Network Camera

User Manual

About this Manual

This Manual is applicable to Network Camera (V5.3.2).

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website.

Please use this user manual under the guidance of professionals.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS", WITH ALL FAULTS AND ERRORS, AND OUR COMPANY MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL OUR COMPANY, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF OUR COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY

TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. OUR COMPANY SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Regulatory Information

FCC Information

FCC compliance: This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. 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.

FCC Conditions

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

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

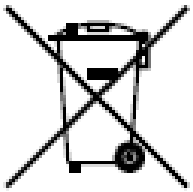
EU Conformity Statement

CE

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable

harmonized European standards listed under the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Safety Instruction

These instructions are intended to ensure that the user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into ‘Warnings’ and ‘Cautions’:

Warnings: Serious injury or death may be caused if any of these warnings are neglected.

Cautions: Injury or equipment damage may be caused if any of these cautions are neglected.

Warnings Follow these safeguards to prevent serious injury or death.	**Cautions** Follow these precautions to prevent potential injury or material damage.

Warnings:

- Please adopt the power adapter which can meet the safety extra low voltage (SELV) standard. And source with 12 VDC or 24 VAC (depending on models) according to the IEC60950-1 and Limited Power Source standard.
- To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture.
- This installation should be made by a qualified service person and should conform to all the local codes.
- Please install blackouts equipment into the power supply circuit for convenient supply interruption.
- Please make sure that the ceiling can support more than 50(N) Newton gravities if the camera is fixed to the ceiling.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

Cautions:

- Make sure the power supply voltage is correct before using the camera.
- Do not drop the camera or subject it to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use a clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the lens cap to protect the sensor from dirt.
- Do not aim the camera lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the camera.
- The sensor may be burned out by a laser beam, so when any laser equipment is being used, make sure that the surface of the sensor not be exposed to the laser beam.
- Do not place the camera in extremely hot, cold temperatures (the operating temperature should be between -30°C ~ 60°C, or -40°C ~ 60°C if the camera model has an "H" in its suffix), dusty or damp environment, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, good ventilation is required for a proper operating environment.
- Keep the camera away from water and any liquid.
- While shipping, the camera should be packed in its original packing.
- Improper use or replacement of the battery may result in hazard of explosion. Please use the manufacturer recommended battery type.

Notes:

For the camera supports IR, you are required to pay attention to the following precautions to prevent IR reflection:

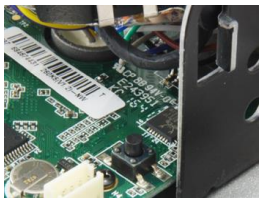
- Dust or grease on the dome cover will cause IR reflection. Please do not remove the dome cover film until the installation is finished. If there is dust or grease on the dome cover, clean the dome cover with clean soft cloth and isopropyl alcohol.
- Make certain the installation location does not have reflective surfaces of objects too close to the camera. The IR light from the camera may reflect back into the lens causing reflection.
- The foam ring around the lens must be seated flush against the inner surface of the bubble to isolate the lens from the IR LEDS. Fasten the dome cover to camera body so that the foam ring and the dome cover are attached seamlessly.

• MicroSD Card Slot & RESET Button

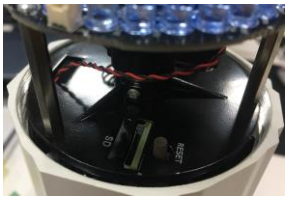
Unscrew the microSD/RESET/ Cover, and you can see the RESET button and the microSD card slot. Press RESET about 10s when the camera is powering on or rebooting to restore the default settings, including the user name, password, IP address, port No., etc.

Reset Button & SD card Slot Position

FCS-5058	FCS-5067



FCS-3084	FCS-3073	FCS-3085	FCS-3086
FCS-3090	FCS-3096	FCS-3087	



FCS-5059	FCS-5060	FCS-5068

FCS-4103

FCS-3097	FCS-3098	FCS-4203

FCS-5092	FCS-5093

FCS-5094	FCS-5095	FCS-5096

Table of Contents

Chapter 1 System Requirement *12*

Chapter 2 Network Connection *13*

2.1 Setting the Network Camera over the LAN **13**

2.1.1 Wiring over the LAN 13

2.1.2 Creating a Password 14

2.2 Setting the Network Camera over the WAN **18**

2.2.1 Static IP Connection 18

2.2.2 Dynamic IP Connection 19

Chapter 3 Access to the Network Camera *22*

3.1 Accessing by Web Browsers **22**

Chapter 4 Wi-Fi Settings *25*

4.1 Configuring Wi-Fi Connection in Manage and Ad-hoc Modes **25**

4.2 Easy Wi-Fi Connection with WPS function **30**

4.3 IP Property Settings for Wireless Network Connection **32**

Chapter 5 Live View *34*

5.1 Live View Page **34**

5.2 Starting Live View **35**

5.3 Recording and Capturing Pictures Manually **36**

5.4 Operating PTZ Control **36**

5.4.1 PTZ Control Panel 36

5.4.2 Setting / Calling a Preset 37

5.4.3 Setting / Calling a Patrol 39

Chapter 6 Network Camera Configuration *40*

6.1 Configuring Local Parameters **40**

6.2 Configuring Time Settings **42**

6.3 Configuring Network Settings **44**

6.3.1 Configuring TCP/IP Settings 44

6.3.2 Configuring Port Settings 45

6.3.3 Configuring PPPoE Settings 46

6.3.4 Configuring DDNS Settings 47

6.3.5 Configuring SNMP Settings 49

6.3.6 Configuring 802.1X Settings 51

6.3.7 Configuring QoS Settings 52

6.3.8 Configuring UPnP™ Settings 53

6.3.9 Configuring Wireless Dial Settings 53

6.3.10 Email Sending Triggered by Alarm 56
6.3.11 Configuring NAT (Network Address Translation) Settings 58
6.3.12 Configuring FTP Settings 59
6.3.13 Platform Access 60
6.3.14 HTTPS Settings 61
6.4 Configuring Video and Audio Settings 63
6.4.1 Configuring Video Settings 63
6.4.2 Configuring Audio Settings 66
6.4.3 Configuring ROI Encoding 67
6.4.4 Display Information on Stream 69
6.4.5 Configuring Target Cropping 69
6.5 Configuring Image Parameters 70
6.5.1 Configuring Display Settings 70
6.5.2 Configuring OSD Settings 76
6.5.3 Configuring Text Overlay Settings 77
6.5.4 Configuring Privacy Mask 78
6.5.5 Configuring Picture Overlay 79
6.6 Configuring and Handling Basic Events 80
6.6.1 Configuring Motion Detection 80
6.6.2 Configuring Video Tampering Alarm 87
6.6.3 Configuring Alarm Input 88
6.6.4 Configuring Alarm Output 89
6.6.5 Handling Exception 90
6.6.6 Configuring Other Alarm 91
6.7 Configuring and Handling Smart Events 94
6.7.1 Configuring Audio Exception Detection 94
6.7.2 Configuring Defocus Detection 96
6.7.3 Configuring Scene Change Detection 96
6.7.4 Configuring Face Detection 97
6.7.5 Configuring Line Crossing Detection 99
6.7.6 Configuring Intrusion Detection 101
6.7.7 Configuring Region Entrance Detection 103
6.7.8 Configuring Region Exiting Detection 104
6.7.9 Configuring Unattended Baggage Detection 105
6.7.10 Configuring Object Removal Detection 107
6.8 VCA Configuration 109
6.8.1 Behavior Analysis 109
6.8.2 Face Capture 116
6.8.3 People Counting 119
6.8.4 Heat Map 122
6.8.5 Counting 125
Chapter 7 Storage Settings 129

7.1 Configuring NAS Settings 129
7.2 Configuring Recording Schedule 131
7.3 Configuring Snapshot Settings 135
7.4 Configuring Lite Storage 137
7.5 Configuring Cloud Storage 138
Chapter 8 Road Traffic 140
Chapter 9 Playback 144
Chapter 10 Log Searching 146
Chapter 11 Others 148
11.1 Managing User Accounts 148
11.2 Authentication 150
11.3 Anonymous Visit 151
11.4 IP Address Filter 152
11.5 Security Service 153
11.6 Viewing Device Information 154
11.7 Maintenance 155
11.7.1 Rebooting the Camera 155
11.7.2 Restoring Default Settings 155
11.7.3 Exporting / Importing Configuration File 156
11.7.4 Upgrading the System 157
11.8 RS-232 Settings 157
11.9 RS-485 Settings 158
11.10 Service Settings 159
Appendix 160
Appendix 1 SADP Software Introduction 160
Appendix 2 Port Mapping 163

Chapter 1 System Requirement

Operating System: Microsoft Windows XP SP1 and above version / Vista / Win7 / Server 2003 / Server 2008 32bits

CPU: Intel Pentium IV 3.0 GHz or higher

RAM: 1G or higher

Display: 1024×768 resolution or higher

Web Browser: Internet Explorer 6.0 and above version, Apple Safari 5.02 and above version, Mozilla Firefox 3.5 and above version and Google Chrome8 and above version.

Chapter 2 Network Connection

Note:

- You shall acknowledge that the use of the product with Internet access might be under network security risks. For avoidance of any network attacks and information leakage, please strengthen your own protection. If the product does not work properly, please contact with your dealer or the nearest service center.
- To ensure the network security of the network camera, we recommend you to have the network camera assessed and maintained termly. You can contact us if you need such service.

Before you start:

- If you want to set the network camera via a LAN (Local Area Network), please refer to *Section 2.1* ***Setting the Network Camera over the LAN***.
- If you want to set the network camera via a WAN (Wide Area Network), please refer to *Section 2.2* ***Setting the Network Camera over the WAN***.

2.1 Setting the Network Camera over the LAN

Purpose:

To view and configure the camera via a LAN, you need to connect the network camera in the same subnet with your computer, and install the SADP or iVMS-4200 software to search and change the IP of the network camera.

Note: For the detailed introduction of SADP, please refer to Appendix 1.

2.1.1 Wiring over the LAN

The following figures show the two ways of cable connection of a network camera and a computer:

Purpose:

- To test the network camera, you can directly connect the network camera to the computer with a network cable as shown in Figure 2-1.

- Refer to the Figure 2-2 to set network camera over the LAN via a switch or a router.

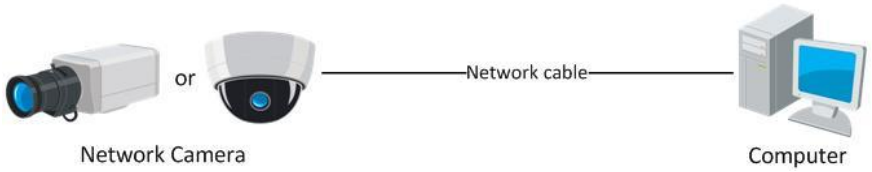


Figure 2-1 Connecting Directly

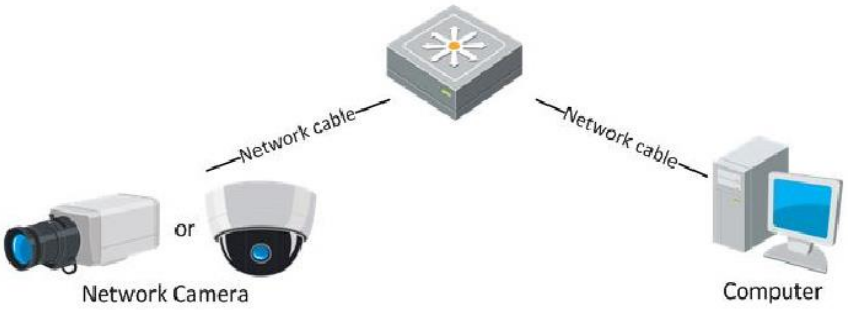


Figure 2-2 Connecting via a Switch or a Router

2.1.2 Creating a Password

You are required to activate the camera first by setting a strong password for it before you can use the camera.

Creating a Password via Web Browser, Creating a Password via SADP, and Creating a Password via Client Software are all supported.

❖ Creating a Password via Web Browser

Steps:

1. Power on the camera, and connect the camera to the network.

2. Input the IP address into the address bar of the web browser, and click Enter to enter the activation interface.

Notes:

- The default IP address of the camera is 192.168.1.64.
- For the camera enables the DHCP by default, the IP address is allocated automatically. And you need to activate the camera via SADP software. Please refer to the following chapter for Activation via SADP.

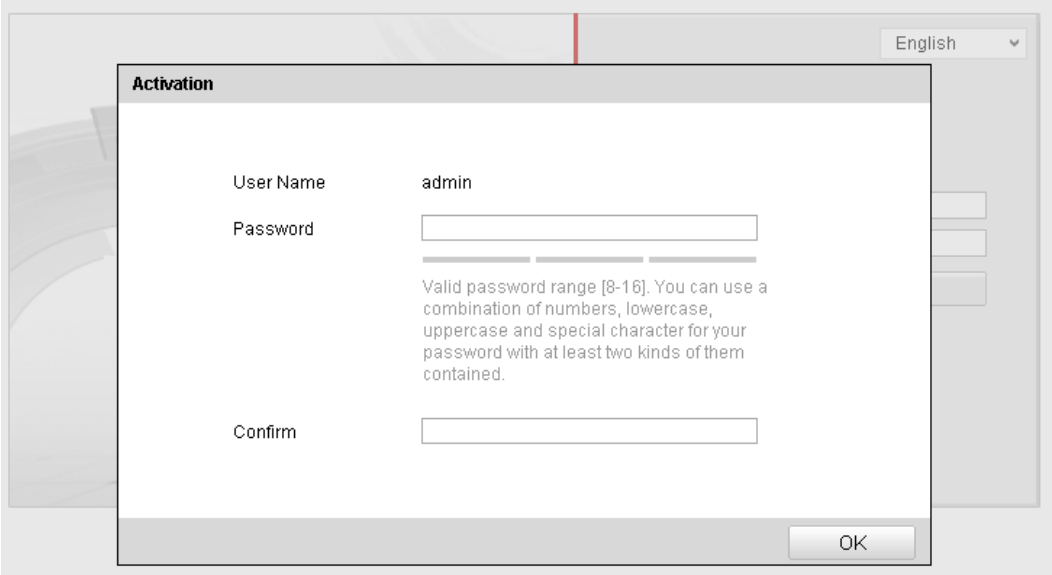


Figure 2-3 Creating a Password via Web Browser

3. Create a password and input the password into the password field.

STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Confirm the password.

5. Click OK to save the password and enter the live view interface.

❖ Creating a Password via SADP Software

SADP software is used for detecting the online device, activating the camera, and resetting the password.

Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts. Follow the steps to activate the camera.

Steps:

1. Run the SADP software to search the online devices.

2. Check the device status from the device list, and select the inactive device.

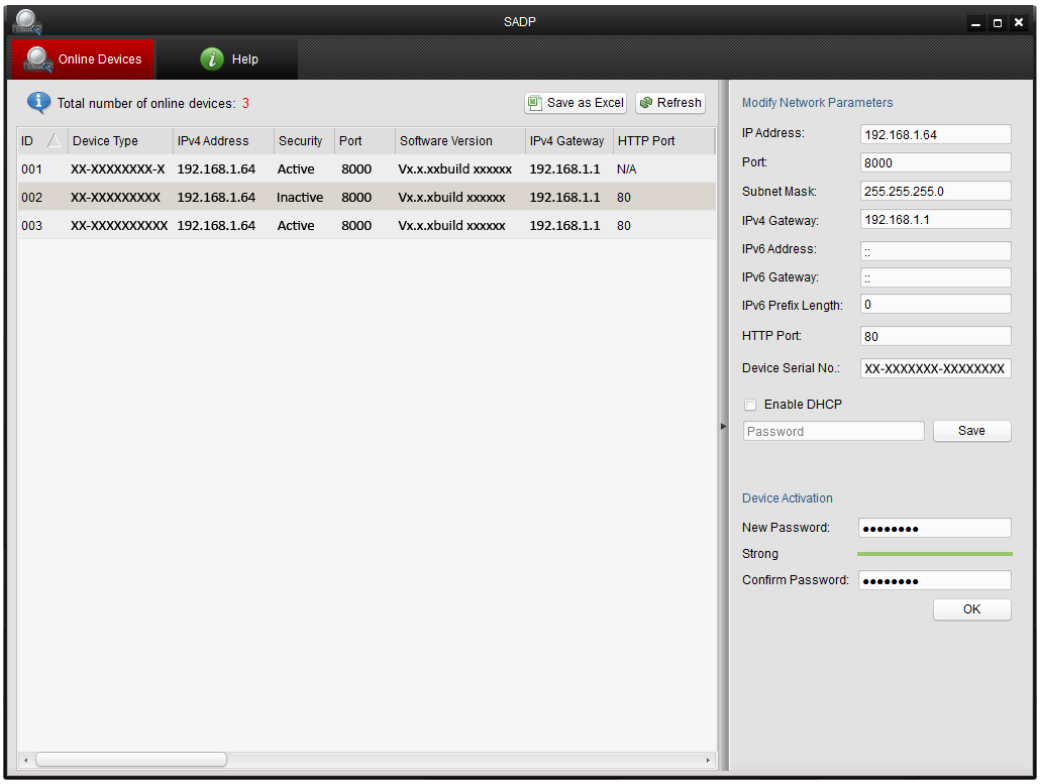


Figure 2-4 SADP Interface

3. Create a password and input the password in the password field, and confirm the password.

STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **OK** to save the password.

You can check whether the activation is completed on the popup window. If activation failed, please make sure that the password meets the requirement and try again.

5. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

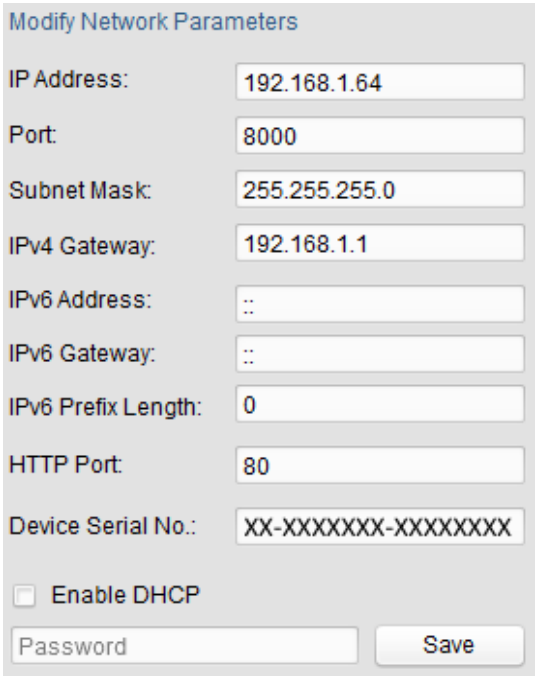


Figure 2-5 Modify the IP Address

6. Input the password and click the **Save** button to activate your IP address modification.

Figure 2-6 Creating a Password via Client Software

1. Click **OK** button to start activation.
2. Click the Modify Netinfo button to pop up the Network Parameter Modification interface, as shown in the figure below.

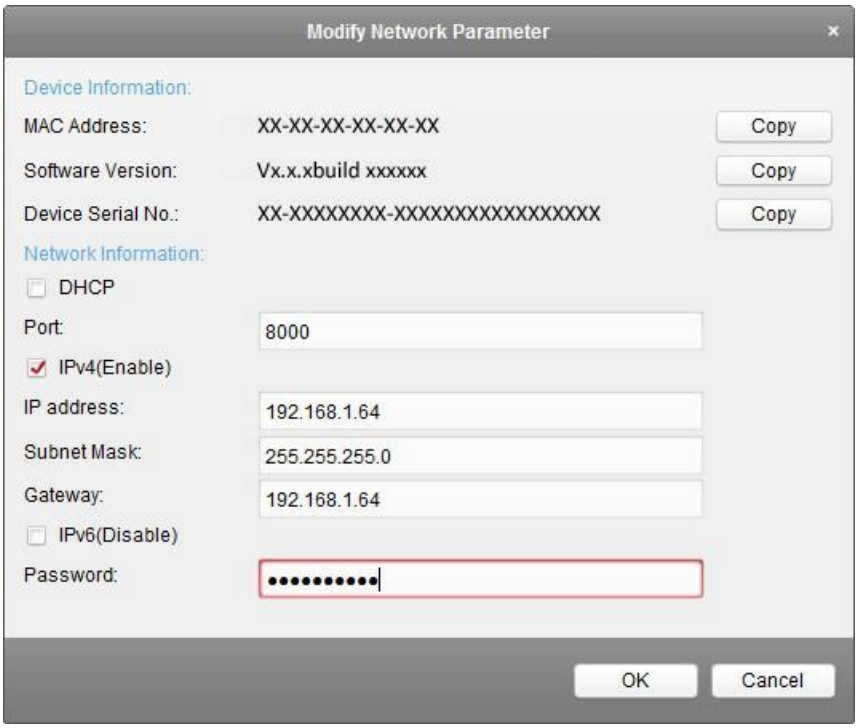


Figure 2-7 Modifying the Network Parameters

3. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

4. Input the password to activate your IP address modification.

2.2 Setting the Network Camera over the WAN

Purpose:

This section explains how to connect the network camera to the WAN with a static IP or a dynamic IP.

2.2.1 Static IP Connection

Before you start:

Please apply a static IP from an ISP (Internet Service Provider). With the static IP address, you can connect the network camera via a router or connect it to the WAN directly.

- **Connecting the network camera via a router**

Steps:

1. Connect the network camera to the router.
2. Assign a LAN IP address, the subnet mask and the gateway. Refer to Section 2.1.2 for detailed IP address configuration of the network camera.
3. Save the static IP in the router.
4. Set port mapping, e.g., 80, 8000, and 554 ports. The steps for port mapping vary according to the different routers. Please call the router manufacturer for assistance with port mapping.

Note: Refer to Appendix 2 for detailed information about port mapping.

5. Visit the network camera through a web browser or the client software over the internet.

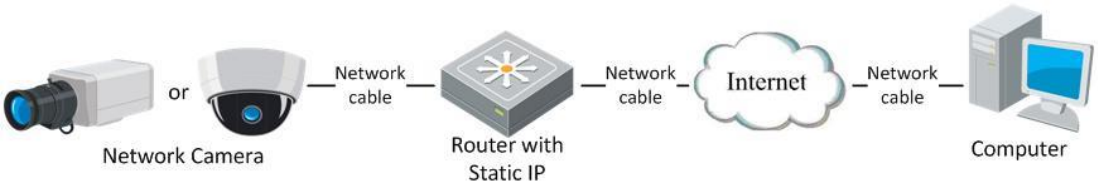


Figure 2-8 Accessing the Camera through Router with Static IP

- **Connecting the network camera with static IP directly**

You can also save the static IP in the camera and directly connect it to the internet without using a router. Refer to Section 2.1.2 for detailed IP address configuration of the network camera.

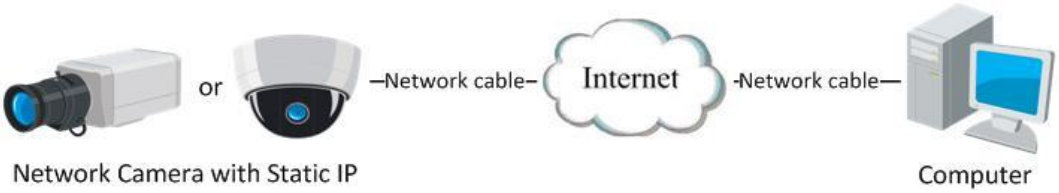


Figure 2-9 Accessing the Camera with Static IP Directly

2.2.2 Dynamic IP Connection

Before you start:

Please apply a dynamic IP from an ISP. With the dynamic IP address, you can connect the network camera to a modem or a router.

- **Connecting the network camera via a router**

Steps:

1. Connect the network camera to the router.
2. In the camera, assign a LAN IP address, the subnet mask and the gateway. Refer to Section 2.1.2 for detailed IP address configuration of the network camera.
3. In the router, set the PPPoE user name, password and confirm the password.
4. Set port mapping. E.g. 80, 8000, and 554 ports. The steps for port mapping vary depending on different routers. Please call the router manufacturer for assistance with port mapping.

Note: Refer to Appendix 2 for detailed information about port mapping.

5. Apply a domain name from a domain name provider.
6. Configure the DDNS settings in the setting interface of the router.
7. Visit the camera via the applied domain name.

- **Connecting the network camera via a modem**

Purpose:

This camera supports the PPPoE auto dial-up function. The camera gets a public IP address by ADSL dial-up after the camera is connected to a modem. You need to configure the PPPoE parameters of the network camera. Refer to *Section 6.3.3* ***Configuring PPPoE Settings*** for detailed configuration.

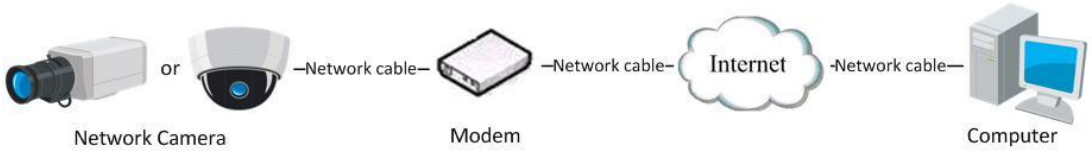


Figure 2-10 Accessing the Camera with Dynamic IP

Note: The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (E.g. DynDns.com). Please follow the steps below for normal domain name resolution and private domain name resolution to solve the problem.

♦ Normal Domain Name Resolution

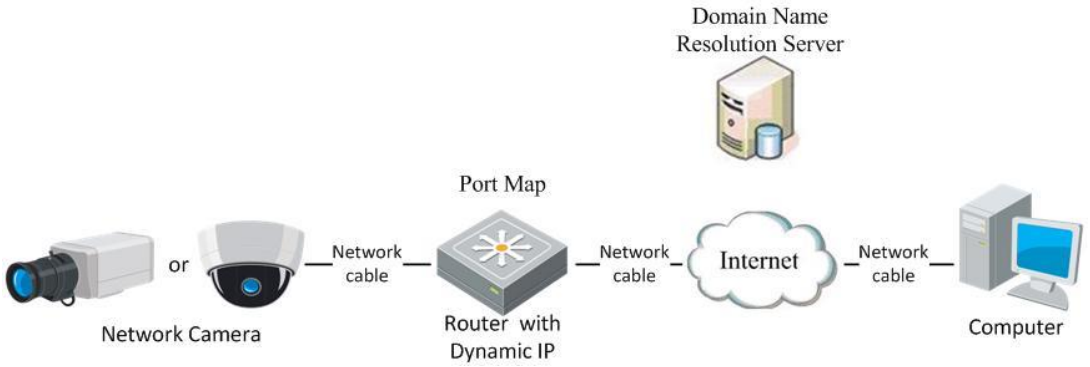


Figure 2-11 Normal Domain Name Resolution

Steps:

1. Apply a domain name from a domain name provider.
2. Configure the DDNS settings in the **DDNS Settings** interface of the network camera. Refer to *Section 6.3.4* ***Configuring DDNS Settings*** for detailed configuration.
3. Visit the camera via the applied domain name.

♦ Private Domain Name Resolution

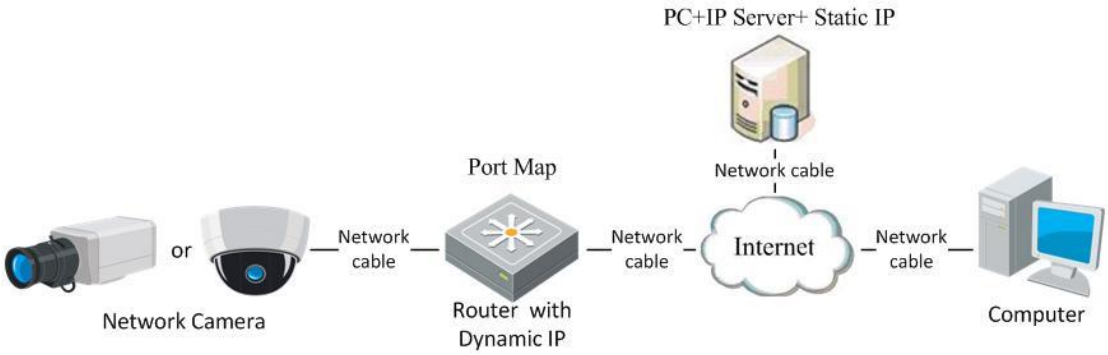


Figure 2-12 Private Domain Name Resolution

Steps:

1. Install and run the IP Server software in a computer with a static IP.
2. Access the network camera through the LAN with a web browser or the client software.
3. Enable DDNS and select IP Server as the protocol type. Refer to *Section 6.3.4* ***Configuring DDNS Settings*** for detailed configuration.

Chapter 3 Access to the Network Camera

3.1 Accessing by Web Browsers

Steps:

1. Open the web browser.
2. In the browser address bar, input the IP address of the network camera, and press the **Enter** key to enter the login interface.
3. Activate the network camera for the first time using, refer to the section 2.1.2 for details..

   Note:

   - The default IP address is 192.168.1.64.
   - If the camera is not activated, please activate the camera first according to Chapter 3.1 or Chapter 3.2.

4. Select English as the interface language on the top-right of login interface.
5. Input the user name and password and click Login.

   The admin user should configure the device accounts and user/operator permissions properly. Delete the unnecessary accounts and user/operator permissions.

   Note:

   The IP address gets locked if the admin user performs 7 failed password attempts (5 attempts for the user/operator).

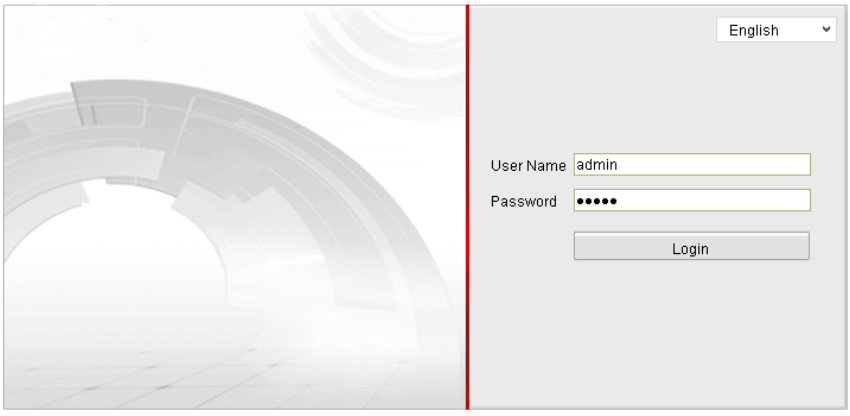


Figure 3-1 Login Interface

6. Install the plug-in before viewing the live video and operating the camera. Please follow the installation prompts to install the plug-in.

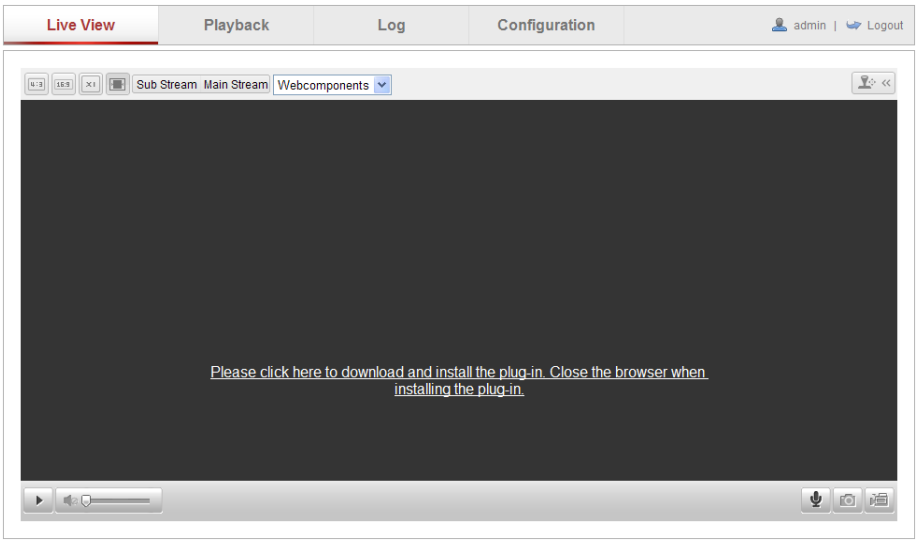


Figure 3-2 Download and Install Plug-in

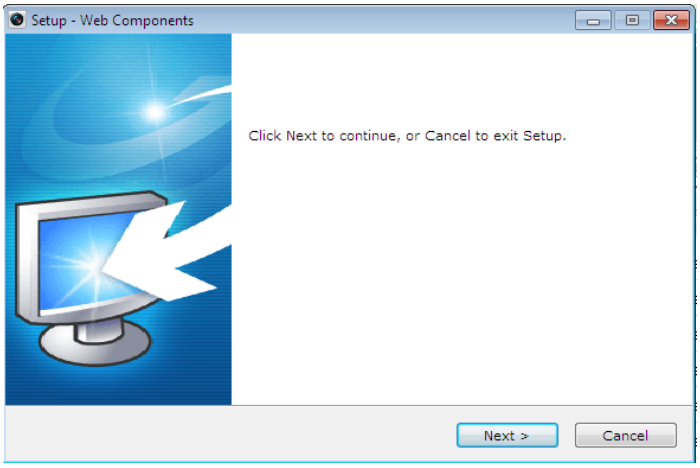


Figure 3-3 Install Plug-in (1)

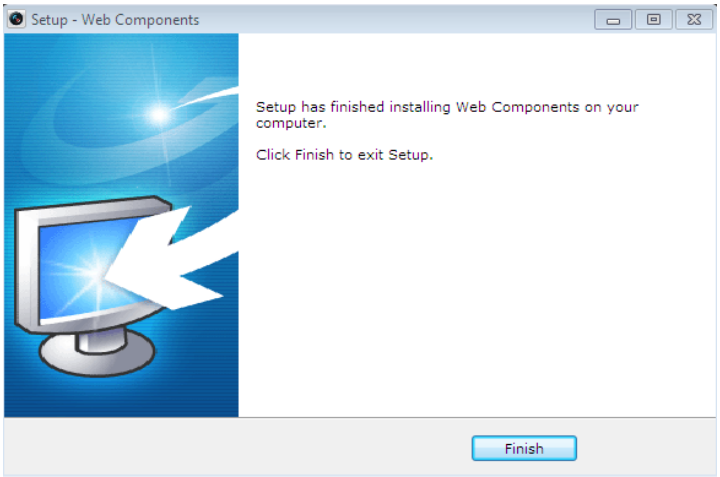


Figure 3-4 Install Plug-in (2)

Note: You may have to close the web browser to install the plug-in. Please reopen the

web browser and log in again after installing the plug-in.

Chapter 4 Wi-Fi Settings

Purpose:

By connecting to the wireless network, you don't need to use cable of any kind for network connection, which is very convenient for the actual surveillance application.

Note: This chapter is only applicable for the cameras with the built-in Wi-Fi module.

4.1 Configuring Wi-Fi Connection in Manage and Ad-hoc Modes

Before you start:

A wireless network must be configured.

Wireless Connection in Manage Mode

Steps:

1. Enter the Wi-Fi configuration interface.

Configuration> Advanced Configuration> Network> Wi-Fi

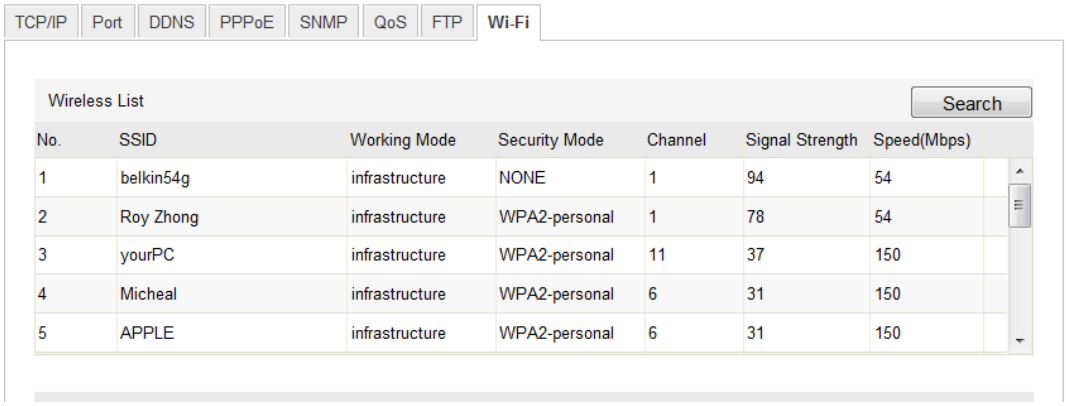


Figure 4-1 Wireless Network List

2. Click **Search** to search the online wireless connections.
3. Click to choose a wireless connection on the list.

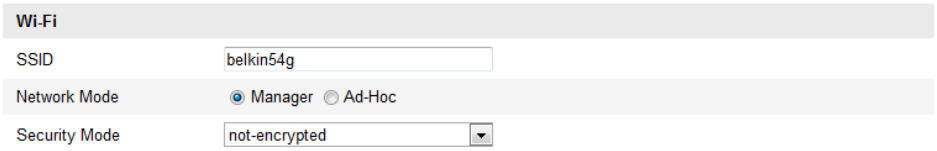


Figure 4-2 Wi-Fi Setting- Manage Mode

4. Check the checkbox to select the *Network mode* as *Manage*, and the *Security mode* of the network is automatically shown when you select the wireless network, please don't change it manually.

Note: These parameters are exactly identical with those of the router.

5. Enter the key to connect the wireless network. The key should be that of the wireless network connection you set on the router.

Wireless Connection in Ad-hoc Mode

If you choose the Ad-hoc mode, you don't need to connect the wireless camera via a router. The scenario is the same as you connect the camera and the PC directly with a network cable.

Steps:

1. Choose Ad-hoc mode.

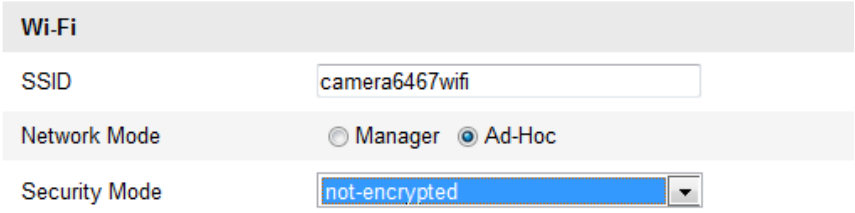


Figure 4-3 Wi-Fi Setting- Ad-hoc

2. Customize a SSID for the camera.
3. Choose the Security Mode of the wireless connection.

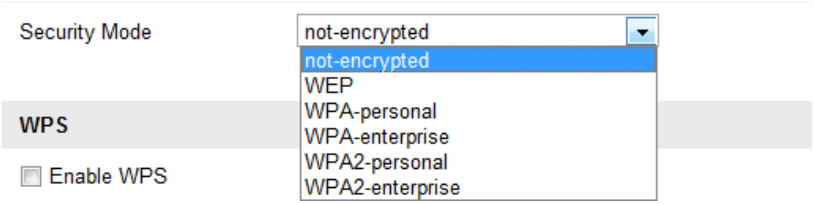


Figure 4-4 Security Mode- Ad-hoc Mode

4. Enable the wireless connection function for your PC.
5. On the PC side, search the network and you can see the SSID of the camera listed.

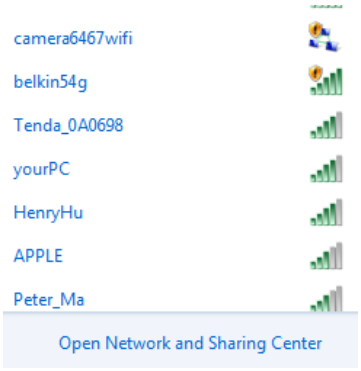


Figure 4-5 Ad-hoc Connection Point

6. Choose the SSID and connect.

Security Mode Description:

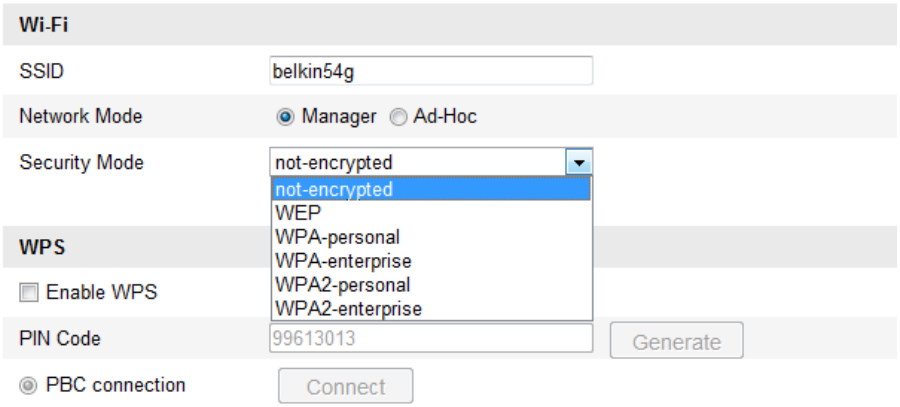


Figure 4-6 Security Mode

You can choose the Security Mode as not-encrypted, WEP, WPA-personal, WPA-enterprise, WPA2-personal, and WPA2-enterprise.

WEP mode:

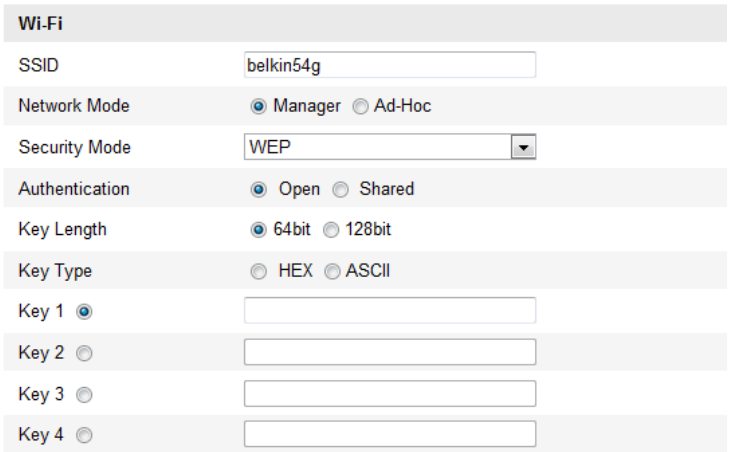


Figure 4-7 WEP Mode

- Authentication - Select Open or Shared Key System Authentication, depending on

the method used by your access point. Not all access points have this option, in which case they probably use Open System, which is sometimes known as SSID Authentication.

- *Key length* - This sets the length of the key used for the wireless encryption, 64 or 128 bit. The encryption key length can sometimes be shown as 40/64 and 104/128.
- *Key type - The key types available depend on the access point being used. The following options are available:*

  HEX - Allows you to manually enter the hex key.

  ASCII - In this method the string must be exactly 5 characters for 64-bit WEP and 13 characters for 128-bit WEP.

WPA-personal and WPA2-personal Mode:

Enter the required Pre-shared Key for the access point, which can be a hexadecimal number or a passphrase.

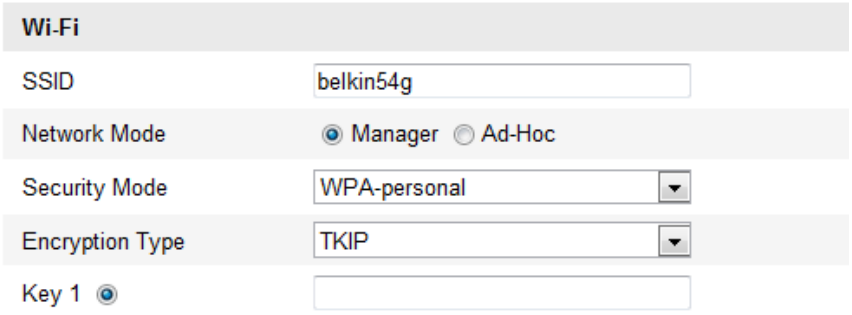


Figure 4-8 Security Mode- WPA-personal

WPA- enterprise and WPA2-enterprise Mode:

Choose the type of client/server authentication being used by the access point; EAP-TLS or EAP-PEAP.

EAP-TLS

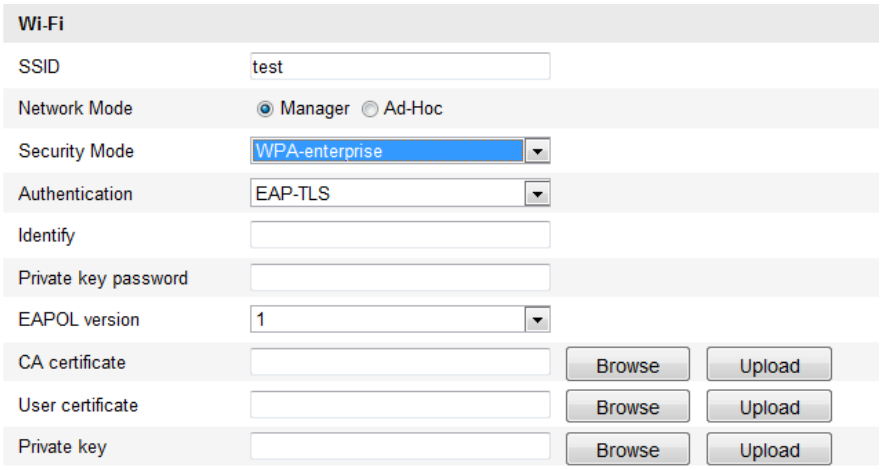


Figure 4-9 EAP-TLS

- Identity - Enter the user ID to present to the network.
- Private key password – Enter the password for your user ID.
- EAPOL version - Select the version used (1 or 2) in your access point.
- CA Certificates - Upload a CA certificate to present to the access point for authentication.

EAP-PEAP:

- User Name - Enter the user name to present to the network
- Password - Enter the password of the network
- PEAP Version - Select the PEAP version used at the access point.
- Label - Select the label used by the access point.
- EAPOL version - Select version (1 or 2) depending on the version used at the access point
- CA Certificates - Upload a CA certificate to present to the access point for authentication

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories:*

upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.

- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

4.2 Easy Wi-Fi Connection with WPS function

Purpose:

The setting of the wireless network connection is never easy. To avoid the complex setting of the wireless connection you can enable the WPS function.

WPS (Wi-Fi Protected Setup) refers to the easy configuration of the encrypted connection between the device and the wireless router. The WPS makes it easy to add new devices to an existing network without entering long passphrases. There are two modes of the WPS connection, the PBC mode and the PIN mode.

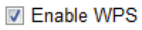
Note: If you enable the WPS function, you do not need to configure the parameters such as the encryption type and you don't need to know the key of the wireless connection.

Steps:

Figure 4-10 Wi-Fi Settings - WPS

PBC Mode**:**

PBC refers to the Push-Button-Configuration, in which the user simply has to push a button, either an actual or virtual one (as the Connect button on the configuration interface of the IE browser), on both the Access Point (and a registrar of the network) and the new wireless client device.

1. Check the checkbox of  to enable WPS.

2. Choose the connection mode as PBC.

Note: Support of this mode is mandatory for both the Access Points and the connecting devices.

3. Check on the Wi-Fi router to see if there is a WPS button. If yes push the button and you can see the indicator near the button start flashing, which means the WPS function of the router is enabled. For detailed operation, please see the user guide of the router.
4. Push the WPS button to enable the function on the camera.

If there is not a WPS button on the camera, you can also click the virtual button to enable the PBC function on the web interface.

5. Click **Connect** button.

When the PBC mode is both enabled in the router and the camera, the camera and the wireless network is connected automatically.

PIN Mode:

The PIN mode requires a Personal Identification Number (PIN) to be read from either a sticker or the display on the new wireless device. This PIN must then be entered to connect the network, usually the Access Point of the network.

Steps:

1. Choose a wireless connection on the list and the SSID is shown.

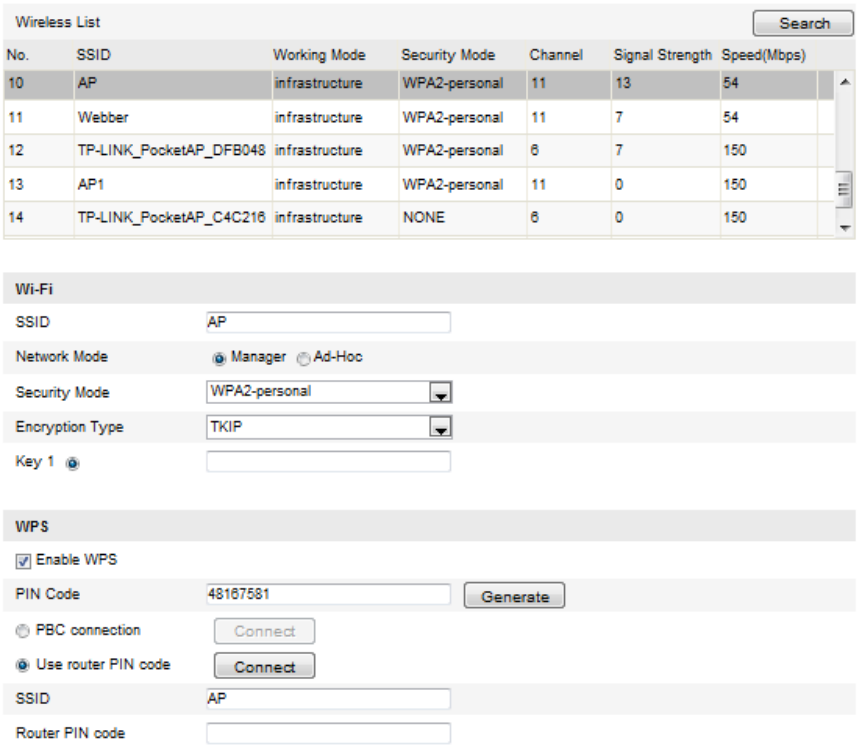


Figure 4-11 Wi-Fi Settings – WPS PIN Mode

2. Choose **Use route PIN code**.

If the PIN code is generated from the router side, you should enter the PIN code you get from the router side in the **Router PIN code** field.

3. Click **Connect**.

Or

You can generate the PIN code on the camera side. And the expired time for the PIN code is 120 seconds.

1. Click **Generate**.

2. Enter the code to the router, in the example, enter 48167581 to the router.

4.3 IP Property Settings for Wireless Network Connection

The default IP address of wireless network interface controller is 192.168.1.64. When you connect the wireless network you can change the default IP.

Steps:

1. Enter the TCP/IP configuration interface.

Configuration> Advanced Configuration> Network> TCP/IP

Or

Configuration> Basic Configuration> Network> TCP/IP

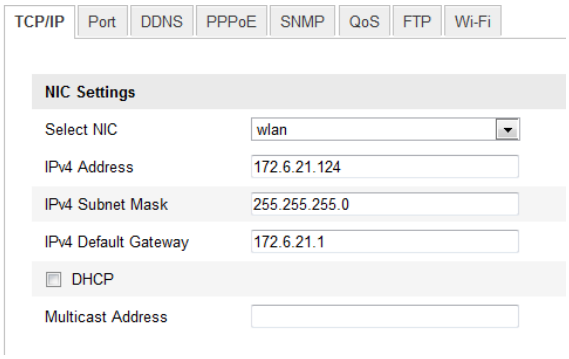


Figure 4-12 TCP/IP Settings

2. Select the NIC as wlan.

3. Customize the IPv4 address, the IPv4 Subnet Mask and the Default Gateway.

The setting procedure is the same with that of LAN.

If you want to be assigned the IP address you can check the checkbox to enable the DHCP.

Chapter 5 Live View

5.1 Live View Page

Purpose:

The live view page allows you to view the real-time video, capture images, realize PTZ control, set/call presets and configure video parameters.

Log in the network camera to enter the live view page, or you can click **Live View** on the menu bar of the main page to enter the live view page.

Descriptions of the live view page:

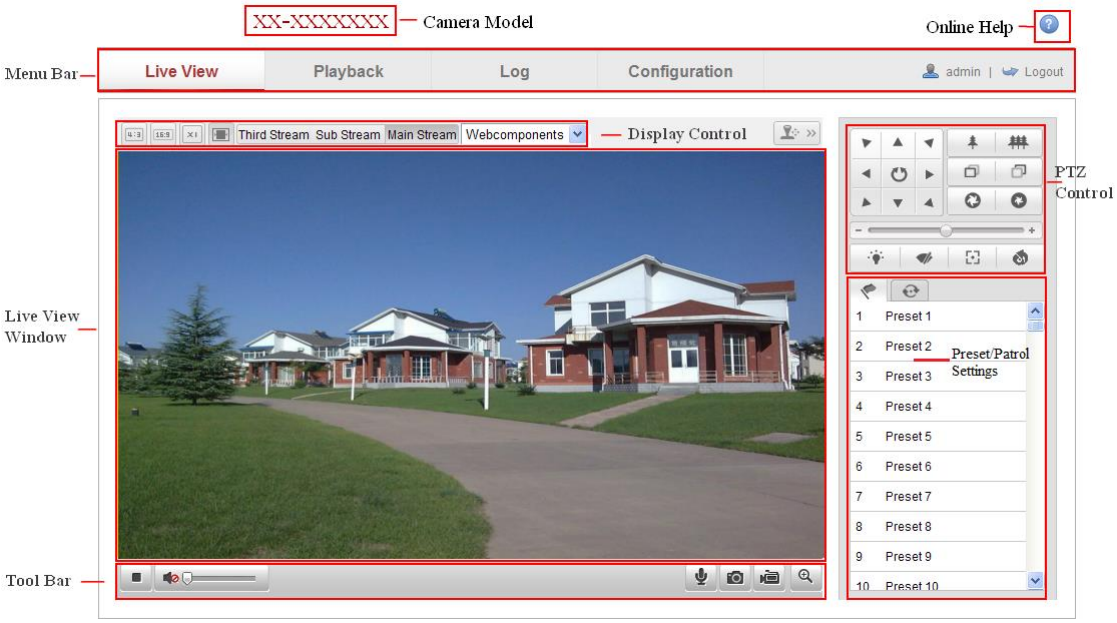


Figure 5-1 Live View Page

Camera Model:

It lists the camera model you are connecting to.

Online Help:

Click to get the online help, which will guide you through the basic operations for each function.

Menu Bar:

Click each tab to enter Live View, Playback, Log and Configuration page respectively.

Display Control:

Click each tab to adjust the layout and the stream type of the live view. And you can click the drop-down to select the plug-in. For IE (internet explorer) user, webcomponents and quick time are selectable. And for Non-IE user, webcomponents, quick time, VLC or MJPEG is selectable if they are supported by the web browser.

Live View Window:

Display the live video.

Toolbar:

Operations on the live view page, e.g., live view, capture, record, audio on/off, two-way audio, etc.

PTZ Control:

Panning, tilting and zooming actions of the camera and the light and wiper control. (only available for cameras supporting PTZ function)

Preset/Patrol Settings:

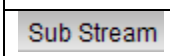
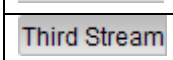
Set/call/delete the presets or patrols for PTZ cameras.

5.2 Starting Live View

In the live view window as shown in Figure 5-2, click on the toolbar to start the live view of the camera.

Figure 5-2 Live View Toolbar

Table 5-1 Descriptions of the Toolbar

Icon	Description
	Start/Stop live view.
	The window size is 4:3.
	The window size is 16:9.
	The original widow size.
	Self-adaptive window size.
	Live view with the main stream.
	Live view with the sub stream.
	Live view with the third stream.

Webcomponents	Click to select the third-party plug-in.
	Manually capture the picture.
/	Manually start/stop recording.
/	Audio on and adjust volume /Mute.
/	Turn on/off microphone.
/	Turn on/off digital zoom function.
/	Turn on/off 3D positioning function.

Note: The third stream and 3D positioning require the support of camera.

5.3 Recording and Capturing Pictures Manually

In the live view interface, click on the toolbar to capture the live pictures or click to record the live view. The saving paths of the captured pictures and clips can be set on the **Configuration > Local Configuration** page. To configure remote scheduled recording, please refer to *Section 7.2*.

Note: The captured image will be saved as JPEG file or BMP file in your computer.

5.4 Operating PTZ Control

Purpose:

In the live view interface, you can use the PTZ control buttons to realize pan/tilt/zoom control of the camera.

Note: To realize PTZ control, the camera connected to the network must support the PTZ function or a pan/tilt unit has been installed to the camera. Please properly set the PTZ parameters on RS-485 settings page referring to *Section 12.9* ***RS-485 Settings***.

5.4.1 PTZ Control Panel

On the live view page, click to show the PTZ control panel or click to hide it.

Click the direction buttons to control the pan/tilt movements.

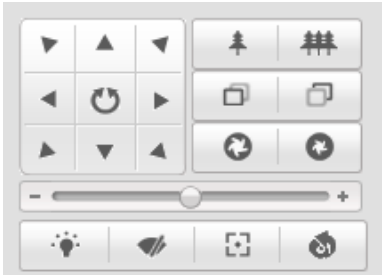


Figure 5-3 PTZ Control Panel

Click the zoom/iris/focus buttons to realize lens control.

***Notes*:**

- There are 8 direction arrows (△,▽,◁, ▷,▽,▽,▷,◁) in the live view window when you click and drag the mouse in the relative positions.
- For the cameras which support lens movements only, the direction buttons are invalid.

Table 5-2 Descriptions of PTZ Control Panel

Icon	Description
	Zoom in/out
	Focus near/far
	Iris +/-
	Light on/off
	Wiper on/off
	Auxiliary focus
	Initialize lens
	Adjust speed of pan/tilt movements

5.4.2 Setting / Calling a Preset

- **Setting a Preset:**

1. In the PTZ control panel, select a preset number from the preset list.

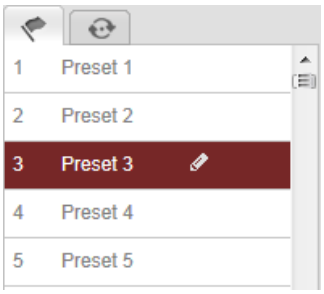


Figure 5-4 Setting a Preset

2. Use the PTZ control buttons to move the lens to the desired position.
   - Pan the camera to the right or left.
   - Tilt the camera up or down.
   - Zoom in or out.
   - Refocus the lens.
3. Click to finish the setting of the current preset.
4. You can click to delete the preset.

***Note*:** Up to 16 presets can be configured for the Network Mini PT Camera.

- **Calling a Preset:**

This feature enables the camera to point to a specified preset scene manually or when an event takes place.

For the defined preset, you can call it at any time to the desired preset scene.

In the PTZ control panel, select a defined preset from the list and click to call the preset.

Or you can place the mouse on the presets interface, and call the preset by typing the preset No. to call the corresponding presets.

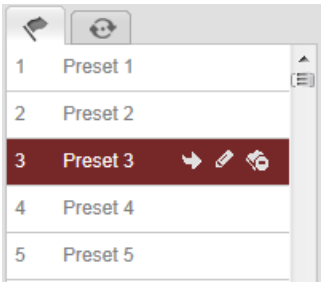


Figure 5-5 Calling a Preset

5.4.3 Setting / Calling a Patrol

Note:

No less than 2 presets have to be configured before you set a patrol.

Steps:

1. Click to enter the patrol configuration interface.
2. Select a path No., and click to add the configured presets.
3. Select the preset, and input the patrol duration and patrol speed.
4. Click OK to save the first preset.
5. Follow the steps above to add the other presets.

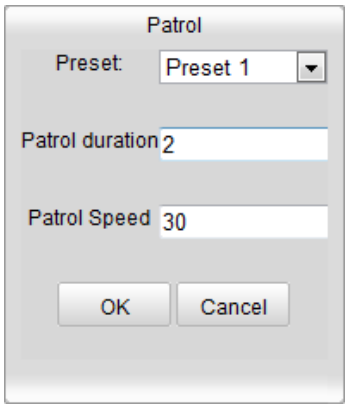


Figure 5-6 Add Patrol Path

6. Click to save a patrol.
7. Click to start the patrol, and click to stop it.
8. (Optional) Click to delete a patrol.

Chapter 6 Network Camera Configuration

6.1 Configuring Local Parameters

Note: The local configuration refers to the parameters of the live view, record files and captured pictures. The record files and captured pictures are the ones you record and captured using the web browser and thus the saving paths of them are on the PC running the browser.

Steps:

1. Enter the Local Configuration interface:

Configuration > Local Configuration

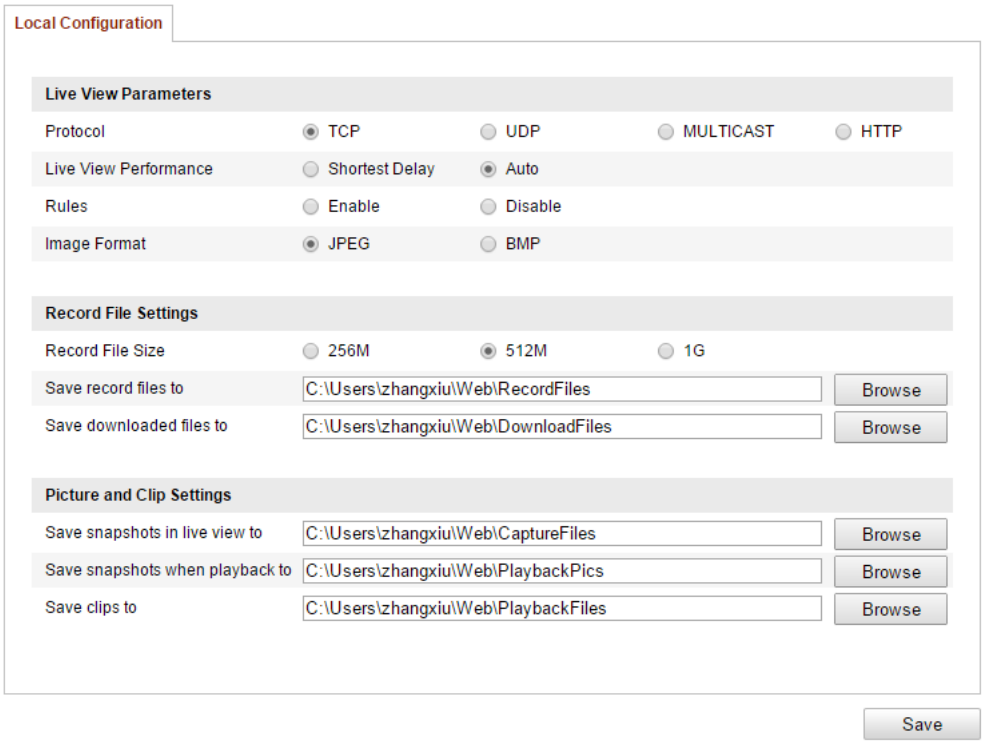


Figure 6-1 Local Configuration Interface

2. Configure the following settings:

- **Live View Parameters:** Set the protocol type and live view performance.
  - **Protocol Type:** TCP, UDP, MULTICAST and HTTP are selectable.

    TCP: Ensures complete delivery of streaming data and better video quality,

yet the real-time transmission will be affected.

UDP: Provides real-time audio and video streams.

HTTP: Allows the same quality as of TCP without setting specific ports for streaming under some network environments.

MULTICAST: It's recommended to select MCAST type when using the Multicast function. For detailed information about Multicast, refer to *Section 6.3.1* ***Configuring TCP/IP Settings***.

- **Live View Performance:** Set the live view performance to Shortest Delay or Auto.
- **Rules:** It refers to the rules on your local browser, select enable or disable to display or not display the colored marks when the motion detection, face detection, or intrusion detection is triggered. E.g.: enabled as the rules are, and the face detection is enabled as well, when a face is detected, it will be marked with a green rectangle on the live view.
- **Image Format:** Choose the image format for picture capture.

- **Record File Settings:** Set the saving path of the recorded video files. Valid for the record files you recorded with the web browser.
  - **Record File Size:** Select the packed size of the manually recorded and downloaded video files to 256M, 512M or 1G. After the selection, the maximum record file size is the value you selected.
  - **Save record files to:** Set the saving path for the manually recorded video files.
  - **Save downloaded files to:** Set the saving path for the downloaded video files in playback mode.
- **Picture and Clip Settings:** Set the saving paths of the captured pictures and clipped video files. Valid for the pictures you captured with the web browser.
  - **Save snapshots in live view to:** Set the saving path of the manually captured pictures in live view mode.
  - **Save snapshots when playback to:** Set the saving path of the captured pictures in playback mode.
  - **Save clips to:** Set the saving path of the clipped video files in playback mode.

Note: You can click **Browse** to change the directory for saving the clips and pictures.

3. Click **Save** to save the settings.

6.2 Configuring Time Settings

Purpose:

You can follow the instructions in this section to configure the time synchronization and DST settings.

Steps:

1. Enter the Time Settings interface:

   Configuration > Basic Configuration > System > Time Settings

   Or **Configuration > Advanced Configuration > System > Time Settings**

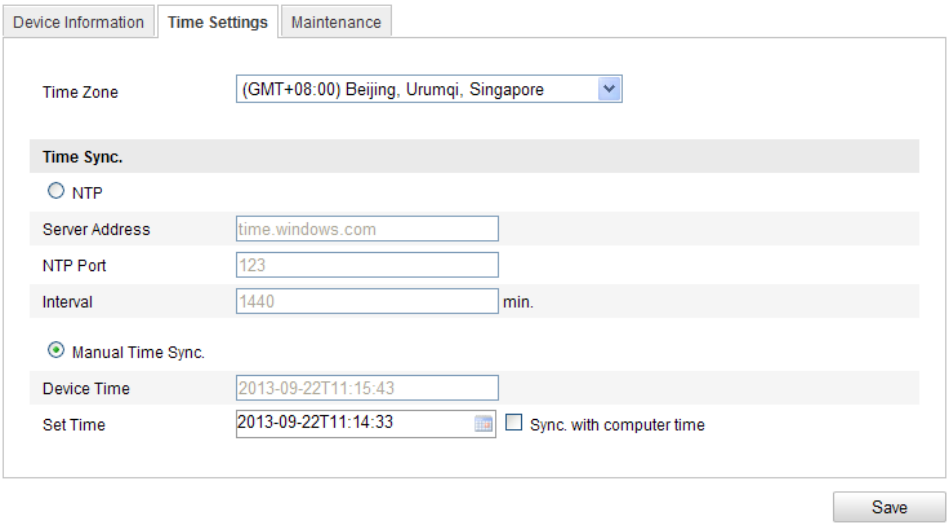


Figure 6-2 Time Settings

- Select the Time Zone.

  Select the Time Zone of your location from the drop-down menu.

♦ Synchronizing Time by NTP Server.

(1) Check the checkbox to enable the **NTP** function.

(2) Configure the following settings:

Server Address: IP address of NTP server.

NTP Port: Port of NTP server.

Interval: The time interval between the two synchronizing actions with NTP

server.

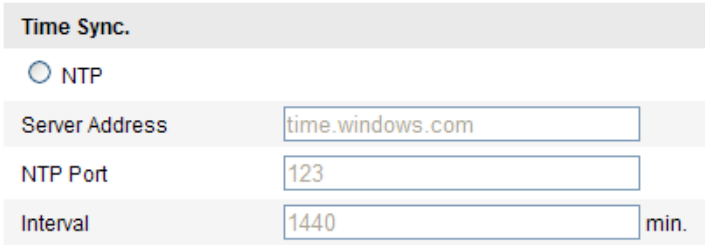


Figure 6-3 Time Sync by NTP Server

***Note*:** If the camera is connected to a public network, you should use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the camera is set in a customized network, NTP software can be used to establish a NTP server for time synchronization.

♦ Synchronizing Time Synchronization Manually

Enable the **Manual Time Sync** function and then click to set the system time from the pop-up calendar.

Note: You can also check the **Sync with computer time** checkbox to synchronize the time of the camera with that of your computer.

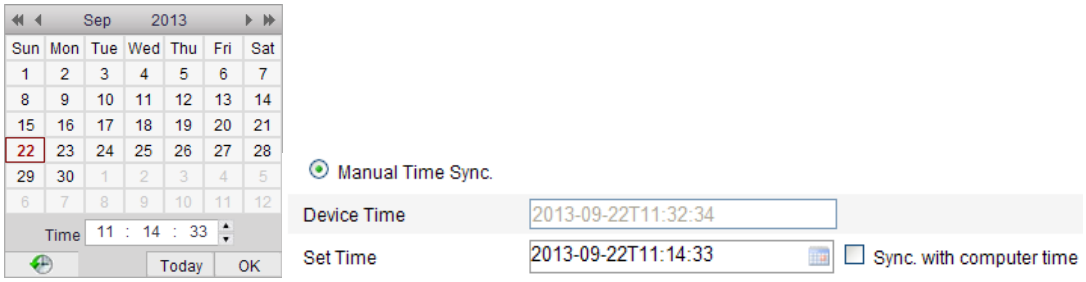


Figure 6-4 Time Sync Manually

- Click the **DST** tab page to enable the DST function and Set the date of the DST period.

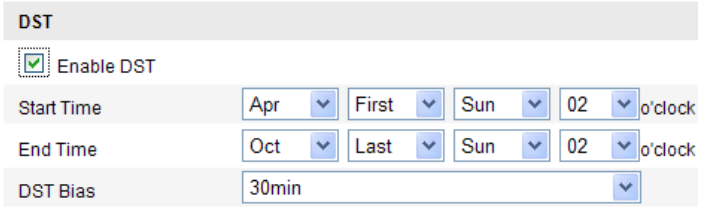


Figure 6-5 DST Settings

2. Click **Save** to save the settings.

6.3 Configuring Network Settings

6.3.1 Configuring TCP/IP Settings

Purpose:

TCP/IP settings must be properly configured before you operate the camera over network. The camera supports both the IPv4 and IPv6. Both versions may be configured simultaneously without conflicting to each other, and at least one IP version should be configured.

Steps:

1. Enter TCP/IP Settings interface:

   Configuration > Basic Configuration > Network > TCP/IP

   Or **Configuration > Advanced Configuration > Network > TCP/IP**

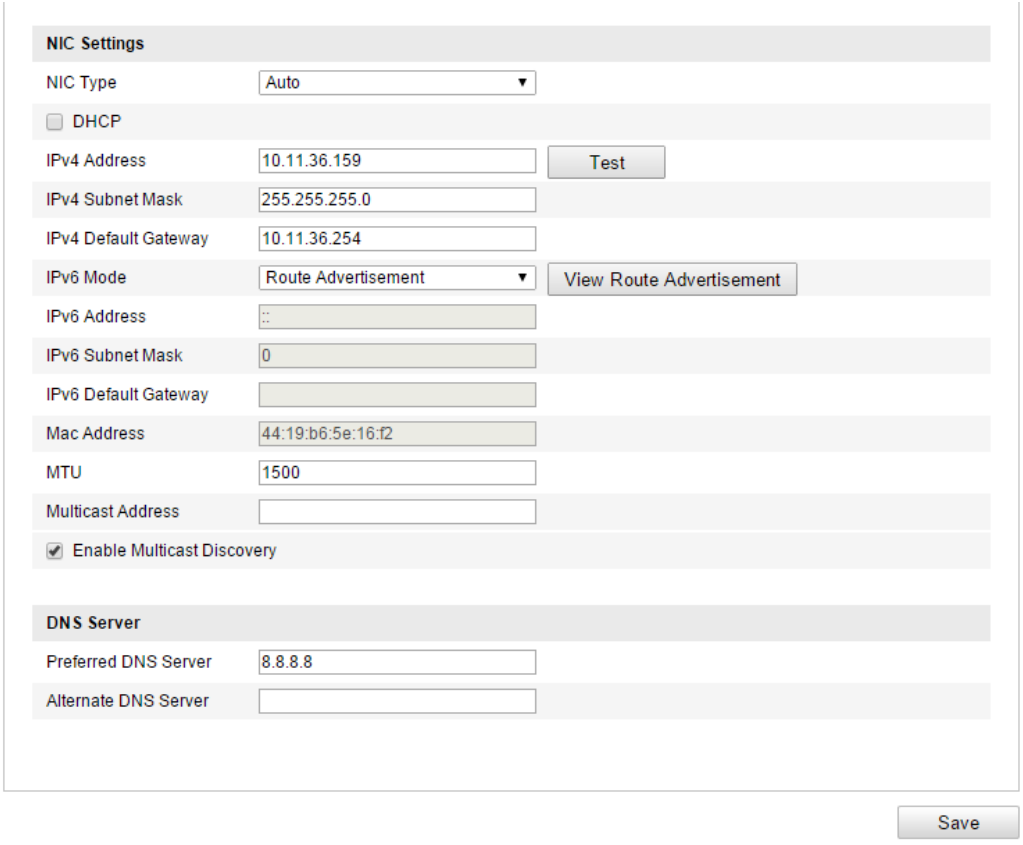


Figure 6-6 TCP/IP Settings

2. Configure the basic network settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, MTU settings

and Multicast Address.

3. (Optional) Check the checkbox of **Enable Multicast Discovery**, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.
4. Click **Save** to save the above settings.

***Notes*:**

- The valid value range of MTU is 1280 ~ 1500.
- The Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Before utilizing this function, you have to enable the Multicast function of your router.
- A reboot is required for the settings to take effect.

6.3.2 Configuring Port Settings

Purpose:

You can set the port No. of the camera, e.g. HTTP port, RTSP port and HTTPS port.

Steps:

1. Enter the Port Settings interface:

   Configuration > Basic Configuration > Network > Port

   Or **Configuration > Advanced Configuration > Network > Port**

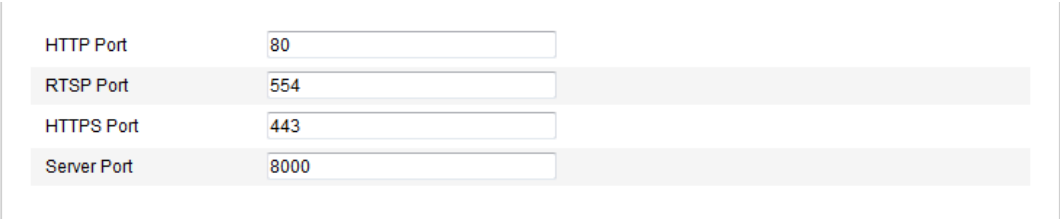


Figure 6-7 Port Settings

2. Set the HTTP port, RTSP port, HTTPS port and server port of the camera.

   HTTP Port: The default port number is 80, and it can be changed to any port No. which is not occupied.

   RTSP Port: The default port number is 554 and it can be changed to any port No.

ranges from 1024 to 65535.

HTTPS Port: The default port number is 443, and it can be changed to any port No. which is not occupied.

Server Port: The default server port number is 8000, and it can be changed to any port No. ranges from 2000 to 65535.

3. Click **Save** to save the settings.

***Note*:** A reboot is required for the settings to take effect.

6.3.3 Configuring PPPoE Settings

Steps:

1. Enter the PPPoE Settings interface:

Configuration >Advanced Configuration > Network > PPPoE

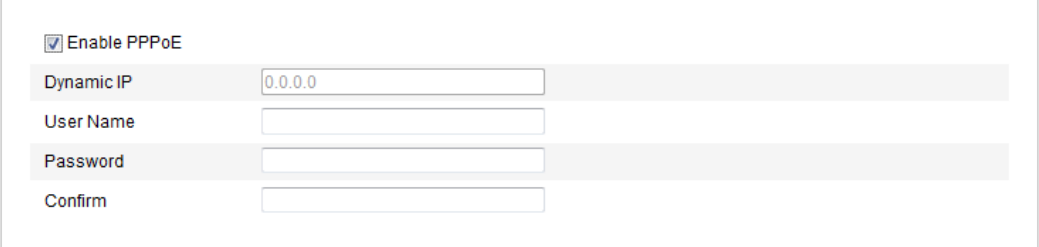


Figure 6-8 PPPoE Settings

2. Check the **Enable PPPoE** checkbox to enable this feature.
3. Enter **User Name**, **Password**, and **Confirm** password for PPPoE access.

Note: The User Name and Password should be assigned by your ISP.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

4. Click **Save** to save and exit the interface.

***Note*:** A reboot is required for the settings to take effect.

6.3.4 Configuring DDNS Settings

Purpose:

If your camera is set to use PPPoE as its default network connection, you can use the Dynamic DNS (DDNS) for network access.

***Before you start*:**

Registration on the DDNS server is required before configuring the DDNS settings of the camera.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Steps:

1. Enter the DDNS Settings interface:

   Configuration > Advanced Configuration > Network > DDNS

2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Four DDNS types are selectable: IPServer, NO-IP, and DynDNS.
   - DynDNS:

   Steps:

   (1)Enter **Server Address** of DynDNS (e.g. members.dyndns.org).

(2)In the **Domain** text field, enter the domain name obtained from the DynDNS website.

(3)Enter the **Port** of DynDNS server.

(4)Enter the **User Name** and **Password** registered on the DynDNS website.

(5)Click **Save** to save the settings.

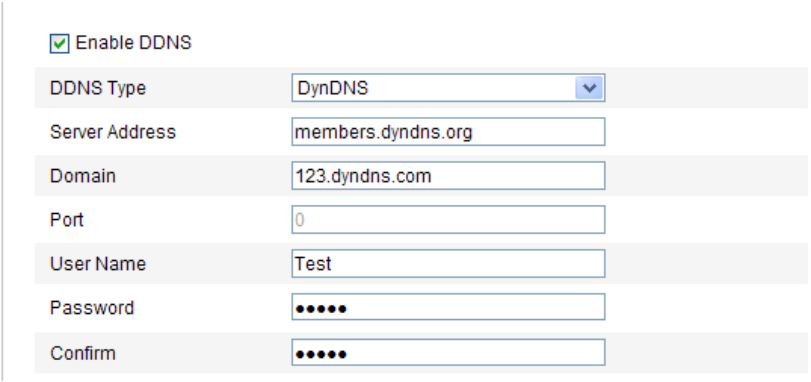


Figure 6-9 DynDNS Settings

- IP Server:

Steps:

(1) Enter the Server Address of the IP Server.

(2) Click **Save** to save the settings.

Note: For the IP Server, you have to apply a static IP, subnet mask, gateway and preferred DNS from the ISP. The **Server Address** should be entered with the static IP address of the computer that runs the IP Server software.

Figure 6-10 IPServer Settings

Note: For the US and Canada area, you can enter 173.200.91.74 as the server address.

- NO-IP:

Steps:

(1) Choose the DDNS Type as NO-IP.

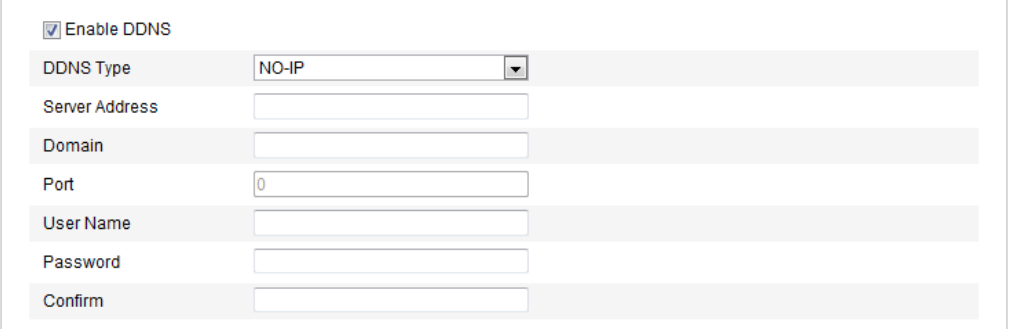


Figure 6-11 NO-IP Settings

(2) Enter the Server Address as www.noip.com

(3) Enter the Domain name you registered.

(4) Enter the Port number, if needed.

(5) Enter the User Name and Password.

(6) Click **Save** and then you can view the camera with the domain name.

***Note*:** A reboot is required for the settings to take effect.

6.3.5 Configuring SNMP Settings

Purpose:

You can set the SNMP function to get camera status, parameters and alarm related information and manage the camera remotely when it is connected to the network.

Before you start:

Before setting the SNMP, please download the SNMP software and manage to receive the camera information via SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center.

Note: The SNMP version you select should be the same as that of the SNMP software. And you also need to use the different version according to the security level you required. SNMP v1 provides no security and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Steps:

1. Enter the SNMP Settings interface:

   Configuration > Advanced Configuration > Network > SNMP

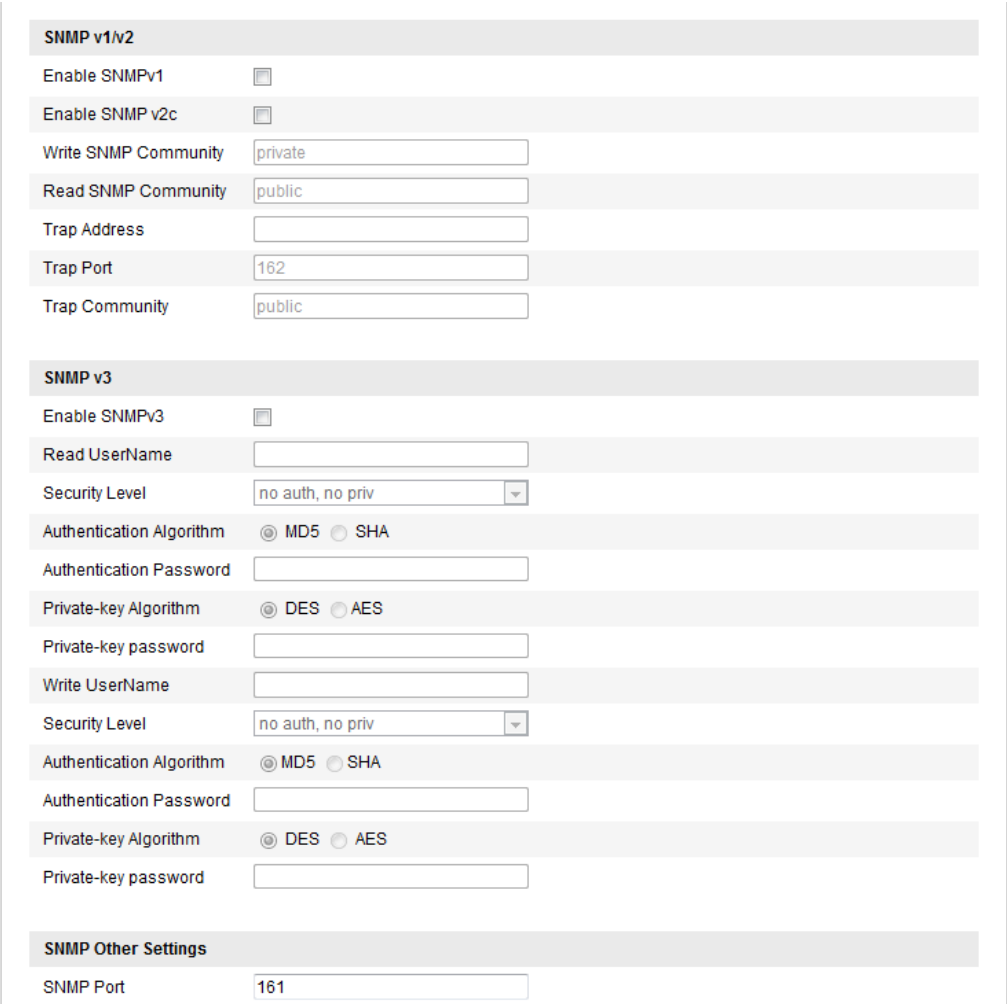


Figure 6-12 SNMP Settings

2. Check the corresponding version checkbox (Enable SNMP SNMPv1 , Enable SNMP v2c , Enable SNMPv3) to enable the feature.
3. Configure the SNMP settings.

   Note: The settings of the SNMP software should be the same as the settings you configure here.
4. Click **Save** to save and finish the settings.

Note: A reboot is required for the settings to take effect.

6.3.6 Configuring 802.1X Settings

Purpose:

The IEEE 802.1X standard is supported by the network cameras, and when the feature is enabled, the camera data is secured and user authentication is needed when connecting the camera to the network protected by the IEEE 802.1X.

Before you start:

The authentication server must be configured. Please apply and register a user name and password for 802.1X in the server.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Steps:

1. Enter the 802.1X Settings interface:

   Configuration > Advanced Configuration > Network > 802.1X

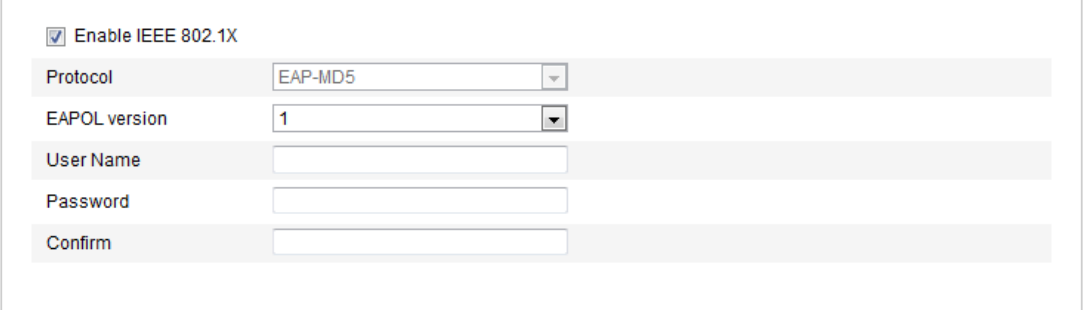


Figure 6-13 802.1X Settings

2. Check the **Enable IEEE 802.1X** checkbox to enable the feature.
3. Configure the 802.1X settings, including EAPOL version, user name and password.

   Note: The EAPOL version must be identical with that of the router or the switch.
4. Enter the user name and password to access the server.
5. Click **Save** to finish the settings.

Note: A reboot is required for the settings to take effect.

6.3.7 Configuring QoS Settings

Purpose:

QoS (Quality of Service) can help solve the network delay and network congestion by configuring the priority of data sending.

Steps:

1. Enter the QoS Settings interface:

   Configuration >Advanced Configuration > Network > QoS

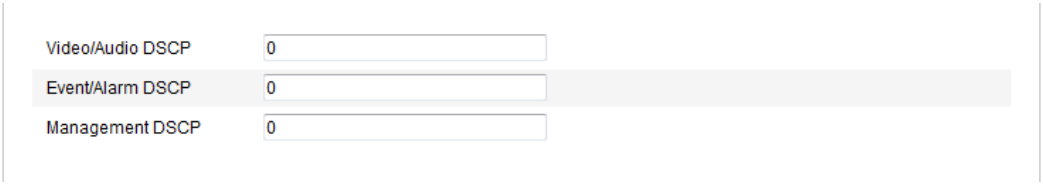


Figure 6-14 QoS Settings

2. Configure the QoS settings, including video / audio DSCP, event / alarm DSCP and Management DSCP.

   The valid value range of the DSCP is 0-63. The bigger the DSCP value is, the

higher the priority is.

Note: DSCP refers to the Differentiated Service Code Point; and the DSCP value is used in the IP header to indicate the priority of the data.

3. Click **Save** to save the settings.

Note: A reboot is required for the settings to take effect.

6.3.8 Configuring UPnP™ Settings

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

With the function enabled, you don't need to configure the port mapping for each port, and the camera is connected to the Wide Area Network via the router.

Steps:

1. Enter the UPnP™ settings interface.

   Configuration >Advanced Configuration > Network > UPnP

2. Check the checkbox to enable the UPnP™ function.

   The name of the device when detected online can be edited.

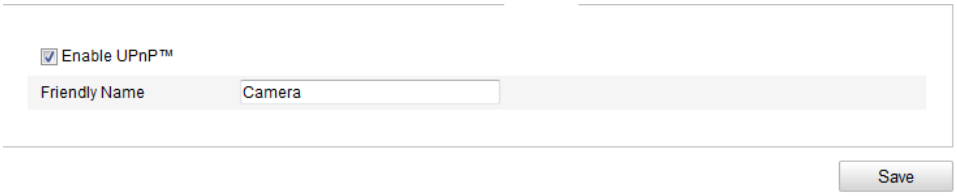


Figure 6-15 UPnP Settings

6.3.9 Configuring Wireless Dial Settings

Purpose:

Data stream of audio, video and image can be transferred via 3G / 4G wireless network.

Note: The wireless dial function requires the support of the camera.

1. Click the **Wireless Dial** tab to enter the Wireless Dial configuration interface.
2. Check the checkbox of **Enable** to enable the wireless dial settings.
3. Configure the dial parameters.
   1) Select the dial mode from the drop-down list. Auto and Manual are selectable. If Auto is selected, you can set the arming schedule for dialing; If Manual is selected, you can set the offline time and manual dialing parameters.
   2) Set the access number, user name, password, APN, MTU and verification protocol. You can also leave these parameters blank, and the device will adopt the default settings for dialing after other parameters are configured.
   3) Select the network mode from the drop-down list. Auto, 3G and 4G are selectable. If Auto is selected, the network selection priority comes as: 4G > 3G > Wired Network.
   4) Input the offline time if Manual is selected as the dial mode.
   5) Input the UIM Number (Mobile Phone Number).
   6) Click the **Edit** button to set the arming schedule if Auto is selected as the dial mode.
   7) Click **Save** to save the settings.

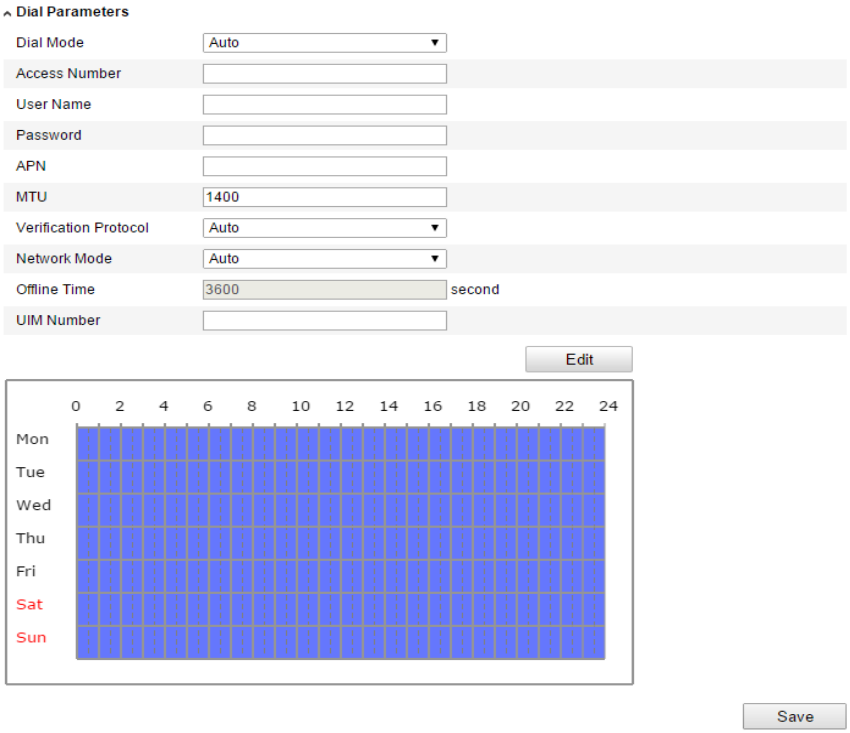


Figure 6-16 Dial Parameters

4. View the dial status.

   1) Click the **Refresh** button to view the dial status including real-time mode, UIM status, signal strength, etc.

   2) If Manual is selected as the dial mode, you can also manually connect / disconnect the wireless network.

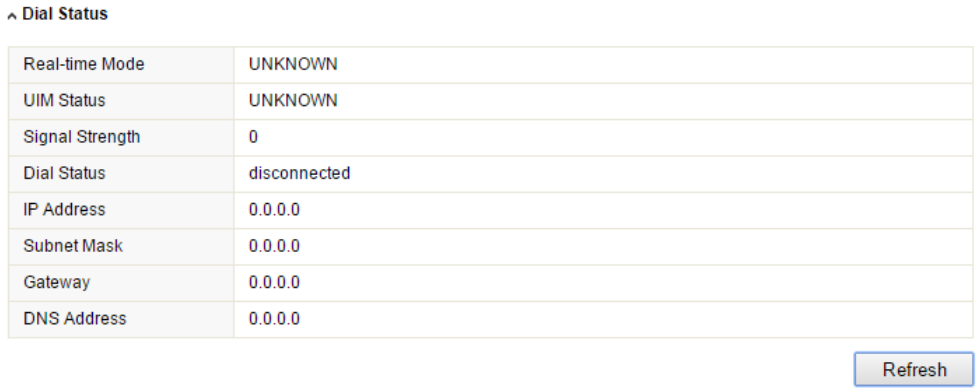


Figure 6-17 Dial Status

5. Set the white list.

   1) Check the checkbox of **Enable SMS Alarm**.

      The mobile phone number on the white list can receive the alarm message from the device and reboot the device via SMS.

      Note: Up to 8 mobile phone numbers can be added on the white list.

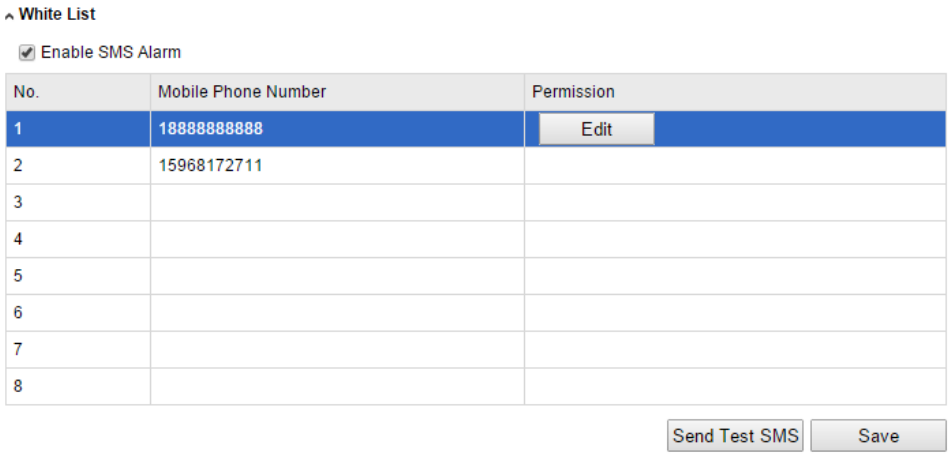


Figure 6-18 White List Settings

   2) Select the item on the white list, and click the **Edit** button to enter the SMS Alarm Settings interface.

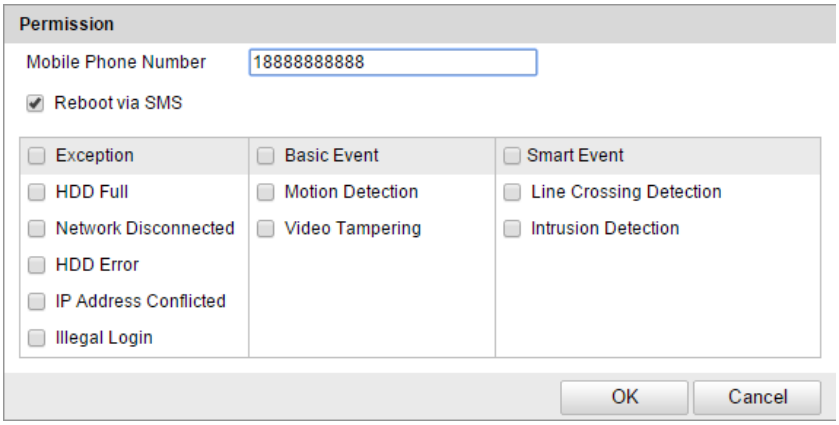


Figure 6-19 SMS Alarm Settings

3) Input the mobile phone number for the white list, check the checkbox of **Reboot via SMS**, select the alarm for SMS push, and click **OK**.

   Note: To reboot the device via SMS, send the message "reboot" to the device, and the device will reply a message "reboot success" after rebooting succeeded.

4) (Optional) You can click **Send Test SMS** to send a message to the mobile phone for test.

5) Click **Save** to save the settings.

6.3.10 Email Sending Triggered by Alarm

Purpose:

The system can be configured to send an Email notification to all designated receivers if an alarm event is detected, e.g., motion detection event, video loss, video tampering, etc.

Before you start:

Please configure the DNS Server settings under **Basic Configuration > Network > TCP/IP** or **Advanced Configuration > Network > TCP/IP** before using the Email function.

Steps:

1. Enter the TCP/IP Settings (**Configuration > Basic Configuration > Network > TCP/IP** or **Configuration > Advanced Configuration > Network > TCP/IP)** to

set the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway and the Preferred DNS Server.

Note: Please refer to *Section 6.3.1* ***Configuring TCP/IP Settings*** for detailed information.

2. Enter the Email Settings interface:

Configuration > Advanced Configuration > Network > Email

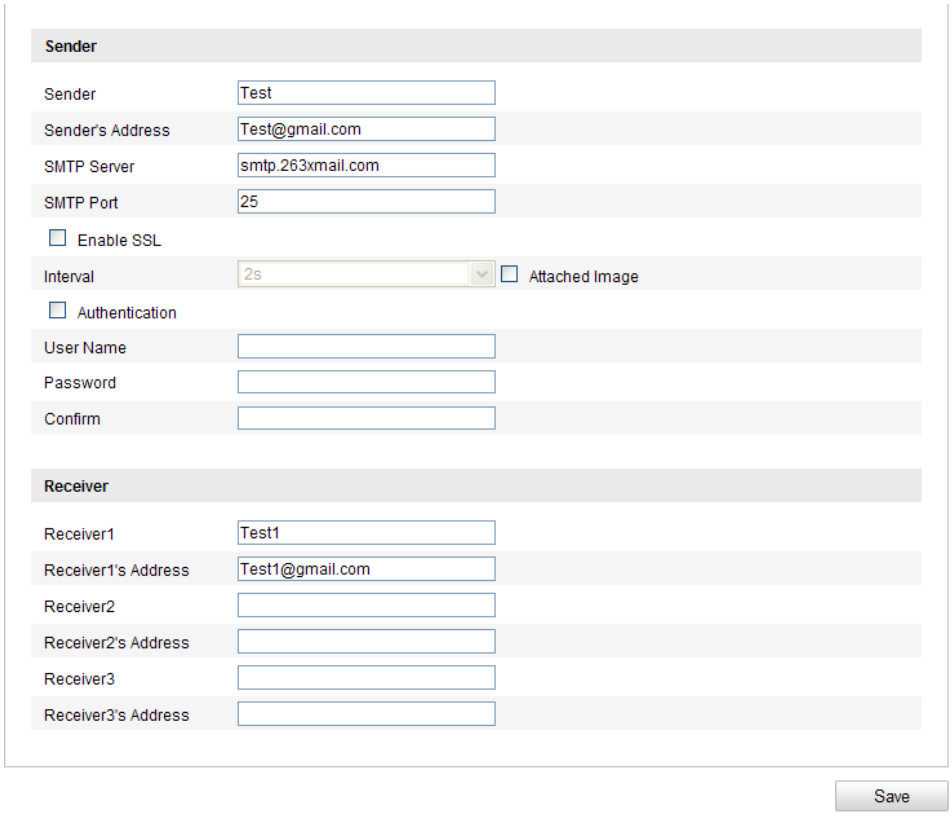


Figure 6-20 Email Settings

3. Configure the following settings:

Sender: The name of the email sender.

Sender's Address: The email address of the sender.

SMTP Server: The SMTP Server IP address or host name (e.g., smtp.263xmail.com).

SMTP Port: The SMTP port. The default TCP/IP port for SMTP is 25 (not secured). And the SSL SMTP port is 465.

Enable SSL: Check the checkbox to enable SSL if it is required by the SMTP server.

Attached Image: Check the checkbox of Attached Image if you want to send emails with attached alarm images.

Interval: The interval refers to the time between two actions of sending attached pictures.

Authentication (optional): If your email server requires authentication, check this checkbox to use authentication to log in to this server and enter the login user Name and password.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Choose Receiver: Select the receiver to which the email is sent. Up to 2 receivers can be configured.

Receiver: The name of the user to be notified.

Receiver's Address: The email address of user to be notified.

4. Click **Save** to save the settings.

6.3.11 Configuring NAT (Network Address Translation) Settings

Purpose:

1. Enter the NAT settings interface.

   Configuration >Advanced Configuration > Network > NAT

2. Choose the port mapping mode.

   To port mapping with the default port numbers:

   Choose Port Mapping Mode as **Auto**.

To port mapping with the customized port numbers:

Choose Port Mapping Mode as **Manual**.

And for manual port mapping, you can customize the value of the port number by yourself.

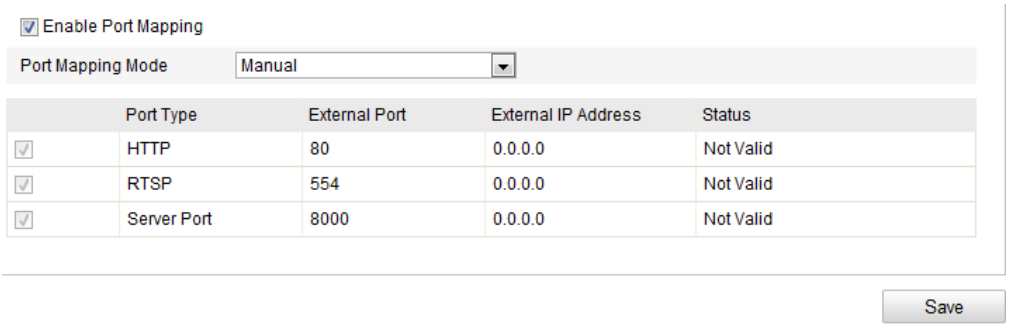


Figure 6-21 Configure NAT Settings

3. Click **Save** to save the settings.

6.3.12 Configuring FTP Settings

Purpose:

You can configure the FTP server related information to enable the uploading of the captured pictures to the FTP server. The captured pictures can be triggered by events or a timing snapshot task.

Steps:

1. Enter the FTP Settings interface:
   Configuration >Advanced Configuration > Network > FTP

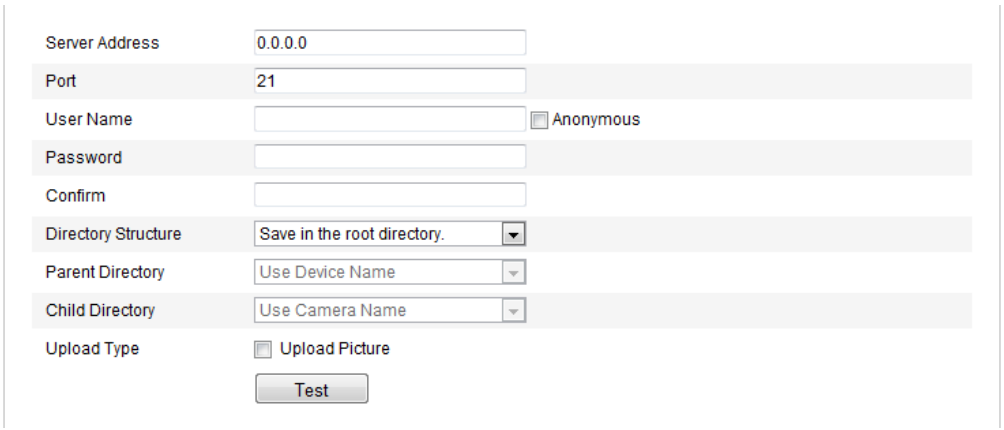


Figure 6-22 FTP Settings

2. Configure the FTP settings; and the user name and password are required for

login the FTP server.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Directory: In the **Directory Structure** field, you can select the root directory, parent directory and child directory. When the parent directory is selected, you have the option to use the Device Name, Device Number or Device IP for the name of the directory; and when the Child Directory is selected, you can use the Camera Name or Camera No. as the name of the directory.

Upload type: To enable uploading the captured picture to the FTP server.

Anonymous Access to the FTP Server (in which case the user name and password won't be required.): Check the **Anonymous** checkbox to enable the anonymous access to the FTP server.

Note: The anonymous access function must be supported by the FTP server.

3. Click **Save** to save the settings.

   Note: If you want to upload the captured pictures to FTP server, you have to enable the timing snapshot or event-triggered snapshot on **Snapshot** page. For detailed information, please refer to the *Section 7.3.*

6.3.13 Platform Access

Platform access provides you an option to manage the devices via EZVIZ Cloud P2P platform.

Note: Platform access function varies according to the camera model and it requires

for the support of the camera.

Check the checkbox of **Enable** to enable the EZVIZ Cloud P2P, and you are able to manage the device via EZVIZ Cloud P2P website, or EZVIZ Cloud P2P client, which is a mobile phone app.

For some users don't want to manage the devices via EZVIZ Cloud P2P, you can just simply leave the checkbox unchecked.

Figure 6-23 Platform Access

6.3.14 HTTPS Settings

Purpose:

HTTPS provides authentication of the web site and associated web server that one is communicating with, which protects against Man-in-the-middle attacks. Perform the following steps to set the port number of https.

E.g.: If you set the port number as 443 and the IP address is 192.168.1.64, you may access the device by inputting https://192.168.1.64:443 via the web browser.

Steps:

1. Enter the HTTPS settings interface.

   Configuration > Advanced Configuration > Network > HTTPS

2. Check the checkbox of Enable HTTPS to enable the function.
3. Create the self-signed certificate or authorized certificate.

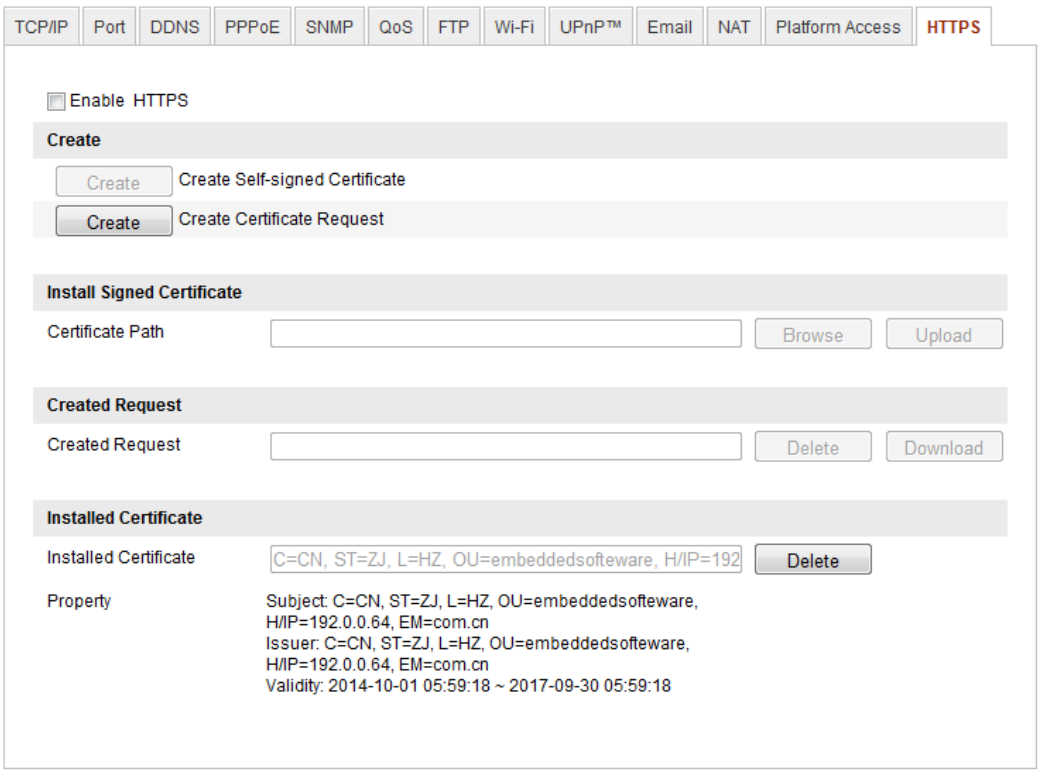


Figure 6-24 HTTPS Settings

- Create the self-signed certificate

1) Click **Create** button to enter the creation interface.

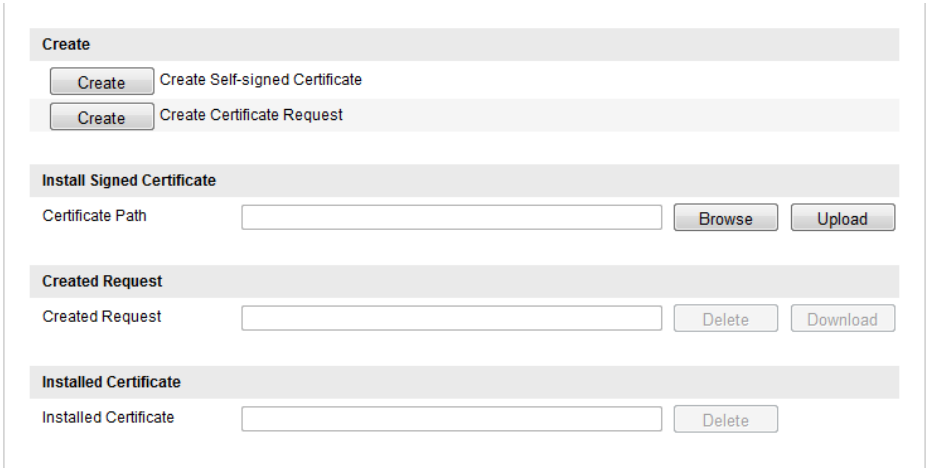


Figure 6-25 Create Self-signed Certificate

2) Enter the country, host name/IP, validity and other information.

3) Click **OK** to save the settings.

Note: If you already had a certificate installed, the Create Self-signed Certificate is grayed out.

- Create the authorized certificate

1) Click **Create** button to create the certificate request.
2) Download the certificate request and submit it to the trusted certificate authority for signature.
3) After receiving the signed valid certificate, import the certificate to the device.

4. There will be the certificate information after you successfully create and install the certificate.

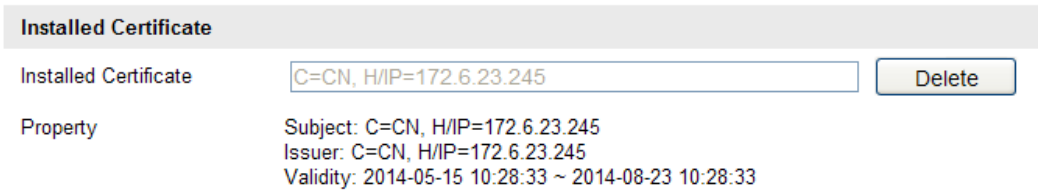


Figure 6-26 Installed Certificate

5. Click the **Save** button to save the settings.

6.4 Configuring Video and Audio Settings

6.4.1 Configuring Video Settings

Steps:

1. Enter the Video Settings interface:

Configuration >Basic Configuration > Video / Audio > Video

Or **Configuration > Advanced Configuration > Video / Audio > Video**

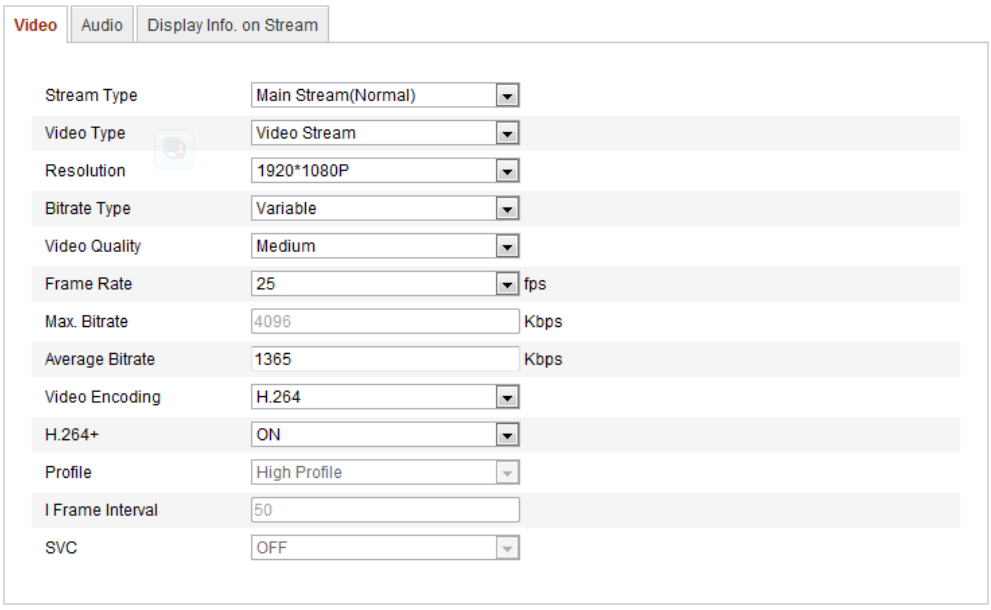


Figure 6-27 Video Settings

2. Select the **Stream Type** of the camera to main stream (normal), sub-stream or third stream.

   The main stream is usually for recording and live viewing with good bandwidth, and the sub-stream and third stream can be used for live viewing when the bandwidth is limited.

3. You can customize the following parameters for the selected main stream or sub-stream:

   Video Type:

   Select the stream type to video stream, or video & audio composite stream. The audio signal will be recorded only when the **Video Type** is **Video & Audio**.

   Resolution:

   Select the resolution of the video output.

   Bitrate Type:

   Select the bitrate type to constant or variable.

   Video Quality:

   When bitrate type is selected as **Variable**, 6 levels of video quality are selectable.

   Frame Rate:

   Set the frame rate to 1/16~25 fps. The frame rate is to describe the frequency at

which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Max. Bitrate:

Set the max. bitrate to 32~16384 Kbps. The higher value corresponds to the higher video quality, but the higher bandwidth is required.

Note: The maximum limit of the max. bitrate value varies according to different camera platforms. For some certain cameras, the maximum limit is 8192Kbps or 12288Kbps.

Video Encoding:

If the **Stream Type** is set to main stream: H.264 and MPEG4 are selectable; if the stream type is set to sub stream or third stream, H.264, MJPEG, and MPEG4 are selectable.

Note: The video encoding type varies according to different camera platforms. For some certain cameras, H.265 is supported while MPEG4 is not.

H.264+:

If you set the main stream as the stream type, and H.264 as the video coding, you can see H.264+ is available. H.264+ is an advanced compression coding technology. By enabling H.264+, user can calculate the HDD consumption by its average bitrate, and save the storage by lowering the bitrate as well.You need to reboot the camera if you want to turn on or turn off the H.264+.

After H.264+ is enabled, when you set the Variable as the bitrate type, average bitrate is configurable, and you can calculate the HDD consumption according to the average bitrage, or you can set the average bitrate manually, which should be smaller than Max. bitrate.

Profile:

Basic profile, Main Profile and High Profile for coding are selectable.

I Frame Interval:

Set the I-Frame interval to 1~400.

SVC:

Scalable Video Coding is an extension of the H.264/AVC standard. Select OFF / ON to disable / enable the SVC function. Select Auto, and the device will automatically extract frames from the original video when the network bandwidth is insufficient.

Smoothing:

It refers to the smoothness of the stream. The higher value of the smoothing, the better fluency of the stream, though, the video quality may not be so satisfied. The lower value of the smoothing, the higher quality of the stream, though it may appear not fluent.

4. Click **Save** to save the settings.

6.4.2 Configuring Audio Settings

Steps:

1. Enter the Audio Settings interface

   Configuration > Basic Configuration > Video / Audio > Audio

   Or **Configuration > Advanced Configuration > Video / Audio > Audio**

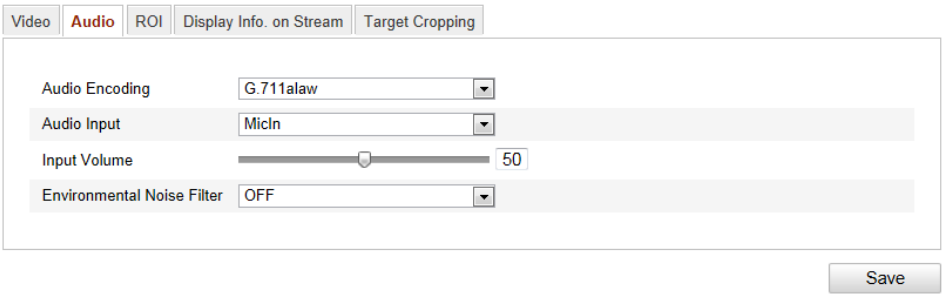


Figure 6-28 Audio Settings

2. Configure the following settings.

   Note: Audio settings vary according to different camera models.

   Audio Encoding: G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2 and PCM are selectable. For MP2L2, the sampling rate and audio stream bitrate are configurable; for PCM, the sampling rate can be set.

   Audio Input: MicIn and LineIn are selectable for the connected microphone and pickup respectively.

Input Volume: 0-100

Environmental Noise Filter: Set it as OFF or ON. When the function is enabled, the noise in the environment can be filtered to some extent.

3. Click **Save** to save the settings.

6.4.3 Configuring ROI Encoding

Purpose:

ROI (Region of Interest) encoding helps to discriminate the ROI and background information in video compression, which means, the technology assigns more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

Note: ROI function varies according to different camera models.

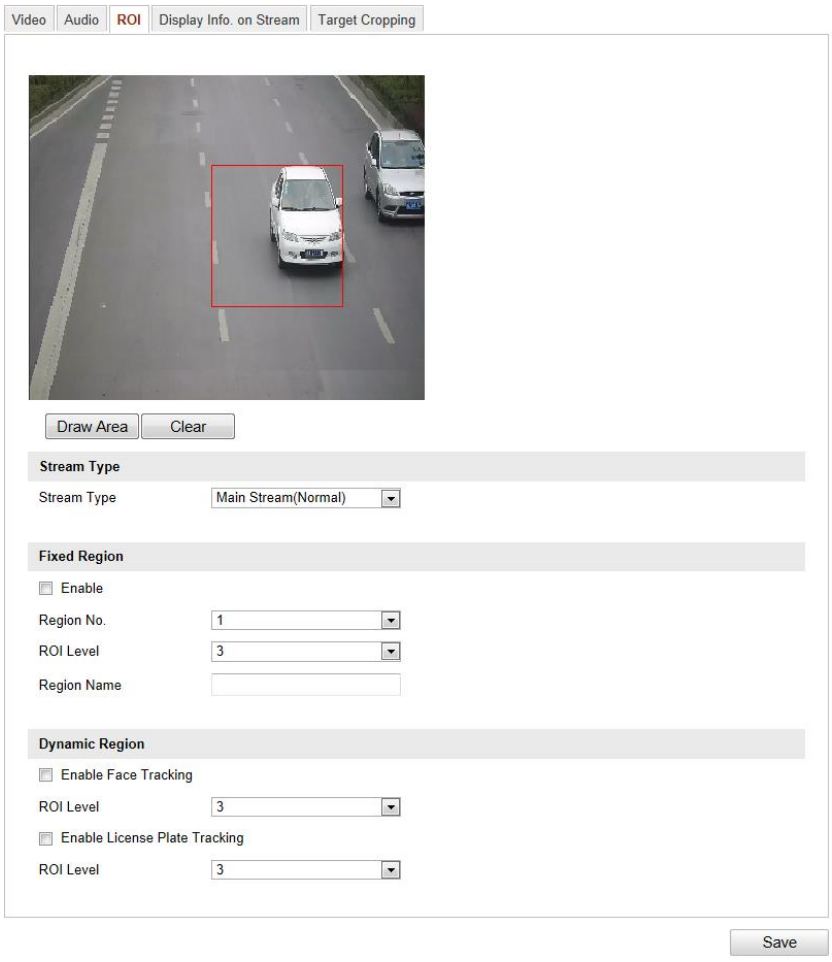


Figure 6-29 Region of Interest Settings

Configuring Fixed Region for ROI:

Steps:

1. Enter the ROI settings interface:

   Configuration> Advanced Configuration> Video/Audio> ROI
2. Check the checkbox of **Enable** under Fixed Region item.
3. Select the stream type for ROI encoding.
4. Select the region from the drop-down list for ROI settings. There are four fixed regions selectable.
5. Click the **Draw Area** button, and then click-and-drag the mouse to draw the region of interest on the live video.
6. Select the ROI level to set the image quality enhancing level. The larger the value is, the better the image quality is.
7. Input the region name for ROI as desired.
8. Click **Save** to save the settings.

Configuring Dynamic Region for ROI:

1. Enter the ROI settings interface:

   Configuration> Advanced Configuration> Video/Audio> ROI
2. Check the checkbox of **Enable Face Tracking**, and then the captured face picture is set as region of interest.

   Note: To enable face tracking function, the face detection function should be supported and enabled.
3. Check the checkbox of **Enable License Plate Tracking**, and then the captured license plate picture is set as region of interest.

   Note: To enable license plate tracking function, the vehicle detection function should be supported and enabled.
4. Respectively set the ROI level. The larger the value is, the better the image quality is.
5. Select the stream type for ROI encoding.

6. Click **Save** to save the settings.

6.4.4 Display Information on Stream

Check the checkbox of **Enable Dual-VCA**, and the information of the objects (e.g. human, vehicle, etc.) will be marked in the video stream. And then you can set rules on the connected rear-end device to detect the events including line crossing, intrusion, etc.

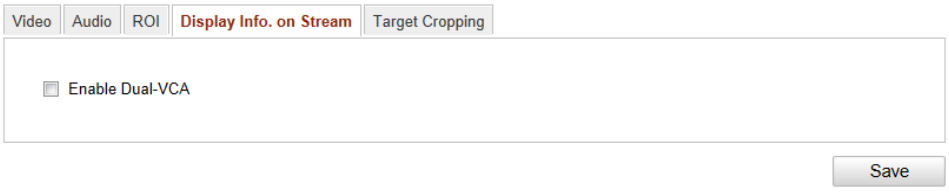


Figure 6-30 Display Info. on Stream

6.4.5 Configuring Target Cropping

Purpose:

You can specify a target area on the live video, and then it can be displayed via the third stream in some certain resolution, thus providing more details of the target area if needed.

Note: Target cropping function varies according to different camera models.

Steps:

1. Enter the Target Cropping settings interface:
   Configuration> Advanced Configuration> Video/Audio> Target Cropping.
2. Check the checkbox of **Enable Target Cropping** to enable the function.
3. Set Third Stream as the stream type.
4. Select the cropping resolution for the video display of target area. A red rectangle is displayed on the live video to mark the target area, and you can click-and-drag the rectangle to locate the target area as desired.
5. Click **Save** to save the settings. You can go to the Live View page and click the

Third Stream tab to view the video of the target area.

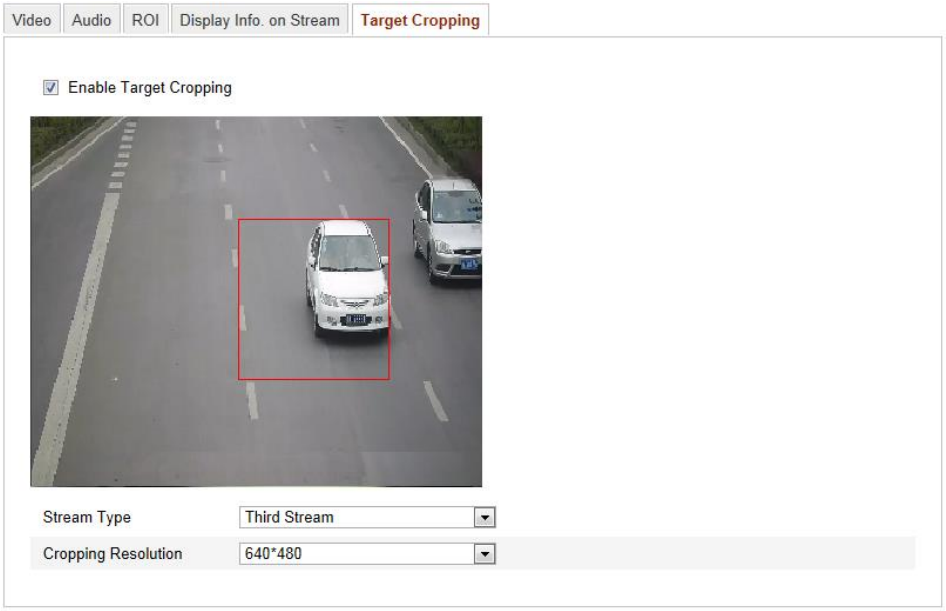


Figure 6-31 Target Cropping

6.5 Configuring Image Parameters

6.5.1 Configuring Display Settings

Purpose:

You can set the image quality of the camera, including brightness, contrast, saturation, hue, sharpness, etc.

Note: The display parameters vary according to the different camera model. Please refer to the actual interface for details.

Steps:

1. Enter the Display Settings interface:

   Configuration > Basic Configuration> Image> Display Settings

   Or **Configuration > Advanced Configuration> Image> Display Settings**

2. Set the image parameters of the camera.

Note: In order to guarantee the image quality in the different illumination, it provides two sets of parameters for user to configure.

Day/Night Auto-switch

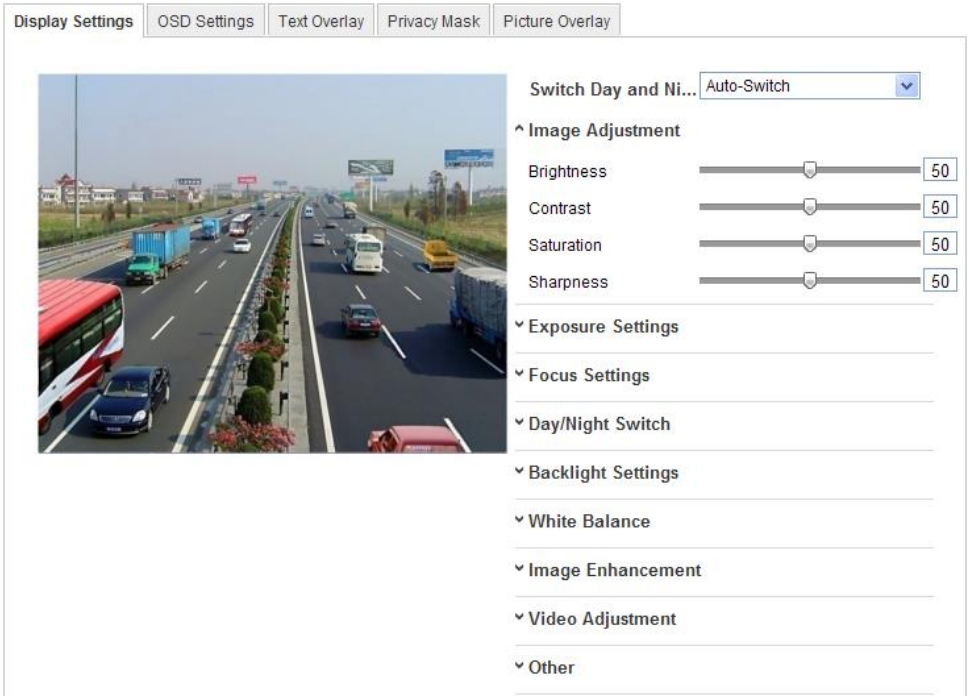


Figure 6-32 Display Settings of Day/night Auto-switch

♦ Image Adjustment

Brightness describes bright of the image, which ranges from 1~100, and the default value is 50.

Contrast describes the contrast of the image, which ranges from 1~100, and the default value is 50.

Saturation describes the colorfulness of the image color, which ranges from 1~100, and the default value is 50.

Sharpness describes the edge contrast of the image, which ranges from 1~100, and the default value is 50.

♦ Exposure Settings

If the camera is equipped with the fixed lens, only **Manual** is selectable, and the iris mode is not configurable.

If **Auto** is selected, you can set the auto iris level from 0~ 100.

For the camera supports **P-Iris** lens, if P-Iris lens is adopted, then the P-Iris lens type is selectable, e.g.: Tamron 2.8-8mm F1.2 (M13VP288-IR), or if DC lens is adopted, then manual and auto are selectable.

The exposure time refers to the electronic shutter time, which ranges from 1 ~

1/100,000s. Adjust it according to the actual luminance condition.

♦ **Focus Settings**

For the camera supports electronic lens, you can set the focus mode as Auto, Manual or Semi-auto. If auto is selected, the focus is adjusted automatically according to the actual monitoring scenario; if manual is selected, you can control the lens by adjusting the zoom, focus, lens initialization, and auxiliary focus via the PTZ control interface; if semi-auto is selected, the camera will focus automatically when you adjust the zoom parameters.

♦ **Day/Night Switch**

Select the day/night switch mode, and configure the smart IR settings from this option.

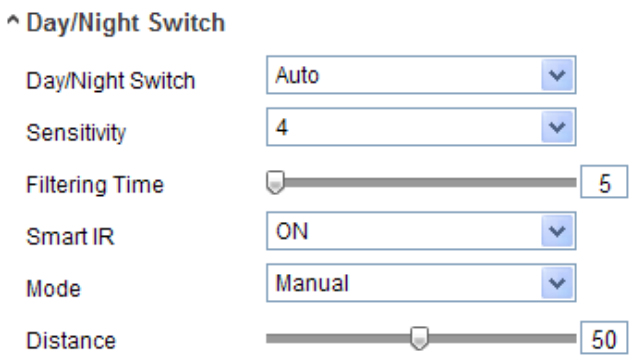


Figure 6-33 Day/Night Switch

Day, night, auto, schedule, and triggered by alarm input are selectable for day/night switch.

Day: the camera stays at day mode.

Night: the camera stays at night mode.

Auto: the camera switches between the day mode and the night mode according to the illumination automatically. The sensitivity ranges from 0~7, the higher the value is, the easier the mode switches. The filtering time refers to the interval time between the day/night switch. You can set it from 5s to 120s.

Schedule: Set the start time and the end time to define the duration for day/night mode.

Triggered by alarm input: The switch is triggered by alarm input, and you can set

the triggered mode to day or night.

Smart IR: Smart IR function gives user an option to adjust the power of the IR LED, thus providing a clear image that is not overexposed or too dark. Select ON to enable the smart IR, and then Auto and Manual are selectable for IR mode.

Select AUTO, and the power of IR LED changes automatically according to the actual luminance. E.g.: if the current scene is bright enough, then the IR LED adjusts itself to lower power; and if the scene is not bright enough, the IR LED adjusts itself to higher power.

Select Manual, and you can manually set the value of distance between the IR camera and object, to adjust the power of IR LED. Small distance value indicates the object is near the IR camera, and the device adjusts the IR LED to lower power to avoid overexposure; large distance value indicates the object is far away, and the device adjusts the IR LED to higher power to avoid too dark image.

♦ **Backlight Settings**

BLC: If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC compensates light to the object in the front to make it clear. OFF, Up, Down, Left, Right, Center and customize are selectable.

WDR: Wide Dynamic Range can be used when there is a high contrast of the bright area and the dark area of the scene.

HLC: High Light Compression function can be used when there are strong lights in the scene affecting the image quality.

♦ **White Balance**

White balance is the white rendition function of the camera used to adjust the color temperature according to the environment.

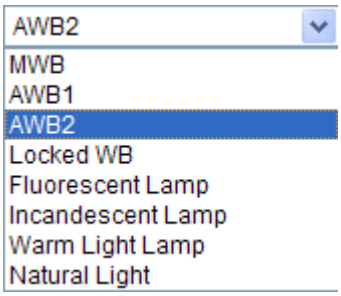


Figure 6-34 White Balance

♦ **Image Enhancement**

Digital Noise Reduction: DNR reduces the noise in the video stream. OFF, Normal Mode and Expert Mode are selectable. Set the DNR level from 0~100, and the default value is 50 in Normal Mode. Set the DNR level from both space DNR level [0~100] and time DNR level [0~100] in Expert Mode.

Defog Mode: You can enable the defog function when the environment is foggy and the image is misty. It enhances the subtle details so that the image appears clearer.

Electrical Image Stabilizer: EIS reduces the effects of vibration in a video.

Grey Scale: You can choose the range of the grey scale as [0-255] or [16-235].

♦ **Video Adjustment**

Mirror: It mirrors the image so you can see it inversed. Left/Right, Up/Down, Center, and OFF are selectable.

Rotate: To make a complete use of the 16:9 aspect ratio, you can enable the rotate function when you use the camera in a narrow view scene.

When installing, turn the camera to the 90 degrees or rotate the 3-axis lens to 90 degrees, and set the rotate mode as on, you will get a normal view of the scene with 9:16 aspect ratio to ignore the needless information such as the wall, and get more meaningful information of the scene.

Scene Mode: Choose the scene as indoor or outdoor according to the real environment.

Video Standard: 50 Hz and 60 Hz are selectable. Choose according to the different video standards; normally 50 Hz for PAL standard and 60 Hz for NTSC standard.

Capture Mode: It's the selectable video input mode to meet the different demands of field of view and resolution.

Lens Distortion Correction: Select ON / OFF to enable / disable the lens distortion correction. The distorted image caused by the wide-angle lens can be corrected if this function enabled.

♦ **Other**

Some of the camera supports CVBS, SDI, or HDMI output. Please refer to the actual camera model for details.

Day/Night Scheduled-Switch

Day/Night scheduled-switch configuration interface enables you to set the separate camera parameters for day and night to guarantee the image quality in different illumination.

Figure 6-35 Day/Night Scheduled-Switch Configuration Interface

Steps:

1. Click the time line to select the start time and the end time of the switch.
2. Click Common tab to configure the common parameters applicable to the day mode and night mode.

   Note: The detailed information of each parameter please refers to day/night auto switch session.
3. Click Day tab to configure the parameters applicable for day mode.
4. Click Night tab to configure the parameters applicable for night mode.

   Note: The settings saved automatically if any parameter is changed.

6.5.2 Configuring OSD Settings

Purpose:

You can customize the camera name and time on the screen.

Steps:

1. Enter the OSD Settings interface:

   Configuration > Advanced Configuration > Image > OSD Settings

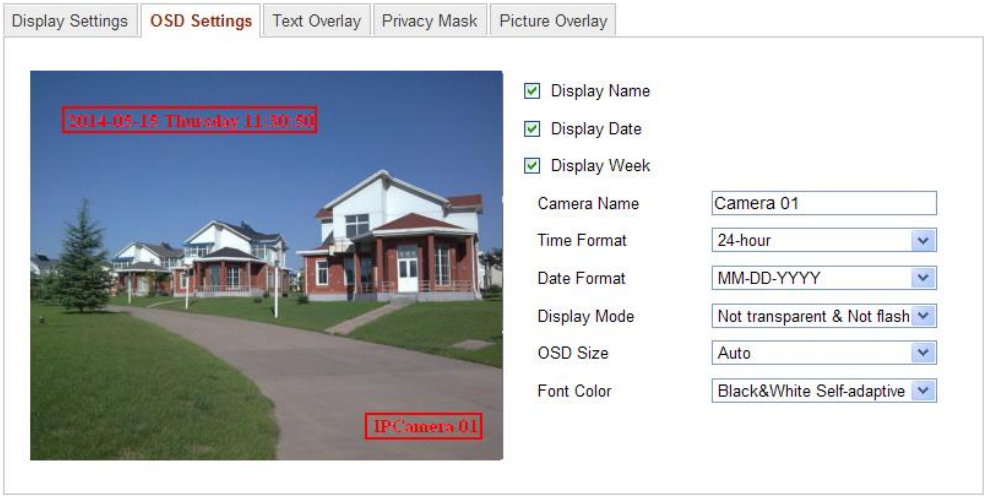


Figure 6-36 OSD Settings

2. Check the corresponding checkbox to select the display of camera name, date or week if required.
3. Edit the camera name in the text field of **Camera Name**.
4. Select from the drop-down list to set the time format, date format, display mode and the OSD font size.
5. Define the font color of the OSD by clicking the drop-down, and black & white self-adaptive and custom are selectable.

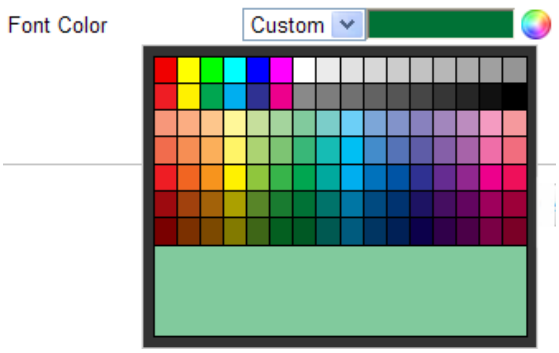


Figure 6-37 Font Color-Custom

6. You can use the mouse to click and drag the text frame IPCamera 01 in the live view window to adjust the OSD position.

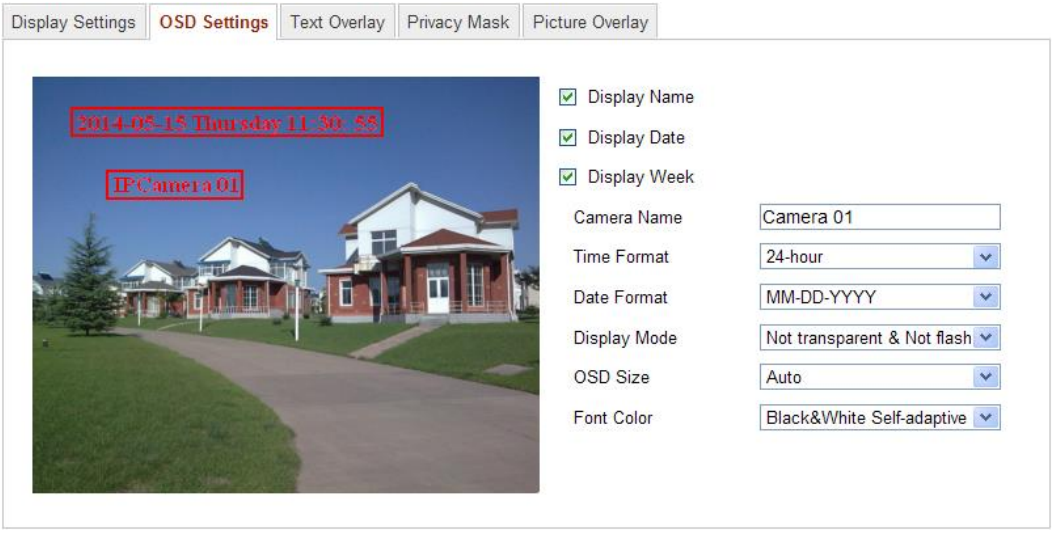


Figure 6-38 Adjust OSD Location

7. Click **Save** to activate the above settings.

6.5.3 Configuring Text Overlay Settings

Purpose:

You can customize the text overlay.

Steps:

1. Enter the Text Overlay Settings interface:

Configuration > Advanced Configuration > Image > Text Overlay

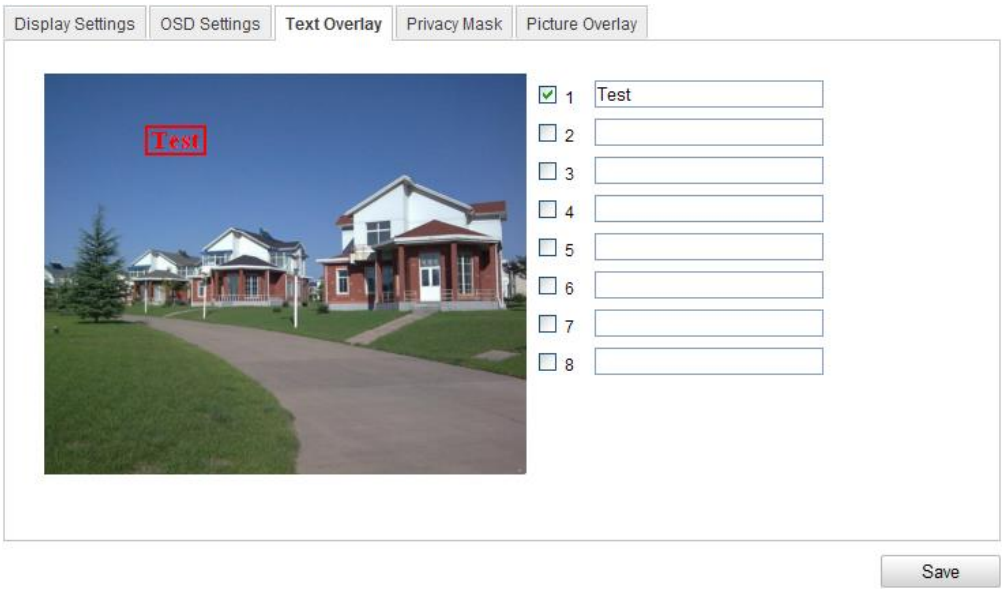


Figure 6-39 Text Overlay

2. Check the checkbox in front of textbox to enable the on-screen display.
3. Input the characters in the textbox.
4. (Optional)Use the mouse to click and drag the red text frame

in the live view window to adjust the text overlay position.
5. Click **Save** to save the settings.

Note: Up to 8 text overlays are configurable.

6.5.4 Configuring Privacy Mask

Purpose:

Privacy mask enables you to cover certain areas on the live video to prevent certain spots in the surveillance area from being live viewed and recorded.

Steps:

1. Enter the Privacy Mask Settings interface:

Configuration > Advanced Configuration> Image > Privacy Mask

2. Check the checkbox of **Enable Privacy Mask** to enable this function.
3. Click **Draw Area**.

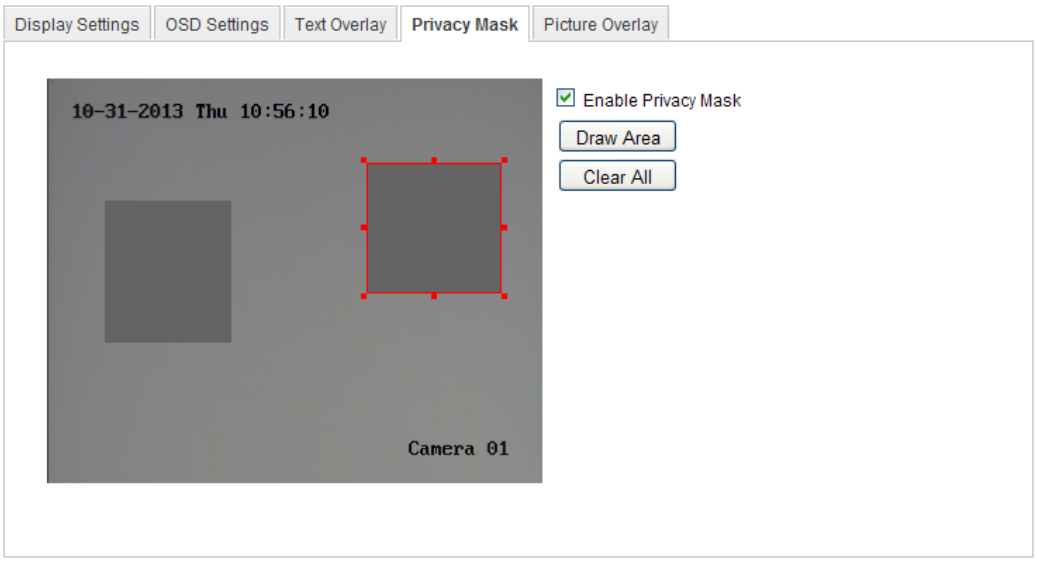


Figure 6-40 Privacy Mask Settings

4. Click and drag the mouse in the live video window to draw the mask area.

Note: You are allowed to draw up to 4 areas on the same image.

5. Click **Stop Drawing** to finish drawing or click **Clear All** to clear all of the areas you set without saving them.

6. Click **Save** to save the settings.

6.5.5 Configuring Picture Overlay

Purpose:

Picture overlay enables you to overlay a picture on the image. This function enables a certain enterprise or users to overlay their logo on the image.

Note: The picture must be in RGB24 bmp format and the maximum size of the picture is 128*128.

Steps:

1. Enter the Picture Overlay Settings interface:

Configuration > Advanced Configuration> Image > Picture Overlay

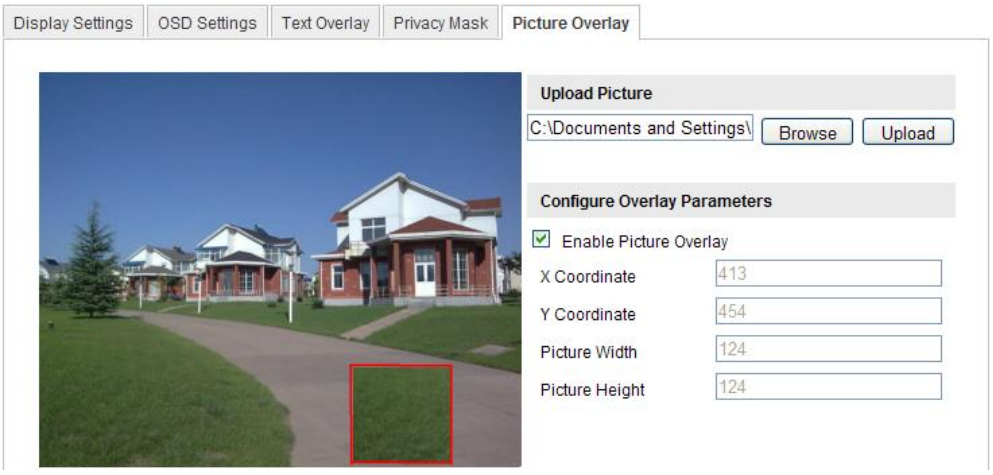


Figure 6-41 Picture Overlay

2. Click **Browse** to select a picture.
3. Click **Upload** to upload it.
4. Check **Enable Picture Overlay** checkbox to enable the function.

X Coordinate and Y Coordinate values are for the location of the picture on the image. And the Picture width and height shows the size of the picture.

6.6 Configuring and Handling Basic Events

This section explains how to configure the network camera to respond to basic events, including motion detection, video tampering, alarm input, alarm output, and exception. These events can trigger the linkage methods, such as Notify Surveillance Center, Send Email, Trigger Alarm Output, etc.

Note:

Check the checkbox of Notify Surveillance Center if you want the alarm information to be pushed to PC or mobile client software as soon as the alarm is triggered.

6.6.1 Configuring Motion Detection

Purpose:

Motion detection detects the moving objects in the configured surveillance area, and a series of actions can be taken when the alarm is triggered..

In order to detect the moving objects accurately and reduce the false alarm rate,

normal configuration and expert configuration are selectable for different motion detection environment.

➢ Normal Configuration

Normal configuration adopts the same one set of motion detection parameters in the daytime and at night.

Tasks:

1. Set the Motion Detection Area.

Steps:

(1)Enter the motion detection settings interface

Configuration > Advanced Configuration> Basic Event > Motion Detection

(2)Check the checkbox of **Enable Motion Detection**.

(3)Check the checkbox of **Enable Dynamic Analysis for Motion** if you want to mark the detected objects with green rectangles.

Note: Select Disable for rules if you don't want the detected objected displayed with the rectangles. Select disable from **Configuration-Local Configuration-Live View Parameters-rules**.

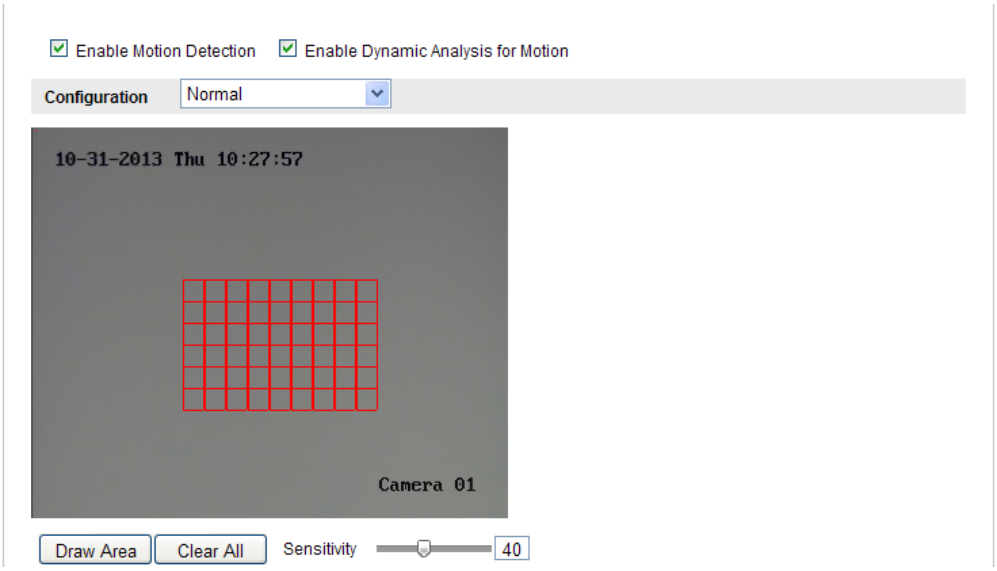


Figure 6-42 Enable Motion Detection

(4)Click **Draw Area**. Click and drag the mouse on the live video to draw a motion detection area.

(5)Click **Stop Drawing** to finish drawing one area.

(6)(Optional) Click **Clear All** to clear all of the areas.

(7)(Optional) Move the slider to set the sensitivity of the detection.

2. Set the Arming Schedule for Motion Detection.

Steps:

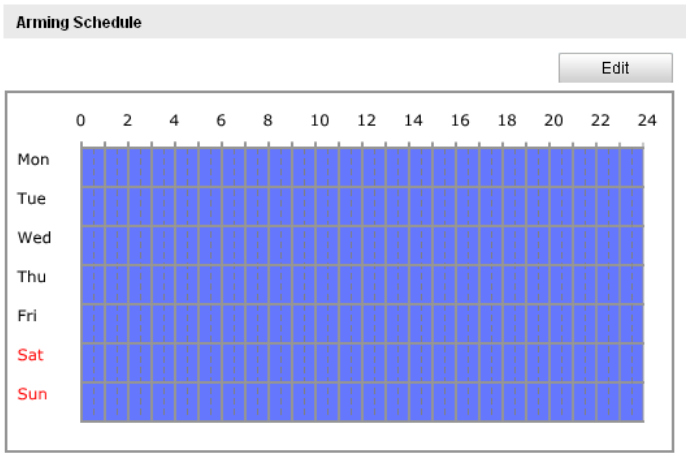


Figure 6-43 Arming Time

(1)Click **Edit** to edit the arming schedule. The Figure 6-34 shows the editing interface of the arming schedule.

(2)Choose the day you want to set the arming schedule.

(3)Click to set the time period for the arming schedule.

(4)(Optional) After you set the arming schedule, you can copy the schedule to other days.

(5)Click **OK** to save the settings.

Note: The time of each period can't be overlapped. Up to 8 periods can be configured for each day.

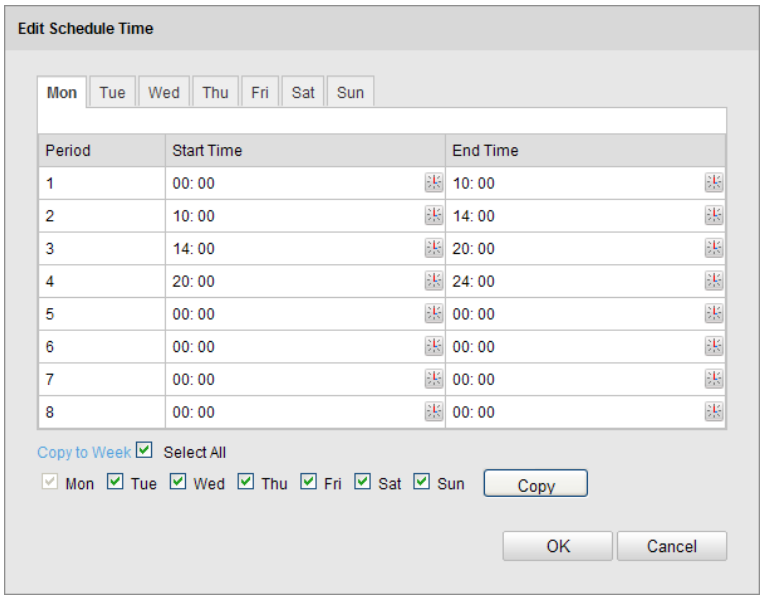


Figure 6-44 Arming Time Schedule

3. Set the Alarm Actions for Motion Detection.

Check the checkbox to select the linkage method. Notify surveillance center, send email, upload to FTP, trigger channel and trigger alarm output are selectable. You can specify the linkage method when an event occurs.

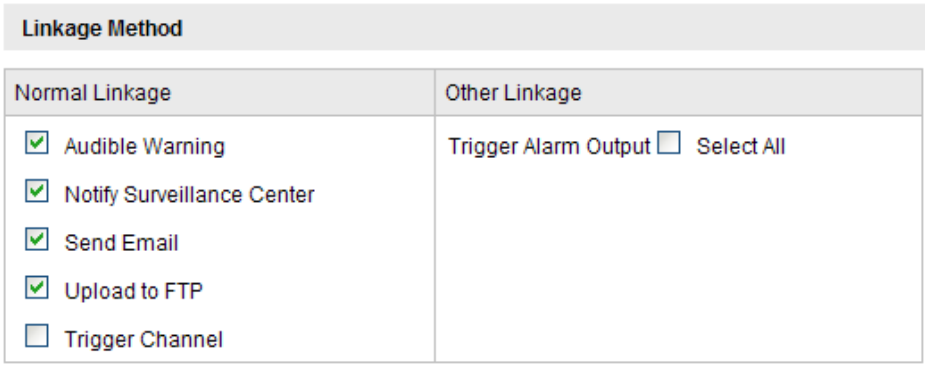


Figure 6-45 Linkage Method

- **Audible Warning**

Trigger the audible warning locally. And it only supported by the device have the audio output.

- **Notify Surveillance Center**

Send an exception or alarm signal to remote management software when an event occurs.

- **Send Email**

Send an email with alarm information to a user or users when an event occurs.

Note: To send the Email when an event occurs, you need to refer to *Section 6.3.10* ***Email Sending Triggered by Alarm*** to set the related parameters.

- **Upload to FTP**

Capture the image when an alarm is triggered and upload the picture to a FTP server.

Notes:

- Set the FTP address and the remote FTP server first. Refer to *Section 6.3.12* ***Configuring FTP Settings*** for detailed information.
- Go to **Advanced Configuration > Storage > Snapshot** page, enable the event-triggered snapshot, and set the capture interval and capture number.
- The captured image can also be uploaded to the available SD card or network disk.

- **Trigger Channel**

The video will be recorded when the motion is detected. You have to set the recording schedule to realize this function. Please refer to *Section 7.2* for detailed information.

- **Trigger Alarm Output**

Trigger one or more external alarm outputs when an event occurs.

Note: To trigger an alarm output when an event occurs, please refer to *Section 6.6.4* ***Configuring Alarm Output*** to set the related parameters.

➢ Expert Configuration

Expert mode is mainly used to configure the sensitivity and proportion of object on area of each area for different day/night switch.

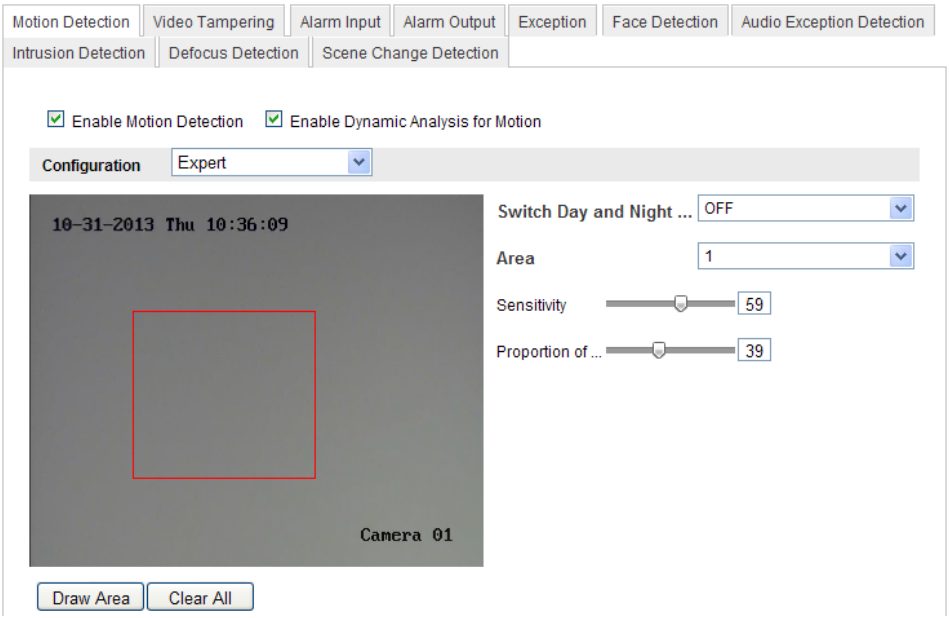


Figure 6-46 Expert Mode of Motion Detection

- Day/Night Switch OFF

Steps:

(1)Draw the detection area as in the normal configuration mode. Up to 8 areas are supported.

(2)Select **OFF** for **Switch Day and Night Settings**.

(3)Select the area by clicking the area No..

(4)Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area.

(5)Set the arming schedule and linkage method as in the normal configuration mode.

(6)Click **Save** to save the settings.

- Day/Night Auto-Switch

Steps:

(1)Draw the detection area as in the normal configuration mode. Up to 8 areas are supported.

(2)Select **Auto-Switch** for **Switch Day and Night Settings**.

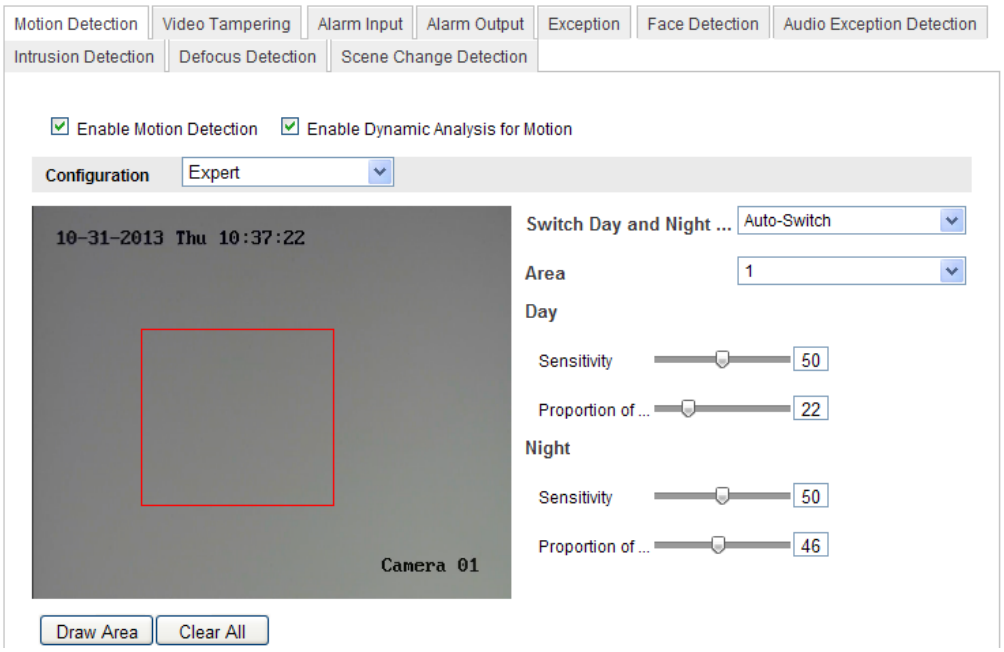


Figure 6-47 Day/Night Auto-Switch

(3)Select the area by clicking the area No.

(4)Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area in the daytime.

(5)Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area at night.

(6)Set the arming schedule and linkage method as in the normal configuration mode.

(7)Click **Save** to save the settings.

- Day/Night Scheduled-Switch

(1)Draw the detection area as in the normal configuration mode. Up to 8 areas are supported.

(2)Select **Scheduled-Switch** for **Switch Day and Night Settings**.

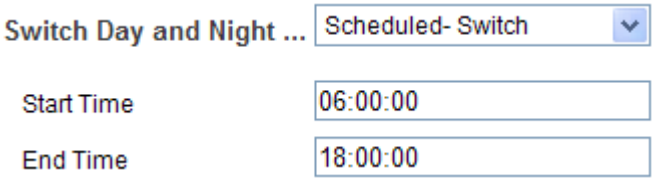


Figure 6-48 Day/Night Scheduled-Switch

(3)Select the start time and the end time for the switch timing.

(4)Select the area by clicking the area No.

(5)Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area in the daytime.

(6)Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area at night.

(7)Set the arming schedule and linkage method as in the normal configuration mode.

(8)Click **Save** to save the settings.

6.6.2 Configuring Video Tampering Alarm

Purpose:

You can configure the camera to trigger the alarm when the lens is covered and take some certain alarm response actions.

Steps:

1. Enter the video tampering Settings interface:

   Configuration > Advanced Configuration > Basic Event > Video Tampering

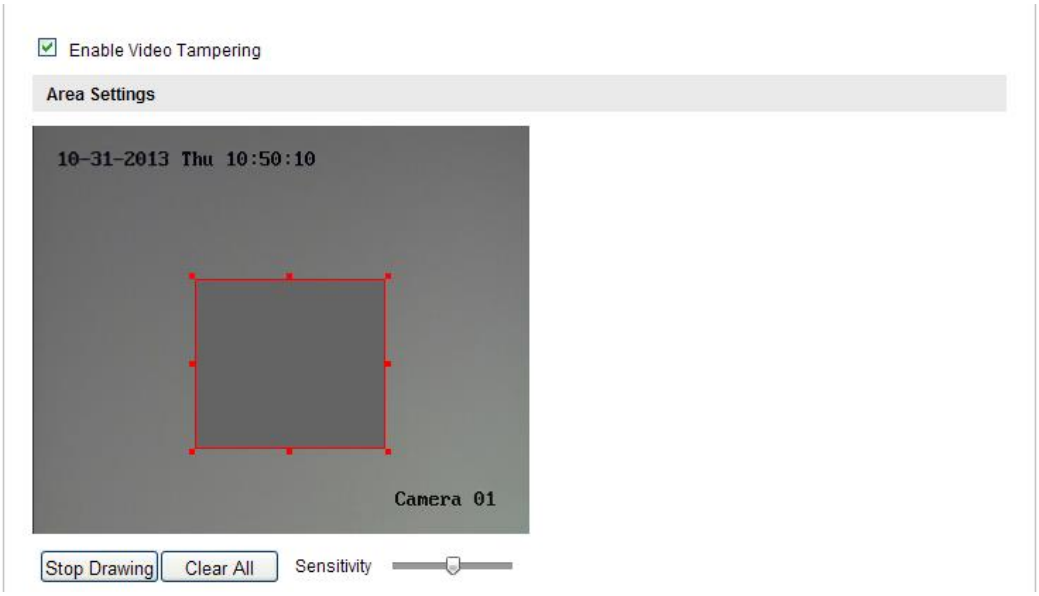


Figure 6-49 Video Tampering Alarm

2. Check **Enable Video Tampering** checkbox to enable the video tampering

detection.

3. Set the video tampering area. Refer to *Task 1* ***Set the Motion Detection Area*** in *Section 6.6.1*.
4. Click **Edit** to edit the arming schedule for video tampering. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to *Task 2* ***Set the Arming Schedule for Motion Detection*** in *Section 6.6.1*.
5. Check the checkbox to select the linkage method taken for the video tampering. Audible warning, notify surveillance center, send email and trigger alarm output are selectable. Please refer to *Task 3* ***Set the Alarm Actions for Motion Detection*** in *Section 6.6.1*.
6. Click **Save** to save the settings.

6.6.3 Configuring Alarm Input

Steps:

1. Enter the Alarm Input Settings interface:

   Configuration > Advanced Configuration> Basic Event > Alarm Input:
2. Choose the alarm input No. and the Alarm Type. The alarm type can be NO (Normally Open) and NC (Normally Closed). Edit the name to set a name for the alarm input (optional).

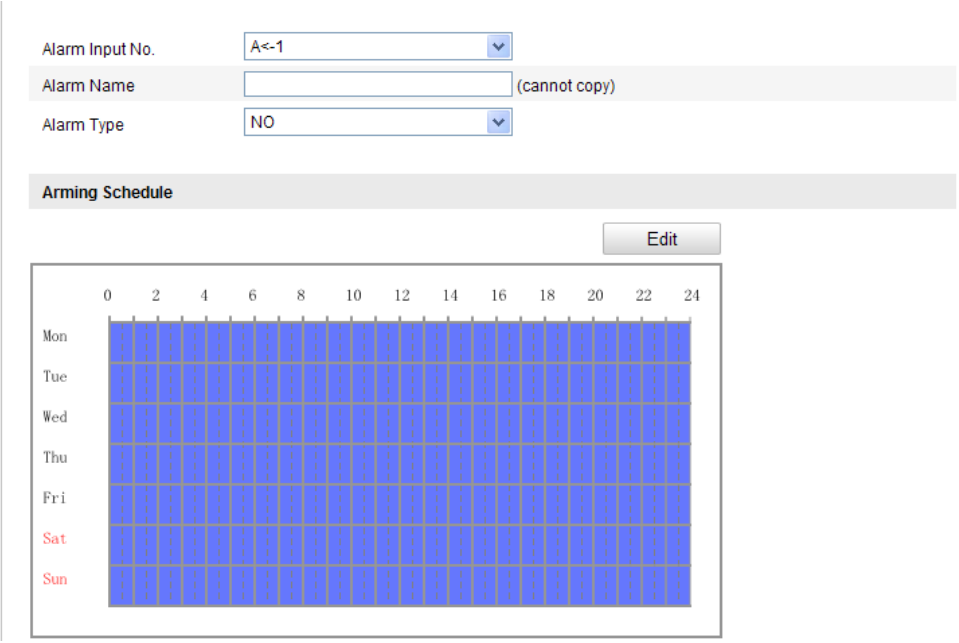


Figure 6-50 Alarm Input Settings

3. Click **Edit** to set the arming schedule for the alarm input. Refer to *Task 2* ***Set the Arming Schedule for Motion Detection*** in *Section 6.6.1*.
4. Check the checkbox to select the linkage method taken for the alarm input. Refer to *Task 3* ***Set the Alarm Actions for Motion Detection*** in *Section 6.6.1*.
5. You can also choose the PTZ linking for the alarm input if your camera is installed with a pan/tilt unit. Check the relative checkbox and select the No. to enable Preset Calling, Patrol Calling or Pattern Calling.
6. You can copy your settings to other alarm inputs.
7. Click **Save** to save the settings.

6.6.4 Configuring Alarm Output

Steps:

1. Enter the Alarm Output Settings interface:

   Configuration>Advanced Configuration> Basic Event > Alarm Output
2. Select one alarm output channel in the **Alarm Output** drop-down list. You can also set a name for the alarm output (optional).
3. The Delay time can be set to 5sec, 10sec, 30sec, 1min, 2min, 5min, 10min or

Manual. The delay time refers to the time duration that the alarm output remains in effect after alarm occurs.

4. Click **Edit** to enter the Edit Schedule Time interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection Refer to *Task 2* ***Set the Arming Schedule for Motion Detection*** in *Section 6.6.1*.
5. You can copy the settings to other alarm outputs.
6. Click **Save** to save the settings.

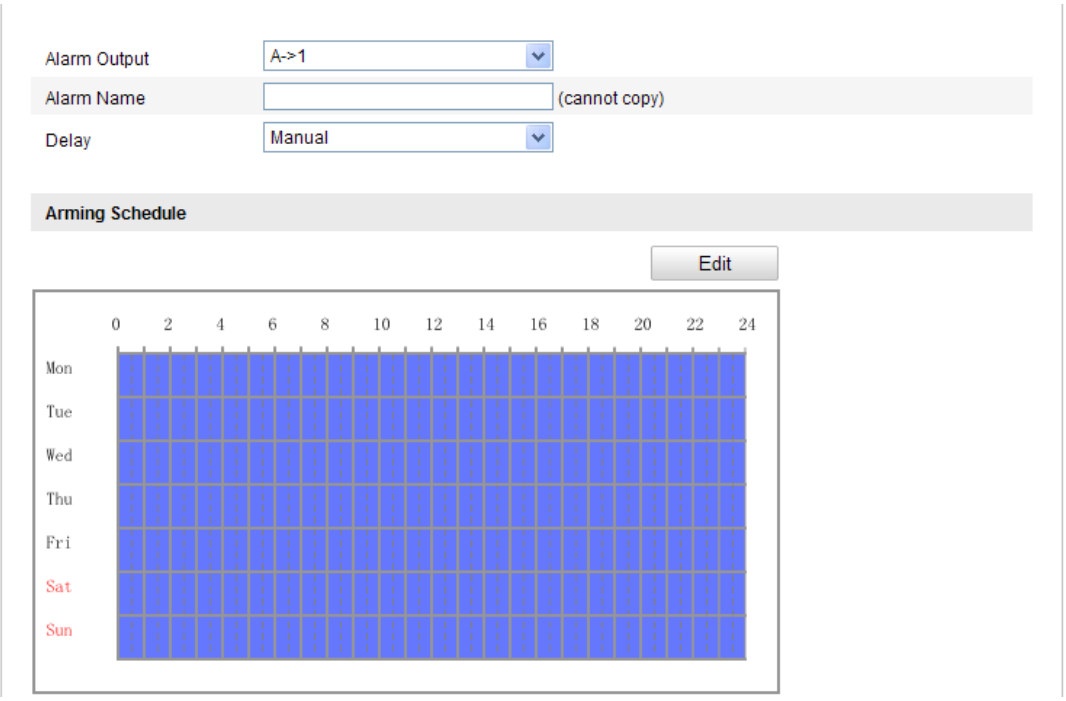


Figure 6-51 Alarm Output Settings

6.6.5 Handling Exception

The exception type can be HDD full, HDD error, network disconnected, IP address conflicted and illegal login to the cameras.

Steps:

1. Enter the Exception Settings interface:

   Configuration > Advanced Configuration> Basic Event > Exception
2. Check the checkbox to set the actions taken for the Exception alarm. Refer to

Task 3 ***Set the Alarm Actions Taken for Motion Detection*** in *Section 6.6.1*.

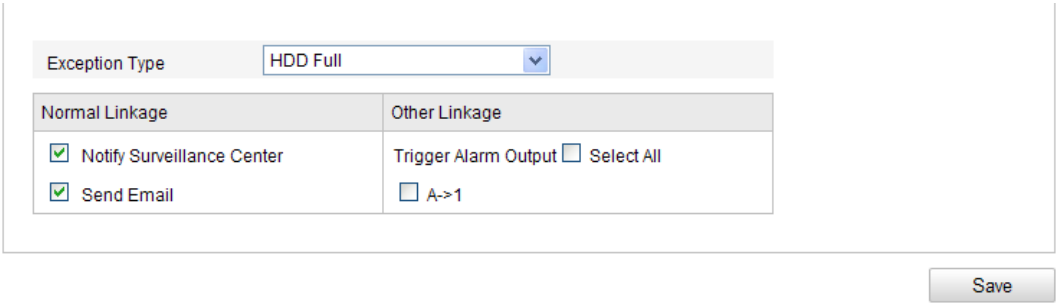


Figure 6-52 Exception Settings

3. Click **Save** to save the settings.

6.6.6 Configuring Other Alarm

Note: Some certain cameras support Wireless Alarm, PIR (passive infrared sensor) Alarm or Emergency Alarm.

- **Wireless Alarm**

Purpose:

When wireless alarm signal is sent to the camera from the detector, such as the wireless door contact, the wireless alarm is triggered and a series of response actions can be taken.

Steps:

1. Enter the Wireless Alarm Settings interface:

   Configuration > Advanced Configuration> Basic Event> Other Alarm

2. Select the wireless alarm number.

   Up to 8 channels of external wireless alarm input are supported.

3. Check the checkbox of **Enable Wireless Alarm** to activate the wireless alarm.
4. Input the alarm name in the text field as desired.
5. Check the checkbox to select the linkage methods taken for the wireless alarm.
6. Click **Save** to save the settings.
7. Locate the external wireless device beside the camera, and go to **Configuration > Advanced Configuration> System> Remote Control** to arm the camera and

study the wireless alarm.

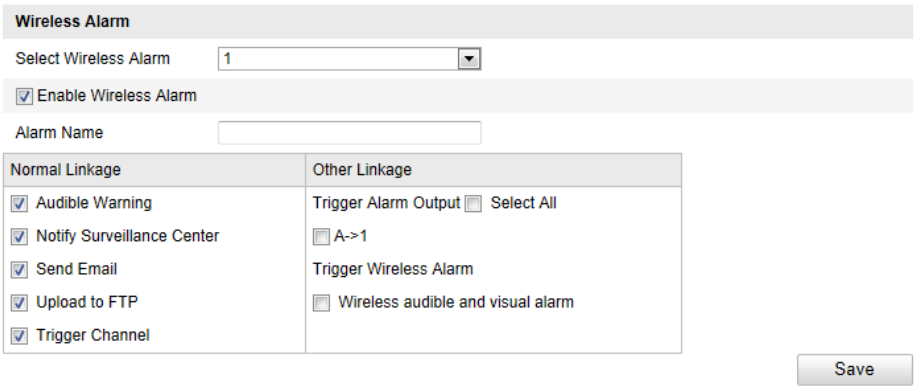


Figure 6-53 Configuring Wireless Alarm Settings

● PIR Alarm

Purpose:

A PIR (Passive Infrared) alarm is triggered when an intruder moves within the detector's field of view. The heat energy dissipated by a person, or any other warm blooded creature such as dogs, cats, etc., can be detected.

Steps:

1. Enter the PIR Alarm Settings interface:

   Configuration > Advanced Configuration> Basic Event> Other Alarm
2. Check the checkbox of **Enable PIR Alarm** to activate the PIR alarm function.
3. Input the alarm name in the text field as desired.
4. Check the checkbox to select the linkage methods taken for the PIR alarm.
5. Click the **Edit** button to set the arming schedule.
6. Click **Save** to save the settings.
7. Go to **Configuration > Advanced Configuration> System> Remote Control** to arm the camera.

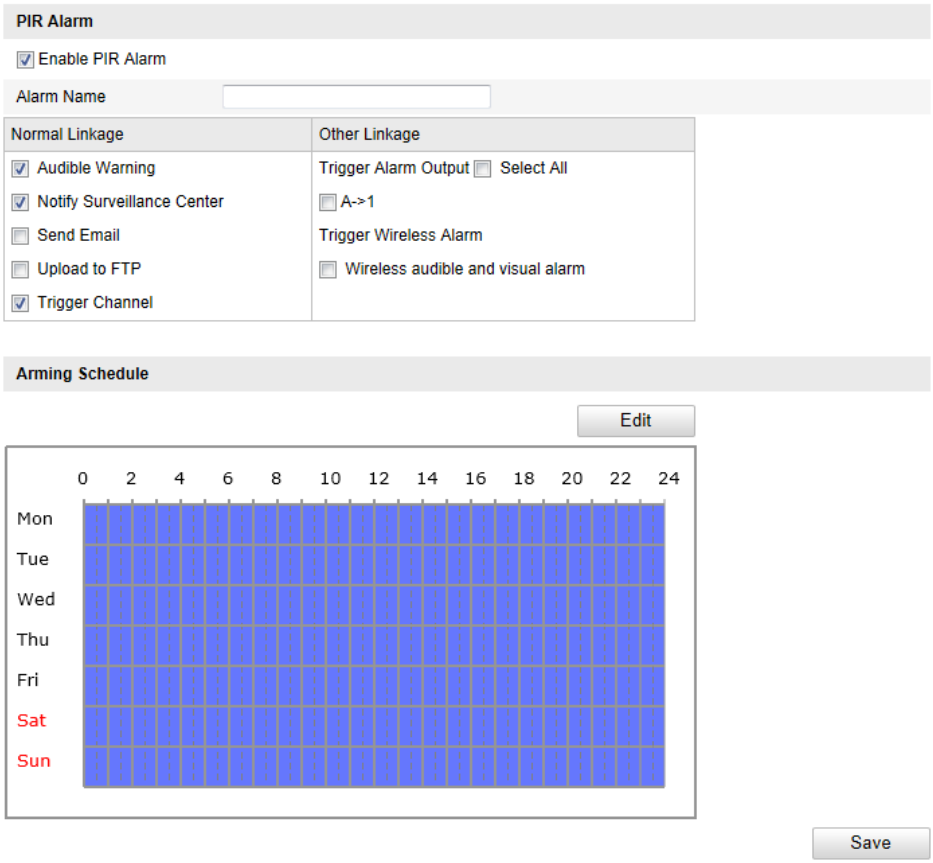


Figure 6-54 Configuring PIR Alarm Settings

● Emergency Alarm

Purpose:

You can press the Emergency button on the remote control to trigger the Emergency Alarm in case of an emergency.

Note: The remote control is required for the Emergency Alarm. Go to **Configuration > Advanced Configuration> System> Remote Control** to study the remote control first.

Steps:

1. Enter the Emergency Alarm Settings interface:

   Configuration > Advanced Configuration> Basic Event> Other Alarm

2. Check the checkbox to select the linkage methods taken for the Emergency alarm.
3. Click **Save** to save the settings.

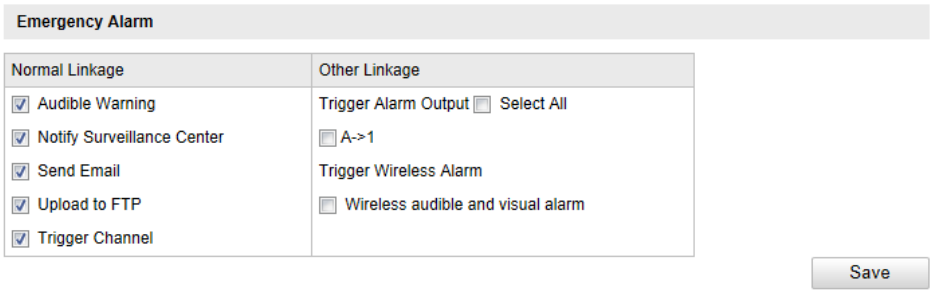


Figure 6-55 Configuring Emergency Alarm Settings

6.7 Configuring and Handling Smart Events

This section explains how to configure the network camera to respond to smart events, including face detection, audio exception detection, intrusion detection, defocus detection, scene change detection, line crossing detection, intrusion detection, region intrusion detection, region existing detection, unattended baggage detection, and object removal detection. These events can trigger the linkage methods, such as Notify Surveillance Center, Send Email, Trigger Alarm Output, etc.

Note:

Check the checkbox of Notify Surveillance Center if you want the alarm information to be pushed to PC or mobile client software as soon as the alarm is triggered.

6.7.1 Configuring Audio Exception Detection

Purpose:

Audio exception detection function detects the abnormal sounds in the surveillance scene, such as the sudden increase / decrease of the sound intensity, and some certain actions can be taken when the alarm is triggered.

Note: Audio exception detection function varies according to different camera models.

Steps:

1. Enter the Audio Exception Detection settings interface:

   Configuration > Advanced Configuration> Smart Event> Audio Exception

Detection

2. Check the checkbox of **Audio Loss Exception** to enable the audio loss detection function.
3. Check the checkbox of **Sudden Increase of Sound Intensity Detection** to detect the sound steep rise in the surveillance scene. You can set the detection sensitivity and threshold for sound steep rise.
4. Check the checkbox of **Sudden Decrease of Sound Intensity Detection** to detect the sound steep drop in the surveillance scene. You can set the detection sensitivity and threshold for sound steep drop.

   Notes:

   - Sensitivity: Range [1-100], the smaller the value is, the more severe the change should be to trigger the detection.
   - Sound Intensity Threshold: Range [1-100], it can filter the sound in the environment, the louder the environment sound, the higher the value should be. You can adjust it according to the real environment.
5. You can view the real-time volume of the sound.
6. Click the **Edit** button to set the arming schedule.
7. Select the linkage methods for audio exception, including Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel for recording and Trigger Alarm Output.
8. Click **Save** to save the settings.

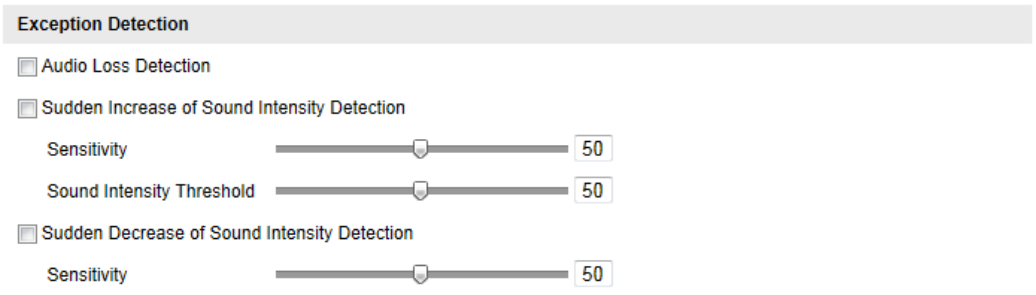


Figure 6-56 Configuring Audio Exception Detection

6.7.2 Configuring Defocus Detection

Purpose:

The image blur caused by defocus of the lens can be detected, and some certain actions can be taken when the alarm is triggered.

Note: Defocus detection function varies according to different camera models.

Steps:

1. Enter the Defocus Detection settings interface:
   Configuration> Advanced Configuration> Smart Event> Defocus Detection
2. Check the checkbox of **Enable Defocus Detection** to enable the function.
3. Click-and-drag the slider to set the detection sensitivity. The sensitivity value ranges from 1 to 100, and the higher the value is, the more easily the defocus image can trigger the alarm.
4. Select the linkage methods for defocus, including Notify Surveillance Center, Send Email and Trigger Alarm Output.
5. Click **Save** to save the settings.

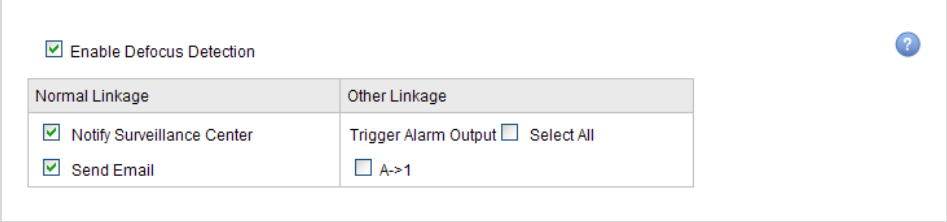


Figure 6-57 Configuring Defocus Detection

6.7.3 Configuring Scene Change Detection

Purpose:

Scene change detection function detects the change of surveillance environment affected by the external factors; such as the intentional rotation of the camera, and some certain actions can be taken when the alarm is triggered.

Note: Scene change detection function varies according to different camera models.

Steps:

1. Enter the Scene Change Detection settings interface:

   Configuration> Advanced Configuration> Smart Event> Scene Change Detection

2. Check the checkbox of **Enable Scene Change Detection** to enable the function.
3. Click-and-drag the slider to set the detection sensitivity. The sensitivity value ranges from 1 to 100, and the higher the value is, the more easily the change of scene can trigger the alarm.
4. Click the **Edit** button to set the arming schedule.
5. Select the linkage methods for scene change, including Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel and Trigger Alarm Output.
6. Click **Save** to save the settings.

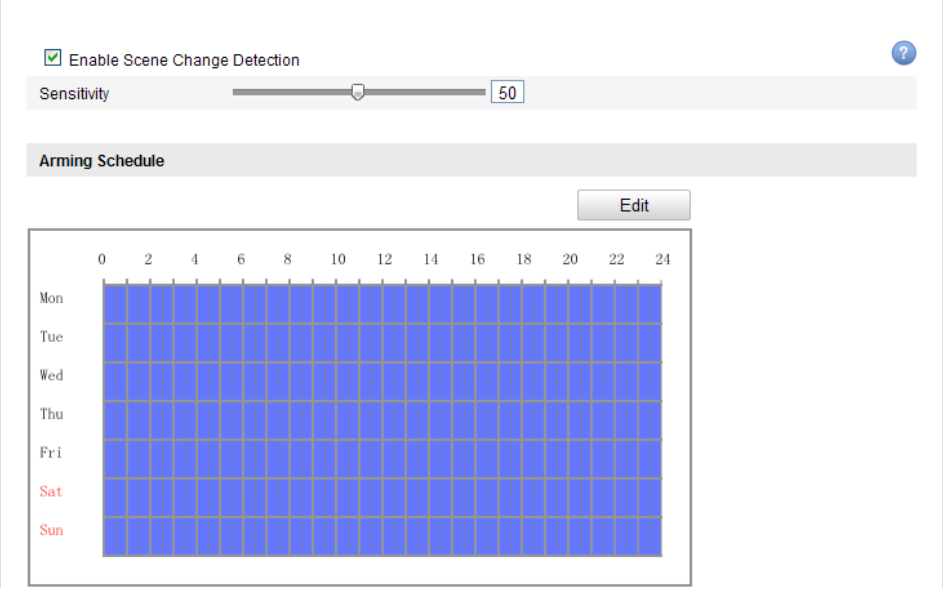


Figure 6-58 Configuring Scene Change Detection

6.7.4 Configuring Face Detection

Purpose:

Face detection function detects the face appears in the surveillance scene, and some certain actions can be taken when the alarm is triggered.

Note: Face detection function varies according to different camera models.

Steps:

1. Enter the Face Detection settings interface:

   Configuration> Advanced Configuration> Smart Event> Face Detection

2. Check the checkbox of **Enable Face Detection** to enable the function.
3. (Optional) Check the checkbox of **Enable Dynamic Analysis for Face Detection**, and then the detected face is marked with green rectangle on the live video.

   Note: To mark the detected face on the live video, go to Local Configuration> Live View Parameters and enable the Rules.

4. Click-and-drag the slider to set the detection sensitivity.

   Sensitivity: Range [1-5]. The higher the value is, the more easily the face can be detected.

5. Click the **Edit** button to set the arming schedule.
6. Select the linkage methods for face detection, including Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel and Trigger Alarm Output.
7. Click **Save** to save the settings.

Figure 6-59 Configuring Face Detection

6.7.5 Configuring Line Crossing Detection

Purpose:

Line crossing detection function detects people, vehicle or other objects which cross a pre-defined virtual line, and some certain actions can be taken when the alarm is triggered.

Note: Line crossing detection function varies according to different camera models.

Steps:

1. Enter the Line Crossing Detection settings interface:

   Configuration> Advanced Configuration> Smart Event> Line Crossing Detection

2. Check the checkbox of **Enable Line Crossing Detection** to enable the function.

3. Select the line from the drop-down list for detection settings.
4. Click the **Draw Area** button, and a virtual line is displayed on the live video.
5. Click-and-drag the line, and you can locate it on the live video as desired. Click on the line, two red squares are displayed on each end, and you can click-and-drag one of the red squares to define the shape and length of the line.
6. Select the direction for line crossing detection. And you can select the directions as A<->B, A ->B, and B->A.

   A<->B: Only the arrow on the B side shows; when an object going across the plane with both direction can be detected and alarms are triggered.

   A->B: Only the object crossing the configured line from the A side to the B side can be detected.

   B->A: Only the object crossing the configured line from the B side to the A side can be detected.
7. Click-and-drag the slider to set the detection sensitivity.

   Sensitivity: Range [1-100]. The higher the value is, the more easily the line crossing action can be detected.
8. Repeat the above steps to configure other lines. Up to 4 lines can be set. You can click the **Clear** button to clear all pre-defined lines.
9. Click the **Edit** button to set the arming schedule.
10. Select the linkage methods for line crossing detection, including Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel and Trigger Alarm Output.
11. Click **Save** to save the settings.

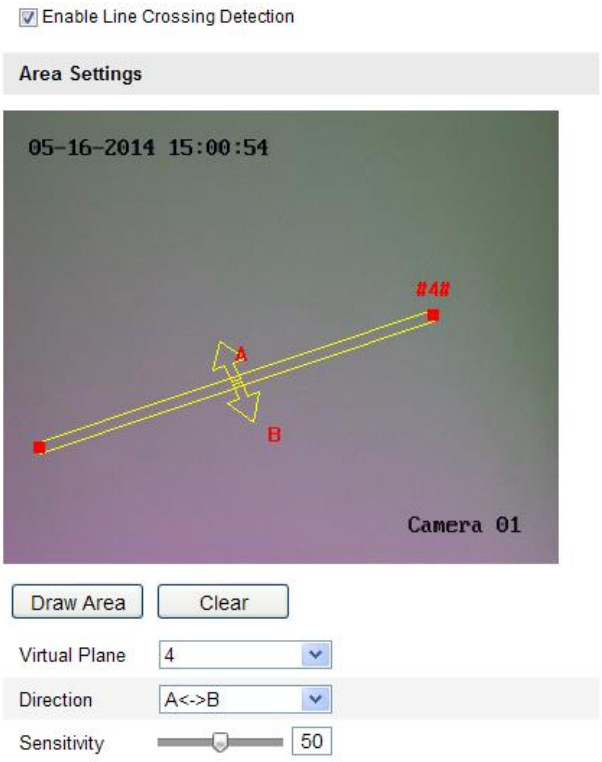


Figure 6-60 Draw Crossing Line

6.7.6 Configuring Intrusion Detection

Purpose:

Intrusion detection function detects people, vehicle or other objects which enter and loiter in a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

Note: Intrusion detection function varies according to different camera models.

Steps:

1. Enter the Intrusion Detection settings interface:

   Configuration> Advanced Configuration> Smart Event> Intrusion Detection
2. Check the checkbox of **Enable Intrusion Detection** to enable the function.
3. Select the region from the drop-down list for detection settings.
4. Click the **Draw Area** button to start the region drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.

6. Set the time threshold, detection sensitivity and object percentage for intrusion detection.

   Threshold: Range [0s-10s], the threshold for the time of the object loitering in the region. If you set the value as 0, alarm is triggered immediately after the object entering the region.

   Sensitivity: Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm. When the sensitivity is high, a very small object can trigger the alarm.

   Percentage: Range [1-100]. Percentage defines the ratio of the in-region part of the object which can trigger the alarm. For example, if the percentage is set as 50%, when the object enters the region and occupies half of the whole region, the alarm is triggered.
7. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
8. Click the **Edit** button to set the arming schedule.
9. Select the linkage methods for intrusion detection, including Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel and Trigger Alarm Output.
10. Click **Save** to save the settings.

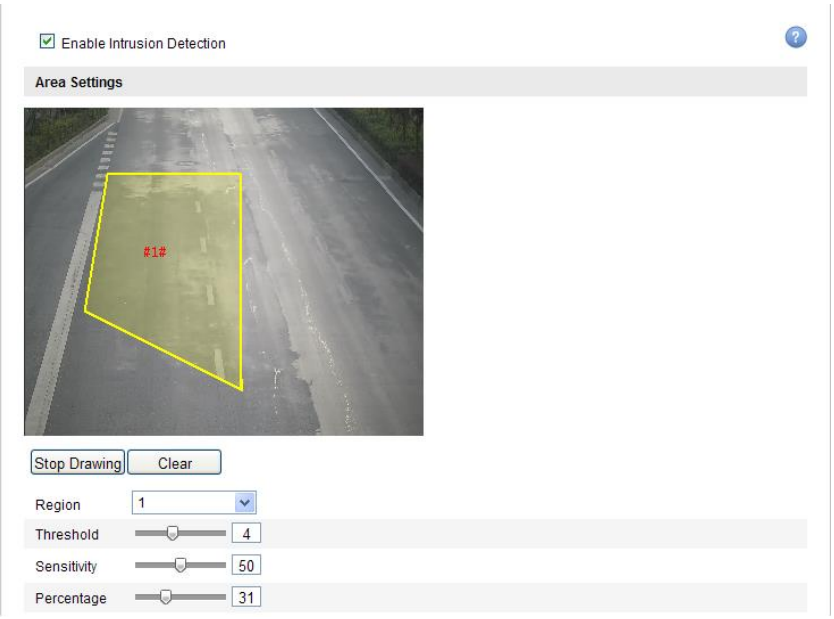


Figure 6-61 Configuring Intrusion Area

6.7.7 Configuring Region Entrance Detection

Purpose:

Region entrance detection function detects people, vehicle or other objects which enter a pre-defined virtual region from the outside place, and some certain actions can be taken when the alarm is triggered.

Note: Region entrance detection function varies according to different camera models.

Steps:

1. Enter the Region Entrance Detection settings interface:

   Configuration> Advanced Configuration> Smart Event> Region Entrance Detection
2. Check the checkbox of **Enable Region Entrance Detection** to enable the function.
3. Select the region from the drop-down list for detection settings.
4. Click the **Draw Area** button to start the region drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Click-and-drag the slider to set the detection sensitivity.

   Sensitivity: Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm. When the sensitivity is high, a very small object entering the region can trigger the alarm.
7. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the Clear button to clear all pre-defined regions.
8. Click the **Edit** button to set the arming schedule.
9. Select the linkage methods for region entrance detection, including Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel and Trigger Alarm Output.
10. Click **Save** to save the settings.

Figure 6-62 Configuring Region Entrance Detection

6.7.8 Configuring Region Exiting Detection

Purpose:

Region exiting detection function detects people, vehicle or other objects which exit from a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

Note: Region exiting detection function varies according to different camera models.

Steps:

1. Enter the Region Exiting Detection settings interface:

   Configuration> Advanced Configuration> Smart Event> Region Exiting Detection

2. Check the checkbox of **Enable Region Exiting Detection** to enable the function.
3. Select the region from the drop-down list for detection settings.
4. Click the **Draw Area** button to start the region drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Click-and-drag the slider to set the detection sensitivity.

   Sensitivity: Range [1-100]. The value of the sensitivity defines the size of the

object which can trigger the alarm. When the sensitivity is high, a very small object exiting from the region can trigger the alarm.

7. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
8. Click the **Edit** button to set the arming schedule.
9. Select the linkage methods for region exiting detection, including Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel and Trigger Alarm Output.
10. Click **Save** to save the settings.

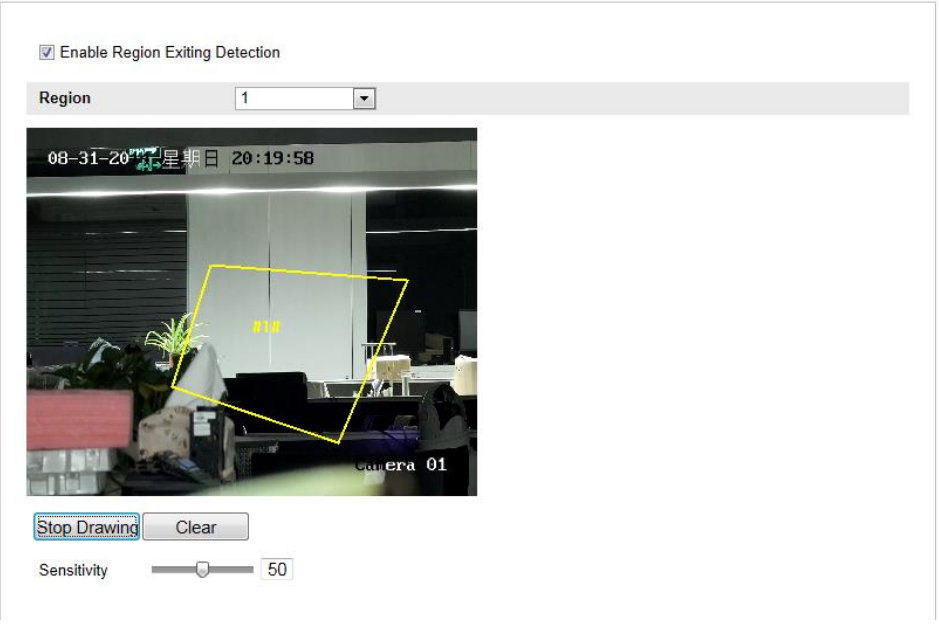


Figure 6-63 Configuring Region Exiting Detection

6.7.9 Configuring Unattended Baggage Detection

Purpose:

Unattended baggage detection function detects the objects left over in the pre-defined region such as the baggage, purse, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.

Note: Unattended baggage detection function varies according to different camera models.

Steps:

1. Enter the Unattended Baggage Detection settings interface:

   Configuration> Advanced Configuration> Smart Event> Unattended Baggage Detection
2. Check the checkbox of **Enable Unattended Baggage Detection** to enable the function.
3. Select the region from the drop-down list for detection settings.
4. Click the **Draw Area** button to start the region drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Set the time threshold and detection sensitivity for unattended baggage detection.

   Threshold: Range [5s-20s], the threshold for the time of the objects left over in the region. If you set the value as 10, alarm is triggered after the object is left and stay in the region for 10s.

   Sensitivity: Range [1-100]. The value of sensitivity defines the similarity degree of the background image. Usually, when the sensitivity is high, a very small object left in the region can trigger the alarm.
7. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
8. Click the **Edit** button to set the arming schedule.
9. Select the linkage methods for unattended baggage detection, including Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel and Trigger Alarm Output.
10. Click **Save** to save the settings.

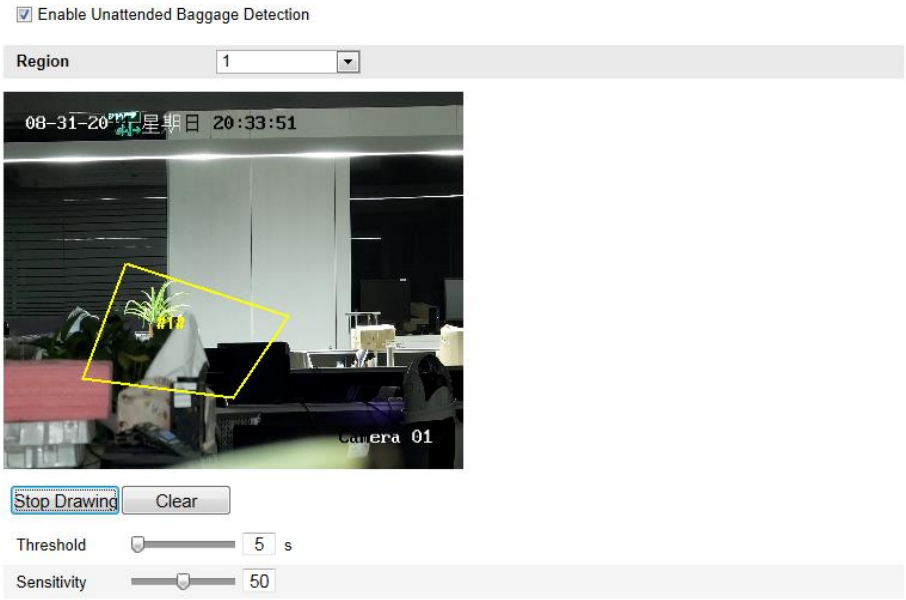


Figure 6-64 Configuring Unattended Baggage

6.7.10 Configuring Object Removal Detection

Purpose:

Object removal detection function detects the objects removed from the pre-defined region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.

Note: Object removal detection function varies according to different camera models.

Steps:

1. Enter the Object Removal Detection settings interface:

   Configuration> Advanced Configuration> Smart Event> Object Removal Detection

2. Check the checkbox of **Enable Object Removal Detection** to enable the function.
3. Select the region from the drop-down list for detection settings.
4. Click the **Draw Area** button to start the region drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.

6. Set the time threshold and detection sensitivity for object removal detection.

   Threshold: Range [5s-20s], the threshold for the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object disappears from the region for 10s.

   Sensitivity: Range [1-100]. The value of sensitivity defines the similarity degree of the background image. Usually, when the sensitivity is high, a very small object taken from the region can trigger the alarm.

7. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
8. Click the **Edit** button to set the arming schedule.
9. Select the linkage methods for object removal detection, including Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel and Trigger Alarm Output.
10. Click **Save** to save the settings.

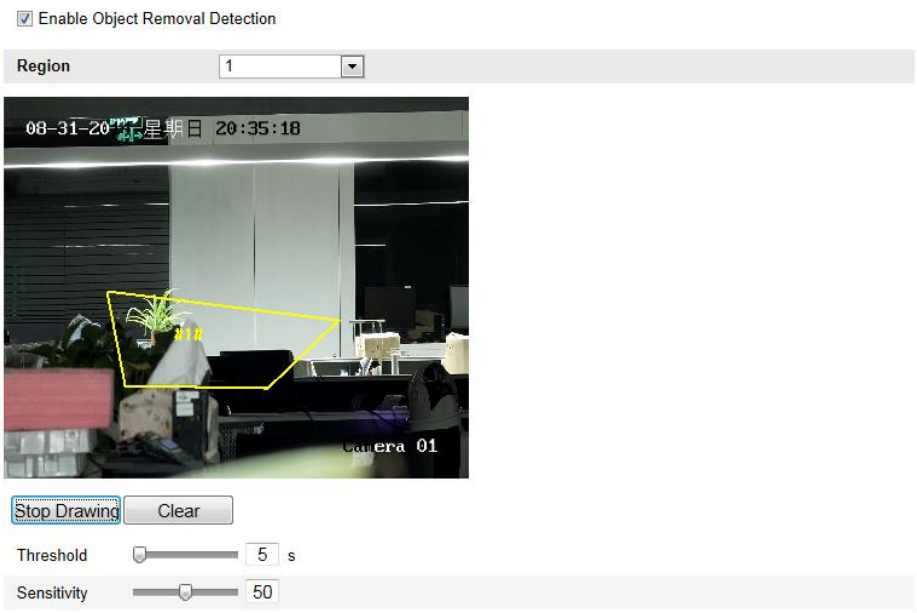


Figure 6-65 Configuring Object Removal Detection

6.8 VCA Configuration

6.8.1 Behavior Analysis

The behavior analysis detects a series of suspicious behavior, and certain linkage methods will be enabled if the alarm is triggered.

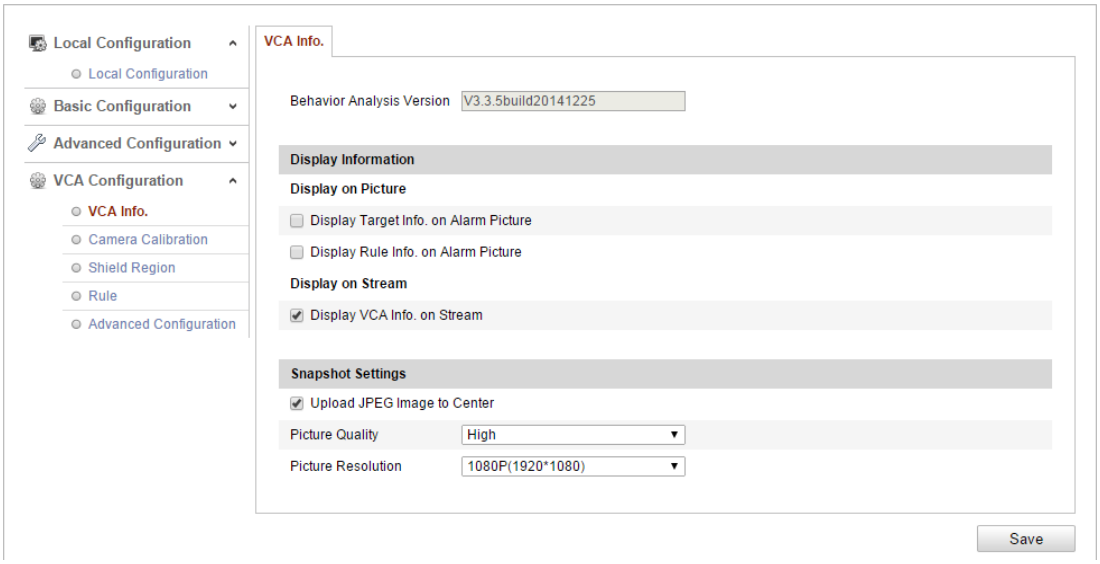


Figure 6-66 Behavior Analysis

❖ **VCA Info**

Behavior Analysis Version: It lists the version of the algorithms library.

Display information includes the display on picture and display on stream.

Display Target info. on Alarm Picture: There will be a frame on the target on the uploaded alarm picture if the checkbox is checked.

Display Rule info. on Alarm Picture: The captured target and the configured area will be framed on the alarm picture.

Display VCA info. on Stream: The green frames will be displayed on the target if in a live view or playback.

Note: Make sure the rules are enabled in your local settings. Go to **Configuration** > **Local Configuration** > **Rules** to enable it.

Snapshot Setting: You can set the quality and resolution for the captured picture.

Upload JPEG Image to Center: Check the checkbox to upload the captured

image to the surveillance center when a VCA alarm occurs.

Picture Quality: High, Medium and Low are selectable.

Picture Resolution: CIF, 4CIF, 720P, and 1080P are selectable.

❖ **Camera Calibration**

Perform the following steps to three-dimensionally measure and quantize the image from the camera, and then calculate the size of every target. The VCA detection will be more accurate if the camera calibration is configured.

Steps:

1. Check the checkbox of **Camera Calibration** to enable this function.
2. Select the calibration mode as Input Basic Data or Draw on Live View Video.

   Input Basic Data: Input the mounting height, viewing angle, and horizon ratio of the camera manually.

   Draw on Live View Video: Click **Draw Verification Line (Horizontal) / (Vertical)** to draw a horizontal/vertical line in the live view, and input the actual length in Real Length field. With the drawn reference lines and their real length, the camera can conclude other objects appear in the live view.
3. (Optional) Check the checkbox of **Enable Verification of Camera Calibration**, click the **Horizontal Verify / Vertical Verify** button to draw a horizontal / vertical line on the live video, and then click the **Calibrate** button to calculate the line length. Compare the calculated line length to the actual length to verify the calibration information you set.
4. You can click **Delete** to delete the drawn lines.
5. Click **Save** to save the settings.

   Note: If the live view is stopped, the camera calibration is invalid.

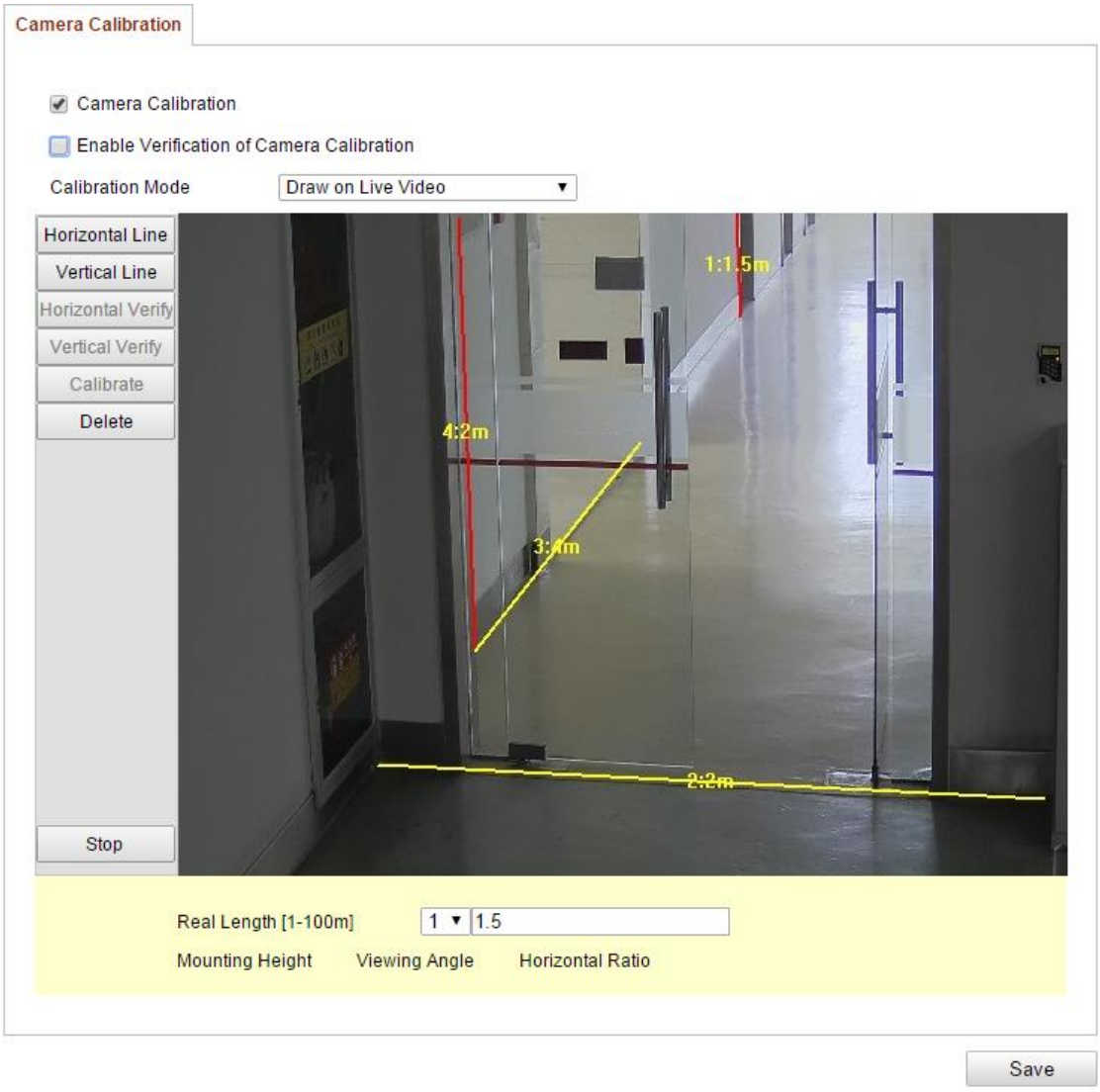


Figure 6-67 Draw on Live View Window

❖ Shield Region

The shield region allows you to set the specific region in which the behavior analysis will not function. Up to 4 shield regions are supported.

Steps:

1. Click **Shield Region** tab to enter the shield region configuration interface.
2. Click **Draw Area**. Draw area by left click end-points in the live view window, and right click to finish the area drawing.

   Notes:

   - Polygon area with up to 10 sides is supported.
   - Click **Delete** to delete the drawn areas.
   - If live view is stopped, there is no way to draw the shield regions.

3. Click **Save** to save the settings.

❖ **Rule**

The behavior analysis supports a series of behaviors, including line crossing detection, intrusion, region entrance, and region exiting, etc.

Note: Please refer to each chapter for detailed information of each behavior.

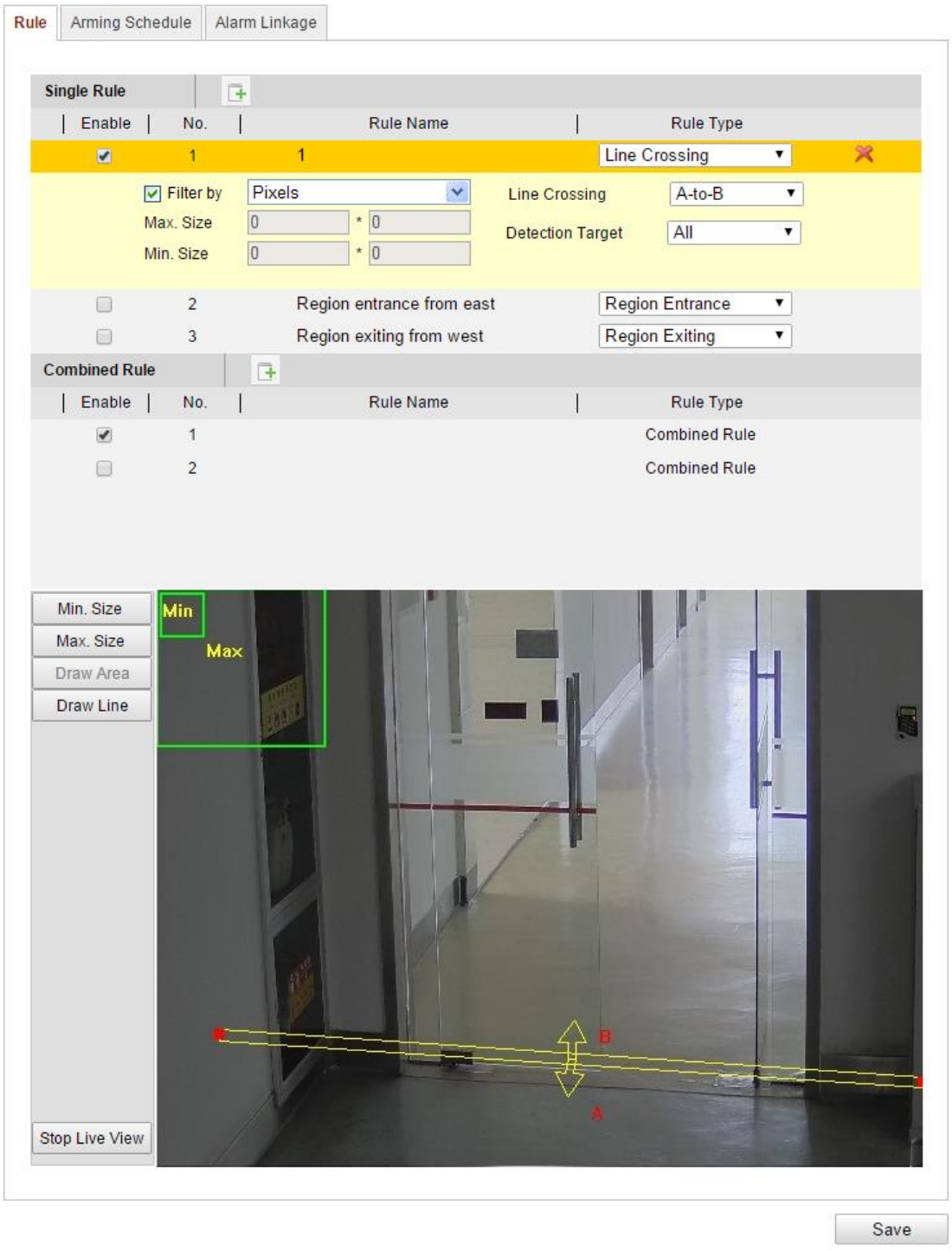


Figure 6-68 Configure the Rule

Steps:

1. Click **Rule** Tab to enter the rule configuration interface.
2. Check the checkbox of the single rule to enable the rule for behavior analysis.
3. Select the rule type, set the filter type, and then draw the line / area on the live video for the single rule.

   Filter type: Pixels and Actual Size are selectable. If Pixels is selected, draw the area of maximum size and minimum size on the live video for each rule. If Actual Size is selected, input the length and width of the maximum size and minimum size. Only the target whose size is between the minimum value and maximum value will trigger the alarm.

   Note: Make sure the camera calibration is configured if actual size is selected.

   Detection Target: Select Human or Vehicle as the detection target. You can also select All to detect all the objects as the target.

   Draw line / area: For line crossing detection, you have to draw a line, and select the crossing direction, which is bidirectional, A-to-B, or B-to-A. For other events such as intrusion, region entrance, region exiting, etc., you have to left click on the live video to set the end points of the area and right click to finish the area drawing.

   Note: If the live view is stopped, the detection area / line cannot be draw and the rules cannot be set.
4. Check the checkbox of the combined rule to enable the rule for behavior analysis.
5. Select two configured single rules as the Rule A and Rule B of the combined rule, set the minimum and maximum time interval for the two single rules, and then select the trigger order of the single rules for alarm filtering.

   Notes:

   - If you select the rule type as None, the rule option is invalid, and no behavior analysis can be configured.
   - The trigger order of the single rules for alarm filtering can be set as In Ascending Order or In Ascending/Descending Order.
   - Up to 8 single rules and 2 combined rules are configurable. And the line crossing, intrusion, region exiting and region entrance are supported for the combined rules.

6. Click **Save** to save the settings.
7. Click **Arming Schedule** tab, click **Edit** to set the schedule time for each rule, and click **Save** to save the settings.
8. Click **Alarm Linkage** tab, check the checkbox of corresponding linkage method for each rule, and click **Save** to save the settings.

❖ **Advanced Configuration**

- **Parameter**

Configure the following parameters to detail the configuration.

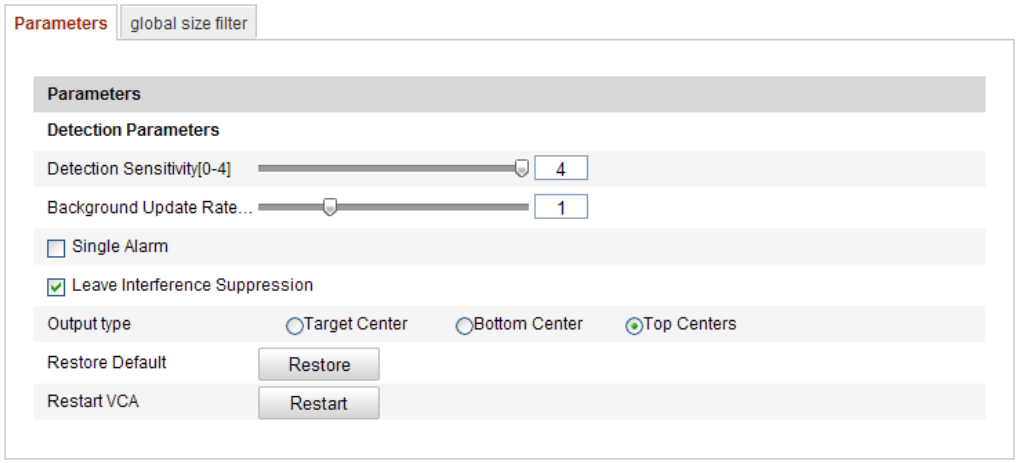


Figure 6-69 Advanced Configuration

Detection Sensitivity [0~4]: Refers to the sensitivity of the camera detects a target. The higher the value, the easier a target be recognized, and the higher the misinformation is. The default value of 3 is recommended.

Background Update Rate [0~4]: It refers to the speed of the new scene replaces the previous scene. The default value of 3 is recommended.

Single Alarm: If single alarm is selected, the target in the configured area will trigger the alarm for only once. If it is not checked, the same target will cause the continuous alarm in the same configured area.

Leave Interference Suppression: Check this checkbox to stop the interference caused by the leaves in the configured area.

Output Type: Select the position of the frame. Target center, bottom center, and top centers are selectable. E.g.: The target will be in the center of the frame if target center is selected.

Restore Default: Click to restore the configured parameters to the default.

Restart VCA: Restart the algorithms library of behavior analysis.

- Global Size Filter

  Note: Compared with the size filter under rule, which is aiming at each rule, the global size filter is aim at all rules.

Steps:

1. Check the checkbox of **Global Size Filter** to enable the function.
2. Select the Filter Type as Actual Size or Pixel.

Actual Size: Input the length and width of both the maximum size and the minimum size. Only the target whose size is between the minimum value and maximum value will trigger the alarm.

Notes:

- Camera calibration has to be configured if you select the filter by actual size.
- The length of the maximum size should be longer than the length of the minimum size, and so does the width.

Pixel: Click Minimum Size to draw the rectangle of the min. size on the live view. And click Maximum Size to draw the rectangle of the max. size on the live view. The target is smaller than the min. size or larger than the max. size will be filtered.

Notes:

- The drawn area will be converted to the pixel by the background algorithm.
- The global size filter cannot be configured if the live view is stopped.
- The length of the maximum size should be longer than the length of the minimum size, and so does the width.

3. Click **Save** to save the settings.

6.8.2 Face Capture

Face capture can capture the face appears in the configured area, and the face characters information, including the age, gender, and wearing glasses or not will be uploaded with the captured picture as well.

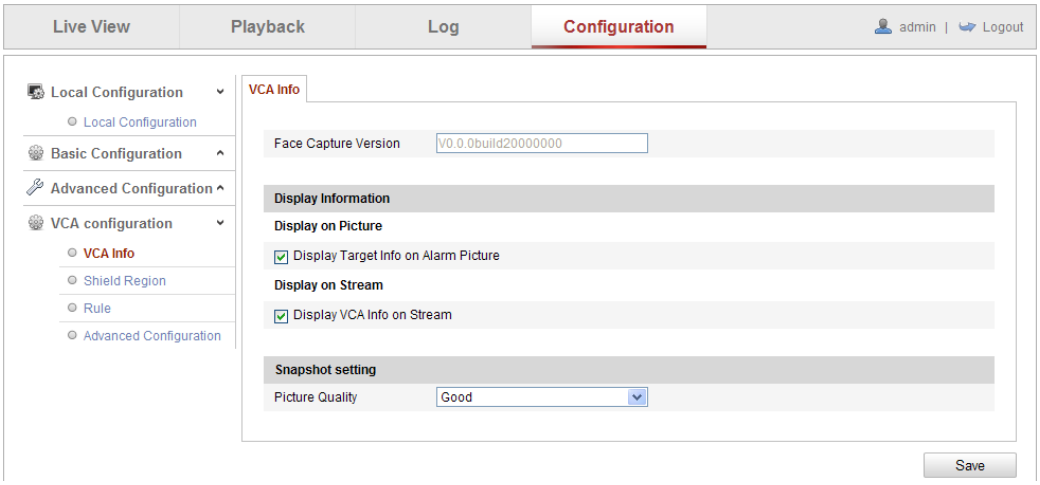


Figure 6-70 Face Capture

❖ **VCA Info**

Face Capture Version: It lists the version of the algorithms library.

Display information includes the display on picture and display on stream.

Display Target info. on Alarm Picture: There will be a frame on the target on the uploaded alarm picture if the checkbox is checked.

Display VCA info. on Stream: The green frames will be displayed on the target if in a live view or playback.

Snapshot Setting: Select the picture quality for the captured picture. Good, better, and best are selectable.

❖ **Shield Region**

The shield region allows you to set the specific region in which the face capture will not function. Up to 4 shield regions are supported.

Steps:

1. Click **Shield Region** tab to enter the shield region configuration interface.
2. Click **Draw Area**. Draw area by left click four end-points in the live view window, and right click to finish the area drawing.

Notes:

- Click **Delete** to delete the drawn areas.
- If the live view is stopped, there is no way to draw the shield regions.

3. Click **Save** to save the settings.

❖ **Rule**

Steps:

1. Check the checkbox of **Rule** to enable rules of face capture.
2. Click **Minimize Pupil Distance** to draw the minimum pupil distance. The distance of the drawn pupil will be displayed on the box below the live view. The minimize pupil distance refers to the minimum square size composed by the area between two pupils, and it is the basic standard for a camera to identify a target.
3. Click **Draw Area** to draw the area you want the face capture to take effect. Draw area by left click end-points in the live view window, and right click to finish the area drawing.

   Notes:

   - Polygon area (4~10 sides) sides is supported.
   - If the live view is stopped, there is no way to draw the configured area.
4. Click **Save** to save the settings.

❖ **Advanced Configuration**

Configure the following parameters according to your actual environment.

Detection Parameters:

Generation Speed [1~5]: The speed to identify a target. The higher the value, the faster the target will be recognized. Setting the value quite low, and if there was a face in the configured area from the start, this face will not be captured. It can reduce the misinformation of the faces in the wall painting or posters. The default value of 3 is recommended.

Capture Times [1~10]: Refers to the capture times a face will be captured during its stay in the configured area. The default value is 1.

Sensitivity [1~5]: The sensitivity to identify a target. The higher the value, the easier a face will be recognized, and the higher misinformation is. The default value of 3 is

recommended.

Capture Interval [1~255 Frame]: The frame interval to capture a picture. If you set the value as 1, which is the default value, it means the camera captures the face in every frame.

Capture Sensitivity [0~20]: The threshold the camera treats the target as a face. Only when the face score generated by the algorithm is equal or higher than the value, the camera will treat the target as a face. The default value of 2 is recommended.

Face Capture Advanced Parameters:

Face Exposure: Check the checkbox to enable the face exposure.

Reference Brightness [0~100]: The reference brightness of a face in the face exposure mode. If a face is detected, the camera adjusts the face brightness according to the value you set. The higher the value, the brighter the face is.

Minimum Duration [1~60min]: The minimum duration of the camera exposures the face. The default value is 1 minute.

Note: If the face exposure is enabled, please make sure the WDR function is disabled, and the manual iris is selected.

Enable Face ROI: If the camera captures a face, the face area will be treated as the region of interest, and the image quality of this area will be improved.

Restore Default: Click **Restore** to restore all the settings in advanced configuration to the factory default.

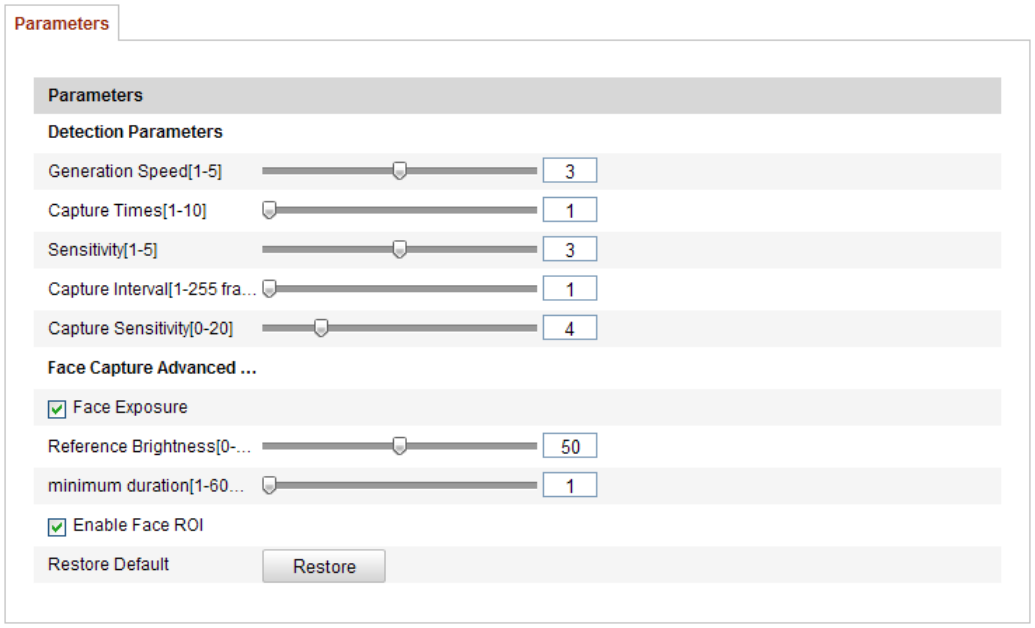


Figure 6-71 Advanced Configuration

6.8.3 People Counting

Purpose:

People function is used to calculate the number of object entered or exited a certain configured area and is widely applied to the entrances or exits.

Notes:

- Compared with the counting function supported by the Non-iDS camera, the people counting requires for calibration settings for better counting accuracy.
- It is recommended to install the camera as right above the entrance/exit as possible, and make sure it is horizontal to improve the counting accuracy.

Steps：

❖ **People Counting Configuration**

1. Enter the Counting Configuration interface:

   Configuration > **Advanced Configuration** > **People Counting**

Figure 6-72 People Counting Configuration

2. Select **People Counting Configuration** tab to set the detailed parameters.
3. Check the checkbox of **Enable Counting** to enable the function.
4. (Optional) Check the checkbox of **Enable OSD Overlay**, and the real-time number of object entered and exited is displayed on the live video.
   You can also adjust the OSD position according to the actual needs.
5. Set the detection line.
   An orange line, called detection line can be set on the live video, and the object entering or exiting through the line will be detected and counted.
   1) Click **Draw Line**, and an orange detection line will appear on the image.
      Note:
      - The detection line should be drawn at the position right below the camera, and it should cover the whole entrance / exit.
      - Draw the detection line at the position don't have many people lingering.
   2) Click-and-drag the detection line to adjust its position.
   3) Click-and-drag the two end points of the detection line to adjust its length.
   4) To delete the detection line, click the **Delete Line** button.
6. Check the checkbox of **Enable Calibration** to enable camera calibration.

A vertical line appears in the configuration window after you enable the calibration. And a horizontal line (blue) appears if one target passed the detection line. Up to 8 horizontal lines can be displayed on one side of the detection line.

The horizontal line is calculated according to the shoulder width of the target. And you can decide the calibration line position according to the width of the targets. You can click-and-drag to adjust the calibration line position.

7. Click the **Reset Counter** button, and the number of the people entered and exited will be cleared to zero.
8. Click **Edit** to set the arming schedule.
9. Check the checkbox of **Notify Surveillance Center** to set the linkage action.
10. Click **Save** to save the settings.

❖ **People Counting Statistics**

Steps:

1. Click **People Counting Statistics** to enter the data statistics interface.
2. Select the report type by clicking the drop-down menu. Daily report, weekly report, monthly report, and annual report are selectable.
3. Select the Statistics Type as People Entered or People Exited.

   Note: Daily report calculates the data on the date you selected; weekly report calculates for the week your selected date belongs to; monthly report calculates for the month your selected date belongs to; and the annual report calculates for the year your selected date belongs to.
4. Select the Statistics Time.
5. Click **Counting** to calculate the data.
6. Select to export the **Statistics Result** as Table, Bar Chart, or Line Chart.

   Note: If you select table to display the statistics, there is an **Export** button to export the data in an excel file.

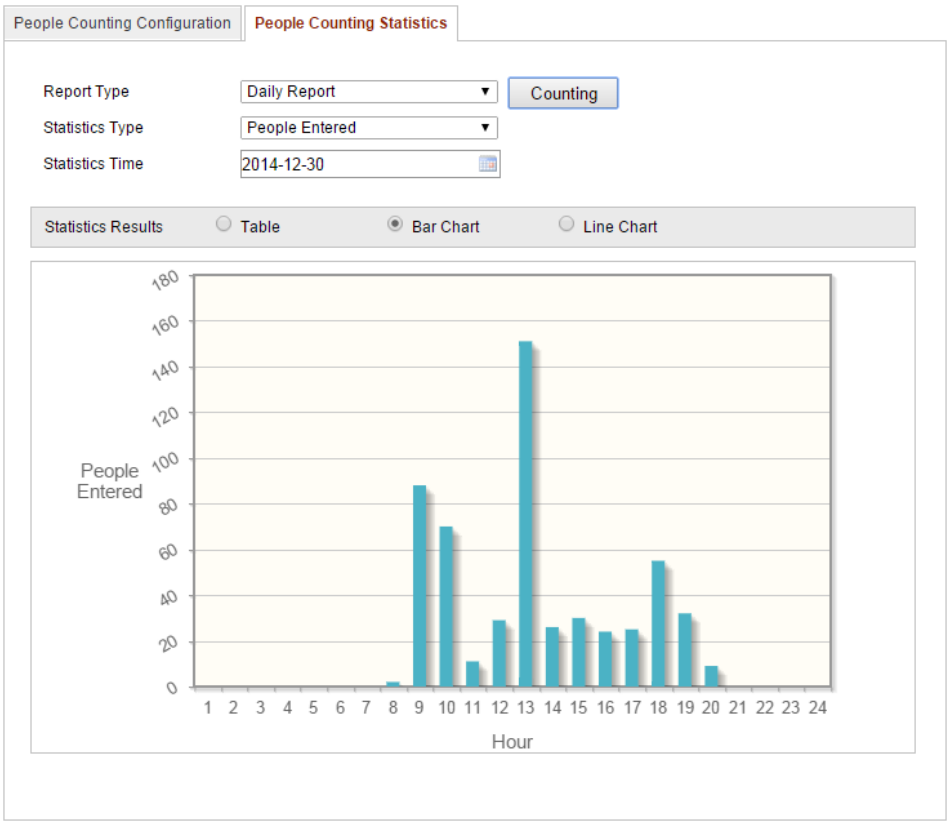


Figure 6-73 Statistics Result

6.8.4 Heat Map

Heat map is a graphical representation of data represented by colors. The heat map function of the camera usually be used to analyze the visit times and dwell time of customers in a configured area.

❖ **Heat Map Configuration**

Steps:

1. Enter the Heat Map configuration interface: **Configuration > Advanced Configuration > Heat Map**

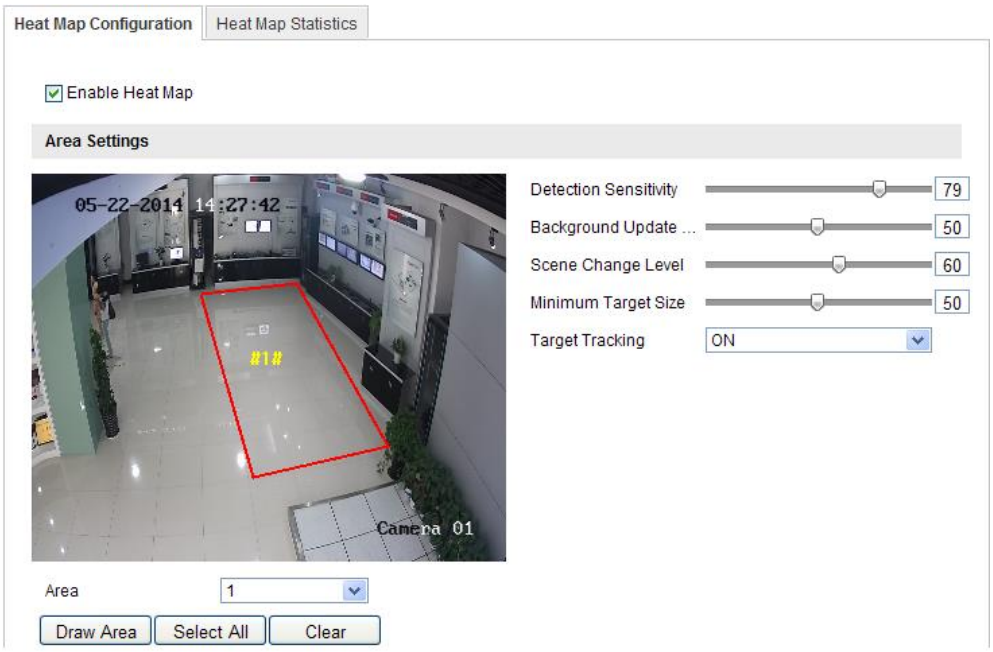


Figure 6-74 Heat Map Configuration

2. Select **Heat Map Configuration** tab to set the detailed parameters.
3. Check the checkbox of **Enable Heat Map** to enable the function.
4. Click **Draw Area** to define the area for heat value statistics. Draw area by left click four end-points in the live view window, and right click to finish the area drawing. Up to 8 areas are configurable.

   Note: You can click **Select All** to select the whole live view window as the configured area. Or click **Delete** to delete the current drawn area.
5. Configure the parameters for drawn area.

   Detection Sensitivity [0~100]: It refers to the sensitivity of the camera identify a target. The over-high sensitivity may cause the misinformation. It is recommended you set the sensitivity as the default value, which is 50.

   Background Update Rate [0~100]: It refers to the speed of the new scene replaces the previous scene. E.g.: In front of a cabinet, the people besides the cabinet will be double counted if the goods moved from the cabinet, and the camera treats the cabinet (on which the good removed) as a new scene. The default value of 50 is recommended.

   Scene Change Level [0~100]: It refers to level of the camera responses to the dynamic environment, e.g., a swaying curtain. The camera may treat the swaying curtain as a target. Setting the level properly will avoid the

misinformation. The default level is 50.

Minimum Target Size [0~100]: It refers to the size of the camera identify a target. You can set the target size according to the actual environment. The default size is 50.

Target Track: Select ON or OFF to enable or disable the tracking of the target.

6. Click **Edit** to set the arming schedule.
7. Select the linkage method by checking the checkbox of notify the surveillance center.
8. Click **Save** to save the settings.

❖ **Heat Map Statistics**

Steps:

1. Click **Heat Map Statistics** to enter the data statistics interface.
2. Select the report type by clicking the drop-down menu. Daily report, weekly report, monthly report, and annual report are selectable.
3. Click **Counting** to export the data.
4. Select **Statistics Result** as Space Heat Map or Time Heat Map, and the corresponding heat map will be displayed.

   If you select the time heat map to list the statistics, there is an **Export** button to export the data in an excel file.

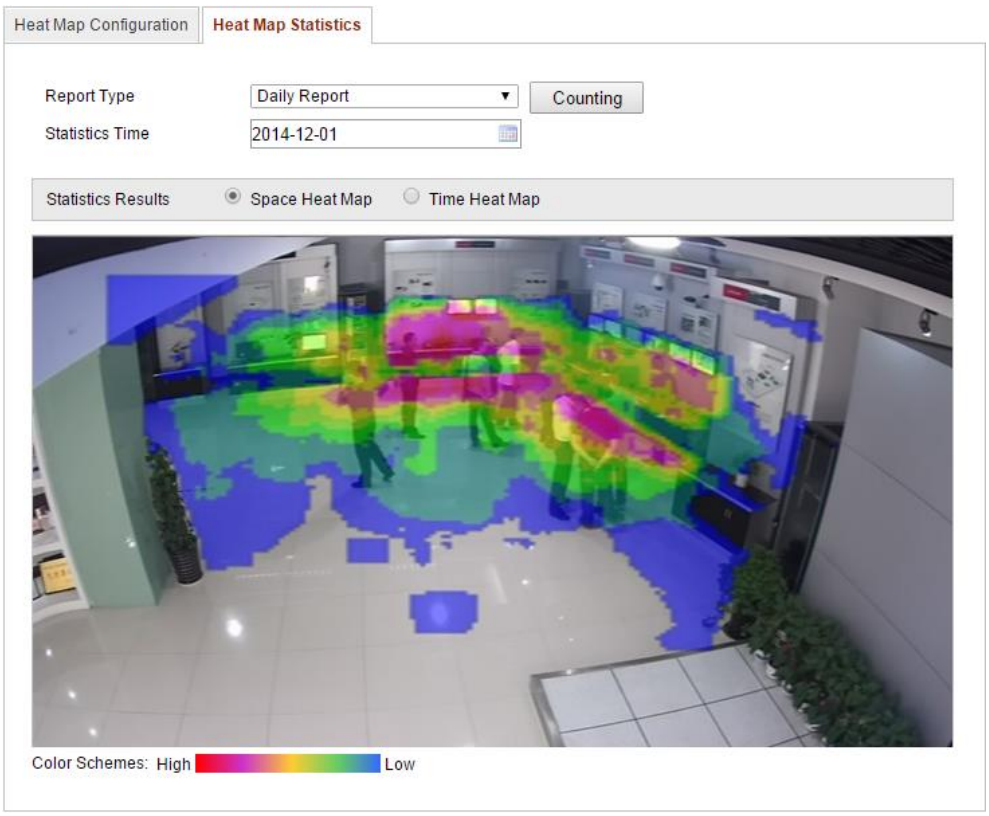


Figure 6-75 Space Heat Map

Notes:

- As shown in the figure above, red color block (255, 0, 0) indicates the most welcome area, and blue color block (0, 0, 255) indicates the less-popular area.
- It is recommended that you do not adjust the electronic lens after the installation is completed, which may cause the inaccuracy of the data in some degree.

6.8.5 Counting

Counting function helps to calculate the number of people entered or exited a certain configured area and is widely applied to the entrances or exits.

Notes:

It is recommended to install the camera as right above the entrance/exit as possible, and make sure it is horizontal to improve the counting accuracy.

❖ **Counting Configuration**

Steps:

1. Enter the Counting Configuration interface:
   Configuration > Advanced Configuration > Counting
2. Select **Counting Configuration** tab to set the detailed parameters.

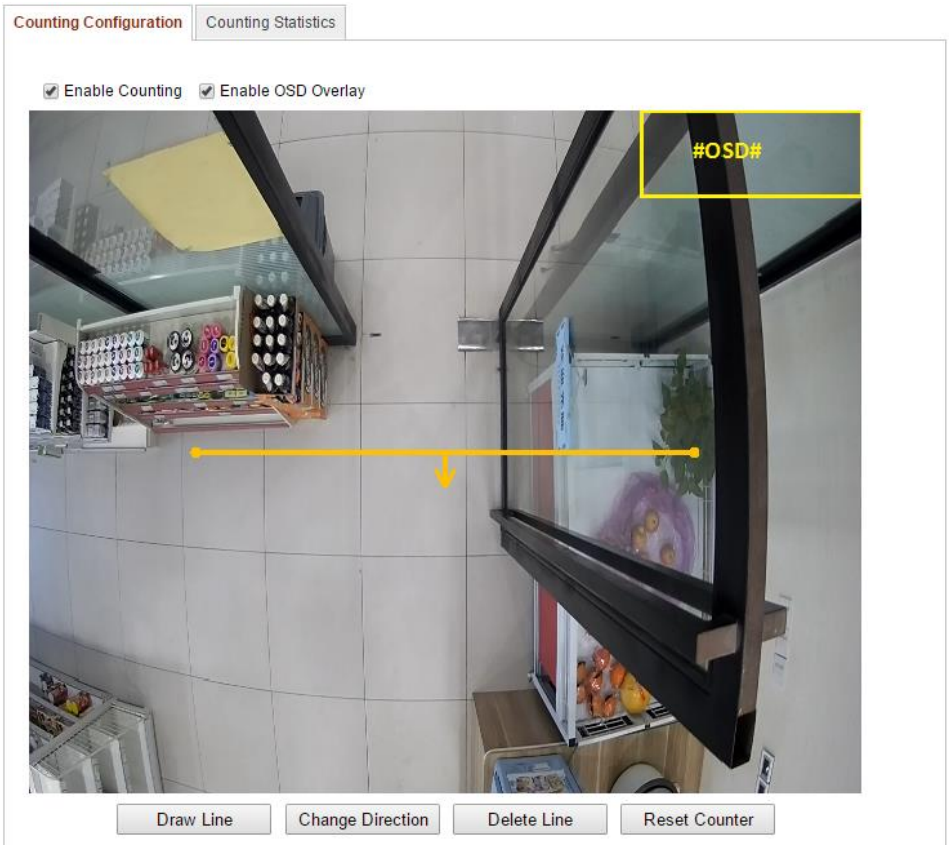


Figure 6-76 Counting Configuration

3. Check the checkbox of **Enable Counting** to enable the function.
4. (Optional) Check the checkbox of **Enable OSD Overlay**, and the real-time number of people entered and exited is displayed on the live video.
5. Set the detection line.
   An orange line, called detection line can be set on the live video, and the people entering or exiting through the line will be detected and counted.
   1) Click **Draw Line**, and an orange detection line will appear on the live view.
      Notes:
      - The detection line should be drawn at the position right below the camera, and it should cover the whole entrance / exit.
      - Draw the detection line at the position don't have many people lingering.

2) Click-and-drag the detection line to adjust its position.
3) Click-and-drag the two end points of the detection line to adjust its length.
4) To delete the detection line, click the **Delete Line** button.

6. An arrow indicating the entering direction of people is shown after the detection line is selected. You can click the **Change Direction** button to adjust the arrow direction to opposite side.
7. Click the **Reset Counter** button, and the number of the people entered and exited will be cleared to zero.
8. Click **Edit** to set the arming schedule.
9. Check the checkbox of **Notify Surveillance Center** to set the linkage action.
10. Click **Save** to save the settings.

❖ **Counting Statistics**

Steps:

1. Click **People Counting Statistics** to enter the data statistics interface.
2. Select the report type by clicking the drop-down menu. Daily report, weekly report, monthly report, and annual report are selectable.
3. Select the **Statistics Type** as People Entered or People Exited.
4. Select the **Statistics Time**.

   Note: Daily report calculates the data on the date you selected, weekly report calculates for week your selected date belongs to, monthly report calculates for the month your selected date belongs to, and the annual report calculates for the year your selected date belongs to.
5. Click **Counting** to calculate the data.
6. Select to export the **Statistics Result** as Table, Bar Chart, or Line Chart.

   Note: If you select table to list the statistics, there is an **Export** button to export the data in an excel file.

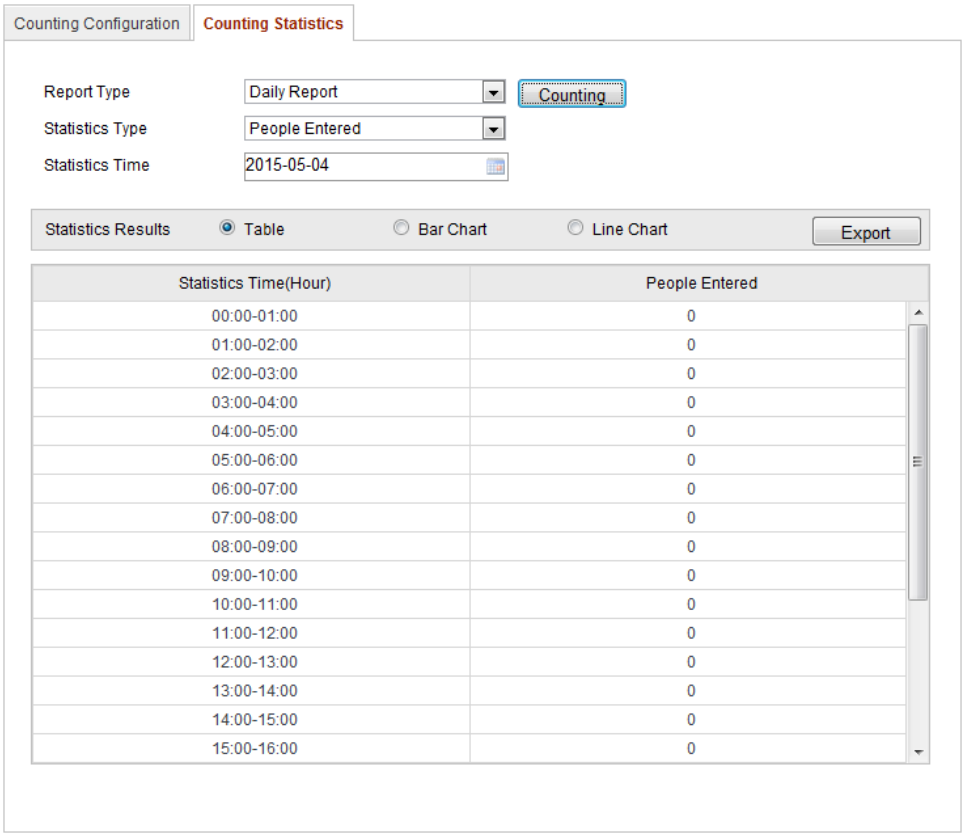


Figure 6-77 Statistics Result

Note: It is recommended that you do not adjust the electronic lens after the installation is completed, which may cause the inaccuracy of the data in some degree.

Chapter 7 Storage Settings

Before you start:

To configure record settings, please make sure that you have the network storage device within the network or the SD card inserted in your camera.

7.1 Configuring NAS Settings

Before you start:

The network disk should be available within the network and properly configured to store the recorded files, log files, etc.

Steps:

1. Add the network disk

   (1) Enter the NAS (Network-Attached Storage) Settings interface:

Configuration > Advanced Configuration > Storage > NAS

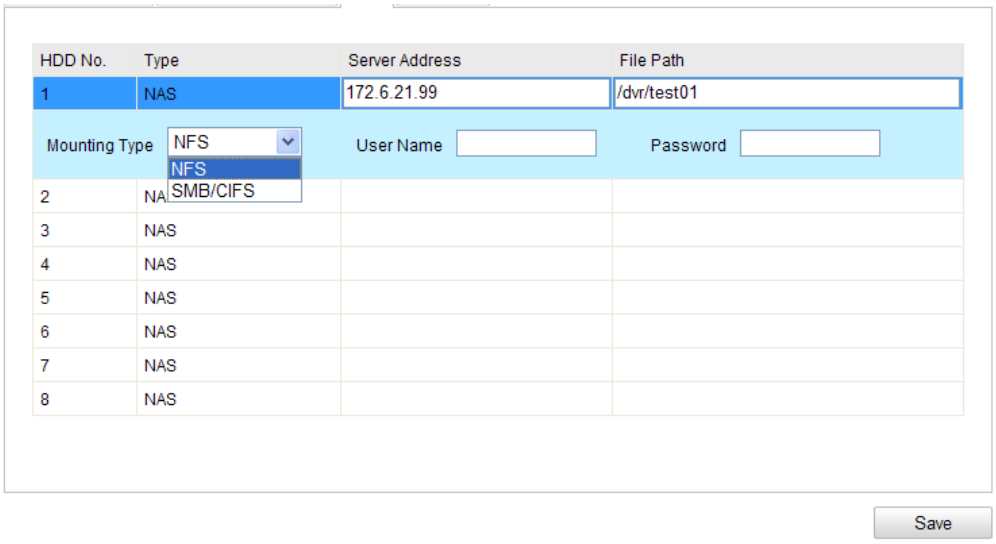


Figure 7-1 Add Network Disk

   (2) Enter the IP address of the network disk, and enter the file path.

   (3) Select the mounting type. NFS and SMB/CIFS are selectable. And you can set the user name and password to guarantee the security if SMB/CIFS is selected.

   Note: Please refer to the *User Manual of NAS* for creating the file path.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

(4) Click **Save** to add the network disk.

2. Initialize the added network disk.

(1) Enter the HDD Settings interface (**Advanced Configuration** > **Storage** > **Storage Management**), in which you can view the capacity, free space, status, type and property of the disk.

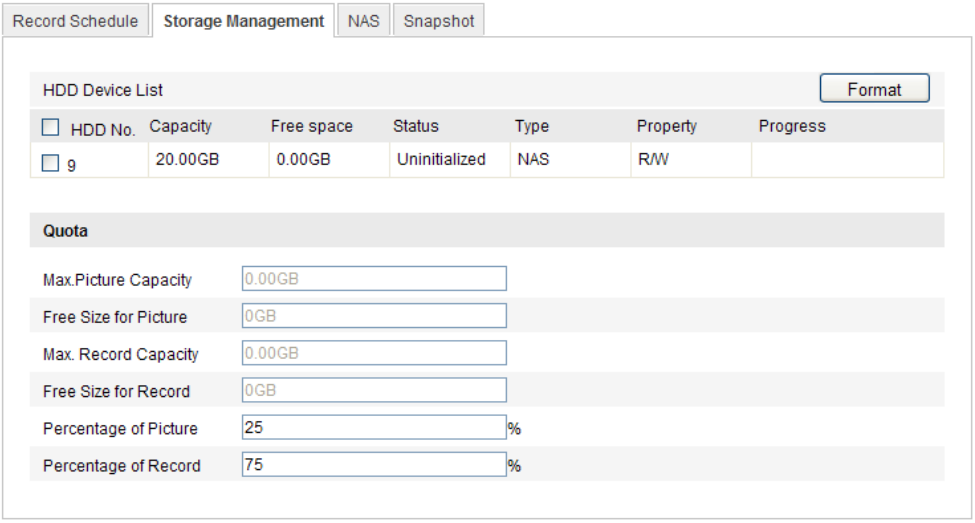


Figure 7-2 Storage Management Interface

(2) If the status of the disk is **Uninitialized**, check the corresponding checkbox to select the disk and click **Format** to start initializing the disk.

When the initialization completed, the status of disk will become **Normal.**

Figure 7-3 View Disk Status

3. Define the quota for record and pictures.

   (1) Input the quota percentage for picture and for record.

   (2) Click **Save** and refresh the browser page to activate the settings.

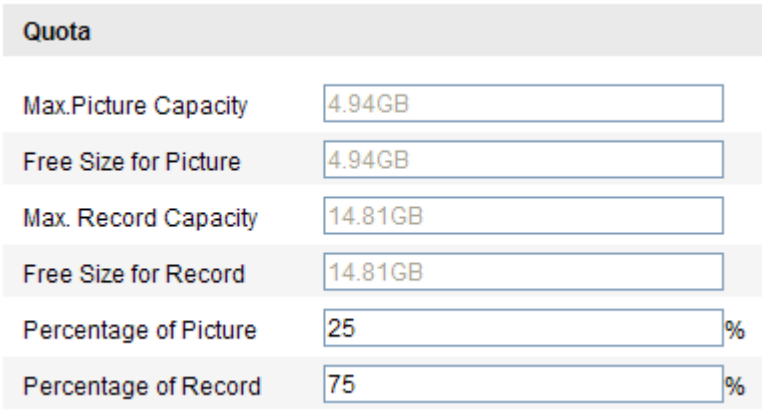


Figure 7-4 Quota Settings

Notes:

- Up to 8 NAS disks can be connected to the camera.
- To initialize and use the SD card after insert it to the camera, please refer to the steps of NAS disk initialization.

7.2 Configuring Recording Schedule

Purpose:

There are two kinds of recording for the cameras: manual recording and scheduled recording. For the manual recording, refer to *Section 5.3* ***Recording and Capturing Pictures Manually***. In this section, you can follow the instructions to configure the scheduled recording. By default, the record files of scheduled recording are stored in the SD card (if supported) or in the network disk.

Steps:

1. Enter the Record Schedule Settings interface:

Configuration > Advanced Configuration> Storage > Record Schedule

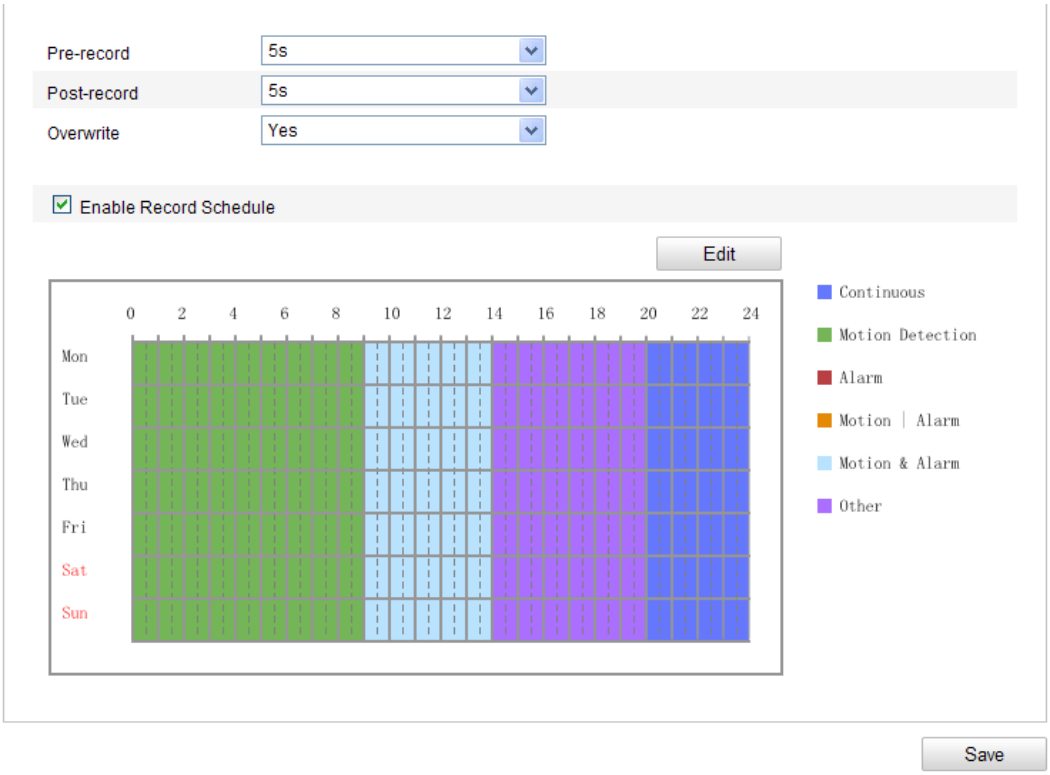


Figure 7-5 Recording Schedule Interface

2. Check the checkbox of **Enable Record Schedule** to enable scheduled recording.
3. Set the record parameters of the camera.

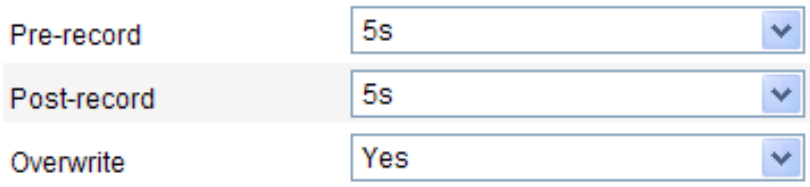


Figure 7-6 Record Parameters

- Pre-record: The time you set to start recording before the scheduled time or the event. For example, if an alarm triggers recording at 10:00, and the pre-record time is set as 5 seconds, the camera starts to record at 9:59:55.

  The Pre-record time can be configured as No Pre-record, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s or not limited.
- Post-record: The time you set to stop recording after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05.

The Post-record time can be configured as 5 s, 10 s, 30 s, 1 min, 2 min, 5 min or 10 min.

Note: The record parameter configurations vary depending on the camera model.

4. Click **Edit** to edit the record schedule.

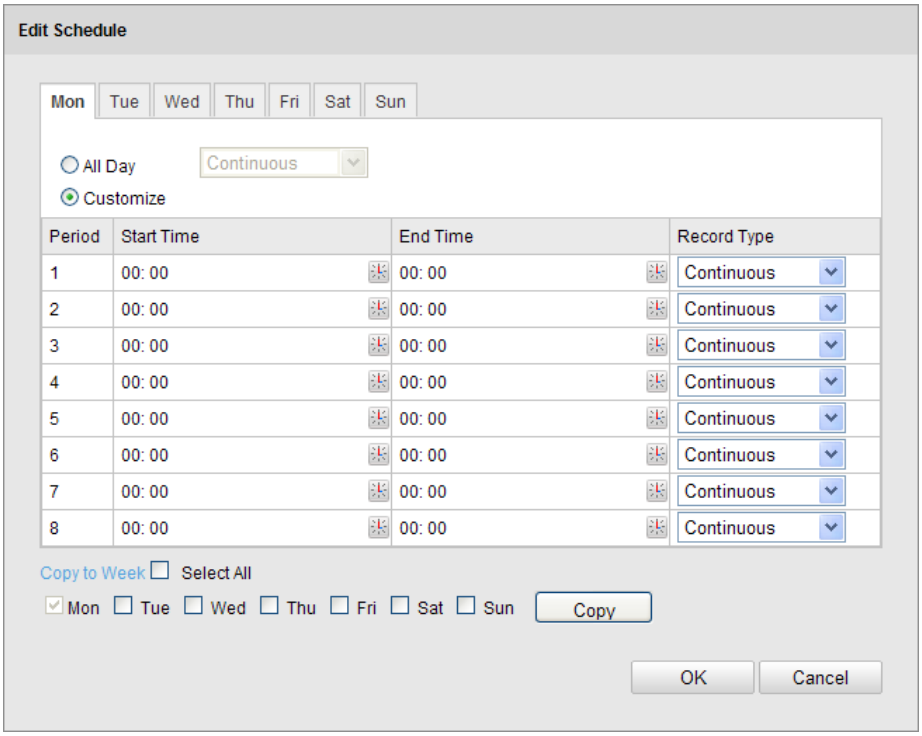


Figure 7-7 Record Schedule

5. Choose the day to set the record schedule.

(1) Set all-day record or segment record:

- If you want to configure the all-day recording, please check the **All Day** checkbox.
- If you want to record in different time sections, check the **Customize** checkbox. Set the **Start Time** and **End Time.**

  Note: The time of each segment can't be overlapped. Up to 4 segments can be configured.

(2) Select a **Record Type**. The record type can be Continuous, Motion Detection, Alarm, Motion | Alarm, Motion & Alarm, PIR Alarm, Wireless Alarm, Emergency Alarm, or Motion | Alarm Input | PIR | Wireless | Emergency.

- **Continuous**

  If you select **Continuous**, the video will be recorded automatically according

to the time of the schedule.

- **Record Triggered by Motion Detection**

  If you select **Motion Detection**, the video will be recorded when the motion is detected.

  Besides configuring the recording schedule, you have to set the motion detection area and check the checkbox of **Trigger Channel** in the **Linkage Method** of Motion Detection Settings interface. For detailed information, please refer to the *Step 1* ***Set the Motion Detection Area*** *in the Section 6.6.1*.

- **Record Triggered by Alarm**

  If you select **Alarm**, the video will be recorded when the alarm is triggered via the external alarm input channels.

  Besides configuring the recording schedule, you have to set the **Alarm Type** and check the checkbox of **Trigger Channel** in the **Linkage Method** of **Alarm Input Settings** interface. For detailed information, please refer to *Section 6.6.3*.

- **Record Triggered by Motion & Alarm**

  If you select **Motion & Alarm**, the video will be recorded when the motion and alarm are triggered at the same time.

  Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Please refer to *Section 6.6.1* and *Section 6.6.3* for detailed information.

- **Record Triggered by Motion | Alarm**

  If you select **Motion | Alarm**, the video will be recorded when the external alarm is triggered or the motion is detected.

  Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Please refer to *Section 6.6.1* and *Section 6.6.3* for detailed information.

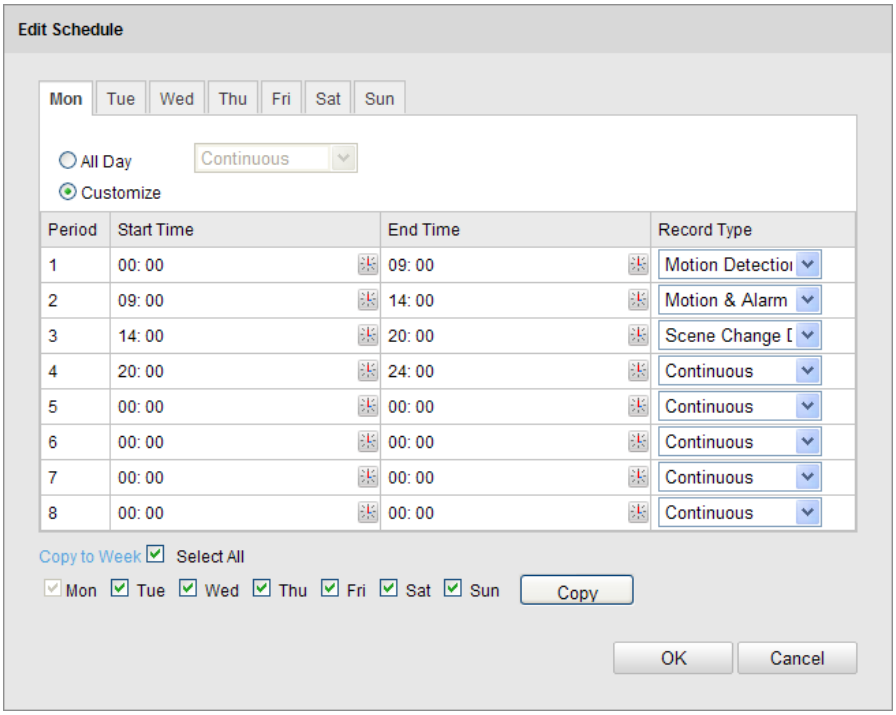


Figure 7-8 Edit Record Schedule

(3) Check the checkbox of **Select All** and click **Copy** to copy settings of this day to the whole week. You can also check any of the checkboxes before the date and click **Copy**.

(4) Click **OK** to save the settings and exit the **Edit Record Schedule** interface.

6. Click **Save** to save the settings.

7.3 Configuring Snapshot Settings

Purpose:

You can configure the scheduled snapshot and event-triggered snapshot. The captured picture can be stored in the SD card (if supported) or the netHDD (For detailed information about netHDD, please refer to *Section 7.1* ***Configuring NAS Settings***). You can also upload the captured pictures to a FTP server.

Basic Settings

Steps:

1. Enter the Snapshot Settings interface:

Configuration > Advanced Configuration > Storage > Snapshot

2. Check the **Enable Timing Snapshot** checkbox to enable continuous snapshot.

Check the **Enable Event-triggered Snapshot** checkbox to check event-triggered snapshot.

3. Select the quality of the snapshot.
4. Set the time interval between two snapshots.
5. Click **Save** to save the settings.

Uploading to FTP

You can follow below configuration instructions to upload the snapshots to FTP.

- Upload continuous snapshots to FTP

Steps:

1) Configure the FTP settings and check **Upload Picture** checkbox in FTP Settings interface. Please refer to *Section 6.3.12* ***Configuring FTP Settings*** for more details to configure FTP parameters.
2) Check the **Enable Timing Snapshot** checkbox.

- Upload event-triggered snapshots to FTP

Steps:

1) Configure the FTP settings and check **Upload Picture** checkbox in FTP Settings interface. Please refer to *Section 6.3.12* ***Configuring FTP Settings*** for more details to configure FTP parameters.
2) Check **Upload Picture** checkbox in Motion Detection Settings or Alarm Input interface. Please refer to *Step 3* ***Set the Alarm Actions Taken for Motion Detection*** in *Section 6.6.1, or Step 4* ***Configuring External Alarm Input*** in *Section 6.6.4.*
3) Check the **Enable Event-triggered Snapshot** checkbox.

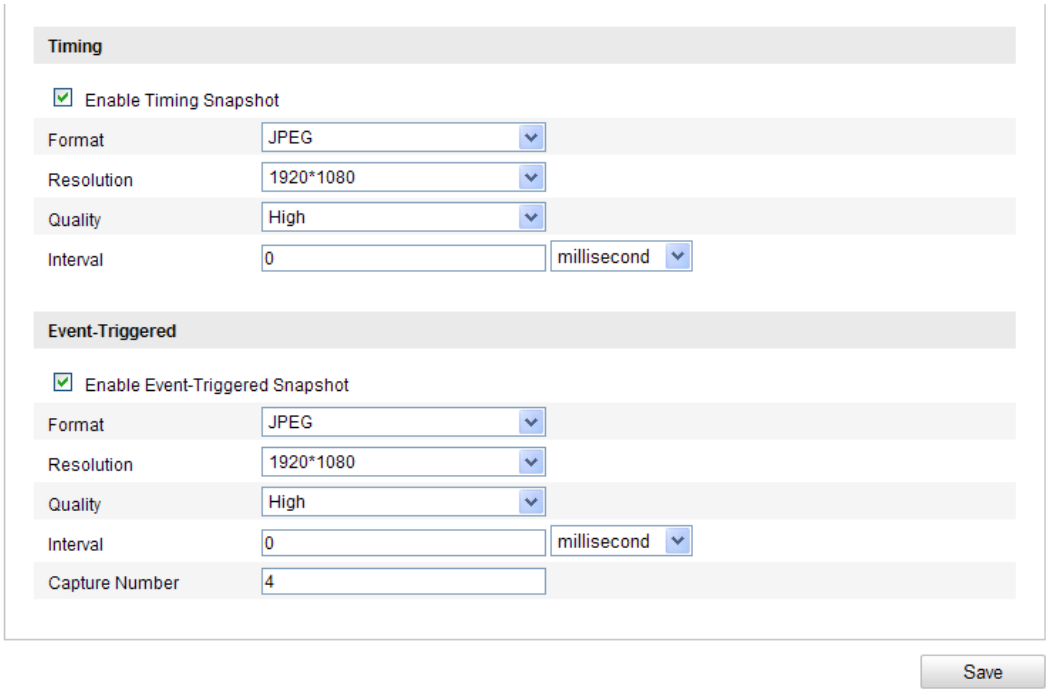


Figure 7-9 Snapshot Settings

7.4 Configuring Lite Storage

Purpose:

When there is no moving object in the monitoring scenario, the frame rate and bitrate of the video stream can be reduced to lengthen the storage time of the SD card.

Notes:

- Lite storage function varies according to different camera models.
- The video files recorded in lite storage mode will be played back in full frame rate (25fps / 30fps), and thus the playback process is speeded up to the eye.

1. Enter the Lite Storage interface: **Configuration** > **Advanced Configuration** > **Storage** > **Lite Storage**.
2. Check the Checkbox of **Enable** to enable the lite storage function.
3. Input the storage time in the text field. You can view the available space of the SD card on the page.
4. Click **Save** to save the settings.

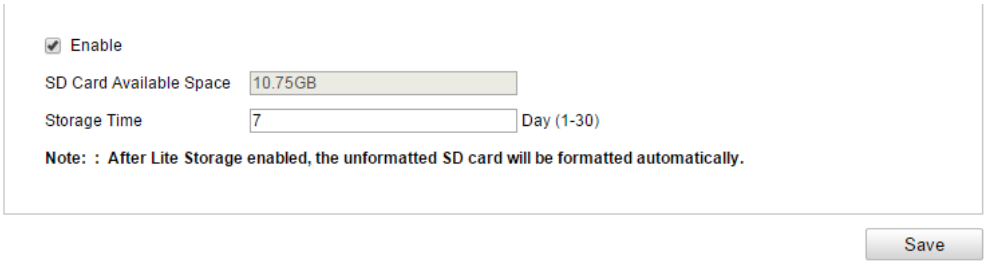


Figure 7-10 Lite Storage Settings

7.5 Configuring Cloud Storage

Purpose:

The captured pictures can be saved on a NVR which works in the Cloud Storage mode.

Note: Cloud storage function varies according to different camera models.

Before you start:

Make sure the NVR has been switched into the Cloud Storage working mode, refer to the User Manual of NVR for details.

Steps:

1. Enter the Cloud Storage interface: **Configuration > Advanced Configuration > Storage > Cloud Storage**.
2. Check the checkbox of **Enable Cloud Storage**.
3. Input the IP address and port of the storage server.
4. Input the user name, password and confirm password for the authentication of the storage server.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*

- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

5. Input picture storage pool ID of the server.
6. (Optional) You can click **Test** to test the cloud storage settings.
7. Click **Save** to save the settings.

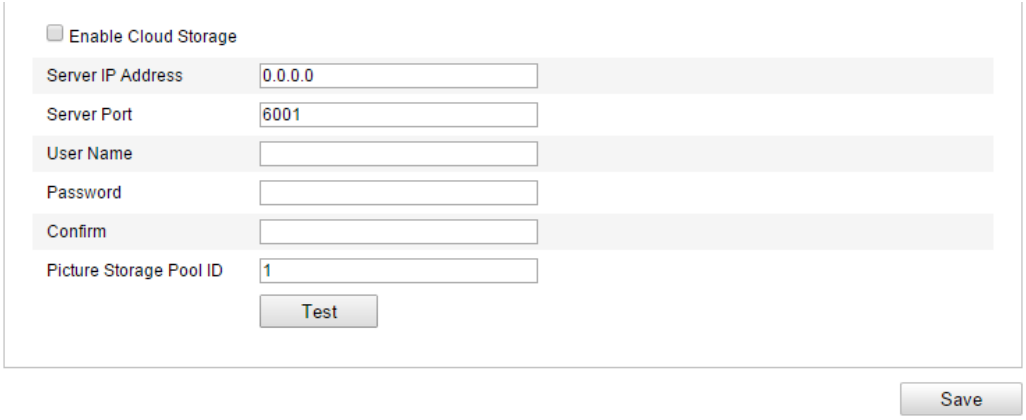


Figure 7-11 Cloud Storage Settings

Chapter 8Road Traffic

Purpose:

Vehicle Detection and Mixed-traffic Detection are available for the road traffic monitoring. In Vehicle Detection, the passed vehicle can be detected and the picture of its license plate can be captured; besides, the vehicle color, vehicle logo and other information can be recognized automatically. In Mixed-traffic Detection, the pedestrian, motor vehicle and non-motor vehicle can be detected, and the picture of the object (for pedestrian / non-motor vehicle / motor vehicle without license plate) or license plate (for motor vehicle with license plate) can be captured. You can send alarm signal to notify the surveillance center and upload the captured picture to FTP server.

Note: Road traffic function varies according to different camera models.

Steps:

❖ **Configuring the Detection Settings**

1. Select the detection type from the list. Vehicle Detection and Mixed-traffic Detection are selectable.

   Note: Reboot the device to activate the new settings when switching the detection type of road traffic.
2. Check the checkbox of **Enable** the enable the selected detection function.
3. Select the lane number in the corresponding dropdown list. Up to 4 lanes are selectable.
4. Click and drag the lane line to set its position, or click and drag the line end to adjust the length and angle of the line.
5. Adjust the zoom ratio of the camera so that the size of the vehicle in the image is close to that of the red frame. Only the position of red frame is adjustable.

   Note: Only 1 license plate can be captured at one time for each lane.
6. Select a Province/State Abbreviation in the drop down list when the attribution of license plate cannot be recognized.
7. Set the Arming Schedule for Vehicle Detection.

1) To edit the arming schedule, click **Edit** button.
2) Choose the day you want to set the arming schedule.
3) Click to set the time period for the arming schedule.
4) (Optional) After you set the arming schedule, you can click the **Copy** button to copy the schedule to other days.
5) Click **OK** to save the settings.

Note: The time of each period cannot be overlapped.

8. Check the checkbox to select the linkage method. Notify surveillance center and upload to FTP are selectable.

   Notify Surveillance Center: Send an exception or alarm signal to remote management software when an event occurs.

   Upload to FTP: Capture the image when an alarm is triggered and upload the picture to a FTP server. And save the picture on the local SD card or connected NAS.

9. Click **Save** to save the settings.

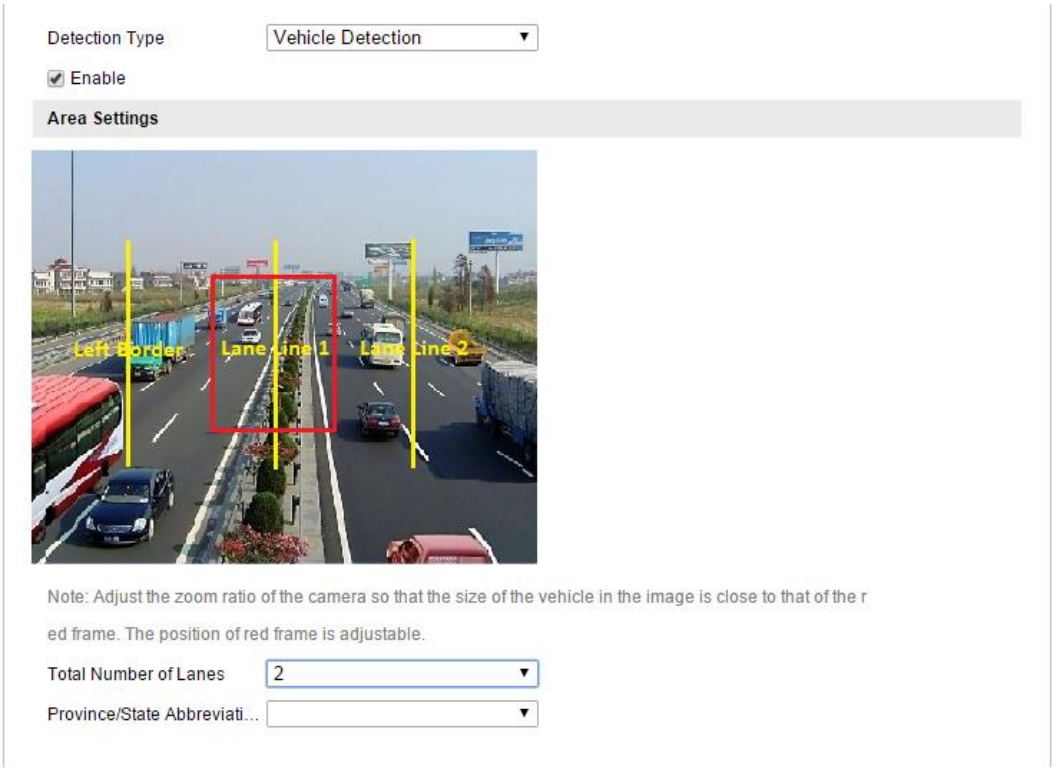


Figure 8-1 Vehicle Detection Configuration

❖ Configuring the Upload Picture

1. Set the picture quality.

   Either Picture Quality or Picture Size can be set to specify the picture quality.2.

2. (Optional) Enable and edit the text overlay on the upload picture.

   You can set the font color and background color by clicking the icon , and click the desired color in the pop-up palette.

3. Select the information for the text overlay, including camera No., camera info, device No., capture time, plate No., vehicle color, etc. You can also click the up and down direction buttons to adjust the sequence of the text.

4. Click the **Save** button to activate the settings.

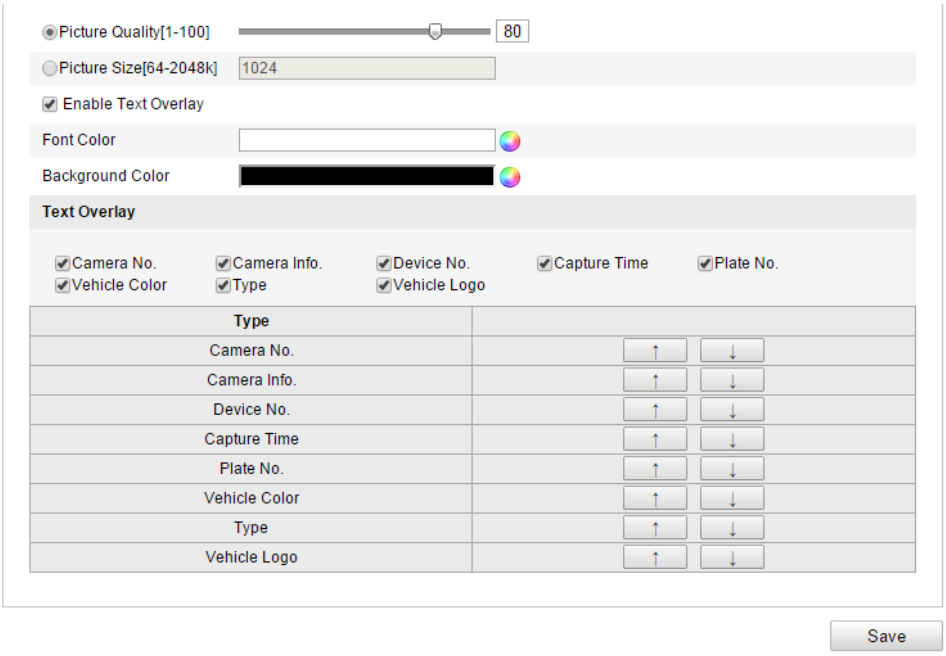


Figure 8-2 Upload Picture Settings

❖ Configuring the Overlay Content

1. Edit the content of the camera No., camera information and device information in the corresponding text filed.
2. (Optional) Enable and edit the text overlay on the picture to upload.
3. Click the **Save** button to activate the settings.

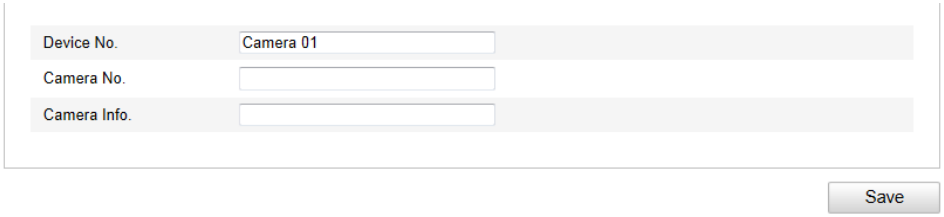


Figure 8-3 Overlay Content Settings

Chapter 9 Playback

Purpose:

This section explains how to view the remotely recorded video files stored in the network disks or SD cards.

Steps:

1. Click **Playback** on the menu bar to enter playback interface.

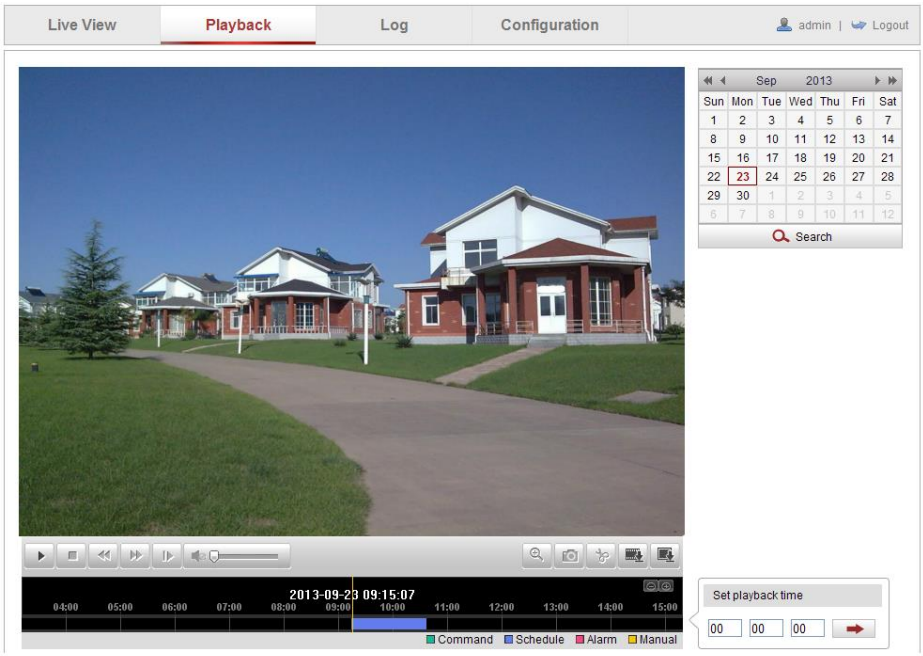


Figure 9-1 Playback Interface

2. Select the date and click **Search**.

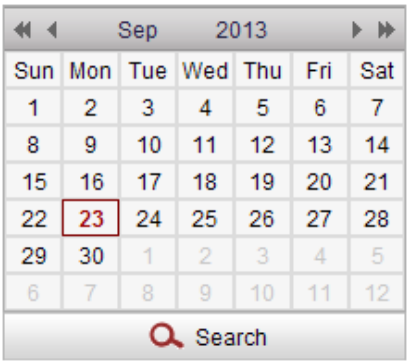


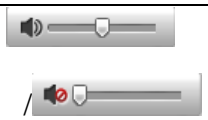
Figure 9-2 Search Video

3. Click to play the video files found on this date.

The toolbar on the bottom of Playback interface can be used to control playing process.

Figure 9-3 Playback Toolbar

Table 9-1 Description of the buttons

Button	Operation	Button	Operation
	Play		Capture a picture
	Pause		Start/Stop clipping video files
	Stop		Audio on and adjust volume/Mute
	Speed down		Download video files
	Speed up		Download captured pictures
	Playback by frame		Enable/Disable digital zoom

Note: You can choose the file paths locally for downloaded playback video files and pictures in Local Configuration interface. Please refer to *Section 6.1* for details.

Drag the progress bar with the mouse to locate the exact playback point. You can also input the time and click to locate the playback point in the **Set playback time** field. You can also click to zoom out/in the progress bar.

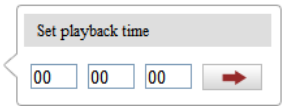


Figure 9-4 Set Playback Time

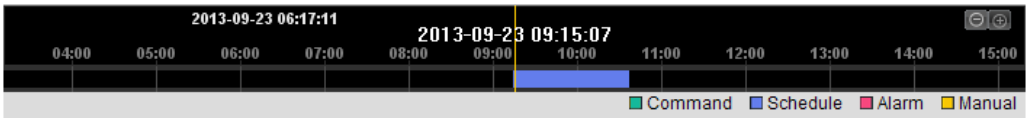


Figure 9-5 Progress Bar

The different colors of the video on the progress bar stand for the different video types.

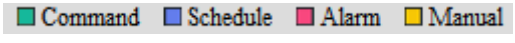


Figure 9-6 Video Types

Chapter 10 Log Searching

Purpose:

The operation, alarm, exception and information of the camera can be stored in log files. You can also export the log files on your demand.

Before you start:

Please configure network storage for the camera or insert a SD card in the camera.

Steps:

1. Click **Log** on the menu bar to enter log searching interface.

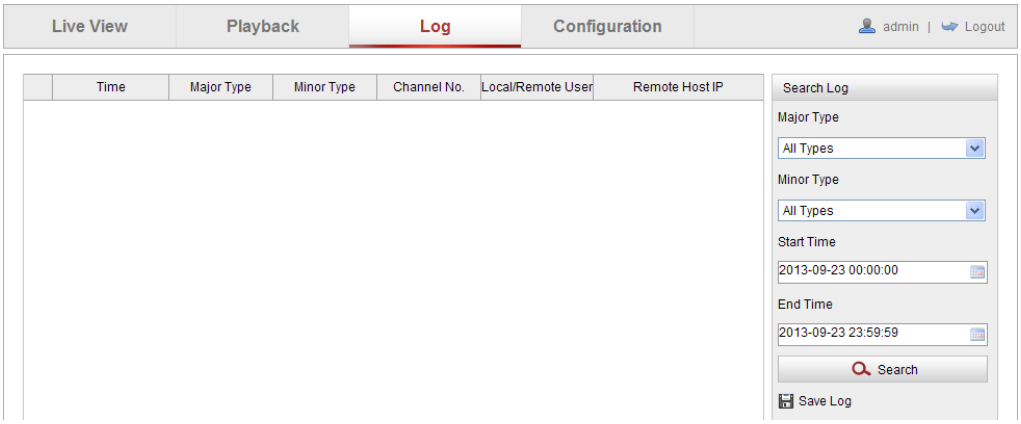


Figure 10-1 Log Searching Interface

2. Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time.
3. Click **Search** to search log files. The matched log files will be displayed on the **Log** interface.

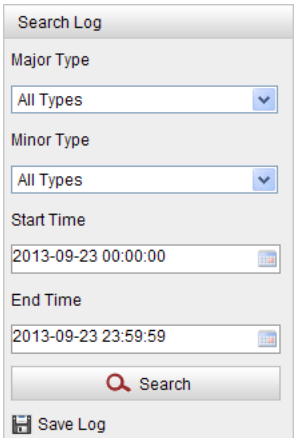


Figure 10-2 Log Searching

4. To export the log files, click **Save log** to save the log files in your computer.

Chapter 11 Others

11.1 Managing User Accounts

Enter the User Management interface:

Configuration >Basic Configuration> Security > User

Or **Configuration > Advanced Configuration> Security > User**

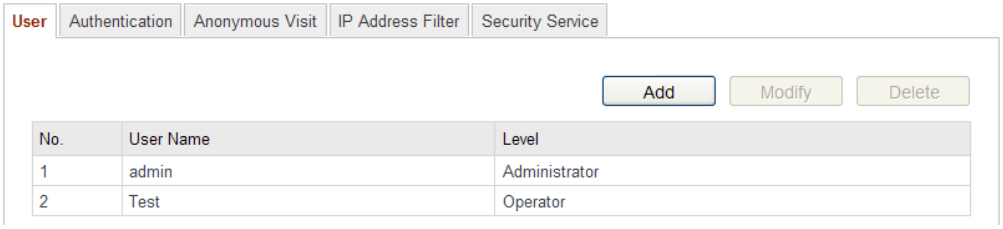


Figure 11-1 User Information

- **Adding a User**

The *admin* user has all permissions by default and can create / modify / delete other accounts.

The *admin* user cannot be deleted and you can only change the *admin* password.

Steps:

1. Click **Add** to add a user.
2. Input the **User Name**, select **Level** and input **Password.**

Notes:

- Up to 31 user accounts can be created.
- Different level user owns different permissions. Operator and user are selectable.

For your privacy *and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8* characters, *including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*

- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

3. In the **Basic Permission** field and **Camera Configuration** field, you can check or uncheck the permissions for the new user.
4. Click **OK** to finish the user addition.

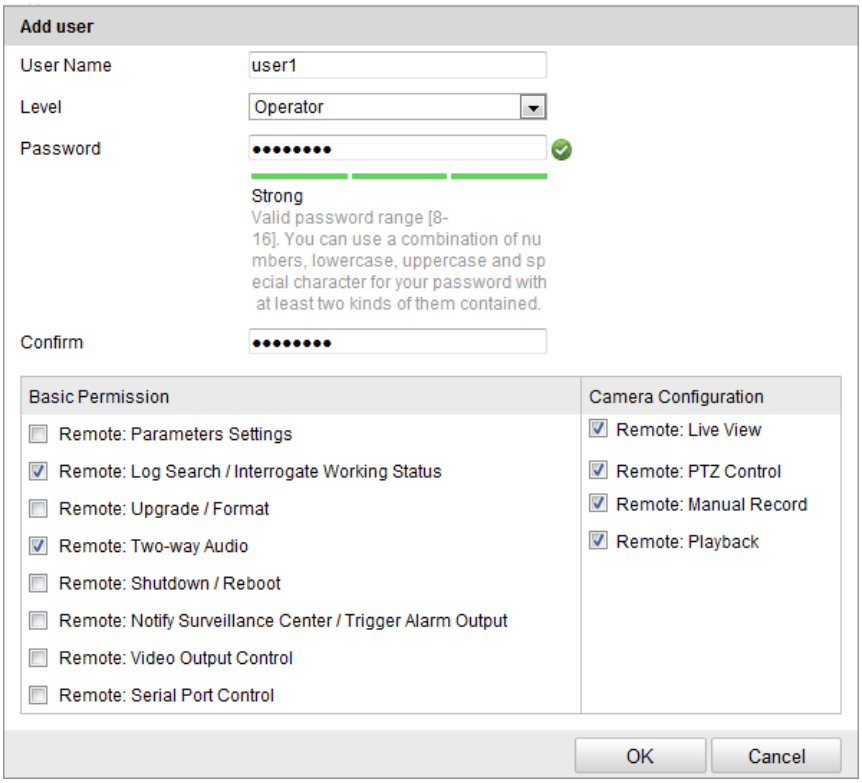


Figure 11-2 Add a User

- **Modifying a User**

Steps:

1. Left-click to select the user from the list and click **Modify**.
2. Modify the **User Name**, **Level** or **Password**.
3. In the **Basic Permission** field and **Camera Configuration** field, you can check or uncheck the permissions.
4. Click **OK** to finish the user modification.

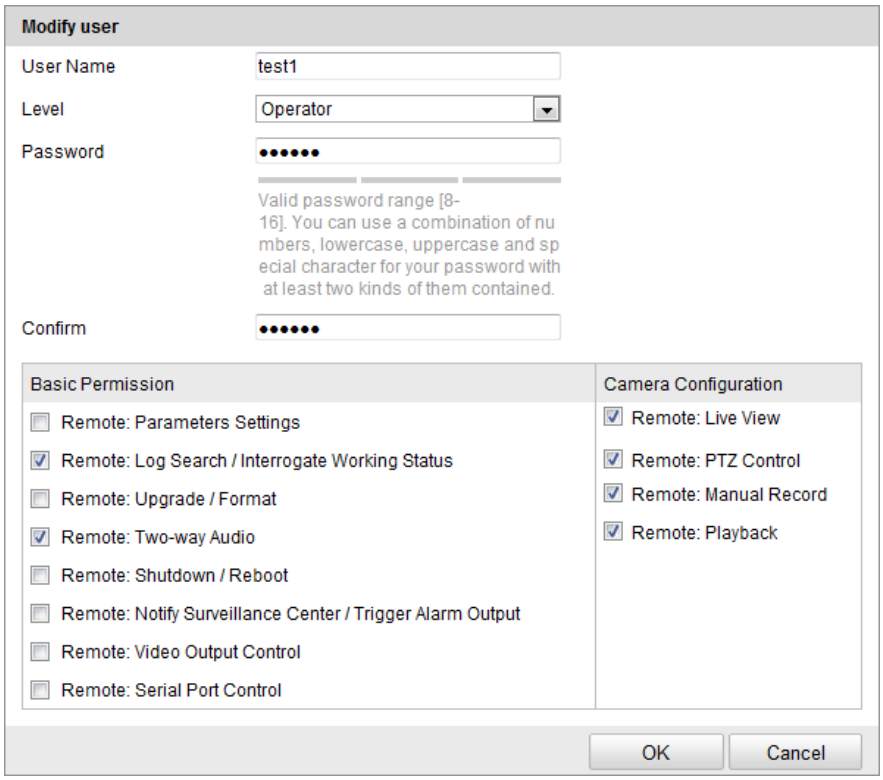


Figure 11-3 Modify a User

- **Deleting a User**

Steps:

1. Click to select the user you want to delete and click **Delete**.
2. Click **OK** on the pop-up dialogue box to delete the user.

11.2 Authentication

Purpose:

You can specifically secure the stream data of live view.

Steps:

1. Enter the Authentication interface: Configuration> Advanced Configuration> Security > Authentication

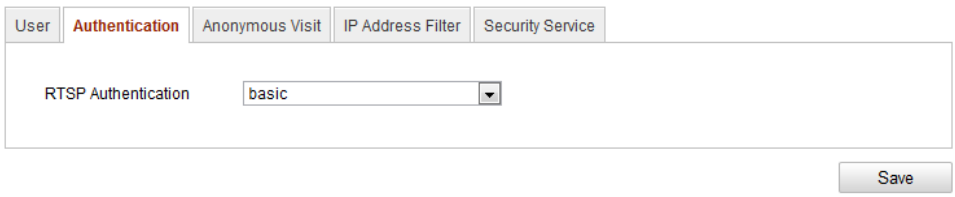


Figure 11-4 RTSP Authentication

2. Select the RTSP **Authentication** type **basic** or **disable** in the drop-down list to enable or disable the RTSP authentication.

Note: If you disable the RTSP authentication, anyone can access the video stream by the RTSP protocol via the IP address.

3. Click **Save** to save the settings.

11.3 Anonymous Visit

Enabling this function allows visit for whom doesn't have the user name and password of the device.

Note: Only live view is available for the anonymous user.

Steps:

1. Enter the Anonymous Visit interface:

Configuration> Advanced Configuration> Security > Anonymous Visit

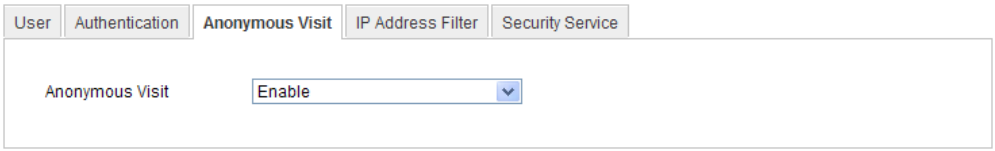


Figure 11-5 Anonymous Visit

2. Set the **Anonymous Visit** permission **Enable** or **Disable** in the drop-down list to enable or disable the anonymous visit.
3. Click **Save** to save the settings.

   There will be a checkbox of Anonymous by the next time you logging in.

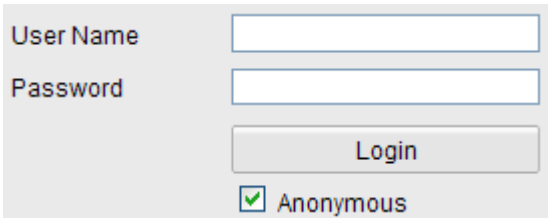


Figure 11-6 Login Interface with an Anonymous Checkbox

4. Check the checkbox of **Anonymous** and click **Login**.

By permitting the Anonymous "Live View" function, you may enable others to access your camera and view live images without providing login credentials. It therefore is

critical when permitting the Anonymous "Live View" function to ensure that your camera's field of view does not impact the privacy of individuals whose images might be captured without authorization.

Given its inherent intrusiveness, video surveillance is inappropriate in areas where people have a higher expectation of privacy.

11.4 IP Address Filter

Purpose:

This function makes it possible for access control.

Steps:

1. Enter the IP Address Filter interface:

Configuration> Advanced Configuration> Security > IP Address Filter

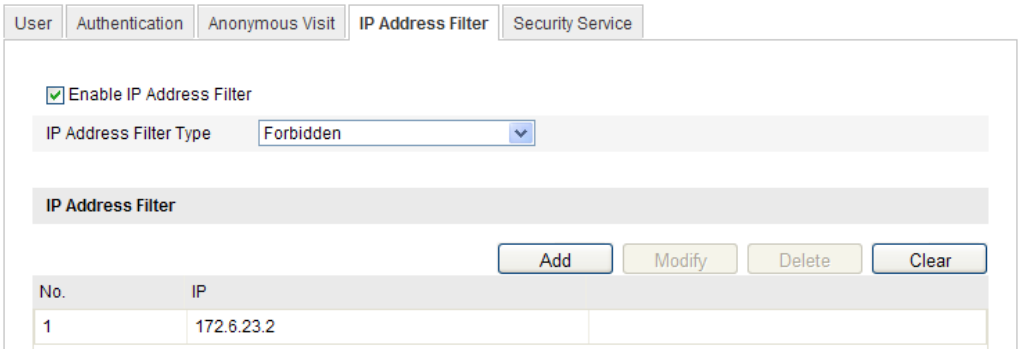


Figure 11-7 IP Address Filter Interface

2. Check the checkbox of **Enable IP Address Filter**.
3. Select the type of IP Address Filter in the drop-down list, **Forbidden** and **Allowed** are selectable.
4. Set the IP Address Filter list.
   - Add an IP Address

     Steps:

   (1) Click the **Add** to add an IP.

   (2) Input the IP Adreess.

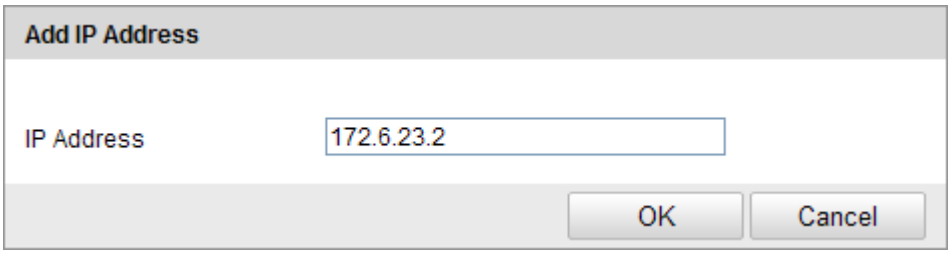


Figure 11-8 Add an IP

(3) Click the **OK** to finish adding.

- Modify an IP Address

Steps:

(1) Left-click an IP address from filter list and click **Modify**.

(2) Modify the IP address in the text filed.

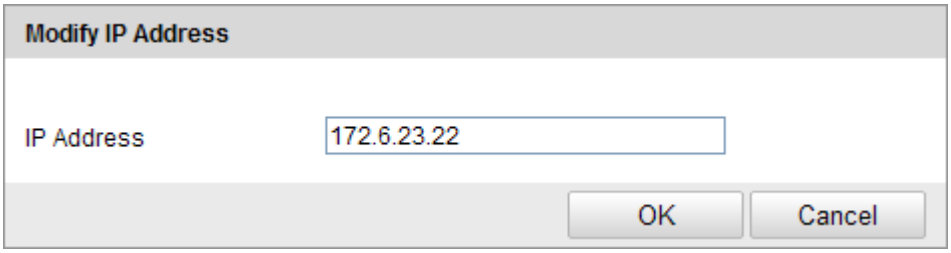


Figure 11-9 Modify an IP

(3) Click the **OK** to finish modifying.

- Delete an IP Address

  Left-click an IP address from filter list and click **Delete**.

- Delete all IP Addresses

  Click **Clear** to delete all the IP addrsses.

5. Click **Save** to save the settings.

11.5 Security Service

To enable the remote login, and improve the data communication security, the camera provides the security service for better user experience.

Steps:

1. Go to **Configuration** > **Advanced configuration** > **Security** >**Security Service** to enter the security service configuration interface.

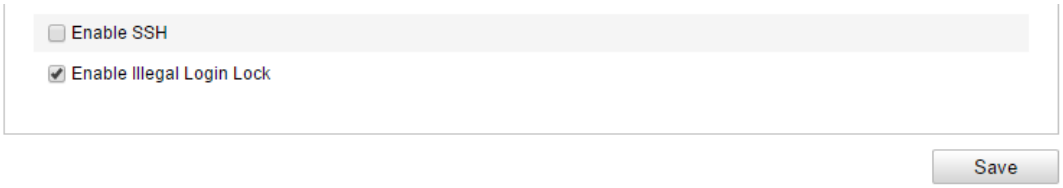


Figure 11-10 Security Service

2. Check the checkbox of **Enable SSH** to enable the data communication security, and uncheck the checkbox to disable the SSH.
3. Check the checkbox of **Enable Illegal Login Lock**, and then the IP address will be locked if the admin user performs 7 failed user name/ password attempts (5 times for the operator/user).

   Note: If the IP address is locked, you can try to login the device after 30 minutes.

11.6 Viewing Device Information

Enter the Device Information interface: **Configuration** > **Basic Configuration**> **System** > **Device Information** or **Configuration** > **Advanced Configuration**> **System** > **Device Information**.

In the **Device Information** interface, you can edit the Device Name.

Other information of the network camera, such as Model, Serial No., Firmware Version, Encoding Version, Number of Channels, Number of HDDs, Number of Alarm Input and Number of Alarm Output are displayed. The information cannot be changed in this menu. It is the reference for maintenance or modification in future.

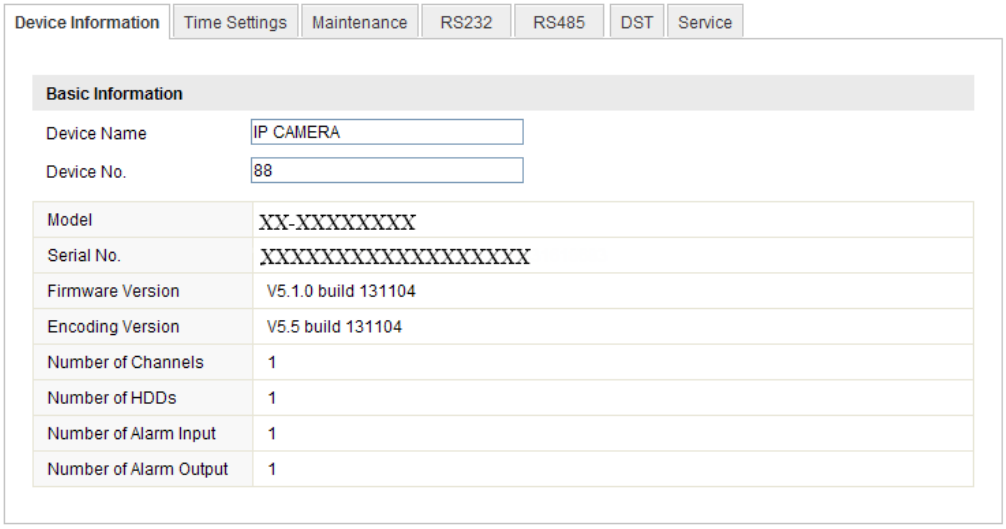


Figure 11-11 Device Information

11.7 Maintenance

11.7.1 Rebooting the Camera

Steps:

1. Enter the Maintenance interface:

Configuration > Basic Configuration> System > Maintenance

Or **Configuration > Advanced Configuration> System > Maintenance:**

2. Click **Reboot** to reboot the network camera.

Figure 11-12 Reboot the Device

11.7.2 Restoring Default Settings

Steps:

1. Enter the Maintenance interface:

Configuration > Basic Configuration> System > Maintenance

Or **Configuration > Advanced Configuration> System > Maintenance**

2. Click **Restore** or **Default** to restore the default settings.

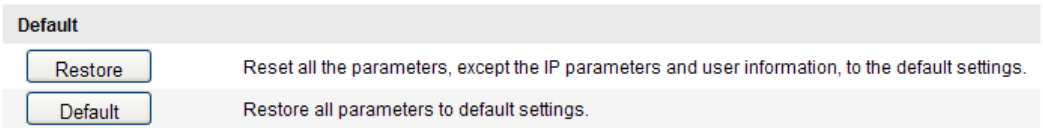


Figure 11-13 Restore Default Settings

Note: After restoring the default settings, the IP address is also restored to the default IP address, please be careful for this action.

11.7.3 Exporting / Importing Configuration File

Purpose:

Configuration file is used for the batch configuration of the camera, which can simplify the configuration steps when there are a lot of cameras needing configuring.

Steps:

1. Enter the Maintenance interface: Configuration > Basic Configuration> System > Maintenance, or Configuration>Advanced Configuration> System > Maintenance
2. Click **Export** to export the current configuration file, and save it to the certain place.
3. Click **Browse** to select the saved configuration file and then click **Import** to start importing configuration file.

   Note: You need to reboot the camera after importing configuration file.
4. Click **Export** and set the saving path to save the configuration file in local storage**.**

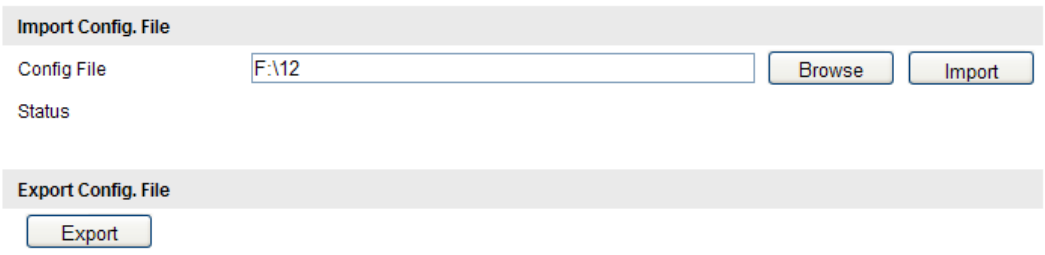


Figure 11-14 Import/Export Configuration File

11.7.4 Upgrading the System

Steps:

1. Enter the Maintenance interface: Configuration > Basic Configuration> System > Maintenance , or Configuration > Advanced Configuration> System > Maintenance
2. Select firmware or firmware directory to locate the upgrade file.

   Firmware: Locate the exact path of the upgrade file.

   Firmware Directory: Only the directory the upgrade file belongs to is required.
3. Click **Browse** to select the local upgrade file and then click **Upgrade** to start remote upgrade.

Figure 11-15 Remote Upgrade

Note: The upgrading process will take 1~10 minutes. Please don't disconnect power of the camera during the process, and the camera reboots automatically after upgrade.

11.8 RS-232 Settings

The RS-232 port can be used in two ways:

- Parameters Configuration: Connect a computer to the camera through the serial port. Device parameters can be configured by using software such as HyperTerminal. The serial port parameters must be the same as the serial port parameters of the camera.
- Transparent Channel: Connect a serial device directly to the camera. The serial device will be controlled remotely by the computer through the network.

Steps:

1. Enter RS-232 Port Setting interface:

Configuration> Advanced Configuration> System > RS232

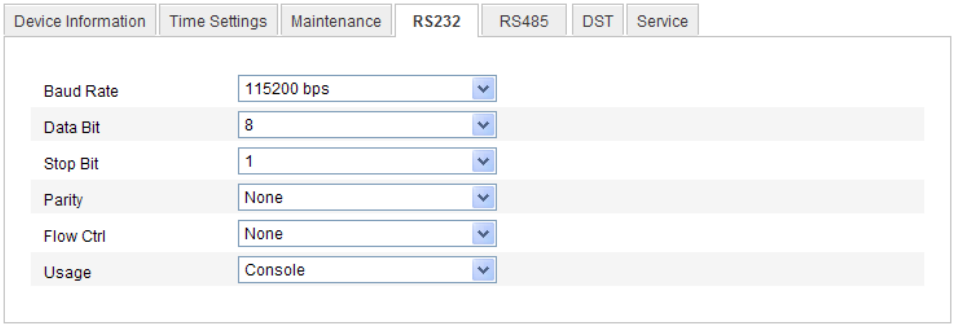


Figure 11-16 RS-232 Settings

Note: If you want to connect the camera by the RS-232 port, the parameters of the RS-232 should be exactly the same with the parameters you configured here.

2. Click **Save** to save the settings.

11.9 RS-485 Settings

Purpose:

The RS-485 serial port is used to control the PTZ of the camera. The configuring of the PTZ parameters should be done before you control the PTZ unit.

Steps:

1. Enter RS-485 Port Setting interface:

Configuration> Advanced Configuration> System > RS485

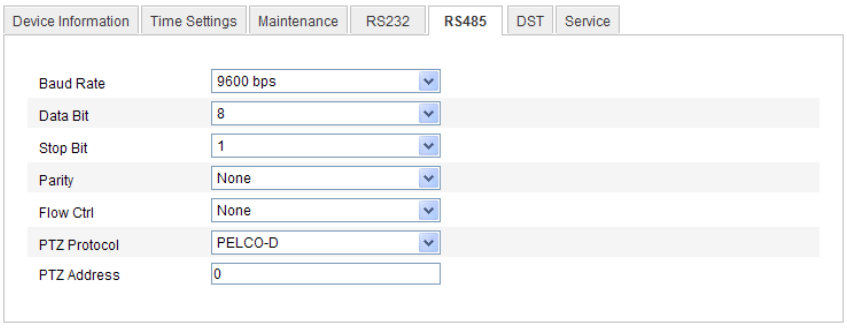


Figure 11-17 RS-485 Settings

2. Set the RS-485 parameters and click **Save** to save the settings.

   By default, the Baud Rate is set as 9600 bps, the Data Bit is 8, the stop bit is 1 and the Parity and Flow Control is None.

   Note: The Baud Rate, PTZ Protocol and PTZ Address parameters should be exactly the same as the PTZ camera parameters.

11.10 Service Settings

Go to **Configuration> Advanced Configuration> System > Service** to enter the service settings interface.

Service settings refer to the hardware service the camera supports, and it varies according to the different cameras.

For the cameras support IR LED, ABF (Auto Back Focus), Auto Defog, or Status LED, you can go to the hardware service, and select to enable or disable the corresponding service according to the actual demands.

Appendix

Appendix 1 SADP Software Introduction

- **Description of SADP**

SADP (Search Active Devices Protocol) is a kind of user-friendly and installation-free online device search tool. It searches the active online devices within your subnet and displays the information of the devices. You can also modify the basic network information of the devices using this software.

- **Search active devices online**

♦ **Search online devices automatically**

After launch the SADP software, it automatically searches the online devices every 15 seconds from the subnet where your computer locates. It displays the total number and information of the searched devices in the Online Devices interface. Device information including the device type, IP address and port number, etc. will be displayed.

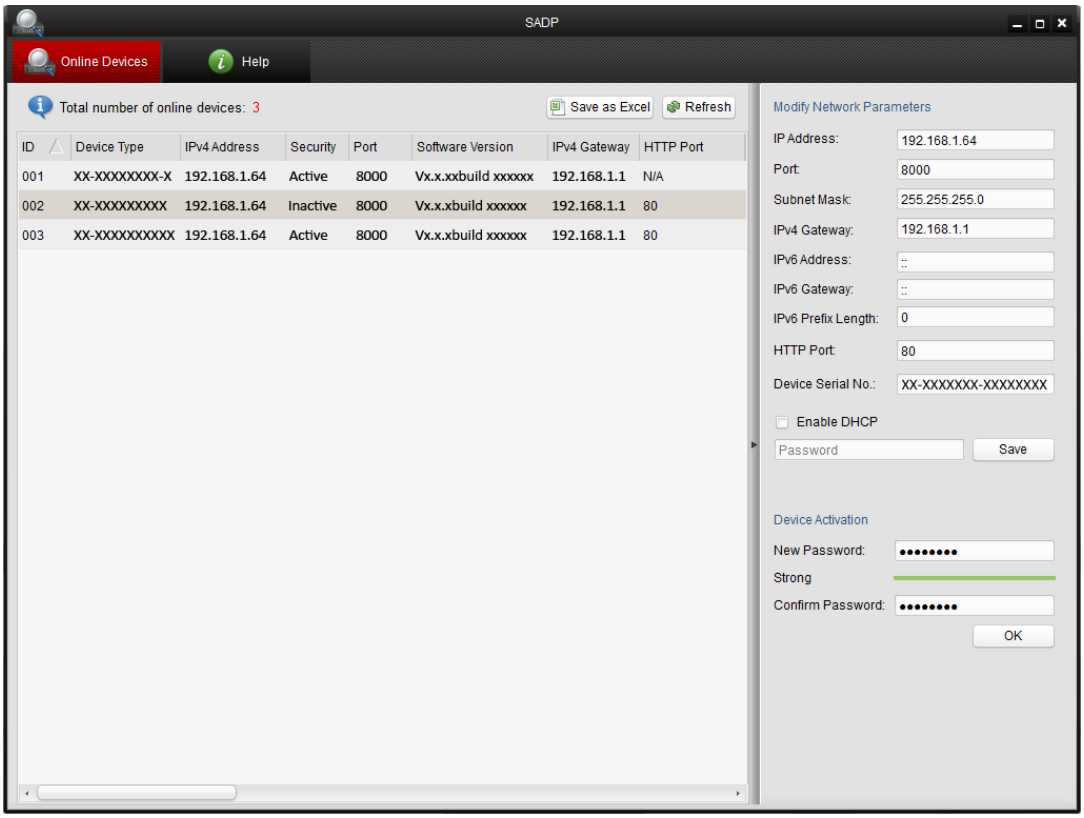


Figure A.1.1 Searching Online Devices

Note:

Device can be searched and displayed in the list in 15 seconds after it went online; it will be removed from the list in 45 seconds after it went offline.

♦ **Search online devices manually**

You can also click Refresh to refresh the online device list manually. The newly searched devices will be added to the list.

NOTE You can click △ or ▽ on each column heading to order the information; you can click ▶ to expand the device table and hide the network parameter panel on the right side, or click ◀ to show the network parameter panel.

● Modify network parameters

Steps:

1. Select the device to be modified in the device list and the network parameters of the device will be displayed in the **Modify Network Parameters** panel on the right side.
2. Edit the modifiable network parameters, e.g. IP address and port number.
3. Enter the password of the admin account of the device in the **Password** field and click Save to save the changes.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

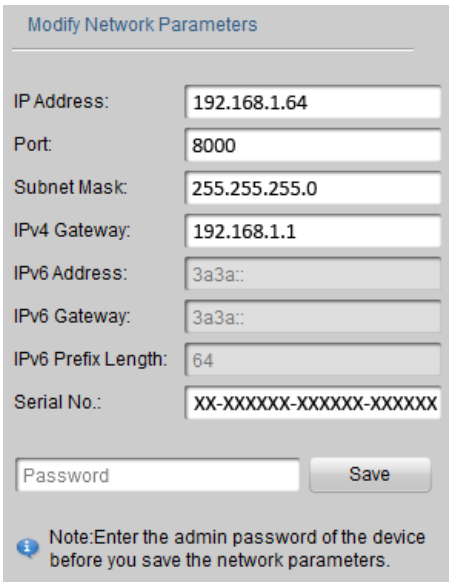


Figure A.1.2 Modify Network Parameters

Appendix 2 Port Mapping

The following settings are for TP-LINK router (TL-WR641G). The settings vary depending on different models of routers.

Steps:

1. Select the **WAN Connection Type**, as shown below:

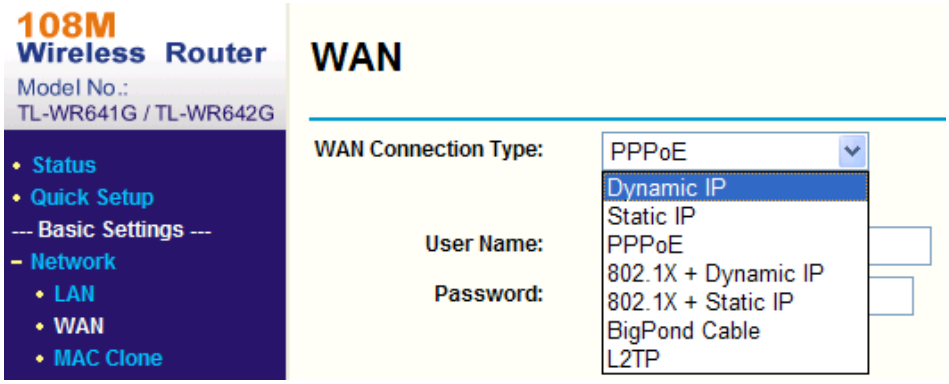


Figure A.2.1 Select the WAN Connection Type

2. Set the **LAN** parameters of the router as in the following figure, including IP address and subnet mask settings.

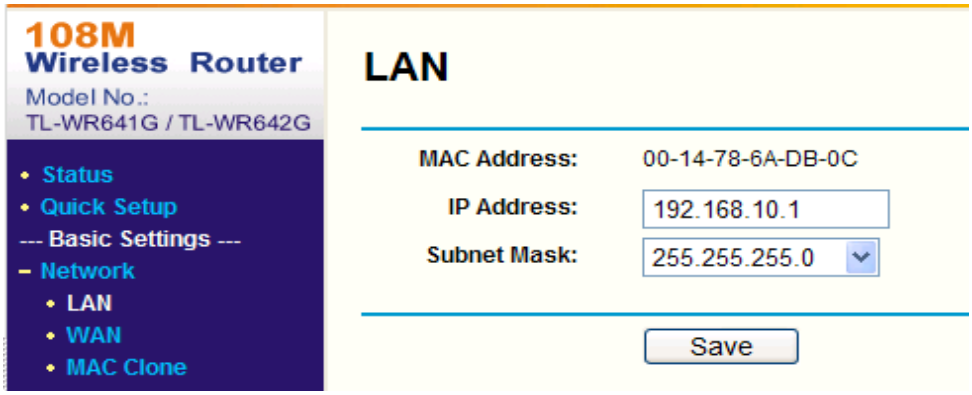


Figure A.2.2 Set the LAN parameters

3. Set the port mapping in the virtual severs of **Forwarding**. By default, camera uses port 80, 8000 and 554. You can change these ports value with web browser or client software.

Example:

When the cameras are connected to the same router, you can configure the ports of a camera as 80, 8000, and 554 with IP address 192.168.1.23, and the ports of

another camera as 81, 8001, 555, 8201 with IP 192.168.1.24. Refer to the steps as below:

Steps:

1. As the settings mentioned above, map the port 80, 8000, 554 and 8200 for the network camera at 192.168.1.23
2. Map the port 81, 8001, 555 and 8201 for the network camera at 192.168.1.24.
3. Enable **ALL** or **TCP** protocols.
4. Check the **Enable** checkbox and click **Save** to save the settings.

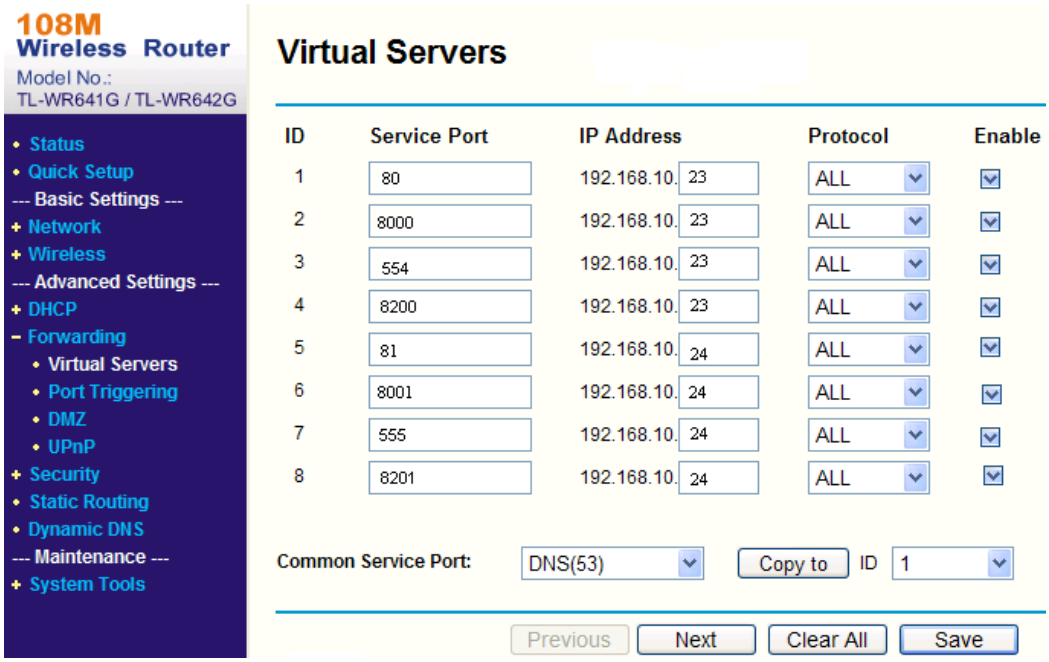


Figure A.2.3 Port Mapping

Note: The port of the network camera cannot conflict with other ports. For example, some web management port of the router is 80. Change the camera port if it is the same as the management port.

Notification of Compliance

Appendix

Europe - EU Declaration of Conformity

For complete DoC please visit
http://global.level1.com/downloads.php?action=init

GPL License Agreement

GPL may be included in this product, to view the GPL license agreement goes to
http://download.level1.com/level1/gpl/GPL.pdf

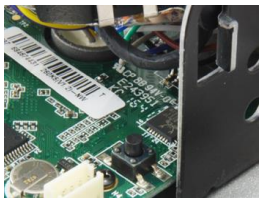
For GNU General Public License (GPL) related information, please visit
http://global.level1.com/downloads.php?action=init

Appendix A. microSD Card Slot & RESET Button (Optional)

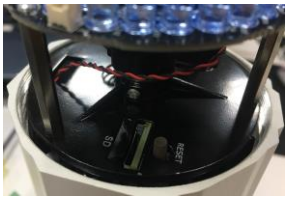
Unscrew the microSD/RESET/ Cover, and you can see the RESET button and the microSD card slot. Press RESET about 10s when the camera is powering on or rebooting to restore the default settings, including the user name, password, IP address, port No., etc.

Reset Button & SD card Slot Position

FCS-5058	FCS-5067



FCS-3084	FCS-3073	FCS-3085	FCS-3086
FCS-3090	FCS-3096	FCS-3087	



FCS-5059	FCS-5060	FCS-5068

FCS-4103

FCS-3097	FCS-3098	FCS-4203

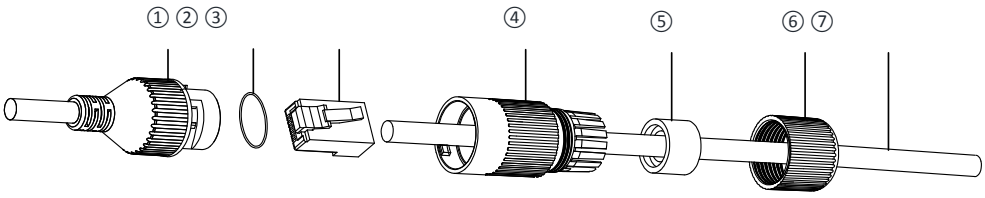
FCS-5092	FCS-5093

FCS-5094	FCS-5095	FCS-5096

Appendix B. Network Cable Water-proof Jacket Installation (Optional)

Purpose:

If the camera is installed outdoor, you can adapt the water-proof accessory for the network cable after the camera is secured on the installation surface.



Water-proof Accessory Components

Components

No.	Components
1	Camera's Network Interface Socket
2	O-Type Gasket
3	Network Plug
4	Waterproof Endcap
5	Waterproof Rubber Gasket
6	Lock Nut
7	Network Cable from Router/Switch

Steps:

1. Feed the plugless network cable ⑦ through the lock nut ⑥, waterproof rubber gasket ⑤ (rubber gasket inset ridge must face waterproof endcap), and the water-proof endcap ④ in order.
2. Crimp an RJ-45 network plug ③onto the end of the cable,

   taking care to insert the twisted pairs of wires in correct order.
3. Place the O-type gasket ② onto the end of the camera's

   network interface socket ①.
4. Insert the network plug ③ into the camera's network interface

   socket①.