



**Safety Technology
International**

STI G3 & GF Cam (IPCAMERA) User Manual

Version: 1.0.1

Date: 2024.07.24

1 Contents

1.	Product description	5
1.1	Product brief introduction	5
1.2	Product features.....	5
2	Installation & use.....	7
2.1	Connecting to ONVIF compatible NVR.....	7
2.2	Local desktop access using a web browser	7
2.2.1	Install ONVIF Device Manager v2.2.250 or newer	7
2.2.2	Expert installation (TCP/IPv4).....	8
2.2.3	Beginner installation procedure (TCP/IPv4).....	8
2.2.4	Beginner Network Troubleshooting.....	10
2.3	Web Interface - Camera first log in and control installation	12
2.3.1	Alternative way to find and download “Webconfig.exe”	14
2.4	Resetting IPv4 to automatically obtain IP address.....	15
3	Web - Main dashboard layout.....	16
4	Camera settings.....	19
4.1	Video capture image settings.....	19
4.2	OSD settings	21
4.3	Custom Title Settings.....	22
4.4	Privacy mask settings	22
4.5	Video encoding settings	23
5	Network.....	24
5.1.1	Dynamic (DHCP) enables automatic IP address assignment	24
5.1.2	Basic configuration – Static IP address you choose	24
5.2	P2P settings	25
5.3	Stream media	26
6	Event settings	27
6.1	Motion detection / Alarm settings.....	27
6.2	IO Events.....	31
6.3	Intelligent detect.....	33

7	Storage settings.....	34
7.1	Storage settings.....	34
7.2	Timed recording	36
7.3	Storage device information.....	37
8	System settings.....	39
8.1	Account management.....	39
8.2	Device language	41
8.3	Timer settings.....	42
8.4	Restore factory	43
8.5	Reboot the device	45
8.6	Regular maintenance	45
8.7	Firmware upgrade	46
8.8	Version Information	47
9	FAQ.....	48
9.1	The device cannot be accessed through a browser.....	48
9.2	Normal data cannot pass through the switch.....	48
9.3	Error accessing the device through the browser after upgrading.....	48
10	Revisions.....	49

Thank you for purchasing STI's products. If you have any questions regarding use, please feel free to contact us.

This user manual is written according to the current software and hardware. Due to the update, modification, and upgrade of the software version, and the upgrade of the hardware equipment, there may be inaccuracies or imperfections in the technical problems described in the manual. Please understand, if you cannot solve the problem according to the user manual during use, please call our company's technical department to inquire about the relevant operation methods. The manual will be updated regularly, if necessary, please go to our official website to download without prior notice.

Software download address: www.sti-global.com

Recommended PC base configuration: CPU quad-core 3.0GHz, 4G memory, 512M independent graphics card, 2.1 sound card, Audio output, Mic input, Windows 2000/2003/XP/7, IE browser 6.0~9.0.

1. Product description

1.1 Product brief introduction

IPCAMERA is an embedded system, which is a 38*38 HD dedicated network module for compressing and processing audio and video data. It consists of audio and video compression encoder, input and output channels, network interface, audio and video interface, RS485 serial interface and protocol interface. The software interface and the like also provide video processing functions, mainly complete Figure data collection, H.264 Figure data compression, Internet transmission data and audio data processing, and can transmit real-time Figures and sounds simultaneously through the network.

IPCAMERA uses a faster computing digital processor to quickly compress larger and clearer Figures. It uses an advanced operating system and audio and video compression algorithms to make sound and Figure transmission smoother and clearer and more detailed. The embedded server is completely out of the PC platform, the system scheduling efficiency is high, the code is solidified in FLASH, and the system runs stably and reliably. Support remote Figure access via Internet Explorer. Supports two-way voice intercom, supports dynamic IP address, and facilitates network transmission of Figures and sounds.

1.2 Product features

- H.264/H.265 video compression standard, AAC/G.711 audio compression standard
- Embedded Web Server, fully supports Internet Explorer monitoring, configuration and upgrade
- Two-way audio real-time transmission on the Internet, video frame rate is automatically adjusted according to the bandwidth
- Support variable rate, while setting the quality of video and Figure, it can also limit the compression code stream of the video Figure
- Support level 2 domain name, easy to achieve dynamic IP address (ADSL dial-up)
- Video code rate 50Kbps-8Mbps (50Kbps-6Mbps) continuously adjustable, frame rate 1-30 (1-25) continuously adjustable
- Support capture, local video
- Support motion detection (settable area and sensitivity)
- Alarm pre-recording function
- 10/100M Ethernet interface support
- Support IO interface to connect other peripherals
- RS485 interface, network transparent channel connection, the client can be controlled by the transparent channel of the device
- Support multiple users to access simultaneously
- Alarm signal input and output
- Support for scheduled maintenance
- Support for networked storage and capture

-
- Support WEB configuration
 - Support OSD
 - Support client remote monitoring software
 - Support mobile phone monitoring
 - Support for crossing services



2 Installation & use

2.1 Connecting to ONVIF compatible NVR

Connect your Global Cam to your POE NVR via ethernet cable. Follow the instructions from the chosen NVR manufacturer to find and add Global Cam to your system.

NOTE/Troubleshooting: If your chosen NVR is not capable of power over ethernet (POE) you will need to add a 12VDC transformer to power your camera.

2.2 Local desktop access using a web browser

The connection diagram of the entire system framework of IPCAMERA is shown in Figure 2.1. Connect the various parts and connect the PC and IPCAMERA device directly through the computer, ethernet switch, or router.

NOTE/Troubleshooting: Depending on your chosen setup hardware (computer, ethernet switch, or router) capabilities, the next steps may require a POE injector device to power the IP camera during setup.

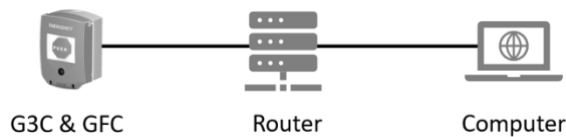


Figure 2.1 network connection diagram

2.2.1 Install ONVIF Device Manager v2.2.250 or newer

Download Link <https://sourceforge.net/projects/onvifdm/>

With the camera connected to the computer allow the camera to boot this could take 1min, then click refresh. The device list will show the Global Cam that you just connected, and you will see the IP address associated with the Global Cam.

Write down

IP Address: _____

Subnet Mask: 255.255.255.0

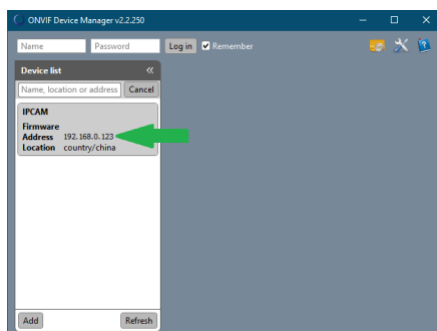


Figure 2.2.1 ONVIF device manager layout

2.2.2 Expert installation (TCP/IPv4)

The IP address of the device at the factory is **(recorded in step 2.2.1)**. The subnet mask is **255.255.255.0**.

Internet Protocol Version 4 (TCP/IPv4): If you know how to change your ethernet adapter settings on your camera to match this IP range please do so and skip to (Section 2.3 Camera first log in and control installation) if you do not, please follow section 2.2.3 Beginner installation procedure.

NOTE/Troubleshooting: Additional troubleshooting solution to determine the IP address of the camera, you can use:

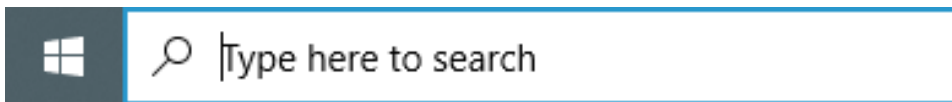
- Download ONVIF Device Manager v2.2.250 or newer.
- Install the LMS (License Management software is 3rd party option chosen to view IP cameras) client in Device Management > Add Device) to set the PC to access the 0-network segment.

2.2.3 Beginner installation procedure (TCP/IPv4)

Configure your personal computer's (PC) ethernet settings to the following basic network parameters:

- Click the windows icon (typically in the bottom left side of your screen).

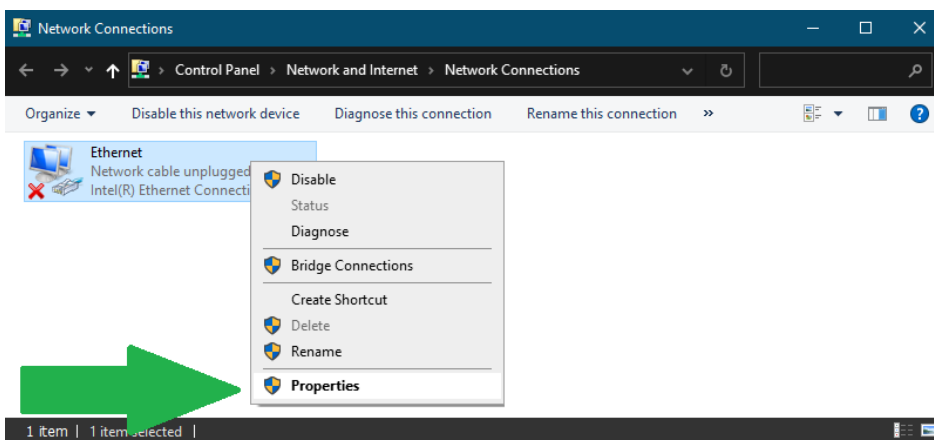
You will see “**Type here to search**”



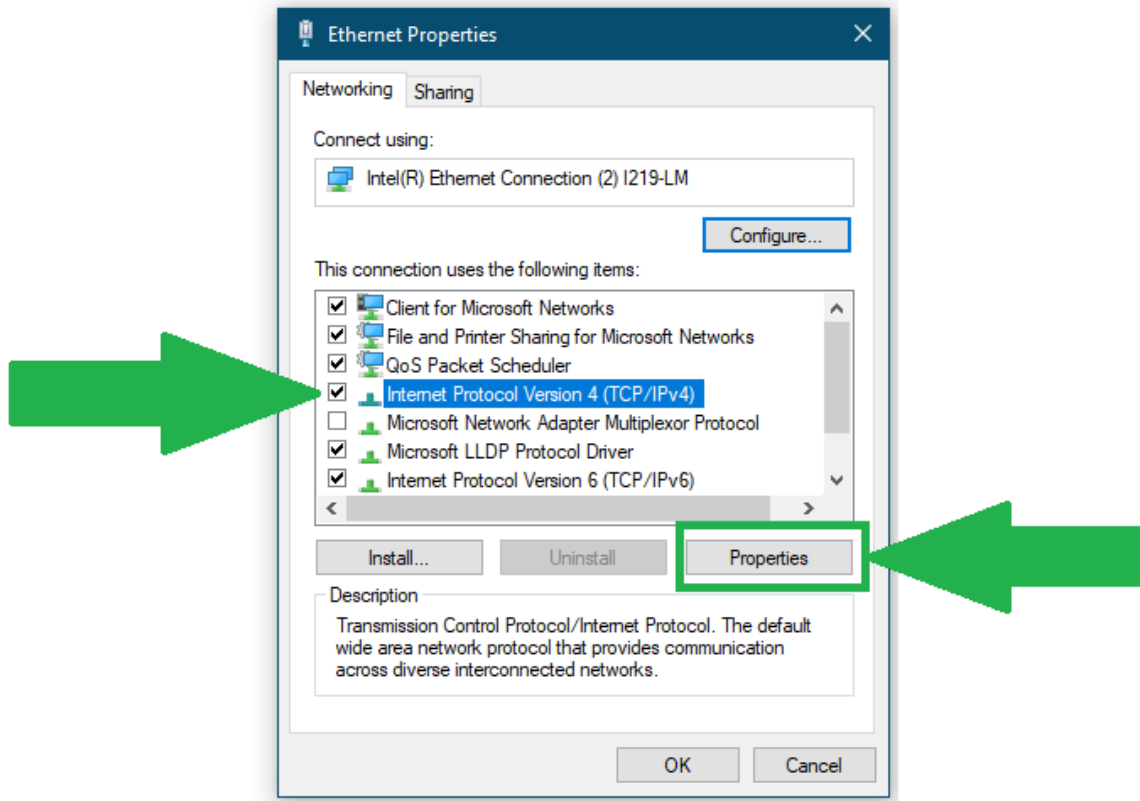
- Type “**Network connections**” then press the enter key on your keyboard.



- Right click “**Ethernet**” then select “**Properties**”



- Highlight “**Internet Protocol Version 4 (TCP/IPv4)**” Then select “**Properties**”

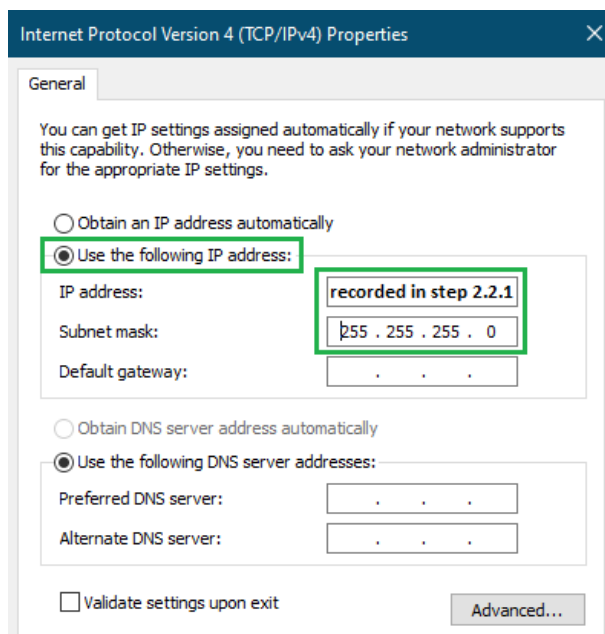


e. Make selections / inputs circled in green below.

IP address: **recorded in step 2.2.1**

Subnet mask: **255.255.255.0**

Then select: **OK**



disc

- f. Congratulations, your personal computer is now set to the same Internet protocol (IP) as your camera. Please proceed to section: 2.3 Camera first log in and control installation.

2.2.4 Beginner Network Troubleshooting

NOTE: may not be required - this is only needed if your camera will not open in your chosen web browser.

The IP address of the camera device at the factory is:

IP address recorded in step 2.2.1. The subnet mask is **255.255.255.0**

NOTE: If you have changed your camera's IP address from the default factory IP address

STI cannot fix this for you so make sure you recorded. If you get stuck you can push and hold the factory reset button for 5 seconds to complete factory reset.

You will need to follow advice in step 2.2.1 to find your camera's non-factory / current IP address.

- Troubleshooting to determine the IP address of the camera, you can use "ONVIF Device Manager v2.2.250" or install the LMS client in Device Management > Add Device) to set the PC to access the 0 network segment.
- In WINDOWS, press: Start-Run-cmd (figure 1.2) then you will see (figure 1.3), enter "**ping IP address recorded in step 2.2.1**" and press enter to determine if the network is open (figure 1.4) you will see "0% loss" and you can continue to Step 2.3.

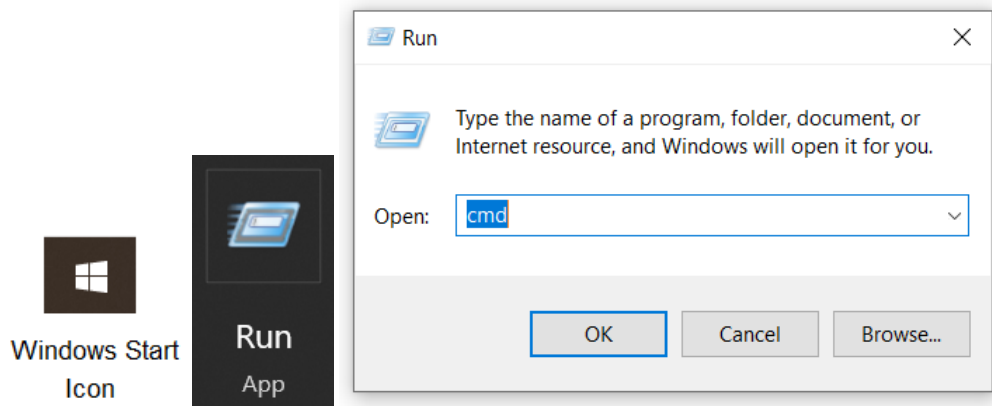


Figure 1.2 Enter "cmd" command in "Start" - "Run"

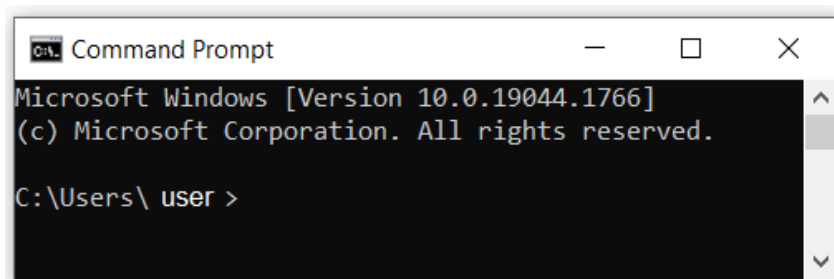
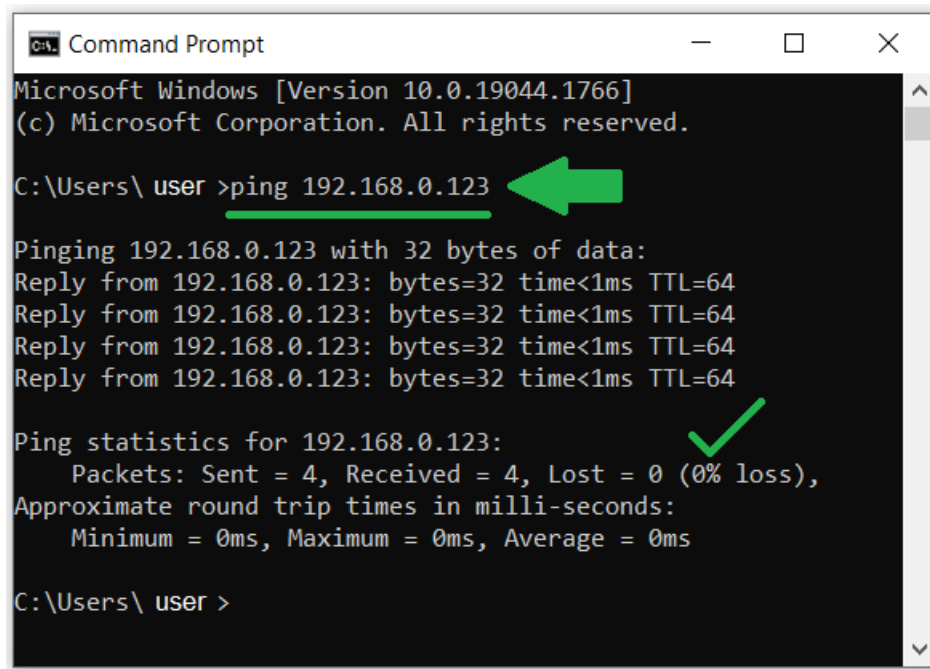


Figure 1.3 Enter “cmd” and press “Enter” and enter the “ping 192.168.0.123” command



```
Microsoft Windows [Version 10.0.19044.1766]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>ping 192.168.0.123

Pinging 192.168.0.123 with 32 bytes of data:
Reply from 192.168.0.123: bytes=32 time<1ms TTL=64
Reply from 192.168.0.123: bytes=32 time<1ms TTL=64
Reply from 192.168.0.123: bytes=32 time<1ms TTL=64
Reply from 192.168.0.123: bytes=32 time<1ms TTL=64

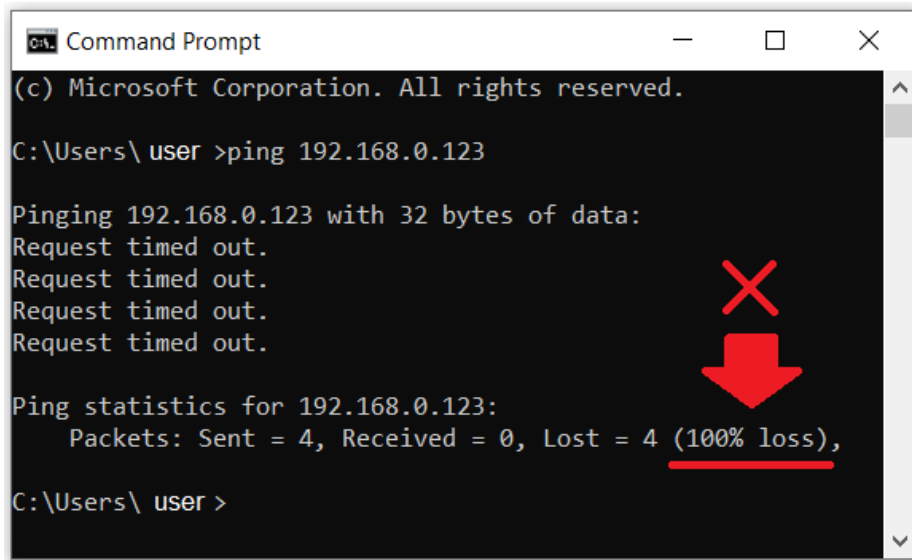
Ping statistics for 192.168.0.123:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\user>
```

A screenshot of a Windows Command Prompt window. The title bar says "Command Prompt". The text inside shows the command prompt version and copyright information. The user has entered the command `ping 192.168.0.123`. The output shows four successful replies from 192.168.0.123 with a time of less than 1ms and a TTL of 64. The ping statistics show 4 packets sent, 4 received, and 0 lost (0% loss). The round trip times are all 0ms. A green arrow points to the IP address in the command, and a green checkmark is next to the statistics.

Figure 1.4 Enter the “ping 192.168.0.123” (replace underlined with your IP address recorded in step 2.2.1) command and press “Enter” to connect the network

- c. Troubleshooting: When the network is unreachable you will see “100% loss” (figure 1.5), please recheck and correct the network connection and settings to ensure network connectivity. Please go back and complete steps 2.2.1



```
Microsoft Windows [Version 10.0.19044.1766]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>ping 192.168.0.123

Pinging 192.168.0.123 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.123:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\user>
```

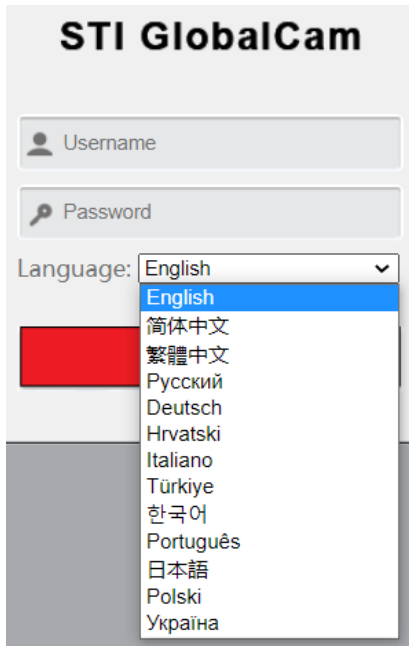
A screenshot of a Windows Command Prompt window. The title bar says "Command Prompt". The text inside shows the command prompt version and copyright information. The user has entered the command `ping 192.168.0.123`. The output shows four "Request timed out" messages. The ping statistics show 4 packets sent, 0 received, and 4 lost (100% loss). A red 'X' and a red arrow point to the "100% loss" text.

Figure 1.5 Enter the “ping” command and press “Enter”, the network is unreachable Please go back and complete steps 2.2.1 to ensure you have the correct IP address.

2.3 Web Interface - Camera first log in and control installation

*** After all parts of the device are connected and your computers ethernet adapter network settings are completed to match your camera's IP range. ***

- a. Go to your PC web browser and enter the IP address **recorded in step 2.2.1** in the address bar, press **'Enter'**. You will see the device web login interface.
- b. Choose **Language** from the drop-down. 12 languages:



- c. Type the default username and password (unless you have changed from the factory default).

Default username: **admin**

Default password: **123456**

- d. Then press **“login”**

NOTE: If the control of the same version has been installed on the PC, you will directly enter the login interface shown in figure 2.3.

NOTE: If you access the device through a browser for the first time, you may be prompted to install controls. If so, follow steps 2.3e-2.3i. If no prompt continues to Step 3.

During the control installation process, due to different versions of the IE kernel browser, different interfaces may appear. Users need to follow the prompts to install. Some anti-virus software will prompt that the security problem is caused by the security authentication of the control, but it will not cause any security risks. This kind of prompt can be ignored, click OK to complete the installation process.

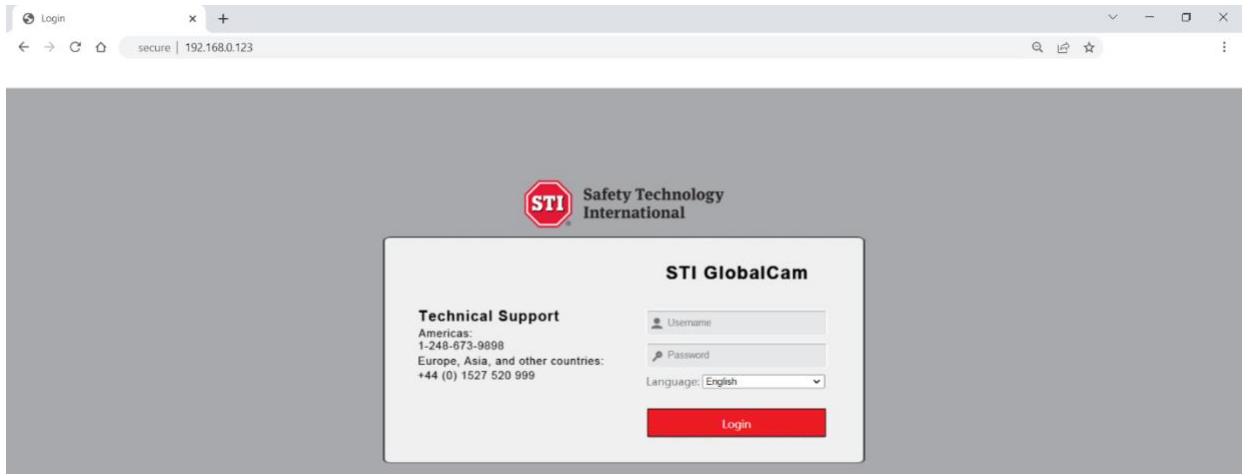

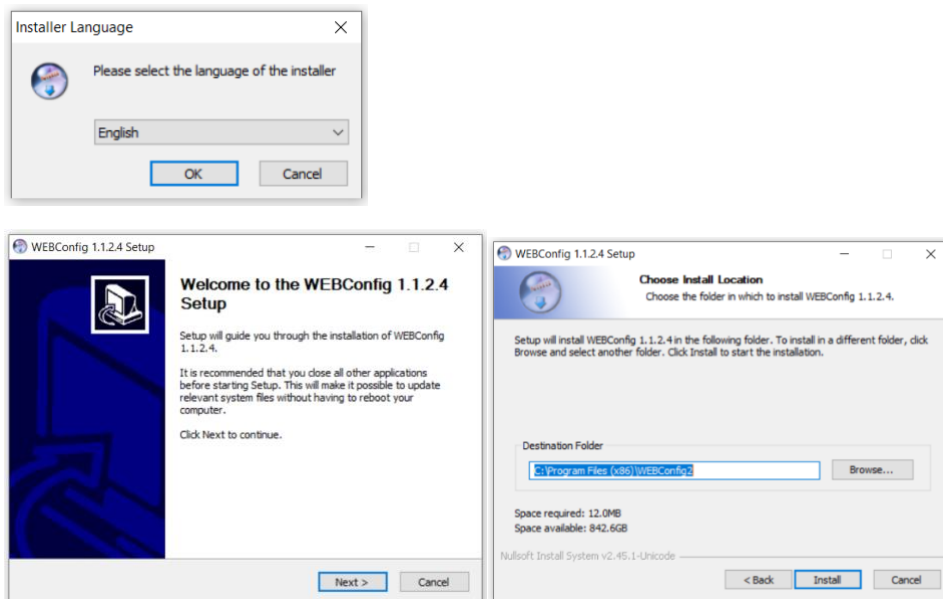


Figure 2.3 After installing the controls correctly, enter the device login interface

- e. Before installing the controls, you need to close all currently open browser interfaces, otherwise the installation may be unsuccessful. If multiple installations are unsuccessful, it is recommended to clear the browser's cache before reinstalling.
- f. After entering the IP address of the device, the interface shown in the figure below may appear. This is because the control is not authenticated. Click the "Allow" button.

 WEBConfig.exe	8/29/2022 10:48 AM	Application	3,847 KB
---	--------------------	-------------	----------

Then you will see message as below, select language then click “OK”.



- g. After clicking "OK", different interfaces may appear depending on the browser version. If the browser does not pop up this interface, look at the bottom of the browser, there will be a line of

text "Please install the control", click on the line of text, you can also link to the control installation interface.

- h. According to the prompts to correctly install the control, it is necessary to note that during the installation process, all open browsers on the computer must be closed, otherwise the control may not be installed successfully.
- i. After the installation is successful, reopen the browser, enter the camera device IP address in the browser address bar, and press "Enter" to go to the device login interface, as shown in the following Figure 2.4.



Figure 2.4 After installing the controls correctly, enter the device login interface

2.3.1 Alternative way to find and download "Webconfig.exe"

- a. Log in to IP camera following steps found in 2.4 then make selections found in figure 2.5
- b. Select configuration
- c. Select Information > Version
- d. Locate "Web Plug-in Version > "Download Web Plug-in"

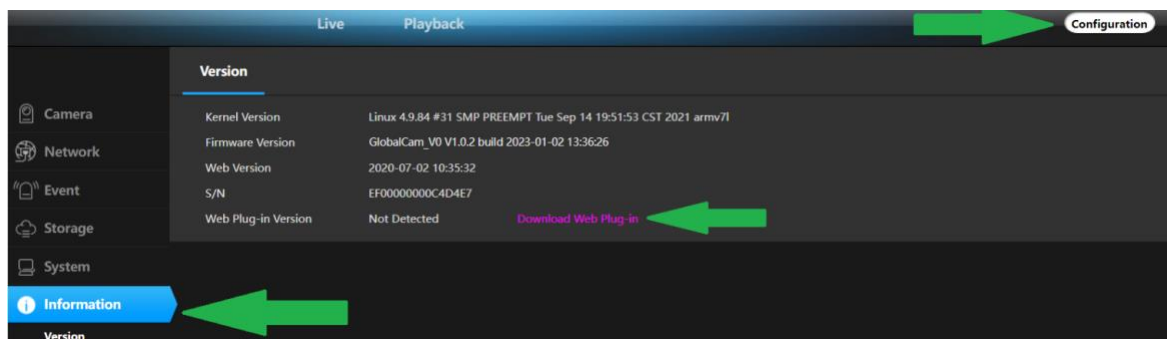


Figure 2.5 Download Web Plug-in

2.4 Resetting IPv4 to automatically obtain IP address

After all personalized IPC settings have been made. Converting your computer ethernet adapter settings back to “Obtain an IP address automatically” is necessary.

If you are not done making personalized IPC settings, please finish. Come back to this step when you are done.

IMPORTANT NOTE: after you are done modifying your camera settings you **MUST** reconfigure your computer ethernet adapter settings back to “automatic” to restore your computer's ability to connect to the internet via an ethernet cable. Follow steps 2.2.3a - 2.2.3f then make the selections shown in figure 2.4a then select ok.

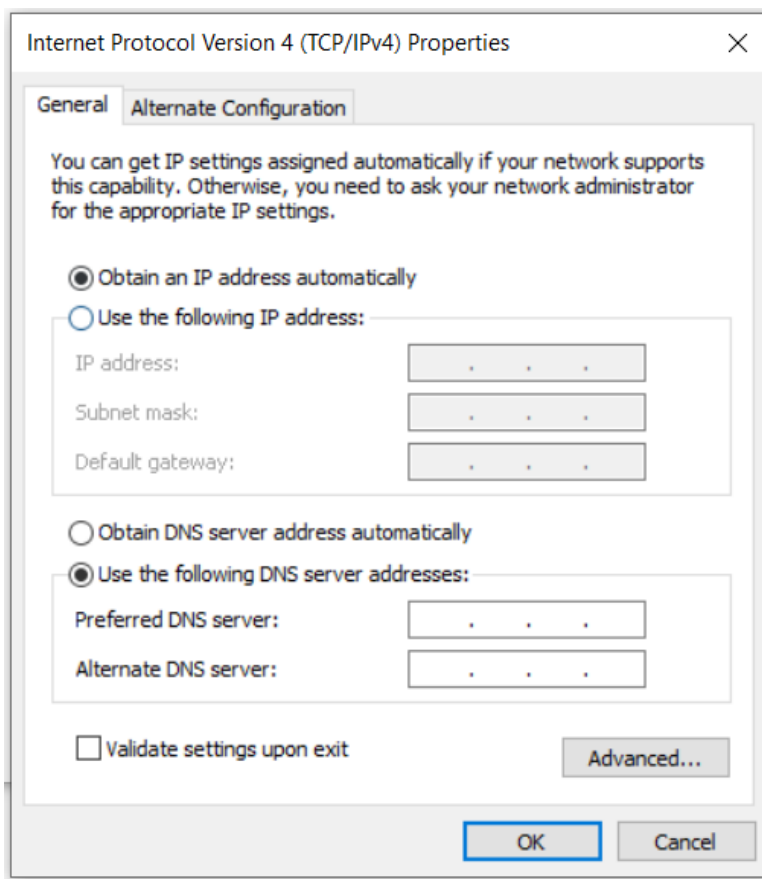


Figure 2.4a ethernet adapter IPV4 properties (typical default settings)

3 Web - Main dashboard layout

After entering the correct user's name and password in Figure 2.4, you will enter Figure 3.1, as follows:

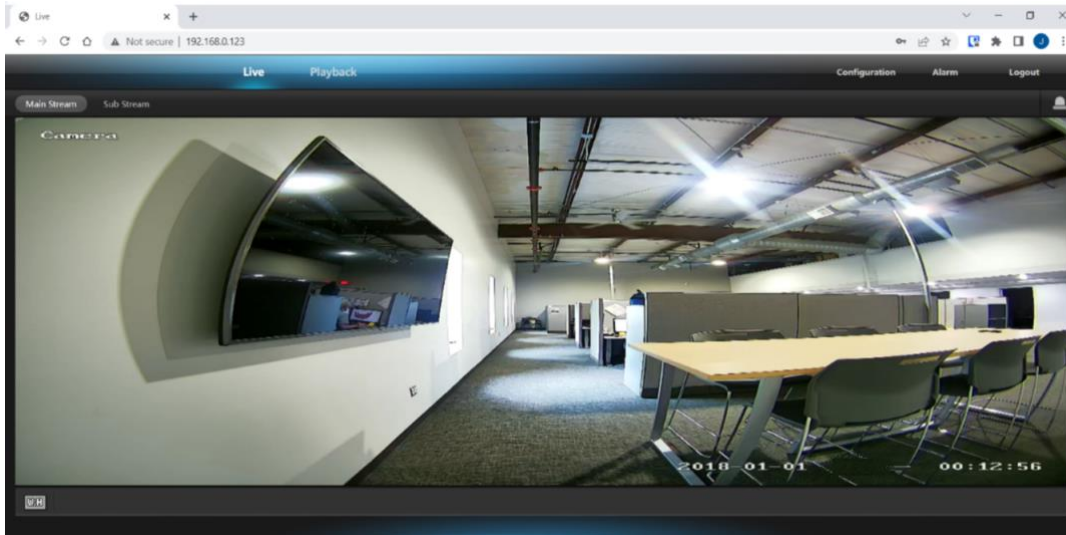


Figure 3.1 Main dashboard

The interface after the web login, it is composed of three parts:

A: Upper functional area: This part has five function buttons; Live, Playback, Configuration, Alarm, and Logout.

1. **Live** - is the current broadcast stream. It contains two categories.
 - a. **Main Stream** – Highest quality stream based on camera configuration. More internet bandwidth is needed for smooth playback.
 - b. **Sub Stream** – Lower quality stream uses less bandwidth. May be helpful if your internet speeds are low. ***if Sub Stream is used, do you still get 180° view?
2. **Playback** - The function of playback is to watch, download, and delete the previously stored video. After opening, it will enter Figure 3.2. Here we perform the operations of the functions provided by the playback.

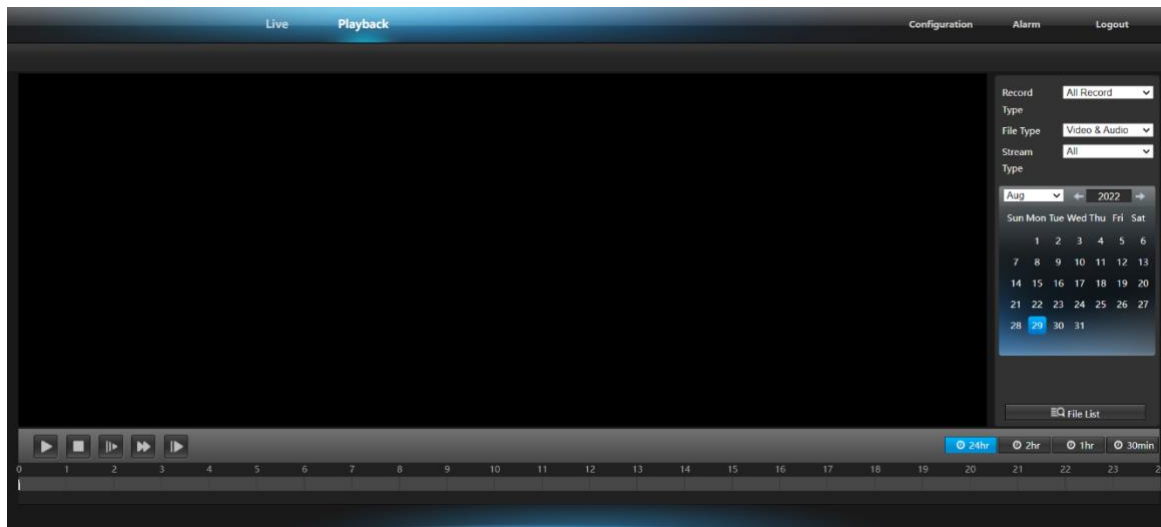


Figure 3.2 Playback

3. **Configuration** - The function of configuration is to perform network settings, media settings, storage settings, alarm settings and system settings. After opening, it will enter Figure 3.3, where we can configure various parameters of the device. Detailed parameter settings will be introduced in the next chapter.

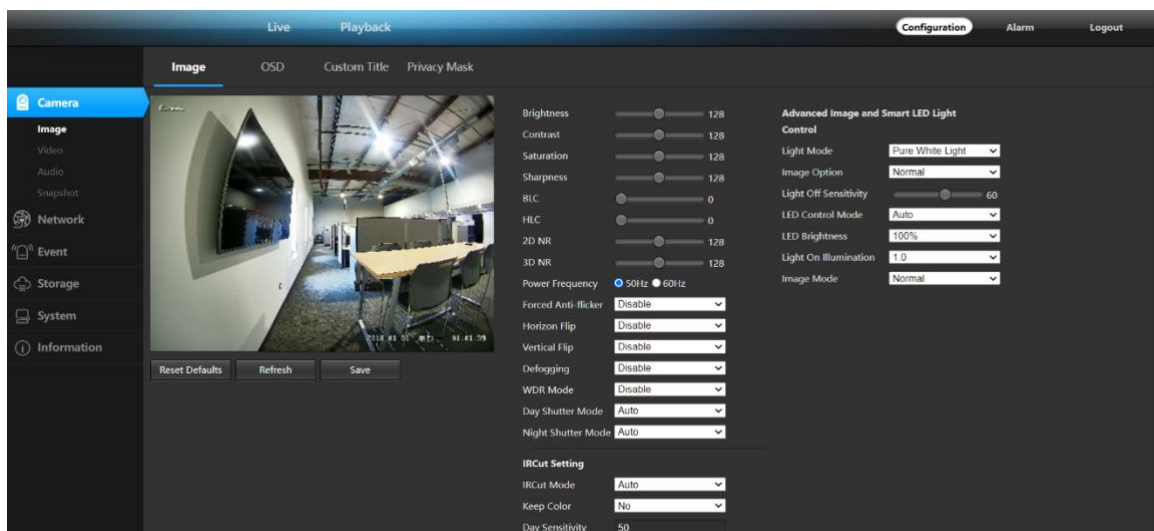
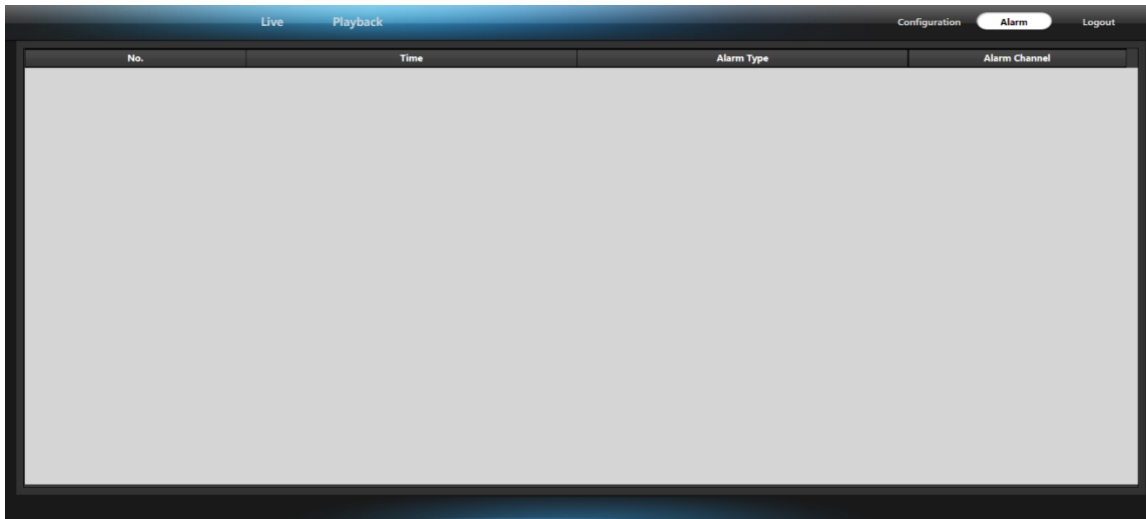


Figure 3.3 Configuration

4. **Alarm** - The alarm is used to display alarm information such as motion detection and humanoid detection.
 - a. Here we can configure various parameters of the device. Detailed parameter settings will be introduced in the next chapter.



5. **Logout** - The function of Logout is to exit the web side of the device and go back to IPC device login page Figure 2.4.

Stream setting: Set the video playback window to play the video main stream or the video sub stream.

C: Surveillance video playback window on the right: Play the real-time stream, you can choose to play the main video stream or the video sub-stream according to your needs. Double-click the playback window during playback to achieve full-screen display of the video.

Storage Path: Configure the storage path for snapshot pictures and videos. After setting, when a snapshot picture or video is generated, the system will automatically generate a folder of the current date in the set directory to save the picture or video file. It is worth noting that the set storage path is not saved after exiting.

Capture: Click the button to capture the current video screen.

Video: You can record by clicking the button. A red dot appears in the upper right corner of the right monitor video playback window to indicate that the device is recording. The storage file save path defaults to the folder created under the C drive with the current date as the file name, and the storage path can be modified by itself. It should be noted that when the remaining space of the disk where the set video file save path is located is less than 2G, recording will not be possible.

4 Camera settings

4.1 Video capture image settings

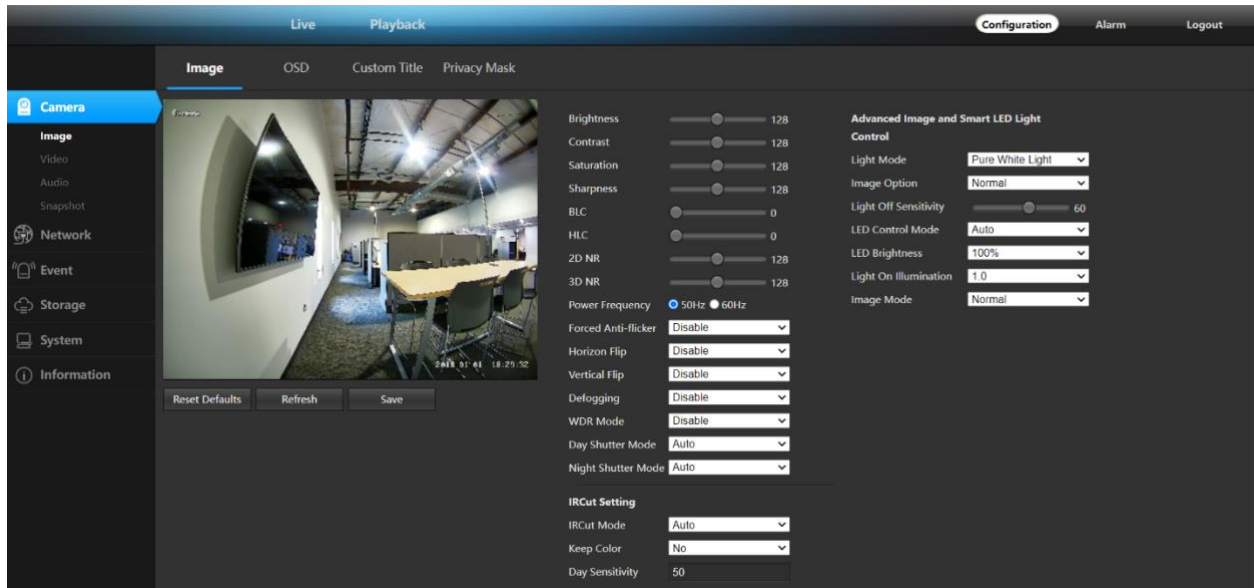


Figure 4.1 Video capture settings

- A set of default parameter settings is provided in the video capture parameter settings. Click the “Default Parameters” button at the bottom right of the interface, and all the parameters in the interface will be restored to the default values. If you think that the default parameters are not optimal, you can set the parameters according to your needs.
- The brightness, saturation, sharpness, contrast, and backlight values need to be chosen manually. The setting range is 0-255. *The settings of brightness, saturation, sharpness, contrast, and backlight value should be adjusted according to the actual environment of the site, not the larger the value, the better.*
 - **Brightness** - The larger the brightness value, the brighter the field of view.
 - **Contrast** – The Larger the contrast value, the image looks lively; conversely, if the contrast is low, the image looks flat and monotonous in the shadow areas.
 - **Saturation** - The larger the saturation value, the more obvious the color discrimination
 - **Sharpness** - The larger the sharpness value, the more saturated the image; the larger the contrast, the more obvious the contrast effect of the image.
 - **BLC** – Black Light compensation, is a setting that allows you to choose which areas of your scene should be properly exposed instead of letting the camera choose for you. More often than not, cameras like to automatically adjust exposure based on what it thinks is the primary scene.

- **HLC** – High light compensation, on the other end of the spectrum, is a setting that allows your camera to compensate for brighter parts of your image, maintaining detail in brighter parts of the image that would otherwise be blown out.
- **2D NR** – 2d noise reduction, work with low light security camera images that are amplified. Works best to clean up the foreground of an image. This can be noticed when you look at security camera footage of a streetlamp at night, for instance.
- **3D NR** – 3d noise reduction, decreases picture noise and reduces color mixture errors. 3D-DNR stands for multidimensional digital noise reduction, can cause motion blur if too high
- **Power Frequency** - 50Hz/60Hz set to your local region's power frequency.
- **Forced Anti-flicker** - (still image) Detects flickering/blinking from artificial light sources such as fluorescent lighting and times the shooting of images to moments when flickering will have less of an impact.
- **Horizon Flip** - enabling horizontal flipping, the video screen will be rotated 180 degrees horizontally
- **Vertical Flip** - vertical flipping enabled, and the video screen will be rotated 180 degrees vertically
- **Defogging** - After the defogging function is turned on, there is a similar effect of increasing the contrast to achieve the defogging function
- **WDR Mode** - WDR is a wide dynamic function, and WDR is the ratio of the brightest signal to the darkest signal that the device can distinguish.
- **Day Shutter Mode** - Auto recommended
- **Night Shutter Mode** - Auto recommended
- **IR CUT Setting**
 - IR Cut Mode - Auto is recommended
 - Keep Color - NO is recommended IRCUT will not switch and will result in poor performance in dark environments. Traditionally black and white is a better choice for low light application.
 - Day Sensitivity - 50 is recommended Change only if you wish for IR cut to switch earlier or later.

Video capture settings are divided into two parts "IRCUT settings" and "video capture parameter settings".

IRCUT has four working modes: active mode, day and night mode, passive mode, and manual mode.

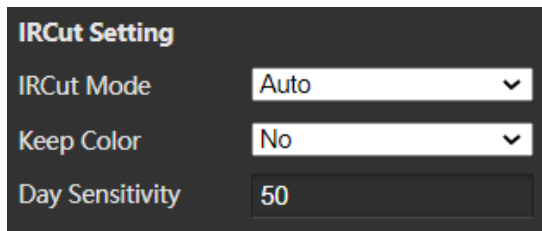


Figure 4.2

The active mode is controlled by the module to control the light board, and the color and black and white pictures are automatically switched by the light intensity; the day and night mode is set by the night start time and the night end time, and when enabled, the black and white picture is always maintained during the set time period. The set time is determined according to the device time, so the device is also based on the device time when switching the IRCUT; the passive mode is switched by the level control signal control module IRCUT sent by the light board; the manual mode can be manually switched Day and night mode; reverse passive mode is the same as passive mode, except that the high and low levels are exchanged, that is, when the video picture is colored in passive mode.

When you want the device to be in full color mode, you can turn on the "Keep Color" feature. "Keep color" select "Yes", regardless of the working mode set, regardless of the external conditions, the device is always in color mode, IRCUT will not switch. "Sensitivity" refers to the agility of the device's sensitivities and only works in "active mode".

4.2 OSD settings

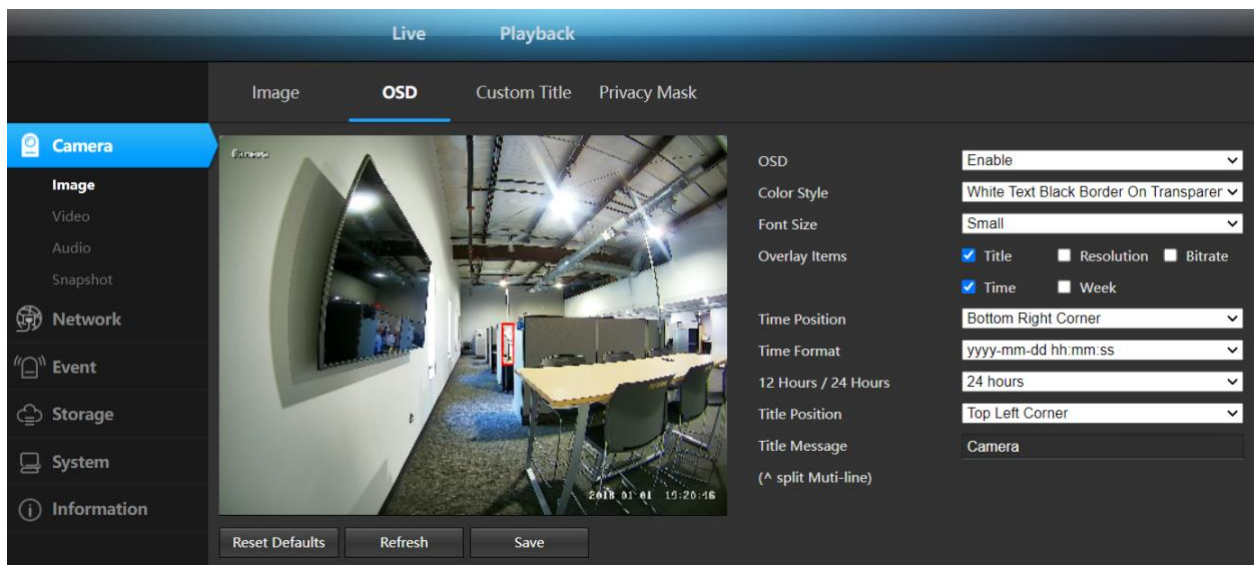
The time and title settings are a setting for setting the time and title display on the video interface. The user can define the title content, set the time and title display position, select the overlay information, and set the display format of the time.

When the OSD display is set to Enabled, time and title information will be displayed on the video screen; no information will be displayed when disabled.

Additional information is used to set whether to display resolution and bit rate. There are four options: no overlay, overlay resolution, overlay rate, overlay resolution, and bitrate. The user can set whether to superimpose the display resolution or code rate on the video screen according to his own needs.

The style display default transparent background black box white, users can choose one of 4 modes.

The time display has 8 formats to choose from.



4.3 Custom Title Settings

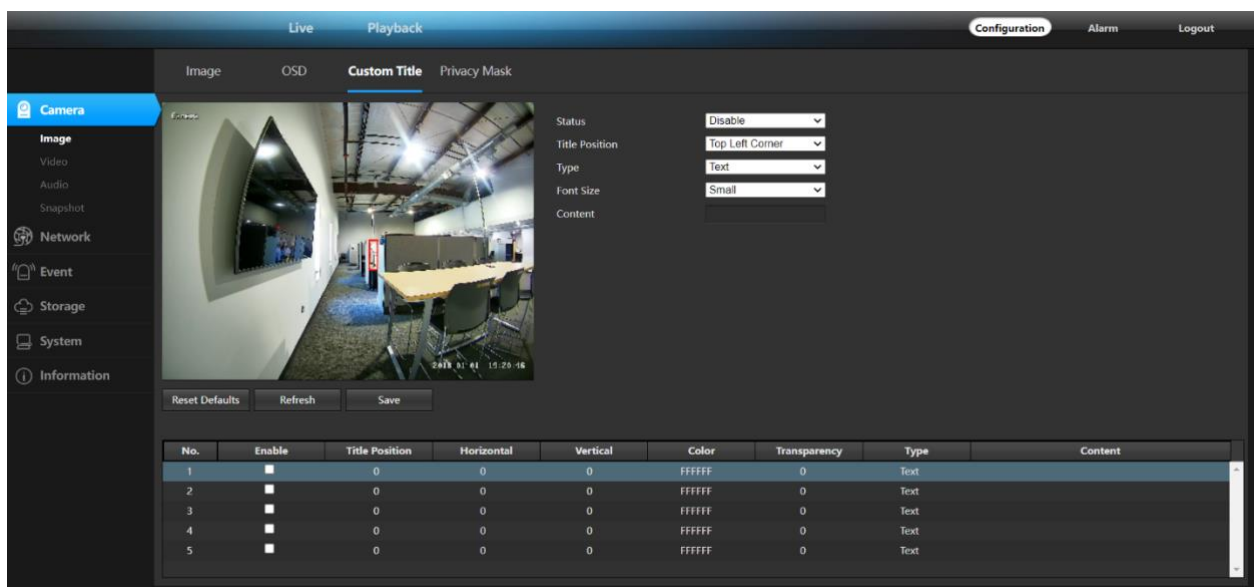


Figure 4.3

4.4 Privacy mask settings

When some parts of the video picture are desired to be hidden, these areas can be set as privacy occlusion areas. When configuring the privacy mask area, you can use the mouse frame in the image area and click OK to complete the setup. The place that is set as the privacy zone is displayed in black or white, whether it is in the live stream or in the video file.

If the set privacy mask needs to be modified or removed (Note: this will remove all of your current privacy masks), you can click the “Reset Defaults” button and click “Save”, the privacy mask area will be cleared.

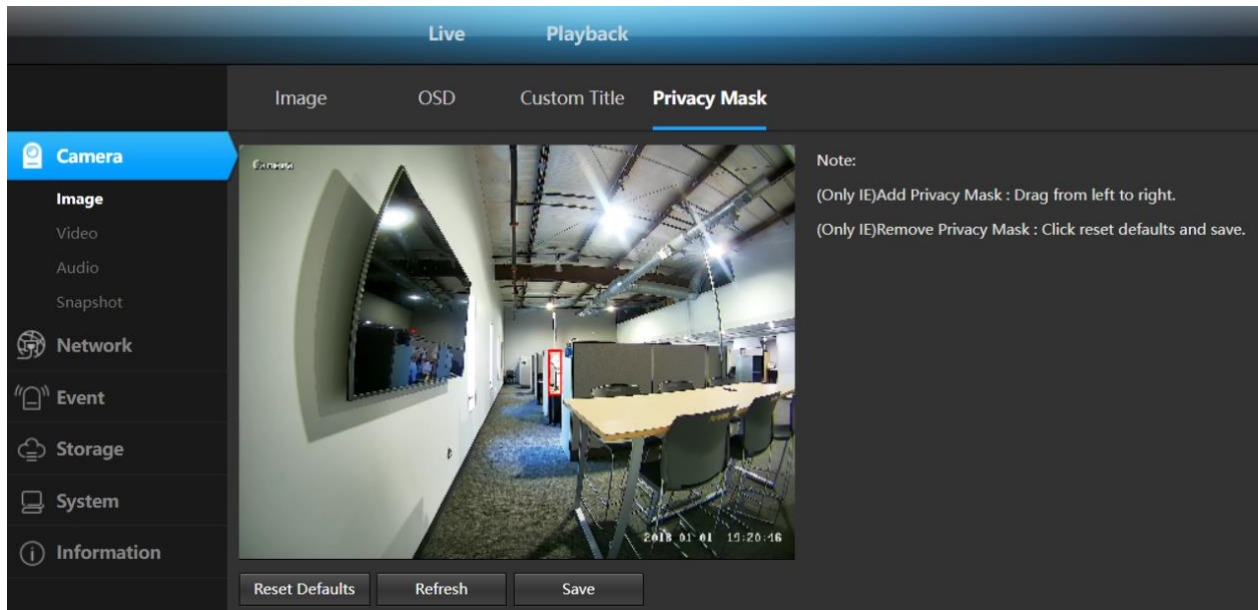


Figure 4.5

4.5 Video encoding settings

The video encoding setting area includes two parts: video encoding parameter setting (Figure 4.4) and advanced encoding parameter setting (Figure 4.5).

The video has two streams, one is the main stream and the other is the sub-stream, and the encoding format is H.265.

IPCAMERA main stream has three resolutions, namely 1080P, 960P, 720P and other resolutions (depending on the specific model), users can set according to their own needs. In order to achieve a trade-off between network bandwidth and Figure quality, a bit rate control method is adopted. When the amount of Figure information increases suddenly and the bandwidth is limited, dynamic bit rate (VBR) transmission can be adopted to ensure Figure quality. If the fixed bit rate (CBR) transmission is adopted, the Figure may appear mosaic, jitter and other phenomena. CVBR is a priority fixed rate transmission, compatible with variable rate control. When the network bandwidth is sufficient, the bit rate control has no obvious effect on the Figure quality, and the specific selection of the control method should be determined according to the client network.

A frame is a key identification frame for video coding. If the frame interval is too large when the network bandwidth is too small, the acquired image quality may be poor or even a real image may not be obtained. When the network conditions are good, there is no strict requirement for the frame interval setting. The specific settings can be gradually adjusted to the optimal value by the preview setting effect.

The bit rate Kbps refers to the network transmission speed, that is, how many thousands of bits of information are transmitted per second, compatible with multiple resolutions, because the resolution of

the primary stream is multiples of the sub-stream, and the amount of information transmitted per unit time. Large, so a relatively large transfer rate is required. The main code stream generally requires not less than 500 kbps, and the sub-stream requirement is not less than 50 kbps. The transmission rate is too small, and the image will appear sticky, slow update, and poor interaction.

The larger the frame rate, the smoother and more realistic the picture. When the frame rate is low, the image update is slow, and the interaction is poor. Generally, the frame rate is set to 20 frames or more per second to obtain an image with a strong sense of interaction and realism.

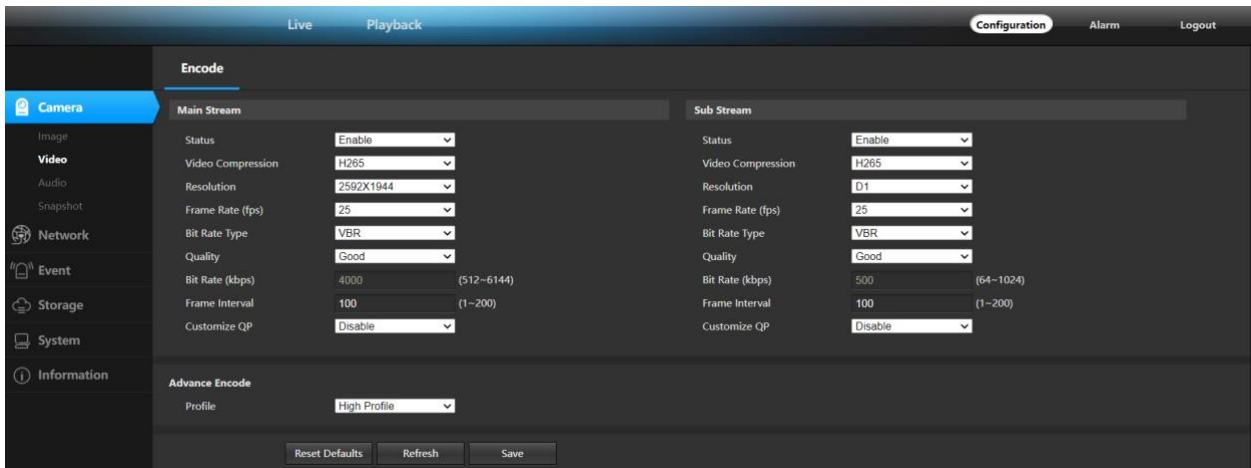


Figure 4.4

5 Network

5.1.1 Dynamic (DHCP) enables automatic IP address assignment

DHCP is a LAN network protocol that enables automatic assignment of IP addresses to devices. When there is a DHCP server (usually a router) in the LAN and the DHCP function is enabled, and the device also enables the "DHCP function", an IP address can be automatically obtained according to the DHCP settings of the DHCP server.

5.1.2 Basic configuration – Static IP address you choose

Basic configuration is to set the network parameters of the device, and the set network parameters will be displayed in Network Settings accordingly. The setting of each parameter will be explained in detail below.

The IP address is the address used when accessing the device. You can use the matching AjDevTools search tool to search and modify the IP address of the device. Make sure that the IP address of the computer and the IP address of the camera device are on the same network segment, and there is no IP conflict between the IP addresses in the LAN, so that the device can be accessed correctly. After the IP address is modified and saved, the system will restart, and then the changed IP address will be used to access the device. An illegal IP address could not be saved, and an error was indicated.

The subnet mask is combined with the IP address to divide the network address and host address, usually 255.255.255.0. The correct subnet mask can be saved, the wrong illegal subnet mask cannot be saved, and an error is indicated.

A gateway is a level between two networks (between the internal network and the public network, or between different network segments of the internal network). A general gateway is a router. Set the gateway address and fill in the IP address of the router. When setting up the gateway, the IP address and gateway address must be on the same network segment.

The DNS server address is the host address where the domain name service program is running. The DNS server address is provided by the local network operator. When you do not know the DNS, you can use the Internet to query. When the DNS server address is incorrectly filled, the device cannot connect to the public network, but it does not affect the LAN.

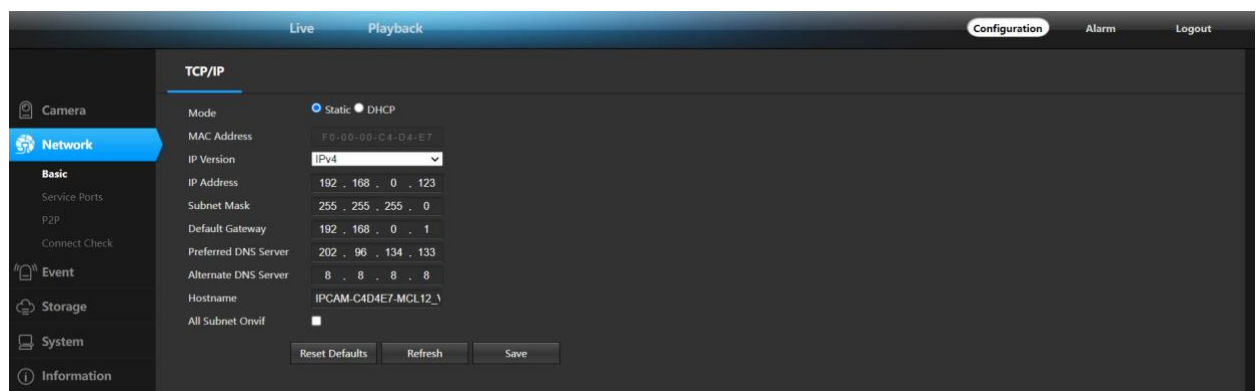


Figure 5.1

5.2 P2P settings

The P2P setting is used to support the external network access of the mobile client. After this function is enabled, if the device is connected to the Internet, you can log in to the device anywhere. This greatly facilitates the user's management and use of the device and is no longer limited by time and location. The feature is off by default as shown below.

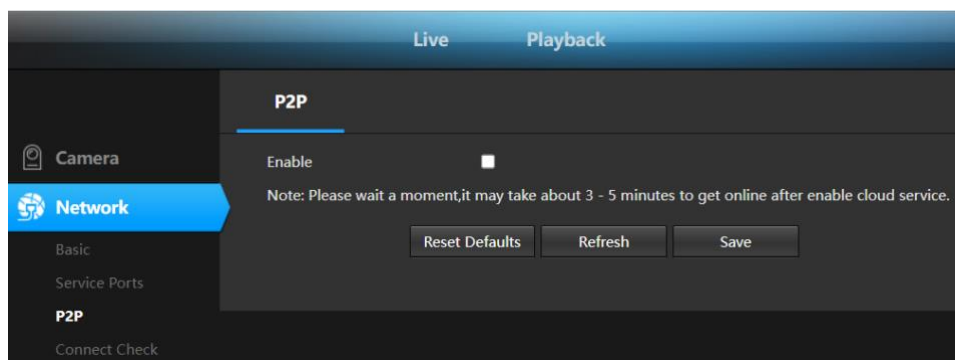


Figure 5.2

5.3 Stream media

The streaming settings are shown in Figure 5.3.

ONVIF: When enabled, devices that support the onvif protocol, such as platform software or NVR, can search and add devices. After authentication is enabled, a password is required to log in.

Control Protocol: This protocol is the transmission protocol for changing various settings of the camera, and the device cannot be controlled after it is turned off.

RTSP: When enabled, third-party software (such as VLC) accesses the device and needs to enter a username and password, when disabled, the device can be accessed directly without authentication.

HIK: When enabled, the platform software or NVR and other devices that support the HIK protocol can be used to search and add devices. After enabling authentication, a password is required to log in.

Note: The media access port, PTZ control port, and web access port need to meet the following conditions when setting: 1. The three cannot be the same; 2. Common ports (such as 3000) cannot be used; 3. When the set port number is not the default port, it must be both greater than 1000 and less than 65536.

The screenshot shows a web management interface with a sidebar on the left and a main configuration area on the right. The sidebar includes icons and labels for 'Camera', 'Network' (highlighted in blue), 'Basic', 'Service Ports', 'P2P', 'Connect Check', 'Event', 'Storage', 'System', and 'Information'. The main area is titled 'Service Ports' and has two tabs: 'Live' and 'Playback'. The configuration is organized into sections: WEB/ONVIF, Control Protocol, RTSP, and HIK. Each section contains checkboxes for enabling features and input fields for port numbers, with range restrictions shown in parentheses. At the bottom, there are three buttons: 'Reset Defaults', 'Refresh', and 'Save'.

Section	Setting	Value	Range
WEB/ONVIF	WEB Enable	<input checked="" type="checkbox"/>	
	Onvif Enable	<input checked="" type="checkbox"/>	
	Onvif Authentication	<input type="checkbox"/>	
	HTTP/Onvif Port	80	(80,1~65535)
Control Protocol	Enable	<input checked="" type="checkbox"/>	
	Port	8091	(8091,1~65535)
RTSP	Authentication	<input checked="" type="checkbox"/>	
	Port	554	(554,1~65535)
HIK	Enable	<input checked="" type="checkbox"/>	
	Authentication	<input type="checkbox"/>	
	Port	8000	(8000,1~65535)

Figure 5.3

6 Event settings

6.1 Motion detection / Alarm settings

NOTE: You cannot use this feature if you wish to use Intelligent Detect feature found in section 6.3

The relevant parameters of motion detection alarm settings are shown in Figure 6.1:

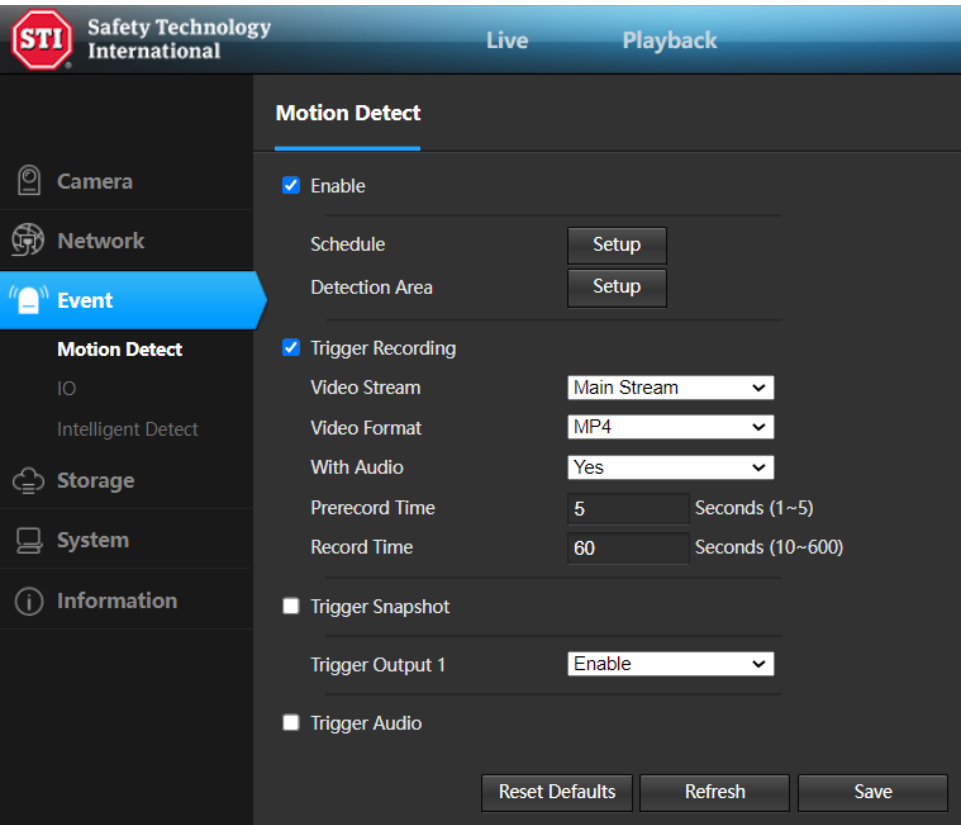


Figure 6.1 Motion detection settings

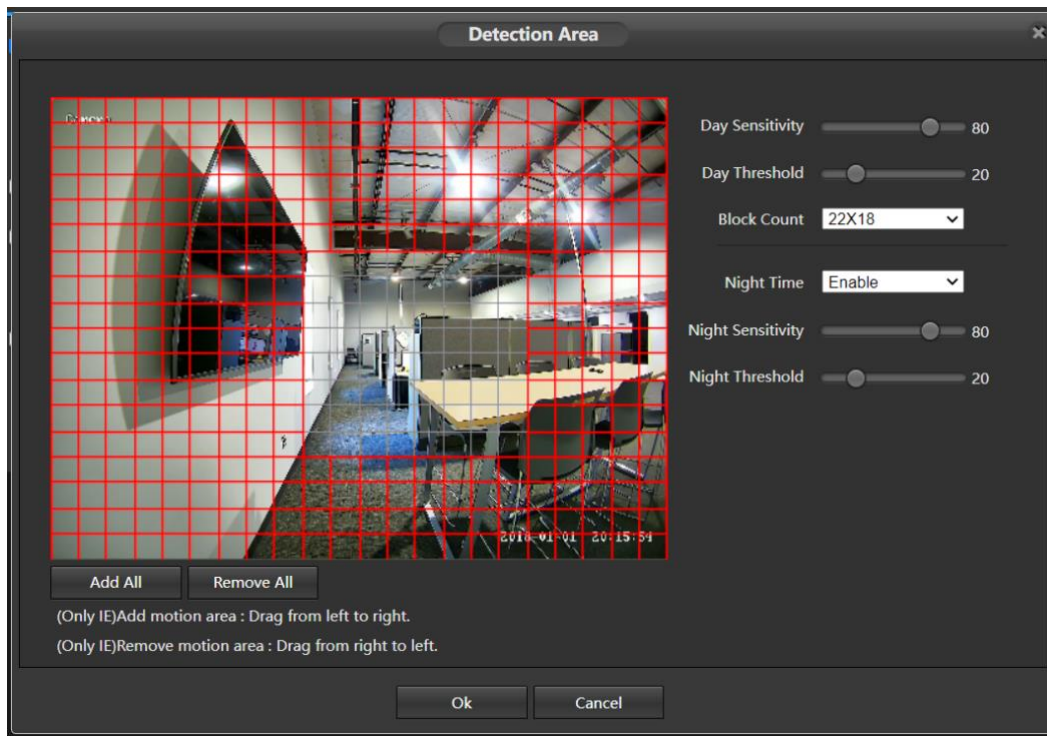


Figure 6.2 Detection Area

Motion detection event enable button: When "Enable" is selected, other parameters can be set, otherwise all parameters cannot be modified.

Sensitivity: For the sensitivity of video range changes, the greater the sensitivity value, the easier it is to generate an alarm.

Alarm threshold: Whether the alarm is measured when the video range changes. The smaller the threshold, the easier it is to generate an alarm.

Number of areas: Select how to divide the video range area, the divided video, the motion detection generated by the area contained in the red box will cause an alarm, and the motion detection generated by the area not included in the box will not cause Alarm.

Enable nighttime parameters: When the device is monitoring, it may require different degrees of motion detection for the same degree of day and night, which can be achieved by enabling nighttime parameters. After the nighttime parameter is enabled, the nighttime parameter will be used during the set nighttime period. If the nighttime period conflicts with the standard time period, the nighttime parameter will still prevail.

- **Night start time** - The start time that night parameters take effect.
- **Night end time** - The end time that the night parameter takes effect.
- **Night sensitivity** - Sensitivity during the nighttime parameter period.
- **Night alarm threshold** - the alarm threshold in the night parameter time period.

After setting the relevant parameters of motion detection, it is also necessary to set the time period for the motion detection to generate an alarm. This function is realized by the motion detection and foot defense time period, as shown in the lower part of Figure 7.3.

Use the mouse frame to select the time range for time deployment. If you need to select the entire day, click the Select All button.

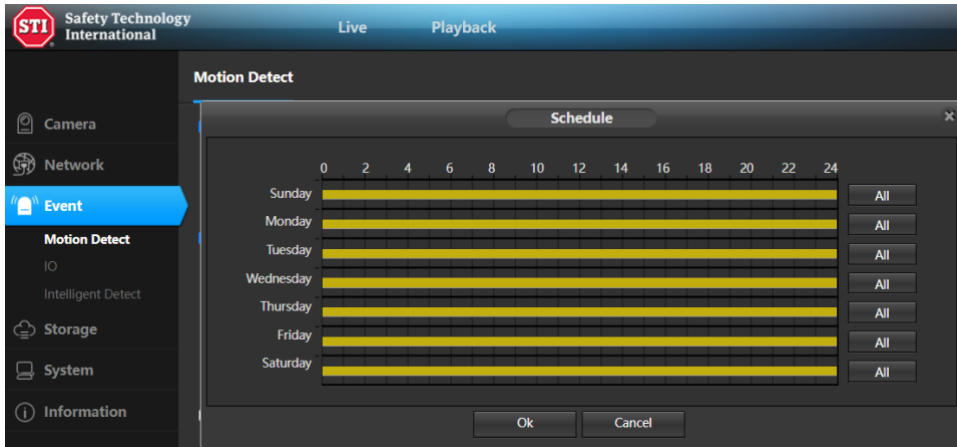


Figure 7.3

The motion detection alarm recording settings are shown in Figure 7.4.

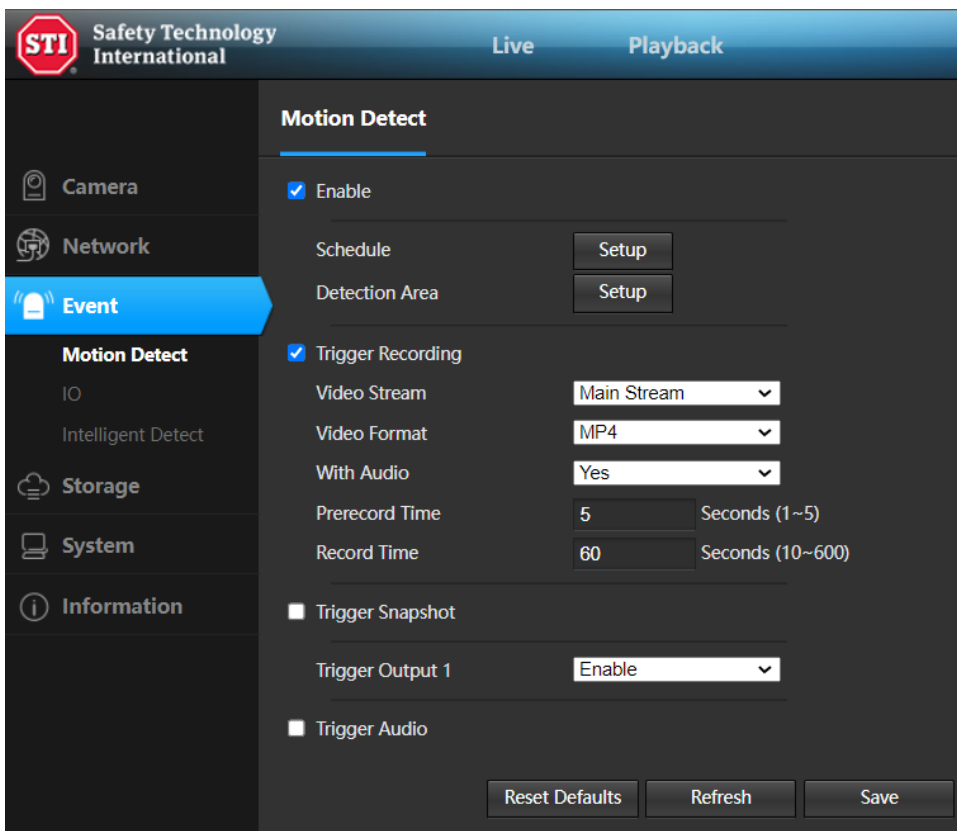


Figure 6.4

When the motion detection alarm recording function is enabled, when the device generates a motion detection alarm, the corresponding video file is generated according to the configuration.

Motion detection alarm recording enable button: When "Enable" is selected, other parameters can be set, otherwise the parameters cannot be modified.

Video source: You can select the video main stream or sub-stream. After selecting the video source, the device will record according to the resolution of the main stream or sub-stream set in [Video Encoding Settings].

Media type: When the device has audio function, the media type can be “Audio and Video” or “Video Only”. When the device does not have audio function, the media type has only one choice, “Video Only”. Select "Video and Audio" and if the device is properly connected to the audio device, the resulting video file will have sound.

Pre-recording duration: The system supports the pre-recording function. When there is no official recording, the data is saved in the temporary buffer. The pre-recorded data is extracted during the official recording. The maximum pre-recording duration of the system is 5 seconds.

Recording duration: The recording time of the video file is 10 to 600 seconds (about 10 minutes). The length of the recorded video file is the set recording duration.

Upload to FTP: When the FTP-related parameters are properly configured and the upload to FTP function is enabled, the generated video file will be sent to the corresponding location on the server.

Send to Email: When the Email related parameters are configured correctly, the Send to Email function is enabled, and the generated video file will be sent to the configured mailbox by email. [65]

The motion detection alarm capture settings are shown in Figure 6.5.

The screenshot shows the 'Motion Detect' configuration window. The left sidebar includes 'Camera', 'Network', 'Event' (highlighted), 'Motion Detect', 'IO', 'Storage', 'System', and 'Information'. The 'Motion Detect' section is active, showing options to 'Enable' motion detection. Below this, there are 'Schedule' and 'Detection Area' buttons. The 'Trigger Recording' section is expanded, showing settings for Video Stream (Main Stream), Video Format (MP4), With Audio (Yes), Prerecord Time (5 seconds), and Record Time (60 seconds). The 'Trigger Snapshot' section is also expanded, showing Presnapshot Time (5 seconds) and Snapshot Time (10 seconds). The 'Trigger Output 1' is set to 'Enable', and 'Trigger Audio' is unchecked. At the bottom, there are 'Reset Defaults', 'Refresh', and 'Save' buttons.

Figure 6.5

When the movement is generated, if the storage space is limited or the video screen that generates the alarm is not required to be recorded, but the reason for generating the alarm needs to be checked, the user can select the motion detection alarm capture function. When the motion detection alarm capture function is enabled, when the device generates a motion detection alarm, it generates a corresponding snapshot image according to the configuration.

- **Motion detection alarm capture enable button** - When "Enable" is selected, other parameters can be set, otherwise all parameters cannot be modified.
- **Photo Duration** - The time to generate an alarm photo, usually 1 second.
- **Upload to FTP** - When the FTP related parameters are correctly configured, and the upload to FTP function is enabled, the generated snapshot will be sent to the corresponding location on the server.
- **Send to Email** - When the SMTP/Email related parameters are configured correctly, the Send to Email function is enabled, and the generated snapshot image will be sent to the configured mailbox by email.
- **Sending frequency** - The time it takes to send a snapshot.

6.2 IO Events

There is a 5 Pin Wire Harness required to use the IO Event functions. IO events will allow you to control devices that accept use of relay inputs and or outputs.

5 PIN – Wire Harness Colors

IO IN
IO Ground
Normally Closed Relay
Common Relay
Normally Open Relay

- a. **IO Event Schedule** – Each day can have a unique schedule that is customizable to 1-hour increments.
 - a. Select the All box on the right includes the entire day for your schedule.
 - b. To make custom time changes click and drag in the area of time that you want to use. Example is shown on Sunday below.
- b. **Enable** – Turns on the function and allows you to begin choosing how your system needs to operate.
 - a. Trigger Type
 - i. Normal Open
 - ii. Normal Closed

b. Trigger Output 1

- i. Enable
- ii. Disable

c. Trigger Recording

a. Video Stream

- i. Main Stream – Highest quality settings
- ii. Sub Stream – Lower quality settings

b. Video Format

- i. AVI
- ii. MP4

c. With Audio – Note this option is not included on the standard product please contact STI if you need

- i. Yes
- ii. No

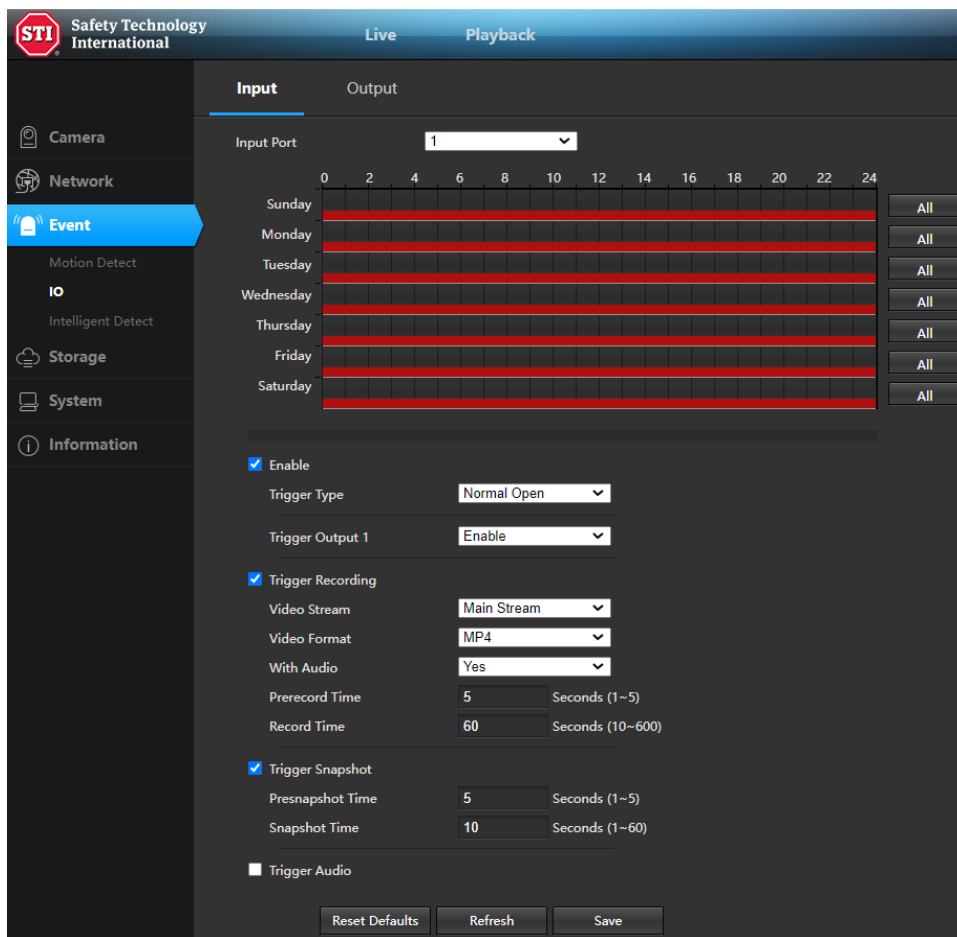
d. Prerecord Time – Choose from 1-5 seconds

e. Record Time – Choose 10-600 seconds

d. Trigger Snapshot

a. Pre-Snapshot Time – Choose 1-5 seconds

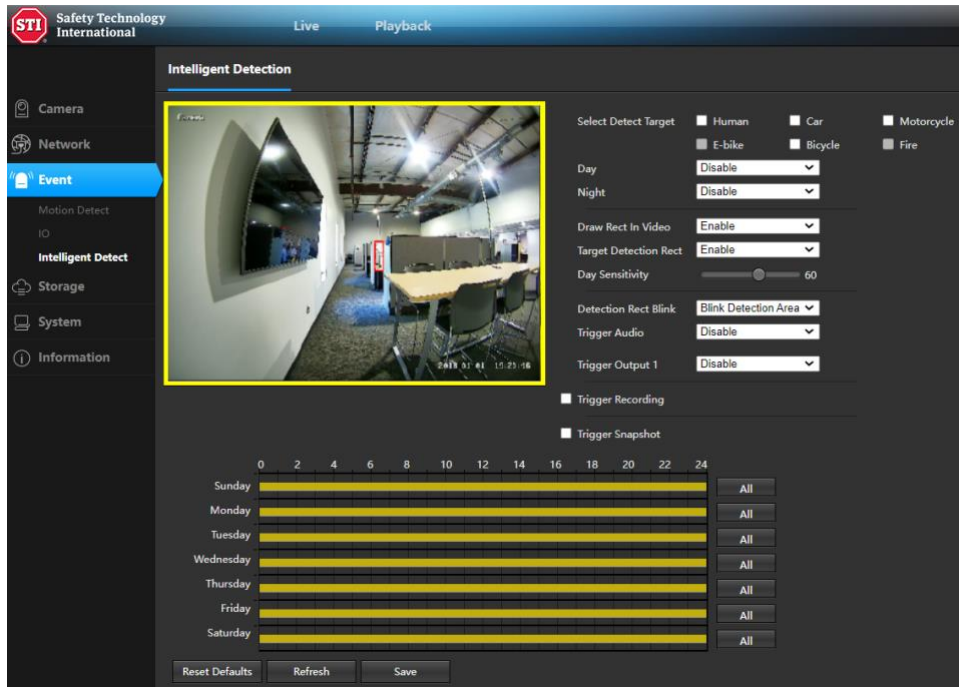
b. Snapshot Time – Choose 10-60 seconds



6.3 Intelligent detect

NOTE: To use this feature, you must disable Motion detection found in section 7.1

Intelligent detect will allow you to use AI to look for specific types of objects limited to: human, car, motorcycle, ebike, bicycle, and fire.



Intelligent detection event enable button: When "Enable" is selected, other parameters can be set, otherwise all parameters cannot be modified.

- a. Select detect target type.
- b. Day / Night enable or disable depending on your needs
- c. Draw Rect in video: This will draw a rectangle around an object the camera believes it sees depending on the chosen detect target.
- d. Target detection rect: This will draw a rectangle around an object the camera believes it sees depending on the chosen detected target.
- e. Detection rect blink: This will make the rectangle blink to draw extra attention to detect target.
- f. Trigger Audio: is disabled and will not function without a speaker.
- g. Trigger Output 1: Will send a signal to the relay contact connections described in section 7.2.
- h. Trigger recording: Will record based on set up recording method (micro SD card slot available).
- i. Trigger snapshot: Will take a snapshot based on set up recording method (micro SD card slot available).
- j. Set schedule: click and drag to set schedule based on environment requirements.

7 Storage settings

7.1 Storage settings

The storage settings have three parts of settings, storage settings, motion detection alarm recording, motion detection alarm capture, and timing recording, as shown in Figure 7.1.

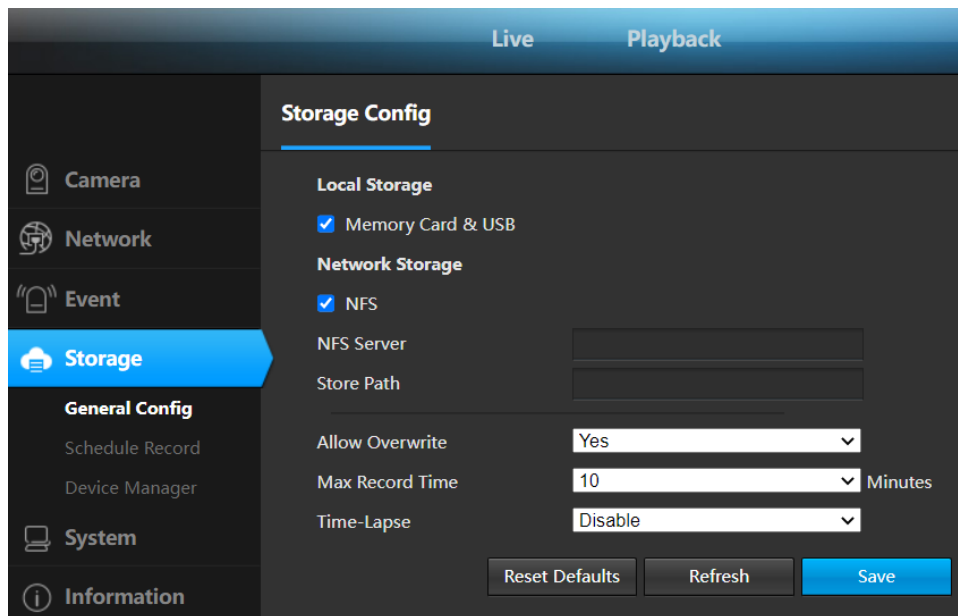


Figure7.1

The following is a detailed introduction to the configuration of these four parts.

The basic settings of the storage settings are shown in Figure 7.2.

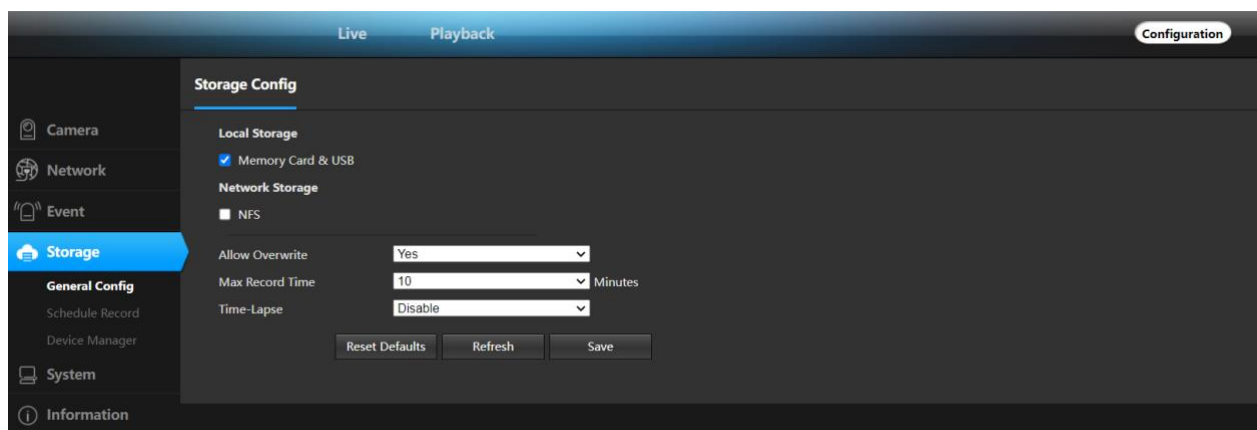


Figure 7.2

Local storage: Local storage (USB/memory card) must be enabled to enable storage of video files and snapshots. Otherwise, storage cannot be implemented.

Storage policy: The storage policy at this location refers to the way the storage device handles when there is insufficient space. Stop recording means that when the storage device is full, the recording will be stopped automatically; overwriting the old record means that when the storage device is full, the system will automatically delete the oldest day's video file, and so on.

Maximum recording duration: refers to the fixed time of each recording file when the device is configured for timed recording. The system provides 5 video file durations to choose from: 2 minutes / 5 minutes / 10

minutes / 20 minutes / 30 minutes. Limiting the length of a single video file can effectively prevent the problem that the playback of a single file is too slow or even impossible to play.

Time-lapse photography: Video compression will be performed after opening, compressing a long video in a short period of time and storing it as a video.

7.2 Timed recording

The settings are shown in Figure 7.3

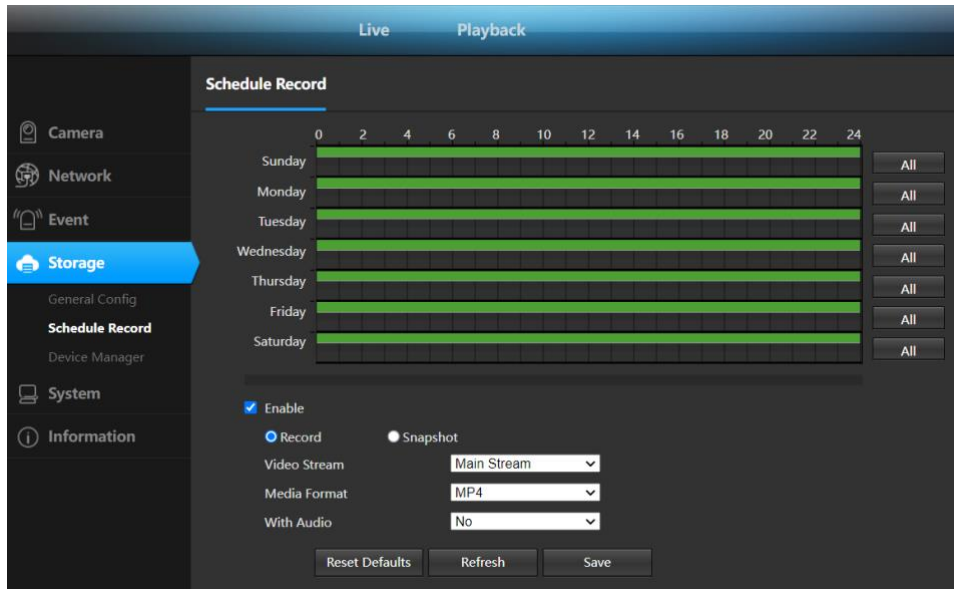


Figure 7.3

Motion detection alarm recording (capture capture) and IO alarm recording (capture capture) are triggered by corresponding alarms, collectively referred to as alarm recording. In addition, the device also supports another form of recording (capture), without conditional triggering, after activation. During the set time, the device will record according to the configuration (take a snapshot), which we call timing recording (capture).

It should be noted that during the same period of time, the timer recording, and alarm recording cannot be enabled at the same time.

Timing Record Enable Button: When “Enable” is selected, other parameters can be set, otherwise the parameters cannot be modified.

Video source: You can select the video main stream, sub-stream or picture capture. When the main stream or sub-stream is selected, the video file is obtained. When the picture is captured, the picture is captured.

Video format: According to the selected video source, if it is a video, the video format is AVI; if it is a snapshot, the video format is JPG.

Recording type: According to the selected video source, if it is recording, the recording type is “Video Only” and “Video and Audio”. If it is a snapshot, the recording type is “Snap Picture”.

Capture frequency: This option can be set only when the video source selects “Snap Picture”. Used to set the frequency of the snapshot, that is, how many seconds to capture.

Upload to FTP: This option can be set only when the video source selects “Snap Picture”. When the FTP-related parameters are properly configured and the upload to FTP function is enabled, the generated snapshot image will be sent to the corresponding location on the server.

Send to Email: This option can be set only when the video source selects “Snap Picture”. When the Email related parameter is correctly configured and the Send to Email function is enabled, the generated captured image will be sent to the configured mailbox in the form of an email.

Time period setting: used to set the time period of the timed recording (capture). The time period is determined by the date, start time and end time. After setting the time, click the “Select All” button to directly select 24 time slots. After the timer recording is turned on, the device will record (take a snapshot) according to the settings during the set time period.

Note: 1. The front-end recording and capture function is a front-end independent function and does not require network transmission. Therefore, as long as the capture or recording function is enabled and properly configured, the device will record or capture according to the configuration when the device is powered on.

2. When the device is not connected to the storage device, no front-end video files can be generated.

3. When the device is not connected to the storage device, the image capture function is enabled, and upload FTP is enabled, and the FTP parameters are correctly configured, and the snapshot image can be generated normally and can be found in the server.

7.3 Storage device information

Click [Storage setting information] to enter the storage device information display interface. The interface displays the device status, total capacity, used space, remaining space, and usage percentage of the storage device in detail. As shown in Figure 7.4.

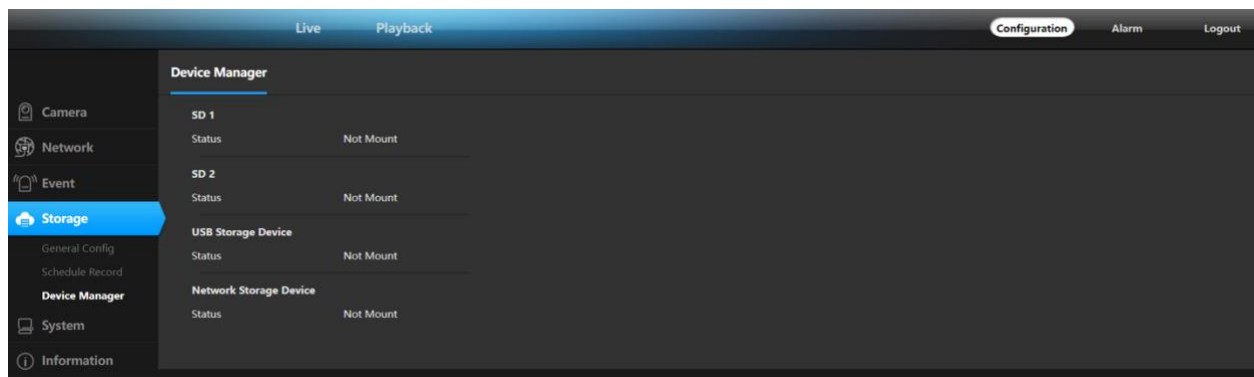


Figure 7.4

7.4 Storage device management

As shown in Figure 7.5, the management of storage devices mainly involves unmounting and formatting storage devices from the device. Uninstalling a storage device is an operation to safely remove a storage device from the IPC, which can prevent damage to the storage device or damage to the stored data caused by hot swapping of the storage device. After selecting the storage device that needs to be uninstalled, click "Uninstall" button, click OK to start uninstalling the storage device. Once a storage device is safely unmounted, the storage device will cease to be used. Click Cancel to interrupt the uninstall operation.

When a device is connected to a storage device, but the display keeps showing that it is not mounted, it may be because the formats of the device and the storage device are different. You can format the storage device first. Select the storage device to be formatted, click Format, the system pops up a warning dialog box as shown in Figure 7.7. Click OK, the device starts to format the storage device. After the storage device is formatted, all the data in it will be lost, so if there is data in the storage device that needs to be saved, it is recommended to transfer it to other places first. After the format is successful, the device will mount normally.

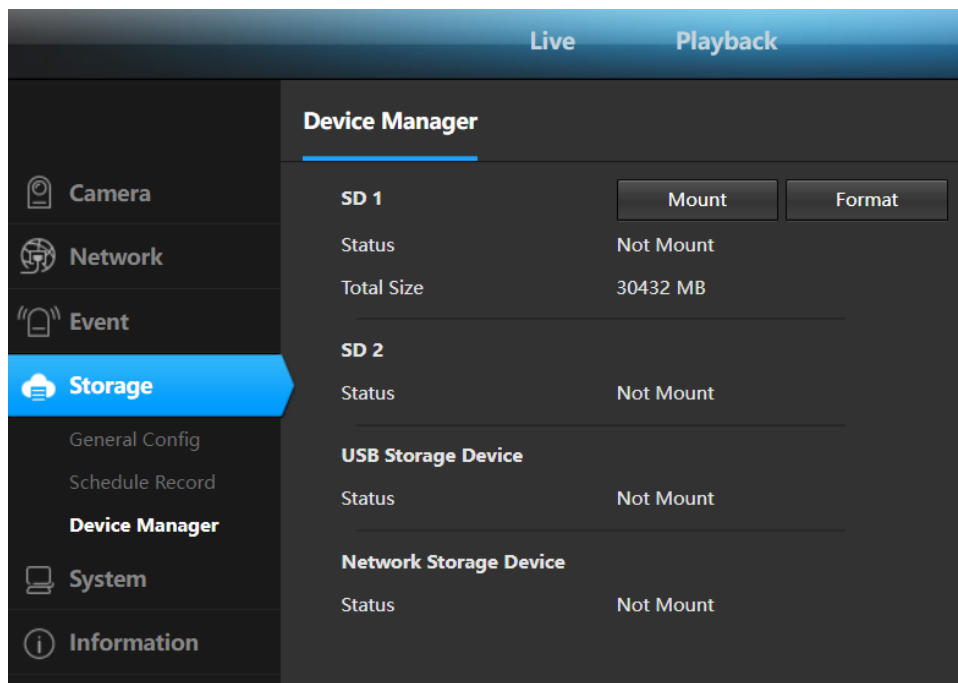


Figure 7.5



Figure 7.6

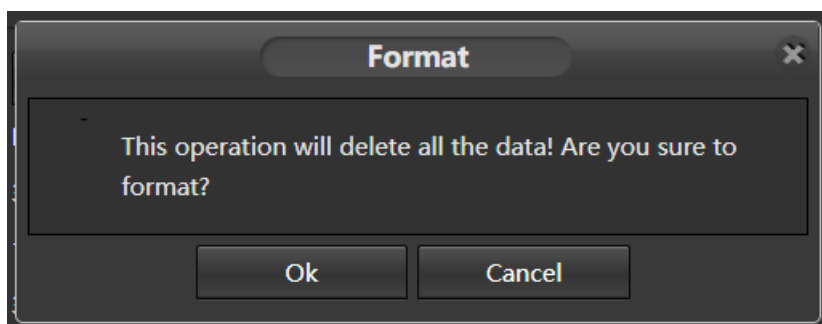


Figure 7.7

8 System settings

8.1 Account management

In order to facilitate the management of the device, the super user (the default is admin) is allowed to add, delete, modify user information and assign different user rights to different users.

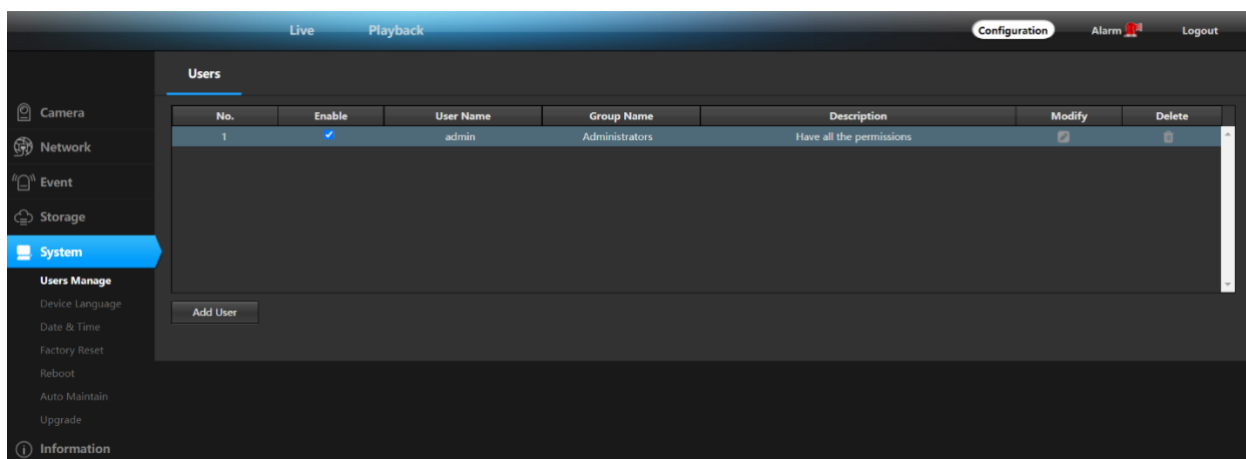


Figure 8.1

Click the option in front of "Add User", enter the user account, user password, and confirm password of the new user correctly, select the user group and enable information of the new user, and click the "Save" button to successfully add a user. As shown in Figure 8.2.

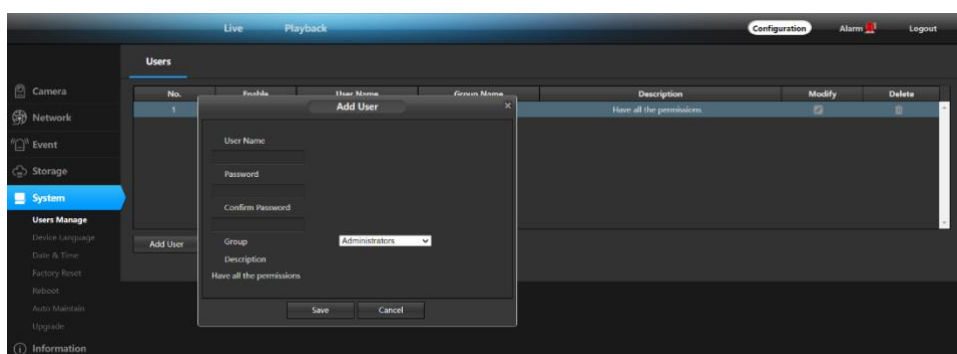


Figure 8.2

When adding a user, it is required that the user account and user password cannot be empty, and the user password and confirmation password must be the same. The user group is used to limit the user's authority: the administrator's authority is not restricted and can perform any operation on the device; the operator only has the operation authority and cannot view the device information; the viewer can only view the device information and cannot modify the device configuration. Whether to enable or not is used to set the validity of the user. When enabled, the added user is activated. After logging out, the newly added username and password can be used to log in to the device; when disabled, the added username and password cannot log in normally. After the information is added correctly, click the "Save" button, and the user is added successfully.

When you need to modify a user's information, click the button behind "Modify User". When modifying a user, you cannot modify the user's username, and other information can be modified. As shown in Figure 8.3.

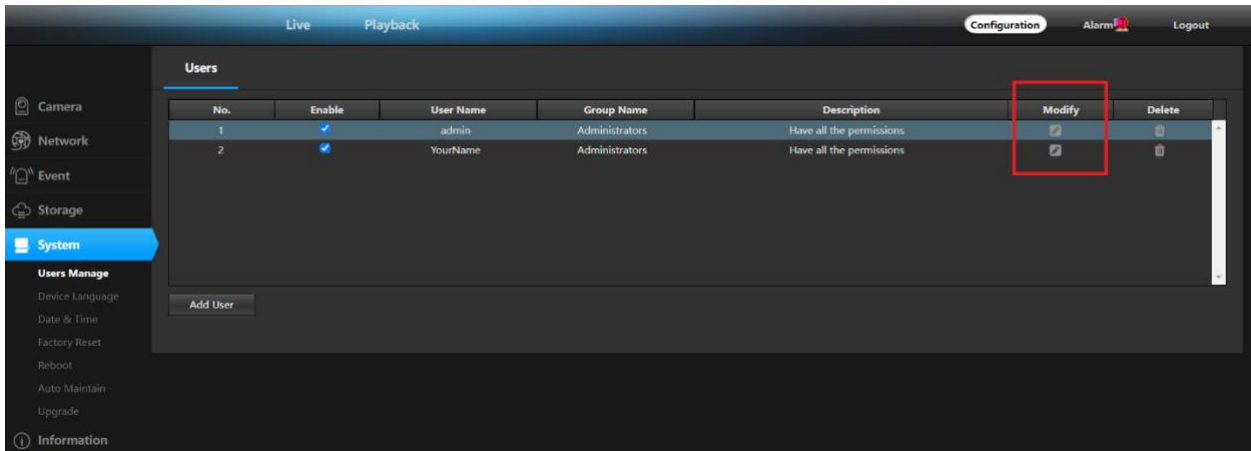


Figure 8.3

Click the user to be modified in the user list, and the user information will be displayed below. User accounts are grayed out and cannot be modified. You can modify the user's password, user group information and whether to enable or not. After modification, click the "Save" button, and the user information is modified successfully.

When a user is no longer used, click the button in front of "Delete User" to delete the user. When deleting a user, it should be noted that the currently logged-in user cannot be deleted the own account cannot be deleted. As shown in Figure 8.4.

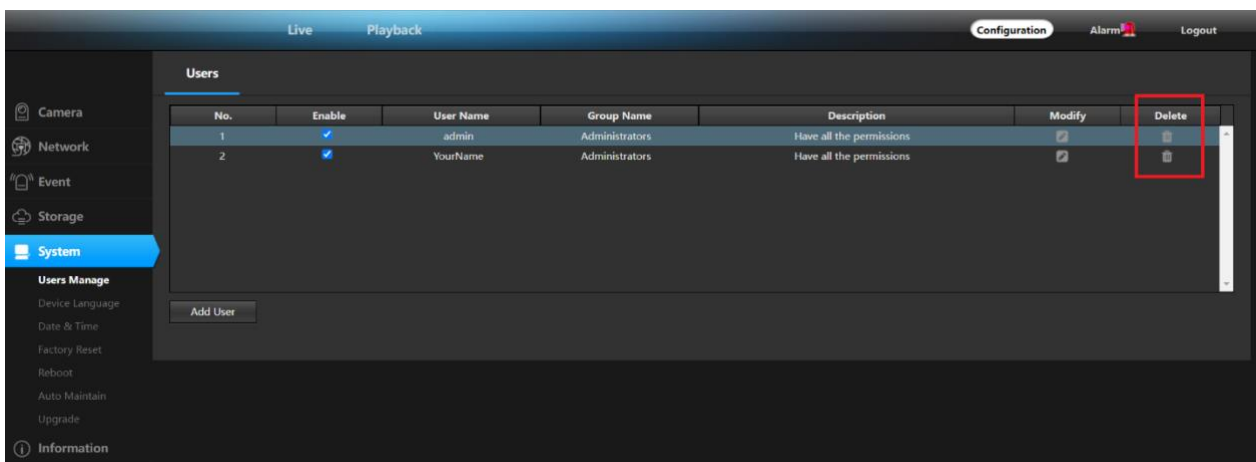


Figure 8.4

Click on the user you want to delete in the user list, and the user information will be displayed below. Click the "Save" button, the user will be deleted, the deleted user will disappear in the user list, and then the user account and user password will not be able to log in to the device.

8.2 Device language

IPCAMERA now supports three languages: Simplified/Traditional Chinese, English and Czech. After selecting the language, click the "Save" button, the setting is successful, and then the system

automatically jumps to the login interface. After the language version is set, when you access the device again, the login interface displayed is the interface of the set language.

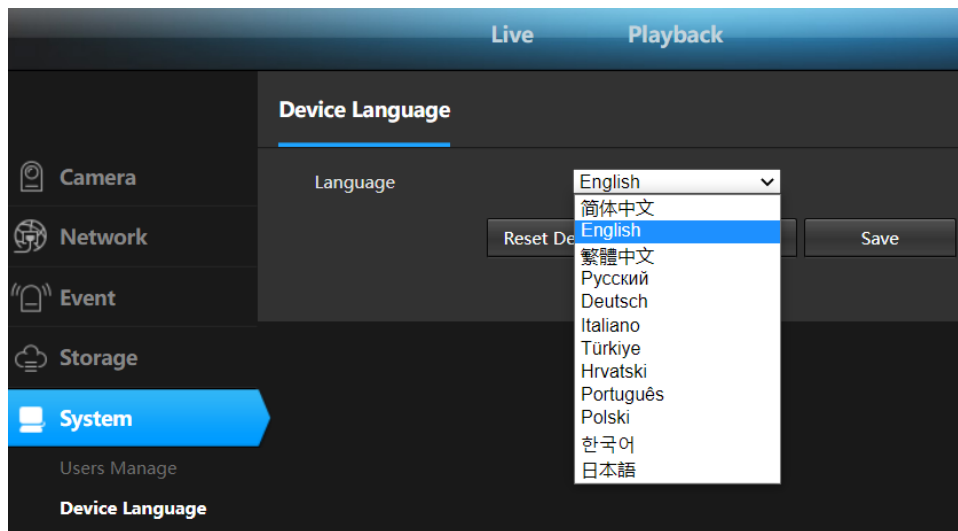


Figure 8.5

8.3 Timer settings

The system provides three clock setting modes: using NTP service, manual setting and P2P.

The NTP service is a protocol used to synchronize device time, which allows the device to synchronize its server or clock source, providing highly accurate time correction. After you select Use NTP Service, set the time zone where the device is located, the IP address of the NTP server, and the NTP service port. After the refresh interval is set and saved, the device can synchronize the time. It should be noted that since the device uses network synchronization, implementing this function requires the device to connect to the Internet.

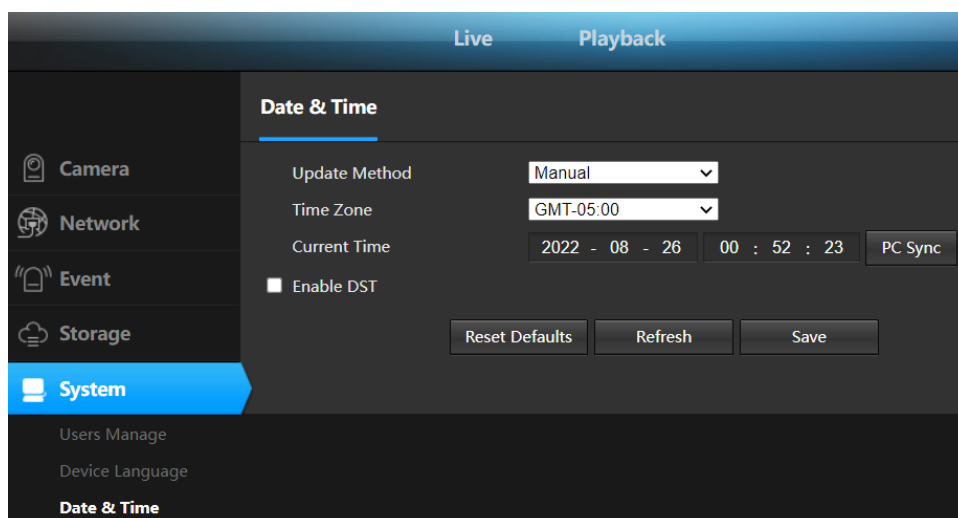
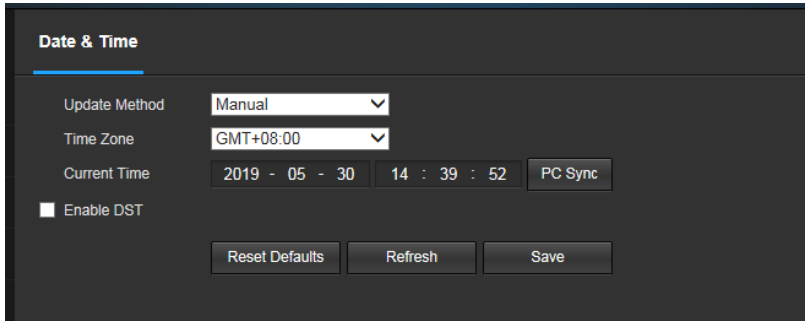


Figure 8.6

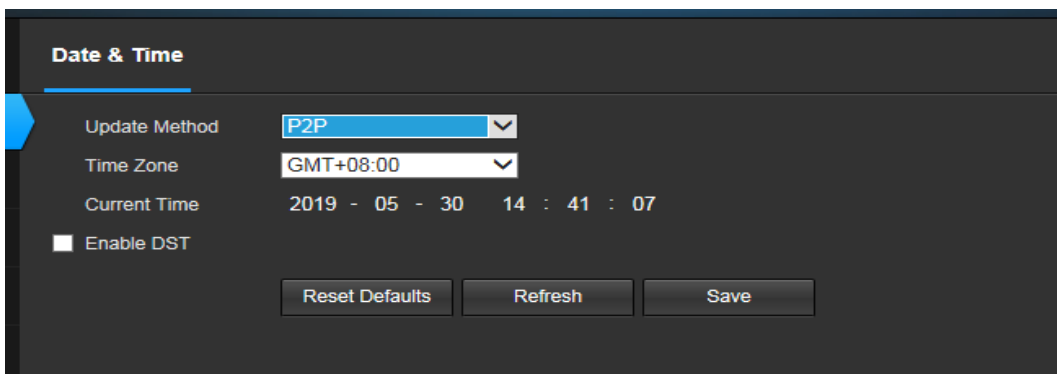
Manually setting the time refers to setting the year, month, day, hour, minute, and second. After saving, the time displayed by the device is the time entered manually. In the manual time setting, the function of automatically synchronizing to the current PC time is provided. Check the box in front of "PC Sync" and save the device time to synchronize the computer time.



The screenshot shows the 'Date & Time' configuration window. The 'Update Method' is set to 'Manual'. The 'Time Zone' is 'GMT+08:00'. The 'Current Time' is displayed as '2019 - 05 - 30 14 : 39 : 52'. There is a 'PC Sync' button next to the time display. The 'Enable DST' checkbox is unchecked. At the bottom, there are 'Reset Defaults', 'Refresh', and 'Save' buttons.

Figure 8.7

The P2P setting time refers to the time when the remote access device is synchronized. If the mobile client is used to access the device, the time of the mobile terminal is synchronized.



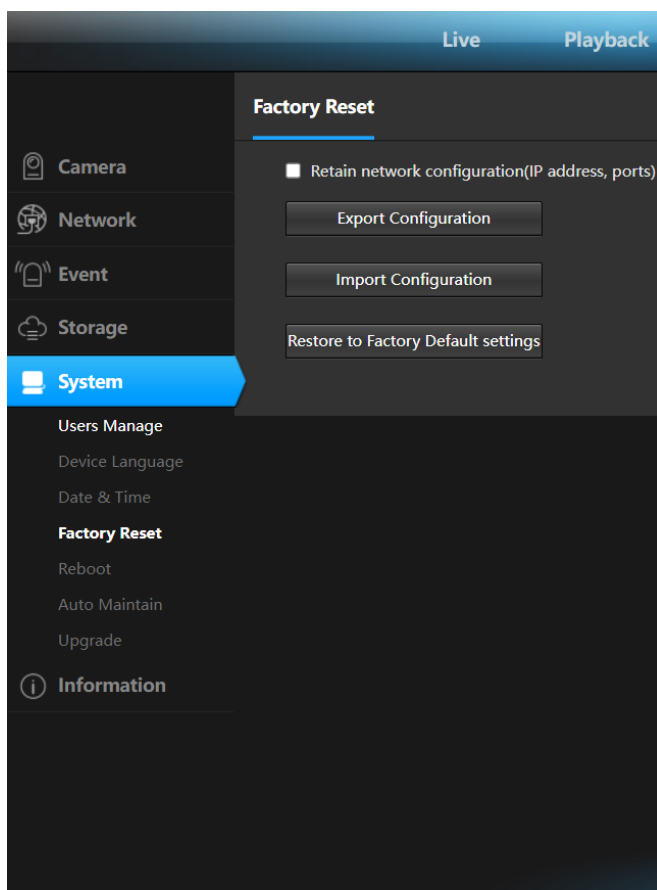
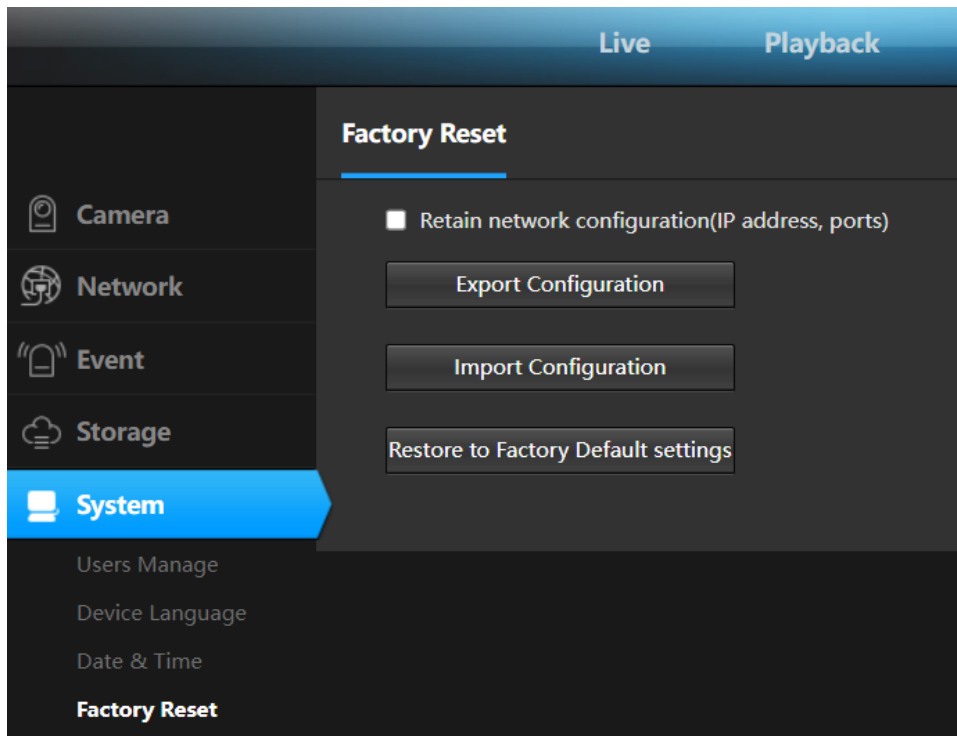
The screenshot shows the 'Date & Time' configuration window. The 'Update Method' is set to 'P2P'. The 'Time Zone' is 'GMT+08:00'. The 'Current Time' is displayed as '2019 - 05 - 30 14 : 41 : 07'. The 'Enable DST' checkbox is unchecked. At the bottom, there are 'Reset Defaults', 'Refresh', and 'Save' buttons.

Figure 8.8

8.4 Restore factory

Recommended to export your current configuration before a factory reset is started. This will create a file that you can later import if needed (NOTE you will need to do this on a personal computer via the web portal instructions to access this are found in section 2)

The system recovery interface is shown in Figure 8.9. After the device is restored to the factory default configuration, the current configuration information such as IP address, video parameters, etc. will be restored to the factory default values, and will not be restored, so you need to be careful when using this function. consider. After clicking "Restore Factory Defaults", a prompt window will pop up to confirm again, as shown in Figure 8.10. System restart will make the device suspend all current processes. After the restart is successful, it will jump to the device login interface.



config.xml ^ 

8.4 Export configurations – After you have the camera working how you like be sure to save its settings.

8.5 Import configurations - Helpful to quickly import settings based on your environmental requirements.

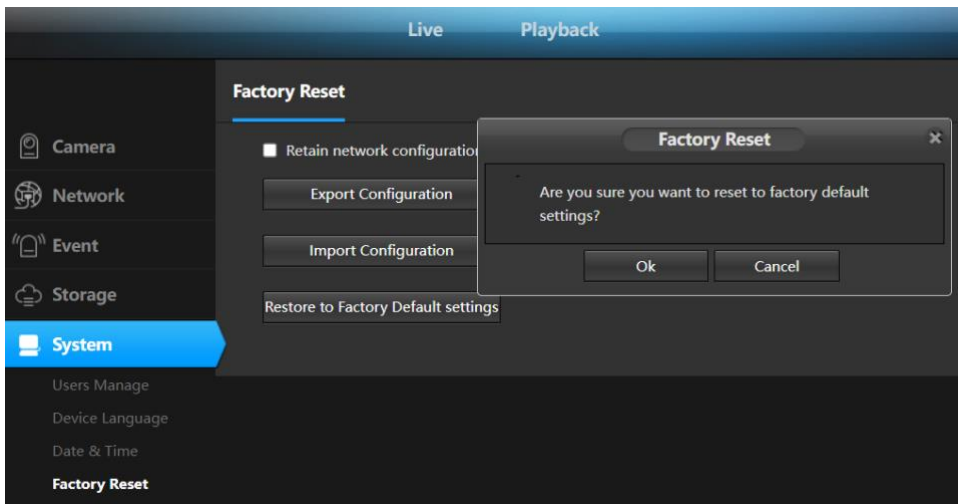


Figure 8.9

8.5 Reboot the device

System restart will make the device suspend all current processes. After the restart is successful, it will jump to the device login interface.

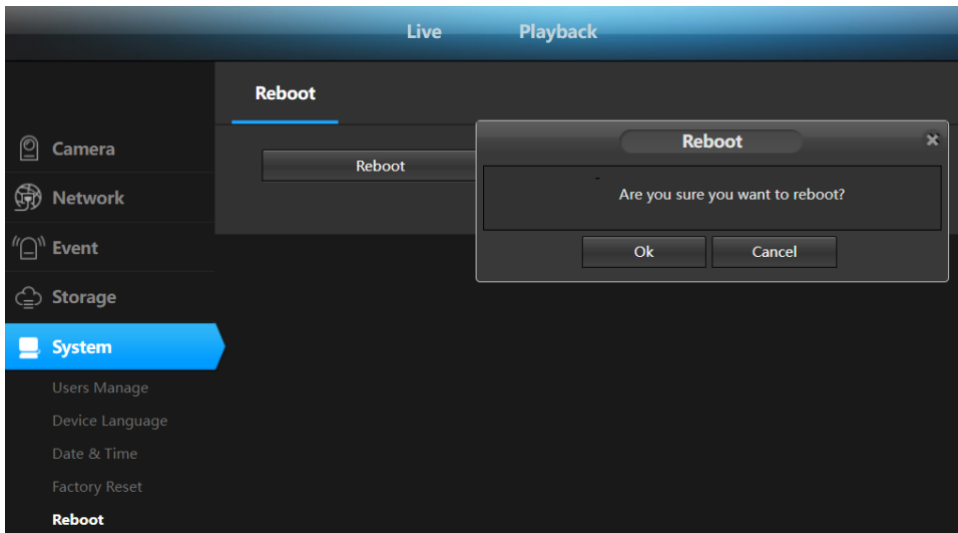


Figure 8.10

8.6 Regular maintenance

Timed maintenance is used to set the device to restart at the set time. After the date and time are set and saved, the device will automatically restart when the device time runs to the set time. The timed maintenance function allows the device to initialize certain functions by restarting during long-term use, which can extend the life of the device.

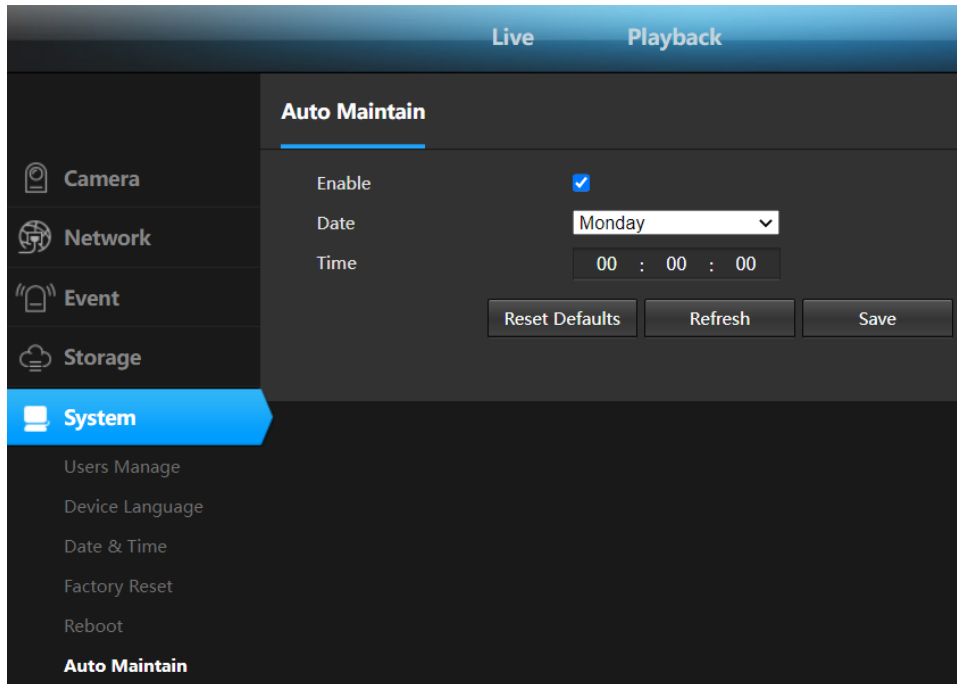


Figure 8.11

8.7 Firmware upgrade

The system upgrade interface is shown in Figure 8.12. Click the "Browse" button to jump to the local computer to select the firmware file to be upgraded, as shown in Figure 8.13. After selecting the firmware file, click "Open", and the file path will be automatically filled in the text box after "Firmware file". Click the "Upgrade" button to start the upgrade. The firmware upgrade is divided into three stages: the first is the upload of the firmware file, and then the firmware is upgraded. When the firmware is upgraded, the system will count the seconds. Finally, the device is restarted. After the restart, the system automatically jumps to the login interface. From the start of the upgrade to the completion of the device restart, the process takes about two minutes. During this time, please do not disconnect the power of the device.

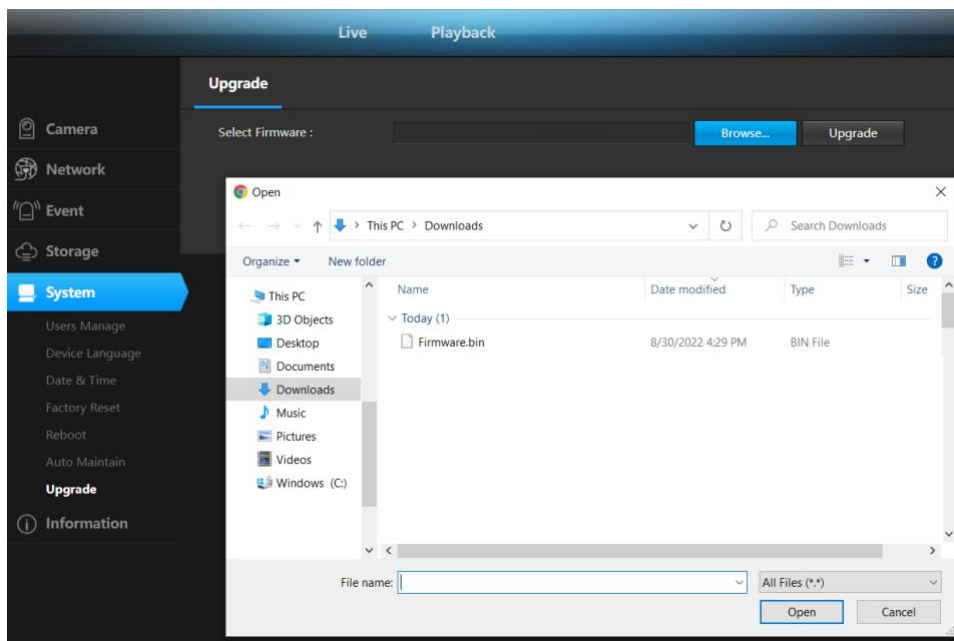


Figure 8.12 & Figure 8.13

8.8 Version Information

This interface shows the system kernel version, file system version, device serial number, and Web control version of the device in detail, as shown in Figure 9.14.

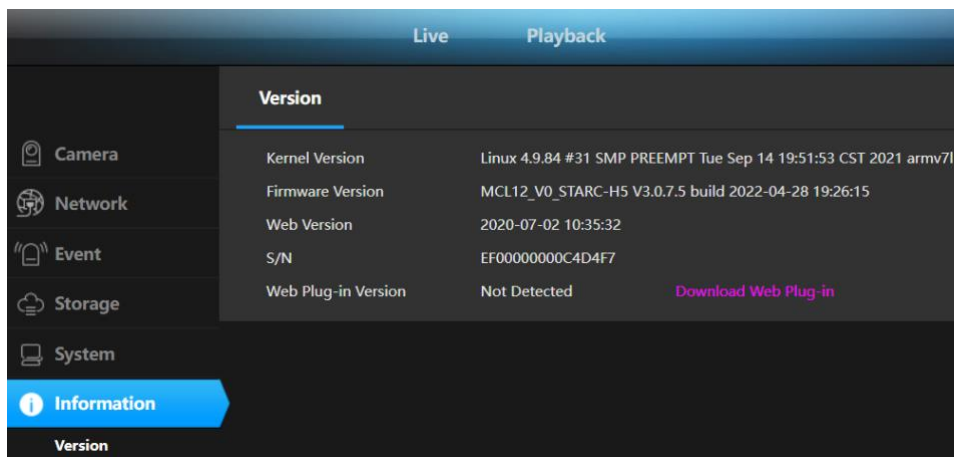


Figure 9.14

9 FAQ

9.1 The device cannot be accessed through a browser

There are four possible reasons for this:

(A) The network is unreachable: The solution is to use the PC to access the network to test whether the network connection can be normal. First, eliminate the cable fault, the network fault caused by the PC virus, until the PC can ping each other (see ping operation section 2.2.4).

(B) The IP address is occupied by other devices: the solution is to disconnect the IPCAMERA device from the network, connect it to the PC separately, and reset the IP address according to the appropriate recommended operation (using the ONVIF Device Manager V2.2.250).

(C) The IP address is in a different subnet segment: Solution, check IPCAMERA's IP address and subnet mask address and gateway settings (using the ONVIF Device Manager V2.2.250).

(D) Unknown cause: Press and hold factory reset button located on the camera module.

9.2 Normal data cannot pass through the switch

Normal data cannot pass through the switch and may be caused by the following three conditions:

(A) There is a Layer 2 switch. Is the address wrong?

Solution: Before looking for a network failure, be sure to use the ping command to connect to the other party's address in command line mode. Looking at the information returned after ping is an especially important part. If no message is returned, the network must be faulty.

(B) Is there a Layer 3 switch, is port and physical address binding?

Solution: If IP and MAC addresses are bound, then you need to make such settings inside the switch, adding a new binding, that is, the camera's IP address and Mac address binding.

(C) Is the ACL not considered when configuring firewall rules?

Solution: If the switch does not consider the camera when configuring the firewall rules, then it is necessary to allow the camera to communicate on ports 554, 3001, 8000, 8091, 8200, 80 in the default configuration of the camera. Otherwise, all packets will be filtered and cannot be reached. If the port of the camera has changed, open the corresponding port of the camera in the switch firewall.11.4 An error occurs when accessing the device through a browser after the upgrade.

9.3 Error accessing the device through the browser after upgrading

In this case, delete your browser's cache.

The specific steps are as follows: Open the browser, select "Tools Menu - Internet Options", click the "Delete Files" button in the second item (Temporary Internet Files), and check the "Delete All Offline Content" option. Then select OK. You can also start - run - enter the "cm" command on the desktop - enter "arp -d" to clear the cache, and then log in to the device again

10 Revisions

This chapter describes changes to the document from the previous revision.

Rev No.	Revision Note	Date (YYYY.MM.DD)	By (X. Xxxx)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
23			
25			
26			
27			
28			
29			
30			



Safety Technology International

2306 Airport Rd. • Waterford, MI 48327, USA
Phone: 248-673-9898 • info@sti-usa.com • www.sti-global.com

Taylor House • 34 Sherwood Road • Bromsgrove, Worcestershire • B60 3DR • England
Tel: +44 (0)1527 520 999 • info@sti-emea.com • www.sti-global.com

Unit 7A • Lockhead Avenue • Airport Business Park • Waterford • X91 HWF2 • Ireland
info@sti-emea.com • www.sti-global.com



USA

Subject to change without notice.
Printed in USA

G3 & GF CAMERA IS
JULY2024