Network Fisheye Camera

User Manual

UD14558B-A

Initiatives on the Use of Video Products

Thank you for choosing Hikvision products.

Technology affects every aspect of our life. As a high-tech company, we are increasingly aware of the role technology plays in improving business efficiency and quality of life, but at the same time, the potential harm of its improper usage. For example, video products are capable of recording real, complete and clear images. This provides a high value in retrospect and preserving real-time facts. However, it may also result in the infringement of a third party's legitimate rights and interests if improper distribution, use and/or processing of video data takes place. With the philosophy of "Technology for the Good", Hikvision requests that every end user of video technology and video products shall comply with all the applicable laws and regulations, as well as ethical customs, aiming to jointly create a better community.

Please read the following initiatives carefully:

- Everyone has a reasonable expectation of privacy, and the installation of video products should not be in conflict with this reasonable expectation. Therefore, a warning notice shall be given in a reasonable and effective manner and clarify the monitoring range, when installing video products in public areas. For non-public areas, a third party's rights and interests shall be evaluated when installing video products, including but not limited to, installing video products only after obtaining the consent of the stakeholders, and not installing highly-invisible video products.
- The purpose of video products is to record real activities within a specific time and space and under specific conditions. Therefore, every user shall first reasonably define his/her own rights in such specific scope, in order to avoid infringing on a third party's portraits, privacy or other legitimate rights.
- During the use of video products, video image data derived from real scenes will continue to be generated, including a large amount of biological data (such as facial images), and the data could be further applied or reprocessed. Video products themselves could not distinguish good from bad regarding how to use the data based solely on the images captured by the video products. The result of data usage depends on the method and purpose of use of the data controllers. Therefore, data controllers shall not only comply with all the applicable laws and regulations and other normative requirements, but also respect international norms, social morality, good morals, common practices and other non-mandatory requirements, and respect individual privacy, portrait and other rights and interests.
- The rights, values and other demands of various stakeholders should always be considered when processing video data that is continuously generated by video products. In this regard, product security and data security are extremely crucial. Therefore, every end user and data controller, shall undertake all reasonable and necessary measures to ensure data security and avoid data leakage, improper

disclosure and improper use, including but not limited to, setting up access control, selecting a suitable network environment (the Internet or Intranet) where video products are connected, establishing and constantly optimizing network security.

- Video products have made great contributions to the improvement of social security around the world, and we believe that these products will also play an active role in more aspects of social life. Any abuse of video products in violation of human rights or leading to criminal activities are contrary to the original intent of technological innovation and product development. Therefore, each user shall establish an evaluation and tracking mechanism of their product application to ensure that every product is used in a proper and reasonable manner and with good faith.

User Manual

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 Network Fisheye Camera.

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 RESPONSIBILITIES 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

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a

residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help

FCC Conditions

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

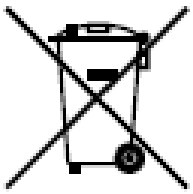
1. This device may not cause harmful interference.

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 (B)/NMB-3(B) standards requirements.

Safety Instruction

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

The precaution measure is divided into 'Warnings' and 'Cautions':

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

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

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

 **Warnings:**

- Please adopt the power adapter which can meet the safety extra low voltage (SELV) standard. And source with 12 VDC or 24 VAC (depending on models) according to the IEC60950-1 and Limited Power Source standard.
- To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture.
- This installation should be made by a qualified service person and should conform

to all the local codes.

- Please install blackouts equipment into the power supply circuit for convenient supply interruption.
- Please make sure that the ceiling can support more than 50(N) Newton gravities if the camera is fixed to the ceiling.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

 **Cautions:**

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

- Improper use or replacement of the battery may result in hazard of explosion. Please use the manufacturer recommended battery type.

Notes:

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

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

Table of Contents

Chapter 1System Requirement

Operating System: Microsoft Windows XP SP1 and above version

CPU: 2.0 GHz or higher

RAM: 1G or higher

Display: 1024×768 resolution or higher

Web Browser: Internet Explorer 8.0 and above version, Apple Safari 5.0.2 and above version, Mozilla Firefox 5.0 and above version and Google Chrome 18 and above version

Chapter 2Network 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.

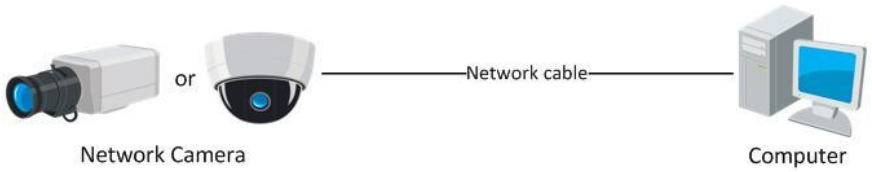


Figure 2-1 Connecting Directly

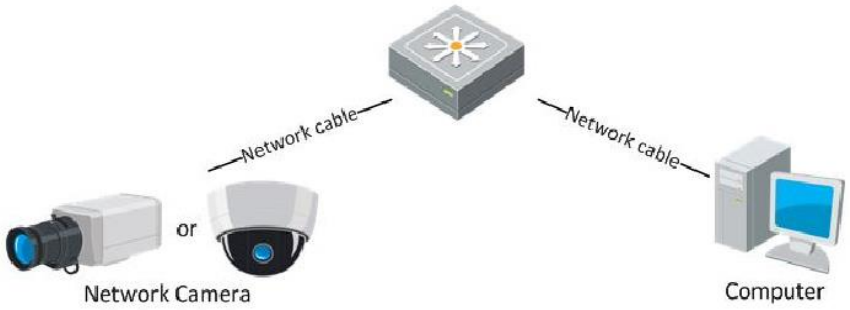


Figure 2-2 Connecting via a Switch or a Router

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.
- The computer and the camera should belong to the same subnet.

For the camera enables the DHCP by default, you need to use the SADP software to search the IP address.

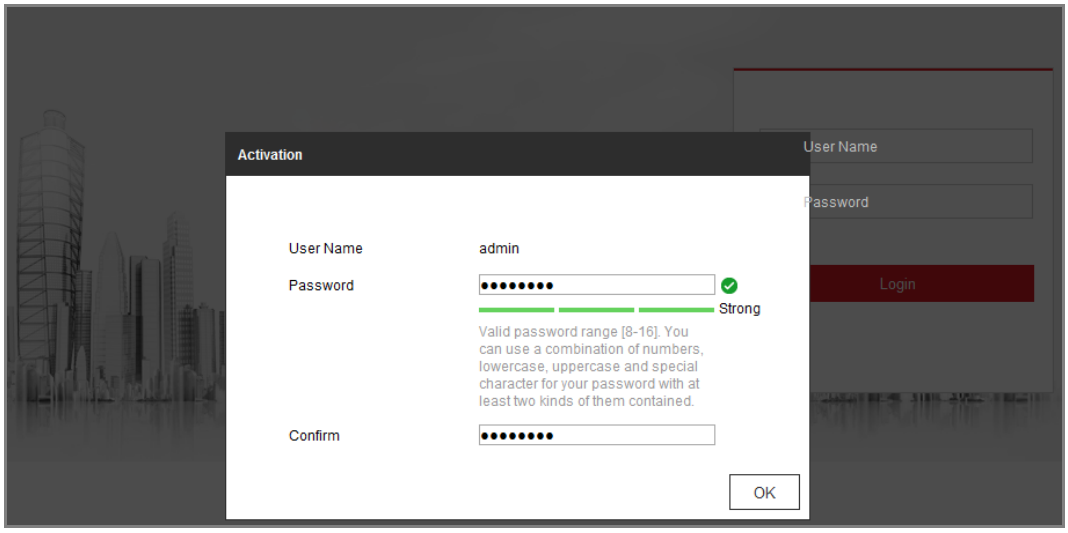


Figure 2-3 Activation via Web Browser

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

A password with user name in it is not allowed.

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

4. Confirm the password.

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

❖ 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.

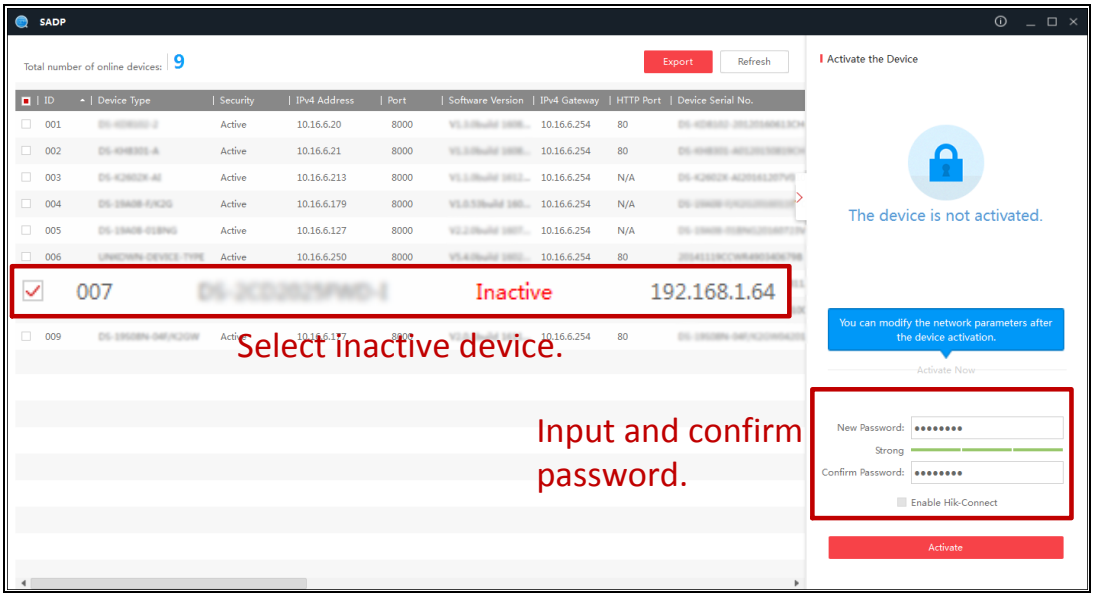


Figure 2-4 SADP Interface

Note:

The SADP software supports activating the camera in batch. Refer to the user manual of SADP software for details.

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

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

Note:

You can enable the Hik-Connect service for the device during activation.

4. Click **Activate** to start activation.

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.

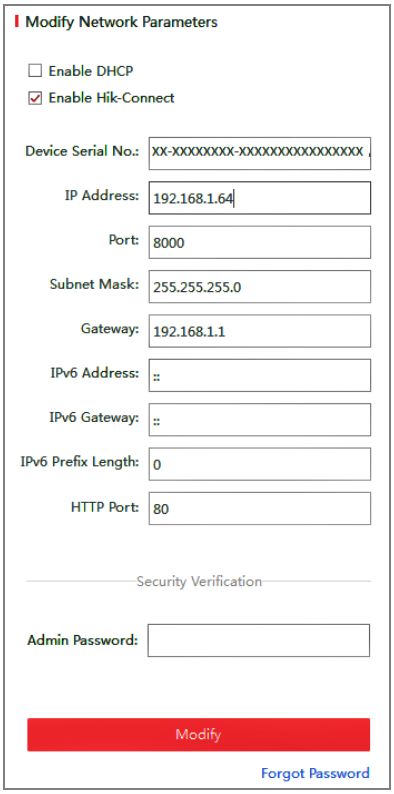


Figure 2-5 Modify the IP Address

6. Input the admin password and click Modify to activate your IP address modification.

The batch IP address modification is supported by the SADP. Refer to the user manual of SADP for details.

❖ 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.

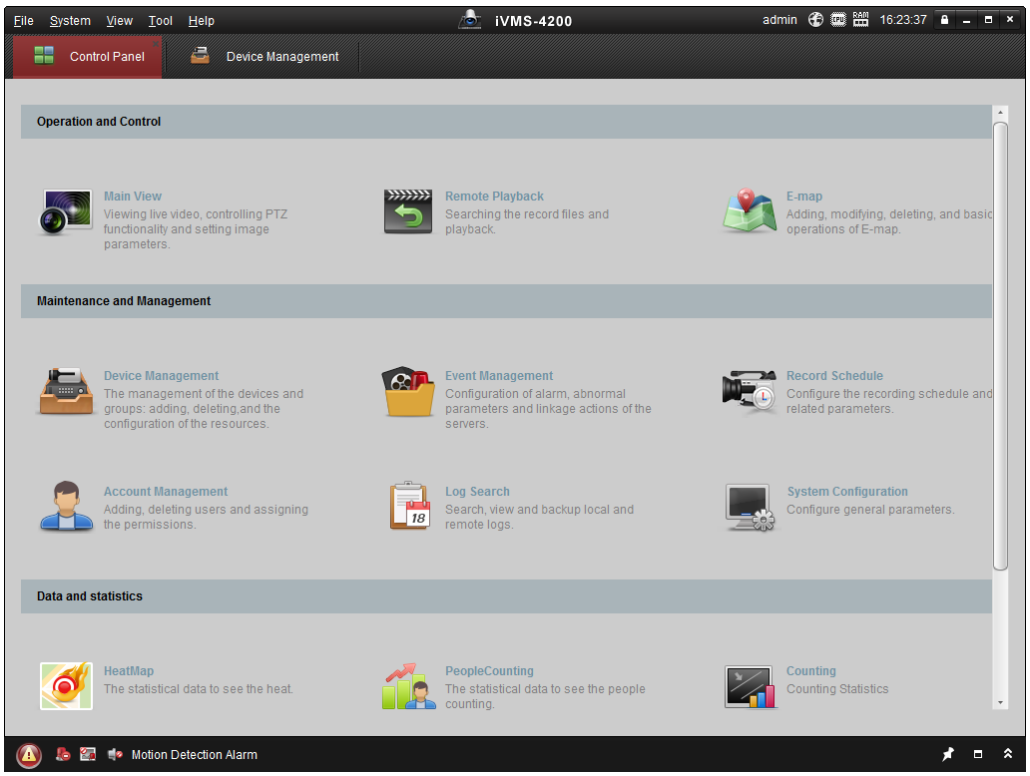


Figure 2-6 Control Panel

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

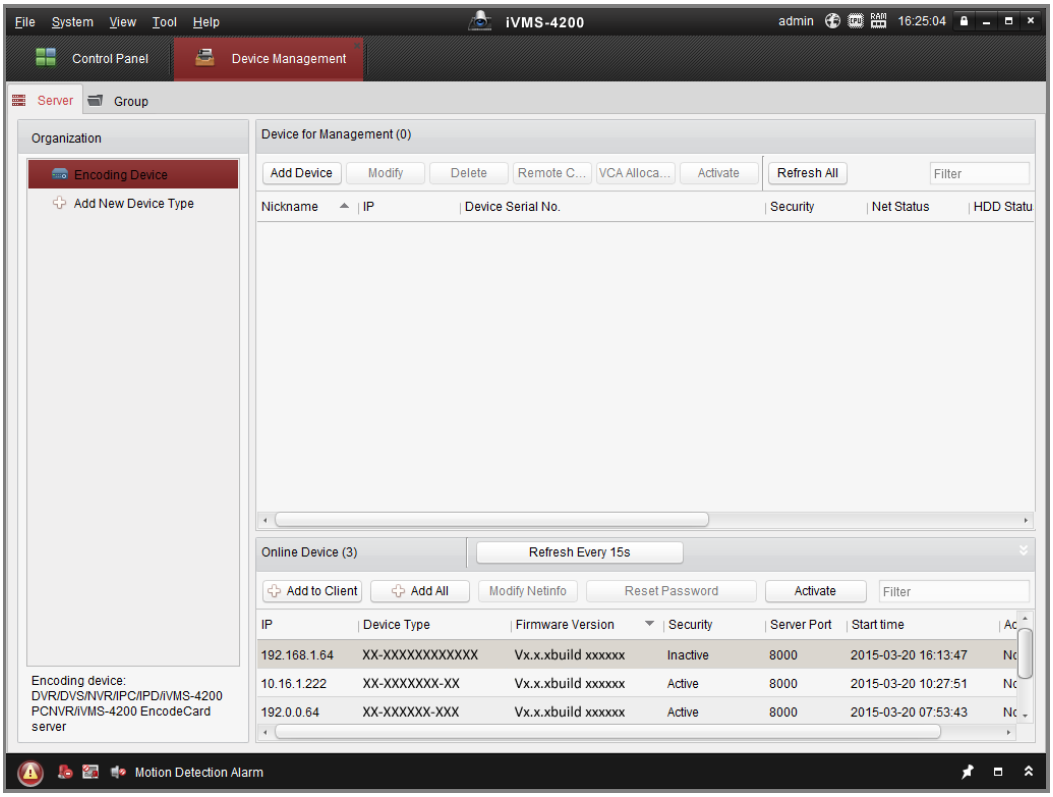


Figure 2-7 Device Management Interface

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

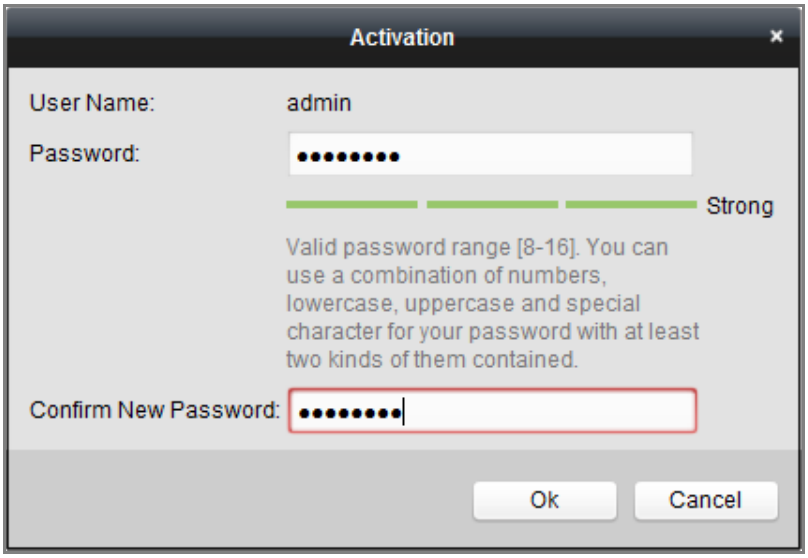


Figure 2-8 Activation Interface (Client Software)

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.

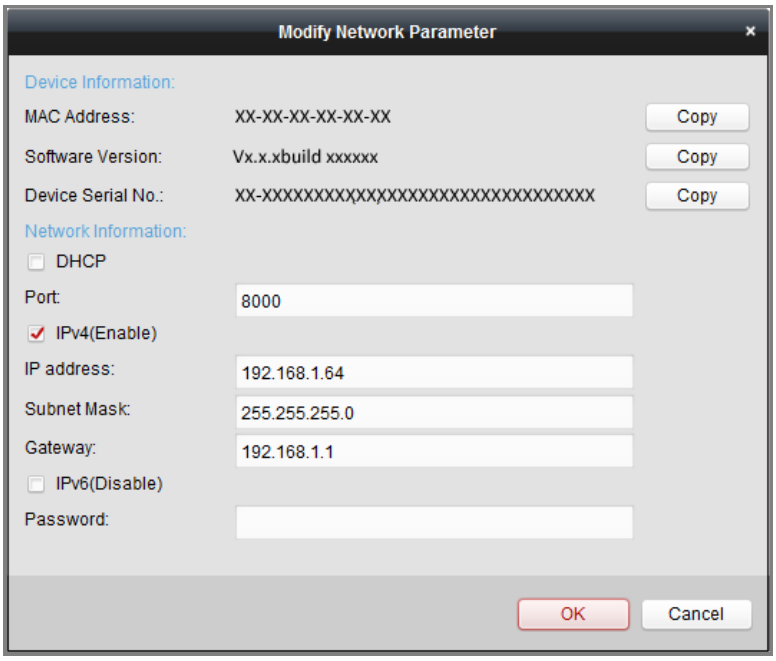


Figure 2-9 Modifying the Network Parameters

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.

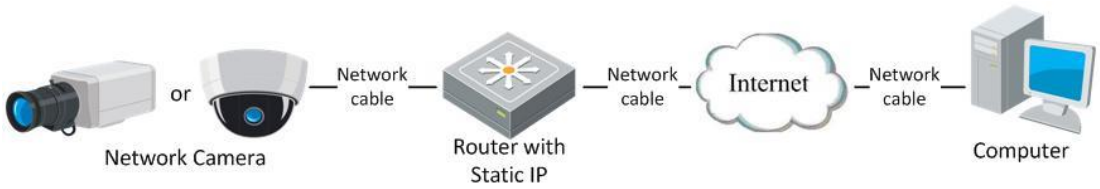


Figure 2-10 Accessing the Camera through Router with Static IP

- **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.

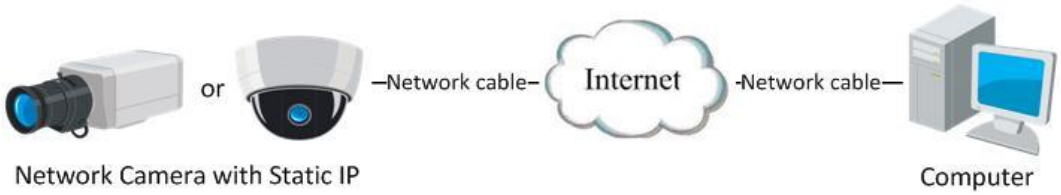


Figure 2-11 Accessing the Camera with Static IP Directly

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 5.3.3* ***Configuring PPPoE Settings*** for detailed configuration.

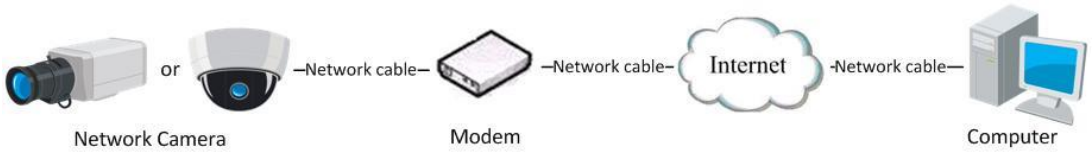


Figure 2-12 Accessing the Camera with Dynamic IP

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

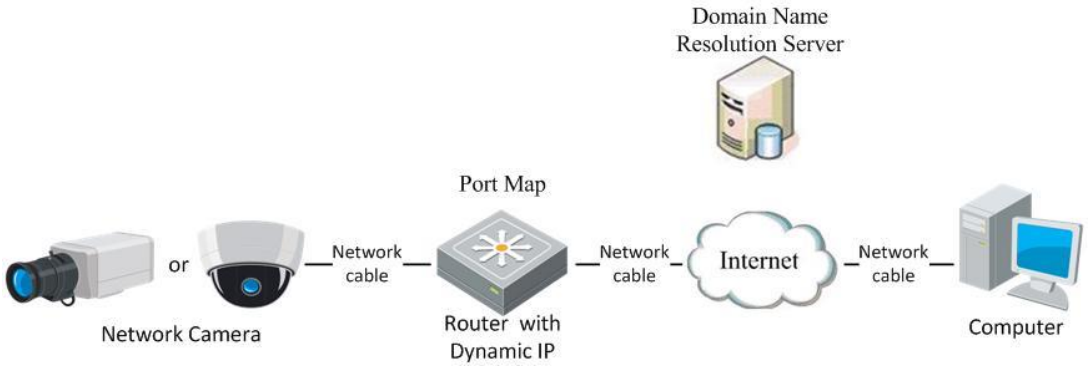


Figure 2-13 Normal Domain Name Resolution

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 5.3.4* ***Configuring DDNS Settings*** for detailed configuration.
3. Visit the camera via the applied domain name.

Chapter 3 Access to the Network Camera

3.1 Accessing by Web Browsers

Note:

For certain camera models, HTTPS is enabled by default and the camera creates an unsigned certificate automatically. When you access to the camera the first time, the web browser prompts a notification about the certificate issue.

To cancel the notification, install a signed-certificate to the camera. For detailed operation, see *6.2.5 HTTPS Settings.*

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.

   Note:

   The default IP address is 192.168.1.64. You are recommended to change the IP address to the same subnet with your computer.
3. Input the user name and password and click **Login**.

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

Note:

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

Figure 3-1 Login Interface

4. Click **Login**.
5. (Optional) Install the plug-in before viewing the live video and operating the camera. Follow the installation prompts to install the plug-in.

Note:

For camera that supports plug-in free live view, if you are using Google Chrome 45 and its above version or Mozilla Firefox 52 and its above version, plug-in installation is not required. But **Picture** and **Playback** functions are hidden. To use mentioned function via web browser, change to their lower version, or change to Internet Explorer 8.0 and above version.

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 interface of iVMS-4200 client software is shown as bellow.

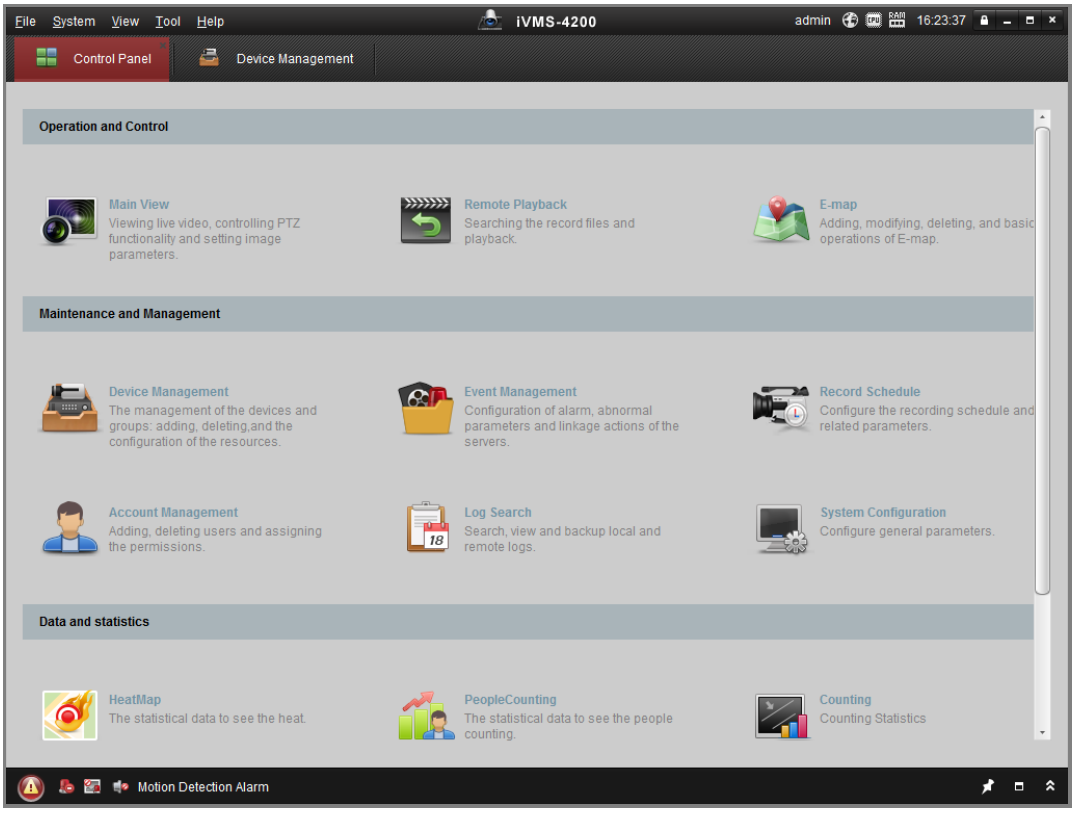


Figure 3-2 iVMS-4200 Client Software

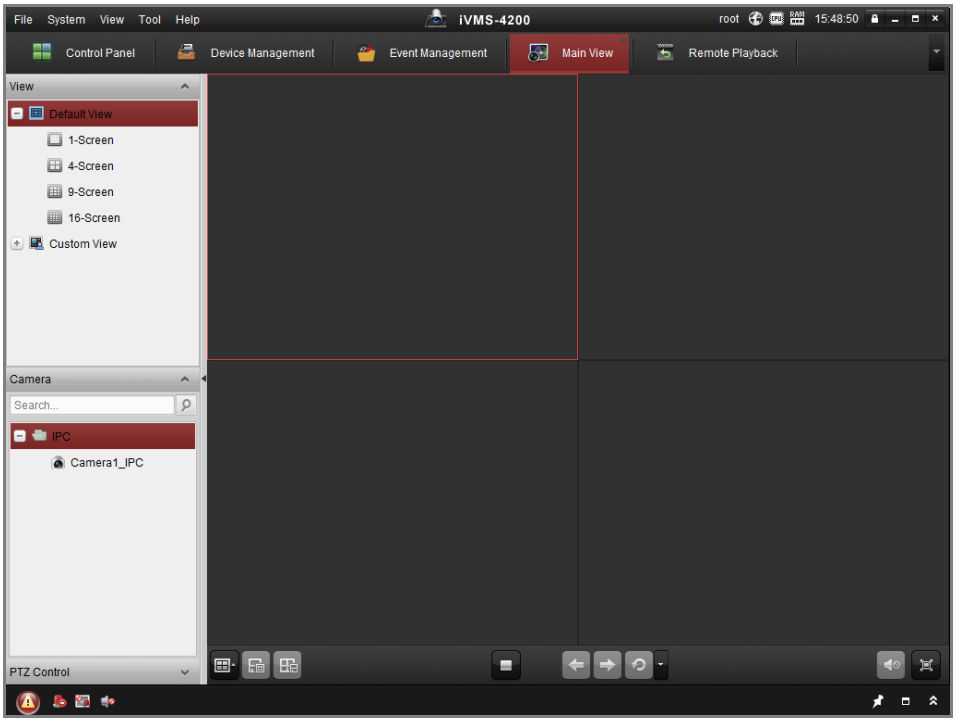


Figure 3-3 iVMS-4200 Main View

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

Chapter 4 Live 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.

Note:

You can also visit the fisheye camera to get the live view in different live view modes via iVMS-4200 client software. Please refer to the User Manual of iVMS-4200 Client Software for detailed instructions.

Introduction:

The **Live View Page** is mainly composed of three parts, the display control area on the left, the live view screen in the middle and a PTZ panel which can be shown or hidden on the right.

Descriptions of the live view page:

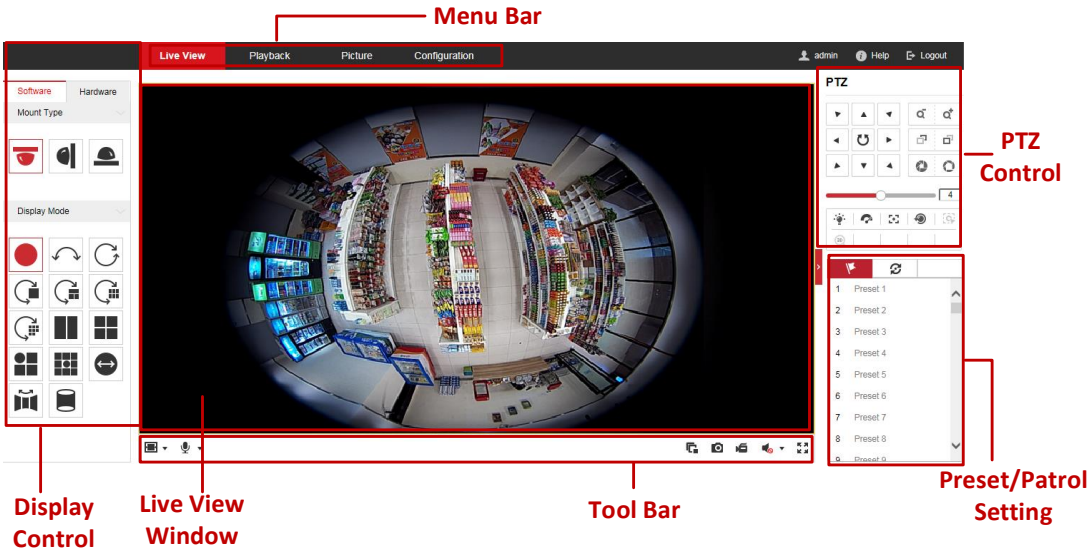


Figure 4-1 Live View Page (Software Decoding)

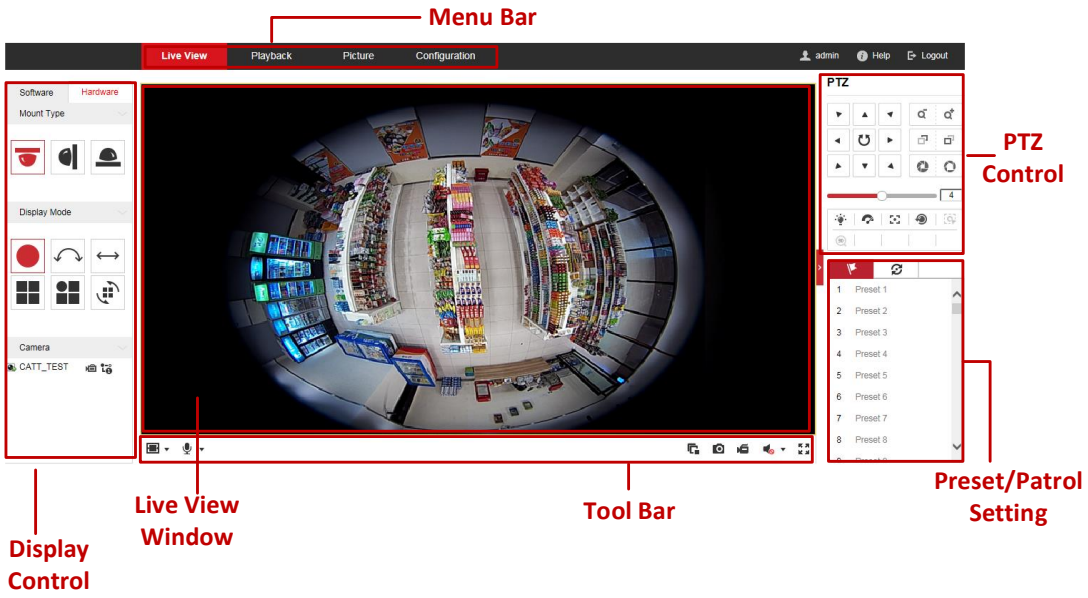


Figure 4-2 Live View Page (Hardware Decoding)

Menu Bar:

Click the tab to enter Live View, Playback, Picture, Application and Configuration page respectively.

Display Control:

The display control area allows you to select decoding mode, mount type and display mode of live view. Software decoding and hardware decoding are selectable for decoding mode. On the software tab, mount type and display mode are configurable. While on the hardware tab, besides the mount type and display mode, stream type of each camera channel is also configurable.

- **Decoding Mode**

  Software decoding means the obtained live view video is decoded by using the CPU of your PC that is running the web browser. The live view performance depends on the decoding ability of your PC.

  Hardware decoding means the obtained live view video is decoded by the camera itself.

- **Mount Type**

  Select ceiling mounting, wall mounting and table mounting according to the actual mount type you adopted for your camera.

Table 4-1 Description of Mount Types

Mount Type Icon	Description
	Ceiling mounting.
	Wall mounting.
	Table mounting.

- **Display Mode**

  You can select a display mode for the layout of the live view window. The description of each display mode is shown in the following table.

  - **Fisheye View**: In the Fisheye View mode, the whole wide-angle view of the fisheye camera is displayed. This view mode is called Fisheye View because it approximates the vision of a fish's convex eye. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image.
  - **Panorama View**: In the Panorama View mode, the round fisheye image is transformed to rectangular image by some calibration methods.
  - **PTZ View**: The PTZ View is the close-up view of some defined area in the Fisheye View or Panorama View.

  Note: Each PTZ View is marked on the Fisheye View and Panorama View with a specifically colored region under software decoding mode, and with a specific navigation box under hardware decoding mode.

Table 4-2 Description of Display Modes

Mode	Description	Mode	Description
	Fisheye view.		180 degrees panorama view.
	360 degrees panorama view.		Live view with a 360 degrees panorama view and a PTZ view.
	Live view with a 360 degrees panorama view and 3 PTZ views.		Live view with a 360 degrees panorama view and 6 PTZ views.
	Live view with a 360 degrees panorama view and 8 PTZ views.		Live view with 2 PTZ views.

Mode	Description	Mode	Description
	Live view with into 4 PTZ views.		Live view with 1 fisheye view and 3 PTZ views.
	Live view with 1 fisheye view and 8 PTZ views.		Panorama view.
	Live view with a panorama view and 3 PTZ views.		Live view with a panorama view and 3 PTZ views.
	Live view with a fisheye view, a panorama view and 3 PTZ views.		Live view with a hemisphere view
	Live view with a AR hemisphere view		Live view with a cylinder view
	Live view with a 4 PTZ fusion view		

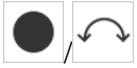
Note:

- Available display modes vary according to decoding modes and camera models.
- When you change display mode on hardware tab, a reboot is required to for the display mode switch to take effect.
- When you display hardware-decoded live view under the display mode of 360 panorama view or 4 PTZ, you cannot switch the decoding mode directly from hardware to software. Switch to the other display mode first.

Stream Type Setting (Hardware Decoding Only):

Steam type switch for camera channels is only supported when the live view video is decoded by hardware. You can set stream type as main stream  or sub stream  . The default stream type for every channel is main stream.

Table 4-3 Selectable Stream Types for Camera Channels

Display Mode	Channel No.	Selectable Stream Type
	Camera 01	Main stream/Sub stream
	Camera 01/02/03/04	Main Stream
	Camera 01	Main stream/Sub stream
	Camera 02/03/04	Main Stream
	Camera 01/02/03/04/05	Main stream

Note: Selectable stream types may be different between camera channels under different display modes. Detailed information is shown in the following table.

Live View Window:

Display the live video on the display window of live view.

Toolbar:

Start/Stop the live view, enable/disable the two-way audio, adjust the audio volume, capture pictures, record the video files, etc.

Note: Icons on tool bar are different under different decoding mode. Refer to Table 4-4 for detailed description.

PTZ Control:

Realize the pan/tilt/zoom function of PTZ view via the navigation box, and set the PTZ moving speed.

Preset/Patrol Settings:

Set and call the preset/patrol for the camera.

4.2 Starting Live View

Starting live view under decoding modes of software and hardware is a bit different.

Software Decoding Mode:

You can click the icon  on the toolbar to start/stop all live view of the camera.

Hardware Decoding Mode:

Under hardware decoding mode, live video will be automatically displayed when you click Live View on menu bar, click Hardware in display control area, change mount type or display mode.

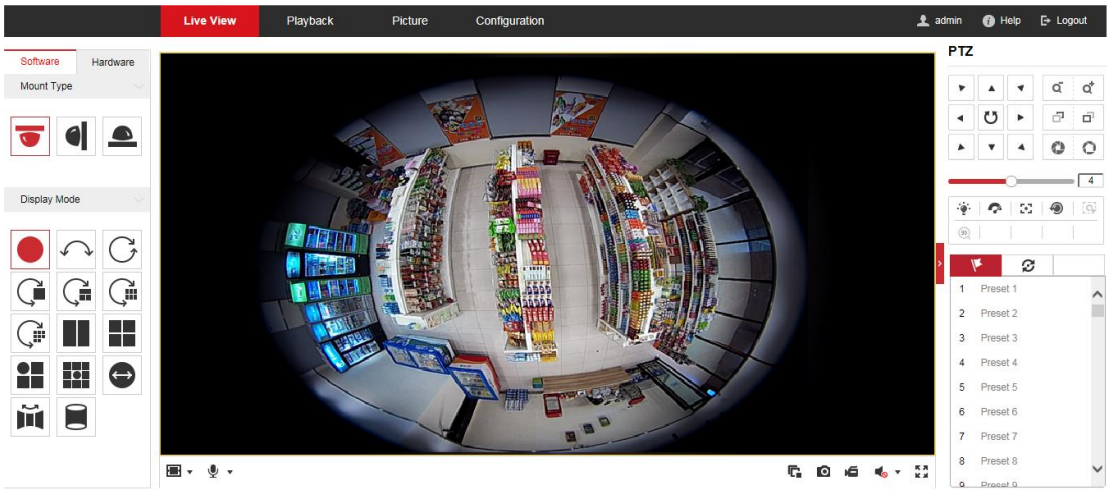


Figure 4-3 Live View Interface (Software Decoding)

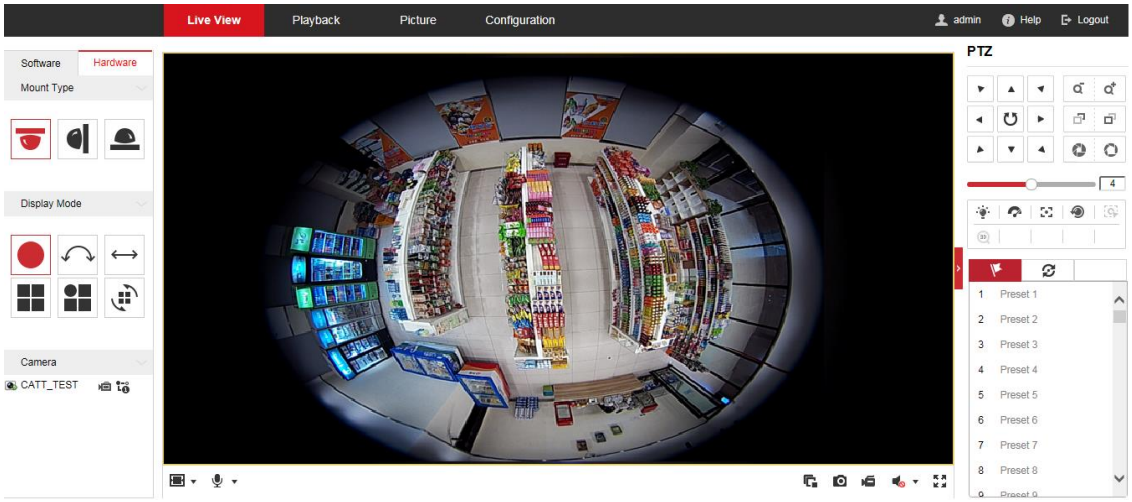


Figure 4-4 Live View Interface (Hardware Decoding)

Table 4-4 Descriptions of Live View Icons

Icon	Description
	Start all live view.
	Stop all live view.
	Set aspect ratio as 4:3.
Icon	**Description**
	Set aspect ratio as 16:9.
	Window size for original video stream.
	Self-adaptive window size.
	Window division, 1x1.
	Window division, 2x2.
	Window division, 3x3.
/	Manually start/stop recording.

	Audio on and adjust the volume.
	Mute.
	Start/stop two-way audio.
	Start/stop digital zoom).
	Manually capture a picture.
	Full screen.
	Show/hide the PTZ panel.

Notes: Toolbar icons on the live view page vary according to decoding modes and camera models.

Digital Zoom:

1) Click  to start the function.
2) Click the mouse on the live view image and drag it to a lower right position. The area in the red rectangle will be zoomed in after you release the mouse.
3) Click the mouse on the zoomed-in image, drag it to a higher left position and release the mouse to zoom out.
4) Click  to stop the 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 video. The saving paths of the captured pictures and record files can be set on the **Configuration > Local Configuration** page. To configure remote scheduled recording, please refer to *Section 6.1*

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

4.4 Operating PTZ Control

Purpose:

A PTZ View is a close-up view of some defined area on the panoramic and fisheye view, and it supports digital PTZ control.

When PTZ View is selected for live view, you can use the PTZ control panel on the

right of the window to realize pan/tilt/zoom control of the PTZ View.

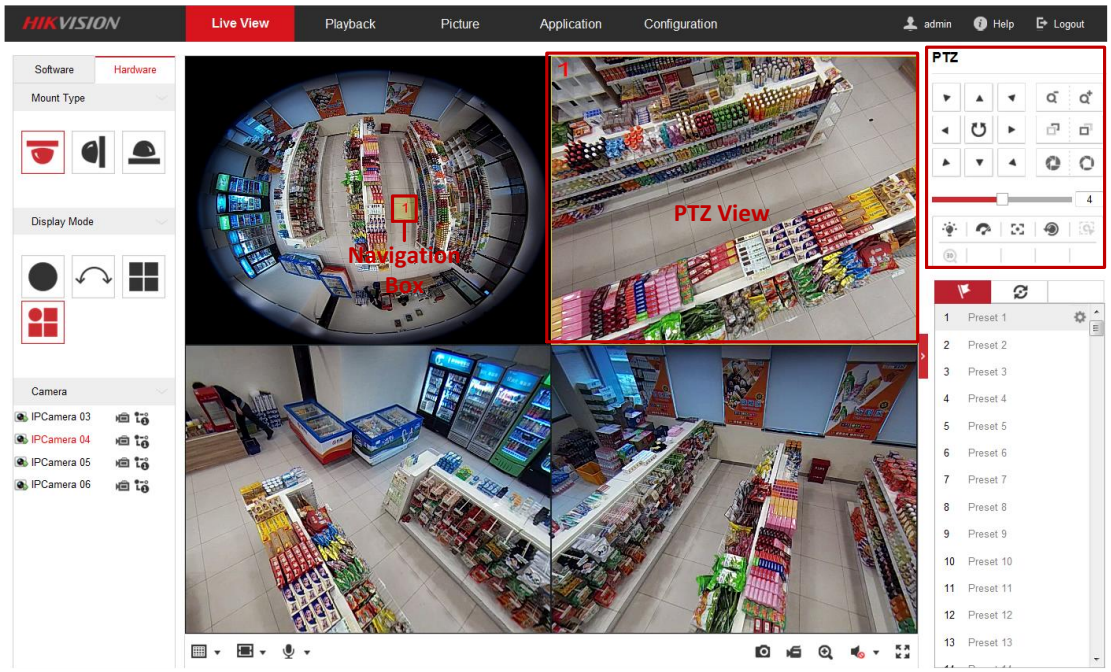


Figure 4-5 PTZ Control

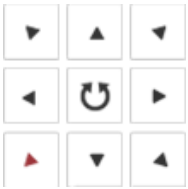
Note: If Fisheye View or Panorama View is selected for live view together with the PTZ View, when you click on a random PTZ view, a navigation box indicating the location of the PTZ view will be shown on the fisheye or panorama view. See Figure 4-5.

4.4.1 PTZ Control Panel

On the live view page, you can click ‹ to show the PTZ control panel, and click › to hide it.

Figure 4-6 PTZ Control Panel

Table 4-5 Descriptions of PTZ Control Panel

Icon	Description
	Direction buttons
	Start/stop auto scan
	Zoom out/Zoom in
	Focus -/Focus +
	Iris -/Iris +
	Adjust speed of pan/tilt movements
	Enable/disable light
	Auxiliary Focus
	Enable/disable wiper
	Lens initialization
	Start manual tracking
	Start 3D zoom
	Click to set presets
	Click to set patrol

Steps:

1. Click to select a PTZ View on the display window, and then the navigation box appears on the Fisheye View and Panorama View.
2. Click the direction arrows on the PTZ control panel. The navigation box will move in the corresponding pan/tilt direction.
3. Adjust zoom, focus and iris level of the PTZ view image.
4. Click-and-drag the slider on the speed bar to adjust the moving speed of PTZ View when auto scan is enabled.

5. (Optional) you can click on other buttons to realize corresponding functions.

4.4.2 Setting/Calling/Deleting a Preset

- **Setting a Preset:**

Purpose:

A preset for the fisheye camera is a predefined PTZ View which contains information of pan, tilt, focus and other parameters.

Steps:

1. Click to select a PTZ View on the display window.
2. Click the direction/zoom buttons on the PTZ Control panel to adjust the PTZ View as desired.
3. Select a preset number from the preset list.
4. Click the icon to save the current PTZ View as the preset.

   The preset name turns from grey to black.

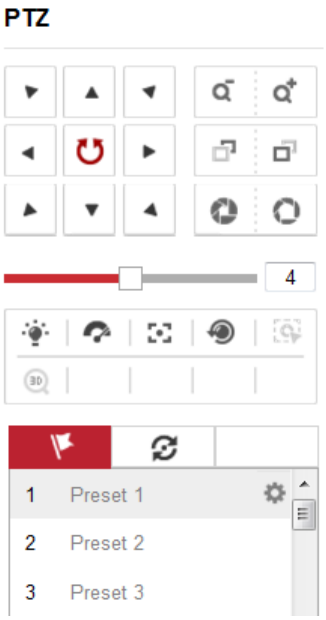


Figure 4-7 Setting a Preset

Note: Up to 256 presets are supported.

- **Calling a Preset:**

Purpose:

The PTZ View of the fisheye camera can directly and quickly move to the area of interest, which is defined as a preset.

Before you start:

Set the preset. The icons (, and) will appear on the preset list.

Steps:

1. Click to select a PTZ View on the display window.
2. Select the preset number from the list.
3. Click the icon to call the selected preset.

   The selected PTZ View will move to the pre-defined preset scene.

- **Deleting a Preset**

Steps:

1. Select the preset number from the list.
2. Click the icon to delete the selected preset.

   The preset name turns from black to grey.

4.4.3 Setting/Calling/Deleting a Patrol

Purpose:

A patrol is a scanning track specified by a group of defined presets, with the duration time at each preset separately programmable.

Before you start:

At least 2 presets are required to set a patrol.

- **Setting a Patrol**

Steps:

1. Click the icon to enter the patrol configuration interface.

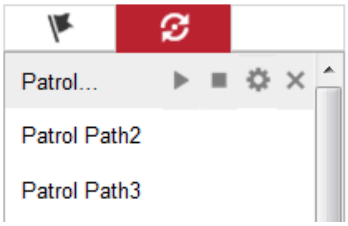


Figure 4-8 Patrol Configuration (1)

2. Select a path No. from the drop-down list, and click the icon to configure patrol path.
3. Click to add a preset into the path, and click to delete a preset.
4. Set the preset number, speed and lingering time at each preset. You can adjust the order of presets by using and .

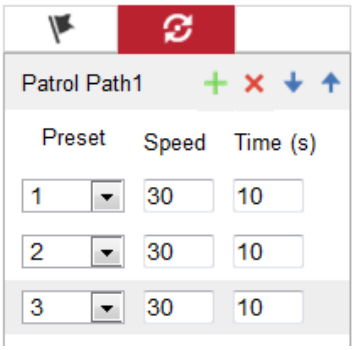


Figure 4-9 Patrol Configuration (2)

5. Click **OK** to save patrol path.

Note: Up to 32 patrol paths can be set, and each path supporting 16 key points at most.

- **Calling a Patrol**

Steps:

1. Click to select a PTZ View on the display window.
2. Select the patrol path number from the drop-down list.
3. Click the icon to start the selected patrol and to stop it.

- **Deleting a Patrol**

1. Select the patrol path number from the drop-down list.
2. Click the icon to delete the patrol path.

Chapter 5 Network Camera Configuration

5.1 Configuring Local Parameters

Purpose:

The local configuration refers to the parameters of the live view, record files and captured pictures. The record files and captured pictures are the ones you record and capture 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**.
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 multicast type when using the Multicast function. For detailed information about Multicast, refer to *Section 7.1.1* ***Configuring TCP/IP Settings***.
  - **Play Performance:** Set the live view performance to Shortest Delay, Balanced, Fluent or Custom. For Custom, you can set the frame rate for live view.
  - **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.

- **Display POS Information:** Enable the function, feature information of the detected target is dynamically displayed near the target in the live image.

  The feature information of different functions are different. For example, ID and waiting time for Queue Management, height for People Counting, etc.

  Note:

  Display POS Information is only available for certain camera models.

- **Image Format:** Choose the image format for picture capture.

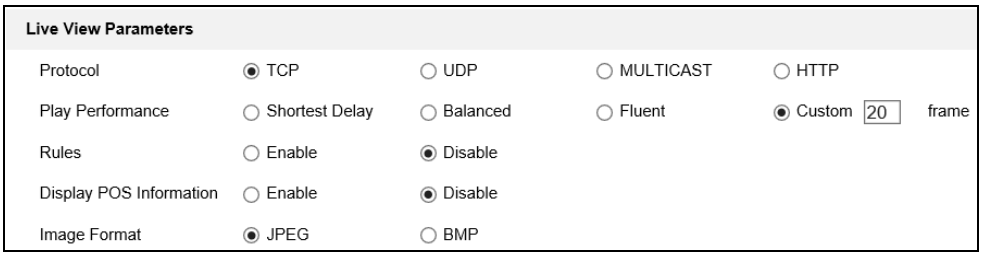


Figure 5-1 Live View Parameters

- **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 capture 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, and click Open to open the set folder of clips and picture saving.

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

5.2 Configure System Settings

Purpose:

Follow the instructions below to configure the system settings, include System Settings, Maintenance, Security, and User Management, etc.

5.2.1 Configuring Basic Information

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

In the **Basic Information** interface, you can edit the Device Name and Device No.

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.

5.2.2 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 > System> System Settings > Time Settings**.

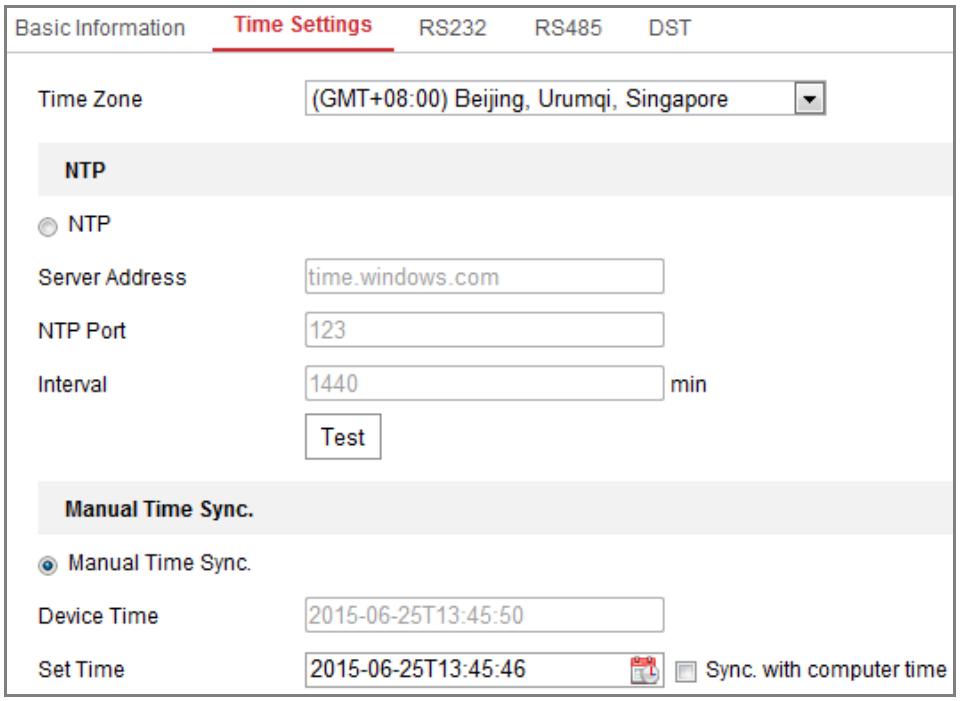


Figure 5-2 Time Settings

2. Select the Time Zone of your location from the drop-down menu.
3. Configure the NTP settings.

(1) Click 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.

(3) (Optional) You can click the **Test** button to test the time synchronization function via NTP server.

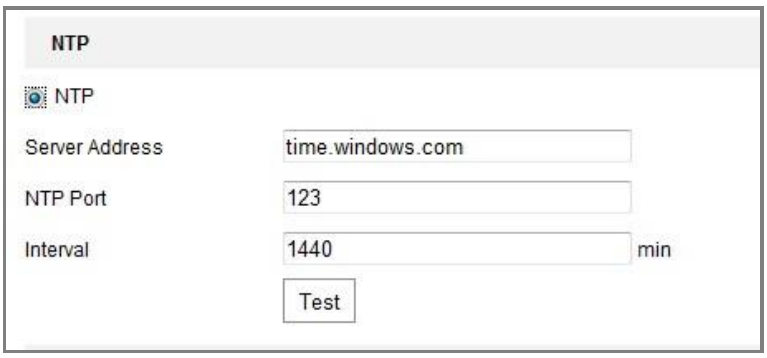


Figure 5-3 Time Sync by NTP Server

***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.

- Configure the manual time synchronization.

  (1) Check the **Manual Time Sync.** item to enable the manual time synchronization function.

  (2) Click the icon to select the date, time from the pop-up calendar.

  (3) (Optional) You can check **Sync. with computer time** item to synchronize the time of the device with that of the local PC.

Figure 5-4 Time Sync Manually

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

5.2.3 Configuring RS232 Settings

The RS232 port can be used in two ways:

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

Steps:

1. Enter RS232 Port Setting interface: **Configuration** > **System** > **System Settings** > **RS232**.
2. Configure the Baud Rate, Data Bit, Stop Bit, Parity, Flow Control, and Usage.

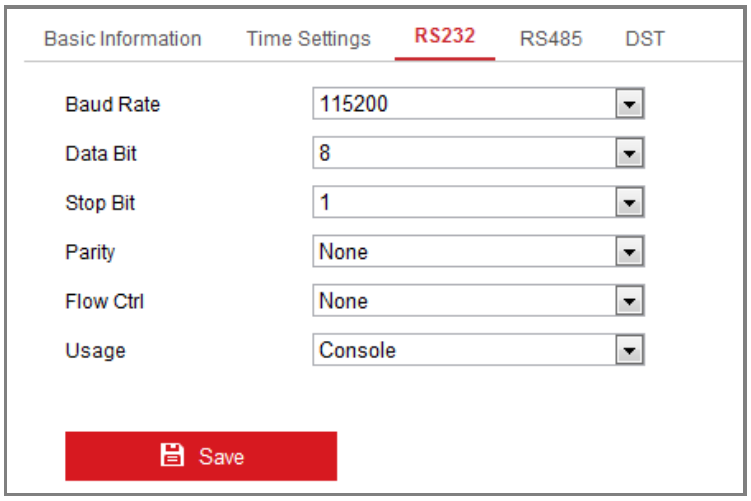


Figure 5-5 RS232 Settings

Note: If you want to connect the camera by the RS232 port, the parameters of the RS232 should be exactly the same with the parameters you configured here.

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

5.2.4 Configuring RS485 Settings

Purpose:

The RS485 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** > **System** > **System Settings** > **RS485**.

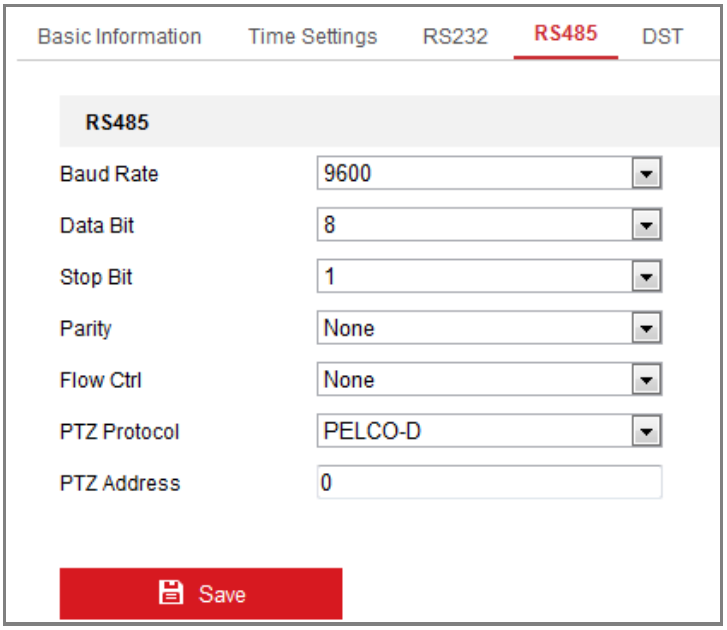


Figure 5-6 RS-485 Settings

2. Set the RS485 parameters and click **Save** to save the settings.

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

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

5.2.5 Configuring DST Settings

Purpose:

Daylight Saving Time (DST) is a way of making better use of the natural daylight by setting your clock forward one hour during the summer months, and back again in the fall.

Configure the DST according to your actual demand.

Steps:

1. Enter the DST configuration interface.

   Configuration > **System** > **System Settings** > **DST**

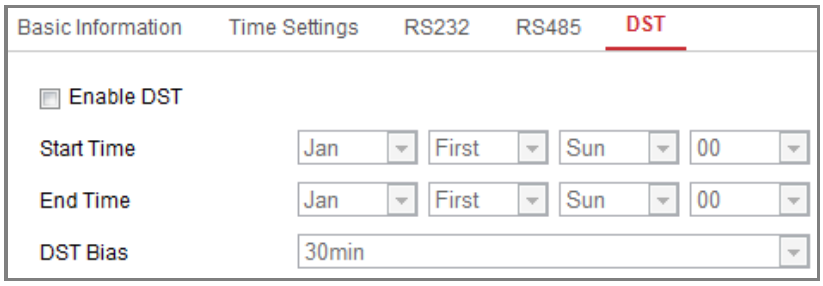


Figure 5-7 DST Settings

2. Select the start time and the end time.
3. Select the DST Bias.
4. Click **Save** to activate the settings.

5.2.6 Configuring Metadata Settings

Purpose:

Metadata is the raw data the camera collects before algorithm processing. Metadata of intrusion detection, line crossing detection, region entrance detection, region exiting detection, unattended baggage detection, object removal, queue management and face capture are supported. If enabled, the metadata of the corresponding event are available for users to explore the possibility of various data usage.

Steps:

1. Enter Metadata settings interface:

   Configuration > System > System Settings > metadata Settings

2. Check the checkbox of the corresponding function to enable the metadata function.

- The metadata of the smart event includes the target ID, target coordinate and time information.
- The metadata of queue management includes the rule information, region ID, target ID, target coordinate and time information. The camera detects the whole image by default. If the region is configured in the queue management settings, the camera detects the configured region.
- The metadata of face capture includes the rule information, target ID, target coordinate, face grading and time information. The camera detects the whole

image by default. If the region is configured in the face capture settings, the camera detects the configured region.

5.2.7 Open Source Software License

Information about the open source software that applies to the IP camera can be checked if required. Go to **Configuration > System Settings > About.**

5.3 Maintenance

5.3.1 Upgrade & Maintenance

Purpose:

The upgrade & maintenance interface allows you to process the operations, including reboot, partly restore, restore to default, export/import the configuration files, and upgrade the device.

Enter the Maintenance interface: **Configuration** > **System** > **Maintenance** > **Upgrade & Maintenance**.

- **Reboot**: Restart the device.
- **Restore:** Reset all the parameters, except the IP parameters and user information, to the default settings.
- **Default**: Restore all the parameters to the factory default.

  Notes:

  - After restoring the default settings, the IP address is also restored to the default IP address, please be careful for this action.
  - For camera that supports Wi-Fi, wireless dial, or wlan function, **Restore** action does not restore the related settings of mentioned functions to default.
- **Information Export**

  Device Parameters: click to export the current configuration file of the camera.

  This operation requires admin password to proceed.

  For the exported file, you also have to create an encryption password. The

encryption password is required when you import the file to other cameras.

Diagnose Information: click to download log and system information.

- **Import Config. File**

  Configuration file is used for the batch configuration of the cameras.

  Steps:

  1. Click **Browse** to select the saved configuration file.
  2. Click **Import** and input the encryption password that you set during exporting.

  Note: You need to reboot the camera after importing configuration file.

- **Upgrade**: Upgrade the device to a certain version.

  Steps:

  1. 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.
  2. Click **Browse** to select the local upgrade file and then click **Upgrade** to start remote upgrade.

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

5.3.2 Log

Purpose:

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

Before you start:

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

Steps:

1. Enter log searching interface: **Configuration** > **System** > **Maintenance** > **Log**.

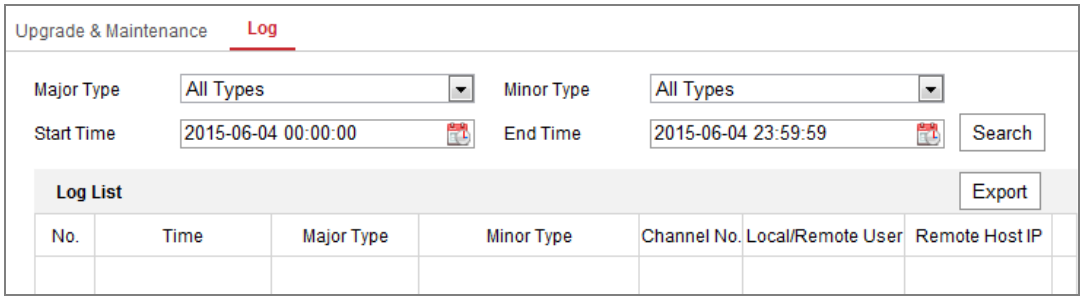


Figure 5-8 Log Searching Interface

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 list interface.

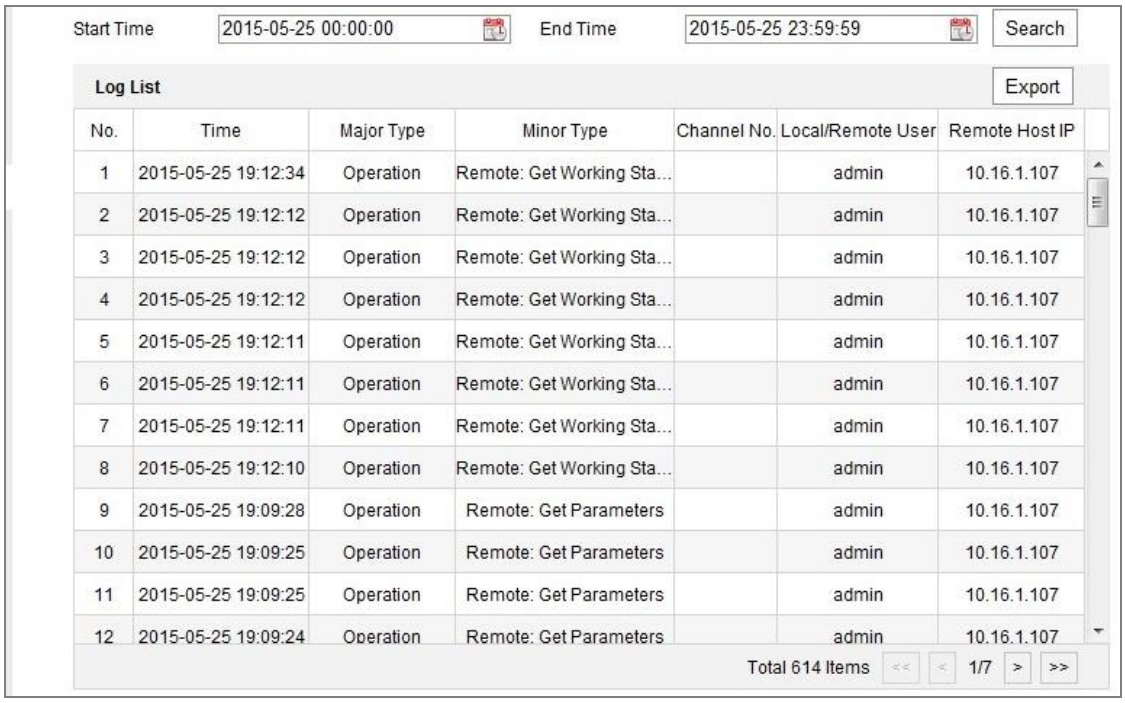


Figure 5-9 Log Searching

4. To export the log files, click **Export** to save the log files.

5.4 Security Settings

Configure the parameters, including Authentication, IP Address Filter, and Security Service from security interface.

5.4.1 Authentication

Purpose:

You can specifically secure the stream data of live view.

Steps:

1. Enter the Authentication interface: **Configuration** > **System** > **Security** > **Authentication.**

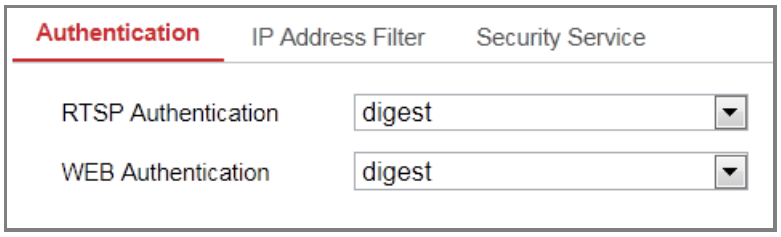


Figure 5-10 Authentication

2. Set up authentication method for RTSP authentication and WEB authentication.

   Caution:

   Digest is the recommended authentication method for better data security. You must be aware of the risk if you adopt basic as the authentication method.

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

5.4.2 IP Address Filter

Purpose:

This function makes it possible for access control.

Steps:

1. Enter the IP Address Filter interface: **Configuration** > **System** > **Security** > **IP Address Filter**

Figure 5-11 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 5-12 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 5-13 Modify an IP

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

- Delete an IP Address or IP Addresses.

  Select the IP address(es) and click **Delete**.

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

5.4.3 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** > **System** > **Security** > **Security Service**.

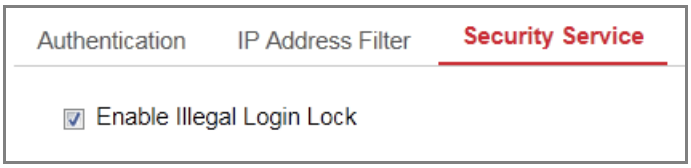


Figure 5-14 Security Service

2. Check the checkbox of **Enable Illegal Login Lock**.

   Illegal Login Lock: it is used to limit the user login attempts. Login attempt from the IP address is rejected if admin user performs 7 failed user name/password attempts (5 times for the operator/user).

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

5.5 User Management

5.5.1 User Management

- **As Administrator**

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

Enter the User Management interface: **Configuration** > **System** > **User Management**

Note:

Admin password if required for adding and modifying a user account.

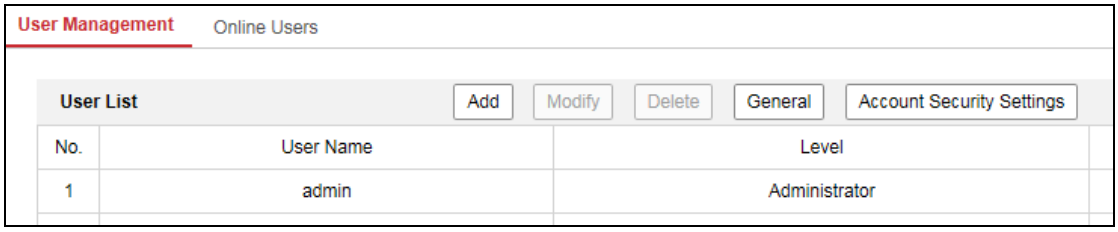


Figure 5-15 User Management Interface

- **Adding a User**

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

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

Steps:

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

   Notes:

   - Up to 31 user accounts can be created.
   - Users of different levels own different default permissions. Operator and user are selectable.

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

3. You can check or uncheck the permissions for the new user.
4. Click **OK** to finish the user addition.

- **Modifying a User**

Steps:

1. Left-click to select the user from the list and click **Modify**.
2. Modify the **User Name**, **Level** and **Password**.

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

3. You can check or uncheck the permissions.
4. Click **OK** to finish the user modification.

- **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 confirm the deletion.

- **Setting Simultaneous Login**

Steps:

1. Click **General**.

2. Slide the slide bar to set the simultaneous login. If the number of the illegal login attempts exceeds the set threshold, your access will be denied.

- **As Operator or User**

  Operator or user can modify password. Old password is required for this action.

5.5.2 Online Users

Purpose:

You can see the current users who are visiting the device through this interface. User information, such as user name, level, IP address, and operation time, is displayed in the User List.

Click **Refresh** to refresh the list.

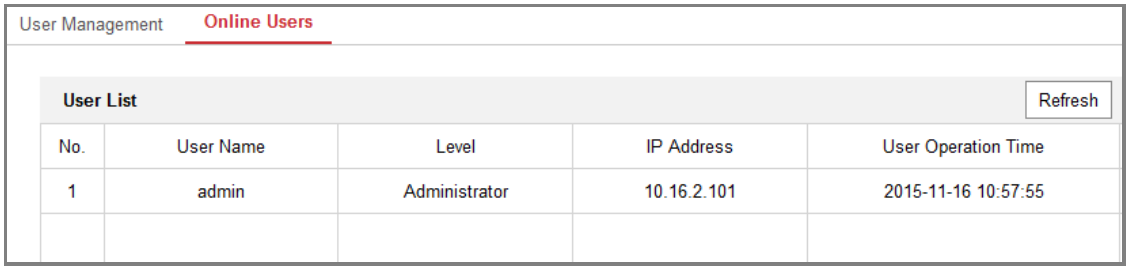


Figure 5-16 View the Online Users

Chapter 6Network Settings

Purpose:

Follow the instructions in this chapter to configure the basic settings and advanced settings.

6.1 Configuring Basic Settings

Purpose:

You can configure the parameters, including TCP/IP, DDNS, PPPoE, Port, and NAT, etc., by following the instructions in this section.

6.1.1 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 can be configured simultaneously without conflicting to each other, and at least one IP version should be configured.

Steps:

1. Enter TCP/IP Settings interface: **Configuration > Network > Basic Settings > TCP/IP**

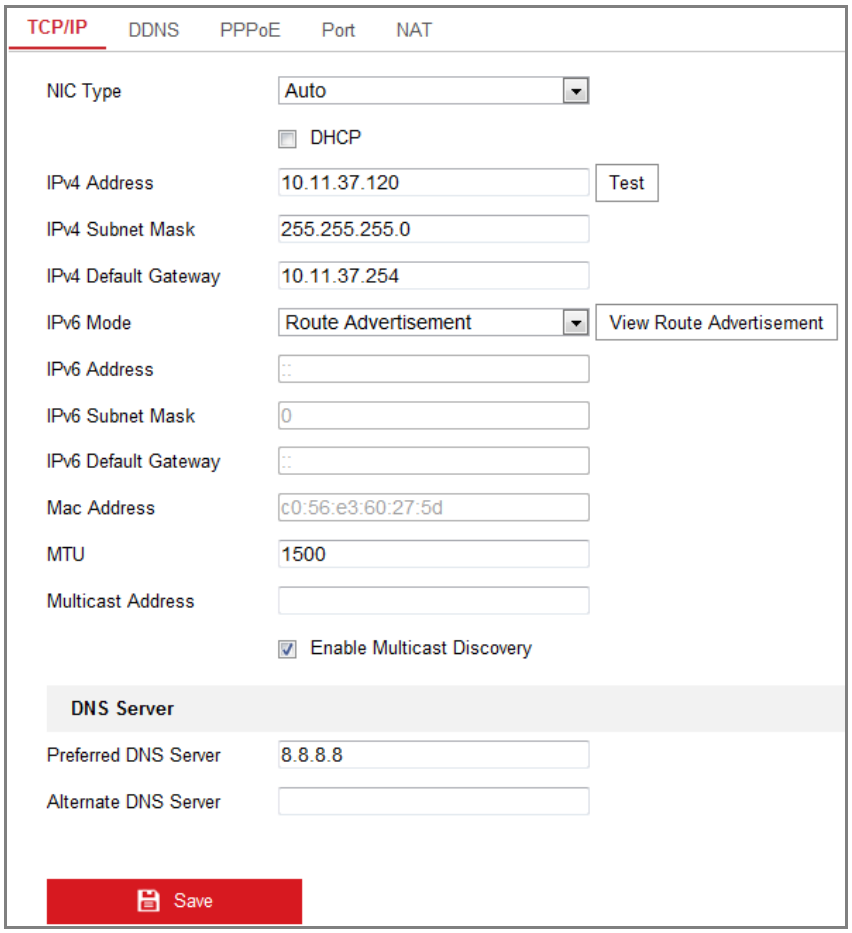


Figure 6-1 TCP/IP Settings

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. Configure the DNS server. Input the preferred DNS server, and alternate DNS server.
5. Click **Save** to save the above settings.

***Notes*:**

- The valid value range of MTU is 1280 to 1500.
- The Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the

multicast group address. Before utilizing this function, you have to enable the Multicast function of your router.

- A reboot is required for the settings to take effect.

6.1.2 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.

Steps:

1. Enter the DDNS Settings interface: **Configuration** > **Network** > **Basic Settings** > **DDNS**.
2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Two DDNS types are selectable: DynDNS and NO-IP.
   - 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 **User Name** and **Password** registered on the DynDNS website.

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

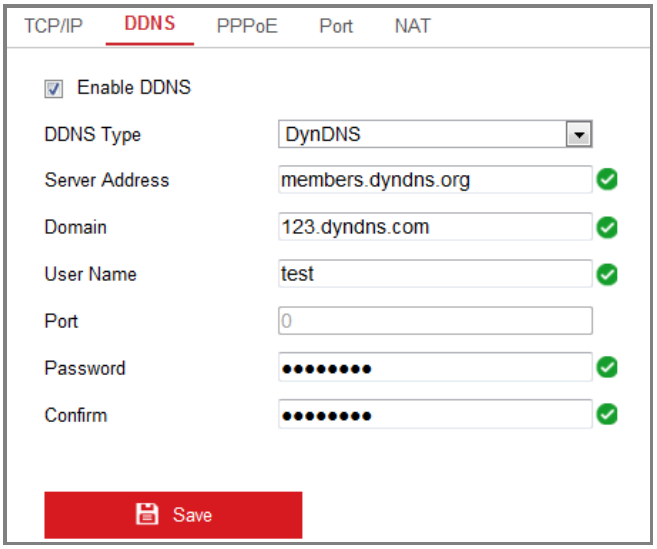


Figure 6-2 DynDNS Settings

- NO-IP:

Steps:

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

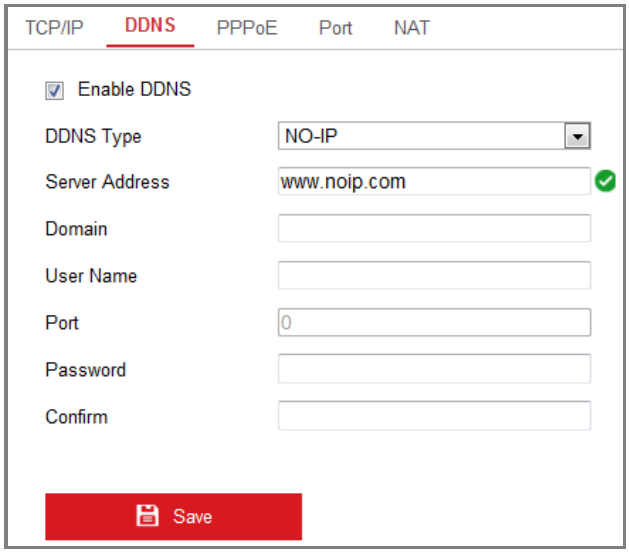


Figure 6-3 NO-IP DNS Settings

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

(3) Enter the Domain name you registered.

(4) Enter the User Name and Password.

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

Note: Reboot the device to make the settings take effect.

6.1.3 Configuring PPPoE Settings

Steps:

1. Enter the PPPoE Settings interface: **Configuration** > **Network** > **Basic Settings** > **PPPoE**

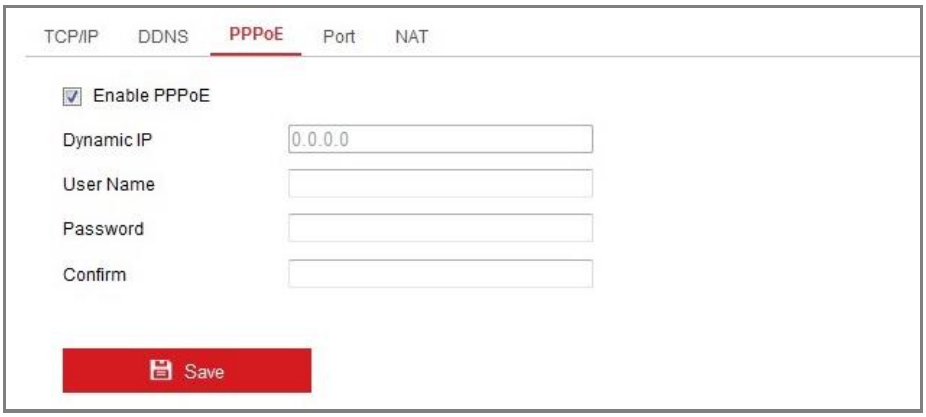


Figure 6-4 PPPoE Settings

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

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

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

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

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

6.1.4 Configuring Port Settings

Purpose:

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

Steps:

1. Enter the Port Settings interface, **Configuration > Network > Basic Settings > Port**

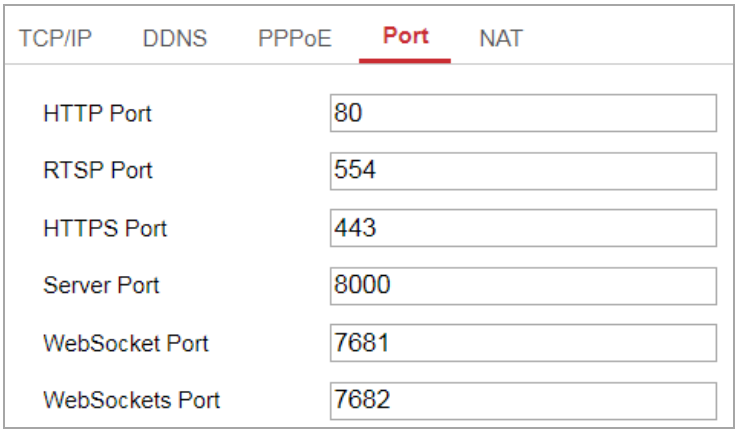


Figure 6-5 Port Settings

2. Set the ports 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 1 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.

   Note:

   When you use client software to visit the camera and you have changed the server port number, you have to input the correct server port number in login interface to access to the camera.

   WebSocket Port: The default port number is 7681. It can be changed to any port

No. ranges from 1 to 65535.

WebSockets Port: The default server port number is 7682. It can be changed to any port No. ranges from 1 to 65535.

Note:

WebSocket and WebSockets protocol are used for plug-in free live view.

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

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

6.1.5 Configure NAT (Network Address Translation) Settings

Purpose:

NAT interface allows you to configure the UPnP™ parameters.

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

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

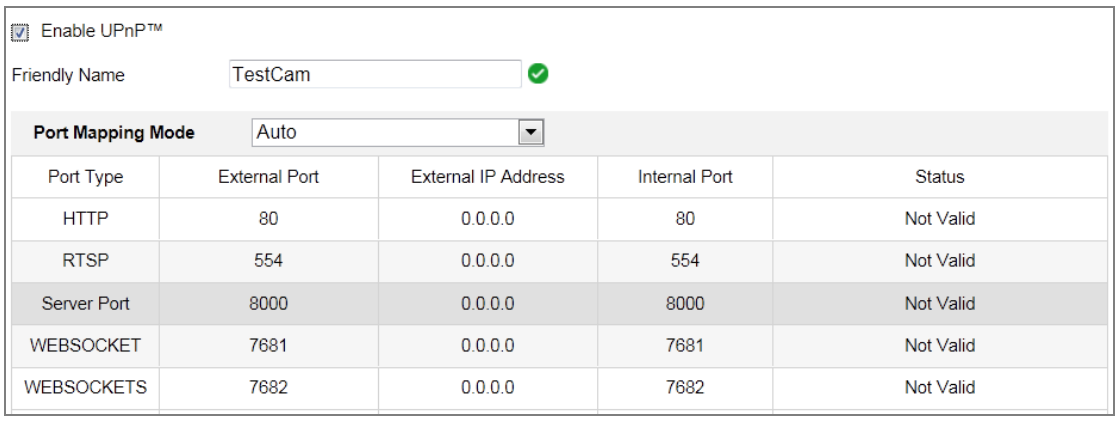


Figure 6-6 UPnP Settings

Steps:

1. Enter the NAT settings interface. **Configuration > Network > Basic Settings > NAT.**
2. Check the checkbox to enable the UPnP™ function.

Note:

Only when the UPnP™ function is enabled, ports of the camera are active.

3. Choose a friendly name for the camera, or you can use the default name.
4. Select the port mapping mode. Manual and Auto are selectable.

   Note:

   If you select Auto, you should enable UPnP™ function on the router.

   If you select Manual, you can customize the value of the external port and complete port mapping settings on router manually.
5. Click **Save** to save the settings.

6.2 Configure Advanced Settings

Purpose:

You can configure the parameters, including SNMP, FTP, Email, HTTPS, QoS, 802.1x, etc., by following the instructions in this section.

6.2.1 Configuring SNMP Settings

Purpose:

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

Before you start:

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

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

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

Steps:

1. Enter the SNMP Settings interface: **Configuration > Network > Advanced Settings > SNMP**.

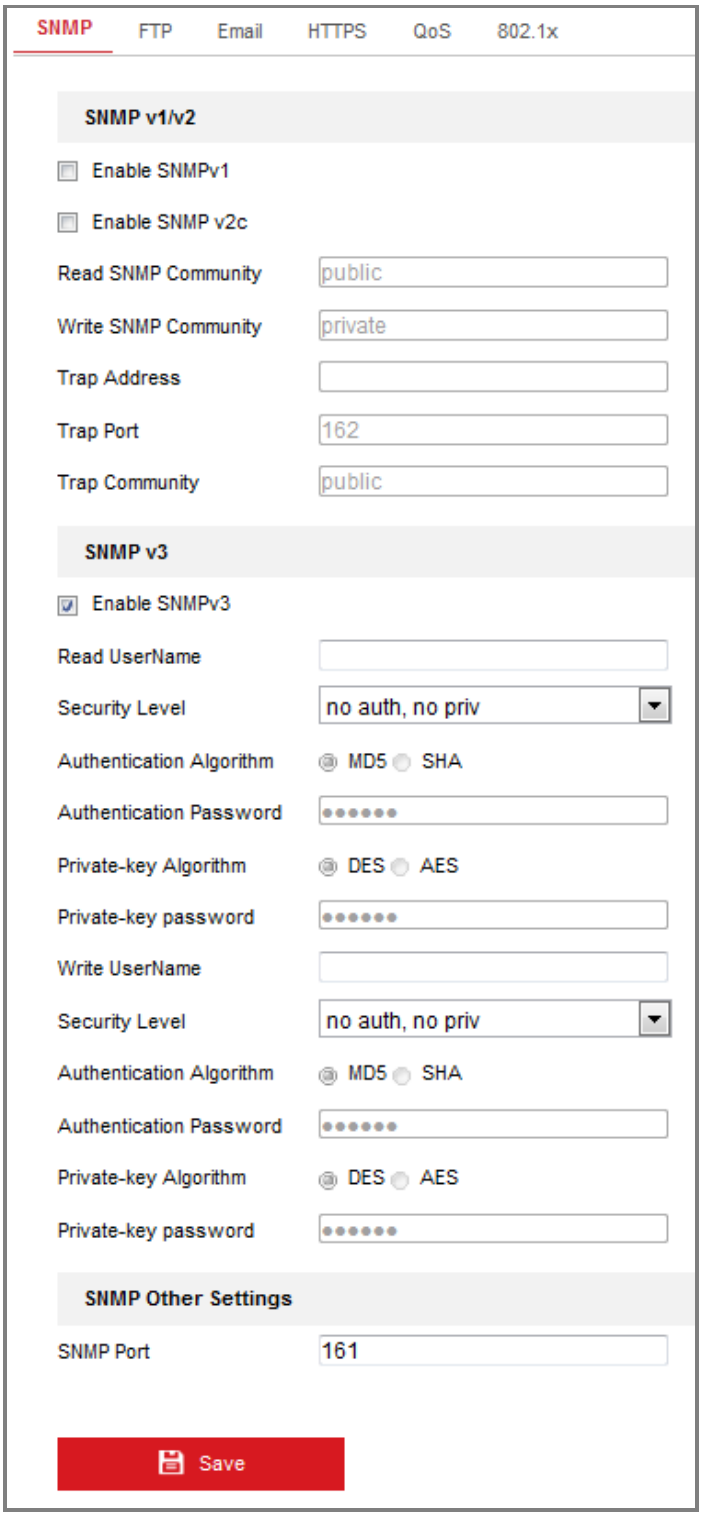


Figure 6-7 SNMP Settings

2. Check the checkbox of Enable SNMPv1, Enable SNMP v2c, Enable SNMPv3 to enable the feature correspondingly.

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.

***Notes*:**

- A reboot is required for the settings to take effect.
- To lower the risk of information leakage, you are suggested to enable SNMP v3 instead of SNMP v1 or v2.

6.2.2 Configuring FTP Settings

Purpose:

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

Steps:

1. Enter the FTP Settings interface:

   Configuration > Network > Advanced Settings > FTP

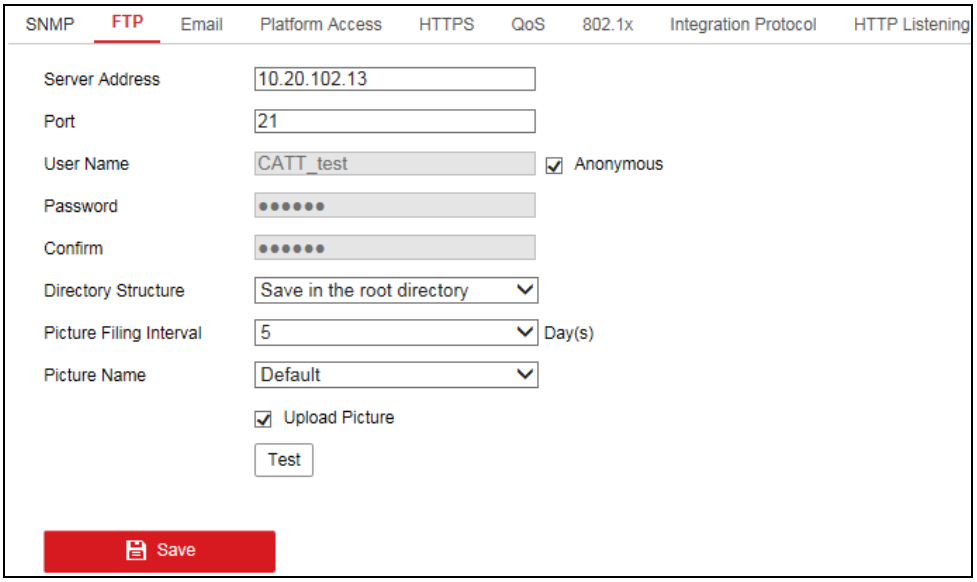


Figure 6-8 FTP Settings

2. Input the server address and port.
3. Configure the FTP settings; and the user name and password are required for the server login.

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

4. Set the directory structure and picture filing interval.

   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.

   Picture Filing Interval: For better picture management, you can set the picture filing interval from 1 day to 30 days. Pictures captured in the same time interval will be saved in one folder named after the beginning date and ending date of the time interval.

   Picture Name: Set the naming rule for captured picture files. You can choose **Default** in the drop-down list to use the default rule, that is,

   IP address_channel number_capture time_event type.jpg

   (e.g., *10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg*).

   Or you can customize it by adding a **Custom Prefix** to the default naming rule.

5. Check the Upload Picture checkbox to enable the function.

   Upload Picture: 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.

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

6.2.3 Configuring Email Settings

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 **Configuration > Network > Basic Settings > TCP/IP** before using the Email function.

Steps:

1. Enter the TCP/IP Settings (**Configuration > Network > Basic Settings > TCP/IP**) to set the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway and the Preferred DNS Server.

   Note: Please refer to *Section 7.1.1* ***Configuring TCP/IP Settings*** for detailed information.

2. Enter the Email Settings interface: **Configuration** > **Network** >**Advanced Settings** > **Email**.

3. Configure the following settings:

   Sender: The name of the email sender.

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

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

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

   Email Encryption: None, SSL, and TLS are selectable. When you select SSL or TLS and disable STARTTLS, e-mails will be sent after encrypted by SSL or TLS. The SMTP port should be set as 465 for this encryption method. When you select

SSL or TLS and enable STARTTLS, emails will be sent after encrypted by STARTTLS, and the SMTP port should be set as 25.

Note: If you want to use STARTTLS, make sure that the protocol is supported by your e-mail server. If you check the Enable STARTTLS checkbox when the protocol is not supported by your e-mail sever, your e-mail will not be encrypted.

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 input the login user name and password.

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

The **Receiver** table**:** 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.

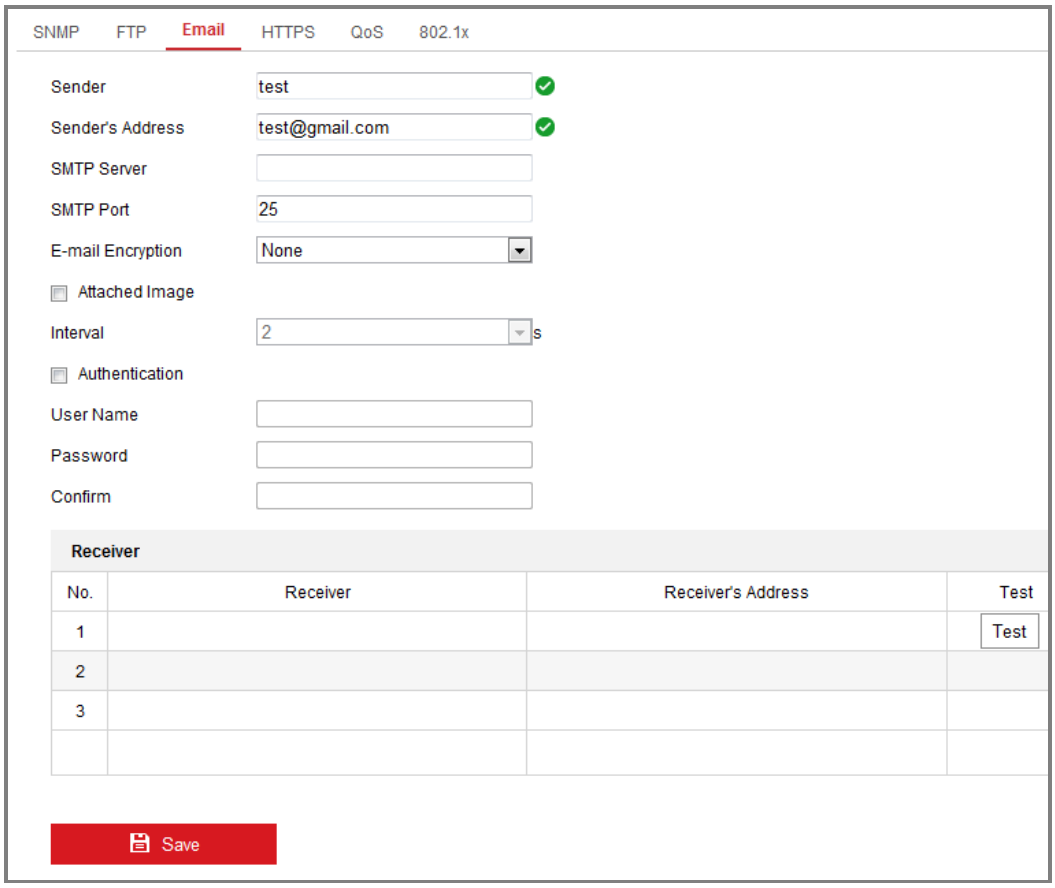


Figure 6-9 Email Settings

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

6.2.4 Platform Access

Purpose:

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

Steps:

1. Enter the **Platform Access** settings interface: **Configuration** > **Network** > **Advanced Settings** > **Platform Access**
2. Check the checkbox of Enable to enable the platform access function of the device.
3. Select the Platform Access Mode.

   Note: Hik-Connect is an application for mobile devices. With the App, you can view live image of the camera, receive alarm notification and so on.

If you select Platform Access Mode as Hik-Connect,

1) Click and read "Terms of Service" and "Privacy Policy" in pop-up window.
2) Create a verification code or change the verification code for the camera.

   Note:

   - The verification code is required when you add the camera to Hik-Connect app.
   - For more information about the Hik-Connect app, refer to Hik-Connect Mobile Client User Manual.
3) You can use the default server address. Or you can check the Custom checkbox on the right and input a desired server address.

6.2.5 HTTPS Settings

Purpose:

HTTPS provides authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks.

Note:

- For the camera that supports plug-in free live view, when you use HTTPS to visit the camera, you should enable **Websockets** for live view. Go to **Configuration** > **Network** > **Advanced Settings** > **Network Service**.
- If HTTPS is enabled by default, the camera creates an unsigned certificate automatically. When you visit the camera via HTTPS, the web browser will send a notification about the certificate issue. Install a signed-certificate to the camera to cancel the notification.

Steps:

1. Enter the HTTPS settings interface. **Configuration** > **Network** > **Advanced Settings** > **HTTPS**.
2. Check **Enable** to access the camera via HTTP or HTTPS protocol.
3. Check **Enable HTTPS Browsing** to access the camera only via HTTPS protocol.

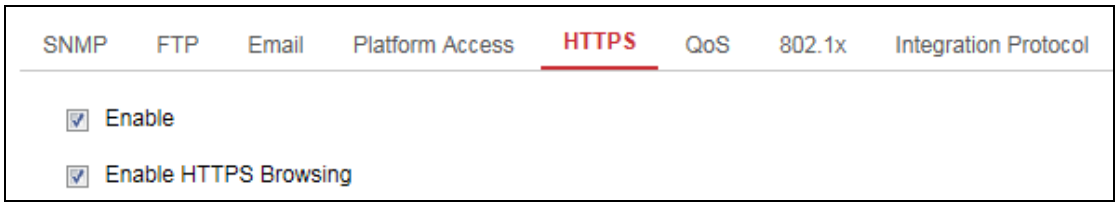


Figure 6-10 HTTPS Configuration Interface

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

Figure 6-11 Create Self-signed Certificate

- Create the self-signed certificate

(1) Select **Create Self-signed Certificate** as the Installation Method.

(2) Click **Create** button to enter the creation interface.

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

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

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

- Create the request and import the authorized certificate

(1) Select **Create the certificate request first and continue the installation** as the Installation Method.

(2) Click **Create** button to create the certificate request. Fill in the required information in the popup window.

(3) Click **Download** to download the certificate request and submit it to the trusted certificate authority for signature.

(4) After receiving the signed valid certificate, you can import the certificate in two ways:

a) Select **Signed certificate is available, Start the installation directly**. Click **Browse** and **Install** to import the certificate to the device.

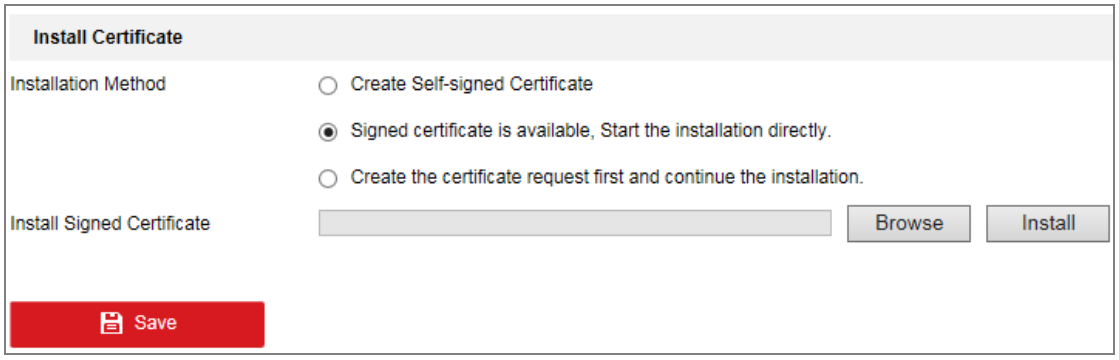


Figure 6-12 Import the Certificate (1)

b) Select **Create the certificate request first and continue the installation**. Click **Browse** and **Install** to import the certificate to the device.

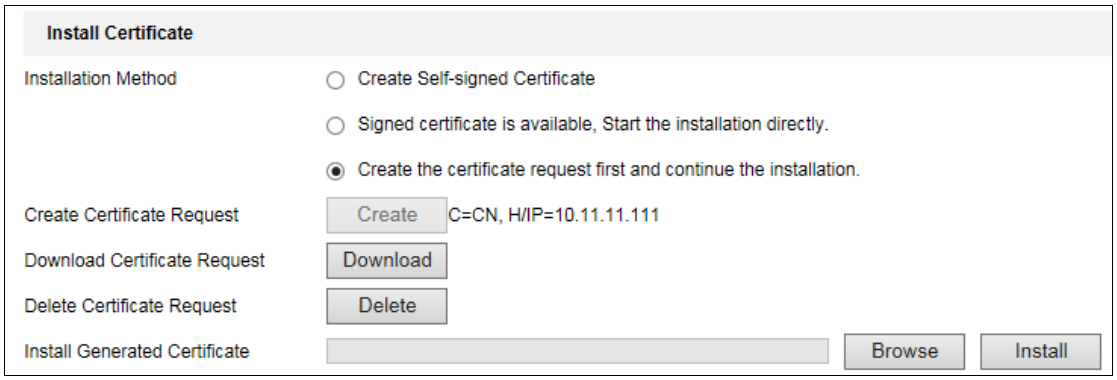


Figure 6-13 Import the Certificate (2)

5. There will be the certificate information after your successfully creating and installing the certificate.

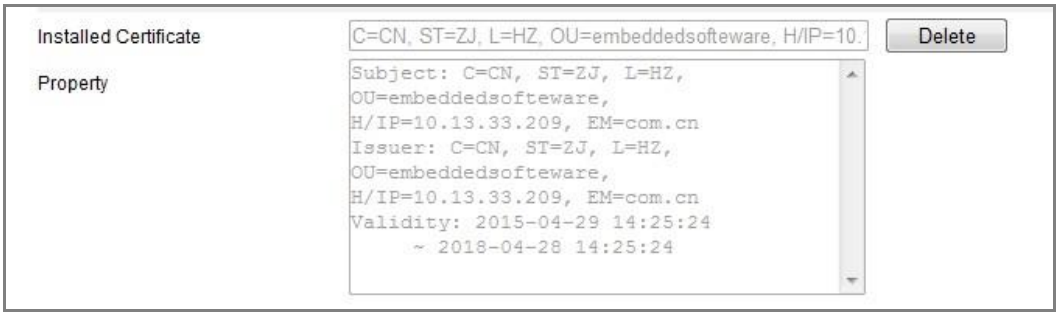


Figure 6-14 Installed Certificate

6. Export and save the certificate for verification when adding the device to client software.

Note:

The exported certificate should be saved in the certificate folder of your client software before adding the device to your PC client.

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

6.2.6 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** > **Network** > **Advanced Settings** > **QoS**

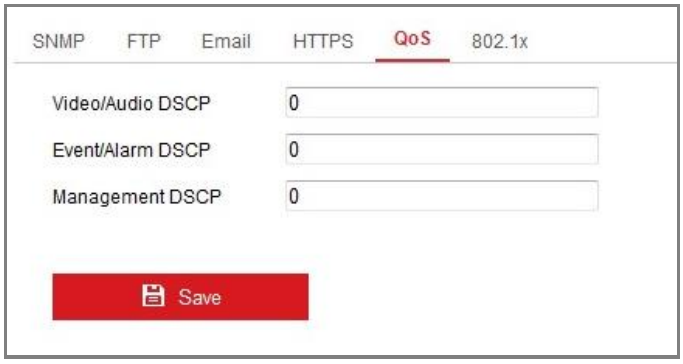


Figure 6-15 QoS Settings

2. Configure the QoS settings, including Video/Audio DSCP, Event/Alarm DSCP and Management DSCP.

   The valid value range of the DSCP is 0 to 63. The bigger the DSCP value is, the higher the priority is.

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

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

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

6.2.7 Configuring 802.1X Settings

Purpose:

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

Before you start:

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

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

Steps:

1. Enter the 802.1X Settings interface, **Configuration > Network > Advanced Settings > 802.1X**

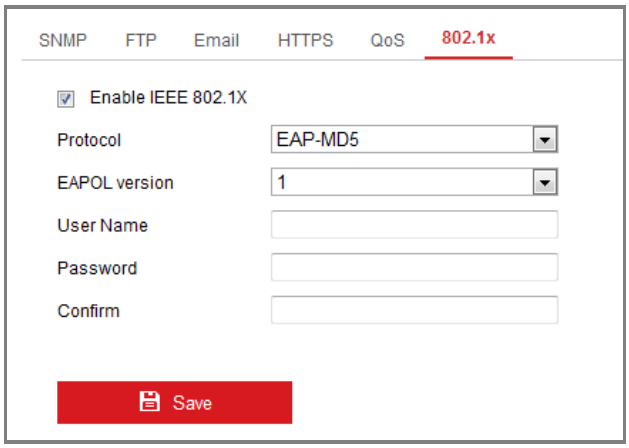


Figure 6-16 802.1X Settings

2. Check the **Enable IEEE 802.1X** checkbox to enable the feature.
3. Configure the 802.1X settings, including Protocol, EAPOL version, User Name, Password and Confirm.

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

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

6.2.8 Integration Protocol

Purpose:

If you need to access to the camera through the third party platform, you can enable CGI function. And if you need to access to the device through ONVIF protocol, you can configure ONVIF user in this interface. Refer to ONVIF standard for detailed configuration rules.

- **CGI**

  Check the Enable Hikvision_CGI checkbox and then select the authentication from the drop-down list.

  Note: Digest is the recommended authentication method.

- **ONVIF**

  Steps:

  1. Check the Enable ONVIF checkbox to enable the function.
  2. Add ONVIF users. Up to 32 users are allowed.

     Set the user name and password, and confirm the password. You can set the user as media user, operator, and administrator.

     Note: ONVIF user account is different from the camera user account. You have set ONVIF user account independently.
  3. Save the settings.

  Note: User settings of ONVIF are cleared when you restore the camera.

6.2.9 Configuring HTTP Listening

Purpose:

The camera can send alarm information to the destination IP or host name via HTTP protocol. If the network is disconnected, the data can be uploaded to the destination IP or host name after the network connection is normal.

Before you start:

The destination IP or host name should support the HTTP protocol to receive the alarm information.

Steps:

1. Enter the HTTP Listening interface, **Configuration > Network > Advanced Settings > Listening.**

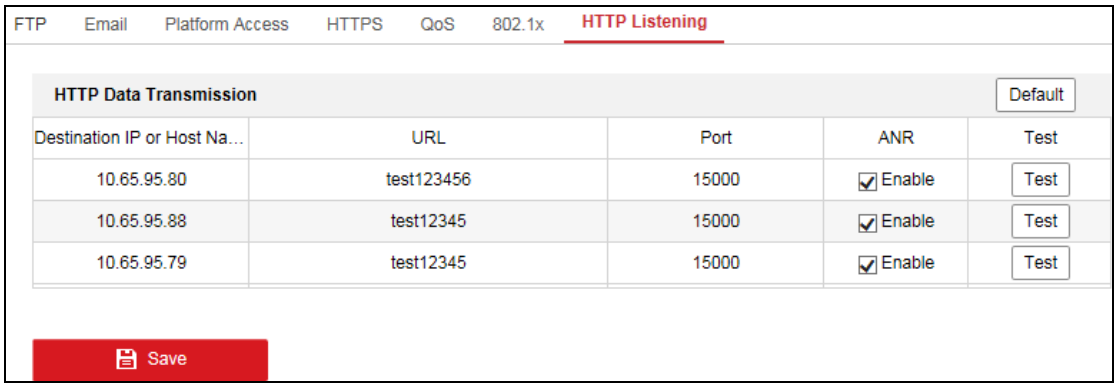


Figure 6-17 HTTP Listening

2. Enter the desired destination IP or host name, URL and port.
3. You can click **Test** to test whether the entered IP address or host name are valid.
4. Or you can click **Default** to reset the destination IP or host name.

Chapter 7Video/Audio Settings

Purpose:

Follow the instructions below to configure the video setting, audio settings, ROI, Display info. on Stream, etc.

7.1 Configuring Video Settings

For certain camera models, you can configure parameters for available video streams, for example, the main stream, the sub-stream, etc.

Steps:

1. Enter the Video Settings interface, **Configuration** > **Video/Audio** > **Video**

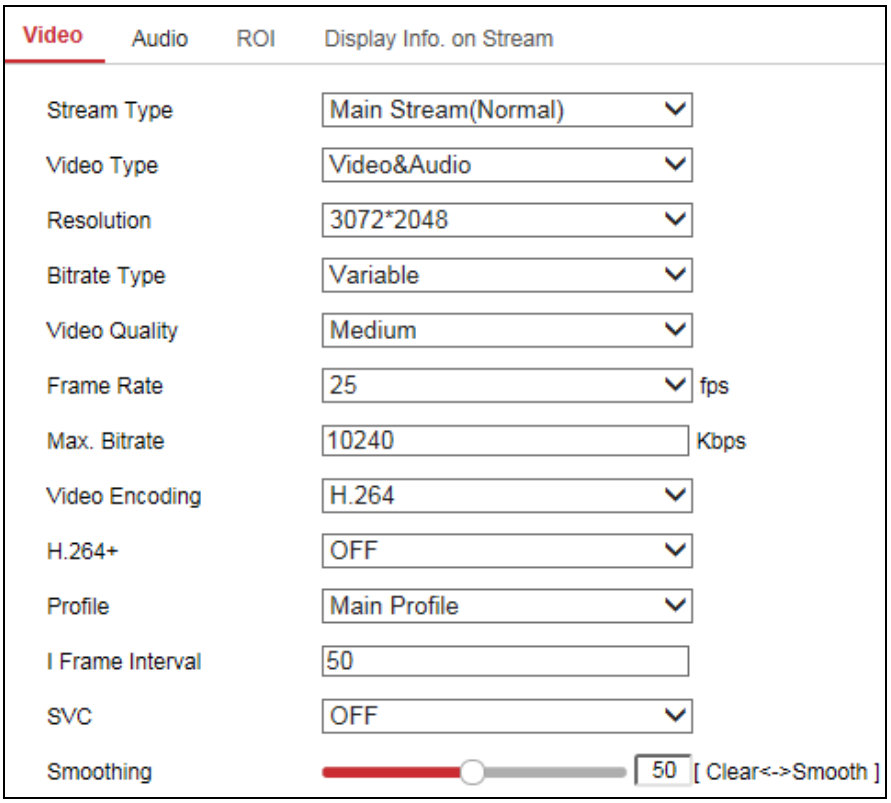


Figure 7-1 Video Settings

2. Select the Stream Type.

   Supported stream types are listed in the drop-down list.

   Notes:

   - For some models, the **Third Stream** is not enabled by default. Go to **System** >

Maintenance > System Service> Software to enable the function is required.

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

3. You can customize the following parameters for the selected stream type.

Video Type:

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

Resolution:

Select the resolution of the video output.

Bitrate Type:

Select the bitrate type to constant or variable.

Video Quality:

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

Frame Rate:

Set the frame rate. 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 from 32 to 16384 Kbps. The higher value corresponds to the higher video quality, but the better bandwidth is required.

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

Video Encoding:

The camera supports multiple video encodings types, such as H.264, H.265, MJPEG, and MPEG4. Supported encoding type for different stream types may differ. H.265 is a new encoding technology. Compared with H.264, it reduces the transmission bitrate under the same resolution, frame rate and image quality.

Note: Selectable video encoding types may vary according to different camera modes.

H.264+ and H.265+:

- **H.264+:** If you set the main stream as the stream type, and H.264 as the video encoding, you can see H.264+ available. H.264+ is an improved compression coding technology based on H.264. By enabling H.264+, users can estimate the HDD consumption by its maximum average bitrate. Compared to H.264, H.264+ reduces storage by up to 50% with the same maximum bitrate in most scenes.
- **H.265+:** If you set the main stream as the stream type, and H.265 as the video encoding, you can see H.265+ available. H.265+ is an improved compression coding technology based on H.265. By enabling H.265+, users can estimate the HDD consumption by its maximum average bitrate. Compared to H.265, H.265+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

You need to reboot the camera if you want to turn on or turn off the H.264+/H.265+. If you switch from H.264+ to H.265+ directly, and vice versa, a reboot is not required by the system.

Notes:

- Upgrade your video player to the latest version if live view or playback does not work properly due to compatibility.
- With H.264+/H.265+ enabled, the parameters such as profile, I frame interval, video quality, and SVC are greyed out.
- With H.264+/H.265+ enabled, some functions are not supported. For those functions, corresponding interfaces will be hidden.
- H.264+/H.265+ can spontaneously adjust the bitrate distribution according the requirements of the actual scene in order to realize the set maximum average bitrate in the long term. The camera needs at least 24 hours to adapt to a fixed monitoring scene.

Max. Average Bitrate:

When you set a maximum bitrate, its corresponding recommended maximum average bitrate will be shown in the Max. Average Bitrate box. You can also set the maximum average bitrate manually from 32 Kbps to the value of the set maximum bitrate.

Profile:

When you select H.264 or H.265 as video encoding, you can set the profile. Selectable profiles vary according to camera models.

I Frame Interval:

Set I Frame Interval from 1 to 400.

SVC:

Scalable Video Coding is an extension of the H.264/AVC and H.265 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 is, the better fluency of the stream will be, though, the video quality may not be so satisfactory. The lower value of the smoothing is, the higher quality of the stream will be, though it may appear not fluent.

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

Note:

The video parameters vary according to different camera models. Refer to the actual display page for camera functions.

7.2 Configuring Audio Settings

Steps:

1. Enter the Audio Settings interface: **Configuration > Video/Audio > Audio**.

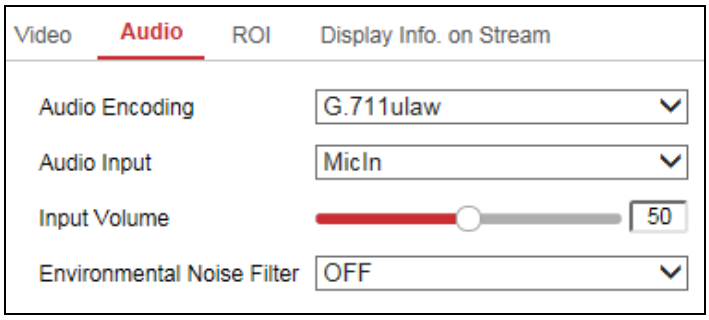


Figure 7-2 Audio Settings

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, PCM and MP3 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 adjustable.

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

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

7.3 Configuring ROI Encoding

Purpose:

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

Note: ROI function varies according to different camera models.

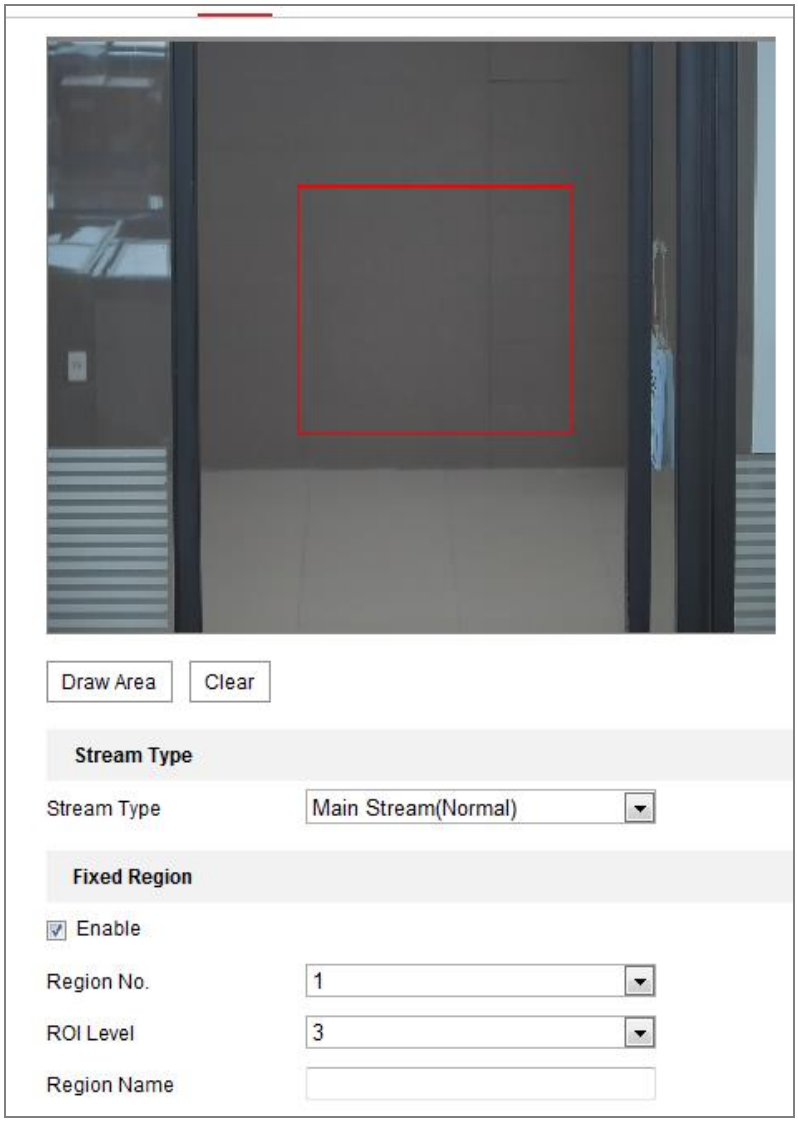


Figure 7-3 Region of Interest Settings

Steps:

1. Enter the ROI settings interface: **Configuration > Video/Audio > ROI**.
2. Select the Stream Type for ROI encoding.
3. Check the checkbox of **Enable** under Fixed Region item.
4. Set **Fixed Region** for ROI.
   (1) Select the Region No. from the drop-down list.
   (2) Check the **Enable** checkbox to enable ROI function for the chosen region.
   (3) Click **Drawing**. Click and drag the mouse on the view screen to draw a red rectangle as the ROI region. You can click **Clear** to cancel former drawing. Click **Stop Drawing** when you finish.

(4) Select the ROI level.

(5) Enter a region name for the chosen region.

(6) Click **Save** the save the settings of ROI settings for chosen fixed region.

(7) Repeat steps (1) to (6) to setup other fixed regions.

7.4 Display Info. on Stream

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

Figure 7-4 Display Info. on Stream

Chapter 8 Configuring Image Parameters

8.1 Configuring Display Settings

Purpose:

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

Steps:

1. Enter the Display Settings interface:

   Configuration > Image> Display Settings

2. Set the image parameters of the camera.

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

Day/Night Auto-switch

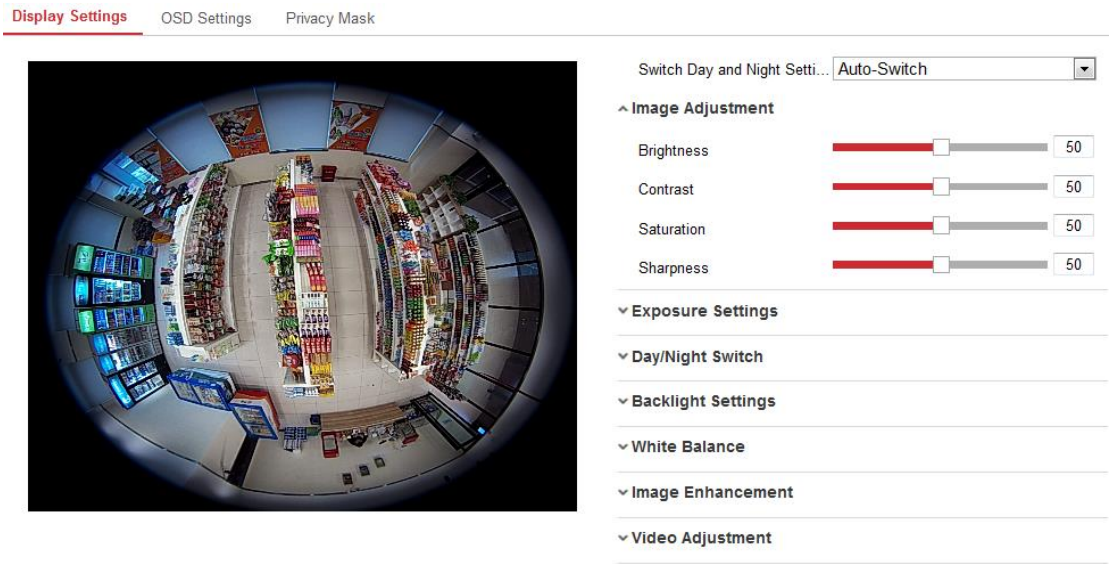


Figure 8-1 Display Settings of Day/night Auto-switch

- **Image Adjustment**

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

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

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

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

- **Exposure Settings**

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

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

Exposure Time: It refers to the electronic shutter time, which ranges from 1/3 to 1/100,000s. Adjust it according to the actual luminance condition.

Gain: Gain of the image can also be manually configured from 0 to 100. The bigger the value is, the brighter would the image be, and the noise would also be amplified to a larger extent.

- **Day/Night Switch**

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

Day: the camera stays at day mode.

Night: the camera stays at night mode.

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

Schedule: The camera switches between the day mode and the night mode according to the configured time period.

Triggered by Alarm Input: The camera switches to the day mode or the night mode after the alarm is triggered.

Smart Supplement Light: Smart Supplement Light function gives user an option to adjust the power of the IR LED, thus avoiding image over-exposure.

When the light is turned on, and Auto and Manual are selectable for IR mode.

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

Select Manual, and you can adjust the IR LED by adjusting the distance. The higher the value is, the higher the power of the light would be, and it can reach objects farther away.

- **Backlight Settings**

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

  WDR: Wide Dynamic Range can be used when there is a high contrast of the bright area and the dark area of the scene. The wide dynamic level can be adjusted from 0 to 100.

- **White Balance**

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

- **Image Enhancement**

  Digital Noise Reduction: DNR reduces the noise in the video stream. OFF, Normal Mode and Expert Mode are selectable. Under normal mode, set the DNR level from 0 to 100, and the default value is 50. Under expert mode, you can set Space DNR Level and Time DNR Level separately.

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

- **Video Adjustment**

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

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

Day/Night Scheduled Switch

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

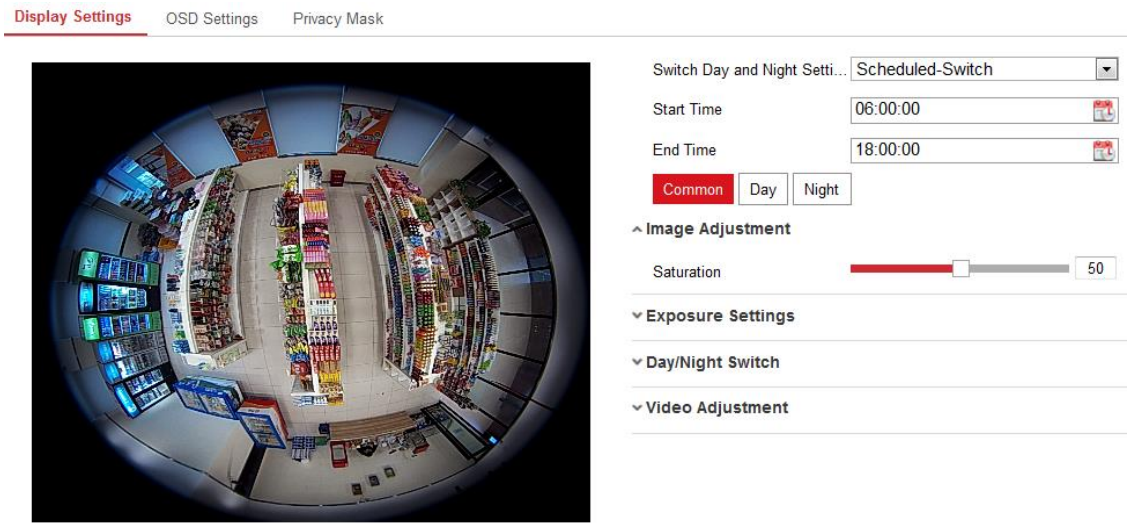


Figure 8-2 Day/Night Scheduled-Switch Setting

Steps:

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

   Note: For the detailed information of each parameter, please refer to the description in *Day/Night Auto-Switch*.
3) Click Day tab to configure the parameters applicable for day mode.
4) Click Night tab to configure the parameters applicable for night mode.

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

8.2 Configuring OSD Settings

Purpose:

OSD (On-screen Display) refers to the camera name, time/date format, display mode, and OSD size displayed on the live view.

Steps:

1. Enter the OSD Settings interface: **Configuration > Image > OSD Settings**

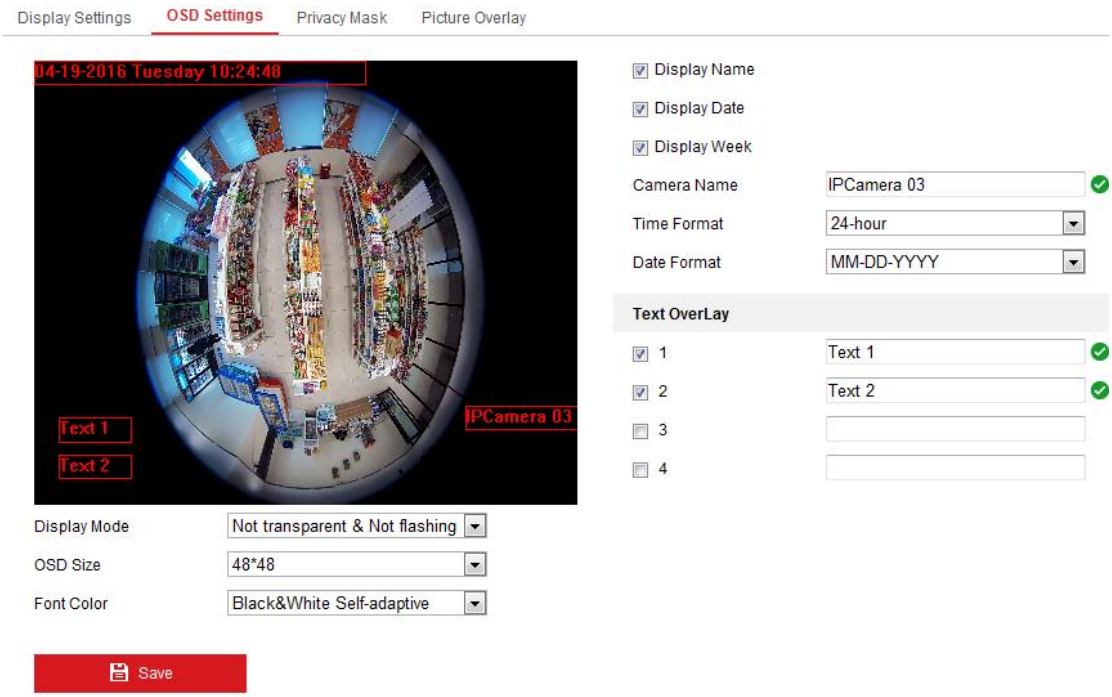


Figure 8-3 OSD Settings

2. Select a camera channel to configure.
3. Check the corresponding checkbox to select the display of camera name, date or week if required.
4. Edit the camera name in the text field of Camera Name.
5. Select from the drop-down list to set the time format, date format, display mode and the OSD font size.
6. Set overlaid text if needed.
   1) Check the checkbox on the left to enable the on-screen display.
   2) Input the desired information in the textbox.

   Notes:

- Up to 8 texts are configurable.
- Text overlay is only supported when the live view stream is decoded by hardware and display mode is Fisheye View.

7. Adjust the position and alignment of text frames.

   Left align, right align and custom are selectable. If you select custom, you can use the mouse to click and drag text frames in the live view window to adjust their positions.

   Note: The alignment adjustment is only applicable to Text Overlay items.

8. (Optional) Click **Copy to** to copy the parameters of set camera channels to other channels.
9. Click **Save** to save the settings.

8.3 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.

Note: Privacy Mask function may not be supported by certain display modes, refer to the actual interface for detailed information.

Steps:

1. Enter the Privacy Mask Settings interface:

   Configuration > Image > Privacy Mask

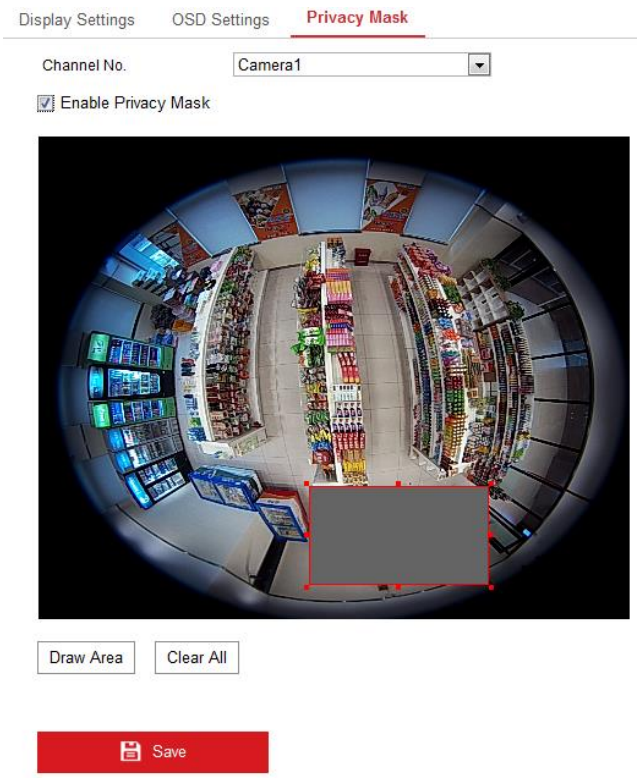


Figure 8-4 Privacy Mask Settings

2. Select a camera channel to configure.
3. Check the checkbox of **Enable Privacy Mask** to enable this function.
4. Click the **Draw Area** button to start drawing.
5. Click-and-drag the mouse in the live video window to draw the mask area.
6. Click **Stop Drawing** to finish drawing.
7. You can click **Clear All** to clear all the configured privacy masks.
8. Click **Save** to save the settings.

Note: Up to 4 privacy masks are configurable.

8.4 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.

Steps:

1. Enter the Picture Overlay Settings interface, **Configuration** > **Image** > **Picture**

Overlay.

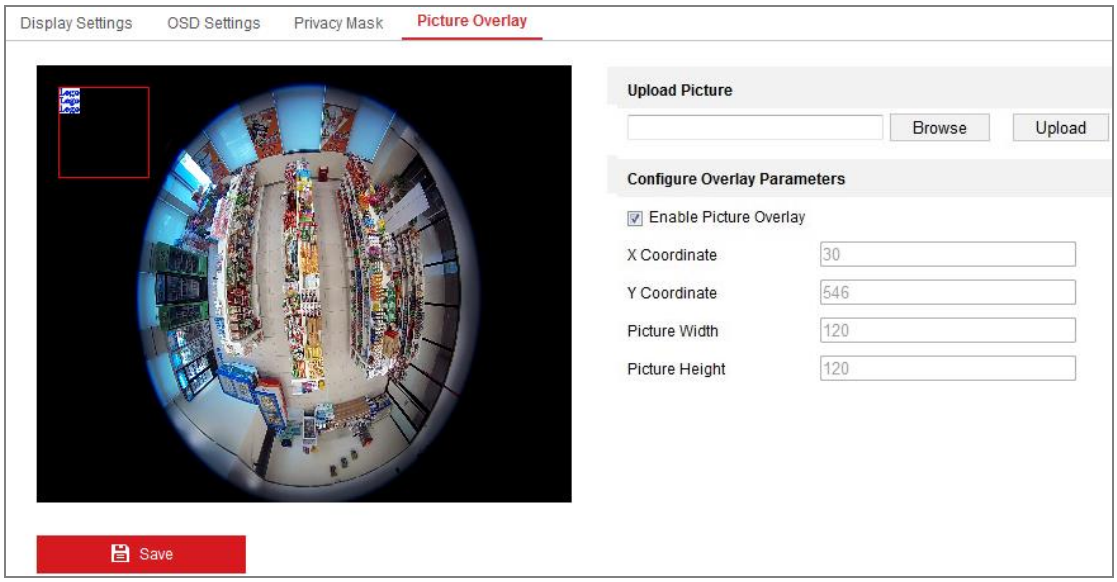


Figure 8-5 Picture Overlay

2. Click **Browse** to select a picture.
3. Click **Upload** to upload it.
4. Check **Enable Picture Overlay** checkbox to enable the function.
5. Drag the red rectangle to adjust the position.
6. Click **Save** to save settings.

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

Chapter 9 Configuring Event Settings

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

Note: Check the checkbox of **Notify Surveillance Center** if you want to push the alarm information to the surveillance client such as the mobile phone, computer, etc., as soon as the alarm is triggered.

9.1 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.

Note: Motion Detection is not supported when the decoding mode is hardware decoding and the display mode is 4PTZ.

- **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 > Event > Basic Event > Motion Detection

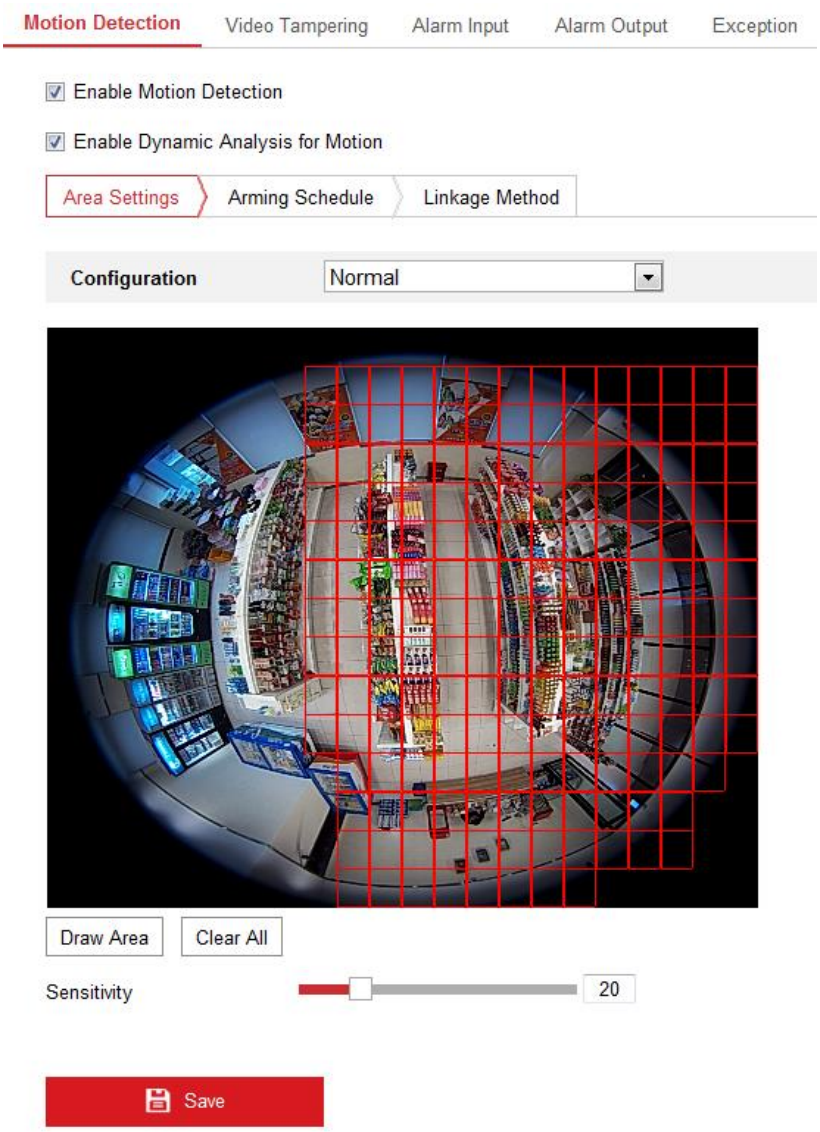


Figure 9-1 Motion Detection Settings

2. Check the checkbox of **Enable Motion Detection**.
3. (Optional) Check the checkbox of **Enable Dynamic Analysis for Motion** if you want to mark the detected objects with green rectangles on the live view window.

   Note: You can go to **Configuration > Local Configuration > Live View Parameters**, and then select Disable for **Rules** if you don't want the detected objected displayed with the rectangles.
4. Click **Draw Area**. Click and drag the mouse on the live video to draw a motion detection area. Click **Stop Drawing** to finish drawing one area.
5. (Optional) Click **Clear All** to clear all of the areas.

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

Task 2: Set the Arming Schedule for Motion Detection

Steps:

1. Click **Arming Schedule** to edit the arming schedule.

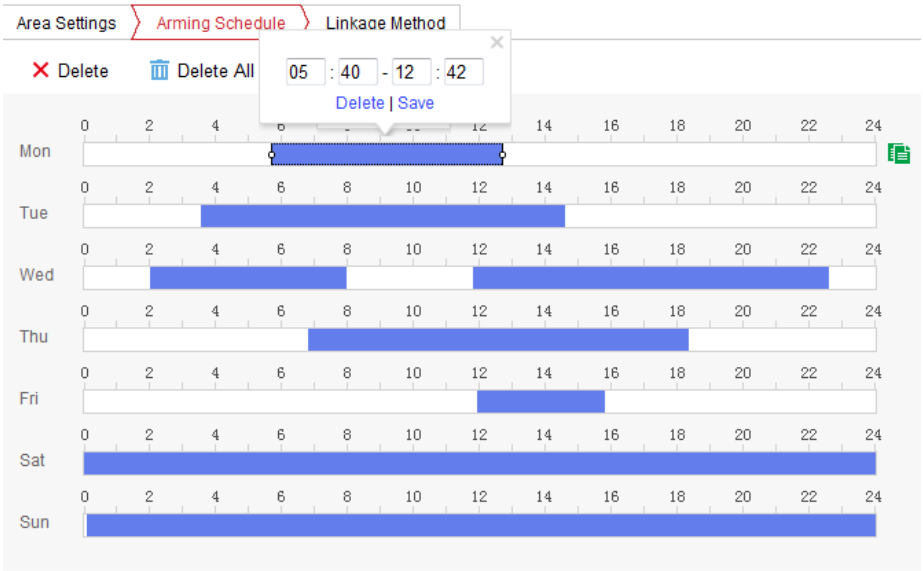


Figure 9-2 Arming Schedule Setting

2. Click on the time bar and drag the mouse to select the time period.

   Note: Click on the selected time period, you can adjust the time period to the desired time by either moving the time bar or input the exact time period.

3. (Optional) Click **Delete** to delete the current arming schedule, or click **Save** to save the settings.
4. Move the mouse to end of each day, a green copy icon appears. You can click the icon to copy the current time schedule to other days.
5. Click **Save** to save the settings.

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

Task 3: Set the Linkage Method for Motion Detection

Click Linkage Method and check the checkbox to select the linkage method. audible warning, notify surveillance center, send email, upload to FTP/Memory Card/NAS, trigger channel, trigger alarm output, and smart tracking are selectable. You can specify the linkage method when an event occurs.

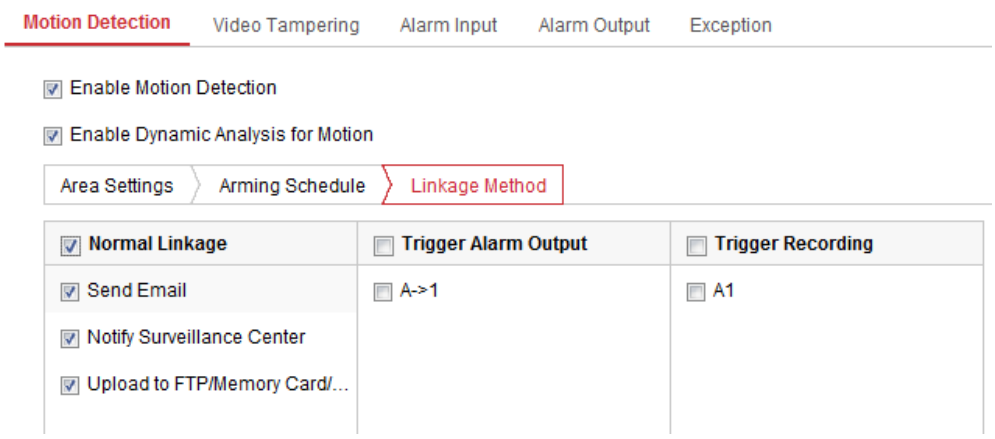


Figure 9-3 Linkage Method Settings

- **Audible Warning**

  Trigger the audible warning locally. And it only supported by the device that has 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, please refer to *Section 5.3.8* to complete Email setup in advance.

- **Upload to FTP/Memory Card/NAS:** Capture the image when an alarm is triggered and upload the picture to the configured FTP server, memory card and NAS.

  Notes:

  - Set the FTP address and the remote FTP server first. Refer to *Section 5.3.7 Configuring FTP Settings* for detailed information.
  - The captured image can also be uploaded to the available memory card or network disk (NAS). Go to **Configuration** > **Storage** > **Storage Management to** set the memory card and NAS.
  - Go to **Configuration** > **Storage** > **Schedule Settings** > **Capture** > **Capture Parameters** page, enable the event-triggered snapshot, and set the capture interval and capture number.

- **Smart Tracking:** It can make the speed dome to track target manually by clicking the target on the live view of fisheye camera.

  Note: In order to make smart tracking take effect, you need to have a speed dome which has auto tracking function installed near your fisheye camera, and you have to configure relevant settings on 4200 Client Software. Refer to the user manual of 4200 Client Software for detailed information.

- **Trigger Channel:** The video will be recorded when the motion is detected. You have to set the recording schedule first.

- **Trigger Alarm Output:** Trigger one or more external alarm outputs when an event occurs.

  Note: Go to Advanced Configuration > Basic Event > Alarm Output page, set the arming schedule of the alarm output.

Expert Mode

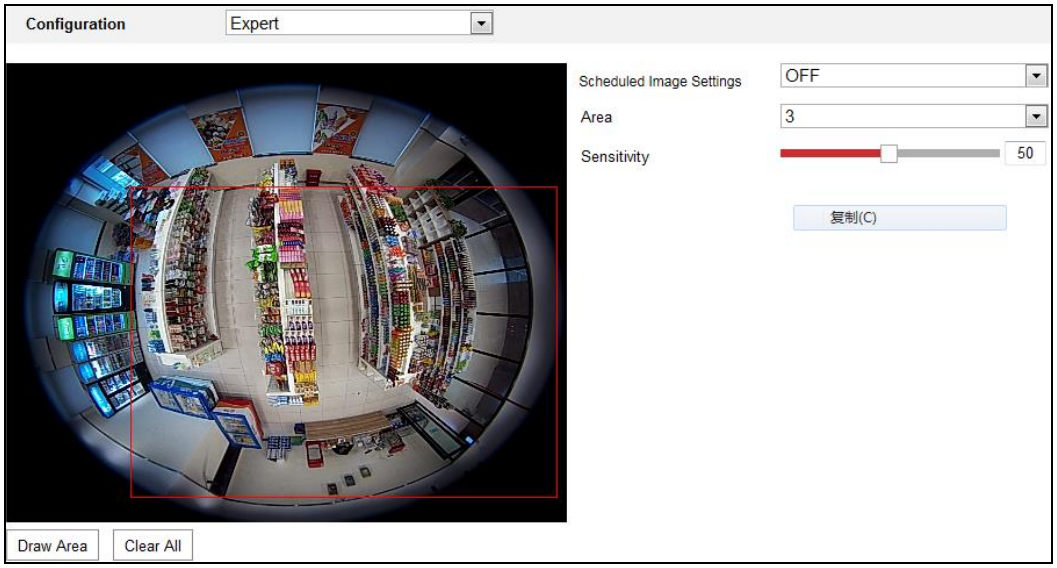


Figure 9-4 Motion Detection Settings-Expert Mode

If Expert is selected as the configuration mode, different sets of parameters are adopted for motion detection at day and night.

- Day/Night Switch OFF

  Steps:

  (1) Draw the detection area as in the normal configuration mode. The

supported area number varies according to different camera models.

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

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

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

Sensitivity: The greater the value is, the easier the alarm will be triggered.

Percentage: When the size of the moving object exceeds the set percentage of the predefined area, the alarm will be triggered. The smaller the percentage is, the easier the alarm will be triggered.

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

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

- Day/Night Auto-Switch

Steps:

(1) Draw the detection area as in the normal configuration mode. The supported area varies according to the different camera models.

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

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

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

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

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

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

- Day/Night Scheduled-Switch

Steps:

(1) Draw the detection area as in the normal configuration mode. The supported area number varies according to different camera models.

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

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

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

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

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

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

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

9.2 Configuring Video Tampering Alarm

Purpose:

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

Note: Video Tampering Detection is not supported when the decoding mode is hardware decoding and the display mode is 180 Panorama View or 4PTZ.

Steps:

1. Enter the Tamper-proof Settings interface:

   Configuration > Event > Basic Event > Video Tampering

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

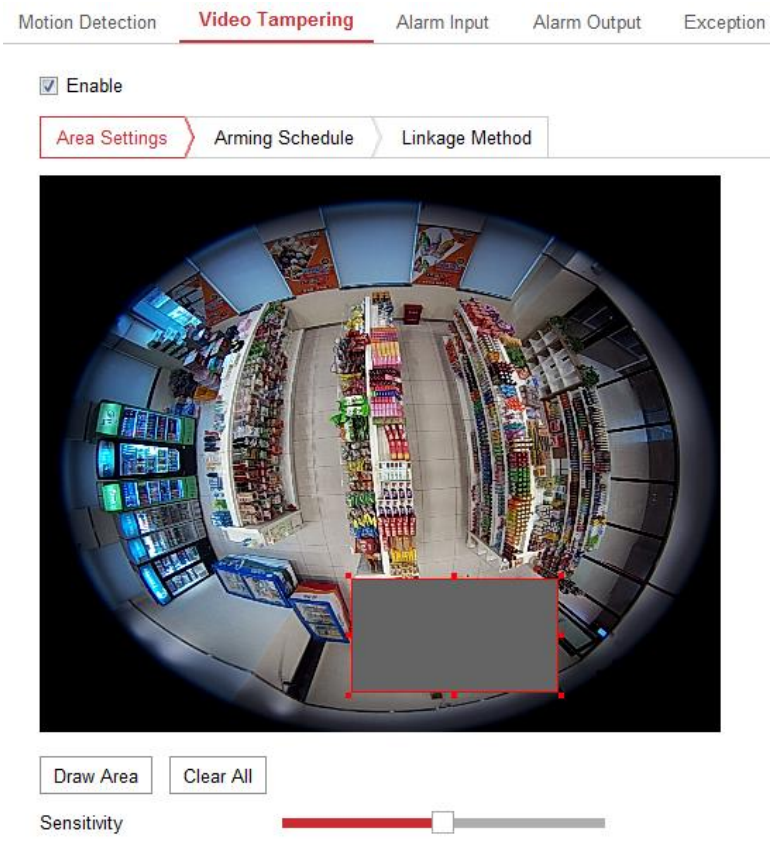


Figure 9-5 Video Tampering Detection Settings

3. Draw the detection area as in the normal configuration mode.
4. Move the slider to set the sensitivity.
5. Click **Arming Schedule** to set arming schedule as that in *Task 2 Set the Arming Schedule for Motion Detection in Section 5.6.1*.
6. Click **Linkage Method** to set linkage method as that in *Task 3 Set the Linkage Method for Motion Detection in Section 5.6.1*.
7. Click **Save** to save the settings.

9.3 Configuring Alarm Input

Steps:

1. Enter the Alarm Input Settings interface:

   Configuration > Events > Basic Event > Alarm Input

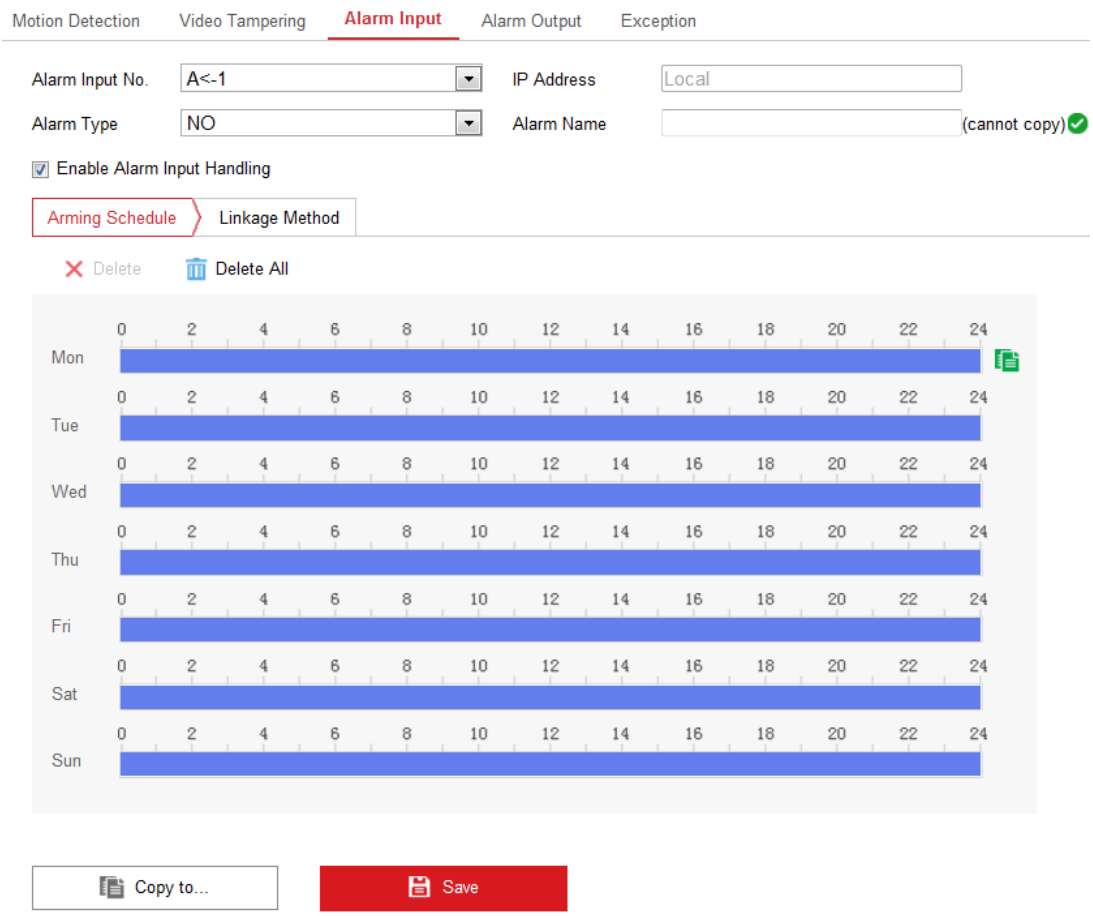


Figure 9-6 Alarm Input Settings

2. Choose the alarm input No. and the Alarm Type. The alarm type can be NO (Normally Open) and NC (Normally Closed). Edit the alarm name (optional).
3. Check the checkbox of Enable Alarm Input Handling to enable the function.
4. Set the arming schedule. Refer to *Task 2: Set Arming Schedule for Motion Detection in Section 5.6.1.*
5. Set the linkage method. Refer to *Task 3: Set Linkage Method for Motion Detection in Section 5.6.1.*
6. (Optional) You can copy your settings to other alarm inputs.
7. Click **Save** to save the settings.

Note: Alarm input settings vary according to the camera model.

9.4 Configuring Alarm Output

Steps:

1. Enter the Alarm Output Settings interface:

   Configuration > Events > Basic Event > Alarm Output

2. Select one alarm output channel in the Alarm Output drop-down list.
3. (Optional) Input the alarm output name in the text field.
4. 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.
5. Set the arming schedule. Refer to *Task 2: Set Arming Schedule for Motion Detection in Section 5.6.1*.
6. (Optional) You can copy the settings to other alarm outputs.
7. Click Manual Alarm to trigger an alarm manually. Click Clear Alarm to cancel the alarm.
8. Click **Save** to save the settings.

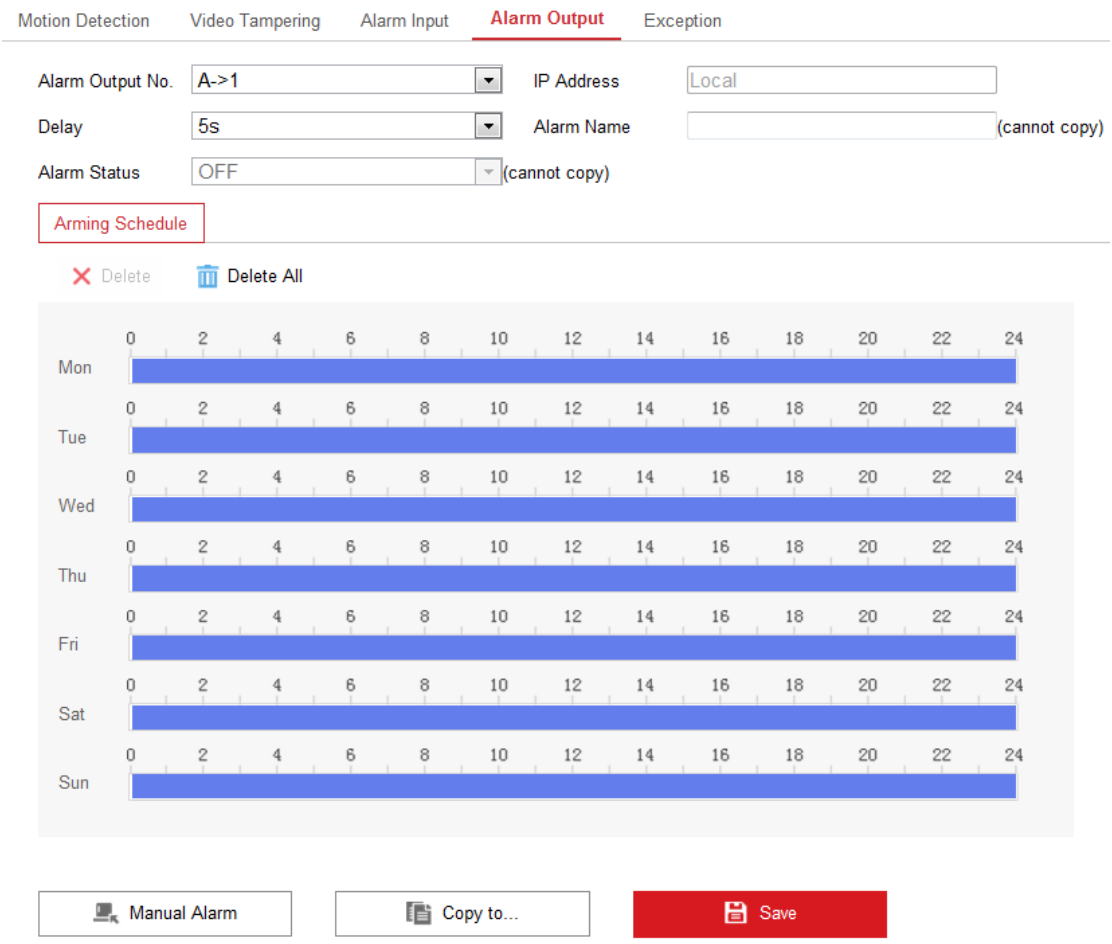


Figure 9-7 Alarm Output Settings

Note: Alarm output settings vary according to the camera model.

9.5 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 > Event > Basic Event > Exception

2. Check the checkbox to select the linkage method taken for exception. For details, refer to *Task 3: Set Linkage Method for Motion Detection* in *Section 5.6.1*.

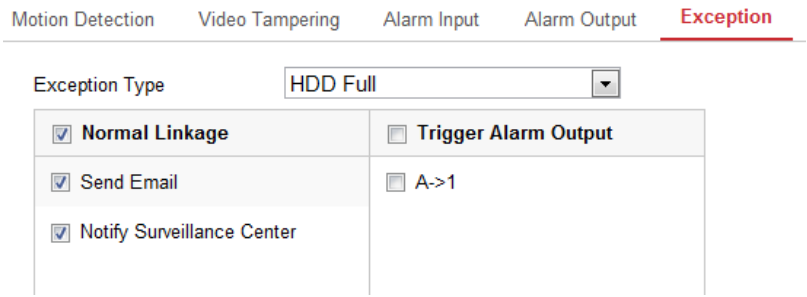


Figure 9-8 Exception Settings

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

9.6 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 > Event > Smart Event > Audio Exception Detection**.

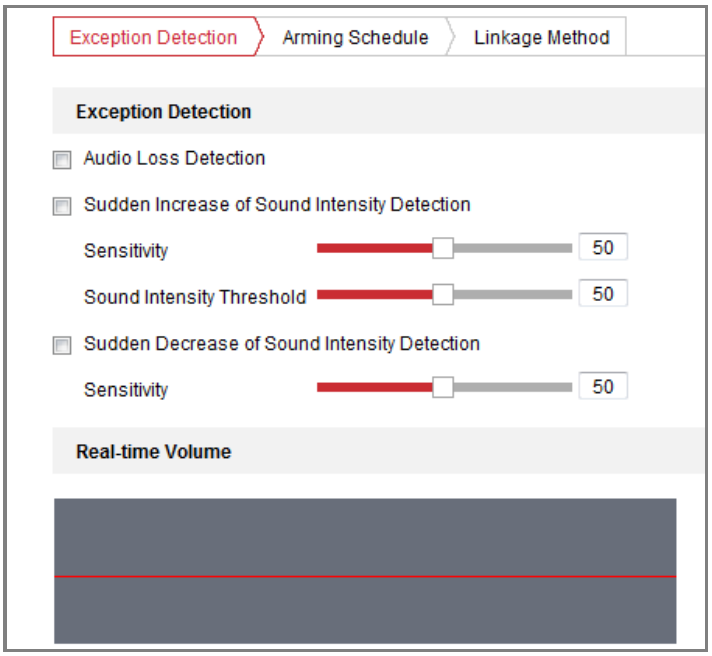


Figure 9-9 Audio Exception Detection

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.
   - You can view the real-time volume of the sound on the interface.
5. Click **Arming Schedule** to set the arming schedule. Refer to ***Task 2 Set the Arming Schedule for Motion Detection*** in *Section 9.1* for detailed steps.
6. Click **Linkage Method** and select the linkage methods for audio exception,

including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel for recording and Trigger Alarm Output.

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

9.7 Configuring Intrusion Detection

Purpose:

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

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

Steps:

1. Enter the Intrusion Detection settings interface, **Configuration> Event > Smart Event > Intrusion Detection**.

Figure 9-10 Intrusion Detection

2. Check the checkbox of **Enable** to enable the function.
3. Select a region number from the drop-down list of **Region**.

   Region: A pre-defined vertexes area on the live view image. Targets, such as, people, vehicle or other objects, who enter and loiter in the region will be detected and trigger the set alarm.
4. Click **Area Settings** tab and click **Draw Area** button to start the region drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Set the Max. Size and Min. Size for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

   Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.

   Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
7. Click **Stop Drawing** when finish drawing.
8. Set the time threshold for intrusion detection.

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

   Sensitivity: Range [1-100]. Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region.

   Sensitivity = $100 – S_1/S_T*100$

   S_1 stands for the target body part that goes across the pre-defined region. S_T stands for the complete target body.

   Example: if you set the value as 60, the action can be counted as an intrusion only when 40 percent body part enters the region.

   Note: The **Sensitivity** of the detection is supported by certain models. Refer to actual display for details.

10. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
11. Click **Arming Schedule** to set the arming schedule.
12. Click **Linkage Method** to select the linkage methods for intrusion detection, including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel and Trigger Alarm Output.
13. Click **Save** to save the settings.

9.8 Configuring Line Crossing Detection

Purpose:

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

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

Steps:

1. Enter the Line Crossing Detection settings interface, **Configuration > Event > Smart Event > Line Crossing Detection**.

Figure 9-11 Line Crossing Detection

2. Check the checkbox of **Enable** to enable the function.
3. Select the line from the drop-down list.
4. Click **Area Settings** tab and click **Draw Area** button, and a virtual line is displayed on the live video.
5. Drag the line, and you can locate it on the live video as desired. Click on the line, two red squares are displayed on each end, and you can click-and-drag one of the red squares to define the shape and length of the line.
6. Set the Max. Size and Min. Size for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

   Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.

   Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
7. Select the direction for line crossing detection. And you can select the directions

as A<->B, A ->B, and B->A.

A<->B: The object going across the plane with both directions can be detected and alarms are triggered.

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

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

8. Click **Stop Drawing** when finish drawing.
9. Drag the slider to set the sensitivity value.

   Sensitivity: Range [1-100]. It stands for the percentage of the body part of an acceptable target that goes across the pre-defined line.

   Sensitivity = $100 - S_1/S_T*100$

   S_1 stands for the target body part that goes across the pre-defined line. S_T stands for the complete target body.

   Example: if you set the value as 60, the action can be counted as a line crossing action only when 40 percent or more body part goes across the line.

   Note: The **Sensitivity** of the detection is supported by certain models. Refer to actual display for details.
10. Repeat the above steps to configure other lines. Up to 4 lines can be set. You can click the **Clear** button to clear all pre-defined lines.
11. Click the **Arming Schedule** to set the arming schedule.
12. Select the linkage methods for line crossing detection, including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel and Trigger Alarm Output.
13. Click **Save** to save the settings.

9.9 Configuring Region Entrance Detection

Purpose:

Region entrance detection function detects people, vehicle or other objects which

enter a pre-defined virtual region from the outside place, and some certain actions can be taken when the alarm is triggered.

Steps:

1. Enter the Region Entrance Detection settings interface, **Configuration > Event > Smart Event > Region Entrance Detection**.

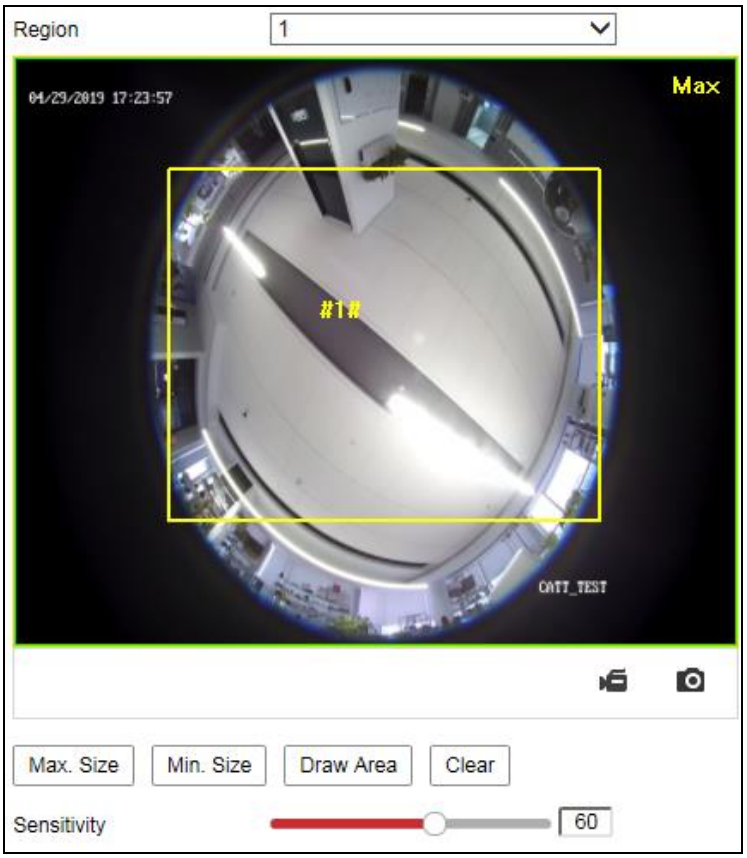


Figure 9-12 Region Entrance Detection

2. Check the **Enable** checkbox to enable the function.
3. Select the **Region** from the drop-down list for detection settings.
4. Click **Area Settings** and click **Draw Area** button to start the area drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Set the Max. Size and Min. Size for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

   Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.

Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.

7. Click **Stop Drawing** when finish drawing.
8. Drag the slider to set the sensitivity value.

   Sensitivity: Range [1-100]. Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region.

   Sensitivity = $100 – S_1/S_T*100$

   S_1 stands for the target body part that enters the pre-defined region S_T stands for the complete target body.

   Example: if you set the value as 60, the action can be counted as a region entrance action only when 40 percent body part enters the region.

   Note: The **Sensitivity** of the detection is supported by certain models. Refer to actual display for details.
9. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
10. Click **Arming Schedule** to set the arming schedule.
11. Click **Linkage Method** to select the linkage methods.
12. Click **Save** to save the settings.

9.10 Configuring Region Exiting Detection

Purpose:

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

Steps:

1. Enter the Region Exiting Detection settings interface, **Configuration** > **Event** > **Smart Event** > **Region Exiting Detection**.

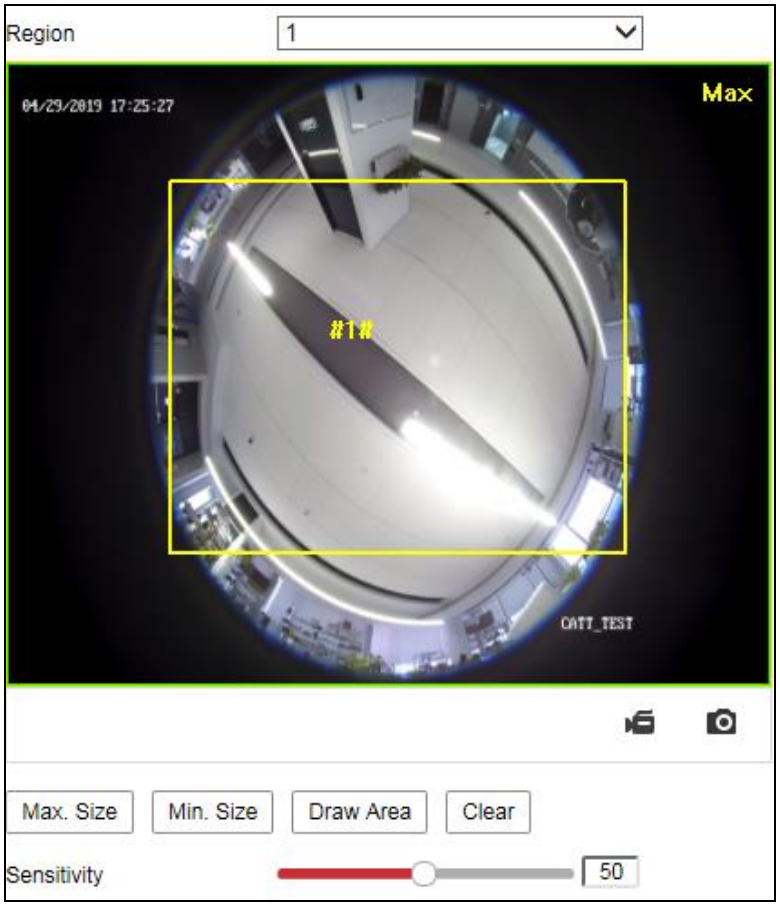


Figure 9-13 Region Exiting Detection

2. Check **Enable** checkbox to enable the function.
3. Select the **Region** from the drop-down list for detection settings.
4. Click **Area Settings** and click **Draw Area** button to start the area drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Set the Max. Size and Min. Size for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

   Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.

   Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
7. Click **Stop Drawing** when finish drawing.
8. Drag the slider to set the sensitivity value.

   Sensitivity: Range [1-100]. Sensitivity stands for the percentage of the body part

of an acceptable target that exits the pre-defined region.

Sensitivity = 100 – S_1/S_T*100

S_1 stands for the target body part that exits the pre-defined region. S_T stands for the complete target body.

Example: if you set the value as 60, the action can be counted as a region exiting action only when 40 percent body part exits the region.

Note: The **Sensitivity** of the detection is supported by certain models. Refer to actual display for details.

9. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
10. Click **Arming Schedule** to set the arming schedule.
11. Click **Linkage Method** to select the linkage methods.
12. Click **Save** to save the settings.

9.11 Configuring Unattended Baggage Detection

Purpose:

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

Steps:

1. Enter the Unattended Baggage Detection settings interface, **Configuration > Event > Smart Event > Unattended Baggage Detection**.

Figure 9-14 Unattended Baggage Detection

2. Check **Enable** checkbox to enable the function.
3. Select the **Region** from the drop-down list for detection settings.
4. Click **Area Settings** and click **Draw Area** to start the area drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Set the Max. Size and Min. Size for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

   Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.

   Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
7. Click **Stop Drawing** when finish drawing.
8. Set the time threshold and detection sensitivity for unattended baggage detection.

Threshold: Range [5-100s], the threshold for the time of the objects left over in the region. If you set the value as 10, alarm is triggered after the object is left and stay in the region for 10s.

9. Drag the slider to set the sensitivity value.

   Sensitivity: Range [1-100]. Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region.

   Sensitivity = $100 – S_1/S_T*100$

   S_1 stands for target body part that enters the pre-defined region. S_T stands for the complete target body.

   Example: if you set the value as 60, a target is possible to be counted as an unattended baggage only when 40 percent body part of the target enters the region.

   Note: The **Sensitivity** of the detection is supported by certain models. Refer to actual display for details.

10. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
11. Click **Arming Schedule** to set the arming schedule.
12. Click **Linkage Method** to select the linkage methods.
13. Click **Save** to save the settings.

9.12 Configuring Object Removal Detection

Purpose:

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

Steps:

1. Enter the Object Removal Detection settings interface, **Configuration > Event > Smart Event > Object Removal Detection**.

Figure 9-15 Object Removal Detection

2. Check **Enable** checkbox to enable the function.
3. Select the **Region** from the drop-down list for detection settings.
4. Click **Area Settings** and click **Draw Area** button to start the area drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Set the Max. Size and Min. Size for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

   Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.

   Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
7. Click **Stop Drawing** when finish drawing.
8. Set the time threshold for object removal detection.

Threshold: Range [5-100s], the threshold for the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object disappears from the region for 10s.

9. Drag the slider to set the sensitivity value.

   Sensitivity: Range [1-100]. It stands for the percentage of the body part of an acceptable target that leaves the pre-defined region.

   Sensitivity = $100 - S_1/S_T*100$

   S_1 stands for the target body part that leaves the pre-defined region. S_T stands for the complete target body.

   Example: if you set the value as 60, a target is possible to be counted as a removed object only when 40 percent body part of the target leaves the region.

   Note: The **Sensitivity** of the detection is supported by certain models. Refer to actual display for details.

10. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
11. Click **Arming Schedule** to set the arming schedule.
12. Click **Linkage Method** to select the linkage methods.
13. Click **Save** to save the settings.

Chapter 10Storage Settings

10.1 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 > Storage > Schedule Settings > Record Schedule

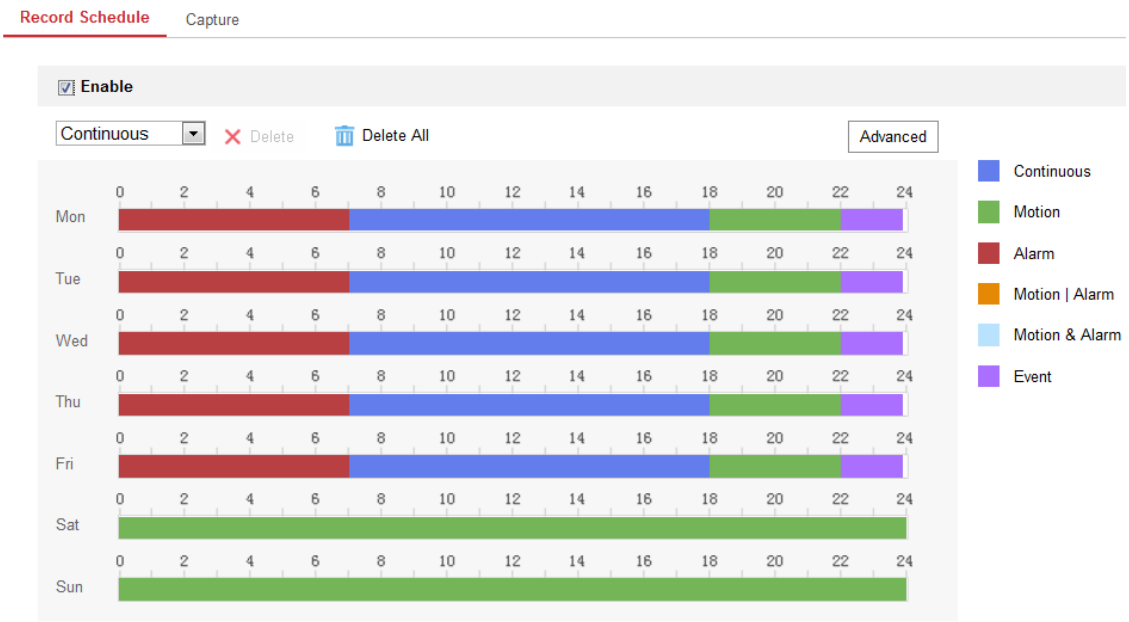


Figure 10-1 Recording Schedule Interface

2. Check the checkbox of **Enable** to enable scheduled recording.
3. Click **Advanced** to set the camera record parameters, including overwrite, pre-record, post-record and stream type.

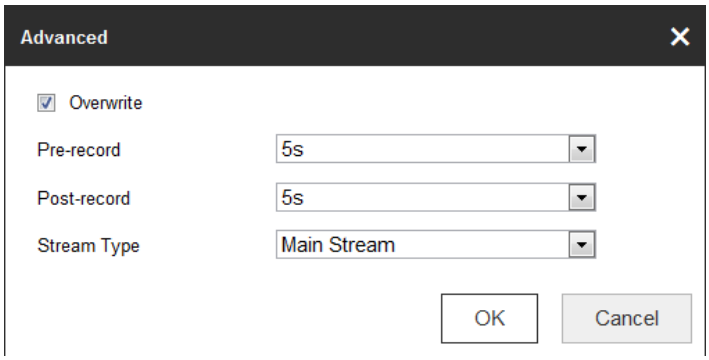


Figure 10-2 Record Parameters

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.

Overwrite: Check the checkbox of **Overwrite**, and then the data will be overwritten when HDD or network disk becomes full. If you uncheck it, the recording will stop when HDD or network disk becomes full.

Note:

The local storage (SD card/micro SD card) doesn't support overwrite function.

Recording Stream: Set the stream type for recording. Main Stream and Sub Stream are selectable.

4. Select record type from the drop-down list. Continuous, Motion, Alarm, Motion | Alarm, Motion & Alarm, and Event are selectable.

   ♦ **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**, 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 *Section 5.6.1 Configuring Motion Detection.*

- **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 Configuring Alarm Input*.

- **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 Line Crossing Detection**

  If you select **Line Crossing Detection**, the video will be recorded when the line crossing event is detected.

  Besides configuring the recording schedule, you have to set the detection line

and check the checkbox of **Trigger Channel** in the **Linkage Method** of Line Crossing Detection Settings interface. For detailed information, please refer to *Section 5.6.6 Configuring Line Crossing Detection.*

- **Record Triggered by Intrusion Detection**

  If you select **Intrusion Detection**, the video will be recorded when the intrusion event is detected.

  Besides configuring the recording schedule, you have to set the intrusion detection area and check the checkbox of **Trigger Channel** in the **Linkage Method** of Intrusion Detection Settings interface. For detailed information, please refer to *Section 5.6.7 Configuring Intrusion Detection.*

- **Record Triggered by Event**

  If you select **Event**, the video will be recorded when **Line Crossing Detection** or **Intrusion Detection** is triggered.

  Besides configuring the recording schedule, you have to set the Line Crossing Detection and Intrusion Detection and check the checkbox of **Trigger Channel** in the Linkage Method. Refer to *Section 5.6.6* and S*ection 5.6.7* for detailed information.

5. Click and drag the mouse on the time bar to set the record schedule. Up to 8 time segments can be set for each day.
6. Click the time segment, you can change the record type and edit the start and stop time of the time segment.

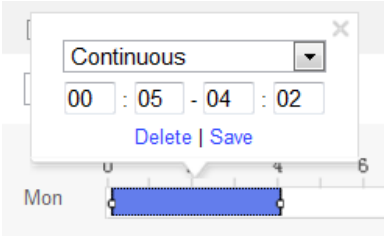


Figure 10-3 Editing Time Schedule

7. Click  and copy the time schedule to other days as desired.
8. Click **Save** to save the settings.

10.2 Configuring Capture Setting

Purpose:

You can configure the scheduled capture and event-triggered capture. The captured picture can be stored in the SD card (if supported) or in the network disk (For details, please refer to *Section 6.3* ***Configuring Net HDD***). The captured pictures can also be uploaded to a FTP server.

Steps:

1. Enter **Capture** setting interface: **Configuration > Storage > Schedule Setting**
2. Go to **Capture Schedule** tab to configure the capture schedule by click-and-drag the mouse on the time bar.

Figure 10-4 Capture Schedule Setting

3. Click **Save** to save the settings.
4. Go to **Capture Parameters** tab to configure the capture parameters.
   (1) Check the **Enable Timing Snapshot** checkbox to enable continuous capture.
   (2) Select the picture format, resolution, quality and capture interval.
   (3) Check the **Enable Event-triggered Snapshot** checkbox to enable event-triggered capture.

   Note: Select **Upload to FTP/Memory Card/NAS** as the linkage method for

the events, including motion detection, alarm input, line crossing detection and intrusion detection. For details, please refer to *Section 5.6*.

(4) Select the picture format, resolution, quality, capture interval, and capture number.

5. Set the time interval between two snapshots.
6. Click **Save** to save the settings.
7. (Optional) To upload the captured pictures to the FTP server, configure the FTP parameters and check **Upload Picture** checkbox in FTP Settings interface. For details, please refer to *Section 5.3.7* ***Configuring FTP Settings***.

10.3 Configuring Net HDD

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 Net HDD.

(1) Enter the Net HDD settings interface, **Configuration** > **Storage** > **Storage Management** > **Net HDD**.

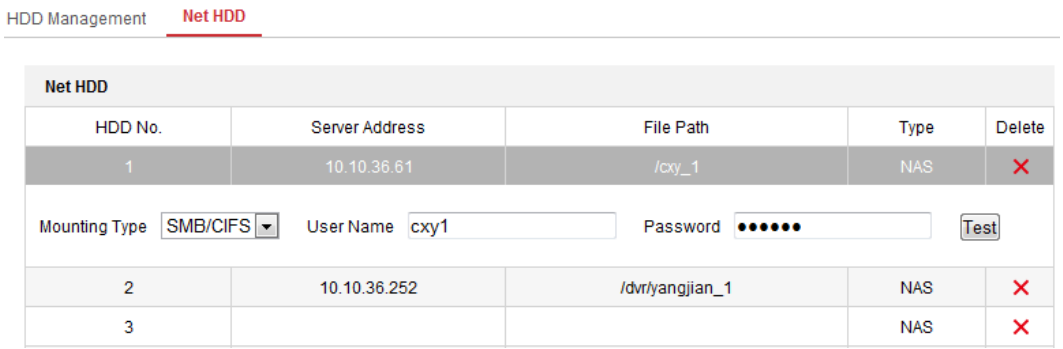


Figure 10-5 Add Network Disk

(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 *NAS User Manual* for creating the file path.

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

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

2. Initialize the added network disk.

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

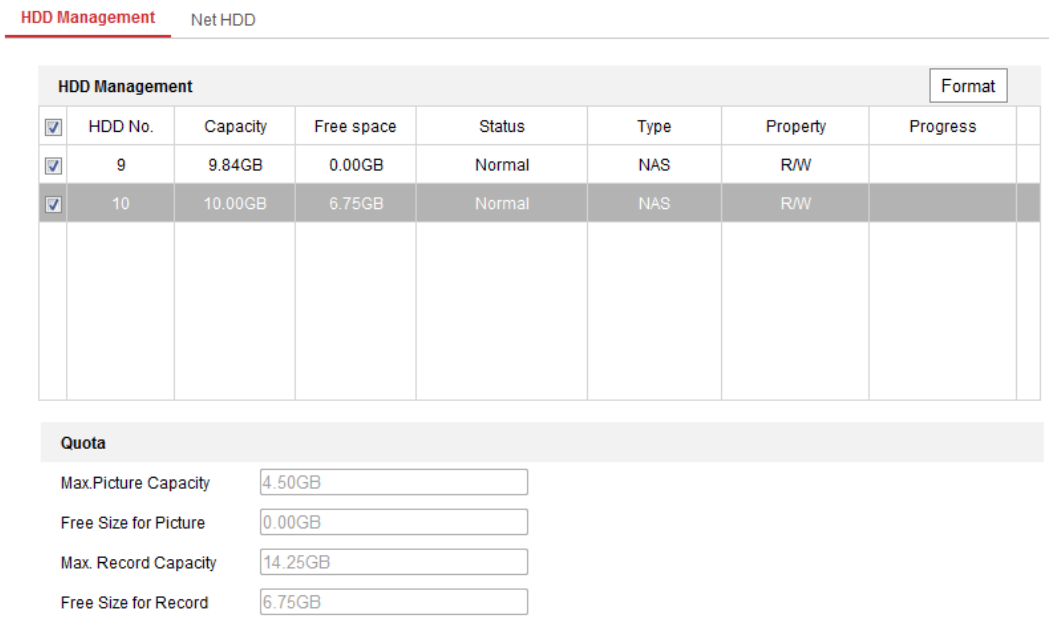


Figure 10-6 Storage Management Interface

(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.**

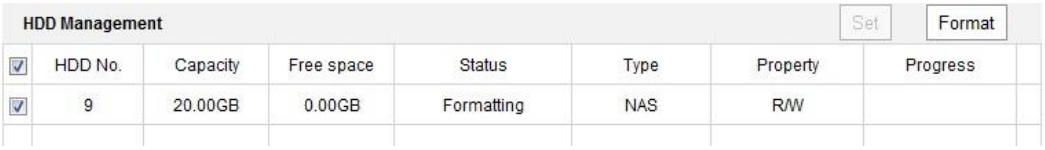


Figure 10-7 View Disk Status

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.

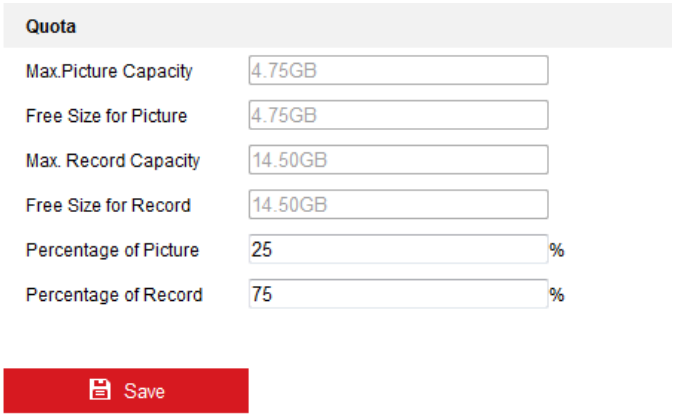


Figure 10-8 Quota Settings

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.

Chapter 11 People Counting

To complete the configuration, you should:

- Set up counting rule.
- Set up data uploading.
- Set up advanced parameters.

11.1 Rule Settings

Rule setting is compulsory for proper functioning of the camera.

11.1.1 Rule

Steps:

1. Enter the Configuration interface: **Configuration** > **People Counting**.
2. Check **Enable People Counting** checkbox to enable the function.
3. Click  on the left of the live view image and draw a red count area.
4. Set the detection line.

   An orange line, named as detection line can be set on the live video, and the object entering or exiting through the line will be detected and counted.

   - Click  button on the left of the live view image. An orange line will appear on the image.
   - Drag the detection line to adjust its position.
   - Drag the yellow end points of the detection line to adjust its length.

     Note:

     - The detection line should be drawn at the position right below the camera, and it should cover the whole entrance/exit.
     - Don’t draw the line at the place where people may linger.
   - You can click  to delete the detection line.
   - You can click  to change the direction. The yellow arrow indicates the direction of entering.
   - You can click  to rest the counter.

11.1.2 Arming Schedule

Steps:

1. Click **Arming Schedule** to edit the arming schedule.
2. Click on the time bar and drag the mouse to select the time period.

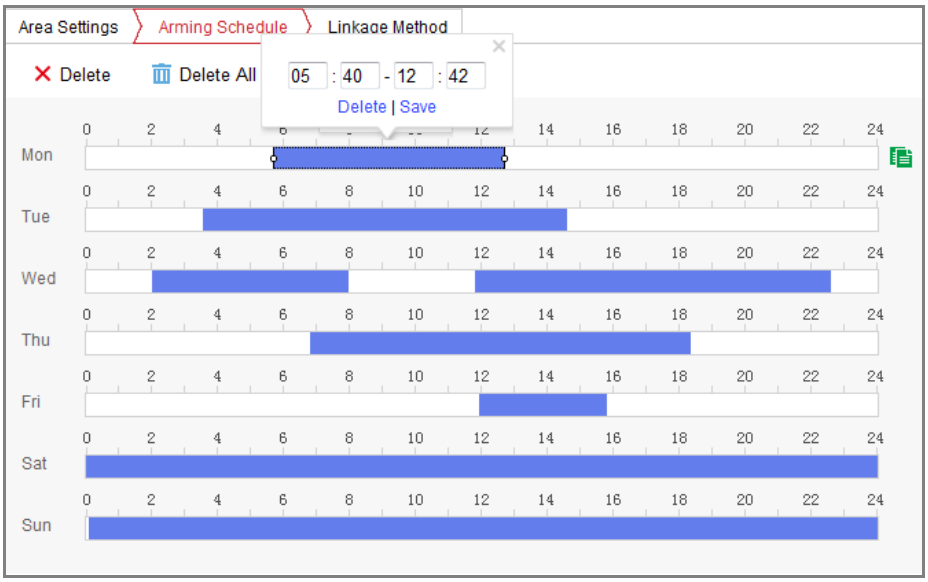


Figure 11-1 Arming Schedule

Note: Click on the selected time period, you can adjust the time period to the desired time by either moving the time bar or input the exact time period.

3. (Optional) Click **Delete** to delete the current arming schedule, or click Save to save the settings.
4. Move the mouse to the end of each day, a copy dialogue box pops up, and you can copy the current settings to other days.
5. Click Save to save the settings.

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

11.1.3 Linkage Method

1. Check the checkbox to select the linkage method. You can enable the linkage method Notify Surveillance Center when an event occurs.

Note: The linkage methods vary according to the different camera models.

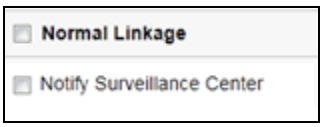


Figure 11-2 Linkage Method

- **Notify Surveillance Center**

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

11.2 Data Uploading Setting

Data uploading is about how and when the counting data can be sent to clients and users.

- You can upload people counting data to surveillance center and client software through SDK and HTTP (if configured).

  To upload real-time data, check the **Real-Time Upload Data** checkbox.

  To upload data regularly, set the **Data Statistics Cycle** as desired.

  Note: If data uploading by HTTP is required, set up the HTTP Data Transmission parameters.

- You can send people counting report to configured email address.

  Select report type (daily report, weekly report, monthly report, and annual report) to activate the function.

  Note: Go to **Configuration > Network > Advanced Settings > Email** to set up email.

11.3 Advanced Settings

Advanced page shows some maintenance settings which are not necessary for proper functioning.

- **Flow Overlay**

  It displays real-time flow information on screen. You can select displayed data type from the drop-down list.

- **Daily Reset Time**

  You can set up a daily reset time. Or you can reset the counter manually by click **Manual Reset**.

Chapter 12Heat Map

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

Steps:

1. Enter the Heat Map configuration interface: **Configuration > Heat Map Configuration**.
2. Check **Enable Heat Map** checkbox to enable the function.
3. Go to **Area Settings** to draw detection area. Click **Draw Area** to draw a detection area. Draw area by left click the end-points in the live view window, and right click to finish the area drawing. Up to 8 areas are configurable.
   Note: You can click **Select All** to select the whole live view window as the configured area. Or click **Clear** to delete the current drawn area.
4. Set the Max. Size and Min. Size for valid targets by clicking the corresponding button and drawing on live image. Targets smaller or larger than the valid target size are not able to trigger detection.
   Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.
   Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
5. Set the validity value. 0 to 100 are available.
   Validity: Camera uses this value to judge if a target it detects is a valid one or not. Invalid target will not be included in the statistics. The higher you set the value, the harder a target would be treated as a valid one.
6. Select the uploading data type.
7. Select data type (daily report, weekly report, monthly report, and annual report). You can send heat map report to the configured email address.
8. Go to **Arming Schedule** tab, and click-and-drag the mouse on the time bar to set the arming schedule.
9. Go to **Linkage Method** tab, and select the linkage method by checking the checkbox of notify the surveillance center.
10. Go to **Shield Region** to draw the shield area.

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

Note:

The heat map statistics will be calculated under Application tab. Go to **Application** to check the heat map statistics.

Chapter 13Intersection Analysis

Purpose:

Intersection Analysis is used to monitor the human flow in an intersection-like scene.

Note: The function varies according to different camera models.

Steps:

1. Enter the Intersection Analysis configuration interface: **Configuration** > **Intersection Analysis**.
2. Check **Enable Intersection Analysis** checkbox to enable the function.
3. Set up rules.

a) Go to Area Settings.

b) Click Draw Area. Draw area in the live view window by left click the end-points. The area should be a polygon which has no more than 10 edges. Each edge covers one way of the intersection.

c) Adjust the arrow direction on each edge of the area. The arrow stands for the direction that the flow leaves the intersection.

d) Select data type (daily report, weekly report, monthly report, and annual report). You can send the intersection analysis report to the configured email address.

4. Go to **Arming Schedule** tab, and click-and-drag the mouse on the time bar to set the arming schedule.
5. Go to **Linkage Method** tab, and select the linkage method by checking the checkbox of notify the surveillance center.
6. Click **Save** to save the settings.

   Note: The Intersection Analysis statistics will be calculated in Application tab. Go to **Application** to check the reports.

Chapter 14Playback

Purpose:

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

Note:

You can also search the records files and play it back in different playback modes via iVMS-4200 client software. Please refer to the User Manual of iVMS-4200 Client Software for detailed instructions.

Steps:

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

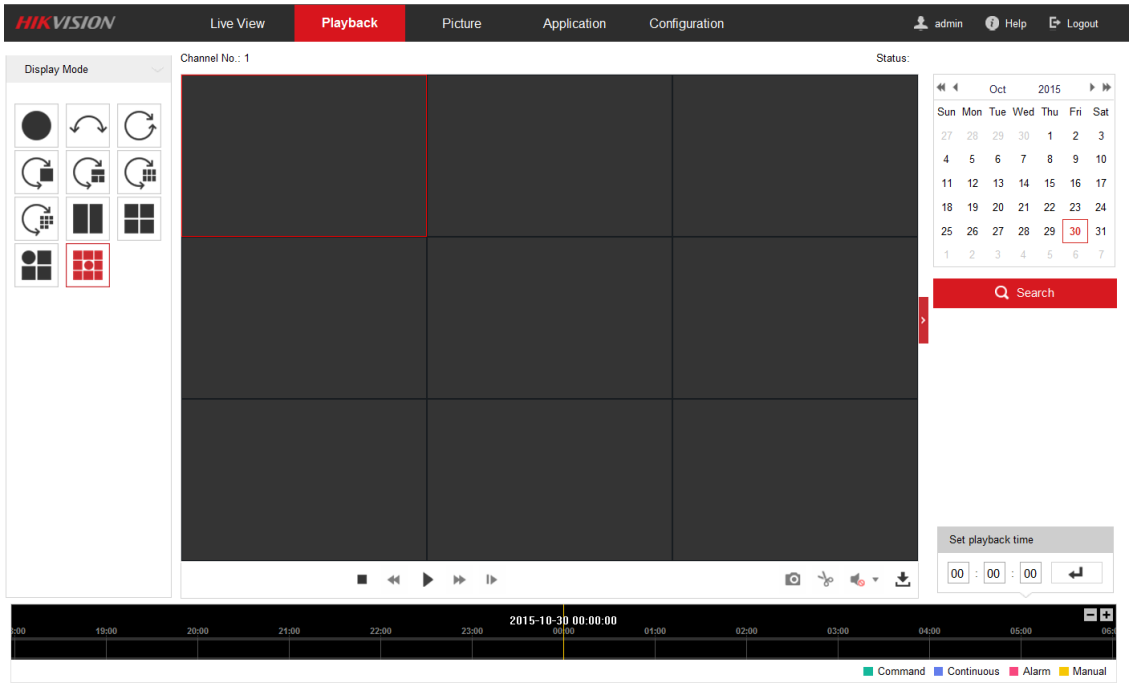


Figure 14-1 Playback Interface

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

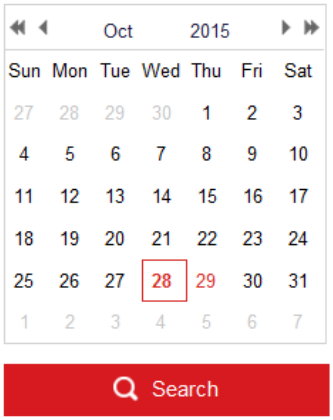


Figure 14-2 Search Video

3. Choose a display mode to play the video.

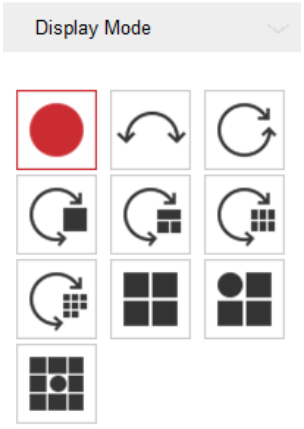


Figure 14-3 Playback Display Mode Setting

Note: For detailed description of each display mode, refer to *Section 4.1 Live View Page*.

4. 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 14-4 Playback Toolbar

Table 14-1 Description of Playback Icons

Button	Operation	Button	Operation
▶	Play		Capture a picture

Button	Operation	Button	Operation
	Pause	/	Start/Stop clipping video files
	Stop		Playback by frame
	Slow Forward	/	Audio on and adjust volume/Mute
	Fast Forward		Download
/	Enable/Disable digital zoom		Stop all playback
	Play with full screen		

Notes:

- You can set the local file saving path for the downloaded video files and pictures in Local Configuration interface. For details, please refer to *Section 5.1*.
- The playback mode varies according to the different mount type.
- PTZ function is also supported in playback.

5. 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.

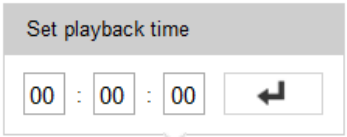


Figure 14-5 Set Playback Time

Figure 14-6 Progress Bar

Different video types are marked in different colors on the progress bar.

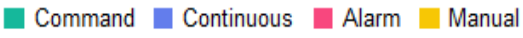


Figure 14-7 Video Types

Chapter 15 Picture

Click Picture to enter the picture searching interface. You can search, view, and download the pictures stored in the local storage or network storage.

Notes:

- Make sure HDD, NAS or memory card are properly configured before you process picture searching.
- Make sure the capture schedule is configured. Go to **Configuration** > **Storage** > **Schedule Settings** > **Capture** to set the capture schedule.

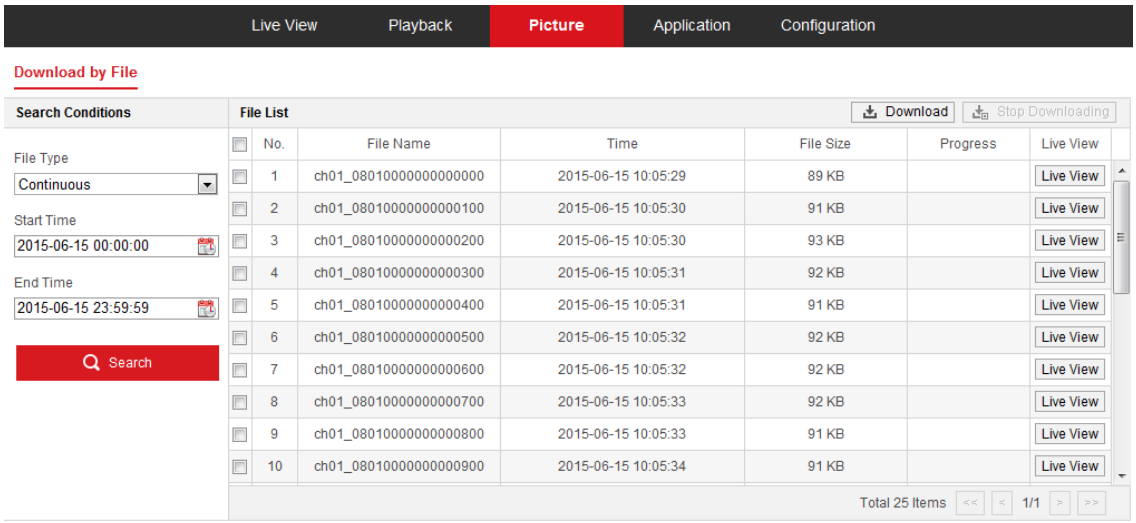


Figure 15-1 Picture Searching Interface

Steps:

1. Select the file type from the dropdown list. Continuous, Motion, Alarm, Motion | Alarm, Motion & Alarm, Line Crossing, Intrusion Detection, and Scene Change Detection are selectable.
2. Select the start time and end time.
3. Click **Search** to start searching.
4. Click Live View to view the captured pictures.
5. Click Download to download the selected pictures.

Note: Up to 4000 pictures can be displayed at one time.

Chapter 16 Application

Click **Application** to enter the heat map statistics interface. You can search, view, and download the counting data stored in the local storage or network storage.

16.1 People Counting Statistics

After you enable the people counting function, you can view and download the people counting data from application tab. To get more intuitional results, you can display the data in different charts.

Steps:

1. Select the report type. Daily report, weekly report, monthly report, and annual report are selectable.

   Note: Daily report calculates the data on the date you selected; weekly report calculates for the week your selected date belongs to; monthly report calculates for the month your selected date belongs to; and the annual report calculates for the year your selected date belongs to.

2. Select the statistics type. People Entered, and People Exited are selectable.

3. Select the start time, and click **Counting**.

   The counting result displays in the statistic result area. Click List, Bar Chart, or Line Chart to display the result in different way.

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

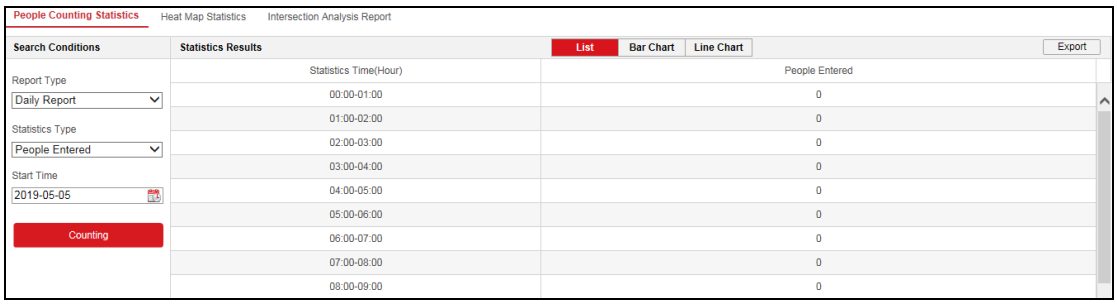


Figure 16-1 People Counting

16.2 Heat Map Statistics

Purpose:

Heat map is a graphical representation of data represented by colors. The heat map function of the camera usually be used to analyze the visit times and dwell time of customers in a configured area. To get more intuitional results, you can display the data in different charts.

Before you start:

You have to configure Heat Map setting before you can view and download the heat map data from application tab. Refer to *Section Configuring Heat Map* for detailed information.

Note: The heat map function is not supported when you choose the decoding mode as hardware decoding and the display mode as 180 Panoramic View or 4PTZ. Thus, you will not see the **Application** on menu bar when you choose the mentioned modes.

Steps:

1. Click **Heat Map Statistics** to enter the data statistics interface.
2. Select the report type by clicking the drop-down menu. Daily report, weekly report, monthly report, and annual report are selectable.

   Note: Daily report calculates the data on the date you selected; weekly report calculates for the week your selected date belongs to; monthly report calculates for the month your selected date belongs to; and the annual report calculates for the year your selected date belongs to.
3. Select the statistics time, and click **Counting** to list the heat map data.
4. Select **Space Heat Map** or **Time Heat Map** to display the results.

   Space Heat Map:

   The different colors that mark areas in the surveillance scene stand for different frequency of visits. The color closer to the red end of the color scheme shows a relatively high frequency of visits.

   The duration displayed next to “High” or “Low” stands for the cumulative time that the area keeps certain level of visit frequency.

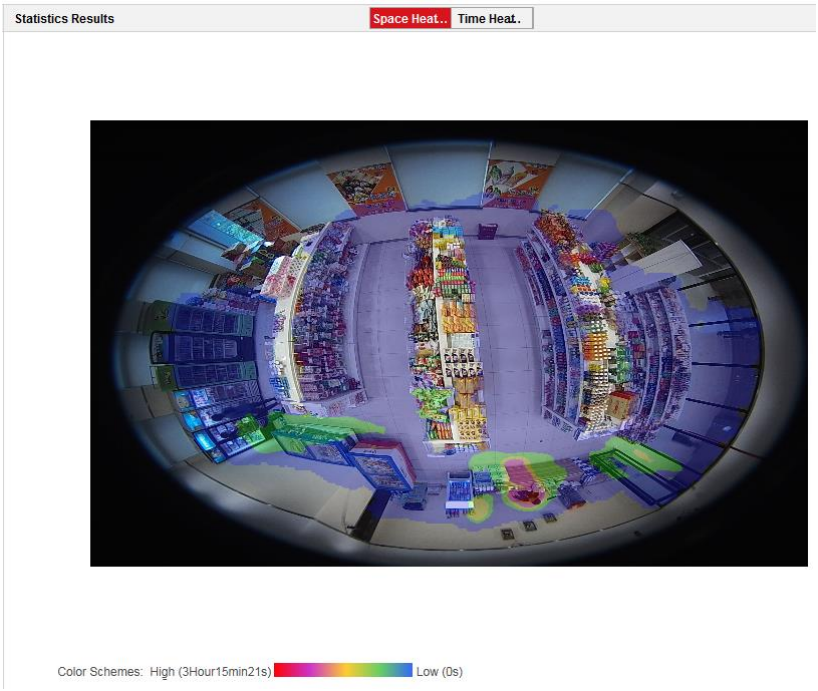


Figure 16-2 Space Heat Map

Time Heat Map:

The heat value of the pre-defined area is calculated by hour, day, or month. You can click the **Export** button to export the data in an excel file.

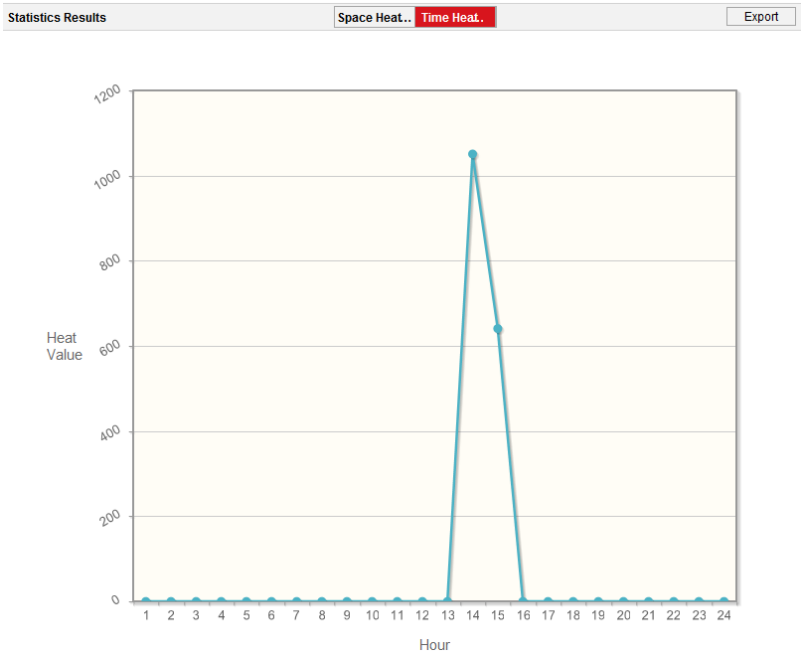


Figure 16-3 Time Heat Map

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

16.3 Intersection Analysis Statistics

After you enable the intersection analysis function, you can view and download the intersection analysis data from application tab. To get more intuitional results, you can display the data in different charts.

Steps:

1. Select a **Flow In** entrance.
2. Select the report type. Daily report, weekly report, monthly report, and annual report are selectable.

   Note: Daily report calculates the data on the date you selected; weekly report calculates for the week your selected date belongs to; monthly report calculates for the month your selected date belongs to; and the annual report calculates for the year your selected date belongs to.
3. Select the statistics time, and click **Counting** to start calculating.

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.

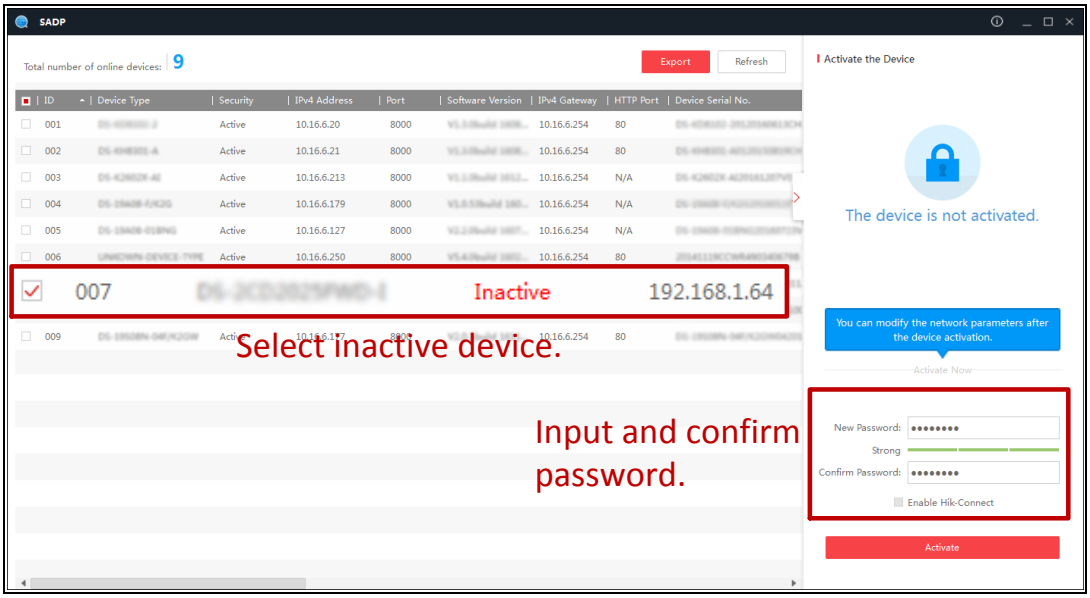


Figure A.1.1 Searching Online Devices

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** button 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 **Modify** to save the changes.

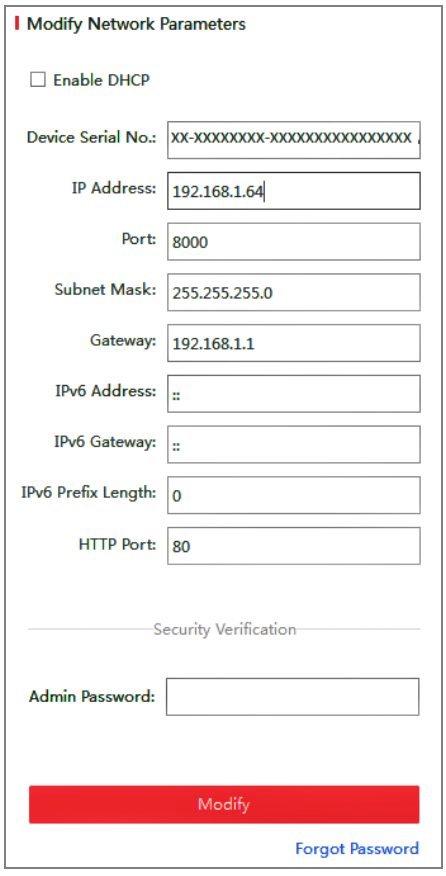


Figure A.1.2 Modify Network Parameters

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:

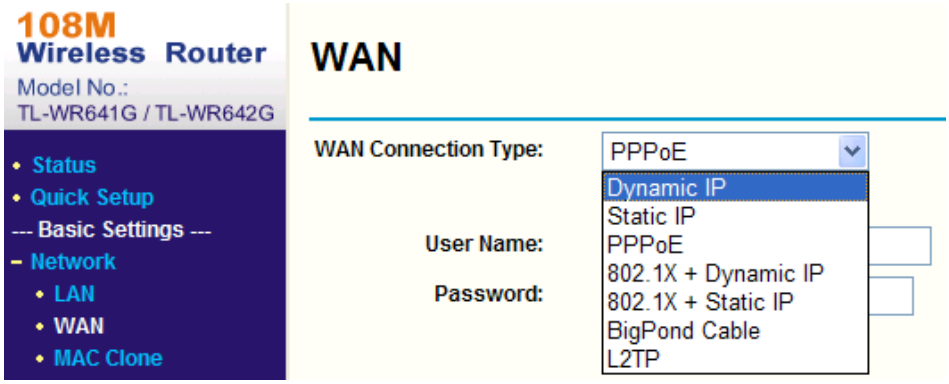


Figure A.2.1 Select the WAN Connection Type

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

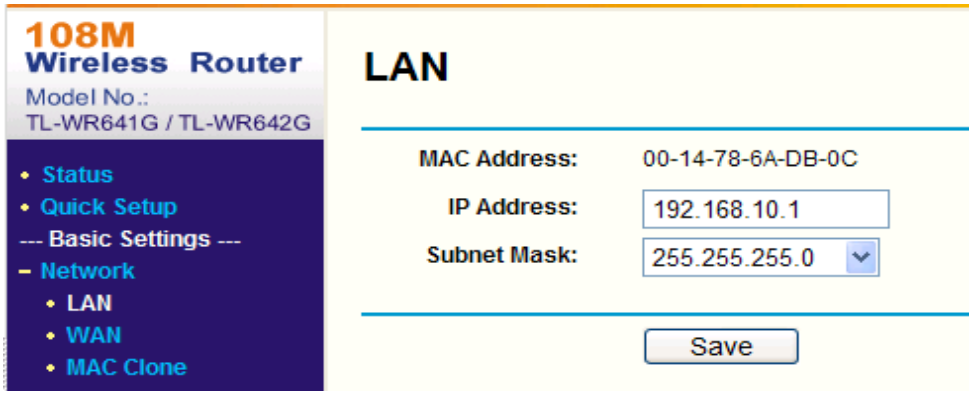


Figure A.2.2 Set the LAN parameters

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**.

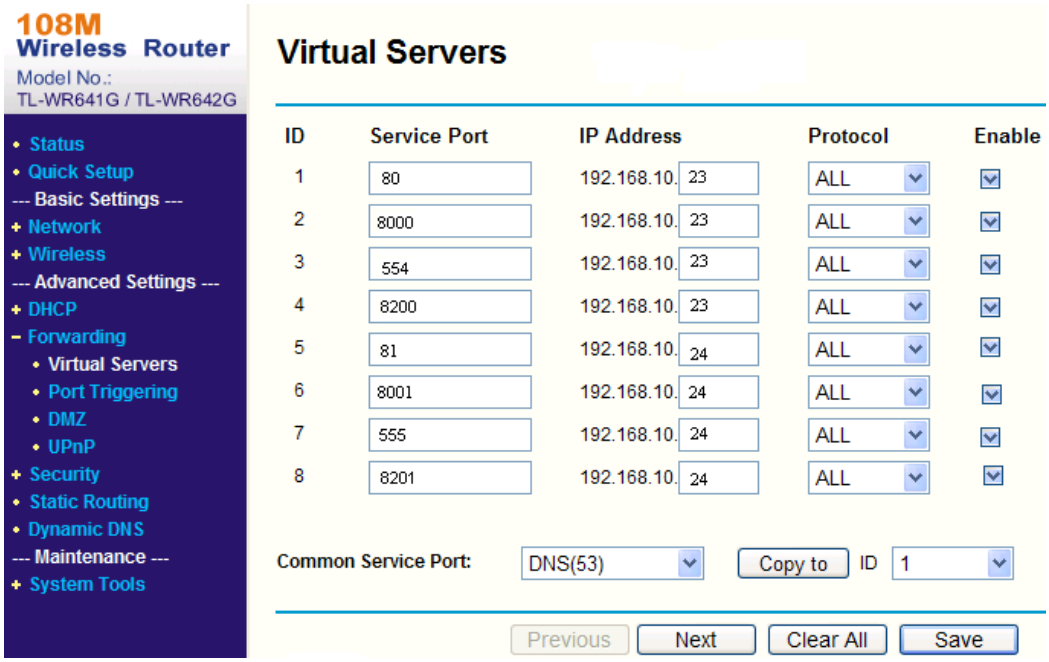


Figure A.2.3 Port Mapping

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.


See Far, Go Further