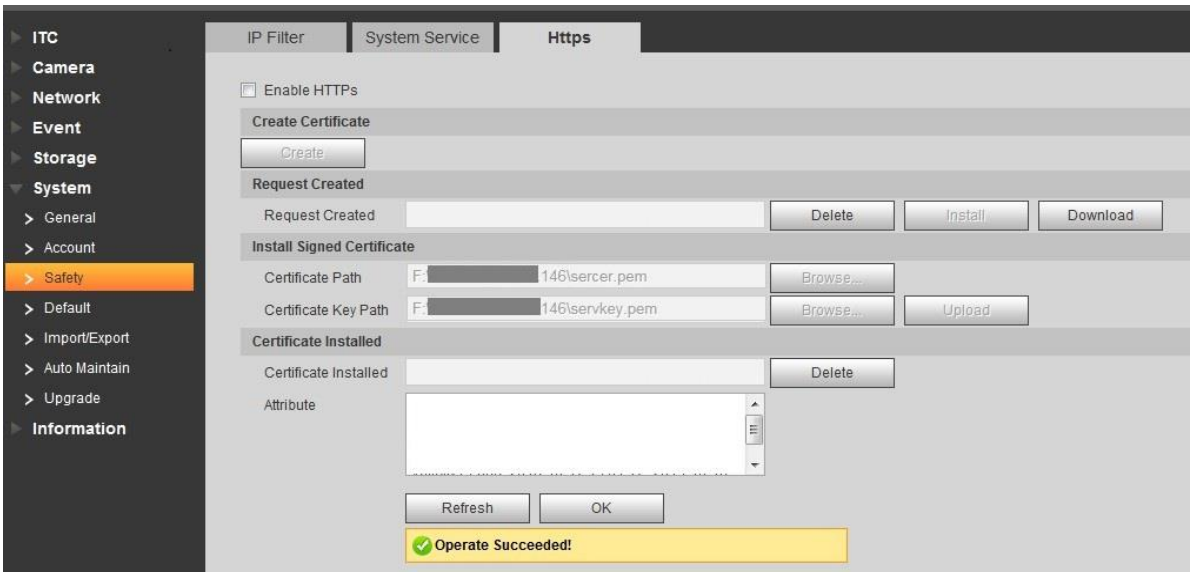
Figure 5-88 Import succeeded!

- If you select **install signed certificate**, follow the steps below.

1) Select **Setting** > **Network** > **HTTPS**.

The **HTTPS** interface is displayed. See Figure 5-89.

Figure 5-89 Install signed certificate



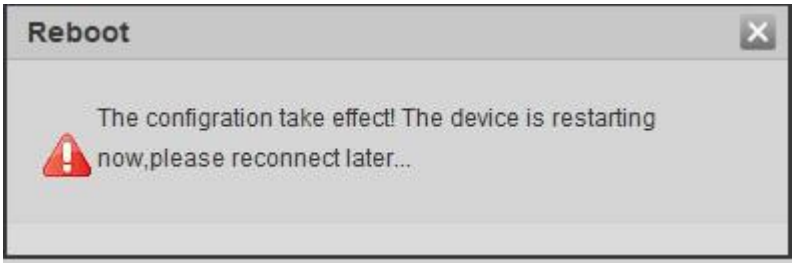
2) Click “Browse” to upload the signed certificate and certificate key, and then click **Upload**.

3) To install the root certificate, see operation steps from 5) to 11) in **Create Certificate**.

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

Need to Reboot Device interface is displayed. Config takes effect.

Figure 5-90 Need to reboot device



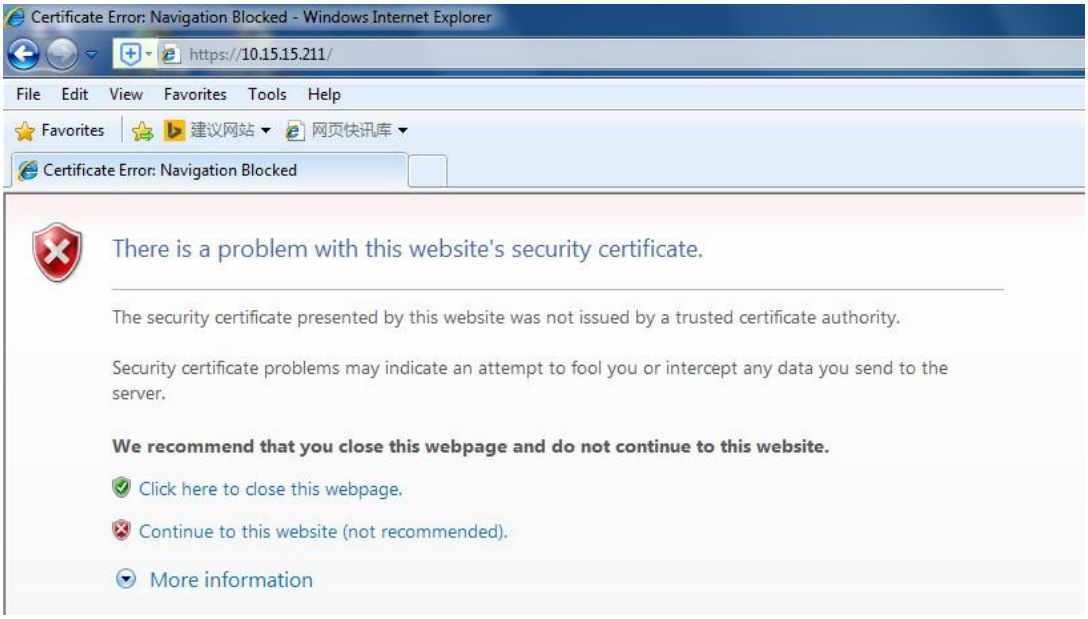
Use HTTPs

xx.xx.xx.xx corresponds to your device IP address or domain name.

Use HTTPs login

Inputhttps://xx.xx.xx.xx in the browser, the login interface is displayed; the browser will prompt certificate error if certificate is not installed. See Figure 5-91.

Figure 5-91 Certificate error



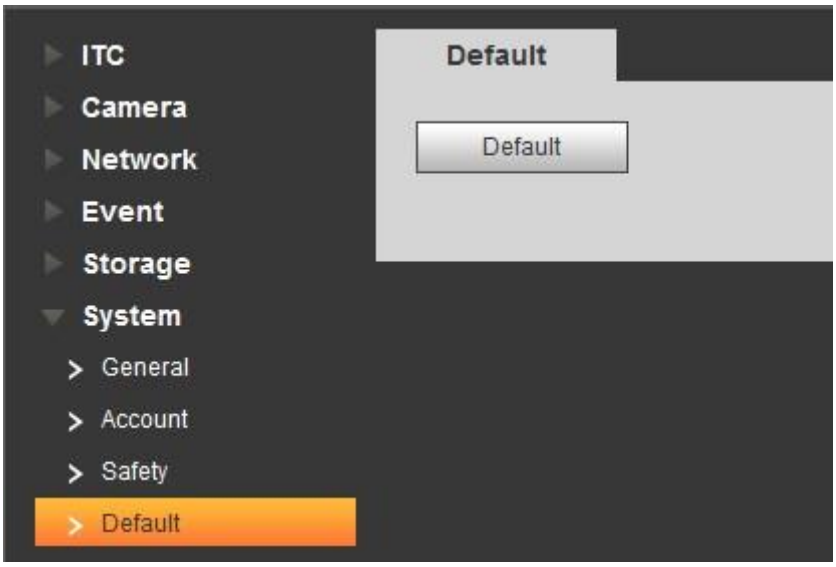
5.4.6.4 Default setting

It can realize device default setting in this interface, click **Default** and the device reboots and the system will restore.

Select **Setting** > **System** > **Default**, the **Default** interface interface is displayed, see Figure 5-92

Network IP address information is not restored to default.

Figure 5-92 Default setting



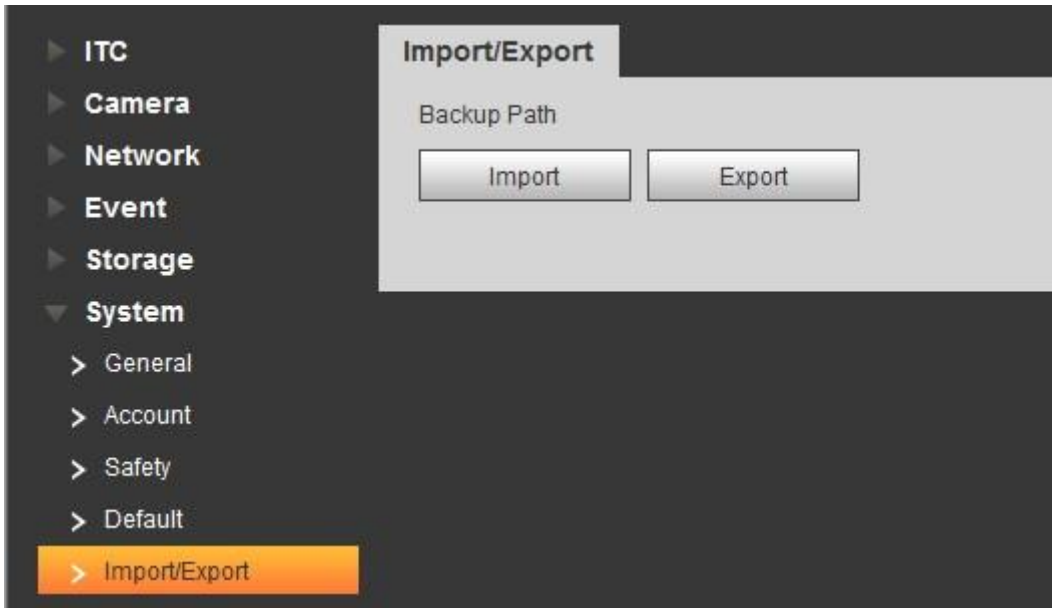
5.4.6.5 Import/Export

Export the system configuration file to backup the system configuration; Import system configuration file to make quick configuration or recover system configuration.

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

The **Import/Export** interface is displayed. See Figure 5-93.

Figure 5-93 Import/Export



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

- Import: Import the local system configuration file to the system.
- Export: Export associated config 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.

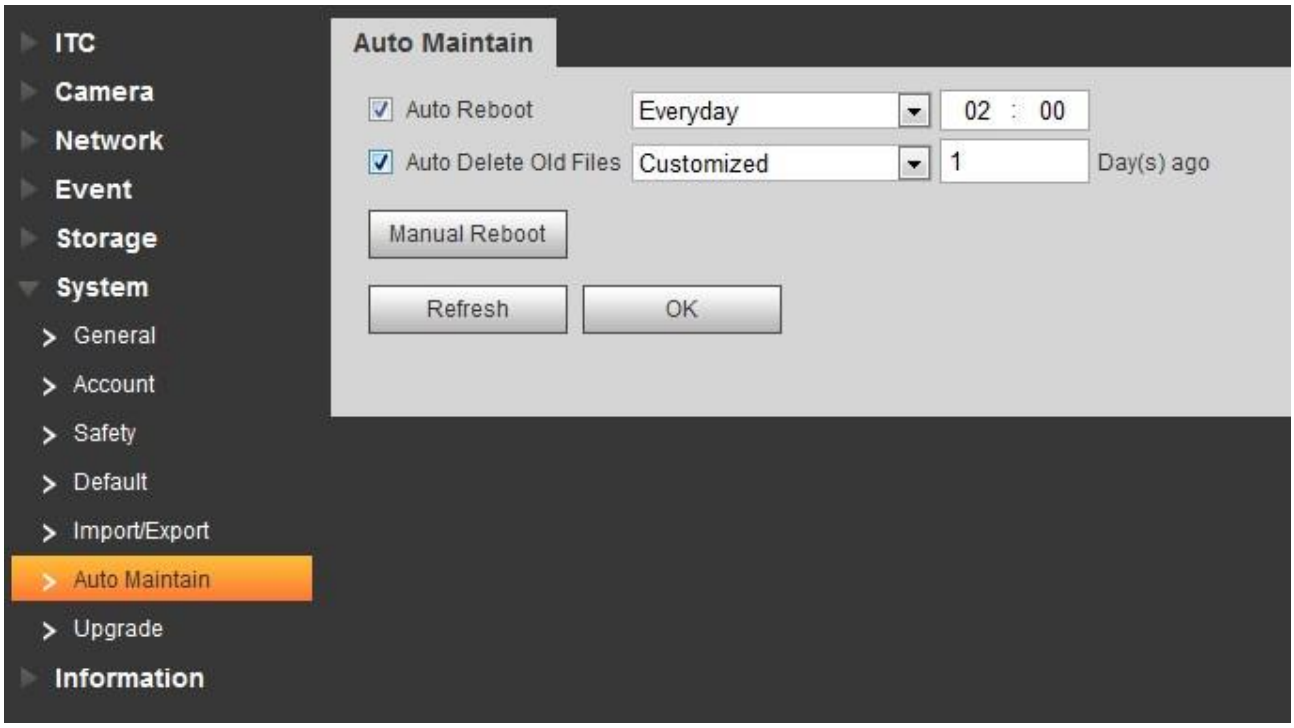
5.4.6.6 Automatic Maintenance

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

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

The **Auto Maintain** interface is displayed. See Figure 5-94.

Figure 5-94 Automatic Maintenance



Step 2 Configure parameters according to actual requirement. Please refer to Table 5-39 for more details.

Table 5-39 Auto maintain parameter description

Parameter	Note
Auto Reboot	● The system will automatically reboot within the set period and time. ● Select and set reboot period and time.
Auto delete old files	Customize time and delete all the old files before the time.
Reboot device	Manual Reboot

Step 3 Click **OK** to finish configuration.

5.4.6.7 Firmware Upgrade

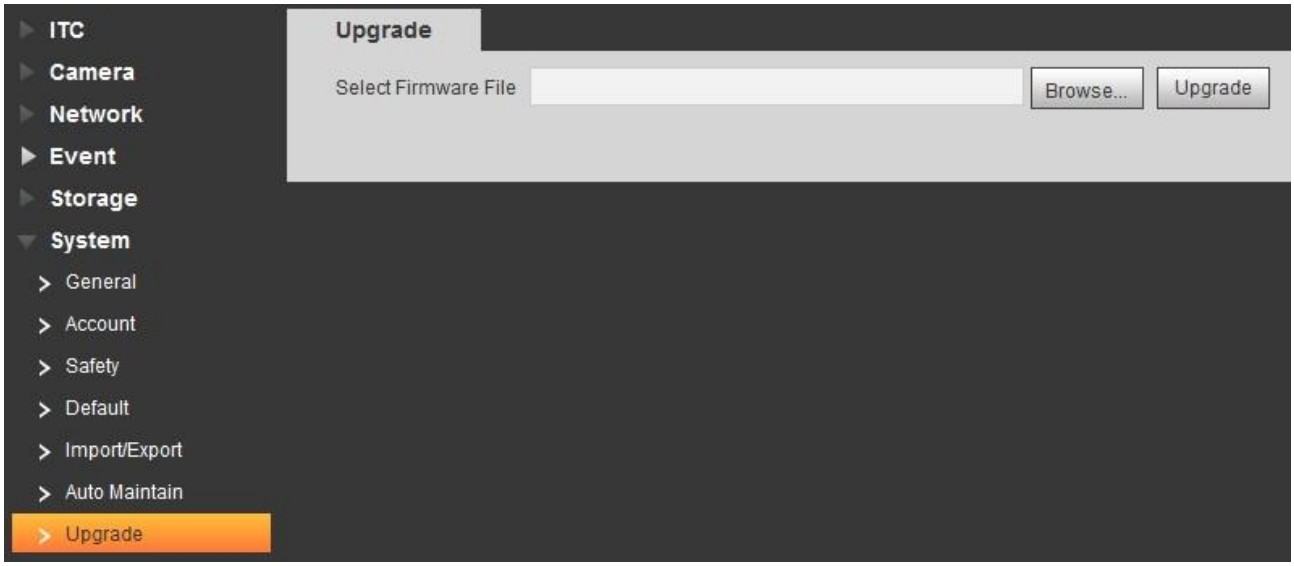
- Upgrading the wrong program might result in the device not working properly.
- During upgrading, make sure the device is not disconnected from power and network, and reboot or shut down the Web.

Upgrade device firmware.

Step 1 Select Setting > System > Upgrade.

The **Upgrade** interface is displayed. See Figure 5-95.

Figure 5-95 Firmware 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.

5.4.7 Information

The system supports viewing version, user and log etc.

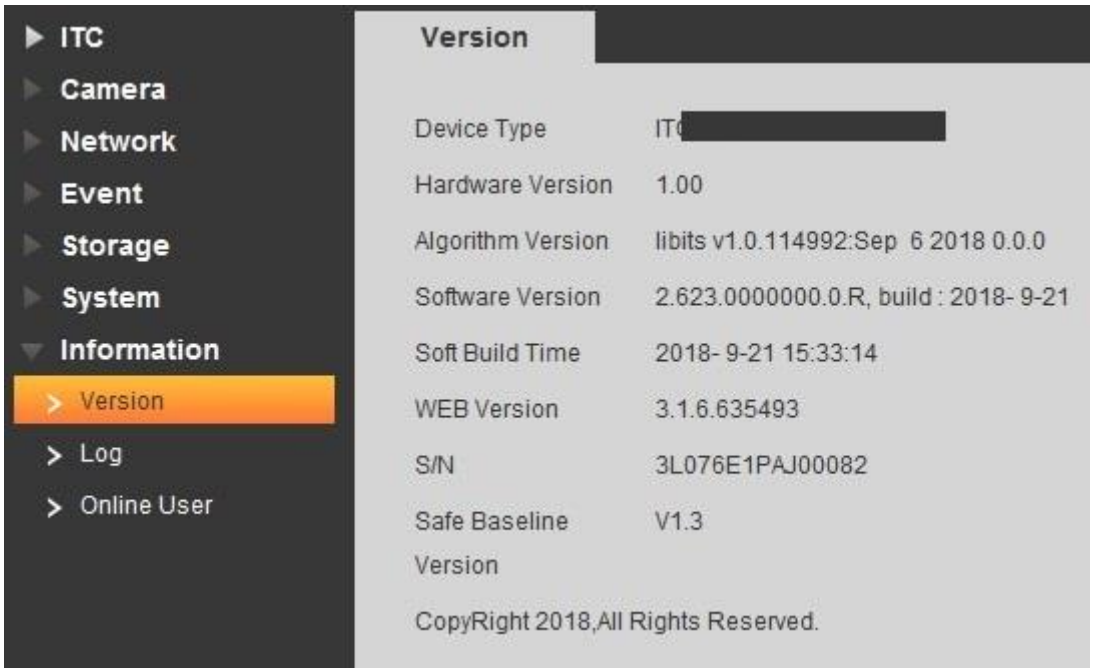
5.4.7.1 Version

In this section, it can view the version information of current WEB.

Select **Setting** > **Information** > **Version**, and the **Version** interface is displayed. See Figure 5-96.

Versions of different devices might vary, and the actual WEB interface shall prevail.

Figure 5-96 Version



5.4.7.2 Log

5.4.7.2.1 Log

The earliest log records will be covered when the number of log records reaches 2014.

In this interface, you can view log information such as system, config, data:, event, record, user management and clear log etc.

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

The **Log** interface is displayed. See Figure 5-97.

Figure 5-97 Log

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

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

Step 4 View, backup and clear the searching result.

Backup: Backup the inquired system log information to local, the backup is **.txt** file.

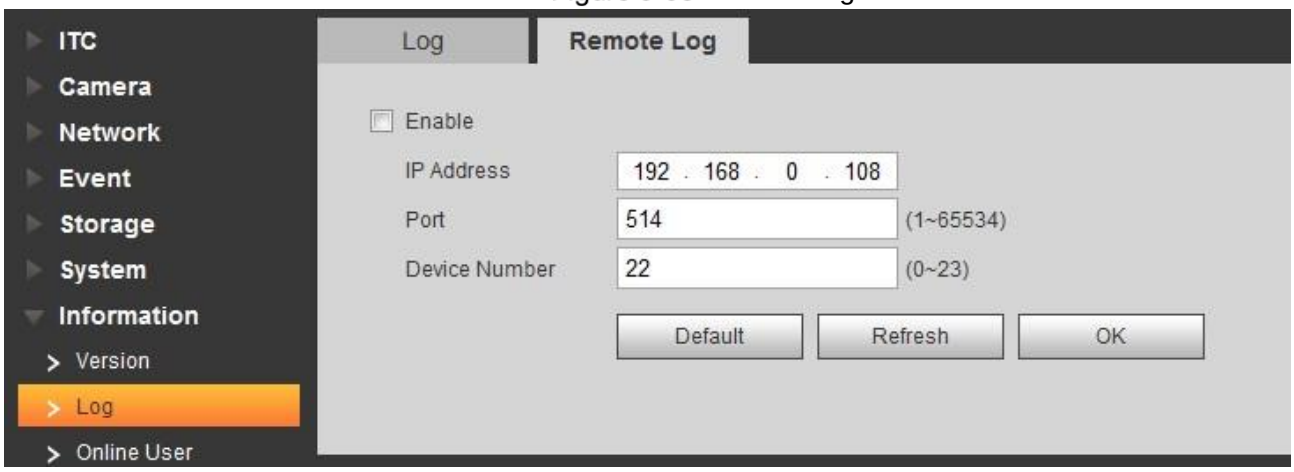
5.4.7.2.2 Remote Log

Enable remote log and set IP address of remote log server.

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

The **Remote Log** interface is displayed. See Figure 5-98.

Figure 5-98 Remote Log



Step 2 Select **Enable** and remote log function is enabled.

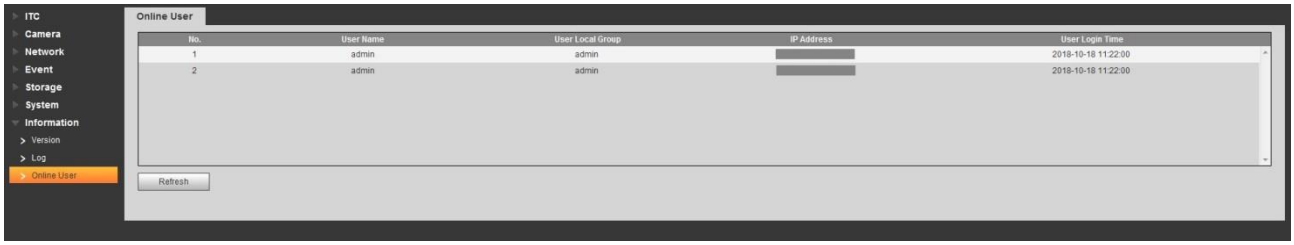
Step 3 Refer to the setting above. Click **OK** to finish configuration.

5.4.7.3 Online User

It can view the information of all the online users in this interface.

Select **Setting** > **Information** > **Online User**, and the **Online User** interface is displayed, see Figure 5-99.

Figure 5-99 Online User



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

5.5 Alarm

Click the **Alarm** tab and the alarm tab is displayed. See Figure 5-100.

In this interface, you can select alarm type, operation and tone, view the alarm time, type and channel. Please refer to Table 5-40 for more details.

Figure 5-100 Alarm

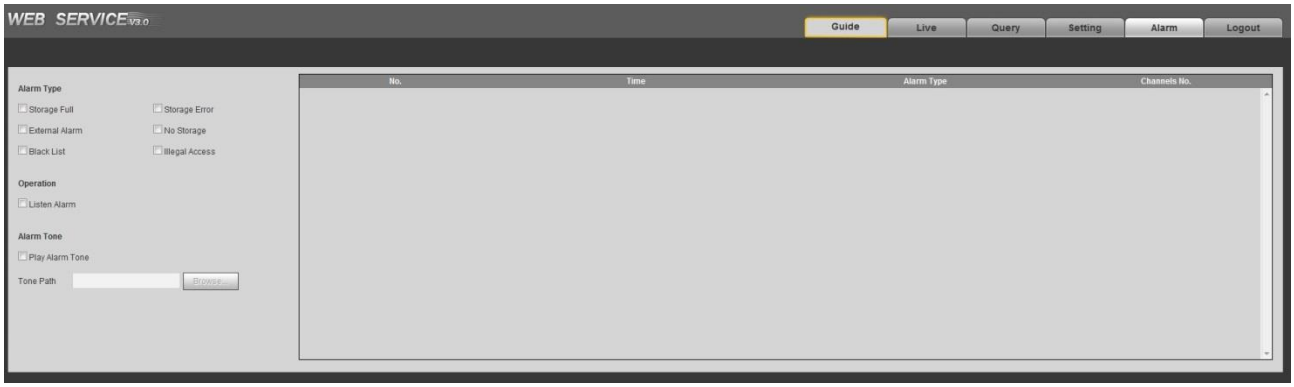


Table 5-40 Alarm parameters description

Type	Parameter	Parameters description
Alarm Type	Storage Card Full	It triggers alarm when storage card is full.
	Storage Card Fault	It triggers alarm when storage card fault occurs.
	Peripheral Alarm	It generates alarm via peripheral device when alarm is triggered.
	No Storage Card	It triggers alarm when there is no storage card.
	Plate 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.
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 setting
	Tone Path	The path of customized alarm tone.

5.6 Logout

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

Figure 5-101 Login again

6 Technical Parameters

Table 6-1 Technical parameter table

Parameter Category	Parameter Name	Value
Model		ITC215-PW4I-LZF27135, ITC215-PW4I- IRLZF27135
Camera	Sensor type	1/2.8 inch CMOS
	Shutter	1/50～1/10000, auto or manual.
	Scanning mode	Progressive scanning
	Exposure mode	Supports full auto; customized auto; customize.
	White balance	Supports full auto; color temperature auto; customized color temperature
	Edge enhance	Supported
	WDR	Supported
Lens	Lens mount	Φ14 (motorized vari-focal)
	Lens Focal Length	2.7mm～13.5mm
	Iris Control	Auto iris
Image	Image compression standard	JPEG
	Image resolution	1920×1080 or 1280×720
	Video compression standard	Standard H.264 high profile 5.0
	Video bit rate	H.265 Or H.264 bit rate adjustable
	Video frame rate	● PAL 25fps ● NTSC 30fps
	Video resolution	1920×1080 or 1280×720
	Image setting	Saturation, brightness, contrast, white balance, gain, 3DNR can be adjusted via software, supports WDR.
Trigger Mode	I/O coil trigger	Supported
	RS-485 coil trigger	Supported
	Video detection	Supported
	Black/white list	● Supports max 10,000 white list vehicles, and directly links barrier output. ● Supports max 10,000 black list vehicles, and generates alarm event.
	Smart Recognition	Vehicle recognition, plate recognition, vehicle color recognition, logo recognition, model recognition, series recognition, head direction and vehicle features.
	Remote control	Implement remote config and control via WEB.
	OSD info overlay	Supported, it can customize time, location and plate etc.

Parameter Category	Parameter Name	Value
	Image Tampering proof	Supported, video/picture equipped with watermark and verification function.
Interface	Built-in LED	Built-in 6 LED lights NO, flash light brightness adjustable.
	Network port	1 , 10M/100M Ethernet port
	RS-485 port	2, RS-485 port, used to externally connect to 485 devices such as vehicle detector, display screen and so on.
	RS-485/232 port	1, RS-485/232 signal switchable, used to externally connect to 485 or 232 device.
	I/O input port	2, optocoupler input (switching value), used for vehicle detector signal input.
	Alarm input port	1, optocoupler input (switching value), used to trigger voice intercom and so on.
	Relay-out	2 channel optocoupler output, 1 channel relay output; used to link barrier and so on.
	HDCVI port	1 channel, connect to panoramic camera and used for scene monitoring.
	Storage port	Built-in 1 SD card port, supports max 128G.
General Parameter	Power supply	DC 12V or POE802.3at
	Power Consumption	<24W
	Working temperature	- 30℃～+ 65℃
	Working humidity	10%～90%
	Enclosure material	Plastic decoration accessory + die casting aluminum
	Size (mm)	296.5×124×108
	Weight	1.9kg
	Protection level	IP67

Table 7-1

FAQ	Measures
Device error. Failed to normally operate or start.	Press the **Reset** button for 5 seconds and make the device restore to default setting.
Storage card hot swap	Please stop recording and snapshot before removing storage card. Operation can be made after 15 seconds in order to guarantee data completeness; otherwise it may cause the danger of data loss.
Write times limit of storage card	Please do not set the storage card as the storage media of scheduled record, otherwise it will rapidly reach the write longevity and cause damage to the storage card.
Failed to use disk for storage	When the storage card shows sleep mode or 0 capacity, please first format it via WEB interface.
Network upgrade failed	When network upgrade fails, the status indicator light shows red. At this moment, upgrade can be continued via port 3800.
SD card recommended type	Kingston 16GB, Kingston 32GB, Kingston 64GB. It is recommended to use class 10 high capacity card, which supports max 128G SD card.
Failed to pop up the installation dialog box of WEB control webrec.cab.	Please set the security level of IE browser as **Low**, **Active Plug-in and Control** is set as **Enable**.