HIKVISION

Thermometric Network Bullet Camera

User Manual

User Manual

COPYRIGHT ©2016 Hangzhou Hikvision Digital Technology Co., Ltd.

ALL RIGHTS RESERVED.

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be "Hikvision"). This user manual (hereinafter referred to be "the Manual") cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

About this Manual

This Manual is applicable to Thermal Network Bullet Camera (V5.3.7).

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 (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

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 HIKVISION 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 HIKVISION, 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 HIKVISION 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. HIKVISION 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, HIKVISION 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. HIKVISION 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

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 2014/30/EU, 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.
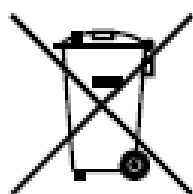
2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (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 -40°C ~ 65°C), 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.

Table of Contents

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.
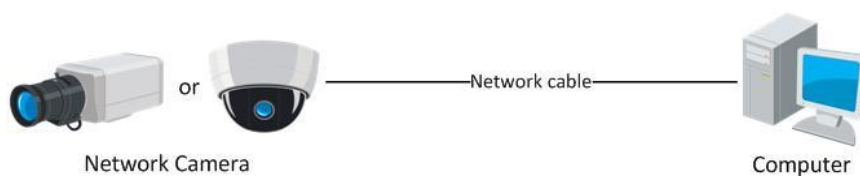

Figure 2-1 Connecting Directly
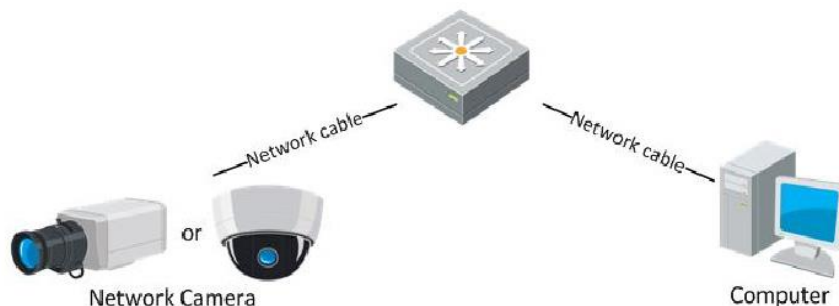
Figure 2-2 Connecting via a Switch or a Router

2.1.2 Activating the Camera

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

Activation via Web Browser, Activation via SADP, and Activation via Client Software are all supported.
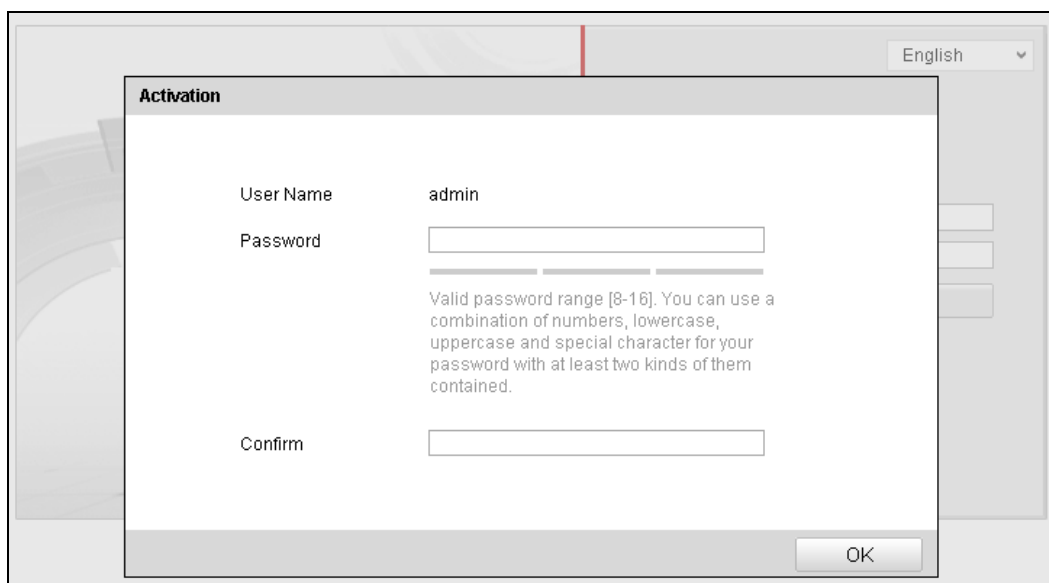
❖ Activation via Web Browser

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, you need to activate the camera via SADP software. Please refer to the following chapter for Activation via SADP.

Figure 2-3 Activation Interface(Web)

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 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.

❖ **Activation 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 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.

❖ Activation via Client Software

The client software is versatile video management software for multiple kinds of
devices.

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

Steps:

1. Run the client software and the control panel of the software pops up, as shown in
   the figure below.
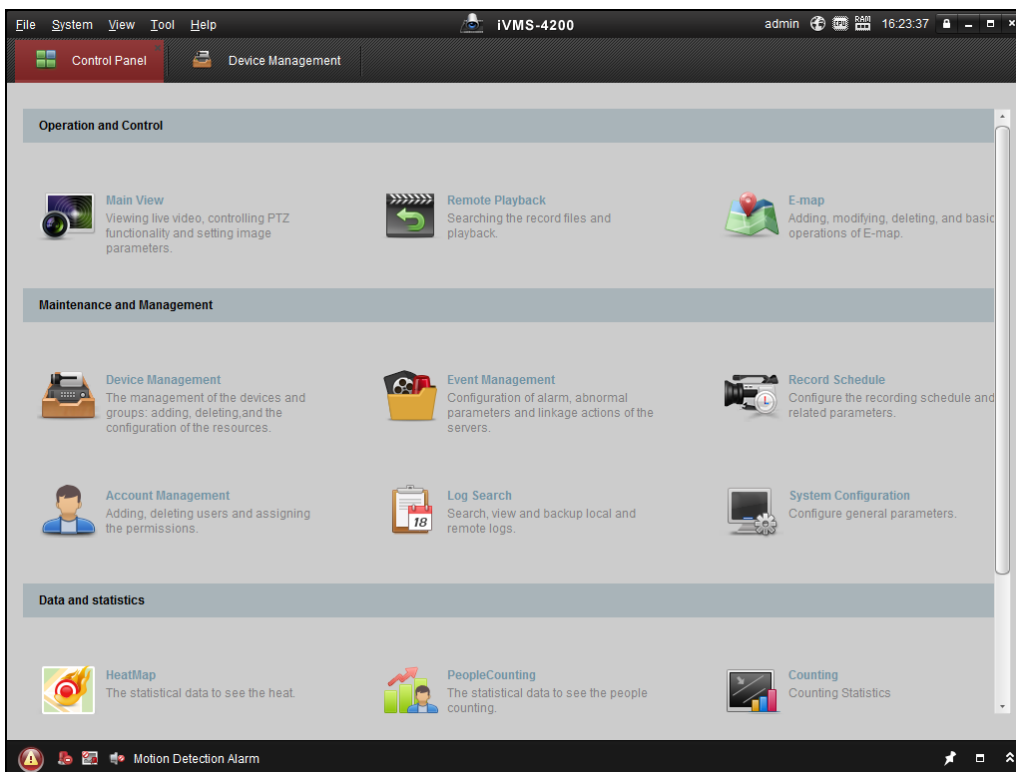
Figure 2-6 Control Panel

2. Click the **Device Management** icon to enter the Device Management interface, as shown in the figure below.
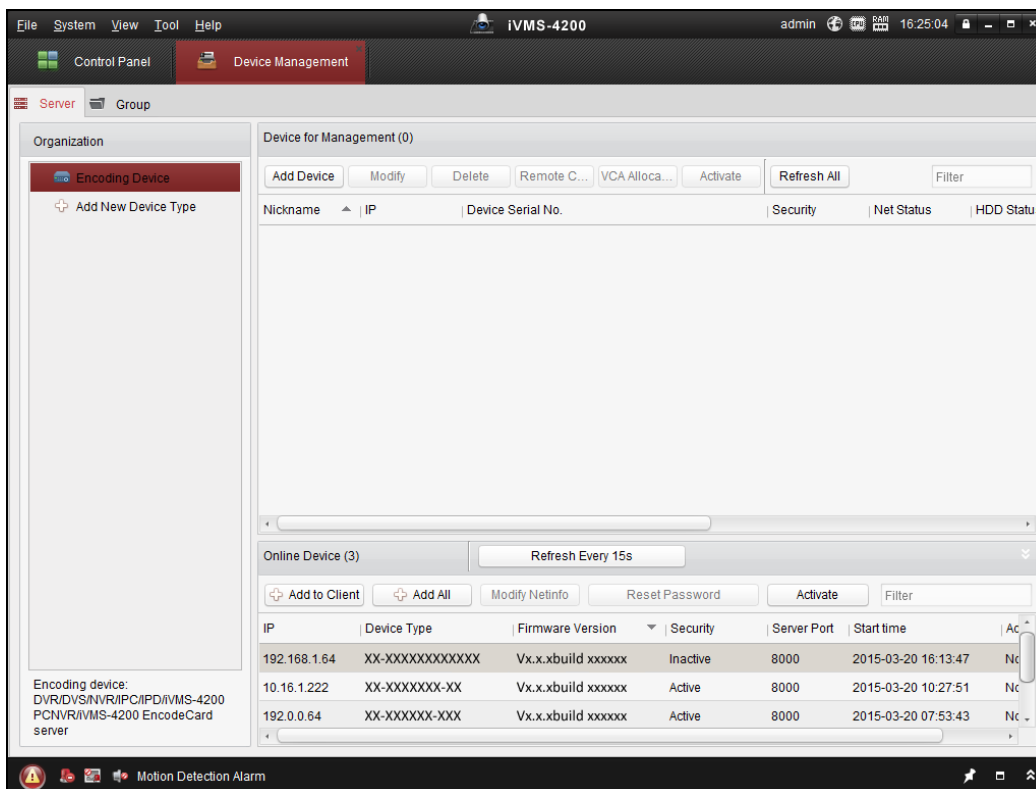
Figure 2-7 Device Management Interface

3. Check the device status from the device list, and select an inactive device.
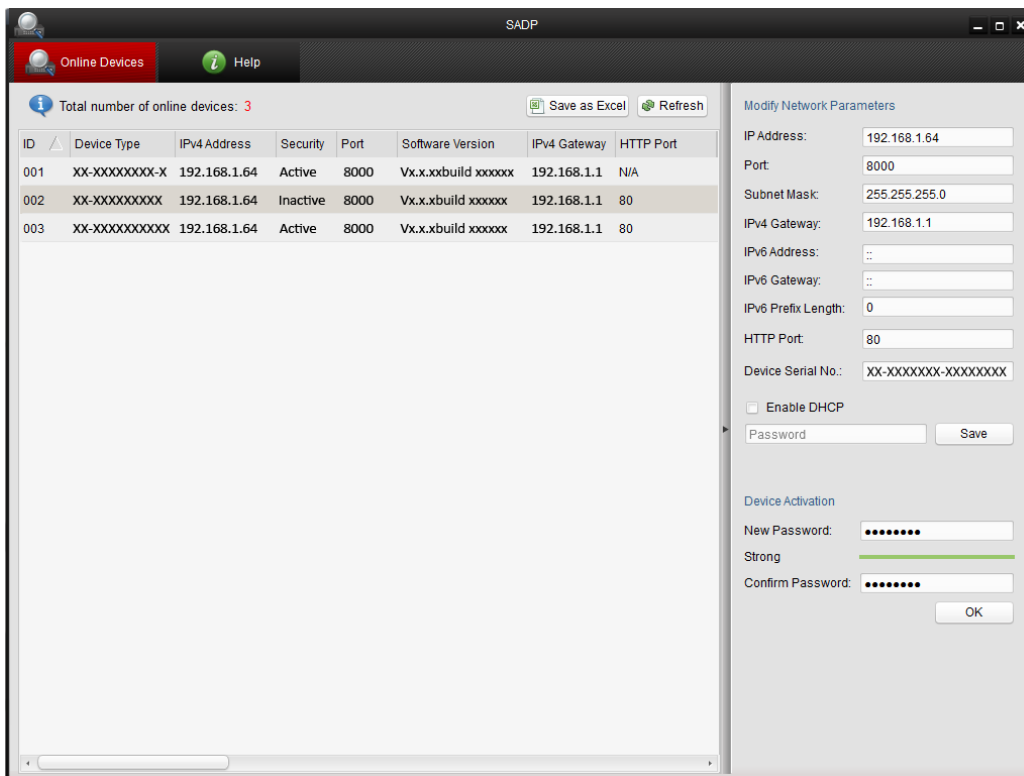
4. Click the **Activate** button to pop up the Activation interface.

5. 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 upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Figure 2-8 Activation Interface (Client Software)

6. Click **OK** button to start activation.

7. Click the Modify Netinfo button to pop up the Network Parameter Modification interface, as shown in the figure below.
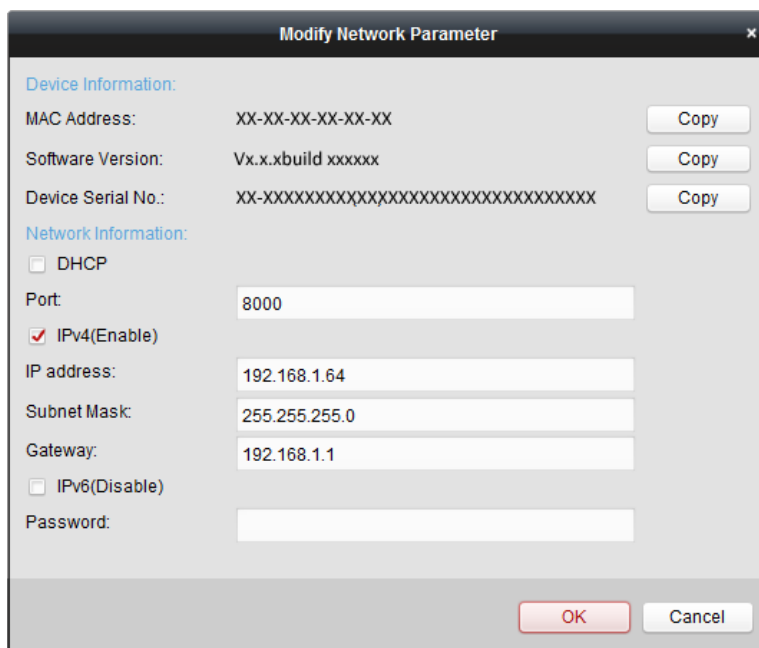
Figure 2-9 Modifying the Network Parameters

8. 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.

9. 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.
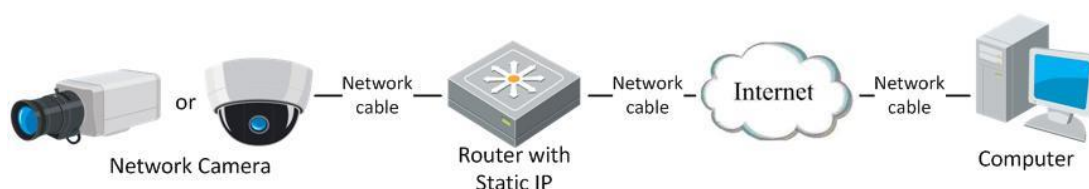
Figure 2-10 Accessing the Camera through Router with Static IP

● **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.
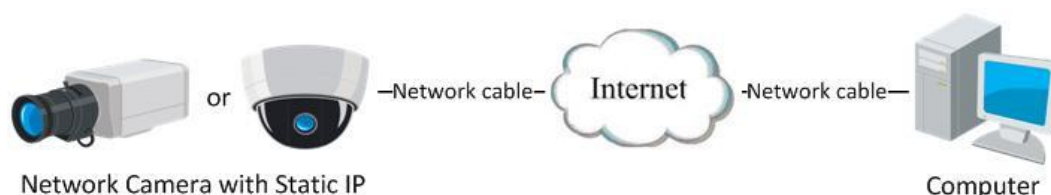
Figure 2-11 Accessing the Camera with Static IP Directly

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.
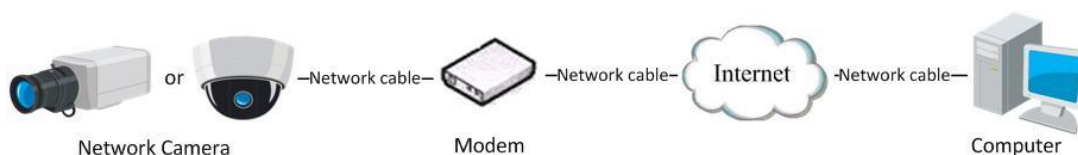
Figure 2-12 Accessing the Camera with Dynamic IP

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
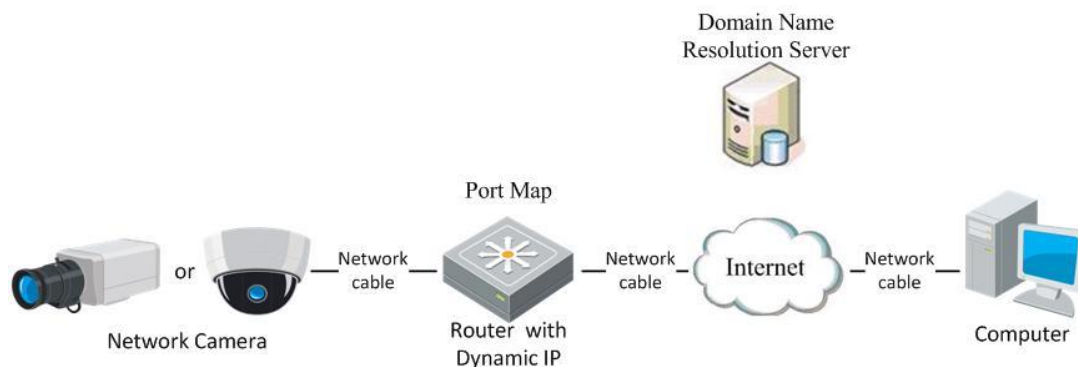
Figure 2-13 Normal Domain Name Resolution

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
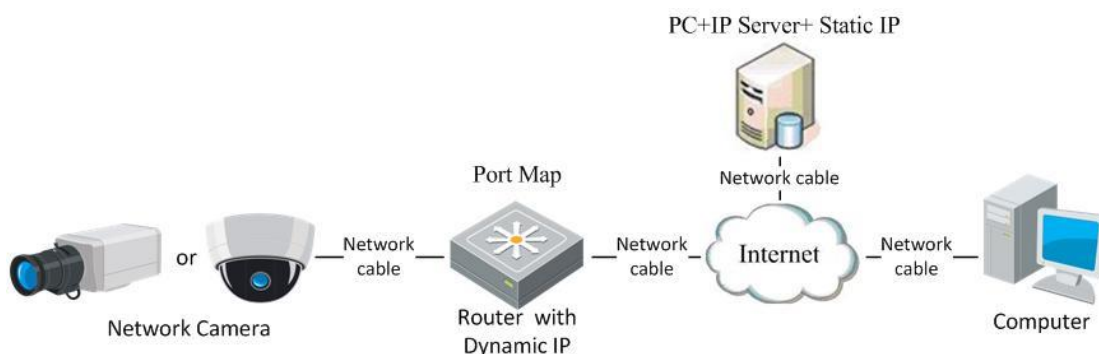
Figure 2-14 Private Domain Name Resolution

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.
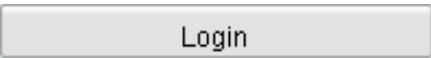
Chapter 3 Access to the Network Camera

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 device IP address gets locked if the admin user performs 7 failed password attempts (5 attempts for the user/operator).
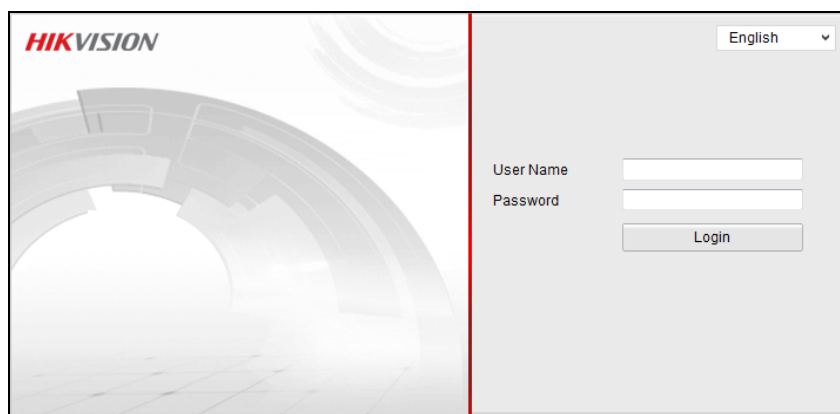
Figure 3-1 Login Interface

6. Install the plug-in before viewing the live video and operating the camera. Please follow the installation prompts to install the plug-in.
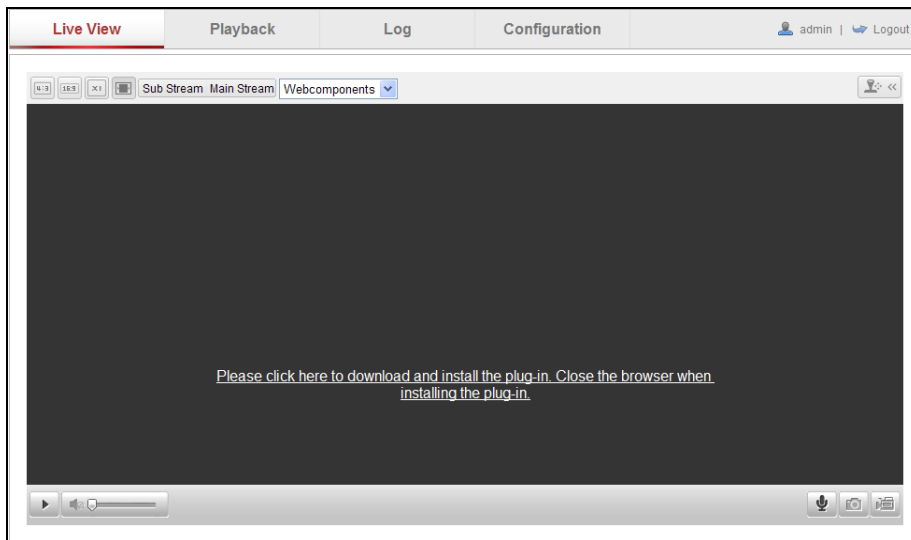
Figure 3-2 Download and Install Plug-in
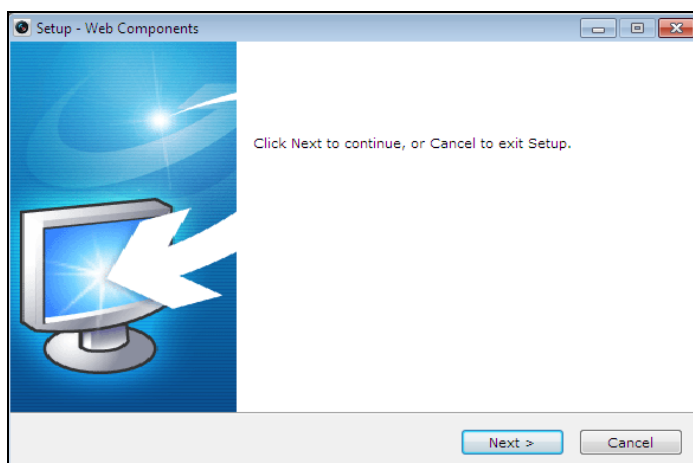
Figure 3-3 Install Plug-in (1)
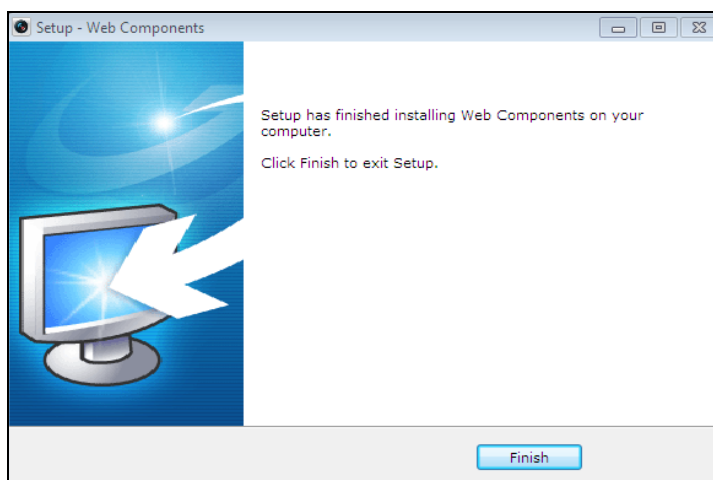
Figure 3-4 Install Plug-in (2)

23

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.

3.2 Accessing by Client Software

The product CD contains the iVMS-4200 client software. You can view the live video and manage the camera with the software.

Follow the installation prompts to install the software. The control panel and live view interface of iVMS-4200 client software are shown as below.
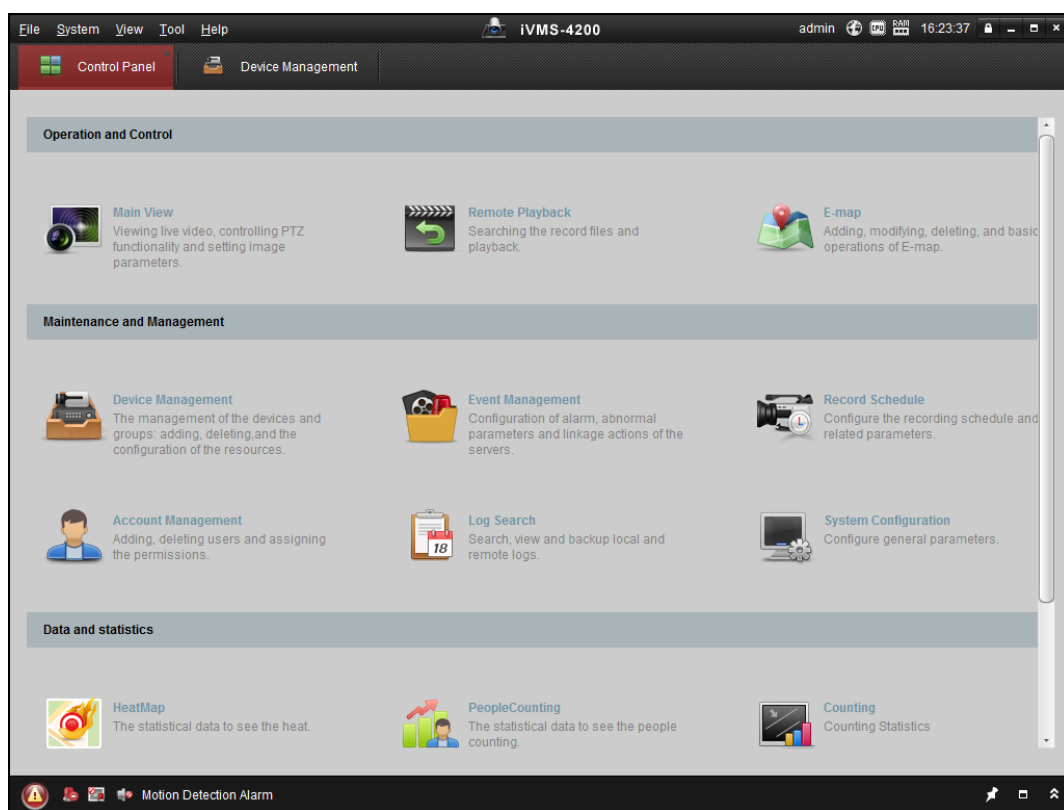
Figure 3-5 iVMS-4200 Control Panel
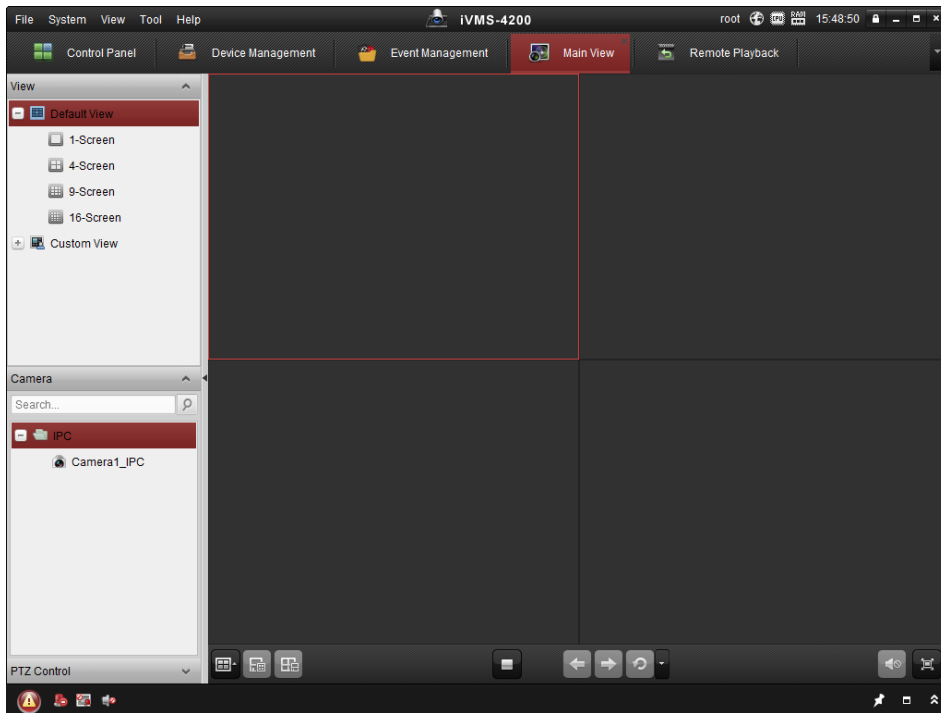
Figure 3-6 iVMS-4200 Main View

Note: For detailed information about the software, please refer to the user manual of the iVMS-4200.

Chapter 4Live View

4.1 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:
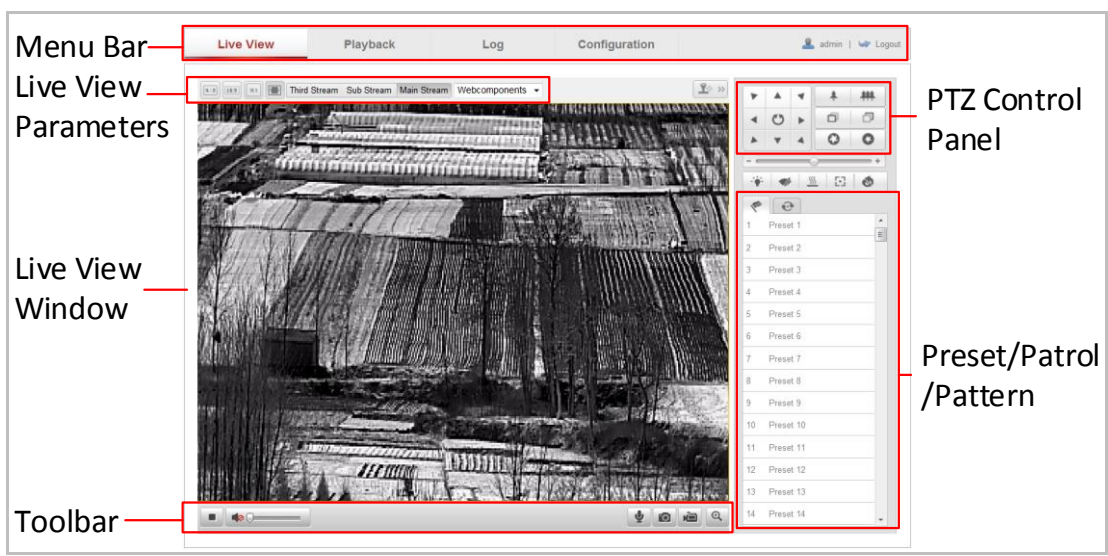
Figure 4-1 Live View Page

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 button to adjust the layout and the stream type of the live view. You can click the drop-down to select the layout for display. 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., start/stop live view, capture, record, start/stop 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.

4.2 Starting Live View

In the live view window as shown in Figure 4-2, click on the toolbar to start the live view of the camera.

Figure 4-2 Live View Toolbar

Table 4-1 Descriptions of the Display Control Bar and the Toolbar

Icon	Description
▶ / ■	Start/Stop live view.
4:3	The window size is 4:3.
16:9	The window size is 16:9.
x1	The original widow size.
▣	Self-adaptive window size.
Main Stream	Live view with the main stream.
Sub Stream	Live view with the sub stream.
Webcomponents ▾	Click to select the third-party plug-in.

2*2 ▾	Window division
📷	Manually capture the picture.
📹 / 📹	Manually start/stop recording.
🔊 / 🔇	Audio on and adjust volume /Mute.
🎤 / 🎤	Start/stop two-way audio.
🔍 / 🔍	Enable/disable e-PTZ function.

4.3 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 6.3*.

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

Chapter 5 Network Camera Configuration

5.1 Configuring Local Parameters

Note: The local configuration refers to the parameters of the live view, record files and captured pictures and clips. The record files, captured pictures and clips 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 5-1 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 5.3.1 Configuring TCP/IP Settings*.

  - **Live View Performance:** Set the live view performance to Shortest Delay or Auto.

  - **Auto Start Live View:** If you enable this function, live view images will be automatically started when **Live View** tab is activated. If the function is disabled, you can also manually start live view in the Live View interface.

  - **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.

  - **Fire Point:** Select Fire Source Detection as VCA Resource Type. Check the checkbox to enable the functions required. Display Fire Point Distance, Display Highest Temperature, Locate Highest Temperature Point and Frame Fire Point are selectable.

  - **Display Temperature Info. on Stream:** Select Temperature Measurement as VCA Resource Type. Check the checkbox to display the temperature information on the live view interface.

  - **Display Temperature Info. on Capture:** Select Temperature Measurement as VCA Resource Type. Check the checkbox to display the temperature

information on the captures.

- **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.

5.2 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**
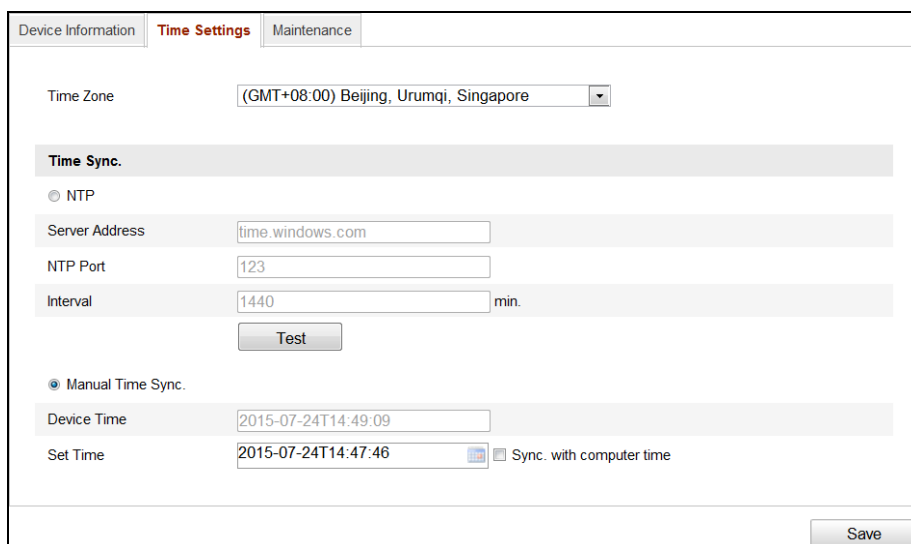
Figure 5-2 Time Settings

2. Select the Time Zone.

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

3. Set Time Synchronization.

You can synchronize the time through NTP, or you can do it manually.

● 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.
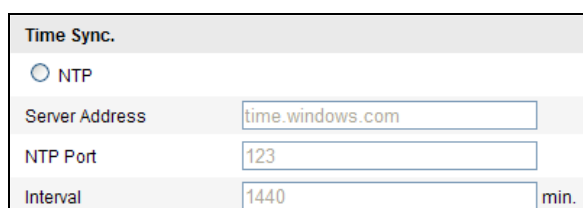
Figure 5-3 Time Sync by NTP Server

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 Manually

Enable the **Manual Time Sync** function and then click [image] 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.
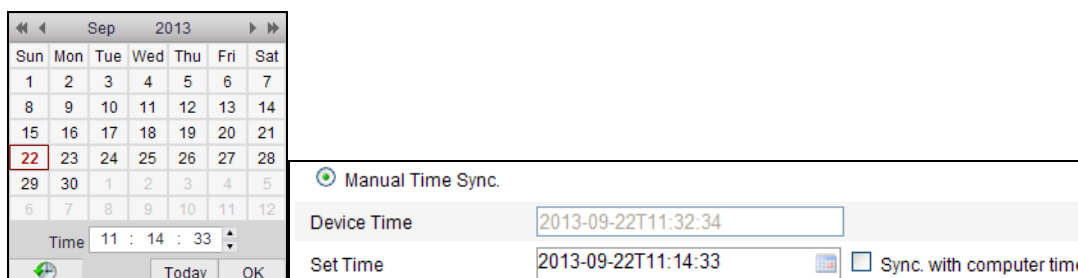
Figure 5-4 Time Sync Manually

4. Click the **DST** tab page (**Configuration > Advanced Configuration > System > DST**) to enable the DST function and Set the date of the DST period.
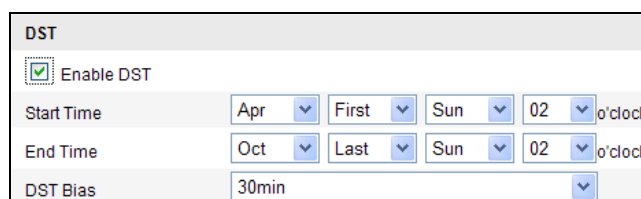
Figure 5-5 DST Settings

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

5.3 Configuring Network Settings

5.3.1 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 with 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 5-6 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.

5.3.2 Configuring Port Settings

Purpose:

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

Steps:

1. Enter the Port Settings interface:

    Configuration > Basic Configuration > Network > Port

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

HTTP Port	80
RTSP Port	554
HTTPS Port	443
Server Port	8000

Figure 5-7 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.

5.3.3 Configuring PPPoE Settings

Purpose:

If you have no router but only a modem, you can use Point-to-Point Protocol over

Ethernet (PPPoE) function.

Steps:

1. Enter the PPPoE Settings interface:

    Configuration >Advanced Configuration > Network > PPPoE

Figure 5-8 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 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.

5.3.4 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 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

Figure 5-9 DDNS Settings

2. Check the **Enable DDNS** checkbox to enable this feature.

3. Select **DDNS Type**. Four DDNS types are selectable: HiDDNS, 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 5-10 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 5-11 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 5-12 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.

● HiDDNS

Steps:

(1) Choose the DDNS Type as HiDDNS.

Figure 5-13 HiDDNS Settings

(2) Enter the Server Address *www.hik-online.com.*

(3) Enter the Domain name of the camera. The domain is the same with the device alias in the HiDDNS server.

(4) Click **Save** to save the new settings.

Note: A reboot is required for the settings to take effect.
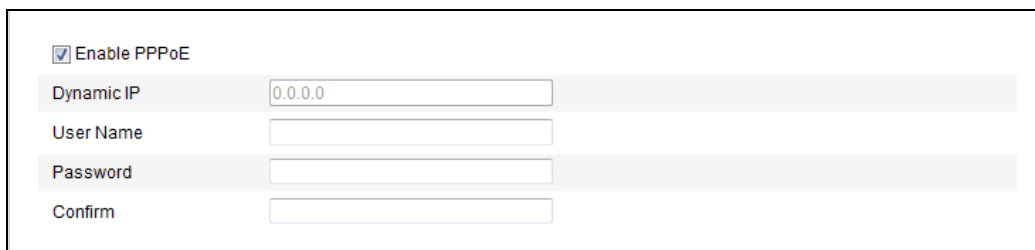
5.3.5 Configuring SNMP Settings

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. SNMP v2 requires password for access. 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 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 5-14 SNMP Settings

2. Check the corresponding version checkbox (**Enable SNMPv1**, **Enable SNMPv2c**, and **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.

5.3.6 Configuring 802.1X Settings

Purpose:

The IEEE 802.1X standard is supported by the network cameras. 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 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

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.

Figure 5-15 802.1X Settings

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

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

5.3.7 Configuring QoS Settings
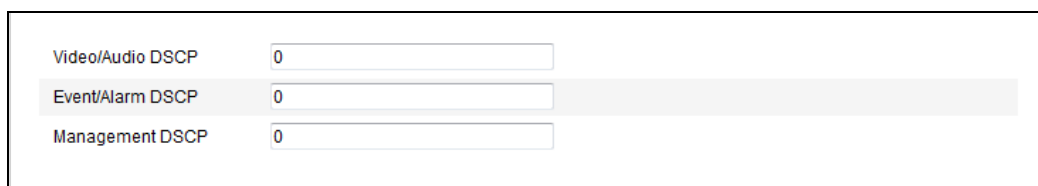
Purpose:

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

    | Video/Audio DSCP | 0 |
    | Event/Alarm DSCP | 0 |
    | Management DSCP | 0 |

    Figure 5-16 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.

5.3.8 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 at home and in 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 5-17 UPnP™ Settings

5.3.9 **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 5.3.1* *Configuring TCP/IP Settings* for detailed information.

2. Enter the Email Settings interface:

   Configuration > Advanced Configuration > Network > Email

Figure 5-18 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 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 3 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.

5.3.10 Configuring NAT (Network Address Translation) Settings

Purpose:

NAT refers to the port mapping when UPnP™ is enabled.

Steps:

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 5-19 Configure NAT Settings

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

5.3.11 Configuring FTP Settings

Purpose:

You can configure the related FTP server 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

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 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.*
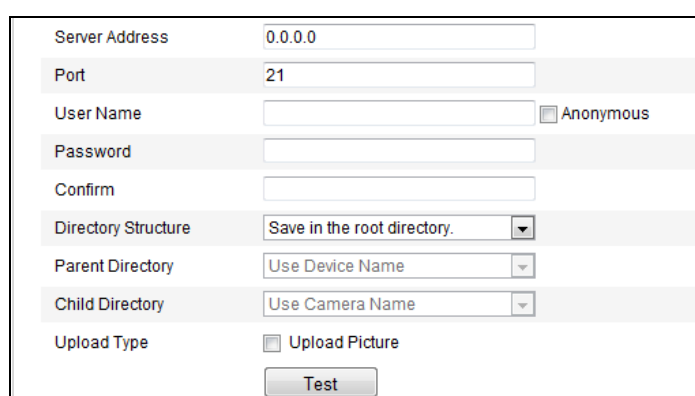
   Directory: In the **Directory Structure** field, you can select the root directory, parent directory and child directory. When the parent directory is selected, you

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.

Figure 5-20 FTP Settings

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 6.4.*

5.3.12 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

Figure 5-21 HTTPS Settings

2. Check the checkbox of Enable HTTPS to enable the function.

3. Create the self-signed certificate or authorized certificate.

   ● Create the self-signed certificate

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

Figure 5-22 Create Self-signed Certificate

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

Figure 5-23 Create a Certificate

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

Note: If you already have 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 5-24 Installed Certificate

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

5.4 Configuring Video and Audio Settings

5.4.1 Configuring Video Settings

Steps:

1. Enter the Video Settings interface:

   Configuration >Basic Configuration > Video/Audio > Video

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

Figure 5-25 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 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

51

audio signal can 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 256~16384 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, H.264, MJPEG, and MPEG4 are selectable.

Note: The video encoding type varies according to different camera platforms.

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.

5.4.2 Configuring Audio Settings

Steps:

1. Enter the Audio Settings interface

    Configuration > Basic Configuration > Video/Audio > Audio

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

Figure 5-26 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, AAC 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 out to some extent.

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

5.4.3 Configuring ROI Encoding

Purpose:

ROI (Region of Interest) encoding helps to discriminate between 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.

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 Region No. drop-down list for ROI settings. There are four fixed regions selectable.

5. Click the **Draw Area** button, 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.
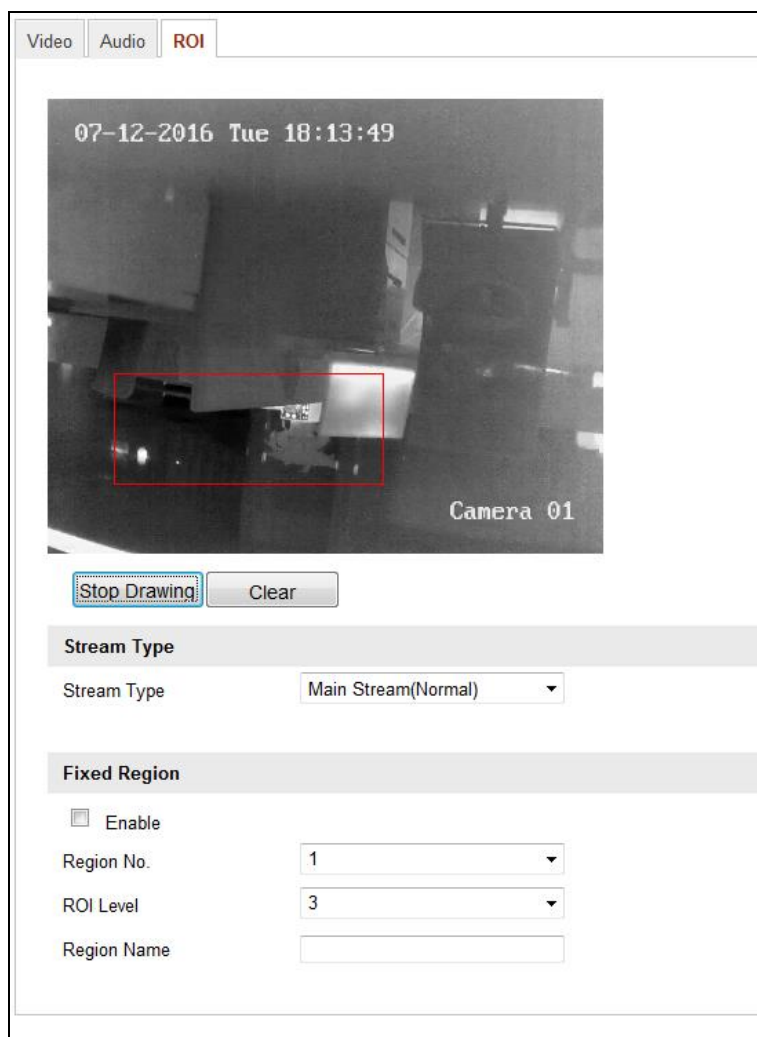
Figure 5-27 Region of Interest Settings

7. Input the region name for ROI as desired.

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

5.5 Configuring Image Parameters

5.5.1 Configuring Display Settings

Purpose:

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

Note: The display parameters vary according to the different camera models. 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.
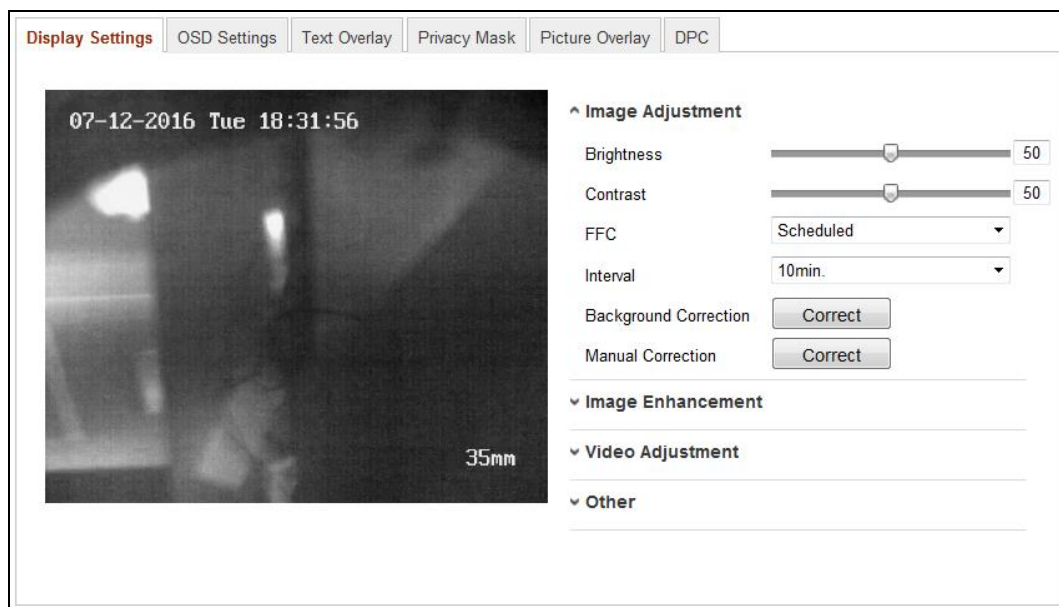
Figure 5-28 Configuring Display Settings for Camera 2

- **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.

  FFC (Flat Field Correction) improves the quality in digital imaging. It can remove artifacts from 2-D images that are caused by variations in the pixel-to-pixel sensitivity of the detector or by distortions in the optical path. Schedule, Temperature, and OFF are selectable.

  - **Schedule:** You can select the correction interval among 10, 20, 30, 40, 50, 60, 120, 180, and 240minutes.

  - **Temperature:** Camera adjusts the image according to the temperature.

  Manual Background Correction: Fully cover the lens with an object (lens

cover is recommended) and click the Manual Background Correction button, and then the camera adjusts the image according to the current environment.

Manual Shutter Correction: Click the Manual Shutter Correction button and then the camera adjusts the image according to the temperature of the camera itself.

- **Image Enhancement**

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

  Palettes: The palettes allow you to select the desired colors. white hot, black hot, fusion 1, rainbow, fusion 2, ironbow 1, ironbow 2, sepia, color 1, color 2, ice fire, rain, red hot, and green hot are selectable.

  DDE: The DDE (Digital Detail Enhancement) can adjust the details of the image. And you can set it to OFF or Normal mode. And DDE Level can be adjusted from 1 to 100 when in normal mode.

- **Video Adjustment**

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

  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.

  Digital Zoom: Select digital zoom as OFF, 2X, or 4X to display live view in original size, 2X size digital zoomed, or 4X size digital zoomed.

- **Other**

  Local Output: Turn on or off the local output of device.

3. (Optional) Click **Default** to restore the default settings

5.5.2 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
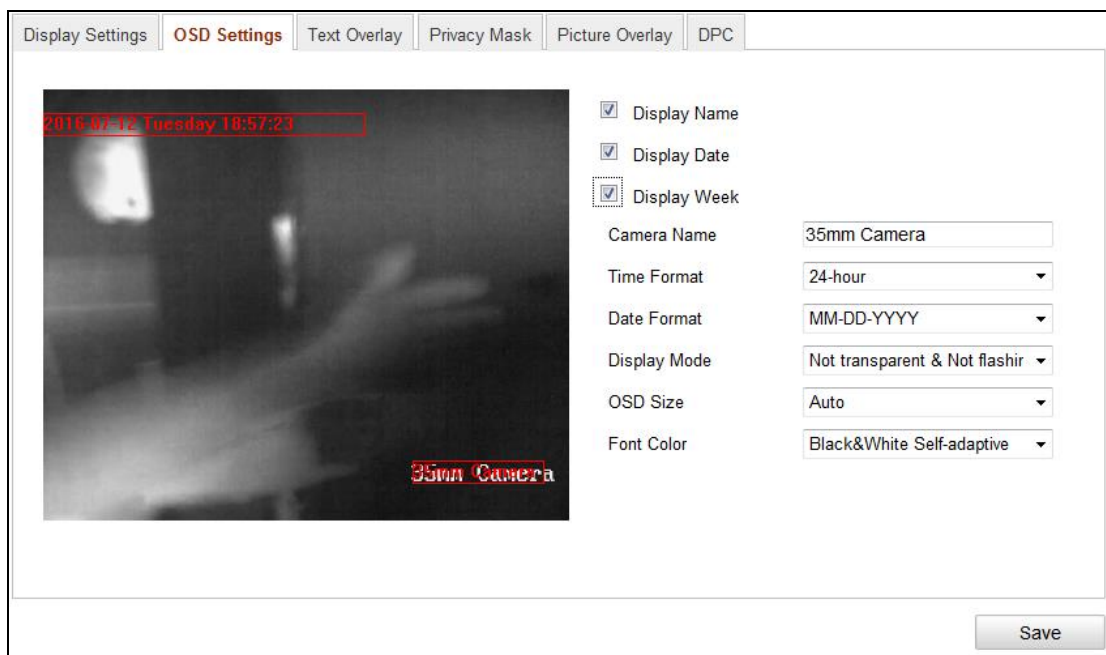
Figure 5-29 OSD Settings

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.
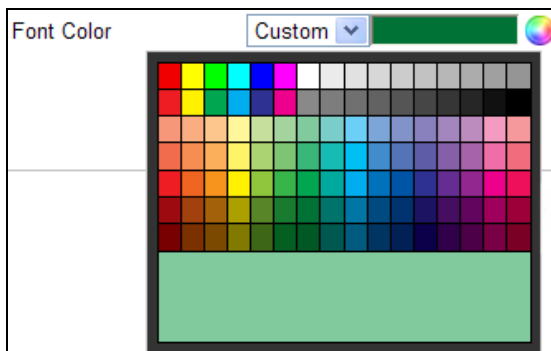
Figure 5-30 Font Color-Custom

6. You can use the mouse to click and drag the text frame 35mm Camera in the live view window to adjust the OSD position.
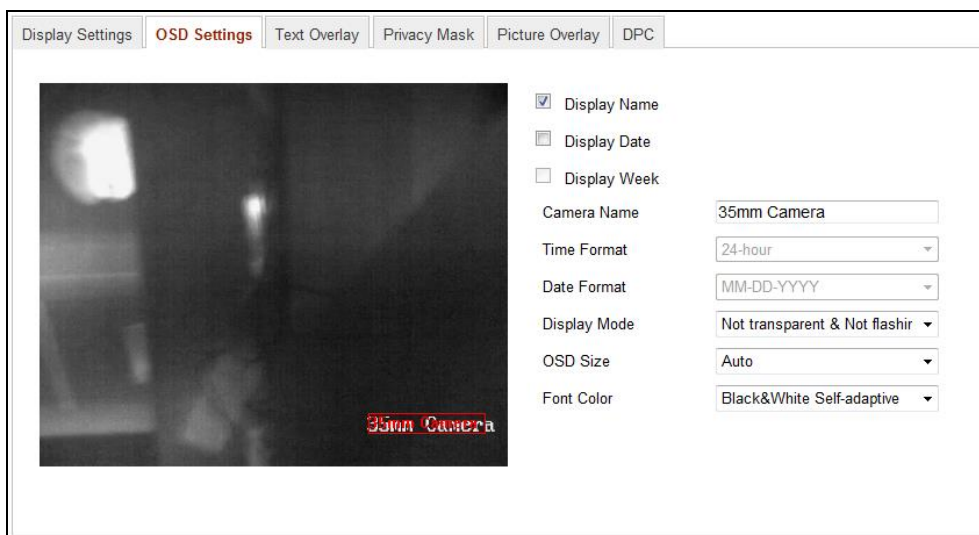
Figure 5-31 Adjusting OSD Location

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

5.5.3 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
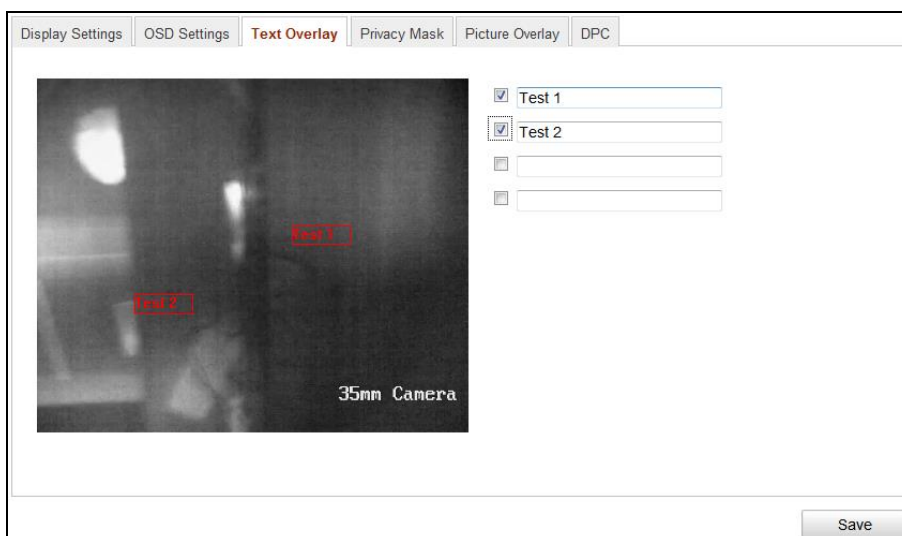
Figure 5-32 Text Overlay

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 `Test 1` 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.

5.5.4 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

Figure 5-33 Privacy Mask Settings

2. Check the checkbox of **Enable Privacy Mask** to enable this function.

3. Click **Draw Area**.

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.

5.5.5 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 5-34 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.

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

5.5.6 Configuring DPC (Defective Pixel Correction)

Purpose:

DPC (Defective Pixel Correction) refers to the function that the camera can correct

the defective pixels on the LCD which are not performing as expected.

Note: This function is only available to certain camera models.

Steps:

1. Enter the DPC Settings interface.

   Configuration > Advanced Configuration> Image > DPC

2. Click on the image to select the defective pixel. The cursor on the image will

   move to the clicked position. You can click   to slightly adjust the cursor

   position.

3. Click   to start correction.

Figure 5-35 Defective Pixel Correction

4. (Optional) Click ![icon] to cancel the correction.

5.6 Configuring and Handling Alarm Events

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

Notes:

● 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.

● Click ![icon] for help when you configure the intelligent functions, including face detection, audio exception detection, intrusion detection, defocus detection, scene change detection, etc. A help document will guide you to go through the configuration steps.

5.6.1 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 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 on the live video.

Note: To enable/disable marking the motion objects on the live video, go to Local Configuration> Live View Parameters and enable/disable the Rules.
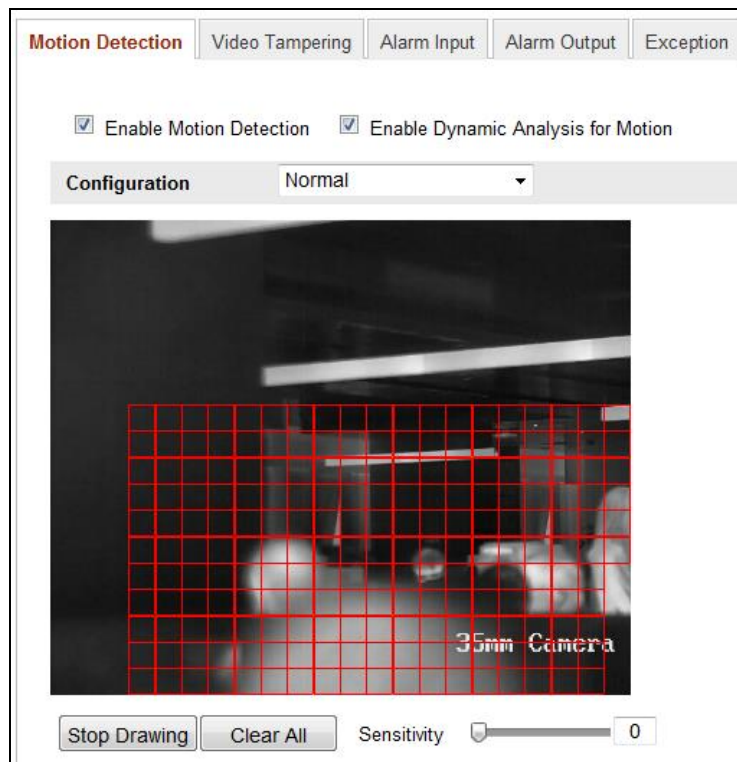
Figure 5-36 Enable Motion Detection

(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.

Task 2: Set the Arming Schedule for Motion Detection.

Steps:
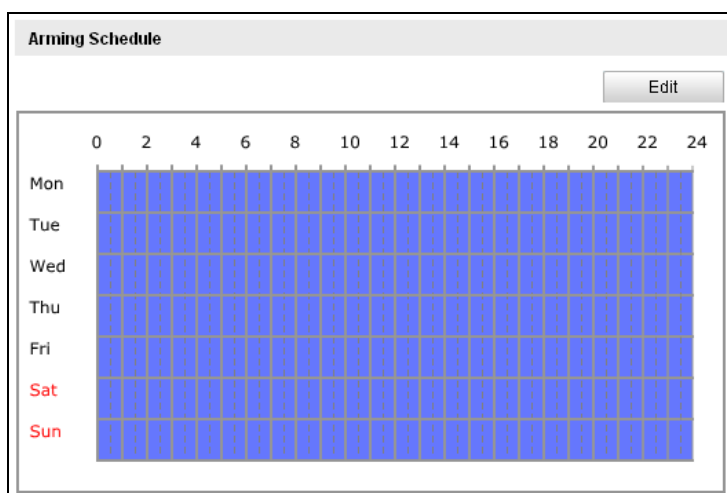
Figure 5-37 Arming Time

(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.
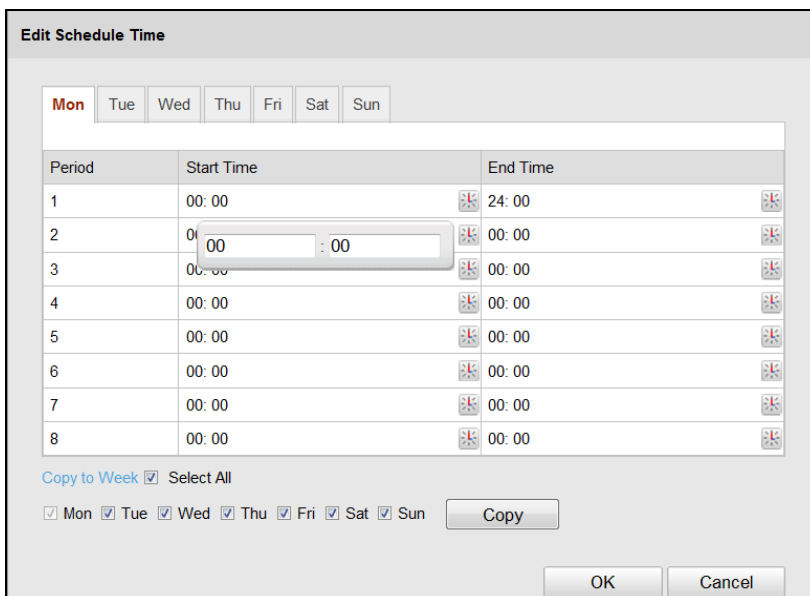
Figure 5-38 Arming Time Schedule

Task 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.
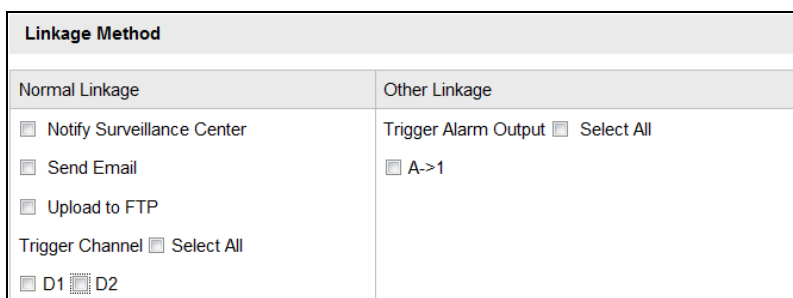
Figure 5-39 Linkage Method

● **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 5.3.9 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 5.3.11 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 6.3* 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 5.6.4 Configuring Alarm Output* to set the related parameters.

● **Expert Configuration**

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

Note: Day/night switch can't be realized for thermal camera channel. But Area, Sensitivity and Proportion of Object on Area are still configurable.
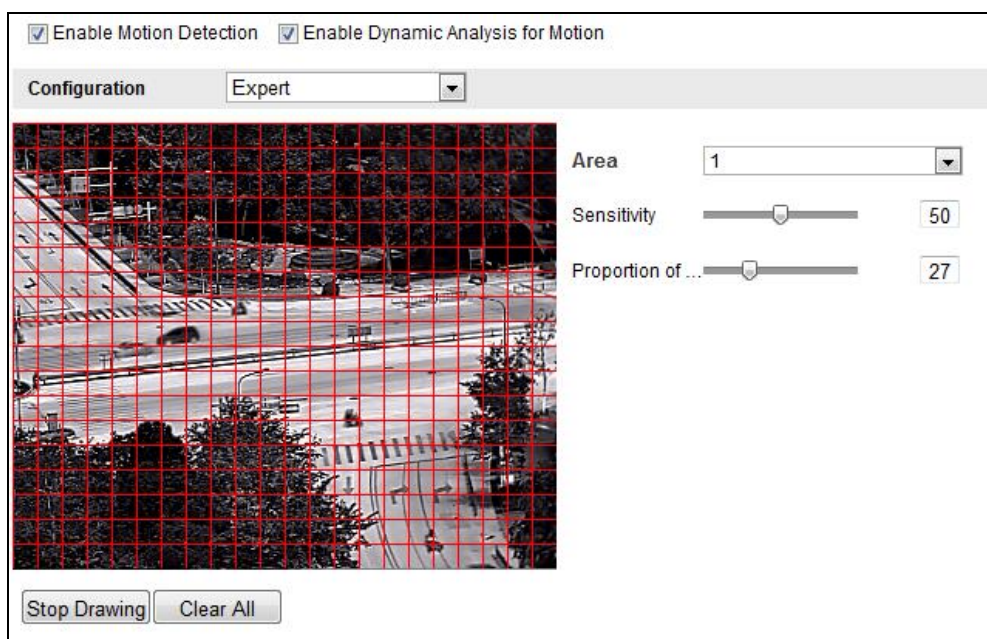
Figure 5-40 Expert Mode of Motion Detection

5.6.2 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
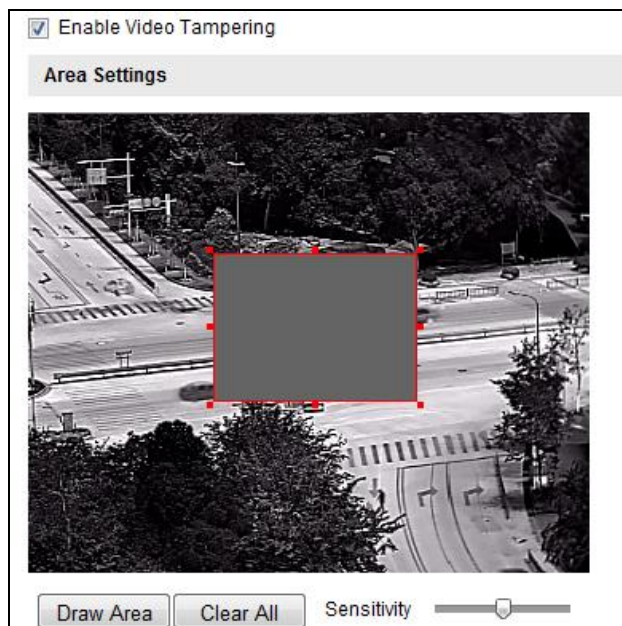
Figure 5-41 Video Tampering Alarm

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 5.6.1.*

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 5.6.1.*

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 5.6.1.*

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

5.6.3　Configuring Alarm Input

Purpose:

It detects the alarm input, and take response actions when the alarm is triggered.

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 5-42 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 5.6.1*.

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 5.6.1*.

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.

5.6.4 Configuring Alarm Output

Purpose:
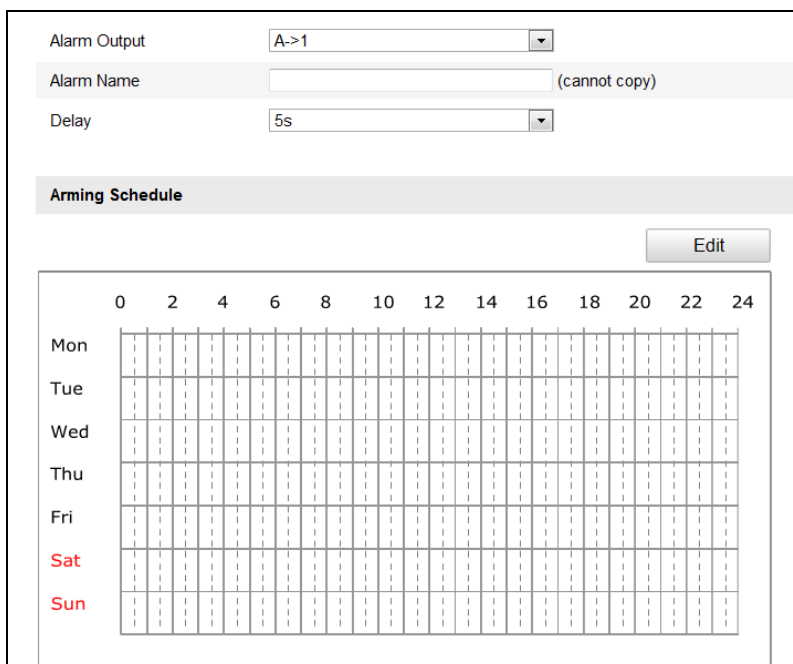
It detects the alarm output, and take response actions when the alarm is triggered.

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 5.6.1.*

5. You can copy the settings to other alarm outputs.

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

Figure 5-43 Alarm Output Settings

5.6.5 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 5.6.1*.

Exception Type	HDD Full	
Normal Linkage	**Other Linkage**	
☐ Notify Surveillance Center	☐ Trigger Alarm Output ☐ Select All	
☐ Send Email	☐ A->1	
		Save

Figure 5-44 Exception Settings

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

5.6.6 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.
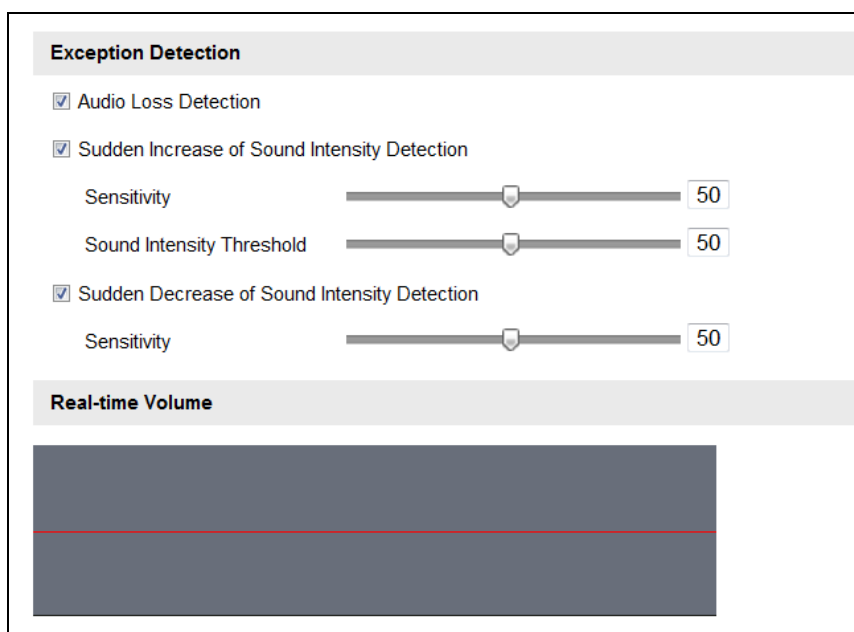
Figure 5-45 Configuring Audio Exception Detection

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. Refer to *Task 3 Set the Alarm Actions Taken for Motion Detection* in *Section 5.6.1*.

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

5.6.7 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.

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.

5.6.8 Configuring Dynamic Fire Source Detection

Purpose:

When you enable this function and fire source is detected, the alarm actions will be triggered.

Steps:

1. Enter the Dynamic Fire Source Detection setting interface:

    Configuration > Advanced Configuration> Smart Event> Dynamic Fire Source Detection

2. Check the checkbox of **Enable Dynamic Fire Source Detection** to enable the function.

Figure 5-46 Configuring Dynamic Fire Source Detection

3. Check the checkbox of **Display Fire Source Frame on Stream** to display a red frame around the fire source on stream when fire occurs. (Optional)

4. You can slide the cursor to adjust the sensitivity degree of dynamic fire source detection from 1to 10. The bigger the number is, the more sensitive the detecting would be.

5. Check the checkbox to select the linkage method taken for the alarm input. Please refer to *Task 3: Set the Alarm Actions for Motion Detection* in Section *Motion Detection*. In the field of Other Linkage, you can check the checkbox to enable the alarm output (The alarm output number varies depending on device ability).

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

5.7 Temperature Measurement

Purpose:

When you enable this function, it measures the actual temperature of the spot being monitored. The device alarms when temperature exceeds the temperature threshold value.

Before You Start:

Enter **Configuration > Advanced Configuration > System > VCA Resource Type** to select **Temperature Measurement + Behavior Analysis** as VCA Resource Type.

5.7.1 Temperature Measurement Configuration

Steps:

1. Enter **Configuration > Advanced Configuration > Temperature Measurement** Configuration.

Figure 5-47 Dynamic Fire Source Detection

2. Check the checkboxes of the interface to set the temperature measurement configurations.
   ● **Enable Temperature Measurement:** Check the checkbox to enable temperature measurement function.
   ● **Display Temperature Info. on Stream:** Check the checkbox to display temperature information in live view.
   ● **Add Original Data on Capture:** Check the checkbox to add original data on capture.
   ● **Add Original Data on Stream:** Check the checkbox to add original data on stream.
   ● **Data Refresh Interval:** Select the data refresh interval from 1s to 5s.
   ● **Unit:** Display temperature with Degree Celsius (°C)/Degree Fahrenheit (°F)/Degree Kelvin (K）.
   ● **Temperature Range:** Set the temperature range.
3. Clcik **Save** to save the settings .

5.7.2 Temperature Measurement and Alarm

Purpose:

This function is used for measuring the temperature of detected spot and the device compares temperature of selected regions and alarms.

Steps:

1. Enter **Configuration > Advanced Configuration > Temperature Measurement and Alarm**.

2. Set the alarm rule: Select a temperature measurement rule from the rule list and configure the parameters.
   ● **Name:** You can customize the rule name.
   ● **Type:** Select point, line, or frame as rule type.
   ● **Emissivity:** Set the emissivity of your target. Note: The emissivity of each object is different.
   ● **Distance (m):** The straight-line distance between the target and the device.
   ● **Reflective Temperature:** If there is any target with high emissivity in the scene, check the checkbox and set the reflective temperature to correct the temperature. If no such target exists, uncheck the checkbox.
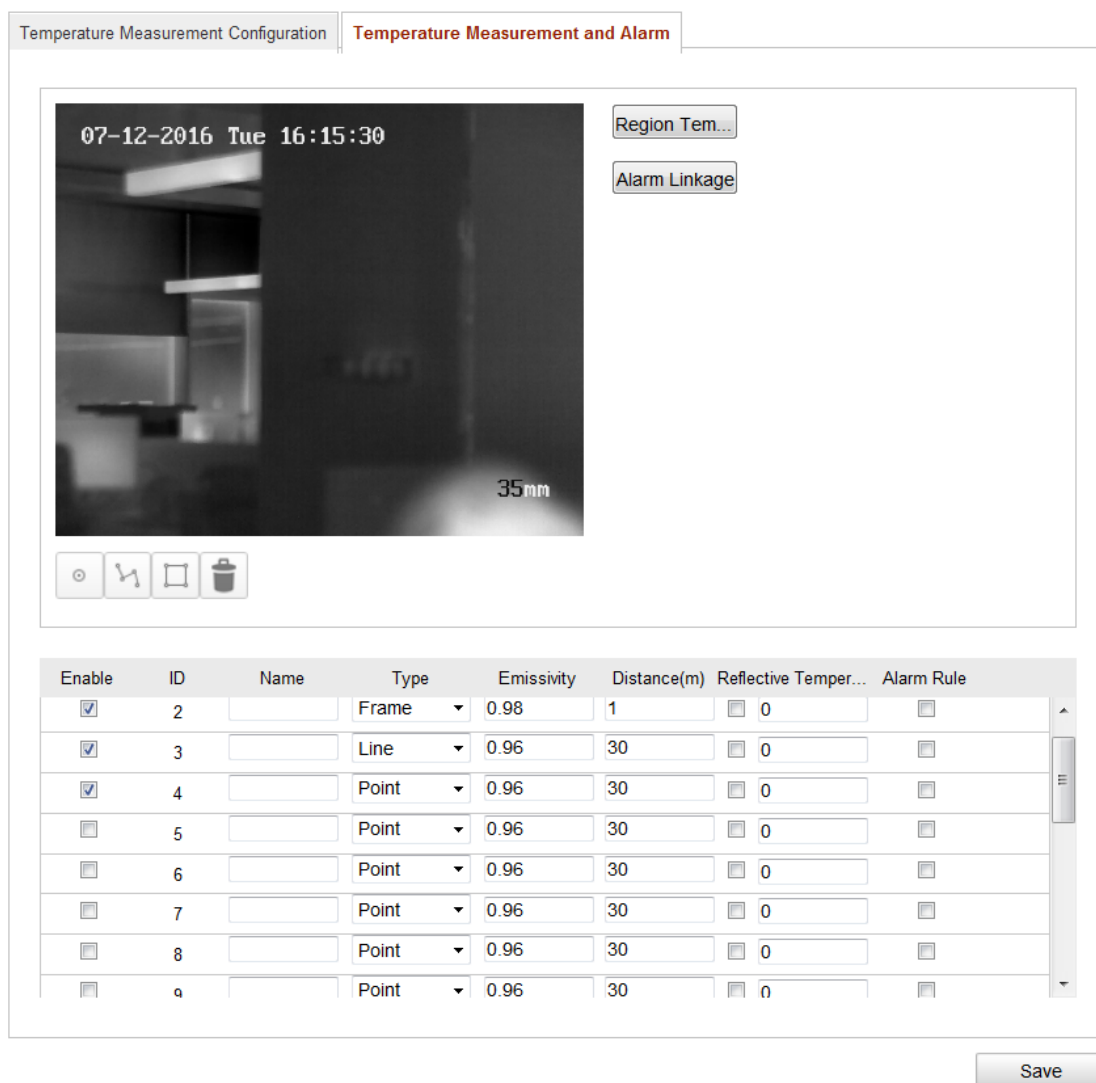
Figure 5-48 Temperature Measurement Configuration

3. Click [pencil icon] in the list to show the alarm rule interface.

   ● **Alarm Rule:** The alarm rule varies according to different types. The rule is to compare the temperature information of two selected regions. For targets set by frame, the rules include: **Max. Temperature is Higher than**, **Max. Temperature is Lower than**, **Min. Temperature is Higher than**, **Min.**

Temperature is Lower than, **Average Temperature is Higher than**, **Average Temperature is Lower than**, **Temperature Difference is Higher than**, and **Temperature Difference is Lower than**. For targets set by line, the rules include Max. Temperature, Min. Temperature, and Average Temperature. For targets set by point, the rules are distinguished by Average Temperature.

● **Pre-Alarm Temperature and Alarm Temperature:** Set the pre-alarm temperature and alarm temperature, the device sends pre-alarm when its rule temperature exceeds pre-alarm temperature and sends alarm when its rule temperature exceeds alarm temperature.

● **Tolerance Temperature:** Set the tolerance temperature and the device judges whether the triggered alarm stops until the device temperature/temperature difference is lower than rule temperature by tolerance temperature. For example, set tolerance temperature as 3°C, set alarm temperature as 55°C, and set pre-alarm temperature as 50°C. The device sends pre-alarm when its temperature reaches 50°C and it alarms when its temperature reaches 55°C and only when the device temperature is lower than 52°C will the alarm be cancelled.

4. Draw the Target Region: Select the rule and draw the corresponding frame/line/point. Click to draw the point. Click to draw the line. Click to draw the frame.

5. Set Temperature Difference Alarm: Click Temperature Difference Alarm to enter the temperature difference alarm interface, up to four temperature difference alarms can be set.

NOTE

Temperature Difference Alarm only applies to the targets set by frame.

6. Set Alarm Linkage: Click Alarm Linkage to enter the alarm linkage interface and set the linkage methods.

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

5.8 VCA Configuration

5.8.3 VCA Resource Type

Before using the VCA rules of the camera, you should select the VCA resource type first.

To use Temperature Measurement and Behavior Analysis, select **Temperature Measurement and Behavior Analysis**. To use Dynamic Fire Source Detection function, select **Dynamic Fire Source Detection**. Once you selected any of the

resources, the other VCA rule cannot be enabled.

5.8.4 VCA Information

● **Behavior Analysis Version:**

It lists the version of the algorithms library.

● **Display information**

It includes the display on picture and display on stream. Check the checkboxes to enable corresponding displays.

Figure 5-49 VCA Information

● **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:** 384*288, CIF, 4CIF, 720P, and 1080P are selectable.

  Note: Selectable picture resolution options vary according to different camera models.

5.8.5 Behavior Analysis

Purpose:

The behavior analysis detects a series of suspicious behavior, and certain linkage methods will be enabled if the alarm is triggered. Refer to the following steps to configure behavior analysis settings.

Steps:

1. Configure the display information and snapshot settings from the **VCA Info.** page.

2. Set the **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) Enter the Camera Calibration setting interface:

      Configuration > VCA Configuration > Camera Calibration

   2) Check the checkbox of **Camera Calibration** to enable this function.

   3) 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.

4) (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.

5) You can click **Delete** to delete the drawn lines.

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

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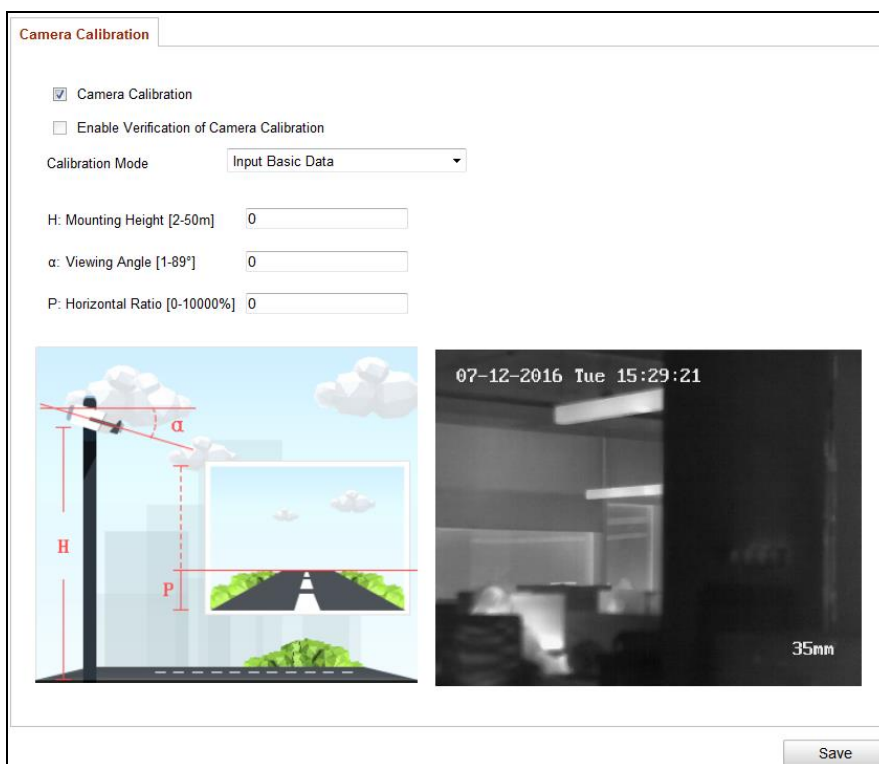

Figure 5-50 Input Basic Data
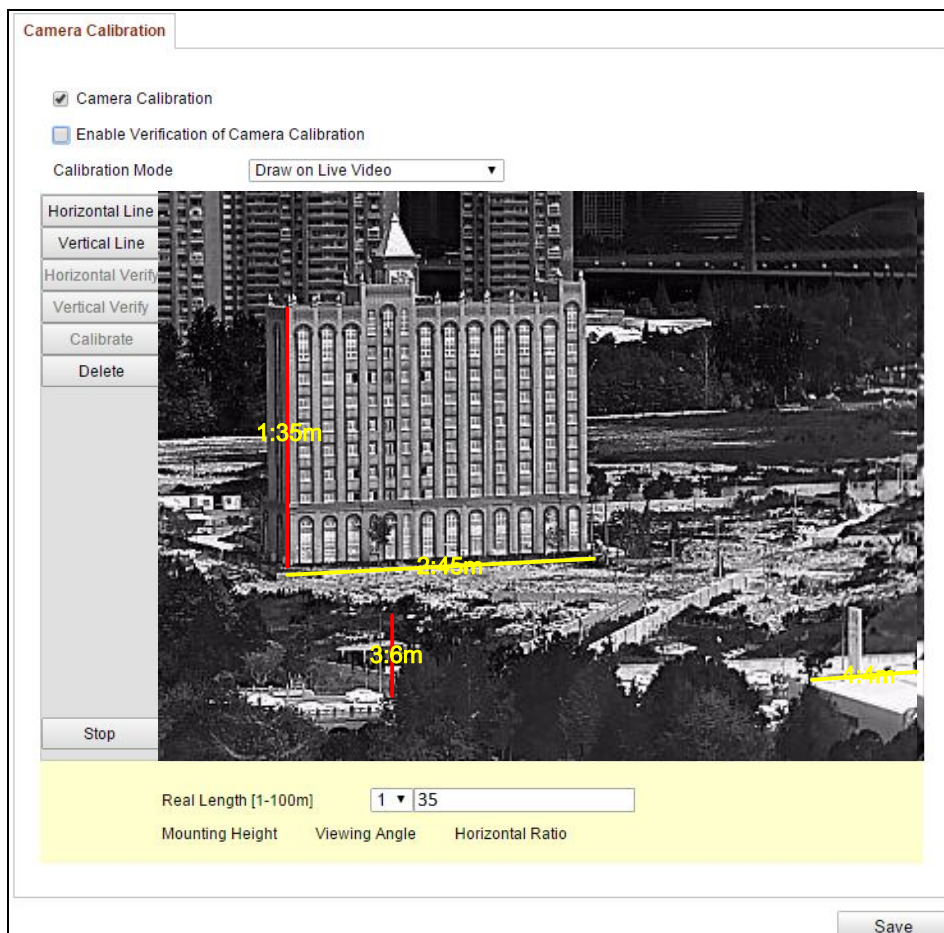
Figure 5-51 Draw on Live View Window

3. Draw the **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) Enter the Shield Region setting interface:

   Configuration > VCA Configuration > Shield Region

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.

4. Configure the **Rule**

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

Note: The rule type for setting varies according to different camera models.

Steps:

1) Click **Rule** Tab to enter the rule configuration interface.

2) Click to add a new rule. (Optional) Click to delete it.

3) Check the checkbox of the desired rule to enable the rule for behavior analysis.

4) Select the rule type, set the filter type, and then draw the line/area on the live video for the single rule.

- **Line Crossing** 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.

  When you select this rule type, you have to select the crossing direction before drawing a line. Bidirectional, A-to-B, and B-to-A are selectable.

- **Intrusion** 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.

  When you select this rule type, you have to set the duration time for intrusion. Available duration range is from 1s to 100s.
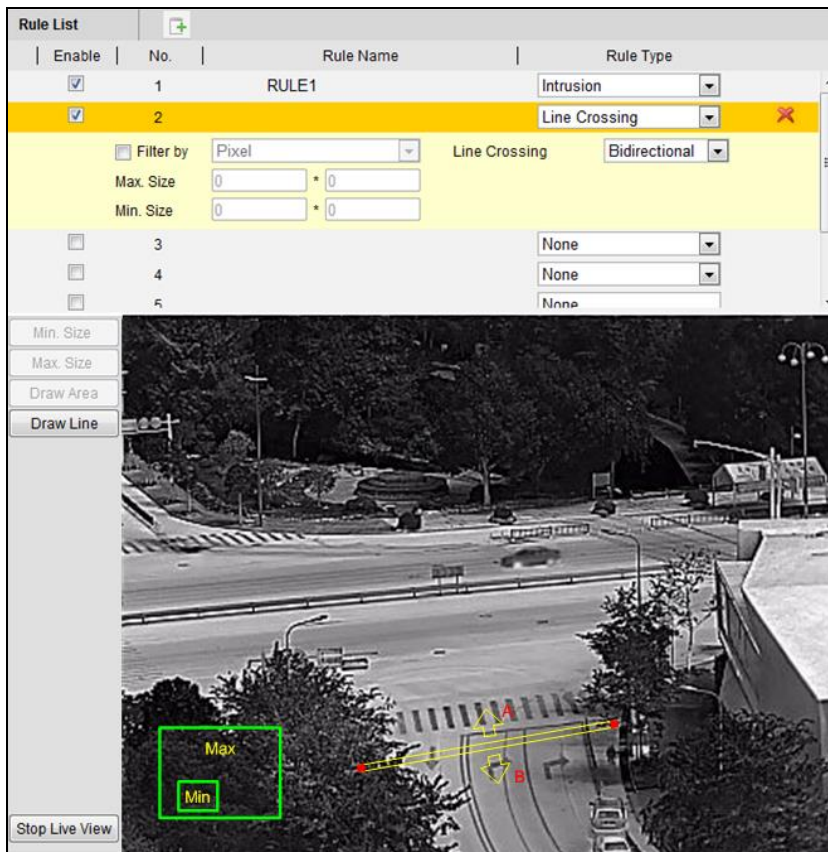
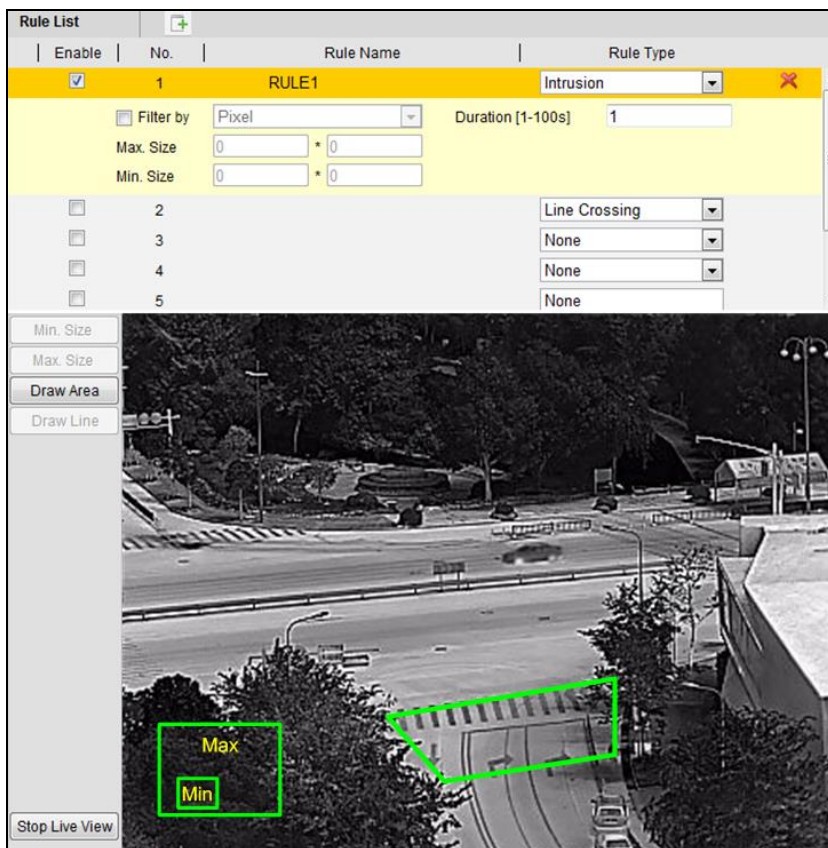Figure 5-52 Rule Type-Line Crossing

Figure 5-53 Rule Type-Intrusion

- **Region Entrance** 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.

- **Region Exiting** 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.
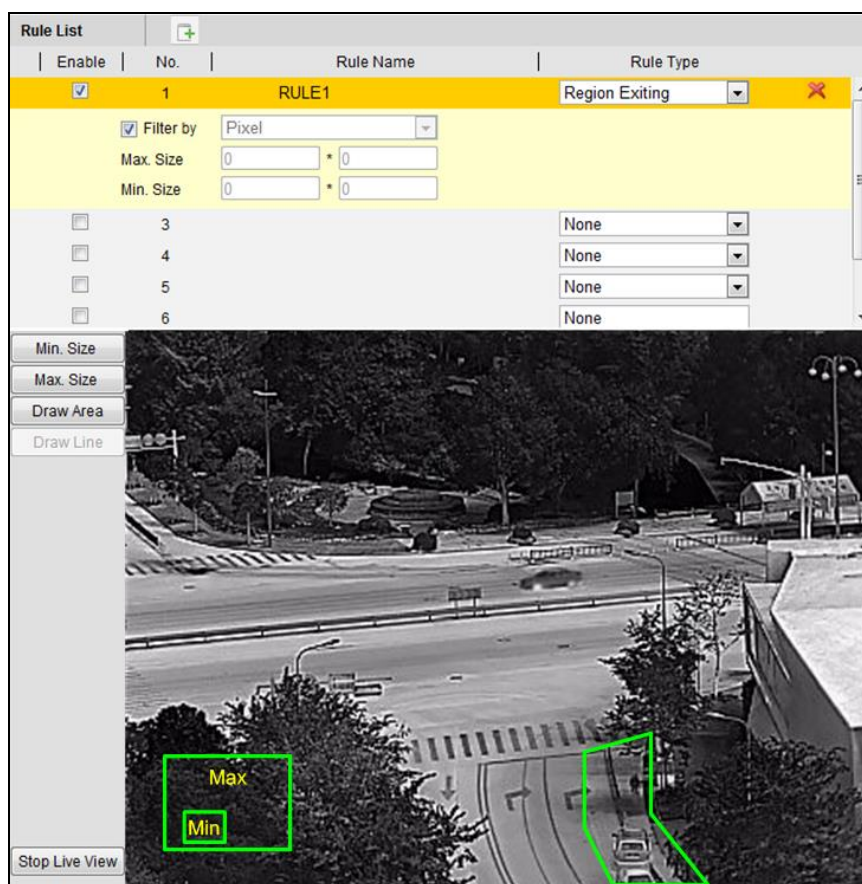
Figure 5-54 Rule Type-Region Exiting

- **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.

- **Draw line/area:** 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.

5) Check the checkbox of the combined rule to enable the rule for behavior analysis.

6) 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.

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

8) Click **Arming Schedule** tab, click **Edit** to set the schedule time for each rule, and click **Save** to save the settings.

9) Click **Alarm Linkage** tab, check the checkbox of corresponding linkage method for each rule, and click **Save** to save the settings.

5. Set the **Advanced Configuration**

● **Parameter**

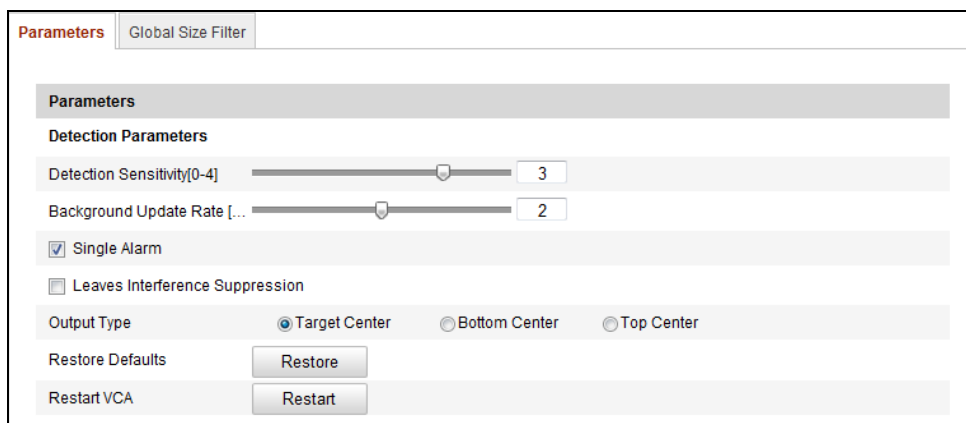Configure the following parameters to detail the configuration.

Figure 5-55 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 2 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 aiming 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

Chapter 6Storage 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.

6.1 Storage Management

Storage management allows you to view the HDD status, including the capacity, free space, status, type, and progress, etc. You can also format the HDD if it is required. Besides, you can assign the quota for pictures and record files.

Note: Before you can manage HDD devices, they have to be added first. Insert the SD card or refer to the next section to add HDD devices.
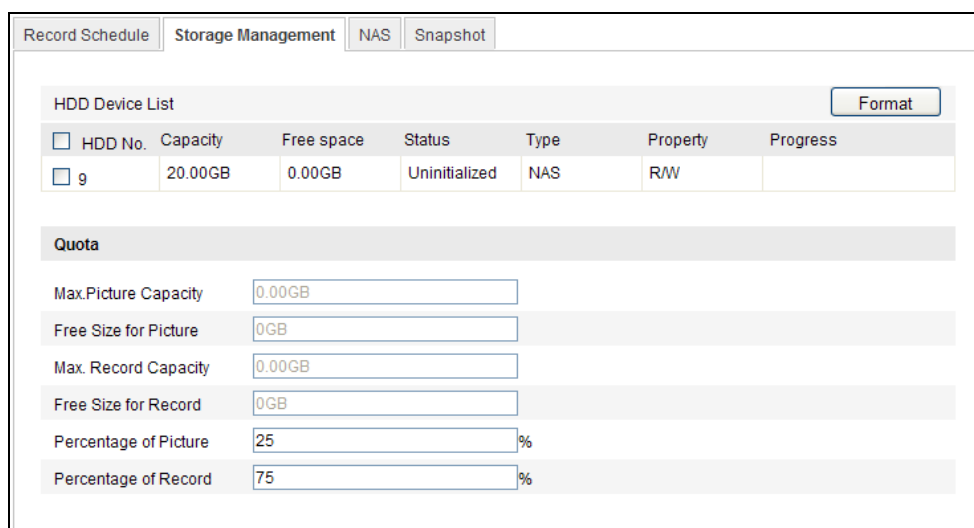

Figure 6-1 Storage Management Interface

6.2 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 6-2 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 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

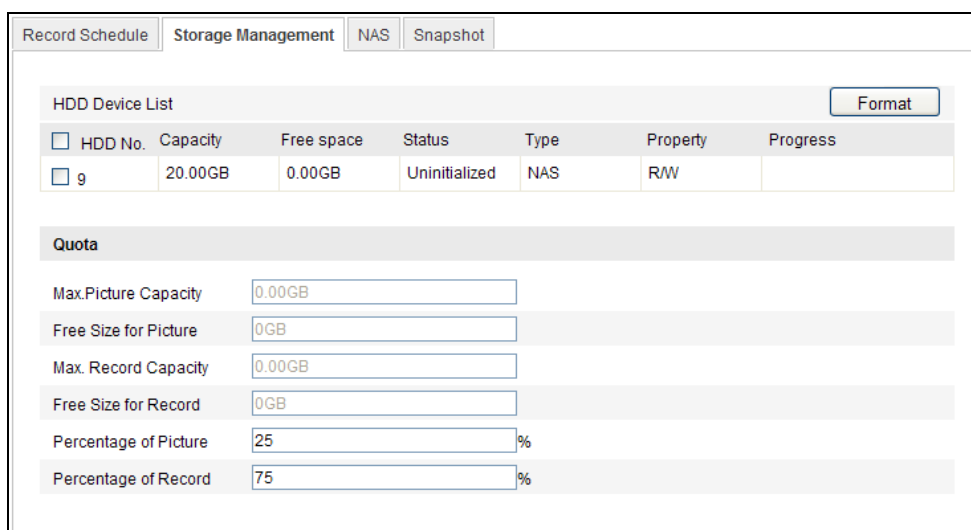**Advanced Configuration > Storage > Storage Management**

Figure 6-3 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.**
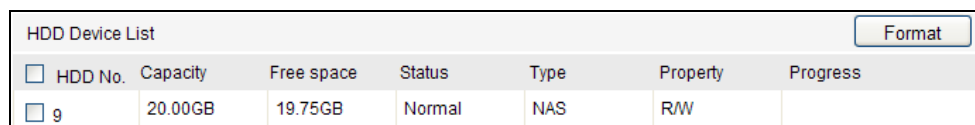

Figure 6-4 View Disk Status

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.
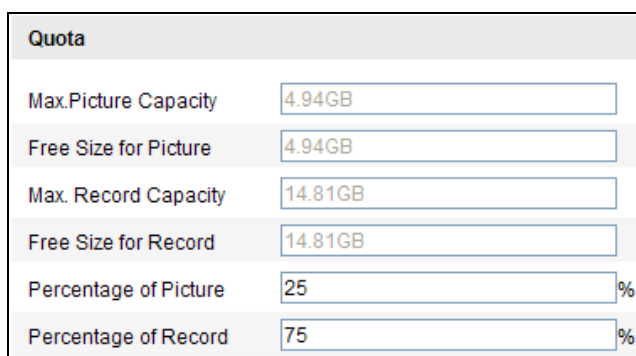

Figure 6-5 Quota Settings

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.

6.3 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 4.3 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:

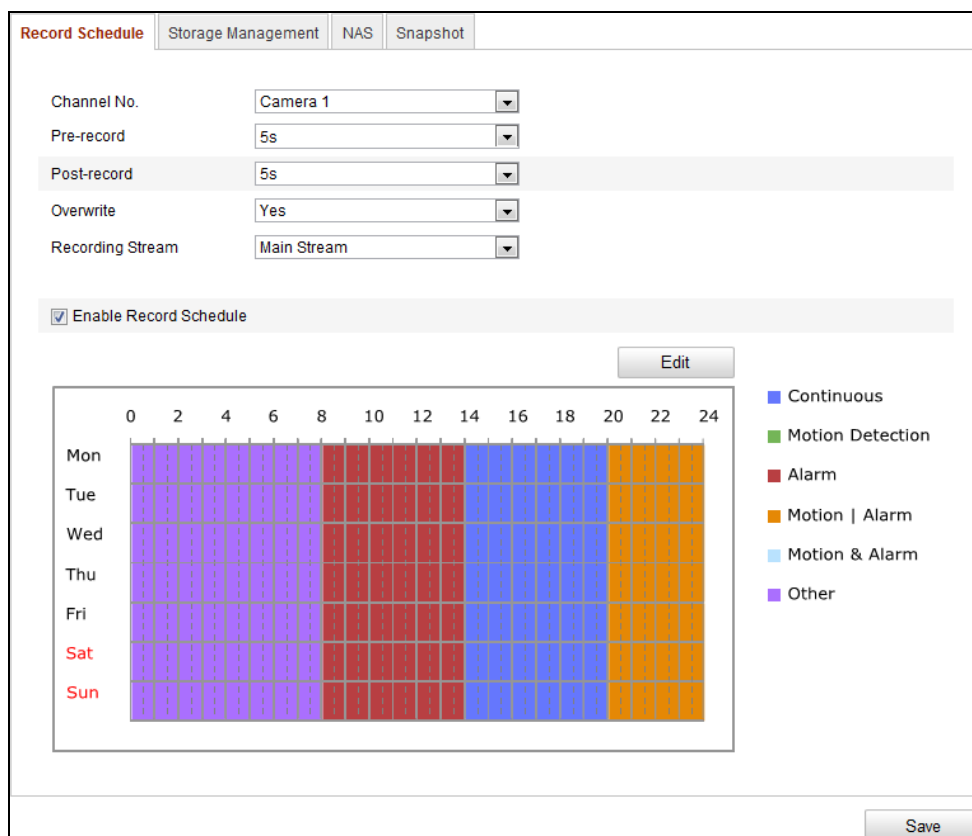   **Configuration > Advanced Configuration> Storage > Record Schedule**

Figure 6-6 Recording Schedule Interface

2. Check the checkbox of **Enable Record Schedule** to enable scheduled recording.

3. Set the record parameters of the camera.

Figure 6-7 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.

● Recording Stream: Main Stream and Sub Stream are selectable. 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.

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

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

Figure 6-8 Edit 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 periods, check the **Custom** checkbox. Set the **Start Time** and **End Time.**

Note: The time of each segment can't be overlapped. Up to 8 segments can be configured.

(2) Select a **Record Type**.

The record type can be Continuous, Motion Detection, Alarm, Motion | Alarm, Motion & Alarm, Audio Exception Detection, VCA Recording, Fire Source Detection, and All Events.

● **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 *Task 1: Set the Motion Detection Area in the Section 5.6.1*.

● **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 5.6.3*.

● **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 5.6.1* and *Section 5.6.3* 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 5.6.1* and *Section 5.6.3* for detailed information.

● **Record Triggered by Audio Exception Detection**

If you select **Audio Exception Detection**, the video will be recorded when abnormal sounds in the surveillance scene such as the sudden

increase/decrease of the sound intensity are detected.

Besides configuring the recording schedule, you have to configure the settings on the **Audio Exception Detection** interface. Refer to *Section 5.6.6* for detailed information.

- **Record Triggered by VCA Recording**

  If you select **VCA Recording**, the video will be recorded when the VCA detects series of suspicious behaviors, such as line crossing, intrusion, region entrance and region exiting.

  Besides configuring the recording schedule, you have to configure the Rule setting on VCA Configuration interface. Refer to *Section 5.7.2* for detailed information.

- **Record Triggered by Fire Source Detection**

  If you select **Fire Source Detection**, the video will be recorded when fire source is detected.

  Besides configuring the recording schedule, you have to configure the settings on the **Dynamic Fire Source Detection** interface. Refer to *Section 5.6.7* for detailed information.

- **Record Triggered by All Events**

  If you select **All Events**, the video will be recorded when any of the above-mentioned events happens.

  Besides configuring the recording schedule, you have to configure the settings on corresponding event interfaces.

(3) (Optional) 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.

6.4 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 NAS (For detailed information, please refer to *Section 6.2 Configuring NAS Settings*). You can also upload the captured pictures to a FTP server.

Basic Settings

Steps:

1. Enter the Snapshot Settings interface:
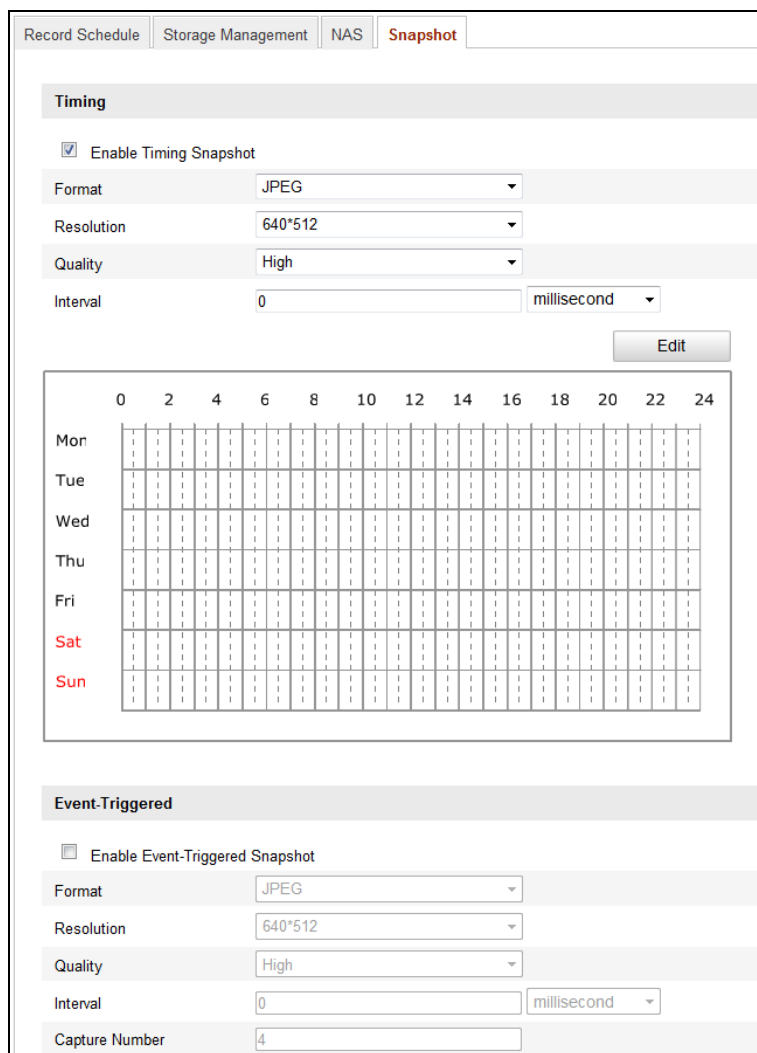
   Configuration > Advanced Configuration > Storage > Snapshot

Figure 6-9 Snapshot Setting Interface

2. Select a channel number. For camera models which have more than one camera channels, you should first select the channel number to configure.

3. Check the **Enable Timing Snapshot** checkbox to enable continuous snapshot. Edit schedule time for snapshots. For detailed setting procedures, refer to ***Section 6.3 Configuring Recording Schedule.***

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

5. Select the format, resolution, and quality of the snapshot.

6. Set the time interval between two snapshots.

7. 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 5.3.12* ***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 5.3.12* ***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 ***Task 3: Set the Alarm Actions Taken for Motion Detection*** in *Section 5.6.1,*

3) Check the **Enable Event-triggered Snapshot** checkbox.

Chapter 7Playback

Purpose:

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

Steps:

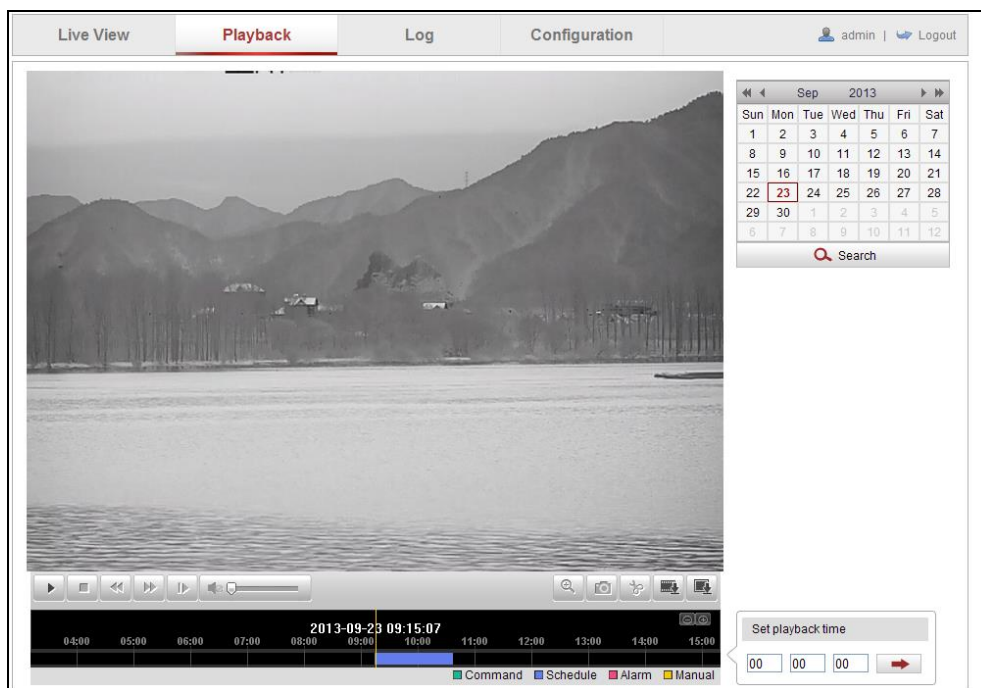1. Click **Playback** on the menu bar to enter playback interface.

Figure 7-1 Playback Interface

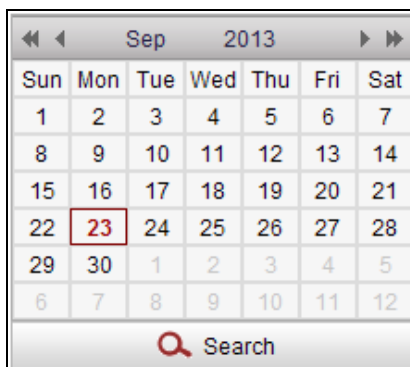2. Select a date and click **Search** to search record files.

Figure 7-2 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 7-3 Playback Toolbar

Table 7-1 Description of the buttons

Icon	Description	Icon	Description
▶	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 5.1* for details.

4. 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.
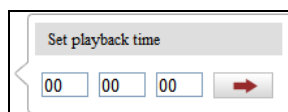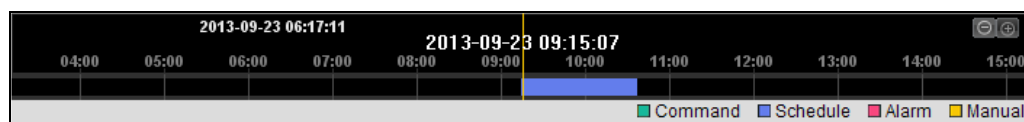

Figure 7-4 Set Playback Time

Figure 7-5 Progress Bar

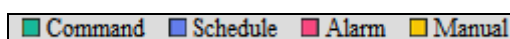The different colors of the video on the progress bar stand for the different video types.

Figure 7-6 Video Types

Chapter 8 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 make sure the network storage for the camera is configured, or the local storage (SD card) is working.

Steps:

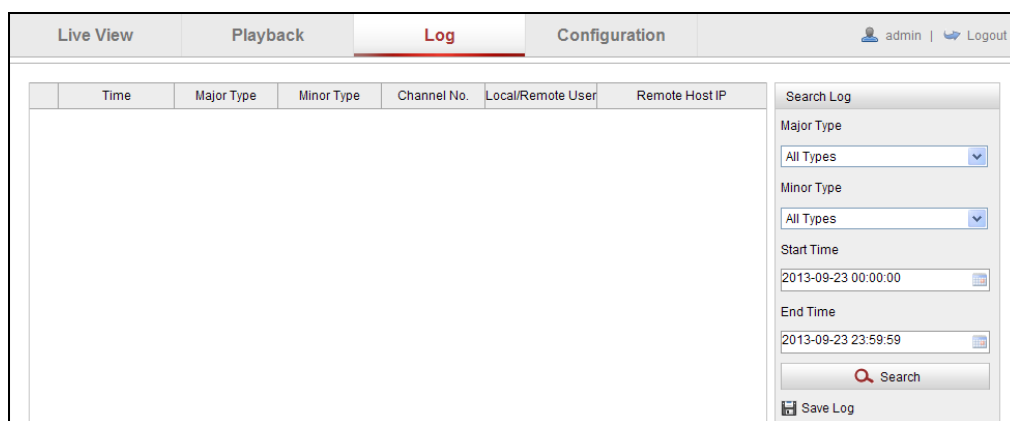1. Click **Log** on the menu bar to enter log searching interface.

Figure 8-1 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.
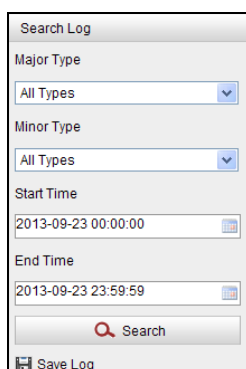

Figure 8-2 Log Searching

4. To export the log files, click **Save log** to save the log files in your computer.
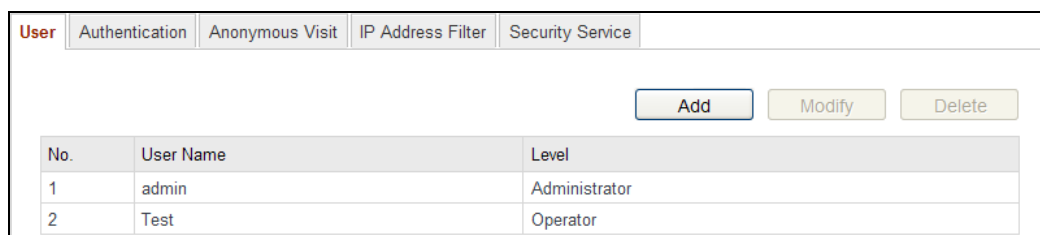
Chapter 9 Others

9.1 Managing User Accounts

Purpose:

The admin user can add, delete or modify user accounts, and grant them different permissions. We highly recommend user manage the device accounts and user permissions properly.

Enter the User Management interface to complete settings: **Configuration >Basic Configuration> Security > User** or **Configuration > Advanced Configuration> Security > User**

Figure 9-1 User Information

● **Adding a User**

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

Note: 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 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 9-2 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 9-3 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.

9.2 Authentication

Purpose:

You can specifically secure the stream data of live view.

Steps:

1. Enter the Authentication interface:

   Configuration> Advanced Configuration> Security > Authentication

Figure 9-4 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.

9.3 Anonymous Visit

Enabling this function allows visit from visitors who don't have the user name or password of the device.

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

Steps:

1. Enter the Anonymous Visit interface:

    Configuration> Advanced Configuration> Security > Anonymous Visit
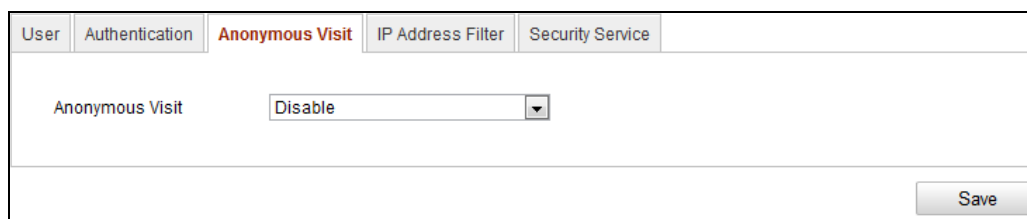
Figure 9-5 Anonymous Visit

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 9-6 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.

9.4 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 9-7 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.
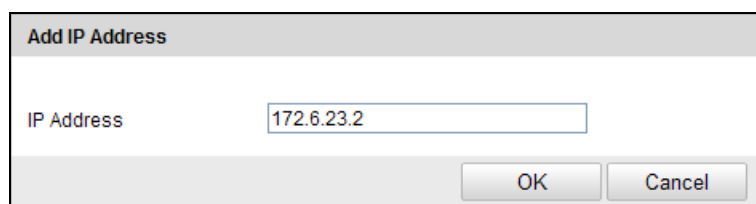
    (2) Input the IP Adreess.

Figure 9-8 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**.

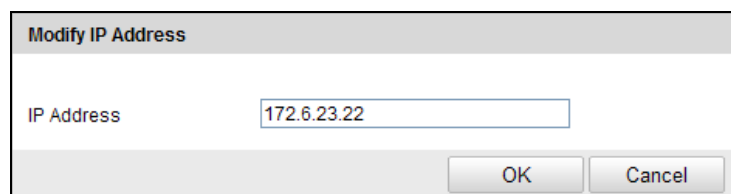   (2) Modify the IP address in the text filed.

Figure 9-9 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.

9.5 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. Enter the security service configuration interface:

    Configuration > **Advanced configuration** > **Security** >**Security Service**

Figure 9-10 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 device will be locked if you input the incorrect user name or password for 5 continuous times.

    Note: If the device is locked, you can try to login the device after 30 minutes, or reboot the device first before retry.

9.6 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 9-11 Device Information

9.7   Maintenance

9.7.1   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 9-12 Reboot the Device

9.7.2   Restoring Default Settings

Steps:

1.   Enter the Maintenance interface:

Configuration > Basic Configuration> System > Maintenance

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

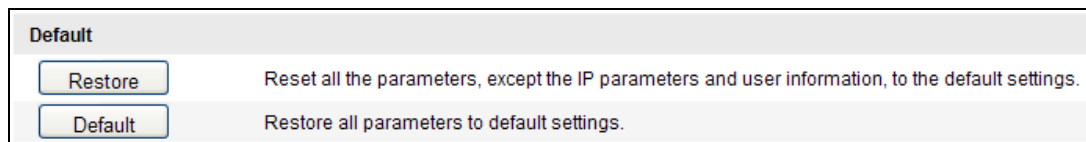2. Click **Restore** or **Default** to restore the default settings.

Default	
Restore	Reset all the parameters, except the IP parameters and user information, to the default settings.
Default	Restore all parameters to default settings.

Figure 9-13 Restore Default Settings

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

9.7.3 Exporting/Importing Configuration File

Purpose:

Configuration file is used for the batch configuration for cameras, 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**.**
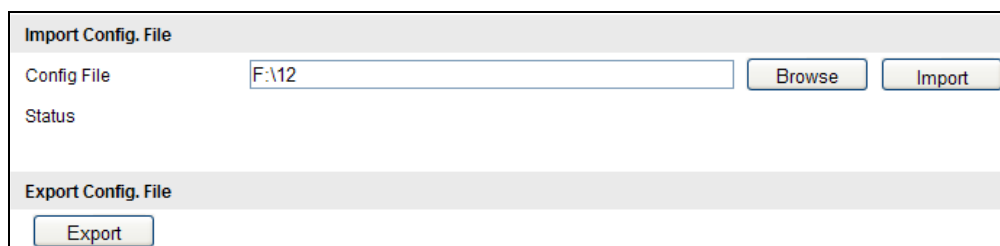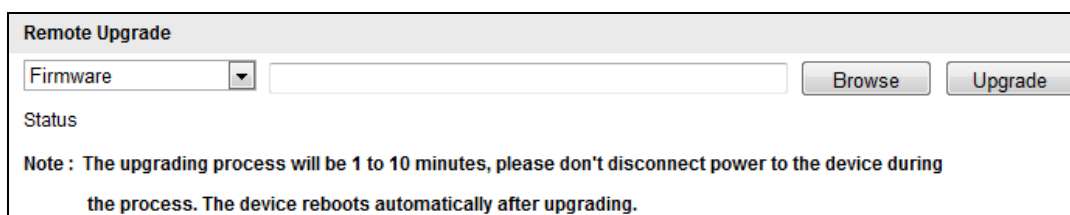
Import Config. File			
Config File	F:\12	Browse	Import
Status			
Export Config. File			
Export			

Figure 9-14 Import/Export Configuration File

9.7.4 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 9-15 Remote Upgrade

Note: The upgrading process will take 1 to 10 minutes. Please don't disconnect power to the device during the process. The device reboots automatically after upgrade.

9.8 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 9-16 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 are None.

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

9.9   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.

For the camera support de-icing heater, you can check the checkbox to enable automatic de-icing.

Note: The de-icing heater is only supported under POE+, 24VAC, or 12VDC power supply. Only 802.3at standard power supply is supported for De-icing heater, 802.3af standard power is not supported for the De-icing heater.

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.
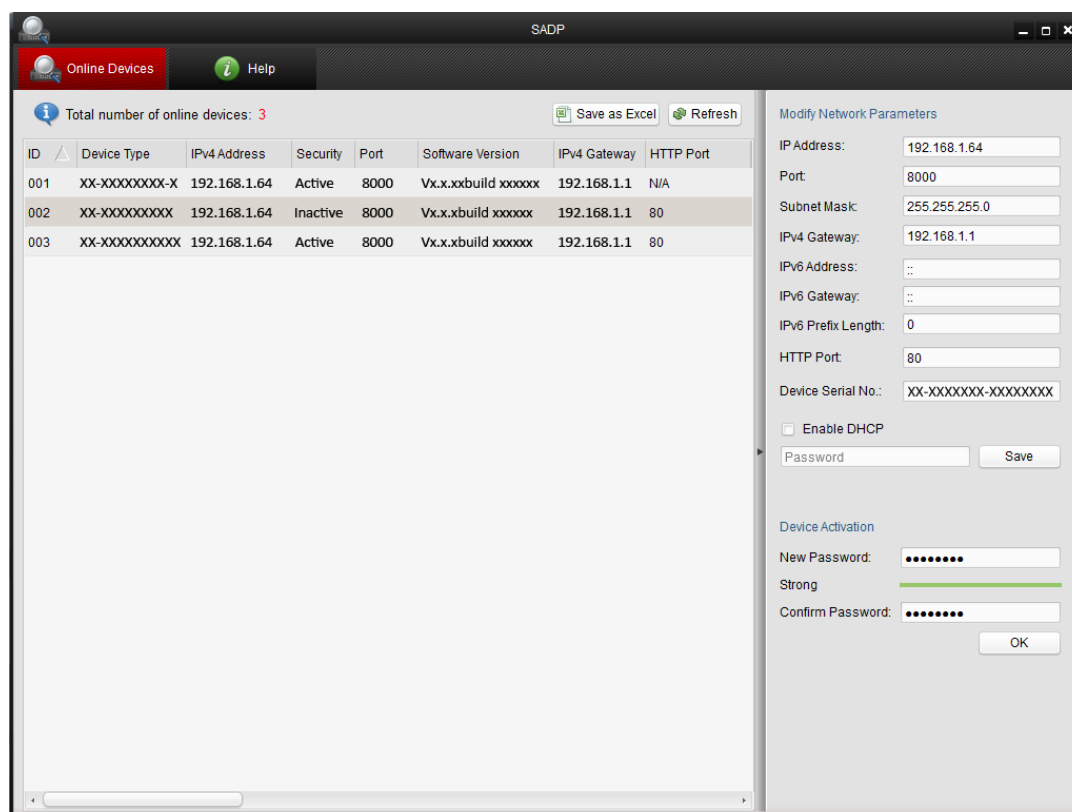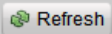
Figure A.1.1 Searching Online Devices

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.
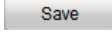
◆ **Search online devices manually**

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.

![warning triangle]

- *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 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.*

114

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:

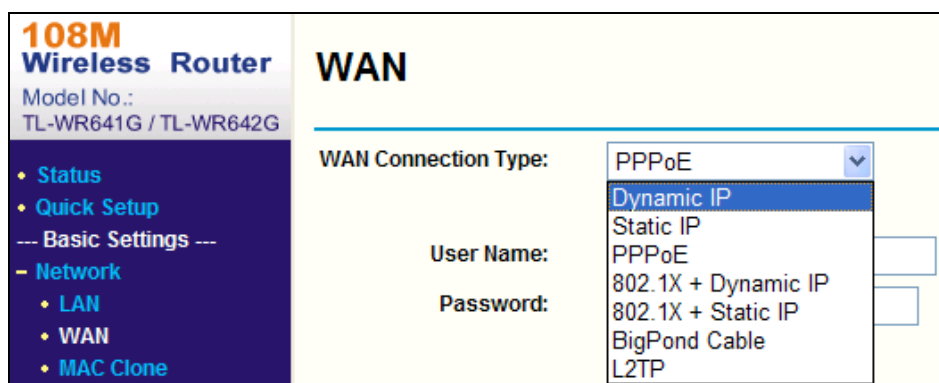1. Select the **WAN Connection Type**, as shown below:

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.
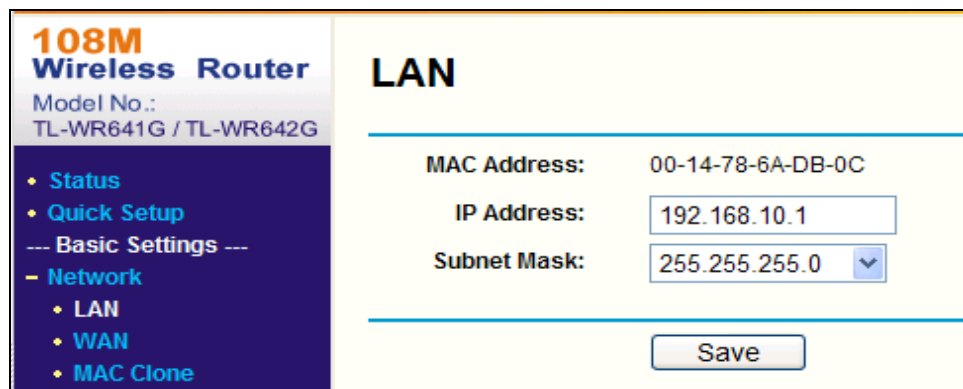

Figure A.2.2 Set the LAN parameters

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.

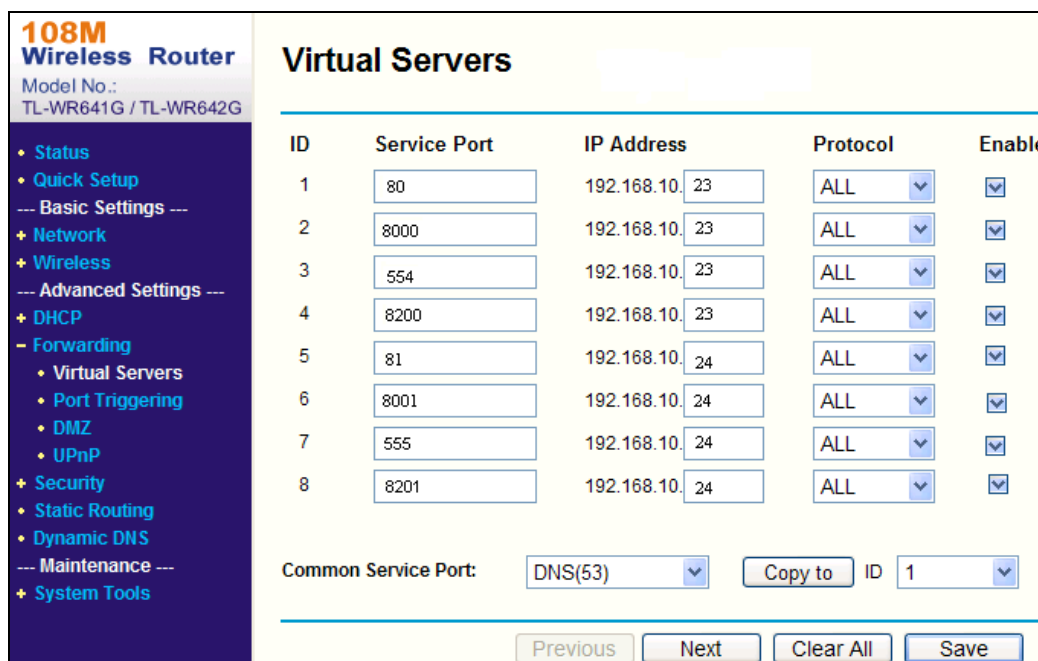4. Check the **Enable** checkbox and click **Save** to save the settings.

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.

First Choice for Security Professionals