

# PRODUCT MANUAL

**ON ALERT  
SERIES****INTEGRATED  
PIR****2-WAY  
AUDIO****4 MEGAPIXEL****IR  
ILLUMINATION****FIXED LENS****PROGRAMMABLE  
ANALYTICS**

## KEY FEATURES

- 4 MegaPixel 1/3" Progressive Scan CMOS Sensor (2560×1440 Res.)
- Built-in PIR, Two-Way Audio, Echo Cancellation & Noise Reduction
- 2.1mm Fixed Wide Angle Lens with 137° Horizontal Field of View
- True Day/Night Function with ICR and 33' IR Night Vision
- 2.4GHz Wi-Fi (IEEE 802.11 b/g/n) with Up to 165' Range
- Smart Event Alarms: Motion, Person, PIR, Audio, Scene Change, Blur, and Color Abnormality
- Programmable Analytics: Line Crossing and Region Intrusion Detection
- H.265+/H.265/H.264+/H.264 Compression
- Built-in microSD Card Slot Supports Up to 256GB of Local Recording
- Designed for the Transcendent Platform, with seamless integration with the Transcendent Recorders, Apps, and VMS with Push Notifications
- Supports Simultaneous Viewing for Up to 4 Users
- 100Mbps RJ45 Network Port + IEEE 802.3af PoE Support
- Versatile Mounting Options: Wall, Ceiling, or Desktop
- Power Options: DC12V or PoE with <5W Consumption
- 3-Year Warranty
- Power Supply (Included) : 12VDC @ 1.5A (UL Listed)

*\*Research local, state and federal laws regarding the implementation of audio surveillance.*



### PLEASE NOTE:

Complete User Guide, Software, Tools, and Updates are available online. Scan the QR Code or visit:  
<https://www.vitekccv.com>

Please read this instruction carefully before operating the unit and keep it for further reference

The following symbols or words may be found in this manual.

| Symbols/Words                                                                                    | Description                                                                                                                                 |
|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
|  <b>Warning</b> | Indicates a medium or low potential hazardous situation which, if not avoided, will or could result in slight or moderate injury            |
|  <b>Caution</b> | Indicates a potential risk which, if not avoided, will or could result in device damage, data loss, lower performance or unexpected results |
|  <b>Note</b>    | Provides additional information to emphasize or supplement important points of the text.                                                    |

## About the Manual

- This manual is suitable for many models. All examples, screenshots, figures, charts, and illustrations used in the manual are for reference purposes, and actual products may be different with this Manual.
- Please read this user manual carefully to ensure that you can use the device correctly and safely.
- Within the maximum scope permitted by the law, the products described in this Manual (including hardware, software, firmware, etc.) are provided “AS IS”. The information in this document (including URL and other Internet site reference data) is subject to change without notice. This Manual may contain technical incorrect places or printing errors. This information will be periodically updated, and these changes will be added into the latest version of this Manual without prior notice.
- In this manual, the trademarks, product names, service names and company names that are not owned by our company are the properties of their respective owners.

## Use of the Product

- This product should not be used for illegal purposes.
- The company does not allow anyone to use the Company's products to infringe the privacy, personal information, and portrait rights of others. The user shall not use this product for any illegal use or any prohibited use under these terms, conditions, and declarations. When using this product, the user shall not damage, disable, overload or obstruct any of the hardware of this product in any way, or interfere with the use of this product by any other users. Also, the user should not attempt to use the product or the software, by hacking, stealing the password, or any other means.

## Electrical Safety

- This product is intended to be supplied by a Listed Power Unit, marked with 'Limited Power Source', 'LPS' on unit, output rated minimum 12V/2 A or POE 48V/ 350mA, no more than 2000m altitude of operation and Tma=60 Deg.C.
- As for the modes with PoE function, the function of the ITE being investigated to IEC 60950-1 standard is considered not likely to require connection to an Ethernet network with outside plant routing, including campus environment and the ITE is to be connected only to PoE networks without routing to the outside plant.
- Improper handling and/or installation could run the risk of fire or electrical shock.
- The product must be grounded to reduce the risk of electric shock.
- ⚠ Warning: Wear anti-static gloves or discharge static electricity before removing the bubble or cover of the camera.

## Environment

- Heavy stress, violent vibration or exposure to water is not allowed during transportation, storage and installation.
- Avoid aiming the camera directly towards extremely bright objects, such as, sun, as this may damage the image sensor.
- Keep away from heat sources such as radiators, heat registers, stove, etc.
- Do not expose the product to the direct airflow from an air conditioner.
- Do not block any ventilation openings and ensure proper ventilation around the camera.
- Do not place the device in a damp, dusty, extremely hot, or cold environment, or in locations with strong electromagnetic radiation or unstable lighting.
- Make sure that no reflective surface is too close to the camera lens. The IR light from the camera may reflect into the lens, resulting in image blur.

## Operation and Daily Maintenance

- There are no user-serviceable parts inside. Please contact the nearest service center if the product does not work properly.
- Please shut down the device and then unplug the power cable before you begin any maintenance work.
- ⚠ Warning: All the examination and repair work should be done by qualified personnel.
- Do not touch the CMOS sensor optic component. You can use a blower to clean the dust on the lens surface.
- Always use a dry soft cloth to clean the device. If there is too much dust, use a cloth cleaning (such as using cloth) may result in poor IR/illumination LEDs functionality and/or IR/illumination LEDs reflection.
- The IR LEDs should at no time be covered when the camera is running to prevent overheating and the possible risk of fire.

## Privacy Protection

- When installing cameras in public areas, a warning notice shall be given in a reasonable and effective manner, and clarify the monitoring range.
- As the device user or data controller, you might collect the personal data of others, such as face, car plate number, etc. As a result, you shall implement reasonable and necessary measures to protect the legitimate rights and interests of other people, avoiding data leakage, improper use, including but not limited to setting up access control, providing clear and visible notice to inform people of the existence of the surveillance area, providing required contact information, and so on.

## **Disclaimer**

- With regard to the product with internet access, the use of the product shall be wholly at your own risk. Our company shall not be responsible for abnormal operation, privacy leakage, or other damages resulting from a cyber attack, hacker attack, virus inspection, or other internet security risks; however, our company will provide timely technical support if necessary.
- Surveillance laws vary from country to country. Check all laws in your local region before using this product for surveillance purposes. We shall not take the responsibility for any consequences resulting from illegal operations.

## **Cybersecurity Recommendations**

- Use a strong password. At least 8 characters or a combination of characters, numbers, and upper and lower case letters should be used in your password.
- Regularly change the passwords of your devices to ensure that only authorized users can access the system (recommended time is 90 days).
- It is recommended to change the service default ports (like HTTP-80, HTTPS-443, etc.) to reduce the risk of outsiders being able to access.
- It is recommended to set the firewall of your router. But note that some important ports cannot be closed (like HTTP port, HTTPS port, Data Port).
- It is not recommended to expose the device to the public network. When it is necessary to be exposed to the public network, please set the external hardware firewall and the corresponding firewall policy.
- It is not recommended to use the v1 and v2 functions of SNMP.
- In order to enhance the security of WEB client access, please create a TLS certificate to enable HTTPS.
- Use a black and white list to filter the IP address. This will prevent everyone, except those specified IP addresses from accessing the system.
- If you add multiple users, please limit the functions of guest accounts.
- If you enable UPnP, it will automatically try to forward ports in your router or modem. It is really very convenient for users, but this will increase the risk of data leakage when the system automatically forwards ports. Disabling UPnP is recommended when the function is not used in real applications.

- Check the log. If you want to know whether your device has been accessed by unauthorized users or not, you can check the log. The system log will show you which IP addresses were used to log in to your system and what was accessed.

## Regulatory Information

### FCC Information

Please take note that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

#### 1. FCC compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. 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.

#### 2. FCC conditions:

- This device complies with part 15 of the FCC Rules. Operation of this product is subject to the following two conditions:
- This device may not cause a harmful interface.
- This device must accept any interference received, including interference that may cause undesired operation.

### RoHS

The products have been designed and manufactured in accordance with Directive EU RoHS Directive 2011/65/EU and its amendment Directive 2015/863 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.



EU

2012/19/EU (WEEE directive): The Directive on waste electrical and electronic equipment (WEEE Directive). To improve the environmental management of WEEE, the improvement of collection, treatment, and recycling of electronics at the end of their life is essential.

Therefore, the product marked with this symbol must be disposed of in a responsible manner.

Directive 94/62/EC: The Directive aims at the management of packaging and packaging waste and environmental protection. The packaging and packaging waste of the product in this manual refers to must be disposed of at designated collection points for proper recycling and environmental protection.

REACH(EC1907/2006): REACH concerns the Registration, Evaluation, Authorization and Restriction of Chemicals, which aims to ensure a high level of protection of human health and the environment through better and earlier identification of the intrinsic properties of chemical substances. The product in this manual refers to conforms to the rules and regulations of REACH. For more information on REACH, please refer to DG GROWTH or ECHA websites.

# Table of Contents

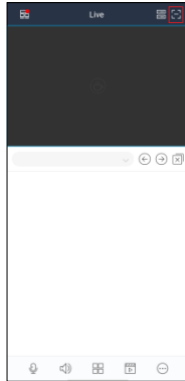
|          |                                   |           |
|----------|-----------------------------------|-----------|
| <b>1</b> | <b>Network.....</b>               | <b>8</b>  |
| 1.1      | APP Connection .....              | 8         |
| 1.2      | Wired Network Connection.....     | 9         |
| 1.2.1    | Access through IP-Tool.....       | 9         |
| 1.2.2    | WAN.....                          | 11        |
| 1.3      | Wi-Fi Connection .....            | 13        |
| <b>2</b> | <b>Live View via Web.....</b>     | <b>15</b> |
| <b>3</b> | <b>Configuration via Web.....</b> | <b>17</b> |
| 3.1      | System Configuration.....         | 17        |
| 3.1.1    | Basic Information.....            | 17        |
| 3.1.2    | Date and Time.....                | 17        |
| 3.1.3    | Local Config .....                | 18        |
| 3.1.4    | Storage .....                     | 18        |
| 3.2      | Image Configuration.....          | 22        |
| 3.2.1    | Display Configuration.....        | 22        |
| 3.2.2    | Video / Audio Configuration ..... | 24        |
| 3.2.3    | OSD Configuration .....           | 26        |
| 3.2.4    | Video Mask .....                  | 26        |
| 3.2.5    | ROI Configuration .....           | 27        |
| 3.3      | Alarm Configuration .....         | 28        |
| 3.3.1    | Motion Detection .....            | 28        |
| 3.3.2    | Exception Alarm .....             | 31        |
| 3.3.3    | Alarm In .....                    | 33        |
| 3.3.4    | Alarm Out .....                   | 34        |
| 3.3.5    | Alarm Server .....                | 35        |
| 3.3.6    | Audio Alarm .....                 | 35        |
| 3.3.7    | Video Exception.....              | 38        |
| 3.3.8    | Disarming.....                    | 38        |
| 3.3.9    | Person Detection .....            | 39        |
| 3.3.10   | PIR Alarm .....                   | 39        |
| 3.4      | Event Configuration .....         | 40        |
| 3.4.1    | Line Crossing .....               | 40        |
| 3.4.2    | Region Intrusion.....             | 43        |
| 3.5      | Network Configuration.....        | 45        |
| 3.5.1    | TCP/IP.....                       | 45        |
| 3.5.2    | Port.....                         | 46        |
| 3.5.3    | Server Configuration.....         | 47        |
| 3.5.4    | Onvif .....                       | 47        |
| 3.5.5    | DDNS.....                         | 48        |

|                                         |                                 |           |
|-----------------------------------------|---------------------------------|-----------|
| 3.5.6                                   | SNMP .....                      | 49        |
| 3.5.7                                   | 802.1x .....                    | 50        |
| 3.5.8                                   | RTSP .....                      | 51        |
| 3.5.9                                   | RTMP .....                      | 52        |
| 3.5.10                                  | UPNP .....                      | 52        |
| 3.5.11                                  | Email .....                     | 53        |
| 3.5.12                                  | FTP .....                       | 54        |
| 3.5.13                                  | HTTP POST .....                 | 55        |
| 3.5.14                                  | HTTPS .....                     | 56        |
| 3.5.15                                  | NAT .....                       | 58        |
| 3.5.16                                  | QoS .....                       | 58        |
| 3.5.17                                  | Wi-Fi Settings .....            | 59        |
| 3.6                                     | Security Configuration .....    | 60        |
| 3.6.1                                   | User Configuration .....        | 60        |
| 3.6.2                                   | Online User .....               | 62        |
| 3.6.3                                   | Block and Allow Lists .....     | 63        |
| 3.6.4                                   | Security Management .....       | 63        |
| 3.7                                     | Maintenance Configuration ..... | 64        |
| 3.7.1                                   | Backup and Restore .....        | 64        |
| 3.7.2                                   | Reboot .....                    | 65        |
| 3.7.3                                   | Upgrade .....                   | 66        |
| 3.7.4                                   | Operation Log .....             | 67        |
| 3.7.5                                   | Serial Output .....             | 67        |
| 3.7.6                                   | Maintenance Information .....   | 67        |
| 4                                       | Search .....                    | 67        |
| 4.1                                     | Image Search .....              | 68        |
| 4.2                                     | Video Search .....              | 69        |
| <b>Appendix .....</b>                   |                                 | <b>72</b> |
| <b>Appendix 1 Troubleshooting .....</b> |                                 | <b>72</b> |

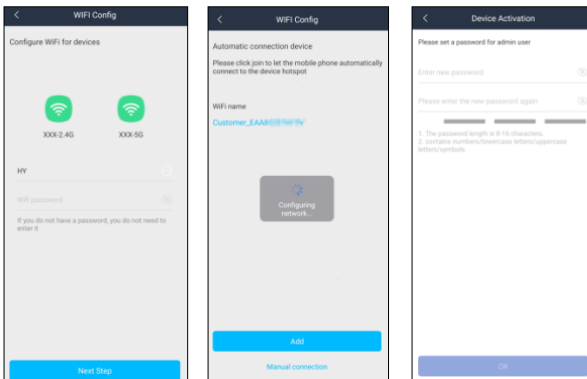
# 1 Network

## 1.1 APP Connection

- ① Enable Wi-Fi network on your phone. Then scan the QR Code of the APP in the QSG (Quick Start Guide) or open your phone's APP store and search "Transcendent viewer". Then install the mobile APP on your phone.
- ② Run the mobile APP and then log in to your account on the APP (if you haven't registered, please register and log in first). Then, enter the server list interface of the APP.
- ③ Then tap  in the live interface of the APP. Scan the QR Code attached to the back of the device or the QR Code of the device in the QSG. After that, tap "Add". When the indicator of the device is blue, check "Confirmed that..." and tap "Next Step".



- ④ Enter the key (or password) of the Wi-Fi network. Tap "Next Step". Click the searched device's hotspot name, and then the device will automatically configure WIFI.
- ⑤ After you activate the device, it will be automatically added to the server list.



**Note:** 1. When configuring the Wi-Fi network via the APP, (a). Your mobile phone must be connected to the Wi-Fi network; (b). The device must be within the mobile phone signal coverage area. **DO NOT** move your phone too far away from the device.

2. After the Wi-Fi of the device is successfully connected, you can use Wi-Fi or mobile web in your mobile phone as needed. However, if you want to remotely view the device video via mobile web, please make sure the wireless router/AP connected to the device has been connected to the Ethernet.

## 1.2 Wired Network Connection

Using a Web browser for example.

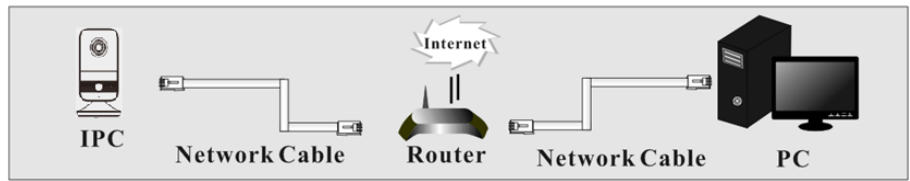
**Web browser:** Firefox/Edge/Safari/Google Chrome

It is recommended to use the latest version of these web browsers.

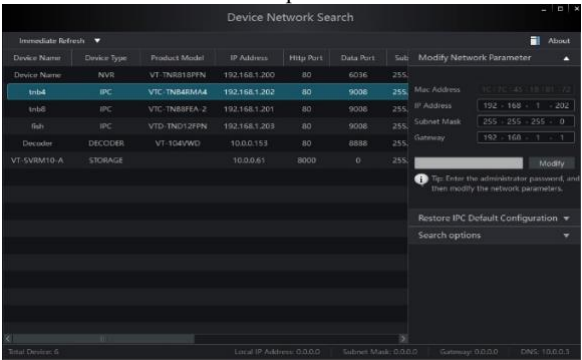
The menu display and operation of the camera may be slightly different by using the browser with plug-in or without plug-in. Installing the plug-in will display more functions of the camera. Connect the IP camera via LAN or WAN.

### 1.2.1 Access through IP-Tool

Network connection:



- ① Make sure the PC and device are connected to the same local network and the IP-Tool is installed on the PC.
- ② Double click the IP-Tool icon on the desktop to run this software as shown below:



- ③ Double click the device information listed in the IP-Tool and then the system will open a

web browser to connect the camera. If there are many devices, please find your device via its part number or MAC address. After you read the privacy statement, check and click “Already Read”. This will bring you to a configuration wizard interface.

- a. Select the location (e.g. US Pacific). Then click [Next].
- b. Set the zone, video format (frequency), date and time format.

The screenshot shows a web interface titled "Config". It contains four dropdown menus arranged vertically:

- Frequency: 60HZ
- Zone: GMT-05 (New York, Torc
- Date Format: MM-DD-YYYY
- Time Format: 12-Hour

At the bottom of the form are two buttons: "Back" and "Next".

- c. Set security questions and answers as needed. After setting the questions and answers, click [Next] to continue. It is very important for you to reset your password. Please remember these answers.

- d. Activate the device.

The screenshot shows a web interface titled "Device Activation". It contains the following fields and options:

- User Name: admin
- ☒ Activate Onvif User
- New Password: (empty field)
- 8~16 characters; Numbers, special characters, upper case letters and lower case letters must be included.
- Confirm Password: (empty field)

At the bottom of the form are two buttons: "Back" and "Save".

The default username is “admin” . Please self-define the password of the admin according to the tip.

**Note:** It is highly recommended to use a strong password for your account security. If you want to change your password level, you can go to **Config→Security Management →Password Security** to change the level and then modify the admin password (Go to **Config→User**).

By default, the ONVIF password will match the admin password that you set. Should you wish to change the ONVIF password to a different password than your admin password, go to the ONVIF section to change the password (**Config→Network→Onvif**)

When you connect the camera through the ONVIF protocol in a third-party platform, you can use the username and the password set to connect.

e. Click “Save” to save the settings.

Read the privacy statement, check, and click “Already Read”. Then the login interface will appear as shown below.

If it is the first time for you to log in, follow directions to download, install, and run the Plug-in if prompted.

The image shows a login form with the following elements:

- Name:** A text input field containing the text "admin".
- Password:** A text input field with masked characters represented by seven dots ".....".
- Language:** A dropdown menu showing "English" with a blue arrow icon on the right.
- Forgot Password?** A blue, underlined text link located below the language dropdown.
- Login** A large blue rectangular button at the bottom of the form.

Please enter the username (admin) and password. Then select the language as needed.

If you forget the admin password, you can reset the password by clicking **Forget Password** on the login page. Then you can reset the password with the security questions and answers you set. You can set the account security question during the activation, or you can go to **Config→Security→User**, click **Safety Question**, select the security questions and input your answers.

After that, you can add your device to the APP. The steps are as follows:

- 1) Scan the QR Code of the APP in the QSG (Quick Start Guide) or open your phone's APP store and search “Transcendent viewer”. Then install the mobile APP (Transcendent viewer) on your phone.
- 2) Run the mobile APP and then log in your account of the APP (if you haven't register, please register and log in first). Then enter the server list interface of the APP.
- 3) Tap “Add Device” in the server list interface of the APP. Scan the QR Code to add the device to the server list of the APP.

### 1.2.2 WAN

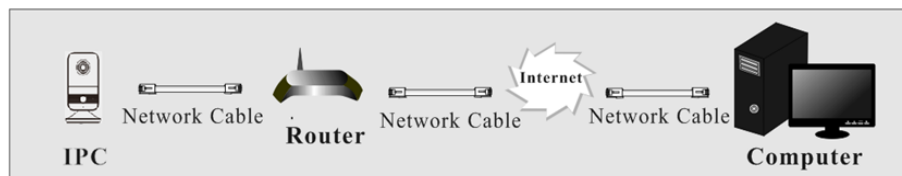
#### ➤ Access via NAT

Connect and activate the device according to the above-mentioned steps. Enable NAT service (click **Config→Network→NAT**) and then enter the address in the address bar of a web browser

to access remotely.

After you bind the camera to your APP account and enable the NAT service, a verification code will be required when logging onto the web client by using the above address (different areas and regions maybe have different visit addresses). Please enter the correct verification code from the APP.

### ➤ Access through the router or virtual server



To remotely access the device via Web, the setting steps are as follows:

- ① Make sure the camera is connected to the local network and then log in the camera via LAN and go to **Config** → **Network** → **Port** to set the port number.

|            |                                   |
|------------|-----------------------------------|
| HTTP Port  | <input type="text" value="80"/>   |
| HTTPS Port | <input type="text" value="443"/>  |
| Data Port  | <input type="text" value="9008"/> |
| RTSP Port  | <input type="text" value="554"/>  |

Port Setup

- ② Go to **Config** → **Network** → **TCP/IP** to modify the IP address.

|                                                               |                                                                                  |
|---------------------------------------------------------------|----------------------------------------------------------------------------------|
| <input type="radio"/> Obtain an IP address automatically      |                                                                                  |
| <input checked="" type="radio"/> Use the following IP address |                                                                                  |
| IP Address                                                    | <input type="text" value="192.168.226.201"/> <input type="button" value="Test"/> |
| Subnet Mask                                                   | <input type="text" value="255.255.0.0"/>                                         |
| Gateway                                                       | <input type="text" value="192.168.1.1"/>                                         |
| Preferred DNS Server                                          | <input type="text" value="223.6.6.6"/>                                           |
| Alternate DNS Server                                          | <input type="text" value="192.168.0.5"/>                                         |

IP Setup

- ③ Go to the router's management interface through a web browser to forward the IP address

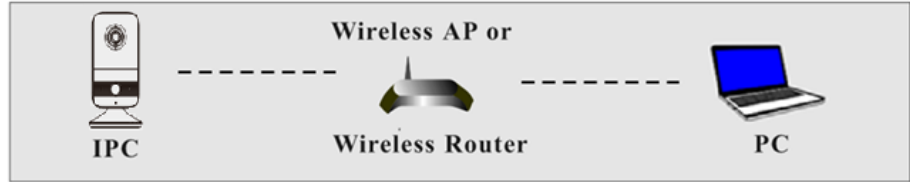
and port of the camera in the “Virtual Server”.

| Port Range  |       |    |       |          |               |                                     |
|-------------|-------|----|-------|----------|---------------|-------------------------------------|
| Application | Start |    | End   | Protocol | IP Address    | Enable                              |
| 1           | 9007  | to | 9008  | Both     | 192.168.1.201 | <input checked="" type="checkbox"/> |
| 2           | 80    | to | 81    | Both     | 192.168.1.201 | <input checked="" type="checkbox"/> |
| 3           | 10000 | to | 10001 | Both     | 192.168.1.166 | <input type="checkbox"/>            |
| 4           | 21000 | to | 21001 | Both     | 192.168.1.166 | <input type="checkbox"/>            |

Router Setup

④ Open a web browser and enter its WAN IP and http port to access. (For example, if the HTTP port is changed to 81, please enter “192.198.1.201:81” in the address bar of the web browser to access.)

1.3 Wi-Fi Connection



- ① Use the network cable to connect the device to and wireless router or AP.
- ② Connect to the above wireless network with your PC. Then run the IP-Tool on your PC and find the device via its MAC address. Then double-click it. This will bring you to the login interface of the camera. Enter the default username and password to log in. (See 1.2.1 for details)
- ③ Click **Config** → **Network** → **WIFI** to go to the following interface. Enable WI-FI, select the desired router, enter the key, and select the encryption type.

☒ Enable

| Wi-Fi Networks |              |              |               |         |                  |      |                   | Search |
|----------------|--------------|--------------|---------------|---------|------------------|------|-------------------|--------|
| Index          | SSID         | Working Mode | Security Mode | Channel | Signal Intensity | Mbps | Connection Status |        |
| 1              | Customer_... | Manage       | WPA2-personal | 1       | 80               | 150  | Unconnected       |        |
| 2              | ...          | Manage       | WPA2-personal | 1       | 59               | 150  | Unconnected       |        |
| 3              | l... 4567... | Manage       | WPA2-personal | 11      | 52               | 150  | Unconnected       |        |
| 4              | z...         | Manage       | WPA2-personal | 1       | 48               | 150  | Unconnected       |        |
| 5              | ink...       | Manage       | WPA2-personal | 3       | 43               | 150  | Unconnected       |        |

**Wi-Fi**

SSID:

Security Mode:

Key 1:

Encryption Type:

After that, select “Obtain an IP address automatically” or manually enter the IP address by clicking “Use the following IP address”. Then click “Test” to check whether the wireless network is connected. After successful connection, click “Save” to save the settings.

**LAN**

☒ Obtain an IP address automatically

☐ Use the following IP address

IP Address:

Subnet Mask:

Gateway:

Preferred DNS Server:

Alternate DNS Server:

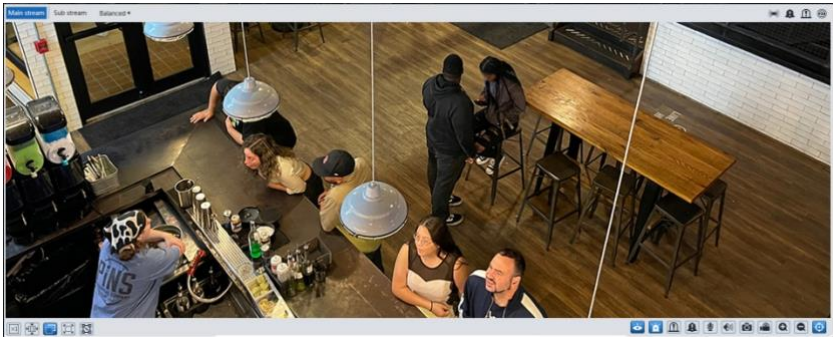
③ Pull the network cable out of the camera.

⑤ Run the IP-Tool to locate the device IP address again as it may have changed after unplugging the cable. Then double-click it in the IP-Tool or enter the IP address of the camera in the address bar of the web browser to access the camera.

After that, you can also use the downloaded APP to scan the QR code of the device to directly add it to the server list of the APP.

## 2 Live View via Web

After logging in, the following window will be shown.  
The following pictures and descriptions are for reference only.



The following table is the instructions of the icons on the live view interface.

| Icon | Description            | Icon | Description              |
|------|------------------------|------|--------------------------|
|      | Original size          |      | Zoom out                 |
|      | Fit correct scale      |      | Rule information display |
|      | Auto (fill the window) |      | Sensor alarm indicator   |
|      | Full screen            |      | Alarm output indicator   |
|      | Measure Tool           |      | Audio alarm indicator    |

| Icon                                                                              | Description                         | Icon                                                                              | Description                 |
|-----------------------------------------------------------------------------------|-------------------------------------|-----------------------------------------------------------------------------------|-----------------------------|
|  | Start/stop live view                |  | PIR alarm indicator         |
|  | Enable/disable alarm status display |  | SD card recording indicator |
|  | Enable/disable alarm output         |  | Motion alarm indicator      |
|  | Enable or disable audio alarm       |  | Color abnormal indicator    |
|  | Start/stop two-way audio            |  | Abnormal clarity indicator  |
|  | Enable/disable audio                |  | Scene change indicator      |
|  | Snapshot                            |  | Person detection indicator  |
|  | Start/stop local recording          |  | Line crossing indicator     |
|  | Zoom in                             |  | Region intrusion indicator  |

\*Measure Tool: get the height and width in pixels of the selected region in the live view interface. (This function is only available for mainstream.) Click  and drag the mouse on the image to draw a desired box. The width and height in pixels will directly display in the box.

\*The smart alarm indicators will flash only when the camera supports those functions and the corresponding events are enabled.

\*After clicking the audio alarm icon, the sound warning will be triggered according to the set warning times (you can set the warning times by clicking **Config**→**Alarm**→**Audio Alarm**). Click the icon again. After the current warning voice has sounded, it will stop.

\*Plug-in free live view: Two-way audio and local recording are not supported, and the preview mode switch (real-time/balanced/fluent mode) is not available.

\* In full-screen mode, double-click on the mouse to exit or press the ESC key on the keyboard. To set the stream profile, select Mainstream or sub-stream. Go to **Configure**→**Video/Audio** to set the resolution for each stream as needed.

## Descriptions of Rule Information



Color Descriptions of Target Recognition box:

Green box: detect human

Purple box: detect motor vehicle

Light blue box: detect non-motor vehicle (motorcycle/bicycle)

Target box after an event is triggered: turn yellow

Rule line or area color display:

Rule line or area: blue

Rule line or area after an event is triggered: turn from blue to red

## 3 Configuration via Web

In the Webcam client, choose “Config” to go to the configuration interface.

**Note:** Wherever applicable, click the “Save” button to save the settings.

### 3.1 System Configuration

#### 3.1.1 Basic Information

In the “Basic Information” interface, the system information of the device is listed, such as product model, brand, firmware version, ONVIF version, MAC address, device ID, etc. In addition, you can modify the device name as needed.

#### 3.1.2 Date and Time

Go to *Config* → *System* → *Date and Time*. Please refer to the following interface.

The screenshot shows the 'Date and Time' configuration window. At the top, there's a title bar with 'Date and Time' and a sub-header 'Summer Time'. Below this, the 'Zone' is set to 'GMT-08 (Las Vegas, San Francisco, Vancouver)'. The 'Time Mode' section has two radio buttons: 'Synchronize with NTP server' (unselected) and 'Set manually' (selected). Under 'Synchronize with NTP server', there's an 'NTP server' field with 'time.windows.com' and an 'Update period' of '1440' minutes. Under 'Set manually', there's a 'Set Time' field with '10/2/2025, 9:39:13 AM' and a checkbox 'Sync with computer local time' which is unchecked. A 'Save' button is located at the bottom right.

Select the time zone and time mode as needed.

**Note:** The time zone of the camera and the computer must be the same. It is recommended to modify the time zone of the camera according to the time zone of the computer. If the time zone of the computer is modified, the current web client needs to be closed. Then re-open it and log in again.

Time Mode:

NTP: Specify an NTP server to synchronize the time.

Manual: Set the system time manually, or you can synchronize the time with the time of the local computer.

Click the “Summertime” tab to set DST (Daylight Saving Time) as needed.

☒ DST

☒ Auto DST

☐ Manual DST

Start Time: January, First, Sunday, 00:00 Hour

End Time: February, First, Monday, 00:00 Hour

Time Offset: 120 Minutes

Save

### 3.1.3 Local Config

Go to **Config** → **System** → **Local Config** to set up the storage path of captured pictures and recorded videos on the local PC. There is also an option to enable or disable audio in the recorded files.

Picture Path: C:\Program Files\NetIPCamera\Picture Browse

Record Path: C:\Program Files\NetIPCamera\Record Browse

Video Audio Settings: ☐ Open ☒ Close

Show Bitrate: ☐ Open ☒ Close

Local Smart Snapshot Storage: ☐ Open ☒ Close

Save

Show Bitrate: enable or disable bitrate display on the live video.

Additionally, “Local smart snapshot storage” can be enabled or disabled here. If enabled, the captured pictures triggered by smart events will be saved to the local PC.

**Note:** when you access your camera by a web browser without the plug-in, only Show Bitrate can be set in the above interface.

### 3.1.4 Storage

Go to **Config** → **System** → **Storage** to go to the interface as shown below.

| Management                                                                    | Record Parameters | Schedule Record | Snapshot | FTP Snapshot |
|-------------------------------------------------------------------------------|-------------------|-----------------|----------|--------------|
| Total picture capacity                                                        | 380 MB            |                 |          |              |
| Picture remaining space                                                       | 379 MB            |                 |          |              |
| Total recording capacity                                                      | 3328 MB           |                 |          |              |
| Record remaining space                                                        | 3200 MB           |                 |          |              |
| State                                                                         | Normal            |                 |          |              |
| Snapshot Quota                                                                | 10 %              |                 |          |              |
| Video Quota                                                                   | 90 %              |                 |          |              |
| Changes in the quota ratio need to be formatted before they become effective. |                   |                 |          |              |
| <input type="button" value="Eject"/> <input type="button" value="Format"/>    |                   |                 |          |              |

## ● SD Card Management

Click the “Format” button to format the SD card. All data will be cleared by clicking this button. Click the “Eject” button to stop writing data to the SD card. Then the SD card can be ejected safely.

**Snapshot Quota:** Set the capacity proportion of captured pictures on the SD card.

**Video Quota:** Set the capacity proportion of record files on the SD card.

**Note:** This series of products supports ANR (Automatic Network Replenishment) function. The offline video recorded files can be searched in the search interface.

1. When the network of the camera is disconnected (for example, the network cable is unplugged), the camera will automatically trigger record and store the recorded files to the SD card.
2. After the IPC is added to the NVR supporting ANR function and the ANR function of the IPC is enabled in the NVR, the IPC will automatically trigger recording and store the recorded files to the SD card when the network between the NVR and the IPC is disconnected. After resuming the connection, the IPC will automatically upload the recorded files during the offline period to the NVR.

## ● Configuring Record Parameters

Go to **Config** → **System** → **Storage** → **Record Parameters**.

| Management                          | Record Parameters | Schedule Record | Snapshot | FTP Snapshot |
|-------------------------------------|-------------------|-----------------|----------|--------------|
| Cycle Write                         | Yes               |                 |          |              |
| <input type="button" value="Save"/> |                   |                 |          |              |

**Overwrite (Cycle Write):** the earliest record data will be replaced by the latest when the SD card is full.

## ● Schedule Recording Settings

Go to **Config** → **System** → **Storage** → **Schedule Record** to go to the interface as shown below.

| Management                                                 | Record Parameters             | Schedule Record | Snapshot | FTP Snapshot |
|------------------------------------------------------------|-------------------------------|-----------------|----------|--------------|
| <b>Parameter Settings</b>                                  |                               |                 |          |              |
| Record Stream                                              | Main stream                   |                 |          |              |
| Pre Record Time                                            | 6 Seconds (H.264,H.265,MJPEG) |                 |          |              |
| <b>Timing</b>                                              |                               |                 |          |              |
| <input checked="" type="checkbox"/> Enable Schedule Record |                               |                 |          |              |

**Pre-Record Time:** Set the time to record before the actual recording begins.

**Schedule Record:** Check “Enable Schedule Record” and set the schedule.

☐ Erase
 ☒ Add
 Manual Input Select All Invert Clear

| Week Schedule                                                                                                                                                                                                                 |                                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sun.                                                                                                                                                                                                                          | <div>0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24</div> <div>00:00-24:00 Apply settings to Manual Input Select All Invert Clear</div> |
| Mon.                                                                                                                                                                                                                          | <div>0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24</div> <div>00:00-24:00 Apply settings to Manual Input Select All Invert Clear</div> |
| Tue.                                                                                                                                                                                                                          | <div>0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24</div> <div>00:00-24:00 Apply settings to Manual Input Select All Invert Clear</div> |
| Wed.                                                                                                                                                                                                                          | <div>0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24</div> <div>00:00-24:00 Apply settings to Manual Input Select All Invert Clear</div> |
| Thu.                                                                                                                                                                                                                          | <div>0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24</div> <div>00:00-24:00 Apply settings to Manual Input Select All Invert Clear</div> |
| Fri.                                                                                                                                                                                                                          | <div>0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24</div> <div>00:00-24:00 Apply settings to Manual Input Select All Invert Clear</div> |
| Sat.                                                                                                                                                                                                                          | <div>0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24</div> <div>00:00-24:00 Apply settings to Manual Input Select All Invert Clear</div> |
| <b>Holiday Schedule</b>                                                                                                                                                                                                       |                                                                                                                                                           |
| <div>Date(MM-DD) 10-13</div> <div> <div>+</div> <div>-</div> </div> <div>0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24</div> <div>00:00-24:00 Apply settings to Manual Input Select All Invert Clear</div> |                                                                                                                                                           |
| <div>Save</div>                                                                                                                                                                                                               |                                                                                                                                                           |

### Weekly schedule

Set the alarm time from Sunday to Saturday for a single week. Each day is divided into one-hour increments. Green means scheduled. Blank means unscheduled.

“Add”: Add the schedule for a special day. Drag the mouse to set the time on the timeline.

“Erase”: Delete the schedule. Drag the mouse to erase the time on the timeline.

Manual Input: Click it for a specific day to enter specific start and end times. This adds more granularities (minutes).

### Day schedule

Set the alarm time for a special day, such as a holiday.

**Note:** Holiday schedule takes priority over weekly schedule.

● **Snapshot Settings**

Go to *Config* → *System* → *Storage* → *Snapshot* to go to the interface as shown below.

The screenshot shows the 'Snapshot' tab in the configuration menu. It contains three sections: 'Snapshot Parameters' with 'Image Format' set to 'JPEG' and 'Resolution' set to '2560x1440'; 'Event Trigger' with 'Snapshot Interval' set to '1' Second and 'Snapshot Quantity' set to '5'; and 'Timing' with 'Enable Timing Snapshot' checked and 'Snapshot Interval' set to '1' Second (0 Day 00 Hour 00 Minute 01 Second).

Set the format, resolution and quality of the image saved on the SD card and the snapshot interval and quantity and the timing snapshot here.

**Snapshot Quantity:** The number you set here is the maximum quantity of snapshots. The actual quantity of snapshots may be less than this number. Supposing the occurrence time of an alarm event is less than the time of capturing pictures, the actual quantity of snapshots is less than the set quantity of snapshots.

**Timing Snapshot:** Enable timing snapshot first and then set the snapshot interval and schedule. The setup steps of the schedule are the same as the schedule recording setup (See [Schedule Recording](#)).

● **FTP Snapshot**

Enable timing snapshot. If enabled, the system will upload snapshots to the FTP server according to the set snapshot interval.

The screenshot shows the 'FTP Snapshot' tab. It includes a checkbox for 'Enable Timing Snapshot' which is checked. Below it, 'Server Address' is set to '172.19.21.129(172.xxx.xxx.129)'. 'Snapshot Interval' is set to '60' Second (0 Day 00 Hour 01 Minute 00 Second). 'Sub Storage Path&Name' is set to '%a/FTP\_TIMING\_SNAP/%4y-%2m-%2d/%h/FTP\_TIMING\_SNAP\_%4y%2m%2d%2h%2n%2s\_%r.\*'. There are 'Reset Default' and 'Help' links, and a 'Save' button at the bottom.

**Server Address:** select the set FTP server. See [FTP section](#) for the FTP server setting.

**Sub Storage Path& Name:** Click “Help” to view the rule and then set it as needed.

Meanings of the default Path & Name Settings:

“%a/FTP\_TIMING\_SNAP/%4y-%2m-%2d/%h” stands for sub storage path

“FTP\_TIMING\_SNAP\_%4y%2m%2d%2h%2n%2s\_%r.\* ” stands for file name

The entire default value means that a jpg file named “FTP\_TIMING SNAP\_Year Month Day Hour Minute Second Random number” will be generated under FTP root directory> MAC address>FTP\_TIMING SNAP>Year-Month-Day>Hour

“FTP\_TIMING SNAP” refers to the event type. You can modify the event name as needed (for example: FTP Snapshot).

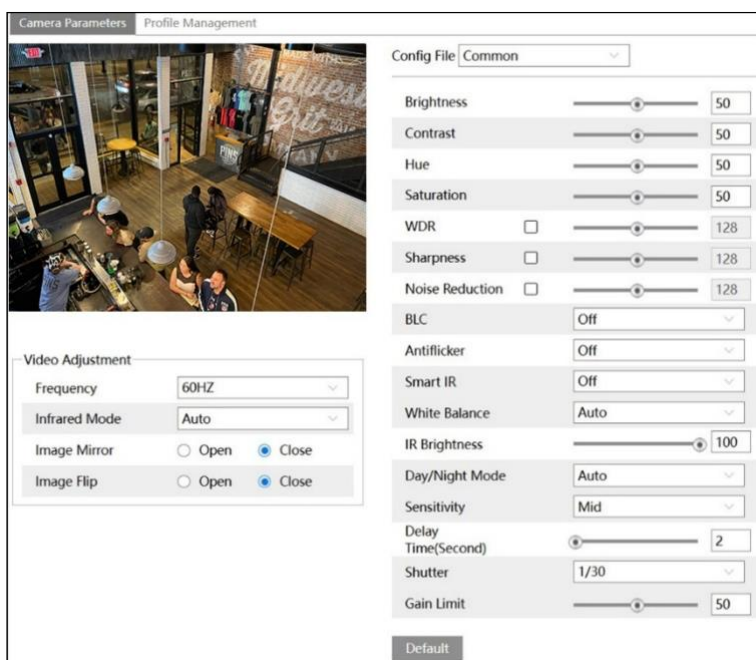
If the sub storage path and name box is empty, the snapshot will be uploaded and named according to the default settings.

If you only enter the file name rule, the snapshot will be uploaded to the root directory of the FTP server.

## 3.2 Image Configuration

### 3.2.1 Display Configuration

Go to **Image** → **Display Settings** as shown below. The image's brightness, contrast, hue and saturation and so on for common, day and night mode can be set up separately. The image effect can be quickly seen by switching the configuration file.



**Brightness:** Set the brightness level of the camera's image.

**Contrast:** Set the color difference between the brightest and darkest parts.

**Hue:** Set the total color degree of the image.

**Saturation:** Set the degree of color purity. The purer the color, the brighter the image is.

**WDR:** WDR can adjust the camera to provide a better image when there are both very bright and very dark areas simultaneously in the field of view by lowering the brightness of the bright area and increasing the brightness of the dark area.

Recording will be stopped for a few seconds while the mode is changing from non-WDR to WDR mode.

**Sharpness:** Set the resolution level of the image plane and the sharpness level of the image edge.

**Noise Reduction:** Decrease the noise and make the image more thorough. Increasing the value will make the noise reduction effect better, but it will reduce the image resolution.

**Backlight Compensation (BLC):**

- Off: disables the backlight compensation function. It is the default mode.
- HLC: lowers the brightness of the entire image by suppressing the brightness of the image's bright area and reducing the size of the halo area.
- BLC: If enabled, the auto exposure will activate according to the scene so that the object of the image in the darkest area will be seen clearly.

**Antiflicker:**

- Off: disables the anti-flicker function. This is used mostly in outdoor installations.
- 50Hz: reduces flicker in 50Hz lighting conditions.
- 60Hz: reduces flicker in 60Hz lighting conditions.

**Smart IR:** Choose "ON" or "OFF". This function can effectively avoid image overexposure to make the image more realistic. The higher the level is, the more overexposure compensation will be given.

**White Balance:** Adjust the color temperature according to the environment automatically.

**IR Brightness:** The value ranges from 1 to 100. Please set as needed.

**Day/Night Mode:** Choose "Auto", "Day", "Night", "Alarm input linkage", or "Timing".

If "Timing" is selected, you need to set daytime and nighttime. For example, if "Daytime" is set to "7:00", the camera will switch to Day mode at 7:00 o'clock; if "Nighttime" is set to "17:00", the camera will switch from Day mode to Night mode at 17:00 o'clock.

If "Alarm input linkage" is selected, the system will switch to day or night mode (according to your choice) upon the occurrence of the sensor alarm.

**Shutter:** Set the upper limit of the effective exposure time. The exposure time will be automatically adjusted (within the set shutter limit value) according to the actual situation.

**Gain Limit:** Set the upper limit of the gain. The gain value will be automatically adjusted (within the set gain limit value) according to the actual situation.

**Frequency:** 50Hz and 60Hz can be optional.

**Note:** If the frequency is switched, the camera will reboot automatically.

**Infrared Mode:** Choose "Auto", "ON", or "OFF".

**Image Mirror:** Turn the current video image horizontally.

**Image Flip:** Turn the current video image vertically.

Schedule Settings of Image Parameters:

Click the "Profile Management" tab as shown below.

Set a full-time schedule for common, auto mode, and a specified time schedule for day and night.

Auto mode: in the daytime, it will automatically perform the day config file set above; at night, it will automatically perform the night config file set above.

Choose “Timing” in the drop-down box of the schedule as shown below.

Drag “” icons to set the time of day and night. Blue means daytime and blank means night time. If the current mode of camera parameters is set to schedule, the image configuration mode will automatically switch between day and night according to the schedule.

### 3.2.2 Video / Audio Configuration

Go to **Image**→**Video / Audio** as shown below. In this interface, set the resolution, frame rate, bitrate type, video quality, and so on subject to the actual network condition.

| Index | Stream Name | Resolution | Frame Rate | Bitrate Type | Bitrate(Kbps) | Video Quality | I Frame Interval | Video Compression | Profile      |
|-------|-------------|------------|------------|--------------|---------------|---------------|------------------|-------------------|--------------|
| 1     | Main stream | 2560x1440  | 30         | VBR          | 4096          | Higher        | 60               | H.265             | Main Profile |
| 2     | Sub stream  | 704x480    | 30         | CBR          | 512           | Higher        | 60               | H.265             | Main Profile |

Send Snapshot: Sub stream Size: 704x480

☐ Video encode slice split

☐ Watermark(Only supports H.264, H.265) Watermark content:

Two video streams can be adjusted.

**Resolution:** The size of the image.

**Frame rate:** The higher the frame rate, the video is smoother.

**Bitrate type:** CBR and VBR are optional. Bitrate is related to image quality. CBR means that no matter how much change is seen in the video scene, the compression bitrate will be kept constant. VBR means that the compression bitrate will be adjusted according to scene changes. For example, for scenes that do not have much movement, the bitrate will be kept at a lower value. This can help optimize network bandwidth usage.

**Bitrate:** it can be adjusted when the mode is set to CBR. The higher the bitrate, the better the image quality will be.

**Video Quality:** It can be adjusted when the mode is set to VBR. The higher the image quality, the more the bitrate will be required.

**I Frame interval:** It determines how many frames are allowed between “a group of pictures”. When a new scene begins in a video, until that scene ends, the entire group of frames (or pictures) can be considered as a group of pictures. If there is not much movement in the scene, setting the value higher than the frame rate is fine, potentially resulting in less bandwidth usage. However, if the value is set too high, and there is a high frequency of movement in the video, there is a risk of frame skipping.

**Video Compression:** MJPEG, H264+, H264, H265 or H265+ can be optional. MJPEG is only available for sub stream. If H.265/H.265+ is chosen, make sure the client system can decode H.265/H.265+. Compared to H.265, H.265+ saves more storage space with the same maximum bitrate in most scenes. Compared to H.264, H.265 reduces the transmission bitrate under the same resolution, frame rate, and image quality.

**Profile:** For H.264. Baseline, main and high profiles are selectable.

**Send Snapshot:** Set the snapshot stream.

**Video encode slice split:** If this function is enabled, a smooth image can be obtained even though using a low-performance PC.

**Watermark:** When playing back the local recorded video in the search interface, the watermark can be displayed. To enable it, check the watermark box and enter the watermark text.

Click the “Audio” tab to go to the interface as shown below.

| Video                                      |                                      | Audio |
|--------------------------------------------|--------------------------------------|-------|
| <input checked="" type="checkbox"/> Enable |                                      |       |
| Audio Encoding                             | G711A                                |       |
| Audio Type                                 | MIC                                  |       |
| Speaker                                    | Auto                                 |       |
| MIC In Volume                              | <div><div></div><div></div></div> 75 |       |
| Audio Out Volume                           | <div><div></div><div></div></div> 75 |       |

**Audio Encoding:** G711A and G711U are selectable.

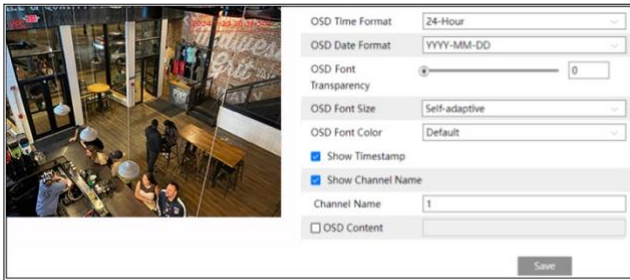
**Audio Type:** MIC.

**Speaker:** Talkback, warning, or auto can be optional. If “Talkback” is selected, the built-in speaker will be used for two-way audio. If “Warning” is selected, the built-in speaker will be used to play the pre-defined audio alarm. If “Auto” is selected, the system will output sound for two-way audio or warning voice as needed. But when it is warning and two-way audio is being enabled simultaneously, two-way audio will be output first.

**MIC IN/Audio Out Volume:** Set the volume as needed.

### 3.2.3 OSD Configuration

Go to **Image** → **OSD** as shown below.

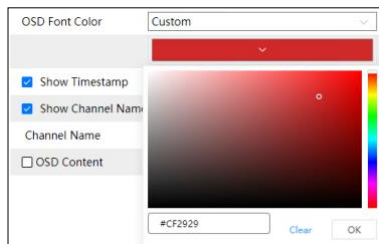


Set time format, date format, OSD content, and OSD font transparency/size/color here. After enabling the corresponding display and entering the content, drag them to change their position. Then click the “Save” button to save the settings.

**OSD Font Size:** When the image resolution is less than 720P, the OSD font size will be automatically changed to 16\*16 and will not follow the change of the font size you have set.

**OSD Font Color:** You can use the default OSD font color (white) or customize the OSD font color as needed.

To customize the font size and color:



1. Select “Custom” and then click on the blank box under it.
2. Select a color on the colorful bar (right).
3. Click on the left color box to choose the desired color. Or you can directly enter the hexadecimal color code to set the color.
4. Click “OK” to save the OSD font color settings.

### 3.2.4 Video Mask

Go to **Image** → **Video Mask** as shown below. A maximum of 4 zones can be set up.



To set up a video mask:

1. Enable video mask.
2. Click the “Draw Area” button and then drag the mouse to draw the video mask area.
3. Click the “Save” button to save the settings.
4. Return to the live to verify that the area has been drawn as shown, as blocked out in the image.

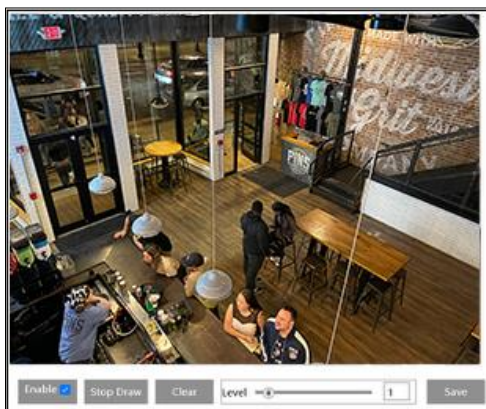


To clear the video mask:

Click the “Clear” button to delete the current video mask area.

### 3.2.5 ROI Configuration

Go to **Image**→**ROI Config** as shown below. An area in the image can be set as a region of interest. This area will have a higher bitrate than the rest of the image, resulting in better image quality for the identified area.



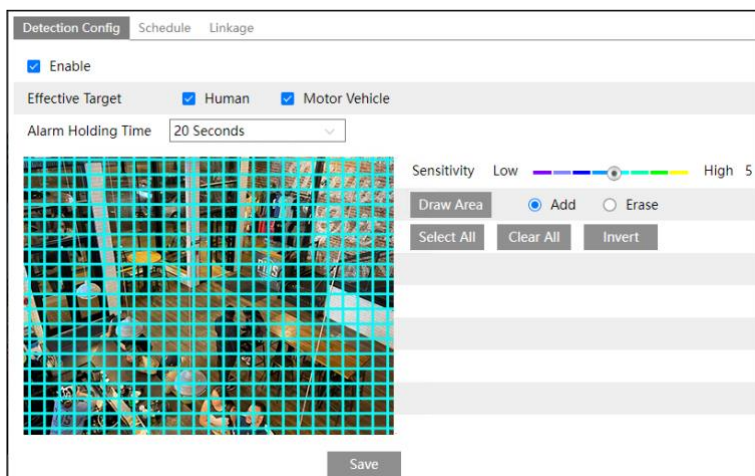
1. Check “Enable” and then click the “Draw Area” button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the “Save” button to save the settings.

## 3.3 Alarm Configuration

### 3.3.1 Motion Detection

**Motion Detection:** When a moving object appears in the detection area, and the percentage of the moving area exceeds the configured sensitivity level, an alarm will be triggered.

Go to **Alarm → Motion Detection** to set the motion detection alarm.



1. Check “Enable” check box to activate motion-based alarms. If unchecked, the camera will not send out any signals to trigger motion-based recording to the NVR or CMS, even if there

is motion in the video.

**Effective Target:** Choose “Human” or “Motor Vehicle”. If “Human/Motor Vehicle” is enabled, the camera will only detect the movement of humans/motor vehicles. If no target is enabled, alarms will be triggered when a moving object appears on the image, including humans, vehicles, or other moving objects.

**Alarm Holding Time:** It refers to the time that the alarm extends after an alarm ends. For instance, if the alarm holding time is set to 20 seconds, once the camera detects motion, it will go into alarm and will not detect any other motion for 20 seconds. If there is another motion detected during this period, it will be considered as continuous movement; otherwise, it will be considered as a single motion.

## 2. Set motion detection area and sensitivity.

Clear all grids. Then move the “Sensitivity” scroll bar to set the sensitivity. A higher sensitivity value means that motion will be triggered more easily.

Select “Add” and click “Draw”. Drag the mouse to draw the motion detection area; Select “Erase” and drag the mouse to clear the motion detection area.

You can set different sensitivity levels for different areas.

After that, click the “Save” button to save the settings.

Note:

- a) The area without colored grids means the sensitivity value is 0, which will be considered as a blocked area.
- b) After detecting a moving object in the area covered with grid lines, an alarm will be triggered when the number of red grid lines exceeds the threshold of the sensitivity level.

## 3. Set the schedule for motion detection.

Detection Config
Area and Sensitivity
Schedule

☐ Erase
☒ Add
Manual Input
Select All
Invert
Clear

Week Schedule

|      |             |                   |              |            |        |       |
|------|-------------|-------------------|--------------|------------|--------|-------|
| Sun. | 00:00-24:00 | Apply settings to | Manual Input | Select All | Invert | Clear |
| Mon. | 00:00-24:00 | Apply settings to | Manual Input | Select All | Invert | Clear |
| Tue. | 00:00-24:00 | Apply settings to | Manual Input | Select All | Invert | Clear |
| Wed. | 00:00-24:00 | Apply settings to | Manual Input | Select All | Invert | Clear |
| Thu. | 00:00-24:00 | Apply settings to | Manual Input | Select All | Invert | Clear |
| Fri. | 00:00-24:00 | Apply settings to | Manual Input | Select All | Invert | Clear |
| Sat. | 00:00-24:00 | Apply settings to | Manual Input | Select All | Invert | Clear |

Holiday Schedule

Date(MM-DD) 10-18
+
-

00:00-24:00
Apply settings to
Manual Input
Select All
Invert
Clear

Save

### Weekly schedule

Set the alarm time from Monday to Sunday for a single week. Each day is divided into one-hour increments. Green means scheduled. Blank means unscheduled.

“Add”: Add the schedule for a special day. Drag the mouse to set the time on the timeline.

“Erase”: Delete the schedule. Drag the mouse to erase the time on the timeline.

Manual Input: Click it for a specific day to enter specific start and end times. This adds more granularities (minutes).

### Day schedule

Set the alarm time for a special day, such as a holiday.

**Note:** Holiday schedule takes priority over weekly schedule.

4. Click “Linkage” to configure the alarm linkage items.

| Detection Config                    | Schedule | Linkage                   |
|-------------------------------------|----------|---------------------------|
| <input type="checkbox"/>            |          | Trigger Audio Alarm       |
| <input checked="" type="checkbox"/> |          | Trigger SD Card Snapshot  |
| <input checked="" type="checkbox"/> |          | Trigger SD Card Recording |
| <input type="checkbox"/>            |          | Trigger Email             |
| <input type="checkbox"/>            |          | Trigger FTP               |
| Trigger Alarm Out                   |          |                           |
| <input checked="" type="checkbox"/> |          | Alarm Out                 |

**Trigger Audio Alarm:** If selected, the warning voice will be played upon detecting a motion-based alarm. After checking it, you need to select the voice file as needed. If “Default” is selected, the voice file is the voice set in the audio alarm interface (see [Audio Alarm](#) for details). If “Specified” is selected, you can specify the warning voice and language for the motion alarm.

**Trigger SD Card Snapshot:** If selected, the system will capture images on motion detection and save the images on an SD card.

**Trigger SD Card Recording:** If selected, the video will be recorded on an SD card on motion detection.

**Trigger Email:** If “Trigger Email” and “Attach Picture” are checked (email address must be set first in the [Email configuration](#) interface), the captured pictures and triggered event will be sent to those addresses.

**Trigger FTP:** If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent to the FTP server address. You can set the sub storage path and name as needed. Please refer to the [FTP](#) configuration for more details.

**Alarm Out:** If selected, this would trigger an external relay output that is connected to the camera on detecting a motion-based alarm.

After that, click “Save” to save the settings.

### 3.3.2 Exception Alarm

- SD Card Full

1. Go to *Config* → *Alarm* → *Exception Alarm* → *SD Card Full*.

2. Click “Enable”.

3. Set the alarm holding time and alarm trigger options. The setup steps are the same as motion detection. Please refer to the motion detection section for details.

### ● SD Card Error

When there are some errors in writing to the SD card, the corresponding alarms will be triggered.

1. Go to **Config → Alarm → Exception Alarm → SD Card Error** as shown below.

2. Click “Enable”.

3. Set the alarm holding time and alarm trigger options. Trigger alarm out, Email, and FTP. The setup steps are the same as motion detection. Please refer to [Motion Detection](#) for details.

### ● IP Address Conflict

1. Go to **Config → Alarm → Exception Alarm → IP Address Conflict** as shown below.

| SD Card Full                               | SD Card Error | IP Address Conflict | Cable Disconnected |
|--------------------------------------------|---------------|---------------------|--------------------|
| <input checked="" type="checkbox"/> Enable |               |                     |                    |
| Alarm Holding Time                         |               | 20 Seconds          |                    |
| Trigger Alarm Out                          |               |                     |                    |
| <input type="checkbox"/> Alarm Out         |               |                     |                    |
| Save                                       |               |                     |                    |

2. Click “Enable” and set the alarm holding time.
3. Trigger the alarm out. When the IP address of the camera conflicts with the IP address of other devices, the system will trigger the alarm out.

### ● Cable Disconnection

1. Go to **Config** → **Alarm** → **Exception Alarm** → **Cable Disconnected** as shown below.

| SD Card Full                               | SD Card Error | IP Address Conflict | Cable Disconnected |
|--------------------------------------------|---------------|---------------------|--------------------|
| <input checked="" type="checkbox"/> Enable |               |                     |                    |
| Alarm Holding Time                         |               | 20 Seconds          |                    |
| Trigger Alarm Out                          |               |                     |                    |
| <input type="checkbox"/> Alarm Out         |               |                     |                    |
| Save                                       |               |                     |                    |

2. Click “Enable” and set the alarm holding time.
3. Trigger alarm out. When the camera is disconnected, the system will trigger the alarm out.

### 3.3.3 Alarm In

To set sensor alarm (alarm in):

Go to **Config** → **Alarm** → **Alarm In** as shown below.

| Detection Config                           | Schedule   | Linkage |
|--------------------------------------------|------------|---------|
| <input checked="" type="checkbox"/> Enable |            |         |
| Alarm Type                                 | NO         |         |
| Sensor Name                                |            |         |
| Alarm Holding Time                         | 20 Seconds |         |
| Save                                       |            |         |

1. Click “Enable” and set the alarm type, alarm holding time, and sensor name.
2. Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording setup. (See [Schedule Recording](#)).
3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to [Motion Detection](#) for details.
4. Click the “Save” button to save the settings.

### 3.3.4 Alarm Out

Go to *Config* → *Alarm* → *Alarm Out*.

|                    |                 |
|--------------------|-----------------|
| Alarm Out Mode     | Alarm Linkage ▼ |
| Alarm Out Name     | alarmOut1       |
| Alarm Holding Time | 20 Seconds ▼    |
| Alarm Type         | NC ▼            |
| Save               |                 |

**Alarm Out Mode:** Alarm linkage, manual operation, day/night switch linkage, and timing are optional.

**Alarm Linkage:** Having selected this mode, select the alarm out name, alarm holding time at the “Alarm Holding Time” pull-down list box, and alarm type.

**Manual Operation:** Having selected this mode, select the alarm type and click “Open” to trigger the alarm immediately; click “Close” to stop the alarm.

|                  |                    |
|------------------|--------------------|
| Alarm Out Mode   | Manual Operation ▼ |
| Alarm Type       | NC ▼               |
| Manual Operation | Open Close         |
| Save             |                    |

**Day/Night Switch Linkage:** Having selected this mode, select the alarm type and then choose to open or close the alarm out when the camera switches to day mode or night mode.

|                 |                     |
|-----------------|---------------------|
| Alarm Out Mode  | Day/night switch li |
| Alarm Type      | NC                  |
| Day             | Close               |
| Night           | Close               |
| <div>Save</div> |                     |

**Timing:** Select the alarm type. Then click “Add” and drag the mouse on the timeline to set the schedule of alarm out; click “Erase” and drag the mouse on the timeline to erase the set time schedule. After this schedule is saved, the alarm will be triggered at the specified time.

|                                                                             |                                                                                                                                     |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Alarm Out Mode                                                              | Timing                                                                                                                              |
| Alarm Type                                                                  | NC                                                                                                                                  |
| <div><input type="radio"/> Erase <input checked="" type="radio"/> Add</div> |                                                                                                                                     |
| Time Range                                                                  | <div><div>0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24</div><div>10:00-14:00</div><div>Manual Input</div></div> |
| <div>Save</div>                                                             |                                                                                                                                     |

### 3.3.5 Alarm Server

Go to *Alarm* → *Alarm Server* as shown below.

|                                       |         |        |
|---------------------------------------|---------|--------|
| Server Address                        | 0.0.0.0 |        |
| Port                                  | 8010    |        |
| Heartbeat                             | Disable |        |
| Heartbeat interval                    | 30      | Second |
| <div><div></div><div>Edit</div></div> |         |        |

Click “Edit” to set the alarm server.  
Set the server address, port, heartbeat, and heartbeat interval. When an alarm occurs, the camera will transfer the alarm event to the alarm server. If an alarm server is not needed, there is no need to configure this section.

Click  to view the entire server address; click  to hide a part of sensitive data.

### 3.3.6 Audio Alarm

Go to *Alarm* → *Audio Alarm* as shown below.  
Enable audio alarm. If disabled, the camera will not play the desired warning voice even if an event triggers audio alarm. Additionally, you need to enable audio in the audio configuration interface, and the audio output type should be “Warning” or “Auto”, or the warning voice cannot play.

The screenshot shows a 'Sound Config' window with two tabs: 'Sound Config' and 'Schedule'. The 'Sound Config' tab is active. It features a checked 'Enable' checkbox. Below this is the 'Voice Configuration' section, which includes a 'Warning Language' dropdown set to 'English', a 'Voice' dropdown set to 'Howling alarm sound' with a 'Listen' button next to it, a 'Warning Times' input field set to '5' with the unit 'times', and a 'Volume' slider set to '75' with a speaker icon. An 'OK' button is located at the bottom right of the window.

① Select the warning voice. If you want to customize the voice, you can choose “Customize”. Click “Select File” or “Browse” to choose the audio file you want to upload, and then enter the audio name. Finally, click “Upload” to upload the audio file. Note that the format of the audio file must meet the requirement (see Tips), or it will not be uploaded. After you upload the audio file, you can select the audio name from the audio list and click “Listen” to listen to it. Click “Delete” to delete the audio.

Sound ConfigSchedule

☒ Enable

Voice Configuration

Warning LanguageCustomize

VoiceSelectListenDelete

Warning Times5times

Volume75

Upload Audio

Upload PathSelect FileNo file selected

Audio NameUpload

Tips: audio format (WAV, 8000Hz, monophonic, 16bit, less than 200K)

Voice Record

Save PathBrowse

Audio Name

Record Audio10StartUpload

OK

You can also record your own voice in the above interface and then upload.

- Insert the microphone into your PC.
- Click “Browse” to choose the save path of the audio you want to record.
- Set the record audio volume and then click “Start” to start recording your voice.
- Click “Upload” to upload your customized voice.

**Note:** when you access your camera by a web browser without the plug-in, “Video Record” is not available in the above interface.

② Select the voice and then set the warning times and volume as needed.

Warning times range from 1 to 50.

③ Set the schedule of audio alarm. The setup steps of the schedule are the same as the schedule recording setup. (See [Schedule Recording](#)).

④ Click “OK” to save the settings.

37

### 3.3.7 Video Exception

This function can detect changes in the surveillance environment affected by external factors. To set video exception detection:

Go to **Config→Alarm→Video Exception** as shown below.

1. Enable the applicable detection that's desired.

**Scene Change Detection:** Alarms will be triggered if the scene of the monitor video has changed.

**Video Blur Detection:** Alarms will be triggered if the video becomes blurry.

**Abnormal Color Detection:** Alarms will be triggered if the image is abnormal because of color deviation.

2. Set the alarm holding time.

3. Set the sensitivity of the exception detection.

Drag the slider to set the sensitivity value or directly enter the sensitivity value in the textbox.

**The sensitivity value of Scene Change Detection:** The higher the value is, the more sensitive the system responds to the amplitude of the scene change.

**The sensitivity value of Video Blur Detection:** The higher the value is, the more sensitive the system responds to the blurriness of the image.

**The sensitivity value of Abnormal Color Detection:** The higher the value is, the more sensitive the system responds to the color shift of the image.

4. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as motion detection. Please refer to [Motion Detection](#) for details.

After checking “Trigger SD Card Snapshot” and/or “Trigger SD Card Recording”, you can search the recorded files or snapshots of video exception by selecting the “Common” event.

#### ※ The requirements of the camera and the surrounding area

1. Auto-focusing function should not be enabled for exception detection.
2. Try not to enable exception detection when light changes greatly in the scene.
3. Please contact us for more detailed application scenarios.

### 3.3.8 Disarming

You can disarm alarm linkage actions quickly in this interface.

Disarming Config Schedule

Disarming ☐ Open ☒ Close

Scheduled Disarming ☐ "Scheduled disarming" takes effect after disabling "Disarming".

Alarm Linkage ☒ Select All

☒ Email ☒ FTP ☒ HTTP POST ☒ Alarm Server

☒ Alarm Out ☒ Audio Alarm ☒ Cloud Push

Save

**Disarming:** The system stops triggering alarm linkage actions immediately.

**Scheduled Disarming:** The system stops triggering alarm linkage actions in the selected period. Click "Schedule" to set the schedule. The setup steps of the schedule are the same as the motion detection schedule settings (See [Motion Detection](#) for details).

**Note:** After "Disarming" or "Scheduled Disarming" is enabled, the reported general alarms (the alarm start time and end time of alarm out and audio alarm) will probably not match the actual situation. You need to handle it manually.

### 3.3.9 Person Detection

Alarms will be triggered when the camera detects a person. Go to **Config** → **Alarm** → **Person Detection**.

Detection Config Schedule Linkage

☒ Enable

Alarm Holding Time 20 Seconds

Save

1. Enable person detection and then set the alarm holding time.
2. Set the schedule of person detection. The setup steps of schedule are the same as the schedule recording setup (See [Schedule Recording](#)).
3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to the motion detection section for details.

### 3.3.10 PIR Alarm

PIR alarm: Alarms will be triggered when the camera detects human bodies or animals.

1. Enable PIR alarm and then set the alarm holding time.
2. Set the schedule for PIR alarm. The schedule setup steps of the PIR alarm are the same as the schedule recording setup (See [Schedule Recording](#)).
3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to the motion detection section for details.

|                                            |            |          |         |
|--------------------------------------------|------------|----------|---------|
| Detection Config                           |            | Schedule | Linkage |
| <input checked="" type="checkbox"/> Enable |            |          |         |
| Alarm Holding Time                         | 20 Seconds |          |         |
| Save                                       |            |          |         |

## 3.4 Event Configuration

For more accuracy, here are some recommendations for installation.

- Cameras should be installed on stable surfaces, as vibrations can affect the accuracy of detection.
- Avoid pointing the camera at the reflective surfaces (like shiny floors, mirrors, glass, lake surfaces, and so on).
- Avoid places that are narrow or have too much shadow.
- Avoid scenarios where the object's color is similar to the background color.
- At any time of day or night, please make sure the image of the camera is clear and with adequate and even light, avoiding overexposure or too much darkness on both sides.

### 3.4.1 Line Crossing

**Line Crossing:** Alarms will be triggered if the target crosses the pre-defined alarm lines.

Go to **Config→Event→Line Crossing** as shown below.

| Detection Config                                                                                                                                                                         |             | Schedule                                                                                                                                                                                                                                                                                                                                                                                                                             | Linkage |        |             |                                           |    |                                                   |    |                                                        |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|--------|-------------|-------------------------------------------|----|---------------------------------------------------|----|--------------------------------------------------------|----|
| <input checked="" type="checkbox"/> Enable<br><input checked="" type="checkbox"/> Save Original Picture To SD Card<br><input checked="" type="checkbox"/> Save Target Picture To SD Card |             |                                                                                                                                                                                                                                                                                                                                                                                                                                      |         |        |             |                                           |    |                                                   |    |                                                        |    |
| Alarm Holding Time                                                                                                                                                                       |             | 3 Seconds                                                                                                                                                                                                                                                                                                                                                                                                                            |         |        |             |                                           |    |                                                   |    |                                                        |    |
|                                                                                                       |             | Alarm Line: 1<br>Direction: A→B                                                                                                                                                                                                                                                                                                                                                                                                      |         |        |             |                                           |    |                                                   |    |                                                        |    |
| Draw Area   Clear   Draw Target Size                                                                                                                                                     |             | <b>Alarm Line Parameters</b><br>Detection target and sensitivity<br><table border="1"> <thead> <tr> <th>Target</th> <th>Sensitivity</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Human</td> <td>50</td> </tr> <tr> <td><input checked="" type="checkbox"/> Motor Vehicle</td> <td>50</td> </tr> <tr> <td><input checked="" type="checkbox"/> Motorcycle/Bicycle</td> <td>50</td> </tr> </tbody> </table> |         | Target | Sensitivity | <input checked="" type="checkbox"/> Human | 50 | <input checked="" type="checkbox"/> Motor Vehicle | 50 | <input checked="" type="checkbox"/> Motorcycle/Bicycle | 50 |
| Target                                                                                                                                                                                   | Sensitivity |                                                                                                                                                                                                                                                                                                                                                                                                                                      |         |        |             |                                           |    |                                                   |    |                                                        |    |
| <input checked="" type="checkbox"/> Human                                                                                                                                                | 50          |                                                                                                                                                                                                                                                                                                                                                                                                                                      |         |        |             |                                           |    |                                                   |    |                                                        |    |
| <input checked="" type="checkbox"/> Motor Vehicle                                                                                                                                        | 50          |                                                                                                                                                                                                                                                                                                                                                                                                                                      |         |        |             |                                           |    |                                                   |    |                                                        |    |
| <input checked="" type="checkbox"/> Motorcycle/Bicycle                                                                                                                                   | 50          |                                                                                                                                                                                                                                                                                                                                                                                                                                      |         |        |             |                                           |    |                                                   |    |                                                        |    |
| <b>Target Size Filter</b><br>Target: Human<br>Min Size Width: 1 %   Height: 1 %<br>Max Size Width: 90 %   Height: 90 %                                                                   |             |                                                                                                                                                                                                                                                                                                                                                                                                                                      |         |        |             |                                           |    |                                                   |    |                                                        |    |

1. Enable line crossing detection and select the snapshot type.

**Save Original Picture to SD Card:** If it is enabled, the detected original pictures will be captured and saved to the SD card when the targets cross the alarm line.

**Save Target Picture to SD Card:** If it is enabled, the detected target cutout pictures will be captured and saved to the SD card when the targets cross the alarm line.

**Note:** To save snapshots to the local PC, please enable “Local Smart Snapshot Storage” in the local config interface first. To save snapshots to the SD card, please install an SD card first.

2. Set the alarm holding time.

3. Set alarm lines, targets, and target size filter for line crossing detection.

Set the alarm line number and direction. Four lines can be added. Multiple lines cannot be added simultaneously.

**Direction:** A<->B, A->B, and A<-B are optional. This indicates the direction of the intruder who crosses over the alarm line that would trigger the alarm.

**A<->B:** The alarm will be triggered when the intruder crosses over the alarm line from B to A or from A to B.

**A->B:** The alarm will be triggered when the intruder crosses over the alarm line from A to B.

**A<-B:** The alarm will be triggered when the intruder crosses over the alarm line from B to A.

Click the “Draw Area” button and then drag the mouse to draw a line in the image. Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the lines. Click the “Save” button to save the settings.

**Note:** If the set rule line is very close to the edge of the screen, it may be difficult for the target to trigger the alarm. Please make sure that there is at least one full target-sized space between the rule line and the edge of the screen.

### **Detection Target:**

**Human:** Select it, and then alarms will be triggered if someone crosses the pre-defined alarm lines.

**Motor Vehicle:** Select it and then alarms will be triggered if a vehicle with four or more wheels (e.g. a car, bus, or truck) crosses the pre-defined alarm lines.

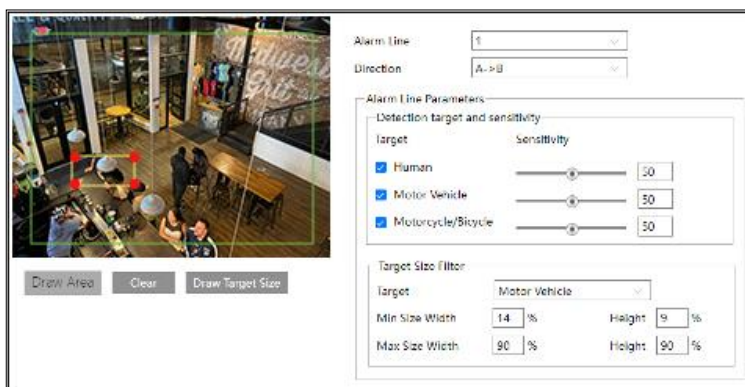
**Motorcycle/Bicycle:** Select it and then alarms will be triggered if a vehicle with two wheels (e.g. a motorcycle or bicycle) crosses the pre-defined alarm lines.

All three types of objects can be selected simultaneously. Please select the detection objects as needed. If no object/target is selected, alarms will not be triggered even if line crossing detection is enabled.

**Sensitivity:** The higher the value is, the easier the alarm can be triggered.

### **To set the target size filter:**

Click “Draw Target Size” to draw the maximum and minimum size of a specific target as shown below.



**Target:** choose “Human”, “Motor Vehicle” or “Motorcycle/Bicycle” as needed.

The green box is the maximum target detection box; the yellow box is the minimum target detection box.

Click the green box to edit the maximum target detection box; click the yellow box to edit the minimum target detection box.

Drag one of four corners of the green or yellow box to change the box size. The corresponding size value on the right will be changed too. You can also enter the digital number to directly change the box size.

Click and drag the green or yellow box to move its position.

Finally, click “Save” to save the settings.

After the target size range is set, only the target whose size is between the minimum value and the maximum value can be detected.

After that, click the “Save” button to save the settings.

4. Set the schedule of line crossing detection. The setup steps of the schedule are the same as the motion detection schedule settings (See [Motion Detection](#) for details).

5. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as motion detection. Please refer to [Motion Detection](#) for details.

### ※ Configuration requirements of the camera and the surrounding area

1. Avoid scenes with many trees or scenes with various light changes (like many flashing lights). The ambient brightness of the scenes shouldn't be too low.
2. For pedestrians, their heads and main bodies should be clearly visible in a video.



3. For vehicles, the depression angle should not be more than the recommended value. The

sideways or horizontal viewing angle is recommended for a video (see below).



- 4. Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.
- 5. Adequate light and clear scenery are crucial for line crossing detection.
- 6. Please adjust the installation position or focus to meet the requirements of the target recognition size.

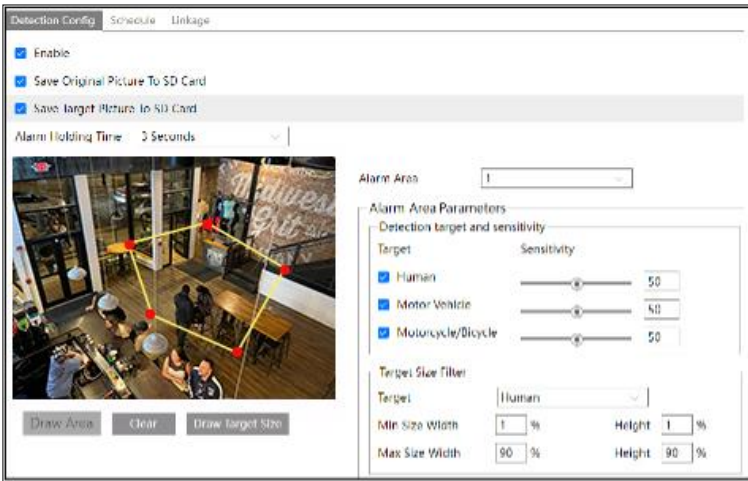
The recommended target recognition size:

| Percentage                  | Human    | Motor Vehicle | Motorcycle/Bicycle |
|-----------------------------|----------|---------------|--------------------|
| Minimum<br>(Width × Height) | 4% × 8%  | 8% × 8%       | 4% × 4%            |
| Maximum<br>(Width × Height) | 50%× 50% | 50%× 50%      | 50%× 50%           |

**Note:** The percentage means that a target occupies the percentage of the entire image. For example: In a 1080P(1920×1080) video image, the minimum resolution of human is 80×160 (w =1920x4%=80, h=1920x8%=160)

3.4.2 Region Intrusion

**Region Intrusion:** Alarms will be triggered if the target intrudes into the pre-defined areas. Go to **Config→Event→Region Intrusion** as shown below.



1. Enable region intrusion detection and select the snapshot type and the detection target.

**Save Original Picture to SD Card:** If it is enabled, the detected original pictures will be captured and saved to the SD card when the target intrudes into the pre-defined areas.

**Save Target Picture to SD Card:** If it is enabled, the detected target cutout pictures will be captured and saved to the SD card when the target intrudes into the pre-defined areas.

**Note:** To save snapshots to the local PC, please enable “Local Smart Snapshot Storage” in the local config interface first. To save snapshots to the SD card, please install an SD card first.

2. Set the alarm holding time.

3. Set alarm areas, targets and target size filter for regional intrusion detection.

Set the alarm area number. Four alarm areas can be added.

Click the “Draw Area” button and then click around the area where you want to set as the alarm area in the image (the alarm area should be a closed area). Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the alarm area. Click the “Save” button to save the settings.

**Note:** If the set rule line is very close to the edge of the screen, it may be difficult for the target to trigger the alarm. Please make sure that there is at least one full target-sized space between the rule line and the edge of the screen.

### Detection Target:

**Human:** Select it and then alarms will be triggered if someone intrudes into the pre-defined area.

**Motor Vehicle:** Select it and then alarms will be triggered if a vehicle with four or more wheels (e.g. a car, bus, or truck) intrudes into the pre-defined area.

**Motorcycle/Bicycle:** Select it and then alarms will be triggered if a vehicle with two wheels (e.g. a motorcycle or bicycle) intrudes into the pre-defined area.

All of the three types of objects can be selected simultaneously. Please select the detection objects as needed. If no object/target is selected, alarms will not be triggered even if intrusion detection is enabled.

**Sensitivity:** The higher the value is, the easier the alarm can be triggered.

**Target size filter setup:** The setup steps of the target size filter are the same as the line crossing target size filter setup (See [Line Crossing](#) for details).

4. Click the “Save” button to save the settings.

5. Set the schedule of region intrusion detection. The setup steps of the schedule are the same as the motion detection schedule settings (See [Motion Detection](#) for details).

6. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as motion detection. Please refer to [Motion Detection](#) for details.

### ※ Configuration requirements of the camera and surrounding area

The requirements are similar to line crossing detection. Please refer to [Configuration requirements of the camera and surrounding area](#) of line crossing detection for details.

## 3.5 Network Configuration

### 3.5.1 TCP/IP

Go to *Config*→*Network*→*TCP/IP* as shown below. There are two ways for network connection.

| IPv4   IPv6   PPPoE Config   IP Change Notification Config    |                                                     |
|---------------------------------------------------------------|-----------------------------------------------------|
| <input type="radio"/> Obtain an IP address automatically      |                                                     |
| <input checked="" type="radio"/> Use the following IP address |                                                     |
| IP Address                                                    | 192.168.226.201 <input type="button" value="Test"/> |
| Subnet Mask                                                   | 255.255.255.0                                       |
| Gateway                                                       | 192.168.226.1                                       |
| Preferred DNS Server                                          | 192.168.226.1                                       |
| Alternate DNS Server                                          | 8.8.8.8                                             |
| <input type="button" value="Save"/>                           |                                                     |

**Use IP address (take IPv4 for example)**—There are two options for IP setup: obtain an IP address automatically by DHCP and use the following IP address. Please choose one of the options needed.

**Test:** Test the effectiveness of the IP address by clicking this button.

**Use PPPoE**—Click the “PPPoE Config” tab to go to the interface as shown below. Click “Edit”, enable PPPoE and then enter the username and password from your ISP.

|                                                                                   |      |                          |                                     |
|-----------------------------------------------------------------------------------|------|--------------------------|-------------------------------------|
| IPv4                                                                              | IPv6 | <b>PPPoE Config</b>      | IP Change Notification Config       |
| <input type="checkbox"/> Enable                                                   |      |                          |                                     |
| User Name                                                                         |      | <input type="text"/>     |                                     |
| Password                                                                          |      | <input type="password"/> |                                     |
|  |      |                          | <input type="button" value="Edit"/> |

Either of these two network connection methods can be used. If PPPoE is used to connect to the internet, the camera will get a dynamic WAN IP address. This IP address will change frequently. To be notified, the IP change notification function can be used.

Click “IP Change Notification Config” to go to the interface as shown below.

|                                        |      |              |                                      |
|----------------------------------------|------|--------------|--------------------------------------|
| IPv4                                   | IPv6 | PPPoE Config | <b>IP Change Notification Config</b> |
| <input type="checkbox"/> Trigger Email |      |              |                                      |
| <input type="checkbox"/> Trigger FTP   |      |              |                                      |
| <input type="button" value="Save"/>    |      |              |                                      |

**Trigger Email:** when the IP address of the device is changed, the new IP address will be sent to the email address that has been set up.

**Trigger FTP:** when the IP address of the device is changed, the new IP address will be sent to the FTP server that has been set up.

### 3.5.2 Port

Go to **Config** → **Network** → **Port** as shown below.

|                                     |                                                                              |
|-------------------------------------|------------------------------------------------------------------------------|
| HTTP Port                           | <input type="text" value="80"/>                                              |
| HTTPS Port                          | <input type="text" value="443"/>                                             |
| Data Port                           | <input type="text" value="9008"/>                                            |
| RTSP Port                           | <input type="text" value="554"/>                                             |
| RTSP over TLS                       | <input type="text" value="332"/>                                             |
| Subscription<br>Listening Port      | <input type="text" value="8080"/> <input checked="" type="checkbox"/> Enable |
| <input type="button" value="Save"/> |                                                                              |

**HTTP Port:** The default HTTP port is 80. It can be changed to any port which is not occupied.

**HTTPS Port:** The default HTTPS port is 443. It can be changed to any port which is not occupied.

**Data Port:** The default data port is 9008. Please change it as necessary.

**RTSP Port:** The default port is 554. Please change it as necessary.

**RTSP over TLS:** Supports media stream transmission based on TLS channel encryption protection.

**Subscription Listening Port:** The port is used for a persistent connection of the third-party platform to push smart data.

### 3.5.3 Server Configuration

This function is mainly used for connecting network video management system.

☐ Enable

|                |                                   |
|----------------|-----------------------------------|
| Server Port    | <input type="text" value="2009"/> |
| Server Address | <input type="text"/>              |
| Device ID      | <input type="text" value="1"/>    |



1. Click “Edit” and then check “Enable”.
2. Check the IP address and port of the transfer media server in the Transcendent VMS. Then enable the auto report in the Transcendent VMS when adding a new device. Next, enter the remaining information of the device in the Transcendent VMS. After that, the system will automatically allot a device ID. Please check it in the Transcendent VMS.
3. Enter the above-mentioned server address, server port and device ID in the corresponding boxes. Click the “Save” button to save the settings. You can show or hide the sensitive data as needed.

### 3.5.4 Onvif

The camera can be searched and connected to the third-party platform via ONVIF/RTSP protocol.

If “Match Onvif Password” is enabled in the device activation interface, the password of ONVIF admin user can be modified simultaneously. When you connect the camera through the ONVIF protocol in the third-party platform, you can use this onvif user to connect.

You can also modify the password of admin sperately in the following interface and add new users in the Onvif interface.

**Note:** when adding the device to the third-party platform with ONVIF/RTSP protocol, please use the Onvif user in the above interface.

### 3.5.5 DDNS

If the camera is set up with a DHCP connection, DDNS should be set for the internet.

1. Go to **Config** → **Network** → **DDNS**.

2. Apply for a domain name. Take www.dvrddns.com for example.

Enter www.dvrddns.com in the address bar of a web browser to visit its website. Then Click the “Registration” button.

| NEW USER REGISTRATION                                                      |                                                                         |
|----------------------------------------------------------------------------|-------------------------------------------------------------------------|
| USER NAME                                                                  | <input type="text" value="XXXX"/>                                       |
| PASSWORD                                                                   | <input type="password" value="•••••"/>                                  |
| PASSWORD CONFIRM                                                           | <input type="password" value="•••••"/>                                  |
| FIRST NAME                                                                 | <input type="text" value="XXX"/>                                        |
| LAST NAME                                                                  | <input type="text" value="XXX"/>                                        |
| SECURITY QUESTION.                                                         | My first phone number.                                                  |
| ANSWER                                                                     | <input type="text" value="XXXXXXXX"/>                                   |
| CONFIRM YOU'RE HUMAN                                                       | <br>New Captcha<br><input type="text"/><br>Enter the text you see above |
| <input type="button" value="Submit"/> <input type="button" value="Reset"/> |                                                                         |

Create domain name.

*You must create a domain name to continue.*

Domain name must start with (a-z, 0-9). Cannot end or start, but may contain a hyphen and is not case-sensitive.

After the domain name is successfully applied for, the domain name will be listed as below.

Click a name to edit your domain settings.

| NAME      | STATUS | DOMAIN                |
|-----------|--------|-----------------------|
| 654321ABC | ✔      | 654321abc.dvrddns.com |

Last Update: Not yet updated IP Address: 210.21.229.130

Create additional domain names

3. Click “Edit” and then enter the username, password, domain you apply for in the DDNS configuration interface.

4. Click the “Save” button to save the settings.

### 3.5.6 SNMP

To get camera status, parameters and alarm information and remotely manage the camera, the SNMP function can be used. Before using SNMP, please install an SNMP management tool and set the parameters of the SNMP, such as SNMP port, trap address.

1. Go to **Config** → **Network** → **SNMP**.

| SNMP v1/v2                                                                                                              |                                                                |
|-------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| <input type="checkbox"/> Enable SNMPv1                                                                                  |                                                                |
| <input type="checkbox"/> Enable SNMPv2                                                                                  |                                                                |
| Read SNMP Community                                                                                                     | public                                                         |
| Write SNMP Community                                                                                                    | private                                                        |
| Trap Address                                                                                                            | 192. ***. ***. 201                                             |
| Trap Port                                                                                                               | 162                                                            |
| Trap community                                                                                                          | public                                                         |
| SNMP v3                                                                                                                 |                                                                |
| <input type="checkbox"/> Enable SNMPv3                                                                                  |                                                                |
| Read User Name                                                                                                          | public                                                         |
| Security Level                                                                                                          | auth, priv                                                     |
| Authentication Algorithm                                                                                                | <input checked="" type="radio"/> MD5 <input type="radio"/> SHA |
| Authentication Password                                                                                                 | ••••••••                                                       |
| Private-key Algorithm                                                                                                   | <input checked="" type="radio"/> DES <input type="radio"/> AES |
| Private-key Algorithm                                                                                                   | ••••••••                                                       |
| Write User Name                                                                                                         | private                                                        |
| Security Level                                                                                                          | auth, priv                                                     |
| Authentication Algorithm                                                                                                | <input checked="" type="radio"/> MD5 <input type="radio"/> SHA |
| Authentication Password                                                                                                 | ••••••••                                                       |
| Private-key Algorithm                                                                                                   | <input checked="" type="radio"/> DES <input type="radio"/> AES |
| Private-key Algorithm                                                                                                   | ••••••~                                                        |
| Other Settings                                                                                                          |                                                                |
| SNMP Port                                                                                                               | 161                                                            |
|  <input type="button" value="Edit"/> |                                                                |

- Click “Edit” and then check the corresponding version checkbox (Enable SNMPv1, Enable SNMPv2, Enable SNMPv3) according to the version of the SNMP software that will be used.
  - Set the values for “Read SNMP Community”, “Write SNMP Community”, “Trap Address”, “Trap Port” and so on. Please make sure the settings are the same as that of the SNMP software.
- Note:** Please use the different version in accordance with the security level you required. The higher the version is, the higher the level of security.

### 3.5.7 802.1x

If it is enabled, the camera’s data can be protected. When the camera is connected to the

network protected by the IEE802.1x, user authentication is needed.

☐ Enable

Protocol Type

EAP\_TLS

EAPOL Version

1

Identify

Client Certificate Installation

Select File No file selected

Install

Certificate Installation

Select File No file selected

Install

Edit

To use this function, the camera should be connected to a switch supporting 802.1x protocol. The switch can be regarded as an authentication system to identify the device in a local network. If the camera connected to the network interface of the switch has passed the authentication of the switch, it can be accessed via the local network.

Click “Edit” to start the setup.

**Protocol type:** Choose “EAP\_MD5” or “EAP\_TLS” as needed.

Select EAP-TLS as the EAP method. Enter your ID issued by the CA, and then upload related certificate(s). Before connecting the camera to the protected network with 802.1x, apply a digital certificate from a Certificate Authority (i.e., your network administrator) which can be validated by a RADIUS server.

Select EAP\_MD5 as the EAP method. You need to enter the username and password.

**Username and password:** The username and password must be the same as the username and password applied for and registered in the authentication server.

### 3.5.8 RTSP

Go to *Config* → *Network* → *RTSP*.

☒ Enable

Port

554

Address

rtsp://IP or domain name:port/profile1

rtsp://IP or domain name:port/profile2

Multicast address

Main stream239. \*\*\*. \*\*\*. 05054☒ Automatic start

Sub stream239. \*\*\*. \*\*\*. 15154☐ Automatic start

Audio239. \*\*\*. \*\*\*. 35354☐ Automatic start

☒ Allow anonymous login (No username or password required)

RTSP over TLS

☒ Enable

Port

332

Address

rtsp://IP or domain name:port/profile2

☒ Allow anonymous login (No username or password required)

Edit

Click “Edit” and then select “Enable” to enable the RTSP function.

**Port:** Access port of the streaming media. The default number is 554.

**RTSP Address:** The RTSP address (unicast) format that can be used to play the stream in a media player.

### **Multicast Address**

**Main stream:** The address format is

“rtsp://IP address: rtsp port/profile1?transportmode=mcast”.

**Sub stream:** The address format is

“rtsp://IP address: rtsp port/profile2?transportmode=mcast”.

**Audio:** Having entered the main/sub stream in a VLC player, the video and audio will play automatically.

If “Allow anonymous login...” is checked, there is no need to enter the username and password to view the video.

If “auto start” is enabled, the multicast received data should be added into a VLC player to play the video.

**RTSP over TLS:** Enable RTSP stream encryption by using TLS.

**Note:** 1. The IP address mentioned above cannot be the address of IPv6.

2. Avoid the use of the same multicast address in the same local network.

3. When playing the video through the multicast streams in a VLC player, please pay attention to the mode of the VLC player. If it is set to TCP mode, the video cannot be played.

## **3.5.9 RTMP**

You can access the third-party (like YouTube) to view live view through RTMP protocol.

Go to **Config** → **Network** → **RTMP**.

Click “Edit” and then check “Enable”, select stream type and set the reconnection time after timeout and server address as needed.

Server address: Enter the server address allocated by the third-party server.

After that, click “Save” to save the settings. Then click “Refresh” to view the connection status.

## **3.5.10 UPNP**

If this function is enabled, the camera can be quickly accessed through the LAN.

Go to **Config** → **Network** → **UPnP**. Enable UPnP and then enter UPnP name.

☒ Enable

UPnP Name

Save

### 3.5.11 Email

If you need to trigger an Email when an alarm happens or IP address is changed, please set the Email here first.

Go to *Config* → *Network* → *Email*.

Sender

Sender Address

User Name

☐ Anonymous Login

Password

Server Address

Secure Connection

Unnecessary

SMTP Port

25

☐ Send Interval(S)

60

(10-3600)

Recipient

 Edit and Test

Click “Edit and Test” to set the sender and the recipient.

**Sender Address:** sender’s e-mail address.

**Username and password:** sender’s username and password (you don’t have to enter the username and password if “Anonymous Login” is enabled).

**Server Address:** The SMTP IP address or host name.

Select the secure connection type at the “Secure Connection” pull-down list according to what’s required.

**SMTP Port:** The SMTP port.

**Send Interval(S):** The time interval of sending an email. For example, if it is set to 60 seconds and multiple motion detection alarms are triggered within 60 seconds, they will be considered as only one alarm event and only one email will be sent. If one motion alarm event is triggered and then another motion detection alarm event is triggered after 60 seconds, two emails will be sent. When different alarms are triggered at the same time, multiple emails will be sent separately.

Click the “Test” button to test the connection of the account.

**Recipient Address:** receiver’s e-mail address.

### 3.5.12 FTP

After an FTP server is set up, captured pictures from events will be uploaded to the FTP server.

1. Go to **Config** → **Network** → **FTP**.

| Server Name | Server Address | Server Type | Port | User Name | Upload Path |
|-------------|----------------|-------------|------|-----------|-------------|
| FTP         | 10.15.239      | FTP         | 21   | anonymous | /           |

Add FTP

Server Name  
Server Address  
Upload Path  
Port  
User Name  
Password  
Server Type

Example/Dir/folder  
21  
  
  
FTPS

OK Cancel

Add Modify Delete Test Save

2. Click “Edit and Test” and then click “Add” to add the information of the FTP. After that, click “Save” to save the settings.

**Server Name:** The name of the FTP server.

**Server Address:** The IP address or domain name of the FTP.

**Upload Path:** The directory where files will be uploaded to.

**Port:** The port of the FTP server.

**Username and Password:** The username and password that are used to login to the FTP server.

**Server Type:** FTP or FTPS

3. In the event setting interface (like motion detection, region intrusion, line crossing, etc.), trigger FTP as shown below.

☒ Trigger FTP

Server Name  
Server Address

☐ FTP 10.\*\*\*.\*\*\*.239 ☐ Attach Picture

Sub Storage Path&Name %a/MOTION/%4y-%2m-%2d/%h/MOTION\_%4y-%2m-%2d-%2h-%2s-%3u-%3l.\*

Reset Default Help

If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent to the FTP server address.

**Sub Storage Path& Name:** Click “Help” to view the rule and then set it as needed.

Meanings of the default Path & Name Settings (taking motion detection as an example):  
“%0a/MOTION/%4y-%2m-%2d/%h” stands for sub storage path  
“MOTION\_%4y-%2m-%2d-%2h-%2n-%2s-%3u-%3i.\* ” stands for file name  
When an motion alarm is triggered and “Trigger FTP” and “Attach Picture” are checked, a jpg file named “MOTION\_Year Month Day Hour Minute Second\_Event number” and a txt file named “MOTION\_Year Month Day Hour Minute Second\_Event number” will be generated under FTP root directory> MAC address>MOTION>Year-Month-Day>Hour  
“MOTION” refers to the event type. You can modify the event name as needed (for example: Motion). You can also change the display order and contents of the sub storage path and file name.  
If the sub storage path and name box is empty, the snapshot will be uploaded and named according to the default settings.  
If you only enter the file name rule, the snapshot will be uploaded to the root directory of the FTP server.

3.5.13 HTTP POST

Go to *Config* → *Network* → *HTTP POST*.

Push Protocol Version

V2

Push Type

☐ Push By Subscription ☒ Actively Push

Push By Subscription

Subscription Listening Port

8080

Actively Push

| Index | Enable | IP address/domain | Port | Path | Connection Status | Connection Type | Send Heartbeat | Heartbeat Interval (Second) | Smart Alarm Type |
|-------|--------|-------------------|------|------|-------------------|-----------------|----------------|-----------------------------|------------------|
|-------|--------|-------------------|------|------|-------------------|-----------------|----------------|-----------------------------|------------------|

Edit

Click “Edit” and then check “Enable”.

Push Protocol Version: Choose “V1” or “V2” as needed. It is recommended to use V2.

Push Type: “Push by Subscription” and/or “Actively Push” can be selected.

Push by Subscription: Push target trajectory (moving coordinate) to API test tool with a persistent connection. If enabled, the system will push the target trajectory upon detecting a target. If disabled, the system will push the target trajectory only when triggering a smart event (such as line crossing detection, region intrusion detection, etc.)

If the subscription listening port is occupied, you can modify it.

Actively Push: Click “Add” to add HTTP POST.

Protocol type: HTTP

Domain/IP: the IP address/domain name of the third-party platform.

Server port: the server port of the third-party platform.

Path: enter the subdomain of the above server, for example, the URL of alarm information push: “/SendAlarmStatus” .

Username and password: Please enable and enter as needed.

Connection Type: Choose persistent connection or short connection as needed.

Enable “Send heartbeat” and set heartbeat interval as needed. Check smart alarm data and type. After the above parameters are set, click “Save” to save the settings. Select one URL and click “Test” to test the connection of the URL. Then the camera will automatically connect to the third-party platform. The online state can be viewed in the above interface. After the camera is successfully connected, it will send the selected alarm data to the third-party platform once the selected smart alarm is triggered.

### 3.5.14 HTTPS

HTTPS provides authentication of the web site and protects user privacy.

Go to **Config** → **Network** → **HTTPS** as shown below.

☒ Enable

☐ Disable HTTP

Certificate installed

C=US, ST=Some-State, O=embeddedsoftware

Replace Certificate

Attribute

Issued to: C=US, ST=Some-State,  
O=embeddedsoftware, H=IPC,  
Issuer: C=US, ST=Some-State,  
O=embeddedsoftware, H=IPC,  
Validity date: 2024/10/21 16:38:58 ~  
2034/10/19 16:38:58

Save

There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via the web browser (e.g. https://192.168.226.201:443).

A private certificate can be created if users don't want to use the default one. Click "Replace Certificate" to change a certificate. Then the following interface will be displayed.

☒ Enable

☐ Disable HTTP

Installation type

☒ Have signed certificate, install directly

☐ Create a private certificate

☐ Create a certificate request

Install certificate

Select File No file selected

Install

Save

- \* If there is a signed certificate, click "Select File" to select it and then click "Install" to install it.
- \* Click "Create a private certificate" to enter the following creation interface.

☐ Enable

Installation type

☐ Have signed certificate, install directly

☒ Create a private certificate

☐ Create a certificate request

Create a private certificate

Create

Save

Click the "Create" button to create a private certificate. Enter the country (only two letters available), domain (camera's IP address/domain), validity date, password, province/state, region and so on. Then click "OK" to save the settings.

- \* Click "Create a certificate request" to enter the following interface.

☐ Enable  
 Installation type: ☐ Have signed certificate, install directly  
☐ Create a private certificate  
☒ Create a certificate request  
 Create a certificate request:     
 Install Created Certificate:

Click “Create” to create the certificate request. Then download the certificate request and submit it to the trusted certificate authority for signature. After receiving the signed certificate, import the certificate to the device.

### 3.5.15 NAT

If this function is enabled, the network camera can be quickly accessed by scanning the QR Code in mobile APP via WAN. In addition, you can also enter the visit address in the address bar of a web browser to log in the camera via WAN. Enable this function by going to **Config → Network → Cloud Service**.

☒ Enable  
 Visit Address:   
 Online State:    
   
 Please use the mobile client to scan the code to add a device  
 Security Code:   
 Required when adding to Account/Cloud device list

After the device is successfully bound, you can unbind it via APP (go to the server list of the APP and delete the device).

Note that after you bind the camera to your APP account, a verification code will be required when logging onto the web client by using the above-mentioned visit address.

### 3.5.16 QoS

QoS (Quality of Service) function is used to provide different quality of services for different network applications. With deficient bandwidth, the router or switch will sort the data streams and transfer them according to their priority to solve the network delay and network congestion by using this function.

Go to **Config → Network → QoS**.

|                  |                                 |
|------------------|---------------------------------|
| Video/Audio DSCP | <input type="text" value="13"/> |
| Alarm DSCP       | <input type="text" value="35"/> |
| Manager DSCP     | <input type="text" value="53"/> |

Video/Audio DSCP: The range is from 0 to 63.

Alarm DSCP: The range is from 0 to 63.

Manager DSCP: The range is from 0 to 63.

Generally speaking, the larger the number is, the higher the priority is.

### 3.5.17 Wi-Fi Settings

Go to **Config** → **Network** → **WIFI** as shown below.

☒ Enable

Wi-Fi Networks

Search

| Index | SSID      | Working Mode | Security Mode | Channel | Signal Intensity | Mbps | Connection Status |
|-------|-----------|--------------|---------------|---------|------------------|------|-------------------|
| 1     | HAMSA3    | Manage       | WPA2-personal | 2       | 58               | 150  | Unconnected       |
| 2     | APP-Test1 | Manage       | WPA2-personal | 11      | 51               | 150  | Unconnected       |

Wi-Fi

SSID

Test

Security Mode

WPA-personal

Key 1

Encryption Type

AES

1. Checkmark “Enable” to enable Wi-Fi.
  - Click “Search” to refresh the online wireless devices.
  2. Choose a wireless device on the list. The SSID and security mode of the wireless device will be shown automatically. Please don’t change it manually.
  3. Enter the key to connect the wireless device. This key should be set on the wireless device in advance for wireless network connection.
- After the above-mentioned wireless network is configured, you can choose “Obtain an IP address automatically” or “Use the following IP address”.

**LAN**

☒ Obtain an IP address automatically
 ☐ Use the following IP address

IP Address

Subnet Mask

Gateway

Preferred DNS Server

Alternate DNS Server

If you choose “Obtain an IP address automatically”, you shall get the IP address from the router. Or you can choose “Use the following IP address” to set the network parameters manually. Then you can use this IP address to log in mobile surveillance APP/ web client/CMS/NVR/...

## 3.6 Security Configuration

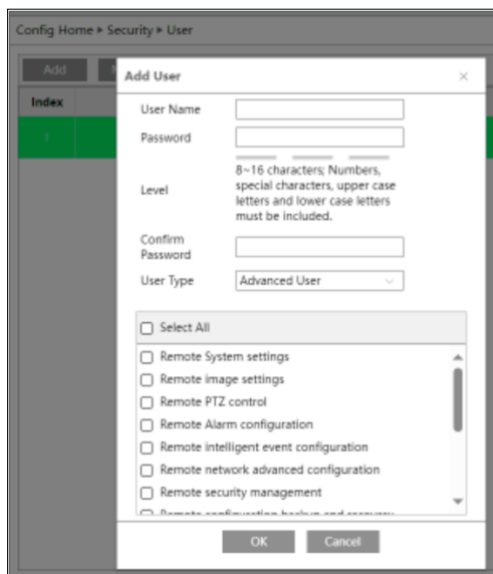
### 3.6.1 User Configuration

Go to *Config* → *Security* → *User* as shown below.

| Add Modify Delete Security Question |           |               |
|-------------------------------------|-----------|---------------|
| Index                               | User Name | User Type     |
| 1                                   | admin     | Administrator |

#### Add user:

1. Click the “Add” button to display the following textbox.



2. Enter username in the “User Name” textbox.
3. Enter the password in the “Password” and “Confirm Password” textbox. Please set the password according to the requirement of the password security level (Go to **Config→Security→Security Management→Password Security** to set the security level).
4. Choose the user type and select the desired user permissions.
5. Click the “OK” button and then the newly added user will be displayed in the user list.

### Modify user:

1. Select a user to modify password if necessary, in the user configuration list box.
2. The “Edit user” dialog box pops up by clicking the “Modify” button.

**Edit User**

User Name: admin

Old Password:

New Password: ☒

Level: 8~16 characters; Numbers, special characters, upper case letters and lower case letters must be included.

Confirm Password:

User Type: Administrator

Modify Onvif Password: ☒

☒ Select All

- ☒ Remote System settings
- ☒ Remote image settings
- ☒ Remote PTZ control
- ☒ Remote Alarm configuration
- ☒ Remote intelligent event configuration
- ☒ Remote network advanced configuration
- ☒ Remote security management
- ☒ Remote configuration backup and recovery

OK Cancel

3. Enter the old password of the user in the “Old Password” text box.
4. Enter the new password in the “New password” and “Confirm Password” text box.
5. For admin, you can check “Match Onvif password” when modifying the password as needed.
6. Select the user permissions for advanced or normal user.
7. Click the “OK” button to save the settings.

**Note:** When the password level is set to “Strong”, the password cannot be set the same as the previous five.

#### Delete user:

1. Select the user to be deleted in the user configuration list box.
2. Click the “Delete” button to delete the user.

**Note:** The default administrator account cannot be deleted.

**Safety Question Settings:** set the questions and answers for admin to reset the password after you forget the password.

### 3.6.2 Online User

Go to **Config**→**Security**→**Online User** to view the user who is viewing the live video.

| Index | Client Address | Port  | User Name        | User Type      | Video Stream |                          |
|-------|----------------|-------|------------------|----------------|--------------|--------------------------|
| 1     | 239.0.0.0      | 50554 | MulticastUser(s) | Anonymous User | 1            |                          |
| 2     | 172.19.18.44   | 50761 | admin            | Administrator  | 1            | <a href="#">KICK OUT</a> |

In addition, you can also view the number of video streams, IP address, user type, etc. An administrator user can kick out all the other users (including other administrators).

### 3.6.3 Block and Allow Lists

Go to *Config*→*Security*→*Block and Allow Lists* as shown below.

IP Address Filter Settings

☒ Enable address filtering

☒ Block the following address ☐ Allow the following address

Add

Delete

☒ IPv4 ☐ IPv6

Save

The setup steps are as follows:  
Check the “Enable address filtering” check box.  
Select “Block/Allow the following address”, IPv4/IPv6 and then enter IP address in the address box and click the “Add” button.

### 3.6.4 Security Management

Go to *Config*→*Security*→*Security Management* as shown below.

☒ Enable 'Illegal Login Lock' function

☐ Trigger Email

Logout Time

Seconds

Save

In order to prevent against malicious password unlocking, “Illegal Login Lock” function can be enabled here. If this function is enabled, login failure after trying five times will make the login interface locked. The camera can be logged in again after a half hour or after the camera reboots.  
Trigger Email: if enabled, e-mail will be sent when logging in/out or illegal login lock occurs.

- Password Security

|                  |                          |                |
|------------------|--------------------------|----------------|
| Security Service | <b>Password Security</b> | Authentication |
| Password Level   | Weak                     |                |
| Expiration Time  | Never                    |                |
|                  |                          | Save           |

Please set the password level and expiration time as needed.

Password Level: Weak, Medium or Strong.

Weak level: Numbers, special characters, upper- or lower-case letters can be used. You can choose one of them or any combination of them when setting the password.

Medium Level: 8~16 characters, including at least two of the following categories: numbers, special characters, upper case letters and lower-case letters.

Strong Level: 8~16 characters. Numbers, special characters, upper case letters and lower-case letters must be included.

For your account security, it is recommended to set a strong password and change your password regularly.

Authentication: you can set RTSP/HTTP authentication as needed.

|                                            |                   |                       |
|--------------------------------------------|-------------------|-----------------------|
| Security Service                           | Password Security | <b>Authentication</b> |
| <b>RTSP</b>                                |                   |                       |
| Authentication                             | Basic             |                       |
| <b>API Services</b>                        |                   |                       |
| <input checked="" type="checkbox"/> Enable |                   |                       |
| Authentication                             | Basic             |                       |
| <b>Subscribe to push services</b>          |                   |                       |
| Authentication                             | Basic             |                       |
|                                            |                   | Save                  |

RTSP Authentication: Digest or basic can be selected.

API Service Authentication: Digest or basic can be selected.

Push Subscription Authentication: Digest or basic can be selected.

## 3.7 Maintenance Configuration

### 3.7.1 Backup and Restore

Go to *Config* → *Maintenance* → *Backup and Restore*.

The screenshot displays a web-based configuration interface for a camera. It is divided into four main sections, each with a title bar and a corresponding button:

- Import Setting:** Contains a 'Path' label, a text input field with 'Select File' and 'No file selected' buttons, and an 'Import Setting' button.
- Export Settings:** Contains an 'Export Settings' button.
- Restore Default Parameters:** Contains a 'Keep' label and a list of three checkboxes: 'Network Config', 'Security Configuration', and 'Image Configuration'. Below the list is a 'Restore Default Parameters' button.
- Restore Factory Settings:** Contains a 'Restore Factory Settings' button.

### ● Import & Export Settings

Configuration settings of the camera can be exported from a camera into another camera.

1. Click “Browse” to select the save path for import or export information on the PC.
2. Click the “Import Setting” or “Export Setting” button.

**Note:** \*The login password needs to be entered after clicking the “Import Setting” button.

\* The customized audio files are not supported to export or importing.

### ● Restore Default Parameters

Click the “Restore Default Parameters” button and then verify the password to restore all parameters to the default parameters except those you want to keep.

### ● Restore Factory Settings

Click the “Restore Factory Settings” button and then verify the password to restore all system settings to the default factory settings.

## 3.7.2 Reboot

Go to *Config* → *Maintenance* → *Reboot*.

Click the “Reboot” button and then enter the password to reboot the device.

### Timed Reboot Setting:

If necessary, the camera can be set up to reboot on a time interval. Enable “Time Settings”, set the date and time, click the “Save” button and then enter the password to save the settings.

### 3.7.3 Upgrade

Go to **Config → Maintenance → Upgrade**. In this interface, the camera firmware can be updated.

#### ● Local Upgrade

1. Click the “Select File” button to select the save path of the upgrade file.
2. Click the “Upgrade” or “Back up and upgrade” button to start upgrading the firmware.
3. Enter the correct password and then the device will restart automatically.

**Note:** If “Back up and upgrade” is selected, the configuration file will be exported to your local PC before starting upgrading.

#### ● Cloud Upgrade

**Note:** Before you use cloud upgrade, please make sure the cloud service is enabled successfully. After the cloud server pushes the latest version, you can upgrade the camera by itself or NVR.

1. Go to **Config → Maintenance → Upgrade**.
2. Select “Notify Only” in the cloud upgrade options or click “Manual Check” to check whether the current version is the latest. If your software version is not the latest, click “Upgrade” to download and upgrade from the cloud server.

#### Caution:

1. You cannot downgrade to a lower version.
2. Do not refresh/close the browser or disconnect the camera from the network during the upgrade, or it will cause system failure. After the device is successfully upgraded, there are ten minutes of observation. During this observation period, do not upgrade the device again.

**Note:** To decrease the upgrade risk, this series of cameras adopts two systems. After one system is successfully upgraded, the other system will be synchronized. If one system fails caused by power failure or other reasons during the upgrade, the other system will not be affected, and the camera still can work normally. You can also upgrade your camera through the normal system.

**Export Upgrade Log:** If upgrade error occurs, the upgrade log can be exported to help the technician to analyze and solve the problem.

### 3.7.4 Operation Log

To query and export log:

1. Go to **Config**→**Maintenance**→**Operation Log**.

Main Type

Sub Type

Start Time

End Time

| Index | Time               | Main Type | Sub Type | User Name | Login IP   | Hostname |
|-------|--------------------|-----------|----------|-----------|------------|----------|
| 1     | 2021-09-06 03:1... | Operation | Log in   | admin     | 10.20.52.7 |          |
| 2     | 2021-09-06 03:1... | Operation | Log in   | admin     | 10.20.52.7 |          |

2. Select the main type, sub type, start and end time.
3. Click “Search” to view the operation log.
4. Click “Export” to export the operation log.

### 3.7.5 Serial Output

Serial output mode is used to record and collect the required system data, so that the technician can quickly find out and analyze the problem and help us to improve service.  
Before enabling the mode, you are advised to consult our technical support.

☒ Enable

Debug Level

### 3.7.6 Maintenance Information

When the device failure occurs, you can export the maintenance information and send it to the technicians, so that they can quickly find out and analyze the problem. Go to **Config**→**Maintenance Information** to export.

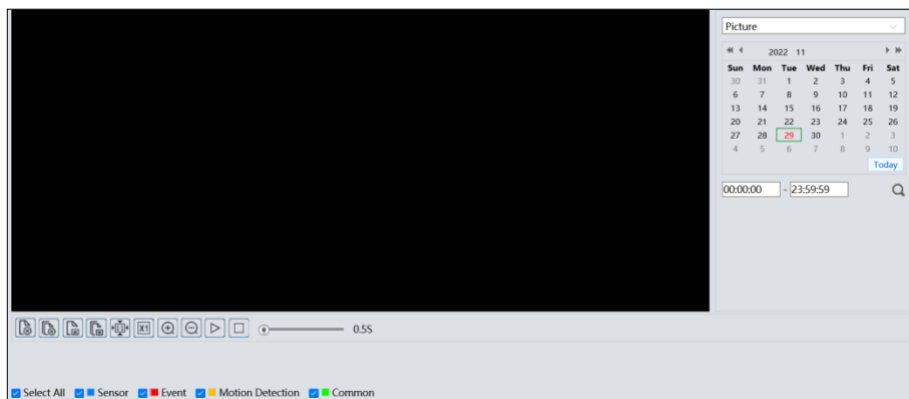
## 4 Search

## 4.1 Image Search

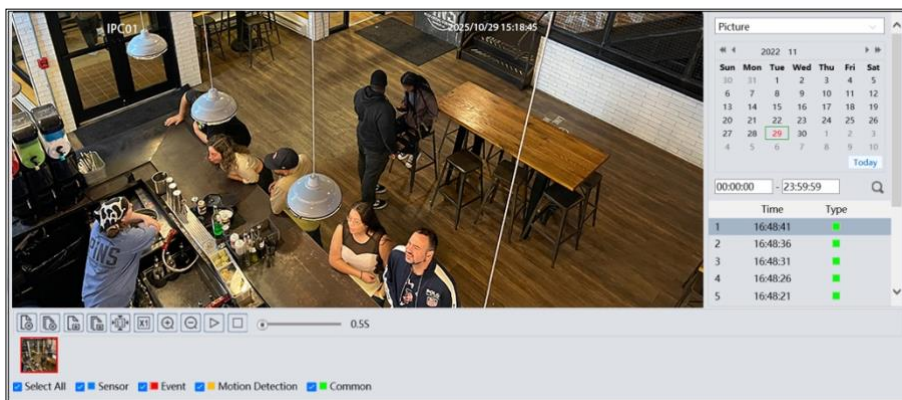
Click Search to go to the interface as shown below. Images that are saved on the SD card can be found here.

### ● SD Card Image Search

1. Choose "Picture".



2. Set time: Select date and choose the start and end time.
3. Choose the alarm events at the bottom of the interface.
4. Click  to search the images.
5. Double click a file name in the list to view the captured photos.



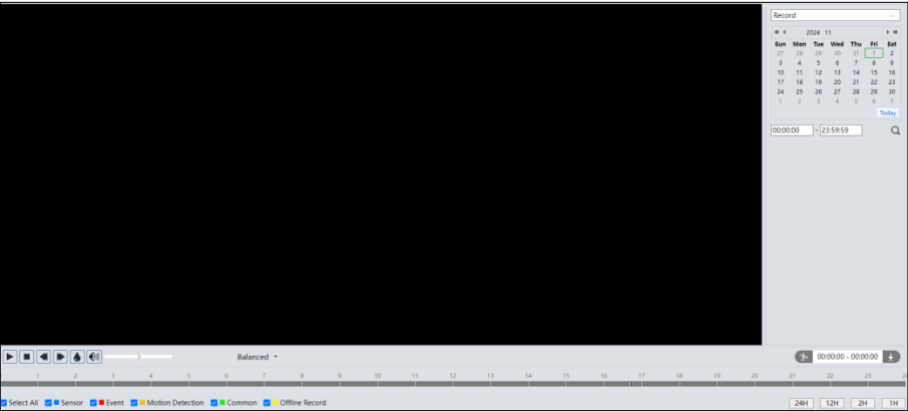
The descriptions of the buttons are shown as follows.

| Icon | Description                                                                | Icon                                      | Description                                                                       |
|------|----------------------------------------------------------------------------|-------------------------------------------|-----------------------------------------------------------------------------------|
|      | Close: Select an image and click this button to close the image.           |                                           | Close all: Click this button to close all images.                                 |
|      | Save: Click this button to select the path for saving the image on the PC. |                                           | Save all: Click this button to select the path for saving all pictures on the PC. |
|      | Fit size: Click to fit the image on the screen.                            |                                           | Actual size: Click this button to display the actual size of the image.           |
|      | Zoom in: Click this button to digitally zoom in.                           |                                           | Zoom out: Click this button to digitally zoom out.                                |
|      | Slide show play: Click this button to start the slide show mode.           |                                           | Stop: Click this button to stop the slide show.                                   |
|      |                                                                            | Play speed: Play speed of the slide show. |                                                                                   |

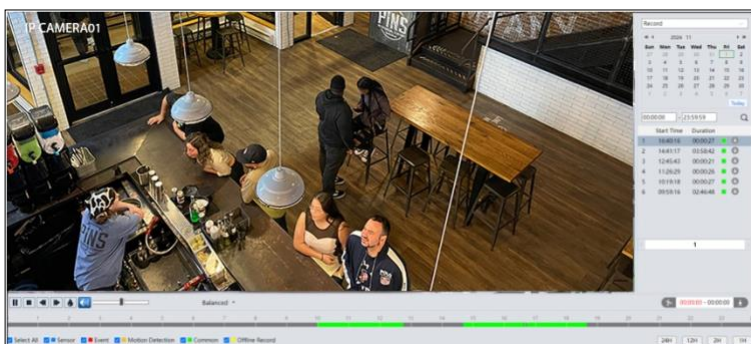
4.2 Video Search

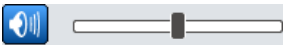
Click Search to go to the interface as shown below. Videos that were recorded on the SD card can be played in this interface.

- 1. Choose “Record”.
- 2. Set search time: Select the date and choose the start and end time.
- 3. Click to search the images.



- 4. Select the alarm events at the bottom of the interface.
- 5. Double click on a file name in the list to start playback.



| Icon                                                                              | Description                                                                        | Icon                                                                              | Description       |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-------------------|
|  | Play button. After pausing the video, click this button to continue playing.       |  | Pause button      |
|  | Stop button                                                                        |  | Speed down        |
|  | Speed up                                                                           |  | Watermark display |
|  | Enable / disable audio; drag the slider to adjust the volume after enabling audio. |                                                                                   |                   |

**Note:**  and  cannot be displayed in the above interface via the plug-in free browser. Additionally, for plug-in free playback, playback mode switch (balanced/real-time/fluent mode) and downloading functions are not supported too.

The time table can be shown in 24H/12H/2H/1H format by clicking the corresponding buttons.

### Video clip and downloading

1. Search the video files according to the above mentioned steps.
2. Select the start time by clicking on the timetable.
3. Click  to set the start time and then this button turns blue (  ).
4. Select the end time by clicking on the time table. Then click  to set the end time.
5. Click  to download the video file to the PC.



# Appendix

## Appendix 1 Troubleshooting

### How to find the password?

- A: The password for **admin** can be reset through “Edit Safety Question” function. Click “Forget Password” in the login window and then enter the corresponding answer of the selected question in the popup window. After you correctly answer all questions, you can reset the password for **admin**. If you forget the answer of the question, this way will be invalid, please contact your dealer for help.
- B: The passwords of other users can be reset by **admin**.

### Fail to connect devices through a web browser.

- A: Network is not well connected. Check the connection and make sure it is connected well.
- B: IP address is not available. Reset the IP address.
- C: Web port number has been changed: contact administrator to get the correct port number.
- D: Exclude the above reasons. Restore to default setting by IP-Tool.

### IP tool cannot search devices.

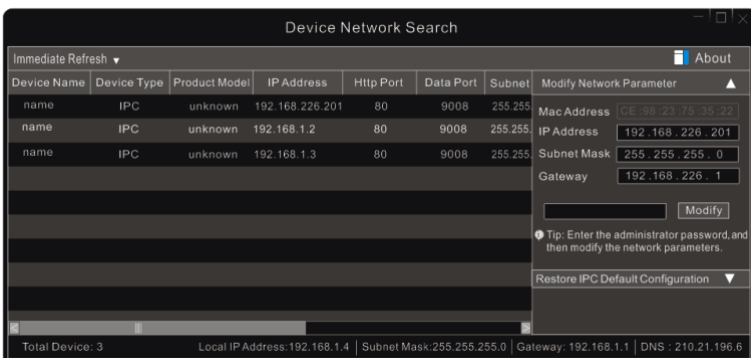
It may be caused by the anti-virus software in your computer. Please exit it and try to search device again.

### No sound can be heard.

- A: Audio input device is not connected. Please connect and try again.
- B: Audio function is not enabled at the corresponding channel. Please enable this function.

### How to modify IP address through IP-Tool?

- A: After you install the IP-Tool, run it as shown below.



The default IP address of this camera is DHCP. You can find your device by its MAC address. Click the information of the camera listed in the above table to show the network information on the right hand. Modify the IP address and gateway of the camera and make sure its network address is in the same local network segment as the computer's. Please modify the IP address of your device according to the practical situation.

Modify Network Parameter ▲

Mac Address

IP Address

Subnet Mask

Gateway

●●●●●

Modify

For example, the IP address of your computer is 192.168.1.4. So, the IP address of the camera shall be changed to 192.168.1.X. After modification, please enter the password of “admin” which is set in the device activation interface in advance and then click the “Modify” button to change the network parameters.

How to restore to factory default setting through IP-Tool?

- A: Drag the slider at the bottom of the device list to the right and then the MAC address of the searched devices will be viewed. Find the MAC address of the IPC you want to restore to the factory default setting, click ▼ next to “Restore IPC Default Configuration” to expand the menu, then enter the MAC address and click “OK”. After that, manually reboot your camera within 30s. Then the camera will successfully restore to the factory default setting

Device Network Search

Immediate Refresh ▼ About

| Device Name | Device Type | Product Model | IP Address      | Http Port | Data Port | Subnet  | Modify Network Parameter ▲                                                     |
|-------------|-------------|---------------|-----------------|-----------|-----------|---------|--------------------------------------------------------------------------------|
| name        | IPC         | unknown       | 192.168.226.201 | 80        | 9008      | 255.255 | Mac Address <input type="text" value="CE:98:23:75:35:22"/>                     |
| name        | IPC         | unknown       | 192.168.1.2     | 80        | 9008      | 255.255 | IP Address <input type="text" value="192.168.226.201"/>                        |
| name        | IPC         | unknown       | 192.168.1.3     | 80        | 9008      | 255.255 | Subnet Mask <input type="text" value="255.255.255.0"/>                         |
|             |             |               |                 |           |           |         | Gateway <input type="text" value="192.168.226.1"/>                             |
|             |             |               |                 |           |           |         | <div><div></div><div>Modify</div></div>                                        |
|             |             |               |                 |           |           |         | Tip: Enter the administrator password, and then modify the network parameters. |
|             |             |               |                 |           |           |         | Restore IPC Default Configuration ▼                                            |

Total Device: 3

Local IP Address: 192.168.1.4 | Subnet Mask: 255.255.255.0 | Gateway: 192.168.1.1 | DNS : 210.21.196.6

When configuring the network through the APP for the first time, you cannot log in via web by manually entering the IP address.

- A. If it happens, you can double click the device information listed in the IP Tool to open the

web browser and then log in.

## Detailed Specifications: VTC-TNC4FW-2

|                         |                                                                                                               |
|-------------------------|---------------------------------------------------------------------------------------------------------------|
| Image Sensor            | 1/3" Progressive Scan CMOS                                                                                    |
| Image Size              | 2560×1440                                                                                                     |
| Electronic Shutter      | 1/3s ~ 1/100000s                                                                                              |
| Iris Type               | Fixed IRIS                                                                                                    |
| Min. Illumination       | 0.0035 lux @F1.2, AGC ON (Color) / 0 lux with IR On (B&W)                                                     |
| Lens                    | 2.1mm @F2.1 / Horizontal FoV: 137°                                                                            |
| WDR                     | 78dB                                                                                                          |
| BLC                     | Yes                                                                                                           |
| HLC                     | Yes                                                                                                           |
| Defog                   | No                                                                                                            |
| DNR                     | 2D/3D NR                                                                                                      |
| Angle Adjustment        | Pan: 0°~230°; Tilt: 0°~71°; Rotate: 0°~360°                                                                   |
| Main Stream Compression | H.265+/H.265/H.264+/H.264                                                                                     |
| Sub Stream Compression  | H.265+/H.265/H.264+/H.264/MJPEG                                                                               |
| H.264 Compression       | Baseline/Main/High Profile                                                                                    |
| Bit Rate Type           | VBR/CBR                                                                                                       |
| Bit Rate                | 64Kbps ~ 6Mbps                                                                                                |
| Resolution              | 4MP (2560×1440), 3MP (2304×1296), 1080P (1920×1080), 720P(1280×720), D1, VGA (640×480), 640×360, 480×240, CIF |
| Main Stream             | 60Hz: 4MP/3MP/1080P/720P (1~30fps); 50Hz: 1~25fps                                                             |
| Sub Stream              | 720P/D1/VGA/640×360/480×240/CIF (60Hz:1~30fps; 50Hz: 1~25fps)                                                 |
| Image Settings          | Saturation, Hue, Brightness, Contrast, WDR, Sharpness, NR, Flip                                               |
| ROI                     | 8 configurable regions                                                                                        |
| Audio Compression       | G711A/U                                                                                                       |
| Wi-Fi                   | 2.4GHz (IEEE 802.11 b/g/n), Up to 165' range                                                                  |
| APP WiFi Config         | QR Code                                                                                                       |
| Snapshot                | Yes                                                                                                           |
| Recording               | Yes                                                                                                           |
| Two-Way Audio           | Yes                                                                                                           |

## Detailed Specifications Cont'd: VTC-TNC4FW-2

|                         |                                                                                                                  |
|-------------------------|------------------------------------------------------------------------------------------------------------------|
| Storage                 | Built-in microSD slot, up to 256GB                                                                               |
| Network Interface       | 100M RJ45                                                                                                        |
| Audio                   | Built-in Mic x1, Speaker x1 (Echo Cancellation Supported)                                                        |
| Alarm                   | 1CH input, 1CH output                                                                                            |
| Reset Button            | Yes                                                                                                              |
| PIR                     | 17' Range / 100° Horizontal angle                                                                                |
| Remote Monitoring       | Web client / Mobile App                                                                                          |
| Simultaneous Users      | Up to 4                                                                                                          |
| Network Protocol        | UDP, IPv4/6, DHCP, NTP, RTSP, PPPoE, DDNS, SMTP, SNMP, FTP, 802.1x, UPnP, HTTPS, HTTP, HTTP POST, RTMP, QoS, P2P |
| Interface Protocol      | ONVIF                                                                                                            |
| Smart Alarm             | Motion, PIR, Audio, Sensor, Person, SD Full/Error, IP Conflict, Cable Disconnect, Video Exception                |
| Analytics               | Line Crossing Detection, Region Intrusion Detection (Human/Vehicle Classification)                               |
| General Function        | Watermark, IP Filtering, Video Mask, Illegal Login Lock, Disarming, Cloud Upgrade, ANR                           |
| Security                | Video/Firmware/Config Encryption, HTTPS, 802.1x, IP Filtering, Digest Authentication                             |
| IR Range                | Up to 33'                                                                                                        |
| Water-proof             | No                                                                                                               |
| PoE                     | Yes (IEEE 802.3af)                                                                                               |
| Power                   | DC12V / PoE                                                                                                      |
| Power Consumption       | <5W                                                                                                              |
| Power Supply (Included) | 12VDC @ 1.5A (UL Listed)                                                                                         |
| Certifications          | RoHS 2.0, REACH, WEEE, Directive 94/62/EC                                                                        |
| Operating Temp          | -4°F~122°F (-20°C~50°C), <95% RH                                                                                 |
| Dimensions              | 5.11" x 2.8" x 2.8" (130 x 71.1 x 71.7mm)                                                                        |
| Weight                  | 4.93oz / 0.3lbs / 0.14kg                                                                                         |

*\*Please research local, state and federal laws regarding the implementation of audio surveillance.*



**OPTIONAL ACCESSORIES AND  
RELATED PRODUCTS FOR  
NDAA COMPLIANT  
TRANSCENDENT IP CAMERAS**

# **TRANSCENDENT NVRs: Professional Recording Solutions for Every Installation**

*Transcendent PN and PFN Series Recorders deliver professional-grade performance with seamless plug-and-play installation, integrated PoE, and advanced GEN IV Analytics. From 4 to 32 channels, each NVR provides reliable 4K recording, full remote access, and intuitive control via the Transcendent VMS 2.0 software and mobile apps.*



**4K  
8MP**



- **4K HDMI Output | H.265S / H.265+ Compression**
- **Built-in PoE Switch (4 / 8 / 16 Ports)**
- **GEN IV Analytics with Face Detection & LPR (PFN Models)**
- **Fisheye De-Warping via Web & App (PFN Models)**
- **Free Transcendent VMS for Multi-Site Management**
- **iOS & Android Apps + Mac Remote Viewing**
- **3-Year Warranty NDAA Compliant**

VT-TNR414PN  
VT-TNR818PN



VT-TNR1626PN



VT-TNR818PFN  
VT-TNR1646PFN



VT-TNR3216PFN



**An Eye On  
Innovation**

## Also Consider Vitek's Next Generation of Smart Home Products Integrated with the Transcendent Platform!

**Secure entryways and access points with the VITEK OnAlert Series High Definition Four MegaPixel NDAA Compliant IP Doorbell Camera.**



Fully designed for the Transcendent Platform, this model offers native integration with recorders, mobile apps, and the Transcendent VMS for seamless setup, control, and video management. Featuring a square 1:1 aspect ratio and wide-angle view, it delivers enhanced **Face Detection** and Intelligent Face Capture with tracking and scoring. **Dual-band Wi-Fi** provides improved stability, and support for wired mechanical, electronic, and wireless chimes ensures flexible installation. Ideal for residential and small business deployments.

# LIMITED PRODUCT WARRANTY

This VITEK product carries a three (3) year limited warranty. VITEK warrants to the purchaser that products manufactured by VITEK are free of any rightful claim of infringement or the like, and when used in the manner intended, will be free of defects in materials and workmanship for a period of three (3) years, or as otherwise stated above, from the date of purchase by the end user. This warranty is nontransferable and extends only to the original buyer or end user customer of a VITEK Authorized Reseller.

The product must have been used only for its intended purpose, and not been subjected to damage by misuse, willful or accidental damage, caused by excessive voltage or lightning.

The product must not have been tampered with in any way or the guarantee will be considered null and void.

This guarantee does not affect your statutory rights.

Contact your local VITEK Reseller should servicing become necessary.

VITEK makes no warranty or guarantee whatsoever with respect to products sold or purchased through unauthorized sales channels. Warranty support is available only if product is purchased through a VITEK Authorized Reseller.

## **CLASS A DIGITAL DEVICE (INDUSTRIAL & COMMERCIAL ENVIRONMENT)**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to CE and FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. 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.



28492 CONSTELLATION ROAD VALENCIA, CA 91355  
WWW.VITEKCCTV.COM