

The logo features the word "HIKVISION" in a bold, italicized, white sans-serif font, centered within a red horizontal bar. The bar has a white diagonal stripe on the left side.

HIKVISION

PanoVu Mini Series
Network PTZ Camera
User Manual

User Manual

COPYRIGHT ©2018 Hangzhou Hikvision Digital Technology Co., Ltd.

ALL RIGHTS RESERVED.

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

About this Manual

This Manual is applicable to PanoVu Mini Series Network PTZ 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.

0504121080517

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 A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

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

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the Low Voltage Directive 2015/35/EU, the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU.



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



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

Industry Canada ICES-003 Compliance

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

Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.



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:

- Adopt the power adapter which can meet the safety extra low voltage (SELV) standard. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as an adapter overload may cause over-heating and can be a fire hazard.
- When the product is installed on a wall or ceiling, the device should be firmly fixed.
- To reduce the risk of fire or electrical shock, do not expose the indoor product to rain or moisture.
- This installation should be made by a qualified service person and should conform to all the local codes.
- Install blackouts equipment into the power supply circuit for convenient supply interruption.
- If the product does not work properly, contact your dealer or the nearest service center. Never attempt to disassemble the product yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)



Cautions:

- If the camera fails to synchronize local time with that of the network, you need to set up camera time manually. Visit the camera (via web browser or client software) and enter system settings interface for time settings.
- Make sure the power supply voltage is correct before using the product.
- Do not drop the product or subject it to physical shock. Do not install the product on vibratory surface or places.
- Do not expose it to high electromagnetic radiating environment.

- Do not aim the lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the product.
- 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.
- For working temperature, refer to the specification manual for details.
- To avoid heat accumulation, good ventilation is required for a proper operating environment.
- While shipping, the product should be packed in its original packing.
- Use the provided glove when open up the product cover. Do not touch the product cover with fingers directly, because the acidic sweat of the fingers may erode the surface coating of the product cover.
- Use a soft and dry cloth when clean inside and outside surfaces of the product cover. Do not use alkaline detergents.
- Improper use or replacement of the battery may result in hazard of explosion. Use the manufacturer recommended battery type.

Table of Contents

CHAPTER 1	OVERVIEW	1
1.1	SYSTEM REQUIREMENT	1
1.2	FUNCTIONS.....	1
CHAPTER 2	NETWORK CONNECTION	3
2.1	SETTING THE NETWORK CAMERA OVER THE LAN	3
2.1.1	<i>Wiring over the LAN</i>	<i>3</i>
2.1.2	<i>Activating the Camera</i>	<i>4</i>
2.2	SETTING THE NETWORK CAMERA OVER THE WAN	9
2.2.1	<i>Static IP Connection</i>	<i>9</i>
2.2.2	<i>Dynamic IP Connection</i>	<i>10</i>
CHAPTER 3	ACCESSING TO THE NETWORK CAMERA.....	12
3.1	ACCESSING BY WEB BROWSERS	12
3.2	ACCESSING BY CLIENT SOFTWARE.....	13
CHAPTER 4	BASIC OPERATIONS	15
4.1	CONFIGURING LOCAL PARAMETERS	15
4.2	LIVE VIEW PAGE	16
4.3	STARTING LIVE VIEW	17
4.4	OPERATING PTZ CONTROL	19
4.4.1	<i>PTZ Control Panel.....</i>	<i>19</i>
4.4.2	<i>Auxiliary Functions.....</i>	<i>21</i>
4.4.3	<i>Setting/Calling a Preset</i>	<i>22</i>
4.5	PLAYBACK.....	24
4.5.1	<i>Play Back Video Files</i>	<i>24</i>
4.5.2	<i>Downloading Video Files</i>	<i>25</i>
CHAPTER 5	SYSTEM CONFIGURATION.....	27
5.1	STORAGE SETTINGS	27
5.1.1	<i>Configuring Recording Schedule</i>	<i>27</i>
5.1.2	<i>Configuring Capture Schedule</i>	<i>29</i>
5.1.3	<i>Configuring Net HDD</i>	<i>30</i>
5.2	BASIC EVENT CONFIGURATION.....	33
5.2.1	<i>Configuring Motion Detection</i>	<i>33</i>
5.2.2	<i>Configuring Video Tampering Alarm</i>	<i>37</i>
5.2.3	<i>Configuring Alarm Input</i>	<i>39</i>
5.2.4	<i>Configuring Alarm Output</i>	<i>40</i>
5.2.5	<i>Handling Exception</i>	<i>41</i>
5.3	SMART EVENT CONFIGURATION.....	42
5.3.1	<i>Detecting Audio Exception.....</i>	<i>42</i>
5.3.2	<i>Configuring Intrusion Detection.....</i>	<i>44</i>
5.3.3	<i>Configuring Line Crossing Detection.....</i>	<i>45</i>

5.4	PTZ CONFIGURATION	47
5.4.1	<i>Configuring Basic PTZ Parameters</i>	47
5.4.2	<i>Configuring PTZ Limits</i>	48
5.4.3	<i>Configuring Initial Position</i>	49
5.4.4	<i>Configuring Park Actions</i>	50
5.4.5	<i>Configuring Privacy Mask</i>	51
5.4.6	<i>Configuring Panorama Linkage</i>	53
5.4.7	<i>Configuring Scheduled Tasks</i>	54
5.4.8	<i>Clearing PTZ Configuration</i>	55
CHAPTER 6	CAMERA CONFIGURATION	56
6.1	CONFIGURING NETWORK SETTINGS	56
6.1.1	<i>Basic Settings</i>	56
6.1.2	<i>Advanced Settings</i>	60
6.2	CONFIGURING VIDEO AND AUDIO SETTINGS.....	69
6.2.1	<i>Configuring Video Settings</i>	69
6.2.2	<i>Configuring Audio Settings</i>	70
6.2.3	<i>Configuring ROI Settings</i>	71
6.2.4	<i>Display Info. on Stream</i>	73
6.3	CONFIGURING IMAGE SETTINGS.....	73
6.3.1	<i>Configuring Display Settings</i>	73
6.3.2	<i>Configuring OSD Settings</i>	77
6.3.3	<i>Configuring Text Overlay Settings</i>	78
6.3.4	<i>Configuring Privacy Mask</i>	79
6.3.5	<i>Configuring Image Parameters Switch</i>	80
6.4	CONFIGURING SYSTEM SETTINGS	81
6.4.1	<i>System Settings</i>	81
6.4.2	<i>Maintenance</i>	84
6.4.3	<i>Security</i>	86
6.4.4	<i>User Management</i>	88
APPENDIX	93	
	SADP SOFTWARE INTRODUCTION	93

Chapter 1 Overview

1.1 System Requirement

System requirement of web browser accessing is as follows:

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

CPU: Intel Pentium IV 3.0 GHz or higher

RAM: 1G or higher

Display: 1024 × 768 resolution or higher

Web Browser: Internet Explorer 8 to 11, Google Chrome 31 to 44, and Mozilla Firefox 30 to 51

1.2 Functions



The functions vary depending on different camera models.

- **PTZ Limits**

The camera can be programmed to move within the PTZ limits (left/right, up/down).

- **Presets**

A preset is a predefined image position. When the preset is called, the camera will automatically move to the defined position. The presets can be added, modified, deleted and called.

- **Label Display**

The on-screen label of the preset title, azimuth/elevation, zoom, time and camera name can be displayed on the monitor. The displays of time and camera name can be programmed.

- **Privacy Mask**

This function allows you to block or mask certain area of a scene, for preventing the personal privacy from recording or live viewing. A masked area will move with pan and tilt functions and automatically adjust in size as the lens zooms telephoto and wide.

- **3D Positioning**

In the client software, use the left key of mouse to click on the desired position in the video image and drag a rectangle area in the lower right direction, then the camera system will move the position to the center and allow the rectangle area to zoom in. Use the left key of mouse to drag a rectangle area in the upper left direction to move the position to the center and allow the rectangle area to zoom out.

- **Proportional Pan/Tilt**

Proportional pan/tilt automatically reduces or increases the pan and tilt speeds according to the amount of zoom. At telephoto zoom settings, the pan and tilt speeds will be slower than at wide zoom settings. This keeps the image from moving too fast on the live view image when there is a large amount of zoom.

- **Auto Focus**

The auto focus enables the camera to focus automatically to maintain clear video images.

- **Day/Night Auto Switch**

The cameras deliver color images during the day. And as light diminishes at night, the cameras switch to night mode and deliver black and white images with high quality.

- **Backlight Compensation (BLC)**

If you focus on an object against strong backlight, the object will be too dark to be seen clearly. The BLC (Backlight Compensation) function can compensate light to the object in the front to make it clear, but this causes the over-exposure of the background where the light is strong.

- **Wide Dynamic Range (WDR)**

The wide dynamic range (WDR) function helps the camera provide clear images even under back light circumstances. When there are both very bright and very dark areas simultaneously in the field of view, WDR balances the brightness level of the whole image and provide clear images with details.

- **White Balance (WB)**

White balance can remove the unrealistic color casts. White balance is the white rendition function of the camera to adjust the color temperature according to the environment automatically.

- **Power Off Memory**

The camera supports the power off memory capability with the predefined resume time. It allows the camera to resume its previous position after power is restored.

- **Park Action**

This feature allows the camera to start a predefined action automatically after a period of inactivity.

- **User Management**

The camera allows you to edit users with different levels of permission, in the admin login status. Multiple users are allowed to access and control the same network camera via network simultaneously.

- **3D Digital Noise Reduction**

Comparing with the general 2D digital noise reduction, the 3D digital noise reduction function processes the noise between two frames besides processing the noise in one frame. The noise will be much less and the video will be clearer.

Chapter 2 Network Connection



- 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, strengthen your own protection. If the product does not work properly, 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), 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), 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 camera in the same subnet with your computer, and install the SADP or client software to search and change the IP of the network camera.



For the detailed introduction of SADP, refer to Appendix.

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 the network camera over the LAN via a switch or a router.

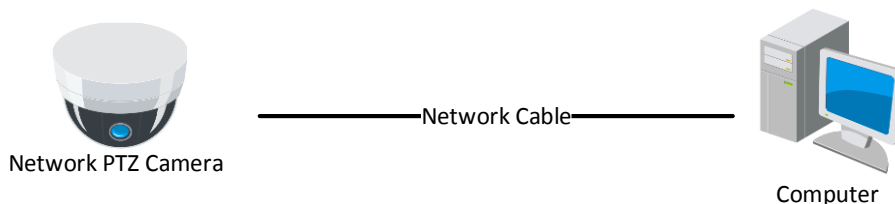


Figure 2-1 Connecting Directly

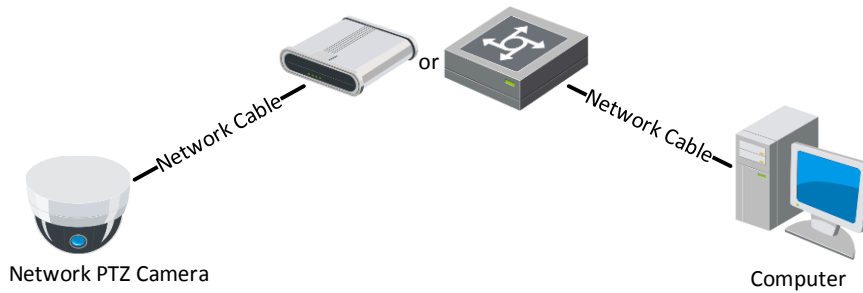


Figure 2-2 Connecting via a Switch or a Router

2.1.2 Activating the Camera

Purpose:

You are required to activate the camera first before you can use the camera.

Activation via web browser, activation via SADP, and activation via client software are 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 enter the activation interface.



The default IP address of the camera is 192.168.1.64.

The screenshot shows a web browser window titled 'Activation'. It contains the following fields and text:

- User Name:** admin
- Password:** An empty text input field.
- Confirm:** An empty text input field.
- OK:** A button at the bottom right.
- Instructions:** Below the password field, it states: "Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained."

Figure 2-3 Activation Interface (Web)

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



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

- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*
4. Confirm the password.
 5. Click **OK** to activate the camera and enter the live view interface.

◆ Activation via SADP Software

SADP software is used for detecting the online device, activating the device, 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 an inactive device.

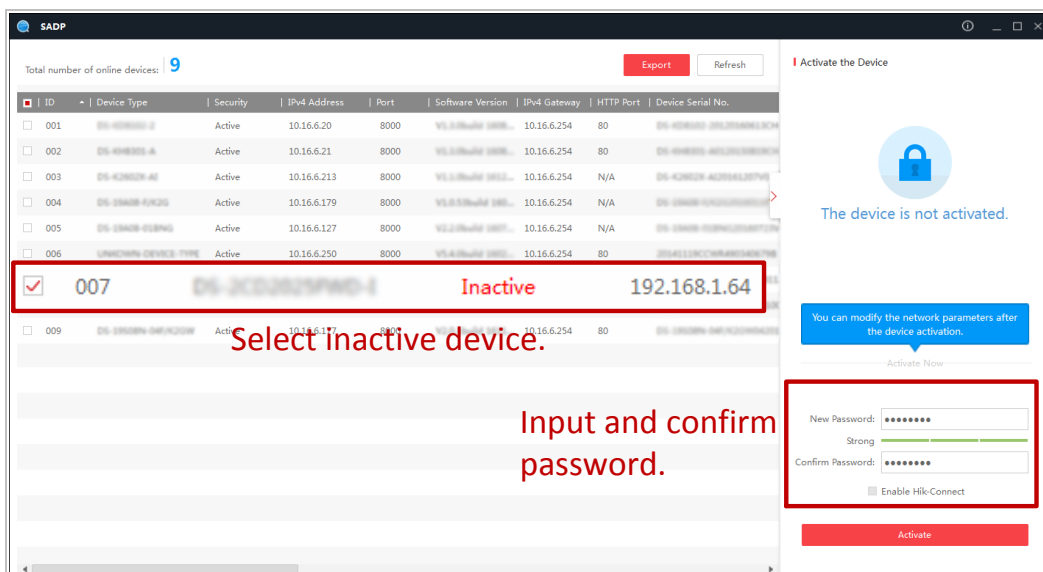


Figure 2-4 SADP Interface



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.



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



You can enable the Hik-Connect service for the device during activation. Hik-Connect function varies depending on different camera models.

4. Click **Activate** to start activation. You can check whether the activation is completed on the popup window. If activation failed, make sure that the password meets the requirement and then try again.
5. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking **Enable DHCP**.

Figure 2-5 Modify the IP Address

6. Input the 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 Figure 2-6.

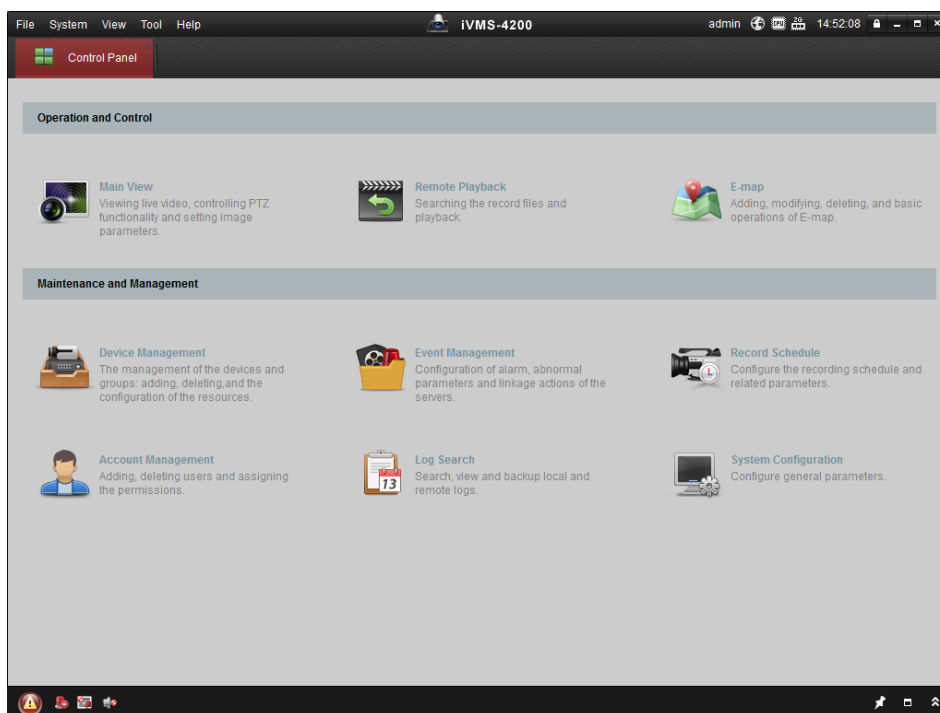


Figure 2-6 iVMS-4200 Control Panel

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

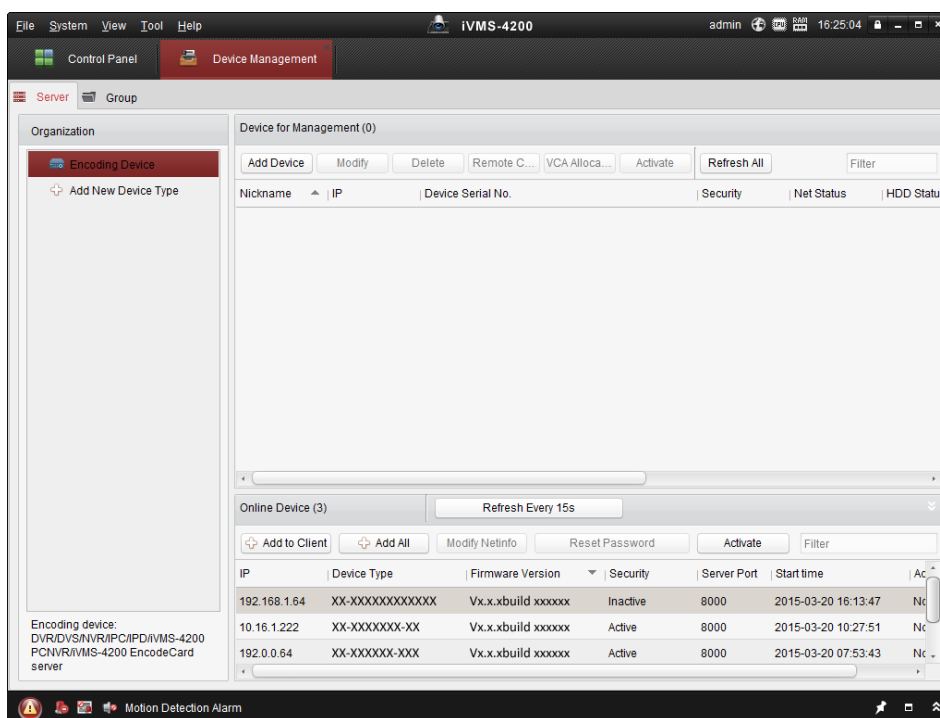


Figure 2-7 Device Management Interface

3. Check the device status from the device list, and select an inactive device.
4. Click **Activate** to pop up the Activation interface.
5. Create a password and input the password in the password field, and confirm the password.



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

Figure 2-8 Activation Interface

6. Click **OK** to start activation.
7. Click **Modify Netinfo** to pop up the Network Parameter Modification interface, as shown in Figure 2-9.

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 **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:

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 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 depending on different routers. Call the router manufacturer for assistance with port mapping.
5. Visit the network camera through a web browser or the client software over the internet.

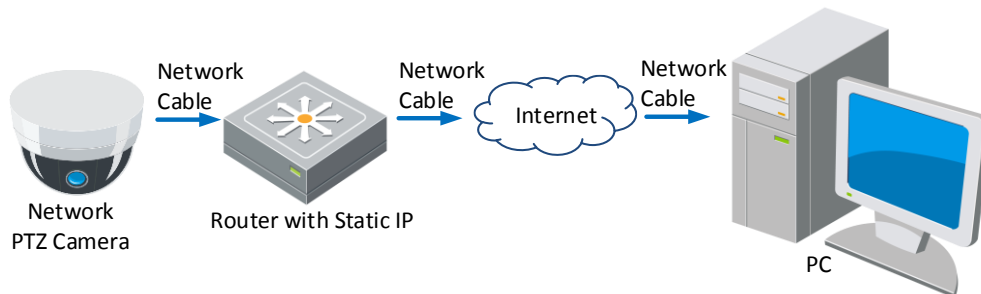


Figure 2-10 Accessing the Camera through Router with Static IP

- **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 camera.

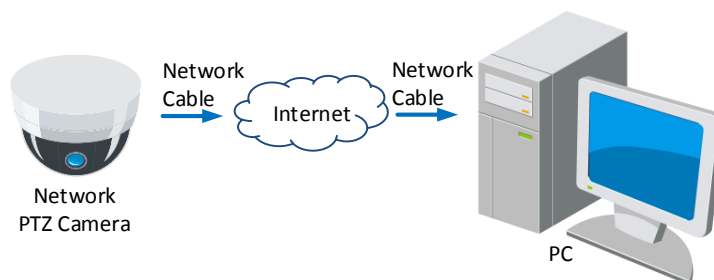


Figure 2-11 Accessing the Camera with Static IP Directly

2.2.2 Dynamic IP Connection

Before you start:

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 LAN configuration.
3. In the router, set the PPPoE user name, password and confirm the password.



- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
 - *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*
4. Set port mapping. E.g. 80, 8000 and 554 ports. The steps for port mapping vary depending on different routers. Call the router manufacturer for assistance with port mapping.
 5. Apply a domain name from a domain name provider.
 6. Configure the DDNS settings in the setting interface of the router.
 7. Visit the camera via the applied domain name.

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

Purpose:

This camera supports the PPPoE auto dial-up function. The camera gets a public IP address by ADSL dial-up after the camera is connected to a modem. You need to configure the PPPoE parameters of the network camera. Refer to **Section 6.1.1 Configuring PPPoE Settings** for detailed configuration.



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). Follow the steps below for normal domain name resolution and private domain name resolution to solve the problem.

- ◆ **Normal Domain Name Resolution**

Steps:

1. Apply a domain name from a domain name provider.
2. Configure the DDNS settings in the **DDNS Settings** interface of the network camera. Refer to


Section 6.1.1 Configuring DDNS Settings for detailed configuration.

3. Visit the camera via the applied domain name.

Chapter 3 Accessing to the Network Camera

3.1 Accessing by Web Browsers

Steps:

1. Open the web browser.
2. In the address field, input the IP address of the network camera, e.g., 192.168.1.64 and enter the login interface.
3. Activate the camera for the first time using, refer to the **section 2.1.2 Activating the Camera**.
4. Select English as the interface language on the top-right of login interface.
5. Input the user name and password and click 

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



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

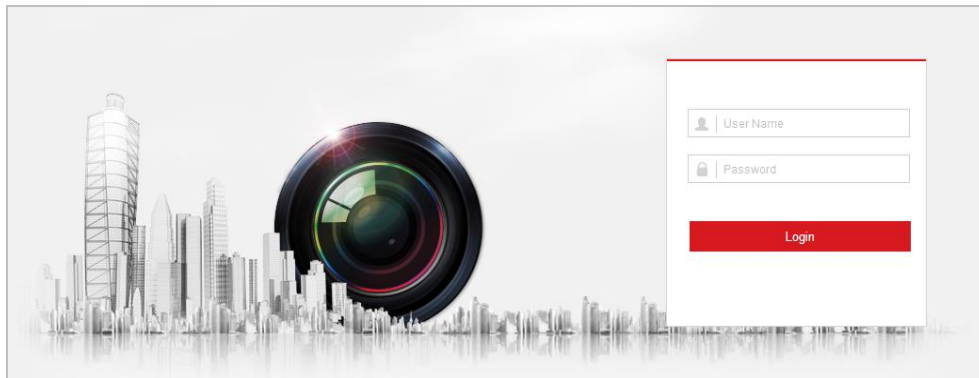


Figure 3-1 Login Interface

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



You may have to close the web browser to install the plug-in. Reopen the web browser and log in again after installing the plug-in.

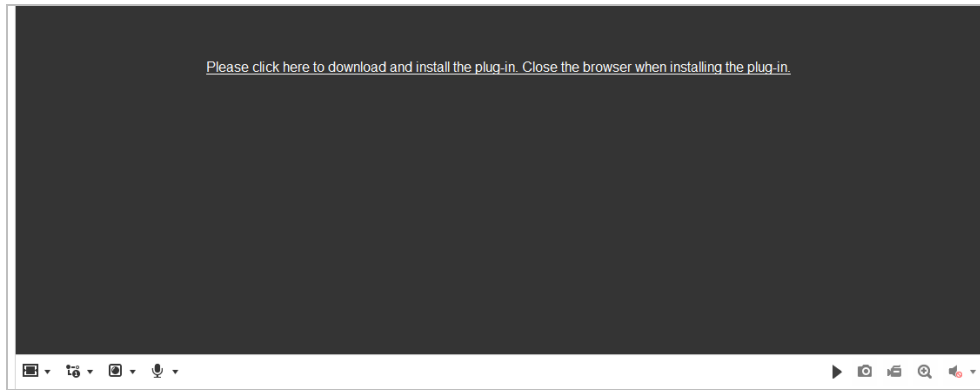


Figure 3-2 Download and Install Plug-in

3.2 Accessing by Client Software

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

Follow the installation prompts to install the client software and WinPcap. The configuration interface and live view interface of client software are shown in Figure 3-3.

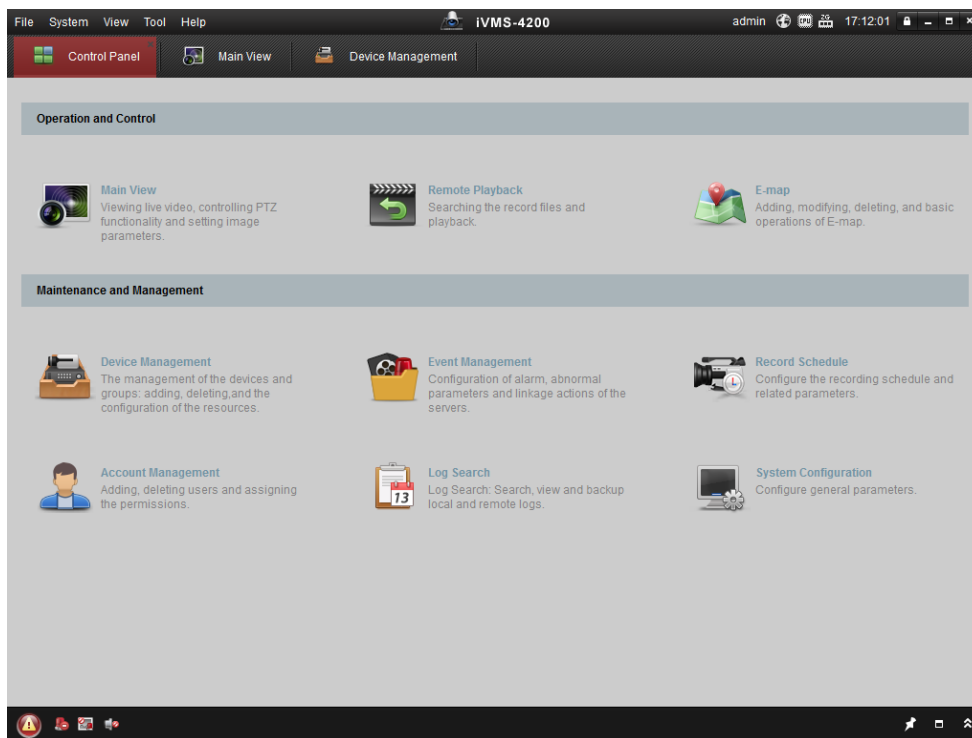


Figure 3-3 iVMS-4200 Control Panel

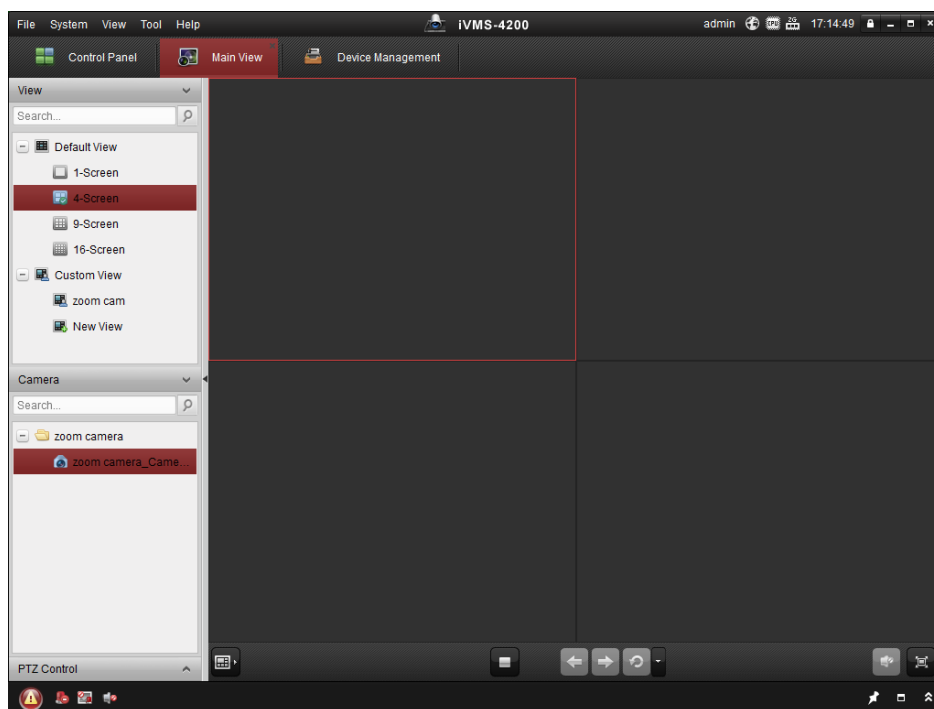


Figure 3-4 iVMS-4200 Live View Interface



- If you use third party VMS software, contact technical support of our branch for camera firmware.
- For detailed information about client software of our company, refer to the user manual of the software. This manual mainly introduces accessing to the network camera by web browser.

Chapter 4 Basic Operations

In this and the following chapters, operation of the camera by the web browser will be taken as an example.

4.1 Configuring Local Parameters



The local configuration refers to the parameters of the live view and other operations using the web browser.

Steps:

1. Enter Local Configuration interface:

Configuration > Local

The screenshot shows the 'Local Configuration' interface with three main sections:

- Live View Parameters:**
 - Protocol: TCP, UDP, MULTICAST, HTTP
 - Play Performance: Shortest Delay, Balanced, Fluent
 - Rules: Enable, Disable
 - Auto Start Live View: Yes, No
 - Image Format: JPEG, BMP
- Record File Settings:**
 - Record File Size: 256M, 512M, 1G
 - Save record files to: [Text Field] [Browse] [Open]
 - Save downloaded files to: [Text Field] [Browse] [Open]
- Picture and Clip Settings:**
 - Save snapshots in live view to: [Text Field] [Browse] [Open]
 - Save snapshots when playback to: [Text Field] [Browse] [Open]
 - Save clips to: [Text Field] [Browse] [Open]

Figure 4-1 Local Configuration Interface

2. Configure the following settings:

- **Live View Parameters:** Set the protocol type, play performance, rules and image format.

- ◆ **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.

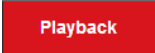

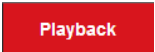

UDP: Provides real-time audio and video streams.

MULTICAST: It's recommended to select the protocol type to **MULTICAST** when using the Multicast function.

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

- ◆ **Play Performance:** Set the live view performance to Shortest Delay, Balanced, or Fluent.

- ◆ **Rules:** You can enable or disable the rules of dynamic analysis for motion here.

- ◆ **Auto Start Live View:** Set it as Yes or NO. If Yes is selected, live view will start automatically when you go to live view interface.
- ◆ **Image Format:** The captured pictures can be saved as different format. JPEG and BMP are available.
- **Record File Settings:** Set the saving path of the video files.
 - ◆ **Record File Size:** Select the packed size of manually recorded and downloaded video files. The size can be set to 256M, 512M or 1G.
 - ◆ **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  interface.
- **Picture and Clip Settings:** Set the saving paths of the captured pictures and clipped video files.
 - ◆ **Save snapshots in live view to:** Set the saving path of the manually captured pictures in  interface.
 - ◆ **Save snapshots when playback to:** Set the saving path of the captured pictures in  interface.
 - ◆ **Save clips to:** Set the saving path of the clipped video files in  interface.



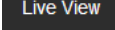
- You can click **Browse** to change the directory for saving video files, clips and pictures.
- You can click **Open** to directly open the video files, clips and pictures.

3. Click  to save the settings.

4.2 Live View Page

Purpose:

The live video page allows you to view live 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  on the menu bar of the main page to enter the live view page.



The functions vary depending on different camera models. Refer to the actual interface as standard.


Descriptions of the live view page:




Figure 4-2 Live View Page

Menu Bar:

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

Click  to display the help file of the network camera.

Click  to logout the system.

Live View Window:

Display the live video.

Camera Channel:

Camera 01: Tracking PTZ Camera

Camera 02: Panoramic Camera

Camera 03: Panoramic Camera (not supported by all camera models)

Camera 04: Panoramic Camera (not supported by all camera models)

Toolbar:

Operations on the live view page, e.g., live view, capture, record, audio on/off, regional exposure, regional focus, etc.

PTZ Control:

Panning, tilting, focusing and zooming actions of the network. The lighter, wiper, one-touch focus and lens initialization control.


Preset:

Set and call the preset for the camera.

Live View Parameters:

Configure the image size, stream type, plug-in type, and two-way audio of the live video.

4.3 Starting Live View

In the live view window as shown in Figure 4-3, click  on the toolbar to start the live view of the network.

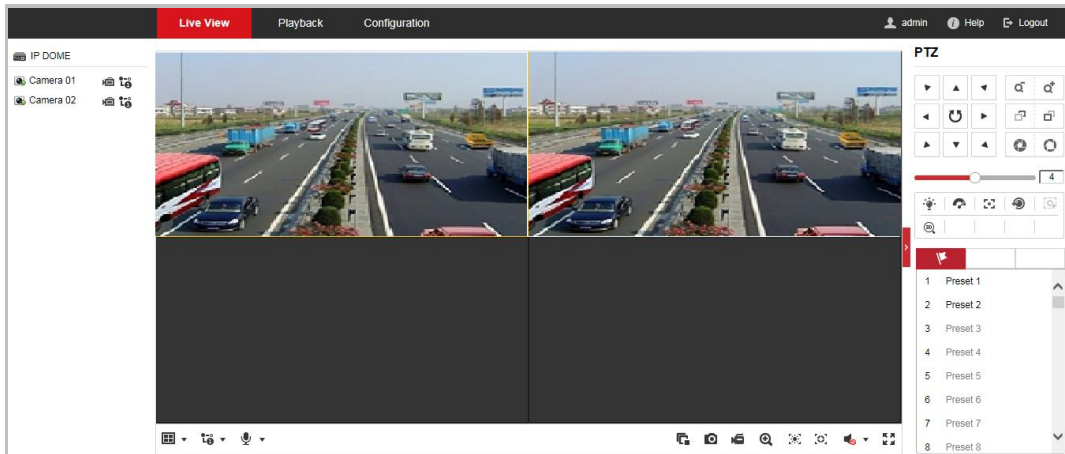




Figure 4-3 Start Live View

Table 4-1 Descriptions of the Toolbar

Icon	Description	Icon	Description
	Display in 1*1/2*2/PIP (Picture in Picture.)		Live view with the main/sub stream. (Sub-stream is not supported by all camera models.)
	Start/stop two-way audio.		Start/stop all live view.
	Manually capture the pictures.		Manually start/stop all recording.
	Start/stop digital zoom.		Enable/disable regional exposure
	Mute/audio on and adjust volume		Enable/disable regional focus
	Display in full screen mode.		

- Double-click on the live video to switch the current live view into full-screen or return to normal mode from the full-screen.
- Click to select the stream type and display live video with the main stream/sub-stream. The main stream is with a relatively high resolution and needs much bandwidth. The default setting of stream type is . Sub-stream is not supported by all camera models.
- Click and it displays . Click to enable two-way audio and the icon turns into . Click the icon again to stop two-way audio.
- Click to enable digital zoom function and the icon turns into . Then drag the mouse towards low right direction to draw a rectangle on the image as the desired zoom. After viewing it you can click any place of the picture to get back to normal picture.

- Click the  on the toolbar to enter the regional exposure operation mode and the icon turns into . Then drag the mouse to draw a rectangle on the image as the desired exposure region.

- Click  to display the . Drag the slider to adjust the volume.



Before using the two-way audio or recording with audio functions, set the **Stream Type** to **Video & Audio** referring to *Section 6.2.1 Configuring Video Settings*.

Refer to the following sections for more information:

- Configuring remote recording in *Section 5.1.1 Configuring Recording Schedule*.
- Setting the image quality of the live video in *Section 6.3 Configuring Image Settings* and *Section 6.2.1 Configuring Video Settings*.
- Setting the OSD text on live video in *Section 6.3.2 Configuring OSD Settings*.

4.4 Operating PTZ Control



Purpose:

In the live view interface, you can use the PTZ control buttons to control panning, tilting and zooming.



PTZ functions vary depending on different camera models.

4.4.1 PTZ Control Panel

On the live view page, click  to show the PTZ control panel or click  to hide it. Click the direction buttons to control the pan/tilt movements. Click the zoom/iris/focus buttons to realize lens control.

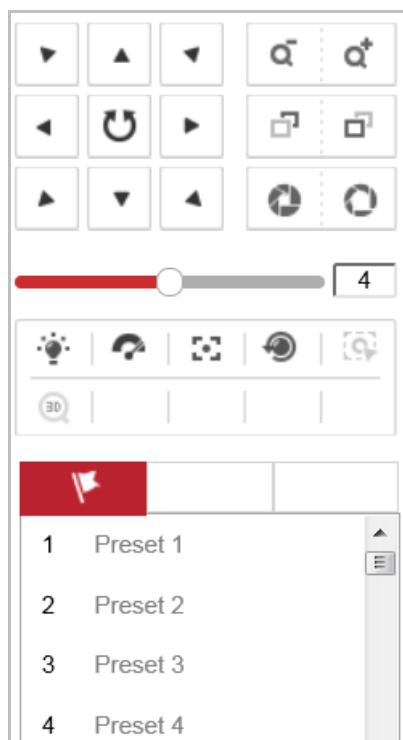












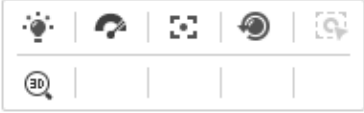




Figure 4-4 PTZ Control Panel




Table 4-2 Descriptions of PTZ Control Panel

Button	Name	Description
	PTZ Control Panel	<p>Hold and press the direction button to pan/tilt the camera.</p> <p>Click  and the camera keeps panning, the icon turns into .</p> <p>Click the icon again to stop the camera.</p> <p>Note: This type of camera model does not support auto scan.</p>
	Zoom out/in	<p>Click , the lens zooms in, click , and the lens zooms out.</p>
	Focus far/near	<p>Click , the lens focus far and the items far away gets clear. Click , the lens focus near and the items nearby gets clear.</p>

Button	Name	Description
	Iris close/open	When the image is too dark, click  to open the iris. When the image is too bright, click  to close the iris.
	Auxiliary Functions	The auxiliary functions include light, wiper, auxiliary focus, lens initialization, and 3D positioning, etc.
	Speed Adjustment	Adjust speed of pan/tilt movements.
	Preset	Refer to 4.4.3 for detailed information of setting preset.

- **Buttons on the Preset interface:**

Table 4-3 Descriptions of Buttons






Buttons	Description
	Call the selected preset.
	Set the selected preset.
	Delete the selected preset.


4.4.2 Auxiliary Functions


The Auxiliary functions panel is shown in Figure 4-5.



Figure 4-5 Auxiliary Functions


-  Light
Click  to enable/disable the light supplement of the camera. This function is reserved.
-  Wiper
Click  to move the wiper once.
-  Auxiliary Focus
The auxiliary focus function is reserved.

-  Lens Initialization

Click  to initialize the lens. The function varies depending on different camera models.

-  3D Positioning

Steps:

1. Click  on the toolbar of live view interface.
2. Operate the 3D positioning function:
 - Click a position of the live video. The corresponding position will be moved to the center of the live video.
 - Hold down the left mouse button and drag the mouse to the lower right on the live video. The corresponding position will be moved to the center of the live video and zoomed in.
 - Hold down the left mouse button and drag the mouse to the upper left on the live video. The corresponding position will be moved to the center of the live video and zoomed out.

Note:

For the multichannel camera that supports panorama linkage, the operations to panoramic camera channels are displayed in PTZ camera channel.

4.4.3 Setting/Calling a Preset

Purpose:

A preset is a predefined image position. For the defined preset, you can click the calling button to quickly view the desired image position.

- **Setting a Preset:**

Steps:

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

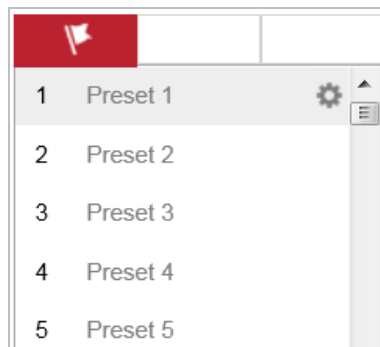




Figure 4-6 Setting a Preset

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

4. Edit a preset name by double clicking on the default name such as preset 1. (The pre-defined presets are named already and not configurable. Refer to the user manual for detailed function description.)
5. You can click  to delete the preset.



You can configure up to 300 presets.

- **Calling a Preset:**


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



Figure 4-7 Calling a Preset

For convenient preset selection, refer to the following steps to navigate to the preset you want.

Steps:

1. Select any preset from the list.
2. Click the preset number you need on the keyboard.



The following presets are predefined with special commands. You can only call them but not configure them.

Table 4-4 Special Presets

Preset	Function	Preset	Function
34	Back to origin	92	Set manual limits
39	Day mode	93	Save manual limits
40	Night mode	94	Remote reboot

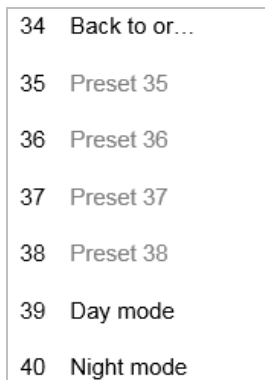


Figure 4-8 Special Preset

4.5 Playback

Purpose:

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

4.5.1 Play Back Video Files

Steps:

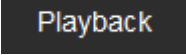
1. Click  on the menu bar to enter playback interface.



Figure 4-9 Playback Interface

2. Select the date and click .

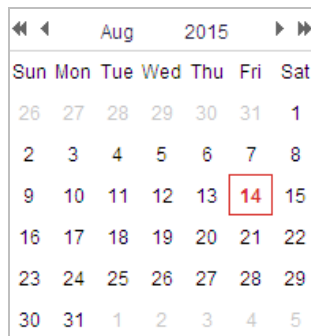



Figure 4-10 Search Video











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

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





Figure 4-11 Playback Toolbar

Table 4-5 Description of the buttons

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



You can choose the file paths locally for downloaded playback video files and pictures in Local Configuration interface. Refer to **Section 4.1 Configuring Local Parameters** for details.

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

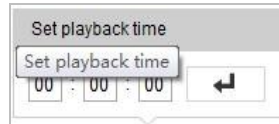


Figure 4-12 Set Playback Time

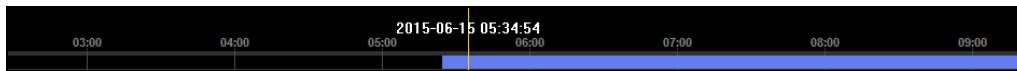


Figure 4-13 Progress Bar

The different colors of the video on the progress bar stand for the different video types as shown in Figure 4-14.

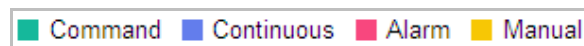



Figure 4-14 Video Types

4.5.2 Downloading Video Files

Steps:

1. Click  on the playback interface. The pop-up menu is shown in Figure 4-15.
2. Set the start time and end time. Click **Search**. The corresponding video files are listed on the left.

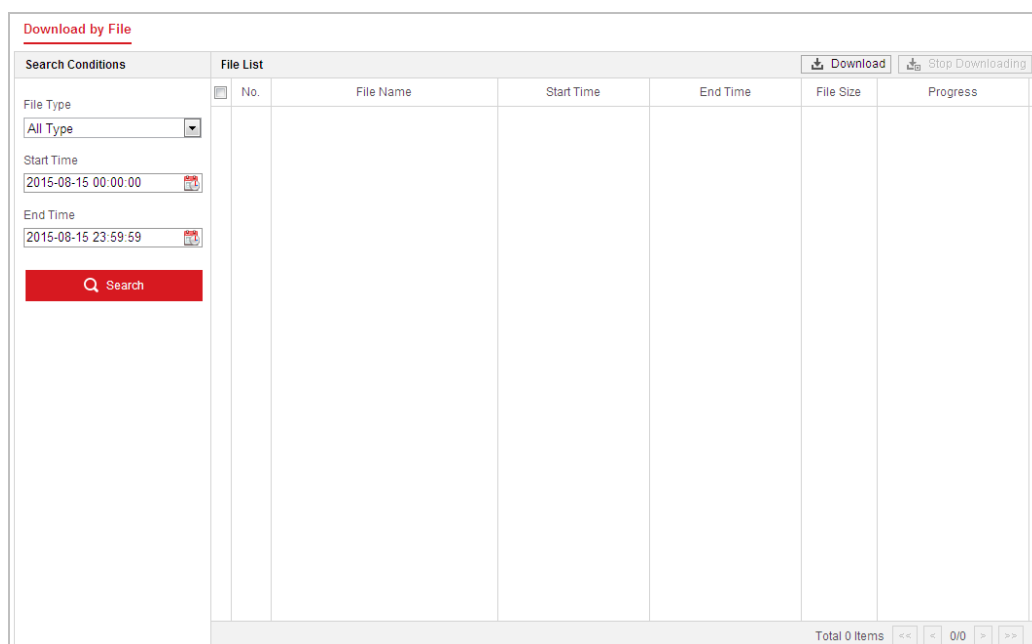



Figure 4-15 Video Downloading interface

3. Check the checkbox in front of the video files that you need to download.
4. Click  **Download** to download the video files.

Chapter 5 System Configuration

5.1 Storage Settings

Before you start:

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

5.1.1 Configuring Recording Schedule

Purpose:

There are two kinds of recording for the camera: manual recording and scheduled recording. 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 memory card (if supported) or in the network disk.

Steps:

1. Enter Record Schedule settings interface:

Configuration > Storage > Schedule Settings > Record Schedule

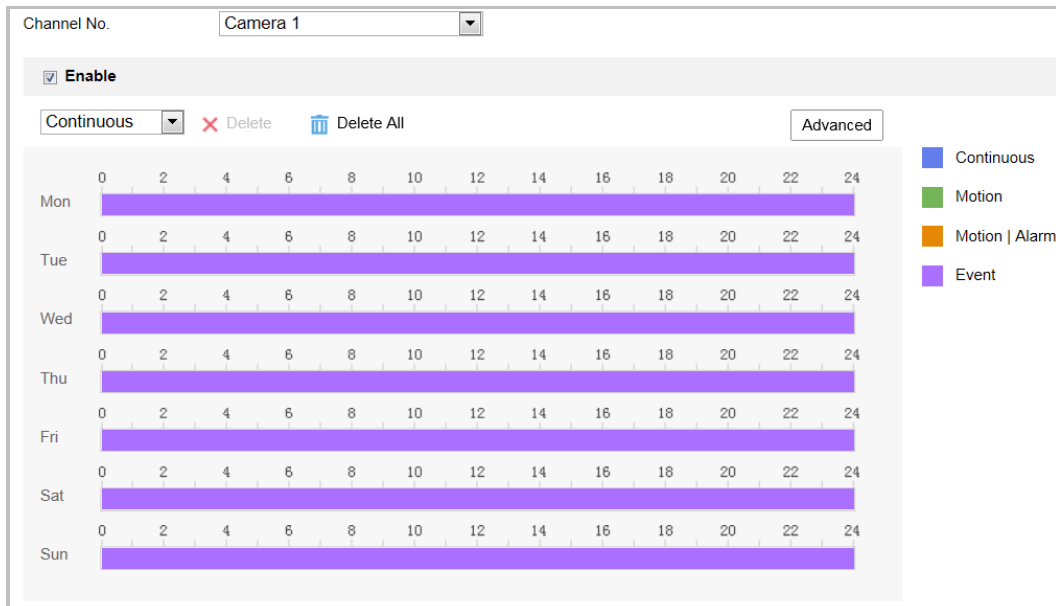


Figure 5-1 Recording Schedule Interface

2. Select the camera channel to configure.
3. Check **Enable** to enable scheduled recording.
4. To set the advanced settings of the camera, click **Advanced** to enter the advanced settings interface.

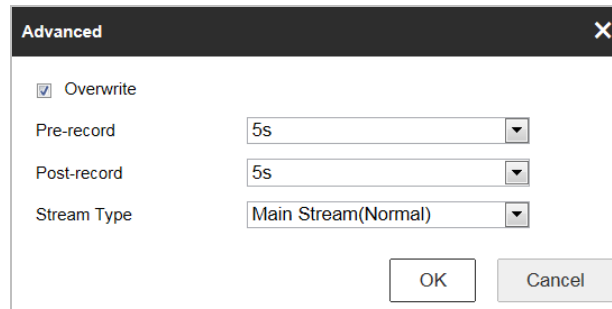


Figure 5-2 Record Parameters

- **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.




The pre-record time changes according to the video bitrate.

- **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.
- **Stream Type:** You can select the stream type for recording.



The Pre-record and Post-record parameters vary depending on different camera models.

5. Click **OK** to save the advanced setting.
6. Select a Record Type. The record type can be Continuous, Motion, Motion | Alarm, and Event.
 - Normal: 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 **Trigger Channel** in the Linkage Method of Motion Detection settings interface. For detailed information, refer to Section **Motion Detection**.
 - 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 settings interfaces.
 - Record Triggered by Event: If you select to record by event, the video will be recorded when any of the events is triggered.
7. Click  Save to save the settings.

5.1.2 Configuring Capture Schedule

Purpose:

You can configure the scheduled snapshot and event-triggered snapshot. The captured picture can be stored in the local storage or network storage.

Note:

FTP is invalid when sub-stream is enabled.

Steps:

1. Enter the Snapshot settings interface:

Configuration > Storage > Storage Settings > Capture

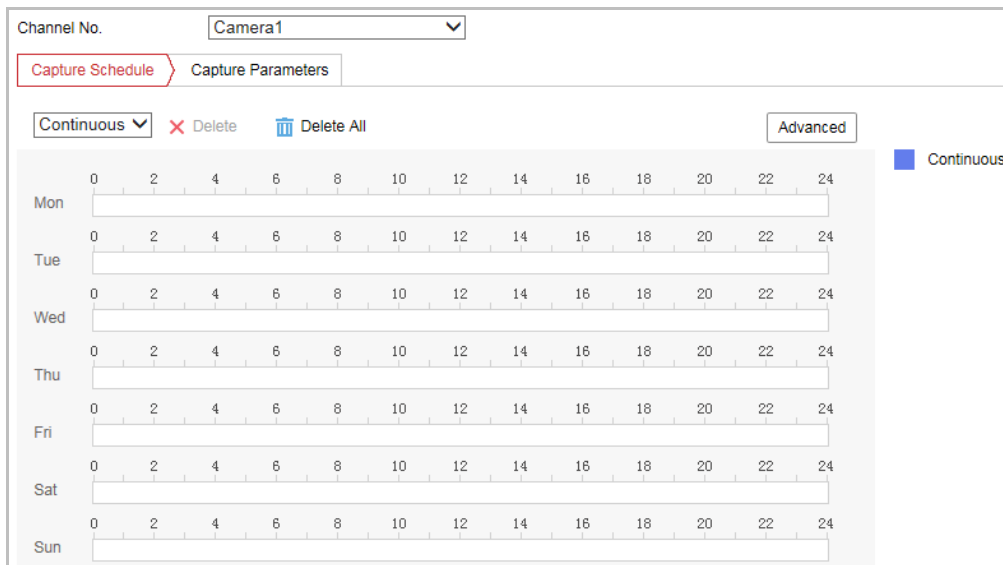



Figure 5-3 Snapshot Settings

2. Click **Capture Schedule** to enter the capture schedule interface.
3. Select the timeline of a certain day, and drag the left button of the mouse to set the capture schedule (the start time and end time of the recording task).
4. After you set the scheduled task, you can click  and copy the task to other days (optional).
5. After setting the capture schedule, you can click a capture segment to display the segment capture settings interface to edit the segment capture parameters. (optional)

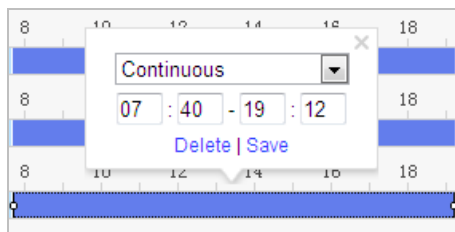


Figure 5-4 Segment Snapshot Settings

6. Click **Advanced** to enter the advanced setting interface. You can select the stream type of the capture.

7. Click **Capture Parameters** to enter the capture parameters Interface.
8. Check **Enable Timing Snapshot** to enable continuous snapshot, and configure the schedule of timing snapshot. Check **Enable Event-triggered Snapshot** to enable event-triggered snapshot.
9. Select the format, resolution, quality of the snapshot.
10. Set the time interval between two snapshots.
11. Click **Save** to save the settings.

Uploading to FTP



Make sure that the FTP server is online.

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

- **Upload continuous snapshots to FTP**

Steps:

- 1) Configure the FTP settings and check **Upload Picture** in FTP Settings interface. Refer to **Section 6.1.2 Configuring FTP Settings** for more details to configure FTP parameters.
- 2) Check **Enable Timing Snapshot**.
- 3) Click **Edit** to set the snapshot schedule. Refer to **Section 5.2.1 Configuring Motion Detection**.

- **Upload event-triggered snapshots to FTP**

Steps:

- 1) Configure the FTP settings and check **Upload Picture** in FTP Settings interface. Refer to **Section 6.1.2 Configuring Settings** for more details to configure FTP parameters.
- 2) Check **Upload to FTP** in Motion Detection Settings interface. Refer to **Section 5.2.1 Configuring Motion Detection**.
- 3) Check **Enable Event-triggered Snapshot**.

5.1.3 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:

- **Add the network disk**

1. Enter NAS (Network-Attached Storage) settings interface:
Configuration > Storage > Storage Management > Net HDD

HDD Management **Net HDD**

Net HDD				
HDD No.	Server Address	File Path	Type	Delete
1	10.10.36.61	/cxy_1	NAS	✘
Mounting Type: <input type="text" value="SMB/CIFS"/> User Name: <input type="text" value="cxy1"/> Password: <input type="password" value="••••••"/> <input type="button" value="Test"/>				
2	10.10.36.252	/dvr/yanjian_1	NAS	✘
3			NAS	✘

Figure 5-5 Select Net HDD Type

- Input the IP address and the file path of the network disk.
- Select the mounting type. NFS and SMB/CIFS are selectable. You can set the user name and password to guarantee the security if SMB/CIFS is selected.



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 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.

- Click  to add the network disk.

- Initialize the added network disk.**

- Enter 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.

HDD Management Net HDD

HDD Management							Format
<input checked="" type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress
<input checked="" type="checkbox"/>	9	9.84GB	0.00GB	Normal	NAS	R/W	
<input checked="" type="checkbox"/>	10	10.00GB	6.75GB	Normal	NAS	R/W	

Quota

Max. Record Capacity

Free Size for Record

Percentage of Record %

Figure 5-6 Storage Management Interface

- 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** as shown in Figure 5-7.

HDD Management							Format
<input checked="" type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress
<input checked="" type="checkbox"/>	9	20.00GB	0.00GB	Formatting	NAS	R/W	

Figure 5-7 View Disk Status

- **Define the Quota for Record and Pictures**

- Input the quota percentage for picture and for record.
- Click **Save** and refresh the browser page to activate the settings.

Quota

Max. Record Capacity

Free Size for Record

Percentage of Record %

Figure 5-8 Quota Settings



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



5.2 Basic Event Configuration

Purpose:

This section explains how to configure the network camera to respond to alarm events, including motion detection, video tampering, and exception. These events can trigger the alarm actions, such as Send Email, Notify Surveillance Center, etc.

For example, when motion detection is triggered, the network camera sends a notification to an e-mail address.



- On the event configuration page, click  to show the PTZ control panel or click  to hide it.
- Click the direction buttons to control the pan/tilt movements.
- Click the zoom/iris/focus buttons to realize lens control.
- The functions vary depending on different camera models.

5.2.1 Configuring Motion Detection

Purpose:

Motion detection is a feature which can trigger alarm actions and actions of recording videos when the motion occurred in the surveillance scene.

Steps:

1. Enter the Motion Detection settings interface:
Configuration > Event > Basic Event > Motion Detection
2. Select the Channel No. from the dropdown list.
3. Set the Motion Detection Area.
 - i. Check the **Enable Motion Detection** checkbox.
 - ii. Check the **Enable Dynamic Analysis for Motion** checkbox.
4. Select the configuration mode as *Normal* or *Expert* and set the corresponding motion detection parameters.
 - **Normal:**

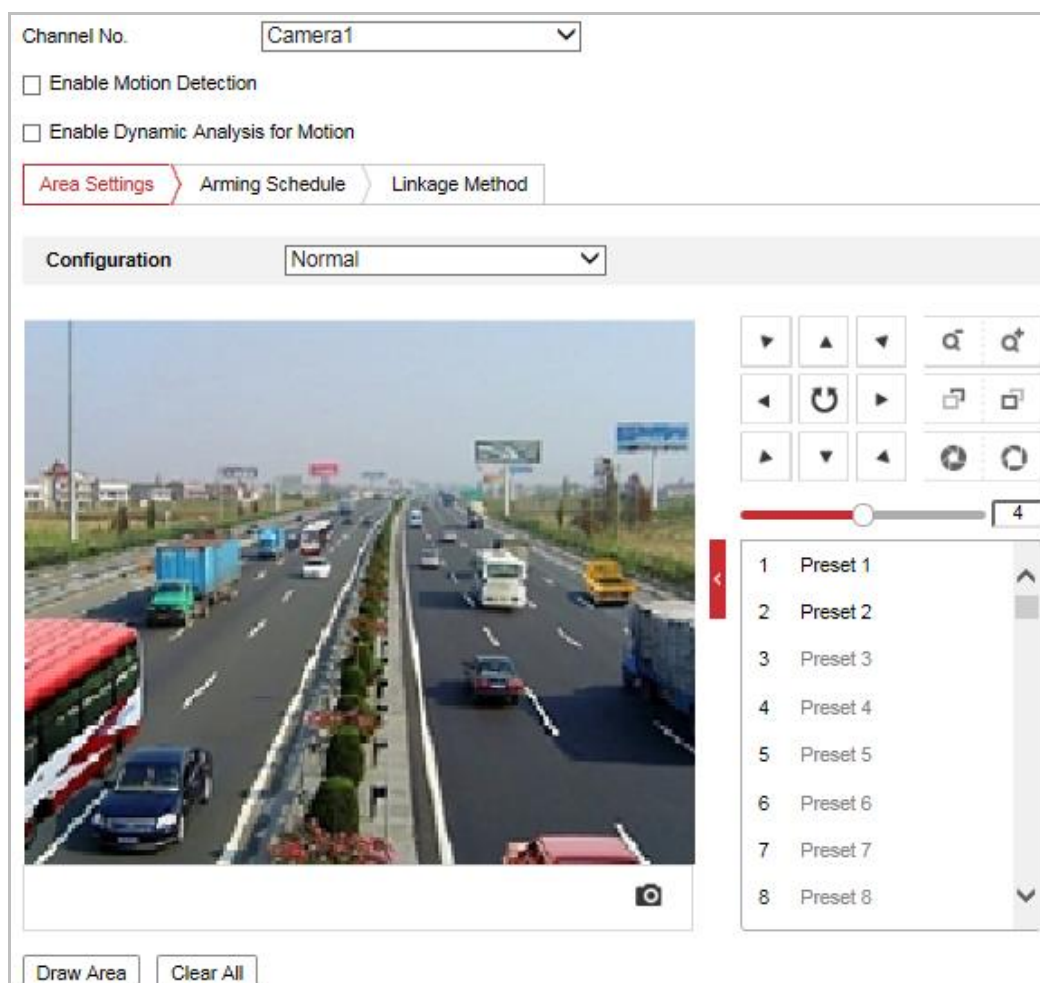



Figure 5-9 Motion Detection Settings-Normal

- i. Click **Draw Area**. Drag the mouse on the live view image to draw a motion detection area.
- ii. Click **Stop Drawing** to finish drawing.
- iii. Move the slider  to set the sensitivity of the detection.

- **Expert:**

Note:

To send the Email when an event occurs, you need to refer to **Section Configuring FTP Settings**

Purpose:

You can set a FTP server and configure the following parameters for uploading captured pictures.

Note:

FTP function is invalid when the sub-stream is enabled

Steps:

1. Enter the FTP settings interface:

Configuration > Network > Advanced Settings > FTP

Server Address	<input type="text" value="0.0.0.0"/>
Port	<input type="text" value="21"/>
User Name	<input type="text"/> <input type="checkbox"/> Anonymous
Password	<input type="password"/>
Confirm	<input type="password"/>
Directory Structure	<input type="text" value="Save in the root directory"/> ▼
Picture Filing Interval	<input type="text" value="OFF"/> ▼ Day(s)
Picture Name	<input type="text" value="Default"/> ▼
	<input type="checkbox"/> Upload Picture
	<input type="button" value="Test"/>

Figure 5-11 FTP Settings

2. Configure the FTP settings, including server address, port, user name, password, directory, and upload type.



The server address supports both the domain name and IP address formats.



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

- **Setting the directory in FTP server for saving files:**

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

- ◆ **Root directory:** The files will be saved in the root of FTP server.
- ◆ **Parent directory:** The files will be saved in a folder in FTP server. The name of folder can be defined as shown in Figure 6-9.

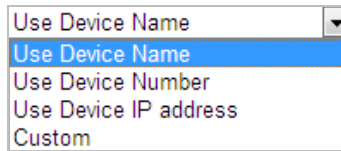


Figure 5-12 Parent Directory

- ◆ **Child directory:** It is a sub-folder which can be created in the parent directory. The files will be saved in a sub-folder in FTP server. The name of folder can be defined as shown in Figure 6-10.

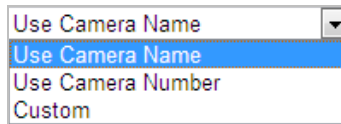


Figure 5-13 Child Directory

- **Upload type:** To enable uploading the captured picture to the FTP server.
3. Click **Save** to save the settings.
 4. You can click **Test** to confirm the configuration.



If you want to upload the captured pictures to FTP server, you also have to enable the continuous snapshot or event-triggered snapshot in **Snapshot** interface.

Configuring Email Settings to set the Email parameters.

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

Note: You need a FTP server and set FTP parameters first. Refer to Section FTP for setting FTP parameters.

- **Trigger Recording:** Record a video when an event occurs.

Note:

You have to set the recording schedule to realize this function. Refer to **Section 5.1.1 Configuring Recording Schedule** for settings the recording schedule.

- **PTZ Linking:**

Target Linkage: The PT camera channel moves to capture the detected motion and upload captured picture to surveillance center. **Response Time** here means the time interval between two linkage actions. You can specify the **Response Time** to avoid too frequent camera movement.

5.2.2 Configuring Video Tampering Alarm

Purpose:

You can configure the camera to trigger the alarm actions when the lens is covered.

Steps:

1. Enter Video Tampering settings interface :

Configuration > Event > Basic Event > Video Tampering

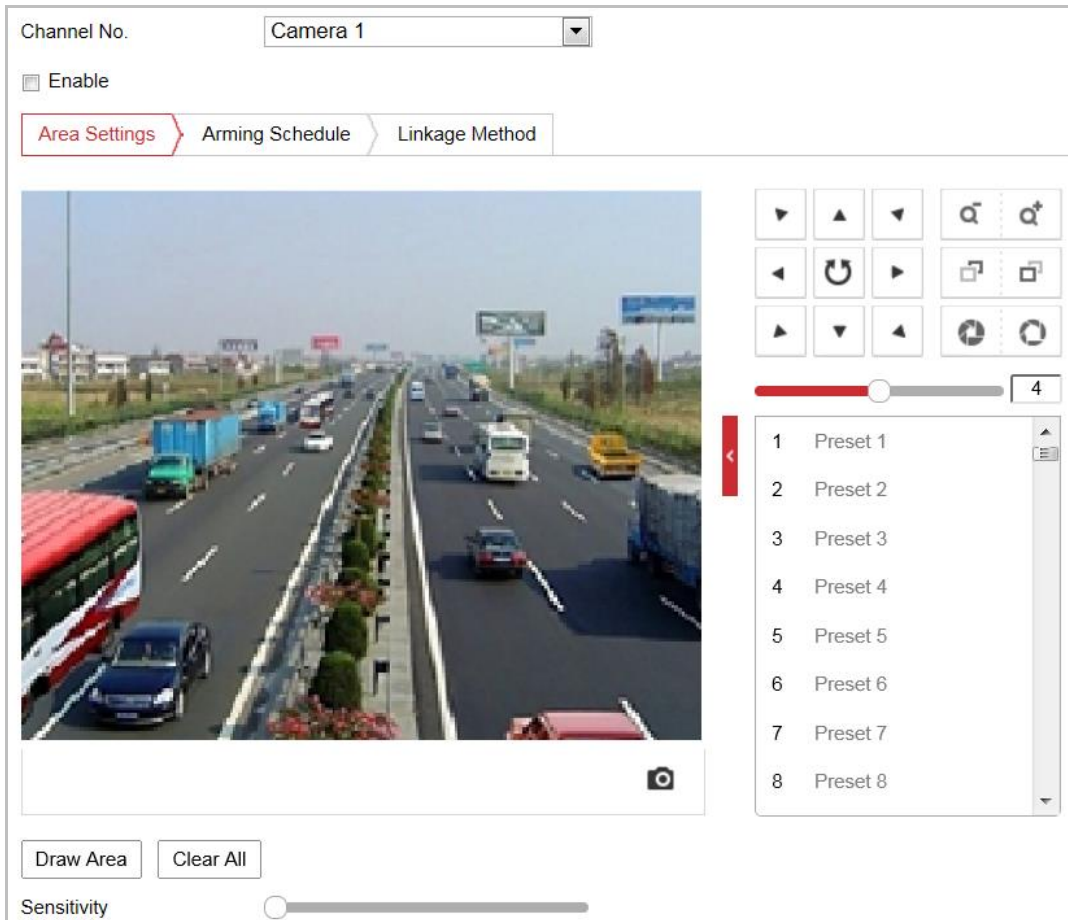


Figure 5-14 Tampering Alarm

2. Select the camera channel to configure.
3. Check **Enable** to enable the tampering detection.
4. Click **Draw Area**. Drag the mouse on the live view image to draw a motion detection area.
5. Click **Stop Drawing** to finish drawing or click **Clear All** to clear all of the areas you set without saving them.
6. **Sensitivity**: Move the slider to set the sensitivity of alarm action. The levels of sensitivity can be set as **Low**, **Medium**, and **High**. The higher the value is, the easier the alarm will be triggered.
7. Click **Arming Schedule** tab to enter the arming schedule setting interface. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection**.
8. Click **Linkage Method** tab to select the linkage method taken for tampering, notify surveillance center, and send email are selectable. Refer to **Section 5.2.1 Configuring Motion Detection**.
9. Click **Save** to save the settings.

5.2.3 Configuring Alarm Input

Note:

This function varies depending on different camera models.

Steps:

1. Enter the Alarm Input settings interface:

Configuration > Event > Basic Event > Alarm Input

2. Choose the Alarm Input No. and the Alarm Type. The alarm type can be NO (Normally Open) and NC (Normally Closed).

3. Edit the name in (cannot copy) to set a name for the alarm input (optional).

Figure 5-15 Alarm Input Settings

4. Click **Arming Schedule** tab to enter the arming schedule setting interface. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection**.
5. Click **Linkage Method** tab to select the linkage method taken for tampering, notify surveillance center, and send email are selectable. Refer to **Section 5.2.1 Configuring Motion Detection**.
6. You can also choose the PTZ linking for the alarm input. Check the relative checkbox and select the No. to enable Preset Calling, Patrol Calling or Pattern Calling.
7. You can copy your settings to other alarm inputs.
8. Click **Save** to save the settings.

Arming Schedule		Linkage Method	
<input type="checkbox"/> Normal Linkage	<input type="checkbox"/> Trigger Alarm Output	<input type="checkbox"/> Trigger Recording	PTZ Linking A1
<input type="checkbox"/> Send Email <input type="checkbox"/> Notify Surveillance Center <input type="checkbox"/> Upload to FTP/Memory Card/...	<input type="checkbox"/> A->1 <input type="checkbox"/> A->2	<input type="checkbox"/> A1	<input type="checkbox"/> Preset No. 1
			Duration 0 s
			<input type="checkbox"/> Patrol No. 1
			<input type="checkbox"/> Pattern 1

Figure 5-16 Linkage Method

5.2.4 Configuring Alarm Output

Note:

This function varies depending on different camera models.

Steps:

1. Enter the Alarm Output settings interface:
Configuration > Event > Basic Event > Alarm Output
2. Select one alarm output channel in the **Alarm Output** dropdown list.
3. Set a name in (cannot copy) for the alarm output (optional).
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. Click tab to enter the arming schedule setting interface. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection**.

Alarm Output No. IP Address

Delay Alarm Name

Alarm Status (cannot copy)

Arming Schedule

Mon	0	2	4	6	8	10	12	14	16	18	20	22	24
Tue	0	2	4	6	8	10	12	14	16	18	20	22	24
Wed	0	2	4	6	8	10	12	14	16	18	20	22	24
Thu	0	2	4	6	8	10	12	14	16	18	20	22	24
Fri	0	2	4	6	8	10	12	14	16	18	20	22	24
Sat	0	2	4	6	8	10	12	14	16	18	20	22	24
Sun	0	2	4	6	8	10	12	14	16	18	20	22	24

Figure 5-17 Alarm Output Settings

- You can copy the settings to other alarm outputs.
- Click to save the settings.

5.2.5 Handling Exception

The exception type can be HDD full, HDD error, and illegal login to the cameras.

Steps:

- Enter Exception settings interface:
Configuration > Event > Basic Event > Exception
- Check the checkbox to set the actions taken for the exception alarm. Refer to **Section 5.2.1 Configuring Motion Detection**.

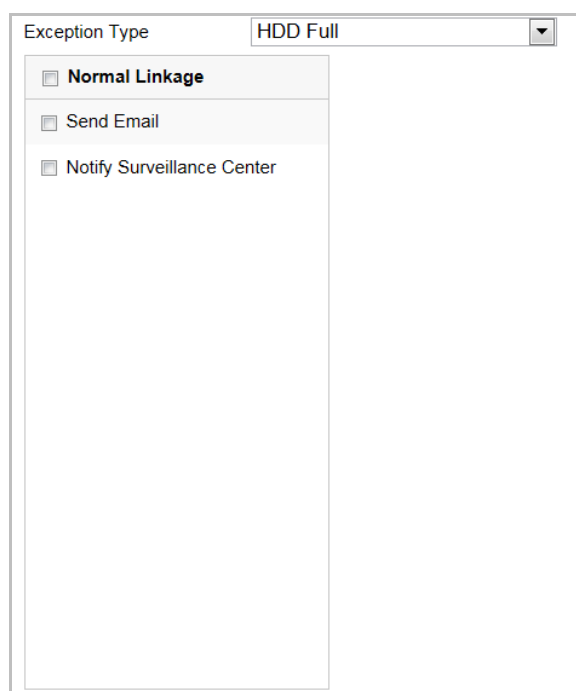


Figure 5-18 Exception Settings

3. Click  to save the settings.

5.3 Smart Event Configuration



The functions vary depending on different camera models.

5.3.1 Detecting Audio Exception

Purpose:

When you enable this function and audio exception occurs, the alarm actions will be triggered.

Steps:

1. Enter Audio Exception Detection interface:
Configuration > Event > Smart Event > Audio Exception Detection

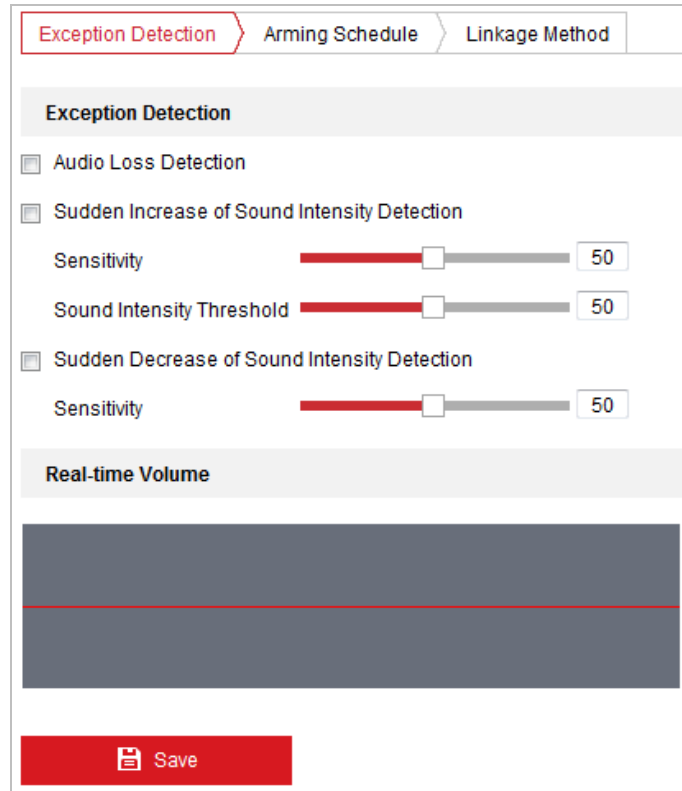


Figure 5-19 Audio Exception Detection

2. Check **Audio Loss Detection** to enable the audio input exception detection.
3. Check **Sudden Increase of Sound Intensity Detection** to enable the sudden rise detection.
 - **Sensitivity:** Range [1-100], the smaller the value the more severe the sound change will 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 actual environment.
4. Check **Sudden Decrease of Sound Intensity Detection** to enable the sudden drop detection.
 - **Sensitivity:** Range [1-100], the smaller the value the more severe the sound change will trigger the detection.
5. Click **Arming Schedule** tab to enter the arming schedule setting interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection**.
6. Click **Linkage Method** tab to select the linkage method taken for the audio input exception, Notify Surveillance Center, Send Email, and Trigger Recording are selectable. Refer to **Section 5.2.1 Configuring Motion Detection**.
7. Click **Save** to save the settings.

5.3.2 Configuring Intrusion Detection

Intrusion detection can set an area in the surveillance scene and once the area is entered, a set of alarm action is triggered.

Steps:

1. Enter Intrusion Detection interface:

Configuration > Events > Smart Event > Intrusion Detection

2. Check **Enable**.

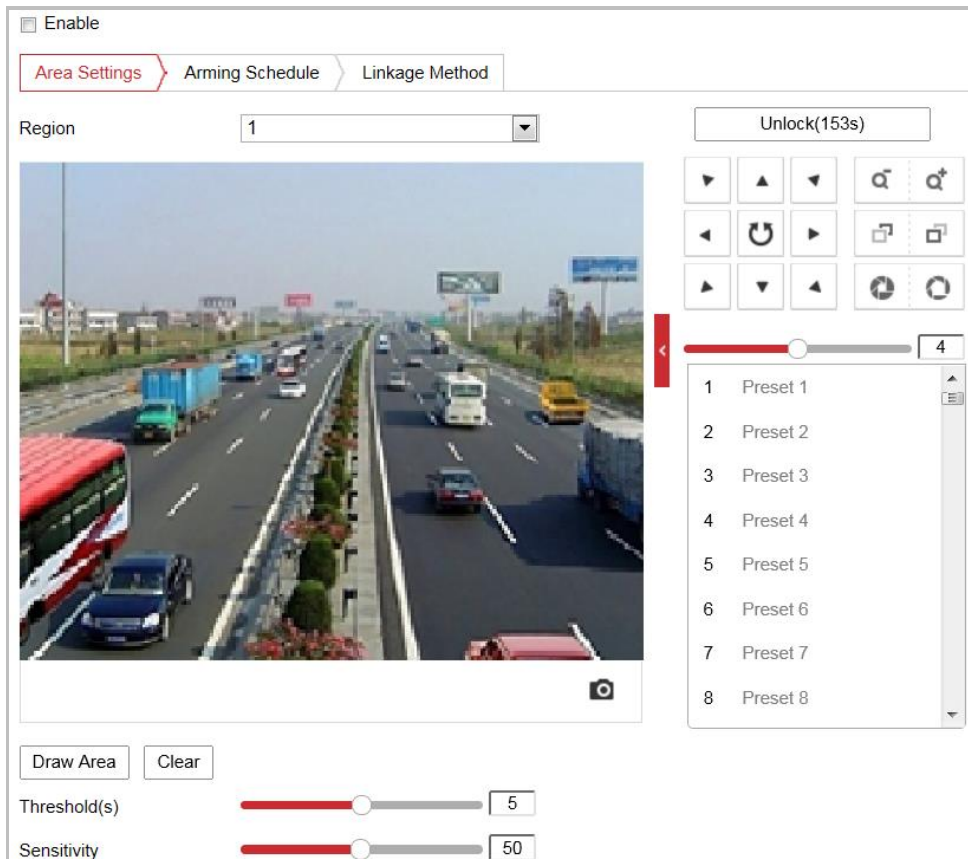


Figure 5-20 Configuring Intrusion Area

3. The event triggered and park action related PTZ movement will be locked for 180 seconds after you enter the intrusion detection interface. Optionally, you can click the




Unlock(69s)

button to manually activate the movement, or lock the movement

when the button turns to Lock by clicking it.

4. Draw area.



- 1) Select the Region No.in dropdown list.
- 2) Click Draw Area to draw a rectangle on the image as a defense region.
- 3) Click on the image to specify a corner of the rectangle, and right-click the mouse after four corners are configured.

5. Configure the parameters for each defense region separately.
 - **Threshold:** Range [0-10s], the threshold for the time of the object loitering in the region. If you set the value as 0, alarm is triggered immediately after the object entering the region.
 - **Sensitivity:** Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.
6. Click  tab to enter the arming schedule setting interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection**.
7. Click  tab to select the linkage method taken for intrusion detection, Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, and Trigger Recording are selectable. Refer to **Section 5.2.1 Configuring Motion Detection**.
8. Click  to save the settings.

5.3.3 Configuring Line Crossing Detection

The virtual plane detection can be adopted for the intrusion detection. Once the virtual plane is detected being traversed according to the configured direction, a set of alarm action is triggered.

Steps:

1. Enter Line Crossing Detection interface:
Configuration >Event > Smart Event > Line Crossing Detection
2. Check **Enable** to enable the line crossing detection function.
3. Select the Line in dropdown list to configure.
4. The event triggered and park action related PTZ movement will be locked for 180 seconds after you enter the line crossing detection interface. Optionally, you can click the  button to manually activate the movement, or lock the movement when the button turns to  by clicking it.

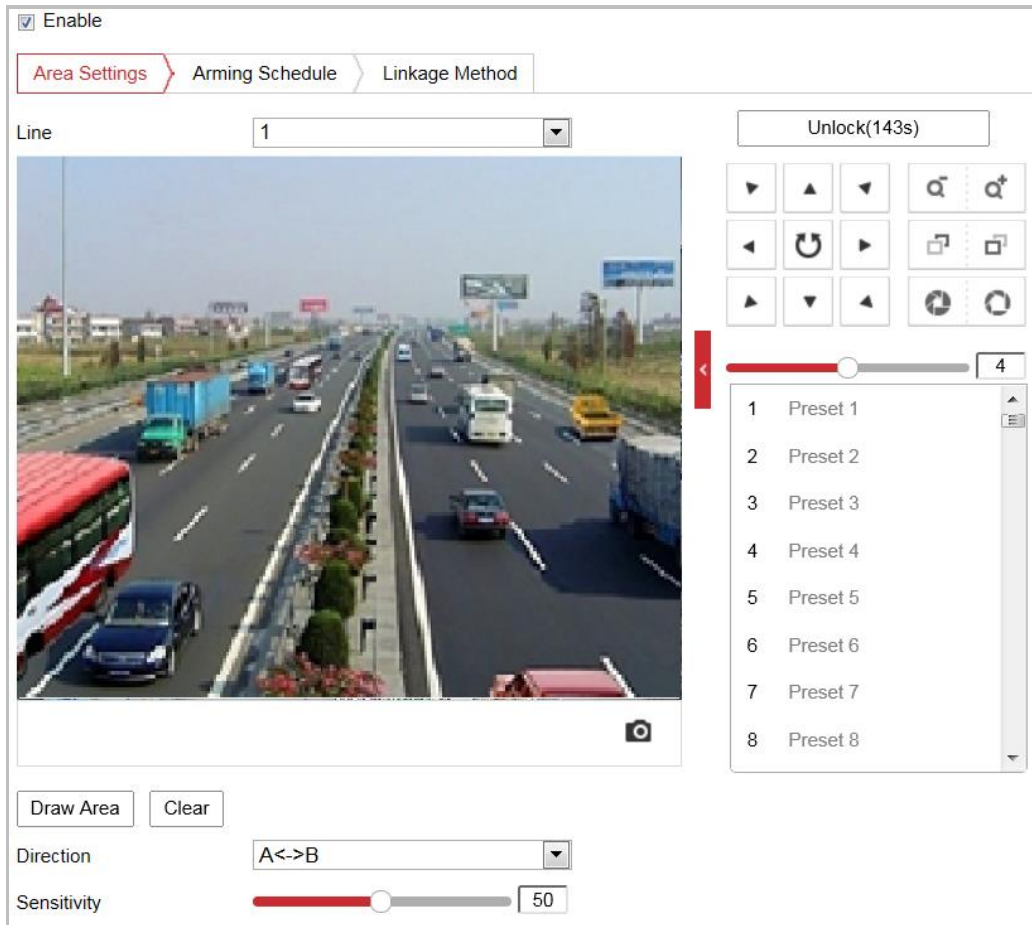


Figure 5-21 Configuring Line

5. Draw area.

- 1) Click **Draw Area** to draw a line on the image.
- 2) Click the line to switch to the editing mode.

Drag an end to the desired place to adjust the length and angle of the line. And drag the line to adjust the location.

6. Configure the parameters for each defense region separately.

- **Direction:** Select the detection direction in the dropdown list, there are A<->B, A->B and B->A selectable.
- **Sensitivity:** Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.



7. Click **Arming Schedule** tab to enter the arming schedule setting interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection**.8. Click **Linkage Method** tab to select the linkage method taken for the line crossing detection, Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Recording

are selectable. Refer to **Section 5.2.1 Configuring Motion Detection**.

- Click  to save the settings.

5.4 PTZ Configuration



- On the event configuration page, click  to show the PTZ control panel or click  to hide it.
- Click the direction buttons to control the pan/tilt movements.
- Click the zoom/iris/focus buttons to realize lens control.
- The functions vary depending on different camera models.

5.4.1 Configuring Basic PTZ Parameters

You can configure the basic PTZ parameters, including proportional pan, preset freezing, preset speed, etc.

- Enter Basic Settings interface:


Configuration > PTZ > Basic Settings

Basic Parameter	
<input type="checkbox"/>	Enable Proportional Pan
<input type="checkbox"/>	Enable Preset Freezing
Preset Speed	4
Manual Control Speed	Auto
Keyboard Control Speed	Medium
Max. Tilt-angle	(0 - 90)Degree
Zooming Speed	3
PTZ OSD	
Zoom Status	2s
PT Status	2s
Preset Status	2s
Power Off Memory	
Set Resume Time Point	30s

Figure 5-22 Basic Settings

- Configure the following settings:

- **Basic Parameters:** Set the basic parameters of PTZ.
 - ◆ **Proportional Pan:** If you enable this function, the pan/tilt speeds change according to the amount of zoom. When there is a large amount of zoom, the pan/tilt speed will be slower for keeping the image from moving too fast on the live view image.

- ◆ **Preset Freezing:** This function enables the live view to switch directly from one scene defined by a preset to another, without showing the middle areas between these two, to ensure the surveillance efficiency. It can also reduce the use of bandwidth in a digital network system.
 - ◆ **Preset Speed:** You can set the speed of a defined preset from 1 to 8.
 - ◆ **Manual Control Speed:** The manual control speed can be set as Compatible, Pedestrian, Non-motor Vehicle, Motor Vehicle or Auto.
 - Compatible: The control speed is same as the Keyboard Control Speed.
 - Pedestrian: Choose the **Pedestrian** when you monitor the pedestrians.
 - Non-motor Vehicle: Choose the **Non-motor Vehicle** when you monitor the non-motor vehicles.
 - Motor Vehicle: Choose the **Motor Vehicle** when you monitor the motor vehicles.
 - Auto: You are recommended to set it as **Auto** when the application scene of the camera is complicated.
 - ◆ **Keyboard Control Speed:** Define the speed of PTZ control by a keyboard as Low, Medium or High.
 - ◆ **Max. Tilt-angle:** Set the tilt-angle of the camera from the dropdown list.
 - ◆ **Zooming Speed:** The zoom speed is adjustable from level 1 to 3.
 - **PTZ OSD:** Set the on-screen display duration of the PTZ status.
 - ◆ **Zoom Status:** Set the OSD duration of zooming status as 2 seconds, 5 seconds, 10 seconds, NC (Normally Closed), or NO (Normally Open).
 - ◆ **PT Status:** Set the azimuth angle display duration while panning and tilting as 2 seconds, 5 seconds, 10 seconds, NC (Normally Closed), or NO (Normally Open).
 - ◆ **Preset Status:** Set the preset name display duration while calling the preset as 2 seconds, 5 seconds, 10 seconds, NC (Normally Closed), or NO (Normally Open).
 - **Power-off Memory:** The camera can resume its previous PTZ status or actions after it restarted from a power-off. You can set the time point of which the dome resumes its PTZ status. You can set it to resume the status of 30 seconds, 60 seconds, 300 seconds or 600 seconds before power-off.
3. Click  to save the settings.

5.4.2 Configuring PTZ Limits

Purpose:


The camera can be programmed to move within the configurable PTZ limits (left/right, up/down).

Steps:

1. Enter Limit configuration interface:
Configuration > PTZ > Limit



Figure 5-23 Configure the PTZ Limit

2. Click **Enable Limit** and choose the limit type.
 - **Manual Stops:**
When manual limit stops are set, you can operate the PTZ control panel manually only in the limited surveillance area.
3. Click the PTZ control buttons to find the left/right/up/down limit stops; you can also call the defined presets and set them as the limits of the camera.
4. Click **Set** to save the limits or click **Clear** to clear the limits.
5. Click  **Save** to save the settings.

5.4.3 Configuring Initial Position

Purpose:

The initial position is the origin of PTZ coordinates. It can be the factory default initial position. You can also customize the initial position according to your own demand.

- **Customize an Initial Position:**



Steps:

1. Enter Initial Position configuration interface:
Configuration > PTZ > Initial Position



Figure 5-24 PTZ Configuration

2. Click the PTZ control buttons to find a position as the initial position of the camera; you can also call a defined preset and set it as the initial position of the camera.
3. Click **Set** to save the position.
- **Call/delete an Initial Position:**

You can click  to call the initial position. You can click  to delete the initial position and restore the factory default initial position.

5.4.4 Configuring Park Actions

Purpose:


This feature allows the camera to start a predefined park action automatically after a period of inactivity (park time).



- **Scheduled Tasks** function is prior to **Park Action** function. When these two functions are set at the same time, only the **Scheduled Tasks** function takes effect.
- Park function varies depending on different camera models.


Steps:

1. Enter Park Action settings interface:
Configuration > PTZ > Park Action



<input checked="" type="checkbox"/> Enable Park Action	
Park Time	5 s
Action Type	Preset
Action Type ID	1

Figure 5-25 Set the Park Action

2. Check **Enable Park Action**.
3. Set the **Park Time** as the inactivity time of the camera before it starts the park actions.
4. Choose **Action Type** from the dropdown list.
5. If you select Preset as Action Type, you need to select Action Type ID from the dropdown list.
6. Click  to save the settings.

5.4.5 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.



You can only configure privacy mask function for tracking PTZ camera.

Steps:

1. Enter Privacy Mask settings interface:
Configuration > PTZ > Privacy Mask

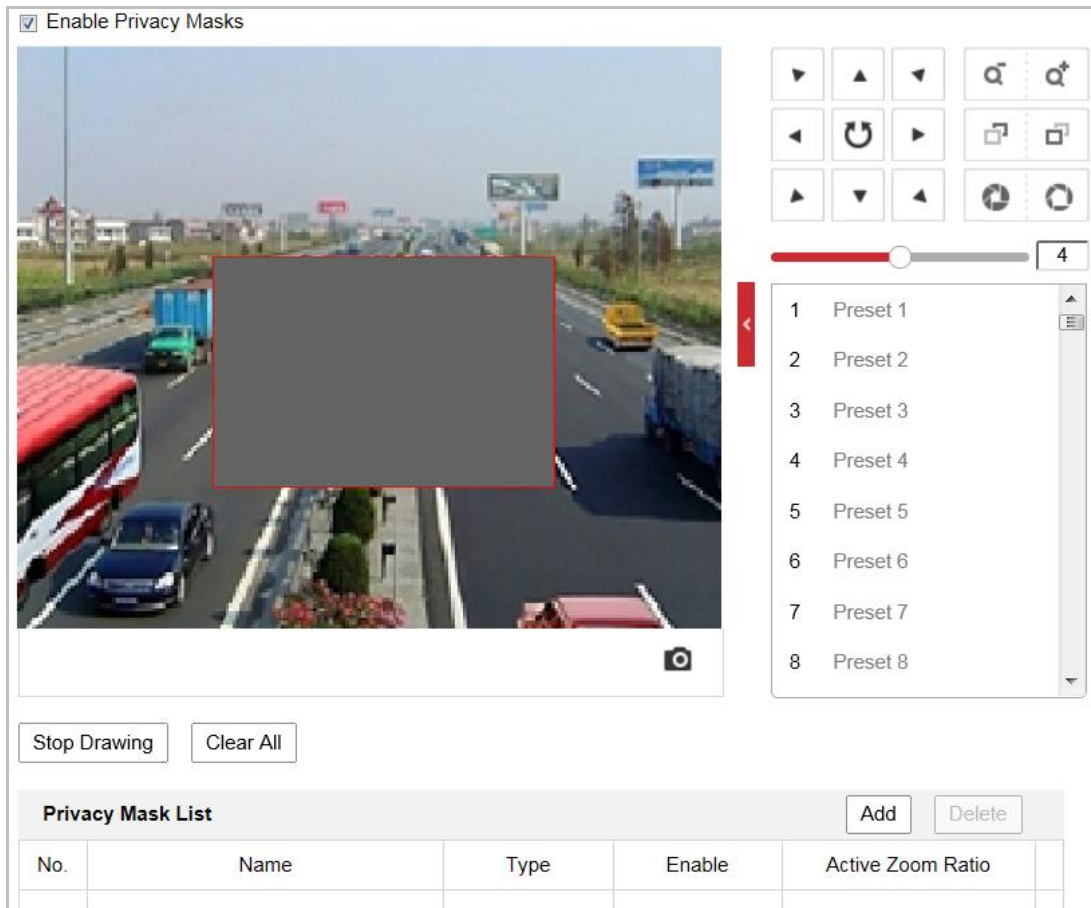


Figure 5-26 Privacy Mask

2. Click the PTZ control buttons to find the area you want to set the privacy mask.
3. Click ; drag the mouse in the live video window to draw the area.
4. You can drag the corners of the red rectangle area to draw a polygon mask.
5. Click to finish drawing or click to clear all of the areas you set without saving them.
6. Click to save the privacy mask, and it will be listed in the **Privacy Mask List** area; set the value of **Active Zoom Ratio** on your demand, and then the mask will only appear when the zoom ratio is greater than the predefined value.

Privacy Mask List					<input type="button" value="Add"/>	<input type="button" value="Delete"/>
No.	Name	Type	Enable	Active Zoom Ratio		
1	Privacy Mask 1	gray	Yes	1		

Figure 5-27 Privacy Mask List

7. Check **Enable Privacy Mask** to enable this function.
8. Click **Save** to save the settings.

5.4.6 Configuring Panorama Linkage

Purpose:

Panorama linkage builds up the connection between the panoramic camera channel and the PTZ camera channel of a multi-channel camera. Once the connection set up, certain live view operations to panoramic camera channels can be displayed in PTZ camera channel.

To use the function, see the operations of 3D positioning on live view page.

To set up the connection, complete calibration. Manual calibration and auto calibration are selectable.

Note:

Panorama linkage function varies depending on different camera models. For indoor camera model, panorama linkage function does not show on the interface. It is set with default parameters. Outdoor camera model supports panorama linkage configuration interface.

● Auto Calibration

Steps:

1. Enter **Panorama Linkage** setting interface. Configuration > PTZ > Panorama Linkage.
2. Click **Start Calibration** and enter the auto calibration interface.
3. Match up the PTZ camera channel with panoramic camera channels.
 - i. Select a panoramic camera channel.
 - ii. Adjust PTZ in PTZ control panel or click 3D positioning to find the same scene in PTZ camera channel.
 - iii. Click **Adjusting succeeded**.
 - iv. Repeat to complete matching for other panoramic camera channels.
4. Click **Next**.
5. Click **One-touch Calibration** or **Single Scene Calibration** and auto calibration starts.

Notes:

- ◆ When you select **One-touch Calibration**, the camera performs calibration one by one starting from panorama view 1 automatically.
- ◆ When you select **Single Scene Calibration**, the camera only perform calibration for the selected panoramic camera channel.

6. Click **Auto Calibrating Succeeded** and exit the auto calibration interface.

● Manual Calibration

Steps:

1. Enter **Panorama Linkage** setting interface. Configuration > PTZ > Panorama Linkage.
2. Select a panoramic camera channel.
3. Click **Add** in Calibration Parameter panel to add a new calibration point.

A numbered green cross displayed on the panoramic image. Drag the green cross to adjust its position.
4. Adjust PTZ to place the green cross in the PTZ camera channel to the same position of the green cross in panoramic camera channel. 1× is recommended.
5. Click **Get PTZ Position**, and the PTZ position is displayed in Calibration Parameter list.
6. Click **Start Calibration**. Repeat the steps above to add more calibration points for the selected panoramic camera channel.

Notes:

- ◆ Up to 12 calibration points are supported. At least 4 points should be added. More calibration points can increase the rate for successful calibration.
 - ◆ Scatter the calibration points equably in live view image for better calibration effect.
7. Repeat above steps to complete calibration for other panoramic camera channel.

5.4.7 Configuring Scheduled Tasks

Purpose:

You can configure the network camera to perform a certain action automatically in a user-defined time period.


Steps:

1. Enter Scheduled Task settings interface:

Configuration > PTZ > Scheduled Tasks

The screenshot displays the 'Scheduled Tasks' configuration page. At the top, there is a checkbox for 'Enable Scheduled Task' which is checked. Below it is a dropdown menu currently set to 'OFF', along with 'Delete' and 'Delete All' buttons. The main area consists of seven rows, one for each day of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun). Each row has a horizontal timeline from 0 to 24 hours with tick marks every 2 hours. A legend on the right side of the interface defines the task types: a grey square for 'OFF', a red square for 'Preset', an orange square for 'Dome Reboot', and a green square for 'Dome Adjust'. At the bottom of the interface, there is a 'Park Time' field with the value '5' and a unit 's'.

Figure 5-28 Configure Scheduled Tasks

2. Check **Enable Scheduled Task**.
3. Set the **Park Time**. You can set the park time (a period of inactivity) before the camera starts the scheduled tasks.
4. Select the task type from the dropdown list.
5. Select the timeline of a certain day, and drag the mouse to set the recording schedule (the start time and end time of the recording task).
6. After you set the scheduled task, you can click  and copy the task to other days (optional).

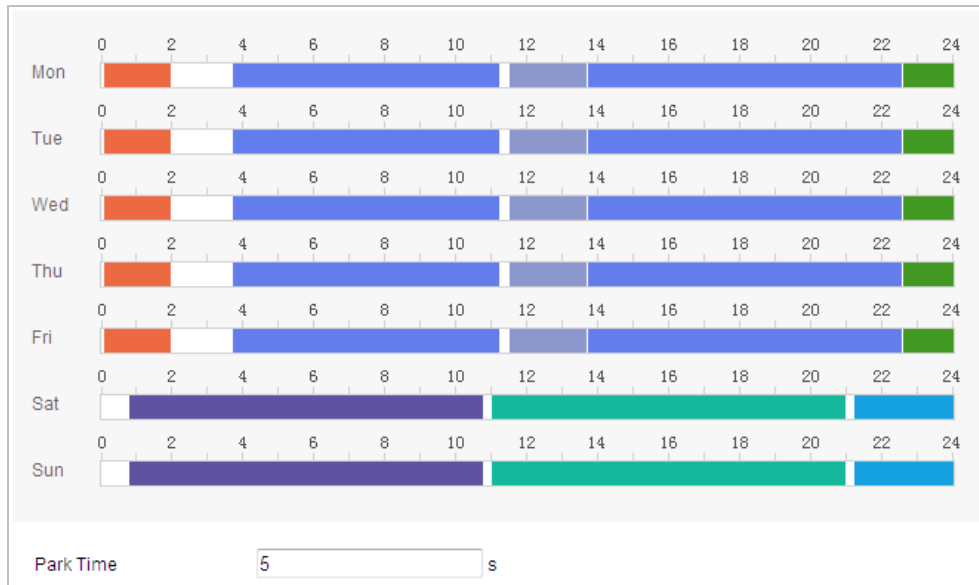


Figure 5-29 Edit the Schedule and Task Type

7. Click  to save the settings.

5.4.8 Clearing PTZ Configuration

Purpose:

You can clear PTZ configurations in this interface, including all presets, privacy masks, PTZ limits, scheduled tasks and park actions.

Steps:

- Enter Clearing Configuration interface:
Configuration > PTZ > Clear Config
- Check the checkbox of the items you want to clear.

Select All

Clear All Presets

Clear All Privacy Masks

Clear All PTZ Limited

Clear All Scheduled Tasks

Clear All Park Action

Figure 5-30 Clear Config

3. Click  to clear the settings.

Chapter 6 Camera Configuration

6.1 Configuring Network Settings



The functions vary depending on different camera models.

6.1.1 Basic Settings

Configuring TCP/IP Settings

Purpose:

TCP/IP settings must be properly configured before you operate the camera over network. IPv4 and IPv6 are both supported.

Steps:

1. Enter TCP/IP settings interface:

Configuration > Network > Basic Settings > TCP/IP

TCP/IP		DDNS	PPPoE	Port	NAT
NIC Type	Auto				
	<input checked="" type="checkbox"/> DHCP				
IPv4 Address	10.16.1.250				Test
IPv4 Subnet Mask	255.255.255.0				
IPv4 Default Gateway	10.16.1.254				
IPv6 Mode	Route Advertisement				View Route Advertisement
IPv6 Address	::				
IPv6 Subnet Mask	0				
IPv6 Default Gateway	::				
Mac Address	c0:56:e3:b3:bc:c0				
MTU	1500				
Multicast Address					
	<input checked="" type="checkbox"/> Enable Multicast Discovery				
DNS Server					
Preferred DNS Server	8.8.8.8				
Alternate DNS Server					

Figure 6-1 TCP/IP Settings

2. Configure the NIC settings, including the **IPv4(IPv6) Address**, **IPv4(IPv6) Subnet Mask** and **IPv4(IPv6) Default Gateway**.

3. Click  to save the above settings.

You can click **Test** to make sure that the IP address is valid.



- If the DHCP server is available, you can check DHCP to automatically obtain an IP address and other network settings from that server.
- The valid value range of Maximum Transmission Unit (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 and configure the gateway of the network camera.
- If the DNS server settings are required for some applications (e.g., sending email), you should properly configure the **Preferred DNS Server** and **Alternate DNS server**.

DNS Server	
Preferred DNS Server	<input type="text" value="8.8.8.8"/>
Alternate DNS Server	<input type="text"/>

Figure 6-2 DNS Server Settings



The router must support the route advertisement function if you select **Route Advertisement** as the IPv6 mode.

Configuring DDNS Settings

Purpose:

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

Before you start:

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



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


Steps:

1. Enter DDNS settings interface:
Configuration > Network > Basic Settings > DDNS
2. Check **Enable DDNS** 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, input the domain name obtained from the DynDNS website.
- (3) Input the **Port** of DynDNS server.
- (4) Input the **User Name** and **Password** registered on the DynDNS website.
- (5) Click  to save the settings.

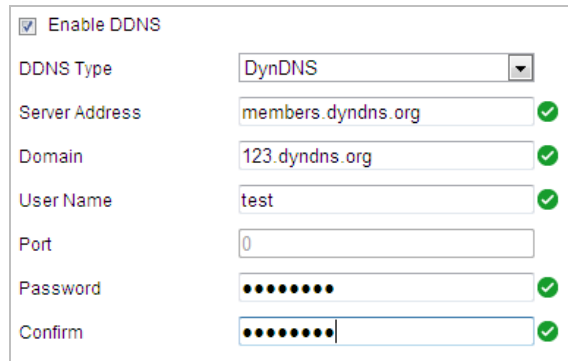



Figure 6-3 DynDNS Settings

- **NO-IP:**

Steps:

- (1) Enter **Server Address** of NO-IP.
- (2) In the **Domain** text field, input the domain name obtained from the NO-IP website.
- (3) Input the **Port** of NO-IP server.
- (4) Input the **User Name** and **Password** registered on the NO-IP website.
- (5) Click  to save the settings.

Configuring PPPoE Settings

Purpose:

If you have no router but only a modem, you can use Point-to-Point Protocol over Ethernet (PPPoE) function.

Steps:

1. Enter PPPoE settings interface:

Configuration > Network > Basic Settings > PPPoE



Figure 6-4 PPPoE Settings


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



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



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

4. Click  to save and exit the interface.

Configuring Port Settings

Purpose:

If there is a router and you want to access the camera through Wide Area Network (WAN), you need to forward the 3 ports for the camera.

Steps:

1. Enter Port settings interface:

Configuration > Network > Basic Settings > Port

HTTP Port	<input type="text" value="80"/>
RTSP Port	<input type="text" value="554"/>
HTTPS Port	<input type="text" value="443"/>
Server Port	<input type="text" value="8000"/>

Figure 6-5 Port Settings

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

HTTP Port: The default port number is 80.

RTSP Port: The default port number is 554.

HTTPS Port: The default port number is 443.

Server Port: The default port number is 8000.

3. Click  to save the settings.

Configuring NAT (Network Address Translation) Settings

Purpose:

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 house and corporate environments.

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

Steps:

1. Enter UPnP™ settings interface.

Configuration > Network > Basic Settings > NAT

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



You can edit the Friendly Name of the camera. This name can be detected by corresponding device, such as a router.

3. Set the port mapping mode:

To port mapping with the default port numbers:

Choose **Port Mapping Mode**

To port mapping with the customized port numbers:

Choose **Port Mapping Mode**

And you can customize the value of the port number by yourself.

Enable UPnP™
 Nickname: ✔

Port Mapping Mode

Port Type	External Port	External IP Address	Internal Port	Status
HTTP	80	0.0.0.0	80	Valid
RTSP	554	0.0.0.0	554	Valid
Server Port	8000	0.0.0.0	8000	Valid

Figure 6-6 Port Mapping Mode

4. Click  to save the settings.

6.1.2 Advanced Settings

Configuring SNMP Settings

Purpose:

You can use SNMP to get camera status and parameters related information.

Before you start:

Before setting the SNMP, use 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.



The SNMP version you select should be the same as that of the SNMP software.

Steps:

1. Enter SNMP settings interface:

Configuration > Network > Advanced Settings > SNMP

The screenshot displays the SNMP configuration interface, organized into three sections:


- SNMP v1/v2:**
 - Enable SNMPv1
 - Enable SNMP v2c
 - Read SNMP Community:
 - Write SNMP Community:
 - Trap Address:
 - Trap Port:
 - Trap Community:
- SNMP v3:**
 - Enable SNMPv3
 - Read UserName:
 - Security Level:
 - Authentication Algorithm: MDS SHA
 - Authentication Password:
 - Private-key Algorithm: DES AES
 - Private-key password:
 - Write UserName:
 - Security Level:
 - Authentication Algorithm: MDS SHA
 - Authentication Password:
 - Private-key Algorithm: DES AES
 - Private-key password:
- SNMP Other Settings:**
 - SNMP Port:

Figure 6-7 SNMP Settings

2. Check the corresponding version checkbox (**Enable SNMP v1**, **Enable SNMP v2c**, **Enable SNMP v3**) to enable the feature.
3. Configure the SNMP settings.



The configuration of the SNMP software should be the same as the settings you configure here.

4. Click  to save and finish the settings.

Configuring FTP Settings**Purpose:**

You can set a FTP server and configure the following parameters for uploading captured pictures.

Note:

FTP function is invalid when the sub-stream is enabled

Steps:

5. Enter the FTP settings interface:

Configuration > Network > Advanced Settings > FTP

Server Address	0.0.0.0
Port	21
User Name	<input type="text"/> <input type="checkbox"/> Anonymous
Password	<input type="password"/>
Confirm	<input type="password"/>
Directory Structure	Save in the root directory
Picture Filing Interval	OFF Day(s)
Picture Name	Default
	<input type="checkbox"/> Upload Picture
	<input type="button" value="Test"/>

Figure 6-8 FTP Settings

6. Configure the FTP settings, including server address, port, user name, password, directory, and upload type.



The server address supports both the domain name and IP address formats.



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

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

- ◆ **Root directory:** The files will be saved in the root of FTP server.
- ◆ **Parent directory:** The files will be saved in a folder in FTP server. The name of folder can be defined as shown in Figure 6-9.

Use Device Name
Use Device Name
Use Device Number
Use Device IP address
Custom

Figure 6-9 Parent Directory

- ◆ **Child directory:** It is a sub-folder which can be created in the parent directory. The files will be saved in a sub-folder in FTP server. The name of folder can be defined as shown in Figure 6-10.

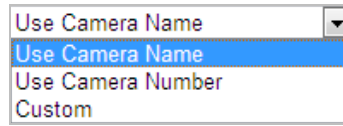


Figure 6-10 Child Directory

- **Upload type:** To enable uploading the captured picture to the FTP server.
7. Click **Save** to save the settings.
 8. You can click **Test** to confirm the configuration.



If you want to upload the captured pictures to FTP server, you also have to enable the continuous snapshot or event-triggered snapshot in **Snapshot** interface.

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:

Configure the DNS Server settings under **Configuration > Network > Basic Settings > TCP/IP** before using the Email function.

Steps:

1. Enter Email settings interface:

Configuration > Network > Advanced Settings > Email

Sender	<input type="text"/>
Sender's Address	<input type="text"/>
SMTP Server	<input type="text"/>
SMTP Port	<input type="text" value="25"/>
E-mail Encryption	<input type="text" value="None"/> ▼
<input type="checkbox"/> Attached Image	
Interval	<input type="text" value="2"/> ▼ s
<input type="checkbox"/> Authentication	
User Name	<input type="text"/>
Password	<input type="text"/>
Confirm	<input type="text"/>

Receiver			
No.	Receiver	Receiver's Address	Test
1			<input type="button" value="Test"/>
2			

Figure 6-11 Email Settings

2. Configure the following settings:

Sender: The name of the email sender.

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

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

SMTP Port: The SMTP port. The default TCP/IP port for SMTP is 25.

E-mail 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.



STARTTLS protocol must be supported by the email server for e-mail encryption with STARTTLS. When it is not supported by the email server and **Enable STARTTLS** is checked, the email will not be encrypted.

Attached Image: Check **Attached Image** if you want to send emails with attached alarm images.



Attached Image function is invalid when sub-stream is enabled.

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



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

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

Receiver: The name of the user to be notified.

Receiver's Address: The email address of user to be notified. (Optional: click **Test** to make sure that the email server can send email out.)

3. Click  to save the settings.


Configuring Platform Settings

Purpose:

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

Steps:

1. Enter Platform 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 access type, and set the related parameters.
4. Click  to save the settings.

Configuring HTTPS Settings

Purpose:

HTTPS is consisted by SSL&HTTP. It is used for encryption transmission, identity authentication network protocol which enhances the security of WEB accessing.



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

Steps:

1. Enter HTTPS settings interface.

Configuration > Network > Advanced Settings > HTTPS

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

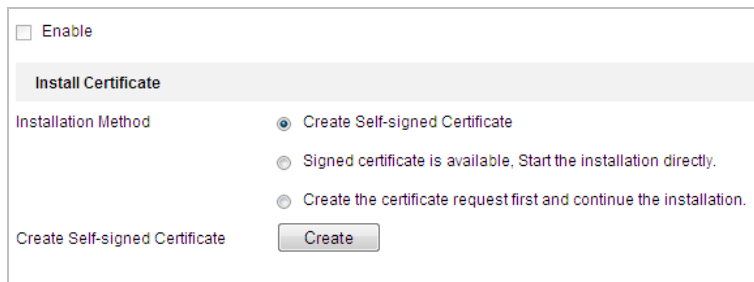


Figure 6-12 Create Certificate

OPTION 1: Create the self-signed certificate

- 1) Select Create Self-signed Certificate.
- 2) Click **Create** to create the following dialog box.

Figure 6-13 Create Self-signed Certificate

- 3) Input the country, host name/IP, validity and other information.
- 4) Click **OK** to save the settings.

OPTION 2: Start the installation when signed certificate is available.

- 1) Select Signed certificate is available, Start the installation directly.
- 2) Click **Browse** to upload the available certificate.
- 3) Click **Install** button to install the certificate.
- 4) Click **OK** to save the settings.

OPTION 3: Create certificate request first and continue the installation.

- 1) Select Create certificate request first and continue the installation.
 - 2) Click **Create** to create the certificate request, and fulfill the required information.
 - 3) Download the certificate request and submit it to the trusted certificate authority for signature.
 - 4) After receiving the signed valid certificate, import the certificate to the device.
 - 5) Click **OK** to save the settings.
3. There will be the certificate information after you successfully create and install the certificate.

Figure 6-14 Installed Certificate Property



- The default port number of HTTPS is 443. The port value ranges from 1 to 65535.
- When the port number is the default number 443, the format of the URL is **https://IP address**, eg., https://192.168.1.64.

- When the port number is not the default number 443, the format of the URL is **https://IP address:port number**, eg., https://192.168.1.64:81.

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 QoS settings interface:

Configuration > Advanced Configuration > Network > QoS

Video/Audio DSCP	<input type="text" value="0"/>
Event/Alarm DSCP	<input type="text" value="0"/>
Management DSCP	<input type="text" value="0"/>

Figure 6-15 QoS Settings

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

The valid DSCP value ranges from 0 to 63. The DSCP value is bigger, the priority is higher.

3. Click  to save the settings.



- Make sure that you enable the QoS function of your network device (such as a router).
- It will ask for a reboot for the settings to take effect.

Configuring 802.1X Settings

Purpose:

The camera supports IEEE 802.1X standard.

IEEE 802.1X is a port-based network access control. It enhances the security level of the LAN. When devices connect to this network with IEEE 802.1X standard, the authentication is needed. If the authentication fails, the devices don't connect to the network.

The protected LAN with 802.1X standard is shown in Figure 6-16.

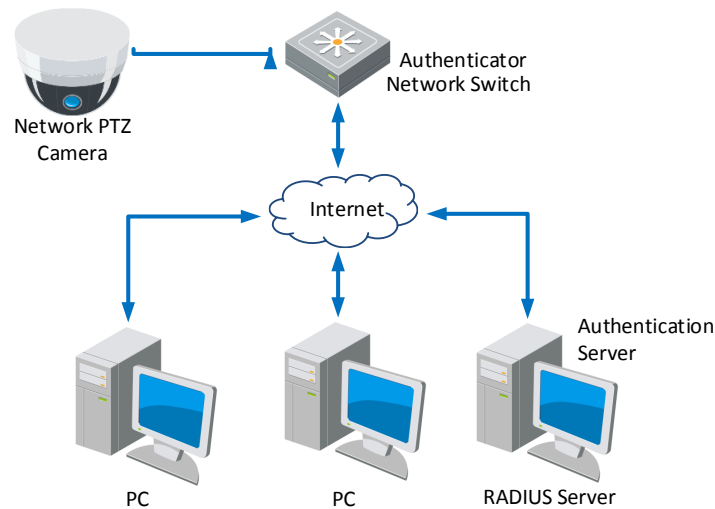


Figure 6-16 Protected LAN

- Before connecting the Network Camera to the protected LAN, apply a digital certificate from a Certificate Authority.
- The network camera requests access to the protected LAN via the authenticator (a switch).
- The switch forwards the identity and password to the authentication server (RADIUS server).
- The switch forwards the certificate of authentication server to the network camera.
- If all the information is validated, the switch allows the network access to the protected network.



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

Steps:

1. Connect the network camera to your PC directly with a network cable.
2. Enter 802.1X settings interface:

Configuration > Network > Advanced Settings > 802.1X

<input type="checkbox"/>	Enable IEEE 802.1X
Protocol	EAP-MD5
EAPOL version	1
User Name	<input type="text"/>
Password	<input type="password"/>
Confirm	<input type="password"/>

Figure 6-17 802.1X Settings

3. Check **Enable IEEE 802.1X** to enable it.
4. Configure the 802.1X settings, including user name and password.



The EAP-MD5 version must be identical with that of the router or the switch.

5. Click  to finish the settings.



The camera reboots when you save the settings.

6. After the configuration, connect the camera to the protected network.

6.2 Configuring Video and Audio Settings

6.2.1 Configuring Video Settings

Steps:

1. Enter Video settings interface:

Configuration > Video/Audio > Video


Channel No.	Camera 1	▼
Stream Type	Main Stream(Normal)	▼
Video Type	Video Stream	▼
Resolution	1920*1080P	▼
Bitrate Type	Variable	▼
Video Quality	Medium	▼
Frame Rate	25	▼ fps
Max. Bitrate	2048	Kbps
Video Encoding	H.265	▼
Profile	Main Profile	▼
I Frame Interval	50	
Smoothing		50 [Clear<->Smooth]

Figure 6-18 Configure Video Settings

2. Select the camera channel to configure.
3. Select the **Stream Type** of the camera to main stream (normal) or sub-stream. The main stream is usually for recording and live viewing with good bandwidth, and the sub-stream can be used for live viewing when the bandwidth is limited. Refer to the **Section 4.1 Configuring Local Parameters** for switching the main stream and sub-stream for live viewing.



Sub-stream is not supported by certain camera models.

4. You can customize the following parameters for the selected stream.



The parameters vary depending on different camera models.

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:

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. The higher value corresponds to the higher video quality, but the higher bandwidth is required.

Video Encoding:

Select **Video Encoding** from the dropdown list for different stream type.

Profile:

Basic Profile, Main Profile and High Profile are selectable.

I Frame Interval:

Set the I-Frame interval from 1 to 250.

SVC:

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

Smoothing:

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

5. Click  to save the settings.

6.2.2 Configuring Audio Settings

Steps:

1. Enter Audio settings interface
Configuration > Video/Audio > Audio

Audio Encoding	G.711ulaw
Audio Input	LineIn
Input Volume	<input type="range" value="50"/>
Environmental Noise Filter	OFF

Figure 6-19 Audio Settings

- Configure the following settings.

Audio Encoding: G.722.1, G.711ulaw, G.711alaw, MP2L2, and G.726 are selectable.

Audio Input: When an intercom is connected to the camera, you need to set this option to **LineIn**.

Audio Stream Bitrate: When the Audio Encoding is selected as MP2L2, you can configure the Audio Stream Bitrate in the dropdown list. The greater the value is, the better the audio quality will be.

Sampling Rate: When the Audio Encoding is selected as MP2L2, you can configure the Sampling Rate in the dropdown list. The greater the value is, the better the audio quality will be.

Input Volume: Slid the **bar** to turn up/down the volume. The value ranges from 0 to 100.

Environmental Noise Filter: Select ON or OFF in the dropdown list to enable or disable the function. It's recommended to enable the function when sampling rate is lower than 32 kHz.

- Click  to save the settings.

6.2.3 Configuring ROI Settings

Purpose:

ROI (Region of Interest) encoding is used to enhance the quality of images which are specified in advance. When **Fixed Region** is enabled, image quality of ROI area will be enhanced and image quality of other areas will be reduced.



ROI function varies depending on different camera models.

Enter ROI settings interface:

Configuration >Video/Audio > ROI

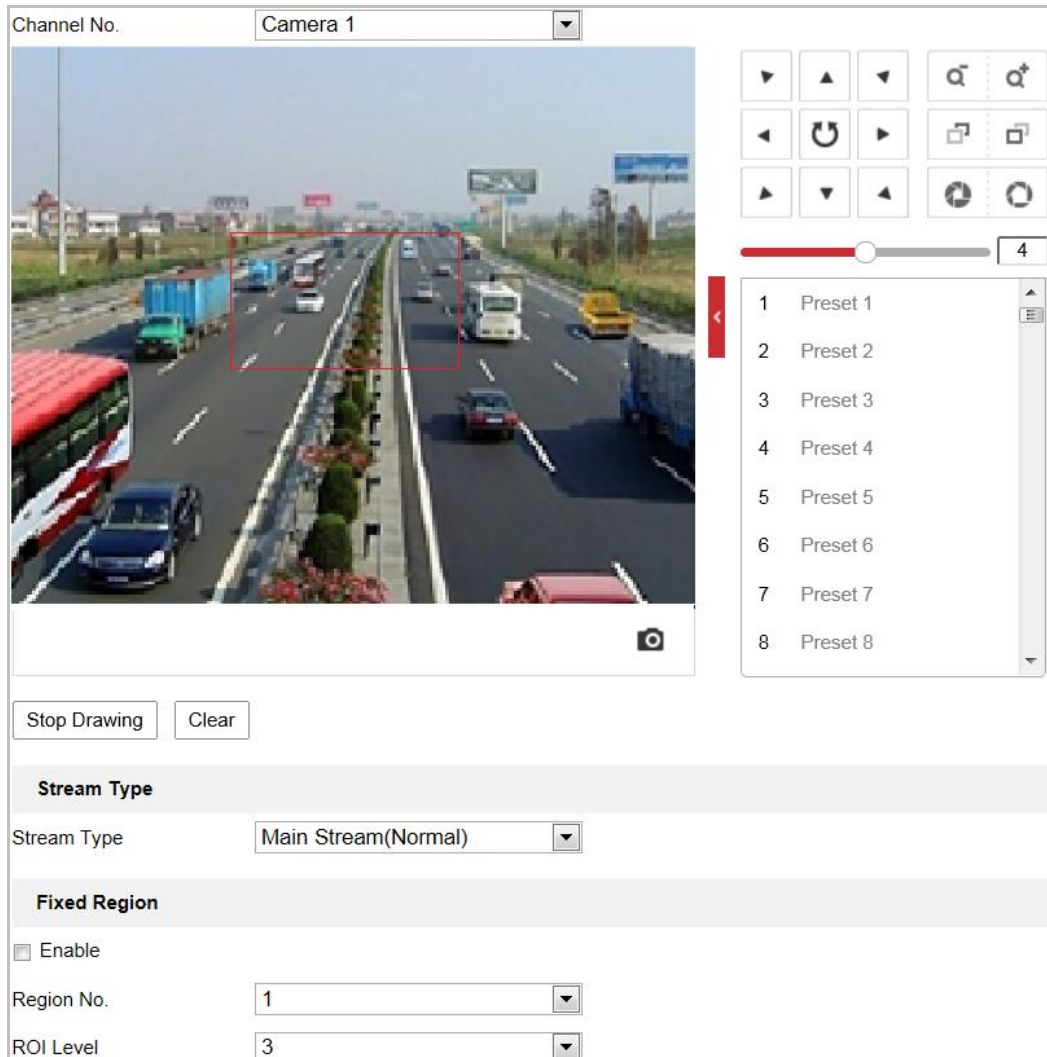


Figure 6-20 Region of Interest

Steps:

1. Select the camera channel to configure.
2. Check **Enable** to enable the **Fixed Region** function.
3. Select a stream type from the dropdown list.
4. Click **Draw Area** and then drag the mouse to draw a red frame in the live view image. You can click **Clear** to clear it.



The number of areas supported in ROI function varies depending different camera models



5. Select the **Region No.** from the dropdown list.
6. Adjust the **ROI level** from 1 to 6. The higher the value, the better image quality in the red frame.
7. Enter a **Region Name**.
8. Click **Save** to save the settings.

6.2.4 Display Info. on Stream

Check **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.

6.3 Configuring Image Settings



- On the event configuration page, click  to show the PTZ control panel or click  to hide it.
- Click the direction buttons to control the pan/tilt movements.
- Click the zoom/iris/focus buttons to realize lens control.
- The functions vary depending on different camera models.

6.3.1 Configuring Display Settings

Purpose:

Configure the image adjustment, exposure settings, focus, day/night switch, backlight settings, white balance, image enhancement, video adjustment, and other parameters in display settings.



- The parameters in **Display Settings** interface vary depending on different camera models.
- You can double click the live view to enter full screen mode and double click it again to exit.

Steps:

1. Enter Display Settings interface:

Configuration > Image > Display Settings

2. Select the camera channel to configure.
3. You can select the **Scene** from the dropdown list with different predefined image parameters.
4. Set the image parameters of the camera.

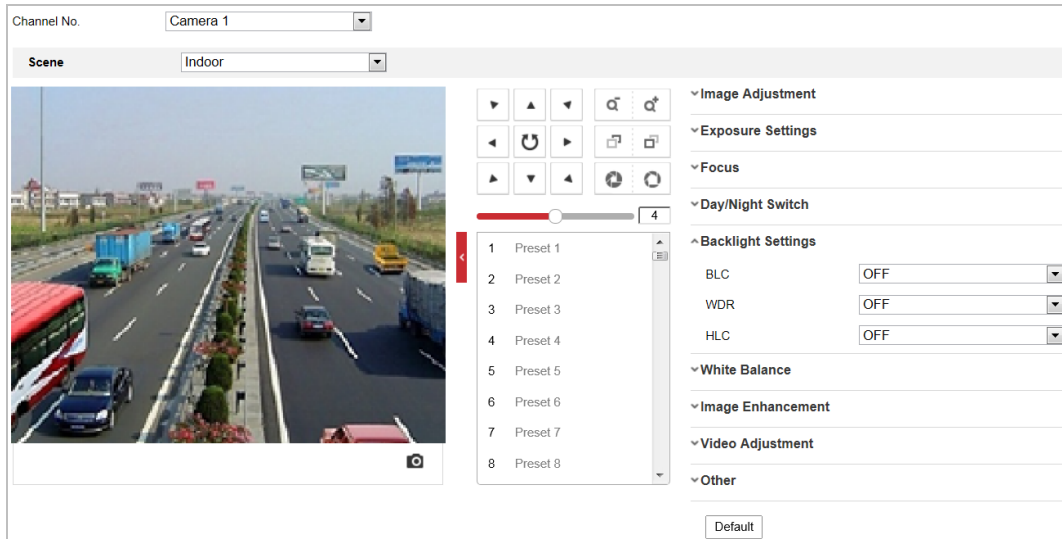


Figure 6-21 Display Settings

Image Adjustment

- **Brightness**

This feature is used to adjust brightness of the image. The value ranges from 0 to 100.

- **Contrast**

This feature enhances the difference in color and light between parts of an image. The value ranges from 0 to 100.

- **Saturation**

This feature is used to adjust color saturation of the image. The value ranges from 0 to 100.

- **Sharpness**

Sharpness function enhances the detail of the image by sharpening the edges in the image. The value ranges from 0 to 100.

Exposure Settings

- **Exposure Mode**

The **Exposure Mode** can be set to **Auto**, and **Manual**.

- ◆ **Auto:**

The iris, shutter and gain values will be adjusted automatically according to the brightness of the environment.

- ◆ **Manual:**

In **Manual** mode, you can adjust the values of **Shutter**, **Gain**, and **Limit Gain** manually.

Focus Settings

- **Focus Mode**

The **Focus Mode** can be set as **Manual**, and **Semi-auto**.

- ◆ **Semi-auto:**

The camera focuses automatically only once after panning, tilting and zooming.

◆ **Manual:**

In **Manual** mode, you need to use   on the control panel to focus manually.

Day/Night Switch

- **Day/Night Switch**

The **Day/Night Switch** mode can be set to **Auto**, **Day**, **Night** and **Scheduled-Switch**.



This function varies depending on the models of camera.

◆ **Auto:**

In **Auto** mode, the day mode and night mode can switch automatically according to the light condition of environment.



Figure 6-22 Auto Mode Sensitivity

◆ **Day:**

In **Day** mode, the camera displays color image. It is used for normal lighting conditions.

◆ **Night:**

In **Night** mode, the image is black and white. **Night** mode can increase the sensitivity in low light conditions.

◆ **Scheduled-Switch:**

In **Schedule** mode, you can set the time schedule for day mode as shown in Figure 6-23.

The rest time out of the schedule is for night mode.

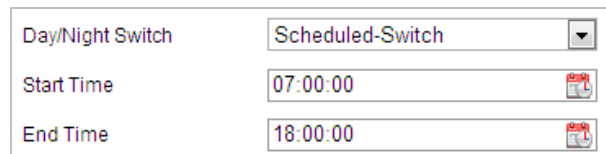


Figure 6-23 Day Night Schedule

Backlight Settings

- **BLC (Back Light Compensation)**

If there's a bright backlight, the subject in front of the backlight appears silhouetted or dark. Enabling **BLC** (back light compensation) function can correct the exposure of the subject. But the backlight environment is washed out to white.

- **WDR (Wide Dynamic Range)**

The wide dynamic range (WDR) function helps the camera provide clear images even under back light circumstances. When there are both very bright and very dark areas simultaneously in the field of view, WDR balances the brightness level of the whole image and provide clear images with details.

You can enable or disable the WDR function. The wide dynamic level ranges from 0 to 100.

- **HLC**

HLC (High Light Compensation) makes the camera identify and suppress the strong light sources that usually flare across a scene. This makes it possible to see the detail of the image that would normally be hidden.

White Balance

The **White Balance** mode can be set to **Auto**, **MWB**, **Outdoor**, **Indoor**, **Fluorescent Lamp**, **Sodium Lamp** and **Auto-tracking**.

- ◆ **Auto:**

In **Auto** mode, the camera retains color balance automatically according to the current color temperature.

- ◆ **Manual White Balance:**

In **MWB** mode, you can adjust the color temperature manually to meet your own demand as shown in Figure 6-24.

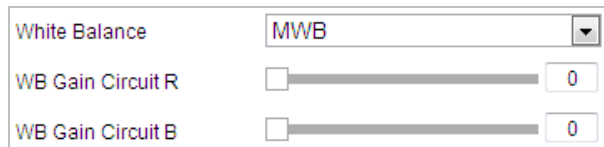


Figure 6-24 Manual White Balance

- ◆ **Outdoor**

You can select this mode when the camera is installed in outdoor environment.

- ◆ **Indoor**

You can select this mode when the camera is installed in indoor environment.

- ◆ **Fluorescent Lamp**

You can select this mode when there are fluorescent lamps installed near the camera.

- ◆ **Sodium Lamp**

You can select this mode when there are sodium lamps installed near the camera.

- ◆ **Auto-tracking**

In **Auto-tracking** mode, white balance is continuously being adjusted in real-time according to the color temperature of the scene illumination.

Image Enhancement

- **3D Digital Noise Reduction**

You can set **Digital Noise Reduction** function to **Normal** and adjust the **Noise Reduction Level** as shown in Figure 6-25. The level ranges from 0 to 100.

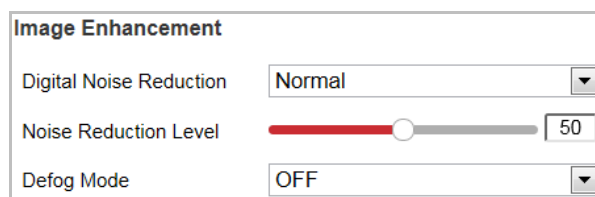


Figure 6-25 3D Digital Noise Reduction-Normal Mode

If you are a professional technician, you can set it to **Expert Mode** then adjust **Space DNR Level** and **Time DNR Level**. The level ranges from 0 to 100.

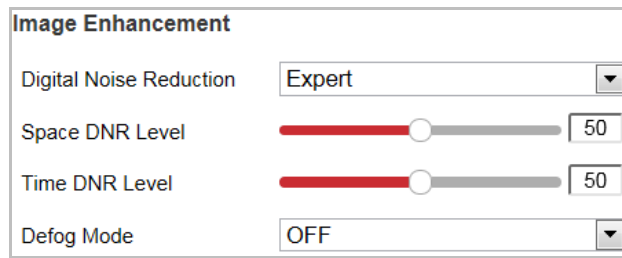


Figure 6-26 3D Digital Noise Reduction-Expert Mode

- **Defog Mode**

You can set the **Defog Mode** to ON or OFF as you need.

Video Adjustment



The functions vary depending on different camera models.

- **Mirror**

If you turn the **MIRROR** function on, the image will be flipped. It is like the image in the mirror. The flip direction can be set to OFF or CENTER.

- **Video Standard**

You can set the **Video Standard** to 50 Hz (PAL) or 60 Hz (NTSC) according to the video system in your country.

- **Capture Mode**

You can disable this function or select the capture mode from the list.

Other



The functions vary depending on different camera models.

- **Lens Initialization**

The lens operates the movements for initialization when you enable **Lens Initialization**.

- **Zoom Limit**

You can set **Zoom Limit** value to limit the maximum value of zooming. The value can be selected from the list.

6.3.2 Configuring OSD Settings

Purpose:

Configure the following on screen displays.

Steps:

1. Enter OSD settings interface:

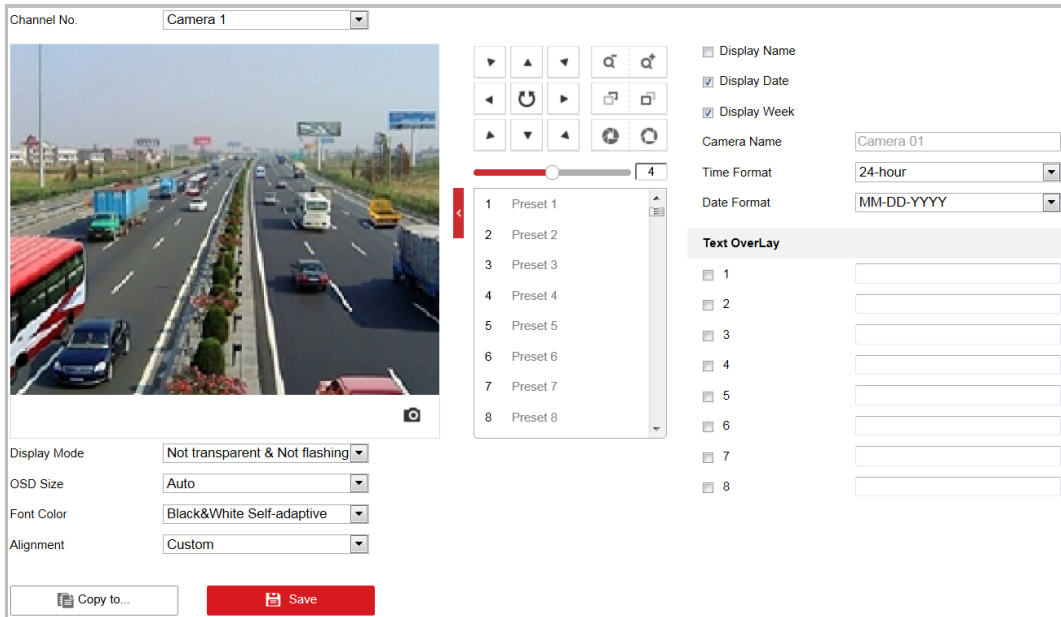

Configuration > Image > OSD Settings

Figure 6-27 OSD Settings


2. Check the corresponding checkbox to select the display of camera name, date or week if required.
3. Edit the camera name in the text field of **Camera Name**.
4. Select from the dropdown list to set the time format, date format, display mode, OSD size, font color, and alignment.
5. You can use the mouse to drag the text frame in the live view window to adjust the OSD position.
6. Click  to activate above settings.

6.3.3 Configuring Text Overlay Settings

Purpose:

You can customize the text overlay.

Steps:

1. Enter Text Overlay settings interface:
Configuration > Image > OSD Settings
2. Check the checkbox in front of textbox to enable the on-screen display.
3. Input the characters in the textbox.
4. Use the mouse to drag the red text frame in the live view window to adjust the text overlay position.
5. Click  to save the settings.

6.3.4 Configuring Privacy Mask

Purpose:


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

Steps:

1. Enter Privacy Mask setting interface
Configuration > Image > Privacy Mask
2. Select the camera channel to configure.



You can only configure privacy mask function for panoramic camera in this interface.

3. Check **Enable Privacy Mask** to enable the function.
4. Click **Draw Area**.
5. Drag the mouse in the live view window to draw the mask area.
6. Click **Stop Drawing** to finish drawing or click **Clear All** to clear all of the areas you set without saving them.
7. Click  to save the settings.

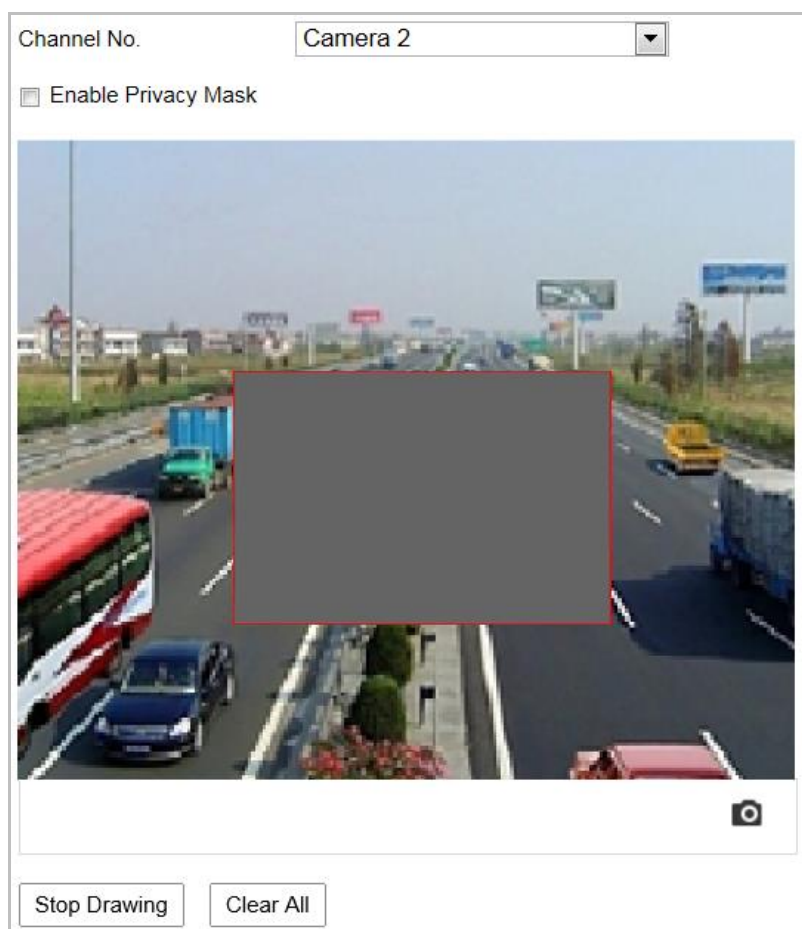


Figure 6-28 Configuring Privacy Mask

6.3.5 Configuring Image Parameters Switch



This function varies depending on different camera models

Purpose:

You can configure **Link to Preset** or **Scheduled-Switch** in this interface. **Link to Preset:** Set the time period and linked scene for the preset and check the corresponding checkbox to go to the linked scene in the configured time period. **Scheduled-Switch:** Set the time period and linked scene and it will go to the linked scene in the configured time period when you check the corresponding checkbox.

Steps:

1. Enter Image Parameters Switch interface:

Configuration > Image > Image Parameters Switch


2. Check **Link to Preset** or **Scheduled-Switch** to enable the function. (Only one function can be enabled in the same time.)
3. When you enable the function of **Link to Preset**, select one preset from the dropdown list, check the corresponding checkbox, set the time period and the linked scene for the selected preset. (Up to 4 periods can be configured for one preset.)

Figure 6-29 Link to Preset

Figure 6-30 Linked Scene

4. When you enable the function of **Scheduled-Switch**, check the corresponding checkbox, set the time period and the linked scene.

Figure 6-31 Schedule-Switch

5. Click  to save the settings.



The two functions are not enabled by default.

6.4 Configuring System Settings

6.4.1 System Settings

Viewing Basic Information

Enter 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 camera, such as Model, Serial No., Firmware Version, Encoding Version, Web Version, Plugin 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.

Device Name	<input type="text"/>
Device No.	<input type="text"/>
Model	<input type="text"/>
Serial No.	<input type="text"/>
Firmware Version	<input type="text"/>
Encoding Version	<input type="text"/>
Web Version	<input type="text"/>
Plugin Version	<input type="text"/>
Number of Channels	<input type="text"/>
Number of HDDs	<input type="text"/>
Number of Alarm Input	<input type="text"/>
Number of Alarm Output	<input type="text"/>

Figure 6-32 Device Information

Time Settings

Purpose:

You can follow the instructions in this section to configure the time which can be displayed on the video. There are Time Zone, Time Synchronization, and Daylight Saving Time (DST) functions for setting the time. Time Synchronization consists of auto mode by Network Time Protocol (NTP) server and manual mode.

Enter Time Settings interface:

Configuration > System > System Settings > Time Settings

Figure 6-33 Time Settings

● Configuring Time Synchronization by NTP Server

Steps:

(1) Check the radio button 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 by NTP server. It can be set from 1 to 10080 minutes.

Figure 6-34 Time Sync by NTP Server

You can click  to make sure that the NTP server is connected.




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.

● Configuring Time Synchronization Manually

Steps:

(1) Check the **Manual Time Sync** radio button.

(2) Click  to set the system time from the pop-up calendar.

(3) Click  to save the settings.



You can also check **Sync with local time** to synchronize the time of the camera with the time of your computer.

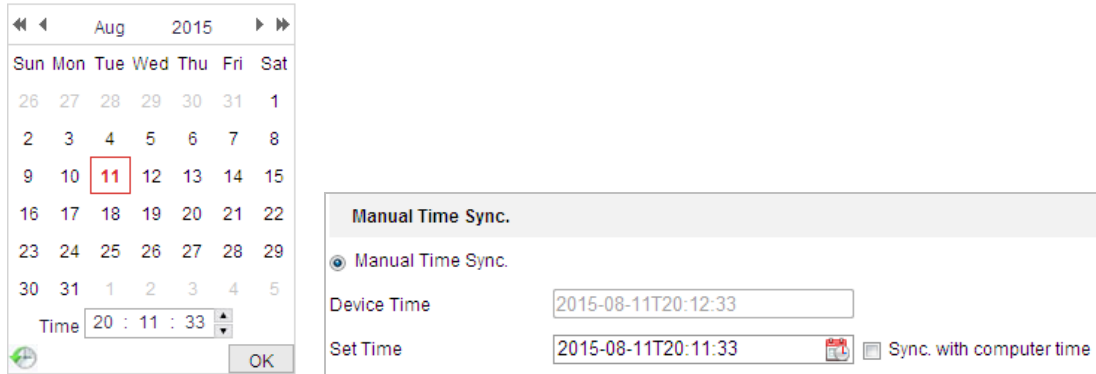


Figure 6-35 Time Sync Manually

● Select the Time Zone

Purpose:

When the camera is taken to another time zone, you can use the **Time Zone** function to adjust the time. The time will be adjusted according to the original time and the time difference between the two time zones.

From the **Time Zone** dropdown menu as shown in Figure 6-36, select the Time Zone in which the camera locates.

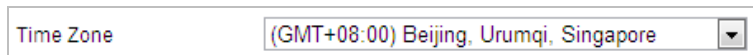


Figure 6-36 Time Zone Settings

Configuring DST (Daylight Saving Time)

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.

If there is the habit of adjusting clocks forward in your country in certain time period of a year, you can turn this function on. The time will be adjusted automatically when the Daylight Saving Time (DST) comes.

Steps:

1. Enter DST settings interface

Configuration > Advanced Configuration > System > DST

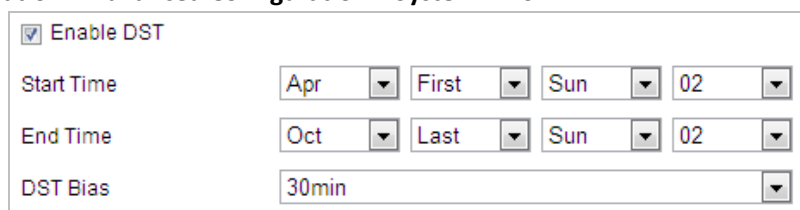



Figure 6-37 DST Settings

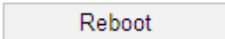
2. Check **Enable DST** to enable the DST function.
3. Set the date of the DST period.
4. Click  to save the settings.

6.4.2 Maintenance

Upgrade & Maintenance

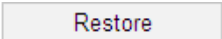
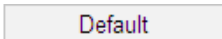
● Rebooting the Camera

Steps:


1. Enter Maintenance interface:
2. **Configuration > System > Maintenance > Upgrade & Maintenance:**
3. Click  to reboot the network camera.

● Restoring Default Settings

Steps:

1. Enter Maintenance interface:
Configuration > System > Maintenance > Upgrade & Maintenance:
2. Click  or  to restore the default settings.



Clicking  restores all the parameters to default settings including the IP address and user information. Use this button with caution.

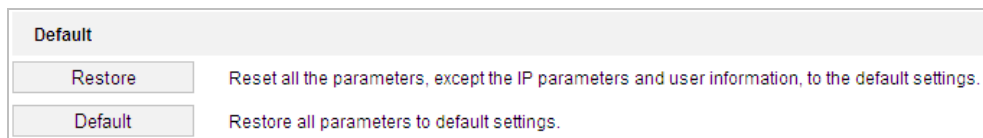


Figure 6-38 Restore Default Settings

● Exporting Configuration File

Steps:

1. Enter Maintenance interface:
Configuration > System > Maintenance > Upgrade & Maintenance
2. Click **Device Parameters** and set the encryption password to export the current configuration file.
3. Set the saving path to save the configuration file in local storage.
4. Click **Diagnose Information** to download the log and system information.

● Importing Configuration File

1. Enter Maintenance interface:
Configuration > System > Maintenance > Upgrade & Maintenance

2. Click **Browse** to select the saved configuration file.
3. Input the encryption password you have set when exporting the configuration file.
4. Click **Import** to import configuration file.



You need to reboot the camera after importing configuration file.

● Upgrading the System

Steps:

1. Enter Maintenance interface:
Configuration >System > Maintenance > Upgrade & Maintenance
2. Select Firmware or Firmware Directory.
 - **Firmware:** when you select **Firmware**, you need to find the firmware in your computer to upgrade the device.
 - **Firmware Directory:** You need to find the directory where the firmware locates. The device can find the firmware in the directory automatically.
3. Click **Browse** to select the local upgrade file and then click **Upgrade** to start remote upgrade.



The upgrading process will take 1 to 10 minutes. Don't disconnect power of the camera during the process. The camera reboots automatically after upgrading.

Log Searching

Purpose:

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

Before you start:

Configure network storage for the camera or insert a memory card in the camera.

Steps:

1. Enter Log interface:
Configuration >System > Maintenance > Log

Upgrade & Maintenance **Log** System Service

Major Type: All Types Minor Type: All Types

Start Time: 2015-08-11 00:00:00 End Time: 2015-08-11 23:59:59 Search

Log List Export

No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP

Total 0 Items << < 0/0 > >>

Figure 6-39 Log Searching Interface

- Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time as shown in Figure 6-39.
- Click **Search** to search log files. The matched log files will be displayed on the **Log** interface.
- To export the log files, click **Save Log** to save the log files in your computer.

System Service

Steps:

- Enter the interface of configuring the remote connection:
Configuration > System > Maintenance > System Service
- Check the checkbox to enable supplement light function if the device supports the function.
- Input a number in text field as the upper limit of the remote connection number. E.g. when you specify the remote connection number as 10, then the 11th remote connection cannot be established.
- Check or uncheck **Enable Sub Stream** to enable/disable the sub-stream.
- Click **Save** to save the settings.


6.4.3 Security

Configuring Authentication Security

Purpose:

You can specifically secure the stream data of live view via authentication configuration. RTSP authentication and WEB authentication are supported.

Steps:

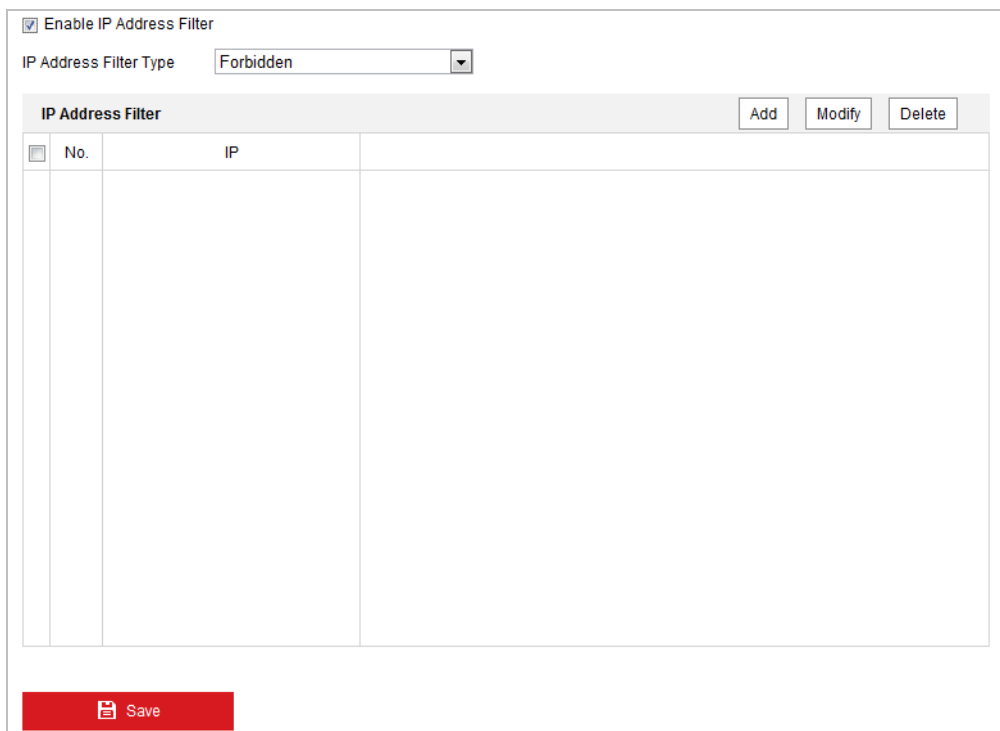
1. Enter the authentication configuration interface:
Configuration > System > Security > Authentication
2. Select the authentication type. Digest is the recommended safer authentication way.
3. Click  to save the settings.

Configuring IP Address Filter**Purpose:**

With this function on, the camera allows certain IP addresses whether to log in or not.

Steps:

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



Enable IP Address Filter

IP Address Filter Type: Forbidden

IP Address Filter Add Modify Delete

<input type="checkbox"/>	No.	IP




Figure 6-40 IP Address Filter

2. Check **Enable IP Address Filter**.
3. Select the type of IP Address Filter in the dropdown list, Forbidden and Allowed are selectable.
4. Set the IP Address Filter list.

- **Add an IP Address**

Steps:

- (1) Click **Add** to add an IP.
- (2) Input the IP Address.



Figure 6-41 Add an IP

(3) Click **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 6-42 Modify an IP

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


- **Delete an IP Address**

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

5. Click  to save the settings.

Configure Security Service Settings

Steps:

1. Enter Security Service interface:
Configuration > System > Security > Security Service
2. Check **SSH** to enable the function.
3. Check **Illegal Login Lock** to enable the function.
Illegal Login Lock: Enabling illegal login lock function is to automatically lock the device IP after the admin user performing 7 failed password attempts (5 attempts for the user/operator).
4. Click  to save the settings.

6.4.4 User Management

Enter User Management interface:

Configuration > System > User Management

The **admin** user has access to create, modify or delete other accounts. Up to 32 user accounts can be created.

User Management		
User List		
No.	User Name	Level
1	admin	Administrator

Figure 6-43 User Information

● Add a User

Steps:

1. Click to add a user.
2. Input the new **User Name**, select **Level** and input **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 level indicates the permissions you give to the user. You can define the user as **Operator** or **User**.

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

Add user

User Name: user1 ✓

Level: Operator

Password: ●●●●●●●● ✓ Strong

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm: ●●●●●●●● ✓

Select All

Remote: Parameters Settings

Remote: Log Search / Interrogate Wo...

Remote: Upgrade / Format

Remote: Two-way Audio

Remote: Shutdown / Reboot

Remote: Notify Surveillance Center / ...

Remote: Video Output Control

Remote: Serial Port Control

Remote: Live View

Remote: Manual Record

Remote: PTZ Control



Remote: Playback

OK Cancel

Figure 6-44 Add a User

● Modify a User

Steps:

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

Modify user

User Name: user1

Level: Operator

Password: ●●●●●●

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm: ●●●●●●

Select All

- Remote: Parameters Settings
- Remote: Log Search / Interrogate Wo...
- Remote: Upgrade / Format
- Remote: Two-way Audio
- Remote: Shutdown / Reboot
- Remote: Notify Surveillance Center /...
- Remote: Video Output Control
- Remote: Serial Port Control
- Remote: Live View
- Remote: Manual Record
- Remote: PTZ Control
- Remote: Playback

OK Cancel

Figure 6-45 Modify a User

● Delete a User

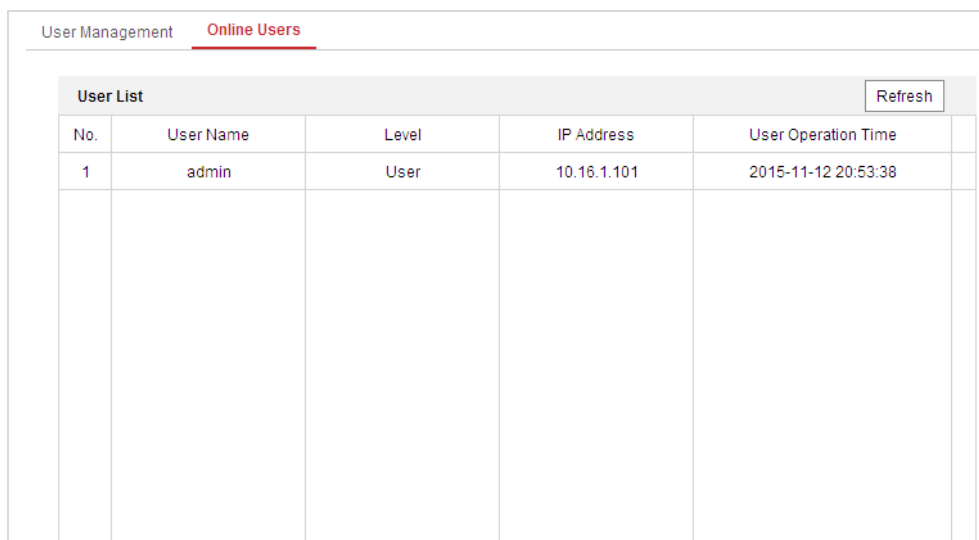
Steps:

1. Left-click the user name you want to delete and click .
2. Click on the pop-up dialogue box to delete the user.

Online Users

Enter Online Users configuration interface:

Configuration > System > User Management > Online Users





The screenshot shows a web interface for 'User Management' with a sub-tab for 'Online Users'. Below the navigation bar is a table titled 'User List' with a 'Refresh' button in the top right corner. The table has five columns: 'No.', 'User Name', 'Level', 'IP Address', and 'User Operation Time'. A single row is visible with the following data: No. 1, User Name 'admin', Level 'User', IP Address '10.16.1.101', and User Operation Time '2015-11-12 20:53:38'.

User List					Refresh
No.	User Name	Level	IP Address	User Operation Time	
1	admin	User	10.16.1.101	2015-11-12 20:53:38	

Figure 6-46 Online Users

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.

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. Input the password of the admin account of the device in the **Password** field and click

 to save the changes.



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

Modify Network Parameters

Enable DHCP
 Enable Hik-Connect

Device Serial No.:

IP Address:

Port:

Subnet Mask:

Gateway:

IPv6 Address:

IPv6 Gateway:

IPv6 Prefix Length:

HTTP Port:

----- Security Verification -----

Admin Password:

[Forgot Password](#)

Figure A.1.2 Modify Network Parameters



See Far, Go Further